Quaternions et arithmétique sur les quaternions entiers

Julie Raniolo

décembre 2016

Université de Fribourg
Département de Mathématiques
Semestre d'automne 2016
Responsable : Dr. Corina Ciobotaru

Table des matières

1 Introduction **3**

2 Quaternions et arithmétique sur les quaternions entiers **3**

2.1 Définition 1 (*quaternions*) . . . 3
2.2 Définitions 2 (*conjugué et norme*) . . . 3
2.3 Proposition 3 . . . 4
2.4 Définitions 4 (*impair/pair*, *premier*, *associé et diviseur à droite*) . . . 4
2.5 Proposition 5 . . . 4
2.6 Lemme 6 (*Algorithme d'Euclide à droite*) . . . 5
2.7 Définition 7 (*pgdc à droite*) . . . 6
2.8 Lemme 8 . . . 6
2.9 Théorème 9 (*existence du pgdc à droite*) . . . 6
2.10 Lemme 10 . . . 6
2.11 Lemme 11 . . . 6
2.12 Théorème 12 . . . 6
2.13 Corollaire 13 . . . 7
2.14 Corollaire 14 . . . 8

1 Introduction

Ce chapitre du proséminaire sur les graphes expanseurs porte sur les quaternions, en particulier sur les quaternions entiers. Une définition de l'algèbre des quaternions sur un anneau commutatif unitaire va être donnée, puis l'intérêt se portera sur les propriétés des quaternions entiers. Certaines propriétés sont modifiées car l'aglèbre des quaternions n'est pas commutative. Enfin, on atteindra l'objectif de ce chapitre qui est de montrer que chaque nombre naturel est une somme de quatre carrés.

2 Quaternions et arithmétique sur les quaternions entiers

Soit R un anneau commutatif unitaire.

2.1 Définition 1 (*quaternions*)

L'algèbre des quaternions sur R, $\mathbb{H}(R)$, est une algèbre associative unitaire ayant les propriétés suivantes :

1. $\mathbb{H}(R)$ est un R-module libre sur les symboles 1, i, j, k, c'est-à-dire $\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k \,|\, a_i \in R\}$.
2. 1 est l'élément neutre de la multiplication.
3. $i^2 = j^2 = k^2 = -1$
4. $ij = -ji = k$
   $jk = -kj = i$
   $ki = -ik = j$

Remarques
$\mathbb{H}(R)$ n'est pas commutative. On le voit directement avec $k = ij \neq ji = -k$.
Une algèbre sur un corps K est une structure algébrique $(A, +, \cdot, \times)$ t.q.

1. $(A, +, \cdot, \times)$ est un espace vectoriel sur K,
2. la loi $\times$ est définie de $A \times A$ dans A,
3. la loi $\times$ est bilinéaire.

Un exemple d'algèbre est $\mathbb{C}$.

2.2 Définitions 2 (*conjugué et norme*)

Soit $q = a_o + a_1 i + a_2 j + a_3 k$ un quaternion.
Son **conjugué** est défini par $\bar{q} = a_o - a_1 i - a_2 j - a_3 k$.
Sa **norme** est définie par $N(q) = q\bar{q} = \bar{q}q = a_o^2 + a_1^2 + a_2^2 + a_3^2$.
La norme quaternionique est multiplicative, c'est-à-dire que pour q_1 et $q_2 \in \mathbb{H}(R)$, on a
$N(q_1 q_2) = N(q_1) N(q_2)$.

Exemple :
Soient $q_1, q_2 \in \mathbb{H}(\mathbb{Z})$.
$q_1 = 1 + 2i + 3j + 4k, \quad q_2 = 5 + 6i + 7j + 8k$
$q_1 q_2 = -60 + 12i + 30j + 24k$
$N(q_1 q_2) = (-60)^2 + 12^2 + 30^2 + 24^2 = 5220$
$N(q_1) = 1^2 + 2^2 + 3^2 + 4^2 = 30$
$N(q_2) = 5^2 + 6^2 + 7^2 + 8^2 = 174$
$N(q_1) N(q_2) = 30 \cdot 174 = 5220$
$\Rightarrow N(q_1 q_2) = N(q_1) N(q_2)$

2.3 Proposition 3

Soit $q = p^k$ avec p un nombre premier impair et k $\in \mathbb{N}$.
Alors, il existe x, y $\in \mathbb{F}_q$ t.q. $x^2 + y^2 + 1 = 0$.

