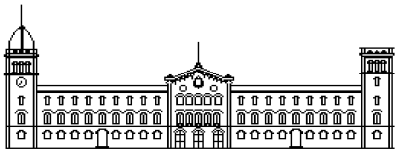

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques
Universitat de Barcelona

EL CONTRAEXEMPLE DE SELMER AL PRINCIPI DE HASSE

Eduard Soto Ballesteros

Director: Pilar Bayer i Isant
Realitzat a: Departament d'Àlgebra i Geometria. UB

Barcelona, 21 de juny de 2013

Introduction

We say that an equation is Diophantine if it is defined by a polynomial with integer (or rational) coefficients and we allow the solutions to take integer (or rational) values only. These equations owe their name to the Greek mathematician Diophantus of Alexandria (s. III AD), who made a first study of them.

It is easy to see that a necessary condition for a Diophantine equation to have integer solutions is that it is solvable in the real field $\mathbb{R}$ and in any ring $\mathbb{Z}/p^n\mathbb{Z}$, for each prime integer p and each $n \geq 1$. We can wonder if these conditions are also sufficient.

At the end of 19th century, H. Minkowski proved that, in very particular cases, the reciprocal is true. Later, in 1920, K. Hensel defined ultrametric distances over $\mathbb{Q}$ and built from them the field $\mathbb{Q}_p$ of the p-adic numbers. Only two years later, Hensel, as advisor of H. Hasse's thesis, suggested him to rewrite former results in number theory by using p-adic tools. Thus, Hasse announced and proved the nowadays known as Hasse-Minkowski's theorem or Hasse's local-to-global principle for quadratic forms. This principle states that for any homogeneous polynomial $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree 2 the following conditions are equivalent:

(a) $P(X_1, \ldots, X_n) = 0$ has non-zero solutions in $\mathbb{Q}$.

(b) $P(X_1, \ldots, X_n) = 0$ has non-zero solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$, for each prime p.

Thus, the existence of non-trivial solutions of a quadratic Diohantine equation over $\mathbb{Q}_p$ and $\mathbb{R}$ give us the existence of non-trivial solutions over $\mathbb{Q}$.

E. Selmer's work in 1951 [10] showed the first counterexamples to the Hasse principle, by means of cubic and quartic Diophantine equations. The equation $3X^3 + 4Y^3 + 5Z^3 = 0$, called Selmer's equation, is the simplest counterexample he gave.

The aim of our work is to present a counterexample to Hasse principle. We will see that Selmer's equation has local non-zero solutions everywhere but not global ones. Thus, its content is divided in 2 parts: the p-adic study of Selmer's equation, which is done in chapters 1 and 3, and its rational study, which is done in chapters 2 and 4.

Let us see its content by chapters.

- In chapter 1 we will build p-adic rings by using projective limits. We will also present basic results on p-adic fields so that we can achieve a local study of Selmer's equation. We will state Hensel'l lemma, which is an essential tool in proving the existence of p-adic solutions of polynomial equations; particularly, we will characterize the cubs of $\mathbb{Q}_p^*$.

- In chapter 2 some basic facts in the geometry of numbers are summarized.

- In chapter 3 we will prove the existence of non-zero solutions of Selmer's equation over $\mathbb{Q}_p$, for each prime p, and over $\mathbb{R}$. Particularly, we will find them in $\mathbb{Z}_p$ due to the fact that we are dealing with homogenous equations.

- In chapter 4 we will prove the non existence of non-zero solutions of Selmer's equation over $\mathbb{Q}$. The main tool for that will be the study of the ring of integers of the cubic number field $\mathbb{Q}(\sqrt[3]{6})$.

We would like to mention that the courses *Topology*, *Algebraic equations* and *Algebraic methods in number theory* have provided basic prerequisites to perform this work.

We shall note that we make use of the arithmetic of a cubic number field, not carried out in the *Algebraic methods in number theory* course, where the systematic study of number fields was done in the quadratic and cyclotomic cases only.

We mention the recent preprint by K. Conrad [5] as a basic reference. It contains (in 4 pages) a simplified proof of Selmer's contraexample. Worth mentioning that this preprint has been modified by his author twice while our work was being developed. Furthermore, we have been in contact with him in order to correct some miscalculations detected in his paper.

In a first edition of the preprint, Conrad deduced the existence of local solutions by using Hasse's inequality on the number of congruence solutions

of diagonal cubic equations. Later, Conrad uploaded a version of the preprint that excluded the use of that theorem. We have decided to explain the last proof of Conrad but we have added our previous study of diagonal equations in an annex since it can be useful in a future treatment of more general equations as can be seen, for example, in Selmer's original paper.

Most of the proofs are complete and self-contained, based on known results acquired in the above mentioned courses. In general, by looking at the references, one can see that our work presents changes in proofs, if able, in order to make them more direct and avoid the use of unnecessary sophisticated technics. Our main contribution in this sense is given in the theorems of Section 4.1, in which we avoid the complex study of the general cubic fields by providing *ad hoc* proofs for arithmetic results in the cubic field $\mathbb{Q}(\sqrt[3]{6})$, the necessary one for the study of Selmer's equation.

Introducció

Diem que una equació és diofantina si és polinòmica de coeficients enters (o racionals) i deixem que les variables prenguin només valors enters (o racionals). Aquest tipus d'equacions deuen el seu nom al matemàtic grec Diofant d'Alexandria (s. III d.C.), que va fer un primer estudi d'equacions d'aquest tipus.

És fàcil veure que una condició necessària perquè una equació diofantina tingui solució en els enters és que en tingui en $\mathbb{R}$ i en els anells $\mathbb{Z}/p^n\mathbb{Z}$, per a cada enter primer p i per a cada $n \geq 1$. Ens podem preguntar si aquestes condicions són suficients.

H. Minkowski, a finals del segle XIX, va demostrar que sota certes condicions molt restrictives el recíproc se satisfà. Anys més tard, al 1920, K. Hensel va definir distàncies ultramètriques sobre el cos dels racionals i, a partir de les quals, va construir el cos $\mathbb{Q}_p$ dels nombres p-àdics. Només dos anys més tard, Hensel, com a director de tesi de H. Hasse, va encarrega-li reescriure antics resultats en teoria de nombres mitjançant l'ús d'eines p-àdiques. Així, va enunciar i demostrar el que ara es coneix com a teorema de Hasse-Minkowski o principi local-global de Hasse per a formes quadràtiques. Aquest principi diu que per a cada polinomi homogeni $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ de grau 2 les condicions següents són equivalents:

(a) $P(X_1, \ldots, X_n) = 0$ té solucions no nul·les en $\mathbb{Q}$.

(b) $P(X_1, \ldots, X_n) = 0$ té solucions no nul·les en $\mathbb{R}$ i en $\mathbb{Q}_p$, per a cada primer p.

Així, l'existència de solucions no trivials en $\mathbb{Q}_p$ i $\mathbb{R}$ d'una equació quadràtica diofantina ens dóna l'existència de solucions no trivials en $\mathbb{Q}$.

El treball de E. Selmer de l'any 1951 [10] mostrà els primers contraexemples del principi de Hasse amb equacions diofantines de grau 3 i grau 4.

L'equació $3X^3 + 4Y^3 + 5Z^3 = 0$, anomenada equació de Selmer, és el contraexemple més senzill que va donar.

L'objectiu principal d'aquest treball és presentar un contraexemple al principi de Hasse. Veurem que l'equació de Selmer té solucions locals no nul·les arreu però no en té de globals. Així, el treball es divideix en dues parts: l'estudi p-àdic de l'equació de Selmer, que es porta a terme en els capítols 1 i 3, i l'estudi racional que s'efectua en els capítols 2 i 4.

Vegem els continguts del treball per capítols.

- En el capítol 1 es fa una construcció d'anells p-àdics mitjançant límits projectius i se n'estudien els resultats necessaris per a fer l'estudi local de l'equació de Selmer. S'introdueix el lema de Hensel, que és una eina fonamental per a demostrar sota certes condicions l'existència de solucions p-àdiques d'equacions polinòmiques i que, en particular, ens permetrà calcular els cubs de $\mathbb{Q}_p^*$.

- En el capítol 2 es resumeixen fets bàsics de geometria dels nombres.

- En el capítol 3 es veu l'existència de solucions no trivials de l'equació de Selmer en els cossos $\mathbb{Q}_p$, per a cada primer p, i sobre $\mathbb{R}$. Concretament, les trobarem a $\mathbb{Z}_p$ per tractar-se d'una equació homogènia.

- En el capítol 4 es demostra la no existència de solucions no trivials de l'equació de Selmer sobre $\mathbb{Q}$ mitjançant l'ús de les propietats de l'anell dels enters del cos cúbic $\mathbb{Q}(\sqrt[3]{6})$.

Com a prerequisits bàsics per a l'elaboració del treball citem continguts de les assignatures de *Topologia*, *Equacions algebraiques* i *Mètodes algebraics en teoria de nombres*.

Cal fer notar que el treball conté l'estudi aritmètic d'un cos de nombres de grau tres, no realitzat en el curs de *Mètodes algebraics en teoria de nombres*, on l'estudi sistemàtic de l'aritmètica de cossos de nombres es va fer únicament en els casos quadràtics i ciclotòmics.

Com a referència bàsica esmentem l'article recent de K. Conrad [5], que conté (en 4 pàgines) una demostració simplificada del contraexemple de Selmer. Val a dir que aquesta prepublicació ha estat modificada pel seu autor en el decurs de l'elaboració del nostre treball. A més, hem mantingut contacte amb ell a fi de corregir-hi certs errors de càlcul.

En una primera redacció, Conrad deduïa l'existència de solucions locals a partir de la desigualtat de Hasse per al nombre de solucions mòdul p d'equacions diagonals cúbiques. Però més endavant, Conrad ha donat una demostració que exclou l'ús del teorema de Hasse. Nosaltres hem optat en el treball per explicar en detall la darrera prova de Conrad però hem inclòs en un apèndix l'estudi previ d'equacions diagonals en tant que pot ésser útil en el tractament d'equacions més generals, tal com es posa de manifest, per exemple, en l'article original de Selmer.

La majoria de demostracions es presenten completes i autocontingudes, partint de la base dels resultats coneguts a partir dels cursos esmentats abans. En general, si es confronten les cites, es pot observar que el treball presenta, sempre que es pot, variants en les demostracions per tal de fer-les més directes i per tal d'evitar l'ús innecessari de tècniques massa sofisticades. En aquesta línia, les nostres principals aportacions es troben en els teoremes de la secció 4.1, on, a fi d'evitar el complex estudi dels cossos cúbics en general, hem fet demostracions *ad hoc* de la aritmètica del cos cúbic $\mathbb{Q}(\sqrt[3]{6})$, necessari per a l'estudi de l'equació de Selmer.

Agraïments

Vull agrair i dedicar aquest treball a dos persones sense les quals no hauria estat possible. La primera, Anna Masip i Navarro per haver-me confiat el seu ordinador quan el meu va deixar de funcionar sobtadament. La segona i imprescindible, la doctora Pilar Bayer i Isant, tutora d'aquest treball, per totes les hores divertides i plenes de coneixement que m'ha dedicat.

Índex

Capítol 1

El cos dels nombres p-àdics

En aquest capítol construirem l'anell dels enters p-àdics mitjançant límits projectius. Veurem els cos p-àdic com el seu cos de fraccions i en veurem propietats aritmètiques i topològiques bàsiques.

Per a simplificar notacions, en aquest capítol p designarà un enter primer qualsevol i A_n l'anell $\mathbb{Z}/p^n\mathbb{Z}$ de les classes de restes mòdul p^n.

1.1 L'anell $\mathbb{Z}_p$ dels enters p-àdics

Definició 1.1.1. Donat, per a cada $n \geq 1$, l'epimorfisme que projecta de forma natural A_{n+1} en A_n

$$\begin{array}{rccc} \phi_{n+1}: & A_{n+1} & \longrightarrow & A_n \\ & a + p^{n+1}\mathbb{Z} & \longmapsto & a + p^n\mathbb{Z}, \quad a \in \mathbb{Z}, \end{array}$$

definim el conjunt dels enters p-àdics

$$\mathbb{Z}_p := \left\{ (x_n)_n = (x_1, \dots, x_k, \dots) \in \prod_{n\geq 1} A_n : \phi_{n+1}(x_{n+1}) = x_n, n \geq 1 \right\}.$$

Observacions 1.1.2. (i) La suma $(+)$ i el producte $(\cdot)$ definits a $\mathbb{Z}_p$ component a component donen a $\mathbb{Z}_p$ una estructura d'anell commutatiu unitari, que l'identifica amb un subanell de $\prod_{n\geq 1} A_n$.

(ii) Podem incloure de forma natural $(\mathbb{Z}, +, \cdot)$ dins de $(\mathbb{Z}_p, +, \cdot)$ mitjançant

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ n & \longmapsto & (n + p\mathbb{Z}, \dots, n + p^s\mathbb{Z}, \dots). \end{array}$$

Per tant, $\mathbb{Z}_p$ és un anell de característica zero.

(iii) L'element neutre per a la suma és $0 = (p\mathbb{Z}, \dots, p^s\mathbb{Z}, \dots)$, i, per al producte, $1 = (1 + p\mathbb{Z}, \dots, 1 + p^s\mathbb{Z}, \dots)$.

(iv) Aquest mètode de construcció d'un anell a partir d'una família d'anells i de projeccions és el que s'anomena límit projectiu que amb notació estàndard s'escriu

$$\mathbb{Z}_p = \varprojlim A_n.$$

Definició 1.1.3. Per a cada $n \geq 1$, notarem per ε_n el morfisme que projecta un enter p-àdic x en la seva component n-èsima.

$$\begin{array}{rccc} \varepsilon_n : & \mathbb{Z}_p & \longrightarrow & A_n \\ & (x_1, \dots, x_n, \dots) & \longmapsto & x_n. \end{array}$$

Observació 1.1.4. Per a cada $n \geq 1$ i $x_n \in A_n$,

$$\varepsilon_n^{-1}(x_n) \neq \emptyset.$$

Lema 1.1.5. *Sigui $x = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_p$, aleshores*

$$a_i \equiv a_j \pmod{p^{\min(i,j)}}, \quad \textit{per a tot } i,\ j \geq 1.$$

Demostració. Per definició, $a_n + p^n\mathbb{Z} = \phi_{n+1}(a_{n+1} + p^{n+1}\mathbb{Z}) = a_{n+1} + p^n\mathbb{Z}$; per tant, $a_{n+1} \equiv a_n \pmod{p^n}$. Llavors

$$a_{n+j+1} \equiv a_{n+j} \equiv \cdots \equiv a_n \pmod{p^n},$$

d'on obtenim el resultat. □

Proposició 1.1.6. *$(\mathbb{Z}_p, +, \cdot)$ és un domini d'integritat.*

Demostració. Siguin $x = (a_n + p^n\mathbb{Z})_n$, $y = (b_n + p^n\mathbb{Z})_n$ enters p-àdics, suposem que $xy = 0$. És a dir, per a cada $n \geq 1$,

$$a_n b_n \equiv 0 \pmod{p^n}.$$

Suposem que $y \neq 0$, aleshores existeix $n_0 = \min\{n : b_n \not\equiv 0 \pmod{p^n}\}$. Del lema 1.1.5 deduïm que

$$b_{n_0+k} \not\equiv 0 \pmod{p^{n_0}}, \quad \text{per a tot } k \geq 0.$$

Per hipòtesi, per a cada $n \geq 1$,

$$a_{n_0+n-1} b_{n_0+n-1} \equiv 0 \pmod{p^{n_0+n-1}}$$

i

$$b_{n_0+n-1} \not\equiv 0 \pmod{p^{n_0}}$$

per tant,

$$a_{n_0+n-1} \equiv 0 \pmod{p^n}.$$

Aplicant el lema anterior, $a_n \equiv 0 \pmod{p^n}$, d'on s'obté el resultat. □

Observació 1.1.7. Sigui $x = (x_n)_n \in \mathbb{Z}_p$, recordem que tota classe $x_n \in A_n$ té un representant $a'_n \in \{0, 1, \ldots, p^n - 1\}$ amb $x_n = a'_n + p^n\mathbb{Z}$. Observem que si prenem l'expressió de a'_n en base p, aleshores existeixen $d_0, \ldots, d_{n-1} \in \{0, \ldots, p-1\}$ tals que

$$a'_n = d_0 + d_1 p + \cdots d_{n-1} p^{n-1}.$$

Del lema anterior es dedueix que

$$\begin{aligned} a'_1 &= d_0, \\ a'_2 &= d_0 + d_1 p, \\ &\vdots \\ a'_n &= \sum_{k=0}^{n-1} a'_k p^k. \end{aligned}$$

Així, cada enter p-àdic x té associada una única sèrie formal de potències

$$x \mapsto \sum_{k \geq 0} d_k p^k$$

amb $d_k \in \{0, 1, \ldots, p-1\}$; i, recíprocament, cada sèrie formal de potències d'aquest tipus té associat un únic enter p-àdic.

Proposició 1.1.8. *$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq A_n$, en un isomorfisme d'anells.*

Demostració. Prenguem per a cada $n \geq 0$ el morfisme

$$\begin{array}{rccc} \varepsilon_n : & \mathbb{Z}_p & \longrightarrow & A_n \\ & (x_1, \ldots, x_n, \ldots) & \longmapsto & x_n. \end{array}$$

Observem que $\mathrm{Im}(\varepsilon_n) = A_n$. En efecte, donat $a + p^n\mathbb{Z} \in A_n$, $x = (a + p^s\mathbb{Z})_s \in \mathbb{Z}_p$ i $\varepsilon_n(x) = a + p^n\mathbb{Z}$.
Se satisfà també que $\ker(\varepsilon_n) = p^n\mathbb{Z}_p$.

(i) $p^n\mathbb{Z}_p \subseteq \ker(\varepsilon_n)$.

Sigui $x \in p^n\mathbb{Z}_p$, llavors existeix $y \in \mathbb{Z}_p$ tal que

$$x = p^n y.$$

Aleshores, $\varepsilon_n(x) = \varepsilon_n(p^n y) = \varepsilon_n(p^n)\varepsilon_n(y) = 0$.

(ii) $\ker(\varepsilon_n) \subseteq p^n\mathbb{Z}_p$.

