USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Formas Cuadráticas

Xabier Legaspi Juanatey

Curso 2016-2017

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Aos meus avós.

"No medio do caos tamén hai oportunidade."
—Sun Tzu, A arte da guerra

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Formas cuadráticas

Xabier Legaspi Juanatey

Xullo, 2017

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Formas Cuadráticas
Director/a: Javier Majadas Soto
Breve descrición do contido
Estudaranse as formas cuadráticas sobre corpos, centrándose especialmente no caso de corpos finitos, p–ádicos e racionais, así como os seus aneis de Witt. Será necesario estudar os capítulos 1 e 2 de [4] e os capítulos do I a IV de [6].
Recomendacións
Unha boa formación en Álxebra é moi recomendable. En particular, recoméndase soltura cos contidos das asignaturas "Estruturas Alxébricas", "Ecuacións Alxébricas" e "Álxebra, Números e Xeometría". Para unha descrición máis detallada do traballo e das recomendacións é recomendable falar co profesor previamente.
Outras observacións
O tema é de gran importancia para quen desexe iniciar a súa formación en *Xeometría Alxébrica* ou en *Teoría de Números*, por iso se recomenda que quen pretenda realizar o traballo teña a súa interese centrada nalgunha destas disciplinas.

Índice xeral

Resumo

A clasificación de formas cuadráticas sobre un corpo é un problema fundamental en matemáticas. Cando o corpo base é $\mathbb{R}$, $\mathbb{C}$ ou un corpo finito, a clasificación é completamente elemental. Nesta memoria trataremos a clasificación sobre o corpo $\mathbb{Q}$ dos números racionais (*Teorema de Hasse-Minkowski*), que é un problema moito máis difícil.

Abstract

The classification of quadratic forms over a field is a fundamental problem in mathematics. When we work with the fields $\mathbb{R}$, $\mathbb{C}$ or a finite one, classification is completely straightforward. On this report we will deal with the classification over the field $\mathbb{Q}$ of rational numbers (*Theorem of Hasse-Minkowski*), which is by far a more difficult problem.

Introdución

Unha ecuación diofántica é unha ecuación $f(x_1, ..., x_n) = 0$ onde f é un polinomio con coeficientes enteiros e buscamos solucións nos números enteiros. Cando f é un polinomio de grao 1, a resolución da ecuación é fácil. Se $n = 1$ é claro, se $n = 2$ temos a ecuación

$$ax + by = c$$

que se resolve facilmente pola *identidade de Bezout* e o caso $n > 2$ redúcese a este.

Cando f é un polinomio de grao ≥ 2, a situación é xa moi complicada. Algunhas ecuacións particulares foron xa estudadas na antigüidade, como a ecuación pitagórica $x^2 + y^2 = z^2$ ou a ecuación $x^2 + y^2 = 2z^2$ que nos dá tres cadrados en progresión aritmética (x^2, z^2, y^2). Se $f(x_1, ..., x_n) = 0$ ten solución, entón a congruencia $f(x_1, ..., x_n) \equiv 0 \pmod{m}$ ten solución para calquera enteiro $m > 0$, e así temos condicións necesarias, facilmente comprobables para a existencia de solucións da ecuación diofántica. Así, por exemplo, a ecuación $x^2 + y^2 = 3z^2$ non ten solución distinta de $(0, 0, 0)$, xa que módulo 3 a única solución é $(0, 0, 0)$, é dicir, as únicas posibles solucións da ecuación serían $(3a)^2 + (3b)^2 = 3(3a)^2$. Tomando unha tal solución non nula co menor posible valor absoluto de x, obtemos a contradición de que $a^2 + b^2 = 3c^2$ danos unha solución menor.

Porén, estas condicións necesarias non son en absoluto suficientes. Por exemplo, a ecuación $3x^3 + 4y^3 + 5z^3 = 0$. Verifícase que ten solución non trivial módulo m para calquera $m > 0$ (e tamén ten solucións nos números reais) e non obstante non ten ningunha solución enteira. Este exemplo aparece en *[5]*.

Estas ecuacións anteriores son ecuacións definidas por polinomios homoxéneos. Neste caso, non hai moita diferencia entre buscar solucións en números

racionais ou en números enteiros, pois podemos multiplicar por un enteiro para eliminar denominadores. O noso principal obxectivo nestas notas é demostrar o *Teorema de Hasse-Minkowski*, que afirma que unha ecuación homoxénea de grao 2 ten solución (non trivial) se e só se ten solución módulo m para todo $m > 0$ e nos números reais. Como acabamos de ver no exemplo de Selmer, isto non é certo xa para o caso de ecuacións de grao 3. No caso de ecuacións de grao 2 non homoxéneas é fácil ver que tampouco é certo. Por exemplo *[7]* a ecuación $x^2 + 23y^2 = 41$ ten a solución racional $(\frac{1}{3}, \frac{4}{3})$ e así ten solución nos números reais e módulo m para calquera m coprimo con 3. Tamén $(\frac{9}{4}, \frac{5}{4})$ é solución co cal tamén ten solución módulo 3^t para todo t. Non obstante unha comprobación directa proba que non ten ningunha solución enteira xa que se $x > 6$ ou $y > 1$, $x^2 + 23y^2 > 41$.

A linguaxe axeitada para traballar non é a das congruencias, senón a dos números p–ádicos. No corpo $\mathbb{Q}$ dos números racionais existe para cada primo p a valoración p–ádica que nos dá unha estrutura de espazo métrico, así como a métrica usual. As completacións respectivas son o corpo dos números p–ádicos $\mathbb{Q}_p$ e o corpo dos números reais $\mathbb{R}$. O corpo $\mathbb{Q}_p$ ten unha estrutura topolóxica e alxébrica moi cómoda: é localmente compacto e é o corpo de fraccións do subanel aberto $\mathbb{Z}_p$ dos enteiros p–ádicos (que é un dominio compacto e así completo) cun subgrupo de unidades fácil de caracterizar. Unha vez estudados estes corpos p–ádicos (sección 2) as seguintes seccións enfócanse na demostración do teorema de Hasse-Minkowski, que neste contexto enúnciase da seguinte forma: *unha ecuación* $f(x_1, ..., x_n) = 0$ *con* f *un polinomio homoxéneo de grao* 2 *con coeficientes racionais ten solución en* $\mathbb{Q}$ *se e só se ten solución en* $\mathbb{R}$ *e en* $\mathbb{Q}_p$ *para todo número primo* p.

Para que o resultado sexa útil, é necesario ter criterios cómodos para saber cando unha ecuación homoxénea cuadrática ten solución en $\mathbb{Q}_p$ ou en $\mathbb{R}$. Isto faise no capítulo 4 resolvendo o problema en termos de certos invariantes numéricos (discriminante e símbolo de Hilbert). O discriminante é inmediato de calcular. Para o *símbolo de Hilbert*, no capítulo 3 obtéñense fórmulas explícitas, grazas a un estudo dos grupos de unidades de $\mathbb{Z}_p$ e $\mathbb{Q}_p$.

Non hai nestas notas ningún resultado nin demostración nova. Esencialmente seguimos os tratados de *J.P Serre [6], Z.I.Borevich, I. Shafarevich [1]*. Aínda que no

primeiro capítulo desenvolvemos toda a teoría que necesitamos de formas cuadráticas sobre corpos arbitrarios, recomendamos *[4]* para afondar en dita teoría.

Notación

– Chamaremos anel a un anel conmutativo con unidade.
– Os seguintes conxuntos serán denotados como segue:

· $\mathbb{N}$ o conxunto dos números naturais,

· $\mathbb{Z}$ o anel dos números enteiros,

· $\mathbb{Q}$ o corpo dos números racionais,

· $\mathbb{R}$ o corpo dos números reais,

· $\mathbb{Z}/n\mathbb{Z}$ o anel das clases de restos (módulo n).

– A inclusión de conxuntos denotarse por $\subset$.
– Todos os corpos que aparecen son de característica $\neq 2$.

Capítulo 1

Formas cuadráticas sobre corpos

1.1. Conceptos básicos

Sexa K un corpo de característica $\neq 2$ (os corpos cos que traballaremos serán de feito de característica cero, pero esta restrición é innecesaria e tampouco simplifica nada).

Definición 1.1.1 Unha forma cuadrática q sobre K é un polinomio homoxéneo de grao 2 sobre K. Como $car(K) \neq 2$, podemos escribir q como

$$q(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \text{ con } a_{ij} = a_{ji} \; \forall i, j$$

A matriz $A := (a_{ij})$ chámase matriz da forma cuadrática q. Chamaremos discriminante de q a $d := det(A)$.

Observación 1.1.2 Podemos pensar unha forma cuadrática como unha aplicación $q\colon W \to K$ dun espazo vectorial W de dimensión finita n en K que verifica:

(I) $q(\lambda w) = \lambda^2 q(w)$ para todo $\lambda \in K, w \in W$.

(II) $b_q\colon W \times W \to K$, $b_q(x,y) := \frac{1}{2}(q(x+y) - q(x) - q(y))$ é unha forma bilinear simétrica, é dicir, $b_q(x_1 + x_2, y) = b_q(x_1, y) + b_q(x_2, y)$, $b_q(\lambda x, y) = \lambda b_q(x, y)$, $b_q(x, y) = b_q(y, x)$. Ademais, $q(x) = b_q(x, x) = x^t A x$, onde x^t denota o vector transposto de x.

Diremos que q ten rango ou dimensión n $(= dim(W))$, e para deixar claro o espazo vectorial ao que asociamos a forma cuadrática, tamén nos referiremos a q como (W, q).

Nótese que se $b\colon W \times W \to K$ é unha forma bilinear simétrica, entón a aplicación $q_b\colon W \to K, x \mapsto q_b(x) := b(x,x)$ é unha forma cuadrática. Deste xeito

$$b_{q_b}(x,y) = b(x,y)$$
$$q_{b_q}(x) = q(x)$$

e así podemos identificar formas cuadráticas con formas bilineares simétricas.

Observación 1.1.3 Se $\{e_1, ..., e_n\}$ é unha base de W e $x = \sum_{i=1}^{n} x_i e_i \in W$, podemos traballar con q nas coordenadas $(x_1, ..., x_n)$, pois tense que a matriz de q respecto desta base será $A = (a_{ij}) = (b_q(e_i, e_j))$; e se P é unha matriz de cambio de base, polo tanto invertible, a matriz de q respecto da nova base será $A' = PAP^t$. Nótese que $det(A') = det(A)det(P)^2$, polo que o discriminante de q está determinado salvo multiplicar por un elemento de $(K^*)^2$, é dicir podemos velo como un elemento de $K^*/(K^*)^2$.

Definición 1.1.4 Se (W, q) é unha forma cuadrática, dous vectores $x, y \in W$ son ortogonais se $b_q(x,y) = 0$. Denótase $x \perp y$. Dous subespazos $U, V \subset W$ son ortogonais se $u \perp v$ para todo $u \in U$ e $v \in V$. Chámase ortogonal de $U \subset W$ a $U^\perp := \{w \in W\colon w \perp u \quad \forall u \in U\}$, que claramente é un subespazo vectorial de W pola bilinearidade de b_q. Chamaremos radical de q a $rad(q) := W^\perp$. Dise que q é non singular (ou non dexenerada, regular) se $rad(q) = 0$.

Observación 1.1.5 Se (W, q) é unha forma cuadrática, temos unha forma cuadrática inducida por q $(W/rad(q), \overline{q})$ que é non singular. Se $U \subset W$ é un subespazo vectorial, $(U, q_{|U})$ é unha forma cuadrática.

Definición 1.1.6 Sexan $U_1, ..., U_m$ subespazos vectoriais de W. Dicimos que W é suma directa ortogonal dos U_i se estes son ortogonais dous a dous e W é suma directa deles. En tal caso escribiremos

$$W = U_1 \perp U_2 \perp ... \perp U_m$$

Observación 1.1.7 Se $x \in W$, $x = x_1 + ... + x_m$, $x_i \in U_i$, entón

$$q(x) = q_1(x_1) + ... + q_m(x_m)$$

onde $q_i = q_{|U_i}$. Reciprocamente, se temos unha familia de formas cuadráticas (U_i, q_i), $i = 1, ..., m$ e $W = \bigoplus_{i=1}^m U_i$, construímos a forma cuadrática

$$(q_1 + ... + q_m)(x_1, ..., x_m) := q_1(x_1) + ... + q_m(x_m)$$

denominada suma directa das formas cuadráticas q_i. Tense $W = \perp_{i=1}^m U_i$.

Lema 1.1.8 Sexa (W, q) unha forma cuadrática, $U \subset W$ un subespazo vectorial. Entón:

(I) $rad(q_{|U}) = U \cap U^\perp = rad(q_{|U^\perp})$ e $(U^\perp)^\perp = U$.

(II) Se $(U, q_{|U})$ é non singular, entón $W = U \perp U^\perp$, e así $dim(q) = dim(q_{|U}) + dim(q_{|U^\perp})$.

Demostración. (I) É claro.

(II) Sexa U^* o espazo vectorial dual de U. A aplicación lineal $B\colon U \to U^*, u \mapsto b_q(u, \cdot)$ ten núcleo $rad(q_{|U}) = 0$. Así, é un isomorfismo. Sexa $\{e_1, ..., e_n\}$ unha base de U, $\{e_1^*, ..., e_n^*\}$ a súa base dual, $f_i = B^{-1}(e_i^*)$. Entón $\{f_1, ..., f_n\}$ é unha base de U e $b_q(f_i, e_j) = b_q(f_i)(e_j) = e_i^*(e_j) = \delta_{ij}$ (delta de Kronecker). Así, para todo $w \in W$, $w = x + y$ con $x = \sum_{i=1}^n b_q(w, e_i) f_i$, $y = w - x = w - \sum_{i=1}^n b_q(w, e_i) f_i$, onde claramente $x \in U$, e como $b_q(y, e_j) = b_q(w, e_j) - b_q(w, e_j) = 0 \quad \forall j$, temos $y \in U^\perp$. Así $W = U + U^\perp$. Por outra parte, $U \cap U^\perp = 0$ por (I).

■

Definición 1.1.9 Unha base $\{e_1, ..., e_n\}$ dunha forma cuadrática (W, q) dise ortogonal se todos os seus elementos son ortogonais dous a dous (i.e., se $b_q(e_i, e_j) = 0 \; \forall i \; \forall j$).

Observación 1.1.10 A matriz dunha forma cuadrática respecto dunha base ortogonal $\{e_1, ..., e_n\}$ é diagonal e, se $x = \sum_{i=1}^n x_i e_i$, a expresión de q nesta base é $q(x) = a_1 x_1^2 + ... + a_n x_n^2$ onde $(a_1, ..., a_n)$ é a diagonal da matriz.

Teorema 1.1.11 Toda forma cuadrática (W, q) ten unha base ortogonal.

Demostración. Se $q = 0$, todas as bases de W son ortogonais. Supoñamos que $q \neq 0$. Usaremos indución en $n = dim(W)$. Se $n = 0$ é trivial. Supoñamos o resultado certo para espazos de dimensión $n-1$. Tomamos un elemento $e_1 \in W$ tal que $q(e_1) = b_q(e_1, e_1) \neq 0$. Tense $dim(\langle e_1 \rangle^\perp) = n - 1$ e como consecuencia do *lema* ***1.1.8*** (II), $W = \langle e_1 \rangle \perp \langle e_1 \rangle^\perp$. Por hipótese de indución, $\langle e_1 \rangle^\perp$ ten unha base ortogonal $\{e_2, ..., e_n\}$. Así, $\{e_1, e_2, ..., e_n\}$ é unha base ortogonal de W. ■

Observación 1.1.12 Do *teorema* ***1.1.11*** e da *observación* ***1.1.3*** deducimos que unha forma cuadrática é non singular se, e só se, o seu discriminante é non nulo.

Definición 1.1.13 Dúas bases ortogonais $E = \{e_1, ..., e_n\}$ e $E' = \{e'_1, ..., e'_n\}$ dunha forma cuadrática (W, q) dinse contiguas se teñen algún elemento en común (i.e., se existen i e j tales que $e_i = e'_j$).

Teorema 1.1.14 Sexa (W, q) unha forma cuadrática non singular de dimensión ≥ 3, e sexan $E = \{e_1, ..., e_n\}$ e $E' = \{e'_1, ..., e'_n\}$ dúas bases ortogonais de W. Existe unha sucesión finita E^0, E^1, ..., E^m de bases ortogonais de W tales que $E^0 = E$, $E^m = E'$ e E^i é contigua a E^{i+1} para $0 \leq i < m$.

Demostración. Distinguiremos 3 casos

(I) $b_q(e_1, e_1)b_q(e'_1, e'_1) - (b_q(e_1, e'_1))^2 \neq 0$. Entón e_1 e e'_1 non son colineares e o plano $P = \langle e_1, e'_1 \rangle$ é non singular. Logo existen v_2, v'_2 tales que

$$P = \langle e_1 \rangle \perp \langle v_2 \rangle = \langle e'_1 \rangle \perp \langle v'_2 \rangle$$

Posto que P é non singular, polo *lema* ***1.1.8*** (II), temos $W = P \perp P^\perp$. Sexa $\{v'_3, ..., v'_n\}$ unha base ortogonal de $P^\perp$. Obtemos así a cadea de bases ortogonais contiguas de E a E' (recordemos que $n \geq 3$)

$$E \to \{e_1, v_2, v_3, ..., v_n\} \to \{e'_1, v'_2, v_3, ..., v_n\} \to E'$$

(II) $b_q(e_1, e_1)b_q(e_2, e_2) - (b_q(e_1, e_2))^2 \neq 0$. A mesma proba, substituíndo e'_1 por e'_2.

(III) $b_q(e_1,e_1)b_q(e_i',e_i') - (b_q(e_1,e_i'))^2 = 0$, para $i = 1,2$.

Probaremos primeiro que existe $k \in K$ tal que $\overline{e_k} := e_1' + ke_2'$ é non isótropo e xera, xunto con e_1, un plano non singular. Enumeraremos os casos non permitidos de k.

Tense $q(\overline{e_k}) = b_q(\overline{e_k},\overline{e_k}) = b_q(e_1',e_1') + k^2 b_q(e_2',e_2')$; logo e_k é non isotrópico se e só se $k^2 \neq -\frac{b_q(e_1',e_1')}{b_q(e_2',e_2')}$. En segundo lugar, pola *observación* ***1.1.12***, o plano

$$\langle e_1\rangle + \langle \overline{e_k}\rangle$$

é non singular se e só se $b_q(e_1,e_1)b_q(\overline{e_k},\overline{e_k}) - (b_q(e_1,\overline{e_k}))^2 \neq 0$, pois este é o seu discriminante. Usando as propiedades de b_q isto redúcese a que se verifique $-2kb_q(e_1,e_1')b_q(e_1,e_2') \neq 0$. Ademais, como tamén por hipótese $b_q(e_1,e_i') \neq 0$ para $i = 1,2$, isto é equivalente a $k \neq 0$. Logo témolo probado para corpos K con máis de tres elementos. Queda o corpo de 3 elementos (recordemos que a característica de K é $\neq 2$), pero para este caso é fácil ver que $k = 1$ é un valor válido. En efecto, temos que comprobar polo que acabamos de ver

$$(i)\ \ \frac{b_q(e_1',e_1')}{b_q(e_2',e_2')} \neq -1 \qquad (ii)\ \ -2b_q(e_1,e_1')b_q(e_1,e_2') \neq 0$$

Temos neste caso (III) que $b_q(e_1,e_1)b_q(e_1',e_1') = b_q(e_1,e_1')^2$ e $b_q(e_1,e_1)b_q(e_2',e_2') = b_q(e_1,e_2')^2$. Dividindo a primeira igualdade pola segunda obtemos

$$\frac{b_q(e_1',e_1')}{b_q(e_2',e_2')} = \frac{b_q(e_1,e_1')^2}{b_q(e_1,e_2')^2} = \Big(\frac{b_q(e_1,e_1')}{b_q(e_1,e_2')}\Big)^2$$

e este valor é $\neq -1$ en $\mathbb{Z}/3\mathbb{Z}$, pois -1 non é un cadrado neste corpo. Isto proba (i). Para ver (ii), como K é un corpo de característica $\neq 2$, é suficiente ver que $b_q(e_1,e_1') \neq 0 \neq b_q(e_1,e_2')$. Pero $b_q(e_1,e_1')^2 = b_q(e_1,e_1)b_q(e_1',e_1') \neq 0$ pois e_1 e e_1' non son isótropos, e así $b_q(e_1,e_1') \neq 0$. De forma análoga vese que $b_q(e_1,e_2') \neq 0$.

Agora ben, tomemos $\overline{e_k}$ tal que k estea nalgunha das condicións anteriores. Posto que $\overline{e_k}$ é non isótropo existe v_2 tal que $\{\overline{e_k}, v_2\}$ forma unha base ortogonal de $\langle e_1', e_2'\rangle$. Poñamos

$$E'' = \{\overline{e_k}, v_2, e_3', \ldots, e_n'\}$$

que é claramente unha base ortogonal de W. Posto que $\langle e_1, \overline{e_k}\rangle$ é un plano non singular por construción, usando $\overline{e_k}$ no lugar de e_1' na proba do caso (I), vemos que existe unha cadea de bases ortogonais contiguas de E a E''. Posto que $n \geq 3$, E'' é contigua a E', e séguese o resultado.

