Algèbres à Division

Astrid Thollet et Alexandre Démoulin sous la direction de Gaëtan Chenevier

6 Juin 2022

Table des matières

1 Introduction

1.1 Motivation

Jusqu'en classe de Terminale le plus gros ensemble de nombres que nous manipulons en mathématique est celui des nombres réels $\mathbb{R}$. Nous apprenons dès lors que ce dernier peut être plongé dans un corps plus gros, celui des nombres complexes $\mathbb{C}$. En license 3 nous expérimentons encore une fois ce phénomène : le corps des nombres complexes peut être plongé (non canoniquement cette fois) dans l'algèbre des quaternions $\mathbb{H}$. Nous perdons cependant la commutativité, nous invitant ainsi à définir une notion plus générale englobant les corps :

Définition : Algèbre à division associative 1.1.1 Soient k un corps et A une k-algèbre. On dit que A est à division si tout élément non nul de A est inversible à gauche et à droite.

On pourrait parler des algèbres à division non-associative mais nous omettrons l'adjectif « associative » pour plus de lisibilité. Une question naturelle est de se demander si ce phénomène se reproduit encore, en clair classifier les $\mathbb{R}$-algèbres à divisions de dimension finie et plus généralement (et trop ambitieusement) :

Peut-on classifier les k-algèbres à division de dimension finie où k est un corps ?

1.2 Le théorème de Frobenius

La question est vite répondue lorsque $k = \mathbb{R}$: il n'y a, à isomorphisme près, que les algèbres citées précédement et la démonstration est très élémentaire, il suffit simplement d'utiliser le polynôme minimal.

Proposition-définition : Polynôme minimal 1.2.1 Soient k un corps et A une k-algèbre de dimension finie. Soit $x \in A$ et soit ψ_x le morphisme d'algèbre :

$$\begin{aligned} \psi_x : \quad k[X] &\longrightarrow A \\ P &\longmapsto P(x) \end{aligned}$$

Alors il existe un unique polynôme unitaire $\mu_x \in k[X]$ appelé polynôme minimal de x sur k tel que $\ker \psi_x = \mu_x k[X]$.

Démonstration. L'application ψ_x est clairement un morphisme d'algèbre ainsi $I := \ker \psi_x$ est un idéal de $k[X]$. On montre que cet idéal est non nul. Soit $n = \dim_k A$ alors la famille $(1, x, x^2, \dots, x^n)$ est une famille de $n+1$ vecteurs, donc liés. Cela assure l'existence de coefficients $(\alpha_0, \dots, \alpha_n)$ non tous nul tel que $\sum_{k=0}^{n} \alpha_k x^k = 0$ ainsi $0 \neq P_0 := \sum_{k=0}^{n} \alpha_k X^k \in I$.
Ainsi par principalité de $k[X]$ il existe un unique polynôme unitaire μ_x tel que $I = \mu_x k[X]$. □

Remarque. En particulier le polynôme minimal μ_x annule toujours x. Lorsque A est une algèbre à division, μ_x est toujours irréductible dans $k[X]$. En effet soit P et $Q \in k[X]$ tel que $\mu_x = PQ$. Alors $\mu_x(x) = P(x)Q(x)$ ainsi ou bien $P(x) = 0$ ou $Q(x) = 0$ car A est à division. Ainsi P ou $Q \in \ker \psi_x$ et donc $\mu_x | P$ ou Q ce qui conclut. Cet outil permet déjà de classer les K-algèbres à division de dimension finie où K est un corps algébriquement clôs.

Lemme 1.2.2 Soit A une K-Algèbre à division de dimension finie où K est un corps algébriquement clôs. Alors $A \simeq K$.

Démonstration. Soit $x \in A$ et μ_x son polynôme minimal. Alors il existe $\lambda \in K$ tel que $\mu_x = X - \lambda$. Ainsi $\mu_x(x) = 0$ donc $x = \lambda \cdot 1_A \in 1_A \cdot K \simeq K$. □

Théorème de Forbenuis 1.2.3 Il existe à isomorphisme près trois $\mathbb{R}$-algèbre à division de dimension finie :

$$\mathbb{R},\ \mathbb{C} \text{ et } \mathbb{H}$$

Démonstration. 1. Soit A une telle algèbre. On a déjà $A \supset \mathbb{R} \cdot 1_A \simeq \mathbb{R}$ donc si $\dim_{\mathbb{R}} A = 1$ cela assure $A \simeq \mathbb{R}$.

2. On suppose qu'il existe $x \in A \setminus 1_A \cdot \mathbb{R}$, on considère son polynôme minimal μ_x. Il est irréductible dans $\mathbb{R}[X]$ car A est à division. Ainsi μ_x est de la forme :

$$X - \lambda,\ \lambda \in \mathbb{R} \text{ ou } (X-a)^2 + b^2\ a \in \mathbb{R},\ b \in \mathbb{R}^*$$

La première forme implique $x = 1_A \cdot \lambda \in 1_A \cdot \mathbb{R}$ qui est exclut. En changeant x en $\frac{x-a}{b}$ on obtient $x^2 = -1$. Ainsi $A \supset \mathbb{R}[x] \simeq \mathbb{C}$ et donc si $\dim_{\mathbb{R}} A = 2$, $A \simeq \mathbb{C}$.

3. On suppose que $A \setminus \mathbb{R}[x] \neq \varnothing$. On considère

$$\begin{aligned} s :\ A &\longrightarrow A \\ u &\longmapsto xux^{-1} \end{aligned} .$$

s est une symétrie, si $s = \mathrm{id}_A$ alors tout élément de A commute avec x et on peut voir A comme une $\mathbb{R}[x]$-algèbre. Mais $\mathbb{R}[x] \simeq \mathbb{C}$ algébriquement clôs alors $A = \mathbb{R}[x]$ d'après le lemme ce qui contredit l'hypothèse.

Prenons ainsi $y \in A \setminus \mathbb{R}[x]$ tel que $xy = -yx$. Il existe $a \in \mathbb{R}$ et $b \in \mathbb{R}^*$ tel que $y^2 = ay - b$. Cependant $xy^2x^{-1} = xyx^{-1} \times xyx^{-1} = (-y) \times (-y) = y^2$ et $xy^2x^{-1} = -ay - b$ ainsi $a = 0$ et on remplace y par $\frac{y}{\sqrt{b}}$ pour obtenir $y^2 = -1$ ($b > 0$ sinon $y \in 1_A \cdot \mathbb{R}$). Ainsi $\mathbb{R}[x,y] = 1_A \cdot \mathbb{R} \oplus x \cdot \mathbb{R} \oplus y \cdot \mathbb{R} \oplus xy \cdot \mathbb{R} \simeq \mathbb{H}$. En effet posons $z = xy$ alors $-1 = x^2 = y^2 = z^2$ et $xyz = -1$ et la famille $(1, x, y, z)$ est bien libre. Donc si $\dim_{\mathbb{R}} A = 4$ alors $A \simeq \mathbb{H}$.

4. On va montrer que $A = \mathbb{R}[x,y]$ avec les hypothèses effectuées jusqu'à présent. On note A^+=ensemble des éléments qui commutent avec x et A^- = ensemble des éléments qui anti-commutent avec x. L'aplication $u :\ t \longrightarrow yt$ est bijective et échange A^+ et A^-. Ainsi $A = A^+ \oplus A^-$ et $\dim_{\mathbb{R}} A = \dim_{\mathbb{R}} A^+ + \dim_{\mathbb{R}} A^- = 2 \dim_{\mathbb{R}} A^+$ mais $A^+ = \mathbb{R}[x]$,en effet, si un élément $t \in A^+ \setminus \mathbb{R}[x]$ alors on considère son polynôme minimal dans $\mathbb{R}[x]$ qui est nécessairement de degré un car $\mathbb{R}[x]$ est algébriquement clôs, les polynômes irréductibles sont les polynômes de degré un. Donc $\dim_{\mathbb{R}} A = 4$ ce qui conclut.

□

1.3 Algèbres centrales

Parmi les $\mathbb{R}$-algèbre de dimension finie, $\mathbb{C}$ se fait particulièrement remarquer car son centre n'est pas $\mathbb{R}$. C'est évidement le cas pour $\mathbb{R}$ mais aussi pour $\mathbb{H}$: on dit que ces algèbres sont centrales.

Définition : Algèbre centrales 1.3.1 Soient k un corps et A une k-algèbre. On appelle centre de A et on note $Z(A)$ la sous-algèbres commutative de A :

$$Z(A) = \{x \in A \mid \forall a \in A,\ ax = xa\}$$

On dit que A est centrale si $Z(A) = k$.

Remarque. On peut toujours considérer une k-algèbre à division de dimension finie comme une K-algèbre à division centrale et de dimension finie où K est un corps. En effet $Z(A)$ est une sous-algèbre de A et dimension finie, étant donné que A est à division, tout élément non nul de $Z(A)$ est inversible, de plus grâce au polynôme minimale, on peut exprimer l'inverse d'un élément comme un polynôme de cet élément, il reste donc dans le centre. Ainsi $K = Z(A)$ est un corps et on peut donc restreindre l'étude en considérant les algèbres centrales. Plus précisément, ce que nous mettons de côté dans ce mémoire sera assuré dans le cours d'Algèbre 2 avec la théorie de Galois qui étudie les extensions finies de corps commutatifs.

1.4 Algèbres de quaternion généralisées

Voyons tout de suite un exemple d'une algèbre centrale (parfois) à division.

Définition : Quaternion généralisés 1.4.1 Soient k un corps, on note $\left(\frac{a,b}{k}\right)$ où $a,b \in k$ non nuls, l'unique algèbre A à isomorphisme près telle que :

$$A = k \oplus x \cdot k \oplus y \cdot k \oplus z \cdot k \text{ avec } x^2 = a,\ y^2 = b,\ z^2 = -ab,\ xy = -yx = z$$

Remarque. Une telle algèbre est bien unique à isomorphisme près car on a défini sa table de multiplication sur une base. Une telle algèbre existe toujours, en effet on peut toujours voir $\left(\frac{a,b}{k}\right)$ comme une sous algèbre de $\mathcal{M}_2(k[\sqrt{a}])$ en posant $x = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}$, $y = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}$ et $z = \begin{bmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{bmatrix}$.

Remarque. Nous verrons que ces algèbres fournissent une réponse partielle mais concrète à notre problème, cependants $\left(\frac{a,b}{k}\right)$ n'est pas toujours à division, c'est l'objet de la proposition suivante :

Proposition 1.4.2 Soit k un corps. On dispose des formules suivantes pour tout $a,b,\lambda \in k$ non nuls :

$$\left(\frac{a,b}{k}\right) \simeq \left(\frac{b,a}{k}\right),\ \left(\frac{\lambda^2 a,b}{k}\right) \simeq \left(\frac{a,b}{k}\right),\ \left(\frac{1,b}{k}\right) \simeq \mathcal{M}_2(k), \text{ et } \mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$$

Démonstration.

1. la première égalité est triviale
2. On note $A' = \left(\frac{\lambda^2 a,b}{k}\right) = k \oplus x' \cdot k \oplus y' \cdot k \oplus z' \cdot k$ et $A = \left(\frac{a,b}{k}\right) = k \oplus x \cdot k \oplus y \cdot k \oplus z \cdot k$ On condidère alors le morphisme k-linéaire $\phi :\ A' \longrightarrow A$ uniquement défini par $\phi(1_{A'}) = 1_A$, $\phi(x') = \lambda x$, $\phi(y') = y$ et $\phi(z') = \lambda z$. ce morphisme respecte la table de multiplication des algèbres et est donc un morphisme de k-algèbre bijectif donc un isomorphisme.
3. Soit $B = \left(\frac{1,b}{k}\right)$, B se plonge dans $\mathcal{M}_2(k)$ et a même dimension donc ces deux algèbres sont isomorphes.