Sigui $x = (x_s)_s \in \ker(\varepsilon_n)$ amb sèrie de potències $\sum_k d_k p^k$, aleshores

$$\varepsilon_n(x) = \sum_{k=0}^{n-1} d_k p^k + p^n\mathbb{Z} = p^n\mathbb{Z},$$

per tant, $d_k = 0$ per a tot $0 \leq k \leq n-1$ i

$$x_s = \begin{cases} p^s\mathbb{Z} & \text{si } s \leq n, \\ \displaystyle\sum_{k=n}^{s-1} d_k p^k + p^s\mathbb{Z} & \text{si } s > n. \end{cases}$$

Prenguem $y = (y_s)_s$, amb

$$y_s = \sum_{k=0}^{s-1} d_{k+n} p^k + p^s\mathbb{Z}.$$

En efecte, $y \in \mathbb{Z}_p$ i per a cada $s > n$

$$\begin{aligned} p^n y_s &= \sum_{k=0}^{s-1} d_{k+n} p^{k+n} + p^s\mathbb{Z} \\ &= \sum_{k=n}^{s+n-1} d_k p^k + p^s\mathbb{Z} \\ &= \sum_{k=n}^{s-1} d_k p^k + p^s\mathbb{Z} \\ &= x_s. \end{aligned}$$

Per tant, $x = p^n y \in p^n\mathbb{Z}_p$.

Aplicant el primer teorema d'isomorfia,

$$\mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}_p/\ker(\varepsilon_n) \simeq \mathrm{Im}(\varepsilon_n) = A_n.$$

□

1.2 Unitats de $\mathbb{Z}_p$ i valoració p-àdica

Proposició 1.2.1. (a) $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : p \nmid x\}$.

(b) *Tot element $x \in \mathbb{Z}_p \setminus \{0\}$ es pot expressar de manera única com*

$$x = p^s u, \quad u \in \mathbb{Z}_p^*, \quad s \geq 0.$$

Demostració. (a) Notem que ser invertible a $\mathbb{Z}_p$ implica ser-ho component a component. Prenguem $x = (x_n)_n \in \mathbb{Z}_p$.

D'una banda, si $p \mid x$, llavors $p \mid x_1$ i x_1 no és invertible en A_1.

D'altra banda, si $p \nmid x$, existeix un índex $i \in \mathbb{N}$ tal que $p \nmid x_i$. Però atès que $\phi_{n+1}(x_{n+1}) = x_n$ i que ϕ_{n+1} és morfisme d'anells, es té que $p \nmid x_n$, per a tot n; així, x_n és invertible en A_n, per a tot n. Ja que $\phi_{n+1}\left(x_{n+1}^{-1}\right) = \phi_{n+1}\left(x_{n+1}\right)^{-1} = x_n^{-1}$, $(x_n^{-1})_n \in \mathbb{Z}_p$ i x és invertible en $\mathbb{Z}_p$.

(b) Observem que si $x = (x_n)_n \in \mathbb{Z}_p \setminus \{0\}$, llavors existeix $n_0 \geq 1$ tal que $x_{n_0} \neq 0$. Per tant, $p^n \nmid x$ per a cada $n \geq n_0$. Així existeix $\max_{p^n \mid x}(n)$. Sigui s aquest màxim, llavors existeix $u \in \mathbb{Z}_p$ tal que

$$x = p^s u$$

A més, $p \nmid u$ ja que $p^{s+1} \nmid x$, per tant, $u \in \mathbb{Z}_p^*$.

La unicitat deriva de ser domini d'integritat de característica zero.

□

Definició 1.2.2. Donat $x \in \mathbb{Z}_p \setminus \{0\}$ denotarem per $v_p(x)$ el màxim n tal que $p^n \mid x$. L'anomenarem valoració p-àdica de x. Notem que $n \geq 0$. Prendrem el conveni $v_p(0) = +\infty$.

Corol·lari 1.2.3. *L'anell $\mathbb{Z}_p$ és un domini d'ideals principals i, per tant, un domini de factorització única (amb un únic element irreductible, llevat d'associats).*

Demostració. Sigui I un ideal de $\mathbb{Z}_p$. Si $I = \{0\}$ ja hem acabat. Si $I \neq \{0\}$, prenguem

$$n := \min_{x \in\ I \setminus \{0\}} v_p(x).$$

Sigui $x \in I \setminus \{0\}$ tal que $v_p(x) = n$, aleshores existeix $u \in \mathbb{Z}_p^*$ tal que

$$x = p^n u.$$

D'una banda, atès que u és invertible,

$$p^n\mathbb{Z}_p = p^n u\mathbb{Z}_p = x\mathbb{Z}_p \subseteq I.$$

D'altre banda, per a cada $y \in I \setminus \{0\}$, $v_p(y) \geq n$, aleshores existeixen $u' \in \mathbb{Z}_p$ i $s \geq 0$ tal que

$$y = p^{n+s}u',$$

llavors, $I \subseteq p^n\mathbb{Z}_p$ i, per tant, I és principal. Com ja hem vist, $\{p^n\}_{n\geq 1}$ són els elements no invertibles de $\mathbb{Z}_p$ mòdul associats. En concret, l'únic element irreductible, llevat d'associats, és p. □

1.3 El cos $\mathbb{Q}_p$

Definició 1.3.1. El cos dels nombres p-àdics, denotat per $\mathbb{Q}_p$, és el cos de fraccions del domini $\mathbb{Z}_p$.

Observacions 1.3.2.

1. És fàcil veure, mitjançant (1.2.1), que

$$\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}].$$

2. Tot element $x \in \mathbb{Q}_p^*$ es pot expressar de manera única com

$$x = p^s u, \quad u \in \mathbb{Z}_p^*, \quad s \in \mathbb{Z}.$$

3. Podem estendre la valoració v_p sobre $\mathbb{Q}_p^*$ de manera que $v_p(x) \in \mathbb{Z}$ amb $v_p(x) \geq 0$ si, i només si, $x \in \mathbb{Z}_p \setminus \{0\}$.

Proposició 1.3.3. *Siguin $x, y \in \mathbb{Q}_p$, aleshores*

(a) $v_p(x \cdot y) = v_p(x) + v_p(y)$.

(b) $v_p(x^n) = n \cdot v_p(x)$. □

1.4 Estructura topològica de $\mathbb{Z}_p$

Proposició 1.4.1. *Per a cada $n \geq 1$, $(A_n, +, \cdot)$, amb la topologia discreta, és un anell topològic compacte.*

Corol·lari 1.4.2. $\mathfrak{A} := \prod_{n\geq 1} A_n$ *amb la topologia producte és un anell topològic compacte.*

Proposició 1.4.3. (a) *$\mathbb{Z}_p$ és un anell topològic compacte com a subespai tancat de $\mathfrak{A}$.*

(b) *$\{p^n\mathbb{Z}_p\}_{n\geq 1}$ és una base d'oberts del 0.*

Demostració. (a) Ja que $\mathbb{Z}_p$ és un subanell de $\mathfrak{A}$, $\mathbb{Z}_p$ és anell topològic. És a dir, la suma, el producte i el pas a l'oposat per la suma són continus. En virtud del corol·lari anterior, per a veure que $\mathbb{Z}_p$ és compacte és suficient veure que és un tancat de $\mathfrak{A}$. Considerem l'aplicació

$$\begin{array}{rccc} f_n: & \mathfrak{A} & \longrightarrow & A_n \\ & x & \longmapsto & \phi_{n+1}(\varepsilon_{n+1}(x)) - \varepsilon_n(x). \end{array}$$

Recordem que la topologia producte satisfà que la projecció ε_n és contínua per a cada $n \geq 1$. A més, les projeccions $\phi_{n+1} : A_{n+1} \to A_n$ són contínues ja que els anells A_{n+1} tenen la topologia discreta. Aplicant també que A_n és un anell topològic, deduïm que f_n és contínua per a cada n. Sigui $x = (x_n)_n \in \mathbb{Z}_p$, aleshores

$$\begin{aligned} f_n(x) = 0 &\iff \phi_{n+1}(\varepsilon_{n+1}(x)) - \varepsilon_n(x) = 0 \\ &\iff \phi_{n+1}(x_{n+1}) - x_n = 0 \\ &\iff \phi_{n+1}(x_{n+1}) = x_n. \end{aligned}$$

Per definició

$$\mathbb{Z}_p = \bigcap_{n\geq 1} f_n^{-1}\left(\{0\}\right),$$

per tant, $\mathbb{Z}_p$ és un tancat de $\mathfrak{A}$ i hereta la seva compacitat.

(b) Atès que $\mathfrak{A} = \prod A_n$ i que, per a cada $n \geq 1$, tot subconjunt de A_n n'és obert, $\mathfrak{A}$ admet la següent base d'oberts

$$\mathfrak{B} = \{U_1 \times \cdots \times U_n \times \cdots \subseteq \mathfrak{A} : U_i = A_i \text{ a.e. } i\}.$$

I.e., $U_i = A_i$, per a cada $i \in \mathbb{N} \setminus I$, amb $\#I < \infty$. Així,

$$\mathfrak{B}_0 = \{U \in \mathfrak{B} : 0 \in U\}$$

és una base d'oberts del 0.

Si considerem $\mathbb{Z}_p \subseteq \mathfrak{A}$ amb la topologia de subespai, aleshores

$$\mathfrak{B}' = \{\mathbb{Z}_p \cap U : U \in \mathfrak{B}\}$$

és una base d'oberts de $\mathbb{Z}_p$ i

$$\mathfrak{B}'_0 = \{U \in \mathfrak{B}' : 0 \in U\}$$

és una base d'oberts del 0 (a $\mathbb{Z}_p$).

Volem veure que $\{p^n\mathbb{Z}_p\}_{n\geq 1}$ i $\mathfrak{B}'_0$ són bases d'entorns de 0 equivalents. Sigui $k \geq 0$, notem que

$$\begin{aligned} p^k\mathbb{Z}_p &= \{x \in \mathbb{Z}_p : \varepsilon_n(x) = 0, \text{ per a cada } n \geq k\} \\ &= \left(\prod_{n=1}^{k}\{0\} \times \prod_{n\geq k+1} A_n\right) \cap \mathbb{Z}_p \in \mathfrak{B}'_0, \end{aligned}$$

així, $p^k\mathbb{Z}_p$ és un obert de $\mathbb{Z}_p$ i, per tant,

$$\{p^n\mathbb{Z}_p\}_n \subseteq \mathfrak{B}'_0.$$

Sigui $U' \in \mathfrak{B}'_0$, per definició existeix $U \in \mathfrak{B}_0$ tal que

$$U' = U \cap \mathbb{Z}_p$$

i

$$U = U_1 \times \cdots \times U_n \times \cdots,$$

amb $0 \in U_i$ i $U_i = A_i$ a.e. i. Sigui

$$i_0 := \max\{i : U_i \neq A_i\},$$

llavors

$$U' = \prod_{n=1}^{i_0} U_n \times \prod_{n\geq i_0+1} A_n$$

i

$$p^{i_0}\mathbb{Z}_p = \left(\prod_{n=1}^{i_0}\{0\} \times \prod_{n\geq i_0+1} A_n\right) \cap \mathbb{Z}_p$$
$$\subseteq \left(\prod_{n=1}^{i_0} U_n \times \prod_{n\geq i_0+1} A_n\right) \cap \mathbb{Z}_p.$$

Per tant, les bases són equivalents.

□

Proposició 1.4.4. (i) *L'aplicació*

$$\begin{array}{rccc} d_p: & \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & [0,+\infty) \\ & (x,y) & \longmapsto & d_p(x,y) \end{array}$$

definida per

$$d_p(x,y) = \begin{cases} \dfrac{1}{p^{v_p(x-y)}} & \text{si } x \neq y, \\ 0 & \text{si } x = y, \end{cases}$$

és una distància ultramètrica en $\mathbb{Z}_p$. És a dir, d_p és una distància que, a més, satisfà

$$d_p(x,y) \leq \max\left(d_p(x,z), d_p(z,y)\right), \quad \text{per a cada } x,\ y,\ z \in \mathbb{Z}_p.$$

(ii) *A l'espai mètric $(\mathbb{Z}_p, d_p)$, $\{p^n\mathbb{Z}_p\}_{n\geq 1}$ és una base d'oberts del 0.*

Corol·lari 1.4.5. *$\mathbb{Z}_p$ és un espai mètric complet; és a dir, tota successió de Cauchy convergeix.*

Demostració. Donat que la base d'entorns del 0 induïda per d_p és equivalent a la produïda com a subespai de $\mathfrak{A}$, i ja que d_p és invariant per translacions i $\mathbb{Z}_p$ és anell topològic, obtenim que les topologies induïdes coincideixen; per tant, $\mathbb{Z}_p$ és un anell mètric compacte, llavors complet. □

Observació 1.4.6. Aquest últim resultat demostra que la construcció per límit projectiu i la construcció per completació de distància ultramètrica de Hensel són equivalents.

1.5 Equacions p-àdiques

A fi de simplificar notacions, donats dos enters p-àdics $x = (x_n)_{n\geq 1}$, $y = (y_n)_{n\geq 1}$, escriurem

$$x \equiv y \pmod{p^n}$$

si

$$x_n = y_n.$$

Lema 1.5.1 (Hensel)**.** *Considerem un polinomi $f \in \mathbb{Z}_p[X]$ i f' el seu polinomi derivat. Siguin $x \in \mathbb{Z}_p$, n, $k \in \mathbb{Z}$ tals que*

$$0 \leq 2k < n, \quad f(x) \equiv 0 \pmod{p^n} \quad i \quad v_p(f'(x)) = k,$$

aleshores existeix $y \in \mathbb{Z}_p$ tal que

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

Demostració. Vegi's [11], Cap. II, §. 3, o bé [3].

□

Teorema 1.5.2. *Considerem un polinomi $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$. Si $x = (x_i) \in \mathbb{Z}_p$, n, k, $j \in \mathbb{Z}$ tals que $1 \leq j \leq m$, $0 \leq 2k < n$ amb*

$$f(x) \equiv 0 \pmod{p^n} \quad i \quad v_p(f'(x)) = k,$$

aleshores, existeix un enter p-àdic y tal que $y \equiv x \pmod{p})^{n-k}$. □

Capítol 2

Aritmètica de cossos de nombres

En aquest capítol veurem un resum de resultats bàsics en extensions algebraiques i aritmètica de cossos de nombres. Entre les demostracions que afegim, és interessant analitzar la de la factorització de primers enters en anells monògens.

Definició 2.0.3. Diem que un cos K és de nombres si $K|\mathbb{Q}$ és una extensió finita. Considerarem tots els cossos de nombres inclosos en una mateixa clausura algebraica $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.

Teorema 2.0.4 (Teorema de l'element primitiu)**.** *Donat un cos K de nombres, existeix un nombre algebraic $\theta \in \overline{\mathbb{Q}}$ tal que*

$$K = \mathbb{Q}(\theta).$$

□

2.1 Traça i norma

Definició 2.1.1. Donats un cos K de nombres, $[K : \mathbb{Q}] = n$, i $\mathcal{B} = \{u_1, \ldots, u_n\}$ una $\mathbb{Q}$-base de K, considerem, per a cada $\alpha \in K$, l'aplicació $\mathbb{Q}$-lineal

$$\begin{array}{rccc} \Phi_\alpha : & K & \longrightarrow & K \\ & x & \longmapsto & \alpha x. \end{array}$$

Si denotem per A_α la matriu associada a Φ_α com a aplicació $\mathbb{Q}$-lineal, definim

(i) La norma de α com

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \det(A_\alpha).$$

(ii) La traça de α com

$$\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \mathrm{Tr}(A_\alpha).$$

Observació 2.1.2. 1. Per a cada $\alpha, \beta \in K$,

$$\mathrm{N}_{K|\mathbb{Q}}(\alpha\beta) = \mathrm{N}_{K|\mathbb{Q}}(\alpha) \cdot \mathrm{N}_{K|\mathbb{Q}}(\beta).$$

2. Si $K|\mathbb{Q}$ és una extensió de grau n aleshores per a cada $a \in \mathbb{Q}$

$$\mathrm{N}_{K|\mathbb{Q}}(a) = a^n.$$

Proposició 2.1.3. *Siguin α un nombre algebraic i $p(x) = \sum_{i=0}^{m} a_i x^i$ el seu polinomi mònic ($a_m = 1$) irreductible sobre $\mathbb{Q}$. Aleshores $\mathrm{N}_{\mathbb{Q}(\alpha)|\mathbb{Q}}(\alpha) = (-1)^m a_0$.*

2.2 Immersions i conjugació

Definició 2.2.1. Diem que dos nombres algebraics θ_1 i θ_2 són conjugats sobre $\mathbb{Q}$ si tenen el mateix polinomi irreductible sobre $\mathbb{Q}$.

Observació 2.2.2. Sigui $\theta \in \overline{\mathbb{Q}}$. Ja que $\mathrm{char}(\overline{\mathbb{Q}}) = 0$, llavors

$$\#\{\gamma \in \overline{\mathbb{Q}} : \ \theta \text{ i } \gamma \text{ són conjugats}\} = [\mathbb{Q}(\theta) : \mathbb{Q}].$$

Teorema 2.2.3. *Sigui K un cos de nombres de grau n sobre $\mathbb{Q}$, aleshores*

(i) *Hi ha exactament n monomorfismes de cossos $\sigma : K \longrightarrow \overline{\mathbb{Q}}$.*

(ii) *Si θ és una element primitiu de K, $K = \mathbb{Q}(\theta)$, i $\theta = \theta_1, \ldots, \theta_n$ són els seus conjugats, aleshores per a cada conjugat θ_i de θ existeix un monomorfisme σ_i tal que*

$$\sigma_i(\theta) = \theta_i.$$

Concretament, $\mathbb{Q}(\theta) \overset{\sigma_i}{\simeq} \mathbb{Q}(\theta_i)$. □

Definició 2.2.4. Siguin K un cos de nombres i $\sigma : K \longrightarrow \overline{\mathbb{Q}}$ un monomorfisme de cossos. Direm que σ és una immersió real de K en $\overline{\mathbb{Q}}$ si $\sigma(K) \subseteq \mathbb{R}$, en cas contrari, direm que σ és una immersió complexa de K en $\overline{\mathbb{Q}}$. Denotem

$$r_1 := \#\{\sigma : K \longrightarrow \overline{\mathbb{Q}} \text{ monomorfisme: } \sigma(\mathbb{Q}(\theta)) \subseteq \mathbb{R}\}$$

i

$$r_2 := \frac{n - r_1}{2} \in \mathbb{N},$$

on $n = [K : \mathbb{Q}]$.

Observacions 2.2.5. Siguin K un cos de nombres, n el grau de l'extensió $K|\mathbb{Q}$ i θ un element primitiu de K.