■

Definición 1.1.15 Dicimos que un elemento x dunha forma cuadrática (W, q) é isótropo se $q(x) = 0$. Un subespazo U de V chámase isótropo se todos os seus elementos son isótropos. En este caso $q_{|U} = 0$ e así $b_{q_{|U}} = 0$. Dicimos que (W, q) é un plano hiperbólico se W ten unha base formada por dous elementos isótropos x, y tales que $b_q(x, y) \neq 0$.

Observación 1.1.16 Na definición de plano hiperbólico podemos supoñer que $b_q(x, y) = 1$ con tal de multiplicar y por $(b_q(x, y))^{-1}$ previamente.

Proposición 1.1.17 Sexa x un elemento isótropo $\neq 0$ dunha forma cuadrática non singular (W, q). Entón existe un subespazo U de W que é un plano hiperbólico e contén a x.

Demostración. Posto que q é non singular, existe un elemento $z \in W$ tal que $b_q(x, z) = 1$. O elemento $y = 2z - b_q(z, z)x$ é isótropo e $b_q(x, y) = 2$. Así, o subespazo $U = \langle x, y\rangle$ ten a propiedade buscada. ■

Corolario 1.1.18 Se (W, q) é unha forma cuadrática non singular que contén un elemento isótropo $\neq 0$, tense $q(W) = K$.

Demostración. Sexa $k \in K$. Vexamos que existe $w \in W$ tal que $q(w) = k$. En vista da proposición anterior, é suficiente con probalo para o caso no que (W, q) é un plano hiperbólico con base formada por dous elementos x, y isótropos tales que $b_q(x, y) = 1$. Tomando $w = x + \frac{k}{2}y$, temos

$$q(x + \frac{k}{2}y) = b_q(x + \frac{k}{2}y, x + \frac{k}{2}y) = b_q(x, x) + 2(\frac{k}{2})b_q(x, y) + (\frac{k}{2})^2 b_q(y, y) = k$$

■

1.2. Teoremas de Witt

Definición 1.2.1 Sexan dúas formas cuadráticas (W,q), (W',q'). Dicimos que unha aplicación linear inxectiva $\sigma\colon W \to W'$ é unha isometría se verifica

$$b_{q'}(\sigma(x),\sigma(y)) = b_q(x,y) \quad \forall (x,y) \in W \times W$$

q e q' diranse isométricas ou equivalentes, e escribiremos $q \sim q'$, se existe unha isometría $\sigma\colon W \to W'$ bixectiva.

Observación 1.2.2 A definición de plano hiperbólico (W,q) é equivalente a que q sexa unha forma cuadrática de dimensión 2 tal que $q(x_1,x_2) \sim x_1x_2 \sim x_1^2 - x_2^2$. Para comprobar a segunda equivalencia basta tomar a isometría bixectiva $\sigma(x_1,x_2) = (\frac{1}{\sqrt{2}}(x_1+x_2), \frac{1}{\sqrt{2}}(x_1-x_2))$.

Proposición 1.2.3 Sexan (W,q) e (W',q') dúas formas cuadráticas non singulares. Se $\sigma\colon W \to W'$ é unha aplicación linear tal que $b_{q'}(\sigma(x),\sigma(y)) = b_q(x,y)\ \forall (x,y) \in W \times W$, entón σ é unha isometría.

Demostración. Supoñamos que $x \in W$ é tal que $\sigma(x) = 0$. Entón para todo $y \in W'$, $b_q(x,y) = b_{q'}(\sigma(x),\sigma(y)) = 0$ e así $x = 0$, xa que q é non singular. ■

Lema 1.2.4 Sexan (W,q), (W',q') dúas formas cuadráticas non singulares e U un subespazo vectorial de W. Supoñamos que existe unha isometría $\sigma\colon U \to W'$. Se $q_{|U}$ é singular, podemos estender σ a unha isometría $\sigma_1\colon U_1 \to W'$, onde U é un hiperplano de U_1.

Demostración. Sexan U^* o espazo vectorial dual de U e $x \in rad(q_{|U})$ non nulo. Podemos tomar $f \in U^*$ de forma que $f(x) = 1$. Doutra banda, a aplicación lineal $B\colon W \to W^*, w \mapsto b_q(w,\cdot)$ é un isomorfismo, tal e como se ve na demostración do *lema 1.1.8*, xa que q é non singular. Logo existe $y \in W$ tal que $f(u) = b_q(y,u)$ para todo $u \in U$. Tomemos $z = y - \frac{1}{2}b_q(y,y)x$. Así $b_q(z,z) = 0$ e $b_q(y,u) = b_q(z,u) = f(u)$ para todo $u \in U$. Poñemos $U_1 := U \bigoplus \langle z \rangle$, que claramente contén a U como hiperplano xa que en caso contrario, $z \in U$ e $f(x) = b_q(z,x) = 0$, pois $x \in rad(q_{|U})$, o que é unha contradición. Podemos aplicar o mesmo procedemento a $U' = \sigma(U), x' = \sigma(x)$ e $f' = f \circ \sigma_{|U}^{-1}$, onde $\sigma_{|U}\colon U \to U'$, obtendo $z' \in W'$ e $U_1' := U' \bigoplus \langle z' \rangle$. É claro que a aplicación lineal $\sigma_1\colon U_1 \to W'$ que coincide con σ en U e envía z en z' é unha isometría

bixectiva de U_1 en U_1' (pois z, z' escolléronse isótropos e se $u' = \sigma(u)$, tense $b_{q'}(z,u) = f'(u') = f(u) = b_q(z,u)$). ■

Teorema 1.2.5 (Teorema de Witt). Sexan (W,q), (W',q') dúas formas cuadráticas non singulares isométricas e U un subespazo vectorial de W. Calquera isometría $\sigma\colon U \to W'$ pode ser estendida a unha isometría bixectiva de W en W'.

Demostración. Posto que q e q' son isométricas, podemos asumir que $(W,q) = (W',q')$. Usaremos indución en $dim(q_{|U})$. Polo *lema* **1.2.4** só temos que preocuparnos do caso U singular.
Se $dim(q_{|U}) = 1$, U está xerado por un elemento x non isótropo; tomamos $y = \sigma(x)$ e tense $b_q(x,x) = b_q(y,y)$ pola propiedade da isometría. Podemos escoller $k = 1$ ou $k = -1$ de forma que $x + ky$ é non isótropo. En caso contrario

$$\begin{aligned} 0 = q(x+y) &= b_q(x+y, x+y) = b_q(x,x) + 2b_q(x,y) + b_q(y,y) \\ &= 2b_q(x,x) + 2b_q(x,y) \\ 0 = q(x-y) &= b_q(x-y, x-y) = b_q(x,x) - 2b_q(x,y) + b_q(y,y) \\ &= 2b_q(x,x) - 2b_q(x,y) \end{aligned}$$

e teríase $q(x) = b_q(x,x) = 0$, absurdo. Poñamos $z = x + ky$ para tal elección de k. Polo *lema* **1.1.8** *(II)*, tense $W = \langle z \rangle \perp \langle z \rangle^\perp$. Sexa $f\colon W \to W$ a simetría con respecto a $\langle z \rangle^\perp$ (que é unha isometría), definida por $f(w) = w - 2(\frac{b_q(w,z)}{b_q(z,z)})z$, que leva z en $-z$ e é a identidade en $\langle z \rangle^\perp$. Posto que $b_q(x - ky, z) = b_q(x,x) - b_q(y,y) = 0$ deducimos que $x - ky \in \langle z \rangle^\perp$ e así

$$\begin{aligned} f(x) - kf(y) &= f(x - ky) = x - ky \\ f(x) + kf(y) &= f(x + ky) = f(z) = -z = -x - ky \end{aligned}$$

co que $f(x) = -ky$ e así $-kf$ é unha estensión de σ.
Se $dim(q_{|U}) > 1$, descompoñemos U na forma $U_1 \perp U_2$ con $U_1, U_2 \neq 0$. Por indución, sabemos que a restrición $\sigma_1\colon U_1 \to W$ de σ a U_1 esténdese a unha isometría bixectiva $\tau_1\colon W \to W$. Se $x \in U_1$ e $z \in U_2$, temos

$$b_q(x, \tau_1^{-1}(\sigma(z))) = b_q(\tau_1(x), \sigma(z)) = b_q(\sigma(x), \sigma(z)) = b_q(x,z) = 0$$

resultando en que $\tau_1^{-1} \circ \sigma(U_2) \subset U_1^\perp$. Como $U_2 \subset U_1^\perp$, pola hipótese de indución na dimensión, a isometría $\tau_1^{-1} \circ \sigma$ restrinxida a U_2 esténdese a unha

isometría bixectiva $\tau_2 \colon U_1^\perp \to U_1^\perp$, que en particular verifica $\tau_1 \circ \tau_2(x) = \sigma(x)$ para todo $x \in U_2$. Está claro que se definimos $\tau \colon W \to W$ como σ en U_1 e como $\tau_1 \circ \tau_2$ en $U_1^\perp$, logo τ é unha isometría bixectiva que estende σ. ■

Corolario 1.2.6 Sexa (W, q) unha forma cuadrática non singular e sexan U, U' dous subespazos vectoriais de W. Se U e U' son isométricos, entón $U^\perp$ e $U'^\perp$ son isométricos.

Demostración. Usando o *teorema* **1.2.5**, estendemos unha isometría entre U e U' a unha isometría bixectiva entre W e W' e restrinximos a $U^\perp$ e $U'^\perp$. ■

Definición 1.2.7 Diremos que unha forma cuadrática (W, q) representa un elemento a de K se existe $x \in W$, $x \neq 0$, tal que $q(x) = a$. En particular, q representa 0 se e só se W ten un elemento isótropo non nulo.

Sexan (W, q) e (W', q') dúas formas cuadráticas de dimensións n e m respectivamente. Denotaremos por $q + q'$ á forma cuadrática

$$(q + q')(x_1, ..., x_{n+m}) := q(x_1, ..., x_n) + q'(x_{n+1}, ..., x_{n+m})$$

de dimensión $n + m$, que estará asociada ao espazo $W \perp W'$. Analogamente, escribiremos $q - q'$ para denotar $q + (-q')$.

Proposición 1.2.8 Se q é unha forma cuadrática non singular que representa 0, existen unha forma cuadrática hiperbólica q_2 e unha forma cuadrática non singular q' tales que $q \sim q_2 + q'$. Ademais, q representa todos os elementos de K.

Demostración. Isto é a proposición **1.1.17** e o *corolario* **1.1.18**. O feito de que q' sexa non singular séguese do *lema* **1.1.8**. ■

Observación 1.2.9 Deducimos da *proposición* **1.2.8** que unha forma cuadrática non singular de rango 2 e discriminante d, representa cero se e só se $-d = 1$ en $K^*/(K^*)^2$ (i.e, $-d$ é un cadrado). Isto tamén é fácil de ver directamente: $a_1x_1^2 + a_2x_2^2 = 0$ con $x_1 \neq 0 \neq x_2 \Leftrightarrow -\frac{a_1}{a_2} = (\frac{x_1}{x_2})^2 \Leftrightarrow -\frac{a_1}{a_2}$ é un cadrado. Pero $-d = -a_1a_2 = \frac{(-a_1)}{a_2}a_2^2 \equiv -\frac{a_1}{a_2} \pmod{(K^*)^2}$.

Corolario 1.2.10 Sexa (W, q) unha forma cuadrática non singular de dimensión $n - 1$ e sexa $a \in K^*$. As seguintes afirmacións son equivalentes

(I) q representa a.

(II) $q \sim q' + az^2$, onde q' é unha forma cuadrática en $n-2$ variables.

(III) A forma $q - az^2$ representa 0.

Demostración. $(I) \Leftrightarrow (II)$. É claro que $(II) \Rightarrow (I)$. Reciprocamente, se q representa a, existe un elemento $x \in W$ tal que $b_q(x,x) = a$, e así $W = \langle x \rangle \perp \langle x \rangle^\perp$ implica $q \sim q' + az^2$, onde q' é unha forma cuadrática asociada a unha base de $\langle x \rangle^\perp$.
$(I) \Rightarrow (III)$. É trivial, tomando $z = 1$ e como $(x_1, ..., x_{n-1})$ unha representación de a.
$(III) \Rightarrow (I)$. Se $q - az^2$ ten un cero non trivial $(\alpha_1, ..., \alpha_{n-1}, \alpha_0)$, temos ou ben $\alpha_0 = 0$ caso no que q representa cero e polo tanto tamén a, ou ben $\alpha_0 \neq 0$ caso no que $q(\frac{\alpha_1}{\alpha_0}, ..., \frac{\alpha_{n-1}}{\alpha_0}) = a$. ■

Corolario 1.2.11 Sexan (W, q) e (W', q') dúas formas cuadráticas non nulas non singulares. As seguintes afirmacións son equivalentes

(I) $q - q'$ representa 0.

(II) Existe $a \in K^*$ tal que está representado por q e por q'.

(III) Existe $a \in K^*$ tal que $q - az^2$ e $q' - az^2$ representan 0.

Demostración. $(I) \Leftrightarrow (II)$. $(II) \Rightarrow (I)$ é trivial. Reciprocamente, vexamos $(I) \Rightarrow (II)$. Se $q - q'$ representa 0, existen $x \in W$ e $y \in W'$ tales que $q(x) = q'(y) = a$. Se $a \neq 0$, está probado. Se $a = 0$, posto que x ou y son $\neq 0$ ao menos unha da formas cuadráticas, poñamos q, representa 0; logo polo *corolario* ***1.1.18*** representa todos os valores de K e en particular os valores non nulos tomados por q'.
$(II) \Leftrightarrow (III)$ Séguese do *corolario* ***1.2.10***. ■

Teorema 1.2.12 (Teorema de cancelación de Witt). Sexan $f_1 = q_1 + q_1'$ e $f_2 = q_2 + q_2'$ dúas formas cuadráticas non singulares. Se $f_1 \sim f_2$ e $q_1 \sim q_2$ entón $q_1' \sim q_2'$.

Demostración. É o *corolario* ***1.2.6***. ■

Corolario 1.2.13 Se q é unha forma cuadrática non singular, entón

$$q \sim q_1 + ... + q_m + q'$$

onde $q_1, ..., q_m$ son hiperbólicas e q' non representa 0. Esta descomposición é única salvo equivalencia.

Demostración. A existencia séguese da *proposición* **1.2.8**. Probemos a unicidade. Sexan

$$q \sim \sum_{i=1}^{m} q_i + q' \sim \sum_{i=1}^{m'} q_i' + q''$$

e asumamos que, por exemplo $m' \leq m$. Posto que todas as formas cuadráticas hiperbólicas son equivalentes o *teorema* **1.2.12** implica que $\sum_{i=1}^{m-m'} q_i + q' \sim q''$, o que é unha contradición se $m \neq m'$, xa que q'' non representa cero mentres que unha forma cuadrática hiperbólica si o fai. Así $m = m'$, $q_i = q_i' \; \forall i = 1, ..., m$ (xa que ambas son planos hiperbólicos), e $q' \sim q''$ polo *teorema* **1.2.12** de novo. ■

Capítulo 2

Corpos p–ádicos

2.1. Introdución

Sexa p un número primo. Se n é un número natural, existe unha expansión "p–ádica"

$$n = a_0 + a_1 p + ... + a_r p^r$$

con $0 \leq a_i < p$, e onde r e os enteiros a_i son únicos. Sexa agora $m \neq 0$ outro número natural, e poñamos $m = m' p^t$ con $(m', p) = 1$. Sexa

$$m' = b_0 + b_1 p + ... + b_s p^s$$

con $0 \leq b_i < p$. Temos $b_0 \neq 0$ xa que $p \nmid m'$, e

$$\frac{n}{m'} = \frac{a_0 + a_1 p + ... + a_r p^r}{b_0 + b_1 p + ... + b_s p^s}$$

Se pensamos as expresións anteriores $\sum_{i=0}^{r} a_i p^i$, $\sum_{k=0}^{s} b_i p^i$ non coma polinomios senón coma series formais en p, entón $b_0 + b_1 p + ... + b_s p^s$ ten inverso (xa que $b_0 \neq 0$) e así

$$\frac{n}{m'} = \sum_{i \geq 0} c_i p^i \quad 0 \leq c_i < p, \forall i$$

Entón o número racional $\frac{n}{m} = \frac{n}{m'} p^{-t}$ o podemos pensar como unha serie de Laurent

$$\sum_{i \geq -t} c_{i+t} p^i$$

Esta é unha das ideas que levaron a considerar os números p–ádicos. Imos a definir o corpo $\mathbb{Q}_p$, que se pode pensar como o conxunto destas expresións

$\sum_{i\geq -t} a_i p^i$ con enteiros $0 \leq a_i < p$ (pero que tamén ten outras interpretacións importantes[1]). Necesitamos tamén introducir a topoloxía axeitada que nos proporcione unha "converxencia" destas expresións.

2.2. Números p–ádicos

Definición 2.2.1 Se $\{A_{n+1} \xrightarrow{\varphi_{n+1}} A_n\}_{n\geq 1}$ é unha familia de aplicacións de conxuntos, defínese o seu *límite proxectivo* como

$$\varprojlim A_n := \left\{ (a_n)_{n\geq 1} \in \prod_{n\geq 1} A_n \colon \varphi_{m+1}(a_{m+1}) = a_m, \forall m \geq 1 \right\}$$

Se os A_n son grupos (resp. aneis conmutativos) e os φ_n homomorfismos de grupos (resp. de aneis) é inmediato comprobar que $\varprojlim A_n$ é un subgrupo (resp. anel) de $\prod_{n\geq 1} A_n$.

Definición 2.2.2 Se A é un anel, unha sucesión de A–módulos e homomorfismos de A–módulos

$$\ldots \to M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \to \ldots$$

dise *exacta* se $\operatorname{Im}(f_{n+1}) = \ker(f_n), \forall n$. Por exemplo:

(I) $0 \to M' \xrightarrow{f} M$ é exacta $\Leftrightarrow$ f é inxectiva.

(II) $M \xrightarrow{g} M'' \to 0$ é exacta $\Leftrightarrow$ g é sobrexectiva.

Unha *sucesión exacta corta* é unha sucesión exacta

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

Unha tal sucesión exacta induce un isomorfismo $M/\operatorname{Im} f = M/\ker g \simeq M''$.

Lema 2.2.3 Sexa $0 \to \{A'_n\}_{n\geq 1} \to \{A_n\}_{n\geq 1} \to \{A''_n\}_{n\geq 1} \to 0$ unha sucesión exacta de sistemas proxectivos de grupos abelianos, é dicir, para cada n tense unha

[1] Por exemplo, $\mathbb{Q}_p$ é a completación de $\mathbb{Q}$ respecto da métrica p–ádica.

sucesión exacta de grupos abelianos

$$0 \to A'_n \xrightarrow{\alpha_n} A_n \xrightarrow{\beta_n} A''_n \to 0$$

e diagramas conmutativos

$$\begin{array}{ccccc} A'_{n+1} & \xrightarrow{\alpha_{n+1}} & A_{n+1} & \xrightarrow{\beta_{n+1}} & A''_{n+1} \\ \downarrow{\scriptstyle \varphi'_{n+1}} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi''_{n+1}} \\ A'_n & \xrightarrow{\alpha_n} & A_n & \xrightarrow{\beta_n} & A''_n \end{array}$$

Supoñamos φ'_n sobrexectivo $\forall n$. Entón tense unha sucesión exacta de grupos

$$0 \to \varprojlim A'_n \to \varprojlim A_n \to \varprojlim A''_n \to 0$$

Demostración. Primeiramente, nótese que se $\tilde{\alpha}$ e $\tilde{\beta}$ son os homomorfismos

$$\tilde{\alpha} = \prod_{n\geq 1} \alpha_n \colon \prod_{n\geq 1} A'_n \to \prod_{n\geq 1} A_n, (a'_n) \mapsto (\alpha_n(a'_n))$$

$$\tilde{\beta} = \prod_{n\geq 1} \beta_n \colon \prod_{n\geq 1} A_n \to \prod_{n\geq 1} A''_n, (a_n) \mapsto (\beta_n(a_n))$$

entón α e β son as restricións de $\tilde{\alpha}$ e $\tilde{\beta}$ a $\varprojlim A'_n$ e $\varprojlim A_n$, respectivamente (e son homomorfismos).

É inmediato ver que $\forall m \geq 1, \forall (a_n) \in \varprojlim A_n,\ \varphi_{m+1}(\alpha_{m+1}(a_{m+1})) = \alpha_m(\varphi'_{m+1}(a_{m+1})) = \alpha_m(a_m) \Rightarrow (\alpha_n(a_n)) \in \varprojlim A_n \Rightarrow \operatorname{Im}\alpha \subset \varprojlim A_n$. Analogamente $\operatorname{Im}\beta \subset \varprojlim A''_n$.

