UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

El principi local-global per a formes quadràtiques racionals

Elena Parés Pàramo

Director: Dr. Carlos de Vera Piquero

Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 20 de juny de 2019

Abstract

The Hasse-Minkowski Theorem states that every quadratic form with rational coefficients has a non-trivial solution in the rational numbers if, and only if, it has a non-trivial solution in each completion of the rationals. We study all the completions of $\mathbb{Q}$ and present a proof of the theorem of Hasse-Minkowski using the Hilbert symbol and the theory of quadratic forms.

Resum

El Teorema de Hasse-Minkowski afirma que tota forma quadràtica amb coeficients racionals té solució no trivial en el cos dels racionals si, i només si, té solució no trivial en totes les seves completacions. En aquest treball descriurem totes les completacions de $\mathbb{Q}$ i demostrarem teorema de Hasse-Minkowksi utilitzant principalment el símbol de Hilbert i la teoria de formes quadràtiques.

2010 Mathematics Subject Classification. 11D09, 11E08, 11E12, 14G05.

Agraïments

Vull agrair al Dr. Carlos de Vera per l'acompanyament, l'interès i la constància. Gràcies per la immensitat de coneixement transmès, per posar en ordre les idees i per les valuoses correccions i propostes, que no han sigut poques. Les hores compartides han sigut un plaer i una motivació per la redacció d'aquest treball.

A en Guillem, per contagiar-me l'entusiasme per les matemàtiques, i a la Júlia, la Sol i la Núria, perquè no concebo la carrera sense la vostra companyia.

A la Berta i les meves germanes, pel suport de cada dia, que no és poc.

Índex

1 Introducció

Motivacions

L'estudi de solucions enteres en equacions polinòmiques racionals s'anomena resolució *d'equacions diofàntiques.*[2] Es tracta d'un dels problemes més importants i antics de l'aritmètica que encara es continua investigant. El seu nom ret homenatge al matemàtic grec Diophantos d'Alexandria (segle III), autor del tractat *Arithmetica.* Aquest és un text algebraic on Diophantos resol, entre molts problemes, equacions de primer i segon grau considerant només les solucions racionals positives. Cal remarcar que també va ser dels primers matemàtics a fer ús d'una notació simbòlica per desenvolupar el seu text algebraic.

És inevitable, seguit d'això, esmentar un dels exemples més motivadors, si més no conegut, de l'estudi d'equacions diofàntiques, l'anomenat *últim Teorema de Fermat*, la demostració del qual culminà a la dècada dels 90 amb els importants treballs d'Andrew Wiles i els seus col·laboradors. Aquest afirma que, per a $n \geqslant 3$, l'equació

$$X^n + Y^n = Z^n,$$

no té solucions enteres (ni racionals) tals que $XYZ \neq 0$, o sigui, que cap de les variables sigui 0. Es va trobar escrit originalment en un dels marges d'una edició de Bachet de l'*Arithmetica* i, tot i esperar més de 350 anys a ser demostrat, l'autor, Pierre de Fermat, assegurà que tenia una meravellosa demostració però no suficient espai per redactar-la.

Actualment, no hi ha algoritmes que, donada una equació diofàntica *qualsevol*, determinin si aquesta té o no solució. De fet, està demostrat que no pot existir tal algoritme! Aquest resultat és producte del treball dels matemàtics M. Davis, Y. Matiyasevich, H. Putnam i J. Robinson entre els anys 1950 i 1970, i resol negativament l'anomenat 10è Problema de Hilbert[3]. Cal destacar que per la contribució de Julia Robinson en aquest problema, la van fer membre l'any 1976 de *National Academy of Sciences*, essent la primera dona en ser-ho. Entre els anys 1982-1983, també va ser la primera dona en presidir la *American Mathematical Society.*

Ara bé, per alguns casos particulars sí que s'ha pogut determinar. Un exemple trivial són les equacions diofàntiques de primer grau, les quals són expressions del tipus

$$a_1X_1 + ... + a_nX_n = b,$$

on $a_i, b \in \mathbb{Z}$, problema que s'esmenta a l'assignatura d'Aritmètica del primer curs del grau. Perquè l'equació tingui solució és necessari i suficient que el màxim comú divisor de tots els coeficients a_i divideixi b.

És clar que si puja el grau de l'equació, la dificultat del problema augmenta, i ja no és tan senzill determinar l'existència de solucions. A més, l'interès no és només en caracteritzar l'existència de solucions, sinó també en descriure-les totes. Aquest treball se centra en respondre aquestes qüestions per a equacions diofàntiques homogènies de grau 2. Tot i presentar una dificultat molt més elevada que les de grau 1, donada una equació polinòmica homogènia de grau 2 es pot determinar si té o no solució racional, i en cas que

[2] Hi ha equacions no polinòmiques que també es consideren diofàntiques, com per exemple $x^y = y^x$ però utilitzarem aquest terme només en referència a equacions polinòmiques.

[3] De la coneguda llista de 23 problemes proposada pel matemàtic alemany D. Hilbert l'any 1900, amb ocasió del Congrés Internacional de Matemàtiques de París.

en tingui, descriure-les totes. Aquest problema va ser resolt a finals del segle XIX i inicis del segle XX, principalment pels matemàtics Kurt Hensel (1861-1941), Herman Minkowksi (1864-1909) i Helmut Hasse (1898-1979). Vegem-ne un breu recorregut històric.

Determinar les solucions enteres d'una equació diofàntica pot resultar difícil, però en canvi, donat un enter $m > 0$, buscar les solucions mòdul m és un problema finit. És immediat que si una equació té solució en $\mathbb{Z}$, aleshores necessàriament ha de tenir solució en $\mathbb{Z}/m\mathbb{Z}$, per tot enter positiu m. Per tant, no tenir solució en $\mathbb{Z}/m\mathbb{Z}$ per algun m, implica no tenir solució en $\mathbb{Z}$. A més, gràcies al Teorema xinès del residu, trobar solucions mòdul m es redueix a trobar solucions mòdul p^n, per a cada primer p tal que p^n divideix exactament m. Però pot ser una condició suficient que una equació tingui solucions en $\mathbb{Z}/m\mathbb{Z}$ per tot enter $m > 0$? En equacions polinòmiques homogènies de grau 2 sí i aquest, essencialment, és el resulat que va enunciar i demostrar Minkowski.

Una part important del treball de Hensel es va centrar en l'estudi de solucions d'equacions polinòmiques sobre els p-àdics. L'anell dels *enters p-àdics* es pot definir com el límit projectiu $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, i el seu cos de fraccions és el cos $\mathbb{Q}_p$ dels *nombres p-àdics*. Sota certes condicions, a partir d'una solució mòdul p d'una equació polinòmica sobre $\mathbb{Z}_p$, es pot construir un sistema coherent de solucions mòdul p^n per a tot $n \geqslant 1$. La noció de coherent fa referència al fet que la reducció mòdul p^n de la solució mòdul p^{n+1} coincideix amb la solució mòdul p^n. Aleshores, aquest sistema de solucions coherents dóna lloc a una solució a $\mathbb{Z}_p$ de l'equació inicial. El cos dels nombres p-àdics $\mathbb{Q}_p$ també es pot caracteritzar com la completació del cos dels racionals amb la mètrica p-àdica, $|\cdot|_p$, i de fet, aquest és el plantejament que seguirà en aquest treball. Així, ens podem sentir familiaritzats amb aquest cos com un anàleg als nombres $\mathbb{R}$ però amb una mètrica diferent. De fet, veurem que les úniques completacions de $\mathbb{Q}$ possibles són el cos dels nombres reals i el cos dels nombres p-àdics, per cada primer p, llevat d'equivalència. És immediat doncs, que el cos dels racionals $\mathbb{Q}$ està contingut en $\mathbb{Q}_p$. Aleshores, si un polinomi amb $\mathbb{Q}$-coeficients no té solució en $\mathbb{Q}_p$, per algun primer p, o en $\mathbb{R}$, no tindrà solució en $\mathbb{Q}$.

Amb aquesta construcció dels nombres p-àdics, Hasse reformulà l'enunciat inicial de Minkowski i el va demostrar amb aquesta visió p-àdica. Per aquest motiu, el teorema rep el nom d'ambdós matemàtics.

Teorema. ***(Hasse-Minkowski)***. *Un polinomi homogeni de grau 2 en $n \geqslant 1$ variables té solució en el cos dels racionals $\mathbb{Q}$ si, i només si, té solució en el cos dels reals $\mathbb{R}$ i en els cossos dels nombres p-àdics $\mathbb{Q}_p$, per tot primer p.*

Així doncs, l'existència de solució en les estructures de $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p (espais locals) ens determina l'existència de solució en $\mathbb{Q}$ (espai global).

Per finalitzar aquest apartat, i abans d'introduir-nos en el contingut del treball, és interessant destacar l'exemple de les equacions diofàntiques de grau 3, a les quals he tingut la sort de fer-ne una petita introducció en el curs optatiu de *Varietats Algebraiques*. Si bé el problema de la resolució d'equacions diofàntiques de grau 1 i 2 està entès satisfactòriament, les equacions polinòmiques de grau 3 presenten una gran immensitat de preguntes i no totes tenen resposta encara. El cas que he tingut l'oportunitat d'estudiar és el de *corbes el·líptiques*, és a dir, equacions diofàntiques de grau 3 en dues variables que definexen una corba algebraica plana no singular. Tanmateix, la definició de corba el·líptica requereix l'existència d'una solució racional, per tant, el repte no és determinar l'existència o no de solucions racionals, sinó descriure el conjunt de totes elles. Un primer resultat, producte de la geometria, l'àlgebra i la teoria de nombres, és que existeix un nombre finit de

punts amb coordenades enteres, ja que les coordenades d'aquests han de verificar certes condicions que generen un nombre finit de valors candidats.

Desafortunadament, buscar la solució en els racionals és molt diferent. No existeix cap resultat anàleg al Teorema de Hasse-Minkowski. No obstant això, l'àlgebra juga un paper molt important en aquest problema i permet determinar que el conjunt de punts racionals d'una corba el·líptica admet una estructura de grup abelià, i que a més, és finitament generat. Aquest últim fet és el Teorema de Mordell. Així doncs, per la classificació de grups abelians finitament generats, el grup abelià de les solucions racionals d'una corba el·líptica és isomorf a $T \oplus \mathbb{Z}^r$, on T és un grup finit i $r \geqslant 0$ és un enter. Doncs bé, no hi ha cap algoritme que donada una corba el·líptica *qualsevol* determini de manera efectiva l'enter r. Entrar en detalls d'aquest estudi però, seria un nou treball.

Objectius

En aquest treball estudiem el problema de l'existència de solucions racionals en equacions polinòmiques de grau 2, les quals tractem com a *formes quadràtiques*. El Teorema de Hasse-Minkowski assegura que la família de formes quadràtiques verifiquen el principi local-global amb els nombres racionals i les seves completacions. Si bé és immediat que una solució racional dóna lloc a una solució a $\mathbb{R}$ i a $\mathbb{Q}_p$, per a tot primer p, ja que $\mathbb{Q}$ és subcos de totes les seves completacions, l'altra implicació del teorema no és òbvia.

En aquest treball doncs, ens proposem:

1. Descriure totes les completacions del cos dels nombres racionals $\mathbb{Q}$, llevat d'equivalència.
2. Demostrar el Teorema de Hasse-Minkowski.

Per al primer objectiu, posarem de manifest una classificació de les mètriques en $\mathbb{Q}$ i les completacions respecte cada una d'aquestes, és a dir, la descripció dels nombres reals $\mathbb{R}$ i dels nombres p-àdics $\mathbb{Q}_p$, per tot primer p. La principal bibliografia per aquesta part és dels llibres *p-adic Numbers, p-adics Analysis and Zeta-Function*, de N. Koblitz ([5]), i *p-adic Numbers* de F. C. Gouvea ([2]).

Per al segon, caldrà fer un estudi previ sobre els símbols de Hilbert i les formes quadràtiques per abordar la demostració del teorema. El plantejament s'ha seguit, entre altres, del llibre *A Course in Arithmetic* de J. Serre ([8]) i *Lectures on elliptic curves* de J.W.S Cassels ([1]).

Estructura de la memòria

El treball comença abordant el primer objectiu plantejat, la descripció de les completacions de $\mathbb{Q}$. Aquest capítol consta de dues parts fonamentals: la demostració del Teorema d'Ostrowski, el qual enuncia una classificació de les mètriques en $\mathbb{Q}$, llevat d'equivalència, i la completació dels nombres racionals respecte aquestes mètriques. El capítol tanca amb una introducció sobre el comportament de les equacions polinòmiques en aquestes completacions de $\mathbb{Q}$.

En el següent capítol comencem amb algunes generalitzacions dels exemples amb els que hem tancat el capítol anterior, que ens ajuden a motivar el Teorema de Hasse-Minkowski i ens proporcionen també un context per aquest resultat. A més, per completar

la visió sobre el problema que tractem, veurem el fet que donada una solució racional d'una forma quadràtica, podem determinar-les totes.

Finalment, i per satisfer el segon objectiu del treball, a l'última part del treball presentem totes les eines necessàries per a la demostració completa del Teorema de Hasse-Minkowski. Veurem al quart i cinquè capítols una introducció als símbols de Hilbert i a les formes quadràtiques, amb la demostració dels resultats més importants, enfocats en base al nostre objectiu, i al sisè capítol, completem la demostració del Teorema de Hasse-Minkowski a través de tots els resultats presentats al llarg de tot el treball. Per acabar el treball, en el capítol 7 es presenten algunes conseqüències del Teorema de Hasse-Minkowski, així com la relació amb alguns resultats clàssics.

2 Nombres p-àdics

L'objectiu d'aquest capítol és descriure totes les completacions de $\mathbb{Q}$, llevat d'equivalència. La idea principal és classificar totes les possibles mètriques en el cos dels racionals, llevat d'equivalència, i considerar les seves corresponents completacions. Recordem que una possible construcció del cos dels nombres reals caracteritza $\mathbb{R}$ com la completació de $\mathbb{Q}$ amb la mètrica induïda pel valor absolut $|\cdot|$ habitual. Tanmateix, es poden definir altres normes no equivalents al valor absolut habitual i, en conseqüència, obtenir completacions de $\mathbb{Q}$ diferents del cos $\mathbb{R}$.

Així doncs, aquest primer capítol està dividit en quatre parts. En la primera, fixat un nombre primer p qualsevol, definirem la norma p-àdica $|\cdot|_p$ en $\mathbb{Q}$ i veurem algunes propietats de l'espai mètric que indueix aquesta norma sobre $\mathbb{Q}$. En el següent apartat, demostrarem el Teorema d'Ostrowski, el qual enuncia que les úniques normes no trivials en $\mathbb{Q}$, llevat d'equivalència, són el valor absolut habitual i les normes p-àdiques, per tot primer p.

En conseqüència d'aquest teorema, la completació dels nombres racionals amb la mètrica induïda per $|\cdot|_p$ és diferent de la completació de $\mathbb{Q}$ amb el valor absolut habitual $|\cdot|$. Així, l'objectiu del tercer apartat és descriure la construcció del cos dels nombres p-àdics, que anotem $\mathbb{Q}_p$, com la completació del cos dels racionals amb la norma p-àdica. Finalment, i per completar el capítol, farem una introducció al tractament de les equacions polinòmiques en $\mathbb{Q}_p$ presentant el Lema de Hensel com a eina principal.

Pel que segueix de capítol, fixem p un nombre primer qualsevol.

2.1 Norma p-àdica

Abans de definir la norma p-àdica $|\cdot|_p$ en els racionals, recordem la noció de norma en un cos k qualsevol.

Recordatori 2.1. *Una norma en un cos k és una aplicació $\|\cdot\| : k \longrightarrow \mathbb{R}^+$, tal que per a tota parella d'elements $x, y \in k$ se satisfà:*

(i) $\|x\| = 0 \Leftrightarrow x = 0$

(ii) $\|xy\| = \|x\| \cdot \|y\|$

(iii) $\|x + y\| \leqslant \|x\| + \|y\|$ *(desigualtat triangular)*

Observació 2.2. *Com a conseqüència de la propietat (ii), qualsevol norma d'un cos k satisfà $\|1\| = 1$, ja que $\|1\| = \|1 \cdot 1\| = \|1\| \cdot \|1\|$.*

Un exemple conegut de norma en el cos dels racionals és el valor absolut habitual, el qual anotem $|\cdot|$ i es defineix:

$$|x| = \begin{cases} x, & \text{si} \quad x \geqslant 0; \\ -x, & \text{si} \quad x < 0. \end{cases}$$

Previ a la definició de norma p-àdica, recordem que qualsevol enter a es pot expressar de forma única com $a = bp^\nu$, on $b \in \mathbb{Z}$, $p \nmid b$ i $\nu \in \mathbb{N}$. Així, la màxima potència de p que divideix a és ν.

Definició 2.3. *Per qualsevol nombre enter a, anomenem ordre p-àdic de a, i ho anotem $ord_p a$, a la màxima potència de p que divideix a. Si $x = \frac{a}{b}$ és un nombre racional, definim $ord_p x$ com $ord_p a - ord_p b$.*

És clar que aquesta última expressió no depèn de l'elecció de a i b.

Definició 2.4. *Anomenem norma p-àdica d'un nombre racional x, i ho anotem $|x|_p$, a:*

$$|x|_p = \begin{cases} p^{-ord_p x}, & si \quad x \neq 0; \\ 0, & si \quad x = 0. \end{cases}$$

Així, si $x = \frac{n}{m} p^\nu$ amb $p \nmid n \cdot m$, el valor de $|x|_p$ és $p^{-\nu}$. Observem que $|p|_p = p^{-1}$.

És fàcil comprovar que $|\cdot|_p$ satisfà totes les propietats de norma:

(i) $|x|_p = 0 \Leftrightarrow x = 0$, per la definició de la norma.

(ii) Si $x = \dfrac{n}{m} p^\nu$ i $y = \dfrac{u}{v} p^\sigma$, amb $p \nmid nmuv$, tenim $x \cdot y = \dfrac{nu}{mv} p^{\nu+\sigma}$. Aleshores:

$$|x \cdot y|_p = |\frac{nu}{mv} p^{\nu+\sigma}|_p = p^{-(\nu+\sigma)} = p^{-\nu} \cdot p^{-\sigma} = |x|_p \cdot |y|_p$$

(iii) Seguint la notació anterior, podem suposar $\nu \leqslant \sigma$ i, per tant, $|x|_p \geqslant |y|_p$. Aleshores:

$$|x + y|_p = |p^\nu (\frac{n}{m} + \frac{u}{v} p^{\sigma-\nu})|_p = |p^\nu|_p \, |(\frac{nv + mup^{\sigma-\nu}}{mv})|_p$$

Com $p \nmid m$ i $p \nmid v$, és clar que $p \nmid m \cdot v$. En conseqüència:

$$ord_p(\frac{nv + mup^{\sigma-\nu}}{mv}) \geqslant 0 \ \text{ i, per tant, } \ |(\frac{nv + mup^{\sigma-\nu}}{mv})|_p \leqslant 1.$$

Aquesta última expressió serà exactament 1 només en el cas que $p \nmid (nv + mup^{\sigma-\nu})$, ja que aleshores

$$ord_p(\frac{nv + mup^{\sigma-\nu}}{mv}) = 0 \quad \text{i} \quad |(\frac{nv + mup^{\sigma-\nu}}{mv})|_p = 1.$$

Així:

$$|x + y|_p = |p^\nu|_p \, |(\frac{nv + mup^{\sigma-\nu}}{mv})|_p \leqslant p^{-\nu} = |x|_p.$$

Per tant, $|x + y|_p \leqslant |x|_p + |y|_p$.

Comprovant la tercera propietat de norma hem demostrat en particular que $|\cdot|_p$ satisfà:

$$|x + y|_p \leqslant max\{|x|_p, |y|_p\} \leqslant |x|_p + |y|_p.$$

Més encara, si $|x|_p \neq |y|_p$, es té la igualtat $|x + y|_p = \max\{|x|_p, |y|_p\}$. Tenim doncs, que la norma p-àdica compleix una propietat més forta que la desigualtat triangular. Aquestes normes les anomenem *ultra-mètriques o no-arquimedianes*. Així, l'espai $(\mathbb{Q}, |\cdot|_p)$ és un espai mètric no-arquimedià amb la distància entre dos nombres $x, y \in \mathbb{Q}$ definida per

$$d(x, y) = |x - y|_p = p^{-ord_p(x-y)}.$$

Notem que dos nombres són més propers com més alta sigui la potència de p que divideix la seva diferència. Per això, en els espais no arquimedians, algunes propietats geomètriques i topològiques poden resultar poc òbvies com per exemple que tots els triangles són isòsceles i que tot punt d'un disc obert o tancat és centre del disc. Vegem aquests dos exemples en l'espai $(\mathbb{Q}, |\cdot|_p)$.

(a) Siguin $d_p(x,y)$, $d_p(x,z)$ i $d_p(y,z)$ la mesura de tres costats d'un triangle i suposem que $d_p(x,z) < d_p(y,z)$.

