Algèbres de quaternions
Bordeaux – Workshop Fast

Aurel Page

But : être familier avec un énoncé tel que « l'anneau des endomorphismes d'une courbe supersingulière en caractéristique p est un ordre maximal dans l'algèbre de quaternions ramifiée en p et l'infini. »

Références : Vignéras, Arithmétique des algèbres de quaternions ; Voight, Quaternion algebras.

0 Échauffement non-commutatif

Tous nos anneaux seront associatifs et unitaires. Soit K un corps.

Definition 1. Une *K-algèbre* est un anneau A muni d'un morphisme d'anneaux $K \to Z(A)$.

En particulier, une K-algèbre est un K-espace vectoriel, et l'application $x \mapsto ax$ de multiplication par un élément fixé a est K-linéaire.

Comment peut-on décrire une algèbre ?

- Si $\dim_K A < \infty$, on peut en donner une table de multiplication : si $e_1, \dots, e_n$ est une K-base de A, alors $e_i e_j = \sum_{k=1}^{n} a_{i,j,k} e_k$. Les *constantes de structure* décrivent complètement la structure d'algèbre de A.

  Exemple : soit G un groupe fini. On peut définir l'algèbre de groupe $K[G]$ ayant une base $(e_g)_{g \in G}$, avec la table de multiplication $e_g e_h = e_{gh}$.

  Remarque : en général il est pénible de vérifier qu'une telle algèbre est associative !
- Une présentation par générateurs et relations.

  Exemple : l'algèbre libre à deux générateurs

$$\langle x, y \rangle_K = K \oplus Kx \oplus Ky \oplus Kx^2 \oplus Kxy \oplus Kyx \oplus Ky^2 \oplus \dots$$

  Remarque : en général (avec des relations), il peut être difficile de calculer la dimension d'une telle algèbre.
- Comme algèbre d'endomorphismes $\mathrm{End}(X)$ (dépend du contexte).

  Exemple : $\mathrm{End}_K(K^n) \cong \mathcal{M}_n(K)$.
- Comme sous-algèbre d'une autre.

  Exemple :

$$\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} : x, y, z \in K \right\} \subset \mathcal{M}_2(K).$$

Definition 2. Soit A une K-algèbre, et $a \in A$. L'élément a est *inversible à gauche* (resp. *à droite*) si il existe $u \in A$ tel que $ua = 1$ (resp. $au = 1$). L'élément a est un *diviseur de zéro à gauche* (resp. *à droite*) s'il existe $b \in A$ non nul tel que $ba = 0$ (resp $ab = 0$). L'ensemble des éléments de A inversibles à gauche et à droite est un groupe, noté $A^\times$.

Invertibilité à gauche et diviseur de zéro à droite sont incompatibles ($b = uab = 0$).

Pour toute notion qui a une version à gauche et à droite, *bilatère* = à gauche et à droite.

TODO vérifier que les notions sont habituellement dans ce sens.

Attention ! En général les notions à gauche et à droite sont distinctes !

Example 3. Soit V l'espace $K^{\mathbb{N}}$ des suites à valeurs dans K et $A = \mathrm{End}_K(V)$, et soit a le décalage vers la gauche : $a(u)_n = u_{n+1}$ pour tout $n \geq 0$. Alors

- a est inversible à droite : soit b le décalage vers la droite : $b(u)_0 = 0$ et $b(u)_n = u_{n-1}$ si $n \geq 1$. Alors $ab = 1$. En particulier a n'est pas un diviseur de zéro à gauche.
- a est un diviseur de zéro à droite : soit $c \in A$ l'application telle que $c(u)_0 = u_0$ et $c(u)_n = 0$. Alors $c \neq 0$ mais $ac = 0$. En particulier a n'est pas inversible à droite.

