UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Àlgebres de quaternions i el Teorema dels quatre quadrats

Autor: Maria Sert Casademont

Director: Dr. Xavier Guitart Morales

Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2024

Abstract

This memory begins with the study of Hamilton quaternions and general quaternion algebras as well as their properties. This is followed by a study of Hurwitz quaternions and their main properties. Finally, the Lagrange four-square theorem is proved using these properties.

Resum

Aquesta memòria comença amb l'estudi dels quaternions de Hamilton i les àlgebres de quaternions generals així com les seves propietats. Tot seguit s'estudien els quaternions de Hurwitz i les seves propietats principals i, finalment, a partir d'aquestes es demostra el Teorema dels quatre quadrats de Lagrange.

2020 Mathematics Subject Classification. 11G05, 11G10, 14G10

Agraïments

Aquest treball no hagués estat possible sense el suport de totes les persones que m'han acompanyat durant aquests anys.

Vull agrair especialment al Dr. Xavier Guitart Morales, tutor d'aquest treball. Gràcies per les hores dedicades, el suport i l'ajut que m'ha proporcionat durant el desenvolupament del treball. Sense ell, no hagués estat possible. Ha estat un gran tutor.

Als meus pares, Josep i Gemma, pel suport incondicional durant aquests anys.

A la meva germana Marta, al meu tiet Joan i a les meves amigues per animar-me a continuar endavant.

Índex

1 Introducció

Un dels teoremes que ha intrigat als matemàtics durant segles ha estat el dels quatre quadrats de Lagrange, també anomenat conjectura de Bachet. Joseph Louis Lagrange (1736-1813), un dels grans matemàtics de l'època de la Revolució i de l'Imperi Francès, va resoldre i demostrar un resultat fonamental en teoria de nombres on es relaciona la representació de nombres enters com la suma dels quatre quadrats enters. Aquest teorema estableix que qualsevol nombre enter positiu n pot expressar-se com la suma de quatre quadrats enters. La seva aplicabilitat i el seu servei en la comprensió dels nombres enters l'han convertit en un teorema fonamental de les matemàtiques. El Teorema dels quatre quadrats de Lagrange té aplicacions diverses en les matemàtiques i la física havent estat fonamental en la comprensió de les propietats dels nombres enters influenciant en àrees tant diverses com la criptografia i la teoria de codis.

En aquesta memòria demostrarem aquest teorema fent servir una estructura algebràica que s'anomenen quaternions que els definirem a l'apartat 2. Concretament utilitzarem els quaternions de Hurwitz que parlarem d'ells l'apartat 3.

Un nombre complex és la suma $a+bi$ amb $a, b \in \mathbb{R}$ i $i^2 = -1$. La suma i la multiplicació es defineixen de la següent forma:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \qquad (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Al 1833 William Rowan Hamilton (1805-1865), matemàtic, físic i astrònom irlandès, va declarar que $a + bi$ és un parell ordenat (a, b), és a dir va definir $\mathbb{C}$ per a ser $\mathbb{R}^2$ amb la suma i multiplicació inspirades amb les dels nombres complexos:

$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b)(c, d) = (ac - bd, ad + bc).$$

L'element neutre per la suma és $(0, 0)$ i l'element neutre per la multiplicació és $(1, 0)$, i per la suma i multiplicació escalar de vectors reals tenim que $(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1)$, que s'assembla a $a + bi$ si definim i com a $(0, 1)$.

Hamilton buscava formes d'estendre els nombres complexos a dimensions més grans. No ho va aconseguir per a tres dimensions, però el 1843 va descobrir una manera de multiplicar en quatre dimensions, a costa de perdre la commutativitat de la multiplicació, i va obtenir així els quaternions.

En aquesta memòria començarem definint els quaternions de Hamilton, que són l'anàleg dels reals per als quaternions, definirem les seves propietats i donarem la demostració del Teorema de Frobenius (2.7) que afirma que l'única àlgebra associativa de divisió de dimensió finita que no és commutativa sobre els nombres reals són els quaternions. Tot seguit introduirem les àlgebres de quaternions sobre un cos, estudiarem els isomorfismes que existeixen entre elles i donarem alguns criteris per detectar isomorfismes.

A continuació, definirem els quaternions de Hurwitz, que com he enunciat abans, seran la base de la demostració del Teorema dels quatre quadrats.
Una de les proposicions que demostrarem és que la norma de tot quaternió de Hurwitz és un enter racional (3.3).

Finalment, demostrarem diferents teoremes que enuncien diferents propietats del quaternions de Hurwitz necessàries per a poder demostrar el Teorema dels quatre quadrats, concloent la memòria amb la demostració d'aquest (4.11).

2 Àlgebres de quaternions

2.1 Quaternions de Hamilton

En aquest apartat introduirem que són els quaternions de Hamilton així com algunes de les seves propietats.

Definició 2.1. *Els quaternions de Hamilton es denoten com* $\mathbb{H}$ *i estan definits com el conjunt*

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

En $\mathbb{H}$ *definim dues operacions: suma i producte.*
La suma es defineix com:

- *Siguin* $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ *i* $\beta = b_0 + b_1 i + b_2 j + b_3 k$*, aleshores* $\alpha + \beta = a_0 + b_0 + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$*.*

El producte es defineix a partir de les identitats:

- $i^2 = j^2 = k^2 = -1$*,*
- $ij = k$*,* $ji = -k$*,* $jk = i$*,* $kj = -i$*,* $ki = j$*,* $ik = -j$*,*
- *Tot* $a \in \mathbb{R}$ *commuta amb* i*,* j*,* k*.*

Anomenem quaternió pur a un quaternió amb $a = 0$. El quadrat d'aquest és una suma negativa de tres quadrats:

$$(bi + cj + dk)^2 = -b^2 - c^2 - d^2.$$

Fixem-nos que $\mathbb{R} \subseteq \mathbb{H}$, identificant $a \in \mathbb{R}$ amb $a + 0i + 0j + 0k$.

Abans de continuar amb les següents definicions, recordem que un anell és una estructura algebraica formada per un conjunt A d'elements on hi ha definides dues operacions binàries: la suma $(+)$ i el producte $(\cdot)$ i que compleixen les següents propietats:

1. $(A, +)$ és un grup commutatiu:
   a. $a + (b + c) = (a + b) + c$ per a tot $a, b, c \in A$ (associativitat).
   b. Existeix un element, 0, tal que $0 + a = a + 0 = a$ per a tot $a \in A$ (element neutre per la suma).
   c. Tot element $a \in A$ té un invers per la suma, $(-a)$, de manera que $a + (-a) = (-a) + a = 0$ (element invers).
   d. $a + b = b + a$ per a tot $a, b \in A$ (commutativitat).

2. $(A, \cdot)$ verifica:

   a. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ per a tot $a, b, c \in A$ (associativitat).

   b. $a \cdot (b + c) = a \cdot b + a \cdot c$ i $(a + b) \cdot c = a \cdot c + b \cdot c$ per a tot $a, b, c \in A$ (propietat distributiva respecte a la suma).

   c. Existeix un element, 1, tal que $1 \cdot a = a \cdot 1 = a$ per a tot $a \in A$ (element neutre pel producte).

A continuació veurem que $\mathbb{H}$ és un anell:

1. Associativitat per la suma: Per a tot $\alpha = a_0 + a_1 i + a_2 j + a_3 k, \beta = b_0 + b_1 i + b_2 j + b_3 k, \gamma = c_0 + c_1 i + c_2 j + c_3 k \in \mathbb{H}$,
   Per l'associativitat dels nombres reals és directe veure que $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

2. Element neutre per la suma: Existeix $0 = 0 + 0i + 0j + 0k \in \mathbb{H}$ tal que $0 + \alpha = \alpha + 0 = \alpha$ per a tot $\alpha \in A$.

3. Element invers: Per a tot $\alpha = a + bi + cj + dk \in \mathbb{H}$, existeix $\beta = -a - bi - cj - dk \in \mathbb{H}$ tal que $\alpha + \beta = 0$

4. Commutativitat: Per tot $\alpha = a_0 + a_1 i + a_2 j + a_3 k, \beta = b_0 + b_1 i + b_2 j + b_3 k \in \mathbb{H}$,
   Per la commutativitat dels nombres reals és directe veure que $\alpha + \beta = \beta + \alpha$.