Com $d_p(\cdot,\cdot)$ és una distància ultra-mètrica, es compleix

$$d_p(x,y) \leqslant max\{d_p(x,z), d_p(y,z)\} = d_p(y,z).$$

Ara bé,

$$d_p(y,z) \leqslant max\{d_p(x,y), d_p(x,z)\} = d_p(x,y),$$

ja que per hipòtesi $d_p(x,z) < d_p(y,z)$. Per tant, $d_p(x,y) = d_p(y,z)$, és a dir, el tercer costat del triangle mesura igual que el costat de longitud màxima.

Mirat en termes de divisibilitat, considerant la definició de la norma p-àdica, és fàcil veure que si els costats $d_p(x,z)$ i $d_p(y,z)$ són divisibles per diferents potències de p, la seva diferència serà divisible exactament per la potència menor. Per tant, tindrà la mateixa norma que el costat divisible per aquesta potència, és a dir, el costat amb la norma p-àdica més gran.

(b) Vegem l'exemple dels discs oberts i tancats. Considerem el disc obert de radi r amb centre $a \in \mathbb{Q}$

$$D_p(a,r) = \{x \in \mathbb{Q} : |x-a|_p < r\},$$

i sigui $b \in D_p(a,r)$. Volem veure que b és centre del disc $D_p(a,r)$, és a dir, que $D_p(a,r) = D_p(b,r)$. En efecte, sigui $x \in D_p(a,r)$, demostrem que $x \in D_p(b,r)$, és a dir, que $|x-b|_p < r$.

$$|x-b|_p = |x-a+a-b|_p \leqslant max\{|x-a|_p, |a-b|_p\} < r,$$

ja que per hipòtesi $|a-b|_p < r$ i $|x-a|_p < r$. Anàlogament veiem que si $x \in D_p(b,r)$, aleshores $x \in D_p(a,r)$ i, per tant, $D_p(a,r) = D_p(b,r)$.

De fet, hem demostrat que el conjunt $D_p(a,r)$ és a la vegada obert i tancat. En efecte, sabem que $D_p(a,r)$ és obert. Vegem que també és tancat. Sigui x un punt de la frontera de $D_p(a,r)$. Així, per qualsevol $s > 0$, $D_p(x,s) \cap D_p(a,r) \neq \emptyset$. Escollim $s \leqslant r$ i sigui $y \in D_p(x,s) \cap D_p(a,r)$. Es compleix que

$$|y-a| < r \quad \text{i} \quad |y-x|_p < s \leqslant r.$$

Per tant, $|x-a|_p \leqslant max\{|y-a|_p, |y-x|_p\} < r$ i $x \in D_p(a,r)$.

2.2 Classificació de les mètriques en $\mathbb{Q}$

El Teorema d'Ostrowski afirma que en el cos dels racionals les úniques mètriques no trivials que hi podem definir són la mètrica induïda pel valor absolut habitual i les induïdes per les normes p-àdiques, llevat d'equivalència. Donat que la norma del valor absolut habitual i les normes p-àdiques, per tot primer p, són no equivalents dos a dos, aquest teorema dóna una classificació de totes les mètriques possibles en $\mathbb{Q}$, llevat d'equivalència.

L'objectiu d'aquest apartat és demostrar el Teorema d'Ostrowski i el fet que les normes $|\cdot|, |\cdot|_p$, per tot primer p, són no equivalents dos a dos. Previ a això, recordem la definició d'equivalència de normes i vegem una caracterització d'aquest concepte que facilitarà les demostracions.

2.2.1 Equivalència de normes

Siguin $\|\cdot\|_1$ i $\|\cdot\|_2$ dues normes sobre un mateix espai vectorial X que indueixen les distàncies d_1, d_2. Diem que $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents si indueixen respectivament la mateixa topologia en X. És a dir, si per qualsevol conjunt U en X, U és a obert a (X, d_1) si, i només si, U és obert a (X, d_2). Observem que aquesta definició correspon al fet que donat un punt x de X qualsevol, tota bola oberta centrada en x per la distància d_1 conté alguna bola oberta centrada en x per la distància d_2, i al revés. Tanmateix, per a la demostració del Teorema d'Ostrowski, volem utilitzar una caracterització d'equivalència que enunciem en la següent proposició.

Proposició 2.5. *Dues normes $\|\cdot\|_1$ i $\|\cdot\|_2$ en $\mathbb{Q}$ no trivials són equivalents si, i només si, existeix un nombre real positiu α tal que $\|x\|_1 = \|x\|_2^\alpha$, per qualsevol $x \in \mathbb{Q}$.*

Demostració. Suposem que existeix α tal que per qualsevol $x \in \mathbb{Q}$, $\|x\|_1 = \|x\|_2^\alpha$. Vegem que en aquesta situació, tota bola oberta en $(\mathbb{Q}, d_1)$ conté una bola oberta de $(\mathbb{Q}, d_2)$. Sigui $B_1(a, r)$ una bola centrada en a i de radi r en $(\mathbb{Q}, d_1)$. Aleshores, $B_2(a, r^{1/\alpha})$ és una bola oberta en $(\mathbb{Q}, d_2)$ continguda en $B_1(a, r)$. En efecte, si $x \in B_2(a, r^{1/\alpha})$, es compleix $\|x - a\|_2 < r^{1/\alpha}$ i, donat que $\|x\|_1 = \|x\|_2^\alpha$, tenim:

$$\|x - a\|_1^{1/\alpha} < r^{1/\alpha} \Rightarrow \|x - a\|_1 < r \Rightarrow x \in B_1(a, r).$$

Anàlogament, $B_2(a, r^{1/\alpha})$ en $(\mathbb{Q}, d_2)$ conté la bola oberta $B_1(a, r)$:

$$x \in B_1(a, r) \Rightarrow \|x - a\|_1 < r \Rightarrow \|x - a\|_2^\alpha < r \Rightarrow x \in B_2(a, r^{1/\alpha}).$$

Així doncs, les normes $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents.

Suposem ara que $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents. La condició de no trivialitat sobre les normes ens assegura l'existència d'un element $x_0 \in \mathbb{Q}$ tal que $\|x_0\|_1 > 1$ i anàlogament amb $\|\cdot\|_2$. En efecte, si suposem $\|\cdot\|$ no trivial i que per tot $x \in \mathbb{Q}$ es compleix $\|x\| < 1$, arribem fàcilment a una contradicció:

$$\|1\| = 1 = \|x \cdot x^{-1}\| = \|x\| \cdot \|x^{-1}\| < 1.$$

Per tant, existeix $x_0 \in \mathbb{Q}$ tal que $\|x_0\|_1 > 1$. Per continuar amb la demostració, vegem el següent resultat:

Lema 2.6. *Si dues normes $\|\cdot\|_1$, $\|\cdot\|_2$ són equivalents, aleshores les condicions $\|x\|_1 < 1$ i $\|x\|_2 < 1$ són equivalents.*

Demostració. Per definició, les boles relatives a aquestes normes,

$$\{B_1(a, r) : a \in \mathbb{Q}, r > 0\} \quad i \quad \{B_2(a, r) : a \in \mathbb{Q}, r > 0\},$$

constitueixen dues bases de la mateixa topologia en $\mathbb{Q}$. Així, podem parlar d'oberts sense especificar per quina topologia. Notem que:

(i) La condició $\|x\|_1 < 1$ implica que $\lim_{n\to\infty} \|x^n\|_1 = 0$. Per tant, per a qualsevol obert U contenint el 0, existeix un $N \in \mathbb{N}$ tal que $x^n \in U$, per a tot $n \geqslant N$.

(ii) Si $\|x\|_1 \geqslant 1$, aleshores existeix un obert V contenint 0 tal que V no conté cap dels x^n. Per exemple, podem prendre V com la bola oberta de radi 1 centrada a 0.

Així, la condició $\|x\|_1 < 1$ és equivalent a dir que qualsevol obert U que contingui el 0 conté tots els x^n excepte un nombre finit. El mateix raonament es pot fer també amb la norma $\|\cdot\|_2$. Per tant, les condicions $\|x\|_1 < 1$ i $\|x\|_2 < 1$ són ambdues equivalents a la mateixa condició: que qualsevol obert U que contingui el 0 conté tots els x^n excepte un nombre finit. Per tant, si $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents, $\|x\|_1 < 1$ si, i només si, $\|x\|_2 < 1$. $\square$

Aleshores, tornant a la demostració de la proposició, pel fet que $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents, si x_0 té norma $\|x_0\|_1 > 1$, aleshores $\|x_0\|_2 > 1$ també. Sigui α el valor real positiu tal que $\|x_0\|_2 = \|x_0\|_1^\alpha$. Volem veure que per tot $x \in \mathbb{Q}$, se satisfà $\|x\|_2 = \|x\|_1^\alpha$.

Sigui $x \in \mathbb{Q}^*$ un valor qualsevol. Existeix $\beta \in \mathbb{R}$ tal que $\|x\|_1 = \|x_0\|_1^\beta$ i podem trobar dues successions d'enters $\{m_i\}, \{n_i\}$ tals que:

$$\beta = \lim_{i\to\infty} \frac{m_i}{n_i}, \quad \text{amb} \quad \frac{m_i}{n_i} > \beta, \quad \text{per tot índex} \quad i.$$

Aleshores, $\|x\|_1 = \|x_0\|_1^\beta < \|x_0\|_1^{m_i/n_i}$ per qualsevol i. D'aquesta expressió deduïm

$$\frac{\|x\|_1}{\|x_0\|_1^{\frac{m_i}{n_i}}} < 1, \quad \text{i per tant,} \quad \frac{\|x\|_1{}^{n_i}}{\|x_0\|_1^{m_i}} = \|\frac{x^{n_i}}{x_0^{m_i}}\|_1 < 1.$$

Aleshores, pel Lema 2.6, $\|\frac{x^{n_i}}{x_0^{m_i}}\|_2 < 1$. Per tant, $\|x\|_2 < \|x_0\|_2^{m_i/n_i}$. Si ho passem al límit, s'obté la desigualtat:

$$\|x\|_2 \leqslant \|x_0\|_2^\beta.$$

Ara bé, si fem el mateix raonament però escollint les successions $\{m_i\}, \{n_i\}$ tals que per tot índex i,

$$\beta = \lim_{i\to\infty} \frac{m_i}{n_i}\ , \text{amb} \quad \frac{m_i}{n_i} < \beta,$$

obtenim la desigualtat contrària: $\|x_0\|_2^\beta \leqslant \|x\|_2$. Per tant, $\|x\|_2 = \|x_0\|_2^\beta$, i en conseqüència,

$$\|x\|_2 = \|x_0\|_2^\beta = \|x_0\|_1^{\alpha\beta} = \|x\|_1^\alpha, \quad \textit{per qualsevol} \quad x \in \mathbb{Q}^*,$$

és a dir, existeix un valor $\alpha \in \mathbb{R}^+$ tal que $\|\cdot\|_2 = \|\cdot\|_1^\alpha$. $\square$

Corol·lari 2.7. *Dues normes $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents si, i només si, les condicions $\|x\|_1 < 1$ i $\|x\|_2 < 1$ són equivalents.*

Demostració. Ambdues implicacions s'han vist en la demostració de la proposició anterior. Amb el Lema 2.6 hem demostrat que si les condicions $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents, aleshores $\|\cdot\|_1 < 1$ si, i només si, $\|\cdot\|_2 < 1$ són equivalents. Seguit, hem vist que si les $\|\cdot\|_1 < 1$ i $\|\cdot\|_2 < 1$ són equivalents, aleshores existeix $\alpha \in \mathbb{R}^+$ tal que $\|\cdot\|_1^\alpha = \|\cdot\|_2$. I per tant, per la Proposició, $\|\cdot\|_1$ i $\|\cdot\|_2$ són equivalents. $\square$

En conseqüència d'aquest corol·lari es pot deduir el següent resultat.

Corol·lari 2.8. *L'única norma equivalent a la norma trivial és la norma trivial.*

2.2.2 Teorema d'Ostrowski

Hem acabat demostrant en l'apartat anterior dues caracteritzacions per a normes equivalents. Utilitzarem la caracterització del primer corol·lari per demostrar que les normes

$|\cdot|$, $|\cdot|_p$ són no equivalents dos a dos, per tot primer p, i la de la proposició per demostrar el Teorema d'Ostrowski. Amb aquestes dues demostracions finalitzarem aquest apartat de classificació de les mètriques en el cos dels nombres racionals.

Proposició 2.9. *Les normes $|\cdot|$, $|\cdot|_p$, per tot primer p, són no equivalents dos a dos.*

Demostració. Vegem primer que $|\cdot|$ no és equivalent a $|\cdot|_p$, per cap primer p. Notem que per tot enter $n > 1$, $|n| > 1$ i $|n|_p \leqslant 1$, per tot primer p. Per tant, pel Lema 2.6, les normes $|\cdot|$ i $|\cdot|_p$ són no equivalents, per cap primer p.

Només falta comprovar que si p i ℓ són dos primers diferents, la norma $|\cdot|_p$ no és equivalent a la norma $|\cdot|_\ell$. Aquest fet és clar amb un argument similar a l'anterior, ja que $|p|_p = p^{-1} < 1$ i $|p|_\ell = 1$. $\square$

Teorema 2.10. ***(Ostrowski).*** *Tota norma no trivial $\|\cdot\|$ a $\mathbb{Q}$ és equivalent o bé a la norma $|\cdot|$ o bé a la norma p-àdica $|\cdot|_p$, per algun primer p.*

Demostració. Sigui $\|\cdot\|$ una norma no trivial en $\mathbb{Q}$. Per demostrar el teorema, distingim dos casos: en el primer suposem que existeix algun enter positiu n tal que $\|n\| > 1$ i en segon cas, suposem que per a tot enter positiu n es compleix $\|n\| \leqslant 1$.

Pel Lema 2.6, observem que en el primer cas, $\|\cdot\|$ no pot ser equivalent a la norma p-àdica perquè aquesta última pren valors $\leqslant 1$ per tot nombre enter i, en efecte, veurem que es equivalent a la norma $|\cdot|$. Pel mateix raonament, en el segon cas, $\|\cdot\|$ no pot ser equivalent al valor absolut habitual, i veurem que és equivalent, per un nombre primer p unívocament determinat, a $|\cdot|_p$.

Primer cas. Suposem que existeix un enter n positiu tal que $\|n\| > 1$. Sigui n_0 l'enter positiu més petit que ho compleix. Com que $\|n_0\| > 1$, existeix un nombre real positiu α tal que $\|n_0\| = n_0^\alpha$.

Sigui n un enter positiu qualsevol i l'escrivim de la forma:

$$n = a_0 + a_1 n_0^1 + ... + a_s n_0^s \quad on \quad 0 \leqslant a_i < n_0 \quad i \quad a_s \neq 0.$$

Aleshores, de les propietats de norma es dedueix que:

$$\|n\| \leqslant \|a_0\| + \|a_1\| n_0^\alpha + ... + \|a_s\| n_0^{\alpha s}.$$

Notem que tots els coeficients $a_i < n_0$ tenen norma < 1 per l'elecció de n_0. En conseqüència:

$$\|n\| \leqslant 1 + n_0^\alpha + ... + n_0^{s\alpha} = n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + ... + n_0^{-s\alpha}) \leqslant n_0^{s\alpha}\left[\sum_{i=0}^{\infty}\left(\frac{1}{n_0^\alpha}\right)^i\right].$$

Donat que $n \geqslant n_0^s$ perquè $a_s \neq 0$, tenim $\|n\| \leqslant n^\alpha \left[\sum_{i=0}^{\infty}\left(\frac{1}{n_0^\alpha}\right)^i\right]$.

Si definim $C := \sum_{i=0}^{\infty}\left(\frac{1}{n_0^\alpha}\right)^i$, aleshores: $\|n\| \leqslant Cn^\alpha$. Notem que aquest valor C no depèn de n. Aleshores, $\|n^N\| \leqslant Cn^{N\alpha}$ i, per tant, $\|n\| \leqslant \sqrt[N]{C}n^\alpha$. Quan $N \to \infty$, obtenim:

$$\|n\| \leqslant n^\alpha \tag{1}$$

Ara bé, és fàcil demostrar la desigualtat contrària. Per fer-ho, observem que:

(i) $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leqslant \|n\| + \|n_0^{s+1} - n\|$. Per tant, $\|n\| \geqslant \|n_0^{s+1}\| - \|n_0^{s+1} - n\|$.

(ii) Com que $n_0^s \leqslant n < n_0^{s+1}$, se satisfà $n_0^{s+1} - n > 0$ i, en conseqüència de (1), tenim:

$$\|n_0^{s+1} - n\| \leqslant (n_0^{s+1} - n)^\alpha.$$

Així, per les observacions (i) i (ii), $\|n\| \geqslant \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^\alpha$, i podem escriure:

$$\|n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^\alpha = n_0^{(s+1)\alpha} - (n_0^{s+1}(1 - \frac{1}{n_0}))^\alpha =$$

$$= n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right] = n_0^{(s+1)\alpha}\, C' \geqslant n^\alpha\, C'.$$

Igual que el procés anterior, C' tampoc depèn de n. Per tant, se satisfà $\|n\| \geqslant n^\alpha \sqrt[N]{C'}$ i quan $N \to \infty$, s'obté $\|n\| \geqslant n^\alpha$. És a dir, la desigualtat contrària a l'anterior. Per tant:

$$\|n\| = n^\alpha.$$

Tenint en compte les propietats de norma, si $x = \dfrac{n}{m} \in \mathbb{Q}$ podem expressar la norma $\|x\|$ com $|x|^\alpha$ on α és un valor fixat i independent de x. Per tant, $\|\cdot\|$ i $|\cdot|$ són normes equivalents.

Segon cas. Suposem que $\|n\| \leqslant 1$ per tot enter positiu n. Sigui n_0 l'enter positiu més petit tal que $\|n_0\| < 1$. Aquest element existeix perquè per hipòtesi $\|\cdot\|$ és no trivial i, a més, n_0 és un nombre primer. En efecte, si n_0 no fos primer, tindríem $n_0 = n_1 \cdot n_2$ on $1 < n_1, n_2 < n_0$. Però $\|n_1\| = \|n_2\| = 1$ per l'elecció del nombre n_0. En conseqüència $\|n_0\| = 1$, en contradicció amb la hipòtesi. Aleshores per facilitar la lectura de la demostració, anotem $p := n_0$, i de fet, demostrarem que la norma $\|\cdot\|$ és equivalent a la norma $|\cdot|_p$.

Per fer-ho, observem primer que per a qualsevol nombre primer q, tal que $q \neq p$, es compleix $\|q\| = 1$. En efecte, suposem $\|q\| < 1$. Per a dos enters N, M suficientment grans es compleix $\|q^N\| < \frac{1}{2}$ i $\|p^M\| < \frac{1}{2}$.

Aleshores $\|q^N\| + \|p^M\| < \frac{1}{2} + \frac{1}{2} = 1$. Ara bé, com p i q són coprimers, q^N i p^M també ho seran. Per la identitat de Bézout, existeixen enters n, m tals que $1 = nq^N + mp^M$, i en conseqüència de les propietats de norma:

$$\|1\| = \|nq^N + mp^M\| \leqslant \|n\|\|q^N\| + \|m\|\|p^M\|.$$

Però per hipòtesi, $\|n\|, \|m\| \leqslant 1$. Per tant, $1 \leqslant \|q^N\| + \|p^M\| < 1$, contradicció. Observem que per la hipòtesi de $\|\cdot\|$ en el segon cas, tampoc podria ser $\|q\| > 1$. Així, tot nombre primer q diferent de p satisfà $\|q\|$=1. Vegem ara l'equivalència amb la norma p-àdica.

Qualsevol racional x positiu el podem factoritzar en un quocient de productes de primers diferents:

$$x = \frac{p_1^{b_1} \cdot \ldots \cdot p_r^{b_r}}{p_{r+1}^{b_{r+1}} \cdot \ldots \cdot p_{r+s}^{b_{r+s}}}, \quad on \;\; b_i = ord_{p_i} x.$$

Com a màxim, un únic valor dels p_i satisfà $p_i = p$. Anotem per $\rho := \|p_i\| = \|p\| < 1$, i notem que $\|p_j\| = 1$ per a tot $j \neq i$. Aleshores, de les propietats de norma,

$$\|x\| = \rho^{ord_p x}.$$

Observem que:

- $|x|_p = p^{-ord_p x}$.
- $\|x\| = \rho^{ord_p x}$, on $\rho = \|p\|$ és un valor entre 0 i 1.

Si $\rho = p^{-1}$, és clar que $\|\cdot\|$ i $|\cdot|_p$ són la mateixa norma. Ara bé, en general ρ pot prendre qualsevol valor de l'interval $(0,1)$, però és fàcil veure que es satisfà:

$$(\rho^{ord_p(x)})^\alpha = p^{-ord_p(x)} \quad on \quad \alpha = -log_\rho(p).$$

Notem que α no depèn del valor de l'element x i, per tant, $\|\cdot\|^\alpha = |\cdot|_p$, és a dir, la norma $\|\cdot\|$ i la norma $|\cdot|_p$, on $p := n_0$, són equivalents. □

Hem demostrat doncs, que qualsevol norma no trivial en $\mathbb{Q}$ serà o bé arquimediana (i per tant, equivalent a $|\cdot|$) o bé no-arquimediana i equivalent a $|\cdot|_p$, per un primer p unívocament determinat. Aquesta classificació de les diferents mètriques en $\mathbb{Q}$ ens permet descriure totes les completacions del cos dels nombres racionals, el principal objectiu d'aquest capítol.

