Universidad de Cantabria

FACULTAD DE CIENCIAS

El Teorema de Minkowski sobre la equivalencia de formas cuadráticas racionales

(Minkowski's Theorem on the equivalence of rational quadratic forms)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autora: Marina Baltanás Álamo

Director: Jesús Javier Jiménez Garrido

Junio-2024

Agradecimientos

En primer lugar, quiero dar las gracias a mi director, Javier. Por pelearse un poco con el Mac en cada reunión de los martes, estar siempre para preguntarle dudas y por su total dedicación para poder completar esta memoria.

Por supuesto a mi familia por apoyarme siempre desde que empecé la carrera. A Ñaña por interesarse y preguntarme tantas veces hasta entender qué significaba TFG y a Aba por dejarme contárselo, a Elsa y Clau por estar siempre ahí, por ser las primeras en celebrar los aprobados y por los "no pasa nada" en los suspensos. Pero sobretodo, quiero dar las gracias a mi madre, a Jesús también, por consolarme siempre, desde el primer suspenso que llegó a casa en primero hasta el último en cuarto.

Gracias a todos mis amigos por escucharme y apoyarme siempre, a Noelia por aprenderse los nombres de todas mis asignaturas de tanto escucharme y aún así no cansarse de oírme y, cómo no, a mis amigos que ya no "los de la uni". Sin ellos llegar hasta aquí no sé si hubiese sido imposible pero sí sé que más difícil. Por consolarme en los suspensos y motivarme a seguir, alegraros por mi y también por los descansitos que tanto nos gustaban. Me siento muy afortunada por haberos encontrado en este camino y sobretodo orgullosa por acabar esta etapa a vuestro lado.

Gracias a todos.

Resumen

El Teorema de Minkowski establece que una forma cuadrática sobre $\mathbb{Q}$ representa a 0 si y solo si la forma cuadrática representa a 0 sobre $\mathbb{R}$ y $\mathbb{Q}_p$ para todo p primo, es decir, afirma que el Principio Local-global se cumple para la representación de 0 en las formas cuadráticas racionales. El objetivo de este trabajo es proporcionar una demostración del mismo. Para ello, introducimos el cuerpo de los p-ádicos así como las propiedades más relevantes que poseen como el Lema de Hensel y también proporcionamos una serie de resultados de las formas cuadráticas sobre $\mathbb{Q}_p$, que incluye el estudio del símbolo de Hilbert y sus propiedades para poder definir el invariante de Hasse, invariante de las formas cuadráticas sobre los p-ádicos. Como consecuencia de este teorema, se establecen las condiciones necesarias y suficientes para que dos formas cuadráticas sobre $\mathbb{Q}$ sean equivalentes.

Palabras clave: forma cuadrática, símbolo de Hilbert, invariante de Hasse, p-ádicos, Teorema de Minkowski.

Abstract

Minkowski's Theorem states that a quadratic form over $\mathbb{Q}$ represents 0 if and only if the quadratic form represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p, i.e., it states that the Local-global Principle holds for the representation of 0 in rational quadratic forms. The goal of this work is to provide a proof of it. For this porpose, we present the field of the p-adic as well as the most relevant properties they have, like the Hensel's Lemma, and we also provide a series of results of the quadratic forms over $\mathbb{Q}_p$, which includes the study of the Hilbert symbol and its properties for to be able to work with the Hasse invariant, invariant of the quadratic forms on the p-adic. As a consequence of this theorem, the necessary and sufficient conditions are established for two quadratic forms on $\mathbb{Q}$ to be equivalent.

Key words: quadratic form, Hilbert symbol, Hasse invariant, p-adics, Minkowski's Theorem

Índice general

Capítulo 1

Introducción

El estudio de la clasificación de las formas cuadráticas es un problema clásico en las matemáticas y tan relevante que su estudio sobre un espacio vectorial real o complejo se incluye habitualmente en el plan de estudios del Grado en Matemáticas.

El matemático Hermann Minkowski trabajó en las formas cuadráticas y en 1883, la Academia de Ciencias Francesa le otorgó el premio de matemáticas *Grand Prix des Sciences Mathématiques* por demostrar que una forma cuadrática sobre $\mathbb{Q}$ representa a 0 si y solo si lo hace en $\mathbb{Q}_p$ para todo primo p y en $\mathbb{R}$. En 1900, Hilbert propone "resolver ecuaciones cuadráticas con coeficientes en cualquier cuerpo de números algebraico" en el Congreso Internacional de Matemáticos, ver [5]; convirtiéndose en el undécimo problema de los veintitrés propuestos en dicho congreso. En la década de 1920 Helmut Hasse resolvió el problema generalizando el Teorema de Minkowski a cuerpos numéricos, extensiones de grado finito de los números racionales. De hecho, Hasse descubre que el trabajo de Minkowski sobre formas cuadráticas racionales podía simplificarse si se expresaban los resultados empleando los números p-ádicos. Más concretamente, su demostración del Teorema se basa en el Principio Local-global o también Principio de Hasse [2], que consiste en estudiar las soluciones de ecuaciones racionales sobre sus diferentes completaciones, los reales y los cuerpos p-ádicos, $\mathbb{Q}_p$, llamados cuerpos locales. No obstante, y pesar de que para el caso de las formas cuadráticas se cumple el Principio Local-global como veremos en el trabajo, en [2] podemos encontrar situaciones donde no se verifica.

El principal objetivo de este trabajo es introducir las herramientas necesarias, entre otras: el cuerpo de los p-ádicos, $\mathbb{Q}_p$, así como los invariantes de las formas cuadráticas sobre $\mathbb{Q}_p$ y algunas de las caracterizaciones que poseen, para poder realizar la demostración del Teorema de Minkowski. Asimismo, una vez obtenido este resultado, podremos determinar la equivalencia o, en su defecto, la no equivalencia de formas cuadráticas con coeficientes racionales a partir del estudio de las formas cuadráticas sobre cada cuerpo local.

La principal referencia de este trabajo ha sido el libro *A Course in Arithmetic* [9] escrito por el matemático francés Jean-Pierre Serre. En general, se siguen las demostraciones proporcionadas por el autor, aunque se han completado los detalles y se han añadido explicaciones para facilitar su comprensión.

La memoria consta de cuatro capítulos, concluyendo con la demostración del Teorema de Minkowski. En el Capítulo 2 se realiza la construcción del cuerpo de los p-ádicos. Se ha optado por definir los números p-ádicos como el cuerpo de fracciones de los enteros p-ádicos, que por su parte se construyen completando el anillo de los enteros mediante la filtración p-ádica. En este capítulo, se prueban las propiedades topológicas más relevantes de estos números, se muestra cómo obtener soluciones aproximadas de una ecuación polinomial empleando el Lema de Hensel y se estudian el grupo multiplicativo y el subgrupo de cuadrados.

En el Capítulo 3 se recuerdan las nociones fundamentales de la teoría de formas cuadráticas. En particular, destacamos el Teorema de diagonalización, el Teorema de existencia de bases contiguas y el Teorema de Witt que son fundamentales en el estudio de la equivalencia de formas cuadráticas. En este sentido, sabemos que dos formas cuadráticas equivalentes representan los mismos elementos y, aunque el recíproco no es cierto, conocer los elementos representados por una forma cuadrática es fundamental para su clasificación. Por este motivo, el capítulo concluye con una serie de resultados que determinan cuándo una forma cuadrática representa un elemento de un cuerpo.

En el Capítulo 4 nos centramos en el estudio de las formas cuadráticas sobre $\mathbb{Q}_p$. A modo ilustrativo y por su relevancia en las aplicaciones, comenzaremos estableciendo la clasificación de las formas cuadráticas sobre cuerpos finitos. En la siguiente sección introduciremos el símbolo de Hilbert y describiremos algunas de sus propiedades, que nos permitirán probar que el invariante de Hasse está bien definido. Veremos que mediante el rango, el discriminante y el invariante de Hasse se pueden caracterizar los elementos representables por una forma cuadrática en $\mathbb{Q}_p$. Gracias a estos resultados, concluimos el capítulo obteniendo la clasificación de formas cuadráticas en $\mathbb{Q}_p$.

En el último capítulo, trataremos las formas cuadráticas sobre los racionales. Comenzamos repasando los resultados para el caso real. Junto con la información del capítulo previo, estamos en condiciones de poder abordar la demostración del Teorema de Minkowski que constituye el núcleo del capítulo. La memoria concluye con una serie de resultados que se deducen de forma más o menos directa del teorema y con algunos ejemplos ilustrativos.

Finalmente, señalamos que intentando que el trabajo sea lo más completo posible y tratando de agilizar su lectura, se han incluido los resultados auxiliares de Álgebra, Teoría de Números y Topología en el Apéndice A. La mayoría de los resultados del mismo se enuncian sin demostración salvo aquellos que por su relevancia o su singularidad se ha creído conveniente detallar.

Capítulo 2

Números p-ádicos

La construcción del cuerpo de los números p-ádicos que presentamos en este capítulo se basa en construir dicho cuerpo como el cuerpo de fracciones del anillo de los enteros p-ádicos siguiendo las ideas descritas en [9, Capítulo II]. Una vez introducido el cuerpo de los p-ádicos, estudiaremos también algunas de sus propiedades así como su grupo multiplicativo o sus cuadrados.

Notación 2.1. *A lo largo de todo el trabajo vamos a suponer que p es un número natural primo. Denotamos por $A_n = \mathbb{Z}/p^n\mathbb{Z}$ el anillo de los enteros módulo p^n con $n \in \mathbb{N}_{\geq 1}$.*

2.1. Enteros p-ádicos

Para cada $n \in \mathbb{N}_{\geq 2}$, consideremos el siguiente homomorfismo de anillos

$$\begin{array}{rccc} \phi_n : & A_n & \longrightarrow & A_{n-1} \\ & a & \longmapsto & a \bmod p^{n-1} \end{array}$$

que es sobreyectivo y cuyo núcleo es $p^{n-1}A_n$. De este modo, se comprueba de forma directa que la sucesión $(\phi_n)_{n\geq 2}$ de homomorfismos $\phi_n : A_n \longrightarrow A_{n-1}$, es decir, dada por

$$\cdots \xrightarrow{\phi_{n+1}} A_n \xrightarrow{\phi_n} A_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_3} A_2 \xrightarrow{\phi_2} A_1$$

forma un sistema proyectivo de anillos en el sentido de la Definición A.2.

Definición 2.2. *Se define al anillo de los **enteros p-ádicos** como el límite proyectivo del sistema $(A_n, \phi_n)_{n\geq 1}$ y se denota por*

$$\mathbb{Z}_p := \varprojlim (A_n, \phi_n).$$

Por construcción, un elemento de $\mathbb{Z}_p$ es una sucesión $x = (x_1, x_2, \ldots, x_n, \ldots) \in \prod_{n\geq 1} A_n$ y $\phi_n(x_n) = x_{n-1}$ si $n \geq 2$. La suma y la multiplicación en este anillo se definen coordenada a coordenada. Como ϕ_n es un homomorfismo de anillos se tiene que los enteros p-ádicos, $\mathbb{Z}_p$, son un subanillo del anillo producto $\prod_{n\geq 1} A_n$. Además, si dotamos a A_n con la topología discreta, por ser finito, A_n es compacto y dotando a $\prod_{n\geq 1} A_n$ de la topología producto, por el Teorema de Tychonoff (Teorema A.17), es compacto. Así, el anillo $\mathbb{Z}_p$ hereda esta topología y es un espacio compacto, debido a que es cerrado como vamos a probar a continuación.

Lema 2.3. *El conjunto de los enteros p-ádicos, $\mathbb{Z}_p$, es cerrado.*

Demostración. Para ello, veamos que el complementario de $\mathbb{Z}_p$ es abierto. Observamos que los elementos $x = (x_1, x_2, \dots) \in \prod_{n\geq 1} A_n$ tal que $x \notin \mathbb{Z}_p$ son aquellos que cumplen que existe $n \geq 2$ tal que $\phi_n(x_n) \neq x_{n-1}$. Para cada $n \in \mathbb{N}_{\geq 1}$, consideramos la proyección dada por $\pi_n : \prod_{j\geq 1} A_j \longrightarrow A_n$ que es una aplicación continua porque en $\prod_{j\geq 1} A_j$ se considera la topología producto. Para cada $a \in A_n$, el conjunto $\{a\}$ es abierto de A_n y el conjunto $A_{n-1} \setminus \{\phi_n(a)\}$ es abierto de A_{n-1} porque en ambos casos se está considerando la topología discreta. Por lo tanto, si definimos

$$\mathcal{U}_a = \pi_n^{-1}(\{a\}) \bigcap \pi_{n-1}^{-1}(A_{n-1} \setminus \{\phi_n(a)\})$$

es abierto por ser intersección de dos abiertos. Para cada $n \in \mathbb{N}_{\geq 2}$, consideramos la unión $\mathcal{U}_n = \bigcup_{a\in A_n} \mathcal{U}_a$ que es abierto por ser unión de abiertos y su unión $\mathcal{U} = \bigcup_{n\geq 2} \mathcal{U}_n$ es abierto por ser unión de abiertos. Finalmente, observamos que

$$\mathcal{U} = \{x \in \prod_{j\geq 1} A_j : \text{ existe } n \in \mathbb{N}_{\geq 2} \text{ tal que } \pi_{n-1}(x) \neq \phi_n(\pi_n(x))\} = \prod_{j\geq 1} A_j \setminus \mathbb{Z}_p.$$

Por tanto, $\mathbb{Z}_p$ es cerrado. □

En el estudio de los enteros p-ádicos, resulta útil considerar las aplicaciones de multiplicar por p y la proyección sobre la coordenada n dadas por

$$\begin{array}{rccc} p: & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & (x_1, x_2, \dots, x_n, \dots) & \longmapsto & (px_1, px_2, \dots, px_n, \dots) \end{array} \qquad \begin{array}{rccc} \varepsilon_n: & \mathbb{Z}_p & \longrightarrow & A_n \\ & (x_1, x_2, \dots, x_n, \dots) & \longmapsto & x_n \end{array}$$

Observación 2.4. *Además, si abusamos de la notación y consideramos el homomorfismo de anillos*

$$\begin{array}{rccc} p: & A_n & \longrightarrow & A_n \\ & a & \longmapsto & pa \end{array}$$

observamos que $Im(p) = pA_n$ y que $Ker(p) = p^{n-1}A_n$, por lo tanto, $Ker(p) = Ker(\phi_n)$.

El siguiente lema nos muestra que dentro de A_m tenemos un subgrupo isomorfo a A_{m-n} para todo $m > n$.

Lema 2.5. *Para todos $m, n \in \mathbb{N}_{\geq 1}$ con $m > n$ se tiene que*

$$\begin{array}{rccc} \psi_{m,n}: & A_{m-n} & \longrightarrow & p^n\mathbb{Z}/p^m\mathbb{Z} \\ & a \bmod p^{m-n} & \longmapsto & p^n \cdot a \bmod p^m \end{array}$$

es un isomorfismo de grupos, con $A_0 = \{0\}$.

Demostración. Basta considerar la composición de los homomorfismos de grupos

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & p^n\mathbb{Z}_p \\ & x & \longmapsto & p^n x \end{array} \qquad \begin{array}{rccc} g: & p^n\mathbb{Z}_p & \longrightarrow & p^n\mathbb{Z}/p^m\mathbb{Z} \\ & a & \longmapsto & a + p^m\mathbb{Z}. \end{array}$$

Se tiene que $g \circ f$ es sobreyectivo porque f y g lo son.
Además, $Ker(g \circ f) = \{x \in \mathbb{Z} : p^n x \equiv 0 \bmod p^m\} = p^{m-n}\mathbb{Z}$. Por el Primer Teorema de Isomorfía $\psi_{m,n}$ es un isomorfismo de grupos. □

Proposición 2.6. *La sucesión* $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ *es una sucesión exacta de anillos donde la aplicación* p^n *es la composición de la aplicación* p *consigo misma* n *veces.*

Demostración. Para ver que la sucesión es exacta, debemos comprobar que p^n es inyectiva, ε_n es sobreyectiva y que $Im(p^n) = Ker(\varepsilon_n)$.

En primer lugar, como la composición de aplicaciones inyectivas es inyectiva, basta probar que p es inyectiva. Tomamos $x = (x_n)_{n\geq 1} \in \mathbb{Z}_p$ tal que $p(x) = 0$ y veamos que $x = 0$. Como $p(x) = 0$, tenemos que $px_n = 0$ en A_n para todo $n \in \mathbb{N}_{\geq 1}$ y teniendo en cuenta la Observación 2.4, $x_n \in p^{n-1}A_n = Ker(\phi_n)$. Por lo tanto, como para cada $n \in \mathbb{N}_{\geq 2}$ se tiene que $\phi_n(x_n) = x_{n-1}$ y $x_n \in Ker(\phi_n)$, entonces $x_{n-1} = 0$ para todo $n \in \mathbb{N}_{\geq 2}$. En conclusión, se tiene que $x = 0$.

En segundo lugar, tenemos que la proyección ε_n es sobreyectiva puesto que dado $x_n \in A_n$ y tomamos $x = (x_i)_{i\geq 1}$ tal que

$$x_i = \begin{cases} x_n, & \text{si } i \geq n, \\ \phi_{i+1}(x_{i+1}), & \text{si } i < n, \end{cases}$$

se tiene que $x \in \mathbb{Z}_p$ y $\varepsilon_n(x) = x_n$.

Finalmente, veamos que $Im(p^n) = p^n\mathbb{Z}_p = Ker(\varepsilon_n)$ por doble contenido. Comenzaremos probando la primera igualdad. Si $x \in Im(p^n)$, lo podemos escribir de la forma $x = p^n y$ con $y \in \mathbb{Z}_p$, luego $Im(p^n) \subseteq p^n\mathbb{Z}_p$. Tomamos $x \in p^n\mathbb{Z}_p$, es decir, $x = p^n y$ con $y \in \mathbb{Z}_p$. Por tanto, tenemos que $x = p^n(y)$, $p^n\mathbb{Z}_p \supseteq Im(p^n)$.

Para concluir, probemos la segunda igualdad por doble contenido. De forma directa, se tiene que $p^n\mathbb{Z}_p \subseteq Ker(\varepsilon_n)$ porque $\varepsilon_n(p^n x) = p^n x_n \equiv 0 \bmod p^n$.En sentido contrario, tomamos $x = (x_m)_{m\geq 1} \in Ker(\varepsilon_n)$, luego $x_m \equiv 0 \bmod p^n$ para todo $m \geq n$. Por lo tanto, $x_m \in p^n\mathbb{Z}/p^n\mathbb{Z}$ y por el isomorfismo del Lema 2.5 existe un único $y_{m-n} \in A_{m-n}$ tal que $\psi_{m,n}(y_{m,n}) = x_m$. Observamos que

$$\phi_{m-n}(y_{m-n}) = (\psi^{-1}_{m-1,n} \circ \phi_m \circ \psi_{m,n})(y_{m-n}) = (\psi^{-1}_{m-1,n} \circ \phi_m)(x_m) = \psi^{-1}_{m-1,n}(x_{m-1}) = y_{m-n-1}.$$

En resumen, $\phi_m(y_m) = y_{m-1}$ y, por ello, los y_i definen un elemento $y = (y_i)_{i\geq 1}$ de $\mathbb{Z}_p$ que además verifica $x = p^n y$. Por consiguiente, se tiene que $x \in p^n\mathbb{Z}_p$.
En conclusión, la sucesión es exacta. □

Además, si aplicamos el Primer Teorema de Isomorfía a la función $\varepsilon_n : \mathbb{Z}_p \longrightarrow A_n$ tenemos que

$$\mathbb{Z}_p/Ker(\varepsilon_n) \simeq Im(\varepsilon_n), \text{ es decir, } \mathbb{Z}_p/(p^n\mathbb{Z}_p) \simeq A_n = \mathbb{Z}/p^n\mathbb{Z}.$$

Proposición 2.7. *Un elemento de* $\mathbb{Z}_p$ *es unidad si y solo si no es divisible por* p*. Además, si denotamos por* $\mathbb{U}^p$ *el grupo de las unidades de* $\mathbb{Z}_p$*, todo elemento no nulo de* $\mathbb{Z}_p$ *se puede escribir de forma única como* $p^n u$*, con* $u \in \mathbb{U}^p, n \in \mathbb{N}$*.*

Demostración. Primero, demostraremos la primera parte de la proposición en A_n, es decir, vamos a probar que $x \in A_n$ es unidad si y solo si no es divisible por p.
Sabemos que $U(A_n) = \{x \in A_n : m.c.d(x, p^n) = 1\}$. Como los únicos divisores de p^n son de la forma p^k con $0 \leq k < n$, se tiene que $m.c.d(x, p^n) = 1$ si y solo si $p \nmid x$, luego $U(A_n) = \{x \in A_n : p \nmid x\}$.

A continuación, veamos por doble implicación que el enunciado se cumple en $\mathbb{Z}_p$. Si $x = (x_n)_{n\geq 1} \in \mathbb{Z}_p$ es invertible, como la multiplicación en $\mathbb{Z}_p$ es coordenada a coordenada, su imagen x_n en A_n es invertible, luego $p \nmid x_n$ y por consiguiente, x no es múltiplo de p. Recíprocamente, si x no es múltiplo de p, existe un $n \in \mathbb{N}_{\geq 1}$ tal que la imagen x_n de x en A_n es invertible. Por tanto, existe un elemento $y_n \in A_n$ tal que $x_n y_n = 1$. Como ϕ_n es homomorfismo de anillos, $\phi_n(x_n y_n) = x_{n-1}\phi_n(y_n) = 1$. Por lo tanto, $\phi_n(y_n)$ es el inverso de x_{n-1} y $\phi_n(y_n) = y_{n-1}$. Con ello, x_i es invertible para todo $i \leq n$. Por lo tanto, x_1 es invertible en A_1 y se tiene que $x_1 y_1 = 1$. En consecuencia, para $x_m \in A_m$ con $m \in \mathbb{N}_{\geq 1}$, tenemos que $x_m y_1 \equiv x_1 y_1 \equiv 1 \bmod p$. Esto es, $x_m y_1 = 1 - pz_m$ con $z_m \in \mathbb{Z}$. Consideramos la igualdad

$$(x_m y_1)(1+pz_m+p^2z_m^2+\cdots+p^{m-1}z_m^{m-1}) = (1-pz_m)(1+pz_m+p^2z_n^2+\cdots+p^{m-1}z_m^{m-1}) = 1-p^m z_m,$$

y tomamos módulo p^m, de esta forma tenemos que

$$x_m\Big(y(1+pz_m+p^2z_n^2+\cdots+p^{m-1}z_m^{m-1})\Big) \equiv 1 \bmod p^m,$$

luego x_m es invertible en A_m para todo $m \in \mathbb{N}_{\geq 1}$ y x es unidad en $\mathbb{Z}_p$.

A continuación, probamos la segunda parte. Tomamos $x \in \mathbb{Z}_p$ no nulo, consideramos $n \in \mathbb{N}$, luego $p^n \mid x$ pero $p^{n+1} \nmid x$, esto es que existe un $u \in \mathbb{Z}_p$ tal que $x = p^n u$ y como p no divide a u, u es unidad. La unicidad se deduce por cómo se escoge n. □

El último apartado de la proposición anterior motiva a introducir la noción de valoración p-ádica.

Definición 2.8. *Sea x un elemento no nulo de $\mathbb{Z}_p$ tal que $x = p^n u$ con $u \in \mathbb{U}^p$ y $n \in \mathbb{N}$. Se llama* ***valoración p-ádica*** *de x al número natural n y se denota por $v_p(x)$. Por convenio, escribimos $v_p(0) = \infty$.*

Observación 2.9. *Además, se comprueba que para cualesquiera $x, y \in \mathbb{Z}_p$ la valoración p-ádica verifica*

$$v_p(xy) = v_p(x) + v_p(y), \qquad v_p(x+y) \geq \min(v_p(x), v_p(y)).$$

Lema 2.10. *La aplicación definida para todos $x, y \in \mathbb{Z}_p$ por $d_p(x,y) = p^{-v_p(x-y)}$ es una distancia.*

Demostración. Veamos que $d_p(x,y) = p^{-v_p(x-y)}$ es una distancia, es decir, que para todos $x, y \in \mathbb{Z}_p$ se satisfacen las siguientes propiedades:

I. $d_p(x,y) \geq 0$. Como $v_p(x-y) \geq 0$ y $p > 0$, se tiene que $p^{-v_p(x-y)} \geq 0$.

II. $d_p(x,y) = 0$ si y solo si $x = y$. Por definición, $d_p(x,y) = 0$ si y solo si $v_p(x-y) = \infty$, es decir, si y solo si $x - y = 0$.

III. $d_p(x,y) = d_p(y,x)$. Distinguimos dos casos:
Supongamos sin pérdida de generalidad que $x = 0$ e $y = p^n u$ con $n \in \mathbb{N}$ y $u \in \mathbb{U}^p$. Observamos que $-y = p^n(-u)$ y que $-u \in \mathbb{U}^p$, entonces se tiene que

$$d_p(x,y) = p^{v_p(-y)} = p^{-n} = p^{-v_p(y)} = d_p(y,x).$$

En segundo lugar supongamos que x e y son no nulos. Escribimos $x = p^n u$, $y = p^m v$ con $u, v \in \mathbb{U}^p$, $n, m \in \mathbb{N}$ tales que $n \leq m$. Entonces, se tiene que

$$d_p(x,y) = p^{-v_p(p^n u - p^m v)} = p^{-v_p(p^n(u-p^{m-n}v))} = p^{-n} = p^{-v_p(p^n(p^{m-n}v-u))} = d_p(y,x).$$

IV. $d_p(x,y) \leq d(x,z)_p + d(z,y)_p$. Supongamos que $x, y, z \in \mathbb{Z}_p$ son no nulos tales que $x = p^n u$, $y = p^m v$, $z = p^s w$ con $n, m, s \in \mathbb{N}$ y $u, v, w \in \mathbb{U}^p$, tenemos que

$$d_p(x,y) = \text{máx}(p^{-n}, p^{-m}) \leq \text{máx}(p^{-n}, p^{-s}) + \text{máx}(p^{-s}, p^{-m}) = d_p(x,z) + d_p(z,y).$$

Por otro lado, si alguno es nulo, se tiene que

$$d_p(0,x) = p^{-n} \leq p^{-s} + \text{máx}(p^{-s}, p^{-n}) = d_p(0,z) + d_p(z,x),$$

$$d_p(x,y) = \text{máx}(p^{-n}, p^{-m}) \leq p^{-n} + p^{-m} = d_p(0,x) + d_p(0,y).$$

Análogamente se razona si dos o los tres son nulos y concluimos que d_p es una distancia en $\mathbb{Z}_p$.

□

Observación 2.11. *Los números enteros están contenidos en los enteros p-ádicos a través de la inclusión canónica*

$$\begin{array}{rccl} i: & \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ & x & \longmapsto & (x \ mod\ p, x \ mod\ p^2, x \ mod\ p^3, \dots) \end{array}$$

en donde el conjunto imagen son las sucesiones constantes de un lugar en adelante.

Observamos que hemos dotado a $\mathbb{Z}_p$ con dos topologías, la dada por la distancia d_p y la topología de subespacio heredada de $\prod_{n=1}^{\infty} A_n$, resulta que ambas topologías coinciden.