– $\operatorname{Im}\alpha = \ker\beta$: tense $(a_n) \in \ker\beta \Leftrightarrow \beta((a_n)) = (\beta_n(a_n)) = (0) \Leftrightarrow \beta_n(a_n) = 0, \forall n \Leftrightarrow (a_n) \in \ker\beta_n = \operatorname{Im}\alpha_n, \forall n \Leftrightarrow (a_n) \in \operatorname{Im}\alpha$.

– α é inxectiva: $(\alpha_n(a'_n)) = (\alpha_n(b'_n)) \Leftrightarrow \alpha_n(a'_n) = \alpha_n(b'_n), \forall n \Rightarrow a'_n = b'_n, \forall n \Rightarrow (a'_n) = (b'_n)$.

– β é sobrexectiva: Sexa $(a''_n) \in \varprojlim A''_n$. Imos construír $(a_n) \in \varprojlim A_n$ tal que $\beta_n(a_n) = a''_n, \forall n$. Farémolo construíndo sucesivamente

$$\begin{aligned} a_1 &\colon \beta_1(a_1) = a''_1 \\ a_i &\colon \beta_i(a_i) = a'_i \text{ e } \varphi(a_i) = a_{i-1}, i \geq 2 \end{aligned}$$

Sexa $a_1 \in A_1 \colon \beta_1(a_1) = a''_1$ (existe por ser β_1 sobrexectiva) e sexa $\tilde{a_2} \in A_2 \colon \beta_2(\tilde{a_2}) = a''_2$. Temos

$$\beta_1(\varphi_2(\tilde{a_2})) = \varphi''_2(\beta_2(\tilde{a_2})) = \varphi''_2(a''_2) = a''_1 = \beta_1(a_1)$$

Así,

$$\beta_1(a_1 - \varphi_2(\tilde{a_2})) = 0$$

Como ademais $\ker \beta_1 = \operatorname{Im} \alpha_1$, $\exists a'_1 \in A'_1$ con $\alpha_1(a'_1) = a_1 - \varphi_2(\tilde{a_2})$. Como φ'_2 é sobre, $\exists a'_2 \in A'_2 \colon \varphi'_2(a'_2) = a'_1$. Entón

$$a_2 := \tilde{a_2} + \alpha_2(a'_2)$$

verifica

$$\varphi_2(a_2) = \varphi_2(\tilde{a_2}) + (\varphi_2 \circ \alpha_2)(a'_2) = a_1 - \alpha_1(a'_1) + (\alpha_1 \circ \varphi'_2(a'_2)) = a_1$$

$$\beta_2(a_2) = \beta_2(\tilde{a_2}) + \beta_2(\alpha_2(a'_2)) = a''_2 + 0 = a''_2$$

Os demais termos constrúense de forma análoga.

■

Definición 2.2.4 Chámase *anel dos enteiros p–ádicos* ao anel (conmutativo)

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

onde os homomorfismos $\varphi_{n+1} \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ son os homomorfismos de paso ao cociente (polo ideal $p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$ de $\mathbb{Z}/p^{n+1}\mathbb{Z}$).

Consideraremos cada $\mathbb{Z}/p^n\mathbb{Z}$ como espazo topolóxico coa topoloxía discreta e $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ coa topoloxía produto (topoloxía de Tychonoff) destas topoloxías[2]. Así, o subconxunto $\mathbb{Z}_p$ é un espazo topolóxico.

Proposición 2.2.5 $\mathbb{Z}_p$ é compacto.

Demostración. Como os $\mathbb{Z}/p^n\mathbb{Z}$ son compactos (son finitos coma conxuntos), $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ é compacto polo teorema de Tychonoff. Así pois, é suficiente demostrar que $\mathbb{Z}_p$ é pechado en $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$. Sexa $(a_n) \in (\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}) \setminus \mathbb{Z}_p$. Entón existe t natural tal que $\varphi_{t+1}(a_{t+1}) \neq a_t$. Así o aberto

$$\ldots \times \mathbb{Z}/p^{t+3}\mathbb{Z} \times \mathbb{Z}/p^{t+2}\mathbb{Z} \times \{a_{t+1}\} \times \{a_t\} \times \ldots \times \{a_1\}$$

contén a (a_n) e non corta a $\mathbb{Z}_p$. ■

[2] É dicir, unha base de abertos son os produtos de abertos, sendo estes abertos todo o espazo $\mathbb{Z}/p^n\mathbb{Z}$ para todo n salvo un número finito deles.

Lema 2.2.6 Sexa $\varepsilon_t\colon \mathbb{Z}_p \to \mathbb{Z}/p^t\mathbb{Z}$ a restrición a $\mathbb{Z}_p$ da proxección canónica t–ésima $\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^t\mathbb{Z}$. Tense unha sucesión exacta

$$0 \to \mathbb{Z}_p \xrightarrow{\cdot p^t} \mathbb{Z}_p \xrightarrow{\varepsilon_t} \mathbb{Z}/p^t\mathbb{Z} \to 0$$

(onde $\cdot p^t$ é a multiplicación por p^t no anel $\mathbb{Z}_p$) e así $\mathbb{Z}_p/p^t\mathbb{Z}_p \simeq \mathbb{Z}/p^t\mathbb{Z}$.

Demostración. Sexa $(\overline{a_n}) \in \mathbb{Z}_p$ tal que $(\overline{a_n}p) = 0$, é dicir, $\overline{a_n}p = 0 \in \mathbb{Z}/p^n\mathbb{Z}$ $\forall n \geq 1$, ou equivalentemente $p^n \mid a_n p$ $\forall n$. Así $a_n = p^{n-1}b_n$ con b_n enteiro e en particular $\overline{a_{n-1}} = \varphi(\overline{a_n}) = p^{n-1}\varphi(\overline{b_n}) = 0 \in \mathbb{Z}/p^{n-1}\mathbb{Z}$. Como isto é certo para todo n, $(\overline{a_n}) = 0$. Así a multiplicación por p é inxectiva en $\mathbb{Z}_p$ e polo tanto a multiplicación por p^t tamén o é (composición de inxectivas).
Vexamos agora que $\operatorname{Im}\cdot p^t = \ker\varepsilon_t$. É claro que $\operatorname{Im}\cdot p^t = p^t\mathbb{Z}_p \subset \ker\varepsilon_t$. Reciprocamente, sexa $(\overline{a_n}) \in \ker\varepsilon_t$, é dicir, $\overline{a_t} = 0 \in \mathbb{Z}/p^t\mathbb{Z}$. Sexa $m \geq t$. Temos que $\varphi_{t+1}\circ\varphi_{t+2}\circ\ldots\circ\varphi_m(\overline{a_m}) = a_m + p^t\mathbb{Z} = a_t + p^t\mathbb{Z} = 0$ e así existe $b_{m-t} \in \mathbb{N}$ tal que $\overline{a_m} = p^t\overline{b_{m-t}} \in \mathbb{Z}/p^m\mathbb{Z}$. Ademais este b_{m-t} é único módulo p^{m-t} (xa que si $p^t b'_{m-t} \equiv p^t b_{m-t} \pmod{p^m}$, entón $p^m \mid p^t(b'_{m-t} - b_{m-t})$), é dicir, a súa clase en $\mathbb{Z}/p^{m-t}\mathbb{Z}$ é única. Temos que $(\overline{b_n}) \in \mathbb{Z}_p$, xa que $p^t\overline{b_{m-t}} = \overline{a_m} = \varphi_{m+1}(\overline{a_{m+1}}) = \varphi_{m+1}(p^t\overline{b_{m+1-t}}) = p^t\varphi_{m+1}(\overline{b_{m-t+1}}) \in \mathbb{Z}/p^m\mathbb{Z}$ e así b_{m-t} coincide con $\varphi_{m-t+1}(\overline{b_{m-t+1}})$ en $\mathbb{Z}/p^{m-t}\mathbb{Z}$ pola unicidade de b_{m-t} que acabamos de ver. Finalmente temos que $(\overline{a_n}) = (\overline{b_{n-t}})p^t$, xa que ambos elementos coinciden en coordenadas $n >> 0$ (de feito para $n \geq t$) e así coinciden todas as súas coordenadas por definición de límite proxectivo.
Finalmente a sobrexectividade de ε_t é clara. ■

Sexa $\mathbb{Z}_p^*$ o grupo de unidades de $\mathbb{Z}_p$.

Proposición 2.2.7 (I) Un elemento de $\mathbb{Z}_p$ é unidade se e só se non é divisible por p.

(II) Todo elemento non nulo de $\mathbb{Z}_p$ pódese escribir de forma única como $p^n u$ con $u \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$.

(III) $\mathbb{Z}_p$ é un dominio.

Demostración. (I) Un elemento $(\overline{a_n})$ de $\mathbb{Z}_p$ é unidade se e só se cada $\overline{a_n}$ é unidade en $\mathbb{Z}/p^n\mathbb{Z}$, xa que a multiplicación en $\mathbb{Z}_p$ está definida compoñente a compoñente, é dicir, $\mathbb{Z}_p^* = \varprojlim((\mathbb{Z}/p^n\mathbb{Z})^*)$. En $\mathbb{Z}/p^n\mathbb{Z}$ o *Teorema de Bezout* dinos que se $p \nmid a$ (co cal $(a, p^n) = 1$) entón $\overline{a}$ é invertible en $\mathbb{Z}/p^n\mathbb{Z}$. Re-

ciprocamente, se $p \mid a$ e $\overline{a}\overline{b} = \overline{1} \in \mathbb{Z}/p^n\mathbb{Z}$, entón $\overline{p} \mid \overline{1}$ en $\mathbb{Z}/p^n\mathbb{Z}$ obtendo unha contradición, xa que isto último non pode ocorrer.

(II) Sexa $0 \neq a = (\overline{a_n}) \in \mathbb{Z}_p$. Pola definición de límite proxectivo, só pode haber un número finito de termos $\overline{a_n}$ non nulos. Sexa entón $t \geq 0$ máximo tal que $\overline{a_t} = 0$, i.e., $\varepsilon_t(a) = 0$ (o caso $t = 0$ é cando $\overline{a_n} \neq 0\ \forall n$). Polo *lema 2.2.6*, $a \in p^t\mathbb{Z}_p$, é dicir, $a = p^t u$ con $u \in \mathbb{Z}_p$. Doutra banda, u é unidade polo apartado (I), pois $p \nmid u$ (se $p \mid u$, entón $p^{t+1} \mid p^t u = a$ e así $\varepsilon_{t+1}(a) = 0$ contradicindo a maximalidade de t). Isto proba a a existencia.

Antes de probar a unicidade probaremos (III): Se $a, b \in \mathbb{Z}_p$, $a \neq 0 \neq b$ polo que acabamos de probar $a = p^n u, b = p^m v$ con u, v unidades. Como ε_t é un homomorfismo de aneis, $\varepsilon_t(uv)$ é unidade e así $\varepsilon_t(ab) = p^{n+m}\varepsilon_t(uv)$ que é un elemento non nulo sempre que $t > n+m$. Así $ab \neq 0$.

Agora a unicidade en (II) é facil: $p^t u = p^r v$ con $u, v \in \mathbb{Z}_p^*$ $\Leftarrow$ $p^r(p^{t-r}u - v) = 0$ (supoñendo p.e. $t \geq r$). Ao ser $\mathbb{Z}_p^*$ dominio, $p^{t-r}u - v = 0$ e como $p \nmid v$ polo apartado (I), temos $t - r = 0$ e así $u - v = 0$.

■

Observación 2.2.8 Os homomorfismos de paso ao cociente $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ para cada $n \geq 1$, inducen un homomorfismo de aneis $i\colon \mathbb{Z} \to \mathbb{Z}_p, a \mapsto i(a) = (\overline{a_n})$ con $a_n = a$ $\forall n$, que é claramente inxectivo ($\ker(i) = \{a \in \mathbb{Z}\colon a \equiv 0 \pmod{p^n}\ \forall n\} = 0$). Así, podemos considerar $\mathbb{Z}$ coma subanel de $\mathbb{Z}_p$.

Definición 2.2.9 *(Valoración p–ádica)* Defínese a *valoración p–ádica* en $\mathbb{Z}_p$ grazas á *proposición 2.2.7* como:

$$\nu_p(0) = \infty$$
$$\nu_p(p^n u) = n, \text{ sendo } u \text{ unha unidade}$$

Tamén definimos $|a| := p^{-\nu_p(a)}$ e $d(a,b) := |a - b|$ para $a, b \in \mathbb{Z}_p$.

Observación 2.2.10 É fácil ver que se verifica

(I) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

(II) $\nu_p(a + b) \geq min\{\nu_p(a), \nu_p(b)\}$

(o único caso non inmediato é cando $ab = 0$, pero pola *proposición* 2.2.7 entón $a = 0$ ou $b = 0$, co que tamén é claro).

Logo temos $d(a,b) = 0 \Leftrightarrow a = b$ e pola propiedade (II) de ν_p temos $d(a,c) \leq max\{d(a,b), d(b,c)\}\ \forall a,b,c \in \mathbb{Z}_p$ (propiedade ultramétrica), e en particular temos a desigualdade triangular $d(a,c) \leq d(a,b) + d(b,c)$, co que d *define unha métrica en* $\mathbb{Z}_p$.

Proposición 2.2.11 A topoloxía que estabamos considerando en $\mathbb{Z}_p$ (como subanel de $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$) está inducida pola métrica d.

Demostración. Temos que $p^n\mathbb{Z}_p = (...\times\mathbb{Z}/p^{n+2}\mathbb{Z}\times\mathbb{Z}/p^{n+1}\mathbb{Z}\times\{0\}\times...\times\{0\})\cap\mathbb{Z}_p$ e así é un aberto. De feito a familia $p^n\mathbb{Z}_p$, $n \geq 0$ forma unha base de veciñanzas de 0 para a topoloxía de $\mathbb{Z}_p$ como límite proxectivo. Doutra banda, $a \in p^n\mathbb{Z} \Leftrightarrow \nu_p(c) \geq n \Leftrightarrow |x| \leq p^{-n}$ co que ambas topoloxías coinciden. ■

Observación 2.2.12 A partir de agora sabemos que podemos considerar $\mathbb{Z}_p$ como espazo métrico, e así, como é compacto (*proposición* 2.2.5), é completo.

Proposición 2.2.13 $\mathbb{Z}$ é denso en $\mathbb{Z}_p$.

Demostración. Sexa $(\overline{a_n}) \in \mathbb{Z}_p$. Sexa $b(n) \in \mathbb{Z}$ tal que $b(n) \equiv a_n \pmod{p^n}$. Consideremos $b(n)$ como elemento de $\mathbb{Z}_p$ como na *observación* 2.2.8. Entón $\nu_p(b(n) - (\overline{a_n})) \geq n$ e así $\lim_{n\to\infty} b(n) = (\overline{a_n})$. ■

Definición 2.2.14 Defínese o *corpo dos números p–ádicos* $\mathbb{Q}_p$ como o corpo de fraccións do dominio $\mathbb{Z}_p$. Como todo elemento non nulo de $\mathbb{Q}_p$ pódese expresar como $\frac{p^n u}{p^m v}$ con u, v unidades de $\mathbb{Z}_p$ (*proposición* 2.2.7), i.e., como $p^t w$ con $t \in \mathbb{Z}$, w unidade de $\mathbb{Z}_p$, temos que o elemento $\frac{1}{p}$ de $\mathbb{Q}_p$ xera $\mathbb{Q}_p$ como $\mathbb{Z}_p$–subáxlebra, i.e., $\mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$.

Observación 2.2.15 Todo elemento de $\mathbb{Q}_p$ pódese expresar como $p^t w$ con $t \in \mathbb{Z}$, $w \in \mathbb{Z}_p^*$, de forma única, e así podemos estender a valoración p–ádica de $\mathbb{Z}_p \subset \mathbb{Q}_p$ mediante $\nu_p(p^t w) = t$, $\nu_p(0) = \infty$.

$\mathbb{Z}_p$ queda caracterizado coma o conxunto de $a \in \mathbb{Q}_p$ tales que $\nu_p(a) \geq 0$. Temos ademais, ao igual que en $\mathbb{Z}_p$, que $d(a,b) = p^{-\nu_p(a-b)}$ é unha métrica en $\mathbb{Q}_p$. O subanel $\mathbb{Z}_p$ é aberto e pechado en $\mathbb{Q}_p$, pois $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : \nu_p(a) \geq 0\} = \{a \in \mathbb{Q}_p : \nu_p(a) > -1\}$ e así de feito é unha bóla pechada e unha bóla aberta (o mesmo razoamento proba que todas as bolas en $\mathbb{Q}_p$ son abertas e pechadas).

Proposición 2.2.16 $\mathbb{Q}_p$ é localmente compacto, completo e $\mathbb{Q}$ é denso en $\mathbb{Q}_p$ (considerando $\mathbb{Q}$ coma subcorpo de $\mathbb{Q}_p$, estendendo de forma obvia a *observación 2.2.12*).

Demostración. Unha bóla de centro $a \in \mathbb{Q}_p$ é da forma $\{x \in \mathbb{Q}_p : \nu_p(x-a) > n\} = \{x \in \mathbb{Q}_p : x - a \in p^{n+1}\mathbb{Z}_p\} = a + p^{n+1}\mathbb{Z}_p$ para un $n \in \mathbb{Z}$, que é claramente homeomorfa a $p^{n+1}\mathbb{Z}_p$, que á súa vez é homeomorfa a $\mathbb{Z}_p$. Así é compacta pola *proposición 2.2.5*.

Para ver que $\mathbb{Q}_p$ é completo, nótese que toda sucesión de Cauchy en $\mathbb{Q}_p$ ten todos os seus termos salvo un número finito en algún $p^n\mathbb{Z}_p$ (e polo tanto todos os seu termos en algún $p^t\mathbb{Z}_p$) con $n \in \mathbb{Z}$, e como $p^n\mathbb{Z}_p$ e $\mathbb{Z}_p$ son isométricos, ten límite pola *observación 2.2.12*.

Finalmente, pódese ver que $\mathbb{Q}$ é denso en $\mathbb{Q}_p$ de forma similar a como vimos que $\mathbb{Z}$ era denso en $\mathbb{Z}_p$ (de feito vemos que $\mathbb{Z}[\frac{1}{p}]$, o subanel de $\mathbb{Q}$ xerado por $\frac{1}{p}$, é denso en $\mathbb{Q}_p$). ■

Observación 2.2.17 $(\mathbb{Q}_p, +, \cdot)$ é un anel topolóxico. En efecto, é sinxelo ver que é suficiente probar que se U é unha bóla de centro cero, entón existe unha bóla de centro cero V tal que $U + U \subset V$, $-U \subset V$, $U \cdot U \subset V$ e isto é claro, pois as bólas de centro cero son $p^n\mathbb{Z}_p$, con $n \in \mathbb{Z}$.

2.3. Unidades p–ádicas

Observación 2.3.1 Sexa $U = \mathbb{Z}_p^*$, $\varepsilon_n : U \to (\mathbb{Z}/p^n\mathbb{Z})^*$ o homomorfismo inducido polo homomorfismo do *lema 2.2.6* sobre os grupos de unidades. Claramente $\ker \varepsilon_n = 1 + p^n\mathbb{Z}_p$. Denotaremos $U_n = \ker \varepsilon_n$. Ademais, $\varepsilon_n : U \to (\mathbb{Z}/p^n\mathbb{Z})^*$ é sobrexectivo pola *proposición 2.2.7 (I)*.

Proposición 2.3.2 (I) $U = \varprojlim_n U/U_n$

(II) Para $t \geq 1$, $U_t = \varprojlim_{n \geq t} U_t/U_n$

Demostración. (I) Na demostración da *proposición 2.2.7 (I)* vimos que $U = \mathbb{Z}_p^* = \varprojlim_n ((\mathbb{Z}/p^n\mathbb{Z})^*)$. Como $U/U_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^*$, deducimos o resultado.

(II) Polo *lema 2.2.3* aplicado a $1 \to U_t/U_n \to U/U_n \to U/U_t \to 1$, deducimos de (I) unha sucesión exacta

$$1 \to \varprojlim_{n \geq t} U_t/U_n \to U \to U/U_t \to 1$$

e así $U_t = \varprojlim_{n \geq t} U_t/U_n$

■

Proposición 2.3.3 (I) U/U_t é cíclico de orde $p-1$.

(II) $|U_1/U_n| = p^{n-1}$

Demostración. (I) $U/U_1 = U/\ker \varepsilon_1 = (\mathbb{Z}/p\mathbb{Z})^*$ que é cíclico por ser o grupo multiplicativo dun corpo finito.

(II) A aplicación $\varphi\colon U_n/U_{n+1} \to \mathbb{Z}/p\mathbb{Z}, 1 + p^n x + U_{n+1} \mapsto x + p\mathbb{Z}$ $(x \in \mathbb{Z}_p)$ está ben definida ($\varphi(U_{n+1}) = \varphi(1 + p^{n+1}\mathbb{Z}) \subset p\mathbb{Z}$) e é un homomorfismo do grupo multiplicativo U_n/U_{n+1} no grupo aditivo $\mathbb{Z}/p\mathbb{Z}$, xa que como

$$1 + p^n + p^{2n}b = (1 + p^n a)(1 + p^{2n}b - p^{3n}ab + p^{4n}a^2b - p^{5n}a^3b + \ldots)$$

temos

$$(1 + p^n a + p^{2n}b)U_{n+1} = (1 + p^n a)U_{n+1}$$

[a] e así

$$\varphi((1 + p^n x)U_{n+1}(1 + p^n y)U_{n+1}) = \varphi((1 + p^n(x+y) + p^{2n}xy)U_{n+1}) =$$
$$\varphi((1 + p^n(x+y))U_{n+1}) = x + y + p\mathbb{Z} = \varphi((1 + p^n x)U_{n+1}) + \varphi((1 + p^n y)U_{n+1})$$

Ademais, φ é claramente sobrexectiva e polo tanto un isomorfismo. Así $|U_n/U_{n+1}| = |\mathbb{Z}/p\mathbb{Z}| = p$.