2.3 Completacions de $\mathbb{Q}$

Recordem alguns conceptes bàsics en referència a la completació d'un cos.

Recordatori 2.11. *Sigui $(k, \|\cdot\|)$ un espai mètric.*

- *Diem que la successió $\{a_i\} \subset k$ és una successió de Cauchy si per qualsevol $\varepsilon > 0$ existeix $n_0 \in \mathbb{N}$ tal que per tot $i, i' > n_0$, $\|a_i - a_{i'}\| < \varepsilon$.*
- *Diem que la successió $\{a_i\} \subset k$ és una successió convergent a un punt $a \in k$ si, per qualsevol $\varepsilon > 0$, existeix $n_0 \in \mathbb{N}$ tal que per tot $i > n_0$, $\|a_i - a\| < \varepsilon$.*

  Observem que tota successió convergent és una successió de Cauchy.
- *Diem que $(k, \|\cdot\|)$ és un espai complet si tota successió de Cauchy és convergent.*

El cos dels nombres racionals amb el valor absolut habitual $|\cdot|$ és un espai incomplet, ja que hi ha successions de Cauchy sense límit. Per exemple la successió $1.4, 1.41, 1.414, 1.4142...$ convergeix al nombre $\sqrt{2} \notin \mathbb{Q}$. El cos dels reals és l'extensió mínima de $\mathbb{Q}$ on totes les successions de Cauchy convergeixen amb la norma del valor absolut habitual estesa.

Amb la norma p-àdica, $\mathbb{Q}$ tampoc és un cos complet, així, té sentit buscar la completesa del cos dels racionals amb la mètrica induïda per $|\cdot|_p$. En efecte, veurem més endavant, amb el Lema de Hensel, que podem trobar una successió d'elements racionals $\{x\} = \{x_0, x_1, ...\}$ que són solució mòdul p^n d'una equació polinòmica que no té solució en $\mathbb{Q}$. Aleshores, el límit d'aquesta successió és solució de l'equació polinòmica i per tant, pren un valor que no pertany en $\mathbb{Q}$.

Des d'aquest punt de vista $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p, són estructures anàlogues respecte del cos dels racionals i construïdes amb la mateixa motivació i, pel Teorema d'Ostrowski, aquestes són les úniques completacions de $\mathbb{Q}$, llevat d'equivalència.

2.3.1 Construcció del cos $\mathbb{Q}_p$

Sigui S el conjunt de successions de Cauchy $\{a_i\} \subset \mathbb{Q}$ respecte de la norma $|\cdot|_p$. Diem que dues successions $\{a_i\}$, $\{b_i\} \in S$ són *equivalents* si $|a_i - b_i|_p \to 0$ quan $i \to \infty$. Aleshores, el conjunt de classes d'equivalència de les successions de Cauchy respecte de la norma $|\cdot|_p$ s'anomena *cos dels nombres p-àdics* i l'anotem $\mathbb{Q}_p$.

Identifiquem els elements $x \in \mathbb{Q}$ a través de les successions constants $\{x\}$, és a dir, tal que tots els seus elements són iguals x. En aquest cas, si $x, x' \in \mathbb{Q}$, $\{x\} \sim \{x'\}$ si, i només si, $x = x'$.

En aquest espai definim la norma $|\cdot|_p$ d'una classe d'equivalència a com $|a|_p = \lim_{i\to\infty} |a_i|_p$, on $\{a_i\}$ és qualsevol representant de la classe. Vegem que aquest límit existeix, que està ben definit i que és una extensió de la norma $|\cdot|_p$ en $\mathbb{Q}$. Remarquem que, fent un abús de notació, ambdues normes les anotem igual.

Per demostrar que el límit existeix, considerem $a \in \mathbb{Q}_p$ una classe d'equivalència i $\{a_i\}$ un representant qualsevol.

- Si $a = 0$, tenim per definició que $\lim_{i\to\infty} |a_i|_p = 0$
- Si $a \neq 0$, aleshores per alguna $\varepsilon > 0$ i qualsevol enter $N > 0$, existeix $i_N > N$ tal que $|a_{i_N}|_p > \varepsilon$. Per hipòtesi, $\{a_i\}$ és de Cauchy, així, si escollim N suficientment gran, tenim $|a_i - a_{i'}|_p < \varepsilon$ per qualsevol $i, i' \geq N$. Aleshores, $|a_i - a_{i_N}|_p < \varepsilon$ per tot $i > N$, és a dir $|a_i - a_{i_N}|_p < |a_{i_N}|_p$.

  Ara bé, hem vist que si $|x|_p < |y|_p$ aleshores, $|x - y|_p = |y|_p$. Per tant, si per qualsevol $i > N$, es compleix que $|a_i - a_{i_N}|_p < |a_{i_N}|_p$, tenim $|a_i|_p = |a_{i_N}|_p$ per tot $i > N$. Així doncs, el $\lim_{i\to\infty} |a_i|_p$ existeix i pren el valor constant $|a_{i_N}|_p$.

Per veure que està ben definit, observem que el valor del límit no depèn del representant de classe escollit. Siguin $\{a_i\}, \{b_i\}$ dos representants qualssevol de la classe d'equivalència a. Volem veure que $\lim_{i\to\infty} |a_i|_p = \lim_{i\to\infty} |b_i|_p$.

- Si $a = 0$, és clar que $\lim_{i\to\infty}\{a_i\} = \lim_{i\to\infty}\{b_i\} = 0$ i per tant, no depèn del representant.
- Si $a \neq 0$, aleshores, per alguna $\varepsilon > 0$ i qualsevol enter $N > 0$, existeix $i_N > N$ tal que $|a_{i_N}|_p > \varepsilon$.

  Ara bé, com $\{a_i\} \sim \{b_i\}$, si N és suficientment gran, tenim $|a_{i_N} - b_i|_p < \varepsilon$, és a dir, $|a_{i_N} - b_i|_p < |a_{i_N}|_p$, per tot $i > N$. Així, pel mateix motiu que en la demostració sobre l'existència del límit, tenim $|b_i|_p = |a_{i_N}|_p$ per tot $i > i_N$. Per tant, $\lim_{i\to\infty} |a_i|_p = \lim_{i\to\infty} |b_i|_p = |a_{i_N}|_p$.

En particular, observem dos fets. Primer, que la norma $|\cdot|_p$ en $\mathbb{Q}_p$ pren valors en $p^{\mathbb{Z}} \cup \{0\}$, on $p^{\mathbb{Z}} := \{p^m : m \in \mathbb{Z}\}$, exactament igual que la norma $|\cdot|_p$ en $\mathbb{Q}$. En segon lloc, la norma $|\cdot|_p$ en $\mathbb{Q}_p$ restringida a $\mathbb{Q}$ és exactament $|\cdot|_p$ en $\mathbb{Q}$. En efecte, tot element $a \in \mathbb{Q}$ s'identifica a $\mathbb{Q}_p$ com la successió constant $a_i = a$ per tot i. Així,

$$|a|_p = \lim_{i\to\infty} |a_i|_p = \lim_{i\to\infty} |a|_p = |a|_p.$$

En aquesta expressió es fa evident l'abús del llenguatge anotant les dues normes iguals, però s'identifica en cada igualtat a quina ens estem referint.

Hem iniciat aquesta part anomenant $\mathbb{Q}_p$ *cos* dels nombres p-àdics. En efecte, vegem que $\mathbb{Q}_p$ té estructura de cos.

Donades dues classes d'equivalència a i b, la suma i la resta de classes estan ben definides. Siguin $\{a_i\}, \{b_i\}$ dos representants respectius, definim $a \pm b$ com $\{a_i \pm b_i\}$. Observem que aquesta definició és independent dels representants escollits. En efecte, siguin $\{a_i'\}, \{b_i'\}$ dos altres representants de les classes a, b respectivament. Vegem-ho per la suma:

$$\begin{aligned}\lim_{i\to\infty} |a_i + b_i - (a_i' + b_i')|_p &= \lim_{i\to\infty} |a_i - a_i' + b_i - b_i'|_p \\ &\leqslant \lim_{i\to\infty} max\{|a_i - a_i'|_p, |b_i - b_i'|_p\} = 0.\end{aligned}$$

Així, $\{a_i + b_i\} \sim \{a_i' + b_i'\}$, tal com volíem veure.

Definim, utilitzant la mateixa notació anterior, la multiplicació entre classes com $a \cdot b := \{a_i \cdot b_i\}$. Comprovem que tampoc depèn dels representants escollits.

$$\begin{aligned}\lim_{i\to\infty} |a_i \cdot b_i - (a_i' \cdot b_i')|_p &= \lim_{i\to\infty} |a_i(b_i - b_i') + b_i'(a_i - a_i')|_p \\ &< \lim_{i\to\infty} max\{|a_i(b_i - b_i')|_p, |b_i'(a_i - a_i')|_p\} = 0,\end{aligned}$$

on aquesta última igualtat l'obtenim de

$$\lim_{i\to\infty} |a_i(b_i - b_i')|_p = |a|_p \lim_{i\to\infty} |(b_i - b_i')|_p = |a|_p \cdot 0 = 0,$$

i anàlogament amb l'altre terme.

Sigui $b \in \mathbb{Q}_p$ tal que $b \neq 0$. Si $\{b_i\}$ és un representant que no té termes nuls, podem definir la classe inversa com $b^{-1} := \{1/b_i\}$. Ara bé, un representant qualsevol de b pot tenir termes nuls. Tanmateix, com b no pertany a la classe del zero, ha de tenir un nombre finit de termes nuls. En aquest cas, podem construir la successió $\{b_i'\}$ tal que $b_i' = b_i$ si $b_i \neq 0$ i $b_i' = p^i$ per tots els índexs i tals que $b_i = 0$, i es verifica $\{b_i'\} \sim \{b_i\}$. Així, per qualsevol representant de la classe b podem trobar una successió equivalent sense termes nuls i definirr la classe inversa de b^{-1} com abans. Es pot comprovar que aquesta definició no depèn del representant.

En definitiva, el conjunt de les classes d'equivalència $\mathbb{Q}_p$ amb totes les operacions anteriors definides és un cos. Comprovem que $(\mathbb{Q}_p, |\cdot|_p)$ és un espai mètric complet.

Proposició 2.12. *$\mathbb{Q}_p$ és complet amb la norma p-àdica $|\cdot|_p$.*

Demostració. Sigui $\{a_j\}_{j=1,2\ldots}$ una successió de Cauchy de classes d'equivalència de $\mathbb{Q}_p$. Per cada classe a_j, podem pendre un representant $\{a_{ji}\}_{i=1,2\ldots}$ que és successió de Cauchy. És a dir, per qualsevol ε, existeix N tal que $|a_{ji} - a_{ji'}|_p < \varepsilon$ per tot $i, i' > N$.

En particular, per qualsevol j, existeix N_j tal que $|a_{ji} - a_{ji'}|_p < p^{-j}$ per tot $i, i' > N_j$. Veurem que $\lim_{j\to\infty}\{a_j\}$ és exactament la successió $\{a_{jN_j}\}$.

Per tot $i > N_j$, $|a_{ji} - a_{jN_j}|_p < p^{-j}$, per tant:

$$\lim_{j\to\infty} |a_{ji} - a_{jN_j}|_p = 0, \quad \text{per tot} \quad i > N_j.$$

Així doncs, la successió $\{a_j\} \subset \mathbb{Q}_p$ és convergent a $\{a_{jN_j}\} \in \mathbb{Q}_p$. □

Si bé treballar en el cos $\mathbb{Q}_p$ com un conjunt de classes d'equivalència de successions de Cauchy pot resultar complicat, amb el següent teorema podem tractar els elements de

$\mathbb{Q}_p$ utilitzant una expressió canònica únicament determinada que facilita el tractament. La demostració del resultat es pot consultar en [5], capítol I, teorema 2 o bé seguint l'explicació en [2] al capítol 3, al llarg de l'apartat *3.3 Exploring* $\mathbb{Q}_p$.

Teorema 2.13. *Tota classe d'equivalència* $a \in \mathbb{Q}_p$ *tal que* $|a|_p \leq 1$ *té exactament una única representació de la forma* $\{a_i\}$ *que compleix:*

(i) $0 \leq a_i < p^i$, *per* $i = 1, 2, 3...$

(ii) $a_i \equiv a_{i+1} (mod\, p^i)$ *per* $i = 1, 2, 3...$

En altres paraules, si $|a|_p \leqslant 1$ i $\{a_i\}$ n'és una representació, aleshores existeix un únic desenvolupament de la forma $a_i = b_0 + b_1 p + ... + b_{i-1} p^{i-1}$ amb $b_i \in \{0, ..., p-1\}$. Aquesta representació, quan $i \to \infty$, l'anomenem *expansió p-àdica* de a.

Observem que si $|a|_p > 1$, aleshores podem multiplicar a per una potència $p^m \geqslant |a|_p$, de manera que $a' = ap^m$ satisfà $|a'|_p \leqslant 1$. Així si $\{a'_i\}$ és un representant de a', tenim $a'_i = b_0 + b_1 p + ... + b_{i-1} p^{i-1}$ i podem escriure els termes $\{a_i\}$ com

$$a_i = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + b_{i-1} p^{i-1-m}.$$

Quan $i \to \infty$ també l'anomenem expansió p-àdica de a.

Aquesta expressió per a nombres racionals positius és simplement l'expressió del nombre en base p. Ara bé, pot desconcertar si pensem en l'expansió p-àdica d'un nombre racional negatiu, ja que tots els termes per expressar a_i plantejats al teorema són positius. Vegem l'exemple de -1 a través d'un raonament que utilitza la definició de suma de classes en $\mathbb{Q}_p$.

Sabem que $1 + (-1) = 0$, i que podem expressar $1, -1$, i 0 com elements de $\mathbb{Q}_p$ de la forma:

$$1 = 1 + \sum_{i=1}^{\infty} 0 \cdot p^i, \quad -1 = \sum_{i=0}^{\infty} b_i p^i \ \text{ i } \ 0 = \sum_{i=0}^{\infty} 0 \cdot p^i.$$

Com que $1 + (-1) = 0$, aleshores:

$$\left(1 + \sum_{i=1}^{\infty} 0 \cdot p^i\right) + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} 0 \cdot p^i.$$

Per tant, $1 + b_0$ o bé és 0, o bé és p (i en aquest últim cas "en portaríem 1"a la següent suma de termes). Per hipòtesi, $b_i \in \{0, ..., p-1\}$, per tant, l'única opció és $b_0 = p - 1$ i conseqüentment, $1 + b_0 = p$.

Seguint el procés, $0 + b_1 + 1$ (on aquest $+1$ ve de la suma de $1 + b_0$) ha de ser o bé 0, o bé p. Anàlogament, tenim doncs que $b_1 = p - 1$. Aplicant reiteradament aquest raonament, podem escriure

$$-1 = \sum_{i=0}^{\infty} (p-1) p^i.$$

i, pel Teorema 2.13, sabem que aquesta expressió és única.

2.3.2 Anell dels enters p-àdics

Considerem el conjunt $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a| \leqslant 1\}$. Pel teorema anterior, el subconjunt $\mathbb{Z}_p$ és el conjunt de números de $\mathbb{Q}_p$ que no tenen potències negatives de p en l'expansió p-àdica, i l'anomenem conjunt d'*enters p-àdics*. És fàcil comprovar que $\mathbb{Z}_p$ és un subanell, ja que la suma, la resta i el producte de dos elements de $\mathbb{Z}_p$ és també un element de $\mathbb{Z}_p$ i clarament, $0, 1 \in \mathbb{Z}_p$.

El grup multiplicatiu $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : 1/x \in \mathbb{Z}_p\}$ d'elements invertibles en $\mathbb{Z}_p$, o *unitats p-àdiques*, està format pels elements que no són múltiples de p. En efecte, si $x \in \mathbb{Z}_p$, aleshores $|x|_p \leqslant 1$. Ara bé, si $1/x$ també està en $\mathbb{Z}_p$, aleshores $|1/x|_p \leqslant 1$. En conseqüència, per les propietats de norma, cal que $|x|_p = 1$. Així, també podem escriure:

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : |x|_p = 1\} = \{x \in \mathbb{Z}_p : x \not\equiv 0 (mod \ \ p)\}.$$

L'únic ideal maximal de $\mathbb{Z}_p$ és $p\mathbb{Z}_p$, i el quocient $\mathbb{Z}_p/p\mathbb{Z}_p$ s'identifica naturalment amb el cos $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ de p elements.

Del fet $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : |x|_p = 1\} = \{x \in \mathbb{Q}_p : |x|_p = 1\}$ i que la norma $|\cdot|$ en $\mathbb{Q}_p$ prèn valors $p^{\mathbb{Z}} \cup \{0\}$, se segueix facilment que

$$\mathbb{Q}_p^* = \{u \cdot p^n : u \in \mathbb{Z}_p^*, n \in \mathbb{Z}\}.$$

2.4 Equacions polinòmiques en $\mathbb{Q}_p$

En aquesta secció veurem alguns resultats importants sobre les arrels de polinomis amb coeficients p-àdics. És raonable preguntar-se si $\mathbb{Q}_p$ és un cos algebraicament tancat. Vegem amb l'exemple d'una equació senzilla que no ho és. Sigui $x^2 = p$, i suposem que té solució, és a dir, que existeix $a \in \mathbb{Q}_p$ tal que $a^2 = p$. Calculant la norma a cada costat de la igualtat, i aplicant les propietats d'aquesta tenim:

$$|a|_p^2 = |p|_p = p^{-1}, \quad \text{és a dir,} \quad |a|_p = \frac{1}{\sqrt{p}}.$$

Sabem per la definició de norma $|\cdot|_p$ en $\mathbb{Q}_p$ que $|a|_p = \lim_{i\to\infty} |a_i|_p = |a_N|_p$, on $a_N \in \mathbb{Q}$. Per tant, existeix $a_N \in \mathbb{Q}$ tal que $|a_N|_p = \dfrac{1}{\sqrt{p}}$, contradient el fet que la norma $|\cdot|_p$ en $\mathbb{Q}_p$ pren valors en $p^{\mathbb{Z}} \cup \{0\}$. Així, el cos $\mathbb{Q}_p$ no és algebraicament tancat per cap p i, en particular hem demostrat que $\sqrt{p} \notin \mathbb{Q}_p$ per tot primer p.

El cos dels reals tampoc és un cos algebraicament tancat però afegint l'element $i = \sqrt{-1}$ s'obté una extensió quadràtica de $\mathbb{R}$ que és algebraicament tancada i a més, completa. En el cos dels nombres p-àdics, la construcció de la clausura algebraica dóna lloc a una extensió $\overline{\mathbb{Q}_p}$ de grau infinit sobre $\mathbb{Q}$ i la norma p-àdica en $\mathbb{Q}_p$ s'estén de manera única a $\overline{\mathbb{Q}_p}$ (també l'anotem $|\cdot|_p$). Aquest últim cos, però, no és un cos complet amb la norma p-àdica estesa. Completant $\overline{\mathbb{Q}_p}$ s'obté un cos Ω que és algebraicament tancat i complet. Aquest cos Ω el podem pensar com l'anàleg de $\mathbb{C}$ en el cas p-àdic. Podem trobar en [5], capítol III, o bé en [2], capítol 5, la descripció completa i detallada de la construcció del cos Ω.

2.4.1 Lema de Hensel

Una eina molt important en l'estudi algebraic dels cossos p-àdics és el Lema de Hensel, el qual ens assegura, sota certes hipòtesis, l'existència d'una solució en $\mathbb{Z}_p^n$ d'una equació

polinòmica $f(X_1, ..., X_n) \in \mathbb{Z}_p[X_1, ..., X_n]$.

La idea és que ens permet construir una successió $\{x_1, x_2, ...\}$ de punts en $\mathbb{Z}_p^n$ de Cauchy i, com $\mathbb{Q}_p$ és un espai complet, aquesta successió és convergent a un punt de $\mathbb{Q}_p^n$. Si x és aquest límit, vegem per construcció que $x \in \mathbb{Z}_p^n$ i verifica $f(x) = 0$. Aquest teorema es troba enunciat amb diferents versions i en aquest treball el presentem com es fa en [8], capítol II, secció *2.2 Amelioration of aproximate solutions* i on també s'hi pot consultar la demostració.