Proposición 2.12. *La topología de subespacio de $\mathbb{Z}_p$ coincide con la topología dada por la distancia d_p. El anillo de los enteros p-ádicos es un espacio métrico completo en donde $\mathbb{Z}$ es denso.*

Demostración. En primer lugar, veamos que las bolas definidas por esta distancia cumplen

$$\overline{B(0,p^{-n})} = \{x \in \mathbb{Z}_p : d_p(x,0) \leq p^{-n}\} = p^n\mathbb{Z}_p.$$

Para probarlo basta observar que $d_p(x,0) \leq p^{-n}$ si y solo si $p^{-v_p(x)} \leq p^{-n}$ o, equivalentemente, despejando $v_p(x) \geq n$, es decir, $x \in p^n\mathbb{Z}_p$. Además, como $v_p(x) \in \mathbb{N}$, se tiene que las bolas verifican $\overline{B(0,p^{-n})} = B(0,p^{-(n-1)})$. Como las bolas forman un sistema fundamental de entornos de 0, basta probar que coinciden con los entornos de la topología de subespacio dada por la topología producto.
Observamos que:

$$p^d\mathbb{Z}_p = \mathbb{Z}_p \bigcap \prod_{n=1}^{\infty} C_n \quad \text{con } C_n = \{0\} \text{ si } n \leq d \text{ y } C_n = A_n \text{ si } n > d.$$

Como $\prod_{n=1}^{\infty} C_n$ es un entorno de 0 en la topología producto, $p^d\mathbb{Z}_p$ es un entorno de 0 en la topología de subespacio de $\mathbb{Z}_p$. Recíprocamente, tomamos $\mathcal{W}$ un entorno de 0 para lo topología producto. Por ello, existe un abierto $\mathcal{U}$ tal que $0 \in \mathcal{U} \subseteq \mathcal{W}$. Por definición de la topología de subespacio, tenemos que $\mathcal{U} = \mathcal{U}' \cap \mathbb{Z}_p$ donde $\mathcal{U}'$ es un abierto de la topología producto. Por la construcción de la topología producto, podemos suponer que $\mathcal{U}' = \prod_{n\in\mathbb{N}} B_n$ donde $B_n \neq A_n$ para un número finito de valores de n. Consideramos d el último natural

para el cual $B_d \neq A_d$. Como $p^d A_n = \{0\} \subseteq B_n$ si $n \leq d$ y $p^d A_n \subseteq A_n$ si $n > d$, tenemos que $p^d \prod_{n=1}^{\infty} A_n \subseteq \mathcal{U}'$, luego $p^d \mathbb{Z}_p \subseteq \mathcal{U}$. Por tanto, los sistemas fundamentales de entornos de ambas topologías coinciden en 0 y, como son invariantes por traslación, coinciden en todo punto de $\mathbb{Z}_p$.

Por otro lado, como $\mathbb{Z}_p$ es un espacio métrico compacto, entonces es completo, ver Teorema A.21.

Por último, veamos que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. Para ello, veamos que dado $x \in \mathbb{Z}_p$ existe un $y \in \mathbb{Z}$ tal que para todo $\varepsilon > 0$ se tiene que $d_p(x, y) < \varepsilon$. Para ello, recordamos lo visto en la Observación 2.11 sobre la inclusión de $\mathbb{Z}$ en $\mathbb{Z}_p$, tomamos $x = (x_1, x_2, \dots, x_n, x_{n+1}, \dots) \in \mathbb{Z}_p$ y dado $\varepsilon > 0$ tomamos $n \in \mathbb{N}_{\geq 1}$ y consideramos $y = x_n \in \mathbb{Z}$, es decir, $y = (x_1, x_2, \dots, x_n, x_n, \dots)$ visto como elemento de $\mathbb{Z}_p$. Con ello, $x - y = (0, 0, \dots, 0, x_{n+1} - x_n, x_{n+2} - x_n, \dots)$. De esta forma, se tiene que $v_p(x - y) > n$, es decir, $d_p(x, y) < p^{-n} \leq \varepsilon$. Por tanto, $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. □

Observación 2.13. . *Algunos autores definen la distancia p-ádica como* $d(x, y) = e^{-v_p(x-y)}$ *como aparece en [9]. La ventaja que presenta la definición que hemos escogido es que verifica* $\prod_{v \in \mathcal{V}} |x|_v = 1$ *donde* $|x|_p = d_p(x, 0)$ *y* $\mathcal{V}$ *es el conjunto de todos los números primos y* $\{\infty\}$*, como veremos en la Sección 4.2.*

2.2. Números p-ádicos

Una vez construidos los enteros p-ádicos y presentadas algunas de sus características, podemos introducir el concepto de los números p-ádicos.

Para ello, observamos que el anillo de los enteros p-ádicos $\mathbb{Z}_p$ es un dominio de integridad dado que si $ab = 0$, entonces $v_p(ab) = v_p(0) = \infty$. Como $v_p(ab) = v_p(a)v_p(b)$, tenemos que $v_p(a)v_p(b) = \infty$, lo que ocurre si y solo si $v_p(a) = \infty$ o $v_p(b) = \infty$, es decir, si $a = 0$ o $b = 0$.

Definición 2.14. *El cuerpo de los* ***números p-ádicos****,* $\mathbb{Q}_p$ *se define como el cuerpo de fracciones de los enteros p-ádicos.*

Lema 2.15. *Los elementos no nulos de* $\mathbb{Q}_p$*, que denotamos por* $\mathbb{Q}_p^*$*, se pueden escribir de forma única como* $p^n u$ *con* $u \in \mathbb{U}^p$ *y* $n \in \mathbb{Z}$*.*

Demostración. Tomamos $x \in \mathbb{Q}_p^*$, luego por ser $\mathbb{Q}_p$ el cuerpo de fracciones de los enteros p-ádicos, existen $d, s \in \mathbb{Z}_p$, no nulos, tales que $x = d/s$ y, por la Proposición 2.7, se cumple que

$$x = \frac{d}{s} = \frac{p^{n_1} u_1}{p^{n_2} u_2} = p^{n_1 - n_2} u,$$

donde $u = u_1 \cdot u_2^{-1} \in \mathbb{U}^p$ por ser producto de dos unidades. □

En resumen, tenemos que $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. De nuevo, el valor n se denomina valoración p-ádica de los números p-ádicos, que abusando de la notación denotaremos también por v_p, y se tiene entonces que $v_p(x) \geq 0$ si y solo si $x \in \mathbb{Z}_p$.

Proposición 2.16. *El cuerpo* $\mathbb{Q}_p$ *con la topología definida por* $d_p(x, y) = p^{-v_p(x-y)}$ *es localmente compacto y contiene a* $\mathbb{Z}_p$ *como subanillo abierto. Además,* $\mathbb{Q}$ *es denso en* $\mathbb{Q}_p$*.*

Demostración. En primer lugar, veamos que $\mathbb{Q}_p$ es localmente compacto. Para ello, tomamos $a \in \mathbb{Q}_p$ y veamos que $\overline{B(a, p^{-n})}$ es compacta. Por la Proposición A.20, sabemos que toda bola cerrada es completa. Veamos que $\overline{B(a, p^{-n})}$ es totalmente acotada. Dado $\varepsilon > 0$, tomamos $m > n$ con $p^{-(m-1)} \leq \varepsilon$ y tenemos que

$$\overline{B(a, p^{-n})} \subseteq \bigcup_{i=0}^{p^{m-n}-1} \overline{B(a + ip^n, p^{-m})} = \bigcup_{i=0}^{p^{m-n}-1} B(a + ip^n, p^{-(m-1)}),$$

donde para probar la primera inclusión es necesario usar que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. Por tanto, $\overline{B(a, p^{-n})}$ es totalmente acotada y por la Proposición A.25, es secuencialmente compacta. Finalmente, por el Teorema A.23, se tiene que $\overline{B(a, p^{-n})}$ es compacta.

Como $\mathbb{Z}_p$ es subanillo de $\mathbb{Q}_p$ basta ver que es abierto. Para ello, tomamos $x \in \mathbb{Z}_p$, como $x + p^n\mathbb{Z}_p \subseteq \mathbb{Z}_p$ concluimos que es abierto.

Por último, veamos que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$. Tomamos $x \in \mathbb{Q}_p$ y veamos que para todo $\varepsilon > 0$ se tiene que $d_p(x, y) < \varepsilon$. Dado $x \in \mathbb{Q}_p$, por el Lema 2.15, podemos escribir $x = p^n u$ con $u \in \mathbb{U}^p$ y $n \in \mathbb{Z}$. Como por la Proposición 2.12, $\mathbb{Z}$ es denso en $\mathbb{Z}_p$, existe un $a \in \mathbb{Z}$ tal que $d_p(u, a) < \varepsilon p^n$. Por lo tanto, se cumple que

$$d_p(x, p^n a) = |p^n|_p |u - a|_p = p^{-n}|u - a|_p < \varepsilon.$$

Como $p^n a \in \mathbb{Q}$, concluimos que $\mathbb{Q}$ es denso en $\mathbb{Q}_p$. □

Observación 2.17. *Los números p-ádicos también se pueden construir como la completación de $\mathbb{Q}$ con la distancia p-ádica definida en la Proposición 2.16, ver [3, Sección 3.2.].*

Observación 2.18. *La distancia d_p satisface la desigualdad ultramétrica, es decir, para todos $x, y, z \in \mathbb{Q}_p$ se verifica*

$$d_p(x, y) \leq \max\left(d_p(x, z), d_p(z, y)\right).$$

Con esta propiedad, se tiene que toda serie converge si y solo si su término general tiende hacia 0.

2.3. Lema de Hensel

A continuación, nos centraremos en estudiar el comportamiento de las raíces de los polinomios con coeficientes p-ádicos. Vamos a denotar por $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ al polinomio con coeficientes en $\mathbb{Z}_p$ y siendo $n \in \mathbb{N}_{\geq 1}$, llamamos f_n al polinomio con coeficientes en A_n obtenido al tomar la clase de f módulo p^n.

Proposición 2.19. *Sea $(f^i)_{i \in I}$ una familia de polinomios de $\mathbb{Z}_p[X_1, \ldots, X_m]$. Entonces las siguientes afirmaciones son equivalentes:*

I. *Los polinomios f^i tienen una raíz común en $(\mathbb{Z}_p)^m$.*

II. *Para todo $n > 1$, los polinomios $(f^i)_n$ tienen una raíz común en $(A_n)^m$.*

Demostración. Vamos a probarlo por doble implicación y para ambas, vamos a llamar D al conjunto de raíces comunes de los f^i en $(\mathbb{Z}_p)^m$ y D_n al conjunto de raíces comunes de los $(f^i)_n$ en $(A_n)^m$ para cada $n \in \mathbb{N}$.
Si D es no vacío, tomando clases módulo p^n, D_n es no vacío. Recíprocamente, suponemos que para cada $n > 1$ D_n es no vacío. Como $(A_n)^m$ es finito, D_n es finito. Por otro lado, como ser raíz módulo p^n implica serlo módulo p^{n-1}, se tiene que la sucesión $(D_n)_{n\in\mathbb{N}_{\geq 1}}$ forma un sistema proyectivo. Resulta que $D = \varprojlim D_n$, luego por el Lema A.4, como cada D_n es finito y no vacío, D es no vacío. □

Para estudiar cómo se relacionan las raíces comunes de una familia de polinomios en $\mathbb{Z}_p$ y $\mathbb{Q}_p$, vamos a introducir la noción de elemento primitivo.

Definición 2.20. *Sea $x = (x_1, \dots, x_m)$ un elemento de $(\mathbb{Z}_p)^m$ se dice que es **primitivo** si para algún $i \in \{1, \dots, m\}$, el elemento x_i es una unidad. De forma análoga, se dice que un elemento $y = (y_1, y_2, \dots, y_m) \in (A_n)^m$ es primitivo si alguno de los y_i es una unidad.*

Recordando lo visto en la Proposición 2.7, tenemos entonces que un elemento dado por $x = (x_1, \dots, x_m)$ es primitivo en $(\mathbb{Z}_p)^m$ si alguno de los x_i no es divisible por p.

Proposición 2.21. *Sean $(f^i)_{i\in I}$ una familia de polinomios homogéneos de $\mathbb{Z}_p[X_1, \dots, X_m]$. Entonces las siguientes afirmaciones son equivalentes:*

I. *Los polinomios f^i tienen una raíz común no trivial en $(\mathbb{Q}_p)^m$.*

II. *Los polinomios f^i tienen una raíz común primitiva en $(\mathbb{Z}_p)^m$.*

III. *Para todo $n > 1$, los polinomios $(f^i)_n$ tienen una raíz primitiva común en $(A_n)^m$.*

Demostración. Veamos que I implica II. Tomamos $x \in (\mathbb{Q}_p)^m$ una raíz no trivial común de los f^i y $h = \min(v_p(x_1), \dots, v_p(x_m))$. Consideramos $y = p^{-h}x$ y supongamos que $h = v_p(x_k)$, luego tenemos que $y_k = p^{-h}x_k = u$ con $u \in \mathbb{U}^p$ y $v_p(y_j) \geq 0$ para todo $j \in \{1, \dots, m\}$ entonces y es primitivo en $(\mathbb{Z}_p)^m$. Veamos que y sigue siendo raíz de los f^i. Como los polinomios son homogéneos, tenemos que $f^i(y) = f^i(p^{-h}x) = p^{-h\deg(f^i)}f^i(x) = 0$, luego y es raíz común.

Veamos II implica I. Si $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ es una raíz común primitiva, entonces $x_k \in \mathbb{U}^p$, luego $x_k \neq 0$, $x \in (\mathbb{Q}_p)^m$ y es no trivial.

Para probar la equivalencia entre II y III notemos que es el enunciado de la proposición anterior añadiendo que la raíz es primitiva, luego basta probar que $x \in (\mathbb{Z}_p)^m$ es primitivo si y solo si $\alpha^n \in (A_n)^m$ lo es para todo $n \in \mathbb{N}_{\geq 1}$ donde α^n es x módulo p^n. Por la Proposición 2.7, tenemos que $x = (x_1, \dots, x_m) \in (\mathbb{Z}_p)^m$ no es primitivo si y solo si para todo $i \in \{1, \dots, m\}, p \mid x_i$. Por tanto, como $\alpha^n = (\alpha_1^n, \dots, \alpha_m^n)$ y $x_i = (\alpha_i^1, \alpha_i^2, \dots)$, x no es primitivo si y solo si para todo $i \in \{1, \dots, m\}$ $p \mid \alpha_i^n$, es decir, si y solo si α^n no es primitivo en A_n. □

Nuestro siguiente objetivo es establecer los resultados que nos indican bajo qué condiciones podemos obtener una solución de una ecuación polinomial módulo p^{n+1} a partir de una solución módulo p^n, lo que nos permitirá pasar de una solución módulo p a una solución en $\mathbb{Z}_p$.

Lema 2.22. *Sean $f \in \mathbb{Z}_p[X]$ y f' su derivada, $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$ tales que*

$$0 \leq 2k < n, \qquad f(x) \equiv 0 \ mod\ p^n, \qquad v_p(f'(x)) = k.$$

Entonces, existe $y \in \mathbb{Z}_p$ verificando:

$$f(y) \equiv 0 \ mod\ p^{n+1}, \quad v_p(f'(y)) = k \qquad e \qquad y \equiv x \ mod\ p^{n-k}.$$

Demostración. Tomamos $y = x + p^{n-k}z$ con $z \in \mathbb{Z}_p$ que elegiremos adecuadamente más adelante. Aplicando la fórmula de Taylor evaluada en y y centrada en x, tenemos que

$$\begin{aligned} f(y) &= f(x) + f'(x)(y-x) + a_1(y)(y-x)^2 = f(x) + f'(x)(p^{n-k}z) + a_1(x + p^{n-k}z)(p^{n-k}z)^2 \\ &= f(x) + f'(x)(p^{n-k}z) + ap^{2n-2k}, \end{aligned}$$

con $a_1(x + p^{n-k}z)z^2 = a \in \mathbb{Z}_p$. Nótese que no hay inconveniente en aplicar la fórmula de Taylor dado que la característica de $\mathbb{Z}_p$ es 0. Por hipótesis tenemos que $f(x) \equiv 0 \bmod p^n$, $v_p(f'(x)) = k$, esto es, $f(x) = p^n b$ y $f'(x) = p^k c$ con $b \in \mathbb{Z}_p$ y $c \in \mathbb{U}^p$, así que podemos tomar z como la solución de $b + zc \equiv 0 \bmod p$. Por tanto, se tiene que:

$$\begin{aligned} f(y) &= f(x) + f'(x)(p^{n-k}z) + ap^{2n-2k} = p^n b + p^k c p^{n-k} z + ap^{2n-2k} \\ &= p^n b + p^n cz + ap^{2n-2k} = p^n(b + cz) + ap^{2n-2k}. \end{aligned}$$

Como $b + zc \equiv 0 \bmod p$, se cumple que $p^n(b + cz) \equiv 0 \bmod p^{n+1}$ y como $2n - 2k > n$, tenemos que

$$f(y) = p^n(b + cz) + ap^{2n-2k} \equiv 0 \bmod p^{n+1}.$$

Por cómo hemos escogido y, $y \equiv x \bmod p^{n-k}$ y aplicando f' tenemos que $f'(y) \equiv f'(x) \bmod p^{n-k}$, de esta forma, usando la hipótesis de $f'(x) = p^k c, c \in \mathbb{U}^p$, tenemos

$$f'(y) \equiv p^k c \bmod p^{n-k}.$$

Como $n - k > k$ porque por hipótesis $2k < n$ y $c \in \mathbb{U}^p$, se concluye que $v_p(f'(y)) = k$. □

Gracias al lema anterior podemos demostrar el siguiente resultado que nos muestra cómo obtener una raíz en $\mathbb{Z}_p$ a partir de una raíz módulo p.

Teorema 2.23. *Sean $f \in \mathbb{Z}_p[X_1, \ldots, X_m], x = (x_1, \ldots, x_m) \in (\mathbb{Z}_p)^m, n, k \in \mathbb{Z}$ y j un entero tal que $0 \leq j \leq m$. Si se tiene que $0 \leq 2k < n$, que*

$$f(x) \equiv 0 \ mod\ p^n \qquad y\ que \qquad v_p(\tfrac{\partial f}{\partial X_j}(x)) = k.$$

Entonces, existe una raíz $y \in (\mathbb{Z}_p)^m$ de f tal que $y \equiv x \ mod\ p^{n-k}$.

Demostración. Dividiremos la demostración en dos casos:

En primer lugar, supongamos que tenemos $m = 1$. Aplicamos el Lema 2.22 a $x := x^{(0)}$. Así, tenemos que existe un $x^{(1)} \in \mathbb{Z}_p$ que verifica

$$f(x^{(1)}) \equiv 0 \bmod p^{n+1}, \quad v_p(f'(x^{(1)})) = k \quad \text{y} \quad x^{(0)} \equiv x^{(1)} \bmod p^{n-k}.$$

Empleando de nuevo el lema para $x := x^{(1)}$, como $m+1-k > k$ tenemos que existe $x^{(2)} \in \mathbb{Z}_p$ tal que

$$f(x^{(2)}) \equiv 0 \bmod p^{n+2}, \quad v_p(f'(x^{(2)})) = k \quad \text{y} \quad x^{(1)} \equiv x^{(2)} \bmod p^{n+1-k}$$

repitiendo este proceso obtenemos una sucesión $(x^{(0)}, x^{(1)}, \dots, x^{(q)}, x^{(q+1)}, \dots)$ que verifica que

$$f(x^{(q)}) \equiv 0 \bmod p^{n+q}, \quad x^{(q+1)} \equiv x^{(q)} \bmod p^{n+q-k}.$$

La sucesión obtenida es de Cauchy y como $\mathbb{Z}_p$ es completo, podemos asegurar que existe su límite $y \in \mathbb{Z}_p$ y tenemos que $f(y) = 0$ y, además, $y \equiv x \bmod p^{n-k}$, luego ya lo hemos probado para $m = 1$.

En segundo lugar, si $m > 1$ lo reduciremos al caso anterior. Tomamos $f \in \mathbb{Z}_p[X_1, \dots, X_m]$ y $x = (x_1, \dots, x_m)$ en las condiciones del enunciado y consideramos $\tilde{f} \in \mathbb{Z}_p[X_j]$ el polinomio obtenido de sustituir X_i por x_i si $i \neq j$. Estamos en las condiciones del caso anterior, luego existe $\tilde{y_j} \in \mathbb{Z}_p$ tal que $\tilde{y_j} \equiv x_j \bmod p^{n-k}$ y $\tilde{f}(\tilde{y_j}) = 0$. Tomamos $y = (y_1, \dots, y_m)$ de forma que $y_j = \tilde{y_j}$ obtenido e $y_i = x_i$ si $i \neq j$, luego y satisface las condiciones. □

Concluimos esta sección enunciando algunas consecuencias del teorema anterior. Para ello, primero introducimos la noción de raíz simple.

Definición 2.24. *Sea $g \in k[X_1, \dots, X_m]$ con k cuerpo. Decimos que x es una **raíz simple** de g si $g(x) = 0$ y g tiene al menos una derivada parcial distinta de cero, esto es $\frac{\partial g}{\partial X_j}(x) \neq 0$.*

El primer corolario es un resultado fundamental cuando se trabaja en la aritmética modular y se corresponde con el análogo al método de Newton en los p-ádicos. Aunque no entremos en detalle, no es complicado demostrar que la raíz que encontramos en $\mathbb{Z}_p$ es única, es decir, cerca de una raíz aproximada existe una única raíz del polinomio. Cabe destacar que existen versiones más generales de este lema, para más información nos referimos al artículo expositorio de K. Conrad [1].

Corolario 2.25 (Lema de Hensel)**.** *Sea f un polinomio en $\mathbb{Z}_p[X_1, \dots, X_m]$ y x una raíz simple de f módulo p. Entonces existe $y \in \mathbb{Z}_p$ tal que $f(y) \equiv 0$ mod p^n y $x \equiv y$ mod p.*

Demostración. Tomamos x la raíz simple del teorema, esto es, $f(x) \equiv 0 \bmod p$ y como es simple, para algún j, $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \bmod p$, por tanto, $v_p\big(\frac{\partial f}{\partial X_j}(x)\big) = 0$. Así, estamos en las condiciones del Teorema 2.23 para $n = 1$ y $k = 0$ y, en conclusión, existe una raíz $y \in \mathbb{Z}_p$ de f tal que $y \equiv x \bmod p$. □

Cuando apliquemos el Lema de Hensel diremos que $y \in \mathbb{Z}_p$ es el levantado de x o que x se levanta a y en $\mathbb{Z}_p$. Para finalizar, el segundo corolario nos muestra la aplicación de estos resultados al estudio de las formas cuadráticas sobre el que profundizaremos en los siguientes capítulos.

Corolario 2.26. *Sean $f(X) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} X_i X_j$ con $a_{ij} = a_{ji}$ coeficientes en $\mathbb{Z}_p$ y $a \in \mathbb{Z}_p$. Denotamos por $A = (a_{ij})_{1 \leq i,j \leq n}$ a la matriz simétrica asociada a f.*

- *Si $p \neq 2$ y $det(A)$ es invertible, entonces toda solución primitiva de $f(x) \equiv a$ mod p se puede levantar a una solución en $\mathbb{Z}_p$.*
- *Si $p = 2$ y x es una solución primitiva de $f(x) \equiv a$ mod 8, entonces x se puede levantar a una solución en $\mathbb{Z}_2$ asumiendo que no todas las derivadas parciales $\frac{\partial f}{\partial X_j}$ se anulan módulo 4.*

Demostración. Probemos el primer apartado. Supongamos que x es una solución primitiva de $f(x) \equiv a \bmod p$. Por el Corolario 2.25, basta ver que x es una raíz simple, es decir, que existe alguna derivada parcial que no se anula. Tenemos que, fijado i, $\frac{\partial f}{\partial X_i} = 2\sum_j a_{ij}X_j$ y veamos que es distinto de cero. Tomamos $x = (x_1, \ldots, x_n)$, razonamos por reducción al absurdo y supongamos que para todo $i \in \{1, \ldots, n\}$ se tiene que $2\sum_j a_{ij}x_j = 2(Ax)_i \equiv 0 \bmod p$, es decir, $2Ax^t \equiv 0 \bmod p$. Como $det(A)$ es invertible, A es invertible y concluimos que $x \equiv 0 \bmod p$ lo que es absurdo porque x es primitiva.

Veamos la demostración para $p = 2$. Basta aplicar el Teorema 2.23 para $n = 3$ y $k = 1$. □

Obsérvese que en el caso $p = 2$ si $det(A)$ es invertible, entonces razonando como en el caso $p \neq 2$ se prueba que no todas las derivadas parciales se anulan módulo 4.

2.4. El grupo multiplicativo en $\mathbb{Q}_p$

El objetivo de esta sección es describir la estructura del grupo multiplicativo en $\mathbb{Q}_p$. Más concretamente, queremos obtener una descripción similar a la que conocemos del grupo multiplicativo en los números reales, recordemos que $(\mathbb{R}^*, \cdot)$ es isomorfo al grupo producto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{R}$. Recordamos que denotamos $\mathbb{U}^p$ el grupo de las unidades de los enteros p-ádicos. Para todo $n \geq 1$, definimos $U_n := 1 + p^n\mathbb{Z}_p$ y consideramos el homomorfismo de grupos

$$f_n : \mathbb{U}^p \to A_n^*$$

que se obtiene como la restricción a $\mathbb{U}^p$ de la proyección canónica ε_n de la Proposición 2.6. Recordemos además, que como vimos en la Sección 2.1, la aplicación ε_n es sobreyectiva y, por tanto, $Im(\varepsilon_n) = A_n$; por otro lado, se tiene que $Ker(\varepsilon_n) = p^n\mathbb{Z}_p$.

Proposición 2.27. *Sea la aplicación $f_n = \varepsilon_n|_{\mathbb{U}^p} : \mathbb{U}^p \to A_n^*$, se cumple que $Ker(f_n) = U_n$.*

Demostración. Por definición, se cumple que

$$\begin{aligned} Ker(f_n) &= \{x \in \mathbb{U}^p : f_n(x) = 1\} = \mathbb{U}^p \cap \{x \in \mathbb{Z}_p : \varepsilon_n(x) = 1\} \\ &= \mathbb{U}^p \cap (1 + p^n\mathbb{Z}_p) = (\mathbb{Z}_p \setminus p\mathbb{Z}_p) \cap (1 + p^n\mathbb{Z}_p) = 1 + p^n\mathbb{Z}_p = U_n. \end{aligned}$$

La penúltima igualdad se tiene porque $U_n \subseteq \mathbb{U}^p$, puesto que dado $x \in U_n$, podemos expresarlo como $x = 1 + p^n y$ y no es múltiplo de p, luego $x \in \mathbb{U}^p$. □

Observación 2.28. *Para cada $n \in \mathbb{N}_{\geq 1}$ se tiene que U_n es un subgrupo de $\mathbb{U}^p$ por ser el núcleo de la aplicación f_n, de hecho, es un subgrupo abierto dado que $U_n = B(1, p^{-(n-1)})$. Además, forman una sucesión decreciente porque todo elemento $x \in U_{n+1}$ lo podemos expresar como $x = 1 + p^{n+1}y$ con $y \in \mathbb{Z}_p$ y tomando $z = py \in \mathbb{Z}_p$, tenemos que $x = 1 + p^n z \in U_n$.*

Corolario 2.29. *El grupo cociente $\mathbb{U}^p/U_1$ es isomorfo a $\mathbb{F}_p^* = A_1^*$, donde $\mathbb{F}_p^*$ es el grupo multiplicativo de $\mathbb{F}_p^*$ que recordamos cíclico de orden $p - 1$.*

Demostración. Consideramos la aplicación para $n = 1, f_1 : \mathbb{U}^p \to A_1^*$. Por la Proposición 2.27, $Ker(f_1) = U_1$ y como f_1 es sobreyectiva aplicando el Primer Teorema de Isomorfía tenemos que $\mathbb{U}^p/Ker(f_1) \simeq Im(f_1)$, luego $\mathbb{U}^p/U_1 \simeq A_1^* = \mathbb{F}_p^*$.

