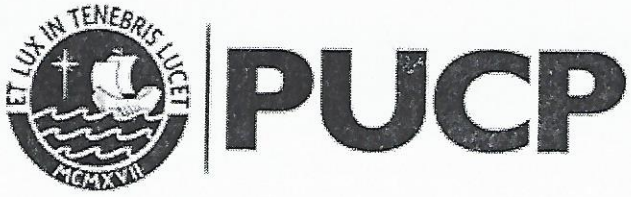
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO



"El teorema de Hasse-Minkowsky para formas cuadráticas de cuatro o más variables"

Tesis para optar el grado de Magíster en Matemáticas

AUTOR

Alberto Alonso Castillo García

ASESOR

Alfredo Poirier Schmitz

JURADO

Christian Valqui Haase

Jaime Cuadros Valle

LIMA – PERÚ

2016

Introducción

El objetivo principal de este trabajo es concluir la prueba del teorema de Hasse Minkowsky (de manera específica, los casos $n = 4$ y $n \geq 5$) iniciada en mi tesis de pregrado [2]. Adicionalmente, regresaremos a resultados cuya prueba quedó pendiente en aquella tesis. Es más, como gran parte de las definiciones y resultados que necesitamos se encuentran ahí, haremos múltiples referencias a [2] a lo largo de este trabajo.

En el primer capítulo nos ocuparemos del teorema de Chevalley, pero principalmente buscamos cómo relacionar este resultado con el lema de Hensel. Ello nos permitirá obtener un mecanismo para encontrar condiciones bajo las cuales una forma cuadrática representa a cero. La ventaja de semejante desarrollo reside en que solo se necesita trabajar con ecuaciones sobre cuerpos finitos (en este caso $\mathbb{Z}/p\mathbb{Z}$), en donde encontrar soluciones resulta menos laborioso que en $\mathbb{Q}_p$.

En el segundo capítulo definimos el símbolo de Legendre, una herramienta necesaria para la prueba de la bimultiplicidad del símbolo de Hilbert (resultado que quedó pendiente en la tesis de pregrado). Como aplicación del concepto y propiedades del símbolo de Legendre probaremos la ley de reciprocidad cuadrática, la cual es útil por mérito propio.

En el tercer capítulo probaremos la bimultiplicidad del símbolo de Hilbert, el primer resultado de relevancia en esta tesis. Lo que en realidad haremos será establecer una fórmula que nos permita hallar el símbolo de Hilbert de cualquier par de números p-ádicos; a partir de ésta, la bimultiplicidad del símbolo resulta obvia. Cerramos el capítulo con la prueba de una proposición que verá utilidad cuando se ataque el teorema de Hasse-Minkowsky.

En el cuarto capítulo exhibiremos algunas propiedades topológicas del cuerpo $\mathbb{Q}_p$. La más notable es el teorema de aproximación débil, que será utilizado para tratar el teorema central.

En el quinto capítulo trabajaremos con símbolos de Hilbert aplicados al cuerpo global $\mathbb{Q}$. Además, se probará un segundo resultado de relevancia, la fórmula producto de Hilbert. Luego se desarrollarán ejemplos ilustrativos sobre ecuaciones y sistemas de ecuaciones con símbolos de Hilbert, lo que dará lugar a un resultado auxiliar que será empleado en la prueba del teorema de Hasse-Minkowsky.

El sexto capítulo es básicamente una extensión del capítulo 5 de [2]. Nos limitamos a presentar algunos resultados adicionales y a probar una proposición que quedó pendiente en [2].

En el sétimo capítulo concluimos la prueba del teorema de Hasse-Minkowsky para los casos $n = 4$ y $n \geq 5$.

El octavo y último capítulo es aplicativo. Utilizaremos el teorema de Hasse Minkowsky para clasificar formas cuadráticas sobre los racionales.

Por último, quisiera reiterar mi agradecimiento a mis familiares y seres queridos por su apoyo incondicional. Como siempre, un agradecimiento especial al Dr. Alfredo Poirier por su tiempo y sus valiosas sugerencias.

Índice General

Capítulo 1

El teorema de Chevalley

Una de las herramientas que requerimos para la prueba de la bimultiplicidad del símbolo de Hilbert es un método para asegurar la existencia de soluciones en ecuaciones sobre los p-ádicos. La primera meta será trabajar un criterio para confirmar la existencia de soluciones no triviales sobre cuerpos finitos, por ejemplo $\mathbb{Z}/p\mathbb{Z}$.

Vamos a probar un conocido resultado debido a Chevalley. Trabajamos en el contexto de un cuerpo finito F con q elementos. Antes de ello abordaremos un par de lemas.

Lema 1.1. *Sea $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ un polinomio de grado menor que q en cada una de sus variables. Si f se anula en todo valor, entonces es idénticamente nulo.*

Prueba. Trabajaremos por inducción. Si se tiene $n = 1$ y f posee q raíces distintas, al ser f de grado menor a q, no queda otra que sea idénticamente nulo. Ahora suponemos que el lema ya fue probado para $n - 1$. Es claro que todo polinomio f de n variables en el contexto puede escribirse cual

$$f(x_1, \cdots, x_n) = \sum_{i=0}^{q-1} g_i(x_1, \cdots, x_{n-1}) x_n^i,$$

donde g_i es un polinomio de grado menor que q en cada una de sus $n-1$ variables. Tomemos $a = (a_1, \cdots, a_{n-1})$. Resulta que $\sum_{i=0}^{q-1} g_i(a) x_n^i$ es un polinomio de una variable que posee q raíces distintas, con lo que éste es idénticamente nulo. Por hipótesis inductiva g_i es idénticamente nulo y lo mismo ocurre para f. □

Recordemos que dos polinomios $f, g \in F[X]$ son **equivalentes** si se verifica $f(a) = g(a)$ para todo $a \in F[X]$.

Lema 1.2. *Todo polinomio $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ es equivalente a un polinomio de grado menor que q en cada una de sus variables.*

Prueba. Al tratarse de un cuerpo con q elementos se tiene que x^q es equivalente a x. De acá fácilmente se sigue que para $d \geq q$ se cumple $x^d = x^{d-q+1}$ y el resultado se sigue por inducción.

Para un polinomio de n variables la cuestión se reduce a analizar cada monomio que lo conforma. Es claro que por la observación anterior el grado de cualquiera se puede reducir a uno menor que q en cada variable. □

Teorema 1.3 (Chevalley). *Sea $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ un polinomio homogéneo de grado $d < n$. Entonces f tiene al menos dos raíces.*

Prueba. Al ser f un polinomio homogéneo, tiene a 0 como raíz. Supongamos que ésta sea la única solución. De ser así, es claro que $f^{q-1}(x)$ toma el valor 1 para todo x salvo 0. De esta forma, el polinomio $u(x) = 1 - f^{q-1}(x)$ (cuyo grado es $d(q-1)$) vale 1 para $x = 0$ y 0 para el resto de puntos. Pero lo anterior también se cumple para el polinomio

$$v(x) = \prod_{i=1}^{n} (1 - x_i^{q-1}),$$

cuyo grado en cada variable es $q - 1$. Ahora, por el Lema 1.2, u es equivalente a un polinomio u' de grado menor a q en cada variable. De esta manera, el polinomio $w(x) = u'(x) - v(x)$ tiene grado menor a q en cada variable y se anula para todo x. Como w cumple las hipótesis del Lema 1.1, resulta ser idénticamente nulo. Se satisface entonces la relación $u'(x) - v(x) = 0$ y se tiene que el grado de u' resulta ser igual a $(q-1)n$. Por otro lado se tiene también $\text{grad}(u') \leq \text{grad}(u) = d(q-1)$ con lo cual se concluye $n \leq d$, lo que contradice la hipótesis. □

Corolario 1.4. *Todas las formas cuadráticas $f(x_1, \cdots, x_n)$ sobre $\mathbb{Z}/p\mathbb{Z}$, con n al menos 3, tienen un cero no trivial.*

Prueba. Las formas cuadráticas son polinomios homogéneos de grado 2, menor que n. □

El corolario del teorema de Chevalley asegura que una forma cuadrática de al menos 3 variables con coeficientes sobre $\mathbb{Z}/p\mathbb{Z}$ representa a cero.

Si bien éste es un resultado útil, necesitamos una herramienta que nos asegure la existencia de ceros de formas cuadráticas sobre $\mathbb{Q}_p$. La idea es la siguiente: podemos asegurar la existencia de una solución no trivial en $\mathbb{Z}/p\mathbb{Z}$ y luego encontrar condiciones para que ello implique la existencia de una solución en $\mathbb{Q}_p$.

A continuación enunciamos la versión generalizada del lema de Hensel, el cual asegura la existencia de ceros de polinomios sobre $\mathbb{Z}_p^n$ bajo ciertas condiciones. Acto seguido presentamos dos corolarios que serán de utilidad para nuestros propósitos.

Teorema 1.5. *Sea $f \in \mathbb{Z}_p[x_1, \cdots, x_n]$. Sea $x \in \mathbb{Z}_p^n$ sujeto a*

$$f(x) \equiv 0 \ (\text{mód } p^{2s+1}),$$

y de modo que para alguna derivada parcial se tenga también

$$\frac{\partial f}{\partial x_i}(x) \equiv 0 \ (\text{mód } p^s),$$

pero se cumpla

$$\frac{\partial f}{\partial x_i}(x) \not\equiv 0 \ (\text{mód } p^{s+1}),$$

donde $s \geq 0$. Entonces existe un cero $\overline{x} \in \mathbb{Z}_p^n$ de f que es congruente a x módulo p^{s+1}.

Prueba. Los detalles de la prueba se pueden revisar en la tesis de Condori [3]. □

A continuación se probarán dos corolarios que aplican el resultado del teorema anterior al caso de formas cuadráticas regulares. Recordemos que una forma cuadrática $f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$ es regular si su discriminante $d_f = a_1 \cdots a_n$ es distinto de cero. Nos remitimos a [2] para más detalles.

Corolario 1.6. *Sea p primo impar. Sea $f(x_1, \cdots, x_n)$ una forma cuadrática regular en $\mathbb{Z}_p$ (interprétese, cuyo discriminante es invertible en $\mathbb{Z}_p$). Sea $x \in \mathbb{Z}_p^n$ tal que al menos una de sus componentes no es divisible por p y que satisface $f(x) \equiv 0$ (mód p). Entonces f representa a 0.*

Prueba. Puesto que se cumple $d_f \neq 0$ (mód p), ningún a_i es divisible por p. Como se tiene $\dfrac{\partial f}{\partial x_i} = 2a_i x_i$, y al menos un x_i no es divisible por p, al menos una derivada parcial no se anula. Finalmente, el Teorema 1.5, para $s = 0$, nos permite concluir que existe $y \in \mathbb{Z}_p^n$ de tal forma que se tiene $f(y) = 0$. □

Corolario 1.7. *Sea $p = 2$ y $f(x_1, \cdots, x_n)$ una forma cuadrática regular en $\mathbb{Z}_2$ (en el sentido utilizado por el corolario anterior). Sea $x \in \mathbb{Z}_2^n$ tal que al menos una de sus componentes no es divisible por 2 y que satisface $f(x) \equiv 0$ (mód 8). Entonces f representa a 0.*

Prueba. Basta aplicar el Teorema 1.5 para $s = 1$. Para asegurar que al menos una derivada parcial no es congruente a 0 módulo 4 basta con tener que al menos una de las componentes de x no sea divisible por 2 y aprovechar que se tiene $d_f \neq 0$ (mód 2). □

Los corolarios del Teorema 1.5 serán de utilidad para verificar si una forma cuadrática representa a 0. Basta invocar el corolario del teorema de Chevalley y verificar que se cumplen condiciones adicionales.

Capítulo 2

El símbolo de Legendre y la ley de reciprocidad cuadrática

El primer resultado de relevancia en este trabajo es la prueba de la bimultiplicidad del símbolo de Hilbert. Para ello es necesario introducir algunos conceptos previos en aras de facilitar el desarrollo de dicha prueba. Dedicamos éste capítulo a introducir el símbolo de Legendre y la nomenclatura asociada con la demostración de la conocida ley de reciprocidad cuadrática. Remitimos al lector a la tesis de Edwin Villogas [8], en donde se amplían los resultados de este capítulo.

Sea p primo impar y u entero módulo p. El **símbolo de Legendre** de u, denotado por $\left(\frac{u}{p}\right)$, es una aplicación definida como

$$\left(\frac{u}{p}\right) = \begin{cases} 1 & \text{si } u \text{ es un residuo cuadrático módulo } p, \\ -1 & \text{si } u \text{ no es un residuo cuadrático módulo } p, \\ 0 & \text{si } u \text{ es divisible por } p. \end{cases}$$

Ilustramos esta idea con un ejemplo sencillo. Para $p = 7$, el símbolo de Legendre de 11 es 1 puesto que se cumple $11 = 7 \cdot 1 + 4$. De igual forma, el símbolo de Legendre de 31 es -1 pues se tiene $31 = 7 \cdot 4 + 3$ y 3 no está en la lista $\{1, 2, 4\}$ de los cuadrados módulo 7.

Cabe mencionar que el símbolo de Legendre es una función multiplicativa, es decir, cumple $\left(\frac{uv}{p}\right) = \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. La demostración de este hecho es sencilla a partir de un resultado más general. Previamente recordemos que $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ es un grupo multiplicativo cíclico (en nuestro caso de orden igual a $p-1$) y que $\mathbb{F}_p^{*2}$ es un subgrupo del mismo.