Nunha sucesión exacta corta de grupos abelianos finitos $1 \to A \to B \to C \to 1$, temos $|B| = |A||C|$. Así, por indución en t nas sucesións exactas

$$1 \to U_{n+1}/U_{n+t} \to U_n/U_{n+1} \to U_n/U_{n+1} \to 1$$

obtemos $|U_n/U_{n+t}| = p^t$. En particular $|U_1/U_n| = p^{n-1}$ como queriamos demostrar.

■

[a] O termo $(1 + p^{2n}b - p^{3n}ab + \ldots)$ existe en $\mathbb{Z}_p$ xa que claramente a serie converxe na métrica p–ádica, e é inmediato que pertence a U_{n+1}.

Lema 2.3.4 Sexa $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ unha sucesión exacta de grupos abelianos finitos con $(|A|, |C|) = 1$. Entón $B \simeq A \times C$.

Demostración. Sexa $a = |A|$, $c = |C|$ e $C' = \{x \in B : cx = 0\}$. Posto que $(a, c) = 1$, pola identidade de Bezout existen $r, s \in \mathbb{Z}$: $ar + cs = 1$. Se $x \in \alpha(A) \cap C'$ entón $ax = cx = 0$ ($ax = 0$ xa que $|x| \mid a$) e $x = (ar + cs)x = 0$. Así $\alpha(A) \cap C' = 0$. É inmediato que $\alpha(A) \bigoplus C' \subset B$. Reciprocamente, se $x \in B$, entón $x = arx + csx$. Posto que $B/\alpha(A) \simeq C$ e $cC = 0$, entón $cB/\alpha(A) \simeq 0$ e $cB \subset \alpha(A)$. Así $csx \in \alpha(A)$. Doutra banda, se $x \in cB \subset \alpha(A)$, $ax = 0$ e $acB = 0$. Tense $carx = 0$ e $arx \in C'$. Así $B = \alpha(A) \bigoplus C'$. Finalmente $C' \simeq (\alpha(A) \bigoplus C')/\alpha(A) = B/\alpha(A) \simeq C$ e como α é inxectivo $\alpha(A) \simeq A$. Temos polo tanto $B \simeq A \bigoplus C \simeq A \times C$, como queriamos demostrar. ■

Proposición 2.3.5 $U \simeq (\mathbb{Z}/p\mathbb{Z})^* \times U_1$.

Demostración. Aplicando o *lema 2.3.4* ás sucesións exactas

$$1 \to U_1/U_n \to U/U_n \to (\mathbb{Z}/p\mathbb{Z})^* \to 1$$

(nótese que $|U_1/U_n| = p^{n-1}$, pola *proposición 2.3.3*, e $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ son coprimos), obtemos

$$U/U_n \simeq U_1/U_n \times (\mathbb{Z}/p\mathbb{Z})^*$$

Tomando límites proxectivos(que conmutan con ${}_\times(\mathbb{Z}/p\mathbb{Z})^*$ claramente, o tamén polo *lema 2.2.3*) obtemos grazas á *proposición 2.3.2*

$$U \simeq U_1 \times (\mathbb{Z}/p\mathbb{Z})^*$$

■

Observación 2.3.6 Chamaremos *t–raíces da unidade* nun corpo K aos elementos $x \in K$ tales que $x^k = 1$. Como sobre un corpo K o polinomio $x^t - 1$ ten ao sumo t raíces, existen ao sumo t raíces da unidade. O grupo $(\mathbb{Z}/p\mathbb{Z})^*$ ten orde $p - 1$, así os seus $p - 1$ elementos x_i verifican $x_i^{p-1} = 1$. Entón pola *proposición 2.3.5* U contén $p - 1$ elementos de orde $p - 1$ (os elementos correspondentes a $(x_i, 1)$ polo isomorfismo da *proposición 2.3.5*). Como $U \subset \mathbb{Q}_p$ e $\mathbb{Q}_p$ é un corpo, $\mathbb{Q}_p$ contén tódalas $(p - 1)$–raíces da unidade.

Lema 2.3.7 (I) Se $p \neq 2$ e $x \in U_n - U_{n+1}$, entón $x^p \in U_{n+1} - U_{n+2}$

(II) Se $p = 2$ e $x \in U_n - U_{n+1}$ con $n \geq 2$, entón $x^p \in U_{n+1} - U_{n+2}$

Demostración. Sexa $x = 1 + p^n y$ con $p \nmid y$. Entón

$$x^p = (1 + p^n y)^p = \sum_{i=0}^{p} \binom{p}{i} (p^n y)^i = 1 + p^{n+1} y + \sum_{i=2}^{p} \binom{p}{i} (p^n y)^i$$

Logo $x^p \equiv 1 + p^{n+1} y \pmod{p^{n+2}}$, onde na congruencia usamos que se $p = 2$ entón $n \geq 2$. ■

Proposición 2.3.8 (I) Se $p \neq 2$, U_1/U_n é un grupo cíclico de orde p^{n-1} e $U_1 \simeq \mathbb{Z}_p$ ($\mathbb{Z}_p$ como grupo aditivo)

(II) Se $p = 2$, $U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ ($\mathbb{Z}_2$ como grupo aditivo)

Demostración. (I) Sexa $\alpha \in U_1 - U_2$. Polo *lema 2.3.7*, $\alpha^{p^i} \in U_{i+1} - U_{i+2}$. Sexa $\alpha_n := \alpha + U_n \in U_1/U_n$. Temos entón $(\alpha_n)^{p^{n-2}} \neq 1 = (\alpha_n)^{p^{n-1}}$. Como $|U_1/U_n| = p^{n-1}$ pola *proposición 2.3.3*, $|\alpha_n| \mid p^{n-1}$ e así $|\alpha_n| = p^{n-1}$, co que $< \alpha_n >= U_1/U_n$.

Sexa entón $\varphi_n \colon \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$ o isomorfismo do grupo cíclico $\mathbb{Z}/p^{n-1}\mathbb{Z}$ no grupo multiplicativo U_1/U_n, $1 \mapsto \alpha_n$. Como o diagrama

$$\begin{array}{ccccc} \ldots & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{n-1}\mathbb{Z} \longrightarrow \ldots \\ & & \simeq \downarrow \varphi_{n+1} & & \simeq \downarrow \varphi_n \\ \ldots & \longrightarrow & U_1/U_{n+1} & \longrightarrow & U_1/U_n \longrightarrow \ldots \end{array}$$

é conmutativo, tomando límites proxectivos obtemos

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \varprojlim_n U_1/U_n = U_1$$

usando a *proposición 2.3.2*

(II) Na sucesión exacta corta (*proposición 2.3.3*)

$$1 \to U_2 \to U_1 \xrightarrow{\pi} U_1/U_2 \simeq \mathbb{Z}/2\mathbb{Z} \to 1$$

o homomorfismo π ten unha sección $\sigma \colon \mathbb{Z}/2\mathbb{Z} \to U_1$, $\sigma(0) = 1$, $\sigma(1) = -1$, e así $U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2$

Sexa $\alpha \in U_2 - U_3$ (i.e., $\alpha \equiv 5 \pmod 8$). De forma análoga ao apartado (I), temos un diagrama conmutativo

$$\begin{array}{ccccc} \ldots & \longrightarrow & \mathbb{Z}/2^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/2^{n-1}\mathbb{Z} \longrightarrow \ldots \\ & & \downarrow & & \downarrow \\ \ldots & \longrightarrow & U_2/U_{n+2} & \longrightarrow & U_2/U_{n+1} \longrightarrow \ldots \end{array}$$

e así, pola *proposición* **2.3.2**, $\mathbb{Z}_2 = \varprojlim \mathbb{Z}/2^n\mathbb{Z} = U_2$.

■

Proposición 2.3.9 (I) $\mathbb{Q}_p^* \simeq \mathbb{Z} \times U$

(II) Se $p \neq 2$, $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$

(III) Se $p = 2$, $\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$

Demostración. Pola *proposición* **2.3.5** e a *proposición* **2.3.8**, (I) e (II) dedúcense de (I). A propiedade (I) dedúcese de que todo elemento $x \in \mathbb{Q}_p^* = \mathbb{Q}_p - \{0\}$ pódese escribir de forma única como $p^n u$ con $n \in \mathbb{Z}, u \in U$ pola *proposición* **2.2.7** (ver *definición* **2.2.14**). ■

Corolario 2.3.10 Sexa $x \in \mathbb{Q}_p^*$. Como vimos na *definición* **2.2.14**, $x = p^n u$ de forma única con $n \in \mathbb{Z}, u \in U$.

(I) Se $p \neq 2$, x é un cadrado en $\mathbb{Q}_p^*$ se e só se n é par e a clase de u en $U/U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^*$ é un cadrado.

(II) Se $p = 2$, x é un cadrado en $\mathbb{Q}_2^*$ se e só se n é par e $u \equiv 1 \pmod 8$ en $\mathbb{Z}_2$.

Demostración. (I) Mediante o isomorfismo $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^*$, o elemento $x = p^n u$ correspóndese cun elemento (n, a, b) onde b é a clase de u en $U/U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^*$. Temos que x é un cadrado en $\mathbb{Q}_p^*$ se e só se n, a, b son cadrados en $\mathbb{Z}, \mathbb{Z}_p, (\mathbb{Z}/p\mathbb{Z})^*$ respectivamente. En $\mathbb{Z}$ (a operación é a suma en $\mathbb{Z}$ e $\mathbb{Z}_p$ e o produto en $(\mathbb{Z}/p\mathbb{Z})^*$) n é un cadrado se e só se n é par. En $\mathbb{Z}_p$ todo elemento é un cadrado xa que como $p \neq 2$, 2 ten inverso en $\mathbb{Z}_p$. Así pois (I) queda demostrado.

(II) Pola *proposición* **2.3.9** *(I)*, $2^n u$ é un cadrado se e só se n é par e u é un cadrado en U. Pola *proposición* **2.3.5** e a *proposición* **2.3.8**, $U \simeq (\mathbb{Z}/2\mathbb{Z})^* \times U_1 = U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2$ e así u é un cadrado en U se e só se o é en $\mathbb{Z}/2\mathbb{Z} \times U_2$, i.e., é da forma $(0, u'), u' \in U_2$, xa que 1 non é cadrado en $\mathbb{Z}/2\mathbb{Z}$. A sucesión exacta da demostración da *proposición* **2.3.8** *(II)* que

daba este isomorfismo $U_1 \simeq \mathbb{Z}/2\mathbb{Z} \times U_2$

$$1 \to U_2 \to U_1 \xrightarrow{\Pi} U_1/U_2 \simeq \mathbb{Z}/2\mathbb{Z} \to 1$$

mostra entón que $u \in U_1$ é cadrado se e só se $\pi(u) = 0$ (i.e., $u \in U_2$) e u é un cadrado en U_2. Isto ocorre se e só se $u \in U_3 = 1 + 2^3\mathbb{Z}_2$, i.e., se e só se $u \equiv 1 \pmod 8$.

■

Corolario 2.3.11 (I) Se $p \neq 2$, $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un conxunto de representantes (en $\mathbb{Q}_p^*$) é $\{1, p, u, up\}$ onde $u \in U$ é un elemento que non sexa cadrado.

(II) Se $p = 2$, $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un conxunto de representantes é $\{\pm 1, \pm 5, \pm 2, \pm 10\} \subset \mathbb{Q}_2^*$.

Demostración. (I) Como a metade dos elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ son cadrados[a], i.e., están no subgrupo $((\mathbb{Z}/p\mathbb{Z})^*)^2$ de $(\mathbb{Z}/p\mathbb{Z})^2$, temos que o índice de este subgrupo é 2 e así a orde do cociente é 2. Polo tanto $(\mathbb{Z}/p\mathbb{Z})^*/((\mathbb{Z}/p\mathbb{Z})^*)^2 \simeq \mathbb{Z}/2\mathbb{Z}$. Logo (I) dedúcese do *corolario* **2.3.10**.

(II) Xa vimos que se $p = 2$, $U \simeq U_1$ e $U_1/U_1^2 \simeq U_1/U_3 = (1 + 2\mathbb{Z}_2)/(1 + 2^3\mathbb{Z}_2) = \{\pm 1, \pm 5\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, o último isomorfismo débese a que os elementos $-1, \pm 5$ teñen orde 2. Entón pola *proposición* **2.3.9** e a demostración do *corolario* **2.3.10***(II)*, $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times U/U_3$, co que un conxunto de representantes é $\{(0, \pm 1), (0, \pm 5), (1, \pm 1), (1, \pm 5)\}$. Como o isomorfismo $\mathbb{Q}_2^* \simeq \mathbb{Z} \times U$ da *proposición* **2.3.9** está dado por $2^n u \mapsto (n, u)$, estes elementos correspóndense con $2^0(\pm 1), 2^0(\pm 5), 2^1(\pm 1), 2^1(\pm 5)$, é dicir, $\pm 1, \pm 5, \pm 2, \pm 10$.

■

[a] Como $(\mathbb{Z}/p\mathbb{Z})^*$ é cíclico, podemos tomar un xerador g, é dicir, $(\mathbb{Z}/p\mathbb{Z})^* = \{g^i : i = 1, \ldots p-1\}$; se i é par, $g^i = (g^m)^2 = a$ e temos que polo menos a metade dos elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ son cadrados; como ademais cada cadrado ten exactamente dúas raíces e son distintas (b e $p - b$) por ser $p \neq 2$, como moito a metade dos elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ son cadrados.

Corolario 2.3.12 $(\mathbb{Q}_p^*)^2$ é un subgrupo aberto de $\mathbb{Q}_p^*$.

Demostración. Supoñamos $p \neq 2$. Sexa $up^n \in (\mathbb{Q}_p^*)^2$, i.e., n é par e a clase de u en $(\mathbb{Z}/p\mathbb{Z})^*$ é un cadrado. Toda bóla aberta con centro up^n é da forma $up^n + p^t\mathbb{Z}_p$. Se tomamos t suficientemente grande ($\geq n$), temos que todo punto desta bola

é da forma $x = up^n + p^t v = p^n(u + p^s v)$, onde $u + p^s v$ é unha unidade ao non ser divisible por p e a súa clase en $(\mathbb{Z}/p\mathbb{Z})^*$ é un cadrado (pois coincide coa clase de u). Así $x \in (\mathbb{Q}_p^*)^2$. O caso $p = 2$ é similar. ■

Capítulo 3

Fórmula produto para o símbolo de Hilbert

3.1. Símbolo de Legendre

Definición 3.1.1 Sexa p un primo impar e $a \in \mathbb{Z}$. Defínese o *símbolo de Legendre* de a con respecto a p como

$$(a/p) := \begin{cases} 0 & \text{se } p \mid a \\ +1 & \text{se } a \text{ é un cadrado módulo } p \\ -1 & \text{se } a \text{ non é un cadrado módulo } p \end{cases}$$

Proposición 3.1.2 Sexa p un primo impar e $a, b \in \mathbb{Z}$. Verifícase

(I) (*Criterio de Euler*). $(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(II) $(a/p)(b/p) = (ab/p)$

(III) $a \equiv b \pmod{p} \Rightarrow (a/p) = (b/p)$.

Demostración. Se p divide a a, as tres afirmacións son triviais. Supoñamos que $p \nmid a$ e $p \nmid b$.

(I) Polo *Pequeno teorema de Fermat* tense $a^{p-1} \equiv 1 \pmod{p}$ e así $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Doutra banda, $(a/p) = 1 :\Leftrightarrow a$ é un cadrado módulo $p \Leftrightarrow$

$a = g^i$: i par, onde $g \in (\mathbb{Z}/p\mathbb{Z})^*$ é un xerador. Logo

$$a^{\frac{p-1}{2}} \equiv g^{\frac{i(p-1)}{2}} \pmod{p}$$

g ten orde $p-1$, é dicir, $p-1$ é o menor enteiro positivo tal que $g^{p-1} \equiv 1 \pmod{p}$. Pero i par $\Leftrightarrow \frac{i(p-1)}{2}$ é múltiplo de $p-1 \Leftrightarrow g^{\frac{i(p-1)}{2}} \equiv 1 \pmod{p} \Leftrightarrow a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}$.

(II) Consecuencia inmediata de (I).

(III) É trivial pola definición.

■

Proposición 3.1.3 Sexa p un primo impar. Verifícase

(I) $(1/p) = 1$

(II) $(-1/p) = (-1)^{\frac{p-1}{2}}$

(III) $(2/p) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 5 \pmod{8} \end{cases}$

Demostración. (I) é trivial e (II) é consecuencia inmediata da *proposición 3.1.2* (I). Probaremos (III). Sexa K o corpo de p elementos e ξ unha 8-raíz primitiva da unidade nunha clausura alxébrica Ω de K. Definimos o elemento $y := \xi + \xi^{-1}$ Tense que:

$$\begin{aligned} (\xi^4)^2 = \xi^8 = 1 \Rightarrow \xi^4 = -1 \quad (\neq 1, \text{pois } \xi \text{ é primitiva}) \\ \Rightarrow \xi^2\xi^2 = -1 \Rightarrow \xi^2 = -\xi^2 \Rightarrow \xi^{-2} + \xi^{-2} = 0 \\ \Rightarrow y^2 = \xi^2 + \xi^{-2} + 2 = 2 \end{aligned}$$

Se ademais usamos a *proposición 3.1.2* (I), obtemos

$$(2/p) = (y^2/p) \equiv y^{p-1} \pmod{p}$$

Doutra banda, como $car(K) = p$, temos $y^p = \xi^p + \xi^{-p}$. Calculemos y^{p-1}:

- Caso $p \equiv \pm 1 \pmod{8}$. Tense $\xi^p = \pm 1$ e así $y^p = y$, é dicir $y^{p-1} = 1$.
- Caso $p \equiv \pm 5 \pmod{8}$. Tense

$$\begin{aligned} \xi^5 = \xi^4\xi = -\xi \\ \xi^{-5} = \xi^{-4}\xi^{-1} = -\xi^{-1} \end{aligned}$$

e así $y^p = -y$, é dicir $y^{p-1} = -1$.

■

Teorema 3.1.4 *(Lei de reciprocidade cuadrática).* Sexan p, q primos impares. Verifícase:

$$(p/q) = (-1)^{\frac{(p-1)(q-1)}{4}}(q/p) = \begin{cases} -(q/p) & \text{se } p \equiv q \equiv 3 \pmod 4 \\ (q/p) & \text{noutro caso} \end{cases}$$

Demostración. (Ver [3]). Imos calcular de dúas formas diferentes o produto T de todos os elementos do grupo $G := ((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)/N$, onde $N := \{(1,1),(-1,-1)\}$. Un conxunto de representantes dos elementos de G é $\{(i,j) : i = 1,...,p-1; j = 1,...,\frac{q-1}{2}\}$ posto que se $\frac{q-1}{2} < m \leq q-1$, $(i,m) = (-i,-m)$ e $\overline{-m} \in \{\overline{1},...,\overline{\frac{q-1}{2}}\} \subset \mathbb{Z}/q\mathbb{Z}$. O produto de todos os elementos é entón

$$T = ([(p-1)!]^{\frac{q-1}{2}}, [(\frac{q-1}{2})!]^{p-1})$$

Como

$$\begin{aligned} (q-1)! &= 1 \cdot 2 \cdot 3 \cdot ... \cdot \frac{q-1}{2}(\frac{q-1}{2}+1)...(q-1) \\ &\equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot \frac{q-1}{2}[(-\frac{q-1}{2})][-(\frac{q-1}{2}-1)]...[-1] \\ &\equiv (-1)^{\frac{q-1}{2}}[(\frac{q-1}{2})!]^2 \pmod q \end{aligned}$$

obtemos

$$T = ([(p-1)!]^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}) \in G$$

Doutra banda, $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})^* \simeq (\mathbb{Z}/pq\mathbb{Z})^*$ polo *Teorema chino dos restos*, e mediante este isomorfismo, N vai no subgrupo $N' := \{-1,1\}$ de $(\mathbb{Z}/pq\mathbb{Z})^*$. Así, un conxunto de representantes de $(\mathbb{Z}/pq\mathbb{Z})^*/N'$ é $\{i \in \{1,2,...,\frac{pq-1}{2}\} : (i,pq) = 1\}$ e os elementos correspondentes en $((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*)/N$ son $\{(i,i) : i \in \{1,2,...,\frac{pq-1}{2}\}, (i,pq) = 1\}$,

co que

$$T = \Big(\frac{(\prod_{i=1}^{p-1} i)(\prod_{i=1}^{p-1} p+i) \cdot \ldots \cdot (\prod_{i=1}^{p-1} (\frac{q-1}{2}-1)p+i)(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2}p+i)}{1q \cdot 2q \cdot \ldots \cdot \frac{p-1}{2}q},$$
$$\frac{(\prod_{i=1}^{q-1} i)(\prod_{i=1}^{q-1} q+i) \cdot \ldots \cdot (\prod_{i=1}^{q-1} (\frac{p-1}{2}-1)q+i)(\prod_{i=1}^{\frac{q-1}{2}} \frac{p-1}{2}q+i)}{1p \cdot 2p \cdot \ldots \cdot \frac{q-1}{2}p} \Big) =$$

(no denominador temos posto dous elementos do numerador que non verifican $(i, pq) = 1$)

$$= \Big(\frac{(p-1)!\ldots(p-1)!(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2}p+i)}{q^{\frac{p-1}{2}}(\frac{p-1}{2})!}, \frac{(q-1)!\ldots(q-1)!(\prod_{i=1}^{\frac{q-1}{2}} \frac{p-1}{2}q+i)}{p^{\frac{q-1}{2}}(\frac{q-1}{2})!} \Big)$$
$$= \Big(\frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}}, \frac{(q-1)!^{\frac{p-1}{2}}}{p^{\frac{q-1}{2}}} \Big)$$

Pola *proposición* **3.1.2** *(I)* e tendo en conta que $(q/p) = \pm 1$,

$$T = \Big(\frac{(p-1)!^{\frac{q-1}{2}}}{(q/p)}, \frac{(q-1)!^{\frac{p-1}{2}}}{(p/q)} \Big) = \Big((p-1)!^{\frac{q-1}{2}}(q/p), (q-1)!^{\frac{p-1}{2}}(p/q) \Big)$$

Comparando os dous cálculos de T, obtemos

$$(1, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}) = ((q/p), (p/q)) \in G$$

é dicir, existe $\varepsilon = 1$ ou $\varepsilon = -1$ tal que $1 \equiv \varepsilon(q/p) \pmod{p}$, $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \varepsilon(p/q) \pmod{q}$, e así

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

■

3.2. Ecuacións sobre corpos finitos

Sexa q unha potencia dun número primo p, e sexa K o corpo de q elementos.