Exemples
Dans $\mathbb{F}_3$: $1^2 + 2^2 + 1 = 0$.
Dans $\mathbb{F}_9$: $1^2 + 5^2 + 1 = 0$.

A partir de maintenant, on se restreint aux quaternions entiers, c'est-à-dire à $\mathbb{H}(\mathbb{Z})$.
Soit $U(\mathbb{H}(\mathbb{Z}))$ le groupe des unités dans $\mathbb{H}(\mathbb{Z})$.
$U(\mathbb{H}(\mathbb{Z})) = \{\pm 1, \pm i, \pm j, \pm k\}$.

2.4 Définitions 4 (*impair/pair, premier, associé et diviseur à droite*)

Soit $q \in \mathbb{H}(\mathbb{Z})$.
q est dit **impair** (*resp.pair*) si $N(q)$ est impaire (*resp.paire*).
q est dit **premier** si

1. $q \notin U(\mathbb{H}(\mathbb{Z}))$
2. $q = \alpha \cdot \beta \Rightarrow \alpha$ ou $\beta \in U(\mathbb{H}(\mathbb{Z}))$.

Deux quaternions q_1 et $q_2 \in \mathbb{H}(\mathbb{Z})$ sont **associés** s'il existe $\epsilon_1, \epsilon_2 \in U(\mathbb{H}(\mathbb{Z}))$ t.q. $q_1 = \epsilon_1 \cdot q_2 \cdot \epsilon_2$.
$\delta \in \mathbb{H}(\mathbb{Z})$ est un **diviseur à droite** de $q \in \mathbb{H}(\mathbb{Z})$ s'il existe $\gamma \in \mathbb{H}(\mathbb{Z})$ t.q. $q = \gamma \cdot \delta$.

Exemples
$q = 1 + 2i + 3j + 4k \Rightarrow N(q) = 1^2 + 2^2 + 3^2 + 4^2 = 30 \Rightarrow q$ est pair.
$q_1 = 1 + 2i + 3j + 4k$, $q_2 = -2 + i - 4j + 3k \Rightarrow q_1$ et q_2 sont associés car $q_2 = i \cdot q_1 \cdot 1$.
q_1 est un diviseur à droite de q_2 car $q_2 = i \cdot q_1$.

Remarques
$N(\epsilon) = 1$ pour tout $\epsilon \in U(\mathbb{H}(\mathbb{Z}))$.
$\Rightarrow$ "*être associés*" définit une relation d'équivalence qui préserve les propriétés arithmétiques (*pair/impair, premier, unité, ...*).
La définition de premier et irréductible ne sont pas équivalentes dans $\mathbb{H}(\mathbb{Z})$ car $\mathbb{H}(\mathbb{Z})$ n'est pas commutative. Un diviseur à droite de xy n'est en général pas un diviseur à droite de x.

2.5 Proposition 5

Chaque quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ est un produit de quaternions premiers.

Preuve par induction sur $N(\alpha)$
Hypothèse : tout quaternion est un produit de quaternions premiers.
Si $N(\alpha) = 1$, cela signifie que α est une unité ($cf.\, remarque\, ci - dessus$). Il n'y a donc rien à montrer.
On prend donc le cas où $N(\alpha) > 1$. On suppose que l'hypothèse est vraie pour tout quaternion de norme $< N(\alpha)$

- Si α est premier, il n'y a rien à montrer.
- Si α n'est pas premier $\Rightarrow \alpha = \beta \cdot \gamma$ où β et $\gamma \notin U(\mathbb{H}(\mathbb{Z}))$
  $\Rightarrow N(\beta) < N(\alpha)$ et $N(\gamma) < N(\alpha)$
  $\Rightarrow$ L'hypothèse est vraie pour β et γ, c-à-d que β et γ sont des produits de quaternions premiers.
  $\Rightarrow \alpha$ est aussi un produit de quaternions premiers.