□

Nous étudierons en détail les algèbres de quaternions plus tard (et nous y consacrerons une partie importante de ce mémoire), nous pouvons cependant déjà remarquer que $\mathcal{M}_2(k)$ n'est pas à division mais inclure cette algèbre dans notre étude n'est pas anodin : toute algèbre à division de dimension finie peut-être aisément plongé dans une algèbre de matrice en identifiant un élément à la multiplication à gauche par ce dernier. Plus généralement nous aurons besoin de considérer un spectre plus large d'algèbre pour mieux comprendre les algèbres à divisions.

2 Algèbres centrales simples

2.1 Définition

Définition : Algèbres simples 2.1.1 Soit k un corps. On dit qu'une k-algèbre A est simple si ses idéaux bilatères sont exactement $\{0\}$ et A.

Remarque. Par exemple, toute les algèbres à division sont simples et $\mathcal{M}_n(k)$ où k est un corps est simple.

L'étude des algèbres centrales simple est un passage obligatoire pour définir le groupe de Brauer, c'est à dire, munir l'ensemble des algèbres à division centrales et de dimension finie sur un même corps d'une loi de groupe. Mais elles permettent aussi d'obtenir des informations sur la dimension des algèbres à division centrale de dimension finie.

Théorème de la dimension carré 2.1.2 Soit k un corps et A une k-algèbre centrale simple de dimension finie. Alors la dimension de A est un carré.

Remarque. C'est bien le cas des $\mathbb{R}$-algèbres centrales à division de dimension finie.

On démontrera ce théorème à la fin de cette partie.

2.2 Propriétés fondamentales des algèbres simples

Tout comme en théorie des repésentations, on peut définir la notion de A-module où A est une k-algèbre. Dans ce contexte un A-module S est A-simple dès lors qu'il ne contient pas d'autre sous A-module que $\{0\}$ ou S. Cela est cohérent avec la définition précédente de simple que nous avons donné car une algèbre A est simple si et seulement si elle est A-simple.

Lemme de Schur 2.2.1 Soit $\varphi : \ S_1 \longrightarrow S_2$ un morphisme d'algèbre entre deux algèbres simples. Alors φ est soit un isomorphisme soit le morphisme nul.

Démonstration. $\ker\varphi$ et resp. $\operatorname{Im}\varphi$ sont des idéaux bilatères de S_1 resp. S_2. Ils sont donc tous deux triviaux, en particulier si $\ker\varphi = S_1$ ou $\operatorname{Im}\varphi = \{0\}$ alors φ est le morphisme nul dans le cas contraire $\ker\varphi = \{0\}$ et $\operatorname{Im}\varphi = S_2$ et φ est un isomorphisme. □

Ce lemme sera fort utile à plusieurs reprises tout le long de ce texte. Il s'inspire également du lemme de Schur de la théorie des A-modules : tout morphisme de A-module entre A-modules simples est soit un isomorphisme, soit le morphisme nul. Il est commode par ailleurs de rappeler quelques définitions et théorèmes clefs de la théorie des A-modules, notamment pour la démontration de **2.6.1**. Nous ne démontrerons pas ces assertions car leur démonstration est très similaire à celle que nous avons pu rencontrer lors du cours d'Algèbre I avec la théorie de représentation.

Définition : Algèbres semi-simples 2.2.2 Un A-module sur un espace vectoriel V est dit semi-simple s'il peut s'écrire comme somme directe de A-modules simples. On rappelle qu'un A-module sur un espace vectoriel est simple s'il ne contient aucun autre sous-A-module que lui-même et $\{0\}$.

Théorème 2.2.3 Soit V un k-espace vectoriel munis d'une strucuture de A-module où A est une k-algèbre. Si V est semi-simple, alors il existe $V_1, \ldots, V_n$ des sous-A-modules :

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$$

Où n est un entier naturel et il existe $S_1, \ldots S_n$ des espaces vectoriels simples non deux à deux isomorphes et $m_1, \ldots, m_n$ des entiers tel que : $V_i \simeq S_i^{\oplus m_i}$ pour tout $1 \leqslant i \leqslant n$. De plus si S un sous-A-module simple de V alors il existe i tel que S_i est isomorphe à l'un des S_i et $S \subset V_i$.

Théorème 2.2.4 Tout sous-A-module d'un A-module semi-simple est semi-simple.

2.3 Produit tensoriel

On se propose ici de construire et d'énoncer quelques propriétés du produit tensoriel dans ce paragraphe, nous verrons que c'est un outil concret pour construire des algèbres centrales simple.

Propriété universelle du produit tensoriel 2.3.1 Soient k un corps et V et W deux k-espaces vectoriels. Alors il existe un k-espace vectoriel $V \otimes_k W$ et une application linéaire bilinéaire $\varphi : \ V \times W \longrightarrow V \otimes_k W$
$(v, w) \longmapsto v \otimes w$
tels que toute application bilinéaire $b : \ V \times W \longrightarrow E$ où E est un espace vectoriel, se factorise en une application $\bar{b} : \ V \otimes W \longrightarrow E$ telle que $b = \bar{b} \circ \varphi$.

Démonstration. On pourrait démontrer l'unicité à isomorphisme près de $V \otimes W$ mais on se contentera de construire un tel espace.

1. Définition de $V \otimes W$. Prenons $A = \bigoplus_{(v,w)\in V\times W} e_{(u,w)}$. Pour obtenir $V \otimes W$ on quotiente par les espaces suivants :
   (a) $\bigoplus_{(v,v',w)\in V^2\times W} (e_{(v+v',w)} - e_{(v,w)} - e_{(v',w)}) \cdot k$
   (b) $\bigoplus_{(v,w,w')\in V\times W^2} (e_{(v,w+w')} - e_{(v,w)} - e_{(v,w')}) \cdot k$

(c) $\bigoplus_{(v,w,\lambda)\in V\times W\times k} (e_{(\lambda\cdot v,w)} - \lambda\cdot e_{(v,w)})\cdot k$

(d) $\bigoplus_{(v,w,\lambda)\in V\times W\times k} (e_{(v,\lambda\cdot w)} - \lambda\cdot e_{(v,w)})\cdot k$

On note π l'application quotient $\pi : A \longrightarrow V\otimes W$.

2. On définit $\varphi : V\times W \longrightarrow V\otimes W$. Le fait d'avoir quotienté par les espaces $(a),(c)$ assure la linéarité
$(u,w)\longmapsto \pi(e_{v,w})$
à droite de φ, et pareillement à gauche pour $(b),(d)$.
3. On démontre la propriété universelle. Soit b une application bilinéaire $b : V\times W\longrightarrow E$ où E est un espace vectoriel. On définit sur une base de A, $\widehat{b} : A\longrightarrow E$. La bilinéarité de b permet de
$e_{(v,w)}\longmapsto b(v,w)$
faire passer au quotient $\widehat{b}$ en une application $\bar{b} : V\otimes W\longrightarrow E$ tel que $\widehat{b} = \bar{b}\circ\pi$. Dès lors si $u = \bar{b}\circ\varphi$, On a $u(v,w) = \bar{b}(\varphi(v,w)) = \bar{b}(\pi(e_{(v,w)})) = \widehat{b}(e_{(v,w)}) = b(v,w)$. Ainsi $\bar{b}\circ\varphi = b$ comme voulu.

□

Définition : Extension des scalaires 2.3.2 Soient k un corps, K un surcorps de k et V un k-espace vectoriel. On note V_K l'extension des scalaires de V par K l'espace vectoriel $V\otimes_k K$, où $\lambda\cdot(v\otimes\mu) = v\otimes(\lambda\times\mu)$.

Étendre les scalaires formalise le plongement $k^n\subset K^n$. Pour faire un tel plongement il fallait nécessaiement fixer une base de V, l'extension des scalaire n'en nécessite pas. Une propriété remarquable est que $\dim_k k^n = \dim_K K^n = n$. Cette propriété est toujours vraie pour l'extension des scalaires.

Théorème : écriture et produits tensoriels 2.3.3 Soient k un corps et V et W deux k-espaces vectoriels. On prend $(v_i)_{i\in I}$ et $(w_j)_{j\in J}$ des bases de V et W. Alors :

1. $(v_i\otimes w_j)_{(i,j)\in I\times J}$ est une base de $V\otimes W$. En particulier si V et W sont de dimensions finies, alors $\dim_k V\otimes W = \dim_k V\times\dim_k W$.
2. Tout vecteur de $x\in V\otimes W$ s'écrit sous la forme $x = \sum_{i=1}^{n} v_i\otimes w_i'$ où les w_i' sont uniques. En particulier $\dim_k V_k = \dim_K V_K$ où K est un surcorps de k.

Démonstration. 1. L'espace vectoriel A est engendré par les $e_{(v,w)}$ donc $V\otimes W$ est engendré par les $v\otimes w = \pi(e_{(v,w)})$. Cependant si $v = \sum_{i\in I}\lambda_i\cdot v_i$ et $w = \sum_{j\in J}\mu_j\cdot w_j$, alors $v\otimes w = \sum_{i,j\in I\times J}\lambda_i\mu_j v_i\otimes w_j$ donc $(v_i\otimes w_j)_{(i,j)\in I\times J}$ est générateur. (On sous-entendra à chaque fois que les coefficients sont presque nuls.)
Prenons $b_{i_0,j_0} : V\times W\longrightarrow k$. Alors elle se factorise en une application linéaire
$\sum_{i\in I}(\lambda_i\cdot v_i, \sum_{j\in J}\mu_j\cdot w_k)\longmapsto \lambda_{i_0}\mu_{j_0}$
$\bar{b}_{i_0,j_0} : V\otimes W\longrightarrow k$. Donc si $\sum_{i,j\in I\times J}\lambda_{ij}v_i\otimes w_j = 0$ on applique $\bar{b}_{i_0j_0}$ de part et d'autre
$\sum_{i,j\in I\times J}\lambda_{ij}v_i\otimes w_j\longmapsto\lambda_{i_0j_0}$
pour obtenir $\lambda_{ij} = 0\ \forall(i,j)\in I\times J$.

2. Soit $x\in V\otimes W$ alors $x = \sum_{i,j\in I\times J}\lambda_{ij}v_i\otimes w_j = \sum_{i\in I}v_i\otimes(\sum_{j\in J}\lambda_{ij}\cdot w_j) = \sum_{i\in I}v_i\otimes w_i'$. Pour l'unicité si $\sum_{i\in I}v_i\otimes w_i' = 0$, alors on écrit $w_i' = \sum_{j\in J}\lambda_{ij}\cdot w_j$, on dévelloppe et on utilise l'unicité de 1).

□

Définition : produit tensoriel d'algèbres 2.3.4 Si k est un corps et A et B deux k-algèbres. Alors $A\otimes B$ peut être muni d'une structure d'algèbre avec $(a\otimes b)\times(a'\otimes b') = (a\times a')\otimes(b\times b')$.