Lema 3.2.1 Sexa s un número enteiro ≥ 0. Entón

$$\sum_{x \in K} x^s = \begin{cases} -1 & \text{se } s \geq 1 \text{ e } q-1 \mid s \\ 0 & \text{noutro caso} \end{cases}$$

Demostración. Se $s = 0$ todos os termos da suma son 1 (establecemos que $x^s = 1$ se $s = 0$ incluso cando $x = 0$), logo

$$\sum_{x \in K} x^s = q1 = 0$$

posto que K ten característica p e q é unha potencia de p.
Se $s \geq 1$ é divisible por $q - 1$, temos $0^s = 0$ e $x^s = 1$ se $x \neq 0$, pois K^* é un grupo de orde $q - 1$. Así

$$\sum_{x \in K} x^s = \sum_{x \in K^*} x^s = (q-1)1 = -1$$

Se $s \geq 1$ non é divisible por $q - 1$, o feito de que $K^* = K - \{0\}$ é cíclico de orde $q - 1$ implica que existe un elemento $y \in K^*$ tal que $y^s \neq 1$. Ademais $K^* \to K^*, x \mapsto y^s x$ é un isomorfismo de grupos. Así, tense

$$\sum_{x \in K} x^s = \sum_{x \in K^*} x^s = \sum_{x \in K^*} y^s x^s = y^s \sum_{x \in K^*} x^s \Rightarrow (1 - y^s) \sum_{x \in K^*} x^s = 0 \Rightarrow \sum_{x \in K^*} x^s = 0$$

■

Teorema 3.2.2 (Chevalley-Warning). Sexan $f_\alpha \in K[X_1, ..., X_n]$ polinomios en n variables tales que $\sum_\alpha deg(f_\alpha) < n$, e sexa $\mathbb{V}$ o conxunto dos seus ceros comúns en K^n. Tense

$$|\mathbb{V}| \equiv 0 \pmod{p}$$

Demostración. Sexa $g = \prod_\alpha (1 - f_\alpha^{q-1})$ e sexa $x = (x_1, ..., x_n) \in K^n$. Se $x \in \mathbb{V}$, todos os $f_\alpha(x)$ son cero e polo tanto $g(x) = 1$; se $x \notin \mathbb{V}$, para algún α tense $f_\alpha(x) \neq 0$ e $f_\alpha^{q-1}(x) = 1$ por ser un elemento de K, e logo $g(x) = 0$. É dicir, tense que g é a función característica de $\mathbb{V}$. Deste xeito

$$|\mathbb{V}| \equiv \sum_{x \in K^n} g(x) \pmod{p}$$

e reducimos o problema a probar que $\sum_{x \in K^n} g(x) = 0$.
Agora ben, por hipótese $\sum_\alpha deg(f_\alpha) < n$ o que implica que $deg(g) < n(q-1)$. Logo g é unha combinación lineal de monomios $g_u(x) = x_1^{u_1} ... x_n^{u_n}$ con $\sum_{i=1}^n u_i <$

$n(q-1)$. É suficiente con probar que, para cada monomio g_u, temos

$$\sum_{x\in K^n} x_1^{u_1}...x_n^{u_n} = 0$$

o que se segue do *lema 3.2.1*, xa que hai al menos un $u_i < q-1$, e así

$$\sum_{x\in K^n} x_1^{u_1}...x_n^{u_n} = \Big(\sum_{\substack{x\in K^n\\ x_i=1}} x_1^{u_1}...x_n^{u_n}\Big) \sum_{x_i\in K} x_i^{u_i} = 0$$

■

Corolario 3.2.3 (I) Se $\sum_\alpha deg(f_\alpha) < n$ e os f_α non teñen termo independente, entón os f_α teñen un cero non trivial común.

(II) Todas as formas cuadráticas en polo menos 3 variables sobre K teñen un cero non trivial.

Demostración. Se $\mathbb{V} = \{0\}$, entón $|\mathbb{V}| = 1$ e o cardinal non sería divisible por p, contradicindo o teorema anterior. ■

3.3. Ecuacións p–ádicas

Teorema 3.3.1 Sexa p un número primo e $F(x_1,...,x_n) \in \mathbb{Z}_p[x_1,...,x_n]$ e $\gamma_1,...,\gamma_n \in \mathbb{Z}_p$. Supoñamos que existe $i \in \{1,...,n\}$ e $\delta \in \mathbb{N}$ verificando as seguintes tres condicións:

(I) $F(\gamma_1,...,\gamma_n) \equiv 0 \pmod{p^{2\delta+1}}$

(II) $\frac{\partial F}{\partial x_i}(\gamma_1,...,\gamma_n) \equiv 0 \pmod{p^{\delta}}$

(III) $\frac{\partial F}{\partial x_i}(\gamma_1,...,\gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$

Entón existen $\theta_1,...,\theta_n \in \mathbb{Z}_p$ tales que

(a) $F(\theta_1,...,\theta_n) = 0$

(b) $\theta_j \equiv \gamma_j \pmod{p^{\delta+1}}$ para todo $j = 1,...,n$

Demostración. Consideremos o polinomio en $\mathbb{Z}_p[x]$

$$f(x) = F(\gamma_1,...,\gamma_{i-1},x,\gamma_{i+1},...,\gamma_n)$$

É suficiente atopar un $\alpha \in \mathbb{Z}_p$, $\alpha \equiv \gamma_i \pmod{p^{\delta+1}}$ tal que $f(\alpha) = 0$ (tomando $\theta_i = \alpha$, $\theta_j = \gamma_j$ para todo $j \neq i$). Imos construír unha sucesión $\{\alpha_t\}_{t\in\mathbb{N}}$ en $\mathbb{Z}_p$ con $\alpha_t \equiv \gamma_i \pmod{p^{\delta+1}}$ para todo t verificando $\alpha_t \equiv \alpha_{t-1} \pmod{\delta + t}$ e $f(\alpha_t) \equiv 0 \pmod{p^{2\delta+1+t}}$ para todo t.
Para $t = 0$ definimos $\alpha_0 = \gamma_i$. Sexa $t > 0$ e supoñamos xa construído $\alpha_0, ...\alpha_{t-1}$ verificando as propiedades anteriores. Constrúamos α_t. Sexa

$$f(x) = \beta_0 + \beta_1(x - \alpha_{t-1}) + \beta_2(x - \alpha_{t-1})^2 + ... \ (\beta_i \in \mathbb{Z}_p)$$

o desenvolvemento do polinomio f en termos de potencias de $(x-\alpha_{t-1})$. Temos $\beta_0 = f(\alpha_{t-1}) \equiv 0 \pmod{p^{2\delta+1+t-1}}$, é dicir $\beta_0 = p^{2\delta+t}a$ con $a \in \mathbb{Z}_p$. Tamén $\beta_1 = f'(\alpha_{t-1}) \equiv 0 \pmod{p^{\delta}}$ e $\beta_1 = f'(\alpha_{t-1}) \not\equiv 0 \pmod{p^{\delta+1}}$ por hipótese (xa que $\alpha_{t-1} \equiv \gamma_i \pmod{p^{\delta+1}}$ e $f'(\alpha_{t-1}) = \frac{\partial F}{x_i}(\gamma_1, ..., \gamma_{i-1}, \alpha_{t-1}, \gamma_{i+1}, ..., \gamma_n)$). Así, $\beta_1 = p^{\delta}b$ con $b \in \mathbb{Z}_p$, $p \nmid b$. Sexa ξ tal que $a + b\xi \equiv 0 \pmod{p}$ (existe xa que $p \nmid b$). Temos

$$f(\alpha_{t-1} + \xi p^{t+\delta}) = p^{2\delta+t}(a + b\xi) + \beta_2\xi^2 p^{2\delta+2t} + ... \equiv 0 \pmod{p^{2\delta+1+t}}$$

Definimos entón $\alpha_t = \alpha_{t-1} + \xi p^{t+\delta}$, que claramente cumpre o requirido. Como $\nu_p(\alpha_t - \alpha_{t-1}) \geq \delta + t$ para todo t e $\mathbb{Z}_p$ é completo, a sucesión $\{\alpha_t\}_{t\in\mathbb{N}}$ converxe. Vexamos que o límite desta sucesión $\alpha \in \mathbb{Z}_p$ verifica o requirido. Claramente $\alpha \equiv \gamma_i \pmod{p^{\delta+1}}$ pois $\alpha_t \equiv \gamma_i \pmod{p^{\delta+1}}$ para todo t. Como $f(\alpha_t) \equiv 0 \pmod{p^{2\delta+1+t}}$ para todo t, a sucesión $\{f(\alpha_t)\}_{t\in\mathbb{N}}$ converxe a 0. Como f é unha aplicación continua por ser un polinomio, $\{f(\alpha_t)\}$ converxe a $f(\alpha)$, co que $f(\alpha) = 0$. ■

3.4. Símbolo de Hilbert

Sexa $V = \{p \in \mathbb{N} : p \text{ primo}\} \cup \{\infty\}$, e poñamos $\mathbb{Q}_\infty = \mathbb{R}$.

Definición 3.4.1 Sexa $v \in V$ e sexan $a, b \in \mathbb{Q}_v^*$. Definimos o símbolo de Hilbert de a e b como

$$(a,b) := \begin{cases} 1 & \text{se } ax^2 + by^2 = z^2 \text{ ten algunha solución } \mathbb{Q}_v^3 \ni (x,y,z) \neq (0,0,0) \\ -1 & \text{en caso contrario} \end{cases}$$

Por exemplo, se $v = \infty$, $(a,b) = 1$ se e só se $\{a > 0 \text{ ou } b > 0\}$.

Proposición 3.4.2 (I) $(a,b) = (b,a) \quad \forall a,b \in \mathbb{Q}_v^*$

(II) $(\lambda^2 a, b) = (a,b) = (a, \lambda^2 b) \quad \forall a,b,\lambda \in \mathbb{Q}_v^*$

(III) $(a,1) = 1 = (a,c^2) \quad \forall a,c \in \mathbb{Q}_v^*$

(IV) $(a,-a) = 1 \quad \forall a \in \mathbb{Q}_v^*$

Demostración. (I) e (II) son claras. (III) dedúcese de que $(0,1,1)$ é solución de $ax^2 + y^2 = z^2$, e (IV) de que $(1,1,0)$ é solución de $ax^2 - ay^2 = z^2$. ■

Sexa p un número primo e q unha forma cuadrática non singular sobre $\mathbb{Q}_p$. Polo *teorema* **1.1.11** podemos supoñer que q é da forma

$$q(x_1,...,x_n) = a_1x_1^2 + ... + a_nx_n^2 \quad a_i \in \mathbb{Q}_p^*$$

Se $a_i = p^{n_i}u_i$ con $u_i \in \mathbb{Z}_p^*$ (*observación* **2.2.15**) e m_i é a parte enteira de $n_i/2$, facendo o cambio de variable $x_i' = p^{m_i}x_i$, podemos supoñer que $n_i = 0$ ou 1. Así, podemos supoñer que q é da forma

$$u_1x_1^2 + ... + u_rx_r^2 + p(u_{r+1}x_{r+1}^2 + ... + u_nx_n^2) \text{ con } u_i \in \mathbb{Z}_p^* \text{ para todo } i$$

Denotaremos $q_0(x_1,...,x_r) = u_1x_1^2 + ... + u_rx_r^2$, $q_1(x_{r+1},...,x_n) = u_{r+1}x_{r+1}^2 + ... + u_nx_n^2$.

Así $q = q_0 + pq_1$ (coa notación de despois da *definición* **1.2.7**).

Proposición 3.4.3 (I) Se $p \neq 2$ e $0 < r < n$, entón q representa 0 se e só se ao menos unha das formas cuadráticas q_0, q_1 representa 0.

(II) Se $p = 2$, q representa 0 se e só se a congruencia $q \equiv 0 \pmod{16}$ admite unha solución $a_1,...,a_n$ cos $a_i \in \mathbb{Z}_2$ tal que $2 \nmid a_i$ para algún i.

Demostración. (I) Supoñamos que q representa 0, é dicir, existen $a_1,...,a_n \in \mathbb{Q}_p$ non todos nulos tales que $u_1a_1^2 + ... + u_ra_r^2 + p(u_{r+1}a_{r+1}^2 + ... + u_na_n^2) = 0$. Multiplicando por algún elemento non nulo para eliminar denominadores, podemos supoñer que $a_1,...,a_n \in \mathbb{Z}_p$. Tamén podemos supoñer que algún a_i non é divisible por p, xa que en caso contrario dividimos todos por p o número de veces necesario. Supoñamos que algún a_i con $i \leq r$ non é divisible por p. Podemos supoñer que $i = 1$. Entón como

$p \mid 0 = q_0(a_1, ..., a_r) + pq_1(a_{r+1}, ..., a_n)$, obtemos

$$q_0(a_1, ...a_r) \equiv 0 \pmod{p}$$

e

$$\frac{\partial q_0}{\partial x_1}(a_1, ..., a_r) = 2u_1a_1 \not\equiv 0 \pmod{p}$$

Polo *teorema* **3.3.1**, q_0 representa 0.

Supoñamos agora que $p \mid a_i$ para todo $i = 1, ..., r$ (pero existe entón un $j > r$ tal que $p \nmid a_j$). Así $p^2 \mid u_1a_1^2 + ... + u_ra_r$, co cal $p^2 \mid p(u_{r+1}a_{r+1}^2 + ... + u_na_n^2)$, é dicir, $p|u_{r+1}a_{r+1}^2 + ... + u_na_n^2$. Aplicamos de novo *teorema* **3.3.1** e deducimos que q_1 representa 0.

O recíproco é claro.

(II) A demostración de "só se" é analoga ao comezo da demostración (I). Recíprocamente, supoñamos $q(a_1, ..., a_n) \equiv 0 \pmod{16}$ con $a_1, ..., a_n \in \mathbb{Z}_2$ e algún a_i non divisible por 2. Supoñamos primeiro que $2 \nmid a_i$ para algún $i \in \{1, ..., r\}$ que podemos supoñer $i = 1$. Temos

$$q(a_1, ..., a_n) \equiv 0 \pmod{8}$$

e

$$\frac{\partial q}{\partial x_1}(a_1, ..., a_n) = 2u_1a_1 \not\equiv 0 \pmod{4}$$

Entón polo *teorema* **3.3.1**, q representa 0.

Supoñamos agora que $2 \mid a_i$ para todo $i \in \{1, ..., r\}$. Poñamos $a_i = 2b_i$ con $b_i \in \mathbb{Z}_2$

Da congruencia

$$u_1 4b_1^2 + ... + u_r 4b_r^2 + 2(u_{r+1}a_{r+1}^2 + ... + u_na_n^2) \equiv 0 \pmod{16}$$

obtemos

$$2(u_1b_1^2 + ... + u_rb_r^2) + (u_{r+1}a_{r+1}^2 + ... + u_na_n^2) \equiv 0 \pmod{8}$$

Como algún a_j non é divisible por 2 con $j \in \{r + 1, ..., n\}$, usando o *teorema* **3.3.1** como antes, deducimos que $2q_0 + q_1$ representa cero.

En xeral (p non necesariamente igual a 2) unha forma q representa cero se e só se pq representa cero, e así como $pq = pq_0 + p^2q_1$ é equivalente a $pq_0 + q_1$, temos que $q_0 + pq_1$ representa cero se e só se $pq_0 + q_1$ representa cero. Isto remata a demostración.

■

Corolario 3.4.4 (I) Supoñamos $p \neq 2$. Entón q_0 representa 0 en $\mathbb{Q}_p$ se e só se a congruencia $q_0 \equiv 0 \pmod{p}$ ten unha solución $a_1, ..., a_r$ con $a_i \in \mathbb{Z}_p$ para todo i con algún $a_i \not\equiv 0 \pmod{p}$.

(II) Supoñamos $p = 2$. Se $q \equiv 0 \pmod{8}$ ten unha solución $a_1, ..., a_n$ con algún $i \in \{1, ..., r\}$ tal que $2 \nmid a_i$ ($a_i \in \mathbb{Z}_2$ para todo i), entón q representa 0 en $\mathbb{Q}_2$.

Demostración. (I) É igual ao principio da demostración da *proposición* **3.4.3** (I): Supoñamos por exemplo $a_1 \not\equiv 0 \pmod{p}$. Como $q_0(a_1, ..., a_r) \equiv 0 \pmod{p}$ e $\frac{\partial q_0}{\partial x_1}(a_1, ..., a_r) = 2u_1a_1 \not\equiv 0 \pmod{p}$, aplicando o *teorema* **3.3.1** obtemos que q representa 0.

(II) De forma similar a (I), é igual ao principio da demostración da *proposición* **3.4.3** (II).

■

Corolario 3.4.5 Sexa $p \neq 2$ e sexa $q = u_1x_1^2 + ... + u_rx_r^2$ con $u_i \in \mathbb{Z}_p^*, r \geq 3$. Entón q representa 0 en $\mathbb{Z}_p$.

Demostración. Dedúcese do *corolario* **3.4.4** (I) usando o *corolario* **3.2.3** *(II)* aplicado ao corpo $K = \mathbb{Z}_p/p\mathbb{Z}_p (= \mathbb{Z}/p\mathbb{Z})$. ■

Lema 3.4.6 Sexa K un corpo. A forma cuadrática $z^2 - ax^2 (a \neq 0)$ representa $b \in K^*$ se e só se a forma cuadrática $ax^2 + by^2 = z^2$ ten solución.

Demostración. Consecuencia inmediata do *corolario* **1.2.10**, $(I) \Leftrightarrow (III)$. ■

Observación 3.4.7 Polo *lema* **3.4.6**, se $a, b \in \mathbb{Q}_p^*$, entón $(a, b) = 1$ se e só se $z^2 - ax^2 = b$ ten solución en $\mathbb{Q}_p$, é dicir, b é a norma dun elemento $\beta \in \mathbb{Q}_p[\sqrt{a}]^*$: $b = N(z - x\sqrt{a}) := (z - x\sqrt{a})(z + x\sqrt{a})$. Claramente $N(\beta_1\beta_2) = N(\beta_1)N(\beta_2)$ e $N(\beta^{-1}) = N(\beta)^{-1}$, co cal o conxunto de normas de elementos de $\mathbb{Q}_p[\sqrt{a}]^*$ forma un subgrupo de $\mathbb{Q}_p^*$. Xuntando todo isto, dado $a \in \mathbb{Q}_p^*$, o conxunto de elementos de $b \in \mathbb{Q}_p^*$ tales que $(a, b) = 1$ é un subgrupo de $\mathbb{Q}_p^*$ que denotaremos H_a e que

coincide co conxunto dos elementos $b \in \mathbb{Q}_p^*$ tales que $z^2 - ax^2 = b$ ten solución en $\mathbb{Q}_p$.

Teorema 3.4.8 Se a é un cadrado en $\mathbb{Q}_p^*$, entón $H_a = \mathbb{Q}_p^*$. Se a non é un cadrado en $\mathbb{Q}_p^*$, entón $(\mathbb{Q}_p^* : H_a) = 2$.