Proposición 2.1. *Para p primo impar, se cumple $[\mathbb{F}_p^* : \mathbb{F}_p^{*2}] = 2$. Además $\mathbb{F}_p^{*2}$ es el núcleo del homomorfismo $f(x) = x^{(p-1)/2}$ definido sobre $\mathbb{F}_p^*$.*

Prueba. Empezamos demostrando la segunda afirmación. Cabe mencionar que el núcleo de f está conformado por todos los elementos de $\mathbb{Z}/p\mathbb{Z}^*$ cuya imagen es 1. Se sabe que siempre se cumple $x^{p-1} = 1$, motivo por el cual se tiene $x^{(p-1)/2} = \pm 1$. Observamos que la ecuación $x^{(p-1)/2} = 1$ solo puede tener $\dfrac{p-1}{2}$ soluciones, por tanto, para los $\dfrac{p-1}{2}$ valores restantes se tendrá $x^{(p-1)/2} = -1$. Si se cumple $x \in \mathbb{F}_p^{*2}$ entonces existe y en $\mathbb{F}_p^*$ tal que $x = y^2$. De esta manera se satisface $x^{(p-1)/2} = y^{p-1} = 1$. Por otro lado, todo $x \in Nu(f)$ satisface $x^{(p-1)/2} = 1$. Si ponemos $x = y^2$, se tiene $(y^2)^{(p-1)/2} = y^{p-1} = 1$. Así logramos $y \in \mathbb{F}_p^*$ y con ello $x \in \mathbb{F}_p^{*2}$. Con esto hemos demostramos que el núcleo coincide con $\mathbb{F}_p^{*2}$. Finalmente, como $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ es isomorfo a $\{\pm 1\}$, el índice de $\mathbb{F}_p^{*2}$ resulta 2. □

Esta proposición nos permite escribir el símbolo de Legendre para u de manera explícita con la fórmula $\left(\dfrac{u}{p}\right) = u^{(p-1)/2} \pmod p = \pm 1$. Visto así, la condición de ser una función multiplicativa es inmediata.

Ahora definimos dos funciones auxiliares que servirán para simplificar notación. Cuando n es un entero impar ponemos

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

y

$$\omega(n) \equiv \frac{n^2-1}{8} (\text{mód } 2) = \begin{cases} 0 & \text{si } n \equiv \pm 1 \pmod 8 \\ 1 & \text{si } n \equiv \pm 5 \pmod 8). \end{cases}$$

Proposición 2.2. *La función ϵ es un homomorfismo del grupo multiplicativo $\mathbb{F}_4^*$ sobre el grupo aditivo $\mathbb{F}_2$ y ω es un homomorfismo del grupo multiplicativo $\mathbb{F}_8^*$ sobre el grupo aditivo $\mathbb{F}_2$.*

Prueba. Veamos primero el caso de ϵ. Es obvio que se cumplen las igualdades

$$\epsilon([1][1]) = \epsilon([1]) = 0 = 0+0 = \epsilon([1]) + \epsilon([1]),$$
$$\epsilon([1][3]) = \epsilon([3]) = 1 = 0+1 = \epsilon([1]) + \epsilon([3]),$$
$$\epsilon([3][3]) = \epsilon([1]) = 0 = 1+1 = \epsilon([3]) + \epsilon([3]).$$

Resulta así que ϵ es un homomorfismo.

Para ω las igualdades a verificar son

$$\omega([\pm1][\pm1]) = \omega([\pm1]) = 0 = 0+0 = \omega([\pm1]) + \omega([\pm1]),$$
$$\omega([\pm1][\pm5]) = \omega([\pm5]) = 1 = 0+1 = \omega([\pm1]) + \omega([\pm5]),$$
$$\omega([\pm5][\pm5]) = \omega([\pm1]) = 0 = 1+1 = \omega([\pm5]) + \omega([\pm5]).$$

De nuevo, resulta claro que ω es un homomorfismo. □

A manera de ejemplo hallaremos el símbolo de Legendre para ciertos números.

Ejemplo 2.3. Siempre se tiene $\left(\frac{1}{p}\right) = 1^{(p-1)/2} = 1$. Por otro lado, el símbolo de Legendre de -1 es el valor $-1^{(p-1)/2}$. Si $p-1$ es múltiplo de 4, entonces se tiene $\left(\frac{-1}{p}\right) = 1$, caso contrario se logra $\left(\frac{-1}{p}\right) = -1$. Como un número primo impar es congruente a 1 módulo 4 o bien a 3 módulo 4, obtenemos la fórmula $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$.

Ejemplo 2.4. Para p primo impar, hallaremos el símbolo de Legendre de 2. Sea α un número que satisface $\alpha^4 = -1$ en alguna extensión de $\mathbb{Z}/p\mathbb{Z}$. Una primera observación indica que se tiene

$$(\alpha^2 + 1/\alpha^2)^2 = \alpha^4 + 2 + 1/\alpha^4 = -1 + 2 - 1 = 0,$$

y con ello $\alpha^2 + 1/\alpha^2 = 0$. Al poner $y = \alpha + 1/\alpha$ notamos que se cumple $y^2 = \alpha^2 + 2 + 1/\alpha^2 = 2$. Como trabajamos en un cuerpo de característica p vale la expresión $y^p = (\alpha + 1/\alpha)^p = \alpha^p + 1/\alpha^p$. Identificamos dos casos. Primero, si $p \equiv \pm 1$ (mód 8), es claro que se cumple

$$y^p = y^{8k\pm1} = \alpha^{8k\pm1} + 1/\alpha^{8k\pm1} = \alpha^{\pm1} + 1/\alpha^{\pm1} = y.$$

Luego, de $y^2 = 2$ se consigue

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1.$$

Por el contrario, si $p = \pm5$ (mód 8), se cumple $y^p = \alpha^5 + 1/\alpha^5$. Y a partir de $\alpha^4 = -1$ conseguimos la igualdad

$$\alpha^5 + 1/\alpha^5 = -(\alpha + 1/\alpha) = -y.$$

De esta manera se tiene $y^p = -y$, lo que conduce a $\left(\frac{2}{p}\right) = y^{p-1} = -1$.

Todo lo anterior puede resumirse en la fórmula $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.

Nota 2.5. A pesar de que el símbolo solo fue definido para números enteros, es posible extender la definición para unidades p-ádicas siempre que se tenga $p \neq 2$. Recordemos que en [2] se demostró que $u = u_0 + u_1p + u_2p^2 + \cdots \in \mathbb{Q}_p$ es un cuadrado perfecto para $p \neq 2$ si y solo si u_0 también lo es. En consecuencia la relación $\left(\frac{u}{p}\right) = \left(\frac{u_0}{p}\right)$ queda bien definida. Es decir, el símbolo de Legendre de una unidad p-ádica coincide con el de su reducción módulo p. También es posible extender la definición de las funciones ϵ y ω en $\mathbb{Z}_2^*$. En el caso de ϵ basta evaluar en la reducción módulo 4 y en el caso de ω, en la reducción módulo 8.

Si bien la fórmula para el cálculo del símbolo de Legendre obtenida a partir de la Proposición 2.1 resulta ser útil, su aplicación puede resultar engorrosa para un valor de n grande. A continuación probaremos el lema de Gauss, que proporciona otra fórmula para el cálculo del símbolo de Legendre.

Primero hagamos una observación. Sea $a \in \mathbb{F}_p^*$ con p primo impar. El conjunto $R = \{r_1, r_2, \cdots, r_{(p-1)/2}\}$ se define de tal forma que r_i es la reducción módulo p del valor ai para $i = 1, \cdots, \frac{p-1}{2}$. Definimos los

siguientes subconjuntos: $M_a = \{a_1, a_2, \cdots, a_k\}$, formado de aquellos r_i menores a $p/2$ y $N_a = \{b_1, \cdots, b_n\}$, formado por los r_i mayores a $p/2$. Es claro que M_a y N_a son disjuntos y además se tiene $R = M_a \cup N_a$.

Lema 2.6 (Lema de Gauss). *Para p primo impar y $a \in \mathbb{F}_p^*$, se cumple $\left(\frac{a}{p}\right) = (-1)^n$, donde n es la cardinalidad del subconjunto N_a mencionado arriba.*

Prueba. A partir de N_a formamos un nuevo subconjunto $S_a = \{s_1, \cdots, s_n\}$ con $s_i = p - b_i$. De $b_i > p/2$ se obtiene $s_i < p/2$. Vamos a comprobar que M_a y S_a son disjuntos. Supongamos se tenga $s_i = a_j$ para ciertos i y j. Entonces se tiene $p - b_i = a_j$ y así $b_i + a_j \equiv 0 \pmod{p}$. Recordemos que se cumple $a_j \equiv a\alpha \pmod{p}$ y $b_i \equiv a\beta \pmod{p}$ para ciertos $\alpha, \beta \leq (p-1)/2$. Así tenemos $b_i + a_j \equiv a(\alpha + \beta) \equiv 0 \pmod{p}$. Pero $\alpha + \beta \leq (p-1)/2 + (p-1)/2 = p - 1 < p$ fuerza a tener $a \equiv 0 \pmod{p}$, con lo que llegamos a una contradicción. Ahora, como M_a y S_a son disjuntos, su unión $M_a \cup S_a$ es un conjunto con $(p-1)/2$ elementos, todos ellos menores a $p/2$. Es inmediata entonces la igualdad $M_a \cup S_a = \{1, 2, \cdots, \frac{p-1}{2}\}$. De esta manera tenemos

$$a_1 \cdots a_k (p - b_1) \cdots (p - b_n) = a_1 \cdots a_k s_1 \cdots s_n = (\frac{p-1}{2})!.$$

Es claro que el producto $(p - b_1) \cdots (p - b_n)$ es congruente a $(-1)^n b_1 \cdots b_n \pmod{p}$. Al reemplazar esto en la equivalencia anterior llegamos a

$$(-1)^n a_1 \cdots a_k b_1 \cdots b_n \equiv (\frac{p-1}{2})! \pmod{p}$$
$$(-1)^n r_1 \cdots r_{(p-1)/2} \equiv (\frac{p-1}{2})! \pmod{p}.$$

Por definición se tiene $r_i \equiv ai \pmod{p}$; se logra entonces

$$(-1)^n a(a \cdot 2) \cdots (a \cdot (p-1)/2) \equiv (\frac{p-1}{2})! \pmod{p}$$
$$(-1)^n a^{(p-1)/2} (\frac{p-1}{2})! \equiv (\frac{p-1}{2})! \pmod{p},$$

y con ello

$$(-1)^n a^{(p-1)/2} \equiv 1 \ (\text{mód } p).$$

De esta manera se deriva $(-1)^n \equiv a^{(p-1)/2} \ (\text{mód } p)$. Como se tiene $\left(\frac{a}{p}\right) = a^{(p-1)/2} \ (\text{mód } p)$, concluimos la igualdad $\left(\frac{a}{p}\right) = (-1)^n$. □

Vemos que el lema de Gauss gira en torno al valor n (la cardinalidad del conjunto N_a definido anteriormente). En realidad, basta conocer la paridad de este número para zanjar el asunto del cálculo del símbolo de Legendre. El siguiente lema arroja mayor luz sobre cómo hallar este valor.

Lema 2.7. *Para $a \in \mathbb{F}_p^*$ impar y positivo se cumple $n \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right]$ (mód 2), acá $[m]$ es la función máximo entero de m.*

Prueba. Usaremos todas las definiciones y resultados que giran en torno al lema anterior. Primero, es inmediato que se tiene

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{n} b_j.$$

Dada la naturaleza de los r_t también se cumple

$$r_t = ta - p\left[\frac{ta}{p}\right].$$

De esa manera tenemos

$$\sum_{t=1}^{(p-1)/2} r_t = a \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right].$$

Así conseguimos la igualdad

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{n} b_j = a \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right]. \tag{1}$$

Por otro lado, gracias a $M_a \cup S_a = \{1, 2, \cdots, \frac{p-1}{2}\}$ se cumple

$$\begin{aligned} \sum_{t=1}^{(p-1)/2} t &= \sum_{i=1}^{k} a_i + \sum_{j=1}^{n} (p - b_j) \\ &= \sum_{i=1}^{k} a_i + pn - \sum_{j=1}^{n} b_j. \end{aligned} \tag{2}$$

Si sumamos las ecuaciones (1) y (2) logramos

$$2\sum_{i=1}^{k} a_i + np = (a+1) \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right].$$

Como se tiene que $a+1$ es par, al reducir módulo 2 se obtiene

$$n \equiv np \equiv -p \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right] \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{ta}{p}\right] \text{ (mód 2)},$$

con lo cual queda demostrada la afirmación. □

A continuación presentamos un último lema previo a la demostración de la ley de reciprocidad cuadrática.

Lema 2.8. *Dado p, q primos distintos, la función $f : \{0, \cdots, p-1\} \times \{0, \cdots, q-1\} \to \mathbb{Z}$ definida por $f(x, y) = qx - py$ es inyectiva.*

Prueba. Supongamos $f(x,y) = f(x',y')$. Entonces se tiene $q(x-x') = p(y-y')$ y por ende se cumple $x - x' \equiv 0 \pmod{p}$ y $y - y' \equiv 0 \pmod{q}$. De ahí es claro que se tiene $x = x'$ e $y = y'$. □

Teorema 2.9 (Ley de reciprocidad cuadrática). *Para p y q primos impares distintos se cumple* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p)\epsilon(q)}$.