On démontre aisément qu'il s'agit bien d'une k-algèbre.
Donnons quelques exemples que nous démontrerons en détail plus tard :

1. $k \otimes A \simeq A$ où A est une k-algèbre.
2. $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathcal{M}_2(\mathbb{C})$ car $\mathbb{H}$ est une $\mathbb{C}$-base de $\mathcal{M}_2(\mathbb{C})$.
3. $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq \mathcal{M}_4(\mathbb{R})$ avec l'isomorphisme induit par l'application bilinéaire $\varphi : \mathbb{H} \times \mathbb{H} \longrightarrow \mathcal{L}(\mathbb{H})$ où $(q_1, q_2) \longmapsto L_{q_1} R_{\overline{q_2}}$
   L_q est la multiplication à gauche par q et R_q la multiplication à droite et $\bar{\cdot}$ est la conjuguaison des quaternions.
4. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$ avec l'isomorphsime induit par l'application bilinéaire $\varphi : \mathbb{C} \times \mathbb{C} \longrightarrow C \times \mathbb{C}$ $(z_1, z_2) \longmapsto (z_1 z_2, z_1 \overline{z_2})$

Proposition 2.3.5 Soient k un corps, $n > 0$ un entier naturel et A une k-algèbre. Alors :

$$\mathcal{M}_n(k) \otimes A \simeq \mathcal{M}_n(A)$$

Démonstration. On considère

$$\begin{aligned} \varphi : \ \mathcal{M}_n(k) \times A &\longrightarrow \mathcal{M}_n(A) \\ (E_{(i,j)}, a) &\longmapsto a E_{(i,j)} \end{aligned}$$

Où $E_{(i,j)} = (\delta_{(i,j),(k,l)})_{1 \leqslant k,l \leqslant n}$ C'est une application k-bilinéaire elle se factorise donc en une application k-linéaire $\bar{\varphi}$ de $\mathcal{M}_n(k) \otimes A$ dans $\mathcal{M}_n(A)$. Elle est aisément bijective et c'est un morphisme d'anneau (on peut le vérifier sur une base). □

En particuler $\mathcal{M}_n(k) \otimes \mathcal{M}_m(k) \simeq \mathcal{M}_n(\mathcal{M}_m(k)) \simeq \mathcal{M}_{nm}(k)$ On ne démontrera pas le dernier isomorphisme, il reflète l'essence du calcul de matrice par bloc.

2.4 Produit tensoriel d'Algèbres centrales simples

L'objet de cette partie est de démontrer le théorème suivant :

Théorème 2.4.1 Soit k un corps et A et B deux k-algèbres centrales simples de dimension finie. Alors $A \otimes B$ est aussi une k-algèbre centrale simple de dimension finie.

Nous allons découper la preuve de ce théorème en deux parties : nous allons d'abord montrer que $A \otimes B$ est centrale (aisé) puis nous montrerons que $A \otimes B$ est simple (plus compliqué).

Lemme 2.4.2 Soient k un corps et A et B deux algèbres centrales. Alors $A \otimes B$ est une k-algèbre centrale.

Démonstration. Soit $(b_i)_{i \in I}$ une k-base de B. On sait alors que tout élément $x \in A \otimes B$ s'écrit sous la forme $x = \sum_{i \in J} a_i \otimes b_i$ où $a_i \in A$ sont uniques et $J \subset I$ est fini. Soit $x \in Z(A \otimes B)$ un tel élément alors si $a \in A$ on dispose de :

$$a \otimes 1 \cdot x = \sum_{i \in J} (a_i \cdot a) \otimes b_i = \sum_{i \in J} (a \cdot a_i) \otimes b_i = x \cdot a \otimes 1$$

Par unicité on en déduit $a \cdot a_i = a_i \cdot a$ pour tout $i \in J$ et $a \in A$ ainsi $a_i \in Z(A) = k$. En réarrangeant les termes, x s'écrit $x = 1 \otimes b$ où $b \in B$ et on conclut de la même façon que $b \in Z(B) = k$ ainsi $x \in k$ ce qui conclut. □

Théorème 2.4.3 Soit k un corps et R et S deux k-algèbres avec S centrale simple. On pose $A = R \otimes S$ et I un idéal bilatère de A non nul. Alors $I \cap (R \otimes 1) \neq \{0\}$.

Démonstration. Prenons $x \in I$ non nul avec $x = \sum_{i=1}^{l} r_i \otimes s_i$ avec l un entier naturel non nul choisi minimal (dans le sens où il n'existe pas d'élément y non nul de I s'écrivant $\sum_{i=1}^{l'} r'_i \otimes s'_i$ où $l' < l$) et $r_i \in R$ et $s_i \in S$ pour tout $1 \leqslant i \leqslant l$. Deux remarques sont à faire :

1. Dans ce cas les r_i sont libres. En effet si $r_{i_0} = \sum_{i \neq i_0} \lambda_i \cdot r_i$ où $\lambda_i \in k$ pour $i \neq i_0$ alors on peut écrire x avec un nombre strictement moindre de terme ce qui contredit la minimalité de l.
2. On peut choisir $s_1 = 1$. En effet, on considère l'idéal bilatère engendré par s_1, par simplicité de S celui-ci est donc égal à S. Or $1 \in S =< s_1 >$ Donc il existe $n \in \mathbb{N}^*$ et $x_j, y_j \in S$ pour $1 \leqslant j \leqslant n$ tel que $1 = \sum_{j=1}^{n} x_j s_1 y_j$. Ainsi en prenant $x' := \sum_{j=1}^{n} (1 \otimes x_i) \cdot x \cdot (1 \otimes y_i)$ on obtient ainsi $x' = \sum_{i=1}^{l} r_i \sum_{j=1}^{n} x_j \cdot s_j \cdot y_j$. Soit en posant $s'_i = \sum_{j=1}^{n} x_j \cdot s_j \cdot y_j$ on a $s'_1 = 1$.

Il reste dès lors à utiliser le caractère centrale de S. Soit $s \in S$ on considère :

$$(1 \otimes s) \cdot x' - x' \cdot (1 \otimes s) = \sum_{i=1}^{l} r_i \otimes (s'_i \cdot s - s \cdot s'_i) = \sum_{i=2}^{l} r_i \otimes (s'_i \cdot s - s \cdot s'_i) \in I$$

Car le terme $i = 1$ est nul étant donné que $s'_i = 1$. Ainsi par minimalité de l la quantité calculée est nulle. Vu que les $(r_i)_{1 \leqslant i \leqslant n}$ sont libres on dispose de $s \cdot s'_i = s'_1 \cdot s$. Ainsi $s_1 \in Z(S) = k$ donc x' s'écrit simplement $x' = 1 \otimes \sum_{i=1}^{l} r_i \cdot s'_i \in I \cap (R \otimes 1)$ donc l'ensemble $I \cap (R \otimes 1)$ est non nul. □

On peut ainsi prouver le caratère simple de $A \otimes B$. Soit I un idéal bilatère de $A \otimes B$ non nul alors $I \cap (B \otimes 1) \neq \{0\}$ car A est central simple donc $I \cap (B \otimes 1) = (B \otimes 1)$ par simplicité de B. Ainsi I contient tout les tenseurs purs car si $b \in B$ et $a \in A$ alors $a \otimes 1 \cdot 1 \otimes b = a \otimes b \in I$. Donc $I = A \otimes B$.

2.5 Algèbres opposées

Le théorème **2.4.1** sera crucial pour bien définir le groupe de Brauer dans la partie **3**. Il admet néanmoins une conséquence directe qui elle aussi sera très utile, pour cela définissons la notion d'anneau opposé.

Définition : Anneau opposé 2.5.1 Soit $(A, +, \cdot)$ un anneau. On note $(A^{opp}, +_{opp}, \cdot_{opp})$ l'anneau définit par

1. $A^{opp} = A$
2. $a +_{opp} b = a + b$
3. $a \cdot_{opp} b = b \cdot a$

On définit de même la notion d'agèbre opposée.

Remarque. Si A est simple alors A^{opp} est également simple et on a aisément $(A^{opp})^{opp} = A$. Une autre façon de voir l'opposée d'une algèbre est de remarquer que $A^{opp} \simeq \mathrm{End}_A(A) =$ endomorphismes A-linéaires, par l'application $\varphi : \mathrm{End}_A(A) \longrightarrow A^{opp}$.

$$f \longmapsto f(1_A)$$

Le théorème suivant concerne le produit tensoriel d'une algèbre centrale simple par son algèbre opposée.

Théorème 2.5.2 Soit k un corps et A une k-algèbre centrale simple de dimension finie égale à n, alors :

$$A \otimes A^{opp} \simeq \mathcal{M}_n(k)$$

Démonstration. On considère l'application $\varphi : \begin{array}{ccc} A \times A^{opp} & \longrightarrow & \mathcal{L}(A) \\ (a,b) & \longmapsto & x \longmapsto axb \end{array}$ bilinéaire. Elle induit donc une application entre k-espaces vectoriels $\bar{\varphi} : \begin{array}{ccc} A \otimes A^{opp} & \longrightarrow & \mathcal{L}(A) \\ a \otimes b & \longmapsto & x \longmapsto axb \end{array}$. Cependant si $x \in A$ et $a, b, a', b' \in A$ alors $\bar{\varphi}((a \cdot a') \otimes (b \cdot_{opp} b'))(x) = (a \cdot a')x(b \cdot_{opp} b') = aa'xb'b = a(a'xb')b = [\bar{\varphi}(a \otimes b) \circ \bar{\varphi}(a' \otimes b')](x)$. Ainsi $\bar{\varphi}$ est un morphisme de k-algèbres, par le lemme de Schur (les deux algèbres sont simples), $\bar{\varphi}$ est donc un ismorphisme ou le morphisme nul. $\bar{\varphi}$ est donc un isomorphisme car son image est non nulle. □

Il est fréquent qu'un anneau soit isomorphe à son anneau opposé, d'une part lorsqu'il est commutatif et d'autre part pour la majorité des algèbres que nous connaissons (les algèbres de quaternions, les algèbres de matrices et les algèbres de la forme $k[G]$ ou k est un corps et G est un groupe).

Théorème 2.5.3 Soit k un corps et A (resp. un anneau) une k algèbre. On suppose qu'il existe $\varphi : A \longrightarrow A$ un isomorphisme de k-linéaire (resp. de groupe) vérifiant pour tout $(x, y) \in A^2$:

$$\varphi(xy) = \varphi(y)\varphi(x)$$

alors A est isomorphe à son algèbre (resp. anneau) opposé

Démonstration. Si $x, y \in A$ alors $\varphi(xy) = \varphi(y)\varphi(x) = \varphi(x) \cdot_{opp} \varphi(y)$ dès lors l'application $\widehat{\varphi} : \begin{array}{ccc} A & \longrightarrow & A^{opp} \\ & & x \longmapsto \varphi(x) \end{array}$ est un isomorphisme d'algèbre (ou d'anneau). □

Remarque. Le théorème s'applique aux matrices avec la transposition et aux quaternions avec le conjugué (défini rigoureusement dans la définition **4.2.1**)

2.6 Classification des algèbres centrales simples

Théorème 2.6.1 Soit k un corps et A une k-algèbre centrale simple de dimension finie. Alors il existe, à isomorphisme près, une unique k-algèbre centrale à division D et n un unique entier naturel tel que :

$$A \simeq \mathcal{M}_n(D)$$

Démonstration. Prenons S un idéal non nul à gauche de A de dimension minimal. S est donc un A-module simple. On considère l'application $\varphi : \begin{array}{ccc} A & \longrightarrow & \mathcal{L}(S) \\ a & \longmapsto & L_a \end{array}$ où L_a est la multiplication à gauche par a. Cette application est injective (si $L_a \in \ker\varphi$ alors $L_a(1) = 0 = a$). De manière plus générale on va considérer $s_1, \ldots, s_p$ une famille génératrice de S et $\psi : \begin{array}{ccc} A & \longrightarrow & S^p \\ a & \longmapsto & (as_1, \ldots, as_p) \end{array}$. Cette application est toujours injective car si $a \in \ker\psi$ alors $\forall s \in S$, $as = 0$ donc $a \in \ker\varphi = \{0\}$. Ainsi $A \simeq \psi(A)$. Cependant $\psi(A)$ est un sous-module de S^p donc il existe $n \leqslant p$ tel que $A \simeq \psi(A) \simeq S^n$ car S est simple.