□

Observación 2.30. *Los U_n forman una sucesión decreciente de subgrupos abiertos de $\mathbb{U}^p$ y verifican que $\mathbb{U}^p = \varprojlim A_n^* = \varprojlim \mathbb{U}^p/U_n$, por las Proposiciones 2.7 y 2.27.*

Proposición 2.31. *El grupo cociente U_n/U_{n+1} es isomorfo a A_1. Además, el orden de U_1/U_n es p^{n-1}.*

Demostración. Consideramos la siguiente aplicación

$$\begin{array}{rccc} \eta: & (U_n,\cdot) & \longrightarrow & (\mathbb{Z}_p,+) \\ & 1+p^n x & \longmapsto & x \end{array}$$

y el homomorfismo $\varepsilon_1 : \mathbb{Z}_p \longrightarrow A_1$ de la Proposición 2.6. La aplicación $\varphi = \varepsilon_1 \circ \eta$ es un homomorfismo de grupos puesto que dados $1+p^n x, 1+p^n y \in U_n$, tenemos que

$$\varphi((1+p^n x)(1+p^n y)) = \varphi(1+p^n(x+y)+p^{2n}xy) = \varepsilon_1(x+y+p^n xy) = x+y = \varphi(1+p^n x)+\varphi(1+p^n y).$$

Veamos que φ es sobreyectiva y que $Ker(\varphi) = U_{n+1}$. Como η y ε_1 son sobreyectivas, φ lo es por su composición. Por otro lado, tenemos que

$$\begin{aligned} Ker(\varphi) &= \{x \in U_n : \varepsilon_1(\eta(x)) = 0\} = \{x \in U_n : \eta(x) = py, y \in \mathbb{Z}_p\} \\ &= \{x \in U_n : x = 1+p^n py, y \in \mathbb{Z}_p\} = U_{n+1}. \end{aligned}$$

Aplicando el Primer Teorema de Isomorfía y tenemos que $U_n/Ker(\varphi) \simeq Im(\varphi)$, es decir, $U_n/U_{n+1} \simeq A_1$.

Por último, veamos que el orden de U_1/U_n es p^{n-1}. Por lo que acabamos de probar, para $n=2$ se cumple que $\#(U_1/U_2) \simeq A_1$, luego $\#(U_1/U_2) = p$. Utilizando el Tercer Teorema de Isomorfía, tenemos que

$$U_1/U_{n-1} \simeq (U_1/U_n)\big/(U_{n-1}/U_n).$$

Supongamos que la hipótesis de inducción se cumple para un cierto $n-1$ que $\#(U_1/U_n) = p^{n-2}$ y veamos que se cumple también para U_1/U_n. Por hipótesis de inducción tenemos que $\#(U_1/U_{n-1}) = p^{n-2}$ luego, $\#(U_1/U_n) = \#(U_1/U_{n-1})\#(U_{n-1}/U_n) = p^{n-2}p = p^{n-1}$. □

Proposición 2.32. *Sea $\mathbb{U}^p$ el grupo de unidades de los enteros p-ádicos. Entonces se tiene que $\mathbb{U}^p = V \times U_1$ donde $V = \{x \in \mathbb{U}^p : x^{p-1} = 1\}$ es el único subgrupo de $\mathbb{U}^p$ isomorfo a $\mathbb{F}_p^*$.*

Demostración. Consideramos la siguiente sucesión de homomorfismos entre grupos abelianos:

$$\{1\} \longrightarrow U_1/U_n \longrightarrow \mathbb{U}^p/U_n \longrightarrow \mathbb{F}_p^* \longrightarrow \{1\}.$$

Notemos que, por el Tercer Teorema de Isomorfía y por el Corolario 2.29, $\mathbb{U}^p/U_1 \simeq \mathbb{F}_p^*$, tenemos que $(\mathbb{U}^p/U_n)/(U_1/U_n) \simeq \mathbb{U}^p/U_1 \simeq \mathbb{F}_p^*$ y, por tanto, la sucesión es exacta. Además el orden de U_1/U_n es p^{n-1} mientras que el de $\mathbb{F}_p^*$ es $p-1$, luego son coprimos. Así, aplicando el Lema A.6, tenemos que $V_n := \{x \in \mathbb{U}^p/U_n : x^{p-1} = 1\}$ es el único subgrupo de $\mathbb{U}^p/U_n$ isomorfo a $\mathbb{F}_p^*$. Por la Observación 2.30, se tiene que $\mathbb{U}^p = \varprojlim \mathbb{U}^p/U_n$ y como cada morfismo lleva V_n a V_{n-1}, podemos considerar el límite proyectivo $V := \varprojlim V_n$. Tenemos entonces que $V = \{x \in \mathbb{U}^p : x^{p-1} = 1\}$ y es el único subgrupo isomorfo a $\mathbb{F}_p^*$ porque V_n es único para cada $n \in \mathbb{N}$.

Finalmente, aplicando el Lema A.6 a la sucesión exacta:

$$\{1\} \longrightarrow U_1 \longrightarrow \mathbb{U}^p \longrightarrow \mathbb{F}_p^* \longrightarrow \{1\},$$

se tiene que $\mathbb{U}^p = U_1 \times V$ dado que V es el único subgrupo de $\mathbb{U}^p$ isomorfo a $\mathbb{F}_p^*$. □

Observación 2.33. *El grupo V se denomina* ***grupo de los representantes multiplicativos de los elementos de*** $\mathbb{F}_p^*$ *y el cuerpo $\mathbb{Q}_p$ contiene a las raíces $(p-1)$-ésimas de la unidad.*

Lema 2.34. *Sea $x \in U_n \setminus U_{n+1}$ con $n \geq 1$ si $p \neq 2$ y con $n \geq 2$ si $p = 2$. Entonces se cumple que $x^p \in U_{n+1} \setminus U_{n+2}$.*

Demostración. Como $x \in U_n \setminus U_{n+1}$, se puede expresar como $x = 1 + kp^n$ con k no múltiplo de p, es decir, $x \notin U_{n+1}$. Desarrollando el binomio de Newton, tenemos que:

$$x^p = \sum_{i=0}^{p} \binom{p}{i} 1^{p-i}(kp^n)^i = 1 + kp^{n+1} + \cdots + k^p p^{np}.$$

El exponente de p de los términos que no aparecen escritos es mayor o igual que $2n+1$ que es mayor que $n+2$. Por tanto, son congruentes con 0 módulo p^{n+2}. Para el último término, tenemos que $np \geq n+2$ por nuestras hipótesis, luego $p^{np} \equiv 0 \mod p^{n+2}$. De esta forma, concluimos que $x^p \equiv 1 + kp^{n+1} \mod p^{n+2}$, es decir, que $x^p \in U_{n+1} \setminus U_{n+2}$. □

Proposición 2.35. *Si $p \neq 2$, U_1 es isomorfo a $\mathbb{Z}_p$. Si $p = 2$, U_1 es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times U_2$ donde U_2 es isomorfo a $\mathbb{Z}_2$.*

Demostración. Vamos a dividir la demostración en dos casos, si $p = 2$ y si $p \neq 2$.

Primero, supongamos que $p \neq 2$ y sea $\alpha \in U_1 \setminus U_2$. Por el Lema 2.34, tenemos que $\alpha^{p^i} \in U_{i+1} \setminus U_{i+2}$ y llamamos α_n a la imagen de α en U_1/U_n. Por lo anterior, tenemos que $\alpha^{p^{n-2}} \in U_{n-1} \setminus U_n$, así, $\alpha^{p^{n-2}} \in U_{n-1}$ y $\alpha^{p^{n-1}} \in U_n$ y, por tanto, $(\alpha_n)^{p^{n-2}} \neq 1$ y $(\alpha_n)^{p^{n-1}} = 1$ en U_1/U_n. Como $\#(U_1/U_n) = p^{n-1}$ y $O(\alpha_n) = p^{n-1}$ tenemos que α_n es un generador. Empleamos este elemento para definir un isomorfismo $\theta_{n,\alpha} : A_{n-1} \longrightarrow U_1/U_n$ dado por $\theta_{n,\alpha}(x) = \alpha_n^x$ y comprobamos de forma directa que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} & \overset{\theta_{n+1,\alpha}}{} & \\ A_n & \longrightarrow & U_1/U_{n+1} \\ \downarrow & & \downarrow \\ & \underset{\theta_{n,\alpha}}{} & \\ A_{n-1} & \longrightarrow & U_1/U_n \end{array}$$

Recordando la Definición 2.2 de enteros p-ádicos y como $\mathbb{U}^p = \varprojlim \mathbb{U}^p/U_n$ deducimos que $U_1 = \varprojlim U_1/U_n$ y comprobamos que la familia $(\theta_{n,\alpha})_{n=1}^{\infty}$ define un isomorfismo $\theta : \mathbb{Z}_p \longrightarrow U_1$.

En segundo lugar, supongamos que $p = 2$. Por un lado, como U_1/U_n tiene orden 2^{n-1} tenemos que $\#(U_1/U_2) = 2$, es decir, $U_1/U_2 \simeq \mathbb{Z}/2\mathbb{Z}$. Por tanto, tenemos que $U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2$. Veamos que U_2 es isomorfo a $\mathbb{Z}_2$. Tomamos $\alpha \in U_2 \setminus U_3$ y de la misma forma que antes, obtenemos isomorfismos $\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \longrightarrow U_2/U_n$. Así, de forma análoga al apartado anterior conseguimos un isomorfismo entre U_2 y $\mathbb{Z}_2$ y, en conclusión,

$$U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2.$$

□

Concluimos con el resultado fundamental de la sección.

Teorema 2.36. *El grupo $\mathbb{Q}_p^*$ es isomorfo a:*

- $\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, *si* $p \neq 2$.
- $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$, *si* $p = 2$.

Demostración. Sabemos que todo $x \in \mathbb{Q}_p^*$ no nulo puede escribirse de forma única como $x = p^n u$ con $u \in \mathbb{U}^p, n \in \mathbb{Z}$. Luego, $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}^p$. Usando la Proposición 2.32, $\mathbb{U}^p \simeq V \times U_1$ donde V es isomorfo al grupo cíclico de orden $p-1$, es decir, $\mathbb{Z}/(p-1)\mathbb{Z}$. Vamos a diferenciar si $p \neq 2$ o $p = 2$:

Si $p \neq 2$, usando la Proposición 2.35 tenemos que $U_1 \simeq \mathbb{Z}_p$. Con todo, tenemos que:

$$\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}^p \simeq \mathbb{Z} \times V \times U_1 \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

Si $p = 2$, usando la Proposición 2.35 tenemos que $U_1 \simeq \{\pm 1\} \times \mathbb{Z}_2$. En conclusión, tenemos que

$$\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{U}^2 \simeq \mathbb{Z} \times V \times U_1 \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2.$$

□

2.5. Cuadrados en $\mathbb{Q}_p$

Para estudiar y clasificar las formas cuadráticas es esencial conocer la estructura del conjunto de elementos del cuerpo que son cuadrados. En esta sección estudiaremos las propiedades de los cuadrados en $\mathbb{Q}_p^*$ y, para ello, emplearemos el símbolo de Legendre cuya definición se recuerda en el Apéndice A. Debemos realizar por separado el estudio de los casos $p = 2$ y $p \neq 2$.

Teorema 2.37. *Sean $p \neq 2$ y $x = p^n u \in \mathbb{Q}_p^*$ con $n \in \mathbb{Z}$ y $u \in \mathbb{U}^p$. Se tiene que x es cuadrado en $\mathbb{Q}_p$ si y solo si n es par y la imagen de u en $\mathbb{F}_p^* \simeq \mathbb{U}^p/U_1$ es cuadrado.*

Demostración. Tomamos $x \in \mathbb{Q}_p^*$ tal que $x = p^n u$. Por la Proposición 2.32, tenemos que $\mathbb{U}^p = V \times U_1$, luego podemos escribir $u = (v, u_1)$ con $v \in V, u_1 \in U_1$. Como $\mathbb{Q}_p^* \simeq \mathbb{Z} \times V \times U_1$, tenemos que x es cuadrado si y solo si n es par y u es cuadrado, es decir, si v y u_1 son cuadrados. Veamos que todos los elementos de U_1 son cuadrados. Por la Proposición 2.35, sabemos que existe un isomorfismo $\varphi : (U_1, \cdot) \longrightarrow (\mathbb{Z}_p, +)$. Como 2 es invertible en $\mathbb{Z}_p$ puesto que estamos suponiendo que $p \neq 2$, tenemos que todo elemento x de $\mathbb{Z}_p$ se puede expresar como $x = 2m$ con $m \in \mathbb{Z}_p$. Por tanto, dado $y \in U_1$ se tiene que $\varphi(y) = 2m = 2\varphi(z) = \varphi(z^2)$ para algún $z \in \mathbb{Z}_p$, es decir, $y = z^2$. De esta manera, bastaría ver que v es cuadrado y como $V \simeq \mathbb{U}^p/U_1 \simeq \mathbb{F}_p^*$, x es cuadrado si y solo si n es par y v es cuadrado en $\mathbb{F}_q^*$. □

Observación 2.38. *La condición de que la imagen de u en $\mathbb{F}_p^*$ sea cuadrado es equivalente a decir que $\left(\frac{u}{p}\right) = 1$, en términos del símbolo de Legendre.*

Corolario 2.39. *El grupo $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y $\{1, p, v, vp\}$ es un sistema completo de representantes de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ donde $v \in \mathbb{F}_p^*$ es un elemento fijo tal que $\left(\frac{v}{p}\right) = -1$.*

Demostración. Tomamos $z = p^n w \in \mathbb{Q}_p^*$ con $n \in \mathbb{Z}$ y $w \in \mathbb{U}^p$ y vamos a distinguir cuatro casos para calcular $z\mathbb{Q}_p^{*2}$ teniendo en cuenta el Teorema 2.37.

Primero, supongamos que n es par y $\left(\frac{w}{p}\right) = 1$, entonces $(p^n w) \cdot 1 \in \mathbb{Q}_p^{*2}$. Por tanto,

se tiene que $z\mathbb{Q}_p^{*2} = \mathbb{Q}_p^{*2}$. Segundo, supongamos que n es impar y $\left(\frac{w}{p}\right) = 1$, entonces $(p^n w) \cdot p^{-1} = p^{n-1}w \in \mathbb{Q}_p^{*2}$. Por tanto, se cumple que $z\mathbb{Q}_p^{*2} = p\mathbb{Q}_p^{*2}$. Tercero, supongamos que n es par y $\left(\frac{w}{p}\right) = -1$, entonces $(p^n w) \cdot v^{-1} \in \mathbb{Q}_p^{*2}$ con $\left(\frac{v}{p}\right) = -1$. Por tanto, se tiene que $z\mathbb{Q}_p^{*2} = v\mathbb{Q}_p^{*2}$. Por último, supongamos que n es impar y $\left(\frac{w}{p}\right) = -1$, entonces $(p^n w) \cdot p^{-1}v^{-1} = p^{n-1}wv^{-1} \in \mathbb{Q}_p^{*2}$ con $\left(\frac{v}{p}\right) = -1$. Por tanto, se tiene que $z\mathbb{Q}_p^{*2} = vp\mathbb{Q}_p^{*2}$. De esta forma, $\{1, p, v, vp\}$ es un sistema completo de representantes. Además, como se cumple que $p^2, v^2, (vp)^2 \in \mathbb{Q}_p^{*2}$, deducimos que $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Teorema 2.40. *Sea $x = p^n u \in \mathbb{Q}_2^*$ con $n \in \mathbb{Z}$ y $u \in \mathbb{U}^2$. Se tiene que x es cuadrado si y solo si n es par y $u \equiv 1$ mod 8.*

Demostración. Tomamos $x = p^n u \in \mathbb{Q}_2^*$ con las condiciones del teorema y, razonando como en la demostración del Teorema 2.37, tenemos que x es cuadrado si y solo si n es par y $u \in \mathbb{U}^2$ es cuadrado. Como $\mathbb{U}^2 = \{\pm 1\} \times U_2$, $u = vw$ es cuadrado en $\mathbb{U}^2$ si y solo v es cuadrado en $\{\pm 1\}$ y w es cuadrado en U_2, es decir, si y solo si $v = 1$ y w es cuadrado en U_2. Por tanto, u es cuadrado en $\mathbb{U}^2$ si y solo si $u = w$ es cuadrado en U_2 . Empleando el isomorfismo $\theta : (\mathbb{Z}_2, +) \longrightarrow (U_2, \cdot)$ dado en la prueba de la Proposición 2.35, como estamos en $(\mathbb{Z}_2, +)$ un elemento x es cuadrado si y solo si lo podemos expresar como $2x$, luego tenemos que un elemento de $\mathbb{Z}_2$ es cuadrado si y solo si su imagen por el isomorfismo está en $U_3 = 1 + 2^3\mathbb{Z}_p$. Por tanto, u es cuadrado en U_2 si y solo si $u \equiv 1 \bmod 2^3$. □

Corolario 2.41. *El grupo $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ es un sistema completo de representantes.*

Demostración. Tomamos $a = 2^n u \in \mathbb{Q}_2^*$ con $n \in \mathbb{Z}$ y $w \in \mathbb{U}^2$ y vamos a distinguir casos para ver cuándo $a \in \mathbb{Q}_2^{*2}$ aplicando el Teorema 2.40.

Primero, supongamos que n es par y $u \equiv 1 \bmod 8$, entonces $(2^n u) \cdot 1 \in \mathbb{Q}_2^{*2}$. Por tanto, se tiene que $a\mathbb{Q}_2^{*2} = \mathbb{Q}_2^{*2}$. Segundo, supongamos que n es par y $u \equiv 3 \bmod 8$, entonces $3u \equiv 1 \bmod 8$, i.e., $3u \in \mathbb{Q}_2^{*2}$ como $3 \equiv -5 \bmod 8$, tenemos que $a\mathbb{Q}_2^{*2} = -5\mathbb{Q}_2^{*2}$. Tercero, supongamos que n es par y $u \equiv 5 \bmod 8$, entonces $a\mathbb{Q}_2^{*2} = 5\mathbb{Q}_2^{*2}$. Por último, supongamos que n es par y $u \equiv 7 \bmod 8$, entonces $a\mathbb{Q}_2^{*2} = (-1)\mathbb{Q}_2^{*2}$.

Para los casos donde n es impar, los casos que salen son los mismos que los anteriores multiplicando por 2. Por tanto, un sistema completo de representantes es $\{\pm 1, \pm 2, \pm 5, \pm 10\}$. □

Concluimos el capítulo empleando la representación algebraica proporcionada por los teoremas anteriores para obtener el siguiente resultado topológico.

Teorema 2.42. *$\mathbb{Q}_p^{*2}$ es un subgrupo abierto de $\mathbb{Q}_p^*$.*

Demostración. Para demostrarlo distinguimos si $p = 2$ o $p \neq 2$.

Si $p = 2$ y tomamos $a \in \mathbb{Q}_2^{*2}$, por el Teorema 2.40 $a = 2^n u$ con n par y $u \equiv 1 \bmod 8$. Veamos que $B(a, 2^{-(n+3)}) \subseteq \mathbb{Q}_2^{*2}$. Tomamos $x \in B(a, 2^{-(n+3)})$ y tenemos que

$$|x - a|_2 < \frac{1}{2^{n+3}} < \frac{1}{2^n} = |a|_2$$

Por la desigualdad ultramétrica, como $|x-a|_2 \neq |a|_2$ tenemos que

$$|x|_2 = \text{máx}\,(|x-a|_2, |a|_2) = |a|_2 = \frac{1}{2^n}.$$

Por tanto, $x = 2^n v$ con $v \in \mathbb{U}^2$. Con ello, se tiene que

$$|v-u|_2 = \left|\frac{1}{2^n}\right|_2 |x-a|_2 < 2^n \frac{1}{2^{n+3}} = \frac{1}{2^{n+3}}.$$

Por ello, se tiene que $v - u = 2^m w$ con $m \geq 3$, es decir, $u \equiv v \equiv 1 \mod 8$ y, por el Teorema 2.40, $x \in \mathbb{Q}_2^{*2}$.

Si $p \neq 2$, tomamos $a \in \mathbb{Q}_p^{*2}$ y por el Teorema 2.37, $a = p^n u$ con n par y $u \equiv b^2 \mod p$ con $b \in \mathbb{Z}$. Veamos que $B(a, p^{-(n+1)}) \subseteq \mathbb{Q}_p^{*2}$. Tomamos $x \in B(a, p^{-(n+1)})$ y veamos que $x \in \mathbb{Q}_p^{*2}$. Como $x \in B(a, p^{-(n+1)})$, tenemos que $|x-a|_p < p^{-(n+1)}$. Llamamos $y = x - a = p^{n+1} v$, luego $x = y + a = p^n(pv + u)$. Con ello, se cumple que $(pv+u) \equiv b^2 \mod p$ y se comprueba que $pv + u \in \mathbb{U}^p$. En conclusión, por el Teorema 2.37, $x \in \mathbb{Q}_p^{*2}$. □

Capítulo 3

Formas cuadráticas

En este capítulo introduciremos las nociones fundamentales sobre formas cuadráticas siguiendo [9, Capítulo III]. Aunque trabajaremos en **un k-espacio vectorial de dimensión finita y donde la característica de k no es 2**, estos resultados se pueden extender a otros contextos y en particular se pueden generalizar para módulos.

3.1. Espacios cuadráticos

El objetivo de esta sección es demostrar el Teorema de Witt para lo cual necesitamos recordar los conceptos fundamentales de la teoría de formas bilineales.

Definición 3.1. *Sea V un k-espacio vectorial. Se llama* ***forma bilineal*** *a una aplicación $F : V \times V \longrightarrow k$ que es lineal en cada variable, es decir, para todos $x, y, z \in V$ y para todo $\alpha \in k$, se cumple que*

- $F(x, y + z) = F(x, y) + F(x, z) \quad y \quad F(x + z, y) = F(x, y) + F(z, y)$.
- $F(\alpha x, y) = \alpha F(x, y) \qquad y \qquad F(x, \alpha y) = \alpha F(x, y)$.

Además, si se cumple que $F(x, y) = F(y, x)$ para todos $x, y \in V$, se dice que F es una ***forma bilineal simétrica.***

Una forma alternativa de presentar las formas bilineales es mediante su forma cuadrática asociada.

Definición 3.2. *Sea F una forma bilineal simétrica, la aplicación $Q : V \longrightarrow k$ definida como $Q(x) := F(x, x)$ es la* ***forma cuadrática asociada a*** *F.*

Como la característica de k es distinta de 2, la forma cuadrática Q determina unívocamente la forma bilineal F. En concreto, para todos $x, y \in V$, por la bilinealidad de F, se cumple que

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

Por simplicidad, escribiremos $x._Q y := F(x, y)$ o, si no hay confusión, $x.y = F(x, y)$.

Al par (V, Q) donde V es un k- espacio vectorial de dimensión finita y Q es una forma cuadrática lo denominaremos **espacio cuadrático.**

Definición 3.3. *Sean (V, Q) y $(\tilde{V}, \tilde{Q})$ dos espacios cuadráticos, se llama* ***morfismo métrico*** *a toda aplicación $f : V \longrightarrow \tilde{V}$ tal que para todos $x, y \in V$, $f(x).\tilde{Q}f(y) = x.Qy$.*

Definición 3.4. *Sean (V, Q) un espacio cuadrático y $B = (e_1, \ldots, e_n)$ una base de V. La* ***matriz de*** *Q respecto de esta base es la matriz $M_B(Q) = A = (a_{ij})_{1 \leq i,j \leq n}$ donde $a_{i,j} = e_i.e_j$. Observamos que $M_B(Q)$ es una matriz simétrica.*

El primer invariante que introducimos para realizar nuestro estudio de las formas cuadráticas es su discriminante.

Definición 3.5. *Sean (V, Q) un espacio cuadrático donde V es un k-espacio vectorial y $A = M_B(Q)$ la matriz de Q en la base B. Si $det(A) \neq 0$, llamamos* ***discriminante de*** *Q a la clase del $det(A)$ en el grupo cociente k^*/k^{*2}, es decir, escribimos*

$$d(Q) = [det(A)] \in k^*/k^{*2}.$$

En el caso de que $det(A) = 0$, diremos que $d(Q) = 0$.

Recordamos que dadas dos bases B y $\tilde{B}$ de un k-espacio vectorial de dimensión finita V, la fórmula de cambio de base para las matrices de una forma cuadrática Q es

$$M_{\tilde{B}}(Q) = (M_{\tilde{B}B})^t M_B(Q) M_{\tilde{B}B},$$

donde $M_{\tilde{B}B}$ representa la matriz de cambio de base de $\tilde{B}$ a B. Por lo tanto, se tiene que

$$det(M_{\tilde{B}}(Q)) = (det(M_{\tilde{B}B}))^2 det(M_B(Q))$$

y como $(det(M_{\tilde{B}B}))^2 \in k^{*2}$, el discriminante está bien definido y no depende de la elección de la base.

Definición 3.6. *Sea (V, Q) un espacio cuadrático sobre k. Decimos que $x, y \in V$ son* ***ortogonales*** *si $x.y = 0$. Al conjunto de elementos formado por los elementos ortogonales a todos los elementos de un subconjunto H de V no vacío, se le denomina* ***ortogonal*** *de H y se denota por H^0. Dados dos subespacios V_1 y V_2 de V, se dice que V_1 es ortogonal a V_2 si $V_1 \subseteq V_2^0$. Obsérvese que si $V_1 \subseteq V_2^0$, entonces $V_1^0 \supseteq V_2$, luego podemos hablar de subespacios ortogonales entre sí.*

Lema 3.7. *Sean (V, Q) un espacio cuadrático y H un subconjunto de V no vacío. El ortogonal de H es un subespacio vectorial.*

Demostración. Para ver que H^0 es subespacio vectorial, vamos a aplicar el test de caracterización de subespacios. Tomamos $h_1, h_2 \in H^0$ y $\lambda_1, \lambda_2 \in k$. Como $h_1, h_2 \in H^0$, tenemos que $h_1.y = 0$ para todo $y \in H$ y $h_2.y = 0$ para todo $y \in H$. Por la bilinealidad $(\lambda_1 h_1 + \lambda_2 h_2).y = \lambda_1 h_1.y + \lambda_2 h_2.y = 0 + 0 = 0$. En conclusión, $\lambda_1 h_1 + \lambda_2 h_2 \in H^0$. □

Definición 3.8. *Sea (V, Q) un espacio cuadrático, al ortogonal de todo el espacio vectorial, es decir, V^0, se le llama* ***radical*** *y se denota por $rad(V)$.*

Gracias al radical, podemos introducir la noción de rango de la forma cuadrática Q.

Definición 3.9. *Sea (V, Q) un espacio cuadrático, se llama rango de Q a la codimensión del radical, es decir, se define el* ***rango de Q*** *como*

$$rango(Q) := dim(V) - dim((rad(V))).$$

Una forma cuadrática se dice **no degenerada** si $V^0 = \{0\}$ y, en la Observación 3.22, probaremos que es equivalente a que $d(Q) \neq 0$.

Toda forma bilineal define de manera habitual una aplicación lineal de V en V^*, que emplearemos para simplificar algunas demostraciones.

Definición 3.10. *Sea U un subespacio de V y sea U^* su dual. Definimos $q_U : V \longrightarrow U^*$ como la aplicación lineal dada para cada $y \in U$ por $q_U(x)(y) = x._Q y$. La aplicación q_U se denomina* ***morfismo de polaridad asociado a Q y restringido a U****.*

Se puede comprobar de forma directa que $M_{BB^*}(q_V) = M_B(Q)$, más precisamente se tiene la información del siguiente lema.

Lema 3.11. *Sean (V, Q) un espacio cuadrático, $U \subseteq V$ un subespacio y $q_U : V \longrightarrow U^*$ la aplicación antes definida. Entonces, se tiene que:*

I. $Ker(q_U) = U^0$.

II. *La forma cuadrática Q es no degenerada si y solo si $q_V : V \longrightarrow V^*$ es un isomorfismo.*

Demostración. Primero, vamos a probar la primera afirmación por doble contenido.Tomamos $x \in Ker(q_U)$, luego $q_U(x) \equiv 0$, es decir, para todo $y \in U$ $x.y = q_U(x)(y) = 0$, por tanto, $x \in U^0$. Recíprocamente, si tomamos $x \in U^0$, tenemos que $x.y = 0$ para todo $y \in U$. Por ello, se tiene que $q_U(x) \equiv 0$ y, por consiguiente, $x \in Ker(q_U)$.