5. Associativitat pel producte: Per a tot $\alpha = a_0 + a_1 i + a_2 j + a_3 k, \beta = b_0 + b_1 i + b_2 j + b_3 k, \gamma = c_0 + c_1 i + c_2 j + c_3 k \in \mathbb{H}$,
   $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
   $\alpha \cdot (\beta \cdot \gamma) = (a_0 + a_1 i + a_2 j + a_3 k) \cdot ((b_0 c_0 - b_1 c_1 - b_2 c_2 - b_3 c_3) + (b_0 c_1 + b_1 c_0 + b_2 c_3 - b_3 c_2) i + (b_0 c_2 - b_1 c_3 + b_2 c_0 + b_3 c_1) j + (b_0 c_3 + b_1 c_2 - b_2 c_1 + b_3 c_0) k) =$
   $(a_0 b_0 c_0 - a_0 b_1 c_1 - a_0 b_2 c_2 - a_0 b_3 c_3) + (a_0 b_0 c_1 + a_0 b_1 c_0 + a_0 b_2 c_3 - a_0 b_3 c_2) i + (a_0 b_0 c_2 - a_0 b_1 c_3 + a_0 b_2 c_0 + a_0 b_3 c_1) j + (a_0 b_0 c_3 + a_0 b_1 c_2 - a_0 b_2 c_1 + a_0 b_3 c_0) k + (a_1 b_0 c_0 - a_1 b_1 c_1 - a_1 b_2 c_2 - a_1 b_3 c_3) i + (-a_1 b_0 c_1 - a_1 b_1 c_0 - a_1 b_2 c_3 + a_1 b_3 c_2) + (a_1 b_0 c_2 - a_1 b_1 c_3 + a_1 b_2 c_0 - a_1 b_3 c_1) k + (-a_1 b_0 c_3 - a_1 b_1 c_2 + a_1 b_2 c_1 - a_1 b_3 c_0) j + (a_2 b_0 c_0 - a_2 b_1 c_1 - a_2 b_2 c_2 - a_2 b_3 c_3) j + (a_2 b_0 c_1 - a_2 b_1 c_0 - a_2 b_2 c_3 + a_2 b_3 c_2) k + (-a_2 b_0 c_2 + a_2 b_1 c_3 - a_2 b_2 c_0 - a_2 b_3 c_1) + (a_2 b_0 c_3 + a_2 b_1 c_2 - a_2 b_2 c_1 + a_2 b_3 c_0) i + (a_3 b_0 c_0 - a_3 b_1 c_1 - a_3 b_2 c_2 - a_3 b_3 c_3) k + (a_3 b_0 c_1 + a_3 b_1 c_0 + a_3 b_2 c_3 - a_3 b_3 c_2) j + (a_3 b_0 c_2 + a_3 b_1 c_3 - a_3 b_2 c_0 - a_3 b_3 c_1) i + (-a_3 b_0 c_3 - a_3 b_1 c_2 + a_3 b_2 c_1 - a_3 b_3 c_0)$

   Per la commutativitat i l'associativitat dels nombres reals, podem reagrupar l'anterior suma de la següent forma:

   $\alpha \cdot (\beta \cdot \gamma) = (a_0 b_0 c_0 - a_1 b_1 c_0 - a_2 b_2 c_0 - a_3 b_3 c_0) + (a_0 b_0 c_1 - a_1 b_1 c_1 - a_2 b_2 c_1 - a_3 b_3 c_1) i + (a_0 b_0 c_2 - a_1 b_1 c_2 - a_2 b_2 c_2 - a_3 b_3 c_2) j + (a_0 b_0 c_3 - a_1 b_1 c_3 - a_2 b_2 c_3 - a_3 b_3 c_3) k + (a_0 b_1 c_0 + a_1 b_0 c_0 + a_2 b_3 c_0 - a_3 b_2 c_0) i + (-a_0 b_1 c_1 - a_1 b_0 c_1 - a_2 b_3 c_1 + a_3 b_2 c_1) + (a_0 b_1 c_2 + a_1 b_0 c_2 + a_2 b_3 c_2 - a_3 b_2 c_2) k + (-a_0 b_1 c_3 - a_1 b_0 c_3 - a_2 b_3 c_3 + a_3 b_2 c_3) j + (a_0 b_2 c_0 - a_1 b_3 c_0 + a_2 b_0 c_0 + a_3 b_1 c_0) j + (-a_0 b_2 c_1 - a_1 b_3 c_1 + a_2 b_0 c_1 - a_3 b_1 c_1) k + (-a_0 b_2 c_2 + a_1 b_3 c_2 - a_2 b_0 c_2 - a_3 b_1 c_2) +$

$(a_0b_2c_3 - a_1b_3c_3 + a_2b_0c_3 + a_3b_1c_3)i + (a_0b_3c_0 + a_1b_2c_0 - a_2b_1c_0 + a_3b_0c_0)k + (a_0b_3c_1 + a_1b_2c_1 - a_2b_1c_1 + a_3b_0c_1)j + (-a_0b_3c_2 - a_1b_2c_2 + a_2b_1c_2 + a_3b_0c_2)i + (-a_0b_3c_3 - a_1b_2c_3 + a_2b_1c_3 - a_3b_0c_3) = ((a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)j + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)k) \cdot (c_0 + c_1i + c_2j + c_3k) = (\alpha \cdot \beta) \cdot \gamma$

6. Distribució respecte la suma: Per a tot $\alpha, \beta, \gamma \in \mathbb{H}$
   $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ i $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$.

   Es pot demostrar de manera semblant a l'anterior punt.

7. Element neutre pel producte: Existeix $1 = 1+0i+0j+0k \in \mathbb{H}$ tal que $1 \cdot \alpha = \alpha \cdot 1 = \alpha$ per a tot $\alpha \in A$.

Definició 2.2. *El conjunt d'elements d'un anell que commuten pel producte amb tot element de l'anell s'anomena centre de l'anell.*

Exemple 2.3. $\mathbb{H}$ és no commutatiu, mentre que la multiplicació en $\mathbb{H}$ per nombres reals és commutativa: $aq = qa, a \in \mathbb{R}, q \in \mathbb{H}$. Tenim doncs que $\mathbb{R}$ està contingut al centre de $\mathbb{H}$.
Per veure que $\mathbb{R}$ és el centre de $\mathbb{H}$, ens falta veure que

$$\{q \in \mathbb{H} : qq' = q'q \ \ per\ a\ tot \ \ q' \in \mathbb{H}\} = \mathbb{R}.$$

Sigui $q = a + bi + cj + dk$, amb $a, b, c, d \in \mathbb{R}$, suposem que q és del centre de $\mathbb{H}$. Aleshores hem de tenir que $qi = iq$ ja que $i \in \mathbb{H}$, però veiem que $qi = -b + ai + dj - ck$ i que $iq = -b + ai - dj + ck$, per tant, per a que $qi = iq$, c i d han de ser zero.
Ara tenim $q = a + bi$ que si que commuta amb i, però per a que q sigui del centre de $\mathbb{H}$ també ha de commutar amb j, ja que $j \in \mathbb{H}$. Veiem que $qj = aj + bk$ i que $jq = aj - bk$, per tant per a que $qj = jq$, b també ha de ser zero.
Veiem doncs que els únics elements que commuten amb tots els elements de $\mathbb{H}$ són els de la forma $q = a$ amb $a \in \mathbb{R}$. Per tant tenim que el centre de $\mathbb{H}$ és $\mathbb{R}$.

Ara que hem vist que $\mathbb{H}$ és un anell i que $\mathbb{R}$ és el centre de $\mathbb{H}$, veurem que $\mathbb{H}$ és una àlgebra sobre $\mathbb{R}$.

Sigui K un cos, i sigui A un espai vectorial sobre K proveït amb una operació binària addicional de $A \times A$ a A, notada aquí per $\cdot$ (és a dir si x i y són dos elements qualssevol de A, $x \cdot y$ és el producte de x i y). Llavors A és una àlgebra sobre K si les identitats següents es compleixen per a tres elements qualssevol $x, y, z \in A$, i tots els elements ("escalars") $a, b \in K$:

1. Propietat distributiva per l'esquerra: $(x + y) \cdot z = x \cdot z + y \cdot z$
2. Propietat distributiva per la dreta: $x \cdot (y + z) = x \cdot y + x \cdot z$
3. Compatibilitat amb escalars: $(ax) \cdot (by) = (ab)(x \cdot y)$.

Com que $\mathbb{H}$ és un anell, els punts 1 i 2 es compleixen per a qualssevol tres quaternions $\alpha, \beta, \gamma \in \mathbb{H}$.
Siguin $a, b \in \mathbb{R}$, i $\alpha, \beta \in \mathbb{H}$, hem vist que els elements de $\mathbb{R}$ commuten amb tot element de $\mathbb{H}$, per tant és fàcil veure que es compleix que $(a\alpha) \cdot (b\beta) = (ab)(\alpha \cdot \beta)$.
Per tant, tenim que $\mathbb{H}$ és una àlgebra sobre $\mathbb{R}$.

Seguim doncs amb les següents definicions de les propietats dels quaternions:

Definició 2.4. *Sigui $q = a + bi + cj + dk$ un quaternió, el seu conjugat $\overline{q}$ es defineix com:*

$$\overline{q} = a - bi - cj - dk.$$

Es compleixen les següents propietats: $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$, $\overline{q_1 q_2} = \overline{q_2 q_1}$, $\overline{\overline{q}} = q$.