Cependant $A^{opp} \simeq \mathrm{End}_A(A) \simeq \mathrm{End}_A(S^n) \simeq \mathcal{M}_n(\mathrm{End}_A(S))$. On pose ainsi $D = \mathrm{End}_A(S)^{opp}$. Montrons que D est à division, pour cela il suffit de montrer que $\mathrm{End}_A(S)$ est à division, c'est le cas par le lemme de Schur. Dès lors $A = (A^{opp})^{opp} \simeq (\mathcal{M}_n(\mathrm{End}_A(S)))^{opp} \simeq \mathcal{M}_n(\mathrm{End}_A(S)^{opp}) \simeq \mathcal{M}_n(D)$. L'unicité est aisée : D est uniquement déterminée par S lui même uniquement determiné par l'unicité de la décomposition en modules simples.

De plus D est bien centrale car $Z(\mathcal{M}_n(D)) = Z(D) \simeq Z(A) = k$. En effet soit $u \in Z(\mathcal{M}_n(D))$. Soit $x \in D^n$ et $v \in \mathcal{M}_n(D)$ un projecteur d'image $D \cdot x$. Alors $u(x) = u(v(x)) = v(u(x)) \in D \cdot x$. Dès lors $(u(x), x)$ est liée pour tout vecteur $x \in D^n$ donc u est une homothétie, et l'ensemble des homothéties est isomorphe à D. □

Pour démontrer le théorème de la dimension carrée **2.1.2** il suffit donc de montrer que toute algèbre à division centrale de dimension finie est de dimension carrée. Il s'agit ici d'étendre D aux scalaires dans K pour mieux comprendre la structure de D. Montrons dans un premier temps que le caractère centrale simple passe à l'extension des scalaires.

Lemme 2.6.2 Si k est un corps, K une extension de k et A une k-algèbre centrale simple alors la K-algèbre $D_K = D \otimes_k K$ est centrale simple.

Démonstration. Les deux points à montrer sont très similaire aux démonstrations de la sous-partie 2.4. □

Théorème 2.6.3 Soit k un corps et D une k-algèbre centrale à division de dimension finie. Alors D a la dimension d'un carré.

Démonstration. Soit K la clôture algébrique de k. On considère $D_K = D \otimes_k K$ l'extension des scalaire de D. D'après le théorème précédent il existe une K-algèbre à division E de dimension finie tel que $D \simeq \mathcal{M}_n(E)$. Cependant $E \simeq K$ car K est algébriquement clôs. Ainsi $\dim_k D = \dim_K D_K = \dim_K \mathcal{M}_n(K) = n^2$, ce qui conclut. □

3 Le groupe de Brauer

Nous avons à présent tous les éléments pour définir le groupe de Brauer.

3.1 Définition

Pour un corps k fixé on va considérer E l'ensembles des k-algèbres centrales simples de dimension finie. Si on munit E du produit tensoriel cela ne munit guère E d'une loi de groupe car la dimension ne fait que croître à mesure que l'on tensorise.

Pour contrer ce problème on munit E de la relation d'équivalence suivante, soit $A, B \in E$:

$$A \sim B \iff \text{il existe } n, m \in \mathbb{N} \text{ tel que } \mathcal{M}_n(A) \simeq \mathcal{M}_m(B)$$

Pour montrer que c'est bien une relation d'équivalence, seul la transitivité est un point non trivial. Supposons $A \sim B$ et $B \sim C$ où $A, B, C \in E$ plus précisément on suppose $\mathcal{M}_n(A) \simeq \mathcal{M}_m(B)$ et $\mathcal{M}_k(B) \simeq \mathcal{M}_l(C)$. Alors $\mathcal{M}_{nk}(A) \simeq \mathcal{M}_k(\mathcal{M}_n(A)) \simeq \mathcal{M}_{mk}(B) \simeq \mathcal{M}_m(\mathcal{M}_l(C)) \simeq \mathcal{M}_{ml}(C)$.

On montre que le produit tensoriel passe au quotient. Soient $A \sim A'$ avec $A, A' \in E$ et $B \in E$. Alors si $\mathcal{M}_n(A) \simeq \mathcal{M}_m(A')$ On dipose de (d'après le Théorème **2.2.5**) :

$$\mathcal{M}_n(A \otimes B) \simeq \mathcal{M}_n(k) \otimes A \otimes B \simeq \mathcal{M}_n(A) \otimes B \simeq \mathcal{M}_m(A') \otimes B \simeq \mathcal{M}_m(k) \otimes A' \otimes B \simeq \mathcal{M}_m(A' \otimes B)$$

Théorème 3.1.1 Soit k un corps. Alors $E/\sim$ est en bijection avec les k-algèbres à division centrale de dimension finie à isomorphisme près.

Démonstration. Il est clair que si que algèbres de E sont isomorphes alors elles sont en relation par $\sim$. Prenons maintenant $A \in E$ il existe d'après le Théorème **2.6.1** $D \in E$ à division telle que $A \sim D$. De plus si $D, D' \in E$ sont deux algèbres à division, la partie unicité du Théorème **2.6.1** assure que $D \sim D' \iff D \simeq D'$. On a ainsi établit que $E/\sim$ est en bijection avec l'ensemble des algèbres de E à division. □

Proposition-définition 3.1.2 L'ensemble $E/\sim$ munit du produit tensoriel est un groupe abélien. Ce groupe est appelé groupe de Brauer et est noté $\mathrm{Br}(k)$.

Démonstration.

1. L'associativité découle de l'associativité du produit tensoriel à isomorphisme près.
2. Le neutre est aisément l'algèbre k. Si $A \in E$ alors $\overline{A} \otimes \overline{k} = \overline{A \otimes k} = \overline{A}$
3. L'inverse d'une algèbre A est son algèbre opposée d'après le théorème **2.5.2**.
4. Le groupe est abélien d'après la commutativité du produit tensoriel à isomorphisme près.

□

On peut ainsi résumer nos travaux exposés dans l'introduction (lemme **1.1.2** et le théorème de Frobenius **1.2.3**) sous la forme suivante :

Proposition 3.1.3

— $\mathrm{Br}(K) = \{K\} \simeq \{0\}$ si K est algébriquement clôs.

— $\mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\} \simeq \mathbb{Z}/2\mathbb{Z}$

3.2 Le théorème de Wedderburn

Le but de cette partie est de calculer le groupe de Brauer d'un corps fini.

Théorème de Wedderburn 3.2.1 Soit k un corps fini D une k-algèbre à division finie centrale. Alors $D = k$.

La preuve est très élémentaire et est inspirée du livre de Daniel Perrin [Per96].

Démonstration. Si $q = |k|$ alors $|D| = q^n$ où n est la dimension de D.

Si $D \neq k$ alors $n > 1$. $D^\times$ opère sur lui-même par automorphisme intérieur. pour $x \in D^\times$ on note $o(x)$ l'orbite de x. On pose $D_x = \{y \in D \mid yx = xy\}$, sous algèbre à division de D. Le stabilisateur de x est $D^\times$. De la même façon on a $|D_x| = q^d$ et $d \mid n$ (Pour le démontrer on peut remarquer que D est un sous-espace vectoriel à gauche sur D_x). Dès lors $|o(x)| = \frac{q^n-1}{q^d-1}$.

On a dans $\mathbb{Z}$: $q^n - 1 = \prod_{m|n} \Phi_m(q)$ et similairement $q^d - 1 = \prod_{m|d} \Phi_m(q)$ donc $\frac{q^n-1}{q^d-1} = \prod_{m|n \text{ et } m\nmid d} \Phi_m(q)$.

Ainsi, $|D^\times| = |k^\times| + \sum_{x \notin k} |o(x)|$. Dès lors que $x \notin k$ on dispose de $q^n - 1 = q - 1 + \sum_{d|n} \frac{q^n-1}{q^d-1}$. Ainsi $|\Phi_n(q)| \leqslant q - 1$ car $|\Phi_n(q)| \mid q - 1$.

Mais $\Phi_n(q) = (q - \zeta_1) \cdot \cdots \cdot (q - \zeta_p)$ où $\zeta_1, \dots \zeta_p \in \mathbb{C}$ sont les racines primitives n-ièmes de 1 et vérifient toutes $|\zeta_i| = 1$ mais $\zeta_i \neq 1$. Dès lors, $|\zeta_i - q| > q - 1$ (faire un dessin) et donc $|\Phi_n(q)| > (q-1)^p \geqslant q - 1$. Contradiction. Ainsi $x \in k$ et $k = D$. □

Corollaire 3.2.2 Si k est un corps fini alors $\mathrm{Br}(k) = \{k\} \simeq \{0\}$

3.3 Sous-groupe des algèbres de Quaternion de $\mathbb{Q}$

Nous savons désormais calculer le groupe de Brauer de nombreux corps que nous connaissons, cependant l'un d'entre eux se démarque particulièrement : il s'agit de $\mathbb{Q}$. Nous consacrerons le reste de ce mémoire à explorer la structure de $\mathrm{Br}(\mathbb{Q})$.

Il est tout d'abord utile de nous intéresser aux algèbres à divisions centrales de petites dimensions. Comme nous savons que la dimension des algèbres à division centrales est un carré, le plus petit carré intéréssant dans notre étude est donc 4 (en dimension 1 on ne retrouve que l'algèbre triviale composée du corps k uniquement). Le théorème suivant classifie les algèbres à division centrales de dimension 4.

Théorème : classification des k-algèbres centrales à division de dimension 4 3.3.1 Soit k un corps de caractéristique $\neq 2$. Alors toute k-algèbre centrale à division de dimension 4 est une algèbre de quaternion.

Démonstration. Prenons $x \in D \diagdown k$. On pose $K = k[x] \subset D$ un sous-corps de D (sous-algèbre de D intègre en dimension fini et commutative). Dès lors

$$\dim_k D = \dim_K D \times \dim_k K \ (*)$$

Ainsi $\dim_K D = 1$, 2 ou 4. Mais :

— Si $\dim_K D = 1$ alors $K \simeq D$ c'est absurde car D est centrale et K est commutatif.

— Si $\dim_k K = 1$ alors $K = k$ et ainsi $x \in k$.

Ainsi $\dim_k D = \dim_k K = 2$. Dès lors $(1, x, x^2)$ est lié et il existe $\alpha, \beta \in k$ tel que $(x-a)^2 = \beta$ (comme k est de caractéristique $\neq 2$ on peut mettre tout polynôme de degré 2 sous forme canonique). On remplace x par $x - \alpha$

Prenons $s : \begin{array}{ccc} D & \longrightarrow & D \\ t & \longmapsto & xtx^{-1} \end{array}$. On dispose de $s^2 = 1$, donc $(s+1)(s-1)$. Comme $1 \neq -1$, s est diagonalisable dans le k-espace vectoriel D. Ainsi on prend y un -1-vecteur propre de s. On dispose de $xy = -yx$.

Annaloguement on peut écrire $y^2 = ay + b$. Mais d'une part : $s(y^2) = xy^2x^{-1} = xyx^{-1}xyx^{-1} = y^2 = ay + b$ et d'autre part : $s(y^2) = s(ay + b) = -ay + b$. Dès lors $y^2 = \frac{b}{2}$. D'où $D \simeq \left(\frac{\beta, \frac{b}{2}}{k}\right)$.