Prueba. El lema de Gauss (Lema 2.6) nos permiten escribir

$$\left(\frac{p}{q}\right) = (-1)^m \quad \text{y} \quad \left(\frac{q}{p}\right) = (-1)^n,$$

con $m \equiv \sum_{x=1}^{(q-1)/2} \left[\frac{xp}{q}\right] \pmod 2$ y $n \equiv \sum_{y=1}^{(p-1)/2} \left[\frac{yq}{p}\right] \pmod 2$. De esta forma se tiene

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

Ahora, como x e y toman valores de 1 a $(q-1)/2$ y $(p-1)/2$, respectivamente, la función $f(x,y)$ definida en el Lema 2.8 toma $\frac{p-1}{2}\frac{q-1}{2}$ valores no nulos distintos (por la inyectividad). Para tales x e y definimos los conjuntos $A = \{(x,y) \text{ con } f(x,y) > 0\}$ y $B = \{(x,y) \text{ con } f(x,y) < 0\}$. Por definición $\frac{p-1}{2}\frac{q-1}{2}$ resulta la suma de las cardinalidades de A y B. Ahora, es claro que se tiene $f(x,y) = px - qy > 0$ si y solo si $px/q > y$, o equivalentemente si $[px/q] \geq y$, puesto que ni p ni $1, \cdots, \frac{q-1}{2}$ tienen factores comunes con q. De esta manera, para un x fijo, el entero $[px/q]$, resulta ser la cantidad de valores y que cumplen $[px/q] \geq y$. Se tiene entonces que $\sum_{x=1}^{(q-1)/2} \left[\frac{xp}{q}\right]$ es la cardinalidad de A. De igual forma, se satisface $f(x,y) < 0$ si y solo si $x > qy/p$, o equivalentemente $[qy/p] \leq x$. Entonces el valor $\sum_{y=1}^{(p-1)/2} \left[\frac{yq}{p}\right]$ es la cardinalidad de B. Concluimos la igualdad

$$\frac{p-1}{2}\frac{q-1}{2} = n + m = \sum_{x=1}^{(q-1)/2} \left[\frac{xp}{q}\right] + \sum_{y=1}^{(p-1)/2} \left[\frac{yq}{p}\right],$$

y queda confirmado el teorema. □

Capítulo 3

Propiedades locales del símbolo de Hilbert

Si bien en [2] ya fueron demostradas gran parte de las propiedades del símbolo de Hilbert que operan sobre los cuerpos locales $\mathbb{Q}_p$ y $\mathbb{R}$, quedó pendiente la prueba de la bimultiplicidad. En este capítulo abordaremos dicha tarea.

La primera labor será encontrar una fórmula cerrada que nos permita obtener el símbolo de Hilbert de dos números $a, b \in \mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$. Cabe subrayar que el caso $p = \infty$ es trivial, pues la ecuación $z^2 - ax^2 - by^2 = 0$ no posee solución únicamente en el caso $a, b < 0$. Por ende se tiene $(a, b) = 1$ si $a > 0$ o $b > 0$ y $(a, b) = -1$ si $a, b < 0$.

Teorema 3.1. *Sean $a, b \in \mathbb{Q}_p^*$. Escribamos estos números en la forma $a = p^m u$ y $b = p^n v$ con $m, n \in \mathbb{Z}$ y $u, v \in \mathbb{Z}_p^*$. Entonces se cumple*

$$(a, b) = \begin{cases} (-1)^{mn\epsilon(p)} \left(\frac{u}{p}\right)^n \left(\frac{v}{p}\right)^m & \text{si } p > 2 \\ (-1)^{\epsilon(u)\epsilon(v)+m\omega(v)+n\omega(u)} & \text{si } p = 2. \end{cases}$$

Vale mencionar que algunas de las herramientas que necesitamos para la prueba ya fueron trabajadas en [2]. Probaremos un lema previo al teorema.

Lema 3.2. *Sea v unidad p-ádica. Si la ecuación $z^2 - px^2 - vy^2 = 0$ tiene una solución no trivial en $\mathbb{Q}_p$, entonces posee una solución (z_0, x_0, y_0) con z_0 e y_0 unidades p-ádicas y x_0 entero p-ádico.*

Prueba. La Proposición 6.1 de [2] asegura la existencia de una solución (z_0, x_0, y_0) con $z_0, x_0, y_0 \in \mathbb{Z}_p$ donde al menos uno de estos valores no es múltiplo de p. Si esta solución no cumple lo deseado se tiene $y \equiv 0$ (mód p) o $z \equiv 0$ (mód p). Gracias a esto, dado que se cumple $z^2 - vy^2 \equiv 0$ (mód p), y como v es unidad p-ádica, tanto y como z resultan simultáneamente múltiplos de p. Es más, dado lo anterior, se tiene que $z^2 - vy^2 = px^2$ es

múltiplo de p^2, con lo cual, necesariamente, x debe ser múltiplo de p, lo que resulta absurdo por lo asumido. □

Ahora abordaremos la prueba del Teorema 3.1.

Prueba (del Teorema 3.1). Es claro que basta realizar la prueba cuando m y n valgan 0 ó 1. Empecemos con p impar.

Caso 1: $m = n = 0$. Acá todo se limita a probar que se cumple $(u, v) = 1$. Si reducimos la ecuación $z^2 - ux^2 - vy^2 = 0$ módulo p, el Corolario 1.4 garantiza la existencia de una solución no trivial en $(\mathbb{Z}/p\mathbb{Z})^3$. Como el discriminante de esta forma cuadrática es uv (unidad p-ádica), queda asegurado que es distinto de 0 módulo p. De esta manera se satisfacen las condiciones del Corolario 1.6, y existe una solución no trivial para $z^2 - ux^2 - vy^2 = 0$ en $\mathbb{Q}_p$.

Caso 2: $m = 1, n = 0$. Esto se reduce a probar la igualdad $(pu, v) = \left(\frac{v}{p}\right)$. Como ya sabemos que se cumple $(u, v) = 1$ (caso anterior), por la Proposición 5.4 de [2] se tiene $(pu, v) = (p, v)$. Si v es un cuadrado, es inmediata la igualdad $(p, v) = 1 = \left(\frac{v}{p}\right)$. Por el contrario, si v no es un cuadrado, se tiene $\left(\frac{v}{p}\right) = -1$. Así, de existir una solución para la ecuación $z^2 - px^2 - vy^2 = 0$ es claro que z o y deben ser múltiplos de p, por lo que es imposible que ambas variables sean unidades p-ádicas. El Lema 3.2 nos permite concluir que no existe una solución no trivial de $z^2 - px^2 - vy^2 = 0$, motivo por el cual se tiene $(p, v) = -1$ por definición.

Caso 3: $m = 0, n = 1$. Esto es idéntico al caso 2.

Caso 4: $m = 1, n = 1$. Ahora se debe probar $(pu, pv) = (-1)^{\epsilon(p)} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Por la Proposición 5.1 de [2] se tiene $(-pu, pu) = 1$ y por la Proposición 5.4 de [2], parte 1, se satisface también

$$(pv, pu) = (-pv \cdot pu, pu) = (-p^2uv, pu) = (-uv, pu).$$

De acá, por el caso 2, se tiene $(pu, -uv) = \left(\frac{-uv}{p}\right)$. Como ya se probó que el símbolo de Legendre es multiplicativo y que se cumple $\left(\frac{-1}{p}\right) = -1^{\epsilon(p)}$, se tiene lo pedido.

Ahora probaremos el teorema para $p = 2$. Se repiten los mismos subcasos de antes.

Caso 1: $m = n = 0$. Debemos probar que se cumple $(u, v) = (-1)^{\epsilon(u)\epsilon(v)}$. Es claro que se satisface $(-1)^{\epsilon(u)\epsilon(v)} = -1$ única y exclusivamente si se tiene $\epsilon(u) = \epsilon(v) = 1$; por ende, se desprenden dos casos. Supongamos primero que se tiene $u \equiv 1$ (mód 4) de modo que $\epsilon(u) = 0$. Esto se desdobla en dos subcasos: o bien $u \equiv 1$ (mód 8) o en su defecto $u \equiv 5$ (mód 8). En la primera vertiente, todo u que satisface $u \equiv 1$ (mód 8) resulta ser un cuadrado perfecto en $\mathbb{Q}_2$ y se tiene $(u, v) = 1$ de manera automática. En la segunda opción se tiene $u \equiv 5$ (mód 8). Como se cumple o bien $v \equiv 1$ (mód 4) o en su defecto $v \equiv 3$ (mód 4) se obtiene siempre $4v \equiv 4$ (mód 8). Entonces, es inmediato que se cumple $u + 4v \equiv 1$ (mód 8), por lo que este valor resulta ser un cuadrado perfecto. Luego, como se tiene $u + 4v = a^2$ para cierto $a \in \mathbb{Q}_2^*$, resulta que el vector $(a, 1, 2)$ es una solución no trivial de $z^2 - ux^2 - vy^2 = 0$. Así se consigue $(u, v) = 1$ y queda liquidado el primer caso pues $v \equiv 1$ (mód 4) implica lo mismo. Ahora supongamos $u \equiv v \equiv 3$ (mód 4), la única posibilidad para tener $\epsilon(u) = \epsilon(v) = 1$. Suponemos que se cumple $(u, v) = 1$, es decir, existe una solución para $z^2 - ux^2 - vy^2 = 0$. Dado esto, la Proposición 6.1 de [2] afirma que existe una terna (z, x, y), con $z, x, y \in \mathbb{Z}_2$, donde algún término es una unidad 2-ádica, de tal forma que resulta ser solución para $z^2 - ux^2 - vy^2 = 0$. Luego, como se tiene $u \equiv v \equiv -1$ (mód 4) es claro que se cumple $z^2 + y^2 + x^2 \equiv 0$ (mód 4). Recordemos que módulo 4 los cuadrados son solo 1 y 0. De esta manera se tiene $z \equiv y \equiv x \equiv 0$ (mód 2), lo cual es absurdo puesto que alguno de esos valores tiene que ser unidad 2-ádica. Como la contradicción nace de suponer $(u, v) = 1$, se tiene obligadamente $(u, v) = -1$ y queda confirmada la aseveración.

Caso 2: $m = 1, n = 0$. Aquí debemos probar $(2u, v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. El primer paso será establecer la igualdad $(2, v) = (-1)^{\omega(v)}$. Supongamos se cumpla $(2, v) = 1$, es decir, aceptemos que la ecuación $z^2 - 2x^2 - vy^2 = 0$ admite una solución no trivial en $\mathbb{Q}_2$. Así, el Lema 3.2 asegura que existe una solución (z_0, x_0, y_0) con z_0 e y_0 unidades 2-ádicas y x_0 entero 2-ádico. Ya fue probado en [2] el hecho de que todas las unidades que

son cuadrados perfectos en $\mathbb{Q}_2$ son congruentes a 1 módulo 8. Con esto se cumple $y^2 = z^2 \equiv 1$ (mód 8) y así se llega a $1 - 2x^2 - v \equiv 0$ (mód 8). Es claro que todo cuadrado perfecto módulo 8 cumple $x^2 \equiv \{0, 1, 4\}$ (mód 8). De esta forma se obtiene $v \equiv \pm 1$ (mód 8), es decir $\omega(v) = 0$. Recíprocamente, para $v \equiv \pm 1$ (mód 8) abordamos dos casos. Si $v \equiv 1$ (mód 8), éste resulta cuadrado perfecto y se verifica inmediatamente la igualdad $(2, v) = 1$. Por el contrario, si $v \equiv -1$ (mód 8), reemplazamos este valor en la ecuación $z^2 - 2x^2 - vy^2 = 0$ y logramos $z^2 - 2x^2 + y^2 \equiv 0$ (mód 8). Es claro que la terna $(1, 1, 1)$ es una solución no trivial de esta ecuación. Así, el Corolario 1.7 asegura la existencia de una solución para $z^2 - 2x^2 - vy^2 = 0$ y de esta forma se satisface nuevamente $(2, v) = 1$. Con esto hemos probado que $(2, v) = 1$ equivale a $v \equiv \pm 1$ (mód 8), o lo que es lo mismo a $(2, v) = (-1)^{\omega(v)}$.

El siguiente paso será probar que se cumple $(2u, v) = (2, v)(u, v)$. Si $(2, v) = 1$ o $(u, v) = 1$, esto resulta inmediato de la Proposición 5.4 de [2]. Ahora supongamos que se tiene $(2, v) = (u, v) = -1$. Por lo anterior se cumple $v \equiv \pm 5$ (mód 8) o de manera equivalente $v \equiv 5$ ó 3 (mód 8). Además, por el Caso 1 se tiene $u \equiv v \equiv -1$ (mód 4) o de manera equivalente $u \equiv v \equiv 3$ ó -1 (mód 8). De esta forma se tiene $v \equiv 3$ y $u \equiv 3$ ó -1 (mód 8). Verificamos cada una de las opciones. Si $v \equiv 3$ (mód 8) y $u \equiv -1$ (mód 8), la ecuación $z^2 + 2x^2 - 3y^2 \equiv 0$ (mód 8) tiene como solución $(1, 1, 1)$. Por otro lado, si $v \equiv -5$ (mód 8) y $u \equiv 3$ (mód 8), la ecuación $z^2 - 6x^2 + 5y^2 \equiv 0$ (mód 8) también tiene como solución $(1, 1, 1)$. Por el Corolario 1.7 se concluye que la ecuación $z^2 - 2ux^2 - vy^2 = 0$ admite solución; por consiguiente, se cumple $(2u, v) = 1$.

Caso 3: $m = 1, n = 0$. Esto es idéntico al caso 2.

Caso 4: $m = 1, n = 1$. Acá se debe probar $(2u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$. Por la Proposición 5.4 de [2] se tiene $(2u, -2u) = 1$, y por lo tanto, en uso reiterado de la Proposición 5.4, se satisface también

$$\begin{aligned}(2u, 2v) &= (-2u \cdot 2v, 2u) \\ &= (2u, -4uv) \\ &= (2u, -uv) \\ &= (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}.\end{aligned}$$

Luego, como ϵ es homomorfismo, se tiene $\epsilon(-uv) = \epsilon(-1)+\epsilon(u)+\epsilon(v)$. Es claro que se cumple $\epsilon(-1) = 1$. Es más, si $\epsilon(u) = 1$, entonces se satisface $\epsilon(u)(1 + \epsilon(u)) = 1 \cdot 0 = 0$, mientras si $\epsilon(u) = 0$, se logra $\epsilon(u)(1 + \epsilon(u)) = 0(1 + 0) = 0$. De esta forma se consigue

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

Ahora, ω también es homomorfismo y por lo tanto se cumple $\omega(-uv) = \omega(-1) + \omega(u) + \omega(v)$. Es evidente que se tiene $\omega(-1) = 0$, por lo que concluimos la igualdad

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

□

Observación 3.3. Si algún $a, b \in \mathbb{Q}_p^*$ resulta ser unidad p-ádica, las fórmulas del Teorema 3.1 se simplifican drásticamente. Es más, si ambos números son unidades p-ádicas se tiene

$$(a, b) = \begin{cases} 1 & \text{si } p > 2 \\ (-1)^{\epsilon(a)\epsilon(b)} & \text{si } p = 2. \end{cases}$$

Teorema 3.4 (bimultiplicidad del símbolo de Hilbert). *Sea $K = \mathbb{Q}_p$ con $p = 2, 3, \cdots, \infty$. Para $a, b, a' \in K^*$ se cumple $(aa', b) = (a, b)(a', b)$.*

Prueba. En el caso $p = \infty$, hay 5 posibilidades.