Definició 2.5. *Sigui $q = a + bi + cj + dk$ un quaternió, definim la seva norma com*

$$N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2.$$

Com que $\overline{q_1 q_2} = \overline{q_2 q_1}$, la norma és multiplicativa:

$$N(q_1 q_2) = q_1 q_2 \overline{q_1 q_2} = q_1 q_2 \overline{q_2 q_1} = q_1 N(q_2) \overline{q_1} = q_1 \overline{q_1} N(q_2) = N(q_1) N(q_2).$$

Sigui q un quaternió, si $q \neq 0$, llavors $N(q) > 0$, de manera que $\frac{\overline{q}}{N(q)}$ és un invers de q pels dos costats:

$$q \frac{\overline{q}}{N(q)} = \frac{\overline{q}}{N(q)} q = \frac{N(q)}{N(q)} = 1.$$

Definició 2.6. *Un anell A en el qual cada element no nul té invers pels dos costats pel producte, s'anomena anell de divisió. En aquest cas, $A^\times = A - \{0\}$ és un grup amb el producte.*

Observem que, tal com hem vist, $\mathbb{H}$ és un anell de divisió.

Teorema 2.7 (Teorema de Frobenius)**.** *Sigui D una àlgebra de divisió sobre $\mathbb{R}$. Aleshores, com a $\mathbb{R}$-àlgebra, D és isomorf a $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$.*

Demostració. Suposem $dim_{\mathbb{R}} D \geq 2$ (en cas contrari tindriem $D = \mathbb{R}$).
Agafem $\alpha \in D \backslash \mathbb{R}$. Aleshores $\mathbb{R}[\alpha]$ és una extensió algebràica de $\mathbb{R}$, per tant $\mathbb{R}[\alpha] \cong \mathbb{C}$.
Denotem el nombre complex $\sqrt{-1} \in \mathbb{C}$ com i. Definim els subespais

$$D^+ = d \in D : di = id \supseteq \mathbb{C},$$

$$D^- = d \in D : di = -id.$$

D^+ I d^- són $\mathbb{C}$-subespais de ${}_{\mathbb{C}}D$ amb $D^+ \cap D^- = 0$. Afirmem que $D^+ \oplus D^- = D$.
De fet, si $a \in D$, és fàcil veure que $d^+ := ia + ai \in D^+$, i $d^- := ia - ai \in D^-$.

Com que $d^+ + d^- = 2ia$, tenim que $a = (2i)^{-1}(d^+ + d^-) \in D^+ + D^-$.
Per tot $d^+ \in D^+$, $\mathbb{C}[d^+]$ és una extensió algebraica de $\mathbb{C}$, per tant, ha de ser $\mathbb{C}$ el que mostra que $D^+ = \mathbb{C}$. Si $D^- = 0$ ja tenim que $D \cong \mathbb{C}$.
Suposem doncs que $D^- \neq 0$. Fixem un element $z \in D^- \backslash \{0\}$. Aleshores l'aplicació $\mathbb{C}$-lineal

$$\mu : D^- \to D^+ \quad \mu(x) = xz$$

és injectiva. Com que $dim_{\mathbb{C}} D^+ = 1$, es segueix que $dim_{\mathbb{C}} D^- = 1$, i per tant $dim_{\mathbb{R}} D = 2dim_{\mathbb{C}} D = 4$.
L'element z és algebraic sobre $\mathbb{R}$ per tant $z^2 \in \mathbb{R} + \mathbb{R}z$. Per altra banda, $z^2 = \mu(z) \in D^+ = \mathbb{C}$, per tant $z^2 \in \mathbb{C} \cap (\mathbb{R} + \mathbb{R}z) = \mathbb{R}$.
Si $z^2 > 0$ a $\mathbb{R}$, podem escriure $z^2 = r^2$ per algun $r \in \mathbb{R}$; això ens porta a que $z = \pm r \in \mathbb{R}$, i per tant tenim una contradicció. Per tant, hem de tenir $z^2 < 0$ en $\mathbb{R}$, i podem escriure $z^2 = -r^2$ per algun $r \in \mathbb{R}^*$. Sigui $j = \frac{z}{r}$, tenim que $j^2 = -1 = i^2$, $ji = -ij$, i $D = \mathbb{C} \oplus \mathbb{C}j = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}ij$, per tant D és una copia dels quaternions de Hamilton. □

2.2 Àlgebres de quaternions generals

En aquest apartat definirem una generalització dels quaternions de Hamilton, on es permeten coeficients en cossos més generals que $\mathbb{R}$, i veurem que els quaternions que tenen norma diferent de zero tenen un invers multiplicatiu pels dos costats.

Sigui F un cos. Els quaternions de Hamilton es poden generalitzar com:

$$\mathbb{H}(F) = \{a + bi + cj + dk : a, b, c, d \in F\}.$$

Amb $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$

Si la característica de F no és 2, aleshores el centre de $\mathbb{H}(F)$ és F.

A partir d'ara, assumim que F no té característica 2.

Ara, anirem un pas més enllà, i definirem àlgebres de quaternions més generals.

Definició 2.8. *Una àlgebra de quaternions sobre F és un anell sobre F amb base $1, u, v, w$ tal que: $u^2 \in F^\times$, $v^2 \in F^\times$, $w = uv = -vu$, i tot $c \in F$ commuta amb u i v. El denotem per $(a, b)_F$ quan $a = u^2$ i $b = v^2$.*

La taula següent mostra els productes de u, v i w a $(a, b)_F$.

	u	v	w
u	a	w	av
v	$-w$	b	$-bu$
w	$-av$	bu	$-ab$

Exemple 2.9. Observem que amb aquesta notació, $\mathbb{H}(F) = (-1,-1)_F$, així que aquesta és una àlgebra de quaternions on $a = b = -1$.

Com que F no té característica 2, $(a,b)_F$ no és commutativa perquè u i v no commuten. El centre de $(a,b)_F$ és F. Per a $q = x_0 + x_1u + x_2v + x_3w$, definim el conjugat de q com

$$\overline{q} = x_0 - x_1u - x_2v - x_3w,$$

i la norma de q com

$$N(q) = q\overline{q} = x_0^2 - ax_1^2 - b_2^2 + abx_3^2.$$

Com hem vist per $\mathbb{H}$, en $(a,b)_F$ també es compleix que $\overline{q}q = q\overline{q}$, $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$, $\overline{q_1q_2} = \overline{q_2q_1}$, $\overline{\overline{q}} = q$ i que $N(q_1q_2) = N(q_1)N(q_2)$. Per tant tenim que la norma és una funció multiplicativa $(a,b)_F \to F$.

Teorema 2.10. *Sigui $q \in (a,b)_F$. Té un invers multiplicatiu pels dos costats en $(a,b)_F$ si i només si $N(q) \neq 0$.*

Demostració. Suposem $qq' = 1$ per algun q'. Aleshores $N(q)N(q') = N(qq') = N(1) = 1$ en $F^\times$, i per tant $N(q) \in F^\times$. D'altra banda, suposem $N(q) \in F^\times$. Com que $N(q)$ commuta amb tots els elements de $(a,b)_F$, podem escriure $N(q) = q\overline{q} = \overline{q}q$ com

$$q \cdot \frac{1}{N(q)}\overline{q} = \frac{1}{N(q)}\overline{q} \cdot q = 1,$$

així doncs $\frac{\overline{q}}{N(q)}$ és un invers multiplicatiu en ambdós costats de q. □

Els quaternions de Hamilton són de divisió. Ens podem preguntar si això sempre és cert també per $(a,b)_F$. Veurem que en general no, però en alguns casos sí com ara el següent:

Teorema 2.11. *Sigui a un enter i sigui p un primer senar tal que a no és un quadrat modul p. Aleshores $(a,p)_\mathbb{Q}$ és un anell de divisió.*

Demostració. Pel teorema anterior, per veure que $(a,p)_\mathbb{Q}$ és un anell de divisió és suficient veure que tot element diferent de zero de $(a,p)_\mathbb{Q}$ té norma diferent de zero.
Provarem que: Un element de $(a,p)_\mathbb{Q}$ amb norma 0 ha de ser el 0.
Sigui $q = x_0 + x_1u + x_2v + x_3w$ en $(a,p)_\mathbb{Q}$. Aleshores

$$N(q) = x_0^2 - ax_1^2 - px_2^2 + apx_3^2,$$

Si $N(q) = 0$, aleshores $x_0^2 - ax_1^2 - px_2^2 + apx_3^2 = 0$, i per tant $x_0^2 - ax_1^2 = p(x_2^2 - ax_3^2)$.
Podem assumir $x_0, x_1, x_2, x_3 \in \mathbb{Z}$. Si reduim $\mod p$, tenim $x_0^2 - ax_1^2 \equiv 0 \mod p$, i per tant $x_0^2 \equiv ax_1^2 \mod p$. Si $x_1 \not\equiv 0$ mod p aleshores $a \equiv \square$ mod p. (on $\square$ es refereix a un element de la forma x^2). Per tant $x_1 \equiv 0 \mod p$, aleshores $x_0^2 \equiv 0 \mod p$, i per tant

$x_0 \equiv 0 \mod p$.
Llavors veiem que $x_0^2 - ax_1^2 = p(x_2^2 - ax_3^2, x_0^2 - ax_1^2)$ és divisible per p^2, i per tant $x_2^2 - ax_3^2 \equiv 0 \mod p$.
Pel mateix argument utilitzat anteriorment, veiem que x_2 i x_3 són divisibles per p. Com que cada x_i és divisible per p, escrivim $x_i = px_i'$ amb $x_i' \in \mathbb{Z}$.
Aleshores tenim que $x_0^2 - ax_1^2 = p(x_2^2 - ax_3^2)$, que implica $p^2(x_0'^2 - ax_1'^2) = p(p^2)(x_2'^2 - ax_3'^2)$, i per tant $x_0'^2 - ax_1'^2 = p(x_2'^2 - ax_3'^2)$. Com que cada x_i' és divisible per p, aleshores x_i és divisible per p^2.
Repetint l'argument, es veu que x_i és divisible per valors arbitràriament grans de p, així doncs, cada x_i ha de ser 0. □

2.3 Isomorfismes entre àlgebres de quaternions

En aquest apartat, definirem què és una base quaterniònica, quan diem que una àlgebra de quaternions és trivial o escindida, i estudiarem els isomorfismes que existeixen entre les àgebres de quaternions.

