Algèbres de quaternions

В.М.

Version du 18 février 2015

K désigne un corps de caractéristique différente de 2.

Définition 1. Une **K**-algèbre **H** est une algèbre de quaternion si et seulement si **H** est une algèbre centrale (de centre **K**) simple (i.e.dépourvue d'idéaux nontriviaux propres) ou encore si et seulement si si et seulement s'il existe des éléments i, j et k vérifiant

$$i^2 = a$$
, $j^2 = b$, $k = ij = -ji$

avec $a, b \in \mathbf{K}^{\times}$. On la note

$$\binom{a,b}{\mathbf{K}}$$

Dans ce cas, $k^2 = -ab$.

Exemple 2. Les quaternions classiques (de Hamilton) sur R sont

$$\binom{-1,-1}{\mathbf{K}}$$
.

Exemple 3. L'algèbre de matrices $\mathscr{M}_2(\mathbf{K})$ est l'algèbre de quaternions $\binom{1,1}{\mathbf{K}}$ par identification de

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Plus généralement, l'algèbre de quaternions $\binom{a,b}{\mathbf{K}}$ peut être représentée par

$$\alpha + \beta i + \gamma j + \delta k \mapsto \begin{pmatrix} \alpha + \sqrt{a}\beta & \sqrt{b}\gamma + \sqrt{ab}\delta \\ \sqrt{b}\gamma - \sqrt{ab}\delta & \alpha - \sqrt{a}\beta \end{pmatrix}$$

En réalité, toute **K**-algèbre de quaternion est soit un corps gauche soit isomorphe à $\mathcal{M}_2(\mathbf{K})$.

Proposition 4. Sont isomorphes les algèbres de quaternion

$$\binom{a,b}{\mathbf{K}} \simeq \binom{b,a}{\mathbf{K}} \simeq \binom{a,-ab}{\mathbf{K}}.$$

De plus, pour tout $d \in \mathbf{K}^{\times}$, $\binom{a,b}{\mathbf{K}} \simeq \binom{ad^2,bd^2}{\mathbf{K}}$.

Proposition 5. Si $L \subseteq K$ est un surcorps de K, on a

$$\begin{pmatrix} a, b \\ \mathbf{K} \end{pmatrix} \otimes_{\mathbf{K}} \mathbf{L} = \begin{pmatrix} a, b \\ \mathbf{L} \end{pmatrix}$$

On note $\mathbf{H_L}$ l'extension $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}$ d'une \mathbf{K} -algèbre de quaternion \mathbf{H} .

Le cas ultime est le cas où tout élément est un carré, ce qui notamment vrai sur une corps algébriquement clos. Dans ce cas, l'exemple 3 est la seule algèbre de quaternion possible.

Définition 6. On dit qu'une algèbre de quaternion \mathbf{H} sur \mathbf{K} est déployée (anglais split) lorsqu'elle est insomorphome à $\mathcal{M}_2(\mathbf{K})$. Lorsqu'un surcorps \mathbf{L} de \mathbf{K} rend $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}$ déployé, on parle de corps neutralisant.

Exemple 7. On note $\overline{\mathbf{K}}$ une cloture algébrique, alors $\mathbf{H} \otimes_{\mathbf{K}} \overline{\mathbf{K}}$ est déployé.

Définition 8. Pour tout $x = \alpha + \beta i + \gamma j + \delta k$ avec $\alpha, \beta, \gamma, \delta \subseteq \mathbf{K}$, on note

$$\overline{x} = \alpha - \beta i - \gamma j - \delta k \qquad \text{(Conjugué)}$$

$$\operatorname{trd}(x) = x + \overline{x} = 2\alpha \qquad \text{(Trace réduite)}$$

$$\operatorname{nrd}(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \qquad \text{(Norme réduite)}$$

On note encore \mathbf{H}^0 l'ensemble des quaternions de trace nulle.

Exemple 9. Dans le cas de $\mathcal{M}_2(\mathbf{K})$, la conjuguée est la transposée de la comatrice

$$\overline{x} = \overline{\begin{pmatrix} r & s \\ t & u \end{pmatrix}} = \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

Par suite,

$$trd(x) = r + u$$
 $nrd(x) = ru - st$.

Théorème 10. Les classes d'isomorphisme d'algèbres de quaternions sur K sont en bijection avec les classes d'isométrie d'espaces quadratiques ternaires non dégénérés de discriminant carré via l'application $H \mapsto \operatorname{nrd}_{H^0}$.