(i) Donat un monomorfisme $\sigma : K \longrightarrow \overline{\mathbb{Q}}$, aleshores

$$\sigma_{|\mathbb{Q}} = \mathrm{Id}_{|\mathbb{Q}}.$$

(ii) Si $\theta_1 = \theta, \ldots, \theta_n$ són els conjugats de θ, aleshores

$$r_1 = \#(\{\theta_i\}_i \cap \mathbb{R}).$$

(iii) Si γ és un altre element primitiu de K i $\gamma_1 = \gamma, \ldots, \gamma_n$ són els conjugats de γ,

$$\{\sigma(\gamma) : \sigma \text{ és un monomorfisme de } K \text{ en } \overline{\mathbb{Q}}\} = \{\gamma_i\}_i.$$

Definició 2.2.6. Donada una $\mathbb{Q}$-base $\mathcal{B} = \{u_1, \ldots, u_n\}$ de K, definim el seu discriminant

$$\mathrm{disc}_{K|\mathbb{Q}}(u_1, \ldots, u_n) = \begin{vmatrix} \sigma_1(u_1) & \cdots & \sigma_1(u_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \cdots & \sigma_n(u_n) \end{vmatrix}^2.$$

2.3 Anell d'enters

Definició 2.3.1. Diem que un nombre algebraic $\alpha \in \overline{\mathbb{Q}}$ és enter algebraic si existeix un polinomi mònic de coeficients enters $P(X) \in \mathbb{Z}[X]$ tal que

$$P(\alpha) = 0.$$

Denotarem per $\overline{\mathbb{Z}}$ el conjunt dels enters algebraics .

Teorema 2.3.2. *Sigui K un cos de nombres, aleshores*

(a) $\mathbb{Z} \subseteq \overline{\mathbb{Z}} \cap K$.

(b) $\overline{\mathbb{Z}} \cap K$ *és un subanell de* K.

Denotarem $\overline{\mathbb{Z}} \cap K$ *per* $\mathcal{O}_K$ *i l'anomenarem l'anell dels enters (algebraics) de* K.

(c) *Si* $[K : \mathbb{Q}] = n$, *aleshores* $\mathcal{O}_K$ *és un* $\mathbb{Z}$*-mòdul lliure de rang* n. *És a dir, existeix una* $\mathbb{Q}$*-base* $\mathfrak{B}$ *de* K, $\mathfrak{B} = \{v_1, \ldots, v_n\}$, *tal que*

$$\mathcal{O}_K = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n.$$

Anomenarem base entera tota $\mathbb{Q}$*-base de* K *que satisfaci aquesta propietat.*

Observacions 2.3.3. (i) L'anell dels enters de $\mathbb{Q}$ és $\mathbb{Z}$.

(ii) El conjunt dels enters algebraics $\overline{\mathbb{Z}}$ és un subanell de $\overline{\mathbb{Q}}$.

Proposició 2.3.4. *El cos de fraccions de l'anell dels enters* $\mathcal{O}_K$ *d'un cos* K *de nombres és* K.

Demostració. Sigui θ un element primitiu de K, $K = \mathbb{Q}(\theta)$, i sigui

$$P(X) = \sum_{i=0}^{n} a_i X^i$$

el seu polinomi mònic irreductible de coeficients racionals amb

$$a_i = \frac{b_i}{c_i}, \quad b_i, c_i \in \mathbb{Z} \text{ per a cada } i \in \{0, \ldots n-1\},$$

considerem

$$m = \prod_{i=0}^{n-1} c_i,$$

$$\gamma = m\theta$$

i

$$Q(X) = \sum_{i=0}^{n} a_i m^{n-i} X^i.$$

Aleshores

$$\begin{aligned} Q(\gamma) =& \sum_{i=0}^{n} a_i m^{n-i} \gamma^i \\ =& \sum_{i=0}^{n} a_i m^{n-i} \theta^i m^i \\ =& \sum_{i=0}^{n} a_i m^{n-i+i} \theta^i \\ =& m^n \sum_{i=0}^{n} a_i \theta^i \\ =& m^n P(\theta) \\ =& 0. \end{aligned}$$

Atès que $Q(X) \in \mathbb{Z}[X]$ és mònic i que $m \in \mathbb{Z} \setminus \{0\}$, es té que $\gamma \in \mathcal{O}_K$ i $\mathbb{Q}(\theta) = \mathbb{Q}(\gamma)$, per tant, s'obté el resultat. □

Teorema 2.3.5. *Donat un cos K de nombres, aleshores $\mathcal{O}_K$ és un domini de Dedekind, és a dir,*

(a) *Tot ideal primer no nul de $\mathcal{O}_K$ és maximal.*

(b) *És noetherià.*

(c) *És enterament tancat.* □

Definició 2.3.6 (Discriminant d'un cos)**.** Donats un cos K de nombres i $\mathfrak{B} = \{v_1, \ldots, v_n\}$ una base entera, aleshores és defineix el seu discriminant

$$d(K) = \mathrm{disc}_{K|\mathbb{Q}}(v_1, \ldots, v_n).$$

Observació 2.3.7. Aquesta definició no depèn de la base entera escollida.

2.4 Ideals fraccionaris

Definició 2.4.1 (Ideal fraccionari)**.** Siguin $\mathcal{D}$ un domini d'integritat i K el seu cos de fraccions. Diem que un subconjunt no buit J de K és un ideal fraccionari de $\mathcal{D}$ si satisfà les propietats següents:

(i) $(J, +)$ és un subgrup additiu de K.

(ii) Si $a \in J$, $r \in \mathcal{D}$, llavors $ra \in J$.

(iii) Existeix $g \in \mathcal{D} \setminus \{0\}$ tal que $gJ \subseteq \mathcal{D}$.

Observacions 2.4.2. (a) Els ideals fraccionaris de $\mathcal{D}$ continguts en $\mathcal{D}$ són exactament els ideals (enters) de $\mathcal{D}$.

(b) Si J és un ideal fraccionari de $\mathcal{D}$, aleshores existeix un $g \in \mathcal{D} \setminus \{0\}$ tal que

$$J = \frac{1}{g} I,$$

per a un ideal enter I de $\mathcal{D}$.

(c) Si $\mathcal{D}$ és un anell noetherià, aleshores tot ideal fraccionari de $\mathcal{D}$ és finitament generat. En concret, donats dos ideals fraccionaris J_1 i J_2, aleshores $J_1 + J_2$ i $J_1 J_2$ són també ideals fraccionaris.

Teorema 2.4.3. *Si $\mathcal{D}$ és un domini de Dedekind, aleshores cada ideal enter, propi i no nul, de $\mathcal{D}$ és pot expressar de manera única, mòdul reordenacions, com a producte d'ideals enters primers.*

Corol·lari 2.4.4. *Sigui K un cos de nombres. Aleshores tot ideal propi de $\mathcal{O}_K$ es pot expressar de manera única, mòdul reordenacions, com a producte d'ideals primers de $\mathcal{O}_K$.*

Definició 2.4.5. Donats A i B ideals fraccionaris no nuls d'un domini de Dedekind $\mathcal{D}$, direm que A divideix B, $A \mid B$, si existeix un ideal enter C tal que $B = AC$.

Teorema 2.4.6. *Donats A i B ideals fraccionaris no nuls d'un domini de Dedekind $\mathcal{D}$, aleshores*

$$A \mid B \iff A \supseteq B.$$

Teorema 2.4.7. *El conjunt de tots els ideals fraccionaris (no nuls) d'un domini de Dedekind $\mathcal{D}$ té estructura de grup respecte de la multiplicació. L'element neutre és $\langle 1 \rangle = \mathcal{D}$.*

Definició 2.4.8. Denotarem per I el grup multiplicatiu dels ideals. fraccionaris de $\mathcal{D}$.
Denotarem per P el subgrup dels ideals fraccionaris principals de $\mathcal{D}$.
Denotarem per H el grup de classes d'ideals I/P.

2.5 Norma d'un ideal

Definició 2.5.1. Siguin K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters.

(i) Donat un ideal (enter) I de $\mathcal{O}_K$, definim la norma de I com

$$N(I) = \#(\mathcal{O}_K/I).$$

(ii) Donat un ideal fraccionari J de $\mathcal{O}_K$, siguin $g \in \mathcal{O}_K \setminus \{0\}$ i I ideal (enter) de $\mathcal{O}_K$ tals que

$$J = \frac{1}{g}I.$$

Definim la norma de J com

$$N(J) = \frac{N(I)}{N(\langle g \rangle)}$$

on $\langle g \rangle$ denota l'ideal generat per g, $g\mathcal{O}_K$.

Proposició 2.5.2. *(a) La norma d'un ideal enter és finita.*

(b) En les notacions de la definició anterior, la norma d'un ideal fraccionari J no depèn de l'elecció de I i g.

(c) Sigui $\gamma \in \mathcal{O}_K$, llavors

$$N(\langle \gamma \rangle) = |\mathrm{N}_{K|\mathbb{Q}}(\gamma)|.$$

□

Proposició 2.5.3. *Siguin I i J dos ideals fraccionaris de $\mathcal{O}_K$, aleshores*

$$N(IJ) = N(I)N(J).$$

□

Corol·lari 2.5.4. *Siguin I i J dos ideals enters de $\mathcal{O}_K$. Si $I \mid J$, aleshores $N(I) \mid N(J)$.* □

2.6 Grup de les unitats

Denotarem $\mathcal{O}_K^*$ el grup de les unitats de $\mathcal{O}_K$, és a dir, el grup dels elements invertibles de $\mathcal{O}_K$.

Teorema 2.6.1.

$$\mathcal{O}_K^* = \{x \in \mathcal{O}_K : \mathrm{N}_{K|\mathbb{Q}}(x) = \pm 1\}.$$

Teorema 2.6.2 (Dirichlet)**.** *Sigui K un cos de nombres amb r_1 immersions reals i $2r_2$ immersions complexes, aleshores*

$$\mathcal{O}_K \simeq \mathbb{Z}^{r_1+r_2-1} \times \mu,$$

on μ denota el grup de les arrels de la unitat que hi ha en K.

2.7 Ideals primers

Com ja sabem, $\mathcal{O}_K$ és un domini de Dedekind i, per tant, tot ideal primer és maximal. Vegem algunes propietats dels ideals primers d'un anell d'enters.

Proposició 2.7.1. *Sigui $\mathfrak{p}$ un ideal propi de $\mathcal{O}_K$, aleshores*

$$\{0\} \subsetneq \mathfrak{p} \cap \mathbb{Z}.$$

Demostració. $0 \in \mathcal{O}_K$ ja que $\mathfrak{p}$ és un ideal de $\mathcal{O}_K$. Vegem ara que existeix $n \in \mathbb{Z} \setminus \{0\}$ tal que $n \in \mathfrak{p}$. Prenguem $\theta \in \mathfrak{p} \setminus \{0\}$ i $K' = \mathbb{Q}(\theta) \subseteq K$. Si $K' = \mathbb{Q}$ ja hem acabat. Si $[K' : \mathbb{Q}] = r > 0$, aleshores els conjugats de θ, $\{\theta_1 = \theta, \ldots, \theta_r\}$, són també enters algebraics. A més, si $a_0 \in \mathbb{Z} \setminus \{0\}$ és el terme independent del polinomi mònic irreductible de θ, es té

$$N_{K'|\mathbb{Q}}(\theta) = (-1)^r a_0 = \theta_1 \cdots \theta_r.$$

Així tenim

$$\begin{cases} \theta_2 \cdots \theta_n = (-1)^r \dfrac{a_0}{\theta} \in \mathbb{Q}(\theta), \\ \theta_2 \cdots \theta_n \in \overline{\mathbb{Z}}, \end{cases}$$

per tant, $\theta_2 \cdots \theta_n \in \overline{\mathbb{Z}} \cap K' \subseteq \overline{\mathbb{Z}} \cap K$. Atès que $\mathfrak{p}$ és un ideal de $\mathcal{O}_K$, $a_0 = \theta(-1)^r(\theta_2 \cdots \theta_r) \in \mathfrak{p}$. □

Teorema 2.7.2. *Sigui $\mathfrak{p}$ un ideal primer (propi) de $\mathcal{O}_K$, aleshores existeix un únic primer $p \in \mathbb{Z}$ tal que $p \in \mathfrak{p}$. En concret, $\mathfrak{p} \mid \langle p \rangle$.*

Demostració. Vegem que $I = \mathfrak{p} \cap \mathbb{Z}$ és un ideal primer de $\mathbb{Z}$. Siguin $a, b \in I$, $m \in \mathbb{Z}$, aleshores

$$\begin{cases} a+b, ma \in \mathfrak{p}, \text{ ja que } \mathfrak{p} \text{ ideal de } \mathcal{O}_K \text{ i } \mathbb{Z} \subseteq \mathcal{O}_K, \\ a+b, ma \in \mathbb{Z}, \text{ ja que } a, b, m \in \mathbb{Z}, \end{cases}$$

Per tant, I és un ideal de $\mathbb{Z}$. Per veure la primeritat de I prenguem $m, n \in \mathbb{Z}$. Si $mn \in I$, aleshores $mn \in \mathfrak{p}$, però $\mathbb{Z} \subseteq \mathcal{O}_K$, llavors $m, n \in \mathcal{O}_K$ i $mn \in \mathfrak{p}$. Atès que $\mathfrak{p}$ és primer de $\mathcal{O}_K$, $m \in \mathfrak{p}$ o bé $n \in \mathfrak{p}$. Així $m \in I$ o bé $n \in I$.
En virtud de la proposició anterior, $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$; a més, els ideals primers (propis) de $\mathbb{Z}$ són de la forma $p\mathbb{Z}$ per a algun enter primer p. Així, existeix $p \in \mathbb{Z}$ tal que $I = p\mathbb{Z}$ i $p \in \mathfrak{p}$. Per tant, $p\mathcal{O}_K \subseteq \mathfrak{p}$ i $\mathfrak{p} \mid \langle p \rangle$.
Per veure la unicitat suposem que existeix un altre primer q tal que $q \in \mathfrak{p}$. Així,

$$p\mathbb{Z} + q\mathbb{Z} \subseteq \langle p, q \rangle \subseteq \mathfrak{p},$$

però $\mathrm{mcd}(p, q) = 1$ per tant,

$$\mathbb{Z} = p\mathbb{Z} + q\mathbb{Z} \subseteq \mathfrak{p}.$$

En concret, $1 \in \mathfrak{p}$ i $\langle 1 \rangle = \mathcal{O}_K \subseteq \mathfrak{p}$, que per hipòtesi no és possible. Així p és únic. □

Corol·lari 2.7.3. *Si $\mathfrak{p}$ és un ideal primer (propi) de $\mathcal{O}_K$, aleshores*

$$N(\mathfrak{p}) = p^s$$

per a algun primer p i per a algun s, $1 \leq s \leq [K : \mathbb{Q}]$.

Corol·lari 2.7.4. *Siguin p un enter primer, $\mathfrak{a}$ un ideal enter de $\mathcal{O}_K$ i*

$$\langle p \rangle = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$$

la descomposició en ideals primers de $p\mathcal{O}_K = \langle p \rangle$. Si

$$N(\mathfrak{a}) = p^s$$

per a algun enter $s \geq 1$, aleshores existeixen $k_i \geq 0$ tals que

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i^{k_i}$$

és la factorització en ideals primers de $\mathfrak{a}$.

Corol·lari 2.7.5. *Siguin I un ideal enter de $\mathcal{O}_K$ i $p \in \mathbb{Z}$ un enter primer. Si $N(I) = p$, aleshores I és un ideal primer.*

2.8 Finitud del nombre de classes. Fita de Minkowski

Definició 2.8.1 (Fita de Minkowski)**.** Siguin K un cos de nombres, $2r_2$ el nombre d'immersions complexes (veure (2.2.4)) i $d(K)$ el discriminant de K. La fita de Minkowski de K es denota per M_K i és donada per

$$M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d(K)|},$$

on $n = [K : \mathbb{Q}]$.

Teorema 2.8.2. *Siguin K un cos de nombres i $a \in H_K$ una classe, aleshores existeix un ideal enter $\mathfrak{a} \subseteq \mathcal{O}_K$ tal que*

$$N(\mathfrak{a}) \leq M_K$$

i

$$\overline{\mathfrak{a}} = a,$$

on $\overline{\mathfrak{a}}$ denota la classe de $\mathfrak{a}$ mòdul ideals principals i M_K denota la constant de Minkowski del cos K.

Corol·lari 2.8.3 (Minkowski)**.** *Donat un cos K de nombres, aleshores*

$$h_K < \infty,$$

on h_K denota l'ordre de I_K/P_K.

Observació 2.8.4. Les següents propietats són equivalents:

(a) $\mathcal{O}_K$ és un domini d'ideals principals.

(b) $h_K = 1$.

2.9 Factorització d'enters primers en anells monògens

Definició 2.9.1. Sigui $K|\mathbb{Q}$ una extensió de grau n, diem que $\mathcal{O}_K$ és monògen si existeix $\theta \in \mathcal{O}_K$ tal que

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1},$$

i $K = \mathbb{Q}(\theta)$.

Teorema 2.9.2. *Sigui $K = \mathbb{Q}(\theta)$ un cos de nombres de grau n, amb $\theta \in \mathcal{O}_K$ tal que*

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}.$$

Siguin $f(X) \in \mathbb{Z}[X]$ el polinomi mònic irreductible de θ i p un enter primer. Siguin $^-$ l'aplicació natural: $\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$ on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ i

$$\bar{f}(X) = g_1(X)^{e_1} \cdots g_r(X)^{e_r}, \quad e_i \geq 1,$$

la factorització en factors mònics irreductibles de $\bar{f}(X)$ en $\mathbb{F}_p[X]$. Per a cada $i \in \{1, 2, \ldots, r\}$ considerem $f_i(X) \in \mathbb{Z}[X]$ mònic tal que $\bar{f}_i(X) = g_i(X)$ i prenguem

$$P_i = \langle p, f_i(\theta) \rangle,$$

l'ideal de $\mathcal{O}_K$ generat per p i $f_i(\theta)$. Aleshores $P_1, \ldots, P_r$ són ideals primers diferents de $\mathcal{O}_K$ amb

$$\langle p \rangle = p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$$

i, a més, per a cada $i \in \{1, \ldots, r\}$,

$$N(P_i) = p^{\deg g_i}$$

on $\deg g_i$ denota el grau de g_i.

Demostració. Atès que $\theta \in \overline{\mathbb{Z}}$, és fàcil veure que $\mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1}$; en el capítol següent en veurem un exemple.