Un isomorfisme entre dues àlgebres de quaternions A i A' sobre un cos F és un isomorfisme d'anells $f : A \to A'$ que fixa els elements de F.

Definició 2.12. *Una base de $(a,b)_F$ de la forma $\{1, e_1, e_2, e_1e_2\}$ on $e_1^2 \in F^\times$, $e_2^2 \in F^\times$ i $e_1e_2 = -e_2e_1$ s'anomena base quaterniònica de $(a,b)_F$.*

Teorema 2.13. *Per tot $a \in F^\times$, $(a,1)_F \cong M_2(F)$.*
L'anell $M_2(F)$ és una àlgebra de quaternions sobre F i $(a,c^2)_F \cong (a,-a)_F \cong M_2(F)$.

Demostració. Enviem la base $1, u, v, w$ de $(a,1)_F$ a $M_2(F)$ de la següent manera:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, u \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, v \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, w \mapsto \begin{pmatrix} 0 & -1 \\ a & 0 \end{pmatrix}.$$

Com que $1 \neq -1$ en F, 1 i v no s'envien a la mateixa matriu. Estenem aquesta correspondència per linealitat a una funció $(a,b)_F \to M_2(F)$:

$$x_0 + x_1u + x_2v + x_3w \mapsto \begin{pmatrix} x_0 + x_2 & x_1 - x_3 \\ a(x_1 + x_3) & x_0 - x_2 \end{pmatrix}.$$

La imatge de $1, u, v, w$ a $M_2(F)$ és un conjunt linealment independent, per tant $(a,b)_F \mapsto M_2(F)$ és una bijecció. Fixa F en el sentit que $c \in F$ en $(a,b)_F$ va a cI_2 en $M_2(F)$.

Ara veurem que $(a,c^2)_F \cong (a,-a)_F \cong M_2(F)$.
En primer lloc considerem l'àlgebra $(a,c^2)_F$ definida per $1, u, v, w$ amb les relacions:

$$u^2 = a, \quad v^2 = c^2, \quad uv = -vu = w.$$

Substituim $v = cv'$, on v' és un nou generador. Aleshores, $v^2 = (cv')^2 = c^2(v')^2$. Per tant, podem definir v' de tal manera que $(v')^2 = 1$. Si agafem $v'^2 = -1$, obtenim:

$$(cv')^2 = c^2(v')^2 = c^2(-1) = -c^2.$$

Si $c \neq 0$, $v' = \frac{v}{c}$ compleix que:

$$(v')^2 = \left(\frac{v}{c}\right)^2 = \frac{v^2}{c^2} = \frac{c^2}{c^2} = -1.$$

Aleshores, al redefinir els generadors amb v', l'àlgebra $(a, c^2)_F$ es pot escriure com: $(a, c^2)F \cong (a, -a)F$, on els nous generadors u i v satisfan:

$$u^2 = a, \quad (v')^2 = -a, \quad uv' = -v'u.$$

Considerem ara l'àlgebra $(a, -a)_F$ definida per:

$$u^2 = a, \quad v^2 = -a, \quad uv = -vu = w.$$

Enviem la base $1, u, v, w$ de $(a, -a)_F$ a $M_2(F)$ de la següent manera:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, u \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, v \mapsto \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix}, w \mapsto \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

Observem que:

$$u^2 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI,$$

$$v^2 = \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -a & 0 \\ 0 & -a \end{pmatrix} = -aI,$$

$$uv = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} = -vu,$$

Per tant, tenim un isomorfisme $(a, -a)_F \cong M_2(F)$.

□

Definició 2.14. *Direm que $M_2(F)$ o una àlgebra de quaternions isomorfa a $M_2(F)$, és una àlgebra de quaternions trivial o escindida sobre F si $(a, b)_F \cong M_2(F)$*

Definició 2.15. *Per a i b en $\mathbb{Q}^\times$ direm que $(a, b)_\mathbb{Q}$ escindeix sobre $\mathbb{R}$ si $(a, b)_\mathbb{R} \cong M_2(\mathbb{R})$ i direm que $(a, b)_\mathbb{Q}$ no escindeix sobre $\mathbb{R}$ si $(a, b)_\mathbb{R} \ncong M_2(\mathbb{R})$.*

Lema 2.16. *Per $a \in F^\times$, el conjunt dels elements no nuls de la forma $x^2 - ay^2$ amb $x, y \in F$ és un subrgrup de $F^\times$.*

Demostració. El nombre 1 és de la forma $x^2 - ay^2$ amb $x = 1, y = 0$. Els nombres d'aquesta forma són tancats sota multiplicació ja que

$$(x_1^2 - ay_1^2)(x_2^2 - ay_2^2 = (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2.$$

Els nombres no nuls d'aquesta forma són tancats sota inversió utilitzant la identitat $\frac{1}{t} = \frac{t}{t^2}$:

$$\frac{1}{x^2 - ay^2} = (\frac{x}{x^2 - ay^2})^2 - a(\frac{y}{x^2 - ay^2})^2.$$

□

Definició 2.17. *Per $a \in F^\times$, anomenem $N_a = N_a(F)$ al conjunt d'elements no nuls de la forma $x^2 - ay^2$ amb $x, y \in F^\times$.*

Teorema 2.18. *Si a és un quadrat en F aleshores $N_a = F^\times$.*

Demostració. Escrivim $a = c^2$ per $c \in F^\times$. Aleshores tenim que $x^2 - c^2y^2 = x^2 - (cy)^2 = (x - cy)(x + cy)$. Fem els canvis de variables $x' = x - cy$ i $y' = x + cy$ que són invertibles ($x = (x' + y')/2$ i $y = (y' - x')/(2c)$), aleshores tenim que $N_a = \{x'y' : x', y' \in F^\times\}$, que assumeix tots els valors a $F^\times$ triant $y' = 1$. □

Teorema 2.19. *Si $b \in N_a$ aleshores $(a, b)_F \cong M_2(F)$.*

Demostració. Escrivim $b = x_0^2 - ay_0^2$ amb $x_0, y_0 \in F$. L'anell $(a, b)_F$ té una base quaterniònica

$$1, u, x_0v + y_0w, u(x_0v + y_0w).$$

El quart terme és $ay_0v + x_0w$ i el canvi de base de v, w a $x_0v + y_0w$, $ay_0v + x_0w$ té determinant $\begin{vmatrix} x_0 & y_0 \\ ay_0 & x_0 \end{vmatrix} = b \neq 0$. Per tant, l'anterior conjunt de quatre elements de $(a, b)_F$ és linealment independent sobre F i per tant és una base de $(a, b)_F$.
Tenim $(x_0v + y_0w)^2 = bx_0^2 - aby_0^2 = b^2$, i u i $x_0v + y_0w$ anticommuten. Per tant, com que $b \in N_a$ tenim que $(a, b)_F \cong (a, b^2)_F \cong (a, 1)_F \cong M_2(F)$. Per tant, és una base quaterniònica. □

Teorema 2.20. *Una àlgebra de quaternions $(a, b)_F$ que no és un anell de divisió, és isomorfa a $M_2(F)$.*

Demostració. Com que sabem que $(c^2, b)_F \cong M_2(F)$, podem assumir que a no és un quadrat a F. Pel Teorema 2.10, si $(a, b)_F$ no és un anell de divisió aleshores conté un element no nul q tal que $N(q) = 0$.
Siqui $q = x_0 + x_1u + x_2v + x_3w$ tal que els seus coeficients són diferents de zero, tenim que $N(q) = 0$ implica que $x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = 0$, i per tant $x_0^2 - ax_1^2 = b(x_2^2 - ax_3^2)$. Com que a no és un quadrat en F, aleshores $x_2^2 - ax_3^2 \neq 0$. Per contradicció: Si $x_2^2 - ax_3^2 = 0$

aleshores $x_3 = 0$ (ja que a no és un quadrat en F), i per tant, també $x_2 = 0$, el que implica que $x_0^2 - ax_1^2 = 0$, per tant $x_1 = 0$ i $x_0 = 0$, però aleshores $q = 0$.
Resolent per b,

$$b = \frac{x_0^2 - ax_2^2}{x_2^2 - ax_3^2} \in N_a,$$

per tant, $(a, b)_F \cong M_2(F)$ pel Teorema 2.19. □

Teorema 2.21. *Per $a, b \in F$, $(a, b)_F \cong M_2(F)$ si i només si $b \in N_a$.*