Remarque
On a aussi une telle factorisation dans $\mathbb{Z}$ qui est unique à associés près.
Dans $\mathbb{H}(\mathbb{Z})$, elle n'est pas forcément unique.
Ex : $13 = (1+2i+2j+2k)(1-2i-2j-2k) = (3+2i)(3-2i)$

L'algorithme d'Euclide existe aussi dans $\mathbb{H}(\mathbb{Z})$. Cependant, il est un peu modifié. On se restreint à la multiplication à droite et à β impair.
On trouve un résultat analogue pour la multiplication à gauche, pour γ',$\delta' \in \mathbb{H}(\mathbb{Z})$ t.q.
$\alpha = \beta \cdot \gamma' + \delta'$ et $N(\delta') < N(\beta)$. γ' et δ' ne sont pas forcément les mêmes que γ et δ du lemme ci-dessous.

2.6 Lemme 6 (*Algorithme d'Euclide à droite*)

Soient $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ t.q. β est impair.
Alors, il existe $\gamma, \delta \in \mathbb{H}(\mathbb{Z})$ t.q. $\alpha = \gamma \cdot \beta + \delta$ et $N(\delta) < N(\beta)$.

On va d'abord montrer une affirmation qui va nous être utile pour la preuve.

Affirmation
Soit $\sigma = s_0 + s_1 i + s_2 j + s_3 k \in \mathbb{H}(\mathbb{Z})$.
Soit m un nombre entier impair et positif.
Alors, il existe $\gamma \in \mathbb{H}(\mathbb{Z})$ t.q. $N(\sigma - \gamma \cdot m) < m^2$.

Preuve de l'affirmation
$\forall s_i \, \exists r_i \in \mathbb{Z}$ t.q. $mr_i - m/2 < s_i < mr_i + m/2$.
On a une inégalité stricte car m est impair.
On pose :
$s_i = mr_i + t_i$ t.q. $|t_i| < m/2$,
$\gamma = r_0 + r_1 i + r_2 j + r_3 k$.
$$\begin{aligned}\Rightarrow \sigma - \gamma \cdot m &= s_0 + s_1 i + s_2 j + s_3 k - mr_o - mr_1 i - mr_2 j - mr_3 k \\ &= mr_o + t_0 + mr_1 i + t_1 i + mr_2 j + t_2 j + mr_3 k + t_3 k - mr_0 - mr_1 i - mr_2 j - mr_3 k \\ &= t_o + t_1 i + t_2 j + t_3 k\end{aligned}$$
$\Rightarrow N(\sigma - \gamma \cdot m) = t_0^2 + t_1^2 + t_2^2 + t_3^2 < 4 \cdot (m/2)^2 = m^2$ car $|t_i| < m/2$

Preuve du lemme
Pour la preuve du lemme, il suffit de poser :
$m = N(\beta) = \beta\bar{\beta}$, m est bien impair car β est impair par hypothèse,
$\sigma = \alpha\bar{\beta}$.
Par l'affirmation au-dessus, il existe $\gamma \in \mathbb{H}(\mathbb{Z})$ t.q. $N(\sigma - \gamma \cdot m) < m^2$.
$m^2 = N(\beta)^2 = N(\beta) N(\bar{\beta})$
$N(\sigma - \gamma \cdot m) = N(\alpha\bar{\beta} - \gamma \cdot \beta\bar{\beta}) = N(\alpha - \gamma\beta) N(\bar{\beta})$
$\Rightarrow N(\beta) N(\bar{\beta}) > N(\alpha - \gamma\beta) N(\bar{\beta})$
$\Rightarrow N(\beta) > N(\alpha - \gamma\beta)$
On pose $\delta = \alpha - \gamma\beta$.
$\Rightarrow N(\beta) > N(\delta)$ et $\alpha = \gamma\beta + \delta$.

2.7 Définition 7 (*pgdc à droite*)

Soient $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$.
$\delta \in \mathbb{H}(\mathbb{Z})$ est dit **le plus grand diviseur commun** (*pgdc*) **à droite** de α et β

1. Si δ est un diviseur à droite de α et de β,
2. Si $\delta_0 \in \mathbb{H}(\mathbb{Z})$ est un diviseur à droite de α et β,
   alors δ_0 est un diviseur à droite de δ.