Sigui, per a cada $i \in \{1, \ldots, r\}$, θ_i una arrel de g_i en una extensió $\mathbb{F}_p[\theta_i]$ de $\mathbb{F}_p$. Considerem l'epimorfisme d'anells

$$\begin{array}{rccc} \nu_i : & \mathbb{Z}[\theta] & \longrightarrow & \mathbb{F}_p[\theta_i] \\ & h(\theta) & \longmapsto & \bar{h}(\theta_i). \end{array}$$

Aplicant el primer teorema d'isomorfia,

$$\mathbb{Z}[\theta]/\ker\nu_i \simeq \nu_i(\mathbb{Z}[\theta]) = \mathbb{F}_p[\theta_i],$$

però $\mathbb{F}_p[\theta_i]$ és un cos per tant, $\ker\nu_i$ és un ideal maximal de $\mathbb{Z}[\theta]$ i, per tant, és un ideal primer. Vegem que $\ker\nu_i = \langle p, f_i(\theta)\rangle$.
D'una banda,

$$\nu_i(p) = 0, \quad \nu_i(f_i(\theta)) = \bar{f}_i(\theta_i) = g_i(\theta_i) = 0,$$

per tant p i $f(\theta) \in \ker\nu_i$ i així,

$$\langle p, f(\theta)\rangle \subseteq \ker\nu_i.$$

D'altra banda, si $g(\theta) \in \ker\nu_i$, on $g(X) \in \mathbb{Z}[X]$, llavors

$$\bar{g}(\theta_i) = \nu_i(g(\theta)) = 0.$$

Recordem que hem pres θ_i una arrel del polinomi irreductible $g_i(X) \in \mathbb{F}_p[X]$; per tant,

$$g_i(X) \mid \bar{g}(X),$$

així que existeix $\bar{h}(X) \in \mathbb{F}_p[X]$ tal que

$$\bar{g}(X) = g_i(X)\bar{h}(X) = \bar{f}_i(X)\bar{h}(X).$$

És a dir, $(g - f_i h)(X) \in \mathbb{Z}[X]$ té els coeficients múltiples de p i, per tant,

$$\begin{aligned} g(\theta) &= (g(\theta) - f_i(\theta)h(\theta)) + f_i(\theta)h(\theta) \\ &\in \langle p\rangle + \langle f_i(\theta)\rangle \\ &= \langle p, f_i(\theta)\rangle, \end{aligned}$$

que demostra

$$\ker\nu_i \subseteq \langle p, f_i(\theta)\rangle.$$

Així hem demostrat que $P_i = \langle p, f(\theta)\rangle = \ker\nu_i$ és ideal primer de $\mathcal{O}_K$ per a cada $i \in \{1, \dots r\}$. Vegem ara que aquests ideals són diferents. Suposem que existeixen i, $j \in \{1, \dots r\}$ tals que $P_i = P_j$. Així,

$$f_j(\theta) \in P_i = \ker\nu_i,$$

per tant,

$$\begin{aligned} g_j(\theta_i) &= \bar{f}_j(\theta_i) \\ &= \nu_i(f_j(\theta)) \\ &= 0. \end{aligned}$$

És a dir, $g_i(X)$ i $g_j(X)$ tenen una arrel comuna, per tant, $i = j$.

Vegem que

$$\langle p \rangle = P^{e_1} \cdots P^{e_r}.$$

Abans, però, notem que donats ideals I, J_1, J_2 d'un anell $\mathcal{D}$, se satisfà que

$$(I + J_1)(I + J_2) \subseteq I + J_1 J_2,$$

i, inductivament, per a una família finita d'ideals $\{J_i\}_i$ de $\mathcal{D}$

$$\prod_i (I + J_i) \subseteq I + \prod_i J_i.$$

Així tenim que

$$\begin{aligned} P^{e_1} \cdots P^{e_r} &= \prod_{i=1}^{r} \langle p, f_i(\theta) \rangle^{e_i} \\ &= \prod_{i=1}^{r} (\langle p \rangle + \langle f_i(\theta) \rangle)^{e_i} \\ &\subseteq \langle p \rangle + \prod_{i=0}^{r} \langle f_i(\theta) \rangle^{e_i} \\ &= \langle p \rangle + \langle \prod_{i=0}^{r} f_i(\theta)^{e_i} \rangle. \end{aligned}$$

Per definició,

$$\begin{aligned} \bar{f}(X) &= \bar{f}_1(X)^{e_1} \cdots \bar{f}_r(X)^{e_r} \\ &= \overline{f_1^{e_1} \cdots f_r^{e_r}}(X), \end{aligned}$$

així, existeix $g(X) \in p\mathbb{Z}[X]$ tal que

$$f(X) = f_1(X)^{e_1} \cdots f_r(X)^{e_r} + g(X).$$

En concret,

$$f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r} = f(\theta) - g(\theta) = -g(\theta) \in p\mathbb{Z}[\theta] = p\mathcal{O}_K,$$

per tant,

$$f_1(\theta)^{e_1} \cdots f_r(\theta)^{e_r} \in p\mathcal{O}_K = \langle p \rangle$$

i

$$P_1^{e_1} \cdots P_r^{e_r} \subseteq \langle p \rangle.$$

Vegem l'altra inclusió.

$$P_1^{e_1} \cdots P_r^{e_r} \subseteq \langle p \rangle \iff \langle p \rangle \mid P_1^{e_1} \cdots P_r^{e_r}$$

per tant, existeix un ideal enter A de $\mathcal{O}_K$ tal que

$$A\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}.$$

Ja que $A\langle p \rangle$ és un ideal enter i tenim la seva descomposició en ideals primers P_i, existeix $k_i \in \{0, \ldots, e_i\}$ per a cada $i \in \{1, \ldots r\}$ tals que

$$\langle p \rangle = P_1^{k_1} \cdots P_r^{k_r}.$$

Recordem que

$$\mathcal{O}_K/P_i = \mathbb{Z}[\theta]/\ker \nu_i \simeq \nu_i(\mathbb{Z}[\theta]) = \mathbb{F}_p[\theta_i];$$

per tant,

$$\begin{aligned} N(P_i) &= \#(\mathcal{O}_K/P_i) \\ &= \#\mathbb{F}_p[\theta_i] \\ &= p^{\deg g_i}. \end{aligned}$$

Així,

$$\begin{aligned} p^n &= \mathrm{N}_{K|\mathbb{Q}}(p) \\ &= N(\langle p \rangle) \\ &= N(P_1^{k_1} \cdots P_r^{k_r}) \\ &= N(P_1^{k_1}) \cdots N(P_r^{k_r}) \\ &= N(P_1)^{k_1} \cdots N(P_r)^{k_r} \\ &= p^{k_1 \deg g_1} \cdots p^{k_r \deg g_r} \\ &= p^{k_1 \deg g_1 + \cdots + k_r \deg g_r}. \end{aligned}$$

És a dir,

$$n = k_1 \deg g_1 + \cdots + k_r \deg g_r,$$

però

$$n = \deg f = e_1 \deg g_1 + \cdots + e_r \deg g_r,$$

per tant, $k_i = e_i$ per a cada $i \in \{1, \ldots, r\}$. □

Capítol 3

Estudi local de l'equació de Selmer

En aquesta secció veurem l'existència de solucions no trivials a $\mathbb{Q}_p$ de l'equació

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

per a tot primer p. Això és, per a cada p primer i per a cada natural $n \geq 1$, existeixen $x, y, z \in \mathbb{Z}/p^n\mathbb{Z}$, $(x, y, z) \neq (0, 0, 0)$ tals que

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod{p^n}.$$

Gran part d'aquesta secció es fonamenta en uns resultats bàsics de teoria de grups i en el lema de Hensel (1.5.2).

3.1 Cubs de $(\mathbb{Z}/p\mathbb{Z})^*$

Proposició 3.1.1. *Siguin $p \neq 3$ un nombre primer i*

$$(\mathbb{Z}/p\mathbb{Z})^* := \mathbb{Z}/p\mathbb{Z} \setminus \{0\},$$
$$(\mathbb{Z}/p\mathbb{Z})^{*3} := \left\{x^3 : x \in (\mathbb{Z}/p\mathbb{Z})^*\right\}.$$

Aleshores

(i) $\left((\mathbb{Z}/p\mathbb{Z})^{*3}, \cdot\right)$ *és un subgrup normal de* $\left((\mathbb{Z}/p\mathbb{Z})^*, \cdot\right)$.

(ii)
$$[(\mathbb{Z}/p\mathbb{Z})^* : (\mathbb{Z}/p\mathbb{Z})^{*3}] = \begin{cases} 3 & si\ p \equiv 1 \pmod 3, \\ 1 & si\ p \equiv 2 \pmod 3. \end{cases}$$

Demostració. (i) $(\mathbb{Z}/p\mathbb{Z})^{*3} \subseteq (\mathbb{Z}/p\mathbb{Z})^*$ i $(\mathbb{Z}/p\mathbb{Z})^*$ és abelià; per tant, només cal veure que $(\mathbb{Z}/p\mathbb{Z})^{*3}$ és un subgrup. En efecte, si $x, y \in (\mathbb{Z}/p\mathbb{Z})^{*3}$ llavors existeixen $z, t \in (\mathbb{Z}/p\mathbb{Z})^*$ tals que $x = z^3$ i $y = t^3$. Llavors $xy^{-1} = z^3t^{-3} = (zt^{-1})^3 \in (\mathbb{Z}/p\mathbb{Z})^{*3}$.

(ii) Com ja sabem, $(\mathbb{Z}/p\mathbb{Z})^*$ és un grup finit cíclic de $p-1$ elements. Sigui γ un generador de $(\mathbb{Z}/p\mathbb{Z})^*$, aleshores γ^3 és un generador de $(\mathbb{Z}/p\mathbb{Z})^{*3}$,

$$(\gamma^3) = (\mathbb{Z}/p\mathbb{Z})^{*3}.$$

En efecte, donat un cub x, $x \in (\mathbb{Z}/p\mathbb{Z})^{*3}$, prenem $z \in (\mathbb{Z}/p\mathbb{Z})^*$ tal que $z^3 = x$ i prenem $n \in \mathbb{Z}$ tal que $\gamma^n = z$, aleshores $x = z^3 = \gamma^{3n} = (\gamma^3)^n$. Recordem que

$$o(\gamma^3) = \frac{o(\gamma)}{\mathrm{mcd}(o(\gamma), 3)}.$$

Per tant,

$$\begin{aligned}\left[(\mathbb{Z}/p\mathbb{Z})^* : (\mathbb{Z}/p\mathbb{Z})^{*3}\right] &= \frac{\#(\mathbb{Z}/p\mathbb{Z})^*}{\#(\mathbb{Z}/p\mathbb{Z})^{*3}} \\ &= \frac{o(\gamma)}{o(\gamma^3)} \\ &= \mathrm{mcd}(o(\gamma), 3) \\ &= \mathrm{mcd}(p-1, 3) \in \{1, 3\}.\end{aligned}$$

d'on s'obté el resultat.

□

3.2 Solucions locals de l'equació de Selmer

Lema 3.2.1. *Siguin $p \neq 3$ un nombre primer i $\alpha = (\alpha_n)_n$ un enter p-àdic, si $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ té una arrel cúbica no nul·la a $\mathbb{Z}/p\mathbb{Z}$, aleshores α té una arrel cúbica a $\mathbb{Z}_p$.*

Demostració. Utilitzarem (1.5.2) per a demostrar-ho.

Prenguem $f(X) = X^3 - \alpha \in \mathbb{Z}_p[X]$ i $0 \neq \beta \in \mathbb{Z}/p\mathbb{Z}$ l'arrel cúbica de α_1. Sigui $x = (x_n)_n$ un enter p-àdic qualsevol tal que $x_1 = \beta$, aleshores

$$f(x) \equiv \beta^3 - \alpha \equiv 0 \pmod{p},$$

i

$$k = v_p(f'(x)) = v_p(3x^2) \overset{p\neq 3}{=} v_p(x^2) = 2v_p(x) \overset{x_1\neq 0}{=} 0.$$

Aleshores $2k = 0 < 1$; per tant existeix una arrel de $f(X)$ a $\mathbb{Z}_p$. □

Teorema 3.2.2. *L'equació de Selmer* $3X^3 + 4Y^3 + 5Z^3 = 0$ *té solucions no trivials en* $\mathbb{Z}_p$ *per a tot* p *primer i en* $\mathbb{R}$.

Demostració. És clar que sobre $\mathbb{R}$

$$\left(\sqrt[3]{5}, 0, -\sqrt[3]{3}\right)$$

és una solució no trivial.

Cal remarcar que, per a cada primer p, 3, 4 i 5 denoten respectivament $(3 + p^s\mathbb{Z})_{s\geq 1}$, $(4 + p^s\mathbb{Z})_{s\geq 1}$ i $(5 + p^s\mathbb{Z})_{s\geq 1}$, els enters p-àdics que resulten d'injectar $\mathbb{Z}$ en $\mathbb{Z}_p$.

Estudiem per casos.

1. $p = 3$.

   Sigui (x, y, z) un element de $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Suposem que $x = 0$, i $z = -1$. Així,

   $$3 \cdot 0 + 4y^3 + 5(-1)^3 = 0 \iff 4y^3 - 5 = 0.$$

   Considerem el polinomi $f(Y) := 4Y^3 - 5$, $f \in \mathbb{Z}_3[Y]$. Notem que si trobem una arrel $y \in \mathbb{Z}_3$ de f, aleshores $(0, y, -1)$ és una solució no trivial de $3X^3 + 4Y^3 + 5Z^3 = 0$ en $\mathbb{Z}_3$. Per a fer-ho utilitzarem el lema de Hensel.

   Fem $n = 1$. Considerem $f_1(Y) = Y^3 + 1$ la reducció de f mòdul 3. Notem que $y = -1$ n'és arrel però no podem aplicar el lema de Hensel ja que

   $$2 \cdot v_3(f_1'(-1)) = 2 \cdot v_3(4 \cdot 3(-1)^2) = 2 \cdot v_3(12) = 2 \not< 1.$$

   Fem $n = 2$. Considerem $f_2(Y) = 4Y^3 - 5$ la reducció de f mòdul 9. Notem que $y = -1$ n'és arrel però, com abans, no podem aplicar el lema de Hensel ja que

   $$2 \cdot v_3(f_2'(-1)) = 2 \not< 2.$$

Fem $n = 3$. Considerem $f_3(Y) = 4Y^3 - 5$ la reducció de f mòdul 27. Notem que $y = 2$ n'és arrel, en efecte $4 \cdot 8 - 5 = 27$. A més,

$$2 \cdot v_3(f_3'(2)) = 2 \cdot v_3(4 \cdot 3 \cdot 2^2) = 2 \cdot v_3(48) = 2 < 3.$$

Ara podem aplicar (1.5.1) i pujar la solució $y = 2$ de $4Y^3 - 5 = 0$ en $\mathbb{Z}/27\mathbb{Z}$ a una solució en $\mathbb{Z}_3$. Per tant, existeix un enter 3-àdic y tal que $(0, y, -1)$ és solució 3-àdica de l'equació de Selmer.

2. $p = 5$.

   Sigui (x, y, z) un element de $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Suposem que $x = 1$ i $z = 0$. Així,

   $$3 + 4y^3 = 0 \Longleftrightarrow y^3 = -3 \cdot 4^{-1},$$

   on 4^{-1} denota l'invers 5-àdic de 4.

   Notem que $5 \nmid 4$, així $4 \in \mathbb{Z}_5^*$, $-3 \cdot 4^{-1} \in \mathbb{Z}_5$ i $f(Y) := Y^3 - 3 \cdot 4^{-1} \in \mathbb{Z}_5[Y]$. Seguint el mateix guió que pel cas $p = 3$, si trobem y una arrel cúbica 5-àdica de $-3 \cdot 4^{-1}$, llavors $(1, y, 0)$ serà solució 5-àdica de l'equació.

   Fem $n = 1$. Considerem $f_1(Y) = Y^3 - 3$ la reducció de f mòdul 5. En efecte, l'invers de 4 és -1 mòdul 5,

   $$-1 \cdot 4 \equiv 1 \pmod 5$$

   i

   $$(-3)4^{-1} \equiv (-3)(-1) \equiv 3 \pmod 5.$$

   Notem que $y = 2$ n'és arrel no nul·la. Podem aplicar el lema (3.2.1) i pujar la solució $y = 2$ de $4Y^3 + 3 = 0$ en $\mathbb{Z}/5\mathbb{Z}$ a una solució en $\mathbb{Z}_5$. Per tant, existeix un enter 5-àdic y tal que $(1, y, 0)$ és solució 5-àdica de l'equació de Selmer.

3. $3 + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^{*3}$, $p \neq 3, 5$.

   D'aquestes hipòtesis deduïm que

   - $p \nmid 3$ per tant, $3 \in \mathbb{Z}_p^*$.
   - Existeix $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$ tal que $\alpha^3 = 3 + p\mathbb{Z}$.
   - Si α^{-1} denota l'invers de α en $\mathbb{Z}/p\mathbb{Z}$, $3^{-1} \in \mathbb{Z}_p$ denota l'invers p-àdic de 3 i $\varepsilon_1(3^{-1}) \in \mathbb{Z}/p\mathbb{Z}$ la seva projecció mòdul p, aleshores $(\alpha^{-1})^3 = \varepsilon_1(3^{-1})$.

Ara, sigui (x, y, z) un element de $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. Suposem que $y = 1$ i $z = -1$. Així,

$$3x^3 + 4y^3 + 5z^3 = 0 \iff x^3 - 3^{-1} = 0.$$

Com ja hem vist, $X^3 - \varepsilon_1(3^{-1}) = 0$ té solució $\alpha^{-1} \neq 0$ en $\mathbb{Z}/p\mathbb{Z}$. Podem aplicar el lema (3.2.1) i pujar la solució $x = \alpha^{-1}$ de $X^3 - \varepsilon_1(3^{-1}) = 0$ en $\mathbb{Z}/p\mathbb{Z}$ a una solució de $X^3 - 3^{-1} = 0$ en $\mathbb{Z}_p$. Per tant, existeix un enter p-àdic x tal que $(x, 1, -1)$ és solució p-àdica de l'equació de Selmer.

4. $3 + p\mathbb{Z} \notin (\mathbb{Z}/p\mathbb{Z})^{*3}$, $p \neq 3, 5$.

   Definim el grup quocient

   $$G := \frac{(\mathbb{Z}/p\mathbb{Z})^*}{(\mathbb{Z}/p\mathbb{Z})^{*3}};$$

   efectivament té sentit parlar del quocient ja que $(\mathbb{Z}/p\mathbb{Z})^*$ és un grup commutatiu.