Por último, probemos la segunda afirmación por doble implicación. Supongamos que Q es no degenerada, es decir, $V^0 = \{0\}$. Sabemos que $Ker(q_V) = V^0$, luego, $Ker(q_V) = \{0\}$ y, por tanto, q_V es inyectivo. Por otro lado, como $dim(V) = dim(V^*)$, se tiene que q_V es sobreyectivo. Con ello, q_V es un isomorfismo. Recíprocamente, supongamos que la aplicación $q_V : V \longrightarrow V^*$ es isomorfismo. En particular, q_V es inyectivo y, por tanto, $Ker(q_V) = \{0\}$. Como $Ker(q_V) = V^0 = \{0\}$, luego Q es no degenerada. □

Definición 3.12. *Sean (V, Q) un espacio cuadrático y $U_1, U_2, \ldots, U_m$ subespacios de V. Decimos que V es* ***suma directa ortogonal*** *de los U_i si son ortogonales dos a dos y, además, V es suma directa de ellos. Se escribe entonces*

$$V = U_1 \mathbin{\widehat{\oplus}} U_2 \mathbin{\widehat{\oplus}} \cdots \mathbin{\widehat{\oplus}} U_m.$$

Observación 3.13. *Notemos que si tenemos $x \in V$ con $x = \sum_{i=1}^{m} x_i$ con $x_i \in U_i$, se tiene que*

$$Q(x) = Q_1(x_1) + Q_2(x_2) + \cdots + Q_m(x_m)$$

donde $Q_i = Q|_{U_i}$ es la restricción de Q a U_i.

Proposición 3.14. *Sean (V, Q) un espacio cuadrático y U un subespacio suplementario de $rad(V)$ en V. Entonces se verifica que $V = U \mathbin{\widehat{\oplus}} rad(V)$.*

Demostración. Como U es el subespacio suplementario de $rad(V)$ por hipótesis de la proposición, tenemos que $V = U \oplus rad(V)$. Además, tenemos que U y $rad(V)$ son ortogonales entre sí porque $rad(V) \subseteq U^0$, luego, se tiene que $V = U \mathbin{\widehat{\oplus}} rad(V)$. □

Proposición 3.15. *Sean (V, Q) y $(\tilde{V}, \tilde{Q})$ dos espacios cuadráticos no degenerados. Entonces, se tiene que:*

I. *Todos los morfismos métricos de (V, Q) a $(\tilde{V}, \tilde{Q})$ son inyectivos.*

II. *Para todo subespacio U de V, se tiene*

$$U^{00} = U, \quad dim(U) + dim(U^0) = dim(V), \quad rad(U) = rad(U^0) = U \cap U^0.$$

Además, el espacio cuadrático U es no degenerado si y solo si U^0 es no degenerado y en ese caso se tiene que $V = U \mathbin{\widehat{\oplus}} U^0$.

III. *Si V es suma directa ortogonal de dos subespacios, es decir, $V = U_1 \mathbin{\widehat{\oplus}} U_2$ con U_1, U_2 subespacios de V, entonces U_1 y U_2 son no degenerados y ortogonales entre sí.*

Demostración. Primero, probamos I. Tomamos $f : V \longrightarrow \tilde{V}$ un morfismo métrico. Supongamos que $f(x) = 0$ y para ver que f es inyectiva, veamos que $x = 0$. Tomamos $y \in V$ cualquiera, como f es morfismo métrico, tenemos que $x.y = f(x).f(y) = 0$, luego tenemos que $x \in rad(V)$. Además por hipótesis, Q es no degenerada, es decir, $V^0 = \{0\}$, y por tanto, $x = 0$.

Veamos que se cumple el apartado II. Tomamos U subespacio de V, veamos que la aplicación lineal $q_U : V \longrightarrow U^*$ es sobreyectiva. Por el Lema 3.11, como Q es no degenerada, $q_V : V \longrightarrow V^*$ es isomorfismo, luego considerando q_U como la composición de q_V con la proyección canónica de V^* a U^* tenemos que q_U es sobreyectivo. Por otro lado, como U^0 es el núcleo de q_U tenemos que la sucesión

$$0 \longrightarrow U^0 \longrightarrow V \longrightarrow U^* \longrightarrow 0$$

es exacta. Utilizando la fórmula de las dimensiones tenemos que

$$dim(V) = dim(Ker(q_U)) + dim(Im(q_U)) = dim(U^0) + dim(U^*) = dim(U^0) + dim(U).$$

Empleando esta fórmula para U^0, tenemos que $dim(V) = dim(U^{00}) + dim(U^0)$ e igualando con la anterior, se tiene que $dim(U) = dim(U^{00})$. Como $U \subseteq U^{00}$, tenemos la igualdad, es decir, $U = U^{00}$. Veamos que $rad(U) = U \cap U^0$. Como

$$rad(U) = \{x \in U : x.y = 0 \text{ para todo } y \in U\},$$

tenemos que $x \in rad(U)$ si y solo si $x \in U$ y $x \in U^0$, es decir, $x \in U \cap U^0$. Para ver que $rad(U^0) = U \cap U^0$, vamos a utilizar la expresión que acabamos de probar, es decir, $rad(U^0) = U^0 \cap U^{00}$ y como $U = U^{00}$ tenemos que $rad(U^0) = U^0 \cap U$. Por último, veamos que el espacio cuadrático U es no degenerado si y solo si el espacio cuadrático U^0 no lo es. Sabemos que U es no degenerado si y solo si $rad(U) = \{0\}$ y como $rad(U) = rad(U^0)$, tenemos probado la doble implicación. Además, en el caso en que lo sean, como

$$dim(V) = dim(U) + dim(U^0) \quad \text{y} \quad U \cap U^0 = rad(U) = 0$$

tenemos que $V = U \oplus U^0$. Por definición de U^0, se tiene que U y U^0 son ortogonales entre sí, luego $V = U \mathbin{\widehat{\oplus}} U^0$.

Por último, probemos III. Por definición de suma directa ortogonal, los subespacios U_1 y U_2 son ortogonales entre sí, es decir, $U_2 \subseteq U_1^0$. Como la suma es directa,

$$dim(V) = dim(U_1) + dim(U_2), \text{ luego } dim(U_2) = dim(V) - dim(U_1)$$

y utilizando lo probado en II, $dim(U_2) = dim(U_1^0)$. Con todo ello, $U_2 = U_1^0$. Tomamos $x \in rad(U_1)$, luego es ortogonal a todos los elementos de U_1. Por estar en U_1 es ortogonal a todos los elementos de U_1^0, así es ortogonal a todos los elementos de $U_1 \oplus U_1^0 = V$ y como V es no degenerada, $x = 0$. □

Definición 3.16. *Sea (V, Q) un espacio cuadrático. Un elemento $x \in V$ se llama **isótropo** si $Q(x) = 0$. Un subespacio U de V se dice isótropo si todos sus elementos son isótropos.*

Como $x.y = 1/2((x+y).(x+y) - x.x - y.y)$, se tiene que U es isótropo si y solo si $U \subseteq U^0$, es decir, que la restricción de Q a U es la forma cuadrática nula.
En los razonamientos inductivos haremos uso de un tipo particular de subespacio cuadrático.

Definición 3.17. *Sea (V, Q) un espacio cuadrático con una base formada por dos elementos isótropos x e y tales que $x.y \neq 0$ se dice que es un **plano hiperbólico**.*

Sin pérdida de generalidad, podemos suponer que $x.y = 1$, luego la matriz de la forma cuadrática en la base $B = (x, y)$ del plano hiperbólico es

$$M_B(Q) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

donde $d(Q) = -1$, luego Q es no degenerada.

Proposición 3.18. *Sean (V, Q) un espacio cuadrático no degenerado y $x \in V$ un elemento isótropo no nulo. Entonces existe un subespacio U de V que es un plano hiperbólico y que contiene a x.*

Demostración. Como V es no degenerado, existe un $z \in V$ tal que $x.z = 1$. Consideramos $y = 2z - (z.z)x$ y veamos que es isótropo. Como $x.x = 0$ e $z.x = 1$, se cumple que

$$y.y = (2z - (z.z)x)^2 = 4(z.z) - 4(z.x)(z.z) + (z.z)^2(x.x) = 4(z.z) - 4(z.x)(z.z) = 0.$$

Además,

$$x.y = x.(2z - (z.z)x) = 2(x.z) - (z.z)(x.x) = 2(x.z) = 2 \neq 0.$$

Por tanto, el subespacio $U = \{\lambda_1 x + \lambda_2 y : \lambda_1, \lambda_2 \in k\}$ es un plano hiperbólico. □

Corolario 3.19. *Sea (V, Q) un espacio cuadrático no degenerado que contiene un elemento isótropo no nulo. Entonces, se cumple que $Q(V) = k$.*

Demostración. Por la Proposición 3.18, existe un subespacio U que es plano hiperbólico. Vamos a demostrar que $Q(U) = k$. Consideramos (x, y) una base de U con x e y isótropos y tales que $x.y = 1$. Tomamos $a \in k$ y veamos que existe un $v \in U$ tal que $v.v = a$. Tomamos $v = x + \frac{a}{2}y$, luego

$$(x + \frac{a}{2}y).(x + \frac{a}{2}y) = x.x + \frac{a}{2}x.y + \frac{a}{2}x.y + \frac{a}{4}y.y = 2\frac{a}{2}x.y = ax.y = a.$$

Por tanto, $Q(U) = k$ y, con ello, $Q(V) = k$. □

Definición 3.20. *Sean (V, Q) un espacio cuadrático con $dim(V) = n$ y $(e_1, \dots, e_n)$ una base. Se dice que es* ***base ortogonal*** *si todos sus elementos son ortogonales dos a dos.*

Con ello, la matriz de Q con respecto a una base ortogonal B es la matriz diagonal

$$M_B(Q) = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix},$$

donde si $x = \sum_{i=1}^{n} x_i e_i$ entonces $Q(x) = a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2$.

Teorema 3.21 (de diagonalización)**.** *Todo espacio cuadrático (V, Q) tiene una base ortogonal.*

Demostración. Tomamos $n = dim(V)$ y vamos a probar el resultado por inducción. Para $n = 1$, tenemos que toda base es ortogonal. Supongamos $dim(V) = n$ y que V es isótropo. En este caso, tenemos que $Q|_V \equiv 0$, luego todas las bases de V son ortogonales. Supongamos que V tiene un elemento no isótropo, esto es, existe $e_1 \in V$ tal que $e_1.e_1 \neq 0$. Llamamos $W := \{e_1\}^0$ y se tiene que $dim(W) = n - 1$. Como W es un hiperplano y $e_1 \notin W$, tenemos que $V = \langle e_1 \rangle \mathbin{\widehat{\oplus}} W$. Por hipótesis de inducción, W tiene una base ortogonal $(e_2, \dots, e_n)$ y, por tanto, $(e_1, \dots, e_n)$ es la base ortogonal que queríamos. □

Observación 3.22. *Como consecuencia, podemos decir que un espacio cuadrático (V, Q) es no degenerado si y solo si $d(Q) \neq 0$, puesto que escribiendo la matriz en forma diagonal ser no degenerado implica que $a_i \neq 0$ para todo i y como $det(M_B(Q)) = \prod_{i=1}^{n} a_i$ se tiene la equivalencia.*

Definición 3.23. *Dos bases ortogonales $(e_1, \dots, e_n)$ y $(e'_1, \dots, e'_n)$ de V son* ***contiguas*** *si tienen un elemento común, es decir, si existen i y j tales que $e_i = e'_j$.*

El siguiente teorema nos dice que dadas dos bases ortogonales podemos encontrar una sucesión finita de bases contiguas empezando en una de ellas y terminando en la otra. Emplearemos este resultado para probar que el invariante de Hasse está bien definido en el Capítulo 4.

Teorema 3.24. *Sean (V, Q) un espacio cuadrático de dimensión mayor o igual que 3 y $\boldsymbol{e} = (e_1, e_2, \dots, e_n)$ y $\boldsymbol{e'} = (e'_1, e'_2, \dots, e'_n)$ dos bases ortogonales de V. Entonces, existe una sucesión finita de bases ortogonales de V $\boldsymbol{e}^{(0)}, \boldsymbol{e}^{(1)}, \dots, \boldsymbol{e}^{(m)}$ con $\boldsymbol{e}^{(0)} = \boldsymbol{e}$, $\boldsymbol{e}^{(m)} = \boldsymbol{e'}$ y verificando también que para todo $0 \leq i < m$, $\boldsymbol{e}^{(i)}$ y $\boldsymbol{e}^{(i+1)}$ son contiguas.*

Demostración. Vamos a dividir la prueba en tres casos:

Supongamos que $(e_1.e_1)(e'_1.e'_1) - (e_1.e'_1)^2 \neq 0$, lo que implica que e_1 y e'_1 no son proporcionales y que el plano $P = \{\mu e_1 + \beta e'_1 : \mu, \beta \in k\}$ es no degenerado porque el discriminante es no nulo. Tenemos que existen vectores ortogonales ε_1 y ε'_1 de e_1 y e'_1, respectivamente. Luego, se tiene que

$$P = \langle e_1 \rangle \mathbin{\widehat{\oplus}} \langle \varepsilon_1 \rangle = \langle e'_1 \rangle \mathbin{\widehat{\oplus}} \langle \varepsilon'_1 \rangle.$$

Como P es no degenerado, $V = P \widehat{\oplus} P^0$, consideramos $(e_3'', \ldots, e_n'')$ base ortogonal de P^0. Con ello, podemos relacionar a **e** y a **e'** mediante la cadena de bases contiguas

$$\mathbf{e} = (e_1, e_2, \ldots, e_n) \to (e_1, \varepsilon_1, e_3'', \ldots, e_n'') \to (e_1', \varepsilon_1', e_3'', \ldots, e_n'') \to (e_1', e_2', \ldots, e_n') = \mathbf{e'}.$$

Supongamos que $(e_1.e_1)(e_2'.e_2') - (e_1.e_2')^2 \neq 0$. La demostración de este apartado es análogo al anterior, intercambiando e_1' por e_2'.

Supongamos que $(e_1.e_1)(e_i'.e_i') - (e_1.e_i')^2 = 0$ para $i = 1, 2$. Primero, veamos que existe un $\lambda \in k$ tal que $e_\lambda = e_1' + \lambda e_2'$ es un elemento no isótropo que genera un plano no degenerado con e_1. Para que e_λ no sea isótropo, se tiene que dar $e_\lambda.e_\lambda \neq 0$. Utilizando la definición de e_λ y que $\mathbf{e}'$ es base ortogonal, tenemos que $e_\lambda.e_\lambda = (e_1' + \lambda e_2'.e_1' + \lambda e_2') = (e_1'.e_1') + \lambda^2(e_2'.e_2')$. Por tanto, se tiene que cumplir

$$\lambda^2 \neq \frac{-e_1'.e_1'}{e_2'.e_2'}.$$

Además, para que genere un plano no degenerado con e_1 se tiene que verificar

$$(e_1.e_1)(e_\lambda.e_\lambda) - (e_1.e_\lambda)^2 \neq 0.$$

Desarrollamos la expresión,

$$(e_1.e_1)(e_\lambda.e_\lambda) - (e_1.e_\lambda)^2 = (e_1.e_1)(e_1'.e_1') + \lambda^2(e_1.e_1)(e_2'.e_2') - (e_1.e_1')^2 - 2\lambda(e_1.e_1')(e_1.e_2') - \lambda^2(e_1.e_2')$$

y por la ortogonalidad y la hipótesis del apartado tenemos que se cumple si y solo si $-2\lambda(e_1.e_1')(e_1.e_2') \neq 0$. Además, la hipótesis implica $(e_1.e_i')^2 \neq 0$ para $i = 1, 2$ luego basta que $\lambda \neq 0$. De este modo, solo tenemos que comprobar que

$$\lambda \neq 0 \quad \text{y} \quad \lambda^2 \neq \frac{-e_1'.e_1'}{e_2'.e_2'}.$$

Esto excluye, como mucho, 3 valores de k para elegir; por tanto, si $\#k \geq 4$ podemos garantizar la existencia de e_λ no isótropo. Si $k = \mathbb{F}_3$, como $(e_1.e_i') \neq 0$ entonces $(e_1.e_i')^2 = 1$, luego la hipótesis se puede reescribir como $(e_1.e_1)(e_i'.e_i') = 1$ si $i = 1, 2$, luego $(e_1'.e_1')/(e_2'.e_2') = 1$, basta tomar $\lambda = 1$ que cumple las condiciones requeridas. Tomamos dicho $e_\lambda = e_1' + \lambda e_2'$ no isótropo y consideramos el plano no degenerado $P = \{\mu e_1 + \beta e_\lambda : \mu, \beta \in k\}$. Como e_λ no es isótropo, existe e_2'' tal que (e_λ, e_2'') es base ortogonal de P. Consideramos **e"** $= (e_\lambda, e_2'', e_3', \ldots, e_n')$ base ortogonal de V que es contigua a **e'**. Por otro lado, como P es no degenerado y e_1 y e_λ verifican el primer punto de la demostración, tenemos que podemos relacionar **e** con **e"** y como **e"** es contigua a **e'**, el teorema está probado. □

Este teorema es válido para aquellos espacios cuadráticos con dimensión mayor que 3, veamos en el siguiente ejemplo que para dimensión 2 no se tiene por qué cumplir.

Ejemplo 3.25. *Consideremos en $\mathbb{R}^2$ el producto escalar estándar y las bases ortogonales $B_c = \big((1,0),(0,1)\big) = (e_1, e_2)$ y $B = \big((1,1),(1,-1)\big)$. Supongamos, sin pérdida de generalidad, que el elemento e_1 es el elemento común entre B_c y otra base ortogonal B_1, es decir, dada $B_1 = (v_1, v_2)$, se tiene que $v_1 = e_1$. Como B_1 también es base ortogonal, necesariamente se tiene que $v_2 = \alpha_1 e_2$ con $\alpha_1 \in \mathbb{R}$. Repitiendo este proceso un número finito de veces, se tendría la siguiente cadena de bases contiguas*

$$B_c \longrightarrow B_1 \longrightarrow \cdots \longrightarrow B_n = (\gamma_n e_1, \alpha_n e_2)$$

con $\gamma_n, \alpha_n \in \mathbb{R}$, en donde nunca se va a poder una cadena entre las bases ortogonales iniciales B_c y B.

Dados (V,Q) y $(\tilde{V},\tilde{Q})$ dos espacios cuadráticos no degenerados y U un subespacio vectorial de V tal que $s : U \longrightarrow \tilde{V}$ sea un morfismo métrico inyectivo, nuestro siguiente objetivo es mostrar cómo se puede extender s a todo V.

Teorema 3.26 (de Witt)**.** *Sean (V,Q) y $(\tilde{V},\tilde{Q})$ dos espacios cuadráticos isomorfos y no degenerados. Entonces, todo morfismo métrico inyectivo $s : U \longrightarrow \tilde{V}$ donde U es un subespacio vectorial de V se puede extender a un isomorfismo métrico de V en $\tilde{V}$.*

Demostración. Para esta prueba vamos a diferenciar dos casos, si U es degenerado y si U es no degenerado. En ambos casos, como por hipótesis (V,Q) y $(\tilde{V},\tilde{Q})$ son espacios cuadráticos isomorfos vamos a suponer $V = \tilde{V}$ y que $Q = \tilde{Q}$.

Supongamos que U es degenerado. Como U es degenerado, existe $x \in rad(U)$ no nulo. Como x es isótropo y V no degenerado, por la Proposición 3.18 tenemos que existe un subespacio de V que contiene a x y que es plano hiperbólico. Luego existe $y \in V$ tal que $x.y = 1$ e $y.y = 0$. Como y no es ortogonal a x, $y \notin U$ y el subespacio $U_1 = \langle y \rangle \mathbin{\widehat{\oplus}} U$ contiene a U como hiperplano. Como s es un morfismo métrico, $s(U)$ es degenerado luego existe $\tilde{y} \in V$ tal que $\tilde{y}.\tilde{y} = 0$ y $s(x).\tilde{y} = 1$. Definimos sobre U_1 la aplicación

$$s_1(z) = \begin{cases} s(z), & \text{si } z \in U \\ \tilde{y}, & \text{si } z = y \end{cases}$$

y tenemos que $s_1|_U = s$. Además, $dim(U_1) = dim(U) + 1$ y, por tanto, si U_1 es degenerado, repetimos este proceso y, en caso de que no lo sea, pasamos al caso siguiente.

Supongamos que U es no degenerado y vamos a probar este caso por inducción en $dim(U)$. Supongamos que $dim(U) = 1$, luego $U = \langle x \rangle$ con $x \in V$ y x no isótropo. Llamamos $y := s(x)$ y como s es morfismo métrico tenemos que $y.y = x.x$. Consideramos los elementos $x + y$ y $x - y$ y veamos que alguno de los dos no es isótropo; si ambos lo fueran tendríamos que

$$0 = Q(x+y) + Q(x-y) = 2(x.x) + 2(y.y) = 4(x.x)$$

y con ello, tendríamos que x es isótropo contradiciendo nuestra hipótesis. Sin pérdida de generalidad, supongamos que $z := x + y$ es el elemento no isótropo y llamamos H a su ortogonal. Por tanto, $V = \langle z \rangle \mathbin{\widehat{\oplus}} H$ y como $(x+y).(x-y) = 0$, tenemos que $(x-y) \in H$. Definimos el automorfismo σ como la simetría respecto de H, es decir, $\sigma|_H = Id|_H$ y $\sigma(w) = -w$ para todo $w \in \langle z \rangle$. De esta forma, $\sigma(x-y) = x-y$ y $\sigma(x+y) = -x-y$ y así, $\sigma(x) = -y$, puesto que $\sigma(x+y+x-y) = \sigma(x+y) + \sigma(x-y) = -x-y+x-y = -2y$ y con ello, el automorfismo $-\sigma$ extiende s a todo V.

Supongamos que para todo subespacio U con $dim(U) = n-1$ para un cierto $n \geq 2$ se cumple la existencia de un morfismo de extensión y veamos que se cumple para $dim(U) = n$. Como U es no degenerada podemos descomponer $U = U_1 \mathbin{\widehat{\oplus}} U_2$ con $U_1, U_2 \neq \{0\}$. Por hipótesis de inducción, tenemos que $s_1 = s|_{U_1}$ se puede extender a un automorfismo σ_1 de V. Consideramos $\widetilde{s} := \sigma_1^{-1} \circ s : U \longrightarrow \tilde{V} = V \longrightarrow V$ que es un morfismo métrico y tenemos que $\tilde{s}|_{U_1} = Id_{U_1}$.

Por otro lado, tenemos que $\tilde{s}(U_2) \subseteq U_1^0$ dado que si $x \in \tilde{s}(U_2)$ e $y \in U_1$, existe $a \in U_2$ tal que $\tilde{s}(a) = x$, es decir, $x.y = \tilde{s}(a).y = \tilde{s}(a).\tilde{s}(y) = a.y \underset{U_2 \subseteq U_1^0}{=} 0$, en conclusión, $x \in U_1^0$.

Consideramos $s_2 = \tilde{s}|_{U_2} : U_2 \longrightarrow U_1^0$ y, como s_2 es morfismo métrico inyectivo, por hipótesis

de inducción existe $\sigma_2 : U_1^0 \longrightarrow U_1^0$ que extiende a s_2.
Definimos

$$\tilde{\sigma}(w) = \begin{cases} Id(w), & \text{si } w \in U_1 \\ \sigma_2(w), & \text{si } w \in U_1^0 \end{cases}$$

y veamos que $\sigma := \sigma_1 \circ \tilde{\sigma}$ es el automorfismo que buscamos, es decir, que $\sigma|_U = s$.

$$\sigma(w)|_U = \begin{cases} \sigma_1(w), & \text{si } w \in U_1 \\ \sigma_1 \circ \sigma_2(w), & \text{si } w \in U_2 \end{cases} = \begin{cases} s_1(w), & \text{si } w \in U_1 \\ \sigma_1 \circ \tilde{s}(w), & \text{si } w \in U_2 \end{cases}$$
$$= \begin{cases} s(w), & \text{si } w \in U_1 \\ \sigma_1 \circ \sigma_1^{-1} \circ s(w), & \text{si } w \in U_2 \end{cases} = \begin{cases} s(w), & \text{si } w \in U_1 \\ s(w), & \text{si } w \in U_2 \end{cases} = s(w).$$

□

En la siguiente sección, emplearemos el Teorema de Witt para probar el Teorema de cancelación (Teorema 3.39) que es esencial para obtener la clasificación de formas cuadráticas.

Corolario 3.27. *Dos subespacios isomorfos de un espacio cuadrático no degenerado tienen ortogonales isomorfos.*

Demostración. Sean (V, Q) el espacio cuadrático y U_1 y U_2 los subespacios. Como son isomorfos, tomamos $\varphi : U_1 \longrightarrow U_2$ el isomorfismo y $s : U_1 \longrightarrow V$ el morfismo métrico definido como $s(u) := \varphi(u)$. Como por el Teorema de Witt existe un isomorfismo métrico σ tal que $\sigma|_{U_1} = s$ y $\sigma|_{U_1}(U_1) = s(U_1) = U_2$ basta probar $\sigma(U_1^0) = U_2^0$ y, por las propiedades de los morfismos métricos biyectivos, tenemos que $\sigma(U_1^0) = (\sigma(U_1))^0 = U_2^0$. □

3.2. Equivalencia de formas cuadráticas

En esta sección vamos a aplicar los resultados de la sección anterior al estudio de la resolución de equivalencia entre formas cuadráticas. En particular, emplearemos el Teorema de Witt para probar el Teorema de cancelación fundamental para los resultados de clasificación.

En lo que sigue, trabajaremos con formas cuadráticas definidas sobre k^n que denotaremos por $f(X_1, X_2, \ldots, X_n) = \sum_{i=1}^n a_{ii}X_i^2 + 2\sum_{i<j} a_{ij}X_iX_j$ y $A = (a_{ij})_{1\leq i,j\leq n}$ a la matriz simétrica correspondiente.

Definición 3.28. *Dos formas cuadráticas f y $\tilde{f}$ se llaman **equivalentes** si sus espacios cuadráticos son isomorfos. En ese caso, se escribe $f \sim \tilde{f}$.*

Además, si f y $\tilde{f}$ son equivalentes, entonces existen bases B_1 y B_2 de k^n, tales que $M_{B_1}(f) = M_{B_2}(\tilde{f})$. Luego, tenemos que $M_{B_2}(\tilde{f}) = M_{B_1}(f) = (M_{B_1B_2})^t M_{B_2}(f) M_{B_1B_2}$, donde $M_{B_1B_2}$ es la matriz de cambio de base de B_1 a B_2.

Definición 3.29. *Sean $f(X_1 \ldots, X_n)$ y $g(X_1, \ldots, X_m)$ dos formas cuadráticas en n y m variables y que forman (k^n, f) y (k^m, g) dos espacios cuadráticos, respectivamente. Definimos la **suma ortogonal** de f y g como la forma cuadrática*

$$f\dot{+}g(X_1, \ldots, X_n, X_{n+1}, \ldots, X_m) = f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m}).$$

De forma análoga, se define $f\dot{-}g := f\dot{+}(-g)$.

Notación 3.30. *En general, se denotan por $+$ y $-$ salvo que sea necesario utilizar el punto.*

Definición 3.31. *Sea $f(X_1, X_2)$ una forma cuadrática en dos variables, se dice que es una* ***forma hiperbólica*** *si se cumple que*

$$f \sim X_1 X_2$$

o, equivalentemente, que $f \sim X_1^2 - X_2^2$.

Observación 3.32. *Recordando la Definición 3.17 de plano hiperbólico, tenemos que el espacio (k^2, f) es un plano hiperbólico si y solo si f es una forma hiperbólica.*

Definición 3.33. *Sea $f(X_1, \ldots, X_n)$ una forma cuadrática. Se dice que* ***representa a un elemento*** *$a \in k$ si existe $x \in k^n$ no nulo tal que $f(x) = a$. Por definición, se tiene que f representa a 0 si y solo si el espacio cuadrático tiene un elemento isótropo no nulo.*

Una vez establecidas estas nociones, veamos algunos de los resultados que caracterizan cuándo una forma cuadrática representa a un determinado elemento.