 $D\acute{e}monstration.$

1 1

Théorème 11 (Skolem-Noether, [Vig80] 2.1 ou [Lan82] 1.3). Les **K**-automorphismes d'une **K**-algèbre de quaternions **H** sont intérieurs (de la forme $x \mapsto g^{-1}xg$).

Démonstration. Nous commenons par noter :

Lemme 12. L'application où $h \otimes h'$ est envoyé sur $x \mapsto hx\overline{h'}$ définie un isomorphisme de \mathbf{K} -algèbres entre $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{H}$ et $End((\mathbf{H}, +))$.

Esquisse : Les propriétés de morphisme se vérifient facilement. Comme les dimensions coïncident, il suffit de montrer que l'application est injective. On se place dans une extension des scalaires $\mathbf{H_L}$ par un corps neutralisant \mathbf{L} . Le noyeau de l'application est alors un idéal de $\mathbf{H_L} \otimes \mathbf{H_L} \simeq \mathscr{M}_2(\mathbf{L})$, qui doit être nul comme $\mathscr{M}_2(\mathbf{L})$ est simple.

Lemme 13. Tout isomorphisme entre deux extensions quadratiques $\mathbf{L}, \mathbf{L}' \subseteq \mathbf{H}$ est la restriction d'un automorphisme intérieur de \mathbf{H} .

Notons ψ l'isomorphisme entre \mathbf{L} et \mathbf{L} . Alors \mathbf{H} peut être vu comme un \mathbf{L} -module à gauche de deux manières : $\forall \lambda \in \mathbf{L}$, $\forall x \in \mathbf{H}$, soit $\lambda \cdot_1 x = \lambda x$, soit $\lambda \cdot_2 x = \psi(\lambda)x$. Pour des raisons de rang identique, les deux \mathbf{L} -modules sont isomorphes et il existe une application u telle que $\forall \lambda \in \mathbf{L}$, $\forall x \in \mathbf{H}$, $u(\lambda \cdot_1 x) = \lambda \cdot_2 u(x)$, autrement dit $u(\lambda x) = \psi(\lambda)u(x)$. Soit $(h'_i)_{i \leq 4}$ une \mathbf{K} -base de \mathbf{H} . D'après le lemme précédent, on peut représenter u par $u: x \mapsto \sum_i h_i x \overline{h'_i}$. Ceci fournit la relation $\sum_i h_i \lambda x \overline{h'_i} = \psi(\lambda) \sum_i h_i x \overline{h'_i}$, soit encore $\sum_i (h_i \lambda - \psi(\lambda) h_i) \otimes \overline{h'_i} = 0 \in \mathbf{H} \otimes \mathbf{H}$ et ce $\forall \lambda \in \mathbf{L}$, $\forall x \in \mathbf{H}$. Aussi $h_i \lambda - \psi(\lambda) h_i = 0$ pour tout i. Il nous suffit de montrer que l'un des h_i est inversible. Nous en choisissons un, disons h, non nul. Comme $h \notin \mathbf{L}$, $\mathbf{H} = \mathbf{L} + h\mathbf{L}$. On en déduit que $\mathbf{H}h$ est un idéal bilatère, car

$$\mathbf{H}h\mathbf{H} = \mathbf{H}h\mathbf{L} + \mathbf{H}hh\mathbf{L} \subseteq [\mathbf{H}\psi(L) + \mathbf{H}h\psi(L)]h \subseteq \mathbf{H}h$$

Mais **H** est une algèbre simple. Donc $\mathbf{H}h = \mathbf{H}$ et h est inversible.

Théorème 14 ([Lan82] IX.1.4). L'application $x \mapsto x_{\gamma}^* = g^{-1}\overline{x}g$ est une involution si et seulement si $g^2 \in \mathbf{K}$. De plus, il n'y a pas d'autre involution.

Démonstration. On doit avoir

$$x = (x_{\gamma}^*)_{\gamma}^* = \gamma^{-2} \overline{x} \gamma^2$$

ce qui est vrai si est seulement si γ^2 est dans le centre, qui est k.

Définition 15. On suppose ici que $\mathbf{K} = \mathbf{Q}$. On dit alors qu'une algèbre de quaternion \mathbf{H} est indéfinie si $\mathbf{H} \otimes_{\mathbf{Q}} \mathbf{R} = \mathscr{M}_2(\mathbf{R})$.

Théorème 16 ([Lan82] IX.2.3). On suppose que $\mathbf{K} = \mathbf{Q}$ et que \mathbf{H} est indéfinie. Soit $(\cdot)_g^*$ l'involution définie ci-dessus $(g^2 \in \mathbf{Q} \text{ en particulier})$. Alors $\operatorname{trd}(xx_g^*) > 0$ pour tout $x \neq 0 \in \mathbf{H}$ si et seulement si $g^2 < 0$.