Prouvons $(*)$. Soit $n = \dim_K D$ et $m = \dim_k K$. Ainsi $(1, x, x^2, \ldots, x^{m-1})$ est une base de K. Soit $(d_1, \ldots, d_n)$ une K-base de D. Montrons que $(d_i \times x^j)_{1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m-1}$ est une k-base de D. Si $z \in D$ alors $z = \sum_{i=1}^{n} \Lambda_i d_i$ où $\Lambda_i \in K$. Mais $\Lambda_i = \sum_{j=0}^{m-1} \lambda_{ij} x^j$. Donc $z = \sum_{i=1}^{n} \sum_{j=0}^{m-1} \lambda_{ij} d_i x^j$, la famille est bien génératrice. Réciproquement si $\sum_{i=1}^{n} \sum_{j=0}^{m-1} \lambda_{ij} d_i x^j = 0$ on reviens à l'écriture $z = \sum_{i=1}^{n} \Lambda_i d_i = 0$, donc $\Lambda_i = 0\ \forall i, 1 \leqslant i \leqslant n$, par liberté de $(d_1, \ldots, d_n)$. Puis $\Lambda_i = \sum_{j=0}^{m-1} \lambda_{ij} x^j = 0$ et donc $\lambda_{ij} = 0$ par liberté de $(1, x, x^2, \ldots, x^{m-1})$ ce qui conclut. □

La structure de $\mathrm{Br}(\mathbb{Q})$ nécessitant beaucoup de travail pour être percée à jour, nous étudierons un sous-groupe particulier de $\mathrm{Br}(\mathbb{Q})$, celui des algèbres de quaternion (on vient de « montrer » que c'est le plus petit sous-groupe intéréssant).

Proposition 3.3.2 Les algèbres de quaternions forment un sous-groupe de $\mathrm{Br}(\mathbb{Q})$.

Démonstration.

1. L'élément neutre $\mathcal{M}_2(\mathbb{Q}) = \left(\frac{1, 1}{\mathbb{Q}}\right)$ est une algèbre de quaternion.
2. Une algèbre de quaternion est sa propre algèbre opposée.
3. Si H_1,H_2 sont deux algèbres de quaternions sur $\mathbb{Q}$ alors il existe une algèbre à division D et un entier naturel n tel que $\mathcal{M}_n(D) \simeq H_1 \otimes H_2$ en particuler $n^2 d = 16$. Ainsi :
   - Si $\dim_{\mathbb{Q}} D = 1$ alors $H_1 \otimes H_2 \sim \mathbb{Q} \sim \mathcal{M}_2(\mathbb{Q})$ qui est une algèbre de quaternion.
   - Si $\dim_{\mathbb{Q}} D = 4$ alors D est une algèbre de quaternion.
   - Le cas $\dim_{\mathbb{Q}} D = 16$ ne se produit jamais car dans ce cas $D = H_1 \otimes H_2$ est à division. Nous le montrerons plus tard.

□

3.4 Exemple d'une $\mathbb{Q}$-algèbre à division qui n'est pas une algèbre de quaternion

Toutes les algèbres à division non triviales étudiées ici ont été des algèbres de quaternion. Une question légitime à ce stade est de se demander si les algèbres à division sont toutes des algèbres de quaternion. La réponse est non et nous allons construire grâce au livre de Blanchard [Bla72] un exemple d'une algèbre à division sur $\mathbb{Q}$ de dimension 9 (c'est bien un carré !).

Étape 1 Nous allons construire un surcorps intermédiaire L d'extension finie sur $\mathbb{Q}$. On pose simplement $L = \mathbb{Q}(\cos(\frac{2\pi}{7}))$. Pour simplifier les calculs on se place dans un premier temps dans $\mathbb{Q}(\exp(\frac{2\pi}{7}))$ et on pose volontier $\theta = \exp(\frac{2\pi}{7})$. On dispose ainsi de $\theta^6 + \theta^5 + \cdots + 1 = 0$. On pose dès lors :

$$\begin{cases} \theta + \theta^6 & = u = \cos(\frac{2\pi}{7}) \\ \theta^2 + \theta^5 & = v = \cos(\frac{4\pi}{7}) \\ \theta^3 + \theta^4 & = w = \cos(\frac{6\pi}{7}) \end{cases}$$

Le calcul nous donne $u+v+w=-1$ et $\begin{cases} u^2 &= v+2 \\ v^2 &= w+2 \\ w^2 &= u+2 \end{cases}$ puis $\begin{cases} uv &= w+u \\ vw &= u+v \\ wu &= v+w \end{cases}$ Il en découle ainsi $uv+vw+wu=-2$ et $uvw=uw+w^2=v+w+u+2=1$. Ainsi u,v et w sont racines du polynôme $P=X^3+X^2-2X-1$. P est irréductible car de degré 3 et ne possède aucune racine rationnelle (les racines rationnelles ne peuvent être que 1 et -1, ce n'est clairement pas le cas). Ainsi on a démontré le théorème suivant :

Théorème 3.4.1 $L=\mathbb{Q}(u)=\mathrm{Vect}_{\mathbb{Q}}(1,u,u^2)=\mathrm{Vect}_{\mathbb{Q}}(u,v,w)$ et $\dim_{\mathbb{Q}} L=3$

Il sera ici commode prendre comme base (u,v,w) au vu de la symétrie de la table de multiplication.

Étape 2 On introduit l'autmorphisme σ uniquement défini par l'image sur une base $\sigma(u)=v,\sigma(v)=w,\sigma(w)=u$. C'est bien bijectif au vu de la matrice de σ dans la base (u,v,w), c'est bien multiplicatif au vu de la symétrie de la table de multiplication. On défini également une **norme** notée N. On la défini de deux façons équivalentes :

Proposition-définition 3.4.2 Les deux quantités suivantes sont égales et sont notée $N(\xi)$ où $\xi\in L$

1. $N(\xi)=\det(\Xi)$ où Ξ est l'opérateur linéaire de multiplication par ξ.
2. $N(\xi)=\xi\times\sigma(\xi)\times\sigma^2(\xi)$

Démonstration. Si $\xi\in\mathbb{Q}$ c'est évident. Maintenant si $\xi\in L\setminus\mathbb{Q}$ alors on a $\xi\neq\sigma(\xi)$ en effet sinon on écrit $\xi=xu+yv+zw$ où $x,y,z\in\mathbb{Q}$, cette information fournirait $x=y=z$ donc $\xi=x(u+v+w)=-x\in\mathbb{Q}$. De la même façon les nombres $\xi,\sigma(\xi),\sigma^2(\xi)$ sont deux à deux distncts. On note μ le polynôme minimal de ξ. On prétend que $\mu=(X-\xi)(X-\sigma(\xi))(X-\sigma^2(\xi))$. En effet $\mu(\sigma(\xi))=\sigma(\mu(\xi))=\sigma(0)=0$ car σ est un automorphisme de corps. De plus $\deg\mu\leqslant 3$ car $\dim_{\mathbb{Q}} L=3$ donc la famille $(1,\xi,\xi^2,\xi^3)$ est liée et donc ξ est annulé par un polynôme de degré inférieur à 3. Ainsi μ possède 3 racine distinctes et est de degré au plus 3 d'où la formule.

On considère maintenant le polynôme minimale de Ξ, c'est le même que celui de μ (on ne le démontrera pas). Ainsi le polynôme minimale et caractéristiquent coïncident. Dès lors on identifie le déterminant comme l'opposé du coefficiant constant : soit le produit des racines. □

Étape 3 On construit l'algèbre D.

On considère formellement D comme la $\mathbb{Q}$-algèbre formé des combinaisons linaires formelles $\xi+a\eta+a^2\zeta$ où $\xi,\eta,\zeta\in L$ avec :

$$a\cdot a=a^2,\ a^2\cdot a=a\cdot a^2=2 \text{ et } \xi\cdot a=a\cdot\sigma(\xi),\ \xi\cdot a^2=a^2\cdot\sigma^2(\xi)$$

On peut aussi donner directement la table de multiplication :

$$(\xi+a\eta+a^2\zeta)\cdot(\xi'+a\eta'+a^2\zeta')=\begin{array}{lll} \xi\xi' & +2\sigma(\zeta)\eta' & +2\sigma^2(\eta)\zeta' \\ a(\eta\xi' & +\sigma(\xi)\eta' & +2\sigma^2(\zeta)\zeta') \\ a^2(\zeta\xi' & +\sigma(\eta)\eta' & +\sigma^2(\xi)\zeta') \end{array}$$

Au vu de cette dernière, D n'est clairement pas commutative. On vérifie à la main (on ne le fera pas c'est beaucoup trop long et lourd) l'associativité.

Théorème 3.4.3 L'algèbre ci-dessus est une algèbre à division de dimension 9.

Démonstration. Pour la dimension on utilise un argument similaire pour la classification des algèbres centrale de dimension 4. Il suffit ici de montrer que tout montrer que $\varphi:\ q\in K\longrightarrow qq'$ où $q'=\xi+a\eta+a^2\zeta\neq 0$ et on calcule le déterminant de la matrice de multiplication.

$$\det\begin{bmatrix}\xi & 2\sigma(\zeta) & 2\sigma^2(\eta)\\ \eta & \sigma(\xi) & 2\sigma^2(\zeta)\\ \zeta & \sigma(\eta) & \sigma^2(\xi)\end{bmatrix}=N(\xi)+2N(\eta)+4N(\zeta)-2(\xi\sigma(\eta)\sigma^2(\zeta)+\zeta\sigma(\xi)\sigma^2(\eta)+\eta\sigma(\zeta)\sigma^2(\xi))$$

On se ramène au cas où les nombres ξ,η,ζ ont des composantes entières. Puis par multiplication par a ou a^{-1} on se ramène au cas où les coordonnées de ξ sont non toutes paires. L'expression ci-dessus est donc impaire donc non nulle. □

Théorème 3.4.4 Le centre de D est $\mathbb{Q}$. Et tout éléments $q \in D \setminus \mathbb{Q}$ a un polynôme minimal de degré 3.

Démonstration. Les sous-corps commutatifs de D ne peuvent pas être de dimension 9 car D n'est pas commutatif. Ainsi si $x \in D \setminus \mathbb{Q}$ on a :

$$9 = \dim_{\mathbb{Q}} D = \dim_{\mathbb{Q}(x)} D \times \dim_{\mathbb{Q}} \mathbb{Q}(x)$$

Dès lors $\dim_{\mathbb{Q}} \mathbb{Q}(x) = 3$. Ainsi si $Z(D) \neq \mathbb{Q}$ alors $\dim_{\mathbb{Q}} Z(D) = 3$ et donc par égalité des diemsions on a $Z(D) = \mathbb{Q}(x)$. Ceci impliquerait l'algèbre commutative car on peut en réalité choisir x quelconque. Ainsi $Z(D) = \mathbb{Q}$. □

4 Forme quadratiques et quaternions sur $\mathbb{Q}$

4.1 Généralités sur les formes quadratiques

Nous introduisons ici les formes quadratiques pour exposer dans la partie suivante une correspondance entre les algèbres de quaternion d'un corps et ses formess quadratiques.

Définition 4.1.1 Soit k un corps de caractéristique $\neq= 2$ et V un k-espace vectoriel on dit que $Q : V \longrightarrow k$ est une forme quadratique si :

— $Q(ax) = a^2 Q(x)$ pour tout $a \in k$ et $x \in V$

— $(x, y) \longmapsto \dfrac{Q(x+y) - Q(x) - Q(y)}{2}$ est une forme bilinéaire on la notera canoniquement $(. \mid .)$.

Elle est dite non dégénérée si ce n'est pas l'application nulle.