Lema 2.14. ***(de Hensel)*** *Sigui $f \in \mathbb{Z}_p[X_1, ..., X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $j \in \{0, ..., m\}$ i $n \in \mathbb{N}$, tal que se satisfà:*

$$f(x) \equiv 0 \ (mod \ \ p^n) \quad i \quad ord_p\left(\frac{\partial f}{\partial X_j}(x)\right) = 0.$$

Aleshores, existeix $y = (y_i) \in (\mathbb{Z}_p)^m$ tal que

$$f(y) \equiv 0(mod \ p^{n+1}) \ \ , \ \ ord_p\left(\frac{\partial f}{\partial Y_j}(y)\right) = 0 \ \ i \ \ y \equiv x(mod \ p^n).$$

En el cas particular $n = 1$ i una sola variable ($m = 1$), el Lema de Hensel ens diu que donada una funció $f \in \mathbb{Z}_p[X]$ i una solució $x_0 \in \mathbb{Z}_p$ mòdul p tal que $p \nmid f'(x_0)$. Aleshores existeix $x_1 \in \mathbb{Z}_p$ que satisfà

$$f(x_1) \equiv 0(mod \ p^2), \quad x_1 \equiv x_0(mod \ p) \ \text{ i } \ p \nmid f(x_1).$$

Un exemple d'aplicació del Lema de Hensel és en la construcció d'una successió de Cauchy de nombres racionals que no convergeix a $\mathbb{Q}$ amb la norma p-àdica. Aquest fet l'hem deixat indicat en la introducció de l'apartat 2.3. Vegem-ho.

Proposició 2.15. *$\mathbb{Q}$ no és complet amb la norma p-àdica $|\cdot|_p$.*

Demostració. Sigui $p \neq 2$. Escollim un nombre enter a lliure de quadrats tal que $p \nmid a$ i a sigui un residu quadràtic mòdul p. Aleshores l'equació $f(X) = X^2 - a$ no té solució en $\mathbb{Q}$ però existeix $x_0 \in \mathbb{Z}$ tal que $x_0^2 \equiv a \ (mod \ p)$ i $p \nmid f'(x_0) = 2x_0$. Pel Lema de Hensel, existeix x_1 tal que

$$f(x_1) \equiv 0 \ (mod \ p^2), \quad x_1 \equiv x_0 \ (mod \ p), \quad \text{i} \ \ p \nmid f'(x_1).$$

Aleshores, podem tornar a aplicar aquest resultat sobre la nova solució x_1. Repetint el procediment, obtenim una successió $\{x_0, x_1, x_2, ...\}$ de nombres racionals tals que:

$$f(x_n) \equiv 0 \ (mod \ p^{n+1}), \quad x_n \equiv x_{n-1} \ (mod \ p^n) \ \ i \ \ p \nmid f'(x_n).$$

En conseqüència de la segona congruència, la successió és de Cauchy, ja que

$$|x_{n+1} - x_n|_p \leqslant p^{-(n+1)}.$$

Ara bé, la successió és convergent a $\sqrt{a} \notin \mathbb{Q}$. En efecte, $|x_n^2 - a|_p \leqslant p^{-(n+1)}$. Per tant, $\mathbb{Q}$ amb la norma p-àdica no és complet.

Pel cas $p = 2$, podem aplicar un argument anàleg escollint $f(X) = X^3 - 3$ i $x_0 = 3$. $\square$

Observem que, per la llei de reciprocitat quadràtica, si $p \equiv 1 \ (mod \ 4)$ podem escollir $a = -1$ i utilitzar $f(X) = X^2 + 1$ en la demostració anterior. En particular, $\sqrt{-1} \in \mathbb{Q}_p$ per tot $p \equiv 1 \ (mod \ 4)$. Per exemple, si $p = 5$, podem aplicar el Lema de Hensel amb la solució inicial $x_0 = 2 \in \mathbb{Z}_p$, ja que satisfà

$$f(2) \equiv 0(mod \ 5) \ \text{ i } \ f'(x_0) = 2x_0 = 4 \ \text{ no és divisible per p.}$$

2.4.2 Nombres quadrats en $\mathbb{Q}_p^*$

Vist aquests exemples d'equacions quadràtiques i, enfocat en la continuació d'aquest treball, tancarem aquest capítol demostrant la caracterització dels nombres quadrats en $\mathbb{Q}_p^*$. En tota aquesta secció, suposarem $a \neq 0$ i p senar. El cas dels quadrats en $\mathbb{Q}_2^*$ el veurem al final de la secció.

Proposició 2.16. *Un element $a \in \mathbb{Q}_p^*$ és quadrat si, i només si, $a = up^n$ per algun n parell i $u \in \mathbb{Z}_p^*$ tal que u és quadrat mòdul p.*

Demostració. Suposem $a \in \mathbb{Q}_p^*$ quadrat. Aleshores $a = b^2$ per algun $b \in \mathbb{Q}_p^*$, $b = vp^m$, $m \in \mathbb{Z}$ i $v \in \mathbb{Z}_p^*$, i per tant,

$$b^2 = v^2 p^{2m} = a,$$

on clarament v^2 és un residu quadràtic a $\mathbb{F}_p$.

Suposem que $a = up^{2n}$, on $u \in \mathbb{Z}_p^*$ és un quadrat a $\mathbb{Z}_p^*$. Aleshores, apliquem el Lema de Hensel a l'equació $X^2 - a = 0$, ja que en efecte, existeix v tal que $v^2 \equiv u \ \ (mod\ p)$, i v verifica $v^2 - a \equiv 0 \pmod p$ i $p \nmid 2v$. □

Corol·lari 2.17. *El subgrup $\mathbb{Q}_p^{*2}$ d'elements quadrats de $\mathbb{Q}_p^*$ és un subgrup obert de $\mathbb{Q}_p^*$.*

Demostració. Sigui $x \in \mathbb{Q}_p^{*2}$. Volem veure que existeix $\varepsilon > 0$, tal que $\forall y \in \mathbb{Q}_p^*$ que $|x - y|_p < \varepsilon$, es compleix $y \in \mathbb{Q}_p^{*2}$.

Podem escriure $x = p^{2n}u^2$ on $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$, per tant $|x|_p = p^{-2n}$. Notem que n depèn unívocament de x. Sigui $\varepsilon = \varepsilon(x) = p^{-2n}$ i sigui $y \in \mathbb{Q}_p^*$ tal que $|x-y|_p < \varepsilon = p^{-2n}$. Tenim

$$|x|_p = p^{-2n} \quad i \quad |x - y|_p < p^{-2n}.$$

Per les propietats ultra-mètriques vistes anteriorment, $|y|_p = p^{-2n}$. Per tant, podem escriure $y = p^{2n}v$, on v és una unitat p-àdica. Així, la desigualtat anterior la reescrivim:

$$|x - y|_p = |p^{2n}(u^2 - v)|_p = p^{-2n}|u^2 - v|_p < p^{-2n}.$$

Per tant, $|u^2 - v|_p < 1$. Això implica $v \equiv u^2 (mod\, p)$. És a dir, v és un quadrat en $\mathbb{Z}_p^*$. Aleshores és clar que $y \in \mathbb{Q}_p^{*2}$ tal com volíem veure. □

Observació 2.18. *El producte de dos nombres quadrats qualssevol de $\mathbb{Q}_p^*$ i el producte dos nombres no quadrats qualssevol en $\mathbb{Q}_p^*$ és un quadrat a $\mathbb{Q}_p^*$. Ara bé, el producte d'un nombre quadrat amb un nombre no quadrat no és un quadrat a $\mathbb{Q}_p^*$. Així, si fem el quocient de $\mathbb{Q}_p^*$ mòdul quadrats, $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, un conjunt de representants serà $\{1, u, p, up\}$ on $u \notin \mathbb{Q}_p^{*2}$.*

Vegem ara, i per tancar la secció, la caracterització dels quadrats en $\mathbb{Q}_2^*$.

Proposició 2.19. *Sigui $a \in \mathbb{Q}_2^*$. Una condició suficient i necessària perquè a sigui un quadrat en $\mathbb{Q}_2^*$ és que $a = u2^n$, per n parell i $u \equiv 1 \ (mod\ 8)$.*

Demostració. Suposem $a \in \mathbb{Q}_2^*$ quadrat. Aleshores $a = b^2$ per algun $b \in \mathbb{Q}_2^*$, $b = v2^m$, $m \in \mathbb{Z}$ i $v \in \mathbb{Z}_2^*$. Per tant, $n = 2m$ i $u = v^2 \equiv 1 \ (mod\ 8)$.

La suficiència es prova anàlogament que el cas p senar, en aquest cas aplicant el Lema de Hensel en $f(X) = X^3 + 1$ i $n = 3$. □

Respecte el corol·lari on demostrem que, per p senar, el subgrup de nombres quadrats $\mathbb{Q}_p^{*2}$ és un conjunt obert, pel cas $p = 2$ es demostra de forma similar.

Observació 2.20. *Si fem el quocient de $\mathbb{Q}_2^*$ mòdul quadrats, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, un conjunt de representants serà $\{1, 3, 5, 7, 2, 3 \cdot 2, 5 \cdot 2, 7 \cdot 2\}$.*

3 Teorema de Hasse-Minkowski

Un cop vista la construcció dels cossos dels nombres p-àdics, en aquest capítol enunciarem el Teorema de Hasse-Minkowski, resultat central d'aquest treball. Per posar aquest resultat en context, descriurem primer algunes generalitats i exemples de la resolució d'equacions polinòmiques sobre els racionals, especialment de còniques planes. També introduirem el concepte de *principi local-global* per a qüestions diofàntiques.

3.1 Punts racionals en còniques

Sigui C una cònica general no singular. Un canvi de variables adequat, transforma la seva expressió en una del tipus $f(X,Y) = aX^2 + bY^2 + c$. D'una manera natural, podem preguntar-nos si existeix sempre una solució racional, i en cas afirmatiu si n'hi ha infinites. Un mètode que pot semblar correcte per trobar punts racionals en la cònica pot ser calcular la intersecció d'aquesta cònica amb una recta racional, ja que podem pensar que els punts de la intersecció tindran coordenades racionals. Però en general això no és cert. En efecte, si considerem el cercle $X^2 + Y^2 = 1$ i la recta $X = Y$, els punts d'intersecció del cercle amb la diagonal satisfan l'equació $2X^2 = 1$, és a dir, $x = \pm\frac{1}{\sqrt{2}} \notin \mathbb{Q}$.

Ara bé, si partim d'un punt racional $P = (x_0, y_0)$ en C, aleshores qualsevol recta R amb coeficients racionals que passi per P talla la cònica en un punt P' racional, amb $P = P'$ només si R és tagent a C en P. Així, donat un punt racional de la cònica, podem determinar tota la resta de punts racionals a través de les coordenades d'aquest (i n'hi haurà infinits, un per cada recta que passa per P). En efecte, el sistema de l'equació de la recta racional juntament amb l'equació de la cònica es redueix a un polinomi de segon grau, una arrel del qual ja sabem que és racional (ja que és una de les coordenades de P), i en conseqüència, l'altra arrel també ho serà. Vegem-ho.

Considerem el feix de rectes racionals que passen pel punt $P = (x_0, y_0)$:

$$X = x_0 \text{ i } Y = sX + y_0 - sx_0, \quad s \in \mathbb{Q}.$$

En primer lloc, si resolem l'equació $aX^2 + bY^2 + c = 0$ quan $X = x_0$, tenim:

$$Y = \sqrt{\frac{-c - ax_0^2}{b}} = \pm y_0 \in \mathbb{Q}.$$

Per tant, si (x_0, y_0) és solució racional de la cònica, clarament, $(x_0, -y_0)$ també és solució i racional.

En segon lloc, si $Y = sX + y_0 - sx_0$, aleshores $aX^2 + bY^2 + c = aX^2 + b(sX + y_0 - sx_0)^2 + c$, d'on resulta la següent equació:

$$(a + bs^2)X^2 + (2bsy_0 - 2bs^2x_0)X + (by_0^2 + bs^2x_0^2 - 2bsy_0x_0 + c) = 0.$$

Observem que si tenim $AX^2 + BX + C = 0$ i x_0, x_1 són les arrels, aleshores $x_0 + x_1 = \frac{-B}{A}$. Per tant:

$$x = \frac{-(2bsy_0 - 2bs^2x_0)}{a + bs^2} + x_0,$$

$$y = s(\frac{-(2bsy_0 - 2bs^2x_0)}{a + bs^2} + x_0) + y_0 - sx_0.$$

Com que $s, y_0, x_0 \in \mathbb{Q}$, aleshores $x, y \in \mathbb{Q}$ són solució racional de la cònica. Per tant, conèixer un punt racional de C ens permet tenir-los tots. De fet, aquesta idea consisteix projectar tots els punts racionals (menys un) d'una cònica sobre una recta afí, amb una correspondència d'un a un entre els punts racionals de la recta i els de cònica. Aleshores, donat qualsevol punt Q de la recta afí, la recta R entre P i Q talla la cònica en un únic punt P', i viceversa.

Aquest raonament es recolza en l'existència d'un punt racional en la cònica. Així doncs, la dificultat està a determinar quan hi ha solució racional i quan no.

3.2 Principi local-global per a formes quadràtiques

Per atacar la qüestió sobre l'existència de punts racionals, observem el cas particular de l'equació quadràtica

$$X^2 - aY^2 = 0.$$

Tindrà solució racional si, i només si, a és un quadrat en $\mathbb{Q}$. Per tant, cal determinar quan a és un quadrat o no en $\mathbb{Q}$, i el següent resultat ens caracteritza aquesta condició a través de les completacions de $\mathbb{Q}$.

Proposició 3.1. *Un nombre $a \in \mathbb{Q}$ és quadrat si, i només si, a és un quadrat en $\mathbb{R}$ i en $\mathbb{Q}_p$ per tot primer p.*

Demostració. És immediat que si $a \in \mathbb{Q}$ és un nombre quadrat aleshores, la seva imatge en tots els $\mathbb{Q}_p$ i en $\mathbb{R}$ també ho serà.

Suposem ara que a és un quadrat en $\mathbb{Q}_p$, per tot p, i en $\mathbb{R}$. Vegem que aquesta condició és suficient perquè a sigui un nombre racional quadrat.

Com a és un quadrat en $\mathbb{R}$, necessàriament $a \geqslant 0$. Per altra banda, podem descompondre a com:

$$a = \prod_{p_i} p_i^{ord_{p_i}(a)},$$

on $p_i \neq p_j$ si $i \neq j$ per un cert nombre finit de $p_i's$. Sabem per la caracterització dels quadrats en $\mathbb{Q}_p$ vista en l'anterior capítol que $ord_{p_i}(a)$ és un nombre parell per tot primer p_i. Aleshores, a també és un quadrat en $\mathbb{Q}$. $\square$

Per tant, podem determinar que l'equació $X^2 - aY^2 = 0$ té solució en $\mathbb{Q}$ si, i només si, $X^2 - aY^2 = 0$ té solució en $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p.

Veurem més endavant, en el capítol dedicat a formes quadràtiques, que si l'expressió $X^2 - aY^2$ representa 0 en k, on k fa referència a $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{Q}_p$, per qualsevol nombre primer p, aleshores $X^2 - aY^2$ representa qualsevol element $\alpha \in k$, és a dir, $X^2 - aY^2 = \alpha$ té solució no trivial en k, per qualsevol $\alpha \in k$. Així, l'equació $X^2 - aY^2 = \alpha$, $\alpha \in \mathbb{Q}$, té solució en $\mathbb{Q}$ si, i només si, $X^2 - aY^2 = \alpha$ té solució en $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p.

Aleshores, amb un canvi de variables adequat, $aX^2 + bY^2 + c = 0$, on $a, b, c \in \mathbb{Q}$, $a \neq 0$, es pot expressar com $X^2 - b'Y^2 - c' = 0$ per certs valors $b', c' \in \mathbb{Q}$. I per tant, es dedueix que $aX^2 + bY^2 + c = 0$ té solució no trivial en $\mathbb{Q}$ si, i només si, té solució en $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p. Aquests dos exemples presentats tenen la mateixa estructura d'enunciat:

Existeix solució en $\mathbb{Q} \Leftrightarrow$ existeix solució $\mathbb{R}$ i $\mathbb{Q}_p$, per tot primer p.

Així, amb els exemples anteriors, veiem que en alguns casos, resoldre un problema a $\mathbb{Q}$ pot ser equivalent a la resolució del problema als cossos $\mathbb{R}$ i $\mathbb{Q}_p$, per tot nombre primer p. Aquesta idea la podem interpretar considerant els cossos $\mathbb{Q}_p$ i $\mathbb{R}$ com *espais locals* i $\mathbb{Q}$ com *espai global*. L'existència d'una arrel global implica l'existència d'una arrel local, per la inclusió de $\mathbb{Q}$ en els espais locals. Ara bé, tenir una resposta satisfactòria d'un problema localment no implica automàticament obtenir una resposta satisfactòria global. Aquest *principi local-global* dependrà del problema. Denotem per $V = \{p : p \text{ primer }\} \cup \{\infty\}$ i utilitzem la notació $\mathbb{Q}_v$, $v \in V$, per fer referència a les completacions de $\mathbb{Q}$, entenent $\mathbb{Q}_\infty = \mathbb{R}$. En la resta del treball se seguirà aquesta notació.

Així doncs, les equacions quadràtiques de la forma

$$aX^2 + bY^2 + c = 0,$$

constitueixen una família d'equacions per a les quals es verifica el principi local-global. Més en general, les expressions de la forma

$$f(X) = \sum_{i=1}^{n} a_{ii}X_i^2 + 2 \cdot \sum_{i<j} a_{ij}X_iX_j, \quad \text{on} \quad a_{ij} \in \mathbb{Q},$$

anomenades *formes quadràtiques* (polinomis homogenis de grau 2) verifiquen el princpi local-global amb un nombre arbitrari de variables. Aquest resultat, és el contingut del Teorema de Hasse-Minkowski.

Teorema 3.2. *(Hasse-Minkowski) Sigui $f(X_1, ..., X_n)$ una forma quadràtica amb tots els seus coeficients a $\mathbb{Q}$. Una condició suficient i necessària perquè $f(X_1, ..., X_n) = 0$ tingui solució no trivial en $\mathbb{Q}$ és que $f(X_1, ..., X_n) = 0$ tingui solució en $\mathbb{R}$ i en $\mathbb{Q}_p$, per tot nombre primer p.*

Tanmateix, traslladar la qüestió de $\mathbb{Q}$ a $\mathbb{R}$ i $\mathbb{Q}_p$, per tot valor de p, no sembla una simplificació del problema: hi ha infinits espais $\mathbb{Q}_p$ i comprovar-ne l'existència o no de solucions en tots aquests no es presenta com una eina fàcil.

Ara bé, donada una forma quadràtica racional, només cal comprovar l'existència de solucions per un nombre finit de cossos $\mathbb{Q}_p$. Això és conseqüència del Lema de Hensel, que permet determinar que existeix solució per quasi tots els $\mathbb{Q}_p$, i ens referim a l'expressió "quasi tots"per indicar tots els primers p menys un nombre finit. Així, el problema de treballar en infinits espais $\mathbb{Q}_p$ s'ha reduït a buscar solucions en un nombre finit de cossos. Per il·lustrar aquest fet, vegem l'exemple per a les equacions

$$aX^2 + bY^2 + c = 0,$$

introduïdes en la secció anterior. Podem suposar, multiplicant pels enters adequats, que $a, b, c \in \mathbb{Z}$. Aplicant el Lema de Hensel vegem que

$$f(X, Y) = aX^2 + bY^2 + c = 0$$

té solució en $\mathbb{Q}_p$ per tot p tal que $p \nmid 2abc$ (i de fet, veurem que les solucions són a $\mathbb{Z}_p$).

Així, per veure que $f(X, Y) = aX^2 + bY^2 + c = 0$ té solució en tots els cossos $\mathbb{Q}_p$, només caldrà fer-ho per tots els valors de p tals que $p \mid 2abc$, és a dir, un conjunt finit de valors. A més, veurem en el capítol dedicat a formes quadràtiques, un teorema que determina l'existència de solucions en $\mathbb{Q}_p$ per un p fixat.

Sigui doncs p tal que $p \nmid 2abc$. Notem que sota aquesta hipòtesi, $|a|_p = |b|_p = |c|_p = 1$ i $p > 2$. Considerem la demostració en tres passos: en el primer vegem que en $\mathbb{F}_p$ les formes $bY^2 + c$ poden prendre $\frac{1}{2}(p+1)$ valors diferents. En el segon, que $aX^2 + bY^2 + c \equiv 0 \pmod p$ té solució no trivial en $\mathbb{F}_p^2$. Finalment al tercer pas, i aplicant el Lema de Hensel, veiem que existeix una solució de $aX^2 + bY^2 + c = 0$ en $\mathbb{Z}_p$.

Primer pas. En $\mathbb{F}_p$, la forma $bY^2 + c$ pren exactament $\frac{1}{2}(p+1)$ valors diferents. Notem que bY^2 i $bY^2 + c$ prendran el mateix nombre de valors diferents en $\mathbb{F}_p$. Per tant, és suficient provar-ho per bY^2 i com b és un element invertible, bY^2 i Y^2 també prenen el mateix nombre de valors difernets en $\mathbb{F}_p$. Per tant, només cal veure que Y^2 pren $\frac{1}{2}(p+1)$ valors diferents en $\mathbb{F}_p$. Considerem l'aplicació:

$$\sigma : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$$

$$y \longrightarrow y^2.$$

Tenim $ker(\sigma) = \{y : y^2 = 1\} = \{\pm 1\}$, i en conseqüència $Im(\sigma) \cong \mathbb{F}_p^*/\{\pm 1\}$. Aleshores $\#Im(\sigma) = \frac{1}{2}(p-1)$.