Démonstration. Supposons que $\mathbf{H} = \binom{b,c}{\mathbf{Q}}$ et que $i^2 = b$ et $g^2 = c$. On peut voir les éléments sous la forme $x = \alpha + \beta j$ avec $\alpha, \beta \in \mathbf{Q}(i)$. On voit par le calcul que

$$\operatorname{trd}(xx^*) = 2(\alpha\alpha' + \beta\beta'b)$$

Il reste à jouer avec cette formule. Si $g^2 < 0$, $\mathbf{Q}(g)$ est un corps quadratique imaginaire, donc $\alpha\alpha'$ $\beta\beta'$ sont positifs

Théorème 17 ([Lan82] IX.2.1). Soit $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{H}$ un sous-corps de degré 2 sur \mathbf{K} d'une algèbre de quaternion \mathbf{H} . Soit $\beta \in \mathbf{L}$ tel que $b = \beta^2 \in \mathbf{K}$ et $\mathbf{L} = \mathbf{K}[\beta]$. Alors il existe une base 1, β , γ , $\beta\gamma$ de \mathbf{H} telle que γ est inversible et

$$\gamma^2 = c \in \mathbf{K}^{\times}, \quad \beta \gamma = -\gamma \beta.$$

Autrement dit, $\mathbf{H} \simeq \begin{pmatrix} b,c \\ \mathbf{K} \end{pmatrix}$.

Démonstration. D'après le lemme 13, il existe un élément γ tel que l'automorphisme non-trivial de \mathbf{L} soit la restriction de l'automorphisme intérieur $x \mapsto \gamma^{-1}x\gamma$. Autrement dit, $\gamma^{-1}\beta\gamma = -\beta$. De plus, on voit que γ^2 commute avec β et γ . Comme $\beta \notin \mathbf{K}[\gamma]$, il s'en suit que $\mathbf{H} = \mathbf{L} + \gamma \mathbf{L}$ (pour des raisons de dimensions). Comme γ^2 est dans le centre de \mathbf{H} , $\gamma^2 \in \mathbf{K}$ ce qui prouve le théorème.

2 2

Nous supposons ici que ${\bf K}$ est un corps de nombre, ${\bf K}_v$ son complété à la place v et R, R_v leur anneau d'entiers respectif.

Définition 18. Soit \mathbf{H} une \mathbf{K} -algèbre de quaternions et v une place de \mathbf{K} . Si $\mathbf{H}_v := \mathbf{H} \otimes_{\mathbf{K}} \mathbf{K}_v$ est un corps gauche, on dit que \mathbf{H} est ramifiée à la place v, sinon on dit non-ramifiée.

Définition 19. Le discriminant disc(H) d'une algèbre de quaternion H est l'idéal entier de R égal au produit des idéaux premiers de R qui ramifie \mathbf{H} .

Théorème 20 ([Voi14] 4.5.4). Soit $\mathbf{H} = \begin{pmatrix} a,b \\ \mathbf{K} \end{pmatrix}$ une algèbre de quaternions sur K. Sont équivalents

- 1. $\mathbf{H} \simeq \mathscr{M}_2(\mathbf{K})$,
- 2. H n'est pas un corps gauche,
- 3. La forme nrd est isotrope (i.e $\exists x \neq 0 \in \mathbf{H}, \operatorname{nrd}(x) = 0$).
- 4. La forme $\operatorname{nrd}_{|\mathbf{H}^0}$ est isotrope (i.e $\exists x \neq 0 \in \mathbf{H}^0$, $\operatorname{nrd}(x) = 0$).
- 5. La forme quadratique binaire $\langle a,b \rangle$ (i.e. la forme $(x,y) \mapsto ax^2 + by^2$) représente 1.
- 6. b appartient à $N_{\mathbf{L}/\mathbf{K}}(\mathbf{L}^{\times})$ où $\mathbf{L} = \mathbf{K}[i]$.

Démonstration. 1 donne 2. est clair.