Demostració. Pel Teorema 2.19, si $b \in N_a$ aleshores $(a, b)_F \cong M_2(F)$.
Per l'altra banda, suposem que $(a, b)_F \cong M_2(F)$. Per veure que $b \in N_a$ podem assumir que a no és un quadrat en $F^\times$, ja que si a fos un quadrat, pel Teorema 2.17, tindriem que $N_a = F^\times$, per tant $b \in N_a$. Quan $(a, b)_F$ no és un anell de divisió i a no és un quadrat, la demostració del Teorema 2.19 mostra que $b \in N_a$. □

Corolari 2.22. *Sigui F un cos de característica $\neq 2$, $\mathbb{H}(F)$ és un anell de divisió si i només si -1 no és la suma de dos quadrats en F.*

Demostració. Provarem que les negacions de les dues condicions són equivalents.
Si $\mathbb{H}(F)$ no és un anell de divisió, aleshores $H(F) \cong M_2(F)$, i pel Teorema 2.20, $(-1, -1)_F \cong M_2(F)$ si i només si $-1 = x^2 - (-1)y^2 = x^2 + y^2$ per algun $x, y \in F$. □

Corolari 2.23. *Per cada primer senar p, tota àlgebra de quaternions sobre $\mathbb{F}_p$ és isomorfa a $M_2(\mathbb{F}_p)$.*

Demostració. Veurem que per a tot $a, b \in \mathbb{F}_p$ no nuls existeixen $x, y \in \mathbb{F}_p$ tal que $b = x^2 - ay^2$.
Escrivim l'equació $b = x^2 - ay^2$ com $b + ay^2 = x^2$. El nombre total de quadrats en $\mathbb{F}_p$ és $(p + 1)/2$, així doncs, $|\{x^2 : x \in \mathbb{F}_p\}| = (p + 1)/2$, i com que $a \neq 0$, també tenim que $|\{b + ay^2 : y \in \mathbb{F}_p\}| = (p + 1)/2$. Si l'equació $b + ay^2 = x^2$ no té solució a $\mathbb{F}_p$, aleshores $\{x^2\}$ i $\{b + ay^2\}$ serien subconjunts disjunts de $\mathbb{F}_p$, però la suma dels seus cardinals és $\frac{(p+1)}{2} + \frac{(p+1)}{2} = p + 1 > \mathbb{F}_p$, així que tenim una contradicció. Per tant existeixen algun x i algun y en $\mathbb{F}_p$ tal que $b + ay^2 = x^2$. □

2.4 Isomorfismes i normes

En aquesta secció donarem alguns criteris per detectar isomorfismes entre certes àlgebres de quaternions.

Teorema 2.24. *Siguin $a, b, b' \in F^\times$. Aleshores, $(a, b)_F \cong (a, b')_F$ si i només si $\frac{b}{b'} \in N_a$.*

Demostració. ($\Leftarrow$) Suposem $\frac{b'}{b} = x_0^2 - ay_0^2$ per algun $x_0, y_0 \in F$. Sigui $\{1, u, v, uv\}$ la base quaterniònica habitual de $(a, b')_F$. Tenim que $1, u, x_0v + y_0w, u(x_0v + y_0w)$, és també una base quaterniònica de $(a, b')_F$. Com que $u^2 = a$ i $(x_0v+y_0w)^2 = b'x_0^2-ab'y_0^2 = b'(b/b') = b$,

tenim que $(a,b')_F \cong (a,b)_F$.
($\Rightarrow$) Per veure que $(a,b)_F \cong (a,b')_F$ implica que $b/b' \in N_a$, les àlgebres de quaternions isomorfes $(a,b)_F$ i $(a,b')_F$ són o bé les dues anells de divisió o bé cap de les dues és anell de divisió.
Primer suposem que $(a,b)_F$ i $(a,b')_F$ no són anells de divisió, de manera que són isomorfes a $M_2(F)$. Llavors $b \in N_a$ i $b' \in N_a$. Com que N_a és un subgrup de $F^\times$, $\frac{b}{b'} \in N_a$.
Suposem ara que $(a,b)_F$ i $(a,b')_F$ són anells de divisió, en particular a no és un quadrat en F. Sigui $\{1,u,v,uv\}$ la base quaterniònica estàndard de $(a,b')_F$, és a dir,

$$u^2 = a, v^2 = b', uv = -vu.$$

Com que $(a,b')_F \cong (a,b)_F$, $(a,b')_F$ conté una base quaterniònica $\{1,u_0,v_0,u_0v_0\}$ on $u_0^2 = a$, $v_0^2 = b$, $u_0v_0 = -v_0u_0$.
El polinomi $T^2 - a$ és irreductible sobre F ja que a no és un quadrat en F, i tant u com u_0 són arrels del polinomi en $(a,b')_F$, per tant $u = qu_0q^{-1}$ per algun $q \in (a,b')_F$ no nul. Definim $\widetilde{v} = qv_0q^{-1}$, de manera que $\widetilde{v}^2 = (qv_0q^{-1})(qv_0q^{-1}) = qv_0^2q^{-1} = qbq^{-1} = b$. Llavors $u_0v_0 = -v_0u_0$ implica que $(qu_0q^{-1})(qv_0q^{-1}) = -(qv_0q^{-1})(qu_0q^{-1})$ i per tant $u\widetilde{v} = -\widetilde{v}u$. Els elements de $(a,b')_F$ que anticommuten amb u són $Fu + Fw$, així $\widetilde{v} = xv + yw$ per algun x, y en F.
Llavors $b = \widetilde{v}^2 = (xv+yw)^2 = b'x^2 - b'ay^2 = b'(x^2 - ay^2)$ implica que $\frac{b}{b'} \in N_a$. □

Corołari 2.25. *Siguin p i q dos primers diferents congruents amb* 3 mod 4. *Aleshores, $(-1,p)_\mathbb{Q}$ no és isomorf a $(-1,q)_\mathbb{Q}$.*

Demostració. Si $(1,p)_\mathbb{Q} \cong (-1,q)_\mathbb{Q}$ aleshores $q/p = x^2 + y^2$ per alguns nombres racionals x i y. Escrivim x i y amb un denominador comú: $x = \frac{m}{d}$, $y = \frac{n}{d}$ amb m,n enters i $d \neq 0$. Aleshores $qd^2 = p(m^2+n^2)$.
Com que $p \neq q$ aleshores $m^2 + n^2 \equiv 0 \mod q$. Això implica que m i n són divisibles per q (ja que $-1 \mod q$ no és un quadrat), per tant qd^2 és divisible per q^2, i per tant $q|d$. En l'equació $qd^2 = p(m^2+n^2)$, m,n i d són tots divisibles per q, de manera que podem dividir per q^2 i obtenir una equació similar on m,n i d són substituïts per m/q, n/q i d/q. Repetint això infinitament, d és divisible per potències arbitràriament altes de q, la qual cosa és una contradicció. □

Teorema 2.26. *Si $f : A_1 \to A_2$ és un isomorfisme d'àlgebres de quaternions sobre F, aleshores tenim que $\overline{f(q)} = f(\overline{q})$ per a tot $q \in A_1$. En particular, $N(f(q)) = N(q)$.*

Demostració. Un cop haguem vist que $\overline{f(q)} = f(\overline{q})$ per tot $q \in A_1$, tindrem que $N(f(q)) = f(q)\overline{f(q)} = f(q)f(\overline{q}) = f(q\overline{q}) = f(N(q)) = N(q)$ ja que $N(q) \in F$ i f fixa tots els elements de F.
Escrivim $q = x_0 + q_0$ on $x_0 \in F$ i q_0 és un quaternió pur en A_1. Aleshores $f(\overline{q}) = f(x_0 - q_0) = x_0 - f(q_0)$.
Mostrarem que $f(q_0)$ és un quaternió pur en A_2. Això és evident si $q_0 = 0$, així que

suposem $q_0 \neq 0$. Com que q_0 és pur en A_1 tenim que $q_0^2 \in F$, així que també $f(q_0^2) \in F$. Aleshores o bé $f(q_0)$ és pur o bé $f(q_0) \in F$. No pot passar que $f(q_0) \in F$ ja que $f(F) = F$, f és injectiva, i $q_0 \notin F$ (l'únic quaternió pur a F és 0). Així que $f(q_0)$ és pur, de manera que $\overline{f(q_0)} = -f(q_0)$, per tant tenim que

$$f(\overline{q}) = x_0 + \overline{f(q_0)} = \overline{x_0 + f(q_0)} = \overline{f(x_0 + q_0)} = \overline{f(q)}.$$

□

Corołari 2.27. *Si A_1 i A_2 són àlgebres de quaternions isomorfes sobre F llavors les aplicacions norma $A_1 \to F$ i $A_2 \to F$ tenen la mateixa imatge.*

Demostració. Això és immediat de $N(q) = N((f(q))$ per a un isomorfisme $f : A_1 \to A_2$. □

3 Quaternions de Hurwitz

En aquest estudiarem un subanell dels quaternions de Hamilton que en cert sentit juga un paper anàleg a $\mathbb{Z}$.