Així doncs, Y^2 pot prendre $\frac{1}{2}(p-1)$ valors diferents més el valor 0, és a dir, $\dfrac{p+1}{2}$, tal com volíem veure.

Segon pas. Vegem que $aX^2 + bY^2 + c \equiv 0$ té solució mòdul p. Si $a \in \mathbb{Z}$ i $p \nmid a$, $bY^2 + c$ i $-aX^2$ prendran $\frac{1}{2}(p+1)$ valors diferents en $\mathbb{F}_p$. Com $\#\mathbb{F}_p = p$, existeix almenys un valor que és representat per $bY^2 + c$ i $-aX^2$. Per tant, existeix $(x_0, y_0) \in (\mathbb{F}_p)^2$ tal que $ax_0^2 + by_0^2 + c \equiv 0 \ \ (mod\ p)$.

Tercer pas. Volem veure que $f(X,Y) = aX^2 + bY^2 + c$ té solució en $\mathbb{Z}_p$. Sabem que existeix $(x_0, y_0) \in (\mathbb{F}_p)^2$ tal que $ax_0^2 + by_0^2 + c \equiv 0$. És a dir, si $f(X,Y) = aX^2 + bY^2 + c$, tenim

$$f(x_0, y_0) \equiv 0 (mod\ p).$$

Aleshores,

$$\frac{\partial f}{\partial x}(x_0, y_0) = 2ax_0 \ \text{ i } \ \frac{\partial f}{\partial x}(x_0, y_0) = 2by_0.$$

Si tinguéssim $p \mid 2ax_0$, $p \mid 2by_0$, com $p > 2$ i $|a|_p = |b|_p = 1$, seria $p \mid x_0$ i $p \mid y_0$, i aleshores, $p \mid c$, en contradicció la hipòtesi $|c|_p = 1$. Per tant, se satisfan les hipòtesis del Lema de Hensel i podem construir una successió de Cauchy $\{(x_0, y_0), (x_1, y_1), ...\}$ formada per solucions de $f(X,Y) \equiv 0 \pmod{p^{i+1}}$ tals que $x_{i+1} \equiv x_i \pmod{p^{i+1}}$ i $y_{i+1} \equiv y_i \pmod{p^{i+1}}$. Aleshores, $(x,y) := \lim_{i\to\infty}\{(x_0, y_0), (x_1, y_1), ...\} \in (\mathbb{Z}_p)^2$ és solució de $f(X,Y) = 0$.

L'objectiu del treball és la demostració del Teorema de Hasse-Minkowski. En els següents dos capítols, es farà una introducció a la teoria dels símbols de Hilbert i a la teoria de formes quadràtiques, ambdues enfocades als resultats més importants per a la demostració. Per tancar el capítol, vegem un apartat sobre el prinicipal contraexemple del Teorema de Hasse-Minkowski en què relaxem la hipòtesi d'estar sobre una forma quadràtica.

3.3 Principi local-global més enllà de les formes quadràtiques

De forma natural, ens podem preguntar si en general, el fet de tenir solucions d'una equació polinòmica racional en $\mathbb{Q}_v$, per tot $v \in V$, és equivalent a tenir solució en $\mathbb{Q}$.

Però en general, no és cert que el principi local-global es verifiqui en qualsevol equació polinòmica. Un exemple són les equacions de grau superior a 2, en les quals no existeix un anàleg al Teorema de Hasse-Minkowski.

Un dels "contraexemples" més coneguts és l'anomenada cúbica de Selmer:

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

Si bé és relativament fàcil comprovar que té solucions no trivials a $\mathbb{R}$ i també en $\mathbb{Q}_p$, per a tot primer p (amb el lema Hensel), es pot demostrar, amb més dificultat, que no admet cap solució no trivial sobre $\mathbb{Q}$. Es pot consultar la demostració a l'article original de Selmer [7] o bé en [1], capítol 18.

Sovint es pot plantejar el principi local-global per a qüestions amb una perspectiva més geomètrica. Per exemple, siguin V, V' dues varietats algebraiques definides sobre $\mathbb{Q}$ i, V_v, V'_v les varietats vistes sobre $\mathbb{Q}_v$. És cert que V, V' són isomorfes sobre $\mathbb{Q}$ si, i només si, V_v, V'_v són isomorfes en $\mathbb{Q}_v$, per tot $v \in V$? En general no. Es pot veure un exemple a l'article [6], el qual utilitza l'equació cúbica de Selmer. Explicat breument, utilitza el terme *companyes* d'una varietat V sobre $\mathbb{Q}$, per anomenar totes les varietats V' sobre $\mathbb{Q}$ tals que totes les varietats locals V'_v són isomorfes a V_v sobre $\mathbb{Q}_v$, per tot $v \in V$. Aleshores, si $V : 3X^3 + 4Y^3 + 5Z^3 = 0$, es pot demostrar que les seves companyes són:

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

$$12X^3 + Y^3 + 5Z^3 = 0,$$

$$15X^3 + 4Y^3 + Z^3 = 0,$$

$$3X^3 + 20Y^3 + Z^3 = 0,$$

$$60X^3 + Y^3 + Z^3 = 0.$$

I aquesta última per exemple, a diferència de la original, té solució no trivial en $\mathbb{Q}$: $(0, 1, -1)$. De fet és la única equació de tot el llistat que admet solució no trivial en $\mathbb{Q}$, i defineix per tant, una corba el·líptica sobre $\mathbb{Q}$.

4 Símbols de Hilbert

Per tractar les formes quadràtiques, i precisament per determinar si tenen o no solucions locals, els símbols de Hilbert són una eina molt important. En aquest capítol donarem la definició i les seves característiques principals, així com el seu algoritme de càlcul.

Recordem que hem definit al capítol anterior el conjunt $V = \{p : \text{ p primer}\} \cup \{\infty\}$. Per fer més lleugera la notació, fixem un valor qualsevol $v \in V$ i escrivim k per referir-nos al cos $\mathbb{Q}_v$.

Definició 4.1. *Siguin $a, b \in k^*$, definim el símbol de Hilbert de a i b en k, i ho anotem $(a, b)_v$, com:*

- $(a, b)_v = 1$ *si* $Z^2 - aX^2 - bY^2 = 0$ *té solució no trivial en* k^3.
- $(a, b)_v = -1$ *en qualsevol altre cas.*

És clar que $(a, b)_v$ no varia si multipliquem a i b per un nombre quadrat. Així, el símbol de Hilbert defineix una aplicació

$$k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}.$$

Proposició 4.2. *Siguin $a, b \in k^*$. Aleshores $(a, b)_v = 1$ si, i només si, $b \in N(k(\sqrt{a})|k)$, on $N(k(\sqrt{a})|k)$ denota la imatge de $k(\sqrt{a})$ en k per l'aplicació norma.*

Demostració. Si suposem $b \in N(k(\sqrt{a})|k)$ existeixen $\alpha, \beta \in k$ tal que $b = \alpha^2 - a\beta^2$. És a dir, b és la norma d'algun element $\alpha + \beta\sqrt{a} \in k(\sqrt{a})$. Aleshores, $Z^2 - aX^2 - bY^2$ representa 0 en $(x, y, z) = (\beta, 1, \alpha)$ i per tant, $(a, b)_v = 1$.

Suposem ara que $(a, b)_v = 1$. Existeix $(x, y, z) \neq (0, 0, 0)$ tal que

$$z^2 - ax^2 - by^2 = 0.$$

Si $y = 0$, $a = \frac{z^2}{x^2}$ és un quadrat i l'extensió $k(\sqrt{a}) = k$. Per tant, $b \in N(k(\sqrt{a})) = N(k)$.

Ara bé, si $y \neq 0$, aleshores b és de la forma $\frac{z^2}{y^2} - \frac{ax^2}{y^2}$, és a dir, és la norma d'un element $\frac{z}{y} + \sqrt{a}\frac{x}{y} \in k(\sqrt{a})$. Per tant, $b \in N(k(\sqrt{a}))$ com volíem veure. □

En conseqüència de la definició i la proposició anterior, es demostra que el símbol de Hilbert verifica les següents propietats, on $a, b, c \in k^*$ són arbitraris i suposem $1 - a \in k^*$ quan sigui necessari.

i) $(a, b)_v = (b, a)_v$ i $(a, c^2)_v = 1$.

ii) $(a, -a)_v = 1$ i $(a, 1 - a)_v = 1$.

iii) $(a, b)_v = 1 \Rightarrow (aa', b)_v = (a', b)_v$.

iv) $(a, b)_v = (a, -ab)_v = (a, (1 - a)b)_v$.

La propietat (iii) és un cas particular de la bilinealitat del símbol de Hilbert:

$$(aa', b)_v = (a, b)_v(a', b)_v.$$

La demostració d'aquesta última propietat té més dificultat que la de les quatre propietats anteriors, que amb la proposició 4.2 és gairebé és suficient. Demostrarem primer un algoritme per calcular el símbol de Hilbert i, es deduirà d'aquest, la propietat de la bilinealitat.

4.1 Algoritme del càlcul de $(a,b)_v$

El càlcul del símbol en $\mathbb{R}$ és immediat. Siguin $a, b \in \mathbb{R}$,

$$(a,b)_\infty = 1 \text{ si } a > 0 \text{ o bé } b > 0,$$

$$(a,b)_\infty = -1 \text{ si } a < 0 \text{ i } b < 0.$$

En efecte, tot nombre real positiu és un nombre quadrat. Així, si a o b són nombres reals positius, per la propietat (i), $(a,b)_\infty = 1$. Si a i b són nombres reals negatius, tenim:

$$(a,b)_\infty = (-1\cdot(-a), -1\cdot(-b))_\infty = (-1,-1)_\infty = -1,$$

ja que, $-X^2 - Y^2 - Z^2 = 0$ només té solució trivial en $\mathbb{R}$ i estem usant que $-a, -b$ són nombres reals positius.

Existeix també un algoritme pel càlcul del símbol de Hilbert en els cossos $\mathbb{Q}_p$. Dediquem la resta de secció a la demostració de l'algoritme de $(a,b)_p$ per qualsevol p primer senar. En el cas $p = 2$, només enunciarem la fórmula de càlcul.

Observació 4.3. *El valor de $(u,v)_p$ per tot primer senar p i $u, v \in \mathbb{Z}_p^*$ és 1.*

Demostració. En l'apartat de *Principi local-global per a formes quadràtiques*, de l'anterior capítol, hem vist que si $u, v \in \mathbb{Z}_p^*$ (i.e. $|u|_p = |v|_p = 1$) aleshores, l'equació $uX^2 + vY^2 - 1 = 0$ té solució en $\mathbb{Z}_p$. □

Notem que en aquesta demostració del capítol 3 també se suposava $p \neq 2$.

Observació 4.4. *Sigui p un nombre primer senar i $v \in \mathbb{Z}_p^*$. Aleshores $(p,v)_p = \left(\frac{v}{p}\right)$, on $\left(\frac{v}{p}\right)$ fa referència al símbol de Legendre amb la reducció de v mòdul p.*

Demostració. Veurem que $(p,v)_p = 1 \Leftrightarrow \left(\frac{v}{p}\right) = 1$. És clar que, com $(p,v)_p$ i $\left(\frac{v}{p}\right)$ només prenen valors en $\{\pm 1\}$, aquesta condició és equivalent a l'enunciat de l'observació.

Suposem $\left(\frac{v}{p}\right) = 1$, és a dir, que v és un quadrat mòdul p. Per la propietat (i) del símbol de Hilbert,

$$(p,v)_p = 1.$$

Si suposem $(p,v)_p = 1$, aleshores l'equació $pX^2 + vY^2 - Z^2 = 0$ té solució (x_0, y_0, z_0) no trivial en $\mathbb{Q}_p$. Sense pèrdua de generalitat podem suposar, multiplicant pels enters p-àdics adequats, que la solució és a $\mathbb{Z}_p$ i que $p \nmid y_0 z_0$. Aleshores l'equació reduïda mòdul p és

$$\overline{v}\ \overline{y_0}^2 - \overline{z_0}^2 = 0,$$

és a dir, $\overline{v} = \left(\frac{\overline{z_0}}{\overline{y_0}}\right)^2$. Per tant, v és un quadrat mòdul p i en conseqüència, $\left(\frac{v}{p}\right) = 1$. □

Proposició 4.5. *Sigui p un nombre primer senar i siguin $a, b \in \mathbb{Q}_p^*$ expressats $a = p^r u$, $b = p^s v$, on $r, s \in \mathbb{Z}$ i $u, v \in \mathbb{Z}_p^*$. Aleshores,*

$$(a,b)_p = (-1)^{rs\varepsilon(p)} \left(\frac{u}{p}\right)^s \left(\frac{v}{p}\right)^r,$$

on $\varepsilon(p) = \dfrac{p-1}{2}$.

Demostració. Notem que tenim $(a,b)_p = (up^r, vp^s)_p$. Per les propietats del símbol de Hilbert només cal considerar els residus mòdul 2 de r i s, ja que el producte de nombres quadrats no altera el valor del símbol de Hilbert. Aleshores, distingim tres casos:

- Suposem $r = s = 0$. Aleshores $(a,b)_p = (u,v)_p = 1$ per l'observació 4.3. I és clar que la fórmula de càlcul en $r = s = 0$ també pren valor 1.
- Suposem $r = 1$ i $s = 0$ (el cas $r = 0$ i $s = 1$ es faria exactament igual). Tenim $(a,b)_p = (up, v)_p$. Aleshores, per la propietat (iii) del símbol de Hilbert, $(up,v)_p = (p,v)_p$ perquè $(u,v)_p = 1$. Aleshores, aplicant l'observació 4.4, tenim:

  $$(a,b)_p = (p,v)_p = \left(\frac{v}{p}\right),$$

  que és exactament el valor de l'algoritme en $r = 1$ i $s = 0$.
- Suposem ara $r = s = 1$. Tenim

  $$(a,b)_p = (up, vp)_p.$$

  Per la quarta propietat del símbol de Hilbert,

  $$(up, pv)_p = (up, -p^2uv)_p = (up, -uv)_p.$$

  Aleshores, aplicant el mateix raonament anterior, donat que $(u, -uv)_p = 1$, tenim $(up, -uv)_p = (p, -uv)_p$. I per l'observació 4.4,

  $$(p, -uv)_p = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) = (-1)^{(p-1)/2}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right),$$

  tal com volíem veure.

□

El cas $p = 2$, només l'enunciarem i es pot consultar una demostració completa en [8], capítol III, theorem 1.

Proposició 4.6. *Sigui $p = 2$ i $a, b \in \mathbb{Q}_p$, aleshores:*

$$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + r\omega(v) + s\omega(u)},$$

on $\varepsilon(x)$ i $\omega(x)$ denoten a la classe mòdul 2 de $\dfrac{x-1}{p}$ i $\dfrac{x^2-1}{p}$, respectivament.

Se segueix d'aquesta demostració que el símbol de Hibert defineix una forma bilineal no degenerada $k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}$. En efecte, és immediat comprovar la propietat de bilinealitat. Per provar la no-degeneració és suficient veure que per tot $a \in k^*/k^{*2}$, diferent de l'element neutre, podem trobar $b \in k^*/k^{*2}$, tal que $(a,b)_v = -1$.

4.2 Propietats del símbol de Hilbert sobre nombres racionals

Observem que donats dos elements $a, b \in \mathbb{Q}^*$, podem considerar $(a,b)_v$, per tot $v \in V$, per la inclusió de $\mathbb{Q}$ en $\mathbb{Q}_v$. Aleshores ens podem preguntar si donat un nombre racional a i una família de símbols $\varepsilon_v \in \{\pm 1\}$, per tot $v \in V$, podem trobar un nombre racional b tal

que $(a,b)_v = \varepsilon_v$. Demostrarem que sota certes hipòtesis naturals, la resposta a aquesta pregunta és afirmativa. Per fer-ho, demostrarem primer el Teorema de Hilbert, també conegut com "'fórmula del producte".

Amb la demostració d'aquests dos resultats, finalitzarem aquest capítol.

Teorema 4.7. *(de Hilbert) Si $a, b \in \mathbb{Q}^*$, tenim $(a,b)_v = 1$ per quasi tots els $v \in V$ i*

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

Utilitzem el terme "quasi tots" per referir-nos a tots els valors de V menys un nombre finit. En particular, se segueix del teorema que $(a,b)_v = -1$ per un nombre finit parell de valors $v \in V$.

Demostració. Per la bilinealitat del símbol de Hilbert, només fa falta comprovar el teorema pels casos $a = -1$ i $b = -1$, $a = -1$ i $b = \ell$, per algun primer ℓ, i $a = \ell'$ i $b = \ell$ per a dos primers diferents ℓ, ℓ'. Cada cas es demostra aplicant l'algoritme de la Proposició 4.5 i la Proposició 4.6. □

Observació 4.8. *En conseqüència del Teorema de Hilbert, si demostrem que la forma quadràtica $f(X,Y,Z) = aX^2 + bY^2 - Z^2$ representa 0 en $\mathbb{Q}_v$ per tots els valors de v menys un, aleshores, $f(X,Y,Z) = aX^2 + bY^2 - Z^2$ representa 0 en $\mathbb{Q}_v$ per tots els valors de v.*

Teorema 4.9. *Sigui $(a_i)_{i \in I}$ una família finita d'elements de $\mathbb{Q}^*$ i sigui $(\varepsilon_{i,v})_{i \in I, v \in V}$ una família de valors iguals a ± 1. Perquè existeixi $x \in \mathbb{Q}^*$ tal que $(a_i, x)_v = \varepsilon_{i,v}$ per tot $i \in I$ i tot $v \in V$, és suficient i necessari que es compleixi:*

1. *Quasi totes les $\varepsilon_{i,v}$ són iguals a 1.*
2. *Per tots els índex $i \in I$, $\prod_{v \in V} \varepsilon_{i,v} = 1$.*
3. *Per qualsevol $v \in V$, existeix $x_v \in \mathbb{Q}_v^*$ tal que $(a_i, x_v)_v = \varepsilon_{i,v}$ per tot $i \in I$.*

Demostració. Demostrem la necessitat de les condicions. Vegem-ho primer pel cas $(a_i) = a \in \mathbb{Q}^*$. Suposem que tenim una família de símbols $(\varepsilon_v) \in \{\pm 1\}$ i un valor $x \in \mathbb{Q}^*$ tal que $(a,x)_v = \varepsilon_v$. Pel Teorema de Hilbert, $(a,x)_v = 1$ per quasi tots els valors de $v \in V$ i $\prod_{v \in V} (a,x)_v = 1$. Per tant, les condicions (1) i (2) són necessàries. Pel que fa la condició (3), és suficient pendre x_v com la imatge de l'element x en els espais $\mathbb{Q}_v$, per tot $v \in V$.

En el cas general d'una família finita d'elements racionals, $(a_i)_{i \in I} \in \mathbb{Q}$, les tres condicions també seran necessàries, ja que s'han de complir els mateixos arguments per cada $i \in I$.

Suposem ara que se satisfan les tres condicions. Volem veure que existeix un nombre racional x tal que $(a_i, x)_v = \varepsilon_{i,v}$ per tot $i \in I$ i tot $v \in V$. Per fer-ho, vegem dos resultats previs:

Lema 4.10. *(Teorema d'aproximació) Sigui S un subconjunt finit de V i considerem l'aplicació d'inclusió*

$$\mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v.$$

Aleshores $Im(\mathbb{Q}) \subset \prod_{v \in S} \mathbb{Q}_v$ és densa.

Demostració. Observem que si la imatge de $\mathbb{Q}$ en la inclusió $\mathbb{Q} \hookrightarrow \prod_{S\cup\infty} \mathbb{Q}_v$ és densa, aleshores la imatge de $\mathbb{Q}$ en la inclusió $\mathbb{Q} \hookrightarrow \prod_S \mathbb{Q}_v$ és també densa. Per tant, podem suposar

$$S = \{\infty, p_1, ..., p_n\}.$$

Sigui $(x_\infty, x_1, ..., x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times ... \times \mathbb{Q}_{p_n}$. Volem veure que per qualsevol $\varepsilon > 0$ i qualsevol enter $N > 0$, existeix $x \in \mathbb{Q}$ tal que:

$$|x - x_\infty| \leqslant \varepsilon,$$

$$ord_{p_i}(x - x_i) \geqslant N.$$

Multiplicant cada x_i per l'enter p-àdic adequat, podem suposar sense pèrdua de generalitat que $x_i \in \mathbb{Z}_{p_i}$.