Demostración. Se a é un cadrado, entón $H_a = \mathbb{Q}_p^*$ pola *proposición* **3.4.2** (III). Supoñamos entón que a non é un cadrado en $\mathbb{Q}_p^*$. Nótese que $(\mathbb{Q}_p^*)^2 \subset H_a$ pola *proposición* **3.4.2** (III).

- Supoñamos primeiro $p \neq 2$. Como $(\mathbb{Q}_p^*)^2 \subset H_a \subset \mathbb{Q}_p^*$ e $(\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2) = 4$ polo *corolario* **2.3.11** (I), é suficiente demostrar $(\mathbb{Q}_p^*)^2 \neq H_a \neq \mathbb{Q}_p^*$.

  Vexamos primeiro $(\mathbb{Q}_p^*)^2 \neq H_a$. Como $-a \in H_a$ pola *proposición* **3.4.2** (IV), se $-a$ non é un cadrado o resultado é certo. Se $-a$ é un cadrado, entón as formas cuadráticas $z^2 - ax^2, z^2 + x^2$ son equivalentes, e esta última representa todos os elementos de $\mathbb{Z}_p^*$ polo *corolario* **3.4.5**: se $u \in \mathbb{Z}_p^*$, $z^2 + x^2 - ut^2$ representa 0 polo *corolario* **3.4.5**, é dicir, existen $a, b, c \in \mathbb{Z}_p$ tales que $(a, b, c) \neq (0, 0, 0)$ e $a^2 + b^2 - uc^2 = 0$; se $c = 0$, entón $z^2 + x^2$ representa cero en $\mathbb{Q}_p$ e así representa todo elemento pola *proposición* **1.2.8**; se $c \neq 0$, $(\frac{a}{c})^2 + (\frac{b}{c})^2 = u$ e así $z^2 + x^2$ representa u. Como $H_a = N(\mathbb{Q}_p[\sqrt{a}]^*)$ e $z^2 - ax^2 = N(z - x\sqrt{a})$, vemos que $\mathbb{Z}_p^* \subset H_a$ e así $(\mathbb{Q}_p^*)^2 \neq H_a$ polo *corolario* **2.3.10** (I).

  Vexamos agora que $H_a \neq \mathbb{Q}_p^*$. Como todo elemento de $\mathbb{Q}_p$ escríbese de forma única up^n con $u \in \mathbb{Z}_p^*$, vemos que up^n é un cadrado se e só se u e p^n o son, é dicir, se e só se a é un cadrado en $\mathbb{Z}_p^*$ e n é par. Como $H_a = H_{ab^2}$ pola *proposición* **3.4.2** (II) e a non é un cadrado, se $a = up^n$, entón $a = a'b^2$ con $a' = u$, $a' = p$ ou $a' = up$ onde u non é un cadrado. Así pois é suficiente demostrar que $H_{a'} \neq \mathbb{Q}_p^*$ nestes tres casos. Pero isto dedúcese de que as formas cuadráticas

  $$ux^2 + py^2 - z^2$$
  $$px^2 + uy^2 - z^2$$
  $$upx^2 + uy^2 - z^2$$

  non representan cero pola *observación* **1.2.9** e a *proposición* **3.4.3** (I).

- Supoñamos agora $p = 2$. Polo *corolario* **2.3.11** (II), un conxunto de representantes de $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ é $\{\pm 1, \pm 5, \pm 2, \pm 10\} \subset \mathbb{Q}_2^*$. Claramente o feito de que $ax^2 + by^2 - z^2$ represente cero só depende das clases de a e b en $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. Imos ver entón en que casos $ax^2 + by^2 - z^2$ representa cero para $a, b \in \{\pm 1, \pm 5, \pm 2, \pm 10\}$. Comprobaremos todos os casos (salvo intercambiar a con b).

  – Cando $a = 1$, claramente a forma representa cero para calquera b (e analogamente cando $b = 1$).

  – Supoñamos $a, b \in \{\pm 2, \pm 10\}$. Poñamos $a = 2u, b = 2v$ con $u, v \in \{\pm 1, \pm 5\}$ unidades de $\mathbb{Z}_2$. Se existe unha solución non trivial

  $$2ux^2 + 2vy^2 - z^2 = 0$$

  podemos supoñer $x, y, z \in \mathbb{Z}_2$, e podemos supoñer que algún deles non é divisible por 2. Como $2 \mid z$, isto implica que $2 \nmid x$ ou $2 \nmid y$ e así $2 \nmid x$ e $2 \nmid y$ (pois $2 \mid z$). Sexa $z = 2t$, co que temos

  $$ux^2 + vy^2 - 2t^2 = 0$$

  Polo *corolario* **3.4.4** (II) esta igualdade equivale a

  $$ux^2 + vy^2 - 2t^2 \equiv 0 \pmod 8 \tag{3.1}$$

  onde como $x \equiv y \equiv 1 \pmod 2$, $x^2 \equiv y^2 \equiv 1 \pmod 8$. Pero $2t^2 \equiv 2 \pmod 8$ ou $2t^2 \equiv 0 \pmod 8$ (segundo que t sexa $\equiv 1$ ou $\equiv 0 \pmod 2$), co que ***(3.1)*** verifícase se e só se $u + v \equiv 0 \pmod 8$ ou $u + v \equiv 1 \pmod 8$, é dicir,

  $$ax^2 + by^2 - z^2$$

  representa cero se e só se a e b están nun dos seguintes casos:

$$\begin{array}{lll} a=2, & b=2 & (u=1,v=1) \\ a=2, & b=-2 & (u=1,v=-1) \\ a=-2, & b=2 & (u=-1,v=1) \\ a=-2, & b=-10 & (u=-1,v=-5) \\ a=10, & b=10 & (u=5,v=5) \\ a=10, & b=-10 & (u=5,v=-5) \\ a=-10, & b=10 & (u=-5,v=5) \\ a=-10, & b=-2 & (u=-5,v=-1) \end{array}$$

– Sexa agora $a \in \{\pm 2, \pm 10\}$, $b \in \{\pm 1, \pm 5\}$ (xa non repetimos o caso cambiando b por a). Sexa $a = 2u$, $b = v$. Se temos unha igualdade non trivial

$$2ux^2 + vy^2 - z^2 = 0$$

podemos supoñer como antes que $x, y, z \in \mathbb{Z}_2$ e que $y \not\equiv 0 \pmod 2$, $z \not\equiv 0 \pmod 2$. Polo *corolario* **3.4.4** (II) isto equivale a que se verifique algunha das congruencias

$$2u + v \equiv 1 \pmod 8 \qquad\qquad v \equiv 1 \pmod 8$$

(segundo $2 \nmid x$ ou $2 \mid x$), e así obtemos que

$$ax^2 + by^2 - z^2$$

representa cero exactamente nos casos

$$\begin{array}{lll} a=2, & b=-1 & (u=1,v=-1) \\ a=-2, & b=-5 & (u=-1,v=-5) \\ a=10, & b=-1 & (u=5,v=-1) \\ a=-10, & b=-5 & (u=-5,v=-5) \end{array}$$

(e nos casos $b = v = 1$ que xa estaban incluídos ao principio)

– Sexa finalmente $a, b \in \{\pm 1, \pm 5\}$, é dicir, con $a = u, b = v$,

$$ux^2 + vy^2 - z^2 = 0$$

onde podemos supoñer que de x, y, z un deles é divisible por 2 e os outros dous non o son. Distinguiremos dous casos:

- Se $2 \mid z$, entón
$$ux^2 + vy^2 \equiv u + v \pmod 4$$
e como $z^2 \equiv 0 \pmod 4$, obtemos
$$u + v \equiv 0 \pmod 4$$
Isto dános os casos
$$\begin{aligned} a = u = -1, &\quad b = v = 5 \\ a = u = 5, &\quad b = v = -5 \\ a = u = 5, &\quad b = v = -1 \\ a = u = -5, &\quad b = v = 5 \end{aligned}$$
(e algúns máis con $a = 1$ ou $b = 1$ xa contemplados ao principio).
- Se $2 \nmid z$, entón
$$ux^2 + vy^2 \equiv 1 \pmod 4$$
e como exactamente un dos números x, y divide a 2, obtemos
$$u \equiv 1 \pmod 4 \text{ (se } 2 \mid y) \quad \text{ou} \quad v \equiv 1 \pmod 4 \text{ (se } 2 \mid x)$$
é dicir, obtemos os casos:
$$\begin{aligned} a = 5, &\quad b \in \{\pm 1, \pm 5\} \\ a \in \{\pm 1, \pm 5\}, &\quad b = 5 \end{aligned}$$
(e os casos $a = 1$ ou $b = 1$ xa incluídos).

Resumindo, marcando con $+$ cando $ax^2 + by^2 - z^2$ representa cero e con $-$ en caso contrario, obtemos

a \ b	1	−1	2	−2	5	−5	10	−10
1	+	+	+	+	+	+	+	+
−1	+	−	+	−	+	−	+	−
2	+	+	+	+	−	−	−	−
−2	+	−	+	−	−	+	−	+
5	+	+	−	−	+	+	−	−
−5	+	−	−	+	+	−	−	+
10	+	+	−	−	−	−	+	+
−10	+	−	−	+	−	+	+	−

Exceptuando a primeira liña, cada liña ten exactamente catro $+$. É dicir, para todo $a \in \mathbb{Q}_2^* - (\mathbb{Q}_2^*)^2$, hai catro clases $b \pmod{(\mathbb{Q}_2^*)^2}$ tal que $ax^2 + by^2 - z^2$ representa cero. Así $(H_a \colon (\mathbb{Q}_2^*)^2) = 4$. Como $(\mathbb{Q}_2^* \colon (\mathbb{Q}_2^*)^2) = 8$ polo *corolario* **2.3.11** (II), deducimos $(\mathbb{Q}_2^* \colon H_a) = 2$ como queriamos demostrar.

■

Corolario 3.4.9 Se $a, b, c \in \mathbb{Q}_v^*$ entón

$$(a, bc) = (a, b)(a, c)$$

Demostración. Se $v = \infty$, é dicir, $\mathbb{Q}_v^* = \mathbb{R}^*$, $(a, b) = 1$ se e só se $a > 0$ ou $b > 0$ co que o resultado é claro. Supoñamos entón $v = p$ primo. Temos $(a, b) = 1$ se e só se $b \in H_a$. Como H_a é un grupo, é pechado para a multiplicación e inverso, e así se dous dos elementos b, c, bc están en H_a, entón o terceiro tamén o está. Isto proba a igualdade en todos os casos excepto cando $(a, b) = -1 = (a, c)$. Este último caso dedúcese do *teorema* **3.4.8**, xa que $(a, b) = -1 = (a, c) \Rightarrow b, c \notin H_a \Rightarrow$ as clases de b e c en $\mathbb{Q}_v^*/H_a \simeq \mathbb{Z}/2\mathbb{Z}$ correspóndense co elemento 1, e así $b \cdot c$ correspóndese con $1 + 1 = 0$, i.e., $bc \in H_a$ e así $(a, bc) = 1$. ■

Corolario 3.4.10 $(a, a) = (a, -1)$, $(a, b) = (a, -ab)$.

Demostración. A primeira igualdade dedúcese de que $(a, a) = (a, -a)(a, -1)$ e de que $(a, -a) = 1$ pola *proposición* **3.4.2** (IV). A segunda igualdade dedúcese de que $(a, -ab) = (a, -a)(a, b) = (a, b)$ ■

Corolario 3.4.11 Sexan $a, b \in \mathbb{Q}_p^*$. Poñamos $a = up^\alpha$, $b = vp^\beta$ con $u, v \in \mathbb{Z}_p^*$.

(I) Se $p \neq 2$, tense

$$(a, b) = (-1)^{\alpha\beta\frac{p-1}{2}} (\overline{u}/p)^\beta (\overline{v}/p)^\alpha$$

onde $\overline{u}$ é a imaxe de u polo homomorfismo de redución módulo p, $\mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^*$, e $(\overline{u}/p)$ é o *símbolo de Legendre*.

(II) Se $p = 2$,

$$(a, b) = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}$$

onde $\varepsilon(u)$ é a clase de $\frac{u-1}{2}$ módulo 2 e $\omega(u)$ é a clase de $\frac{u^2-1}{8}$ módulo 2.

Demostración. Polo *corolario* **3.4.9** e o *corolario* **3.4.10** temos

$$\begin{aligned}(a,b) &= (up^\alpha, vp^\beta) = (u, vp^\beta)(p^\alpha, vp^\beta) = (u,v)(u,p^\beta)(p^\alpha, v)(p^\alpha, p^\beta)\\ &= (u,v)(u,p)^\beta(p,v)^\alpha(p,p)^{\alpha\beta} = (u,v)(u^\beta,p)(v^\alpha,p)(p,p)^{\alpha\beta}\\ &= (u,v)(u^\beta v^\alpha, p)(p,p)^{\alpha\beta} = (u,v)(u^\beta v^\alpha, p)(-1,p)^{\alpha\beta}\\ &= (u,v)(u^\beta v^\alpha, p)((-1)^{\alpha\beta}, p) = (u,v)((-1)^{\alpha\beta}u^\beta v^\alpha, p)\end{aligned}$$

Imos entón calcular (u,v) e (u,p) con $u,v \in \mathbb{Z}_p^*$.

– Se $p \neq 2$, pola *proposición* **3.4.3** (I), $ux^2 + py^2 - z^2$ representa cero se e só se $ux^2 - z^2$ representa cero, é dicir, se e só se u é un cadrado. Así $(u,p) = (\overline{u}/p)$ polo corolario **2.3.10** (I). Por outra parte, polo *corolario* **3.4.9**, a forma $ux^2 + vy^2 - z^2$ representa sempre cero, e así $(u,v) = 1$. Polo tanto neste caso $(p \neq 2)$

$$\begin{aligned}(a,b) &= (u,v)((-1)^{\alpha\beta}u^\beta v^\alpha, p) = ((-1)^{\alpha\beta}u^\beta v^\alpha, p) = ((-1)^{\alpha\beta}\overline{u}^\beta\overline{v}^\alpha/p)\\ &= (-1/p)^{\alpha\beta}(\overline{u}/p)^\beta(\overline{v}/p)^\alpha = (-1)^{\alpha\beta\frac{p-1}{2}}(\overline{u}/p)^\beta(\overline{v}/p)^\alpha\end{aligned}$$

usando a *proposición* **3.1.3**.

– Se $p = 2$, de forma similar a como vimos na demostración do *teorema* **3.4.8** (de feito un caso particular do visto alí), a forma $2x^2 + vy^2 - z^2$ representa cero se e só se $v \equiv 1 \pmod 8$ ou $v \equiv -1 \pmod 8$, e así

$$(2,v) = (-1)^{\frac{\overline{v}^2-1}{8}}$$

Por outra parte, $ux^2 + vy^2 - z^2$ representa cero se e só se $u \equiv 1 \pmod 4$ ou $v \equiv 1 \pmod 4$ como vimos na mesma demostración do *teorema* **3.4.8**, é dicir

$$(u,v) = (-1)^{\frac{\overline{u}-1}{2}\frac{\overline{v}-1}{2}}$$

De todo isto deducimos que (cando $p = 2$)

$$(a,b) = (u,v)((-1)^\beta u^\beta, 2)((-1)^\alpha v^\alpha, 2) = (-1)^{\frac{\overline{u}-1}{2}\frac{\overline{v}-1}{2}}(-1)^{\beta\frac{\overline{u}^2-1}{8}}(-1)^{\alpha\frac{\overline{v}^2-1}{8}}$$

■

3.5. Fórmula produto

Sexa $V = \{p\colon p \text{ primo}\} \cup \{\infty\}$ como na sección anterior. Se $a, b \in \mathbb{Q}^*$, denotaremos por $(a,b)_v$ o símbolo de Hilbert das imaxes de a e b en $\mathbb{Q}_v$.

Teorema 3.5.1 *(Fórmula produto).* Se $a, b \in \mathbb{Q}^*$, verifícase:

(I) $(a,b)_v = 1$ para todo $v \in V$ salvo en grao sumo un número finito.

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

Demostración. Polo *corolario* **3.4.9** é suficiente tratar os casos nos que a e b son -1 ou un número primo. Cando $v = p$ primo, aplicaremos o *corolario* **3.4.11** para estes casos particulares escribindo, como é habitual, $a = up^\alpha$ e $b = u'p^\beta$ e utilizando tamén a notación de $\varepsilon(u), \omega(u)$. Lembremos que cando $v = \infty$, $(a,b) = 1$ se, e só se, $a > 0$ ou $b > 0$.

- Caso $a = b = -1$. Tense

α	u	β	u'
0	-1	0	-1

$$(-1,-1)_2 = (-1)^{\varepsilon(-1)^2+0} = -1$$
$$(-1,-1)_p = (-1)^0(\overline{u}/p)^0(\overline{u'}/p)^0 = 1 \quad \text{se } p \neq 2$$
$$(-1,-1)_\infty = -1$$

  Ademais, o produto é igual a 1.

- Caso $a = -1$, $b = l$ con l primo.

  – Se $l = 2$, tense

	α	u	β	u'
$p = 2$	0	-1	1	1
$p \neq 2$	0	-1	0	l

$$(-1,2)_2 = (-1)^{\varepsilon(-1)\varepsilon(1)+\omega(-1)} = 1$$
$$(-1,2)_p = (-1)^0(\overline{u}/p)^0(\overline{u'}/p)^0 = 1 \quad \text{se } p \neq 2 = l$$
$$(-1,2)_\infty = 1$$

  – Se $l \neq 2$, tense

	α	u	β	u'
$p=2$	0	-1	0	l
$p=l$	0	-1	1	1
$p\neq 2,l$	0	-1	0	l

$$(-1,l)_2=(-1)^{\varepsilon(-1)\varepsilon(l)+0}=(-1)^{\varepsilon(l)}=(-1/l) \quad (\textit{proposición } \textbf{3.1.3} \text{ (II)})$$
$$(-1,l)_l=(-1)^0(-1/l)^1(1/l)^0=(-1/l)$$
$$(-1,l)_p=(-1)^0(\overline{u}/p)^0(\overline{u'}/p)^0=1 \quad \text{se } p\neq 2,l$$
$$(-1,l)_\infty=1$$

Ademais, o produto é igual a 1, pois $(-1/l)(-1/l)=1$.

- Caso $a=l$, $b=l'$ con l,l' primos.

  – Se $l=l'$, polo *corolario* **3.4.10**, $(l,l)_v=(-1,l)_v$ para todo $v\in V$ e redúcese ao caso anterior.

  – Se $l\neq l'$ e se $l'=2$, tense

	α	u	β	u'
$p=2$	0	l	1	1
$p=l$	1	1	0	2
$p\neq 2,l$	0	l	0	2

$$(l,2)_2=(-1)^{\varepsilon(l)\varepsilon(1)+\omega(l)}=(-1)^{\omega(l)}=(2/l) \quad (\textit{proposición } \textbf{3.1.3} \text{ (III)})$$
$$(l,2)_l=(-1)^0(1/l)^0(2/l)^1=(2/l)$$
$$(l,2)_p=(-1)^0(\overline{u}/p)^0(\overline{u'}/p)^0=1 \quad \text{para } p\neq 2,l$$
$$(l,2)_\infty=1$$

Ademais, o produto é igual a 1, pois $(2/l)(2/l)=1$.

– Se l e l' son distintos e diferentes de 2, tense

	α	u	β	u'
$p=2$	0	l	0	l'
$p=l$	1	1	0	l'
$p=l'$	0	l	1	1
$p\neq 2,l,l'$	0	l	0	l'

$$
\begin{aligned}
(l,l')_2 &= (-1)^{\varepsilon(l)\varepsilon(l')+0} \\
(l,l')_l &= (-1)^0(1/l)^0(l'/l)^1 = (l'/l) \\
(l,l')_{l'} &= (-1)^0(l/l')^1(1/l')^0 = (l/l') \\
(l,l')_p &= (-1)^0(\overline{u}/p)^0(\overline{u'}/p)^0 = 1 \quad \text{para } p \neq 2,l,l' \\
(l,l')_\infty &= 1
\end{aligned}
$$

pero pola *Lei de reciprocidade cuadrática* (*teorema* **3.1.4**) tense

$$(l'/l)(l/l') = (-1)^{\varepsilon(l)\varepsilon(l')}$$

e polo tanto o produto é igual a $(-1)^{2\varepsilon(l)\varepsilon(l')} = 1$. Isto remata a demostración.

■

Lema 3.5.2 *(Teorema de aproximación).* A imaxe de $\mathbb{Q}$ en $\prod_{v\in S}\mathbb{Q}_v$ é densa para todo conxunto finito S de V.