3.1 Quaternions de Hurwitz

Direm que un quaternió de Hamilton $\alpha = a + bi + cj + dk$ és un enter de Lipschitz quan $a, b, c, d \in \mathbb{Z}$.

Els enters de Gauss (els nombres complexos de la forma $x + iy$ en que les seves parts real i imaginària són enters) tenen la propietat de la "divisió amb residu petit", és a dir, que qualsevol enter de Gauss d pot ser dividit per qualsevol enter diferent de zero z, per tal de tenir un quocient enter de Gauss q i un residu r estrictament més petit que el divisor.
Si d i $z \neq 0$ són quaternions de Lipzschitz amb $q = dz^{-1} = a + bi + cj + dk$, i siguin a', b', c', d' els enters de Gauss més propers a a, b, c, d, definim $q' = a' + b'i + c'j + d'k$ i $r = d - qz$, aleshores veiem que $N(rz^{-1}) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 + (\frac{1}{2})^2 + (\frac{1}{2})^2 = 1$, però aleshores tenim que la norma del residu r no és estrictament més petita que la norma del divisor z.

A partir d'ara treballarem amb els quaternions de Hurwitz, que definirem en aquest apartat. Aquests quaternions si que tenen la propietat de "divisió amb residu petit", (ho demostrarem a l'apartat 4), i això fa que sigui més fàcil treballar amb quaternions de Hurwitz que amb quaternions de Lipzschitz.

Definició 3.1. *Direm que un quaternió $\alpha = a + bi + cj + dk$ és de Hurwitz si a, b, c, d són tots enters racionals o són tots semienters.*

Definició 3.2. *Anomenem conjugat de α al quaternió $\overline{\alpha} = a - bi - cj - dk$, i norma de α a $N(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = a^2 + b^2 + c^2 + d^2$.*

Proposició 3.3. *La norma de tot quaternió de Hurwitz és un enter racional.*

Demostració. Sigui $\alpha = a + bi + cj + dk$ un quaternió de Hurwitz, la seva norma és: $N(\alpha) = a^2 + b^2 + c^2 + d^2$.
Sabem que a, b, c, d són o bé tots enters, o bé tots semienters.
Si $a, b, c, d \in \mathbb{Z}$, aleshores $N(\alpha)$ serà la suma de quatre enters al quadrat, per tant, serà un enter.
Si $a, b, c, d \in \mathbb{Z}+\frac{1}{2}$, escrivim $a = a' + \frac{1}{2}, b = b' + \frac{1}{2}, c = c' + \frac{1}{2}, d = d' + \frac{1}{2}$, on a', b', c', d' són les parts enteres de a, b, c, d. Aleshores tenim que $N(\alpha) = a'^2 + \frac{1}{4} + b'^2 + \frac{1}{4} + c'^2 + \frac{1}{4} + d'^2 + \frac{1}{4} = a'^2 + b'^2 + c'^2 + d'^2 + 1$ que evidentment, és un enter. □

Definició 3.4. *Direm que α és un quaternió de Hurwitz senar si la seva norma és un enter racional senar, i direm que és un quaternió de Hurwitz parell si la seva norma és un enter racional parell.*

Al segon apartat, hem vist que els quaternions de Hamilton tenen norma multiplicativa i un invers pels dos costats, veiem-ho ara també pels quaternions de Hurwitz:

El conjugat dels quaternions de Hurwitz compleix que $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, per tant, la norma és multiplicativa: $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha}N(\beta) = N(\alpha)N(\beta)$.

Definim α^{-1}, quan $\alpha \neq 0$, com $\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$, i per tant $\alpha\alpha^{-1} = \alpha\frac{\overline{\alpha}}{N(\alpha)} = \frac{\overline{\alpha}}{N(\alpha)}\alpha = \alpha^{-1}\alpha = 1$.

Definició 3.5. *Si α i α^{-1} són tots dos quaternions de Hurwitz, diem que α és una unitat.*

Proposició 3.6. *Un quaternió de Hurwitz és una unitat si i només si té norma 1.*

Demostració. Sigui α una unitat, com que $\alpha\alpha^{-1} = 1$, $N(\alpha)N(\alpha^{-1}) = 1$ i per tant $N(\alpha) = 1$.
D'altra banda, si α és de Hurwitz i $N(\alpha) = 1$, aleshores $\alpha^{-1} = \overline{\alpha}$ també és de Hurwitz. Per tant α és una unitat □

Teorema 3.7. *Hi ha exactament 24 unitats de Hurwitz, $\pm 1, \pm i, \pm j, \pm k, \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$.*

Demostració. Sigui $q = a + bi + cj + dk$ una unitat de Hurwitz, aleshores per definició té norma 1. Per tant, $a^2+b^2+c^2+d^2 = 1$, com que q és de Hurwitz, aleshotes o bé $a, b, c, d \in \mathbb{Z}$, o bé $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$. Si $|a|, |b|, |c|, |d|$, són tots enters l'equació $a^2 + b^2 + c^2 + d^2 = 1$ implica que una de les coordenades ha de ser ± 1 i la resta ha de ser 0. En cas contrari, tenim que $|a|, |b|, |c|, |d|$ són meitats d'enters, i com que $a^2 + b^2 + c^2 + d^2 = 1$, totes han de ser $\pm\frac{1}{2}$. □

Si escrivim

$$\rho = \frac{1}{2}(1 + i + j + k),$$

aleshores qualsevol quaternió de Hurwitz es pot expresar de la forma

$$l_0\rho + l_1 i + l_2 j + l_3 k,$$

on l_0, l_1, l_2, l_3 són enters racionals; i qualsevol quaternió d'aquesta forma és un quaternió de Hurwitz.

Proposició 3.8. *La suma de dos quaternions de Hurwitz és un quaternió de Hurwitz.*

No farem la demostració ja que és fàcil de veure però si que demostrarem la proposició següent.

Proposició 3.9. *El producte de dos quaternions de Hurwitz és un quaternió de Hurwitz.*

Demostració. Siguin $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ i $\beta = b_0 + b_1 i + b_2 j + b_3 k$ dos quaternions de Hurwitz, aleshores $\alpha\beta = a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3 + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i + (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1)j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0)k$.
Ens fixem amb el coeficient del terme i que és $a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2$. Recordem que com que α i β són quaternions de Hurwitz, totes les coordenades a_l i b_g són o bé totes enteres, o bé totes semienteres.
Si totes les coordenades són enteres, aleshores el producte i suma de nombres enters també dona com a resultat un nombre enter, i per tant el coeficient de i també serà un enter.
Si totes les coordenades són semienteres, aleshores cada producte $a_0 b_1$, $a_1 b_0$, $a_2 b_3$, $a_3 b_2$ és de la forma $\frac{n}{2} \cdot \frac{m}{2} = \frac{nm}{4}$ on n i m són enters. La suma i resta de quatre nombres d'aquesta forma, resulta en un nombre de la forma $\frac{t}{2}$, on t és un enter.

Similarment es pot veure que els coeficients real, del terme j i del terme k també seran o bé enters o bé semienters. Per tant hem vist que el producte de dos quaternions de Hurwitz és un quaternió de Hurwitz. □

Definició 3.10. *Donat un quaternió α, un associat de α és un quaternió de la forma $\epsilon\alpha$ o $\alpha\epsilon$, per alguna unitat ϵ.*

Els associats tenen normes iguals, i els associats d'un quaternió de Hurwitz, també són quaternions de Hurwitz.

Si $\gamma = \alpha\beta$, aleshores diem que α és un divisor per l'esquerra de γ i que β és un divisor per la dreta de γ.

Definició 3.11. *Direm que dos quaternions de Hurwitz α i β tenen un màxim comú divisor per la dreta δ si:*

1. *δ és un divisor per la dreta de α i de β,*
2. *Tot divisor per la dreta de α i β és també un divisor per la dreta de δ*

A l'apartat 4, demostrarem que el màxim comú divisor existeix i és únic.

Definició 3.12. *Direm que un conjunt S de quaternions de Hurwitz, un dels quals és diferent de 0, és un ideal per la dreta si té les següents propietats:*

1. *$\alpha \in S$, $\beta \in S$ implica que $\alpha \pm \beta \in S$,*
2. *$\alpha \in S$ implica que $\lambda\alpha \in S$ per qualsevol quaternió de Hurwitz λ.*

Sigui δ qualsevol quaternió de Hurwitz i S el conjunt $(\lambda\delta)$ de tots els múltiples per l'esquerra de δ per quaternions de Hurwitz λ, aleshores és clar que S és un ideal per la dreta.

Definició 3.13. *Direm que un quaternió de Hurwitz π, que no sigui una unitat, és primer si els seus únics divisors són les unitats i els seus associats.*

Es compleix que tots els associats d'un primer són primers.

Si $\pi = \alpha\beta$, aleshores $N\pi = N\alpha N\beta$, per tant π és primer si $N\pi$ és un primer racional.