Recordatori. *(Teorema xinès del residu.) Siguin $a_1, ..., a_n, m_1, ..., m_n$ nombres enters tals que els m_i's són coprimers dos a dos. Aleshores existeix un enter a tal que $a \equiv a_i (mod\, m_i)$ per qualsevol i.*

Si apliquem el Teorema xinès del residu per $m_i = p_i^N$, aleshores existeix $x_0 \in \mathbb{Z}$ tal que $v_{p_i}(x_0 - x_i) \geqslant N$ per qualsevol i. Aleshores, observem que donat un nombre enter q, el conjunt

$$\{a/q^m \quad : \quad a \in \mathbb{Z} \ \text{ i } \ m > 0\},$$

és dens en $\mathbb{R}$. Aleshores suposem q primer tal que $mcd(q, p_1 \cdots p_n) = 1$. Podem escollir $a \in \mathbb{Z}$ i $m \in \mathbb{N}$ tal que

$$|x_0 - x_\infty + \frac{a}{q^m} \cdot (p_1 \cdots p_n)^N| \leqslant \varepsilon.$$

Així, $x = x_0 + up_1^N \cdots p_n^N \in \mathbb{Q}$ verifica l'enunciat. □

El segon resultat determina que en una progressió aritmètica de raó i terme inicial coprimers, hi ha infinits nombres primers. És un resultat molt important i la seva demostració requereix tècniques analítiques que s'escapen de l'objectiu d'aquest treball. Es pot consultar la demostració en [8], capítol VI, o bé [3], capítol 16.

Lema 4.11. *(Teorema de Dirichlet). Si a i m són enters coprimers $\geqslant 1$, aleshores el conjunt $\{a + \lambda m : \lambda \in \mathbb{N}\}$ conté infinits nombres primers.*

Així, tornant a la demostració del teorema, sigui $(\varepsilon_{i,v})$ una família de valors de $\{\pm 1\}$ que satisfà les condicions (1), (2) i (3) del teorema. Podem suposar multiplicant per enters quadrats adequats, que la família de nombres racionals (a_i) són enters sense pèrdua de generalitat, i aquesta transformació no modifica el valor del símbol de Hilbert.

Sigui S un subconjunt de V contenint $\{\infty, 2\}$ i tots els nombres primers que factoritzen a_i, per tot $i \in I$, i sigui T el conjunt de $v \in V$ tals que existeix algun $i \in I$ que $\varepsilon_{i,v} = -1$. És clar per les hipòtesis que tant S com T són finits. Distingim dos casos: $S \cap T = \emptyset$ i $S \cap T \neq \emptyset$.

Primer cas. $S \cap T = \emptyset$. Definim:

$$a = \prod_{\ell \in T,\, \ell \neq \infty} \ell \quad \text{ i } \quad m = 8 \prod_{\ell \in S,\, \ell \neq 2, \infty} \ell$$

Si $S \cap T = \emptyset$ aleshores a i m són coprimers i, pel Teorema de Dirichlet, existeix un nombre primer p tal que $p \equiv a \ \ (mod\ m)$ que a més, podem suposar $p \notin S \cup T$ (ja que el Teorema de Dirichlet ens assegura l'existència d'infinits primers amb la condició descrita).

Prenem $x = ap$ i vegem que x satisfà $(a_i, x)_v = \varepsilon_{i,v}$ per tot $i \in I$ i $v \in V$. Considerem primer el cas $v \in S$ i després, el cas $v \notin S$.

Si $v \in S$, aleshores $\varepsilon_{i,v} = 1$, $\forall i \in I$. Així, només hem de comprovar que $(a_i, x)_v = 1$. El cas $v = \infty$ és immediat: $(a_i, x)_v = 1$ perquè $x > 0$. Si $v = \ell$ per algun nombre primer $\ell \in S$, tenim $x \equiv a^2 (mod\, m)$ perquè $p \equiv a \ \ (mod\ m)$ i $x = ap$.

En particular, $x \equiv a^2 \ \ (mod\ 8)$ i $x \equiv a^2 \ \ (mod\ \ell)$, per tant, x és un quadrat a $\mathbb{Q}_2^*$ i també és un quadrat a $\mathbb{Q}_\ell^*$ per la caracterització dels quadrats en $\mathbb{Q}_p^*$ vista en el capítol de nombres p-àdics. Aleshores, $(a_i, x)_v = 1$ per tot $v \in S$ tal com volíem veure.

Si $v \notin S$, i $v = \ell$, aleshores sabem que $\ell \neq 2$ i $\ell \nmid a_i$ per cap i. Per tant, a_i és una unitat ℓ-àdica per tot índex $i \in I$. Per l'algoritme de càlcul del símbol de Hilbert vist anteriorment:

$$(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{ord_\ell(b)} \tag{2}$$

ja que, seguint la notació de la proposició 4.5, $r = 0$ i $s = ord_\ell(b)$. Recordem que $\ell \notin S$ i seguim la demostració distingint tres opcions: si $\ell \notin T \cup \{p\}$, si $\ell \in T$ i finalment, si $\ell = p$.

- Suposem $\ell \notin T \cup \{p\}$. Tenim $\varepsilon_{i,\ell} = 1, \forall i \in I$. Per altra banda, per la construcció de a, $x = ap$ és una unitat ℓ-àdica i, per tant, $ord_\ell(x) = 0$. Aleshores per l'equació (2) tenim $(a_i, x)_\ell = 1$. Així, clarament se satisfà $(a_i, x)_\ell = \varepsilon_{i,\ell}$.

- Si $\ell \in T$, aleshores $v_\ell(x) = 1$. Per l'equació (2), tenim: $(a_i, x)_\ell = \left(\frac{a_i}{\ell}\right)^{ord_\ell(x)} = \left(\frac{a_i}{\ell}\right)$. Per la condició (3) del teorema, sabem que existeix $x_\ell \in \mathbb{Q}_\ell^*$ per tot $\ell \in T$ tal que

  $$(a_i, x_\ell)_\ell = \left(\frac{a_i}{\ell}\right)^{ord_\ell(x_\ell)} = \varepsilon_{i,\ell}, \quad \forall i \in I.$$

  Com que almenys un $\varepsilon_{i,\ell}$ val -1 perquè $\ell \in T$, tenim que $ord_\ell(x_\ell) \equiv 1 (mod\, 2)$. Si no fos així, és a dir, si $ord_\ell(x_\ell)$ fos un nombre parell, per l'equació (2) tots els símbols $\varepsilon_{i,\ell}$ valdrien $+1$, en contradicció amb el fet que $\ell \in T$. Per tant $ord_\ell(x_\ell)$ és senar, és a dir, $ord_\ell(x_\ell) \equiv 1 (mod\, 2)$. Per tant, $(a_i, x_\ell)_\ell = \left(\frac{a_i}{\ell}\right)^{ord_\ell(x_\ell)} = \left(\frac{a_i}{\ell}\right)$, i s'obté

  $$(a, x)_\ell = \left(\frac{a_i}{\ell}\right) = \varepsilon_{i,\ell},$$

  com volíem veure.

- Finalment, el cas $\ell = p$ es dedueix del Teorema de Hilbert. Com que $\prod_{v \in V} (a_i, x)_v = 1$, tenim que

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

  on, en l'última igualtat, hem utilitzat la condició (2) del teorema.

Segon cas. $S \cap T \neq \emptyset$. Per resoldre aquest cas, reduïm la situació al cas anterior, ja demostrat. Recordem que en la caracterització dels quadrats en $\mathbb{Q}_p^*$ hem vist que el subgrup $\mathbb{Q}_p^{*2} \subset \mathbb{Q}_p^*$ és un conjunt obert. Aleshores, observem:

(i) $\prod_{v \in S} \mathbb{Q}_v^{*2} \subset \prod_{v \in S} \mathbb{Q}_v^*$ és obert per la topologia producte.

(ii) Per a cada $v \in S$, $x_v \cdot (\mathbb{Q}_v^*)^2 \subset \mathbb{Q}_v^*$ és obert.

(iii) Per (i) i (ii) tenim $\prod_{v\in S} x_v \cdot (\mathbb{Q}_v^*)^2 \subset \prod_{v\in S} \mathbb{Q}_v^*$ és obert.

Aleshores, per densitat (Lema 4.10) l'obert $\prod_{v\in S} x_v \cdot (\mathbb{Q}_v^*)^2$ conté la imatge d'algun element $x' \in \mathbb{Q}^*$. Així, per cada $v \in S$ tenim $x' = x_v c_v^2$, on $c_v \in \mathbb{Q}_v^*$, i per tant, x'/x_v és un quadrat a $\mathbb{Q}_v^*, \forall v \in S$.

Per les propietats del símbol de Hilbert, tenim que $(a_i, \frac{x'}{x_v})_v = 1$ i per tant, $(a_i, x'x_v)_v = 1$. Aplicant la bilinealitat del símbol:

$$(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v},$$

on l'última igualtat és per les hipòtesis de la demostració.

Considerem la família $\eta_{i,v} = \varepsilon_{i,v} \cdot (a_i, x')_v$. És clar que $(\eta_{i,v})$ verifica les condicions (1), (2) i (3) del teorema. En particular, $\eta_{v,i} = 1$ si $v \in S$, ja que en aquest cas $\eta_{v,i} = \varepsilon_{i,v} \cdot (a_i, x')_v = \varepsilon_{i,v}^2 = 1$. Aleshores, respecte de la família de valors $(\eta_{i,v})$ es compleix $T \cap S = \emptyset$ i podem aplicar el cas anterior demostrat: existeix $y \in \mathbb{Q}^*$ tal que

$$(a_i, y)_v = \eta_{i,v}, \quad \text{per tot} \quad i \in I \quad \text{i} \quad v \in V.$$

Si $x = x'y$, tenim:

$$(a_i, x)_v = (a_i, x')_v (a_i, y)_v = (a_i, x')_v \eta_{i,v} = (a_i, x')_v (a_i, x')_v \varepsilon_{i,v} = \varepsilon_{i,v}.$$

De manera que queda demostrat el teorema.

$\square$

5 Formes quadràtiques

Tot i la introducció que s'ha fet al concepte de *forma quadràtica* al llarg del treball, en aquest capítol es vol recordar formalment la definició i demostrar alguns dels resultats que faciliten la demostració del Teorema de Hasse-Minkowski. Ja que volem traslladar la qüestió de les formes sobre $\mathbb{Q}$ als cossos locals $\mathbb{Q}_p$ i $\mathbb{R}$, veurem el concepte de formes quadràtiques sobre un cos k qualsevol de característica diferent de 2 (que inclou $\mathbb{Q}, \mathbb{R}$ i $\mathbb{Q}_p$ per tot primer p).

5.1 Definició i primers resultats

Definició 5.1. *Anomenem forma quadràtica de n variables sobre k a tota aplicació $f : E \to k$, on E és un k-espai vectorial de dimensió finita n, tal que:*

- $f(ax) = a^2 f(x)$ *per tot* $a \in k$ *i* $x \in E$,
- *la funció* $(x, y) \mapsto f(x + y) - f(x) - f(y)$ *és una forma bilineal.*

Anomenem mòdul quadràtic a la parella (E, f).

Pel fet que $car(k) \neq 2$, podem considerar:

$$x \cdot y = \frac{1}{2}(f(x + y) - f(x) - f(y)),$$

per tot $x, y \in E$. És immediat veure que $\beta(x, y) := x \cdot y$ és una forma bilineal simètrica sobre E que verifica $\beta(x, x) = f(x)$. Per tant, hi ha una relació bijectiva entre les formes quadràtiques i les formes bilineals simètriques en E.

Definició 5.2. *Siguin f, f' dues formes quadràtiques amb mòduls quadràtics (E, f) i (E', f'). Diem que f, f' són equivalents, i ho anotem $f \sim f'$, si els seus mòduls quadràtics són isomorfs, és a dir, si existeix una aplicació lineal $\varphi : E \to E'$ tal que $f(x) = f'(\varphi(x))$ per tot $x \in E$.*

Notem que és necessari que les dimensions dels espais E i E' coincideixin.

Donada una base (e_i) de l'espai E, podem expressar la forma quadràtica f en forma matricial. Sigui β la forma bilineal associada a f en aquesta base, i A la matriu amb coeficients $a_{ij} = (e_i \cdot e_j)$. Aleshores

$$f(X) = X^T A X,$$

on notem que A és una matriu de dimensió $n \times n$ i simètrica.

Si (e'_i) és una altra base de l'espai E i P és la matriu canvi de base entre (e_i) i (e'_i), la matriu A' de la forma quadràtica f en aquesta nova base és PAP^T.

Aleshores, si dues formes quadràtiques f i f' definides per les matrius A i A', són equivalents, existeix una matriu B invertible tal que $A' = BAB^T$. Notem que un canvi de base de l'espai E genera una forma quadràtica equivalent a l'original.

Obsevem que se satisfà $det(A') = det(A) \cdot det(B)^2$. Per tant, si el determinant és no nul, és un invariant en k^*/k^{*2} de la classe d'equivalència d'una forma quadràtica. L'anomenem *discriminant de la forma quadràtica* i l'anotem $disc(f)$.

5.1.1 Ortogonalitat

Definició 5.3. *Diem que els elements $x, y \in E$ són ortogonals si $x \cdot y = 0$. Diem que H^0 és el conjunt ortogonal a $H \subset E$ si per qualsevol $x \in H^0$, $x \cdot y = 0$ per tot $y \in H$.*

Notem que E_1, E_2 són conjunts ortogonals si $E_1 \subset E_2^0$ i $E_2 \subset E_1^0$.

Anotem per E^0 l'espai ortogonal E. El *rang* d'una forma quadràtica f sobre un espai E és la codimensió de l'espai E^0. Aleshores si $E^0 = 0$ diem que f és *no degenerada*.

En termes matricials, el rang d'una forma quadràtica coincideix amb el rang de la matriu que la defineix. Per tant, hi ha una relació directa entre el discriminant d'una forma quadràtica i el rang: el rang serà màxim si, i només si, el discriminant és no nul, i en aquest cas la matriu és no degenerada.

Així doncs, el rang és un invariant de les classes d'equivalència de les formes quadràtiques.

Suposarem per la resta de capítol que treballem amb formes quadràtiques no degenerades.

5.1.2 Representació de nombres per formes quadràtiques

Definició 5.4. *Diem que una forma quadràtica $f(X)$ representa $a \in k$ si existeix $x \in k^n$, $x \neq 0$, tal que $f(x) = a$. En particular, f representarà 0 si, i només si, existeix un element $x \in k^n$ no nul tal que $f(x) = 0$.*

Proposició 5.5. *Si dues formes quadràtiques f, f' són equivalents, aleshores f representa 0 si, i només si, f' representa 0.*

Demostració. Suposem que f i f', definides per les matrius A i A', són equivalents. Aleshores existeix una matriu B tal que $A = B^T A' B$. Si $f(x) = 0$, $x \neq 0$, aleshores $x^T A x = x^T B^T A' B = y^T A' y = 0$, on $y = Bx$ i és un element no nul. Per tant, $f'(y) = 0$. Anàlogament veiem que si $f'(y) = 0$ per algun element y no nul, aleshores existeix $x \neq 0$ tal que $f(x) = 0$. □

Anomenem *isòtrop* a tot $x \in E$ tal que $f(x) = 0$. Diem que el subconjunt U de k^n és isòtrop si tots els seus elements ho són, és a dir, si $f(x) = 0$ per tot $x \in U$.

Un resultat important de tota aquesta teoria és el fet que si una forma quadràtica representa 0 en k aleshores, representa qualsevol element de k. El que queda de secció està dedicada a la demostració d'aquest fet i les seves conseqüències.

Definició 5.6. *Anomenem pla hiperbòlic a tot mòdul quadràtic isomorf a (k^2, f) que tingui una base formada per dos elements x, y isòtrops tals que $x \cdot y \neq 0$.*

De fet, multiplicant y per $\frac{1}{x \cdot y}$, podem suposar $x \cdot y = 1$ i, en aquest cas, la matriu respecte x, y serà:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Observem que si un mòdul quadràtic (k^n, f) conté un element isòtrop, aleshores existeix un subconjunt U de k^n tal que conté x i és un pla hiperbòlic. En efecte, sota la hipòtesi que $n \geqslant 2$ i f no degenerada, existirà $z \in k^n$ tal que $x \cdot z = 1$. Aleshores, l'element

$$y = 2z - (z \cdot z)x$$

és isòtrop i $x \cdot y = 2$. Per tant, $U = \langle x, y \rangle \subseteq k^n$ és un pla hiperbòlic.

Proposició 5.7. *Sigui f una forma quadràtica no degenerada tal que $f(x) = 0$ per algun element $x \in k^n$ no nul. Aleshores, f representa qualsevol nombre racional.*

Demostració. Per les hipòtesis, existeix $U \subset k^n$ tal que és un pla hiperbòlic. Veurem que $f|_U$ pot representar qualsevol element. Podem suposar que U està generat per dos elements isòtrops x, y tals que $x \cdot y = 1$. Aleshores, per qualsevol $a \in k^*$,

$$f(x + \frac{a}{2}y) = (x + \frac{a}{2}y)^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (x + \frac{a}{2}y) = a$$

□

Siguin $g(X_1, ..., X_n), h(X_1, ..., X_m)$ dues formes quadràtiques. Anotem per $g \pm h$ a la forma quadràtica $g(X_1, ..., X_n) \pm h(X_{n+1}, ..., X_{n+m})$. Se seguirà aquesta notació la resta del treball.

Corol·lari 5.8. *Siguin g i h dues formes quadràtiques no degenerades i $f = g - h$. Aleshores, les següents propietats són equivalents:*

1. *f representa 0.*
2. *Existeix un element $a \in k^*$ tal que és representat per g i per h.*
3. *Existeix un element $a \in k^*$ tal que les formes quadràtiques $g - aZ^2$ i $h - aZ^2$ representen 0.*

Demostració.

1) $\Leftrightarrow$ 2) :

Si $f(x_1, ..., x_n) = 0$, aleshores $g(x_1, ..., x_i) = h(x_{i+1}, ..., x_n)$. Si l'element $a = g(x_1, ..., x_i) = h(x_{i+1}, ..., x_n)$ és diferent de 0, és clar que existeix a representat per g i h. Ara bé, si $a = 0$, en particular tenim que g representa 0 i, en conseqüència de la Proposició 5.7, pot representar qualsevol element no nul de k. Així g representa els elements no nuls que també representa h.

L'altra implicació és evident: si existeix un element $a \in k^*$ tal que $g(x_1, .., x_i) = a$ i $h(x_{i+1}, ..., x_n) = a$, aleshores $f(x_1, ..., x_n) = g(x_1, ..., x_i) - h(x_{i+1}, ..., x_n) = 0$.

2) $\Leftrightarrow$ 3) :

Suposem que $a \in k^*$ és representat per g i per h, és a dir, existeix $(x_1, ..., x_i) \in k^i$, $(x_{i+1}, ..., x_n) \in k^{n-i}$ tal que $g(x_1, ..., x_i) = a = h(x_{i+1}, ..., x_n)$. Aleshores, és immediat veure que

$$g'(X_1, ..., X_{i+1}) = g(X_1, ..., X_i) - aX_{i+1}^2$$
$$h'(X_{i+1}, ..., X_{n+1}) = h(X_{i+1}, ..., X_n) - aX_{n+1}^2$$

representen 0. En efecte, $g'(x_1, ..., x_i, 1) = g(x_1, ..., x_i) - a = 0$ i anàlogament amb h'.

Ara suposem que $g(X_1, ..., X_i) - aZ^2$ representa 0 en $(x_1, ..., x_i, z)$ i $h(X_{i+1}, ..., X_n) - aZ^2$ en $(x_{i+1}, ..., x_n, z')$. Si $z = 0$, és clar que $g(x_1, ..., x_i)$ representa 0 i en particular, també representarà a. Si $z \neq 0$, és fàcil veure que $g(\frac{x_1}{z}, ..., \frac{x_i}{z})$ representa a. Anàlogament es veu per la forma quadràtica h. □

5.1.3 Diagonalització de formes quadràtiques

Tota matriu simètrica diagonalitza a través d'una matriu ortogonal: si A és simètrica, existeix una matriu invertible B tal que $BAB^T = A'$ és una matriu diagonal. En termes d'espais vectorials, aquesta matriu B és una matriu canvi de base de A a una base d'elements ortogonals A'. Per tant, es dedueix el següent resultat.

Teorema 5.9. *Sigui f una forma quadràtica de rang n. Aleshores existeixen a_i, per $i = 1, ..., n$, tals que $f \sim a_{11}X_1^2 + ... + a_{nn}X_n^2$.*

En conseqüència, podem definir el rang d'una forma quadràtica f com el nombre de coeficients a_{ii} no nuls, on $f \sim a_{11}X_1^2 + ... + a_{nn}X_n^2$, i el discriminant és $disc(f) = a_{11} \cdots a_{nn}$

5.2 Formes quadràtiques en $\mathbb{Q}_p$ i $\mathbb{R}$

Fixem un valor qualsevol $v \in V$ i escrivim k per referir-nos al cos $\mathbb{Q}_v$.