Proposition 4. *Soit A une K-algèbre de dimension finie. Soit $a \in A$. Alors*

1. *a est inversible à gauche si et seulement si a est inversible à droite ;*
2. *a est un diviseur de zéro à gauche si et seulement si a est un diviseur de zéro à droite ;*
3. *a est inversible si et seulement si a n'est pas un diviseur de zéro.*

Démonstration. La sous-algèbre $K[a] \subset A$ est de dimension finie, donc a admet un polynôme minimal $P \in K[X]$ non nul. On écrit $P = QX + \lambda$ avec $\lambda \in K$ et $Q \in K[X]$, d'où $Q(a)a = aQ(a) = \lambda$.

- Si $\lambda = 0$, alors a est un diviseur de zéro bilatère pour un même $b = Q(a) \in K[a]$.
- Si $\lambda \neq 0$, alors a est inversible bilatère pour un même $u = Q(a)/\lambda \in K[a]$.

□

Definition 5. Soit A une K-algèbre, et soit $I \subset A$ un sous-espace vectoriel. On dit que I est un *idéal à gauche* (resp. *à droite*) si $AI \subset I$ (resp. $IA \subset I$).

Remarque 6. Pour tout $a \in A$, Aa est un idéal à gauche et aA un idéal à droite. a est inversible à gauche (resp. à droite) si et seulement si $Aa = A$ (resp. $aA = A$).

Attention ! En général les notions à gauche et à droite sont distinctes !

Example 7. Soit $A = \mathcal{M}_2(K)$. Soient

$$I = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} : x, y \in K \right\} \subset A$$

et

$$J = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} : x, y \in K \right\} \subset A$$

Alors I est un idéal à gauche mais pas à droite, et J est un idéal à droite mais pas à gauche.

Rappel : Soit A un anneau commutatif. Alors A est un corps si et seulement si A n'a pas d'idéal non-trivial [1], si et seulement si tout morphisme d'anneau $A \to B$ est injectif.

Definition 8. Soit A une K-algèbre. On dit que A est une *algèbre à division* si $A^\times = A \setminus \{0\}$.

Proposition 9. *Soit A une K-algèbre de dimension finie. Les assertions suivantes sont équivalentes :*

(i) A est une algèbre à division ;

(ii) A n'a pas d'idéal à gauche non-trivial ;

(iii) A n'a pas d'idéal à droite non-trivial.

Démonstration. Si A est une algèbre à division, soit I un idéal à gauche non-nul, et soit $a \in I$ non nul. Alors a est inversible, donc $A = Aa \subset I$.

Réciproquement, supposons que A n'a pas d'idéal à gauche non-trivial. Soit $a \in A$ non nul. Alors $Aa \neq 0$, donc $Aa = A$ et a est inversible. □

Troisième propriété ?

Lemme 10. *Soit $f\colon A \to B$ un morphisme de K-algèbres. Alors* $\ker f$ *est un idéal bilatère de A et* $\ker f \neq A$. *Si $I \subsetneq A$ est un idéal bilatère, alors il existe une unique structure de K-algèbre sur A/I telle que $A \to A/I$ soit un morphisme d'algèbres.*

Démonstration. Exercice. □

Definition 11. Soit A une K-algèbre. On dit que A est *simple* si elle n'a pas d'idéal bilatère non-trivial.

Le lemme précédent implique alors

Proposition 12. *Soit A une K-algèbre. Alors A est simple si et seulement si tout morphisme $A \to B$ est injectif.*

Les notions d'algèbre à division et d'algèbre simple sont distinctes !

Example 13. Soit $A = \mathcal{M}_2(K)$. On sait que A n'est pas une algèbre à division. Montrons que A est simple.

Soit $I \subset A$ un idéal bilatère non trivial. Soit $a \in I$ non nul. Alors $Aa \subset I \neq A$, donc a n'est ni nul ni inversible. C'est donc une matrice de rang 1, donc il existe $u, v \in \mathrm{GL}_2(K)$ tels que $uav = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Quitte à remplacer I par uIv on peut supposer que $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Puisque I est un idéal à gauche, il contient $Aa =$

1. i.e. différent de 0 et A

$\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$; de même, puisque I est un idéal à droite, il contient $aA = \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$. Donc I contient $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, et contient donc également $Ab = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}$. Donc $I = A$, contradiction.