Proposición 3.34. *Sea f una forma cuadrática no degenerada y que representa al 0. Se tiene que $f \sim f_0 + g$ donde f_0 es una forma hiperbólica. Además, f representa a todos los elementos de k.*

Demostración. Consideramos el espacio cuadrático (k^n, f) y recordando la Proposición 3.18, como existe un elemento isótropo no nulo por representar a 0, tenemos que existe un subespacio U de k^n que es plano hiperbólico. Como f es no degenerada, $k^n = U \mathbin{\widehat{\oplus}} U^0$ así que llamamos $f_0 := f|_U$ y $g := f|_{U^0}$ y tenemos que $f \sim f_0 + g$ con f_0 una forma hiperbólica. Además, por el Corolario 3.19, f representa a todo elemento de k. □

Corolario 3.35. *Sea $g = g(X_1, \ldots, X_{n-1})$ una forma cuadrática no degenerada y sea $a \in k^*$. Entonces, las siguientes afirmaciones son equivalentes:*

I. *Se cumple que g representa a a.*

II. *Se tiene que $g \sim h + aZ^2$ donde h es una forma cuadrática en $n-2$ variables.*

III. *La forma $f = g - aY^2$ representa a 0.*

Demostración. Probemos la equivalencia entre I y II por doble implicación. Supongamos que g representa a a, esto es, existe $x \in k^{n-1} \setminus \{0\}$ tal que $g(x) = a$. Consideramos $H := \{x\}^0$, tenemos que $k^n = H \mathbin{\widehat{\oplus}} \langle x \rangle$ porque g es no degenerada. En consecuencia, podemos escribir $g \sim h + aZ^2$ donde $h := g|_H$ y $g|_{\langle x \rangle} := aZ^2$. Recíprocamente, si se cumple II, consideramos $(0, \ldots, 0, 1) \neq 0$, como $g(0, \ldots, 0, 1) = h(0, \ldots, 0) + a = a$, tenemos que g representa a 0.

Veamos que II implica III. Por hipótesis, tenemos que $f = g - aY^2 \sim h + aZ^2 - aY^2$, así, $f(x_1, x_2, \ldots, x_n) = f(0, \ldots, 0, 1, 1) = 0$ y como $(0, \ldots, 0, 1, 1) \neq 0$, entonces f representa a 0.

Por último, veamos que III implica I. Supongamos que $f = g - aY^2$ representa a 0, luego existe $(x_1, x_2, \ldots, x_{n-1}, y) \neq 0$ tal que $f(x_1, x_2, \ldots, x_{n-1}, y) = 0$. Distinguimos dos posibilidades o bien $y = 0$ o $y \neq 0$. Si $y = 0$, tenemos que $g(x_1, \ldots, x_{n-1}) = 0$ con $(x_1, \ldots, x_{n-1}) \neq 0$, luego g representa a 0. Como f es no degenerada, por la Proposición 3.34, g representa a a. Si $y \neq 0$, entonces $g(x_1/y, x_2/y, \ldots, x_{n-1}/y) = a$ y, por tanto, g representa a a. □

Corolario 3.36. *Sean g y h dos formas cuadráticas no degeneradas y sea $f = g - h$. Entonces, las siguientes afirmaciones son equivalentes:*

I. *Se cumple que f representa a 0.*

II. *Existe $a \in k^*$ tal que es representado por g y por h.*

III. *Existe $a \in k^*$ tal que las formas $g - aZ^2$ y $h - aZ^2$ representan a 0.*

Demostración. La equivalencia entre II y III se sigue de la misma equivalencia del Corolario 3.35 para g y h, respectivamente.

Veamos la equivalencia de las dos primeras afirmaciones por doble implicación. Supongamos que f representa a 0. Escribiendo f en la forma $f(X,Y) = g(X) - h(Y)$, sabemos que existe $(x,y) \neq 0$ tal que $a = g(x) = h(y)$. Si $a \neq 0$, se cumple II. Supongamos que $a = 0$. Como $(x,y) \neq 0$ tenemos que o bien $x \neq 0$ o $y \neq 0$. Supongamos sin pérdida de generalidad que $x \neq 0$. Así, tenemos que g representa a 0. Por la Proposición 3.34 como g es no degenerada por hipótesis, tenemos que g representa a todos los elementos de k. En particular, también representará a todos los elementos de k^* representados por h que, al menos tiene uno por ser no degenerada.
Recíprocamente, supongamos que $a \in k^*$ es representado por g y por h. Esto es, existe x_1 tal que $g(x_1) = a$ y existe x_2 tal que $h(x_2) = a$. Tomamos $x = (x_1, x_2)$ y tenemos que $f(x) = g(x_1) - h(x_2) = a - a = 0$. En conclusión, f representa a 0. □

Seguidamente, veamos el resultado análogo al Teorema 3.21 (de diagonalización), que nos permite escribir una forma cuadrática como suma de cuadrados, siendo esta la forma más habitual de representarla.

Teorema 3.37. *Sea f una forma cuadrática en n variables. Entonces, existen $a_1, \ldots, a_n \in k$ tales que*

$$f \sim a_1X_1^2 + \cdots + a_nX_n^2.$$

Demostración. Directa a partir del Teorema 3.21. □

En esta representación, podemos identificar el rango de f fácilmente, pues es el número de términos a_i no nulos. Por otro lado, recordamos que el discriminante, $d(f)$, es o bien nulo si $det(f) = 0$ o bien la clase de $det(f)$ en k^*/k^{*2}. Con el mismo espíritu que en esta definición, a la hora de estudiar la representación diagonal de una forma cuadrática podemos limitarnos a considerar sus coeficientes en k^*/k^{*2}.

Lema 3.38. *Sea $f = a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$ una forma cuadrática de rango n, entonces es equivalente a $\bar{f} = \bar{a_1}X_1^2 + \bar{a_2}X_2^2 + \cdots + \bar{a_n}X_n^2$ donde cada $\bar{a_i}$, para todo $i \in \{1, \ldots, n\}$ es un representante cualquiera de la clase de a_i en k^*/k^{*2}.*

Demostración. Consideramos $B = (v_1, \ldots, v_n)$ una base de la forma cuadrática f tal que la matriz de f es

$$M_B(f) = A = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n \end{pmatrix}.$$

Para cada $i \in \{1, \ldots, n\}$ tomamos $\bar{a_i}$ un representante de la clase de a_i módulo k^*/k^{*2} y $\bar{A} = diag(\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n})$ denotará la correspondiente matriz diagonal. Queremos ver que existe $X \in Gl(n,k)$ tal que $\bar{A} = X^t \cdot A \cdot X$. Por otro lado, tenemos que $\bar{a_i} = \alpha_i^2 a_i$ con $\alpha_i \in k^*$ para todo i, $0 \leq i \leq n$. Tomamos

$$X = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix},$$

luego

$$\begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix} \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix} = \bar{A}.$$

Concluyendo así que f y $\bar{f}$ son equivalentes. □

Como consecuencia del Teorema de Witt obtenemos el siguiente teorema de cancelación.

Teorema 3.39. *Sean $f = g + h$ y $\tilde{f} = \tilde{g} + \tilde{h}$ dos formas cuadráticas no degeneradas. Si $f \sim \tilde{f}$ y $g \sim \tilde{g}$, entonces también $h \sim \tilde{h}$.*

Demostración. Supongamos que $k^{n+m} = U_n \widehat{\oplus} U_m$ es isomorfo a $k^{n+m} = \tilde{U}_n \widehat{\oplus} \tilde{U}_m$ con

$$f|_{U_n} := g \quad , f|_{\tilde{U}_n} := \tilde{g}, \quad f|_{U_m} := h \quad \text{y} \quad f|_{\tilde{U}_m} := \tilde{h}$$

por ser f y $\tilde{f}$ no degeneradas. Como $f \sim \tilde{f}$ y $g \sim \tilde{g}$ por hipótesis, tenemos que $U_n = \tilde{U}_n$. Por el Corolario 3.27, tenemos que $U_m \simeq \tilde{U}_m$ y, por tanto, $h \sim \tilde{h}$. □

Concluimos el capítulo estableciendo un resultado que nos permite descomponer una forma cuadrática separando la parte hiperbólica de la no hiperbólica.

Corolario 3.40. *Si f es una forma cuadrática, entonces*

$$f \sim g_0 + g_1 + \cdots + g_m + h$$

donde $g_1, \ldots, g_m$ son formas hiperbólicas y h no representa a 0. Además, esta descomposición es, salvo equivalencias, única.

Demostración. Consideramos f una forma cuadrática y tomamos $f \sim a_1 X_1^2 + \cdots + a_n X_n^2$ su representación vista en el Teorema 3.37. Separamos los a_i nulos de forma que nos quede $f \sim g_0 + g$ con $g_0 \sim 0$ y g no degenerada y distinguimos dos casos. Si g no representa a 0, tomamos $h := g$ y ya hemos acabado. Supongamos que g representa a 0 y por la Proposición 3.34 tenemos que existe g_1 una forma hiperbólica tal que $g \sim g_1 + h_1$ y repetimos recursivamente este proceso hasta llegar a h_r que no represente a 0. En conclusión, tenemos $f \sim g_0 + g_1 + \cdots + g_r + h_r$ con $g_0 \sim 0$, g_i formas hiperbólicas para $1 \leq i \leq r$ y h_r que no representa a 0. Además, la unicidad se deduce del teorema anterior. □

Capítulo 4

Formas cuadráticas en $\mathbb{Q}_p$

En este capítulo se presentan los elementos fundamentales que nos permiten establecer la clasificación de las formas cuadráticas sobre $\mathbb{Q}_p$. Para la elaboración del mismo se ha seguido [9, Capítulo III] en lo relativo al símbolo de Hilbert y [9, Capítulo IV] en lo relativo a los resultados de clasificación.

4.1. Formas cuadráticas en $\mathbb{F}_q$

Antes de empezar a trabajar con el cuerpo de los p-ádicos, vamos a tratar las formas cuadráticas en el cuerpo finito de q elementos, es decir, vamos a tomar $k = \mathbb{F}_q$ con $q = p^m$ y p un número primo distinto de 2 y $m \in \mathbb{N}_{\geq 1}$.

Proposición 4.1. *Sea una forma cuadrática f sobre $\mathbb{F}_q$ con rango n. Se tiene que*

- *Si $n \geq 3$, f representa a todos los elementos de $\mathbb{F}_q$.*
- *Si $n \geq 2$, f representa a todos los elementos de $\mathbb{F}_q^*$.*

Demostración. Para probar la primera afirmación, basta probar que toda forma cuadrática en 3 variables no degenerada representa a 0 y hacer uso de la Proposición 3.34. Escribimos $f = aX^2 + bY^2 + cZ^2$ con $a, b, c \in \mathbb{F}_q^*$. Para probar que f representa a 0 haremos uso del Corolario 3.35 y probaremos que $g = aX^2 + bY^2$ representa a c, es decir, que la ecuación $aX^2 + bY^2 = c$ tiene solución. Consideramos los conjuntos

$$A = \{ax^2 : x \in \mathbb{F}_q\} \quad \text{y} \quad B = \{bx^2 - c : x \in \mathbb{F}_q\}.$$

Como la mitad de los elementos de $\mathbb{F}_q^*$ son cuadrados, ver Apéndice A.8, añadiendo el cero vemos que ambos conjuntos tienen cardinal $1 + (q-1)/2 = (q+1)/2$, luego $A \cap B \neq \emptyset$. En conclusión, la ecuación tiene solución.

Para probar la segunda afirmación, basta observar que si g es una forma cuadrática de rango 2, entonces para todo $a \in \mathbb{F}_q^*$, $f = g - aZ^2$ es una forma cuadrática de rango 3. Utilizando lo que acabamos de probar f representa a todos los elementos de $\mathbb{F}_q$, en particular, a 0. Por el Corolario 3.35, g representa a todo $a \in \mathbb{F}_q^*$. □

Empleando que $\mathbb{F}_q^*/\mathbb{F}_q^{*2} \simeq \mathbb{Z}/2\mathbb{Z}$ cuya prueba puede encontrarse en el Lema A.8, el siguiente resultado establece que sobre $\mathbb{F}_q$ solo existen dos clases no equivalentes de formas cuadráticas no degeneradas.

Proposición 4.2. *Fijamos un elemento $a \in \mathbb{F}_q^*$ que no es un cuadrado. Toda forma cuadrática no degenerada de rango n sobre $\mathbb{F}_q$ es equivalente a*

$$X_1^2 + X_2^2 + \cdots + X_{n-1}^2 + X_n^2$$

o a

$$X_1^2 + X_2^2 + \cdots + X_{n-1}^2 + aX_n^2$$

dependiendo, respectivamente, si el discriminante es cuadrado o no.

Demostración. Vamos a probarlo por inducción sobre el rango n.
Dada f una forma cuadrática no degenerada con $rango(f) = n = 1$. Tenemos que $\mathbb{F}_q^*/\mathbb{F}_q^{*2}$ tiene dos elementos luego $f \sim X^2$ o $f \sim aX^2$. Ahora, supongamos que para un cierto $n \geq 2$, si $rango(f) < n$ se cumple y veamos que también se verifica para n. Como $n \geq 2$, por la Proposición 4.1 tenemos que f representa, en particular, a 1. Por el Corolario 3.35, tenemos que $f \sim g + X_1^2$ donde g es una forma cuadrática en $n-1$ variables y aplicando la hipótesis de inducción tenemos que o bien $f \sim X_1^2 + \cdots + X_{n-1}^2 + X_n^2$ o bien $f \sim X_1^2 + \cdots + X_{n-1}^2 + aX_n^2$. □

Sabemos que el discriminante y el rango son invariantes de las formas cuadráticas y por la proposición anterior se tiene el siguiente resultado.

Corolario 4.3. *Dos formas cuadráticas sobre $\mathbb{F}_q$ son equivalentes si y solo si tienen el mismo rango y el mismo discriminante.*

Ejemplo 4.4. *Consideramos en $\mathbb{F}_7$ las formas cuadráticas f y g con matrices A y B, respectivamente*

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 4 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 3 & 0 \\ 3 & 6 & 5 \\ 0 & 5 & 2 \end{pmatrix},$$

y veamos que no son equivalentes.

Tenemos que $\mathbb{F}_7^*/\mathbb{F}_7^{*2} = \{[1], [3]\}$, $rango(A) = rango(B) = 3$, $det(A) = 2$ y $det(B) = 5$, luego $d(f) = [1] \neq d(g) = [3]$ y por la Proposición 4.2, f y g no son equivalentes.

Estos resultados nos facilitan calcular el número de clases de formas cuadráticas en $\mathbb{F}_q$ que existen fijado un rango.

Ejemplo 4.5. *Si consideramos el cociente $S_n(\mathbb{F}_q)/\sim$ donde $S_n(\mathbb{F}_q)$ es el conjunto de matrices simétricas y $\sim$ es la relación de congruencia de matrices. Como los posibles rangos para las formas bilineales que define la relación son $\{0, 1, \ldots, n\}$ y para todos los rangos excepto el nulo, por la Proposición 4.2, hay dos posibles clases, tenemos que existen $2n + 1$ clases diferentes.*

4.2. Símbolo de Hilbert e invariante de Hasse

En las secciones previas hemos introducido dos invariantes para las formas cuadráticas: el rango y el discriminante. Para poder establecer la clasificación de formas cuadráticas sobre $\mathbb{Q}_p$ necesitamos incorporar nuevos invariantes dado que por ejemplo, $f = 2X^2 + 15Y^2 + 5Z^2$ y $g = X^2 + 3Y^2 + 7Z^2$ tienen el mismo rango y el mismo discriminante sobre $\mathbb{Q}_5$ pero no son

equivalentes como veremos en el Ejemplo 4.22.

Para poder definir el invariante de Hasse necesitamos introducir primero el símbolo de Hilbert así como algunas de sus propiedades.

Definición 4.6. *Sea k el cuerpo de los reales, $\mathbb{R}$, o el de los p-ádicos, $\mathbb{Q}_p$ y sean $a, b \in k^*$. El **símbolo de Hilbert** se denota por (a, b) y se dice que*

- $(a, b) = 1$ *si existe* $(x, y, z) \in k^3$ *no nulo tal que* $x^2 - ay^2 - bz^2 = 0$.
- $(a, b) = -1$ *en otro caso.*

Si es necesario precisar el cuerpo escribiremos $(a, b)_p$ en $\mathbb{Q}_p$ y $(a, b)_\infty$ en el caso real que por simplicidad denotamos por $\mathbb{Q}_\infty = \mathbb{R}$.

A partir de la definición podemos comprobar de forma directa que el símbolo de Hilbert verifica las siguientes propiedades.

Proposición 4.7. *El símbolo de Hilbert satisface las siguientes fórmulas:*

- $(a, b) = (b, a)$ *y* $(a, c^2) = 1$.
- $(a, -a) = 1$ *y* $(a, 1 - a) = 1$.
- *Si* $(a, b) = 1$, *entonces* $(aa', b) = (a', b)$.
- $(a, b) = (a, -ab) = (a, (1 - a)b)$.

Los siguientes resultados nos proporcionan caracterizaciones del símbolo de Hilbert, que nos permitan el cálculo de su valor y que nos ayudarán en las demostraciones de resultados posteriores. En este caso, no demostraremos todos los enunciados, encontrándose la prueba de los más relevantes en el Apéndice A o de manera más detallada en [9, Capítulo III] debido a que tienen un carácter más combinatorio y a las limitaciones de espacio.

Teorema 4.8. *Sean k un cuerpo y $a, b \in k^*$. Si $k = \mathbb{R}$, entonces $(a, b)_\infty = 1$ si a o b es positivo y $(a, b)_\infty = -1$ si a y b son negativos. Si $k = \mathbb{Q}_p$ y $a, b \in k^*$ son tales que $a = p^n u, b = p^m v$ con $u, v \in \mathbb{U}^p$. Se tiene que*

- *Si* $p \neq 2, (a, b)_p = (-1)^{nm\varepsilon(p)} \left(\frac{u}{p}\right)^m \left(\frac{v}{p}\right)^n$.
- *Si* $p = 2, (a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+n\omega(v)+m\omega(u)}$.

donde $\varepsilon(z) \equiv \frac{z-1}{2}$ *mod* 2, $\omega(z) \equiv \frac{z^2-1}{8}$ *mod* 2 *y* $\left(\frac{x}{y}\right)$ *representa el símbolo de Legendre.*

Teorema 4.9. *El símbolo de Hilbert es una forma bilineal simétrica no de-degenerada en el $\mathbb{F}_2$-espacio vectorial k^*/k^{*2}. En otras palabras, el símbolo de Hilbert satisface las siguientes propiedades:*

- *Para todos* $a, b \in k^*$ *se cumple que* $(a, b) = (b, a)$.
- *Para todo* $\lambda \in \mathbb{F}_2$ *y para todos* $a, b \in k^*$, *se cumple que* $(a^\lambda, b) = (a, b)^\lambda$.
- *Para todos* $a, a', b \in k^*$ *se cumple que* $(aa', b) = (a, b)(a', b)$.

- *El símbolo de Hilbert es no degenerado, es decir, si $b \in k^*$ es tal que $(a,b) = 1$ para todo $a \in k^*$ entonces $b \in k^{*2}$.*

Proposición 4.10. *Sean $a, b \in k^*$ y sea $k_b = k(\sqrt{b})$. Para que el símbolo de Hilbert $(a,b) = 1$ es necesario y suficiente que a esté en el grupo de las normas de los elementos de k_b^* denotado por Nk_b^*. En otras palabras, $(a,b) = 1$ si y solo si existen $z, y \in k$ tales que $a = z^2 - by^2$.*

Continuando con la misma notación que en los capítulos anteriores, llamamos $\mathcal{V}$ al conjunto de los números primos y el símbolo ∞. Recordamos que $\mathbb{Q}_\infty = \mathbb{R}$.

Teorema 4.11. *Si $a, b \in \mathbb{Q}^*$, entonces se cumple que $(a,b)_v = 1$ para todo $v \in \mathcal{V}$ excepto un número finito y se tiene que*

$$\prod_{v \in \mathcal{V}} (a,b)_v = 1.$$

Demostración. Como el símbolo de Hilbert es bilineal, basta probarlo tomando como posibles valores de a y b, -1 y los números primos. Para probarlo, utilizaremos el Teorema 4.8 y las propiedades del símbolo de Legendre, ver Teorema A.10. Distinguimos tres casos:

Primero, si $a = b = -1$, tenemos que $(-1,-1)_\infty = (-1,-1)_2 = -1$ y para $v \neq 2$ primo, $(-1,-1)_v = 1$.

Segundo, si $a = -1$ y $b = p$ primo, distinguimos casos. Si $p = 2$, tenemos que $(-1,2)_v = 1$ para todo $v \in \mathcal{V}$. Por el contrario, si $p \neq 2$, se tiene que $(-1,p)_2 = (-1,p)_p = (-1)^{\varepsilon(p)}$ y $(-1,p)_v = 1$ si $v \neq p$. Por tanto, el producto es 1.

Por último, tomamos $a = p$ y $b = p'$ con p, p' primos. Si $p' = p$, como por las propiedades del símbolo de Hilbert, se cumple que $(q,q) = (-1,q)$, caso probado en el párrafo anterior. Supongamos que $p \neq p'$. Si $p' = 2$, tenemos que $(p,2)_2 = (p,2)_p = (-1)^{\varepsilon(p)}$ y $(p,2)_v = 1$ si $v \neq 2$; por tanto, su producto es 1. Supongamos que $p' \neq 2$ y $p \neq 2$ y distinguimos casos: si $v = 2$, se cumple que $(p,p')_2 = (-1)^{\varepsilon(p)\varepsilon(p')}$ y si $v \neq 2$ tenemos que $(p,p')_p = \left(\frac{p'}{p}\right)$, $(p,p')_{p'} = \left(\frac{p}{p'}\right)$ y $(p,p')_v = 1$ si $v \notin \{p,p'\}$. Por tanto, por la Ley de Reciprocidad Cuadrática A.11, tenemos que el producto es 1. □

Teorema 4.12 (Teorema de Aproximación)**.** *Sea $\mathcal{S}$ un conjunto finito de $\mathcal{V}$. La imagen de $\mathbb{Q}$ en $\prod_{v \in \mathcal{S}} \mathbb{Q}_v$ es densa para la topología producto.*

Demostración. Supongamos que $\mathcal{S} = \{p_1, p_2, \ldots, p_n, \infty\}$ con los p_i números primos distintos es el conjunto finito. Tomamos $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n, \tilde{x}_\infty) \in \prod_{v \in \mathcal{S}} \mathbb{Q}_v$ y veamos que es adherente a $\mathbb{Q}$. En primer lugar, multipliquemos los $\tilde{x}_i$ por un entero de tal forma que obtengamos $(x_1, x_2, \ldots, x_n, x_\infty)$ con $x_i \in \mathbb{Z}_{p_i}$. Tenemos que probar que para todo $\varepsilon > 0$ y todo $N > 0$ existe un $x \in \mathbb{Q}$ tal que

$$|x - x_\infty| \leq \varepsilon \quad \text{y} \quad v_{p_i}(x - x_i) \geq N.$$

Notemos que si aplicamos el Teorema Chino de los Restos A.7 para $m_i = p_i^N$, tenemos que existe un $x_0 \in \mathbb{Z}$ tal que $v_{p_i}(x_0 - x_i) \geq N$ para todo $i \in \{1, \ldots, n\}$. Tomamos q un número coprimo a todos los p_i. Observamos que los números de la forma a/q^m con $a \in \mathbb{Z}$ y $m \in \mathbb{N}$ son densos en $\mathbb{R}$. Tomamos u de la forma a/q^m asegurando que sea próximo a $x_0 - x_\infty$ en $\mathbb{R}$, es decir, tal que

$$|x_0 - x_\infty + u p_1^N p_2^N \cdots p_n^N| \leq \varepsilon$$

y tenemos que el número racional $x = x_0 + up_1^N p_2^N \cdots p_n^N$ verifica las condiciones porque por cómo hemos escogido u tenemos que se verifica $|x - x_\infty| \leq \varepsilon$ y, utilizando las propiedades de v_p, tenemos que $v_{p_i}(x - x_i) \geq \min\left(v_{p_i}(x_0 - x_i), v_{p_i}(up_1^N \cdots p_n^N)\right) \geq N$. □

La última de las propiedades del símbolo de Hilbert que enunciaremos sin demostrar es el teorema de interpolación que fijado el valor de los símbolos de Hilbert nos asegura la existencia de un número racional con dichos valores, para más detalles ver Teorema A.15.

Teorema 4.13. *Sea $(a_i)_{i\in I}$ una familia finita de elementos de $\mathbb{Q}^*$ y sea $(\varepsilon_{i,v})_{i\in I, v\in\mathcal{V}}$ una familia de números de $\{\pm 1\}$. Se tiene que existe un $x \in \mathbb{Q}^*$ verificando $(a_i, x)_v = \varepsilon_{i,v}$ para todos $i \in I$ y $v \in \mathcal{V}$ si y solo si se verifican las siguientes condiciones:*

- *Casi todos los $\varepsilon_{i,v}$ excepto un número finito son 1.*
- *Para todo $i \in I$, $\prod_{v\in\mathcal{V}} \varepsilon_{i,v} = 1$.*
- *Para todo $v \in \mathcal{V}$ existe un $x_v \in \mathbb{Q}_v^*$ tal que $(a_i, x_v)_v = \varepsilon_{i,v}$ para todo $i \in I$.*

Una vez presentado el símbolo de Hilbert, estamos en condiciones de introducir el nuevo invariante de las formas cuadráticas.

Definición 4.14. *Sea (k^n, f) un espacio cuadrático y $\boldsymbol{e} = (e_1, \ldots, e_n)$ una base de k^n, denotamos $a_i = f(e_i)$. Consideramos la función ε dada por*

$$\varepsilon(\boldsymbol{e}) = \prod_{i<j} (a_i, a_j).$$

Por convenio, si $n = 1$, escribimos $\varepsilon(\boldsymbol{e}) = 1$.

Observación 4.15. *Como el símbolo de Hilbert (a, b) solo toma como valores ± 1, entonces $\varepsilon(\boldsymbol{e}) = \prod_{i<j}(a_i, a_j) = \pm 1$.*

Teorema 4.16. *El número $\varepsilon(\boldsymbol{e})$ no depende de la base $\boldsymbol{e}$ escogida.*

Demostración. Consideramos (k^n, f) un espacio cuadrático y $\mathbf{e} = (e_1, \ldots, e_n)$ una base de k^n y para demostrarlo, distinguimos tres casos.

Primero, si $n = 1$, tenemos que $\varepsilon(\mathbf{e}) = 1$.

Segundo, si $n = 2$, tenemos que $\varepsilon(\mathbf{e}) = (a_1, a_2)$. Empleando la definición del símbolo de Hilbert, $\varepsilon(\mathbf{e}) = 1$ si y solo si $g = Z^2 - a_1X^2 - a_2Y^2$ representa a 0. Por el Corolario 3.35, es equivalente a ver que $Q = a_1X^2 + a_2Y^2$ represente a $a = 1$, es decir, que exista $x \in k^2$ no nulo con $Q(x) = 1$ y esto no depende de $\mathbf{e}$.

Por último, supongamos que el invariante de Hasse no depende de la base escogida para toda forma cuadrática sobre k^{n-1} con $n \geq 3$ y veamos se cumple para n. Por el Teorema 3.24 basta probar que $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e'})$ si $\mathbf{e}$ y $\mathbf{e'}$ son contiguas. Supongamos que $e_1 = e_1'$, de esta forma $a_1 = e_1.e_1 = e_1'.e_1' = a_1'$. Utilizando las propiedades del símbolo de Hilbert se tiene que

$$\varepsilon(\mathbf{e}) = \prod_{i<j}(a_i, a_j) = (a_1, a_2 \cdots a_n) \prod_{2\leq i<j} (a_i, a_j) = (a_1, d(f)a_1) \prod_{2\leq i<j} (a_i, a_j).$$

Por otro lado,

$$\varepsilon(\mathbf{e'}) = \prod_{i<j}(a_i', a_j') = (a_1, d(f)a_1) \prod_{2\leq i<j} (a_i', a_j')$$

y aplicando la hipótesis de inducción, tenemos que

$$\prod_{2\leq i<j} (a_i, a_j) = \prod_{2\leq i<j} (a_i', a_j').$$

Por tanto, se cumple que $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e'})$. □

Observación 4.17. *Por el teorema anterior, concluimos que $\varepsilon(\mathbf{e})$ es un invariante, lo denotamos por $\varepsilon(f)$ y lo denominamos* ***invariante de Hasse*** *de (k^n, f), como en [7].*

4.3. Representaciones de elementos de $\mathbb{Q}_p$ por una forma cuadrática

En esta sección, daremos caracterizaciones para ver cuándo una forma cuadrática f representa a un elemento $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Recordemos que nuestro objetivo es determinar cuándo dos formas son equivalentes. Claramente, cuando son equivalentes representan los mismos elementos; no obstante, y pese a que el recíproco no es cierto, también nos ayuda en la clasificación conocer qué elementos representan. Para ello, primero recordamos los resultados de la Sección 2.5, en concreto de los Corolarios 2.39 y 2.41, en los que se veía que el orden de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ es 2^r con $r = 3$ si $p = 2$ y $r = 2$ si $p \neq 2$. El siguiente lema que nos será útil para las demostraciones de esos resultados sobre representación.