Définition 4.1.2 Deux vecteurs $x, y \in V$ sont dits orthogonaux si $(x \mid y) = 0$. On dit qu'un vecteur non nul z est isotrope si $(z \mid z) = 0$.

Définition 4.1.3 Soit Q une forme quadratique sur un espace vectoriel V et soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de V. On note $G_{\mathcal{B}}(Q) = ((e_i \mid e_j))_{1 \leqslant i,j \leqslant n}$ la matrice de Gramm de Q dans la base $\mathcal{B}$.

Si X est le vecteur colonne coordonnée de $x \in V$ on a donc a la formule $Q(x) = {}^t X G_{\mathcal{B}}(Q) X$

Deux formes quadratiques Q et Q' sont dites équivalentes s'il existe deux bases $\mathcal{B}$ et $\mathcal{B}'$ telle que $G_{\mathcal{B}}(Q) = \mathrm{G}_{\mathcal{B}'}(Q')$.

Pour la démonstration des théorèmes suivants on se référera au cours d'arithmétique de Serre [Ser94].

Théorème 4.1.4 Pour toute forme quadratique, on peut trouver une base orthogonale de vecteurs. La forme quadratique s'écrit ainsi $Q(x) = a_1 x_1^2 + \cdots + a_n x_n^2$ où $a_1, \ldots, a_n \in k$ et $x_1, \ldots, x_n$ sont les coordonnées de x dans la base orthogonale.

Proposition-définition 4.1.5 Soit $\mathcal{B}$ une base de V. On peut associer à toute forme quadratique la quantité $\det G_{\mathcal{B}}(Q)$ appelée **discriminant** qui ne dépend pas de la base modulo le groupe k^*.

Proposition-définition 4.1.6 Si x est une vecteur isotrope, il existe $H \subset V$ un sous-espace vectoriel appelé plan hyperbolique telle que la forme quadratique restreinte à H soit de la forme $Q(x) = z^2 - y^2$ où (z, y) sont les coordonnées de x dans une base de H.

4.2 Correspondance entre formes quadratiques et quaternions

Nous allons, dans cette sous-partie, expliciter le liens entre quaternions et formes quadratiques. Cette motivation s'inspire très largement des quaternions de Hamilton $\mathbb{H}$.

Définition 4.2.1 Soit k un corps et $a, b \in k^*$et soit $D = \left(\frac{a,b}{k}\right)$. Soit $q = x + yi + zj + tk \in D$. On note :

1. $q^* = x - yi - zj - tk$
2. $T(q) = q + q^* = 2x$
3. $N(q) = q \times q^* = x^2 - ay^2 - bz^2 + abt^2$

Théorème 4.2.2 Soit $q, w \in D$:

1. $q \longmapsto q^*$ est une anti-involution i.e. :
   (a) c'est un morphisme linéiaire
   (b) $(qw)^* = w^*q^*$
   (c) $q \longmapsto q^*$ est une involution
2. $N(qw) = N(q)N(w)$ et c'est une forme quadratique sur D non dégénérée.
3. T est linéaire et $(q, w) \longmapsto T(qw)$ est une forme quadratique non dégénérée.

Démonstration.
1. Il n'y a que le (b) qui pose réellement problème, il faut et il suffit de le montrer sur une base.
2. $N(qw) = (qw)(qw)^* = qww^*q^* = qN(w)q^*$ mais $N(w) \in k$ donc $N(qw) = N(q)N(w)$. $x^2 - ay^2 - bz^2 + abt^2$ est aisément une forme qudratique non dégénérée.
3. T est aisément linéaire et $(q, w) \longmapsto T(qw)$ est clairement une forme quadratique non dégénérée.

□

On retrouve les propriétés connue avec les quaternions de Hamilton. Un problème persiste : les définitions dépendent de a, b, à ce stade un autre choix a', b' donnerait une autre définition.

Soit $\bar{k}$ la clôture algébrique de k. Dès lors $D \otimes \bar{k} \simeq \mathcal{M}_2(\bar{k})$. Cependant les automorphismes de $\mathcal{M}_2(\bar{k})$ sont des conjuguaisons par des éléments de $\mathcal{M}_2(\bar{k})$. Cependant $\bar{T} := T \otimes \bar{k}$ est la trace et $\bar{N} := N \otimes \bar{k}$ est le déterminant. Ceux-ci étant invariant par conjuguaison $\bar{N}$ et donc $\bar{T}$ ne dépendent pas de a ou b. De même pour N et T.

Dès lors $x \longmapsto x^* = x - T(x)$ non plus. On peut alors définir intrinsequement $D^0 = \ker T$ on l'appelle l'espace pure des quaternions.

Thérème : Correspondance entre formes quadratiques et quaternions 4.2.3 L'application $D \longmapsto N\,|_{D^0}$ défini un isomorphisme entre les classes de d'isomorphismes de quaternions sur k et les classes d'équivalence de formes quadratique non dégénérées sur k^3 de discriminant 1. Dans cette bijection, $\mathcal{M}_2(k)$ correspond à la forme quadratique $x^2 - y^2 - z^2$ (la seule qui possède un vecteur isotrope)

Démonstration. **Surjectivité :** On met une forme quadratique de discriminant 1 sur k^3 sous la forme : $-ax^2 - by^2 + cz^2$. Dès lors $(-a) \cdot (-b) \cdot c = d^2$ d'où $c = \frac{ab}{d^2}$. Elle est ainsi équivalente à $-ax^2 - by^2 + abz'^2$ en posant $z' = dz$. Donc $D = \left(\frac{a,b}{k}\right)$ convient.

Injectivité : Soit D une algèbre de quaternion. O effectue les remarques suivantes :

— Si $q \in D^0$ alors $N(q) = qq^* = -q^2$ (en effet $q^* = T(q) - q = -q$)

— Si $q, w \in D^0$ sont orthogonaux pour N alors $0 = q^*w + wq^* = -(qw + wq)$ c'est à dire que q et w anti-commuttent

Dès lors si $N(D) \sim N(\left(\frac{a,b}{k}\right))$ alors on trouve i, j tel que $N(i) = a$ et $N(j) = b$ et $ij = -ji$ ce qui conclut. □

4.3 Construction des nombres p-adiques

Pour étudier les formes quadratiques sur $\mathbb{Q}$ nous allons les étudier dans un corps nouveau $\mathbb{Q}_p$. Cette étude suffit en fait comme l'illustre le théorème de Hasse-Minkowski expliqué plus tard. Mais que désigne $\mathbb{Q}_p$?

Nous utiliserons la construction du livre de Serre [Ser94]. Soit p un nombre premier. On défini premièrement l'ensemble des entiers p-adiques $\mathbb{Z}_p$. On dispose d'une surjection naturelle de $\mathbb{Z}/p^{i+1}\mathbb{Z}$ dans $\mathbb{Z}/p^i\mathbb{Z}$ donnée par :

$$\begin{aligned} \iota_i \ : \ \mathbb{Z}/p^{i+1}\mathbb{Z} &\longrightarrow \mathbb{Z}/p^i\mathbb{Z} \\ \bar{x} &\longmapsto \bar{\bar{x}} \end{aligned}$$

Où $\bar{\cdot}$ est la congruence modulo p^{i+1} et $\bar{\bar{\cdot}}$ la congruence modulo p^i. Ces morphismes d'anneaux sont bien définis, sont surjectifs et ont tous des fibres de tailles p.

Définition : anneau des entiers p-adiques 4.3.1 Soit p un nombre premier. On note alors

$$\mathbb{Z}_p = \{(x_0, x_1, x_2, \dots, x_n, \dots) \mid x_i \in \mathbb{Z}/p^{i+1}\mathbb{Z} \text{ où } \iota_i(x_i) = x_{i-1}, i \in \mathbb{N}^*\}$$

l'anneau des entiers p-adiques, munis de la multiplication et addition coordonnées par coordonnées.

Remarque. On peut munir $\mathbb{Z}_p$ de la topologie limite projective où chaque anneau $\mathbb{Z}/p^i\mathbb{Z}$ est muni de la topologie discrète. C'est un espace topologique compact (fermé dans le compact $\prod_{i\in\mathbb{N}^*} \mathbb{Z}/p^i\mathbb{Z}$ par Tychonoff). Ainsi une suite converge si et seulement si elle converge coordonnées par coordonnées.

On peut naturellement plonger $\mathbb{Z}$ dans $\mathbb{Z}_p$ avec $k = (\bar{k}, \bar{\bar{k}}, \dots, \bar{\bar{k}}, \dots)$. Un premier fait remarquable est que $p^n \xrightarrow[n\to+\infty]{} 0$. En effet $p = (0, \bar{p}, \bar{p}, \dots, \bar{p}, \dots)$, $p^2 = (0, 0, \overline{p^2}, \dots, \overline{p^2}, \dots)$ et $p^n = (\underbrace{0, 0, \dots, 0}_{n \text{ fois}}, \overline{p^n}, \dots, \overline{p^n}, \dots)$ converge coordonnées par coordonnées vers 0. Cela assure le théorème suivant :

Théorème : écriture des entiers p-adiques 4.3.2 Soit $x \in \mathbb{Z}_p$ alors il existe une unique suite $(a_n)_{n\in\mathbb{N}} \in \{0, \dots p-1\}^{\mathbb{N}}$ tel que :

$$x = (\overline{a_0}, \overline{a_0 + pa_1}, \dots, \overline{a_0 + pa_1 + \dots p^n a_n}, \dots) = \sum_{n\in\mathbb{N}} a_n p^n$$

Réciproquement toute suite d'une telle forme défini un unique nombre p-adique.

L'écrirure en terme de série permet par exemple de constater que $\mathbb{Z}_p$ a le même cardinal que $\mathbb{R}$.

Définition : Valuation p-adique 4.3.3 Soit $x = (x_0, x_1, x_2, \dots, x_n, \dots) \in \mathbb{Z}_p$ on note $v_p(x)$ la valutaion p-adique de x égale à

$$v_p(x) = \min\{k \in \mathbb{N} \mid x_k \neq 0\}$$

Par convention $v_p(0) = \infty$. Il en découle aisément :

Proposition 4.3.4 Soient $x, y \in \mathbb{Z}_p$ non nuls

1. $v_p(x + y) \geqslant \min(v_p(x), v_p(y))$
2. Il existe un unique élément inversible $u \in \mathbb{Z}_p$ tel que $x = p^{v_p(x)}u$
3. $\mathbb{Z}_p$ est intègre et x inversible $\iff v_p(x) = 0$
4. $v_p(xy) = v_p(x) + v_p(y)$
5. $\mathbb{Z}_p$ est principal
6. p est l'unique élément irréductible à association près de $\mathbb{Z}_p$.

Démonstration. On pose $n = v_p(x)$ et $m = v_p(y)$. On peut ainsi écrire : $x = (\underbrace{0, 0, \dots, 0}_{n \text{ fois}}, x_n, \dots, x_{n+i}, \dots) = \sum_{i \geqslant n} a_i p^i$ $y = (\underbrace{0, 0, \dots, 0}_{m \text{ fois}}, y_m, \dots, y_{m+i}, \dots) = \sum_{i \geqslant m} b_i p^i$.