1 Algèbres de quaternions

Soit K un corps de caractéristique $\neq 2$.

Definition 14. Soit $a, b \in K^\times$. L'*algèbre de quaternions* $\left(\frac{a,b}{K}\right)$ est la K-algèbre engendrée par des éléments i et j satisfaisant les relations $i^2 = a$, $j^2 = b$ et $ij = -ji$.

Example 15. TODO Hamiltoniens

1.1 Propriétés élémentaires

Lemme 16. *Soit $A = \left(\frac{a,b}{K}\right)$, et soit $L \supset K$ un corps contenant un élément β tel que $\beta^2 = b$. Dans $\mathcal{M}_2(L)$, soient*

$$I = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \text{ et } J = \begin{pmatrix} \beta & 0 \\ 0 & -\beta \end{pmatrix}.$$

Alors il existe un morphisme d'algèbres $\phi\colon A \to \mathcal{M}_2(L)$ tel que $\phi(i) = I$ et $\phi(j) = J$.

Démonstration. Les matrices I, J satisfont $I^2 = a$, $J^2 = b$ et $IJ = -JI$. □

Proposition 17. *L'algèbre $A = \left(\frac{a,b}{K}\right)$ est de dimension 4 sur K. Les éléments $1, i, j$ et $k = ij$ forment une base de A et satisfont :*

- $i^2 = a$, $j^2 = b$, $k^2 = -ab$;
- $ij = k$, $ik = aj$;
- $ji = -k$, $jk = -bi$;
- $ki = -aj$, $kj = bi$.

Démonstration. Les relations sont laissées en exercice. Montrons l'assertion sur la dimension. $1, i, j, k$ est une famille génératrice : d'après la relation $ij = -ji$, A est linéairement engendrée par les $i^n j^m$, et d'après les relations $i^2 = a$ et $j^2 = b$, A est linéairement engendrée par $1, i, j, k$ et $\dim_K A \leq 4$.

Soient L, β, I, J, ϕ comme dans le Lemme TODO. Comme carac $K \neq 2$, on a $\beta \neq -\beta$ donc $1, I, J, IJ = \begin{pmatrix} 0 & -a\beta \\ \beta & 0 \end{pmatrix}$ sont K-linéairement indépendants, et donc $1, i, j, ij$ sont K-linéairement indépendants. □

Proposition 18. *Soit A une algèbre de quaternions. Alors le centre $Z(A)$ de A est réduit à K.*

Démonstration. Soit $w = x + yi + zj + tk \in Z(A)$ avec $x, y, z, t \in K$. Puisque w commute avec i on a $z = t = 0$. De plus w commute avec j et on a également $y = 0$, d'où $w \in K$. □

Proposition 19. *Soient $a, b, u, v \in K$. On a les isomorphismes suivants :*

1. $\left(\frac{a,b}{K}\right) \cong \left(\frac{u^2 a, v^2 b}{K}\right)$;
2. $\left(\frac{a,b}{K}\right) \cong \left(\frac{b,a}{K}\right) \cong \left(\frac{a,-ab}{K}\right)$;
3. $\left(\frac{a,1}{K}\right) \cong \mathcal{M}_2(K)$.

Démonstration. 1. et 2. sont laissés en exercice. Pour 3. on utilise le morphisme du Lemme TODO avec $L = K$ et on compare les dimensions. □

Corollaire 20. *Si K est algébriquement clos, alors toute algèbre de quaternion sur K est isomorphe à $\mathcal{M}_2(K)$.*

Démonstration. Tout élément de K est un carré, donc d'après Prop TODO 1. et 3. on a $\left(\frac{a,b}{K}\right) \cong \left(\frac{1,1}{K}\right) \cong \mathcal{M}_2(K)$. □

Definition 21. Soit A une algèbre de quaternions sur K, et soit $w = x + yi + zj + tk \in A$. On définit le *conjugué* $\bar{w}$ de w par $\bar{w} = x - yi - zj - tk$. On définit la *trace réduite* $\mathrm{trd}(w) = w + \bar{w}$ de w, la *norme réduite* $\mathrm{nrd}(w) = w\bar{w}$ de w et le *polynôme caractéristique réduit* $\chi_w = X^2 - \mathrm{trd}(w)X + \mathrm{nrd}(w)$ de w.