On écrit $\delta = (\alpha, \beta)_r$.
S'il existe, $\delta = (\alpha, \beta)_r$ est unique à associés près.

Les résultats suivants ne vont pas être prouvés, mais ils vont nous être utiles pour la preuve d'un théorème et de corollaires importants.

2.8 Lemme 8

Soit $\alpha \in \mathbb{H}(\mathbb{Z})$. Alors, il existe une factorisation unique $\alpha = 2^k \cdot \pi \cdot \alpha_0$,
avec k $\in \mathbb{N}$, $\pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (1+i)(1-k)\}$ et $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ impair.

2.9 Théorème 9 (*existence du pgdc à droite*)

Soient $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ t.q. β est impair. Alors, $(\alpha, \beta)_r$ existe.

Remarque
On a la version suivante de la relation de Bézout :
$\exists \gamma, \delta \in \mathbb{H}(\mathbb{Z}[1/2])$ t.q. $(\alpha, \beta)_r = \gamma\alpha + \delta\beta$, où $\mathbb{Z}[1/2] = \{k/2^n | k \in \mathbb{Z}, n \in \mathbb{N}\}$.

2.10 Lemme 10

Soit $\alpha \in \mathbb{H}(\mathbb{Z})$ et m $\in \mathbb{Z}$ impair.
$(m, \alpha)_r = 1 \iff (m, N(\alpha))_r = 1$

2.11 Lemme 11

Hypothèses :
- $p \in \mathbb{N}$ premier et impair,
- $\alpha \in \mathbb{H}(\mathbb{Z})$ t.q. p ne divise pas α, mais p divise $N(\alpha)$,
- $(\alpha, p)_r = \delta$.

Affirmation : δ est premier dans $\mathbb{H}(\mathbb{Z})$ et $N(\delta) = p$.

Remarque
Ce lemme nous dit que si $N(\delta)$ est premier $\mathbb{Z}$, alors δ est premier dans $\mathbb{H}(\mathbb{Z})$.

2.12 Théorème 12

Pour tout $p \in \mathbb{N}$ premier impair, il existe $\delta \in \mathbb{H}(\mathbb{Z})$ premier t.q. $N(\delta) = p = \delta\bar{\delta}$.
En d'autres termes, p n'est pas premier dans $\mathbb{H}(\mathbb{Z})$.

Preuve
Par la proposition 3, on sait qu'il existe $x, y \in \mathbb{Z}$ t.q. $1 + x^2 + y^2 \equiv 0 \, mod \, p$.
On pose $\alpha = 1 + xi + yj$.
$\Rightarrow p$ ne divise pas α, mais $p \,|\, N(\alpha) = 1 + x^2 + y^2$.
On peut utiliser le lemme 11 qui nous dit que $\delta = (\alpha, p)_r$ est premier dans $\mathbb{H}(\mathbb{Z})$ et que $N(\delta) = p$.
$\Rightarrow \delta$ est le quaternion premier recherché.

2.13 Corollaire 13

$\delta \in \mathbb{H}(\mathbb{Z})$ est premier $\Longleftrightarrow N(\delta)$ est premier dans $\mathbb{Z}$

Preuve

$\Leftarrow$: Soit $N(\delta) = p$ t.q. p est un nombre premier dans $\mathbb{Z}$.
Comme chaque quaternion peut être écrit comme le produit de quaternions premiers, on peut écrire $\delta = xy$.
On prend la norme
$N(\delta) = N(x) N(y) = p$.
Comme p est premier $\Rightarrow N(x) = 1$ ou $N(y) = 1$
$\Rightarrow$ x ou y $\in U(\mathbb{H}(\mathbb{Z}))$
$\Rightarrow \delta$ est premier dans $\mathbb{H}(\mathbb{Z})$

$\Rightarrow$: On distingue deux cas :

δ est pair :