   Notem que $\#G = 3$. En efecte, pel lema (3.1.1) sabem que

   $$\#G = [(\mathbb{Z}/p\mathbb{Z})^* : (\mathbb{Z}/p\mathbb{Z})^{*3}] \in \{1, 3\};$$

   a més, $(\mathbb{Z}/p\mathbb{Z})^{*3}$ és un subgrup propi de $(\mathbb{Z}/p\mathbb{Z})^*$ ja que $3 + p\mathbb{Z} \notin (\mathbb{Z}/p\mathbb{Z})^{*3}$, 3 és invertible no cub mòdul p; per tant

   $$\#G \neq 1 \quad \Longrightarrow \#G = 3,$$

   i, a més, G és cíclic.

   Per una banda, notem que $(1+p\mathbb{Z})^3 = 1+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^{*3}$, per tant $1+p\mathbb{Z}$ és un representant del neutre de G. D'altra banda, $3+p\mathbb{Z} \notin (\mathbb{Z}/p\mathbb{Z})^{*3}$; per tant, $3 + p\mathbb{Z}$ és representant d'un element no trivial de G, un grup cíclic d'ordre primer, per tant

   $$G = \langle \overline{3 + p\mathbb{Z}} \rangle,$$

   on $\overline{3 + p\mathbb{Z}}$ denota la classe de $3+p\mathbb{Z}$ mòdul cubs. Atès que $(\overline{3 + p\mathbb{Z}})^2 = \overline{(3 + p\mathbb{Z})^2} = \overline{9 + p\mathbb{Z}}$, es té que

   $$G = \{\mathrm{Id_G} = \overline{1 + p\mathbb{Z}}, \overline{3 + p\mathbb{Z}}, \overline{9 + p\mathbb{Z}}\}.$$

En termes de congruències això és, per a tot enter m no múltiple de p, existeix $k \in \mathbb{Z}$ tal que

$$m \equiv k^3 \pmod{p},$$

o bé

$$m \equiv 3k^3 \pmod{p},$$

o bé

$$m \equiv 9k^3 \pmod{p}.$$

Ara, separem per casos segons la classe de G a la qual pertany $5 = (5 + p^s\mathbb{Z})_{s\geq 1} \in (\mathbb{Z}/p\mathbb{Z})^*$.

(a) Si $\overline{5} = \overline{1 + p\mathbb{Z}} = \mathrm{Id}_G$, aleshores 5 és un cub mòdul p i pel lema (3.1.1) existeix $y \in \mathbb{Z}_p$ tal que

$$y^3 = 5.$$

Així, prenent $(-y, y, -1) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ tenim que

$$\begin{aligned} 3(-y)^3 + 4y^3 + 5(-1)^3 &= -3y^3 + 4y^3 - 5 \\ &= y^3 - 5 \\ &= 5 - 5 = 0; \end{aligned}$$

per tant, és una solució no trivial de l'equació de Selmer.

(b) Si $\overline{5} = \overline{3 + p\mathbb{Z}}$, aleshores existeix un enter t no múltiple de p tal que

$$5 \equiv 3t^3 \pmod{p}.$$

Per tant, $5/3$ és un cub mòdul p. Pel lema (3.1.1) existeix $x \in \mathbb{Z}_p$ tal que

$$x^3 = 5/3.$$

Així, prenent $(x, 0, -1) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ tenim que

$$\begin{aligned} 3x^3 + 4 \cdot 0 + 5(-1)^3 &= 3x^3 - 5 \\ &\overset{x^3=5/3}{=} 0. \end{aligned}$$

per tant, és solució no trivial de l'equació de Selmer.

(c) Si $\overline{5} = \overline{9 + p\mathbb{Z}}$, aleshores existeix un enter t no múltiple de p tal que

$$5 \equiv 9t^3 \pmod{p},$$

d'on s'obté que

$$5 \cdot 3 = 15 \equiv 27t^3 = (3t)^3 \pmod{p};$$

per tant, 15 és un cub mòdul p. Podem afirmar que existeix $w \in \mathbb{Z}_p$ tal que

$$w^3 = 15.$$

Si prenem $(3w, 5, -7) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, aleshores

$$\begin{aligned} 3(3w)^3 + 4 \cdot 5^3 - 5 \cdot 7^3 &= 81w^3 + 5 \cdot 100 + 5 \cdot 343 \\ &= 5 \cdot 243 + 5 \cdot 100 - 5 \cdot 343 \\ &= 5 \cdot (243 + 100 - 343) = 0. \end{aligned}$$

□

3.3 Els cubs de $\mathbb{Q}_p^*$

Mentre estudiàvem l'existència de solucions p-àdiques de l'equació de Selmer hem vist que trobar cubs a $(\mathbb{Z}/p\mathbb{Z})^*$ ens permet, en alguns casos, assegurar l'existència de cubs a $\mathbb{Q}_p^*$; a més, hem vist aplicacions directes del lema de Hensel. En aquesta secció generalitzarem aquests càlculs i estudiarem els cubs de $\mathbb{Q}_p^*$. Recordem que tot element $x \in \mathbb{Q}_p^*$ es pot expressar de manera única com $x = p^s u$ amb $s \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$. Podem deduir el següent resultat

Proposició 3.3.1. *$\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p^*$, en un isomorfisme de grups.*

□

Així, per veure l'estructura de $\mathbb{Q}^*$ és necessari estudiar-ne la de $\mathbb{Z}_p^*$.

3.3.1 Estructura de $\mathbb{Z}_p^*$

En aquesta secció denotarem U_n el subgrup de $\mathbb{Q}_p^*$ definit per

$$U_n = \{1 + p^n x : x \in \mathbb{Z}_p\}.$$

Proposició 3.3.2. *Si $p \neq 2$, $(U_1, \cdot) \simeq (\mathbb{Z}_p, +)$.*
Si $p = 2$, $U_1 = \{-1, 1\} \times U_2$ i $(U_2, \cdot) \simeq (\mathbb{Z}_2, +)$.

Vegeu [3].

Proposició 3.3.3. *Per a cada $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$ existeix un únic $x = (x_n)_n \in \mathbb{Z}_p$ tal que*

$$x_1 = \alpha \quad i \quad x^{p-1} = 1.$$

Demostració. Considerem el polinomi $f(X) = X^{p-1} - 1 \in \mathbb{Q}_p[X]$. Atès que $\mathbb{Q}_p$ és un cos, l'equació

$$f(X) = 0$$

té com a molt $p - 1$ solucions en $\mathbb{Q}_p$.
Prenguem $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$; pel petit teorema de Fermat, tenim que

$$\alpha^{p-1} = 1.$$

Sigui $x = (x_n)_n \in \mathbb{Z}_p$ qualsevol tal que $x_1 = \alpha \neq 0$, aleshores $x \in \mathbb{Z}_p^*$ i

$$\begin{aligned} k = v_p(f'(x)) &= v_p((p-1)x^{p-2}) \\ &= v_p(p-1) + (p-2)v_p(x) \\ &= 0, \end{aligned}$$

amb $0 \leq 2k < 1$; aplicant el lema (1.5.1) tenim que existeix $y \in \mathbb{Z}_p$ tal que

$$y \equiv x \pmod{p}$$

i

$$f(y) = 0.$$

Així, per a cada $\alpha \in (\mathbb{Z}/p\mathbb{Z})$ hi ha al menys un zero y de f tal que $y_1 = \alpha$. Això són $p - 1$ zeros diferents de f i, per tant, obtenim la unicitat. □

Corol·lari 3.3.4. *Existeix un subgrup V de $(\mathbb{Q}_p^*, \cdot)$ tal que*

$$(V, \cdot) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +) \simeq (\mathbb{F}_p^*, \cdot).$$

Demostració. Només cal notar que el conjunt de les arrels $(p-1)$-èsimes de la unitat, es a dir els zeros de

$$f(X) = X^{p-1} - 1,$$

és un grup multiplicatiu cíclic de $p - 1$ elements. □

Proposició 3.3.5. *Si $p \neq 2$ aleshores*

$$\mathbb{Z}_p^* \simeq V \times U_1 \simeq \mathbb{F}_p^* \times \mathbb{Z}_p.$$

Si $p = 2$ aleshores

$$\mathbb{Z}_2^* \simeq V \times U_1 \simeq \{-1, 1\} \times \mathbb{Z}_2.$$

Demostració. Notem que $U_1 = \{x = (x_n)_n \in \mathbb{Z}_p : x_1 = 1\}$. Per tant, és suficient veure que

$$\mathbb{Z}_p^* \simeq V \times \{x = (x_n)_n \in \mathbb{Z}_p : x_1 = 1\}.$$

En efecte, sigui $x = (x_n)_n \in \mathbb{Z}_p^*$, aleshores $p \nmid x$ per tant $x_1 \neq 0$. Així, existeix un $y \in \mathbb{Z}_p^*$ tal que

$$y_1 = x_1 \quad \text{i} \quad y^{p-1} = 1.$$

Sigui $z = xy^{-1} = (z_n)_n \in \mathbb{Z}_p^*$, aleshores

$$z_1 = x_1 y_1^{-1} = 1,$$

així

$$y \in V, \quad z \in U_1, \quad x = yz.$$

□

Corol·lari 3.3.6. *Si $p \equiv 1 \pmod 3$,*

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Si $p \equiv 2 \pmod 3$,

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z}.$$

Si $p = 3$,

$$\mathbb{Q}_3^*/\mathbb{Q}_3^{*3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Demostració. Separem per casos.

- $p \neq 2, 3$.
  Com ja hem vist,

  $$\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p^* \simeq \mathbb{Z} \times \mathbb{F}_p^* \times \mathbb{Z}_p.$$

  Per tant,

  $$\mathbb{Q}_p^{*3} \simeq 3\mathbb{Z} \times \mathbb{F}_p^{*3} \times 3\mathbb{Z}_p$$

i

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*3} \times \mathbb{Z}_p/3\mathbb{Z}_p.$$

Notem que $3 \in \mathbb{Z}_p^*$ per tant $3\mathbb{Z}_p = \mathbb{Z}_p$.
Si $p \equiv 1 \pmod 3$ aleshores hem vist en el lema (3.2.1) que

$$\#(\mathbb{F}_p^*/\mathbb{F}_p^{*3}) = 3,$$

per tant

$$\mathbb{F}_p^*/\mathbb{F}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z}$$

i

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Si $p \equiv 2 \pmod 3$ aleshores hem vist en el lema (3.2.1) que

$$\#(\mathbb{F}_p^*/\mathbb{F}_p^{*3}) = 1,$$

per tant

$$\mathbb{F}_p^* = \mathbb{F}_p^{*3}$$

i

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z}.$$

- $p = 2$.
  Com ja hem vist

  $$\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{Z}_2^* \simeq \mathbb{Z} \times \{-1, 1\} \times \mathbb{Z}_2.$$

  Per tant,

  $$\mathbb{Q}_2^{*3} \simeq 3\mathbb{Z} \times \{-1, 1\}^3 \times 3\mathbb{Z}_2.$$

  Atès que

  $$\{-1, 1\}^3 = \{-1, 1\} \quad \text{i} \quad 3 \in \mathbb{Z}_2^*,$$

  llavors

  $$\{-1, 1\}^3 \times 3\mathbb{Z}_2 = \{-1, 1\} \times \mathbb{Z}_2$$

  i

  $$\mathbb{Q}_2^*/\mathbb{Q}_2^{*3} \simeq \mathbb{Z}/3\mathbb{Z}.$$

- $p = 3$.
  Notem que $\mathbb{F}_3^{*3} = \mathbb{F}_3^*$; a més per la proposició (1.1.8),

  $$\mathbb{Z}_p/p\mathbb{Z}_p \equiv \mathbb{Z}/p\mathbb{Z}.$$

  Així,

  $$\mathbb{Q}_p^*/\mathbb{Q}_p^{*3} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

□

Corol·lari 3.3.7. (a) *Si $p \equiv 1 \pmod 3$, i $x = p^s u \in \mathbb{Q}_p^*$ amb $s \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$, aleshores*

$$x \in \mathbb{Q}_p^{*3}$$

si, i només si,

$$s \in 3\mathbb{Z} \quad i \quad x_1 \in (\mathbb{Z}/p\mathbb{Z})^{*3}.$$

(b) *Si $p \equiv 2 \pmod 3$, i $x = p^s u \in \mathbb{Q}_p^*$ amb $s \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$, aleshores*

$$x \in \mathbb{Q}_p^{*3}$$

si, i només si,

$$s \in 3\mathbb{Z}.$$

(c) *Si $p = 3$, i $x = p^s u \in \mathbb{Q}_p^*$ amb $s \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$, aleshores*

$$x \in \mathbb{Q}_p^{*3}$$

si, i només si,

$$s \in 3\mathbb{Z} \quad i \quad u \equiv \begin{cases} \pm 1 \\ \pm 8 \\ \pm 10 \end{cases} \pmod{27}$$

Demostració. El resultat per al cas $p \neq 3$ es dedueix fàcilment dels isomorfismes de cossos anteriors.
Per al cas $p = 3$ és suficient veure quan una unitat és un cub. Sigui $u = (u_n)_n \in \mathbb{Z}_3^*$, si u és un cub aleshores u_n és cub per a cada $n \geq 1$. Notem que els cubs de $\mathbb{Z}/27\mathbb{Z}$ són $\{\pm 1, \pm 8, \pm 10\}$ d'on obtenim una implicació.

Per a l'altra implicació, sigui $u = (u_n)_n \in \mathbb{Z}_3^*$ amb $u_3 \not\equiv 0 \pmod{27}$ cub, és fàcil veure que existeix $n \in \mathbb{Z}$ tal que

$$u_3 \equiv n \pmod{27}.$$

Aplicant el lema de Hensel en $f(X) = X^3 - n$ s'obté el resultat ja que $2 \cdot v_3(3\alpha^2) = 2 < 3$, on $\alpha^3 \equiv u \pmod{27}$. □

Capítol 4

Estudi global de l'equació de Selmer

En el capítol anterior hem vist que l'equació de Selmer té una solució no trivial a $\mathbb{Z}/p^n\mathbb{Z}$ per a tot primer p i per a tot natural n. Ara veurem que això no s'estén al cas global sobre $\mathbb{Q}$. Suposem que existeix $(x, y, z) \in \mathbb{Q}^3$ tal que

$$3x^3 + 4y^3 + 5z^3 = 0. \tag{4.0.1}$$

Multiplicant l'equació per 2 obtenim

$$6x^3 + 8y^3 + 10z^3 = (2y)^3 + 6x^3 - 10(-z)^3 = 0.$$

Així, trobar solucions racionals de (4.0.1) és equivalent a trobar-ne de

$$X^3 + 6Y^3 = 10Z^3. \tag{4.0.2}$$

Observacions 4.0.8. Sigui $(x, y, z) \in \mathbb{Q}^3$ una solució de (4.0.2).

(i) Netejant denominadors podem suposar que x, y i z són enters.

(ii) És clar que $x = y = z = 0$ n'és solució. De fet, si un és nul, aleshores els altres també ho són.

En efecte, si $x = 0$, $6y^3 = 10z^3 \Leftrightarrow 3y^3 = 5z^3$. Si $yz \neq 0$ existeixen $r, s \geq 0$ i m, n enters, $5 \nmid m, n$ tals que

$$y = m5^r$$
$$z = n5^s$$

Així, $3m^3 5^{3r} = n^3 5^{3s+1}$ que, mitjançant el teorema fonamental de l'aritmètica, ens porta a contradicció.

Pels casos $y = 0$ i $z = 0$ els raonaments són anàlegs.

(iii) Si algun primer p divideix dos dels x, y, z llavors divideix el tercer ja que 6 i 10 són lliures de cubs. Així, per a cada solució de (4.0.2) sobre els enters podem trobar-ne una altra amb x, y, z coprimers dos a dos.

Podem deduir que

$$\begin{aligned} x^3 &\equiv 0 && \pmod 2, \\ x^3 &\equiv 10z^3 \equiv z^3 && \pmod 3, \\ x^3 + y^3 &\equiv x^3 + 6y^3 \equiv 0 && \pmod 5. \end{aligned}$$

Supososant coprimaritat dos a dos i tenint en compte les congruències anteriors, obtenim que

(a) x és parell i y i z són senars.

(b) x i z no són múltiples de 3.

(c) x i y no són múltiples de 5.

(iv) Sigui $\alpha = \sqrt[3]{6} \in \mathbb{R}$, si dividim $x^3 + 6y^3$ per $x + \alpha y$ obtenim que

$$(x + \alpha y)(x^2 - \alpha xy + \alpha^2 y^2) = 10z^3.$$

4.1 El cos cúbic $\mathbb{Q}(\sqrt[3]{6})$

Recordem que el nostre objectiu és demostrar que $3X^3 + 4Y^3 + 5Z^3 = 0$ només té com a solució racional $x = y = z = 0$. Gràcies a les observacions que acabem de fer podem concloure que el nostre problema es redueix a demostrar que $X^3 + 6Y^3 = 10Z^3$ només té solució entera $x = y = z = 0$. Per estudiar aquesta equació prendrem $\alpha = \sqrt[3]{6}$ i considerarem l'extensió de cossos $K|\mathbb{Q}$ on $K = \mathbb{Q}(\alpha)$ i considerarem el seu anell d'enters $\mathcal{O}_K$. En aquesta secció farem una anàlisi concreta de K i la seva aritmètica.

4.1.1 Immersions

Proposició 4.1.1. *L'extensió* $K|\mathbb{Q}$ *és de grau* 3 *i les seves immersions en la clausura algebraica són*

$$\begin{array}{rccccc} \sigma_i: & K & \longrightarrow & \mathbb{Q}(\alpha\rho^{i-1}) & & \\ & \alpha & \longmapsto & \alpha\rho^{i-1} & & \\ & a & \longmapsto & a, & a \in \mathbb{Q}, & \end{array}$$

on ρ *és una arrel cúbica primitiva de la unitat i* $0 \leq i \leq 3$*. A més,*

$$r_1 = r_2 = 1.$$

Demostració. Notem que $P(X) = X^3 - 6$ és un polinomi irreductible en $\mathbb{Q}[X]$ ja que és 3-Eisenstein, a més, $P(\alpha) = 0$; per tant, $[K : \mathbb{Q}] = 3$. Si ρ és una arrel cúbica primitiva de la unitat, aleshores

$$P(X) = (X - \alpha)(X - \alpha\rho)(X - \alpha\rho^2).$$

És a dir, α, $\alpha\rho$ i $\alpha\rho^2$ són els conjugats de α i pel teorema (2.2.3)

$$\begin{array}{rccc} \sigma_i: & K & \longrightarrow & \overline{\mathbb{Q}} \\ & \alpha & \longmapsto & \alpha\rho^{i-1} \end{array}$$

defineix un monomorfisme.
Tenim $\{\alpha, \alpha\rho, \alpha\rho^2\} \cap \mathbb{R} = \{\alpha\}$, per tant $r_1 = 1$ i $r_2 = (3-1)/2 = 1$. □

Observació 4.1.2. Notem que $\mathbb{Q}(\alpha)|\mathbb{Q}$ no és una extensió normal.