Sigui (k^n, f) un mòdul quadràtic de rang n i $f \sim a_{11}X_1^2 + ... + a_{nn}X_n^2$, on $a_{ii} = e_i \cdot e_i$ per alguna base ortogonal (e) de k^n. Definim

$$\varepsilon_v(e) = \prod_{i<j} (a_{ii}, a_{jj})_v \in \{\pm 1\}.$$

Teorema 5.10. *El valor $\varepsilon(e)$ no depèn de la base ortogonal (e_i) escollida.*

Demostració. Vegem-ho per inducció en el nombre de variables n.

Suposem $n = 2$. El valor $\varepsilon(e) = 1$ si, i només si, $Z^2 - a_1X^2 - a_2Y^2 = 0$ té solució. I aquesta última condició és equivalent al fet que la forma $a_1X^2 + a_2Y^2$ representi 1, pel corol·lari 5.8. És a dir, que existeixi $(x, y) \in k^2$ tal que $f(x, y) = 1$, i això no depèn de la base escollida.

Suposem $n \geqslant 3$. Veurem la demostració en dos passos. Primer, veurem que si dues bases ortogonals (e_i) i (e'_i) tenen un element en comú, es verifica $\varepsilon(e) = \varepsilon(e')$. Demostrarem en segon lloc que donades dues bases qualssevol, (e_i) i (e'_i), podem construir una successió de bases ortogonals que comença amb (e_i) i acaba amb (e'_i) tal que tots els termes tenen un element en comú amb el següent.

Suposem dues bases ortogonals (e_i) i (e'_i) que tenen un element en comú. Permutar l'ordre dels elements de la base no altera el valor de $\varepsilon(e)$ ni $\varepsilon(e')$, per tant, podem suposar sense pèrdua de generalitat que $e_1 = e'_1$.

Aplicant la propietat de bilinealitat del símbol de Hilbert, tenim que:

$$\prod_{i<j} (a_i, a_j)_v = (a_1, a_2)_v (a_1, a_3)_v \cdots (a_1, a_n)_v \prod_{2 \leqslant i<j} (a_i, a_j)_v = (a_1, a_2a_3 \cdots a_n)_v \prod_{2 \leqslant i<j} (a_i, a_j)_v.$$

Anàlogament,

$$\prod_{i<j} (a'_i, a'_j)_v = (a'_1, a'_2a'_3 \cdots a'_n)_v \prod_{2 \leqslant i<j} (a'_i, a'_j)_v.$$

Pel fet que $e_1 = e'_1$ i que el discriminant és un invariant en les classes d'equivalència en k^*/k^*, només ens cal veure que

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

que es verifica per hipòtesi d'inducció.

Vegem ara que, donades dues bases ortogonals $(e_i), (e'_i)$ podem construir una successió de bases ortogonals $e^{(0)}, e^{(1)}, ..., e^{(m)}$, tal que $e^{(0)} = (e_i), e^{(m)} = (e'_i)$ i cada terme amb el següent tenen un element en comú. És dir, per qualsevol $i \in \{1, ..., m\}$ existeix j, j' tal que

$$e_j^{(i)} = e_{j'}^{(i+1)}.$$

Ho demostrarem per casos:

- Suposem $(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2 \neq 0$, és a dir que, e_1 i e'_1 no són proporcionals, i el pla que generen, $P = \langle e_1, e'_1 \rangle = \lambda e_1 + \lambda e'_1$ és no degenerat. Podem expressar P com una suma de components ortogonals: existeixen $\varepsilon_2, \varepsilon'_2$ tals que:

  $$P = \lambda e_1 \oplus \lambda \varepsilon_2 \quad i \quad P = \lambda e'_1 \oplus \lambda \varepsilon'_2.$$

  Sigui H el complement ortogonal de P, de manera que $E = H \oplus P$. Aleshores H té rang $n-2$ i podem suposar que $(e''_3, ..., e''_n)$ és una base de H. D'aquesta manera, podem considerar la successió:

  $$(e_i) \to (e_1, \varepsilon_2, e''_3, ..., e''_n) \to (e'_1, \varepsilon'_2, e''_3, ..., e''_n) \to (e'_i).$$

- Si $(e_1 \cdot e_1)(e'_2 \cdot e'_2) - (e_1 \cdot e'_2)^2 \neq 0$, aleshores fem el mateix raonament canviant e'_1 per e'_2.

- Suposem $(e_1 \cdot e_1)(e'_i \cdot e'_i) - (e_1 \cdot e'_i)^2 = 0$, per $i = 1, 2$. Aleshores, o bé e_1 i e'_1 són proporcionals, o bé el pla $P = \langle e_1, e'_1 \rangle = \lambda e_1 + \lambda e'_1$ és degenerat, i anàlogament si $i = 2$. Observem que, com $(e'_i)_{1 \leqslant i \leqslant n}$ és una base, no és possible que a la vegada e_1 sigui proporcional a e'_1 i e'_2.

  Vegem que existeix un element $a \in k$, tal que $e_a = e'_1 + a e'_2$ no és isòtrop i genera amb l'element e_1 un pla no degenerat. Tenim $e_a \cdot e_a = (e'_1 + a e'_2)^2 = (e'_1 \cdot e'_1) + a^2 (e'_2 \cdot e'_2)$, ja que e'_1, e'_2 són ortogonals per hipòtesi. Aleshores, per tal que e_a sigui un element no isòtrop, cal que

  $$a^2 \neq \frac{-(e'_1 \cdot e'_1)}{(e'_2 \cdot e'_2)}.$$

  Una condició necessària i suficient perquè e_1, e_a generin un pla no degenerat, és

  $$(e_1 \cdot e_1)(e_a \cdot e_a) - (e_1 \cdot e_a)^2 \neq 0.$$

  Si desenvolupem, tenint en compte que els elements e'_1 i e'_2 són ortgonals, tenim:

  $$(e_1 \cdot e_1) \left((e'_1 \cdot e'_1) + a^2 (e'_2 \cdot e'_2) \right) - (e_1 (e'_1 + a e'_2))^2 =$$

  $$= (e_1 \cdot e_1) \left((e'_1 \cdot e'_1) + a^2 (e'_2 \cdot e'_2) \right) - ((e_1 \cdot e'_1)^2 + a^2 (e_1 \cdot e'_2)^2 + 2a (e_1 \cdot e'_1)(e_1 \cdot e'_2) =$$

  $$= -2a (e_1 \cdot e'_1)(e_1 \cdot e'_2)$$

  Ja que, $(e_1 \cdot e_1)(e'_i \cdot e'_i) - (e_1 \cdot e'_i)^2 = 0$, per $i = 1, 2$.

  Notem que $(e_1 \cdot e'_1)(e_1 \cdot e'_2) \neq 0$. En efecte, si $(e_1 \cdot e'_1) = 0$, aleshores per la hipòtesi del tercer cas, o bé $(e_1 \cdot e_1) = 0$ o bé $(e'_1 \cdot e'_1) = 0$ i ambdues igualtats són contradiccions pel fet que e_1 i e'_1 no son elements isòtrops. Anàlogament fem per $i = 2$.

Per tant, per qualsevol $a \in k$ tal que

$$a^2 \neq \frac{-(e_1' \cdot e_1')}{(e_2' \cdot e_2')} \quad \text{i} \quad a \neq 0$$

l'element $e_a = e_1' + ae_2' \in E$ és no isòtrop i genera un pla no degenerat amb l'element e_1. En conseqüència, podem aplicar el raonament fet al primer cas.

□

En definitiva tenim que donada una forma quadràtica f tal que $f \sim a_1X_1^2 + ... + a_nX_n^2$,

$$rang(f) = n$$

$$d(f) = a_1 \cdot ... \cdot a_n \quad \text{en} \quad k^*/k^{*2}$$

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

són invariants de la seva classe d'equivalència en k^*.

5.2.1 Representació de nombres p-àdics i nombres reals

Aquesta última secció veurem la demostració d'un teorema que enuncia quines condicions són necessàries i suficients perquè una forma quadràtica representi qualsevol nombre p-àdic o real. Així doncs, aquest teorema ens proporciona una caracterització d'existència solucions en $\mathbb{Q}_v$, per un valor v fixat.

Teorema 5.11. *Sigui f una forma quadràtica, de rang $n \leqslant 4$, $d = d(f)$ i $\varepsilon = \varepsilon_v(f)$. Perquè f representi 0 en k és suficient i necessari que:*

- *si $n = 2$, $d = -1$ a k^*/k^{*2};*
- *si $n = 3$, $(-1, -d)_v = \varepsilon_v$;*
- *si $n = 4$, o bé $d \neq 1$ o bé $d = 1$ i $\varepsilon_v = (-1, -1)_v$.*

Les condicions per a rang n de representació de 0 en el teorema indueixen a la representació d'un nombre en les rang $n - 1$. En efecte, si $a \in k^*/k^{*2}$, la forma quadràtica $f_a = f - aZ^2$ representarà 0 si, i només si, f representa a. Aleshores, fent servir que

$$rang(f_a) = rang(f) + 1, \quad d(f_a) = -ad(f) \quad \text{i} \quad \varepsilon_v(f_a) = (-a, d)_v \cdot \varepsilon_v(f),$$

es dedueix el següent corol·lari.

Corol·lari 5.12. *La forma f de rang $n \leqslant 4$ representa $a \in k^*/k^{*2}$ si, i només si,*

- *Si $n = 1$ i $a = d$;*
- *Si $n = 2$ i $(a, -d)_v = \varepsilon_v$;*
- *Si $n = 3$ o bé $a \neq -d$ o bé $a = -d$ i $(-1, -d)_v = \varepsilon_v$;*

Es demostrarà el teorema per casos i s'utilitzarà aquest corol·lari amb els casos que ja s'hagin demostrat.

Demostració.

- Si $n = 2$, f representa $0 \Leftrightarrow -a_1/a_2$ és un nombre quadrat. Ara, a k^*/k^{*2}, $-a_1/a_2 = -a_1a_2 = -d$, i.e f representa $0 \Leftrightarrow d = -1$ a k^*/k^{*2} .

- Si $n = 3$, f representa 0 si, i només si, la forma

$$-a_3 f \sim -a_3a_1X_1^2 - a_3a_2X_2^2 - X_3^2$$

també. Així, aplicant la definició del símbol de Hilbert, l'última forma representa 0 si, i només si, $(-a_3a_1, -a_3a_2)_p = 1$. Si desenvolupem la part esquerra de la igualtat aplicant les propietats del símbol: (s'ha obviat el subíndex v del símbol de Hilbert per facilitar la lectura)
$(-a_3a_1, -a_3a_2) = (-a_3, -a_3a_2)(a_1, -a_3a_2) =$
$(-a_3, -a_3)(-a_3, a_2)(a_1, -a_3)(a_1, a_2) =$
$(-1, -a_3)(a_3, -a_3)(-1, a_2)(a_3, a_2)(a_1, -1)(a_1, a_3)(a_1, a_2) =$
$(-1, -1)(-1, a_3)(a_3, -1)(a_3, a_3)(-1, a_2)(a_3, a_2)(a_1, -1)(a_1, a_3)(a_1, a_2) =$
$(-1, -1)(a_3, a_3)(-1, a_2)(a_3, a_2)(a_1, -1)(a_1, a_3)(a_1, a_2)$

En particular, per la propietat (iv) dels símbols de Hilbert tenim:

$$(a_3, a_3) = (a_3, -a_3^2) = (a_3, a_3^2)(a_3, -1) = (a_3, -1),$$

i, podem reescriure:
$(-1, -1)(a_3, a_3)(-1, a_2)(a_3, a_2)(a_1, -1)(a_1, a_3)(a_1, a_2) =$
$(-1, -1)(-1, a_3)(-1, a_2)(-1, a_1)(a_1, a_3)(a_1, a_2)(a_2, a_3) =$
$(-1, -1)(-1, a_3a_2)(-1, a_1)(a_1, a_3)(a_1, a_2)(a_2, a_3) =$
$(-1, -1)(-1, a_1a_2a_3)(a_1, a_3)(a_1, a_2)(a_2, a_3) =$
$(-1, -a_1a_2a_3)(a_1, a_3)(a_1, a_2)(a_2, a_3) =$
$(-1, -d(f)) \cdot \varepsilon$

I per tant, f representa 0 si, i només si, $(-1, -d(f)) = \varepsilon$.

- Si $n = 4$, aleshores podem expressar $f(X) = a_1X_1^2 + a_2X_2^2 - (-a_3X_3^2 - a_4X_4^2) = g(X) - h(X)$. Pel Corol·lari 5.8, f representa 0 en k si, i només si, existeix $x \in k^*/k^{*2}$ tal que és representat per $g(X)$ i $h(X)$ i, pel Corol·lari 5.12, aquest element x verifica:

$$(x, -a_1a_2)_v = (a_1, a_2)_v \quad i \quad (x, -a_3a_4)_= (-a_3, -a_4)_v.$$

Siguin $A \subset k^*/k^{*2}$ el subconjunt d'elements x que satisfan la primera igualtat i B el subconjunt anàleg per la segona igualtat. És clar que ambdós són subconjunts no buits: a_1 pertany a A i $-a_3$ a B, per les propietats del símbol de Hilbert. La demostració es redueix a veure que $A \cap B \neq \emptyset$. Pel lema 5.15 (ii) que demostrem més endavant, aquest fet és equivalent a que no es verifiqui

$$a_1a_2 = a_3a_4 \quad i \quad (a_1, a_2)_v = -(-a_3, -a_4)_v.$$

La primera igualtat implica $d = 1$. Per tant, si $d \neq 1$ és clar que f representa 0. Si es compleix $d = 1$, tenim (òvbiant el subindex v del símbol de Hilbert)

$$\varepsilon_p = (a_1, a_2)(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)(a_3, a_4) =$$

$$(a_1, a_2)(a_1, a_3a_4)(a_2, a_3a_4)(a_3, a_4) = (a_1, a_2)(a_1a_2, a_3a_4)(a_3, a_4) =$$

$$(a_1, a_2)(a_3a_4, a_3a_4)(a_3, a_4) = (a_1, a_2)(a_3a_4, -(a_3a_4)^2)(a_3, a_4) =$$

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

Per tant, cal $\varepsilon_v = -(-1, -1)_v$, tal com enuncia el teorema que volem desmotrar.

$\square$

Hi ha un últim resultat que caracteritza que tota forma quadràtica de 5 variables (o més) sempre té solució en $\mathbb{Q}_p$. Notem que separem aquest cas dels anteriors perquè aquest resultat no és cert en $\mathbb{R}$.

Teorema 5.13. *Una condició suficient perquè una forma quadràtica f representi 0 en $\mathbb{Q}_p$ és que $rang(f) = n \geqslant 5$.*

Previ a la demostració d'aquest teorema, vegem que amb el mateix raonament que pel corol·lari anterior, obtenim el següent resultat:

Corol·lari 5.14. *La forma f representa $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ si $rang(f) = n \geqslant 4$.*

Demostració. (del teorema 5.13) Pel cas $n \geqslant 5$ és suficient demostrar per $n = 5$. Pel lema 5.15 (ii), una forma de rang 2 representa almenys 2 o 4 elements en k^*/k^{*2}, segons si p és primer senar o $p = 2$, i en conseqüència també les de rang $\geqslant 2$. Existeix doncs, $a \in k^*/k^{*2}$ tal que $a \neq d$ i és representat per f. Per tant, podem expressar $f = aX^2 + g$, on g és una forma de rang 4 i discriminant $d(f)/a \neq 1$. Aplicant el cas $n = 4$ demostrat anteriorment, tenim que g representa 0, i conseqüentment, f també. $\square$

El següent lema està definit per $k = \mathbb{Q}_p$, és a dir, k no representa en cap cas el cos dels nombres reals. Aquest cas el comentem al final.

Lema 5.15. *(i) Si $a \in k^*/k^{*2}$ i $\varepsilon = \pm 1$, anotem per H_a^ε el conjunt de $x \in k^*/k^{*2}$ tal que $(a, x)_p = \varepsilon$.*

Si $a = 1$, H_a^1 té exactament 4 elements si $p \neq 2$ i 8 elements si $p = 2$ i, $H_a^{-1} = \emptyset$.

Si $a \neq 1$, H_a^ε té exactament 2 elements si $p \neq 2$ i 4 elements si $p = 2$.

(ii) Siguin $a, a' \in k^*/k^{*2}$ i $\varepsilon, \varepsilon' \in \{\pm 1\}$. Si H_a^ε i $H_{a'}^{\varepsilon'}$ són conjunts no buits, aleshores

$$H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset \Leftrightarrow a = a' \quad i \quad \varepsilon = -\varepsilon'.$$

Demostració. (i) Si a és un quadrat, per qualsevol $x \in k^*/k^{*2}$ es verifica $(x, a)_p = 1$. Per tant, $\#H_a^1 = \#k^*/k^{*2}$, i en la caracterització dels nombres quadrats en $\mathbb{Q}_p$, vista en el capítol de Nombres p-àdics, hem vist que $\#k^*/k^{*2}$ és 4 si $p \neq 2$ i 8 si $p = 2$. Pel mateix motiu, $H_a^{-1} = \emptyset$.

Suposem que a no és un quadrat i considerem l'aplicació

$$k^*/k^{*2} \to \{\pm 1\}$$

$$b \mapsto (a, b)_p.$$

Com que el símbol de Hilbert és no degenerat, l'aplicació és exhaustiva. Aleshores, el nucli de l'aplicació, H_a^1, és un subgrup d'índex 2 en el cas $p \neq 2$ i un subgrup d'índex 4 en el cas $p = 2$.

El conjunt H_a^{-1} és el complementari de H_a^1, aleshores, si $p \neq 2$, $\#H_a^{-1} = 4 - 2 = 2$ i si $p = 2$, $\#H_a^{-1} = 8 - 4 = 4$.

(ii) Suposem H_a^ε i $H_{a'}^{\varepsilon'}$ són no buits i disjunts. Aleshores, pel resultat anterior, almenys tenen 2 o 4 elements segons si p és senar o $p = 2$. Observem que:

- Si són disjunts, els elements d'un conjunt són complementaris amb l'altre, per tant, $H_a^{\varepsilon} = H_{a'}^{-\varepsilon'}$ i $H_a^{-\varepsilon} = H_{a'}^{\varepsilon'}$.
- $1 \in H_a^1$ i $1 \in H_{a'}^1$ i per tant, $H_a^1 \cap H_{a'}^1 \neq \emptyset$.

Aleshores, en conseqüència d'aquestes dues observacions, sabem que $H_a^1 = H_{a'}^1$. Per tant, per tot $x \in k^*/k^{*2}$, es verifica $(x, a)_p = (x, a')_p$. Com el símbol de Hilbert és no degenerat, tenim $a = a'$ i conseqüentment $\varepsilon = -\varepsilon'$ per la primera observació.

Per últim, suposem que $a = a'$ i $\varepsilon = -\varepsilon'$. Aleshores tenim:

$$H_a^{\varepsilon} = H_a^{-\varepsilon'} = H_{a'}^{-\varepsilon'},$$

per tant, H_a^{ε} i $H_{a'}^{\varepsilon'}$ són disjunts. $\square$

Pel cas real, és immediat el resultat anàleg ja que el símbol de Hilbert també és no degenerat en $\mathbb{R}$. En efecte, en $\mathbb{R}^*/\mathbb{R}^{*2}$, hi ha dos elements. Seguint la mateixa notació, $\#H_1^1 = 2$ i $\#H_1^{-1} = \emptyset$, i, anàlogament, $\#H_{-1}^1 = 1$ i $\#H_{-1}^{-1} = 1$. Aleshores, amb un raonament similar se segueix exactament l'enunciat (ii).

6 Demostració del Teorema de Hasse-Minskowski

En aquest capítol es fa la demostració del Teorema de Hasse-Minkowski, introduït al capítol 3.

Teorema 6.1. *(Hasse-Minkowski) Sigui $f(X_1, ..., X_n)$ una forma quadràtica de rang n amb tots els seus coeficients a $\mathbb{Q}$. Una condició suficient i necessària perquè $f(X_1, ..., X_n) = 0$ tingui solució no trivial en $\mathbb{Q}$ és que $f(X_1, ..., X_n) = 0$ tingui solució no trivial en $\mathbb{R}$ i en $\mathbb{Q}_p$, per tot nombre primer p.*

Ja hem vist que hi ha una implicació que és molt clara: si f representa 0 en $\mathbb{Q}$, aleshores f representa 0 en $\mathbb{R}$ i també representa 0 en $\mathbb{Q}_p$ per tot nombre primer p. Falta veure l'altra implicació.

Sabem que podem suposar que la forma quadràtica f de la hipòtesi és una forma quadràtica diagonal i cosniderarem 5 casos segons el valor del rang n. Farem per separat els casos $n = 1, 2, 3$ i 4 i, finalment, el cas $n \geq 5$.

Cas $n = 1$. El teorema és trivial ja que aX^2 no representa 0 en cap cos.

Cas $n = 2$. Aquest cas l'hem vist en el capítol 3 a través de la caracterització dels quadrats en $\mathbb{Q}$. Recordem que la idea és que tenim $f(X, Y) = aX^2 + bY^2$, on $a, b \in \mathbb{Q}^*$.