Caso 1: $b > 0$: como b es positivo se tiene $(aa', b) = 1$, $(a', b) = 1$, $(a, b) = 1$.

Caso 2: $b < 0$ y $a', a > 0$: se tiene $(aa', b) = 1$, $(a', b) = 1$, $(a, b) = 1$.

Caso 3: $a, b < 0$ y $a' > 0$: se tiene $(aa', b) = -1$, $(a', b) = 1$, $(a, b) = -1$.

Caso 4: $a', b < 0$ y $a > 0$: se tiene $(aa', b) = -1$, $(a', b) = -1$, $(a, b) = 1$.

Caso 5: $a, a', b < 0$: se tiene $(aa', b) = 1$, $(a', b) = -1$, $(a, b) = -1$.

Ahora, si p es un primo numérico basta trabajar con las fórmulas ya probadas en el Teorema 3.1. Ponemos $a = p^n u$, $a' = p^m u'$ y $b = p^s v$. Si $p = 2$ se tiene

$$\begin{aligned}(aa', b) &= (-1)^{\epsilon(uu')\epsilon(v)+(n+m)\omega(v)+s\omega(u+u')} \\ &= (-1)^{\epsilon(u)\epsilon(v)+\epsilon(u')\epsilon(v)+n\omega(v)+m\omega(v)+s\omega(u)+s\omega(u')} \\ &= (-1)^{\epsilon(u)\epsilon(v)+n\omega(v)+s\omega(u)+\epsilon(u')\epsilon(v)+m\omega(v)+s\omega(u')} \\ &= (-1)^{\epsilon(u)\epsilon(v)+n\omega(v)+s\omega(u)}(-1)^{\epsilon(u')\epsilon(v)+m\omega(v)+s\omega(u')} \\ &= (a, b)(a', b).\end{aligned}$$

Mientras que si p es impar se consigue

$$\begin{aligned}(aa', b) &= (-1)^{(n+m)\epsilon(p)} \left(\frac{uu'}{p}\right)^s \left(\frac{v}{p}\right)^{n+m} \\ &= (-1)^{(n\epsilon(p)+m\epsilon(p))} \left(\frac{u}{p}\right)^s \left(\frac{u'}{p}\right)^s \left(\frac{v}{p}\right)^n \left(\frac{v}{p}\right)^m \\ &= (-1)^{n\epsilon(p)}(-1)^{m\epsilon(p)} \left(\frac{u}{p}\right)^s \left(\frac{v}{p}\right)^n \left(\frac{u'}{p}\right)^s \left(\frac{v}{p}\right)^m \\ &= (-1)^{n\epsilon(p)} \left(\frac{u}{p}\right)^s \left(\frac{v}{p}\right)^n (-1)^{m\epsilon(p)} \left(\frac{u'}{p}\right)^s \left(\frac{v}{p}\right)^m \\ &= (a, b)(a', b).\end{aligned}$$

□

Proposición 3.5. *Dado $c \in \mathbb{Q}_p^*$ con $c \notin \mathbb{Q}_p^{*2}$, existe $b \in \mathbb{Q}_p^*$ que satisface $(b, c) = -1$.*

Prueba. Si $p = \infty$ la hipótesis $c \notin \mathbb{Q}_p^{*2}$ es equivalente a $c < 0$; en este caso es claro que la forma $x^2 - cy^2 + z^2$ no representa a cero. Es decir, se tiene $(c, -1) = -1$.

Si $p > 2$ ponemos $c = p^n u$. Como c no es cuadrado, o bien n es impar o bien se tiene $\left(\frac{u}{p}\right) = -1$. Si n es impar, por el Teorema 3.1 se tiene $(v, c) = \left(\frac{v}{p}\right)$, para v unidad p-ádica; entonces basta elegir v de tal forma que se tenga $\left(\frac{v}{p}\right) = -1$ y hacemos $b = v$. Si n es par se tiene de inmediato $\left(\frac{u}{p}\right) = -1$; basta elegir $b = p$ para que se cumpla $(p, u) = \left(\frac{u}{p}\right) = -1$.

Si $p = 2$ ponemos $c = 2^n u$. De nuevo, como c no es cuadrado o bien n es impar o en su defecto u no es un cuadrado de $\mathbb{Q}_2^*$, es decir u no es congruente a 1 módulo 8. Si n es impar, por el Teorema 3.1 se tiene $(5, 2 \cdot u) = -1^{\epsilon(u)\epsilon(5)+\omega(5)}$. Y como se cumple $\epsilon(5) = 0$ y $\omega(5) = 1$, se logra $(5, 2 \cdot u) = -1$. Basta elegir $b = 5$. Si n es par se tiene de inmediato que u no es congruente a 1 módulo 8. Si $u \equiv 3$ ó 5 (mód 8) se tiene $\omega(u) = 1$ y por el Teorema 3.1 se cumple $(2, u) = -1^{\epsilon(1)\epsilon(u)+\omega(u)} = -1$. Si $u \equiv 7$ (mód 8) queda claro que se tiene $\epsilon(u) = 1$. Como se cumple $\epsilon(-1) = 1$ y u es unidad 2-ádica, se obtiene $(-1, u) = -1^{\epsilon(-1)\epsilon(u)} = -1$. Acá basta hacer $b = -1$. □

La proposición anterior es equivalente a la siguiente expresión: *si existe $b \in \mathbb{Q}_p^*$ que cumple $(a, b) = 1$ para todo $a \in \mathbb{Q}_p^*$, entonces b es cuadrado perfecto*. Si hablamos en términos del grupo cociente $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, esto significa $b = [1]$.

En [2] se definió el símbolo de Hilbert como una aplicación $(\ ,\ ) : \mathbb{Q}_p^* \times \mathbb{Q}_p^* \to \{\pm 1\}$ con $p = 2, 3, \cdots, \infty$. Sin embargo, dado que aparece invarianza por múltiplicación de cuadrados en los argumentos de la función, ésta se puede redefinir como $(\ ,\ ) : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \times \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \{\pm 1\}$. La ventaja de esta presentación radica en el hecho de que $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ es un grupo finito respecto a la multiplicación (ver Proposición 3.3 de [2]). De esta observación se desprende un resultado que nos será de utilidad. Antes de presentar su demostración haremos unas precisiones.

Lema 3.6. *Para $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ distinto de 1, la aplicación $h_a : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \to \{\pm 1\}$ definida por*

$$h_a(x) = (a, x)$$

es un homomorfismo cuyo nucleo tiene tantos elementos como la mitad de la cardinalidad del grupo $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Prueba. Esto es obvio por la bimultiplicidad del símbolo de Hilbert y el hecho de que los grupos $(\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})/Nu(h_a)$ y $\{\pm 1\}$ son isomorfos (como consecuencia directa de la Proposición 3.5). □

Observación 3.7 Si nos limitamos a los primos numéricos $p = 2, 3, \cdots$, la Proposición 3.3 de [2] afirma que la cardinalidad de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ es igual a 8 si $p = 2$ e igual a 4 si p es impar. De esta manera, el nucleo de h_a tiene cardinalidad 2 si $p \neq 2$ y 4 si $p = 2$. Con esto se puede concluir que para $p \neq 2$ hay 2 valores de $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ que resuelven la ecuación $(x, a) = 1$. Evidentemente, el mismo número de valores de x satisfacen la ecuación $(x, a) = -1$. Si $p = 2$, serán 4 los valores de x que satisfagan la relación anterior. Por comodidad vamos a llamar s_p a la cardinalidad del grupo cociente $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ con p primo racional. De esta forma, si $a \neq 1$, hay $s_p/2$ elementos de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ que resuelven la ecuación $(a, x) = 1$. Los $s_p/2$ elementos restantes son los que resuelven $(a, x) = -1$.

Por último cabe notar que no hemos comentado el caso $a = 1$. Acá es trivial verificar que todos los $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ son solución de la ecuación $(1, x) = 1$ (es decir, $(1, x) = 1$ admite s_p soluciones). En revancha, la ecuación $(x, 1) = -1$ no admite solución.

Proposición 3.8. *Sean* $a_i, b_i, c_i \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, *con* $i = 1, 2$, *donde* p *es un primo racional. Consideramos las ecuaciones*

$$(x, a_1) = (b_1, c_1),$$

$$(x, a_2) = (b_2, c_2).$$

Sean M *y* N *el conjunto de los valores en* $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ *que resuelven la primera y segunda ecuación, respectivamente. Si* M *y* N *son no vacíos, entonces se tiene* $M \cap N = \emptyset$ *si y solo si* $a_1 \equiv a_2$ *y* $(b_1, c_1) = -(b_2, c_2)$ *(esto equivale a decir que ambas ecuaciones son contradictorias).*

Prueba. El regreso es trivial. Si se tiene $a_1 \equiv a_2$ y $(b_1, c_1) = -(b_2, c_2)$, es claro que se cumple $M \cap N = \emptyset$.

Ahora suponemos se tenga $M \cap N = \emptyset$. La estrategia consiste en ir descartando posibles valores de a_i y (b_i, c_i) utilizando reducción al absurdo. Empezamos probando que, dadas las características del problema, se cumple $a_i \neq 1$ para $i = 1, 2$. Supongamos sin pérdida de generalidad que se tenga $a_1 = 1$. Entonces, o bien todos los elementos de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ son solución de $(x, 1) = (b_1, c_1)$ o bien $(x, 1) = (b_1, c_1)$ no admite solución. Si se tiene lo primero se logra $x \in M \cap N$ pues N es no vacío. Si se tiene lo segundo, entonces M es vacío. De cualquier forma se llega a una contradicción. A continuación, si se tiene $(b_1, c_1) = (b_2, c_2) = 1$ es claro que se satisface $1 \in M \cap N$ lo cual es una contradicción. Si se tiene $(b_1, c_1) = (b_2, c_2) = -1$ es claro por la Observación 3.7 que tanto M como N poseen $s_p/2$ elementos, todos ellos distintos de 1. De esto último se concluye $M \cap N \neq \emptyset$, lo cual de nuevo es una contradicción. Así, necesariamente se debe cumplir $(b_1, c_1) = -(b_2, c_2)$. Con ello, el sistema de ecuaciones queda cual

$$(x, a_1) = 1,$$

$$(x, a_2) = -1.$$

Ahora, si $M \cap N = \emptyset$ entonces para todo x se tendrá $(x, a_1) = 1$, $(x, a_2) = 1$ o en su defecto $(x, a_1) = -1$, $(x, a_2) = -1$. De cualquier forma se tendrá siempre $(x, a_1 a_2) = 1$ para todo x. Según la Observación 3.7, esto solo es posible con $[a_1 a_2] = 1$, es decir con $[a_1] = [a_2]$. □

Capítulo 4

Aspectos topológicos de $\mathbb{Q}_p$

Recordemos que $\mathbb{R}$ y $\mathbb{Q}_p$ son compleciones de $\mathbb{Q}$. Ello los convierte en espacios topológicos localmente compactos respecto a alguna topología no discreta. En el caso de $\mathbb{R}$, ésta resulta ser la topología métrica inducida por la distancia euclidiana usual, mientras que para $\mathbb{Q}_p$, la métrica está dada por la norma p-ádica. Por definición $\mathbb{Q}$ siempre es denso en $\mathbb{Q}_p$. Es más, la Proposición 3.1 de [2] asegura que todo entero p-ádico es límite de una sucesión de Cauchy de enteros, por lo que $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. En este capítulo exhibiremos otras propiedades topológicas de subconjuntos de $\mathbb{Q}_p$.

Describamos los abiertos de $\mathbb{Q}_p$. Sea $a \in \mathbb{Q}_p$ y $\epsilon > 0$. La **bola abierta centrada en** a **de radio** ϵ es el conjunto $B_a(x, \epsilon) = \{x, |x - a|_p < \epsilon\}$. Como siempre, un conjunto $U \subset \mathbb{Q}_p$ es **abierto** si para todo $a \in U$ existe δ que cumple $B_a(x, \delta) \subset U$.

Proposición 4.1. *El anillo $\mathbb{Z}_p$ es abierto en $\mathbb{Q}_p$.*

Prueba. Dado $a \in \mathbb{Z}_p$ y $x \in B(a, 1)$ se tiene $|a| \leq 1$ y $|x - a| < 1$, con ello se logra $|x| \leq \text{máx}\,\{|a|, |x - a|\} \leq 1$. Es decir se tiene $x \in \mathbb{Z}_p$. □

Teorema 4.2. *El grupo $\mathbb{Q}_p^{*2}$ es abierto en $\mathbb{Q}_p^*$.*

Prueba. Primero tratemos el caso $p = 2$. Si $a = 2^n u \in \mathbb{Q}_2^{*2}$ es claro que n es par y $u \equiv 1$ (mód 8). Si $x \in B(a, 1/2^{n+3})$, por la desigualdad ultramétrica se tiene $|x|_2 = 2^{-n}$ pues se satisface $|x - a|_2 = 1/2^{n+3} < 1/2^n = |a|_2$. Luego, al poner $x = 2^n v$ se tendrá $|u - v|_2 < 1/2^3$. Así, al tenerse $u \equiv 1$ (mód 8) se cumple también $v \equiv 1$ (mód 8) y es posible extraerle raíz cuadrada a x.