Demostración. Se $S_1 \subset S_2 \subset V$ son finitos e $\mathbb{Q}$ é denso en $\prod_{v\in S_2}\mathbb{Q}_v$, entón é denso en $\prod_{v\in S_1}\mathbb{Q}_v$. Así podemos supoñer xa que $\infty \in S$. Sexan entón

$$S = \{p_1,...,p_n,\infty\} \quad (x_1,...,x_n,x_\infty) \in \mathbb{Q}_{p_1}\times ... \times \mathbb{Q}_{p_n}\times\mathbb{R}$$

Podemos multiplicar $x_1,...,x_n,x_\infty$ por un enteiro non nulo (pois en $\mathbb{Q}$ podemos dividir por el), e así podemos supoñer $x_i \in \mathbb{Z}_{p_i}$ para todo i. Imos ver que para todo $\varepsilon > 0$ e todo enteiro $N > 0$, existe $x \in \mathbb{Q}$ tal que $|x - x_\infty| < \varepsilon$, $\nu_{p_i}(x - x_i) \geq N$ para todo i. Aplicando o *Teorema chino dos restos*, existe $y \in \mathbb{Z}$ tal que $\nu_{p_i}(y - x_i) \geq N$ para todo $i = 1,...,n$. Tomando agora un primo $q \neq p_i$ para todo i, como o conxunto dos números racionais da forma $\frac{a}{q^t}$, $a,t \in \mathbb{Z}$, $t \geq 0$, é denso en $\mathbb{R}$, tomamos

$$x = y + \frac{a}{q^t}p_1^N...p_n^N$$

con a e t axeitados para que $|x - x_\infty| < \varepsilon$, é dicir, tomamos a e t tales que

$$\left|\frac{a}{q^t} - \frac{y - x_\infty}{p_1^N ... p_n^N}\right| < \frac{\varepsilon}{p_1^N ... p_n^N}$$

■

Proposición 3.5.3 Sexa $(a_i)_{i\in I}$ unha familia de elementos de $\mathbb{Q}^*$, e $(\tau_{i,v})_{i\in I, v\in V}$ unha familia de números todos eles iguais a ± 1. Entón existe $b \in \mathbb{Q}^*$ tal que $(a_i,b)_v =$

$\tau_{i,v}$ para todo $i \in I$ e todo $v \in V$ se e só se se verifican as seguintes tres condicións:

(I) Todos os $\tau_{i,v}$ salvo un número finito son iguais a 1.

(II) Para todo $i \in I$, $\prod_{v \in V} \tau_{i,v} = 1$.

(III) Para todo $v \in V$, existe $b_v \in \mathbb{Q}_v^*$ tal que $(a_i, b_v)_v = \tau_{i,v}$ para todo $i \in I$.

Demostración. A necesidade é clara: (I) e (II) dedúcense do *teorema* **3.5.1**, e (III) dedúcese tomando $b_v = b$ para todo $v \in V$.
Vexamos a suficiencia. Despois de multiplicar a_i polo cadrado dalgún enteiro, podemos supoñer que os a_i son enteiros.
Sexan

$$S = \{v \in V : v \text{ é factor primo de } a_i \text{ para algún } i\} \cup \{2, \infty\}$$
$$T = \{v \in V : \exists i \in I, \tau_{i,v} = -1\}$$

Nótese que estes conxuntos son finitos.

- Caso $S \cap T = \emptyset$. Poñamos

$$a = \prod_{\substack{l \in T \\ l \neq \infty}} l \qquad\qquad m = 8 \prod_{\substack{l \in S \\ l \neq 2, \infty}} l$$

Posto que $S \cap T = \emptyset$, os enteiros a e m son coprimos e, polo *Teorema de Dirichlet*[a], existe un número primo $p \equiv a \pmod{m}$ con $p \notin S \cup T$. Probaremos que $b = ap$ ten a propiedade buscada, i.e.,

$$(a_i, b)_v = \tau_{i,v} \quad \forall i \in I \quad \forall v \in V$$

Sexa $v \in S$. Tense $\tau_{i,v} = 1$ posto que $S \cap T = \emptyset$, e temos que comprobar que $(a_i, b)_v = 1$.

– Se $v = \infty$, séguese de que $b > 0$.

– Se v é un primo l, temos $b \equiv a^2 \pmod{m}$, e así $b \equiv a^2 \pmod{8}$ para $l = 2$, e $b \equiv a^2 \pmod{l}$ para $l \neq 2$. Posto que a *observación* **2.2.15** garante que b e a son unidades l–ádicas , polo *corolario* **2.3.10** isto proba que b é un cadrado en $\mathbb{Q}_l^*$ e temos $(a_i, b)_v = 1$.

Sexa $v = l \notin S$. Logo a_i é unha unidade l–ádica. Posto que $l \neq 2$ polo *corolario* **3.4.11** tense

$$(a_i, b)_l = (a_i/l)^{v_l(b)} \quad \forall b \in \mathbb{Q}_l^* \tag{3.2}$$

onde ν_l é a valoración l–ádica (*observación* **2.2.15**).

– Se $l \notin T \cup \{p\}$, b é unha unidade l–ádica, así $\nu_l(b) = 0$, e a igualdade **(3.2)** mostra que $(a_i, b)_l = 1$. Doutra banda, temos $\tau_{i,l} = 1$ porque $l \notin T$.

– Se $l \in T$, temos $v_l(b) = 1$. Ademais, pola condición (III) existe $b_l \in \mathbb{Q}_l^*$ tal que $(a_i, b_l)_l = \tau_{i,l}$ para todo $i \in I$. Posto que algún dos $\tau_{i,l}$ é igual a -1 (xa que $l \in T$), temos $v_l(b_l) \equiv 1 \pmod 2$ pola igualdade **(3.2)**, e así

$$(a_i, b)_l = (a_i/l) = (a_i, b_l)_l = \tau_{i,l} \quad \forall i \in I$$

– Se $l = p$, dedúcese dos casos anteriores usando a *Fórmula produto* (*teorema* **3.5.1**):

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

Logo o caso $S \cap T = \emptyset$ queda probado.

- Caso xeral. Sabemos que $(\mathbb{Q}_v^*)^2$ é un subgrupo aberto de $\mathbb{Q}_v^*$ (*corolario* **2.3.12**), e usando a *observación* **2.2.17**, obtemos que $b_v(\mathbb{Q}_v^*)^2$ tamén é aberto en $\mathbb{Q}_v$ (xa que $b_v \cdot$ resulta homeomorfismo). Entón, polo *Teorema de aproximación* (*lema* **3.5.2**), existe $b' \in \mathbb{Q}^* \cap \prod_{v \in S} b_v(\mathbb{Q}_v^*)^2$; é dicir $b' \in \mathbb{Q}^*$ tal que $b_v^{-1} b' \in (\mathbb{Q}_v^*)^2$ para todo $v \in S$.

  En particular $(a_i, b')_v = (a_i, b_v(b_v^{-1}b'))_v = (a_i, b_v)_v = \tau_{i,v}$ para todo $v \in S$ pola *proposición* **3.4.2** (II). Entón, se poñemos $\eta_{i,v} := \tau_{i,v}(a_i, b')_v$ tense

$$\eta_{i,v} = (a_i, b')_v (a_i, b')_v = (a_i, b')_v^2 = 1 \quad \forall v \in S$$

  e así $S \cap T = \emptyset$ (referíndonos aos S, T correspondentes a $(\eta_{i,v})_{i \in I, v \in V}$).

  Ademais, a familia $(\eta_{i,v})_{i \in I, v \in V}$ verifica as condicións (I), (II) (como consecuencia do *teorema* **3.5.1**)) e (III) (pois $(\eta_{i,v} = (a_i, b_v b')$ por *corolario* **3.4.9**). Polo caso $S \cap T = \emptyset$, existe $y \in \mathbb{Q}^*$ tal que $(a_i, y)_v = \eta_{i,v}$ para todo $i \in I$ e para todo $v \in V$. Se poñemos $b := yb' \in \mathbb{Q}$, b verifica

$$(a_i, b)_v = (a_i, y)_v (a_i, b')_v = \eta_{i,v}(a_i, b')_v = \tau_{i,v}(a_i, b')^2 = \tau_{i,v} \quad \forall i \in I \quad \forall v \in V$$

  onde usamos o *corolario* **3.4.9**, concluíndo a demostración.

■

[a] O *Teorema de Dirichlet* afirma que se a, m son enteiros coprimos, entón existen infinitos primos da forma $a + \lambda m$ con $\lambda \in \mathbb{Z}$. Unha demostración pode verse en [6, Chap. VI,4, Th.2].

Capítulo 4

Formas cuadráticas sobre os números p–ádicos e sobre os números reais

4.1. Formas cuadráticas sobre os corpos p–ádicos

Definición 4.1.1 Sexa q unha forma cuadrática non singular sobre un $\mathbb{Q}_p$–espazo vectorial W de dimensión n. Sexa $E = \{e_1, ..., e_n\}$ unha base ortogonal de W e sexa $a_i := b_q(e_i, e_i)$ (así o discriminante de q é $\prod_{i=1}^{n} a_i \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$) denotando tamén por a_i a clase de a_i (mód $(\mathbb{Q}_p^*)^2$). Defínese

$$\varepsilon(q, E) := \prod_{i<j} (a_i, a_j) \in \{-1, 1\} \quad (\text{se } n = 1, \varepsilon(q) = 1)$$

onde (a_i, a_j) é o *símbolo de Hilbert* (proposición **3.4.2** *(II)*).

Proposición 4.1.2 $\varepsilon(q, E)$ non depende da base ortogonal E elixida, e polo tanto podemos denotalo por $\varepsilon(q)$.

Demostración. Se $n = 1$, $\varepsilon(q, E) = 1$ para toda base ortogonal E de W.
Se $n = 2$, $\varepsilon(q, E) = 1$ se e só se $a_1x^2 + a_2y^2 - z^2$ representa cero. Polo *corolario* ***1.2.10***, isto é equivalente a que $a_1x^2 + a_2y^2$ represente 1. Isto é a súa vez equivalente a que exista $w \in W$ tal que $q(w) = 1$, e isto non depende da base elixida.
Sexa agora $n \geq 3$. Usaremos a indución en n. Sexan $E = \{e_1, ..., e'_n\}$, $E' = \{e'_1, ..., e_n\}$ dúas bases ortogonais de W e vexamos que $\varepsilon(q, E) = \varepsilon(q, E')$. Polo

teorema **1.1.14** basta probalo para o caso no que E e E' sexan contiguas (*definición* **1.1.13**), xa que a sucesión que se constrúe nel é finita. Supoñamos entón que E, E' son contiguas e sexa $e_k = e'_m$ un elemento en común. Pola *proposición* **3.4.2** (I), $\varepsilon(q, \cdot)$ resulta invariante por permutacións na base considerada, polo que podemos supoñer sen perda de xeneralidade que $e_1 = e'_1$.
Poñamos $a'_i = b_q(e'_i, e'_i)$ para todo i. Usando os *corolarios* **3.4.9** e **3.4.10** e tendo en conta que $d = a_1 ... a_n = k a'_1 ... a'_n$, $k \in (\mathbb{Q}_p^*)^2$ é o discriminante de q obtemos

$$\begin{aligned}\varepsilon(q, E) &= \prod_{i<j}(a_i, a_j) = \prod_{1<j}(a_1, a_j) \prod_{2\le i<j}(a_i, a_j) = (a_1, a_2 ... a_n) \prod_{2\le i<j}(a_i, a_j) \\ &= (a_1, a_1 a_1 a_2 ... a_n) \prod_{2\le i<j}(a_i, a_j) = (a_1, d a_1) \prod_{2\le i<j}(a_i, a_j)\end{aligned}$$

e analogamente,

$$\varepsilon(q, E') = (a_1, d a_1) \prod_{2\le i<j}(a'_i, a'_j)$$

Se agora aplicamos a hipótese de indución a $\langle e_2, ..., e_n\rangle$ e $\langle e'_2, ..., e'_n\rangle$, que son o mesmo espazo vectorial, pois ambos son o ortogonal de $\langle e_1\rangle = \langle e'_1\rangle$, tense

$$\prod_{2\le i<j}(a_i, a_j) = \prod_{2\le i<j}(a'_i, a'_j)$$

e séguese o resultado. ■

Observación 4.1.3 Lembremos que $|\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2| = 4$ se $p \neq 2$ e $|\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2| = 8$ (*corolario* **3.4.11**). Para todo $a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, sexa

$$\overline{H}_a := \{b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \colon (a, b) = 1\}$$

Entón polo *teorema* **3.4.8**, se $p \neq 2$, $|\overline{H}_1| = 4$, $|\overline{H}_a| = 2$ para todo $1 \neq a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, e se $p = 2$, $|\overline{H}_1| = 8$, $|\overline{H}_a| = 4$ para $a \neq 1$.

Lema 4.1.4 Sexan $a, a' \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$

(I) Existe $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tal que $(a, b) = 1 = (a', b)$. Se $1 \neq a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, entón existe $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tal que $(a, b) = -1$.

(II) Se $a \neq a'$ son ambos distintos de 1 en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, entón existe $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tal que $(a, b) = -1 = (a', b)$.

(III) Se $1 \neq a' \neq a$, entón existe $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ tal que $(a, b) = 1$, $(a', b) = -1$.

Demostración. (I) Tómese $b = 1$.

(II) Se $p \neq 2$, $|\overline{H}_a| = 2 = |\overline{H}_{a'}|$ e o número de elementos de $H_a \cup H_{a'}$ é ≤ 3 pola *observación* **4.1.3**. Así existe $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 - (\overline{H}_a \cup \overline{H}_{a'})$. Se $p = 2$ a demostración é análoga.

(III) Supoñamos $p \neq 2$. Se $a = 1$, basta tomar b tal que $(a', b) = -1$ (existe polo apartado (II)). Se $a \neq 1$, temos $|\overline{H}_a| = 2 = |\overline{H}_{a'}|$. Ademais $\overline{H}_a \neq \overline{H}_{a'}$ (se $\overline{H}_a = \overline{H}_{a'}$ entón $(a, c) = (a', c)$ para todo c e así $(aa', c) = (a, c)^2 = 1$ para todo c, o cal non é posible por (II), xa que $aa' \neq 1 : \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ polo *corolario* **3.4.11** (I) e así o inverso de todo elemento é el mesmo; como $a \neq a'$, $aa' = 1$). Así pois, existe $b \in H_a - H_{a'}$. A demostración cando $p = 2$ é similar.

■

Proposición 4.1.5 Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}_p$, $d \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ o seu discriminante e $\varepsilon = \varepsilon(q)$ (*definición* **4.1.1**).

(I) Se $n = 2$, q representa cero se e só se $d = -1$.

(II) Se $n = 3$, q representa cero se e só se $(-1, -d) = \varepsilon$.

(III) Se $n = 4$, q representa cero se e só se $d \neq 1$ ou $\{d = 1$ e $(-1, -1) = \varepsilon\}$.

(IV) Se $n = 5$, q sempre representa cero.

Demostración. Podemos supoñer $q = a_1x_1^2 + ... + a_nx_n^2$.

(I) Xa visto na *observación* **1.2.9**.

(II) q representa cero $\Leftrightarrow -a_3q$ representa cero $\Leftrightarrow -a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$ representa cero, e pola definición do símbolo de Hilbert, isto equivale a que $(-a_3a_1, -a_3a_2) = 1$. Polo *corolario* **3.4.9** e a *proposición* **3.4.2** (IV)

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

e así

$$(-a_3a_1, -a_3a_2) = 1 \Leftrightarrow (-1, -d) = \varepsilon(q)$$

(III) Polo *corolario* **1.2.11**, q representa cero se e só se existe un elemento $b \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ que está representado polas dúas formas

$$a_1x_1^2 + a_2x_2^2 \quad -a_3x_3^2 - a_4x_4^2$$

Polo *corolario* **1.2.10**, $a_1x_1^2 + a_2x_2^2$ representa b se e só se $a_1x_1^2 + a_2x_2^2 - bz^2$ representa cero. Polo caso $n = 3$ xa probado, isto equivale a

$$(-1, a_1a_2b) = (a_1, a_2)(a_1, -b)(a_2, -b) \tag{4.1}$$

Como

$$(-1, a_1a_2b) = (-1, a_1a_2)(-1, b)$$

e

$$(a_1, a_2)(a_1, -b)(a_2, -b) = (a_1, a_2)(a_1a_2, -b) = (a_1, a_2)(a_1a_2, -1)(a_1a_2, b)$$

(4.1) é equivalente a

$$(-1, b) = (a_1, a_2)(a_1a_2, b) \tag{4.2}$$

e como $(a_1a_2, b)^{-1}(-1, b) = (a_1a_2, b)(-1, b) = (-a_1a_2, b)$, ***(4.2)*** é equivalente a

$$(-a_1a_2, b) = (a_1, a_2) \tag{4.3}$$

Analogamente, $-a_3x_3^2 - a_4x_4^2$ representa b se e só se

$$(-a_3a_4, b) = (-a_3, -a_4) \tag{4.4}$$

Se $a_1a_2 = a_3a_4$ e $(a_1, a_2) \neq (-a_3, -a_4)$, claramente non existe b verificando ***(4.3)*** e ***(4.4)***. Nos demais casos si existe polo *lema* **4.1.4** (nótese que p.e. se $(a_1, a_2) = -1$, para aplicar o *lema* **4.1.4**, necesitamos que $-a_1a_2 \neq 1$, pero como $-1 = (a_1, a_2) = (a_1, -a_1a_2)$ polo *corolario* **3.4.10**, deducimos que $-a_1a_2 \neq 1$). Así pois q representa cero se e só se $a_1a_2 \neq a_3a_4$ (é dicir, $d = a_1a_2a_3a_4 \neq 1$ en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$), ou (cando $a_1a_2 = a_3a_4$) se $(a_1, a_2) = (-a_3, -a_4)$. Esta última condición é equivalente a $\varepsilon = (-1, -1)$ (cando $a_1a_2 = a_3a_4$), xa que

$$\begin{aligned}
\varepsilon &= (a_1, a_2)(a_3, a_4)(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4) = (a_1, a_2)(a_3, a_4)(a_1a_2, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4) = (a_1, a_2)(a_3, a_4)(-1, a_3a_4) \\
&= (a_1, a_2)((-a_3, a_4)(-1, a_4))(-1, a_3a_4) = (a_1, a_2)(-a_3, a_4)(-1, a_3a_4^2) \\
&= (a_1, a_2)((-a_3, -a_4)(-a_3, -1))(-1, a_3) = (a_1, a_2)(-a_3, -a_4)(-1, -a_3^2) \\
&= (a_1, a_2)(-a_3, -a_4)(-1, -1).
\end{aligned}$$

(IV) Supoñamos primeiro $p \neq 2$. Sexa $q = q_0 + pq_1$, coa notación da *proposición* **3.4.3**. Podemos supoñer (de novo con dita notación) que $r \geq n-r$, xa que en caso contrario substituímos q por pq (xa que se unha representa cero a outra tamén), e $pq = pq_0 + p^2q$, é equivalente a $pq_0 + q_1$, xa que verifica (reordenando as variables) $r \geq n-3$. Con esta notación, $n \geq 5 \Rightarrow r \geq 3$ e así o resultado dedúcese do *corolario* **3.4.5** e da *proposición* **3.4.3** (I).

Supoñamos agora $p = 2$. Como vimos ao principio da demostración do caso $n = 4$ (ecuación ***(4.3)***), unha forma cuadrática non singular de rango 2 representa $b \in \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ se e só se $(-d, b) = \varepsilon$. Se $-d \neq 1$, como $|\overline{H}_{-d}| = 4$, $|\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2| = 8$ pola *observación* **4.1.3**, ao menos $(-d, b) = \varepsilon$ para catro elementos $b \in \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. Se $-d = 1$, entón a forma representa cero para o caso $n = 2$ xa visto, e así representa todos os elementos de $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. En ambos casos, a forma (de rango 2) representa ao menos catro elementos e así a forma q (de rango 5) tamén. En particular q representa algún elemento a con $0 \neq a \neq d$. Polo *corolario* **1.2.10**, podemos supoñer $q = ax_1^2 + q'(x_2, ..., x_5)$. O discriminante de q' é $\frac{d}{a} \neq 1$, e así q' representa cero polo caso $n = 4$ xa probado, e por tanto q representa cero.

■

Corolario 4.1.6 Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}_p$, $a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Entón

(I) Se $n = 1$, q representa a se e só se $a = d$.

(II) Se $n = 2$, q representa a se e só se $(-d, a) = \varepsilon$.

(III) Se $n = 3$, q representa a se e só se $-d \neq a$ ou $\{-d = a \text{ e } (-1, -d) = \varepsilon\}$.

(IV) Se $n = 4$, q sempre representa a.

Demostración. Dedúcese facilmente da *proposición* **4.1.5** e do *corolario* **1.2.10** (de feito, o caso $n = 2$ xa se viu na demostración do caso $n = 4$ da *proposición* **4.1.5**). ■

Teorema 4.1.7 Dúas formas cuadráticas non singulares sobre $\mathbb{Q}_p$ son equivalentes se e só se teñen o mesmo rango, o mesmo discriminante d e o mesmo invariante ε.