- $2 \Leftrightarrow 3$ est un exercice facile
- $3 \Rightarrow 4$ Soit x non nul tq $\operatorname{nrd}(x) = 0$ et y orthogonal à 1 et x, si bien que $\operatorname{trd}(xy) = 0$ 0. Alors on ne peut avoir simultanément xy=0 et $\overline{x}y=(\operatorname{trd}(x)-x)y=0$. On peut donc supposer que $xy \neq 0$ et alors $\operatorname{nrd}(xy) = \operatorname{nrd}(x)\operatorname{nrd}(y) = 0$ comme voulu.
- $4 \Rightarrow 1$ Compte tenu des hypothèses, on peut voir que $\operatorname{nrd}_{\mid \mathbf{H}^0}$ est isomorphe à $\langle 1, -1 \rangle \oplus \langle c \rangle$. Le discriminant de $\operatorname{nrd}_{|\mathbf{H}^0}$ est donc -c. Mais $\operatorname{nrd}_{|\mathbf{H}^0} = \langle -a, -b, ab \rangle$ et ce discriminant est un carré. Donc en réalité -c=1 modulo un carré et $\mathbf{H} \simeq {1,1 \choose \mathbf{K}}$ $4\Rightarrow 5$. Si $x=\alpha i+\beta j+\gamma ij \in \mathbf{H}^0$ tq nrd(x)=0,alors

$$-a\alpha^2 - b\beta^2 + ab\gamma^2 = 0$$

Soit $\gamma \neq 0$ est c'est gagné, soit $\gamma = 0$ et la forme $\langle a, b \rangle$ est isotopique, mais alors représente aussi 1

 $5. \Rightarrow 6.$ Si a est un carré, \mathbf{L} . Si a est un non carré, rien à faire. étant donné $ax^2 + by^2 = 1$, on doit avoir $y \neq 0$ d'où l'on tire

$$1/y^2 - a(x/y)^2 = N_{L/K} \left(\frac{1 - x\sqrt{a}}{y} \right) = b$$

 $6. \Rightarrow 3.$ Si $b = x^2 - ay^2$, alors x + yi + j a pour norme réduite 0

Remarque 21. Quand la forme $\langle a, b \rangle$ représente 1, on note (a, b) = 1 (symbole de Hilbert). Sinon, on note (a, b) = -1.

Lemme 22 ([Voi14] 4.5.6). Soit $L \supseteq K$ une extension quadratique du corps K. Alors, L neutralise H si et seulement s'il existe un K-homomorphisme injectif $\mathbf{L} o \mathbf{H}$.

Démonstration. Supposons que **L** s'injecte dans **H**. On peut supposer **L** = $\mathbf{K}[\sqrt{d}]$, on note μ l'image de \sqrt{d} dans **H**. Alors $1 \otimes \sqrt{d} - \mu \otimes 1$ est un diviseur de 0 dans $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}$ car

$$(1 \otimes \sqrt{d} - \mu \otimes 1)(1 \otimes \sqrt{d} + \mu \otimes 1) = 0$$

Donc $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}$ est déployé

Réciproquement, deux cas se préentent : soit $\mathbf{H} \simeq \mathcal{M}_2(\mathbf{K})$ et tout extension quadratique peut se plonger dans \mathbf{H} , soit \mathbf{H} est une algèbre à division. Dans le second cas, en notant $\mathbf{L} = \mathbf{K}[\sqrt{d}]$, on a $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L} = \mathcal{M}_2(\mathbf{L})$ si et seulement si la forme $\langle -a, -b, ab \rangle$ est isotrope sur \mathbf{L} . Donc il existe des coefficients x, y, z, u, v, w tq

$$-a(x + u\sqrt{d})^{2} - b(y + v\sqrt{d})^{2} + ab()^{2} = 0$$

Posons $\alpha = xi + yj + zij$ et $\beta = ui + vj + wij$. Un peu de calcul va montrer que $\gamma = \alpha\beta^{-1}$ est de carré d.

Théorème 23 ([AB04] 1.8). 1. Une K-algèbre de quaternion H est ramifiée en un nombre fini pair de places.

- 2. Deux K-algèbres de quaternion sont isomorphes si et seulement si elles sont ramifiées aux mêmes places.
- 3. Étant donné un nombre fini pair de places non-complexes de K, il existe une K-algèbre de quaternion qui est ramifie exactement en ces places.

 $D\acute{e}monstration.$ Sur \mathbf{Q}

- 1. Découle des propriétés du symbole de Hilbert et du fait que $\prod_{v} (a,b)_v = 1$
- 2. Deux algèbres sont isomorphes quand les formes nrd sont isométriques, ce qui est le cas quand leur symbole d'Hilbert coincide, ou encore quand les algères se ramifient aux mêmes places.

3.

Proposition 24 ([AB04] 1.13, [Voi14] §13.2 -13.3). Une extension finie \mathbf{L} sur \mathbf{K} neutralise une \mathbf{K} -algèbre de quaternion \mathbf{H} si et seulement si \mathbf{L}_w neutralise \mathbf{H}_v pour toute place w|v.