Lema 4.18. *Sean $a, a' \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, $\varepsilon, \varepsilon' \in \{\pm 1\}$ y $r = 3$ si $p = 2$ o $r = 2$ si $p \neq 2$. Consideramos el conjunto*

$$H_a^\varepsilon = \{x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} : (x, a) = \varepsilon\}.$$

Entonces se tiene que:

- *Si $a = 1$, H_a^1 tiene 2^r elementos y $H_a^{-1} = \emptyset$. Si $a \neq 1$, H_a^ε tiene 2^{r-1} elementos.*
- *Si H_a^ε y $H_{a'}^{\varepsilon'}$ son conjuntos no vacíos, se tiene que $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ si y solo si $a = a'$ y $\varepsilon = -\varepsilon'$.*

Demostración. Probemos primero que si $a = 1$ entonces $\#(H_a^1) = 2^r$. Por la definición del símbolo de Hilbert se tiene que $(x, 1) = 1$, luego $\#(H_a^1) = \#(\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}) = 2^r$ y $\#(H_a^{-1}) = \emptyset$. Supongamos que $a \neq 1$, consideremos el homomorfismo $\psi : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \longrightarrow \{\pm 1\}$ definido como $\psi(b) := (a, b)$, tenemos que $Ker(\psi) = H_a^1$ y que es sobreyectiva por el Teorema 4.9 al ser el símbolo de Hilbert no degenerado. Empleando que $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}/H_a^1 \simeq \{\pm 1\}$, tenemos que $\#(H_a^1) = 2^{r-1}$. Por otro lado, H_a^{-1} es el complementario del conjunto anterior y, por ello, $\#(H_a^{-1}) = 2^r - 2^{r-1} = 2^{r-1}$. En conclusión, H_a^ε tiene 2^{r-1} elementos.

En segundo lugar, veamos que si H_a^ε y $H_{a'}^{\varepsilon'}$ son conjuntos no vacíos, entonces su intersección es vacía si y solo si $a = a'$ y $\varepsilon = -\varepsilon'$. Probamos en primer lugar, la implicación directa; por el primer apartado, tenemos que tanto a como a' son distintos de 1 y que H_a^ε

tiene 2^{r-1} elementos. Por ello, y como $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$, los conjuntos son complementarios. En consecuencia, tenemos que $H_a^\varepsilon = H_{a'}^{-\varepsilon'}$. Sabemos que H_a^1 es complementario de H_a^{-1}, veamos qué ocurre con H_a^1 y $H_{a'}^1$. Pero como $1 \in H_a^1$ y $1 \in H_{a'}^1$, tenemos que ambos conjuntos son iguales. Con ello, tenemos que $(x, a) = (x, a')$ para todo $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Como el símbolo de Hilbert es no degenerado por el Teorema 4.9, tenemos que $a = a'$. Concluimos así que si los conjuntos son disjuntos entonces $a = a'$ y $\varepsilon = \varepsilon'$.

Recíprocamente, si $a = a'$ y $\varepsilon = -\varepsilon'$. Como por hipótesis, H_a^ε y $H_{a'}^{\varepsilon'}$ son no vacíos, por el apartado anterior concluimos que $a \neq 1$. Razonamos por reducción al absurdo y supongamos que $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} \neq \emptyset$, en ese caso tendríamos que

$$\#(H_a^\varepsilon \cup H_a^{-\varepsilon}) = \#H_a^\varepsilon + \#H_a^{-\varepsilon} - \#(H_a^\varepsilon \cap H_a^{-\varepsilon}) = 2^r - \#(H_a^\varepsilon \cap H_a^{-\varepsilon}) < 2^r,$$

lo cual sería absurdo. En conclusión, H_a^ε y $H_a^{\varepsilon'}$ son disjuntos. □

Observamos que si una forma cuadrática representa a $a \in \mathbb{Q}_p^*$, entonces a representa a todo elemento de la misma clase que a en $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Para ello, vamos a denotar $f^a := f - aZ^2$ y por el Corolario 3.35, sabemos que f^a representa a 0 si y solo si f representa a a. En primer lugar, veamos la relación existente entre el discriminante y el invariante de Hasse de f^a y f en el siguiente lema.

Lema 4.19. *Sean f una forma cuadrática de rango n, $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ y $f^a := f - aZ^2$. Entonces se cumple que*

$$d(f^a) = -d(f) \cdot a \qquad y \qquad \varepsilon(f^a) = \varepsilon(f)(-a, d(f)).$$

Demostración. Por el Teorema 3.37, $f^a = a_1X_1^2 + \cdots + a_nX_n^2 - aZ^2$. De este modo, tenemos que su discriminante es

$$d(f^a) = a_1a_2 \cdots a_n(-a) = -d(f) \cdot a$$

Por otro lado, empleando la definición del invariante de Hasse

$$\varepsilon(f^a) = (a_1, a_2) \cdots (a_1, a_n)(a_1, -a)(a_2, a_3) \cdots (a_2, a_n)(a_2, -a) \cdots (a_n, -a).$$

Utilizando las propiedades del símbolo de Hilbert tenemos que

$$\varepsilon(f^a) = \varepsilon(f)(-a, a_1a_2 \cdots a_n) = \varepsilon(f)(-a, d(f)).$$

□

Una vez tenemos relacionados estos invariantes, veamos las propiedades que se tienen que verificar en f para que represente a 0 o a $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ según los distintos rangos n.

Teorema 4.20. *Sea f una forma cuadrática de rango n sobre k con $k = \mathbb{R}$ o $k = \mathbb{Q}_p$. Denotamos por $d(f) = d$ y $\varepsilon(f) = \varepsilon$. Para los distintos valores de n, se tiene que:*

I. *Si $n = 2$, f representa a 0 si y solo si $d = -1$.*

II. *Si $n = 1$, f representa a a si y solo si $a = d$.*

III. *Si $n = 3$, f representa a 0 si y solo si $\varepsilon = (-1, -d)$.*

IV. *Si $n = 2$, f representa a a si y solo si $(a, -d) = \varepsilon$.*

Exclusivamente, en el caso $k = \mathbb{Q}_p$ se tiene que:

v. *Si $n = 4$, f representa a 0 si y solo si $d \neq 1$ o $d = 1$ y $\varepsilon = (-1, -1)$.*

vi. *Si $n = 3$, f representa a a si y solo si $a \neq -d$ o $a = -d$ y $\varepsilon = (-1, -d)$.*

vii. *Para $n \geq 5$, f siempre representa a 0.*

viii. *Para $n \geq 4$, f siempre representa a a.*

Demostración. Por el Teorema 3.37, sabemos que $f \sim a_1X_1^2 + \cdots + a_nX_n^2$. Sin pérdida de generalidad, empleando el Lema 3.38 trabajaremos con las clases de los coeficientes a_i en k^*/k^{*2} que, abusando de la notación, denotaremos también por a_i. Para los casos en los que hay que demostrar que f representa a $a \in k^*/k^{*2}$ emplearemos las relaciones del Lema 4.19 y denotaremos por $d_a = d(f^a)$ y $\varepsilon_a = \varepsilon(f^a)$ para simplificar la notación. Pasamos a distinguir los diferentes casos.

i. Si $n = 2$, tenemos que $f \sim a_1X_1^2 + a_2X_2^2$. Por tanto, f representa a 0 si y solo si $-a_1/a_2$ es cuadrado, es decir, $-a_1/a_2 = 1$ en k^*/k^{*2}. Como $-a_1/a_2 = -a_1a_2 = -d$ en k^*/k^{*2}, tenemos que f representa a 0 si y solo si $d = -1$.

ii. Por i, tenemos que f^a representa a 0 si y solo si $d_a = -1$. Utilizando el Lema 4.19, esta condición es equivalente a $d_a = -da = -1$, es decir, $da = 1$. Como $a^2 = 1$, concluimos que, f representa a 0 si y solo si $d = a$.

iii. Si $n = 3$, tenemos que $f \sim a_1X_1^2 + a_2X_2^2 + a_3X_3^3$ representa a 0 si y solo si $-a_3f \sim -a_3a_1X_1^2 - a_3a_2X_2^2 - X_3^2$ representa a 0. Utilizando la definición de símbolo de Hilbert, esto se cumple si y solo si $(-a_3a_1, -a_3a_2) = 1$. Desarrollamos el término de la izquierda, utilizando la bilinealidad del símbolo y que $(a_3, -a_3) = 1$, tenemos que

$$\begin{aligned}(-a_3a_1, -a_3a_2) &= (-1,-1)(-1,a_3)(-1,a_2)(a_3,-a_3)(a_3,a_2)(a_1,-1)(a_1,a_3)(a_1,a_2)\\ &= (-1,-1)(-1,a_1a_2a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)\\ &= (-1,-1)(-1,d)\varepsilon = (-1,-d)\varepsilon.\end{aligned}$$

Por tanto, que f represente a 0 es equivalente a que se cumpla $(-1, -d)\varepsilon = 1$, es decir, $\varepsilon = (-1, -d)$.

iv. Por el apartado iii, f^a representa a 0 para $n = 3$ si y solo si $\varepsilon_a = (-1, -d_a)$. De esta forma, por un lado tenemos que $\varepsilon_a = (-1, -d_a) = (-1, da) = (-1, a)(-1, d)$ y por otro lado, $\varepsilon_a = \varepsilon(d, -a) = \varepsilon(d, -1)(d, a)$. Igualando las expresiones tenemos que

$$(-1, a) = \varepsilon(d, a)$$

y multiplicando a ambos lados por (a, d), se tiene que $(-1, a)(a, d) = \varepsilon$. Aplicando las propiedades del símbolo de Hilbert, $\varepsilon = (a, -d)$.

v. Si $n = 4$, por el Corolario 3.36 tenemos que $f \sim a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$ representa a 0 si y solo si $g = a_1X_1^2 + a_2X_2^2$ y $h = -a_3X_3^2 - a_4X_4^2$ representan un mismo $b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Por el apartado IV, como g y h tienen $n = 2$, representan a $b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ si y solo si $(b, -d(g)) = \varepsilon(g)$ y $(b, -d(h)) = \varepsilon(h)$. En otras palabras, se tiene que cumplir

$$(b, -a_1a_2) = (a_1, a_2) \quad \text{y} \quad (b, -a_3a_4) = (-a_3, -a_4).$$

Consideramos los siguientes conjuntos $A = \{b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} : (b, -a_1a_2) = (a_1, a_2)\}$ y $B = \{b \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} : (b, -a_3a_4) = (-a_3, -a_4)\}$ y tenemos que f representa a 0 si y solo si $A \cap B \neq \emptyset$. Observamos que $A = H_{-a_1a_2}^{(a_1,a_2)}$ y $B = H_{-a_3a_4}^{(-a_3,-a_4)}$, luego por el Lema 4.18, tenemos que

$$A \cap B = \emptyset \iff \begin{cases} a_1a_2 = a_3a_4 \\ (a_1, a_2) = -(-a_3, -a_4). \end{cases}$$

De la primera condición, deducimos que $d = a_1a_2a_3a_4 = (a_1a_2)^2$ es un cuadrado, es decir, $d = 1$. Usando las propiedades del símbolo de Hilbert tenemos que

$$\begin{aligned} \varepsilon &= (a_1, a_2)(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)(a_3, a_4) = (a_1, a_2)(a_1, a_3a_4)(a_2, a_3a_4)(a_3, a_4) \\ &= (a_1, a_2)(a_1a_2, a_3a_4)(a_3, a_4). \end{aligned}$$

Como $a_1a_2 = a_3a_4$, se tiene que

$$\varepsilon = (a_1, a_2)(a_3a_4, a_3a_4)(a_3, a_4) = (a_1, a_2)(-1, a_3a_4)(a_3, a_4).$$

Como $(a_1, a_2) = -(-a_3, -a_4)$, se cumple que

$$\begin{aligned} \varepsilon &= -(-a_3, -a_4)(-1, a_3a_4)(a_3, a_4) = -(-1, -a_4)(a_3, -a_4)(-1, a_3)(-1, a_4)(a_3, a_4) \\ &= -(-1, -a_4^2)(a_3, -a_4)^2 = -(-1, -1). \end{aligned}$$

De esta forma, tenemos que f representa a 0 en $n = 4$ si y solo si $d \neq 1$ o si $d = 1$ y $\varepsilon = (-1, -1)$.

VI. Utilizando V f representa a a, para $n = 3$, si y solo si o bien $d_a \neq 1$ o bien $d_a = 1$ y $\varepsilon_a = (-1, -1)$.
En el caso $d_a \neq 1$, como $1 \neq d_a = -da$, multiplicando a ambos lados por a, tenemos que $a \neq -d$ probando la primera posibilidad.
En el caso $d_a = 1$, de forma análoga a la anterior tenemos que $a = -d$. Además, también se verifica $\varepsilon_a = (-1, -1)$ y usando de nuevo el Lema 4.19, tenemos que

$$\varepsilon_a = \varepsilon(-a, d) = (-1, -1).$$

Multiplicando a ambos lados por $(-a, d)$ y usando las propiedades del símbolo de Hilbert y que $a = -d$ se concluye que

$$\varepsilon = (-1, -1)(-a, d) = (-1, -1)(d, d) = (-1, -1)(-1, d) = (-1, -d).$$

VII. Vamos a probarlo para $n = 5$. Por el apartado I, dada una forma cuadrática de rango 2, si $d = -1$, representa a 0.
Si $d \neq -1$, por el apartado IV, observamos que toda forma de rango 2 representa a $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ si y solo si $\varepsilon = (x, -d)$. Consideramos el conjunto H_{-d}^{ε} y por el Lema 4.18, existen al menos 2^{r-1} elementos representados por una forma cuadrática de rango 2.

En cualquiera de los casos, una forma cuadrática de rango 2 representa al menos 2^{r-1} elementos y necesariamente lo mismo ocurre para una forma de rango 5, como f. Como $2^{r-1} \geq 2$, f representa al menos dos elementos de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. En consecuencia, existe un $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, $a \neq d$ tal que f representa a a, es decir, por el Corolario 3.35, $f \sim aX^2 + g$ con g una forma cuadrática en $n = 4$ variables. Como $d(g) = d/a \neq 1$, por el apartado v, g representa a 0 y tomando $X = 0$, tenemos que f representa a 0.

viii. Repitiendo el mismo razonamiento que hemos utilizado a lo largo de la demostración, si f^a para $n = 5$ representa a 0 siempre, entonces f siempre representa a a.

□

En la siguiente tabla se resumen las diferentes situaciones del teorema anterior.

f representa a	0	a
$n = 1$	Nunca	$a = d$
$n = 2$	$d = -1$	$\varepsilon = (a, -d)$
$n = 3$	$\varepsilon = (-1, -d)$	$a \neq -d$ o $a = -d$ y $\varepsilon = (-1, -d)$
$n = 4$	$d \neq 1$ o $d = 1$ y $\varepsilon = (-1, -1)$	Siempre
$n \geq 5$	Siempre	Siempre

4.4. Clasificación de las formas cuadráticas en $\mathbb{Q}_p$

Gracias a los resultados sobre representación de elementos y al teorema de cancelación podemos dar la clasificación de las formas cuadráticas sobre $k = \mathbb{Q}_p$.

Teorema 4.21. *Dos formas cuadráticas sobre $\mathbb{Q}_p$ son equivalentes si y solo si tienen el mismo rango, el mismo discriminante y el mismo invariante de Hasse.*

Demostración. De forma directa se tiene que si f y g son formas cuadráticas equivalentes, sus invariantes son los mismos por lo probado en las secciones previas.
Para demostrar el recíproco, vamos a aplicar inducción sobre el rango n de las dos formas cuadráticas f y g.

Para $n = 1$, por el Teorema 4.20, dadas f y g dos formas cuadráticas con $d = d(f) = d(g)$, entonces f y g representan los mismos valores, de hecho, se tiene que $f \sim dX^2 \sim g$.

Supongamos que para todas f y g formas cuadráticas de rango $n - 1$ para algún $n \geq 2$ con mismos invariantes entonces son equivalentes y veamos que también se verifica para n. Tomamos f y g dos formas cuadráticas con el mismo rango, mismo discriminante y mismo invariante de Hasse. Por el Teorema 4.20, f y g representan a los mismos valores de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Fijamos $a \in \mathbb{Q}_p^*$ representado por ambas formas cuadráticas y escribimos

$$f \sim aZ^2 + \tilde{f} \qquad \text{y} \qquad g \sim aZ^2 + \tilde{g}$$

donde $\tilde{f}$ y $\tilde{g}$ son formas cuadráticas de rango $n - 1$. Por el Lema 4.19, notemos que

$$d(\tilde{f}) = ad(f) = ad(g) = d(\tilde{g}),$$

$$\varepsilon(\tilde{f}) = \varepsilon(f)(a, d(\tilde{f})) = \varepsilon(g)(a, d(\tilde{g})) = \varepsilon(\tilde{g}).$$

Aplicando la hipótesis de inducción, $\tilde{f} \sim \tilde{g}$ y, por el Teorema 3.39, $f \sim g$. □

Ejemplo 4.22. *Al inicio de la Sección 4.2, dijimos que las formas $f = 2X^2 + 15Y^2 + 5Z^2$ y $g = X^2 + 3Y^2 + 7Z^2$ no eran equivalentes en $\mathbb{Q}_5$ a pesar de tener el mismo discriminante $d(f) = d(g) = 1$ y mismo rango. Por el teorema anterior sabemos que para serlo, también tienen que tener el mismo invariante de Hasse, veamos que esto no es así.*

$$\varepsilon(f) = (2, 15)(2, 5)(15, 5) = (2, 75)(15, 5),$$

y aplicando el Teorema 4.8, tenemos que $(2, 75) = 1$ y $(15, 5) = -1$. Por tanto $\varepsilon(f) = -1$.

$$\varepsilon(g) = (1, 3)(1, 7)(3, 7),$$

y de nuevo, por el Teorema 4.8, tenemos que $\varepsilon(g) = 1$. En conclusión, f y g no son equivalentes por no tener el mismo invariante de Hasse.

A partir del Teorema 4.21, se deduce la unicidad de la forma cuadrática de rango 4 que no representa a 0.

Corolario 4.23. *Toda forma cuadrática sobre $\mathbb{Q}_p$ de rango $n = 4$ que no representa a 0 es equivalente $Z^2 - aX^2 - bY^2 + abT^2$ con $(a, b) = -1$.*

Demostración. Por el Teorema 4.20, sabemos que la forma cuadrática f no representa a 0 si y solo si $d = 1$ y $\varepsilon(f) = -(-1, -1)$ y por el Teorema 4.21 todas las formas cuadráticas con estas propiedades son equivalentes. Consideramos $f = Z^2 - aX^2 - bY^2 + abT^2$ con $(a, b) = -1$ y veamos que verifica estas condiciones. Aplicando la definición de ε y las propiedades del símbolo de Hilbert,

$$\begin{aligned}\varepsilon(f) &= (1, -a)(1, -b)(1, ab)(-a, -b)(-a, ab)(-b, ab) = (1, ab)(1, ab)(-a, -b)(-a, ab)(-b, ab)\\ &= (-1, -1)(-1, b)(a, -b)(ab, ab) = (-1, -1)(-1, b)(a, -1)(a, b)(ab, ab)\\ &= -(-1, -1)(-1, ab)(ab, ab) = -(-1, -1)(-ab, ab) = -(-1, -1).\end{aligned}$$

Por otro lado, por la definición de discriminante, tenemos que

$$d(f) = -a(-b)(ab) = (ab)^2 = 1 \text{ en } \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}.$$

Concluyendo toda forma cuadrática de rango $n = 4$ que no representa a 0 es equivalente a f. □

Seguidamente, veamos el resultado que nos permite caracterizar cuándo existe una forma cuadrática de rango n, discriminante d e invariante ε.

Proposición 4.24. *Sean $n \geq 1$, $d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ y $\varepsilon = \pm 1$. Se tiene que existe una forma cuadrática f de rango n, discriminante $d(f) = d$ e invariante de Hasse ε si y solo si*

- *O bien $n = 1$ y $\varepsilon = 1$.*
- *O bien $n = 2$, $d \neq -1$ o $\varepsilon = 1$.*

- *O bien* $n \geq 3$.

Demostración. Para $n = 1$ se deduce directamente de la Definición 4.14 de invariante de Hasse.

Para el caso $n = 2$, consideramos la forma $f = a_1X_1^2 + a_2X_2^2$. Supongamos que $d(f) = -1$, aplicando las propiedades del símbolo de Hilbert, se tiene que

$$\varepsilon(f) = (a_1, a_2) = (a_1, -a_1a_2) = (a_1, 1) = 1,$$

por tanto, si $d = -1$, entonces $\varepsilon = 1$. En consecuencia, no se cumple que $d = -1$ y $\varepsilon = -1$. Recíprocamente, si $\varepsilon = 1$ consideramos la forma cuadrática $f = X^2 - Y^2$ y si $d \neq -1$ entonces $H^{\varepsilon}_{-d} \neq \emptyset$ y tomamos $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ tal que $(a, -d) = \varepsilon$ y consideramos $g = aX^2 + adY^2$ que cumple $d(g) = a^2d = d$ y que $\varepsilon(g) = (a, ad) = (a, -d) = \varepsilon$.

Si $n = 3$, tomamos $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ tal que $a \neq -d$, es decir, $ad \neq -1$. Por lo probado en el párrafo anterior, existe una forma cuadrática g de rango $n \geq 2$ con $d(g) = ad$ y $\varepsilon(g) = \varepsilon(a, -d)$. Basta tomar la forma cuadrática $f = aX^2 + g$ que cumple que $d(f) = ad(g) = a^2d = d$ y que $\varepsilon(f) = \varepsilon(g)(a, -d) = \varepsilon$.

Para $n \geq 4$, basta con tomar la forma g de rango 3 con los invariantes necesarios y considerar $f = g(X_1, X_2, X_3) + X_4^2 + \cdots + X_n^2$. □

Empleando los Corolarios 2.39 y 2.41, tenemos el siguiente resultado.

Corolario 4.25. *El número de clases de equivalencia de formas cuadráticas de rango n sobre* $\mathbb{Q}_p$*,*

- *Para* $p \neq 2$ *es:*

n	Número de clases
$n = 1$	4
$n = 2$	7
$n \geq 3$	8

- *Para* $p = 2$ *es:*

n	Número de clases
$n = 1$	8
$n = 2$	15
$n \geq 3$	16

Demostración. Primero, supongamos que $p \neq 2$ con p primo y por el Corolario 2.39, tenemos que $\#(\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}) = 4$, por tanto, el número de clases de formas cuadráticas para $n = 1$ es 4. Si $n = 2$, y $d \neq -1$, hay 3 posibles elecciones para d y 2 para ε por cada una y si $d = -1$, $\varepsilon = 1$. Por tanto, hay $3 \cdot 2 + 1 = 7$ posibles clases. Para $n = 3$ como hay 4 posibilidades para d y dos para ε, en total hay 8 clases.

Para el caso de $p = 2$, razonando de forma análoga y teniendo en cuenta que el cardinal de $\mathbb{Q}_2/\mathbb{Q}_2^{*2}$ es 8, para $n = 1$ hay 8 posibles clases, para $n = 2$, 15 y para el caso $n = 3$ hay 16 posibles clases. □

Capítulo 5

Clasificación de las formas cuadráticas en $\mathbb{Q}$

Para concluir el trabajo probaremos el Teorema de Minkowski que nos permite determinar cuándo las formas cuadráticas racionales son equivalentes.

5.1. Formas cuadráticas en $\mathbb{R}$

Antes de abordar al Teorema de Minkowski vamos a hacer un pequeño repaso de las formas cuadráticas en el cuerpo de los números reales $\mathbb{R}$ cuyos resultados podemos encontrar en [6, Capítulo 10].

Teorema 5.1. *Sea V un $\mathbb{R}$-espacio vectorial de dimensión finita y f una forma cuadrática de rango p. Entonces existe una base $B = (v_1, \ldots, v_n)$ de V tal que su matriz es de la forma*

$$M_B(f) = diag(\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{-1, -1, \ldots, -1}_{s}, 0, \ldots, 0),$$

con $r + s = p$.

Teorema 5.2 (Ley de inercia de Sylvester)**.** *Sea V un $\mathbb{R}$-espacio vectorial de dimensión finita y f una forma cuadrática sobre $\mathbb{R}$. Supongamos que existen bases $B = (v_1, v_2, \ldots, v_n)$ y $\tilde{B} = (\tilde{v_1}, \tilde{v_2}, \ldots, \tilde{v_n})$ tales que*

$$M_B(f) = diag(\underbrace{1, 1, \ldots, 1}_{r}, \underbrace{-1, -1, \ldots, -1}_{s}, \underbrace{0, \ldots, 0}_{d})$$

$$M_{\tilde{B}}(f) = diag(\underbrace{1, 1, \ldots, 1}_{\tilde{r}}, \underbrace{-1, -1, \ldots, -1}_{\tilde{s}}, \underbrace{0, \ldots, 0}_{\tilde{d}})$$

entonces se cumple que $r = \tilde{r}$, $s = \tilde{s}$ y $d = \tilde{d}$.

Observación 5.3. *Seguimos suponiendo que las formas cuadráticas con las que trabajamos son no degeneradas así que, en nuestro caso, $n = r + s$.*

Al par (r, s) le denominaremos **signatura de** f. Diremos que f es una forma cuadrática **definida** si $r = 0$ o $s = 0$ y, por el contrario, diremos que es **indefinida** si ambos son no nulos. A partir de esta noción podemos establecer la siguiente relación.

Teorema 5.4. *Dadas dos formas cuadráticas no degeneradas sobre un $\mathbb{R}$-espacio vectorial. Se tiene que*

$$f \sim g \quad \text{si y solo si} \quad r(f) = r(g) \text{ y } s(f) = s(g).$$

Lema 5.5. *Una forma cuadrática f es indefinida si y solo si representa a 0.*

Además, los valores que forman la signatura también determinan el valor del discriminante y del invariante de Hasse.