Par le lemme 8, on a $\delta = 2^k \cdot \pi \cdot \delta_0$,
où k $\in \mathbb{N}, \pi \in \{1, 1+i, 1+j, 1+k, (1+i)(1+j), (i+1,)(1-k)\}$ et δ_0 impair.
2 n'est pas premier dans $\mathbb{H}(\mathbb{Z})$ car $2 = (1+i)(1-i)$.
$\Rightarrow k = 0$ car $\delta \in \mathbb{H}(\mathbb{Z})$ est premier par hypothèse.
$\Rightarrow \delta = \pi \cdot \delta_0$
Comme δ est premier et pair, on a

1. soit $\pi \in U(\mathbb{H}(\mathbb{Z}))$ et δ_0 pair,
2. soit $\delta_0 \in U(\mathbb{H}(\mathbb{Z}))$ et π pair.

Comme δ_0 est impair par hypothèse, on a la deuxième possibilité.
$\Rightarrow N(\delta_0) = 1$ et $\pi \in \{1+i, 1+j, 1+k\}$
$\Rightarrow N(\delta) = N(\pi) N(\delta_0) = 2 \cdot 1 = 2$
2 est bien premier dans $\mathbb{Z}$.

δ est impair :

Soit $p \in \mathbb{N}$ un nombre premier qui divise $N(\delta)$.
A montrer : $N(\delta) = p$.
Soit $\alpha = (p, \delta)_r$.
$\Rightarrow \delta = \gamma\alpha$ pour un certain $\gamma \in \mathbb{H}(\mathbb{Z})$
Par le lemme 10, on a $(N(\delta), p)_r \neq 1$ car $N(\delta)$ divise $p \Rightarrow (\delta, p)_r \neq 1$ donc $\alpha \notin U(\mathbb{H}(\mathbb{Z}))$.
Comme δ est premier dans $\mathbb{H}(\mathbb{Z})$ par hypothèse
$\Rightarrow \gamma \in U(\mathbb{H}(\mathbb{Z}))$
$\Rightarrow \alpha$ et δ sont associés
$\Rightarrow \delta$ est un diviseur à droite de p, $p = \psi\delta$ pour un certain $\psi \in \mathbb{H}(\mathbb{Z})$.
On prend la norme
$N(p) = p^2 = N(\psi) N(\delta)$
Comme p divise $N(\delta)$ par hypothèse, on a $p = N(\psi)(N(\delta)/p)$.
Comme p est premier, on a $N(\psi) = 1$ ou $(N(\delta)/p) = 1$.
Si $N(\psi) = 1$, alors p et δ sont associés.
$\Rightarrow p$ est premier dans $\mathbb{H}(\mathbb{Z})$.
Ceci contredit le théorème 12 qui dit que si $p \in \mathbb{N}$ est premier, alors p n'est pas premier dans $\mathbb{H}(\mathbb{Z})$.
$\Rightarrow (N(\delta)/p) = 1$ et donc $N(\delta) = p$.

2.14 Corollaire 14

Chaque nombre naturel est une somme de quatre carrés.

Preuve

Soit $n \in \mathbb{N}$.
Pour $n = 0$ et $n = 1$, le résultat est clair.
On prend donc $n \geq 2$.
Soit $n = 2^{r_o} \cdot p_1^{r_1} \cdot ... \cdot p_k^{r_k}$ la factorisation de n en nombres premiers t.q. p_i impairs $\forall i$.
Par le théorème 12, il existe $\delta_i \in \mathbb{H}(\mathbb{Z})$ t.q. $p_i = N(\delta_i) = \delta_i \bar{\delta_i}$ et $2 = (1+i)(1-i) = N(1+i)$.

$$\begin{aligned} \Rightarrow n &= N((1+i))^{r_0} N(\delta_1)^{r_1} ... N(\delta_k)^{r_k} \\ &= N((1+i)^{r_0}) N(\delta_1^{r_1}) ... N\left(\delta_k^{r_k}\right) \\ &= N\left((1+i)^{r_o} \cdot \delta_1^{r_1} \cdot ... \cdot \delta_k^{r_k}\right) \end{aligned}$$

par la multiplicativité de la norme quaternionique.
Comme la norme est une somme de quatre carrés ($cf.\ Définition\ 2$), alors n est aussi une norme de quatre carrés.