A l'apartat 4, provarem que el contrari és cert.

4 El Teorema dels quatre quadrats

En aquest apartat, demostrarem el Teorema dels quatre quadrats de Lagrange.

Teorema 4.1 (Teorema dels quatre quadrats de Lagrange)**.** *Tot enter positiu pot ser representat com una suma de quatre quadrats enters no negatius . És a dir, els quadrats formen una base additiva d'ordre quatre:* $p = a^2 + b^2 + c^2 + d^2$*, amb* $a, b, c, d \in \mathbb{Z}$*.*

Veurem que per a demostrar aquest Teorema, és suficient demostrar que *Tot primer es pot representar com la suma de quatre quadrats.*

La identitat dels quatre quadrats d'Euler afirma que $(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2$.

Per donar una intuició de que aquesta identitat és certa, considerem els nombres: a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 com a nombres reals, aleshores podem crear els quaternions $\alpha = a_1 + a_2i + a_3j + a_4k$ i $\beta = b_1 + b_2i + b_3j + b_4k$.
Recordem que $\alpha\beta = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k$.
Prenent normes tenim que $N(\alpha)N(\beta) = N(\alpha\beta)$, que efectivament demostra que la identitat dels quatre quadrats d'Euler es compleix.

D'aquesta igualtat observem que el producte de dos enters es pot escriure com la suma de quatre quadrats, per tant veiem que el Teorema dels quatre quadrats es compleix per a nombres compostos, per tant ara només ens falta demostrar que *Tot primer és la suma de quatre quadrats.*

Per demostrar-ho, necessitem veure que:

1. Un primer racional es pot escriure com el producte de dos quaternions de Hurwitz primers
2. La norma d'un quaternió de Hurwitz primer és un primer enter racional.
3. Si α és un quaternió de Hurwitz, aleshores com a mínim un dels seus associats té coordenades enteres.

Demostrem primer el tercer punt:

Teorema 4.2. *Si* α *és un quaternió de Hurwitz, aleshores com a mínim un dels seus associats té coordenades enteres; i si* α *és senar, aleshores almenys un dels seus associats té coordenades no enteres.*

Demostració. Suposem que les coordenades de α no són enteres, aleshores podem escollir els signes de manera que $\alpha = (b_0 + b_1i + b_2j + b_3k) + \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$, amb b_0, b_1, b_2, b_3

enters parells.
Anomenem $\beta = b_0 + b_1 i + b_2 j + b_3 k$ i $\gamma = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.
Com que tots els b_l són parells, qualsevol associat de β té coordenades enteres, i com que, γ és una unitat, aleshores $\overline{\gamma}$ també ho és i per tant, tenim que $\gamma\overline{\gamma} = 1$ és un associat de γ. Per tant $\alpha\overline{\gamma}$ és un associat de α que té coordenades enteres.
Si α és un quaternió de Hurwitz senar que té coordenades enteres, aleshores podem escriure $\alpha = (b_0 + b_1 i + b_2 j + b_3 k) + (c_0 + c_1 i + c_2 j + c_3 k) = \beta + \gamma$, on b_0, b_1, b_2, b_3 són parells, cada c_0, c_1, c_2, c_3 és 0 o 1 i (com que $N(\alpha)$ és senar) o bé una és 1, o bé ho són tres. Pel mateix argument utilitzat anteriorment, qualsevol associat de β té coordenades enteres. Per tant, n'hi ha prou amb demostrar que qualsevol dels quaternions 1, i, j, k, $1+i+j$, $1+i+k$, $1+j+k$, $i+j+k$ té un associat amb coordenades no enteres.
Sigui $\rho = \frac{1}{2}(1+i+j+k)$ una unitat, aleshores si $\gamma = i$, tenim que $\gamma\rho = -1 + \frac{i}{2} - j + k$ té coordenades no enteres. □

Abans de demostrar els dos primers punts, necessitem alguns Teoremes previs:

Teorema 4.3. *Si κ és un quaternió de Hurwitz, i m un enter positiu, aleshores existeix un quaternió de Hurwitz λ tal que $N(\kappa - m\lambda) < m^2$.*

Demostració. Si $m = 1$ podem agafar $\lambda = \kappa$ i aleshores tenim que $N(\lambda - \kappa) = 0 < 1$.
Suposem ara $m > 1$. Siguin $\kappa = k_0\rho + k_1 i + k_2 j + k_3 k$ i $\lambda = l_0\rho + l_1 i + l_2 j + l_3 k$ dos quaternions de Hurwitz on $k_0, k_1, k_2, k_3, l_0, l_1, l_2, l_3$ són nombres enters i $\rho = \frac{1}{2}(1+i+j+k)$. Les coordenades de $\kappa - m\lambda$ són:

$$\frac{k_0 - ml_0}{2} + \frac{k_0 + 2k_1 - m(l_0 + 2l_1)}{2} i + \frac{k_0 + 2k_2 - m(l_0 + 2l_2)}{2} j + \frac{k_0 + 2k_3 - m(l_0 + 2l_3)}{2} k.$$

Ara, escollim l_0, l_1, l_2, l_3 successivament de manera que minimitzin les coordenades de $\kappa - m\lambda$ en valor absolut.

Volem que $|k_0 - ml_0|$ sigui minim, com que $|x| \geq 0$ per a tot x, en particular busquem l_0 tal que $|k_0 - ml_0|$ sigui el més proper a 0 possible, és a dir, que l_0 sigui l'enter més proper a $\frac{k_0}{m}$. Com que l_0 ha de ser un nombre enter,
1. Si $\frac{k_0}{m} \in \mathbb{Z}$ aleshores podem agafar $l_0 = \frac{k_0}{m}$ i tenim que $|k_0 - ml_0| = 0$.
2. Si $\frac{k_0}{m} \notin \mathbb{Z}$ aleshores escrivim $l_0 = \frac{k_0}{m} + \epsilon$ amb $|\epsilon| \leq \frac{1}{2}$, com l'enter més proper a $\frac{k_0}{m}$. Tenim doncs que $|k_0 - ml_0| = \left|k_0 - m(\frac{k_0}{m} + \epsilon)\right| = |k_0 - k_0 - m\epsilon| = |-m\epsilon| = \mathrm{m}|\epsilon| \leq \frac{m}{2}$.
Per tant, podem acotar $\left|\frac{k_0 - ml_0}{2}\right| \leq \frac{m}{4}$

De manera successiva, podem elegir l_1, l_2, l_3 de manera que el valor absolut de les altres tres coordenades de $\kappa - m\lambda$ no siguin superior a $\frac{1}{2}$.

Per tant $N(\kappa - m\lambda) \leq \frac{1}{16}m^2 + 3\frac{1}{4}m^2 < m^2$. □

El Teorema següent és una analogia amb la divisió a $\mathbb{Z}$.

Teorema 4.4. *Si α i β són dos quaternions de Hurwitz amb $\beta \neq 0$, aleshores existeixen quaternions de Hurwitz λ i γ tal que*

$$\alpha = \lambda\beta + \gamma, \quad N(\gamma) < N(\beta).$$

Demostració. Agafem $\kappa = \alpha\overline{\beta}$, $m = \beta\overline{\beta} = N(\beta)$, ($m$ és un nombre enter positiu ja que β és un quaternió de Hurwitz).
Determinem λ com al teorema anterior i $\gamma = \alpha - \lambda\beta$, aleshores tenim que

$$(\alpha - \lambda\beta)\overline{\beta} = \kappa - \lambda m = \kappa - m\lambda.$$

Per tant, pel Teorema 4.3,

$$N(\alpha - \lambda\beta)N(\overline{\beta}) = N(\kappa - m\lambda) < m^2.$$

Hem vist doncs que existeixen λ i γ tal que $\alpha = \lambda\beta + \gamma$ i $N(\gamma) = N(\alpha - \lambda\beta) < m = N(\beta)$.

□

Sabem que a l'anell dels enters $\mathbb{Z}$ tot ideal és principal. Veurem que això també és cert en els enters de Hurwitz.

Teorema 4.5. *Tot ideal per la dreta és un ideal principal per la dreta.*

Demostració. Sigui S un ideal per la dreta. Per demostrar que és principal hem de veure que existeix un quaternió $\delta \in S$ que generi S, és a dir: $S = \{\lambda\delta \text{ tal que } \lambda \in S\}$.
Dels quaternions de S que no siguin 0, n'hi ha alguns de norma mínima, anomenarem un d'aquests com a δ. Si $\gamma \in S$ i $N(\gamma) < N(\delta)$ com que δ és un element de norma mínima, aleshores $\gamma = 0$.
Si $\alpha \in S$ aleshores, per definició d'ideal per la dreta, $\alpha - \lambda\delta \in S$ per tot quaternió de Hurwitz λ. Pel Teorema 4.4, podem triar λ tal que $N(\gamma) = N(\alpha - \lambda\delta) < N(\delta)$. Però com que $\gamma = 0$, aleshores $\alpha = \lambda\delta$. Per tant, hem vist que qualsevol $\alpha \in S$ pot ser generat per δ, per tant, S és un ideal principal per la dreta. □

Teorema 4.6. *Qualsevol parell de quaternions de Hurwitz α i β, no tots dos 0, tenen un màxim comú divisor per la dreta δ, que és únic excepte per un factor unitat per l'esquerra, i pot ser escrit com*

$$\delta = \mu\alpha + \nu\beta,$$

on μ i ν són quaternions de Hurwitz.