Sea ahora $p > 2$. Si $a = p^n u \in \mathbb{Q}_p^{*2}$, resulta que n es par y se tiene $u \equiv a^2$ (mód p) con $a \in \mathbb{Z}$. Sea $x \in B(a, 1/p^{n+1})$, si ponemos $y = x - a = p^{n+1}v$, se tiene $x = p^n(u + vp)$. Con ello se cumple $u + vp \equiv a^2$ (mód p) y se logra $x \in \mathbb{Q}_p^{*2}$. □

Corolario 4.3. *Para todo $x_p \in \mathbb{Q}_p^*$, el conjunto $x_p\mathbb{Q}_p^{*2}$ es abierto en $\mathbb{Q}_p^*$.*

Prueba. Como $\mathbb{Q}_p^{*2}$ es abierto y multiplicar por $x_p \in \mathbb{Q}_p^*$ es un homeomorfismo reversible, resulta que $x_p\mathbb{Q}_p^{*2}$ es abierto. □

Como ya se dijo, $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, para $p = 2, 3, \cdots, \infty$. Probaremos que también resulta ser denso en el producto cartesiano de un número finito de estos $\mathbb{Q}_p$. Antes, un lema preparatorio.

Lema 4.4. *Dado $m > 1$, el conjunto $Q = \{\frac{z}{m^l} : z \in \mathbb{Z} \text{ y } l \in \mathbb{N}\}$ es denso en $\mathbb{R}$.*

Prueba. Esto es equivalente a que dados $a, b \in \mathbb{R}$ exista $q \in Q$ sujeto a $a < q < b$. Para ello multiplicamos a, b por un m^l lo suficientemente grande como para asegurar la desigualdad $(a - b)m^l > 1$. De este modo existe $c \in \mathbb{Z}$ que cumple $am^l < c < bm^l$. Es evidente entonces que se satisface $a < c/m^l < b$. □

Teorema 4.5 (Teorema de aproximación débil). *Sea P un subconjunto finito de $\{2, 3, \cdots, \infty\}$. Entonces $\mathbb{Q}$ es denso en $\prod_{p\in P} \mathbb{Q}_p$ (con la topología producto, donde la incrustación es diagonal).*

Prueba. Antes que todo pongamos las cosas en perspectiva. Lo que se pide probar es que para todo $\widetilde{x} = (x_{p_1}, x_{p_2}, \cdots, x_{p_n}) \in \prod_{p_i\in P} \mathbb{Q}_{p_i}$ y $\epsilon > 0$ existe $x \in \mathbb{Q}$ que para todo p_i cumple simultáneamente

$$|x - x_{p_i}|_{p_i} < \epsilon.$$

Sin perdida de generalidad podemos suponer la inclusión $\infty \in P$ a fin de tener $\widetilde{x} = (x_\infty, x_{p_1}, x_{p_2}, \cdots, x_{p_n})$. También se puede asumir $x_{p_i} \in \mathbb{Z}_{p_i}$ tras multiplicar por un número entero adecuadamente elegido a fin de limpiar denominadores. Sea $\epsilon > 0$ y k un entero positivo que cumple $1/p_i^k < \epsilon$ para todo $p_i \in P - \{\infty\}$. Llamamos $a_i \in \mathbb{Z}$ a la reducción módulo p_i^k de x_{p_i}. En tal caso, el teorema del resto chino asegura la existencia de $a \in \mathbb{Z}$ que cumple $a \equiv a_i \pmod{p_i^k}$. Por ende se tiene también $a \equiv x_{p_i} \pmod{p_i^k}$

y con ello $|a - x_{p_i}|_{p_i} \leq 1/p_i^k < \epsilon$. Si hacemos $x = a$ se tiene lo pedido para los valores x_{p_i}. Falta asegurar que esto también puede forzarse para x_∞. Sea $p > 2$ primo con $p \notin P$. Por el Lema 4.4 existe un racional de la forma $r = b/p^l$, con $b \in \mathbb{Z}$ y $l \in \mathbb{N}$, que pertenece al intervalo abierto

$$\left(\frac{x_\infty - \epsilon - a}{p_1^k \cdots p_n^k}, \frac{x_\infty + \epsilon - a}{p_1^k \cdots p_n^k} \right).$$

De este modo se tiene

$$x_\infty - \epsilon < a + r p_1^k \cdots p_n^k < x_\infty + \epsilon,$$

o equivalentemente

$$|a + r p_1^k \cdots p_n^k - x_\infty| < \epsilon.$$

Con estos arreglos, el número racional $s = a + r p_1^k \cdots p_n^k$ cumple $|s - x_\infty|_\infty < \epsilon$. Queda comprobar que este nuevo número cumple también $|s - x_{p_i}|_{p_i} < \epsilon$. Y en efecto, del hecho de que se tiene

$$|s - x_{p_i}|_{p_i} \leq \text{máx} \{|a - x_{p_i}|_{p_i}, |r p_1^k \cdots p_n^k|_{p_i}\} \leq 1/p_i^k < \epsilon,$$

se deduce lo pedido. □

Capítulo 5

Propiedades globales del símbolo de Hilbert

En el Capítulo 3 establecimos fórmulas para tabular el símbolo de Hilbert de un par de números p-ádicos con $p = 2, 3, \cdots, \infty$. No hicimos mención a $\mathbb{Q}$ por el simple hecho de que éste resulta ser un subcuerpo de $\mathbb{Q}_p$ en todos los casos. Sin embargo, cabe recordar que $a \in \mathbb{Q}^*$ tiene una representación distinta en cada uno de los $\mathbb{Q}_p$ (ver Capítulos 2 y 3 de [2]). En consecuencia, para el cálculo del símbolo de Hilbert de dos racionales no nulos, debemos expresar ambos números como expansiones p-ádicas para luego aplicar las fórmulas que ya estudiamos. Para $a, b \in \mathbb{Q}^*$, se denota por $(a, b)_p$ al símbolo de Hilbert de las expansiones p-ádicas de a y b. En este capítulo nos concentraremos en importantes propiedades que giran en torno al símbolo de Hilbert de dos números racionales.

Empezamos probando la conocida fórmula producto de Hilbert. Antes una observación.

Observación 5.1 Dados $a, b \in \mathbb{Q}$, existen $c, d \in \mathbb{Z}$ que cumplen $m = ac^2, n = bd^2 \in \mathbb{Z}$. Por las propiedades del símbolo de Hilbert se cumple $(a, b)_p = (m, n)_p$. Es más, podemos descomponer m y n en factores primos cual $m = (-1)^r m_1 \cdots m_k$ y $n = (-1)^s n_1 \cdots n_l$. Por la bimultiplicidad del símbolo de Hilbert se tiene entonces

$$(a, b)_p = \prod_{\substack{i=1,\cdots,k \\ j=1,\cdots,l}} (a_i, b_j)_p \prod_{i=1,\cdots,k} (a_i, (-1)^s)_p \prod_{j=1,\cdots,l} ((-1)^r, b_j)_p ((-1)^r, (-1)^s)_p$$

Para s o r pares los productos $\prod_{i=1,\cdots,k} (a_i, (-1)^s)_p$, $\prod_{j=1,\cdots,l} ((-1)^r, b_j)_p$ y $((-1)^r, (-1)^s)_p$ son trivialmente iguales a 1. De esta manera el cálculo de $(a, b)_p$ se reduce a analizar símbolos de Hilbert del tipo $(q, t)_p$, donde q, t son iguales a un primo o a -1.

Teorema 5.2 (Fórmula producto). *Dados $a, b \in \mathbb{Q}^*$ se cumple $(a, b)_p = 1$ para casi todos los $p = 2, 3, \cdots, \infty$, además de $\prod_{p=2,3,\cdots,\infty} (a, b)_p = 1$.*

Prueba. Por la observación anterior solo es necesario analizar la situación cuando a, b sean primos o iguales a -1.

Caso 1: $a = b = -1$. Es claro que se tiene $(a, b)_\infty = -1$. Si $p = 2$ se cumple $-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 \cdots$ con lo que se tiene $-1 \equiv 3$ (mód 4) y $-1 \equiv 7$ (mód 8). Por ende se consigue

$$(-1, -1)_2 = (-1)^{\epsilon(-1)\epsilon(-1)+0\omega(-1)+0\omega(-1)} = (-1)^1 = -1.$$

Si $p > 2$ se tiene que $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$ es unidad p-ádica. De nuevo, por la Observación 3.3 es obvia la igualdad $(-1, -1)_p = 1$. De aquí es evidente que se cumple

$$\prod_{p=2,3,\cdots\infty} (-1, -1)_p = (-1, -1)_2(-1, -1)_\infty \prod_{p=3,5,\cdots} (-1, -1)_p = -1 \cdot -1 \cdot 1 = 1.$$

Caso 2: $a = -1$ *y* $b = 2$. Este caso es trivial pues la terna $(1, 1, 1)$ siempre resuelve $x^2 + y^2 - 2z^2 = 0$.

Caso 3: $a = -1$ *y* $b = q$ *con* $q \neq 2$. Si $p = \infty$ es que obvio que se tiene $(-1, q)_\infty = 1$ pues q es positivo. Si $p = 2$ se tiene que q es unidad 2-ádica, por ende se cumple

$$(-1, q)_2 = (-1)^{\epsilon(-1)\epsilon(q)} = (-1)^{\epsilon(q)}.$$

Si $p \neq q, 2$ resulta que q es unidad p-ádica y se tiene $(-1, q)_p = 1$. Si $p = q$ se tiene $(-1, q)_q = \left(\dfrac{-1}{q}\right) = (-1)^{\epsilon(q)}$. Ahora resulta evidente que el producto $\prod_{p=2,3,\cdots,\infty} (a, b)_p$ es igual a 1.

Caso 4: $a = s$ *y* $b = r$ *con* s, r *primos.* Si $p = \infty$ es obvio que se tiene $(s, r)_\infty = 1$. Si $p = 2$ tenemos cuatro casos posibles. Si $s = r = 2$ se tiene

$$(2, 2)_2 = (-1)^{\epsilon(1)\epsilon(1)+\omega(1)+\omega(1)} = (-1)^0 = 1.$$

Si $s = 2$ y $r \neq 2$ se tiene

$$(2,r)_2 = (-1)^{\epsilon(1)\epsilon(r)+\omega(r)+0\omega(1)} = (-1)^{\omega(r)}.$$

Así también, si $r = 2$ y $s \neq 2$ se cumple igualmente $(s,2)_2 = (-1)^{\omega(s)}$. Por último, si $s, r \neq 2$ resulta que ambos son unidades p-ádicas y por ende se tiene

$$(s,r)_2 = (-1)^{\epsilon(s)\epsilon(r)}.$$

Si $p > 2$ tenemos diez casos a tratar. Si $s = r = 2$ resulta que ambos son unidades p-ádicas y por ende se tiene $(2,2)_p = 1$. Si $s = 2$ y $r \neq 2, p$, también es claro que éstas son unidades p-ádicas y así tenemos $(2,r)_p = 1$. Si $s = 2$ y $r = p$ se tiene

$$(2,r)_r = (-1)^{1\cdot 0\cdot \epsilon(r)} \left(\frac{2}{r}\right)^1 \left(\frac{1}{r}\right)^0 = \left(\frac{2}{r}\right).$$

Luego, por el Ejemplo 2.3, sabemos que se cumple $(2,r)_r = (-1)^{\omega(r)}$. Si $r = 2$ y $s \neq 2, p$, ambos son unidades y se cumple $(s,2)_p = 1$. Si $r = 2$ y $s = p$, por lo ya visto antes, se tiene $(s,2)_s = (-1)^{\omega(s)}$. Si $s = r \neq 2, p$, ambos son unidades p-ádicas y por ende $(s,r)_p = 1$. Si $s = r = p$ se tiene

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

Si $s \neq r = p$ se tiene que s es unidad p-ádica y por ende cumple

$$(s,r)_r = \left(\frac{s}{r}\right).$$

De igual forma, si $r \neq s = p$ se cumple $(s,r)_s = \left(\frac{r}{s}\right)$. Por último si $s, r \neq p, 2$, ambos son unidades y se cumple $(s,r)_p = 1$. Es claro que el producto queda cual

$$\prod_{p=2,3,\cdots\infty}(a,b)_p = (-1)^{\omega(r)}(-1)^{\omega(s)}(-1)^{\epsilon(s)\epsilon(r)}(-1)^{\omega(r)}(-1)^{\omega(s)}\left(\frac{r}{s}\right)\left(\frac{s}{r}\right)$$
$$= (-1)^{\epsilon(s)\epsilon(r)}\left(\frac{r}{s}\right)\left(\frac{s}{r}\right).$$

Finalmente, por ley de reciprocidad cuadrática se cumple $\left(\frac{r}{s}\right)\left(\frac{s}{r}\right) = (-1)^{\epsilon(s)\epsilon(r)}$ y en consecuencia se tiene $\prod_{p=2,3,\cdots,\infty}(a,b)_p = 1$. □

Si bien hasta ahora hemos resuelto el problema de hallar el símbolo de Hilbert de dos números, es posible plantear un problema novedoso: resolver la "ecuación" $(a,x)_p = (-1)^s$ con p primo, $x, a \in \mathbb{Q}^*$ y $s \in \mathbb{Z}/2\mathbb{Z}$. Ilustramos con un ejemplo.

Ejemplo 5.3. Hallaremos x que resuelva la ecuación $(250,x)_5 = -1$. Ponemos $x = 5^m l$, con l unidad 5-ádica. Como se tiene $250 = 2 \cdot 5^3$, $\omega(5) = 1$ y $\epsilon(5) = 0$, usamos la fórmula del Teorema 3.1 para obtener

$$(250,x)_5 = (-1)^{3m\epsilon(5)}\left(\frac{2}{5}\right)^m\left(\frac{l}{5}\right)^3$$
$$= (-1)^{m\omega(5)}\left(\frac{l}{5}\right)$$
$$= (-1)^m\left(\frac{l}{5}\right).$$

De esta manera, con $m = 1$ y $l = 1$, se resuelve la ecuación. Es obvio que $x = 5$ puede ser elegido.

Sin embargo, es posible encontrar otros x que resuelvan la ecuación planteada en el ejemplo anterior. Surge entonces otra interrogante: dado un "sistema" de ecuaciones, ¿será posible encontrar al menos un x que lo resuelva? Vamos a ilustrar la situación con dos ejemplos.