Démonstration. L neutralise H si et seulement si $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L} \simeq \mathscr{M}_2(\mathbf{L})$, soit encore ssi $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}_w = \mathscr{M}_2(\mathbf{L}_w)$. Mais $\mathbf{H} \otimes_{\mathbf{K}} \mathbf{L}_w = \mathbf{H}_v \otimes_{\mathbf{K}_v} \mathbf{L}_w$.

3 3

Définition 25 ([AB04] 1.31). La différente $\mathcal{D}_{\mathcal{O}}$ d'un ordre \mathcal{O} de R est le R-idéal bilatère de \mathcal{O} calculé comme l'inverse du dual de \mathcal{O} par la forme bilinéaire trd. Le discriminant réduit discrd(\mathcal{O}) d'un ordre \mathcal{O} de R est la norme réduite de la différente $\mathcal{D}_{\mathcal{O}}$.

Lemme 26. Soient \mathcal{O} et \mathcal{O}' deux ordres, alors

$$\operatorname{discrd}(\mathcal{O}) = [\mathcal{O}':\mathcal{O}] \cdot \operatorname{discrd}(\mathcal{O}')$$

Proposition 27 ([AB04] 1.32). Soit \mathcal{O} un R-ordre. Le discriminant réduit $\operatorname{discrd}(\mathcal{O})$ jouit des propriétés suivantes.

1. discrd(\mathcal{O})² est l'idéal de R engendré par {det(tr($\omega_i\omega_j$)_{1≤i,j≤4}); (ω_i)_{i≤4} \in \mathcal{O} }. On a même, quand (v_i)_{i<4} est une R-base de \mathcal{O} ,

$$\operatorname{discrd}(\mathcal{O})^2 = R \det(\operatorname{tr}(v_i v_j)_{1 \le i, j \le 4}).$$

2. Si $\mathcal{O} \subseteq \mathcal{O}'$ sont deux R-ordres dans \mathbf{H} , alors $\operatorname{discrd}(\mathcal{O}')$ divise $\operatorname{discrd}(\mathcal{O})$ avec égalité ssi $\mathcal{O} = \mathcal{O}'$.

Exemple 28. Quand $\mathbf{H} = \binom{a,b}{\mathbf{K}}$ et $\mathcal{O} = R \oplus Ri \oplus Rj \oplus Rij$, discrd $(\mathcal{O})^2$ est l'idéal engendré par

$$\det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & -2ab \end{pmatrix} = -(4ab)^2$$

Théorème 29 ([AB04] 1.50 ou [Voi14] 13.5.5). Soit \mathcal{O} un R-ordre de \mathbf{H} . Alors, \mathcal{O} est maximal si et seulement si discrd(\mathcal{O}) = disc(\mathbf{H}) ou encore si et seulement si \mathcal{O}_v est un R_v -ordre maximal pour toute place finie v.

Démonstration. Un ordre \mathcal{O} est maximal ssi \mathcal{O}_v est maximal pour tout premier v de R. [en effet, rappelons que $\mathcal{O} = \bigcap_v \mathcal{O}_v$. donc si \mathcal{O}_v est maximal, \mathcal{O} l'est aussi. par ailleurs si \mathcal{O}_v est contenu dans un certain \mathcal{O}' , alors $\bigcap_{w\neq v} \mathcal{O}_w \cap \mathcal{O}'$ formerait un ordre contenant \mathcal{O}].

Si \mathbf{H} est déployé en v, alors $\mathbf{H}_v \simeq \mathscr{M}_2(\mathbf{K}_v)$ et un ordre est maximal ssi il est isomorphe à $\mathscr{M}_2(R_v)$. Mais $\mathscr{M}_2(R_v)$ admet R_v pour discriminant. Mais par le lemme 26 un ordre est maximal ssi il admet R_v comme discriminant. De manière semblable, si \mathbf{H} est ramifié en v, alors \mathbf{H}_v admet un unique ordre maximal de discriminant vR_v et le même argument s'applique.

Références

- [AB04] Montserrat Alsina and Pilar Bayer. Quaternion orders, quadratic forms, and Shimura curves, volume 22 of CRM Monograph Series. American Mathematical Society, Providence, RI, 2004.
- [Lan82] Serge Lang. Introduction to algebraic and abelian functions, volume 89 of Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, second edition, 1982.
- [Vig80] Marie-France Vignéras. Arithmétique des algèbres de quaternions, volume 800 of Lecture Notes in Mathematics. Springer, Berlin, 1980.
- [Voi14] John Voight. The arithmetic of quaternion algebras. unpublished, 2014.