Podem considerar $q = X^2 + \frac{b}{a}Y^2$ i és clar que les condicions f representa 0 i q representa 0 són equivalents. Aleshores, pel cas $n = 2$, podem suposar que la nostra forma quadràtica f és de la forma $X^2 - aY^2$, on $a \in \mathbb{Q}^*$.

Per hipòtesi f representa 0 en $\mathbb{R}$ i per tant, necessàriament tenim $a > 0$. Per altra banda, tenim que a és un quadrat en cada $\mathbb{Q}_p$. Per tant, a és un nombre quadrat a $\mathbb{Q}$, condició suficient i necessària perquè f representi 0 en $\mathbb{Q}$.

Cas $n = 3$. Aquest cas en particular és el Teorema de Legendre. Considerem la forma quadràtica

$$f(X, Y, Z) = aX^2 + bY^2 + cZ^2$$

on $a, b, c \in \mathbb{Q}^*$.

Si $q = X^2 + \frac{b}{a}Y^2 + \frac{c}{a}Z^2$, les condicions f representa 0 i q representa 0 són equivalents. Podem multiplicar q per un nombre enter quadrat adequat de manera que tingui tots els coeficients a $\mathbb{Z}$ i és igualment equivalent a f. Per tant, per a $n = 3$ podem suposar que tenim una forma quadràtica de la forma

$$f(X, Y, Z) = Z^2 - aX^2 - bY^2$$

on:

(1) $a, b \in \mathbb{Z}$ i $a \cdot b \neq 0$.

(2) $|a| \leqslant |b|$ (ja que es pot intercanviar el rol de X i Y).

(3) a, b són lliure de quadrats.

Farem inducció sobre $m := |a| + |b|$. Per (1), el cas inicial és $m = 2$. I per tant, tenim: $a = \pm 1$ i $b = \pm 1$.

Com f representa 0 en $\mathbb{R}$ no és possible que $a = -1$ i $b = -1$ perquè $X^2 + Y^2 + Z^2 = 0$ no té solucions no trivials a $\mathbb{R}$. La resta de casos són evidents que representen 0 en $\mathbb{Q}$: $X^2 - Y^2 + Z^2$ i $-X^2 + Y^2 + Z^2$ representen 0 en $(1, 1, 0)$ i $-X^2 - Y^2 + Z^2$ en $(0, 1, 1)$.

Ara suposem $m > 2$. Per (1) i (2) tenim que $|b| \geqslant 2$, i per (3) podem escriure b de la forma:

$$b = \prod_i p_i,$$

amb p_i primers tots diferents. Sigui $p = p_i$ per algun índex i, aleshores observem que a és un residu quadràtic mòdul p. Si $p \mid a$ és clar que a és un residu quadràtic mòdul p. Suposem doncs, que $p \nmid a$. Per hipòtesi existeix $(x, y, z) \in \mathbb{Q}_p^3$, $(x, y, z) \neq (0, 0, 0)$, tal que $z^2 - ax^2 - by^2 = 0$. Definim:

$$h := \inf\{ord_p x, ord_p y, ord_p z\}.$$

Aleshores $(x_0, y_0, z_0) = (p^{-h}x, p^{-h}y, p^{-h}z) \in \mathbb{Z}_p^3$ verfica

$$f(x_0, y_0, z_0) = p^{-2h}(z^2 - ax^2 - by^2) = 0,$$

i almenys una de les coordeandes x_0, y_0 o z_0 és una unitat p-àdica.

Com que $p \mid b$, se segueix que $z_0^2 - ax_0^2 \equiv 0 \pmod{p}$. Si $p \mid x_0$, cal que $p \mid z_0$ també i, per tant, $p^2 \mid by_0^2$. Ara bé, si b és lliure de quadrats, $p \mid y_0$ i això és una contradicció amb el fet que almenys una de les coordeandes és una unitat p-àdica.

Podem repetir l'argument per tot $p \mid b$, i tenim que a és residu quadràtic mòdul p, per tot primer p divisor de b. Aleshores, a és residu quadràtric mòdul b i podem escriure

$$t^2 = a + bb',$$

suposant $|t| < \frac{|b|}{2}$, amb un sistema adequat de representants de les classes laterals mod p.

Aleshores, $bb' = t^2 - a$ és la norma de l'element $t + \sqrt{a} \in (k(\sqrt{a})|k)$, on $k = \mathbb{Q}_v$, per tot $v \in V$. I f representa 0 en k si, i només si, $q = Z^2 - aX^2 - b'Y^2$ representa 0 en k. En efecte, aplicant la proposició 4.2 i el fet que $N(k(\sqrt{a})|k)$ té estructura de grup:

$$f \text{ representa 0 en } k \Leftrightarrow (a, b)_v = 1 \Leftrightarrow b \in N(k(\sqrt{a})|k) \Leftrightarrow$$
$$b' \in N(k(\sqrt{a})|k) \Leftrightarrow (a, b')_v = 1 \Leftrightarrow q \text{ representa 0 en } k.$$

Aleshores, com

$$|b'| = |\frac{t^2 - a}{b}| \leqslant |\frac{t^2}{b}| + |\frac{a}{b}| \leqslant \frac{|b|}{2} + 1 < |b|,$$

perquè estem sota les hipòtesis que $|b| > 2$ i $|t| < \frac{|b|}{2}$, podem escriure

$$b' = b''u^2,$$

de manera que b'' sigui lliure de quadrats.

Les formes quadràtiques $Z^2 - aX^2 - b'Y^2$ i $Z^2 - aX^2 - b''Y^2$ són equivalents i, en particular, aquesta última verifica:

$$|a| + |b''| < |a| + |b|.$$

Per hipòtesi d'inducció, $Z^2 - aX^2 - b''Y^2$ representa 0 en $\mathbb{Q}$ i conseqüentment, f també, tal com volíem demostrar.

Cas $n = 4$. Considerem

$$f(X_1, X_2, X_3, X_4) = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2).$$

Per hipòtesi, f representa 0 en qualsevol $\mathbb{Q}_v$, per tot $v \in V$. Aleshores, pel corol·lari 5.8, existeix $x_v \in \mathbb{Q}_v^*$ tal que és representat per

$$aX_1^2 + bX_2 \quad i \quad cX_3^2 + dX_4^2.$$

Ara bé, l'existència d'aquest element x_v és equivalent a dir que

$$(x_v, -ab)_v = (a, b)_v,$$

$$(x_v, -cd)_v = (c, d)_v,$$

pel cas $n = 2$ del corol·lari 5.12, que podíem aplicar tant a $\mathbb{Q}_p$, per tot primer p, com a $\mathbb{R}$. En efecte, seguint la notació d'aquest corol·lari, l'element que es representa és x_v, $d(g) = -ab$ i $d(h) = -cd$, i $\varepsilon_v(g) = (a, b)_v$ i $\varepsilon_v(h) = (c, d)_v$.

Aleshores, ara podem aplicar el teorema d'existència de nombres racionals donada una família de símbols de Hilbert, el teorema 4.9. En efecte, tenim una família de dos elements racionals $\{-ab, -cd\} \subset \mathbb{Q}^*$ i una família de símbols de Hilbert $(-ab, x_v)_v$,$(-cd, x_v)_v$ per qualsevol $v \in V$. Observem que:

- Es satisfà que $\prod_{v \in V}(-ab, x_v)_v = 1$ perquè per hipòtesi, $(-ab, x_v)_v = (a, b)_v$ on $a, b \in \mathbb{Q}^*$, i per tant, pel Teorema de Hilbert, $\prod_{v \in V}(a, b)_v = 1$. anàlogament, $\prod_{v \in V}(-cd, x_v)_v = 1$.
- És immediat aleshores que quasi tots els símbols $(-ab, x_v)_v$, $(-cd, x_v)_v$ són iguals a 1.
- Per tot v, $(-ab, x_v)_v = (a, b)_v$, $(-cd, x_v)_v = (c, d)_v$, per construcció.

Es compleixen doncs, totes les hipòtesis i per tant, existeix un element $x \in \mathbb{Q}^*$ tal que

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

per qualsevol $v \in V$.

Tornant a aplicar el corol·lari 5.12, aquestes igualtats són equivalents al fet que $aX_1^2 + bX_2^2$ i $cX_1^2 + dX_2^2$ representen x en $\mathbb{Q}_v$. Per tant, $aX_1^2 + bX_2^2 - xX_3^2$ i $cX_1^2 + dX_2^2 - xX_3^2$ representen zero en $\mathbb{Q}_v$.

Aquestes dues formes quadràtiques són de rang 3 i representen 0 en $\mathbb{Q}_v$. Per tant, pel cas $n = 3$ demostrat anteriorment, sabem que també representen 0 en $\mathbb{Q}$. Conseqüentment, x és representat per $aX_1^2 + bX_2^2$ i $cX_1^2 + dX_2^2$ en $\mathbb{Q}$, i per tant,

$$f = aX_1^2 + bX_2^2 - (cX_1^2 + dX_2^2)$$

representa 0 en $\mathbb{Q}$, tal i com volíem demostrar.

Cas $n \geqslant 5$. Finalitzem la demostració fent inducció sobre n. Considerem $f(X_1, ..., X_n)$ de la forma:

$$f = h - g,$$

on $h = a_1X_1^2 + a_2X_2^2$ i $g = -(a_3X_3^2 + ... + a_nX_n^2)$.

Per hipòtesi, f representa 0 en $\mathbb{Q}_v$ per qualsevol $v \in V$. En conseqüència, existeix $a_v \in \mathbb{Q}_v^*$ tal que és representat per h i g en $\mathbb{Q}_v$, és a dir, existeix $(x_1^v, x_2^v, ..., x_{n-1}^v, x_n^v) \in (\mathbb{Q}_v)^n$ tal que:

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, ..., x_n^v).$$

Definim el subjconjunt $S \subset V$ com el conjunt que conté $\{2, \infty\}$ i tots els nombres primers p tals que $p \mid a_i$ per alguna $i \in \{3, ..., n\}$. És clar que S és un subconjunt finit. Suposem $v \in S$.

Recordatori 6.2. *Hem vist en els capítols anteriors:*

(i) $(\mathbb{Q}_v^*)^2 \subset \mathbb{Q}_v^*$ *és obert, i per tant,* $a_v \cdot (\mathbb{Q}_v^{*2}) \subset \mathbb{Q}_v^*$ *és subgrup obert també.*

(ii) Per qualsevol conjunt finit $S \subset \{p : p\, primer\} \cup \{\infty\}$ *tenim que:*

$$i : \mathbb{Q}^* \longrightarrow \prod_{v \in S} \mathbb{Q}_v^*, \quad x \longmapsto (i_v(x))_{v \in S},$$

on $i_v(x)$ *és la imatge de* x *en* $\mathbb{Q}_v$*, té imatge densa.*

Si anotem h_v a la forma quadràtica h definida en $\mathbb{Q}_v \times \mathbb{Q}_v$, és a dir,

$$h_v : \mathbb{Q}_v \times \mathbb{Q}_v \longrightarrow \mathbb{Q}_v$$

$$(x_1^v, x_2^v) \longrightarrow h_v(x_1^v, x_2^v) = a_v$$

Aleshores, $h_v^{-1}(a_v \cdot (\mathbb{Q}^{*2}))$ és un obert en $\mathbb{Q}_v \times \mathbb{Q}_v$. I com el producte de $\mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}_v \times \mathbb{Q}_v$ té imatge densa,

$$Im(\mathbb{Q} \times \mathbb{Q}) \cap h_v^{-1}(a_v \cdot (\mathbb{Q}^{*2})) \neq \emptyset.$$

En conseqüència, existeixen $x_1, x_2 \in \mathbb{Q}$ tals que $a = h(x_1, x_2)$ i $a \cdot a_v \in \mathbb{Q}_v^{*2}$

Considerem la forma

$$f_1 = aZ^2 - g.$$

Veurem que g representa l'element a en $\mathbb{Q}_p$, ja que aleshores, f_1 representa 0 en $\mathbb{Q}_p$ i com té una unitat menys de rang, podem aplicar la hipòtesi d'inducció.

Sota la hipòtesi $v \in S$, g representa a_v en $\mathbb{Q}_v$ i també representa a perquè $a \cdot a_v \in \mathbb{Q}_v^{*2}$. I per tant, f_1 representa 0 en $\mathbb{Q}_v$.

Si $v \notin S$, aleshores els coeficients $-a_3, ..., -a_n$ són unitats v-àdiques, per tant, $disc(g) = (-a_3) \cdots (-a_n)$ també pertany a $\mathbb{Z}_v^*$. A més, com $v \neq 2, \infty$, l'invariant

$$\varepsilon_v(g) = 1,$$

per l'algoritme de càlcul del símbol de Hilbert.

Notem doncs, que si $n = 5$, la forma g té exactament 3 variables i verifica que:

- o bé $a \neq -d$
- o bé, $a = -d$ i $(-1, -d(g))_v = 1$ per l'observació 4.3 i per tant,

$$(-1, -d(g))_v = \varepsilon_v(g).$$

Per tant, pel corol·lari 5.12, g representa a. Si $n > 5$, aleshores g té 4 variables o més i pel mateix corol·lari, g representa a. En equalsevol cas, es compleixen les condicions suficients i necessaries perquè f_1 representi 0 en $\mathbb{Q}_v$. Com que el rang de f_1 és $n - 1$, per hipòtesi d'inducció, f_1 representa 0 en $\mathbb{Q}$. Conseqüentment, g representa a en $\mathbb{Q}$, i per tant, h i g representen el mateix element a en $\mathbb{Q}$. Tenim doncs que $f = h - g$ representa 0 en $\mathbb{Q}$.

D'aquesta manera, queda completada la demostració del Teorema de Hasse-Minkowski, segon i últim objectiu proposat del treball.

7 Comentaris finals

Per tancar el treball, volem esmentar dues conseqüències immediates del Teorema de Hasse-Minkowski, així com dos resultats clàssics relacionats. Amb aquests dos exemples, es vol destacar la importància dels capítols 4 i 5, no només pels resultats presentats com a eines de la demostració del Teorema de Hasse-Minkowski, sinó també com a resultats essencials per l'aplicació d'aquest en problemes.

Hem demostrat al cinquè capítol que una condició suficient i necessària perquè la forma quadràtica f representi a en k és que la forma $f - aZ^2$ representi 0 en k, on k era un cos de característica diferent de 2 (que inclou $\mathbb{Q}, \mathbb{R}$ i $\mathbb{Q}_p$ per tot primer p). Aleshores es dedueix que una forma quadràtica f representa $a \in \mathbb{Q}$ si, i només si, f representa a en $\mathbb{Q}_v$. Per tant, el Teorema de Hasse-Minkowski es pot reformular amb el següent enunciat:

Teorema 7.1. *(Hasse-Minkowski) Sigui $f(X_1, ..., X_n)$ una forma quadràtica de rang n amb tots els seus coeficients a $\mathbb{Q}$ i $a \in \mathbb{Q}^*$. Una condició suficient i necessària perquè $f(X_1, ..., X_n)$ representi a en $\mathbb{Q}$ és que $f(X_1, ..., X_n)$ representi a en $\mathbb{R}$ i en $\mathbb{Q}_p$, per tot nombre primer p.*

Aquest, de fet, és l'enunciat habitual que s'aplica.

En segon lloc, notem que, també en el cinquè capítol, hem demostrat que les formes quadràtiques de rang $n \geqslant 5$ sempre representen 0 en $\mathbb{Q}_p$, per tot nombre primer p (teorema 5.11). Aleshores, pel Teorema de Hasse-Minkowski, qualsevol forma quadràtica $f(X)$ de rang $n \geqslant 5$ representa 0 en $\mathbb{Q}$ si, i només si, representa 0 en $\mathbb{R}$.

Treballar amb formes quadràtiques, i precisament estudiar la representació de nombres racionals per aquestes, ens pot portar a preguntar-nos quins nombres enters es poden expressar com a suma de quadrats. La resposta és un conegut resultat del matemàtic A. M. Legendre:

Tot nombre enter positiu es pot escriure com a suma de quatre nombres quadrats.

La traducció de l'enunciat en termes del treball és que la forma quadràtica

$$f(X) = X_1^2 + X_2^2 + X_3^2 + X_4^2$$

representa qualsevol nombre enter positiu n en $\mathbb{Z}$.

La primera idea és demostrar que tot nombre enter n pot ser representat en $\mathbb{Q}$ per la forma $f(X) = X_1^2 + X_2^2 + X_3^2 + X_4^2$, i pel Teorema de Hasse-Minowski, serà suficient veure-ho en els cossos locals.

Com n és positiu, l'equació $f(X) = X_1^2 + X_2^2 + X_3^2 + X_4^2 = n$ té solució no trivial en $\mathbb{R}$. Pel fet que $n \in \mathbb{Q}^*$, sabem pel corol·lari 5.14 que $f(X) = X_1^2 + X_2^2 + X_3^2 + X_4^2$ també representa n en $\mathbb{Q}_p$. Així doncs, $f(X) = X_1^2 + X_2^2 + X_3^2 + X_4^2 = n$ té solució no trivial en $\mathbb{Q}$.

La segona idea és demostrar que l'existència d'una solució en $\mathbb{Q}$ implica l'existència d'una solució en $\mathbb{Z}$. La demostració d'aquest resultat pot consultar-se en [8], capítol 4, Apendix A.

De fet, està demostrat que tot nombre enter positiu n tal que $n \neq 4^a(8b-1)$, per $a, b \in \mathbb{Z}$, és suma de tres nombres quadrats. Amb el mateix plantejament anterior, vegem que $f(X) = X_1^2 + X_2^2 + X_3^2$ representa qualsevol enter positiu n tal que $n \neq 4^a(8b-1)$ en

tots els espais locals. Sobre el cos dels nombres reals, $f(X)$ representa n pel fet que n és un valor positiu. Aplicant el corol·lari 5.12, és suficient veure que o bé $n \neq -d(f)$ en $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, o bé $(-1, -d(f))_p = \varepsilon_p(f)$. Pel cas p senar, es té $(-1, -d(f))_p = (-1, -1)_p = 1 = \varepsilon_p(f)$. Pel cas $p = 2$, notem que $n = 1$ en $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, ja que la conidició $n \neq 4^a(8b - 1)$ equival a que $-n$ no sigui un quadrat en $\mathbb{Q}_2^*$. Així doncs, existeix una solució en $\mathbb{Q}$, i pel mateix lema referenciat anteriorment, això implica l'existència de solució en $\mathbb{Z}$.

Veiem, doncs, com el Toerema de Hasse-Minkowski junt amb els resultats vistos en els capítols previs, permet abordar de manera sistemàtica certs resultats clàssics.

A mode de conclusió, volem notar que la demostració del Teorema de Hasse-Minkowski pot veure's com un recull ordenat dels resultats vistos en l'estudi sistemàtic que hem fet en els capítols anteriors. La reformulació del Teorema de Hasse-Minkowski que hem fet al Teorema 7.1, per exemple, és fruit d'aquest estudi sistemàtic.

Tot i que alguns passatges dels capítols 2, 4, 5 i 6 són de caràcter més tècnic, s'ha intentat contextualitzar aquestes parts en relació al treball i posar de relleu la importància d'alguns dels resultats que, tot i no ser el teorema central del treball, mereixen especial atenció. Sobretot, els resultats de les seccions *Propietats dels símbols de Hilbert sobre nombres racionals* i *Representació de nombres p-àdics i reals per formes quadràtiques*. Especialment en el capítol 3, si bé s'ha emmarcat el resultat principal del treball en el seu context, també s'ha assenyalat problemes relacionats o possibles continuacions, com ara l'estudi de contraexemples al principi local-global per a cúbiques (amb la cúbica de Selmer), amb les implicacions que això comporta a la teoria de corbes el·líptiques, o bé formulacions més geomètriques del principi local-global.

Referències

[1] Cassels, J.W.S.: *Lectures on elliptic curves. London Mathematical Society student texts; 24. Cambridge University Press, 1991.*

[2] Gouvea, F.Q.: *p-adic Numbers. Universitext; 282. Springer, 1993.*

[3] Ireland, K.; Rosen, M.: *A classical introduction to modern number theory. Graduate Texts in Mathematics, No. 84. Springer-Verlag, New York, 1990.*

[4] Kato, K.; Kurokawa, N.; Saito, T.: *Number Theory 1. Fermat's dream Translations of mathematical monographs; 240. American Mathematical Society, 2011.*

[5] Koblitz, N.: *p-adic Numbers, p-adic Analysis and Zeta-function. Second edition. Texts in Mathematics, No. 58. Springer-Verlag, New York, 1984.*

[6] Mazur, B.: *On the passage from local to global in number theory. Bulletin of the American Mathematical Society, Volume 29 (1993), 14-50. DOI:10.1090/S0273-0979-1993-00414-2*

[7] Selmer, E. S.: *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Acta Math., Volume 85 (1951), 203-362. DOI: 10.1007/BF02395746*

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

[9] Silverman, J.; Tate, J.: *Rational Points on Elliptic Curves. Undergraduate Texts in Mathematics; No. 281. Springer, 1992.*

[10] Travesa, A.: *Teoria de Nombres. Apunts de l'assignatura Mètodes algebraics en Teoria de Nombres. Universitat de Barcelona, 2016.*