Ejemplo 5.4 (un "sistema" de ecuaciones). Vamos a hallar x que resuelva el sistema

$$(8,x)_3 = -1$$
$$(15,x)_5 = 1.$$

Es claro que se cumple $(8,x)_3 = (2,x)_3$. Ponemos $x = 3^m v$ con v unidad 3-ádica. Al ser 2 una unidad 3-ádica se tiene

$$(2,x)_3 = (2,3^m v) = \left(\frac{2}{3}\right)^m.$$

Y como se cumple $\left(\frac{2}{3}\right) = (-1)^{\omega(3)} = -1$, tenemos $(2,x)_3 = (-1)^m$. Vemos que basta con elegir m impar para resolver la ecuación. Ahora, ponemos $x = 5^n l$ con l unidad 5-ádica. Como se cumple $\epsilon(5) = 0$, se tiene

$$(15,x)_5 = (5\cdot 3, 5^n l) = \left(\frac{3}{5}\right)^n \left(\frac{l}{5}\right).$$

Puesto que 3 no es residuo cuadrático módulo 5, resulta

$$(15,x)_7 = (-1)^n \left(\frac{l}{5}\right).$$

En resumen, vemos que basta con tener n impar y que l no sea residuo cuadrático módulo 5 para poder resolver la ecuación. Por ejemplo $x = 60 = 4\cdot 3\cdot 5$ resuelve el sistema pues $12 \equiv 2$ (mód 5) no es residuo cuadrático módulo 5.

Ejemplo 5.5 (una ecuación que barre los primos). Busquemos un x que resuelva la ecuación $(p-1,x)_p = 1$ para $p = 2,3,\cdots$. Esto lógicamente representa un conjunto infinito de ecuaciones (pero que está en concordancia con el Teorema 5.2). El caso $p = 2$ es obvio pues la terna $(1,1,0)$ resuelve la ecuación $a^2 - b^2 - xc^2 = 0$. Si $p > 2$ resulta que $p-1$ es siempre unidad p-ádica, y así basta que x sea unidad p-ádica para todo $p > 2$ (por ejemplo $x = 4$) y quedará liquidado el asunto.

Notemos que se puede reemplazar los valores ± 1 del lado derecho de las ecuaciones por símbolos de Hilbert. La ecuación del ejemplo anterior

pudo escribirse como $(p-1,x)_p = (-1,2)_p$. A continuación presentamos un último ejemplo sobre el particular.

Ejemplo 5.6 (un sistema que barre los primos). Vamos a estudiar el sistema infinito

$$\begin{aligned}(2,x)_p &= (-1,3)_p,\\ (1,x)_p &= (3,4)_p,\end{aligned}$$

con $p = 2,3,\cdots,\infty$. Para $(-1,3)_p$ es claro que se tiene $(-1,3)_\infty = 1$, $(-1,3)_2 = (-1,3)_3 = -1$ y $(-1,3)_p = 1$ para $p = 5,7,\cdots$. Si $p=\infty$, es clara la igualdad $(2,x)_\infty = 1$. Si $p = 2$ ponemos $x = 2^m v$ y se tiene

$$(2,x)_2 = (-1)^{\epsilon(1)\epsilon(v)+m\omega(1)+\omega(v)} = -1^{\omega(v)}.$$

Por consiguiente, se necesita tener $v \equiv \pm 5$ (mód 8). Si $p = 3$, resulta que 2 es unidad y si ponemos $x = 3^n u$ se consigue $(2,x)_3 = \left(\frac{2}{3}\right)^n$. Como 2 no es resto cuadrático módulo 3 se tiene de inmediato $(2,x)_3 = (-1)^n$; por lo que se necesita que n sea impar. Si $p = 5,7,\cdots$, resulta de nuevo que 2 es unidad p-ádica y al poner $x = p^{n_p} w$ tenemos $(2,x)_p = \left(\frac{2}{p}\right)^{n_p}$, por lo que necesitamos n_p par cuando 2 no sea residuo cuadrático módulo p. Por otro lado, es claro que se tiene $(3,4)_p = 1$ pues 4 es cuadrado perfecto. Es obvio también que se tiene $(1,x) = 1$. Así, cualquier x satisface $(1,x)_p = (3,4)_p$. En suma, el valor $x = 3$ (que es unidad p-ádica para $p > 3$) resuelve el sistema.

Vamos a probar un teorema que brinda condiciones bajo las cuales se puede garantizar la existencia de una solución para sistemas como el dado en el Ejemplo 5.6. Previamente enunciamos dos lemas auxiliares y probaremos uno de ellos.

Lema 5.7 (Teorema de Dirichlet sobre primos en series aritméticas). *Sean a, m enteros positivos no nulos y primos entre sí. Entonces, existen infinitos primos p que satisfacen $p \equiv a$ (mód m).*

Prueba. El tratar de probar este resultado elemental nos apartaría de las metas establecidas. El lector interesado puede consultar Apostol [1], Serre [7] o la tesis de Jorge Dioses [4] □

Observación 5.8. Para introducir el segundo lema se requiere cierto trabajo preparatorio. Consideramos el sistema $(a_i, x) = (m_i, n_i)$ con $a_i \in \mathbb{Z}^*$, $m_i, n_i \in \mathbb{Q}^*$, $i = 1, 2, \cdots, k$ y $p = 2, 3, \cdots, \infty$. Vale la pena aclarar que este sistema es similar al del Ejemplo 5.6, salvo que en este caso trabajaremos no solo con dos, sino con k ecuaciones. El Teorema 5.2 asegura que se cumple $(m_i, n_i)_p = 1$ para casi todos los $p = 2, 3, \cdots, \infty$. Por consiguiente, hay solo un número finito de primos para los que se satisface $(m_i, n_i) = -1$. En vista de ello, nombramos N al conjunto de primos $p = 2, 3, \cdots, \infty$ que cumplen $(m_i, n_i)_p = -1$ para cierto i. Por otro lado, la Observación 5.1 afirma que el cálculo del símbolo de Hilbert de dos enteros se reduce al análisis en sus divisores primos o -1, por lo que es deseable identificar tales divisores primos. En concordancia con esto, nombramos D al conjunto de primos impares positivos que son factores de algún a_i. Es claro que ambos N y D son subconjuntos finitos de $p = 2, 3, \cdots, \infty$. El primo $p = 2$ no debe preocuparnos pues siempre merece un análisis aparte.

En el siguiente lema utilizaremos la notación anterior.

Lema 5.9. *Si $N \cap (D \cup \{2, \infty\}) = \emptyset$ y existe $x_p \in \mathbb{Q}_p^*$ que cumple $(a_i, x_p)_p = (m_i, n_i)_p$ para todo $p = 2, 3, \cdots, \infty$, entonces existe un primo q tal que el valor $x = aq$, con $a = \prod_{t \in N} t$, resuelve el sistema.*

Prueba. Empezamos identificando un candidato a q. Ponemos $m = 8 \prod_{l \in D} l$. Como $N \cap (D \cup \{2, \infty\}) = \emptyset$ es claro que m y $a = \prod_{t \in N} t$ son primos entre sí. Con ello, por el teorema de Dirichlet, existen infinitos primos q que satisfacen $q \equiv a \pmod{m}$. Como el conjunto $N \cup D \cup \{2\}$ es finito, existe un primo q que cumple el teorema de Dirichlet y no está en $N \cup D \cup \{2\}$. Afirmamos que este q es el valor buscado, pues $x = aq$ resuelve el sistema.

Ahora pasamos a verificar que efectivamente x resuelve el sistema. Por la definición de N y D, así como por la hipótesis $N \cap (D \cup \{2, \infty\}) = \emptyset$, lo que debemos comprobar se reduce a cinco condiciones.

1. Si $p = \infty$ se tiene $(a_i, x)_\infty = 1$,

2. si $p = 2$ se tiene $(a_i, x)_2 = 1$,

3. si $p \in D$ se tiene $(a_i, x)_p = 1$,

4. si $p \notin N \cup D \cup \{2, \infty, q\}$ se tiene $(a_i, x)_p = 1$,

5. si $p \in N \cup \{q\}$ se tiene $(a_i, x)_p = (m_i, n_i)_p$.

Caso 1. Si $p = \infty$ es claro que se cumple $(a_i, x)_\infty = 1$ pues x es positivo.

Caso 2. Sea $p = 2$, como se tiene $2 \notin N$, es claro que a es unidad 2-ádica. Es más, como $q \neq 2$, se tiene que $x = aq$ también es unidad 2-ádica. Como se tiene $x = aq \equiv a^2 \pmod{m}$ y 8 divide a m, se satisface $x \equiv a^2 \pmod{8}$. Es más, como a es impar, se cumple $a^2 \equiv 1 \pmod{8}$. Así tenemos $x \equiv 1 \pmod{8}$ con lo que x resulta ser cuadrado en $\mathbb{Q}_2^*$; de aquí es claro que se cumple $(a_i, x)_2 = 1$.

Caso 3. Sea ahora $p > 2$ con $p \in D$. Como se tiene $p \notin N$, es claro que a es unidad p-ádica. Es más, como $q \notin D$, el valor $x = qa$ también es unidad p-ádica. Como p divide a m, se cumple $x \equiv a^2 \pmod{p}$. Precisamente, al ser x un resto cuadrático módulo p se tiene que x es un cuadrado de $\mathbb{Q}_p^*$ y por ende se cumple $(a_i, x)_p = 1$.

Caso 4. Cuando se tiene $p \notin D \cup N \cup \{2, \infty, q\}$, tanto a_i como a son unidades p-ádicas (pues los divisores de a_i están en $D \cup \{2\}$ y a es el producto de elementos de N). Es más, al ser a unidad p-ádica, x también lo es. Para $y = p^{n_p} u_p \in \mathbb{Q}_p^*$, por fórmula tenemos

$$(a_i, y)_p = \left(\frac{a_i}{p}\right)^{n_p}.$$

Si ponemos $y = x$, se tiene $n_p = 0$ y por ende se cumple $(a_i, y)_p = 1$.

Caso 5. Si $p \in N$ es claro que se tiene $x = pu_p$ y que se cumple $(a_i, x)_p = \left(\frac{a_i}{p}\right)$. Por hipótesis existe $x_p = p^{n_p} u_p \in \mathbb{Q}_p$ sujeto a $(a_i, x_p)_p = (m_i, n_i)_p$

para $p = 2, 3, \cdots, \infty$. Es más, se tiene $(a_i, x_p)_p = \left(\frac{a_i}{p}\right)^{n_p}$. Al tenerse $p \in N$ existe i con el que se satisface $(m_i, n_i)_p = -1$, por lo que se exige que n_p no sea par. De este modo se cumple $(a_i, x_p)_p = \left(\frac{a_i}{p}\right)$ y se logra

$$(a_i, x)_p = \left(\frac{a_i}{p}\right) = (a_i, x_p)_p = (m_i, n_i)_p$$

para todo $p \in N$. Por último, sea $p = q$. Por la fórmula producto se satisface

$$(m_i, n_i)_q \prod_{p \neq q} (m_i, n_i)_p = 1,$$
$$(a_i, x)_q \prod_{p \neq q} (a_i, x)_p = 1.$$

Por lo ya demostrado, se cumple

$$\prod_{p \neq q} (m_i, n_i)_p = \prod_{p \neq q} (a_i, x)_p.$$

Es claro entonces que se satisface $(m_i, n_i)_q = (a_i, x)_q$. □

Observación 5.10. La prueba del lema muestra que la familia $(m_i, n_i)_p$ puede ser reemplazada por cualquier otra familia de valores $b_{i,p} = \pm 1$ siempre y cuando se satisfaga la fórmula producto $\prod_p b_{i,p} = 1$ para todo $i = 1, \cdots, k$ (notemos que en la prueba anterior, ésta fue la única propiedad de la familia $(m_i, n_i)_p$ que se utilizó).

Teorema 5.11. *Sea el sistema $(a_i, x)_p = (m_i, n_i)_p$ con $a_i, m_i, n_i \in \mathbb{Q}^*$ y $p = 2, 3, \cdots, \infty$. Para que exista $x \in \mathbb{Q}^*$ que resuelva el sistema es necesario y suficiente que exista $x_p \in \mathbb{Q}_p^*$ que cumpla $(a_i, x_p)_p = (m_i, n_i)_p$ para $p = 2, 3, \cdots, \infty$.*

Prueba. Lo que dice el teorema es claro: para que exista una solución en $\mathbb{Q}^*$ (campo global), el sistema debe poder resolverse en cada uno de sus

lugares ($\mathbb{R}$ y los p-ádicos). Es una idea similar a la del teorema de Hasse Minkowsky. Lógicamente basta probar la implicación de regreso.

Una observación inicial es importante: como se satisface $a_i = b_i/c_i$ para ciertos b_i, c_i, se tiene $(a_i, x)_p = (d_i, x)_p$ con $d_i = a_i c_i^2 \in \mathbb{Z}^*$. Con esto, el sistema $(a_i, x)_p = (d_i, x)_p = (m_i, n_i)_p$ resulta ser el mismo del Lema 5.9. Sin embargo, aún no podemos hacer uso de este resultado pues la condición $N \cap (D \cup \{2, \infty\}) = \emptyset$ no se satisface necesariamente. Lo que haremos será buscar un sistema auxiliar sobre el que sí se pueda aplicar el lema.