4.1.2 Norma

Calculem la norma dels elements de K.

Proposició 4.1.3. *Sigui* $a + b\alpha + c\alpha^2 \in K$*, amb* $a, b, c \in \mathbb{Q}$*, aleshores*

$$\mathrm{N}_{K|\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 6b^3 + 36c^3 - 18abc.$$

Demostració. Sigui $\beta = a + b\alpha + c\alpha^2$, considerem l'aplicació $\mathbb{Q}$-lineal

$$\begin{array}{rccc} \Phi_\beta: & K & \longrightarrow & K \\ & x & \longmapsto & \beta x. \end{array}$$

Donat que $K = \mathbb{Q}(\alpha)$ i que $\mathfrak{B} = \{1, \alpha, \alpha^2\}$ n'és base, aleshores

$$\begin{aligned}
&\Phi_\beta(1) = \beta = a + b\alpha + c\alpha^2 = (a, b, c)_{\mathfrak{B}},\\
&\Phi_\beta(\alpha) = \beta\alpha = a\alpha + b\alpha^2 + c\alpha^3 = 6c + a\alpha + b\alpha^2 = (6c, a, b)_{\mathfrak{B}},\\
&\Phi_\beta(\alpha^2) = \beta\alpha^2 = 6b + 6c\alpha + a\alpha^2 = (6b, 6c, a)_{\mathfrak{B}}.
\end{aligned}$$

Per tant, la matriu associada a Φ_β en base $\mathfrak{B}$ és

$$A_\beta = \begin{pmatrix} a & 6c & 6b \\ b & a & 6c \\ c & b & a \end{pmatrix}$$

i

$$\begin{aligned}
\mathrm{N}_{K|\mathbb{Q}}(\beta) &= \det(A_\beta)\\
&= a^3 + 6b^3 + 36c^3 - 6abc - 6abc - 6abc\\
&= a^3 + 6b^3 + 36c^3 - 18abc.
\end{aligned}$$

□

D'aquest resultat deduïm una fórmula que ens serà força útil.

Corol·lari 4.1.4. *Per a cada $a, b \in \mathbb{Q}$,*

$$\mathrm{N}_{K|\mathbb{Q}}(a + b\alpha) = a^3 + 6b^3.$$

4.1.3 Anell d'enters de $\mathbb{Q}(\sqrt[3]{6})$

Proposició 4.1.5. *La $\mathbb{Q}$-base $\{1, \alpha, \alpha^2\}$ és una base entera de K. És a dir,*

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2.$$

Demostració. Si $\mathbb{Z}[\alpha]$ denota el menor anell que conté $\mathbb{Z}$ i α, observem que

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2.$$

D'una banda, és clar que $\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \subseteq \mathbb{Z}[\alpha]$. D'altra banda, considerem

$$x = \sum_{i=0}^{t} a_i \alpha^i \in \mathbb{Z}[\alpha], \quad a_i \in \mathbb{Z}, t \in \mathbb{N}.$$

Substituint α^3 per 6 obtenim

$$\begin{aligned} x &= a_0 + a_1\alpha + a_2\alpha^2 + \sum_{i=3}^{n} 6a_i\alpha^{i-3} \\ &= a_0 + a_1\alpha + a_2\alpha^2 + 6\sum_{i=0}^{n-3} a_{i+3}\alpha^i \\ &= a_0 + 6a_3 + (a_1 + 6a_4)\alpha + (a_2 + 6a_5)\alpha^2 + 6\sum_{i=3}^{n-3} a_{i+3}\alpha^i. \end{aligned}$$

Repetint aquest procés recursivament obtenim que existeixen enters b_0, b_1, b_2 tals que $x = b_0 + b_1\alpha + b_2\alpha^2$. Vegem ara que $\mathbb{Z}[\alpha] = \mathcal{O}_K$.
$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$.
En efecte, $\alpha \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$ i $\mathbb{Z} \subseteq \mathcal{O}_K$, per tant $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$.
$\mathcal{O}_K \subseteq \mathbb{Z}[\alpha]$.
Prenguem $\beta \in \mathcal{O}_K$. Ja que $\mathcal{O}_K \subseteq \mathbb{Q}(\alpha)$, existeixen $x_1, x_2, x_3 \in \mathbb{Q}$ tals que

$$\beta = x_1 + x_2\alpha + x_3\alpha^2.$$

Prenguem els conjugats de β

$$\begin{cases} \beta = x_1 + x_2\alpha + x_3\alpha^2, \\ \beta' := \sigma_2(\beta) = x_1 + x_2\alpha\rho + x_3\alpha^2\rho^2, \\ \beta'' := \sigma_3(\beta) = x_1 + x_2\alpha\rho^2 + x_3\alpha^2\rho, \end{cases}$$

on $\{\sigma_i\}$ són les immersions de K en la clausura algebraica i ρ és una arrel cúbica primitiva de la unitat. Per tant, $1 + \rho + \rho^2 = 0$ i tenim

$$\begin{aligned} \beta + \beta' + \beta'' &= 3x_1 + x_2(1 + \rho + \rho^2) + x_3(1 + \rho^2 + \rho) \\ &= 3x_1, \\ \alpha^2(\beta + \rho^2\beta' + \rho\beta'') &= x_1\alpha^2(1 + \rho^2 + \rho) + 3x_2\alpha^3 + x_3\alpha^4(1 + \rho + \rho^2) \\ &= 18x_2, \\ \alpha(\beta + \rho\beta' + \rho^2\beta'') &= x_1\alpha(1 + \rho + \rho^2) + x_2\alpha^2(1 + \rho^2 + \rho^4) + 3x_3\alpha^4 \\ &= 18x_3. \end{aligned}$$

Ja que $\beta \in \mathcal{O}_K$, tenim que $\beta, \beta', \beta'' \in \overline{\mathbb{Z}}$; ja que $\alpha \in \mathcal{O}_K$, tenim que $\alpha, \alpha^2 \in \overline{\mathbb{Z}}$; ja que $p(X) = X^2 + X + 1$ és el polinomi anul·lador de ρ, tenim que $\rho, \rho^2 \in \overline{\mathbb{Z}}$. Així

$$\beta + \beta' + \beta'', \quad \alpha^2(\beta + \rho^2\beta' + \rho\beta''), \quad \alpha(\beta + \rho\beta' + \rho^2\beta'') \in \overline{\mathbb{Z}}$$

per tant

$$3x_1, \quad 18x_2, \quad 18x_3 \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Fixem

$$y_i = 18x_i \in \mathbb{Z},\ i = 1,\ 2,\ 3,$$

així,

$$18\beta = y_1 + y_2\alpha + y_3\alpha^2. \tag{4.1.1}$$

Abans de seguir, notem el següent resultat. Sigui $n \in \mathbb{Z}$, si $\alpha \mid n$ en $\mathcal{O}_K$, aleshores $6 \mid n$ en $\mathbb{Z}$. En efecte, per hipòtesi existeix $\omega \in \mathcal{O}_K$ tal que $n = \alpha\omega$. Per tant, $n^3 = \alpha^3\omega^3 = 6\omega^3$. Ara $\omega^3 = n^3/6 \in \mathbb{Q}$ i $\omega \in \mathcal{O}_K \subseteq \overline{\mathbb{Z}}$, per tant $\omega^3 \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Així, $2 \mid n^3$ i $3 \mid n^3$ en $\mathbb{Z}$. Però 2 i 3 són primers, per tant $2 \mid n$ i $3 \mid n$, és a dir $6 \mid n$.
Notem també que $\alpha \mid 6$ en $\mathcal{O}_K$ ja que $6 = \alpha^3$. Utilitzant aquests resultats a (4.1.1) veiem que $\alpha \mid y_1$ per tant $6 \mid y_1$. Llavors $\alpha^2 \mid y_2\alpha$ per tant $\alpha \mid y_2$ i $6 \mid y_2$. Per acabar, $\alpha^3 \mid y_3\alpha^2$, per tant $\alpha \mid y_3$ i $6 \mid y_3$.
Per tant, existeixen $z_1,\ z_2,\ z_3 \in \mathbb{Z}$ tals que

$$y_i = 6z_i, \quad i \in \{1,\ 2,\ 3\}$$

i, també,

$$3x_i = z_i, \quad i \in \{1,\ 2,\ 3\}.$$

Si $z_2 = z_3 = 0$ llavors $3\beta = 3x_1 = z_1$ per tant $\beta = z_1/3 \in \mathbb{Q}$. Però $\beta \in \mathcal{O}_K \subseteq \overline{\mathbb{Z}}$ per tant, $\beta = x_1 \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Així, $\beta \in \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$.
Si, en canvi, $(z_2, z_3) \neq (0, 0)$ aleshores $\beta \notin \mathbb{Q}$. Com ja sabem,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 3.$$

Per tant, $[\mathbb{Q}(\beta) : \mathbb{Q}] \in \{1, 3\}$ però $\beta \notin \mathbb{Q}$ així, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. D'aquesta manera, el polinomi mínim de β sobre $\mathbb{Q}$ té grau 3. Atès que $\beta \in \mathcal{O}_K$, existeixen $a,\ b,\ c \in \mathbb{Z}$ tals que

$$P(X) = X^3 + aX^2 + bX + c$$

és el polinomi mònic irreductible de β de coeficients enters. A més, $\beta,\ \beta',\ \beta''$ són les arrels de $P(X)$ ja que són els conjugats de β. Així,

$$P(X) = (X - \beta)(X - \beta')(X - \beta'')$$

i

$$c = -\beta\beta'\beta''.$$

En virtud de les proposicions (2.1.3) i (4.1.3) tenim que

$$\begin{aligned}(-1)^3 c =& \mathrm{N}_{K|\mathbb{Q}}(\beta)\\ =&(x_1^3+6x_2^3+36x_3^3-18x_1x_2x_3)\\ =&\frac{1}{27}(z_1^3+6z_2^3+36z_3^3-18z_1z_2z_3).\end{aligned}$$

Ja que c, z_1, z_2, z_3 són enters,

$$z_1^3+6z_2^3+36z_3^3-18z_1z_2z_3\equiv 0 \pmod{27}$$

d'on deduïm que

$$z_1^3\equiv 0 \pmod 3,$$

per tant, $3 \mid z_1$; a més,

$$6z_2^3\equiv 0 \pmod 9,$$

per tant, $3 \mid z_2$; finalment,

$$36z_3^3\equiv 0 \pmod{27},$$

per tant, $3 \mid z_3$. Així, $x_i = z_i/3 \in \mathbb{Z}$ per a cada $i \in \{1,2,3\}$; per tant, $\beta \in \mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\alpha^2$. □

Corol·lari 4.1.6. *El discriminant de K és $d(K)=-2^2 3^5$.*

Demostració. Com acabem de veure, $\{1,\alpha,\alpha^2\}$ és una base entera de $\mathbb{Q}(\alpha)$. Per definició,

$$\begin{aligned}d(K) &= \mathrm{disc}_{K|\mathbb{Q}}(1,\alpha,\alpha^2)\\ &= \begin{vmatrix}\sigma_1(1) & \sigma_1(\alpha) & \sigma_1(\alpha^2)\\ \sigma_2(1) & \sigma_2(\alpha) & \sigma_2(\alpha^2)\\ \sigma_3(1) & \sigma_3(\alpha) & \sigma_3(\alpha^2)\end{vmatrix}^2\\ &= \begin{vmatrix}1 & \alpha & \alpha^2\\ 1 & \alpha\rho & \alpha^2\rho^2\\ 1 & \alpha\rho^2 & \alpha^2\rho^4\end{vmatrix}^2\\ &= \alpha^6\begin{vmatrix}1 & 1 & 1\\ 1 & \rho & \rho^2\\ 1 & \rho^2 & \rho\end{vmatrix}^2\\ &= 6^2(3\rho^2-3\rho)^2\\ &= 2^2 3^4(\rho^4-2\rho^3+\rho^2)\\ &= -2^2 3^5.\end{aligned}$$

□

Corol·lari 4.1.7. *L'anell d'enters del cos $K = \mathbb{Q}(\sqrt[3]{6})$ és monògen.*

Notació 4.1.8. Donat un ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$, escriurem $\mathfrak{p}_{p^f}$ quan $\mathfrak{p} \cap \mathbb{Z} = (p)$ i f sigui el seu grau residual; és a dir $\#\mathcal{O}_K/\mathfrak{p} = p^f$. Notem que amb el mateix p i el mateix f tindrem, en general, ideals diferents.

4.1.4 Unitats de l'anell d'enters

Proposició 4.1.9. *Si $K = \mathbb{Q}(\sqrt[3]{6})$, es té que*

$$\mathcal{O}_K^* \simeq \mathbb{Z} \times \{-1, 1\}.$$

Demostració. Com ja hem vist, $r_1 = r_2 = 1$. Utilitzant el teorema (2.6.2) només cal veure que el conjunt μ de les arrels de la unitat en K té dos elements. Ja que $\alpha = \sqrt[3]{6} \in \mathbb{R}$, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, així les úniques arrels de la unitat són reals i iguals a 1 i -1. □

Proposició 4.1.10. *El grup quocient $\mathcal{O}_K^*/\mathcal{O}_K^{*3}$ té ordre tres i*

$$(1 - 6\alpha + 3\alpha^2)^k, \quad k \in \{0, 1, 2\},$$

en són representants.

Demostració. En virtud de la proposició anterior, és clar que

$$\begin{aligned} \mathcal{O}_K^*/\mathcal{O}_K^{*3} &\simeq \mathbb{Z}/3\mathbb{Z} \times \{-1, 1\}/\{-1, 1\}^3 \\ &\simeq \mathbb{Z}/3\mathbb{Z}. \end{aligned}$$

Així $\mathcal{O}_K^*/\mathcal{O}_K^{*3}$ és cíclic d'ordre tres.
Vegem que $u := 1 - 6\alpha + 3\alpha^2 \in \mathcal{O}_K^*$.
En efecte,

$$\begin{aligned} \mathrm{N}_{K|\mathbb{Q}}(1 - 6\alpha + 3\alpha^2) &= 1^3 + 6 \cdot (-6)^3 + 36 \cdot 3^3 - 18 \cdot (-6) \cdot 3 \\ &= 1 - 2^4 \cdot 3^4 + 2^2 \cdot 3^5 + 2^2 \cdot 3^4 \\ &= 1 + 2^2 \cdot 3^4 \cdot (3 - 2^2 + 1) \\ &= 1. \end{aligned}$$

Queda veure que $u \notin \mathcal{O}_K^{*3}$. Considerem $\mathfrak{p}_7 = \langle 1 + \alpha \rangle$. Notem que

$$\begin{aligned} \#(\mathcal{O}_K/\mathfrak{p}_7) &= N(\mathfrak{p}_7) \\ &= \mathrm{N}_{K|\mathbb{Q}}(1 + \alpha) \\ &= 1^3 + 6 \cdot 1^3 \\ &= 7. \end{aligned}$$

Atès que 7 és enter primer, $\mathfrak{p}_7$ és un ideal primer. Considerem el morfisme d'anells definit per

$$\begin{array}{rccc} \phi: & \mathcal{O}_K & \longrightarrow & \mathbb{Z}/7\mathbb{Z} \\ & \alpha & \longmapsto & -\overline{1} \\ & a & \longmapsto & \overline{a}, \quad a \in \mathbb{Z}. \end{array}$$

on $\overline{a}$ denota la classe de a mòdul 7. És fàcil veure que

$$\mathrm{Im}(\phi) = \mathbb{Z}/7\mathbb{Z}$$

i

$$\mathfrak{p}_7 \subseteq \ker(\phi).$$

A més, $\mathfrak{p}_7$ és maximal però $1 \notin \ker(\phi)$ per tant, $\ker(\phi) \neq \mathcal{O}_K$ i obtenim

$$\ker(\phi) = \langle \alpha + 1 \rangle = \mathfrak{p}_7.$$

Concretament,

$$\phi(\mathcal{O}_K^*) \subseteq (\mathbb{Z}/7\mathbb{Z})^*$$

i

$$\phi(\mathcal{O}_K^{*3}) \subseteq (\mathbb{Z}/7\mathbb{Z})^{*3} = \{\overline{1}, -\overline{1}\}.$$

Però

$$\begin{aligned} \phi(u) &= \overline{1} - \overline{6} \cdot (-\overline{1}) + \overline{3}(-\overline{1})^2 \\ &= \overline{3} \notin \{\overline{1}, -\overline{1}\}, \end{aligned}$$

així

$$u \notin \mathcal{O}_K^{*3},$$

i, per tant, $\{1, u, u^2\}$ són representants de les classes de $\mathcal{O}_K^*/\mathcal{O}_K^{*3}$. □

4.1.5 Factoritzacions d'alguns ideals

En aquest apartat veurem factoritzacions en ideals primers d'alguns ideals principals, necessaris per a veure la inexistència de solucions racionals de l'equació de Selmer.

Proposició 4.1.11. *Siguin* $K = \mathbb{Q}(\sqrt[3]{6})$, $\alpha^3 = 6$.

$$\begin{aligned} 2\mathcal{O}_K &= \mathfrak{p}_2^3, \\ 3\mathcal{O}_K &= \mathfrak{p}_3^3, \\ 5\mathcal{O}_K &= \mathfrak{p}_5\mathfrak{p}_{5^2}, \\ \alpha\mathcal{O}_K &= \mathfrak{p}_2\mathfrak{p}_3, \\ 7\mathcal{O}_K &= \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7'', \\ 10\mathcal{O}_K &= \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{5^2}, \end{aligned}$$

són les factoritzacions en ideals primers on

$$\begin{aligned} \mathfrak{p}_2 &= \langle \alpha - 2 \rangle, \\ \mathfrak{p}_3 &= \langle \alpha^2 + 2\alpha + 3 \rangle, \\ \mathfrak{p}_5 &= \langle \alpha - 1 \rangle, \\ \mathfrak{p}_{5^2} &= \langle \alpha^2 + \alpha + 1 \rangle, \\ \mathfrak{p}_7 &= \langle \alpha + 1 \rangle, \\ \mathfrak{p}_7' &= \langle 2\alpha^2 + 4\alpha + 7 \rangle, \\ \mathfrak{p}_7'' &= \langle 4\alpha^2 + 7\alpha + 13 \rangle. \end{aligned}$$

Així, $\mathfrak{p}_2$, $\mathfrak{p}_3$ *i* $\mathfrak{p}_5$, *són els únics ideals (enters) de* $\mathcal{O}_K$ *que tenen norma* 2, 3 *i* 5, *respectivament. A més,* $\mathfrak{p}_7$, $\mathfrak{p}_7'$ *i* $\mathfrak{p}_7''$ *són els únics ideals (enters) de norma* 7.