Proposition 22. *Soit A une algèbre de quaternions sur K. Alors pour tout $v, w \in A$ on a*

1. $\overline{vw} = \bar{w}\bar{v}$ *et* $\bar{\bar{w}} = w$;
2. $\mathrm{trd}(w) \in K$ *et* $2\,\mathrm{trd}(w) = \mathrm{Tr}_{A/K}(w)$;
3. $\mathrm{nrd}(w) \in K$, $\mathrm{nrd}(w) = \bar{w}w$ *et* $\mathrm{nrd}(vw) = \mathrm{nrd}(v)\,\mathrm{nrd}(w)$;
4. $\chi_w(w) = 0$.

Démonstration.

1. Puisque les applications $(v, w) \mapsto \overline{vw}$ et $(v, w) \mapsto \bar{w}\bar{v}$ sont K-bilinéaires, il suffit de vérifier la relation sur les paires d'éléments de la base. La vérification est laissée en exercice. Le caractère involutif est immédiat par définition.
2. En notant $w = x + yi + zj + tk$, on a $\mathrm{trd}(w) = 2x \in K$. Comme $2\,\mathrm{trd}$ et $\mathrm{Tr}_{A/K}$ sont K-linéaires, il suffit de vérifier leur égalité sur une base (vérification en exercice à partir de la table de multiplication).
3. Avec la même notation on calcule que $\mathrm{nrd}(w) = \bar{w}w = x^2 - ay^2 - bz^2 + abt^2 \in K$. On a $\mathrm{nrd}(vw) = vw\overline{vw} = vw\bar{w}\bar{v} = v\,\mathrm{nrd}(w)\bar{v} = \mathrm{nrd}(w)v\bar{v} = \mathrm{nrd}(w)\,\mathrm{nrd}(v)$.
4. On a $\chi_w(w) = w^2 - \mathrm{trd}(w)w + \mathrm{nrd}(w) = w^2 - (w + \bar{w})w + \mathrm{nrd}(w) = w^2 - w^2 - \mathrm{nrd}(w) + \mathrm{nrd}(w) = 0$.

□

Example 23. Soit $A = \mathcal{M}_2(K) = \left(\frac{1,1}{K}\right)$. Soit $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A$.

1. On a $\mathrm{trd}(m) = \mathrm{Tr}(m) = a + d$. En effet $2\,\mathrm{trd} = \mathrm{Tr}_{A/K} = 2\,\mathrm{Tr}$.
2. On a $\bar{m} = \mathrm{trd}(m) - m = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

3. On a $\mathrm{nrd}(m) = m\bar{m} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \det(m)$.

4. χ_m est le polynôme caractéristique au sens usuel des matrices.

Corollaire 24. *Soit A une algèbre de quaternions et $a \in A$. Alors a est inversible si et seulement si* $\mathrm{nrd}(a) \neq 0$.

Démonstration. $\mathrm{nrd}(a)$ est le terme constant du polynôme annulateur χ_a de a. □

1.2 Caractérisation

Le but de cette section est de démontrer le théorème suivant.

Théorème 25. *Soit A une K-algèbre. Les assertions suivantes sont équivalentes :*

(i) A est une algèbre de quaternions ;

(ii) il existe une extension de corps L/K telle que $A \otimes_K L \cong \mathcal{M}_2(L)$.