Demostración. Xa sabemos que dúas formas cuadráticas equivalentes sobre $\mathbb{Q}_p$ teñen os mesmos invariantes. Para ver o recíproco, sexan q_1, q_2 dúas formas cuadráticas de rango n co mesmo d e ε. Faremos a demostración por indución en n. O caso $n = 0$ é claro. Polo *corolario* **4.1.6**, q_1 e q_2 representan os mesmos elementos de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Sexa entón $b \in \mathbb{Q}_p^*$ representado por q_1 e q_2. Polo *corolario* **1.2.10**, q_1 e q_2 son respectivamente equivalentes a $bx_1^2 + q_1'(x_2, ..., x_n)$, $bx_1^2 + q_2'(x_2, ..., x_n)$. Temos

$$bd(q_1') = d(q_1) = d(q_2) = bd(q_2')$$

e así $d(q_1') = d(q_2')$. Entón tamén $\varepsilon(q_1) = \varepsilon(q_2')$ xa que

$$\varepsilon(q_1')(b, d(q_1')) = \varepsilon(q_1) = \varepsilon(q_2) = \varepsilon(q_2')(b, d(q_2')) = \varepsilon(q_2')(b, d(q_1'))$$

Como q_1', q_2' teñen rango $n - 1$, vemos que son equivalentes pola hipótese de indución, e así q_1, q_2 son equivalentes. ■

4.2. Formas cuadráticas sobre os números reais

Sexa $\mathbb{Q}$ unha forma cuadrática non singular de rango n sobre $\mathbb{R}$. Como todo número real é un cadrado ou o oposto dun cadrado, eliminando cadrados podemos atopar unha base ortogonal na que $q = x_1^2 + ... + x_r^2 - x_{r+1}^2 - ... - x_{r+s}^2$ con $r + s = h$.

Teorema 4.2.1 (r, s) é independente da base elixida.

Demostración. Sexa $\{e_1, ..., e_n\}$ unha base onde $q = x_1^2 + ... + x_r^2 - x_{r+1}^2 - ... - x_{r+s}^2$ e $\{e_1', ...e_n'\}$ unha base onde $q = x_1^2 + ... + x_r'^2 - x_{r'+1}^2 - ... - x_{r'+s'}^2$. Supoñamos p.e. que $r < r'$. Entón $r' + s > n$ co que $\langle e_{r+1}, ..., e_s\rangle \cap \langle e_1', ..., e_r'\rangle \neq 0$. Pero se $0 \neq w \in \langle e_{r+1}, ..., e_s\rangle$, temos $q(w) > 0$ e se $0 \neq w \in \langle e_1', ..., e_r'\rangle$ temos $q(w) > 0$, o cal é unha contradición. ■

Definición 4.2.2 Chámase signatura de q ao par de números naturais (r, s).

Corolario 4.2.3 Dúas formas cuadráticas non singulares (de rango n) sobre $\mathbb{R}$ son equivalentes se e só se teñen a mesma signatura.

Demostración. Unha implicación é a do *teorema* **4.2.1** e a outra inmediata. ■

4.3. Apéndice: Formas cuadráticas sobre corpos finitos

Aínda que non o necesitamos para esta memoria, estudaremos as formas cuadráticas sobre corpos finitos, xa que a súa clasificación é moi fácil.

Sexa r a potencia dun número primo impar p, e sexa K o corpo de r elementos.

Proposición 4.3.1 Sexa q unha forma cuadrática sobre K de rango n.

(I) Se $n = 2$, q representa todos os elementos de K^*.

(II) Se $n \geq 3$, q representa todos os elementos de K.

Demostración. Supoñamos $n = 2$ e tomemos $a \in K^*$. A forma $q - az^2$ é de rango 3 e polo *corolario* **3.2.3** (II) representa cero. Así, polo *corolario* **1.2.10**, q representa a.

Supoñamos $n \geq 3$. Podemos escribir $q = q_1 + q_2$ como suma de dúas formas cuadráticas de modo que q_1 teña rango 3. Logo, q_1 representa cero (*corolario* **3.2.3** (II)) e pola *proposición 1.2.8* q_1 representa todos os elementos de K. Así, q representa tódolos elementos de K.

■

Proposición 4.3.2 Sexa q unha forma cuadrática non singular de rango n sobre K con discriminante $d \in K^*/(K^*)^2$. Entón

$$q \sim \begin{cases} x_1^2 + \ldots + x_{n-1}^2 + x_n^2 & \text{se } d \in (K^*)^2 \\ x_1^2 + \ldots + x_{n-1}^2 + dx_n^2 & \text{se } d \notin (K^*)^2 \end{cases}$$

Demostración. Usaremos indución en n. Se $n = 1$ é claro. Supoñamos $n \geq 2$. Entón, pola *proposición* **4.3.1** q representa 1, e polo *corolario* **1.2.10** temos $q \sim x_1^2 + q_1$, onde q_1 é unha forma de rango $n - 1$ co mesmo discriminante. Logo podemos aplicar a hipótese de indución a q_1. ■

Corolario 4.3.3 Dúas formas cuadráticas q, q'sobre K son equivalentes se, e só se, teñen o mesmo rango e o mesmo discriminante d.

Demostración. Séguese da *proposición* **4.3.2**. ■

Capítulo 5

Formas cuadráticas racionais

Sexa $q = a_1x_1^2 + ... + a_nx_n^2$ unha forma cuadrática non singular de rango n sobre $\mathbb{Q}$. Sexa $V = \{p\colon p \text{ primo}\} \cup \{\infty\}$. Na *definición* **4.1.1** definimos un invariante $\varepsilon_v = \prod_{i<j}(a_i, a_j)_v$ asociado á forma cuadrática q_v obtida vía a inclusión $\mathbb{Q} \to \mathbb{Q}_v$ cando $v = p$. No caso $v = \infty$, podemos escribir $q_v = x_1^2 + ... + x_r^2 - x_{r+1}^2 - ... - x_{r+s}^2$ con $n = r + s$ (sendo (r, s) a signatura de q_v). Usando o símbolo de Hilbert en $\mathbb{R}$ (*definición* **4.1.1**) podemos definir o invariante ε de q_∞ similarmente ao caso $v = p$. Como $(-1,-1)_\infty = -1, -(1,1) = (1,-1) = 1$, tense

$$\varepsilon_\infty(q) = (-1)^{\frac{s(s-1)}{2}}$$

Nótese que tamén o discriminante está determinado por s, xa que $d_\infty(q) = (-1)^s$. Así pois, a signatura de q_∞ determina os invariantes d_∞ e ε_∞.

Temos tamén que o homomorfismo canónico $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \to \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$ leva $d(q)$ en $d_v(q)$. Así mesmo, a fórmula produto (*teorema* **3.5.1**) dános

$$\prod_{v \in V} \varepsilon_v(q) = 1$$

Teorema 5.0.1 (Hasse-Minkowski). Unha forma cuadrática non singular q sobre $\mathbb{Q}$ representa cero se e só se q_v representa cero para todo $v \in V$.

Demostración. Se q representa cero, claramente q_v tamén para todo $v \in V$. Vexamos o recíproco. Podemos escribir

$$q = a_1x_1^2 + ... + a_nx_n^2 \quad a_1, ..., a_n \in \mathbb{Q}^*$$

Substituíndo q por $a_1 q$, podemos supoñer

$$q = x_1^2 + a_2 x_2^2 + ... + a_n x_n^2 \quad a_1, ..., a_n \in \mathbb{Q}^*$$

- Caso $n = 2$. Temos $q = x_1^2 - a x_2^2$. Como q_∞ representa cero, $a > 0$. Consideremos a factorización en primos distintos

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

  Como q_p representa cero, isto implica que a é un cadrado en $\mathbb{Q}_p$, e así $v_p(a)$ é par para todo p polo *corolario* **2.3.10**. Así a é un cadrado e entón q é equivalente a $x_1^2 - x_2^2$, que claramente representa cero.

- Caso $n = 3$. Poñamos $q = x_1^2 - a x_2^2 - b x_3^2$ como no caso anterior. Multiplicando por denominadores ao cadrado e eliminando cadrados, podemos supoñer que $a, b \in \mathbb{Z}$ e que son libres de cadrados, i.e., $v_p(a), v_p(b) \in \{0, 1\}$ para todo primo p. Cambiando de orde as indeterminadas se é necesario tamén podemos supoñer $|a| \leq |b|$. Demostraremos o caso $n = 3$ por indución en $m = |a| + |b|$.

  Se $m = 2$, $q = x_1^2 \pm x_2^2 \pm x_3^2$ onde ao menos hai un signo "$-$" (como q_∞ representa cero, o caso $x_1^2 + x_2^2 + x_3^2$ non ocorre), e así claramente q representa cero.

  Sexa $m > 2$. Así $|b| \geq 2$. Sexa $b = \pm p_1 ... p_t$ cos p_i primos distintos. Imos ver que a é un cadrado (mód b). Para isto é suficiente ver que a é un cadrado (mód p_i) para todo i, xa que $\mathbb{Z}/(b) = \prod \mathbb{Z}/(p_i)$ polo *Teorema chino dos restos*. Sexa $i \in \{1, ..., t\}$. Se $a \equiv 0 \pmod{p_i}$ o resultado é claro. En caso contrario, $a \in \mathbb{Z}_{pi}^*$. Sexan $\alpha, \beta, \gamma \in \mathbb{Q}_{p_i}$ tales que $\gamma^2 - a\alpha^2 - b\beta^2 = 0$, que existen por hipótese. Podemos supoñer que $\alpha, \beta, \gamma \in \mathbb{Z}_{p_i}^*$ e que algún deles non é múltiplo de p_i (como ao principio da demostración da *proposición* **3.4.3**). Como $p_i \mid b$, temos $\gamma^2 - a\alpha^2 \equiv 0 \pmod{p_i}$. Temos entón que $\alpha \not\equiv 0 \pmod{p_i}$ (do contrario $\gamma \equiv 0 \pmod{p_i}$, así $p^2 \mid b\beta^2$ co que $p_i \mid \beta$ e así p_i divide a α, β e γ). Polo tanto $a \equiv (\frac{\gamma}{\alpha})^2 \pmod{p_i}$ é un cadrado (mód p_i).

  Como a é un cadrado (mód b), existen enteiros t, b' tales que

  $$t^2 - a = bb'$$

onde podemos tomar $0 \leq t < b$ e así (cambiando t por $b - t$ que teñen o mesmo cadrado (mód b) podemos tomar $0 \leq |t| < \frac{|b|}{2}$. Ademais $t^2 - a \neq 0$, pois a non é un cadrado en $\mathbb{Z}$, e así $b' \neq 0$. Tamén é claro que o signo de b' coincide co de b xa que $t^2 - a > 0$.

Así $bb' = t^2 - a$ é a norma dun elemento da estensión de corpos $\mathbb{Q}[\sqrt{a}]|\mathbb{Q}$ (e así de $\mathbb{Q}_v[\sqrt{a}]|\mathbb{Q}_v$). De aquí deducimos que b é unha norma se e só se b' o é, e por tanto, como vimos na *observación* **3.4.7**, $q = x_1^2 - ax_2^2 - bx_3^2$ representa cero en $\mathbb{Q}$ (respectivamente $\mathbb{Q}_v$) se e só se $q' := x_1^2 - ax_2^2 - b'x_3^2$ representa cero en $\mathbb{Q}$ (respectivamente $\mathbb{Q}_v$) (o caso $v = \infty$ dedúcese de que b e b' teñen o mesmo signo). Así pois q' representa cero en $\mathbb{Q}_v$ para todo v. Ademais, $|b'| = |\frac{t^2-a}{b}| \leq \frac{|b|}{4} + 1 < b$ (nótese que as desigualdades débense respectivamente a que $|t| \leq \frac{|b|}{2}$ e $|b| \geq 2$).

Sexa $b' = b''c^2$ con b'' libre de cadrados. Seguimos tendo $|b''| < |b|$ e claramente q' representa cero en $\mathbb{Q}$ (respectivamente $\mathbb{Q}_v$) se e só se $q'' := x_1^2 - ax_2^2 - b''x_3^2$ representa cero en $\mathbb{Q}$ (respectivamente $\mathbb{Q}_v$). Aplicando a hipótese de indución, q'' representa cero en $\mathbb{Q}$ e así q tamén.

- Caso $n = 4$. Podemos escribir $q = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$. Sexa $v \in V$. Como q_v representa cero, existe $t_v \in \mathbb{Q}^*$ representado por $ax_1^2 + bx_2^2$ e por $cx_3^2 + dx_4^2$ (*corolario* **1.2.11**). Isto é equivalente a

$$(-ab, t_v)_v = (a, b)_v$$
$$(-cd, t_v)_v = (c, d)_v$$

(para $v \neq \infty$ polo *corolario* **4.1.6** (II) e o caso $v = \infty$ compróbase de forma directa caso a caso). Como $\prod_{v \in V}(a, b)_v = 1 = \prod_{v \in V}(c, d)_v$ polo *teorema* **5.0.1**, usando a *proposición* **3.5.3** obtemos que existe $x \in \mathbb{Q}^*$ tal que

$$(-ab, x)_v = (a, b)_v$$
$$(-cd, x)_v = (c, d)_v$$

para todo $v \in V$.

A forma $ax_1^2 + bx_2^2 - xz^2$ representa cero en cada $\mathbb{Q}_v$, pois pola *proposición* **4.1.5** representa cero se e só se $(-1, -d)_v = \varepsilon_v$, é dicir, se e só se $(-1, abx)_v = (a, b)_v(a, -x)_v(b, -x)_v$. Isto é equivalente a $(-1, ab)_v(-1, x)_v = (a, b)_v(ab, -x)_v$, que á súa vez equivale a

$(ab,-x)_v(ab,-1)_v(-1,x) = (a,b)_v$, é dicir, $(ab,x)_v(-1,x)_v = (a,b)_v$ ou equivalentemente $(-ab,x)_v = (a,b)_v$, que é a igualdade que tiñamos. Polo caso $n = 3$ xa probado, entón $ax_1^2 + bx_2^2 - xz^2$ representa cero en $\mathbb{Q}$. Así $ax_1^2 + bx_2^2$ representa x en $\mathbb{Q}$ polo *corolario* **1.2.10**. Analogamente $cx_3^2 + dx_4^2$ representa x en $\mathbb{Q}$. Polo *corolario* **1.2.11**, q representa cero en $\mathbb{Q}$.

- Caso $n \geq 5$. Faremos a demostración por indución en n. Sexa $q = a_1x_1^2 + ... + a_nx_n^2$ e escribamos $q = R - S$, onde $R = a_1x_1^2 + a_2x_2^2$ e $S = -(a_3x_3^2 + ... + a_nx_n^2)$. Consideremos o conxunto finito $U := \{p\colon p \text{ primo e } \exists i \geq 3, \nu_p(a_i) \neq 0\} \cup \{2,\infty\} \subset V$. Sexa $v \in U$. Posto que $q_v = R_v - S_v$ representa cero, polo *corolario* **1.2.11** (I)$\Leftrightarrow$ (II) existe $a_v \in \mathbb{Q}_v^*$ que está representado por R_v e S_v, é dicir, existen $x_i^v \in \mathbb{Q}_v$ para todo $i = 1,...,n$ tales que

$$R_v(x_1^v, x_2^v) = a_v = S_v(x_3^v, ..., x_n^v)$$

Usando a *observación* **2.2.17**, obtemos que $a_v(\mathbb{Q}_v^*)^2$ é aberto en $\mathbb{Q}_v$ por ser $(\mathbb{Q}_v^*)^2$ un subgrupo aberto de $\mathbb{Q}_v^*$ (xa que $a_v\cdot$ resulta homeomorfismo), e ademais "elevar ao cadrado" é continua (é a composición da diagonal coa multiplicación, ambas continuas) polo que $R_v\colon \mathbb{Q}_v^2 \to \mathbb{Q}_v$ é unha aplicación continua. Logo, $A_v := R_v^{-1}(a_v(\mathbb{Q}_v^*)^2)$ é un aberto de $\mathbb{Q}_v^2$. Pola densidade de $\mathbb{Q}$ en $\prod_{v\in U}\mathbb{Q}_v$ garantida polo *Teorema de aproximación* (*lema* **3.5.2**), temos que $\mathbb{Q}^m$ é denso en $(\prod_{v\in U}\mathbb{Q}_v)^m$ para calquera enteiro positivo m. Entón, vemos que

$$\mathbb{Q}^2 \cap \prod_{v\in U} A_v \neq \emptyset$$

e así existen $x_1, x_2 \in \mathbb{Q}$ tales que $(x_1,x_2) \in A_v$ para todo $v \in U$. Logo $a := R_v(x_1,x_2)$ está en $\mathbb{Q}$ e $a \in a_v(\mathbb{Q}_v^*)^2$ para todo $v \in U$.

Consideremos a forma cuadrática

$$q' := az^2 - S = az^2 + a_3x_3^2 + ... + a_nx_n^2$$

Se $v \in U$, q' representa cero en $\mathbb{Q}_v$ xa que S representa a_v en $\mathbb{Q}_v$, e entón tamén a, pois $aa_v^{-1} \in (\mathbb{Q}_v^*)^2$.

Se $p \notin U$, entón $\nu(-a_i) = 0$ para todo $i = 3,...,n$ e así os coeficientes $-a_i$ de S_p son unidades p–ádicas, e así tamén o é o seu produto, que é

o discriminante de S_p, $d(S_p)$. Posto que $p \neq 2$, o *corolario* **3.4.11** (I) garante que $(-a_i, -a_j) = 1$ para todo $i, j \geq 3$ e obtemos $\varepsilon(S_p) = 1$. Así, $d(q'_p) = -ad(S_p) = -a$ e $\varepsilon(q'_p) = (a, -d(S_p))\varepsilon(g) = (a, -d(S_p)) = (a, -1)$ (ver o cálculo na demostración da *proposición* **4.1.2**). Se $n = 5$ entón $(-1, -d(q'_p)) = (-1, a) = (a, -1) = \varepsilon(q')$ e se $n = 6$ entón en caso de que $d(q'_p) = -a = 1$, tense $\varepsilon(q'_p) = (a, -1) = (-1, -1)$. Usando a proposición **4.1.5** (II), (III) obtemos que S_p representa cero en $\mathbb{Q}_p$ para $n = 5, 6$. Se $n \geq 7$, entón xa é inmediato por *proposición* **4.1.5** (IV); así q' tamén representa cero en $\mathbb{Q}_p$ para $n \geq 5$.

En calquera caso, vemos que q' representa cero en $\mathbb{Q}_v$ para todo $v \in V$ e posto que q' ten rango $n - 1$, usando a hipótese de indución, deducimos que q' representa cero en $\mathbb{Q}$; é dicir, S representa a en $\mathbb{Q}$ (*corolario* **1.2.10**). Como ademais R representa a en $\mathbb{Q}$ deducimos que $q = R - S$ representa cero en $\mathbb{Q}$ (*corolario* **1.2.11**), como queriamos probar.

■

Corolario 5.0.2 Sexa $a \in \mathbb{Q}^*$. Unha forma cuadrática racional non singular q representa a en $\mathbb{Q}$ se e só se representa a en $\mathbb{Q}_v$ para todo $v \in V$.

Demostración. Aplíquese o *teorema* **5.0.1** a $az^2 - q$. ■

Corolario 5.0.3 Unha forma cuadrática racional non singular de rango ≥ 5 representa cero en $\mathbb{Q}$ se e só se representa cero en $\mathbb{R}$.

Demostración. *Teorema* **5.0.1** e *proposición* **4.1.5**. ■

Corolario 5.0.4 Dúas formas cuadráticas racionais non singulares q, q' son equivalentes sobre $\mathbb{Q}$ se e só se o son sobre $\mathbb{Q}_v$ para todo $v \in V$.

Demostración. Supoñamos que q e q' son equivalentes sobre $\mathbb{Q}_v$ para todo v. Claramente q e q' teñen o mesmo rango n. Faremos indución en n. Se $n = 0$ é claro. Supoñamos $n > 0$. Entón existe $a \in \mathbb{Q}^*$ representado por q e así tamén por q' polo *corolario* **5.0.2**. Polo tanto q é equivalente a unha forma $az^2 + R$ e q' a $az^2 + R'$ con R e R' de rango $< n$ (*corolario* **1.2.10**). Polo *teorema* **1.2.12**, R é equivalente a R' sobre cada $\mathbb{Q}_v$. Pola hipótese de indución, R é equivalente a R' sobre $\mathbb{Q}$. De novo polo *teorema* **1.2.12**, q é equivalente a q' sobre $\mathbb{Q}$. ■

Corolario 5.0.5 Dúas formas cuadráticas racionais non singulares son equivalentes se e só se teñen o mesmo rango, a mesma signatura, o mesmo discriminante (módulo cadrados) e para todo $v \in V$ o mesmo invariante ε_v.

Demostración. Dedúcese do *corolario* ***5.0.4***, o *teorema* ***4.1.7*** e o *corolario* ***4.2.3***. ■

Bibliografía

[1] Borevich, Z.I. and Shafarevich, I. *Number theory*. Academic Press, 1966.

[2] Neukirch, J. *Algebraic number theory*. Springer-Verlag, Berlin, 1999.

[3] Rousseau, G. *On the quadratic reciprocity law*. J.Austral. Math. Soc. (Series A), p. 423-425, 1991.

[4] Scharlau, W. *Quadratic and hermitian forms*. Springer-Verlag, Berlin, 1985.

[5] Selmer, E.S. *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. 85, p. 203-36, 1951.

[6] Serre, J-P. *A course in arithmetic*. Springer-Verlag, New York, 1973.

[7] Voloch, F. *Local-global principles for integral points on curves*. Talk, September 2012.