Por hipótesis existe $x_p \in \mathbb{Q}_p^*$ que cumple $(a_i, x_p)_p = (m_i, n_i)_p$. Ahora, como $D \cup \{2, \infty\}$ es finito, el Teorema 4.5 asegura que $\mathbb{Q}^*$ es denso en $\prod_{p \in D \cup \{2,\infty\}} \mathbb{Q}_p^*$ y por consiguiente se interseca con cualquier abierto de $\prod_{p \in D \cup \{2,\infty\}} \mathbb{Q}_p^*$. Por otro lado, el Corolario 4.3 asegura que $x_p \mathbb{Q}_p^{*2}$ es abierto en $\mathbb{Q}_p^*$ y por consiguiente $\prod_{p \in D \cup \{2,\infty\}} x_p \mathbb{Q}_p^{*2}$ es abierto en $\prod_{p \in D \cup \{2,\infty\}} \mathbb{Q}_p^*$. Así, por el Corolario 4.3 existe un racional no nulo r que cumple $r \in x_p \mathbb{Q}_p^{*2}$ para $p \in D \cup \{2, \infty\}$. Si ponemos $y_p = r/x_p$ resulta que y_p es cuadrado perfecto y por tanto cumple $(d_i, y_p)_p = 1$. De esta manera se tiene

$$(d_i, r)_p = (d_i, y_p x_p)_p = (d_i, y_p)_p (d_i, x_p)_p = (m_i, n_i)_p,$$

para todo $p \in D \cup \{2, \infty\}$. Detengámonos en el producto $(m_i, n_i)_p (d_i, r)_p$, ahora para un p arbitrario. Es evidente que se tiene $(m_i, n_i)_p (d_i, r)_p = \pm 1$. Es más, si $p \in D \cup \{2, \infty\}$, este producto resulta ser 1. Además por fórmula producto se tiene

$$\prod_p (m_i, n_i)_p (d_i, r)_p = \prod_p (m_i, n_i)_p \prod_p (d_i, r)_p = 1,$$

para cada $i = 1, \cdots, k$. De esta manera, por la Observación 5.10, ya tenemos el candidato a sistema auxiliar que buscamos, el cuál será

$$(d_i, x)_p = (m_i, n_i)_p (d_i, r)_p.$$

Ahora comprobamos que este nuevo sistema satisface las condiciones del Lema 5.9. Primero, como se tiene $(m_i, n_i)_p(d_i, r)_p = 1$ para $p \in D \cup \{2, \infty\}$, los subconjuntos N y D de este nuevo sistema satisfacen $N \cap (D \cup \{2, \infty\}) = \emptyset$. Además, el valor $x'_p = x_p r$ cumple $(d_i, x'_p)_p = (m_i, n_i)_p(d_i, r)_p$ para todo $p = 2, 3, \cdots, \infty$. En consecuencia se puede aplicar el Lema 5.9 (más bien la Observación 5.10) al sistema auxiliar y aseguramos así la existencia de un racional z que satisface $(d_i, z)_p = (m_i, n_i)_p(d_i, r)_p$ para todo $p = 2, 3, \cdots, \infty$. Si ponemos $x = zr$ se tiene

$$(d_i, x)_p = (d_i, r)_p(d_i, z)_p = (d_i, r)_p(m_i, n_i)_p(d_i, r)_p = (m_i, n_i)_p.$$

Y x cumple el cometido. □

Capítulo 6

Formas cuadráticas sobre $\mathbb{Q}_p$

Este apartado es el complemento del Capítulo 5 de [2] y por tanto nos remitimos a él a lo largo de esta sección.

Proposición 6.1. *Toda forma cuadrática regular de 3 o más variables sobre $\mathbb{Q}$ representa a 0 sobre $\mathbb{Q}_p$ salvo para un número finito de primos $p = 2, 3, \cdots, \infty$.*

Prueba. Sea f una forma cuadrática regular de $n \geq 3$ variables. Si multiplicamos f por cierto entero a conseguimos una forma af con coeficientes enteros. Sea D el conjunto de todos los divisores primos de los coeficientes de af. Sea p primo con $p \notin D$. Reducimos af módulo p y tenemos una forma regular en $\mathbb{F}_p$ que, por el Corolario 1.4, posee un cero no trivial. Luego se puede aplicar el Corolario 1.6 y resulta que f representa a 0 en $\mathbb{Q}_p$ para todo p salvo, posiblemente, aquellos que pertenecen al conjunto finito D junto con $p = 2$. □

A partir de este punto y en lo que resta del capítulo trabajaremos con formas cuadráticas regulares sobre $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ con $p = 2, 3, \cdots$ (no consideramos el caso real, salvo que se indique lo contrario). El siguiente resultado es el Lema 5.13 de [2], cuya prueba quedó pendiente hasta contar con las herramientas necesarias para este fin.

Proposición 6.2. *Sea $f(x_1, \cdots, x_4) = a_1x_1^2 + \cdots + a_4x_4^2$ una forma cuadrática regular. Entonces f representa a cero única y exclusivamente en los siguientes dos casos: bien $d \neq [1]$ o bien $d = [1]$ y $\epsilon = (-1, -1)$.*

Prueba. El Lema 7.1 (cuya prueba trivial se desarrolla en el próximo capítulo) asegura que f representa a cero si y solo existe $a \in \mathbb{Q}_p^*$ que es representado simultáneamente por las formas

$$g(x_1, x_2) = a_1x_1^2 + a_2x_2^2 \quad \text{y} \quad h(x_3, x_4) = -a_3x_3^2 - a_4x_4^2.$$

Por el Corolario 5.11 de [2] esto se cumple si y solo si existe $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ sujeto a las igualdades

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

Supongamos que no existe a que satisface lo anterior. Sean M y N el conjunto de valores $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ que satisfacen respectivamente las ecuaciones $(x, -a_1a_2) = (a_1, a_2)$ y $(x, -a_3a_4) = (-a_3, -a_4)$. Es claro que M y N son no vacíos, pues los valores $x = a_1$ y $x = -a_3$ resuelven la primera y segunda ecuación respectivamente. Es más, la condición de no existencia de a es equivalente a tener $M \cap N = \emptyset$. Entonces, por la Proposición 3.8, esto se da si y solo si se cumple tanto $a_1a_2 = a_3a_4$ como $(a_1, a_2) = -(-a_3, -a_4)$. De la primera condición extraemos $a_1a_2a_3a_4 = [1]$. Por otro lado tenemos

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

Luego, como se cumple la relación $(a, a) = (-1, a)$, se consigue

$$\begin{aligned}
\epsilon_f &= (a_1, a_2)(a_3, a_4)(-1, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(-1, a_3)(-1, a_4) \\
&= (a_1, a_2)(-a_3, a_4)(-1, a_3) \\
&= (a_1, a_2)(-a_3, a_4)(-1, -a_3)(-1, -1) \\
&= (a_1, a_2)(-a_3, -a_4)(-1, -1).
\end{aligned}$$

Finalmente, usando la relación $(a_1, a_2) = -(-a_3, -a_4)$ se concluye $\epsilon_f = -(-1, -1)$. □

Observación 6.3. De la proposición anterior se desprende que las únicas formas cuadráticas de cuatro variables que no representan 0 son aquellas

cuyo discriminante es 1 en $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ y cuyo invariante de Hasse resulta ser $-(-1,-1)$.

Sea la forma cuadrática

$$f(x_1,\cdots,x_4) = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2.$$

Es claro que se tiene $d_f = -a\cdot -b\cdot ab = (ab)^2 \equiv 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Es más, se cumple también

$$\epsilon_f = (1,-a)(1,-b)(1,ab)(-a,-b)(-a,ab)(-b,ab).$$

Y como se satisface $(1,-a) = (1,-b) = (1,ab) = 1$, logramos

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

Entonces, si elegimos a,b de tal forma que se tenga $(a,b) = -1$, f resulta ser una forma cuadrática de 4 variables que no representa a 0. Se prueba que es la única salvo equivalencia.

A continuación verificaremos que todas las formas cuadráticas de 5 variables representan 0. El resultado se desprenderá del siguiente lema.

Lema 6.4. *Todas las formas cuadráticas regulares de dos o más variables representan al menos 2 clases distintas de* $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Prueba. Es suficiente hacer la prueba para formas de dos variables. El Corolario 5.11 de [2] afirma que una forma f de dos variables representa a $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ si y solo si se cumple la relación $(a,-d) = \epsilon_f$. Observemos que con $d = -1$ se fuerza a tener $\epsilon_f = 1$. Si $p = 2$, la Observación 3.7 asegura que la ecuación $(x,1) = 1$ posee 8 soluciones si $d = -1$. Si $d \neq -1$, la ecuación $(x,-d) = \epsilon_f$ posee 4 soluciones independientemente del valor de

ϵ_f. Si $p \neq 2$, de nuevo por la Observación 3.7, aseguramos que la ecuación $(x, 1) = 1$ posee 4 soluciones si $d = -1$. Si $d \neq -1$, la ecuación $(x, -d) = \epsilon_f$ posee 2 soluciones independientemente del valor de ϵ_f. □

Proposición 6.5. *Todas las formas cuadráticas de 5 o más variables en $\mathbb{Q}_p$ (con $p \neq \infty$) representan a cero.*

Prueba. Probaremos el resultado para una forma f de 5 variables, el caso general se desprende trivialmente. El Lema 6.3 asegura que f representa al menos a un par elementos de $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Como son dos, uno de ellos, digamos a, será distinto de d_f. De este modo sabemos que f representa a $a \neq d_f$. La Proposición 4.6 de [2] garantiza la existencia de una forma g de 4 variables tal que f es equivalente a $az^2 + g$. De esta manera se tiene $d_f = a \cdot d_g$. Al tenerse $a \neq d$, se cumple $d_g \neq 1$. De esta manera, la Proposición 6.2 garantiza que g representa a 0. Al añadir $z = 0$ obtenemos que f también representa a cero. □

Corolario 6.6 *Sea $f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$ una forma cuadrática de 4 o más variables. Si $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, entonces f representa a a.*

Demostración. La forma cuadrática $f'(x_1, \cdots, x_4, z) = f - az^2$ representa a 0 única y exclusivamente si f representa a a. Como f' es de 5 variables se tiene el resultado pedido. □

Observación 6.7 La Proposición 6.5 falla para formas cuadráticas sobre $\mathbb{Q}_\infty$. La forma $f(x_1, \cdots, x_5) = x_1^2 + \cdots + x_5^2$ no representa a -1 en $\mathbb{Q}_\infty^*/\mathbb{Q}_\infty^{*2}$. Es éste el argumento que falla en la prueba de la Proposición 6.5.

Capítulo 7

Teorema de Hasse Minkowsky

En este capítulo terminaremos la prueba del teorema de Hasse Minkowsky iniciada en [2]. Probaremos un par de resultados previos.

Lema 7.1. *Sean* $f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$ *y* $g(y_1, \cdots, y_m) = b_1y_1^2 + \cdots + b_my_m^2$ *dos formas cuadráticas regulares. Entonces* $f - g$ *representa a 0 si y solo si existe* $a \in \mathbb{Q}_p^*$ *que es representado tanto por* f *como por* g*.*

Prueba. El regreso es obvio. Supongamos que $f - g$ representa a 0. De ser así, existen vectores $u = (x_1, \cdots, x_n)$ y $v = (y_1, \cdots, y_m)$ que satisfacen $f(u) = g(v)$. Si $f(u) \neq 0$, hacemos $a = f(u)$. Si $f(u) = 0$, ambas formas f y g representan a 0 y con ello, a todos los elementos de $\mathbb{Q}_p^*$. □

Lema 7.2. *Sean* $a, b, c \in \mathbb{Q}^*$*. Si se cumple la igualdad* $(c, -ab)_p = (a, b)_p$ *para* $p = 2, 3, \cdots, \infty$*, entonces la forma* $ax^2 + by^2$ *representa a* c *en* $\mathbb{Q}$*.*

Prueba. Por bimultiplicidad del símbolo de Hilbert es claro que se cumple

$$(c, -ab)_p = (c, -1)_p(c, a)_p(c, b)_p.$$

Al multiplicar $(-1, a)_p(-1, b)_p$ a ambos lados de $(c, -ab)_p = (a, b)_p$ se consigue

$$(c, -1)_p(c, a)_p(c, b)_p(-1, a)_p(-1, b)_p = (a, b)_p(-1, a)_p(-1, b)_p,$$

de donde se pasa a

$$\begin{aligned}(-1, abc)_p &= (a, b)_p(-1, a)_p(-1, b)_p(c, a)_p(c, b)_p \\ &= (a, b)_p(a, -c)_p(b, -c)_p.\end{aligned}$$

Para la forma $f'(x, y, z) = ax^2 + by^2 - cz^2$ se tiene

$$\epsilon_{f'} = (a,b)_p(a,-c)_p(b,-c)_p \text{ y } det_{f'} = -abc.$$

Por tanto, el Teorema 5.10 de [2] indica que f' representa a cero en $\mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$. Como esta forma es de 3 variables, el teorema de Hasse Minkowski asegura que también representa a cero en $\mathbb{Q}^*$. Debido a esto, la forma $ax^2 + by^2$ representa a c en $\mathbb{Q}^*$. □

Teorema 7.3 (Hasse Minkowsky). *Sea f una forma cuadrática regular sobre $\mathbb{Q}$. Entonces f representa a cero en $\mathbb{Q}$ si y solo si representa a cero en $\mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$.*

Prueba. Recordemos que ya realizamos la prueba para formas de hasta tres variables y que solo se necesita probar el retorno. Sea la forma $f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2$.

Caso $n = 4$. Ponemos $f(x_1, \cdots, x_4) = a_1x_1^2 + a_2x_2^2 - (-a_3x_3^2 - a_4x_4^2)$. Como f representa a cero en $\mathbb{Q}_p$, el Lema 7.1 asegura que existe y_p que es representado tanto por $g(x_1, x_2) = a_1x_1^2 + a_2x_2^2$ como por $h(x_3, x_4) = -a_3x_3^2 - a_4x_4^2$ para $p = 2, 3, \cdots, \infty$. El Corolario 5.11 de [2] asegura que una forma regular k de 2 variables con discriminante d_k representa a y_p si y solo si se satisface $(y_p, -d_k) = \epsilon_k$. De esta manera se tiene

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

Éste resulta ser un sistema como el del Teorema 5.10, así que existe $a \in \mathbb{Q}^*$ sujeto a

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

Con esto y el Lema 7.2 queda garantizado que las formas $a_1x_1^2 + a_2x_2^2 = g(x_1, x_2)$ y $-a_3x_3^2 - a_4x_4^2 = h(x_3, x_4)$ representan a a en $\mathbb{Q}^*$. Como se tiene $f = g - h$ es claro que f representa a cero en $\mathbb{Q}^*$.