Demostració. Com ja sabem, el polinomi irreductible de α és $f(X) = X^3 - 6$. Utilitzarem el teorema (2.9.2).

- $2\mathcal{O}_K$.

  $$X^3 - 6 \equiv X^3 \pmod 2.$$

  Per tant,

  $$\mathfrak{p}_2 := \langle 2, \alpha \rangle$$

  té norma 2 i

  $$2\mathcal{O}_K = \mathfrak{p}_2^3.$$

  L'ideal $\mathfrak{p}_2$ és l'únic de norma 2. En efecte, sigui $\mathfrak{a}$ un ideal enter qualsevol tal que $N(\mathfrak{a}) = 2$, aleshores, pel corol·lari (2.7.4), existeix r tal que

  $$\mathfrak{a} = \mathfrak{p}_2^r.$$

Per tant,

$$2 = N(\mathfrak{a}) = N(\mathfrak{p}_2)^r = 2^r$$

i

$$\mathfrak{a} = \mathfrak{p}_2.$$

Atès que

$$\begin{aligned} N(\langle \alpha - 2 \rangle) &= |\mathrm{N}_{K|\mathbb{Q}}(\alpha - 2)| \\ &= |-2^3 + 6| \\ &= 2, \end{aligned}$$

$\mathfrak{p}_2 = \langle \alpha - 2 \rangle$.

- $3\mathcal{O}_K$.

$$X^3 - 6 \equiv X^3 \pmod 3.$$

Per tant,

$$\mathfrak{p}_3 = \langle 3, \alpha \rangle$$

té norma 3 i

$$3\mathcal{O}_K = \mathfrak{p}_3^3.$$

En concret $\mathfrak{p}_3$ és un ideal primer de norma 3. Fent un raonament anàleg al cas $2\mathcal{O}_K$ tenim que $\mathfrak{p}_3$ és l'únic ideal de norma 3. A més,

$$\begin{aligned} \mathrm{N}_{K|\mathbb{Q}}(\alpha^2 + 2\alpha + 3) &= 3^3 + 6 \cdot 2^3 + 36 - 18 \cdot 3 \cdot 2 \\ &= 3(9 + 16 + 12 - 36) \\ &= 3. \end{aligned}$$

Per tant, $\mathfrak{p}_3 = \langle \alpha^2 + 2\alpha + 3 \rangle$.

- $5\mathcal{O}_K$.

$$X^3 - 6 \equiv X^3 - 1 \equiv (X - 1)(X^2 + X + 1) \pmod 5.$$

Per tant,

$$\begin{aligned} \mathfrak{p}_5 &= \langle 5, \alpha - 1 \rangle, \\ \mathfrak{p}_{5^2} &= \langle 5, \alpha^2 + \alpha + 1 \rangle. \end{aligned}$$

En concret, $\mathfrak{p}_5$ és un ideal de norma 5. Atès que

$$(\alpha - 1)(\alpha^2 + \alpha + 1) = 5,$$

llavors

$$\begin{cases} 5 & \in \langle \alpha - 1 \rangle, \\ 5 & \in \langle \alpha^2 + \alpha + 1 \rangle, \end{cases}$$

i

$$\begin{cases} \mathfrak{p}_5 = \langle \alpha - 1 \rangle, \\ \mathfrak{p}_{5^2} = \langle \alpha^2 + \alpha + 1 \rangle. \end{cases}$$

Per veure l'unicitat de $\mathfrak{p}_5$, és fàcil veure que tot ideal $\mathfrak{a}$ de norma 5 ha de dividir $5\mathcal{O}_K$. Però l'únic ideal divisor de $5\mathcal{O}_K$ de norma 5 és $\mathfrak{p}_5$.

- $\alpha\mathcal{O}_K$.
  En efecte
  $$\begin{aligned} \mathfrak{p}_2\mathfrak{p}_3 &= \langle \alpha - 2 \rangle \langle \alpha^2 + 2\alpha + 3 \rangle \\ &= \langle (\alpha - 2)(\alpha^2 + 2\alpha + 3) \rangle \\ &= \langle \alpha^3 + 2\alpha^2 + 3\alpha - 2\alpha^2 - 4\alpha - 6 \rangle \\ &= \langle -\alpha \rangle \\ &= \langle \alpha \rangle. \end{aligned}$$

- $7\mathcal{O}_K$.
  $$\begin{aligned} X^3 - 6 \equiv X^3 + 1 &\equiv (X+1)(X^2 - X + 1) \\ &\equiv (X+1)(X+2)(X+4) \pmod 7. \end{aligned}$$

  Així,
  $$\langle 7 \rangle = \mathfrak{p}_7 \mathfrak{p}_7' \mathfrak{p}_7''.$$

  on
  $$\begin{aligned} \mathfrak{p}_7 &= \langle 7, \alpha + 1 \rangle, \\ \mathfrak{p}_7' &= \langle 7, \alpha + 2 \rangle, \\ \mathfrak{p}_7'' &= \langle 7, \alpha + 4 \rangle, \end{aligned}$$

  En concret, $\mathfrak{p}_7$, $\mathfrak{p}_7'$ i $\mathfrak{p}_7''$ són ideals de norma 7. Notem que

  $$\begin{cases} \mathrm{N}_{K|\mathbb{Q}}(\alpha + 1) & = 7, \\ \mathrm{N}_{K|\mathbb{Q}}(\alpha + 2) & = 14, \\ \mathrm{N}_{K|\mathbb{Q}}(\alpha + 4) & = 70. \end{cases}$$

  Observem que

  $$\mathrm{N}_{K|\mathbb{Q}} \left(\frac{\alpha + 2}{\alpha - 2} \right) = \frac{\mathrm{N}_{K|\mathbb{Q}}(\alpha + 2)}{\mathrm{N}_{K|\mathbb{Q}}(\alpha - 2)} = -7$$

i

$$\mathrm{N}_{K|\mathbb{Q}}\left(\frac{\alpha+4}{(\alpha-2)(\alpha-1)}\right)=\frac{\mathrm{N}_{K|\mathbb{Q}}(\alpha+4)}{\mathrm{N}_{K|\mathbb{Q}}(\alpha-2)\cdot\mathrm{N}_{K|\mathbb{Q}}(\alpha-1)}=-7.$$

A més,

$$\frac{\alpha+2}{\alpha-2}=-2\alpha^2-4\alpha-7\in\mathcal{O}_K$$

i

$$\frac{\alpha+4}{(\alpha-2)(\alpha-1)}=-4\alpha^2-7\alpha-13\in\mathcal{O}_K.$$

En concret,

$$\langle 7,\alpha+2\rangle=\langle 2\alpha^2+4\alpha+7\rangle$$

i

$$\langle 7,\alpha+4\rangle=\langle 4\alpha^2+7\alpha+13\rangle.$$

Per a veure la unicitat, tot ideal de norma 7 ha de dividir $7\mathcal{O}_K=\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$, per tant ha de ser un d'aquests tres.

- $10\mathcal{O}_K$
  Notem que $10\mathcal{O}_K=2\mathcal{O}_K5\mathcal{O}_K$, per tant
  $$10\mathcal{O}_K=\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{5^2}.$$

□

4.1.6 Càlcul del nombre de classes

Proposició 4.1.12. *$\mathcal{O}_K$ és un domini d'ideals principals quan $K=\mathbb{Q}(\sqrt[3]{6})$.*

Demostració. Com ha hem vist, K té una parella d'immersions complexes, és a dir, $r_2=1$. A més, $d(K)=-2^2\cdot 3^5$. Per tant, la constant de Minkowski del cos K és

$$\begin{aligned}M_K&=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{d(K)|}\\&=\left(\frac{4}{\pi}\right)\frac{3!}{3^3}\sqrt{2^2\cdot 3^5}\\&\approx 8,82.\end{aligned}$$

Per tant, tot element del grup de classes H_K té un representant enter de norma menor que 9. Sigui $\mathfrak{a}$ un ideal enter de norma $N(\mathfrak{a})<9$. Separem per casos:

- $N(\mathfrak{a}) = 2, 3, 5, 7$.
  Com ja hem vist a la proposició (4.1.11), els ideals de norma 2, 3, 5 són únics i són principals:

$$\begin{aligned}\mathfrak{p}_2 &= \langle \alpha - 2 \rangle,\\ \mathfrak{p}_3 &= \langle \alpha^2 + 2\alpha + 3 \rangle,\\ \mathfrak{p}_5 &= \langle \alpha - 1 \rangle.\end{aligned}$$

  Per al cas $N(\mathfrak{a}) = 7$, també hem vist que només existeixen tres ideals de norma 7 a més, són principals:

$$\begin{aligned}\mathfrak{p}_7 &= \langle \alpha + 1 \rangle,\\ \mathfrak{p}_7' &= \langle 2\alpha^2 + 4\alpha + 7 \rangle,\\ \mathfrak{p}_7'' &= \langle 4\alpha^2 + +7\alpha + 13 \rangle.\end{aligned}$$

- $N(\mathfrak{a}) = 4$. Sigui $\mathfrak{a}$ un ideal enter de norma 4, ja que $2\mathcal{O}_K = \mathfrak{p}_2^3$ tenim pel corol·lari (2.7.4) que existeix $r \in \mathbb{Z}$ tal que

$$\mathfrak{a} = \mathfrak{p}_2^r$$

  Però

$$4 = N(\mathfrak{a}) = N(\mathfrak{p}_2)^r = 2^r,$$

  per tant

$$\begin{aligned}\mathfrak{a} &= \mathfrak{p}_2^2\\ &= \langle \alpha - 2 \rangle^2\\ &= \langle (\alpha - 2)^2 \rangle\\ &= \langle \alpha^2 - 4\alpha + 4 \rangle,\end{aligned}$$

  que és principal.

- $N(\mathfrak{a}) = 8$.
  Anàlogament al cas anterior tenim que existeix r tal que

$$\mathfrak{a} = \mathfrak{p}_2^3$$

  i

$$8 = 2^3 = 2^r,$$

  per tant

$$\begin{aligned}\mathfrak{a} &= \mathfrak{p}_2^3\\ &= 2\mathcal{O}_K,\end{aligned}$$

  que és principal.

- $N(\mathfrak{a}) = 6$.
  Considerem
  $$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{q}_i^{e_i}$$
  la factorització de $\mathfrak{a}$ en ideals principals. Així
  $$\begin{aligned} 6 &= N(\mathfrak{a}) \\ &= N\left(\prod_{i=1}^{n} \mathfrak{q}_i^{e_i}\right) \\ &= \prod_{i=1}^{n} N(\mathfrak{q}_i)^{e_i}. \end{aligned}$$
  Així, per a cada $1 \leq i \leq n$,
  $$\begin{cases} N(\mathfrak{q}_i) \mid 2, \text{ o bé,} \\ N(\mathfrak{q}_i) \mid 3. \end{cases}$$
  Per tant, existeixen enters r i s tals que
  $$\mathfrak{a} = \mathfrak{p}_2^r \mathfrak{p}_3^s.$$
  Tanmateix, $N(\mathfrak{a}) = 6$ per tant $r = s = 1$ i
  $$\begin{aligned} \mathfrak{a} &= \mathfrak{p}_2\mathfrak{p}_3 \\ &= \alpha\mathcal{O}_K \\ &= \langle\alpha\rangle, \end{aligned}$$
  que és principal.

Per tant, $h_K = 1$, és a dir $\mathcal{O}_K$ és un domini d'ideals principals. □

Proposició 4.1.13. *Siguin* $x, y, z \in \mathbb{Z}$ *coprimers dos a dos tals que*

$$\begin{aligned} &xyz \neq 0, \\ &x \text{ parell, } y \text{ i } z \text{ senars}, \\ &x, z \notin 3\mathbb{Z}, \\ &x, y \notin 5\mathbb{Z}, \end{aligned}$$

i

$$x^3 + 6y^3 = 10z^3,$$

aleshores existeixen ideals coprimers $\mathfrak{a}$, $\mathfrak{b}$ *de* $\mathcal{O}_K$ *tals que*

$$\langle x^2 - xy\alpha + y^2\alpha^2\rangle = \mathfrak{p}_2^2\mathfrak{p}_{5^2}\mathfrak{a}^3,$$
$$\langle x + y\alpha\rangle = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{b}^3.$$

Demostració. Prenguem ara $x^3 + 6y^3 = (x + y\alpha)(x^2 - xy\alpha + y^2\alpha^2) = 10z^3$ com a equació d'ideals principals.

$$\langle x + y\alpha\rangle\langle x^2 - xy\alpha + y^2\alpha^2\rangle = \langle 10\rangle\langle z\rangle^3.$$

Trobem, primer, els factors comuns de $\langle x + y\alpha\rangle$ i $\langle x^2 - xy\alpha + y^2\alpha^2\rangle$. Sigui $\mathfrak{p}$ un ideal primer tal que

$$\begin{cases} \mathfrak{p} \mid \langle x + y\alpha\rangle \\ \mathfrak{p} \mid \langle x^2 - xy\alpha + y^2\alpha^2\rangle. \end{cases}$$

aleshores

$$\mathfrak{p}^2 \mid \langle 10\rangle\langle z\rangle^3 = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{5^2}\langle z\rangle.$$

Vegem que $\mathfrak{p} = \mathfrak{p}_2$. Ja que

$$x^2 - xy\alpha + y^2\alpha^2 = (x + y\alpha)^2 - 3xy\alpha$$

i que

$$x + y\alpha \in \langle x + y\alpha\rangle \subseteq \mathfrak{p}, \quad x^2 - xy\alpha + y^2\alpha^2 \in \langle x^2 - xy\alpha + y^2\alpha^2\rangle \subseteq \mathfrak{p},$$

tenim que

$$3xy\alpha \in \mathfrak{p}.$$

Per tant,

$$\mathfrak{p} \mid \langle 3xy\alpha\rangle = \mathfrak{p}_3^3\langle x\rangle\langle y\rangle\langle\alpha\rangle$$

Separem per casos

- $\mathfrak{p} \mid \mathfrak{p}_3$.
  Ja que $\mathfrak{p}$ i $\mathfrak{p}_3$ són ideals primers, aleshores $\mathfrak{p} = \mathfrak{p}_3$. Atès que $\mathfrak{p}_2$, $\mathfrak{p}_5$ i $\mathfrak{p}_{5^2}$ són ideals primers diferents de $\mathfrak{p}_3$, es té que $\mathfrak{p}_3 \mid \langle z\rangle$ per tant, $N(\mathfrak{p}_3) \mid N(\langle z\rangle)$, i $3 \mid \mathrm{N}_{K|\mathbb{Q}}(z) = z^3$. Per hipòtesi tenim que $z \notin 3\mathbb{Z}$, per tant, no pot ser que $\mathfrak{p} \mid \mathfrak{p}_3$.

- $\mathfrak{p} \mid \langle x \rangle$.
  Ja que x i $x + \alpha y \in \mathfrak{p}$, $\alpha y \in \mathfrak{p}$ i $\mathfrak{p} \mid \langle y\alpha \rangle = \langle y \rangle \langle \alpha \rangle$. Si fos $\mathfrak{p} \mid \langle y \rangle$, aleshores
  $$N(\mathfrak{p}) \mid \begin{cases} \mathrm{N}_{K|\mathbb{Q}}(x) = x^3, \\ \mathrm{N}_{K|\mathbb{Q}}(y) = y^3, \end{cases}$$
  per tant, x i y no són coprimers. Així $\mathfrak{p} \mid \langle \alpha \rangle$.

- $\mathfrak{p} \mid \langle y \rangle$.
  Com en cas el anterior deduïm que $\mathfrak{p} \mid \langle x \rangle$, que torna a portar a contradicció.