Proposición 5.6. *Sea f una forma cuadrática con signatura (r, s). Entonces se cumple que:*

- $d(f) = (-1)^s = \begin{cases} 1, & si\ s \equiv 0\ mod\ 2, \\ -1, & si\ s \equiv 1\ mod\ 2. \end{cases}$
- $\varepsilon(f) = (-1)^{s(s-1)/2} = \begin{cases} 1, & si\ s \equiv 0, 1\ mod\ 4, \\ -1, & si\ s \equiv 2, 3\ mod\ 4. \end{cases}$

Demostración. Considerando que $f \sim X_1^2 + \cdots + X_r^2 - Y_1^2 - \cdots - Y_s^2$, lo primero se deduce de forma directa utilizando la definición de discriminante.
Por otro lado, teniendo en cuenta que $(1, 1) = 1$, $(1, -1) = 1$ y $(-1, -1) = -1$, tenemos que

$$\varepsilon(f) = \prod_{k=1}^{r-1}(1, 1)^{r-k}(1, -1)^s \prod_{i=1}^{s-1}(-1, -1)^{s-i}$$

y, por tanto,

$$\varepsilon(f) = (-1)^{s(s-1)/2} = \begin{cases} 1, & \text{si } s \equiv 0, 1 \bmod 4, \\ -1, & \text{si } s \equiv 2, 3 \bmod 4. \end{cases}$$

□

5.2. Formas cuadráticas en $\mathbb{Q}$

En esta sección, trabajaremos con formas cuadráticas no degeneradas con coeficientes en $\mathbb{Q}$ siguiendo, como en capítulos anteriores, los resultados de [9]. Recordamos que denotamos por $\mathcal{V}$ a la unión del conjunto de los números primos y el símbolo ∞, y escribimos $\mathbb{Q}_\infty = \mathbb{R}$. A lo largo de la sección, emplearemos la siguiente notación, $f \sim a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$ será una forma cuadrática de rango n, consideramos sus invariantes:

- El discriminante $d(f) = a_1a_2 \cdots a_n \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.
- Para cada $v \in \mathcal{V}$, consideramos la inclusión canónica de $\mathbb{Q}$ en $\mathbb{Q}_v$, consideramos la forma cuadrática f de $\mathbb{Q}$ vista $\mathbb{Q}_v$, que denotamos por f_v. Los invariantes de f_v se denominan **invariantes locales** y tenemos que

  $$\varepsilon(f_v) = \prod_{i<j}(a_i, a_j)_v$$

  y que $d(f_v)$ es la imagen de $d(f)$ de $\mathbb{Q}^*/\mathbb{Q}^{*2}$ en $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$. Más aún, tenemos que por el Teorema 4.11 se cumple

  $$\prod_{v\in\mathcal{V}} \varepsilon(f_v) = 1.$$

- Además, si consideramos f como una forma cuadrática real también tenemos como invariante la signatura (r, s).

5.3. Teorema de Minkowski

Una vez introducidas estas nociones, estamos en condiciones de enunciar y demostrar el teorema principal del trabajo que nos permite determinar cuándo una forma cuadrática representa a 0 en $\mathbb{Q}$.

Teorema 5.7 (Minkowski)**.** *Dada una forma cuadrática f sobre $\mathbb{Q}$ no degenerada. Se tiene que f representa a 0 si y solo si la forma cuadrática f_v representa a 0 para todo $v \in \mathcal{V}$.*

Demostración. De forma directa se tiene que si f representa a 0 en $\mathbb{Q}$, también su imagen f_v representa a 0 para todo $v \in \mathcal{V}$.

Para el recíproco, consideramos la forma $f \sim a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$ con $a_i \in \mathbb{Q}^*$ y supongamos, sin pérdida de generalidad, que $a_1 = 1$. Dividimos la prueba según los diferentes valores del rango.

I. Supongamos que $n = 2$ y sin pérdida de generalidad que $f \sim X_1^2 - aX_2^2$. Por hipótesis, sabemos que f_v representa a 0 para todo $v \in \mathcal{V}$, en particular, para f_∞, luego $a > 0$. Por otro lado, podemos escribir a como

$$a = \prod_p p^{v_p(a)}$$

y como f_v representa a 0 para todo p primo, por el Teorema 4.20, $-a = -1$, luego a es un cuadrado en cada uno de los $\mathbb{Q}_p$, y por los Teoremas 2.37 y 2.40, $v_p(a)$ es par. Con ello, a es cuadrado en $\mathbb{Q}$ y, por tanto, f representa a 0 en $\mathbb{Q}$.

II. Supongamos que $n = 3$ y sin pérdida de generalidad que $f = X_1^2 - aX_2^2 - bX_3^2$ con $a, b \in \mathbb{Z}$ libres de cuadrados y $|a| \leq |b|$, porque realizando un cambio de variable siempre podemos reducir nuestro problema a estudiar una forma cuadrática con este aspecto. Vamos a probar que f representa a 0 en $\mathbb{Q}$ por inducción sobre $m = |a| + |b|$. Si $m = 2$, tenemos $f = X_1^2 \pm X_2^2 \pm X_3^2$ y como por hipótesis f_∞ representa a 0, el caso $f = X_1^2 + X_2^2 + X_3^2$ queda excluido por ser definida; en otro caso, f representa a 0 en $\mathbb{Q}$.
Supongamos que $m > 2$, i.e., $|b| \geq 2$ y por el Teorema Fundamental de la Aritmética escribimos

$$b = \pm \prod_{i=1}^{k} p_i$$

con p_i primos distintos. Fijamos cualquier $p := p_j$ para algún $j \in \{1, \ldots, k\}$ y veamos que a es cuadrado módulo p. Si $a \equiv 0 \bmod p$, ya está resuelto; en otro caso, tenemos que por la Proposición 2.7, $a \in \mathbb{U}^p$. Por hipótesis, tenemos que existe $(\tilde{x}, \tilde{y}, \tilde{z}) \in (\mathbb{Q}_p)^3$ tal que $\tilde{x}^2 - a\tilde{y}^2 - b\tilde{z}^2 = 0$ y, por la Proposición 2.21, existe $(x, y, z) \in (\mathbb{Z}_p)^3$ primitivo con

$$x^2 - ay^2 - bz^2 = 0.$$

Tomando módulo p, tenemos que $x^2 - ay^2 \equiv 0 \bmod p$. Razonamos por reducción al absurdo y supongamos que $y \equiv 0 \bmod p$, por tanto, $x \equiv 0 \bmod p$. Como se tiene que $x^2 - ay^2 \equiv 0 \bmod p^2$, deducimos que $bz^2 \equiv 0 \bmod p^2$ y, como $b \not\equiv 0 \bmod p^2$, concluimos que $z \equiv 0 \bmod p$, lo que es imposible porque (x, y, z) es primitivo. De esta forma, se

tiene que $y \not\equiv 0 \bmod p$, i.e., y es unidad en $\mathbb{Z}_p$. Por ello, $x^2 \equiv ay^2 \bmod p$, y como y es unidad, $(xy^{-1})^2 \equiv a \bmod p$, concluyendo que a es cuadrado módulo p. Como p es cualquiera de los primos que divide a a y como $\mathbb{Z}/b\mathbb{Z} \simeq \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$, tenemos también que a es cuadrado módulo b. Por ello, existen $t, \tilde{b} \in \mathbb{Z}$ tales que $t^2 = a + b\tilde{b}$ y podemos tomar t tal que $|t| \leq |b|/2$. Como $b\tilde{b} = t^2 - a$, entonces $b\tilde{b}$ es un elemento de la de la norma de k_a^* y, por la Proposición 4.10, $(a, b\tilde{b}) = 1$. Como f representa a 0 si y solo si $(a, b) = 1$, por la bilinealidad del símbolo de Hilbert, f representa a 0 si y solo si

$$\tilde{f} = X_1^2 - aX_2^2 - \tilde{b}X_3^2$$

representa a 0. En particular, $\tilde{f}_v$ representa a 0 para todo $v \in \mathcal{V}$ y, por otro lado, teniendo en cuenta la cota de la norma de t, tenemos que

$$|\tilde{b}| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|.$$

Escribimos $\tilde{b} = \hat{b}u^2$ con $\hat{b}, u \in \mathbb{Z}$ y $\hat{b}$ libre de cuadrados y obtenemos $|\tilde{b}| \leq |b|$. Aplicamos la hipótesis de inducción a la forma $\hat{f} = X_1^2 - aX_2^2 - \hat{b}X_3^2$ que es equivalente a $\tilde{f}$, concluyendo así que f representa a 0 en $\mathbb{Q}$.

III. Supongamos que $n = 4$. Consideramos $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_3^2)$ y supongamos que f_v representa a 0 para todo $v \in \mathcal{V}$. Por el Corolario 3.36 esto es que existe un $x_v \in \mathbb{Q}_v^*$ tal que es representado por $g = aX_1^2 + bX_2^2$ y por $h = cX_3^2 + dX_4^2$. Por el apartado IV del Teorema 4.20 esto es

$$\text{para todo } v \in \mathcal{V} \quad (x_v, -ab)_v = (a, b)_v \quad \text{y} \quad (x_v, -cd) = (c, d)_v.$$

Por el Teorema 4.11 tenemos que

$$\prod_{v\in\mathcal{V}} (a, b)_v = \prod_{v\in\mathcal{V}} (c, d)_v = 1$$

y por el Teorema 4.13 existe un $x \in \mathbb{Q}^*$ tal que para todo $v \in \mathcal{V}$

$$(x, -ab)_v = (a, b)_v \quad \text{y} \quad (x, -cd)_v = (c, d)_v.$$

Por tanto, la forma cuadrática g representa a x, por el Corolario 3.36, la forma cuadrática $\tilde{f} = aX_1^2 + bX_2^2 - xZ^2$ representa a 0 en cada $\mathbb{Q}_v$ y, por el apartado anterior, representa a 0 en $\mathbb{Q}$. En otras palabras, $x \in \mathbb{Q}^*$ es representado por $g = aX_1^2 + bX_2^2$. Razonamos de forma análoga para $h = cX_3^2 + dX_4^2$ y, de nuevo, por el Corolario 3.36 $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$ representa a 0.

IV. Supongamos que $n \geq 5$. Consideremos la forma cuadrática

$$f := h - g$$

con $h = a_1X_1^2 + a_2X_2^2$ y $g = -(a_3X_3^2 + a_4X_4^2 + \cdots + a_nX_n^2)$ y el conjunto finito

$$\mathcal{S} = \{\infty, 2, p : p \text{ primo con } v_p(a_i) \neq 0 \quad \forall i \geq 3\}.$$

Tomamos $v \in \mathcal{S}$ y, por hipótesis, f_v representa a 0 en $\mathbb{Q}_v$. Por el Corolario 3.36, sabemos que existe $a_v \in \mathbb{Q}_v^*$ tal que es representado por h_v y por g_v, i.e. , existen x_v^i para $i \in \{1, \dots, n\}$ tales que $h_v(x_v^1, x_v^2) = a_v = g_v(x_v^3, \dots, x_v^n)$. Como $a_v \in \mathbb{Q}_v^*$ y $\mathbb{Q}_v^{*2}$ es un subgrupo abierto de $\mathbb{Q}_v^*$, tenemos que $a_v\mathbb{Q}_v^{*2}$ es abierto y, por el Teorema de Aproximación 4.12, tenemos que existe

$$a \in a_v\mathbb{Q}_v^{*2} \cap \mathbb{Q}.$$

Por tanto, existen $x_1, x_2 \in \mathbb{Q}$ tales que

$$h(x_1, x_2) = a$$

con $a/a_v \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Consideramos la forma cuadrática de rango mayor o igual que 4,

$$f^1 := g_v - aZ^2.$$

Si $v \in \mathcal{S}$, g_v representa a a_v en $\mathbb{Q}_v$ y, como $a/a_v \in \mathbb{Q}_v^{*2}$ se tiene que g_v representa a a en $\mathbb{Q}_v$. Empleando el Corolario 3.35, tenemos entonces que f^1 representa a 0 en $\mathbb{Q}_v$. Si por el contrario $v \notin \mathcal{S}$, tenemos que los coeficientes $-a_3, \dots, -a_n$ son unidades v-ádicas y, por tanto, $d(g_v)$ también. Como $v \neq 2$, por el Teorema 4.8, tenemos que $(a_i, a_j) = 1$ para todo $i, j \in \{3, \dots, n\}$ con $i \neq j$ por ser unidades v-ádicas y, por tanto, $\varepsilon(g_v) = 1$. Supongamos que $rango(g_v) = 3$, de nuevo, por el Teorema 4.8, como d es unidad, $(-1, -d) = 1$ y, con ello, como $\varepsilon = (-1, -d)$, por el Teorema 4.20, g_v representa a 0 en $\mathbb{Q}_p$. Como g_v es no degenerada y representa a 0, por la Proposición 3.34, g_v representa a todo elemento de $\mathbb{Q}_p$ y, en particular, a a. Luego, por el Corolario 3.36, f^1 representa a 0 en $\mathbb{Q}_v$. Como f^1 tiene rango 4, por el apartado III, entonces representa a 0 en $\mathbb{Q}$ y, por ende, g representa a a en $\mathbb{Q}$. Como $h(x_1, x_2) = a$, es decir, h también representa a a, tenemos que f representa a 0 por el Corolario 3.36. Para el caso con $rango(g_v) \geq 4$, como por el Teorema 4.20, g_v siempre representa a a, razonamos de forma análoga y se concluye el resultado.

□

Veamos un ejemplo de la aplicación directa del teorema.

Ejemplo 5.8. *Consideramos la forma*

$$f(X, Y, Z) = -3X^2 + 5Y^2 - 7Z^2$$

y veamos si representa a 0 en $\mathbb{Q}$ aplicando el Teorema de Minkowski (Teorema 5.7). Para ello veamos si f representa a 0 en $\mathbb{Q}_p$ distinguiendo si $p = 2, 3, 5, 7$ o distinto. Notemos que f representa a 0 en $\mathbb{R}$ porque es indefinida.
En $\mathbb{Q}_2$, tomamos $y_0 = 2$ y $z_0 = 0$ y tenemos

$$g(X) = -3X^2 + 20 \quad y \quad g'(X) = -6X.$$

Por tanto, $x = 2$ es una raíz con $v_2(g(2)) = 3$ y $v_2(g'(2)) = 2$ y aplicando el Lema de Hensel, Corolario 2.25, podemos levantar la solución a una solución en $\mathbb{Q}_2$ que denotamos por $\ell(2) \in \mathbb{Q}_2$ de forma que $(\ell(2), 2, 0) \in (\mathbb{Q}_2)^3$ es solución de $f(x, y, z) = 0$, es decir, f representa a 0 en $\mathbb{Q}_2$. Razonamos de forma análoga para $p = 3, 5$ y 7 con $(3, \ell(3), 0) \in (\mathbb{Q}_3)^3$,

$(\ell(1),1,1) \in (\mathbb{Q}_5)^3$ *y* $(\ell(1),3,0) \in (\mathbb{Q}_7)^3$, *respectivamente.*
Para acabar, veamos si f *representa a 0 en* $\mathbb{Q}_p$ *con* $p \neq 2,3,5,7$. *Por la Proposición 4.1, sabemos que en* $(\mathbb{F}_p)^3$ *existe una solución* (x_0,y_0,z_0) *no trivial de*

$$-3X^2+5Y^2-7Z^2 \equiv 0 \ mod\ p.$$

Como la solución (x_0,y_0,z_0) *es no trivial, al menos uno de los números no es divisible por* p, *así que, supongamos sin pérdida de generalidad que* $p \nmid x_0$. *Tenemos entonces que* $g(X) = -3X^2+5y_0^2-7z_0^2$ *tiene* x_0 *como raíz con* $v_p(g(x_0)) \geq 1$ *y como* $v_p(g'(x_0)) = v_p(-6x_0) = 0$, *podemos aplicar el Lema de Hensel como en los casos anteriores y levantamos la solución a* $(\mathbb{Q}_p)^3$. *En conclusión, como* f *representa a* 0 *en* $\mathbb{Q}_v$ *para todo* $v \in \mathcal{V}$, f *representa a* 0 *en* $\mathbb{Q}$.

Observación 5.9. *Cabe destacar que el teorema no es cierto para polinomios homogéneos de grado mayor o igual que 3. Por ejemplo, el matemático noruego Ernst S. Selmer probó que la ecuación*

$$3X^3+4Y^3+5Z^3=0$$

no tiene una solución no trivial en $\mathbb{Q}$ *y, sin embargo, sí la tiene en cada* $\mathbb{Q}_v$, *ver [8].*

A partir del teorema, se pueden deducir los siguientes resultados.

Corolario 5.10. *Sean* f *una forma cuadrática no degenerada sobre* $\mathbb{Q}$ *y* $b \in \mathbb{Q}^*$. *Entonces,* f *representa a* b *si y solo si* f_v *representa a* b *para todo* $v \in \mathcal{V}$.

Demostración. Tomamos la forma cuadrática $g := f - bZ^2$. Por el Corolario 3.35 f representa a b si y solo si g representa a 0. Por el Teorema de Minkowski esto es si y solo g_v representa a 0 para todo $v \in \mathcal{V}$ y nuevamente por el Corolario 3.35 esto ocurre si y solo si f_v representa a b para todo $v \in \mathcal{V}$. □

Corolario 5.11 (Meyer)**.** *Una forma cuadrática de rango mayor o igual que 5 representa a 0 si y solo si es indefinida.*

Demostración. Por el Teorema 4.20, sabemos que una forma cuadrática en $\mathbb{Q}_p$ de rango mayor o igual que 5 siempre representa a 0, así que basta ver cuándo una forma cuadrática representa a 0 en $\mathbb{R}$. Pero, por el Lema 5.5, sabemos que una forma cuadrática real representa a 0 si es indefinida, concluyendo así el enunciado. □

Notemos que entonces sí existen formas cuadráticas indefinidas de rango menor que 5 que no representen a 0. Lo vemos en el siguiente ejemplo.

Ejemplo 5.12. *Consideramos la forma cuadrática* $f = -X_1^2 - X_2^2 + 5X_3^2 + 55X_4^2$ *y veamos que* f *no representa a 0 en* $\mathbb{Q}$. *Empleando los resultados anteriores, veamos que* f *no representa a 0 para algún* $\mathbb{Q}_v$.

Tomamos $p = 5$ *y trabajemos en* $\mathbb{Q}_5$. *Como* $det(f) = 5^2 \cdot 11$ *y tenemos que* $\left(\frac{11}{5}\right) = 1$, *entonces* $d(f_5) = 1$. *Utilizando las propiedades del símbolo de Hilbert y el Teorema 4.8,* $\varepsilon(f_5) = -1$. *Por tanto, por el Teorema 4.20* f_5 *no representa a 0 en* $\mathbb{Q}_5$.

Corolario 5.13. *Sea* f *una forma cuadrática de rango* n *en* $\mathbb{Q}$.

- *Si $n = 3$ y para todo $v \in \mathcal{V}$ f_v representa a 0 en $\mathbb{Q}_v$ excepto a lo sumo uno, entonces f representa a 0.*
- *Si $n = 4$, $d(f_v) = 1$ y para todo $v \in \mathcal{V}$ f_v representa a 0 en $\mathbb{Q}_v$ excepto a lo sumo uno, entonces f representa a 0.*

Demostración. En primer lugar, supongamos que $n = 3$. Por lo visto en el Teorema 4.20, tenemos que f_v representa a 0 en $\mathbb{Q}_v$ si y solo si se cumple

$$\varepsilon(f_v) = (-1, -d(f_v))_v.$$

Sabemos que $\prod_{v\in\mathcal{V}} \varepsilon(f_v) = 1$ y, también tenemos que $\prod_{v\in\mathcal{V}}(-1, -d(f_v))_v = 1$, por el Teorema 4.11. Por tanto, si se tiene que $\varepsilon(f_v) = (-1, -d(f_v))$ para todo $v \in \mathcal{V}$ excepto como mucho para uno, se concluye que se verifica para todos ellos. De esta forma, en virtud del Teorema de Minkowski (Teorema 5.7) tenemos que f representa a 0 en $\mathbb{Q}$.

En segundo lugar, si $n = 4$, $d(f_v) = 1$ y argumentando de forma análoga al primer caso, tenemos que f_v representa a 0 en $\mathbb{Q}_v$ si y solo si

$$\varepsilon(f_v) = (-1, -1).$$

Por tanto, se concluye que f representa a 0 en $\mathbb{Q}$. □

A continuación, veamos los resultados que nos permiten clasificar las formas cuadráticas en el cuerpo de los racionales $\mathbb{Q}$.

Teorema 5.14. *Sean f y $\tilde{f}$ dos formas cuadráticas sobre $\mathbb{Q}$. Se tiene que f y $\tilde{f}$ son equivalentes si y solo si f_v y $\tilde{f}_v$ son equivalentes sobre $\mathbb{Q}_v$ para todo $v \in \mathcal{V}$.*

Demostración. De forma directa tenemos que si f y $\tilde{f}$ son equivalentes sobre $\mathbb{Q}$, entonces las formas f_v y $\tilde{f}_v$ son equivalentes sobre $\mathbb{Q}_v$ para todo $v \in \mathcal{V}$.

Probemos el recíproco por inducción en el rango n de las formas cuadráticas fijando $v \in \mathcal{V}$. Supongamos que $n = 1$ y que f_v y $\tilde{f}_v$ son equivalentes. Tomamos $a \in \mathbb{Q}^*$ representado por f, luego para todo $v \in \mathcal{V}$, f_v representa a a y como f_v y $\tilde{f}_v$ son equivalentes, tenemos que f_v y $\tilde{f}_v$ representan a a. Por tanto, f y $\tilde{f}$ representan a a por el Corolario 5.10, luego $f \sim aZ^2$, $\tilde{f} \sim aZ^2$ y concluimos $f \sim \tilde{f}$. Supongamos que se cumple para un cierto $n - 1$. Para todo $v \in \mathcal{V}$, tomamos f_v y $\tilde{f}_v$ dos formas cuadráticas de rango n equivalentes. Como antes, esto implica que existe un $a \in \mathbb{Q}^*$ tal que es representado por f_v y $\tilde{f}_v$ para todo $v \in \mathcal{V}$. Por el Corolario 3.35, podemos escribir f_v y $\tilde{f}_v$ como

$$f_v \sim h_v + aX_n^2 \text{ con } rango(h_v) = n - 1,$$

$$\tilde{f}_v \sim \tilde{h}_v + aX_n^2 \text{ con } rango(\tilde{h}_v) = n - 1,$$

y por el Teorema 3.39, $h_v \sim \tilde{h}_v$ en $\mathbb{Q}_v$ para todo $v \in \mathcal{V}$. Utilizando la hipótesis de inducción, tenemos que $h \sim \tilde{h}$ en $\mathbb{Q}$ y concluimos que $f \sim \tilde{f}$ en $\mathbb{Q}$. □

Corolario 5.15. *Sean f y $\tilde{f}$ dos formas cuadráticas con signatura (r, s) y $(\tilde{r}, \tilde{s})$, respectivamente. Entonces, f y $\tilde{f}$ son equivalentes si y solo si se cumple que para todo $v \in \mathcal{V}$*

$$rango(f) = rango(\tilde{f}), \quad d(f_v) = d(\tilde{f}_v), \quad (r, s) = (\tilde{r}, \tilde{s}) \quad y \quad \varepsilon(f_v) = \varepsilon(\tilde{f}_v).$$

Demostración. Por el Teorema 5.14, dos formas cuadráticas f y $\tilde{f}$ son equivalentes en $\mathbb{Q}$ si y solo si las formas f_v y $\tilde{f}_v$ lo son en $\mathbb{Q}_v$ para cada $v \in \mathcal{V}$. Por el Teorema 4.21, concluimos que f_v y $\tilde{f}_v$ son equivalentes en $\mathbb{Q}_v$ para todo $v \in \mathcal{V}$ si y solo si

$$rango(f_v) = rango(\tilde{f}_v), \quad d(f_v) = d(\tilde{f}_v), \quad (r,s) = (\tilde{r},\tilde{s}) \quad \text{y} \quad \varepsilon(f_v) = \varepsilon(\tilde{f}_v).$$

□

Observación 5.16. *Los invariantes $d = d(f)$, $\varepsilon_v = \varepsilon(f_v)$, (r,s) no son elementos arbitrarios si no que verifican las siguientes relaciones:*

- $\varepsilon_v = 1$ *para todo* $v \in \mathcal{V}$ *excepto un número finito y* $\prod_{v\in\mathcal{V}} \varepsilon_v = 1$.
- *Si* $n = 1$, *se tiene que* $\varepsilon_v = 1$.
- *Si* $n = 2$ *y la imagen* d_v *de* d *en* $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ *es* -1, *entonces se tiene que* $\varepsilon_v = 1$.
- $r, s \geq 0$ *y* $r + s = n$.
- $d_\infty = (-1)^s$.
- $\varepsilon_\infty = (-1)^{\frac{s(s-1)}{2}}$.

Recíprocamente dados d, $(\varepsilon_v)_{v\in\mathcal{V}}$ y (r,s) verificando las condiciones anteriores, entonces existe una forma cuadrática sobre $\mathbb{Q}$ de rango n con dichos inviariantes, ver [9, Capítulo IV, Proposición 7].

Estos resultados nos son útiles para determinar cuándo dos formas cuadráticas sobre $\mathbb{Q}$ son equivalentes o no, sobretodo para probar que no lo son, basta con encontrar un $v \in \mathcal{V}$ en el que no se cumpla la igualdad entre, al menos, uno de sus invariantes. Veámoslo con un ejemplo:

Ejemplo 5.17. *Consideramos las formas cuadráticas sobre* $\mathbb{Q}$:

$$f(X,Y,Z) = \frac{15}{2}X^2 + \frac{4}{25}Y^2 + \frac{75}{2}Z^2,$$

$$g(X,Y,Z) = \frac{33}{2}X^2 + \frac{4}{15}Y^2 + \frac{45}{2}Z^2.$$

Ambas están ya expresadas de forma diagonalizada y su rango es 3. Denotamos por (r,s) a la signatura de la forma cuadrática f y $(\tilde{r},\tilde{s})$ a la de g y como $r = \tilde{r} = 3$ y $s = \tilde{s} = 0$, tenemos que f y g son equivalentes en $\mathbb{R}$ por el Teorema 5.4. Pero esto no nos sirve para garantizar su equivalencia sobre $\mathbb{Q}$ así que pasamos a trabajar sobre los $\mathbb{Q}_p$. En primer lugar, vamos a calcular su discriminante en los distintos $\mathbb{Q}_p$ y para ello, utilizamos lo visto en la demostración del Corolario 2.39. Denotamos por A a la matriz de f y B a la de g y comenzamos por $\mathbb{Q}_3$. Como $det(A) = 3^2 \cdot 5$ y $\left(\frac{5}{3}\right) = -1$, tenemos que $d(f_3) = [5]$ y razonando de forma análoga para g_3, tenemos que $d(g_3) = [5]$; así que, como son iguales, pasamos a calcular su discriminante en $\mathbb{Q}_5$. En este caso, tenemos que $d(f_5) = [5]$ y $d(g_5) = [1]$ y como son distintos, podemos concluir que f y g no son equivalentes sobre $\mathbb{Q}$.

Apéndice A

Definiciones y resultados auxiliares

En este apéndice, se recogen algunos conceptos y resultados que se han empleado a lo largo del trabajo. La mayoría de estos aparecen en el temario de alguna de las asignaturas del Grado en Matemáticas, pero con el fin de facilitar la lectura de la memoria se incluyen en este apéndice. En general, se omiten las pruebas, salvo aquellas que por su singularidad o relevancia se ha creído apropiado detallar. Los resultados se agrupan por temática en tres secciones.

A.1. Prerrequisitos de Álgebra

Los enteros p-ádicos se construyen como un límite proyectivo de anillos. Para definir esta noción es necesario recordar la noción de grupo/anillo producto. Nos limitaremos a estudiar el caso de familias numerables.

Definición A.1. *Sea $(G_n)_{n\in\mathbb{N}}$ una familia de grupos (anillos). Se define el producto directo de grupos (anillos) como el conjunto $G = \prod_{n\in\mathbb{N}} G_n$ donde las operaciones se definen coordenada a coordenada.*

Para definir el límite proyectivo es necesario que nuestra sucesión de conjuntos, grupos o anillos forme un sistema proyectivo.

Definición A.2. *Se llama **sistema proyectivo** a una sucesión $(X_i, f_{ij})_{i,j\in\mathbb{N}}$ tales que $(X_i)_{i\in\mathbb{N}}$ es una sucesión de conjuntos/grupos/anillos y los f_{ij} son aplicaciones/homomorfismos de grupos/homomorfismos de anillos con*

$$f_{ij}: \ X_j \ \longrightarrow \ X_i$$

de anillos con las siguientes propiedades:

I. *Para todo $i \in \mathbb{N}$ se tiene que $f_{ii} = Id_{X_i}$.*

II. *Para todos $i, j, k \in \mathbb{N}$ con $i \leq j \leq k$ se tiene que $f_{ik} = f_{ij} \circ f_{jk}, \forall i \leq j \leq k$.*

Definición A.3. *Se define **límite proyectivo** como un subconjunto/subgrupo/subanillo particular del producto directo de la siguiente forma*

$$\varprojlim X_i = \{(x_i)_{i\in\mathbb{N}} \in \prod_{i\in\mathbb{N}} X_i : x_i = f_{ij}(x_j) \text{ para todo } i \leq j\}.$$

A continuación, vamos a enunciar y demostrar un lema relacionado con los límites proyectivos que ha sido utilizado en la demostración del Lema de Hensel.