Caso $n \geq 5$. Haremos la prueba por inducción. Sea $f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2 = (a_1x_1^2 + a_2x_2^2) + (a_3x_3^2 + \cdots + a_nx_n^2)$. Ponemos $g = a_1x_1^2 + a_2x_2^2$ y $h = a_3x_3^2 + \cdots + a_nx_n^2$. Definimos el conjunto $N = \{p \text{ primo tal que } h \text{ no representa a cero en } \mathbb{Q}_p\}$. Por la Proposición 6.1, N es finito. De aquí se desprenden dos casos.

Caso 1. Si $N = \emptyset$, entonces h representa a cero en $\mathbb{Q}_p$ para todo $p = 2, 3, \cdots, \infty$. Por hipótesis inductiva h representa a cero en $\mathbb{Q}$. Si g representa a $a \in \mathbb{Q}$, h representa a $-a$ y por ende f representa a 0 en $\mathbb{Q}$.

Caso 2. Sea $N \neq \emptyset$. Como f representa a cero en $\mathbb{Q}_p^*$, existe $a_p \in \mathbb{Q}_p^*$ que cumple

$$g(x_{1p}, x_{2p}) = a_p \text{ y } h(x_{3p}, \cdots, x_{np}) = -a_p.$$

Recordemos que $a_p\mathbb{Q}_p^{*2}$ es abierto en $\mathbb{Q}_p^*$. Por tanto, el Teorema 4.5 asegura la existencia de $x_1, x_2 \in \mathbb{Q}$ que satisfacen $g(x_1, x_2) = a$ con $a \in a_p\mathbb{Q}_p^{*2}$ para todo $p \in N$. Sea entonces $a = a_p u_p^2$ con $u_p \in \mathbb{Q}_p^*$. Sea la forma cuadrática $k(z, x_3, \cdots, x_n) = az^2 + h(x_3, \cdots, x_n)$ de $n-1$ variables, que cumple $k = az^2 + h$. Al evaluar $k(1/u_p, x_{3p}, \cdots, x_{np})$ notamos que k representa cero en $\mathbb{Q}_p$ para $p \in N$. Como h representa a cero para todo $p \notin N$, la forma k también lo hace. De esta manera k representa a cero en $\mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$. Por hipótesis inductiva k representa cero en $\mathbb{Q}$. De aquí h representa a $-a$ en $\mathbb{Q}$. Como g representa a a en $\mathbb{Q}$, se tiene que f representa a cero en $\mathbb{Q}$. □

Capítulo 8

La clasificación de las formas cuadráticas sobre $\mathbb{Q}$

El teorema de Hasse Minkowsky tiene múltiples aplicaciones. En este capítulo final, el mencionado teorema nos servirá para abordar el estudio de la clasificación de formas cuadráticas sobre los racionales. Recordemos que en [2] se realizó la clasificación de formas cuadráticas de hasta tres variables sobre $\mathbb{Q}_p$ con $p = 2, 3, \cdots, \infty$.

Los siguientes resultados complementan al Teorema 5.14 y Teorema 5.15 (ambos en [2]), respectivamente.

Teorema 8.1. *Dos formas cuadráticas regulares sobre $\mathbb{Q}_p$ con $p = 2, 3, \cdots$ son equivalentes si y solo si tienen el mismo discriminante (sobre $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$) y el mismo invariante de Hasse.*

Prueba. El Teorema 5.14 de [2] prueba el caso para formas de hasta tres variables. Para formas de 4 o más variables se sigue el mismo argumento inductivo que se utilizó en aquel teorema. □

Teorema 8.2 *Sea f una forma cuadrática regular de 4 o más variables sobre $\mathbb{Q}_p$ con $p = 2, 3, \cdots$. Entonces, el número de clases de formas equivalentes es 8 si $p > 2$ y 16 si $p = 2$.*

Demostración. La idea es exactamente la misma del Teorema 5.15 de [2]: hallar las combinaciones de ϵ_f y d_f que no se asocian a ninguna forma cuadrática. En este caso la tarea es probar que existe una forma cuadrática de 4 o más variables cuyos invariantes son ϵ_f y d_f, sin importar el valor que estos tomen. Entonces, sean ϵ_f y d_f dados. Por el Teorema 5.15 de [2] existe una forma cuadrática de tres variables f' que cumple $d_{f'} = d_f$ y $\epsilon_{f'} = \epsilon_f$. Luego, es claro que la forma cuadrática $f = f' + x_4^2 + \cdots + x_n^2$ tiene como invariantes d_f y ϵ_f. □

Observación 8.3 La clasificación de formas cuadráticas reales de hasta

tres variables fue tratada en el Capítulo 5 de [2]. Vimos que los invariantes d_f y ϵ_f eran suficientes para clasificar las formas. Sin embargo, para formas cuadráticas de 4 o más variables, la clasificación basada en el discriminante y el invariante de Hasse es insuficiente. Sean $f(x_1, \cdots, x_4) = x_1^2 + \cdots + x_4^2$ y $g(x_1, \cdots, x_4) = -x_1^2 - \cdots - x_4^2$ formas cuadráticas reales. Es evidente que se cumple $\epsilon_f = \epsilon_g = 1$ y $d_f = d_g = 1$. Sin embargo f y g no son equivalentes pues no tienen la misma imagen. Se tiene entonces que para formas cuadráticas reales de 4 o más variables debe especificarse también la signatura (en el ejemplo anterior, la signatura de f y g es 0 y 4 respectivamente).

Para abordar la clasificación de formas regulares racionales necesitamos algunos preparativos.

Lema 8.4 *Sea $f : V \to K$ una forma cuadrática regular sobre un cuerpo de característica distinta de dos y B la forma bilineal asociada. Si existe $y \in V$ que satisface $B(y, y) \neq 0$, entonces la aplicación $r : V \to V$ definida cual $r_y(x) = x - 2\dfrac{B(x, y)}{B(y, y)}y$ es una transformación lineal invertible que cumple $B(u, v) = B(r(u), r(v))$.*

Prueba. Para $u, v \in V$ y $\alpha, \beta \in K$, se tiene

$$\begin{aligned} r_y(\alpha u + \beta v) &= \alpha u + \beta v - 2\frac{B(\alpha u + \beta v, y)}{B(y, y)}y \\ &= \alpha u - \frac{2\alpha B(u, y)}{B(y, y)}y + \beta v - \frac{2\beta B(v, y)}{B(y, y)}y \\ &= \alpha\left(u - \frac{2B(u, y)}{B(y, y)}y\right) + \beta\left(v - \frac{2B(v, y)}{B(y, y)}y\right) \\ &= \alpha r_y(u) + \beta r_y(v), \end{aligned}$$

y así tenemos que r_y es una transformación lineal; es más, resulta ser una involución pues se tiene

$$\begin{aligned}
r_y(r_y(v)) &= r_y(v) - 2\frac{B(r_y(v),y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y - \frac{2B(v-2\frac{B(v,y)}{B(y,y)}y,y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y - 2\frac{B(v,y)+B(-2\frac{B(v,y)}{B(y,y)}y,y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y - 2\frac{B(v,y)-2\frac{B(v,y)}{B(y,y)}B(y,y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y - 2\frac{B(v,y)-2B(v,y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y + 2\frac{B(v,y)}{B(y,y)}y = v.
\end{aligned}$$

Por último probamos que se tiene $B(u,v) = B(r(u),r(v))$, es decir B es $r-$invariante. En efecto, se tiene la siguiente secuencia

$$\begin{aligned}
B(r(u),r(v)) &= B(u-2\frac{B(u,y)}{B(y,y)}y, v-2\frac{B(v,y)}{B(y,y)}y) \\
&= B(u,v) + B(u,-2\frac{B(v,y)}{B(y,y)}y) + B(v,-2\frac{B(u,y)}{B(y,y)}y) \\
&\quad + B(-2\frac{B(u,y)}{B(y,y)}y, -2\frac{B(v,y)}{B(y,y)}y) \\
&= B(u,v) - 2\frac{B(v,y)}{B(y,y)}B(u,y) - 2\frac{B(u,y)}{B(y,y)}B(v,y) \\
&\quad + 4\frac{B(u,y)}{B(y,y)}\frac{B(v,y)}{B(y,y)}B(y,y) \\
&= B(u,v).
\end{aligned}$$

□

Proposición 8.5 *Sean $f,g : V \to K$ formas cuadráticas regulares equivalentes de n variables sobre un cuerpo que no es de característica dos. Si se tiene $f = f' + az^2, g = g' + az^2$ con f' y g' formas cuadráticas de $n-1$ variables, entonces f' es equivalente a g'.*

Prueba. Como f' y g' pueden ser diagonalizados, debemos probar que la equivalencia de

$$f(x_1, \cdots, x_n) = a_1x_1^2 + \cdots + a_{n-1}x_{n-1}^2 + ax_n^2$$

y

$$g(x_1, \cdots, x_n) = b_1x_1^2 + \cdots + b_{n-1}x_{n-1}^2 + ax_n^2$$

implica la equivalencia de $f'(x_1, \cdots, x_{n-1}) = a_1x_1^2 + \cdots + a_{n-1}x_{n-1}^2$ y $g'(x_1, \cdots, x_{n-1}) = b_1x_1^2 + \cdots + b_{n-1}x_{n-1}^2$. Como f y g son equivalentes entonces se expresan como se indica arriba respecto a la misma forma bilineal B, pero en distintas bases, digamos $B_f = \{u_1, \cdots, u_n\}$ y $B_g = \{v_1, \cdots, v_n\}$. Ahora, como la matriz asociada a las formas está diagonalizada se tiene $u_n^{\perp} =< u_1, \cdots, u_{n-1} >= U$ y $v_n^{\perp} =< v_1, \cdots, v_{n-1} >= V$. De este modo, lo que se debe probar es la existencia de una base $\{w_1, \cdots, w_n\}$ de U en la cual la forma restringida resulte ser g'. Si se tiene $u_n = v_n$ entonces no hay nada que probar pues se tiene $U = V$ y la base buscada es $\{v_1, \cdots, v_{n-1}\}$. Si u_n es distinto a v_n entonces se tiene debido a la condición de regularidad $B(u_n - v_n, u_n - v_n) \neq 0$. Luego, mediante el cambio de base $r_{u_n - v_n}$ propuesto en el Lema 8.4 se pasa de la base $\{v_1, \cdots, v_n\}$ a la base $\{r_{u_n-v_n}(v_1), \cdots, r_{u_n-v_n}(v_{n-1}), u_n\}$. Notemos que se tiene

$$B(r_{u_n-v_n}(v_k), u_n) = B(r_{u_n-v_n}(v_k), r_{u_n-v_n}(v_n)) = B(v_k, v_n) = 0,$$

para todo $k = 1, \cdots, n-1$. Así, $\{r_{u_n-v_n}(v_1), \cdots, r_{u_n-v_n}(v_{n-1})\}$ es un conjunto de $n-1$ vectores linealmente independientes que pertenecen al complemento ortogonal de u_n, por lo que $\{r_{u_n-v_n}(v_1), \cdots, r_{u_n-v_n}(v_{n-1})\}$ resulta ser una base de V, precisamente la base buscada. □

Teorema 8.6 *Sean f y g formas cuadráticas regulares de n variables sobre $\mathbb{Q}$. Para que f y g sean equivalentes en $\mathbb{Q}$ es necesario y suficiente que sean equivalentes en $\mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$.*

Demostración. La ida es trivial. Para probar el regreso procedemos por inducción sobre n. Si $n = 1$ se tiene $f(x_1) = a_1x_1^2$ y $g(x_2) = a_2x_2^2$. Como f y g son equivalentes en $\mathbb{Q}_p$ representan a los mismos elementos. Con ello, se cumple que $h(x_1, x_2) = a_1x_1^2 - a_2x_2^2$ representa a 0 en $\mathbb{Q}_p$ para $p = 2, 3, \cdots, \infty$. Por el teorema de Hasse Minkowsky h representa a 0 en $\mathbb{Q}$ y hemos conseguido $a, b \in \mathbb{Q}$ que satisfacen $f(a) = g(b)$. Luego,

como se tiene $a_1a^2 = b_1b^2$, se cumple $a_2 = a_1(b/a)^2$. Con ello obtenemos $g(x_2) = a_1(b/ax_2)^2$ y resulta que g es equivalente a f.

Ahora, sean f y g de n variables. Como antes, se cumple que la forma $h = f - g$ representa a cero en $\mathbb{Q}_p$ y por Hasse Minkowsky también representa a 0 en $\mathbb{Q}$. Con ello, existe $k \in \mathbb{Q}$ que es representado por ambas formas f y g. La Proposición 4.6 de [2] nos permite escribir f y g cual

$$f = f' + kz^2 \quad \text{y} \quad g = g' + kz^2$$

con f', g' formas cuadráticas de $n-1$ variables. Luego, por la Proposición 8.5, resulta que f' y g' son equivalentes sobre $\mathbb{Q}_p$. La hipótesis inductiva permite concluir que f' y g' son equivalentes en $\mathbb{Q}$ y por consiguiente f y g también lo son. □

Bibliografía

[1] Apostol, Tom, *Introducción a la teoría analítica de números*; Reverté, 1984.

[2] Castillo, Alberto, *El teorema de Hasse Minkoski hasta tres variables*; tesis de licenciatura en matemáticas, Pontificia Universidad Católica del Perú, 2015.

[3] Condori, José, *Factorización de polinomios sobre los números p-ádicos*; tesis de maestría en matemáticas, Pontificia Universidad Católica del Perú, 2001.

[4] Dioses, Jorge, *Series de Dirichlet*; tesis de licenciatura en matemáticas, Pontificia Universidad Católica del Perú, 2000.

[5] Ireland, Kenneth; Rosen, Michael, *A clasical introduction to modern number theory*; Springer Verlag, 1990.

[6] Munkres, James, *Topología*; Pearson Educación, 2002.

[7] Serre, Jean Pierre, *A Course in Arithmetic*; Springer Verlag, 1973.

[8] Villogas, Edwin, *Leyes de reciprocidad*; tesis de maestría en matemáticas, Pontificia Universidad Católica del Perú, 2008.