(iii) $Z(A) = K$, A est simple et $\dim_K A = 4$;

Lemme 26. *Soit A une algèbre de quaternions sur K. Alors il existe une extension de corps L/K telle que $A \otimes_K L \cong \mathcal{M}_2(L)$.*

Démonstration. Prendre L une extension au plus quadratique dans laquelle b est un carré. □

Lemme 27. *Soit A une K-algèbre. Supposons qu'il existe L/K une extension telle que $A \otimes_K L \cong \mathcal{M}_2(L)$. Alors A est simple.*

Démonstration. Soit $I \subset A$ un idéal bilatère. Alors $I \otimes_K L \subset \mathcal{M}_2(L)$ est un idéal bilatère, donc de dimension 0 ou 4 sur L, mais $\dim_L I \otimes_K L = \dim_K I$, donc I est un idéal trivial. □

Lemme 28. *Soit A une K-algèbre simple de dimension 4 et qui n'est pas une algèbre à division. Alors $A \cong \mathcal{M}_2(K)$.*

Démonstration. Soit I un idéal à gauche non nul. Par multiplication à gauche sur une base de I, on obtient un morphisme d'algèbres $\phi\colon A \to \mathcal{M}_n(K)$ où $n = \dim_K I$. De plus ϕ est injectif par simplicité de A, donc $n \geq 2$ et ϕ est un isomorphisme si et seulement si $n = 2$. Cherchons donc un idéal à gauche de dimension 2.

Puisque A n'est pas une algèbre à division, elle contient un élément non nul et non inversible a. Soit P le polynôme minimal de a.

- Si P a au moins deux facteurs irréductibles distincts, alors $K[a] \cong R_1 \times R_2$ contient un idempotent e non-trivial ($e^2 = e$ mais $e \neq 0, 1$). On a alors $A = Ae \oplus A(1-e)$, et les idéaux non-nuls Ae et $A(1-e)$ étant de dimension au moins 2, ils sont de dimension exactement 2 et $I = Ae$ convient.
- Sinon, a est nilpotent de degré [2] 2, 3 ou 4.
  — degré 4 : alors $A = K[a] \cong K[X]/(X^4)$. Un tel anneau est commutatif et admet l'idéal bilatère non-trivial Aa : impossible.

2. plus petit n tel que $a^n = 0$

— degré 3 : il existe une base dans laquelle la multiplication à droite par a a pour matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

donc $\dim_K Aa = 2$ et $I = Aa$ convient.

— degré 2 : il existe une base dans laquelle la multiplication à droite par a a pour matrice

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Dans le premier cas, $\dim_K Aa = 2$ donc $I = Aa$ convient, et dans le second cas $\dim_K Aa = 1 < 2$ ce qui est impossible.

□

Lemme 29. *Soit A une algèbre simple de dim 4. Alors il existe une extension telle que M2(L). TODO*

Nous sommes maintenant en mesure de prouver le théorème TODO, dont on rappelle l'énoncé.

Théorème 30. *Soit A une K-algèbre. Les assertions suivantes sont équivalentes :*

(i) A est une algèbre de quaternions ;

(ii) il existe une extension de corps L/K telle que $A \otimes_K L \cong \mathcal{M}_2(L)$.

(iii) $Z(A) = K$, A est simple et $\dim_K A = 4$;

Démonstration. TODO □

Corollaire 31. *Soit A une K-algèbre à division, de centre K et de dimension 4. Alors A est une algèbre de quaternions.*

Démonstration. Une algèbre à division est simple. □

Corollaire 32. *Soit A une algèbre de quaternions. On a exactement l'une des deux possibilités :*

1. *A est une algèbre à division ;*
2. *$A \cong \mathcal{M}_2(K)$.*

Démonstration. TODO mettre 2 lemmes ensemble □

1.3 Classification sur certains corps

Le but de cette section est de classifier les algèbres de quaternions sur $\mathbb{R}$, $\mathbb{C}$, les corps p-adiques et les corps de nombres.

2 Ordres et Idéaux

3 Courbes elliptiques supersingulières