Així hem vist que
$$\begin{cases} \mathfrak{p} \nmid \mathfrak{p}_3. \\ \mathfrak{p} \mid \langle \alpha \rangle = \mathfrak{p}_2 \mathfrak{p}_3. \end{cases}$$
per tant $\mathfrak{p} = \mathfrak{p}_2$. Així, existeixen $\mathfrak{c}$ i $\mathfrak{c}'$ ideals tals que
$$\begin{cases} \langle x + y\alpha \rangle = \mathfrak{p}_2 \mathfrak{c} \\ \langle x^2 - xy\alpha + y^2\alpha^2 \rangle = \mathfrak{p}_2 \mathfrak{c}' \end{cases}$$
A més, per hipòtesi $2 \mid x$ per tant, $\mathfrak{p}_2^3 \mid \langle x \rangle$. Per tant,
$$\mathfrak{p}_2^2 \mid \langle x + y\alpha \rangle \iff \mathfrak{p}_2^2 \mid \langle y \rangle \langle \alpha \rangle.$$
Ja que x i y són coprimers, $\mathfrak{p}_2 \nmid \langle y \rangle$. Atès que
$$\langle \alpha \rangle = \mathfrak{p}_2 \mathfrak{p}_3,$$
tenim que
$$\mathfrak{p}_2^2 \nmid \langle x + y\alpha \rangle,$$
així $\mathfrak{p}_2 \nmid \mathfrak{c}$. Tanmateix,
$$\mathfrak{p}_2^3 \mid \langle x + y\alpha \rangle \langle x^2 - xy\alpha + y^2\alpha^2 \rangle = \mathfrak{p}_2^2 \mathfrak{c}\mathfrak{c}',$$
per tant
$$\mathfrak{p}_2 \mid \mathfrak{c}',$$
i
$$\mathfrak{p}_2^2 \mid \langle x^2 - xy\alpha + y^2\alpha^2 \rangle.$$

És a dir, existeixen ideals $\mathfrak{c}$ i $\mathfrak{c}''$ tals que

$$\begin{cases} \langle x + y\alpha \rangle = \mathfrak{p}_2\mathfrak{c}, \\ \langle x^2 - xy\alpha + y^2\alpha^2 \rangle = \mathfrak{p}_2^2\mathfrak{c}'' \end{cases}$$

i

$$\mathfrak{c}\mathfrak{c}'' = \mathfrak{p}_5\mathfrak{p}_{5^2}\langle z \rangle^3.$$

Notem que, per hipòtesi, $z \notin 2\mathbb{Z}$, per tant $\mathfrak{p}_2 \nmid \langle z \rangle$. Concretament, 3 és el màxim enter s tal que

$$\mathfrak{p}_2^s \mid \langle 10z \rangle,$$

i, ja que l'únic primer comú de $\langle x + y\alpha \rangle$ i $\langle x^2 - xy\alpha + y^2\alpha^2 \rangle$ és $\mathfrak{p}_2$, tenim que $\mathfrak{c}$ i $\mathfrak{c}''$ han de ser coprimers.
Vegem que $\mathfrak{p}_5 \mid \langle x + y\alpha \rangle$. Per hipòtesi, $x, y \notin 5\mathbb{Z}$ i $x^3 + 6y^3 = 10z^3$. Reduint mòdul 5

$$x^3 + y^3 \equiv 0 \pmod 5.$$

Notem que

$$\begin{cases} x \equiv 1 \pmod 5 \Longrightarrow x^3 \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 5 \Longrightarrow x^3 \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 5 \Longrightarrow x^3 \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 5 \Longrightarrow x^3 \equiv 4 \pmod 5, \end{cases}$$

per tant, si $x^3 \equiv -y^3 \pmod 5$ llavors $x \equiv -y \pmod 5$. És a dir,

$$x + y \in 5\mathbb{Z} \subseteq 5\mathcal{O}_K \subseteq \mathfrak{p}_5 = \langle \alpha - 1 \rangle.$$

Observem que

$$\begin{aligned} x + y &= x + y\alpha - y\alpha + y \\ &= x + y\alpha - y(\alpha - 1), \end{aligned}$$

per tant

$$x + y\alpha \in \langle \alpha - 1 \rangle$$

i

$$\mathfrak{p}_5 \mid \langle x + y\alpha \rangle.$$

Vegem que $\mathfrak{p}_{5^2} \mid \langle x^2 - xy\alpha + y^2\alpha^2 \rangle$. Fem-ho per reducció a l'absurd. Suposem que

$$\mathfrak{p}_{5^2} \nmid \langle x^2 - xy\alpha + y^2\alpha^2 \rangle,$$

aleshores

$$\mathfrak{p}_{5^2} \mid \langle x + y\alpha \rangle$$

i

$$\langle 5 \rangle = \mathfrak{p}_5 \mathfrak{p}_{5^2} \mid \langle x + y\alpha \rangle.$$

Així,

$$x + y\alpha \in \langle x + y\alpha \rangle \subseteq \langle 5 \rangle$$

i $5 \mid x + y\alpha$ en $\mathcal{O}_K = \mathbb{Z}[\alpha]$. És a dir existeixen $a, b, c \in \mathbb{Z}$ tals que

$$5(a + b\alpha + c\alpha^2) = x + y\alpha,$$

per tant,

$$\begin{cases} 5a = x, \\ 5b = y, \\ 5c = 0, \end{cases}$$

i x, $y \in 5\mathbb{Z}$. Això es contradiu amb les hipòtesis, per tant

$$\mathfrak{p}_{5^2} \mid \langle x^2 - xy\alpha + y^2\alpha^2 \rangle.$$

Així, deduïm que existeixen dos ideals coprimers $\mathfrak{m}$ i $\mathfrak{m}'$ tals que

$$\begin{aligned} \langle x + y\alpha \rangle &= \mathfrak{p}_2 \mathfrak{p}_5 \mathfrak{m}, \\ \langle x^2 - xy\alpha + y^2\alpha^2 \rangle &= \mathfrak{p}_2^2 \mathfrak{p}_{5^2} \mathfrak{m}'. \end{aligned}$$

Multiplicant-los obtenim que $\mathfrak{p}_2^3 \mathfrak{p}_5 \mathfrak{p}_{5^2} \mathfrak{m}\mathfrak{m}' = \langle 10 \rangle \langle z \rangle^3$, així

$$\mathfrak{m}\mathfrak{m}' = \langle z \rangle^3$$

i, ja que $\mathfrak{m}$ i $\mathfrak{m}'$ són coprimers, són cubs. D'on es deduiex el resultat. □

4.2 Absència de solucions globals de l'equació de Selmer

Teorema 4.2.1. *L'equació de Selmer* $3X^3 + 4Y^3 + 5Z^3 = 0$ *només te la solució* $(0, 0, 0)$ *en* $\mathbb{Q}$.

Demostració. En virtud de les observacions fetes al principi del capítol, és suficient veure que l'equació

$$X^3 + 6Y^3 = 10Z^3 = 0$$

només té solució trivial en $\mathbb{Z}$. Suposarem (x, y, z) solució no trivial, amb $xyz \neq 0$, coprimers dos a dos, x parell, x i y no múltiples de 3, x i y no múltiples de 5. Per la proposició (4.1.6) sabem que existeix un ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ tal que

$$\langle x + y\alpha \rangle = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{b}^3.$$

Atès que $\mathcal{O}_K$ és un domini d'ideals principals, existeix $\beta \in \mathcal{O}_K$ tal que

$$\mathfrak{b} = \langle \beta \rangle.$$

En concret,

$$\begin{aligned} \langle x + y\alpha \rangle &= \langle \alpha - 2 \rangle \langle \alpha - 1 \rangle \langle \beta \rangle^3 \\ &= \langle (\alpha - 2)(\alpha - 1)\beta^3 \rangle. \end{aligned}$$

D'on es dedueix que existeix una unitat $v \in \mathcal{O}_K^*$ tal que

$$x + y\alpha = (\alpha - 2)(\alpha - 1)\beta^3 v.$$

Atès que $u = 1 - 6\alpha + 3\alpha^2$ és un representant d'una classe no trivial de $\mathcal{O}_K^*/\mathcal{O}_K^{*3} \simeq \mathbb{Z}/3\mathbb{Z}$, existeixen $v' \in \mathcal{O}_K^*$ i $k \in \{0, 1, 2\}$ tals que

$$v = u^k (v')^3.$$

Per tant

$$x + y\alpha = (\alpha - 2)(\alpha - 1)(\beta v')^3 u^k.$$

Notem que

$$u = \frac{(2 - \alpha)^3}{2}.$$

En efecte,

$$\begin{aligned} (2 - \alpha)^3 &= 8 - 12\alpha + 6\alpha^2 - \alpha^3 \\ &= 2 - 12\alpha + 6\alpha^2 \\ &= 2u. \end{aligned}$$

Així,

$$(x + y\alpha) = (\alpha - 2)(\alpha - 1)\frac{(\beta v')^3 (2 - \alpha)^{3k}}{2^k} = (\alpha - 2)(\alpha - 1)\frac{\gamma^3}{2^k},$$

on $\gamma = \beta v'(2-\alpha)^k \in \mathcal{O}_K = \mathbb{Z}[\alpha]$. Així, existeixen $A, B, C \in \mathbb{Z}$ no tots zero tals que

$$\gamma = A + B\alpha + C\alpha^2$$

i

$$2^k x + 2^k y\alpha = (\alpha-2)(\alpha-1)(A + B\alpha + C\alpha^2)^3.$$

Operant obtenim que les coordenades $\{\lambda_1, \lambda_2\lambda_3\}$ de $(\alpha-2)(\alpha-1)\gamma^3$ en base $\{1, \alpha, \alpha^2\}$ són

$$\begin{aligned}
\lambda_1 &= 2(A^3 + 6B^3 + 36C^3 + 36ABC) - 54(A^2C + AB^2 + 6BC^2) \\
&\quad + 18(A^2B + 6AC^2 + 6B^2C), \\
\lambda_2 &= 6(A^2B + 6AC^2 + 6B^2C) - 3(A^3 + 6B^3 + 36C^3 \\
&\quad + 36ABC) + 18(A^2C + AB^2 + 6BC^2), \\
\lambda_3 &= A^3 + 6B^6 + 36C^3 + 36ABC - 9(3A^2B + 6AC^2 + 6B^2C) \\
&\quad + 6(A^2C + AB^2 + 6BC^2).
\end{aligned}$$

En efecte, mitjançant el binomi de Newton tenim

$$\begin{aligned}
(A + B\alpha + C\alpha^2)^3 &= A^3 + 3A^2(B\alpha + C\alpha^2) + 3A(B^2\alpha^2 + 2BC\alpha^3 + C^2\alpha^4) + B^3\alpha^3 \\
&\quad + 3B^2C\alpha^4 + 3BC^2\alpha^5 + C^3\alpha^6 \\
&= A^3 + 6B^3 + 36C^3 + 36ABC \\
&\quad + (3A^2B + 18AC^2 + 18B^2C)\alpha \\
&\quad + (3A^2C + 3AB^2 + 18BC^2)\alpha^2
\end{aligned}$$

i

$$(\alpha-1)(\alpha-2) = \alpha^2 - 3\alpha + 2.$$

Per tant,

$$\begin{aligned}
\lambda_1 &= 2(A^3 + 6B^3 + 36C^3 + 36ABC) \\
&\quad - 18(3A^2C + 3AB^2 + 18BC^2) \\
&\quad + 6(3A^2B + 18AC^2 + 18B^2C), \\
\lambda_2 &= 2(3A^2B + 18AC^2 + 18B^2C) \\
&\quad - 3(A^3 + 6B^3 + 36C^3 + 36ABC) \\
&\quad + 6(3A^2C + 3AB^2 + 18BC^2), \\
\lambda_3 &= A^3 + 6B^6 + 36C^3 + 36ABC \\
&\quad - 3(3A^2B + 18AC^2 + 18B^2C) \\
&\quad + 2(3A^2C + 3AB^2 + 18BC^2).
\end{aligned}$$

Igualant coeficients

$$\begin{cases} 2^k x & = \lambda_1, \\ 2^k y & = \lambda_2, \\ 0 & = \lambda_3. \end{cases}$$

Així, de la igualtat sobre els coeficients de α^2 obtenim que

$$0 = A^3+6B^3+36C^3+36ABC-9(A^2B+6AC^2+6B^2C)+6(A^2C+AB^2+6BC^2). \tag{4.2.1}$$

Reduint mòdul 3 obtenim que $3 \mid A$. Reduint mòdul 9,

$$6B^3 \equiv 0 \pmod 9,$$

per tant $3 \mid B$. Reduint mòdul 27,

$$36C^3 \equiv 0 \pmod{27}.$$

Notem que (4.2.1) és una equació homogènia de grau 3. Per tant, podem treure factors comuns a A, B, C, de tal forma que satisfacin la mateixa equació però s'hagin reduït en un factor 3. Això ens porta a descens infinit que no pot ser. Per tant $A = B = C = 0$, així $\beta = 0$ i $z = 0$. Que contradiu el que havíem suposat; per tant, l'equació de Selmer només té la solució trivial. □

Apèndix A

Equacions diagonals

L'objectiu d'aquest apèndix és donar un guió per a demostrar la desigualtat de Hasse que dóna una aproximació de la quantitat de solucions d'una equació polinòmica diagonal homogènia mòdul p. En concret, farem una introducció a la teoria de caràcters i veurem la definició de suma de Jacobi. Donat p enter primer, $\mathbb{F}_p$ denotarà, com fins ara, el cos finit de p elements.

Definició A.0.2. Diem que una aplicació $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ és un caràcter si

$$\chi(ab) = \chi(a)\chi(b), \quad \text{per a tot } a,\, b \in \mathbb{F}_p^*.$$

Observacions A.0.3. Considerem dos caràcters χ, λ sobre $\mathbb{F}_p^*$.

(a) L'aplicació

$$\begin{array}{rccc} \varepsilon : & \mathbb{F}_p^* & \longrightarrow & \mathbb{C}^* \\ & a & \longmapsto & 1 \end{array}$$

és un caràcter, anomenat el caràcter trivial mòdul p.

(b) L'aplicació

$$\begin{array}{rccc} \chi^{-1} : & \mathbb{F}_p^* & \longrightarrow & \mathbb{C}^* \\ & a & \longmapsto & \chi(a)^{-1} \end{array}$$

és un caràcter.

(c) L'aplicació

$$\begin{array}{rccc} \chi\lambda : & \mathbb{F}_p^* & \longrightarrow & \mathbb{C}^* \\ & a & \longmapsto & \chi(a)\lambda(a) \end{array}$$

és un caràcter.

Així, podem dotar el conjunt dels caràcters de $\mathbb{F}_p^*$ d'una estructura de grup abelià.

Definició A.0.4. Siguin p un enter primer, $a \in \mathbb{F}_p^*$ i $n \in \mathbb{N}$ definim

$$N(x^n = a) = \#\{x \in \mathbb{F}_p^* : x^n = a\}.$$

Proposició A.0.5. *Donats $n \geq 1$ i $a \in \mathbb{F}_p^*$, si $n \mid p-1$, aleshores*

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a).$$

Definició A.0.6 (Suma de Jacobi)**.** Siguin $\chi_1,\ldots,\chi_l$ caràcters sobre $\mathbb{F}_p^*$, la suma de Jacobi és definida per la fórmula

$$J(\chi_1, \ldots, \chi_l) = \sum_{t_1+\cdots+t_l=1} \chi(t_1)\cdots\chi(t_l).$$

Anàlogament, es defineix

$$J_0(\chi_1, \ldots, \chi_l) = \sum_{t_1+\cdots+t_l=0} \chi(t_1)\cdots\chi(t_l).$$

Proposició A.0.7. *Siguin $\chi_1, \ldots, \chi_l$ caràcters sobre $\mathbb{F}_p^*$,*

(a) Si $\chi_i = \varepsilon$ per a cada i, aleshores

$$J_0(\chi_1, \ldots, \chi_l) = J(\chi_1, \ldots, \chi_l) = p^{l-1}.$$

(b) Si algun però no tots els caràcters són ε, llavors

$$J_0(\chi_1, \ldots, \chi_l) = J(\chi_1, \ldots, \chi_l) = 0.$$

Teorema A.0.8. *Considerem els caràcters no trivials $\chi_1, \ldots, \chi_l$.*

(a) Si $\chi_1 \cdots \chi_l \neq \varepsilon$, llavors

$$|J(\chi_1, \ldots, \chi_l)| = p^{\frac{l-1}{2}}.$$

(b) Si $\chi_1 \cdots \chi_l = \varepsilon$*, llavors*

$$|J_0(\chi_1, \ldots, \chi_l)| = (p-1)p^{\frac{l}{2}-1}$$

i

$$|J(\chi_1, \ldots, \chi_l)| = p^{\frac{l}{2}-1}.$$

on $|\cdot|$ *designa la norma complexa.* □

Teorema A.0.9. *Considerem l'equació sobre* $\mathbb{F}_p^*$

$$a_1 x_1^{l_1} + \cdots + a_r x_r^{l_r} = 0, \qquad amb\ a_i \in \mathbb{F}_p^*.$$

Siguin N *el nombre de solucions d'aquesta equació i*

$$M = \#\left\{(\chi_1, \ldots, \chi_r)\ \textit{caràcters no trivials} : \chi_i^{l_i} = \varepsilon, \chi_1 \cdots \chi_r = \varepsilon\right\},$$

aleshores

$$|N - p^{r-1}| \leq M(p-1)p^{\frac{r}{2}-1}.$$

□

Corol·lari A.0.10. *El nombre* N_p *de solucions en* $\mathbb{F}_p$ *de l'equació de congruència* $c_1X^3 + c_2Y^3 + c_3Z^3 \equiv 0 \pmod{p}$ *satisfà que*

$$|N_p - p^2| \leq 2(p-1)\sqrt{p}.$$

Demostració. Utilitzant el teorema anterior tenim que

$$|N_p - p^2| \leq M(p-1)p^{\frac{1}{2}} = M(p-1)\sqrt{p},$$

on $M = \#\{(\chi_1, \chi_2, \chi_3)$ caràcters no trivials : $\chi_i^3 = \varepsilon, \chi_1\chi_2\chi_3 = \varepsilon\}$. Atès que els caràcters no trivial d'ordre 3 són

$$\chi_1(a) = e^{\frac{2\pi i a}{3}}$$

i

$$\chi_2(a) = \chi_1(a)^{-1} = e^{\frac{4\pi i a}{3}},$$

tenim que

$$M = \#\{(\chi_1, \chi_1, \chi_1), (\chi_2, \chi_2, \chi_2)\} = 2,$$

d'on s'obté el resultat. □

Observació A.0.11. El treball de Selmer [10] conté més que l'estudi d'una única equació. En l'article, considera equacions diagonals cúbiques generals i determina en certs casos l'existència de solucions locals mitjançant el corol·lari anterior. Un cop demostrada l'existència de solucions en $\mathbb{F}_p^*$, les puja a $\mathbb{Z}_p$ mitjançant el lema de Hensel i obté solucions p-àdiques no trivials. En el nostre cas, però, en seguir la demostració del capítol 3, es veu que el guió és el mateix si bé trobem solucions en $\mathbb{F}_p$ sense necessitat del corol·lari anterior.

Bibliografia

[1] Alaca, Şaban; Williams, Kenneth S.: *Introductory algebraic number theory*. Cambridge University Press, Cambridge, 2004. xviii+428 p. ISBN: 0-521; 0-521-54011-9.

[2] Bourbaki, Nicolas: *General topology*. Chapters 1-4. Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. vii+437 p. ISBN: 3-540-64241-2.

[3] Casassas Massana, Pau: *Nombres p-àdics i mètodes locals-globals*. Treball final de grau de matemàtiques. Universitat de Barcelona, 2013.

[4] Cassels, J. W. S. : *Local fields*. London Mathematical Society Student Texts, 3. Cambridge University Press, Cambridge, 1986. xiv+360 p. ISBN: 0-521-30484-9; 0-521-31525-5.

[5] Conrad, K.: *Selmer's example.* 4p.

www.math.uconn.edu/˜kconrad/blurbs/gradnumthy/selmerexample.pdf.

[6] Ireland, Kenneth; Rosen, Michael: *A classical introduction to modern number theory*. Graduate Texts in Mathematics, No. 84. Springer-Verlag, New York, 1990. xiv+389 p. ISBN: 0-387-97329-X.

[7] Koblitz, Neal: *p-adic numbers, p-adic analysis, and zeta-functions*. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984. xii+150 p. ISBN: 0-387-96017-1.

[8] Llorente, P.; Nart, E.: Effective determination of the decomposition of the rational primes in a cubic field. *Proc. Amer. Math. Soc.* 87 (1983), no. 4, 579–585.

[9] Narkiewicz, Władysław: *Elementary and analytic theory of algebraic numbers*. Second edition. Springer-Verlag, Berlin; PWN—Polish Scientific Publishers, Warsaw, 1990. xiv+746 p. ISBN: 3-540-51250-0.

[10] Selmer, Ernst S.: The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.* 85 (1951), 203–362.

[11] Serre, J. P.: *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. viii+115 p.