Lema A.4. *Sea $(X_i f_{ij})_{i,j\in\mathbb{N}}$ un sistema proyectivo y sea $X = \varprojlim X_n$ su límite proyectivo. Si los X_n son finitos y no vacíos, entonces X es no vacío.*

Demostración. Si los morfismos son todos sobreyectivos, el resultado es cierto pues se puede construir un elemento de X tomando las preimágenes de los elementos de los X_i (siempre existen por ser sobreyectivos) y de esta forma X es no vacío. A continuación, vamos a demostrar el caso general reduciéndolo a este caso especial. Fijamos n y denotamos por $X_{n,p}$ a la imagen de X_{n+p} en X_n, es decir, $X_{n,p} := f_{n,n+p}(X_{n+p})$.
Utilizando la definición de sistema proyectivo :

$$X_{n,p+1} = f_{n,n+p+1}(X_{n+p+1}) = f_{n,n+p}(f_{n+p,n+p+1}(X_{n+p+1})) \subseteq f_{n,n+p}(X_{n+p}) = X_{n,p}.$$

Con ello, tenemos que $(X_{n,p})_p$ es una familia decreciente de conjuntos finitos no vacíos. Por lo tanto, debe ser estacionaria y existe $E_n := \cap_{p\in\mathbb{N}} X_{n,p}$. Consideramos el morfismo $f_{n-1,n} : X_n \longrightarrow X_{n-1}$. Como $f_{n-1,n+p}(X_{n+p}) = X_{n-1,p}$ para todo $p \in \mathbb{N}$, tenemos que al restringir el morfismo a E_n, se tiene que el morfismo $E_n \longrightarrow E_{n-1}$ es sobreyectivo. Los E_n son no vacíos y los morfismos son sobreyectivos, luego por la primera parte de la demostración tenemos que $\varprojlim E_n \neq \emptyset$ y como $E_n \subseteq X_n$ para todo n, se tiene que $\varprojlim X_n \neq \emptyset$. En conclusión, se cumple que $X \neq \emptyset$. □

Continuamos recordando la definición de sucesión exacta.

Definición A.5. *Sean E, F, H grupos y sean $f : E \longrightarrow F$ y $g : F \longrightarrow G$ homomorfismos de grupos. Entonces, se dice que la **sucesión** $E \xrightarrow{f} F \xrightarrow{g} G$ es **exacta** si, f es inyectiva, g sobreyectiva y $Ker(g) = Im(f)$.*

Presentamos un resultado que nos indica cómo descomponer un grupo en suma directa de otros dos que hemos empleado en el estudio del grupo multiplicativo de los p-ádicos.

Lema A.6. *Sea $0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0$ una sucesión exacta de grupos conmutativos, suponiendo con notación aditiva, con A y B grupos de órdenes finitos a y b respectivamente y coprimos. Sea $B' := \{x \in E : bx = 0\}$. Entonces, el grupo $E = A \oplus B'$ y además, B' es el único subgrupo de E isomorfo a B.*

Demostración. Primero, vamos a ver que E es suma directa de A y B', para ello, vamos a ver $A \cap B' = 0$ y que todo elemento de E se puede escribir como combinación de elementos de A y B'.
Como a y b son coprimos, tenemos que existen $r, s \in \mathbb{Z}$ tales que $ar + bs = 1$. Tomamos $x \in A \cap B'$ y como $\#A = a$, tenemos que $a \cdot x = 0$. Por definición de B', tenemos que $b \cdot x = 0$. Por lo tanto, se tiene que

$$x = 1 \cdot x = (ar + bs) \cdot x = r(ax) + s(bx) = 0,$$

luego $x = 0$. Falta probar que todo elemento de E puede escribirse como suma de elementos de A y B'. Como dado $x \in E$ podemos escribir $x = rax + sbx$, basta probar que $sbx \in A$ y $rax \in B'$.

Consideramos $f : A \longrightarrow E$ y $g : E \longrightarrow B$ los morfismos de la sucesión exacta. Primero,

veamos que $bsx \in A$. Como f es inyectivo y la sucesión es exacta, tenemos que $Ker(g) = Im(f) \simeq A$. Veamos que $bE \subseteq A \simeq Ker(g)$. Tomamos $y \in bE$, tenemos que existe $x \in E$ tal que $y = bx$. Aplicamos g y tenemos $g(y) = g(bx) = bg(x) = 0$ porque $\#B = b$, luego $y \in Ker(g)$. Así, como $sx \in E$, $bsx \in A$.

Veamos que $arx \in B'$. Como $bE \subseteq A$ tenemos que $abE \subseteq aA = \{0\}$, porque $\#A = a$, luego $abE = \{0\}$. Por tanto, $arx \in B'$ porque $barx = abrx = 0$.

Por último, probemos la unicidad de B'. Supongamos que existe otro subgrupo B'' de E que es isomorfo a B. Como $\#B = b$, se tiene que $bB'' = \{0\}$ luego $B'' \subseteq B'$, por cómo se ha definido B' y, por tener el mismo orden, $B'' = B'$. □

Para concluir, recordamos el enunciado del Teorema Chino de los Restos que se ha empleado en la largo de la memoria.

Teorema A.7 (Chino de los Restos)**.** *Sea R un anillo conmutativo y unitario y sean $I_1, I_2, \ldots, I_n$ ideales de R comaximales. Entonces el homomorfismo de anillos*

$$\begin{array}{rccc} \phi: & R/(I_1 \cdot I_2 \cdots I_n) & \longrightarrow & \prod_{i=1}^{n}(R/I_i) \\ & x + (I_1 \cdot I_2 \cdots I_n) & \longmapsto & (x + I_1, x + I_2, \ldots, x + I_n) \end{array}$$

es un isomorfismo.

A.2. Prerrequisitos de Teoría de Números

Por la naturaleza de las formas cuadráticas resulta esencial el estudio de los cuadrados del cuerpo sobre el que están definidas. Comenzamos recordando la estructura del grupo de cuadrados sobre un cuerpo finito que se ha empleado en la Sección 4.1 y que es necesaria para probar las propiedades del símbolo de Legendre.

Lema A.8. *Sea p un número primo distinto de 2 y sea $q = p^f$ una potencia, consideramos el cuerpo finito de q elementos $\mathbb{F}_q$. Entonces $\mathbb{F}_q^{*2} = \{x \in \mathbb{F}_q : x^{\frac{q-1}{2}} = 1\}$ y $\mathbb{F}_q/\mathbb{F}_q^{*2} \simeq \mathbb{Z}/2\mathbb{Z}$.*

Demostración. Todos los elementos de $\mathbb{F}_q^*$ son solución de la ecuación $x^{q-1} = 1$ porque $\#\mathbb{F}_q^* = q - 1$. Por otro lado, podemos expresar $x^{q-1} - 1$ como

$$x^{q-1} - 1 = (x^{\frac{q-1}{2}} + 1)(x^{\frac{q-1}{2}} - 1),$$

luego tiene que haber la mitad de soluciones en cada factor del producto.
Claramente, si $a \in \mathbb{F}_q^{*2}$ se tiene que $a^{\frac{q-1}{2}} = (b^2)^{\frac{q-1}{2}} = b^{q-1} = 1$, luego es solución de $x^{\frac{q-1}{2}} = 1$. Recíprocamente, si a es una solución de $x^{\frac{q-1}{2}} = 1$, tomamos b en una extensión algebraica de $\mathbb{F}_q^*$ tal que $a = b^2$, luego $b^{q-1} = 1$, b es solución de $x^{q-1} = 1$ que tiene todas sus soluciones en $\mathbb{F}_q^*$. Por consiguiente, a es cuadrado. Por tanto, $\mathbb{F}_q^{*2}$ tiene la mitad de elementos que $\mathbb{F}_q^*$. □

Seguidamente, vamos a introducir una noción que nos permite determinar el carácter cuadrático de un número y que ha resultado esencial en el Capítulo 4 del trabajo. Es un término que se usa en la teoría de números y la definición que vamos a dar es la que se recoge en [9, Capítulo I]. Asimismo, incluimos algunas de las propiedades que posee y que también se recogen en [9].

Definición A.9. *Se define el* ***símbolo de Legendre*** *como*

$$\left(\frac{a}{p}\right) = a^{\frac{(p-1)}{2}} \in \{\pm 1\}$$

donde a y p son enteros, y p es un número primo que no divide a a. Por el Lema A.8 $\left(\frac{a}{p}\right) = 1$ si y solo si a es cuadrado módulo p.

Si consideramos las aplicaciones $\varepsilon, \omega : \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ dadas por $\varepsilon(z) \equiv \frac{z-1}{2} \bmod 2$ y $\omega(z) \equiv \frac{z^2-1}{8} \bmod 2$, se tiene el siguiente resultado.

Teorema A.10. *Para todo p primo, el símbolo de Legendre satisface las siguientes relaciones:*

$$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)} \qquad y \qquad \left(\frac{2}{p}\right) = (-1)^{\omega(p)}.$$

Teorema A.11 (Ley de Reciprocidad Cuadrática)**.** *Para todos p y q primos impares distintos, se tiene que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(q)}.$$

Veamos cómo se relaciona el símbolo de Legendre con el símbolo de Hilbert.

Lema A.12. *Sea $v \in \mathbb{U}^p$. Si la ecuación $Z^2 - pX^2 - vY^2 = 0$ tiene una solución no trivial en $\mathbb{Q}_p$, tiene una solución (z, x, y) tal que $z, y \in \mathbb{U}^p$ y $x \in \mathbb{Z}_p$.*

Demostración. Basta comprobar que la solución primitiva dada por la Proposición 2.21 cumple las hipótesis. Para ello se razona por reducción al absurdo suponiendo que $y \equiv 0 \bmod p$ o que $z \equiv 0 \bmod p$ y se llega a una contradicción con el carácter primitivo de la solución. □

El siguiente teorema nos proporciona una fórmula para calcular el símbolo de Hilbert en términos del símbolo de Legendre. Incluimos la prueba de este resultado dado que de él se deducen las propiedades del símbolo de Hilbert que se emplean en el estudio del invariante de Hasse.

Teorema A.13. *Sean k un cuerpo y $a, b \in k^*$. Si $k = \mathbb{R}$, entonces $(a, b) = 1$ si a o b es positivo y $(a, b) = -1$ si a y b son negativos. Si $k = \mathbb{Q}_p$ y $a, b \in k^*$ son tales que $a = p^n u, b = p^m v$ con $u, v \in \mathbb{U}^p$. Se tiene que*

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

donde $\varepsilon(z) \equiv \frac{z-1}{2}$ mod 2 y $\omega(z) \equiv \frac{z^2-1}{8}$ mod 2.

Demostración. Tomamos $k = \mathbb{R}$. En primer lugar, supongamos sin pérdida de generalidad que $a > 0$, entonces basta tomar $(1, 0, \sqrt{a})$ para que la ecuación $Z^2 - aX^2 - bY^2 = 0$ tenga solución, es decir, $(a, b) = 1$. En segundo lugar, si a y b son negativos, por definición del símbolo de Hilbert se tiene que $(a, b) = -1$ porque los cuadrados de números reales son positivos.

Tomamos $k = \mathbb{Q}_p$ y supongamos que $p \neq 2$. Por las propiedades del símbolo de Hilbert, basta distinguir tres casos:

Primero, si $n = 0$ y $m = 0$, tenemos que probar que $(u, v) = 1$. Consideramos la ecuación

$$Z^2 - uX^2 - vY^2 \equiv 0 \bmod p$$

que, por la Proposición 4.1, tiene una solución no trivial y por el Corolario 2.26 como $d = uv \in \mathbb{U}^p$ se puede levantar a una solución p-ádica y, por tanto, $(u, v) = 1$.

Segundo, si $n = 1$ y $m = 0$, tenemos que probar que $(pu, v) = \left(\frac{v}{p}\right)$. Como por el caso anterior $(u, v) = 1$ se tiene que $(pu, v) = (p, v)$ por la Proposición 4.7, luego basta probar que $(p, v) = \left(\frac{v}{p}\right)$. Si v es un cuadrado, se tiene que tanto $\left(\frac{v}{p}\right)$ como (p, v) son 1. Si $\left(\frac{v}{p}\right) = -1$, por el Teorema 2.37 v no es cuadrado. Si la ecuación

$$Z^2 - pX^2 - vY^2 = 0$$

tuviera solución, por el Lema A.12, tendríamos (z, x, y) solución con $z, y \in \mathbb{U}^p$. Por tanto, $v \equiv (z/y)^2 \bmod p$ que es absurdo porque tenemos que v no es cuadrado. En conclusión, si v no es cuadrado, $(p, v) = -1$.

Por último, si $n = 1$ y $m = 1$, tenemos que probar que $(pu, pv) = (-1)^{\varepsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$. Empleando las propiedades del símbolo de Hilbert, se tiene que

$$(a, b) = (pu, pv) = (pu, -p^2uv) = (pu, -uv)$$

y, por el apartado anterior, como $(pu, -uv) = \left(\frac{-uv}{p}\right)$, aplicando las propiedades del símbolo de Legendre, se concluye que

$$(a, b) = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{u}{p}\right) \left(\frac{v}{p}\right) = (-1)^{\varepsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right).$$

Supongamos que $p = 2$ y, como antes, basta con probar tres casos.

Primero, si $n = m = 0$, tenemos que probar que $(a, b) = (u, v) = (-1)^{\varepsilon(u)\varepsilon(v)}$. Luego tenemos que ver que $(u, v) = 1$ si u o v son congruentes con 1 módulo 4 o $(u, v) = -1$ en otro caso. Supongamos que $u \equiv 1 \bmod 4$, entonces o bien $u \equiv 1 \bmod 8$ o bien $u \equiv 5 \bmod 8$. En el primer caso, por el Teorema 2.40, u es cuadrado y, por las propiedades del símbolo de Hilbert, tenemos que $(u, v) = 1$. Si $u \equiv 5 \bmod 8$, tenemos que $u + 4v \equiv 1 \bmod 8$ y por el Teorema 2.40, $u + 4v$ es cuadrado, i.e., existe un w tal que $w^2 = u + 4v$. Consideramos la forma $Z^2 - uX^2 - vY^2 = 0$ y tenemos que $(w, 1, 2)$ es solución. Por tanto, $(u, v) = 1$. Supongamos que $u \equiv v \equiv -1 \bmod 4$ y que la ecuación $Z^2 - uX^2 - vY^2 = 0$ tiene solución primitiva no trivial. Luego, tenemos que $z^2 + x^2 + y^2 \equiv 0 \bmod 4$ y como los cuadrados en $\mathbb{Z}/4\mathbb{Z}$ son 0 y 1, concluimos que $x \equiv y \equiv z \equiv 0 \bmod 4$ en contradicción con que la solución (x, y, z) es primitiva. En conclusión, si $u \equiv v \equiv -1 \bmod 4$, tenemos que $(u, v) = -1$.

Segundo, si $n = 1$ y $m = 0$, tenemos que probar que $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$. Veamos que $(2, v) = (-1)^{\omega(v)}$, i.e., $(2, v) = 1$ si y solo si $v \equiv \pm 1 \bmod 8$. Supongamos que $(2, v) = 1$, entonces la ecuación $Z^2 - 2X^2 - vY^2 = 0$ tiene una solución no trivial $(x, y, z) \in (\mathbb{Z}_2)^3$ que, por el Lema A.12, verifica que $y, z \in \mathbb{U}^2$. Por tanto, y, z no son múltiplos de 2 y, con ello, $y^2 \equiv z^2 \equiv 1 \bmod 8$. Entonces, se tiene que $1 - 2x^2 - v \equiv 0 \bmod 8$ y como los cuadrados

módulo 8 son $0, 1$ y 4, concluimos que $v \equiv \pm 1 \bmod 8$. Recíprocamente, si $v \equiv 1 \bmod 8$, por el Teorema 2.40, v es un cuadrado y por las propiedades del símbolo de Hilbert $(2, v) = 1$. Si $v \equiv -1 \bmod 8$, la ecuación $Z^2 - 2X^2 - vY^2 = 0$ tiene a $(1, 1, 1)$ como solución módulo 8 y por el Corolario 2.26, se levanta a una solución 2-ádica, en otras palabras, $(2, v) = 1$. Veamos que $(2u, v) = (2, v)(u, v)$. Si $(2, v) = 1$ o $(u, v) = 1$, por la Proposición 4.7, lo tenemos. Supongamos que $(2, v) = -1$ y $(u, v) = -1$ y veamos que $(2u, v) = 1$. Por los apartados anteriores, tenemos que $v \equiv 3 \bmod 8$ y que $u \equiv -1 \bmod 8$ o $u \equiv 3 \bmod 8$. Por tanto, la ecuación $Z^2 - 2uX^2 - vY^2 = 0$ se reduce a

$$Z^2 + 2X^2 - 3Y^2 \equiv 0 \bmod 8 \quad \text{o} \quad Z^2 - 6X^2 - 3Y^2 \equiv 0 \bmod 8.$$

En ambos casos $(1, 1, 1)$ es solución y de nuevo, por el Corolario 2.26, se levanta a una solución 2-ádica, es decir, $(2u, v) = 1$.

Por último, si $n = 1$ y $m = 1$, tenemos que probar que $(2u, 2v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}$. Utilizando las propiedades del símbolo de Hilbert, tenemos que

$$(2u, 2v) = (2u, -4uv) = (2u, -uv)$$

y aplicando lo que acabamos de probar en el párrafo anterior, tenemos que

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

Utilizando que $\varepsilon(z)$ y $\omega(z)$ son homomorfismo de grupos, se tiene que

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

concluyendo así el resultado. □

Concluimos este apartado del apéndice enunciando y demostrando el Teorema de interpolación que nos dice que, bajo ciertas condiciones, siempre podemos encontrar un número racional cuyos símbolo de Hilbert han sido prefijados.

Para demostrar este teorema necesitamos usar el Teorema de Dirichlet cuya prueba se extiende a lo largo de un capítulo completo [9, Capítulo VI] y requiere del uso de resultados de teoría analítica de números. Por este motivo, su demostración se excluye tanto de la memoria como del apéndice.

Teorema A.14 (Teorema de Dirichlet)**.** *Sean a y m enteros coprimos mayores o iguales que 1, entonces existen infinitos primos p tales que $a \equiv p \bmod m$.*

Recordamos el enunciado del Teorema 4.13.

Teorema A.15. *Sea $(a_i)_{i\in I}$ una familia finita de elementos de $\mathbb{Q}^*$ y sea $(\varepsilon_{i,v})_{i\in I, v\in\mathcal{V}}$ una familia de números de $\{\pm 1\}$. Se tiene que existe un $x \in \mathbb{Q}^*$ verificando $(a_i, x)_v = \varepsilon_{i,v}$ para todos $i \in I$ y $v \in \mathcal{V}$ si y solo si se verifican las siguientes condiciones:*

- *Casi todos los $\varepsilon_{i,v}$ excepto un número finito son 1.*
- *Para todo $i \in I$, $\prod_{v\in\mathcal{V}} \varepsilon_{i,v} = 1$.*
- *Para todo $v \in \mathcal{V}$ existe un $x_v \in \mathbb{Q}_v^*$ tal que $(a_i, x_v)_v = \varepsilon_{i,v}$ para todo $i \in I$.*

Demostración. Las dos primeras condiciones necesarias se siguen del Teorema 4.11 y para la tercera basta tomar $x_v = x$.

Recíprocamente, supongamos que tenemos una familia de números $(\varepsilon_{i,v})_{i\in I, v\in\mathcal{V}}$ verificando las condiciones suficientes del teorema. Multiplicamos los a_i por los cuadrados de sus denominadores si es necesario para obtener una familia de enteros sin alterar las hipótesis del teorema. Consideramos los siguientes conjuntos finitos

$$\mathcal{S} = \{v \in \mathcal{V} : v = \infty, v = 2 \text{ y } v \text{ es factor primo de algún } a_i\},$$

$$\mathcal{T} = \{v \in \mathcal{V} : \text{ existe } i \in I \text{ con } \varepsilon_{i,v} = -1\}$$

y distinguimos dos casos.

Primero, supongamos que $\mathcal{S} \cap \mathcal{T} = \emptyset$ y escribimos

$$a = \prod_{t\in\mathcal{T}} t, \qquad m = 8 \prod_{s\in\mathcal{S}, s\neq 2,\infty} s.$$

Como a y m son coprimos, por el Teorema A.14, tenemos que existe p primo, de hecho existen infinitos, con $a \equiv p \bmod m$ con $p \notin \mathcal{S}\cup\mathcal{T}$. Veamos que $x = ap$ verifica $(a_i, x)_v = \varepsilon_{i,v}$ para todo $i \in I$ y para todo $v \in \mathcal{V}$.

Supongamos que $v \in \mathcal{S}$ y como $\mathcal{S} \cap \mathcal{T} = \emptyset$, tenemos que $\varepsilon_{i,v} = 1$; por tanto, basta ver que $(a_i, x)_v = 1$. Si $v = \infty$, como $x > 0$ por el Teorema 4.8 se cumple $(a_i, x)_\infty = 1$. Si $v = l$ con l primo tenemos que $x \equiv a^2 \bmod m$. Por tanto, si $p = 2$, tenemos que $x \equiv a^2 \bmod 8$ y si $p \neq 2$, $x \equiv a^2 \bmod l$. Por definición de x y a, tenemos que $x, a \in \mathbb{U}^l$ y por el Teorema 2.37 y el Teorema 2.40, tenemos que x es cuadrado. En conclusión, por las propiedades del símbolo de Hilbert, se tiene que $(a_i, x)_l = 1$.

Por otro lado, si $v = l \notin \mathcal{S}$, tenemos que $a_i \in \mathbb{U}^l$ y como $l \neq 2$, por el Teorema 4.8, se tiene que

$$(a_i, b) = \left(\frac{a_i}{l}\right)^{v_l(b)} \text{ para todo } b \in \mathbb{Q}_l^*.$$

Si $l \notin \mathcal{T}\cup\{p\}$, tenemos que $x \in \mathbb{U}^l$, es decir, $v_l(x) = 0$ y, por lo anterior, se tiene que $(a_i, x)_l = 1$; además, como $l \notin \mathcal{T}$, $\varepsilon_{i,l} = 1$ y concluimos que $(a_i, x)_l = \varepsilon_{i,l}$.

Si $l \in \mathcal{T}$, tenemos que $v_l(x) = 1$ y por la tercera condición del teorema tenemos que existe un $x_l \in \mathbb{Q}_l^*$ tal que $(a_i, x_l)_l = \varepsilon_{i,l}$ para todo $i \in I$. Como $l \in \mathcal{T}$, tenemos que $\varepsilon_{i,l} = -1$ luego $v_l(x_l) \equiv 1 \bmod 2$. Por tanto, tenemos que

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l} \text{ para todo } i \in I.$$

Si $l = p$, combinando las condiciones del teorema y el Teorema 4.11, tenemos que

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

Supongamos que $\mathcal{S} \cap \mathcal{T} \neq \emptyset$. Sabemos que $\mathbb{Q}_v^{*2}$ es subgrupo abierto de $\mathbb{Q}_v^*$ y que $\mathcal{S}$ es finito. Tomamos $v \in \mathcal{S}$ y por hipótesis sabemos que existe un $x_v \in \mathbb{Q}_v^*$ tal que $(a_i, x_v)_v = \varepsilon_{i,v}$ para todo $i \in I$. Por el Teorema 4.12, tenemos que existe un $y \in \mathbb{Q}^*$ tal que $y/x_v \in \mathbb{Q}_v^{*2}$. Con ello, $(a_i, y)_v = (a_i, x_v)_v = \varepsilon_{i,v}$. Consideramos $\eta_{i,v} = \varepsilon_{i,v}(a_i, y)_v$ para cada $i \in I$ que verifica las tres condiciones del teorema. Si $v \in \mathcal{S}$, tenemos que $\eta_{i,v} = 1$ y tenemos que $\mathcal{S} \cap \mathcal{T} = \emptyset$,

luego por el apartado anterior, existe un $z \in \mathbb{Q}^*$ tal que $(a_i, z)_v = \eta_{i,v}$ para todo $i \in I$ y para todo $v \in \mathcal{V}$. Definimos $x := yz$ y veamos que

$$(a_i, x)_v = (a_i, y)_v (a_i, z)_v = \varepsilon_{i,v}$$

como queríamos probar. □

A.3. Prerrequisitos de Topología

Concluimos con los resultados de topología que se han empleado para estudiar la topología p-ádica. Comenzamos recordando algunos resultados fundamentales sobre compacidad.

Definición A.16. *Sea (X, τ) un espacio topológico. Decimos que X es **compacto** si todo recubrimiento abierto admite un subrrecubrimiento finito.*

Dado que los p-ádicos están dentro de un anillo producto resulta natural recordar que la topología producto es la topología más gruesa que hace continuas a las proyecciones. Se relaciona con la compacidad mediante el siguiente resultado.

Teorema A.17 (Teorema de Tychonoff)**.** *Sea $(X_i, \tau_i)_{i \in I}$ una familia de espacios topológicos compactos. Entonces el producto cartesiano $\prod_{i \in I} X_i$ dotado con la topología producto es un espacio compacto.*

Pasamos a recordar algunos resultados particulares sobre espacios métricos, ver [4].

Definición A.18. *Sea (X, d) un espacio métrico. Diremos que X es **completo** si toda sucesión de Cauchy en X es convergente.*

Definición A.19. *Sea (X, d) un espacio métrico, llamamos **completación** del espacio métrico (X, d) a un espacio métrico completo (X', d') tal que X es isométrico a un subconjunto denso de X'.*

Proposición A.20. *Sea (X, d) un espacio métrico completo y $A \subseteq X$ un subconjunto cerrado. Entonces A es completo.*

Teorema A.21. *Todo espacio métrico compacto es completo.*

Finalmente, introducimos dos nociones que hemos empleado para probar que los p-ádicos son localmente compactos.

Definición A.22. *Sea (X, d) un espacio métrico y $k \subseteq X$ un subconjunto. Diremos que K es **secuencialmente compacto** si cada sucesión $(x_n)_{n=1}^{\infty}$ en K posee una subsucesión $(x_{n_k})_k$ convergente a un punto en K.*

Teorema A.23. *Sea (X, d) un espacio métrico. Entonces X es compacto si y solo si X es secuencialmente compacto.*

Definición A.24. *Sea (X, d) un espacio métrico. Diremos que es **totalmente acotado** si para todo $\varepsilon > 0$ existe una familia finita de bolas de radio ε cuya unión contiene a X.*

Proposición A.25. *Todo espacio métrico completo y totalmente acotado es secuencialmente compacto.*

Bibliografía

[1] K. Conrad, Hensel's Lemma [en línea]. <https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf>. [Consulta: 22/1/2024]

[2] K. Conrad, The Local-global Principle [en línea]. <https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf>. [Consulta: 15/2/2024]

[3] F. Q. Gouvêa, *p-adic Numbers. An introduction*, Berlin: Springer, 1957.

[4] P.J. Herrero Piñeyro, *Topología de Espacios Métricos*, Universidad de Murcia, 2010. <https://www.um.es/web/innovacion/plataformas/ocw/listado-de-cursos/topologia-de-espacios-metricos/material-de-clase>.[Consulta: 8/6/2024]

[5] D. Hilbert, *Mathematical Problems*, Bulletin of the American Mathematical Society, 8(10), 437-479. <https://www.ams.org/journals/bull/1902-08-10/S0002-9904-1902-00923-3/?active=current>. [Consulta: 4/6/2024] pg. 458

[6] K. Hoffman, R. Kunze, *Álgebra Lineal*, Prentice-Hall Hispanoamericana, México, 1973.

[7] Y. Kitaoka, *Arithmetic of cuadratic forms*, Cambridge University Press, 2010.

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

[9] J-P. Serre, *A Course in Arithmetic*, New York : Springer-Verlag, 1973.