Demostració. Considerem el sistema S de tots els quaternions de la forma $\mu\alpha + \nu\beta$, on μ i ν són enters i α i β són quaternions de Hurwitz. Aquest sistema és un ideal per la dreta ja que:

1. Siguin $x = \mu_1\alpha + \nu_1\beta \in S$ i $y = \mu_2\alpha + \nu_2\beta \in S$, aleshores $x + y = (\mu_1 + \mu_2)\alpha + (\nu_1 + \nu_2)\beta \in S$,

2. Sigui $x = \mu_1\alpha + \nu_1\beta \in S$ i sigui λ un quaternió de Hurwitz, aleshores $x\lambda = \mu\alpha\lambda + \nu\beta\lambda \in S$, ja que la multiplicació per la dreta de quaternions de Hurwitz amb altres quaternions de Hurwitz donen quaternions de Hurwitz.

Pel Teorema 4.5, S és un ideal principal per la dreta format per tots els múltiples $\lambda\delta$ d'un cert quaternió de Hurwitz δ, on λ és qualsevol quaternió de Hurwitz.
Com que S inclou δ, δ pot ser escrit de la forma $\delta = \mu\alpha + \nu\beta$. Com que S inclou α i β, δ és un és un divisor per la dreta comú de α i β; i com que qualsevol divisor d'aquest tipus és un divisor per la dreta de qualsevol quaternió de S, aleshores és també un divisor per la dreta de δ. Per tant δ és el màxim comú divisor per la dreta de α i β.

Suposem ara que existeix un altre màxim comú divisor per la dreta δ'.
Aleshores, tenim que, δ i δ' satisfan les condicions $\delta' = \lambda\delta$ i $\delta = \lambda'\delta'$, on λ i λ' són quaternions de Hurwitz. Per tant $\delta = \lambda'\lambda\delta'$ implica que $1 = \lambda'\lambda$, i per tant tenim que λ' i λ són unitats.

□

Si δ és una unitat ϵ, aleshores el màxim comú divisor per la dreta de α i β serà una unitat. En aquest cas $\mu'\alpha + \nu'\beta = \epsilon$, per alguns quaternions de Hurwitz μ', ν'; i $(\epsilon^{-1}\mu')\alpha + (\epsilon^{-1}\nu')\beta = 1$; per tant $\mu\alpha + \nu\beta = 1$ per alguns quaternions de Hurwitz μ, ν. Aleshores escrivim $(\alpha, \beta)_r = 1$.

Teorema 4.7. *Si α és un quaternió de Hurwitz i $\beta = m$ és un enter positiu, llavors una condició necessària i suficient per a que $(\alpha, \beta)_r = 1$ és que $(N\alpha, N\beta) = 1$, és a dir que $(N\alpha, m) = 1$.*

Demostració. Si $(\alpha, \beta)_r = 1$, aleshores tenim que $\mu\alpha + \nu\beta = 1$ per quaternions de Hurwitz μ i ν apropiats.
Per tant

$$N(\mu\alpha) = N(1 - \nu\beta) = (1 - m\nu)(1 - m\overline{\nu}),$$

i per tant,

$$N\mu N\alpha = 1 - mv - m\overline{\nu} + m^2 N\nu.$$

Veiem que $(N\alpha, m)$ divideix tots els termes d'aquesta equació excepte 1, per tant $(N\alpha, m) = 1$. Com que $N\beta = m^2$, les dues formes de la condició són equivalents. □

Teorema 4.8. *Si p és un primer senar, aleshores existeixen nombres x i y tal que $1 + x^2 + y^2 = mp$, amb $0 < m < p$.*

Demostració. Els $\frac{1}{2}(p+1)$ nombres de la forma $x^2 \quad (0 \leq x \leq \frac{1}{2}(p-1))$ són incongruents mod p, així com també ho són els $\frac{1}{2}(p+1)$ nombres de la forma $-1-y^2 \quad (0 \leq y \leq \frac{1}{2}(p-1))$. Si ajuntem els dos conjunts, veiem que hi ha $p+1$ nombres i només p residus $\mod p$ (de 0 a $p-1$), per tant, algun nombre x^2 ha de ser congruent amb algun $-1-y^2$.
Per tant hi ha algun x i algun y , cadascun numèricament més petit que $\frac{1}{2}p$, tal que

$$x^2 \equiv -1 - y^2, \quad 1 + x^2 + y^2 = mp.$$

També,

$$0 < 1 + x^2 + y^2 < 1 + 2(\frac{1}{2}p)^2 < p^2,$$

de tal manera que $0 < m < p$.

□

Ara sí, demostrem que els primers racionals no són quaternions primers i que les normes de quaternions primers són primers racionals.

Teorema 4.9. *Un primer racional p no pot ser un quaternió primer.*

Demostració. Com que $2 = (1+i)(1-i)$, 2 no és un quaternió primer.
Suposem p senar. Pel Teorema 4.8, existeixen enters racionals r i s tal que

$$0 < r < p, \quad 0 < s < p, \quad 1 + r^2 + s^2 \equiv 0 \pmod{p}.$$

Si $\alpha = 1 + sj - rk$, aleshores, $N\alpha = 1 + r^2 + s^2 \equiv 0 \pmod{p}$, i $(N\alpha, p) > 1$. D'aquí es dedueix, pel Teorema 4.7, que α i p tenen un comú divisor per la dreta δ que no és una unitat. Si $\alpha = \delta_1\delta$, $p = \delta_2\delta$, aleshores δ_2 no és una unitat, ja que si ho fos δ seria un associat de p, en el qual cas p dividria totes les coordenades de $\alpha = \delta_1\delta = \delta_1\delta_2^{-1}p$, i en particular 1. Per tant, $p = \delta_2\delta$, on ni δ ni δ_2 són unitats, tenim doncs que p no és primer.
□

El Teorema 4.9 també se segueix del següent resultat:

Teorema 4.10. *Un quaternió de Hurwitz π és primer si i només si la seva norma $N\pi$ és un primer racional.*

Demostració. Suposem que π és primer, i que p és un divisor primer racional de $N\pi$. Pel teorema 4.7, π i p tenen un divisor comú per la dreta π' que no és una unitat. Com que π és primer, π' és un associat de π i $N\pi' = N\pi$. També $p = \lambda\pi'$, on λ és un quaternió de Hurwitz, i $p^2 = N\lambda N\pi' = N\lambda N\pi$, de tal manera que $N\lambda$ ha de ser 1 o p.
Si $N\lambda$ fos 1, p seria un associat de π' i π, i així un quaternió primer, el que hem vist que no és possible. Per tant, $N\pi = p$, un primer racional. □

Ara que ja hem demostrat els tres punts que necessitàvem veure, podem demostrar que tot primer es pot escriure com la suma de quatre quadrats.

Teorema 4.11. *Tot primer p és la suma de quatre quadrats.*

Demostració. Si p és qualsevol primer racional aleshores escrivim p com el producte de dos quaternions primers de Hurwitz λ i π ja que hem vist pel Teorema 4.9 que p no pot ser un quaternió primer.
Aleshores, sigui $p = \lambda\pi$, com que $N(p) = p^2$ i pel Teorema 4.10 la norma d'un quaternió de Hurwitz primer és un primer racional, alsehores $N\lambda = N\pi = p$.
Si π té coordenades enteres a_0, a_1, a_2, a_3, aleshores

$$p = N\pi = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Si no, pel Teorema 4.2, existeix un associat π' de π que té coordenades enteres. Com que $p = N\pi = N\pi'$, aleshores també tenim que

$$p = N\pi' = b_0^2 + b_1^2 + b_2^2 + b_3^2$$

on b_1, b_2, b_3, b_4 són enters. □

5 Conclusions

L'objectiu principal d'aquesta memòria era donar la demostració del Teorema dels quatre quadrats de Lagrange a partir dels quaternions de Hurwitz.
Els quaternions són una àlgebra que no he estudiat durant la carrera, en aquest treball he estudiat els quaternions de Hamilton, una generalització d'aquests i els de Hurwitz. He demostrat algunes de les seves propietats que m'han servit per a poder demostrar d'una manera senzilla el Teorema dels quatre quadrats, teorema que ja havia vist a Aritmètica, però que no havia demostrat mai.

Referències

[1] Conrad, Keith: *Quaternion Algebras.*

[2] Conway, J. H.; Smith, D. A.: *On Qauternions and Octonions*, A K Peters, Ltd, Massachussets, 2003.

[3] Hardy, G. H.; Wright, E. M.: *An Introduction to the Theory of Numbers*, Oxford University Press, New York, 1979.

[4] Lam, T. Y.: *A First Course in Noncommutative Rings*, Springer Science+Business Media, New York, 2001.