1. Sans pertes de généralités on suppose $n = \min(n, m)$. Ainsi : $x + y = (\underbrace{0, 0, \dots, 0}_{n \text{ fois}}, x_n, x_{n+1}, \dots, x_m + y_m, \dots, x_{m+i} + y_{m+i}, \dots)$ d'où l'inégalité.
2. On pose $u = (\overline{a_n}, \overline{a_n + pa_{n+1}}, \dots, \overline{a_n + pa_{n+1} + \dots p^i a_{n+i}}, \dots)$. Enfin en multipliant coordonnées par coordonnées $up^n = (\underbrace{0, \dots, 0}_{n \text{ fois}}, \overline{a_n p^n}, \dots, \overline{a_n p^n + a_{n+i} p^{n+i}}) = \sum_{i \geqslant n} a_i p^i = x$ l'unicité découle de l'uncité des a_i. L'entier u est bien inversible car a_n n'est pas divisible pas p par hypothèse.
3. Si x est inversible alors sa première coordonnée l'est donc $x_0 \neq 0$ et donc $v_p(x) = 0$. Si $v_p(x) = 0$ on a ainsi $x = p^0 u$ où u est inversible ce qui conclut. Si $xy = 0$ et que aucun des deux ne sont nuls on écrit $x = p^n u$ et $y = p^m v$ où u, v sont inversibles. Donc $p^{n+m} uv = 0$ donc $p^{n+m} = 0$ impossible en regardant la $n + m + 1$-ème coordonnée.
4. $xy = p^{n+m} uv = p^{v_p(xy)} w$ où w est inversible. Mais par intégrité de $\mathbb{Z}_p$, $p^{v_p(xy) - n - m}$ ou $p^{-v_p(xy) + n + m}$ est inversible donc $v_p(xy) = n + m$.
5. Soit I un idéal non nul de $\mathbb{Z}_p$ alors on pose $k = \min\{v_p(x) \mid x \in I\}$. Soit x_0 tel que $v_p(x_0) = k$, on écrit $x_0 = p^k u$ dès lors $p^k \in I$ ainsi $p^k \mathbb{Z}_p \subset I$ et si $p^{k'} \in I$ on a nécéssairement $k' \leqslant k$ donc $I \subset p^k \mathbb{Z}_p$.
6. Cela résulte de l'unicité de la décomposition.

□

Définition : corps des nombres p-adiques 4.3.5 On note $\mathbb{Q}_p$ le corps des nombre p-adique le corps des fractions de $\mathbb{Z}_p$.

Remarque. On peut étendre la valuation p-adique sur $\mathbb{Q}_p$ et les propriétés 1, 2 et 4 sont toujours vraies entrainant le théorème suivant :

Théorème 4.3.6 Soit p un nombre premier, on note $U = \mathbb{Z}_p^*$. On a l'isomorphisme suivant :

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

4.4 Les carrés de $\mathbb{Q}_p^*$

Si $x = p^n u \in \mathbb{Q}_p^*$ alors d'après la partie précédente, x est un carré $\iff u$ est un carré et n est pair. Reste ainsi à voir quand est-ce que u est un carré.

Théorème : relèvement de Teichmüller 4.4.1 Soit p un nombre premier. Alors il existe un unique sous-groupe des racines $(p-1)$-ième de l'unité dans $\mathbb{Z}_p^*$.

Démonstration. Un tel groupe est unique car c'est le groupe des racines de $X^{p-1} - 1$.

Soit $a \in \mathbb{F}_p^*$ on considère $\varphi : (\mathbb{Z}/p^n\mathbb{Z})^* \longrightarrow \mathbb{F}_p^*$ le morphisme surjectif canonique et on considère un relevé α de a. Comme ord $\alpha = p^m k$ alors $\underbrace{\alpha^{p^m}}_{=\beta}$ est d'ordre k et comme $k \mid p - 1$ alors $\beta^{p-1} = 1$ donc $\beta^p = \beta$. On veut montrer que :

— β ne dépend pas de α

— l'ordre de β = l'ordre de a

À cet effet, on montre le lemme suivant :

Lemme 4.4.2 Soit $0 \to A \xrightarrow{i} E \xrightarrow{\pi} B \to 0$ une suite exacte de groupes commutatifs (on les notes additivement pour la preuve), avec A, B finis d'ordre premier entre eux alors si $B' = \{x \in E \mid |B|x = 0\}$. Alors E est somme directe de A et B'.

Démonstration. Notons $|A| = a$ et $|B| = b$ D'après le théorème de Bachet-Bézout on dispose de $r, s \in \mathbb{Z}$ tel que $ar + bs = 1$. Dès lors si $x \in A \cap B'$, $ax = bx = 0$ donc $(ar + bs)x = x = 0$ et si $y \in E$ alors $y = ary + bsy$ mais $b(arx) = \underbrace{ba}_{=|E|} ry = 0$ donc $ary \in B'$. Enfin $\pi(bsy) = b\pi(sy) = 0$ donc $bsy \in \ker \pi = \mathrm{Im} i = A$ ce qui conclut. □

On applique le lemme à $0 \to \underbrace{\ker \varphi}_{\mathrm{card}=p^{n-1}} \to (\mathbb{Z}/p^n\mathbb{Z})^* \to \underbrace{\mathbb{F}_p^*}_{\mathrm{card}=p-1} \to 0$ Dès lors si $\gamma = \beta^k$ alors $\gamma \in \ker \varphi$ (car $\varphi(\beta^k) = a^k = 1$) et $\gamma^{p-1} = \gamma$. Donc $\gamma \in A \cap B'$ d'où $\gamma = 1$. Ainsi si $\mathrm{ord}\, a = k'$ alors $k' \mid k$ et $k \mid k'$ car $\varphi(\beta^k) = a^k = 1$.

De plus si α' est un autre relevé alors on prend β' similairement et on regarde $\delta = \beta\beta'^{-1}$ ainsi $\varphi(\delta) = 1$ et $\delta^p = \delta$ donc $\delta = 1$ et $\beta = \beta'$. Dès lors on a défini pour tout $a \in \mathbb{F}_p^*$ un unique élément d'ordre $k = \mathrm{ord}\, a$ de $(\mathbb{Z}/p^n\mathbb{Z})^*$. Ceci construit un nombre p-adique d'ordre multiplicatif k et de première coordonnée a. □

Corollaire 4.4.3 Si p est un nombre premier alors :

$$\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{F}_p^* \times 1 + p\mathbb{Z}_p$$

Il reste à comprendre la structure de $1 + p\mathbb{Z}_p$. Fort heureusement pour $p \neq 2$ le problème est aisément résolu :

Théorème 4.4.4 Si p est un nombre premier impair, alors tout élément de $1 + p\mathbb{Z}_p$ est un carré.

Démonstration. On considère $f : \quad 1 + p\mathbb{Z}_p \longrightarrow 1 + p\mathbb{Z}_p \qquad$. La série converge pour tout x car

$$1 + x \longmapsto \sqrt{1+x} = \sum_{k=0}^{\infty} x^k \binom{k}{1/2}$$

$v_p(x^k \binom{k}{1/2}) = v_p(x) \times k + v_p((-1)^n \frac{(2k-3)!}{4^{k-1}k!}) \xrightarrow[n\to+\infty]{} \infty$ car $v_p((-1)^n \frac{(2k-3)!}{4^{k-1}k!}) \sim \frac{2k-3}{k} \sim 2$ par la formule de legendre. Donc la série converge. Par calcul formel $f(1+x)^2 = 1 + x$ ce qui conclut. □

Remarque. Cette preuve met en évidence pourquoi le cas $p = 2$ échoue par la présence d'une puissance de 4. Cependant en adaptant la preuve, on montre volontiers que les éléments de $1 + 8\mathbb{Z}_2$ sont tous des carrés.

Proposition 4.4.5

- Soit p un nombre premier impaire. Pour qu'un élément de $\mathbb{Z}_p^*$ soit un carré il faut et il suffit que sa projection modulo p soit un carré. Ainsi $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 = \{1, u, p, up\}$ où $u \in \mathbb{F}_p^*$ n'est pas un carré.
- Un élément de $\mathbb{Z}_2^*$ est un carré si et seulement si sa projection modulo 8 est un carré. Ainsi $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 = \{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Démonstration. Il ne reste que le cas $p = 2$ à prouver. On montre que si $x \in \mathbb{Z}_2^*$ est un carré mod 8 alors $x \in 1 + 8\mathbb{Z}_2$, la réciproque étant claire. Il suffit de remarquer que 1 est le seul carré inversible mod 8 (faire un tableau par exemple). □

4.5 Formes quadratiques sur le corps des p-adiques

Le but de cette partie est de montrer que, tout comme $\mathbb{R}$, $\mathbb{Q}_p$ pour tout nombre premier p possède une seule algèbre de quaternion non triviale. Les similarités entre $\mathbb{Q}_p$ et $\mathbb{R}$ sont frappantes, en plus de partager cette propriété commune, ces corps proviennent tous de la complétion de $\mathbb{Q}$ par une certaine norme (la norme p-adique pour $\mathbb{Q}_p$ et la valeur absolue pour $\mathbb{R}$). Il semble également que ces corps décrivent tout les complétés possible de $\mathbb{Q}$ par une norme d'où la cohérence de l'énoncé du théorème de Hasse Minkowski que nous verrons dans la partie suivante **4.6**.

Théorème 4.5.1 Soit p un nombre premier. Il existe exactement une forme quadratique sur $\mathbb{Q}_p^3$ de discriminant 1 qui ne représente pas 0. Autrement dit, il existe une unique algèbre de quaternion non triviale sur $\mathbb{Q}_p$.

Lemme : Approximations successives 4.5.2 Soient u, v, w trois unités p-adiques où $p \neq 2$. La forme quadratique $ux^2 + vy^2$ représente w.

Démonstration. 1. Initialisation. Le but est de construire deux suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ d'entiers p-adiques convergentes telles que $v_p(ux_n^2 + vy_n^2 - w) \geqslant n + 1$. Si on trouve deux entiers (en plongeant les entiers $\mathbb{Z}$ dans $\mathbb{Z}_p$) tels que $p \mid ux_0^2 + vy_0^2 - w$ on aura l'inégalité voulue pour $n = 0$. Ainsi il suffit de résoudre le problème dans $\mathbb{F}_p$.

Les ensembles $\{\overline{ux_0^2} \mid \overline{x_0} \in \mathbb{F}_p\}$ et $\{\overline{vy_0^2 - w} \mid \overline{y_0} \in \mathbb{F}_p\}$ ont le même cardinal : $\frac{p+1}{2}$. Ainsi ils s'intersectent et on peut trouver x_0 et y_0 deux tels entiers dont l'un des deux est non nul.

2. Récurrence. On suppose construit x_{n-1} et y_{n-1}. On pose $x_n = x_{n-1} + a_n p^n$ et $y_n = y_{n-1} + b_n p^n$. Dès lors si on pose $ux_{n-1}^2 + vy_{n-1}^2 - w = p^n\alpha$ où $\alpha \in \mathbb{Z}_p$ alors on a

$$ux_n^2 + vy_n^2 - w = ux_{n-1}^2 + vy_{n-1}^2 - w + 2(a_n x_{n-1} + b_n y_{n-1})p^n + (a_n^2 + b_n^2)p^{2n}$$

$$ux_n^2 + vy_n^2 - w = (\alpha + 2a_n x_{n-1} + 2b_n y_{n-1})p^n + (a_n^2 + b_n^2)p^{2n}$$

Ainsi si la projection modulo p de $\alpha + 2a_n x_{n-1} + 2b_n y_{n-1}$ s'annule alors $v_p(ux_n^2 + vy_n^2 - w) \geqslant n + 1$ et c'est toujours possible car l'un des deux élément parmi x_{n-1} et y_{n-1} a une projection mod p non nul. Il en est de même de x_n et y_n car sinon $v_p(ux_n^2 + vy_n^2 - w) = v_p(-w) = 0$.

3. Conclusion. Ainsi (x_n) et (y_n) convergent respectivement vers x et $y \in \mathbb{Z}_p$ vérifient ainsi $ux^2+vy^2-w = 0$.

□

La classification des non-carrés permet d'étudier les cas un par un. On considère la forme quadratique $\alpha x^2 + \beta y^2 - \alpha\beta z^2$ qui peut être ramenée à $x^2 - \alpha y^2 - \beta z^2$ si l'on cherche à montrer que la forme représente 0. Si jamais c'est le cas, on peut aisément montrer qu'elle est équivalente à $x^2 - y^2 - z^2$ en construisant un plan hyperbolique.

On suppose dans un premier temps $p \neq 2$.

— Si α ou β est un carré la forme représente 0.

— On suppose α et $\beta \in \mathbb{Z}_p^*$. On construit une solution par approximations successives.

— On montre que la forme $px^2 - uy^2 + puz^2$ où u est un inversible qui n'est pas un carré ne représente pas 0. Par l'absurde prenons un vecteur (x_0, y_0, z_0) isotrope. On peut aisément le choisir dans $\mathbb{Z}_p^3$ avec l'un des éléments inversibles. En passant modulo p on obtient $p \mid y$. En divisant par p on obtient que u est un carré modulo p ce qui est absurde.

— On peut montrer que toute autre forme quadratique se ramène aux cas précédent par changement de bases par dilatation ou permutation. Cela conclut pour $p \neq 2$.

On ne fera pas la démonstration pour $p = 2$ (voir le cours d'arithmétique de Serre [Ser94])

Nous pouvons être même plus précis :

1. La forme quadratique de discriminant 1 isotrope sur $\mathbb{Q}_p^3$ est équivalente à $x^2 - y^2 - z^2$ ou encore à $xy - z^2$. Ainsi si $a \in \mathbb{Q}_p$ alors a est aisément représenté par cette forme.
2. La forme quadratique non isotrope $-ux^2 - py^2 + upz^2$ où u est une unité qui n'est pas un carré sur $\mathbb{Q}_p^3$ représente les classes de carrés p et pu avec les triplets $(0, y_0, z_0)$ et $(0, 0, 1)$ respectivement où $uz_0^2 - y_0^2 = 1$ par approximation succesive.

Il en résulte la proposition suivant :

Proposition 4.5.3 Si $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, on rappelle que l'on peut plonger $\mathbb{Q} \subset \mathbb{Q}_p$ où p est un nombre premier. Il existe alors un nombre fini de nombres premiers tel que $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ soit non triviale

Démonstration. Si $p \nmid ab$ alors si f_p est la forme associée à $\left(\frac{a,b}{\mathbb{Q}_p}\right)$:

$$f_p \sim -ax^2 - by^2 + abz^2 \sim x^2 - y^2 - z^2$$

Car a et b sont inversibles dans $\mathbb{Q}_p$ donc $\left(\frac{a,b}{\mathbb{Q}_p}\right) \simeq \mathbb{Q}_p$. Ainsi pour que $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ soit non triviale il est nécessaire que $p \mid ab$ ne se produisant que pour un nombre fini de nombre premiers. □

4.6 Théorème de Hasse-Minkowski

L'introduction des nombres p-adiques se justifie entièrement par le théorème de Hasse Minkowsi, véritable pont entre $\mathbb{Q}$ et $\mathbb{R}$ et $\mathbb{Q}_p$ pour p premier. On notera $\widehat{\mathbb{P}}$ l'ensemble des nombres premiers et l'infini. On notera $\mathbb{R} = \mathbb{Q}_\infty$.

Théorème de Hasse-Minkowski 4.6.1 Soient n un entier et f, g deux formes quadratiques sur $\mathbb{Q}^n$. Alors f et g sont équivalentes si et seulement si elles le sont sur tout $\mathbb{Q}_v$ pour $v \in \widehat{\mathbb{P}}$.

Nous ne démontrerons pas ce théorème, qui nécessite l'introduction d'outils plus complets comme le symbole de Hilbert.

Ce théorème permet déjà de répondre à une question que nous nous étions posé en **3.3** à savoir si l'ensemble de quaternions rationnelles formaient un sous-groupe de $\mathrm{Br}(\mathbb{Q})$. Nous pouvons dès lors compléter la démonstration de la proposition **3.3.2**, il faut et il suffit de montrer que si H_1 et H_2 sont deux algèbre de quaternion alors $H_1 \otimes H_2$ n'est pas une algèbre à division.

Proposition 4.6.2 Soient H_1 et H_2 deux algèbres de quaternion rationnelles non triviales alors :

— Il existe $d \in \mathbb{Z}$ qui n'est pas un carré parfait et $x \in H_1,\ y \in H_2$ tel que $x^2 = y^2 = d$.

— Si $d \in \mathbb{Z}$ qui n'est pas un carré et $L := \mathbb{Q}(\sqrt{d})$ alors $L \otimes L \simeq L \times L$.

On termine aisément la démonstration du théorème **3.3.2** aisément à partir du théorème **4.6.2** car $H_1 \otimes H_2$ est à division et si d est un tel entier $L \times L \simeq L \otimes L \subset H_1 \otimes H_2$. Cependant $L \times L$ est une sous-algèbre de dimension finie d'une algèbre à division mais elle n'est pas à division. C'est absurde.

Démonstration.

1. Soit H une algèbre de quaternion sur un corps k. Alors si $x^2 = d \in k$ qui n'est pas un carré alors le polynôme minimal de x étant de degré 2 ($x \notin k$) ce dernier est égal à $X^2 - d$. On identifie volontier $N(x) = d$ et $t(x) = 0$. Réciproquement si un élément de $x \in H^0$ vérifie $N(x) = d$ on a dès lors $x^2 = d$. Nous sommes donc ramené à un problème de forme quadratique. On veut montrer que les formes quadratiques associées aux normes N_1, N_2 respectivement de H_1, H_2 représentent un même $d \in \mathbb{Z}$ qui n'est pas un carré.
2. On note $S = \{p_1, \ldots, p_n\}$ l'ensemble fini des nombres premiers p tel que H_1 ou H_2 soit non triviale sur $\mathbb{Q}_p$. On pose $d = -\varepsilon p_1 \times \ldots p_n$ où $\varepsilon = -1$ si H_1 ou H_2 non triviale sur $\mathbb{R}$ et $\varepsilon = 1$ sinon. On a dès lors si $i \in \{1, 2\}$:
   — Lorsque $\left(\frac{a_i, b_i}{\mathbb{Q}_p}\right) \simeq \mathbb{Q}_p$ alors N_i représente d sur $\mathbb{Q}_p^3$ car équivalente à $xy - z^2$
   — Si $\left(\frac{a_i, b_i}{\mathbb{Q}_p}\right)$ est non triviale alors $p \in S$ et la classe de d dans $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ est ou bien p ou up ou u est une unité non carré. Ces deux classes sont représentées par N_i sur $\mathbb{Q}_p^3$.
   — Pour le cas réel, si $d < 0$ alors $\varepsilon = 1$ et donc N_i équivalent à $xy - z^2$ sur $\mathbb{R}^3$ donc d est bien représenté. Dans le cas contraire $d > 0$ est représenté par les deux formes quadratiques possibles $xy - z^2$ et $x^2 + y^2 + z^2$.

   Si $d = 1$ alors N_1 et N_2 sont tout deux isotropes dans $\mathbb{Q}_v^3$ pour $v \in \widehat{\mathbb{P}}$ donc les algèbres H_1 et H_2 seraient triviales, c'est absurde par hypothèse. Dans le cas contraire d est aisément non carré. Le théorème de Hasse-Minkowski assure l'existence d'un tel d non carré commun.

3. On montre $L \otimes L \simeq L \times L$. On note déjà l'égalité des dimensions, on pose ainsi :

$$\begin{aligned} \varphi : \quad & L \times L \longrightarrow L \times L \\ & (\alpha, \beta) \longmapsto (\alpha\beta, \alpha\overline{\beta}) \end{aligned}$$

où $\overline{x + y\sqrt{d}} = x - y\sqrt{d}$. C'est bien une application bilinéaire, elle se factorise donc en une application linéaire de $L \otimes L$ dans $L \times L$. On vérifie aisément la compatibilité avec la multiplication sur une base ainsi que l'injectivité. Cela conclut.

□

4.7 Structure du groupe des quaternions sur $\mathbb{Q}$

Définition 4.7.1 Soit H une algèbre de quaternion sur $\mathbb{Q}$ et $v \in \widehat{\mathbb{P}}$. On note :

$$\varepsilon_v(H) = \begin{cases} 1 & \text{Si l'algèbre } H \text{ est triviale sur } \mathbb{Q}_v \\ -1 & \text{Si l'algèbre } H \text{ n'est pas triviale sur } \mathbb{Q}_v \end{cases}$$

Théorème 4.7.2 Soit H une algèbre de quaternion sur $\mathbb{Q}$.

1. Il existe un nombre fini de $v \in \widehat{\mathbb{P}}$ tel que $\varepsilon_v(H) = -1$
2. $\prod_{v \in \widehat{\mathbb{P}}} \varepsilon_v(H) = 1$
3. Si $\forall v \in \widehat{\mathbb{P}}, \varepsilon_v(H) = 1$, alors $H \simeq \mathcal{M}_2(\mathbb{Q})$
4. Pour toute paire $(u, v) \in \widehat{\mathbb{P}}^2$ d'éléments distinct, il existe $\mathbb{H}$ une algèbre de quaternion tel que : si $w \in \widehat{\mathbb{P}}$ alors : $\varepsilon_w(\mathbb{H}) = -1 \iff w = v$ ou $w = u$.

Les points 1 et 3 ont déjà été démontrés. Nous ne démontrerons pas les autres points (on pourra consulter le cours de G.Chenevier [Che10]). Ce théorème donne explicitement un isomorphisme entre le sous-groupe des algèbres de quaternions de $\mathrm{Br}(\mathbb{Q})$ que nous noterons G avec un sous-groupe de $\{\pm 1\}^{(\widehat{\mathbb{P}})}$

$$\begin{aligned} \varphi : \quad & G \longrightarrow \{\pm 1\}^{(\widehat{\mathbb{P}})} \\ & H \longmapsto (\varepsilon_v(H))_{v \in \widehat{\mathbb{P}}} \end{aligned}$$

En particulier le point 4 dit qu'il existe une infinité d'algèbre de quaternion, la strucure est dès lors beaucoup plus riche que celle des quaternions sur $\mathbb{R}$ ou $\mathbb{C}$.

5 Conclusion

Notre étude permet de mettre en lumière la difficulté d'une classification des k-algèbres centrales à division de dimension finie. Plus précisément, cette difficulté dépend fortement du corps k puisque nous avons montrés qu'il était très simple de les énumérer lorsque $k = \mathbb{R}$ ou un corps algébriquement clôs ou fini, mais qu'énumérer les algèbres centrales à division de dimension 4 rationnelle demande beaucoup plus de travail. Il en demande encore plus pour comprendre la structure de $\mathrm{Br}(\mathbb{Q})$ et son liens avec, encore une fois, le groupe de Brauer des corps des nombres p-adiques et celui du corps des réels ou encore pour classifier des algèbres encore plus générales comme les algèbres non associatives incluant les algèbres d'octonions.

Références

[Bla72] André Blanchard. *Les corps non commutatifs.* 1972.

[Che10] Gaëtan Chenevier. *The infinite fern and families of quaternionic modular forms.* 2010.

[Den93] Benson Farb R. Keith Dennis. *Noncommutative Algebra.* 1993.

[Per96] Daniel Perrin. *Cours d'Algèbre.* 1996.

[Ser94] Jean-Pierre Serre. *Cours d'arithmétique.* 1994.