Corps Non Commutatifs: Constructions
Travail d'Étude et de Recherche

Vincent R.B. Blazy
Encadré par Emmanuel Peyre

24 mai 2017

Table des matières

Conventions

Dans ce texte, un *corps* sera un anneau non nul au sein duquel tout élément non nul est inversible. Un corps peut donc *ne pas* être commutatif.

Remarque. Nous nous plaçons ainsi dans la droite ligne de l'acception terminologique traditionnelle française ; les anglophones préfèrent en effet réserver le terme « field » aux seuls corps commutatifs, et désignent un corps quelconque par l'expression : « division ring » (« anneau à division »).

Notation. $\forall (n,k) \in \mathbb{N}^* \backslash \{1\} \times [\![1,n]\!]$*, la* k*-ième composante de tout* n*-uplet* x *sera notée* x_k*.*

Chapitre I

Le corps des quaternions réels $\mathbb{H}$

Le premier exemple de corps non commutatif que l'on rencontre généralement est celui des quaternions réels, et ce fut le premier découvert, par l'Irlandais W. Hamilton en 1843.

Définition I.0.1. *L'*algèbre des quaternions réels *est $\mathbb{H}$ le groupe additif du $\mathbb{R}$-espace vectoriel $\mathbb{R}^4$ muni de la multiplication bilinéaire (notée par juxtaposition) telle que, en notant $(1, i, j, k)$ sa base usuelle ordonnée :*
- 1 est élément neutre de cette multiplication (faisant ainsi de $\mathbb{H}$ une algèbre unitaire) ;
- Elle est associative et sont vérifiées les relations suivantes :

$$i^2 = j^2 = k^2 = ijk = -1.$$

Remarque.
La distributivité de la multiplication sur l'addition suit de la bilinéarité de la première sur $\mathbb{R}^4$.

Propriété I.0.1. *La sous-$\mathbb{R}$-algèbre*

$$A := \left\{ \begin{pmatrix} a_1 + a_2 i & -a_3 - a_4 i \\ a_3 - a_4 i & a_1 - a_2 i \end{pmatrix} \middle| a \in \mathbb{R}^4 \right\}$$

de $M_2(\mathbb{C})$ est isomorphe à $\mathbb{H}$.

Démonstration. A est engendrée par $1 := I_2(\mathbb{C})$, $I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $K := \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, qui vérifient les relations de la définition :

$$I^2 = J^2 = K^2 = IJK = -1.$$

□

Remarque.
- $\mathbb{H}$ est donc une algèbre associative comme A, sous-algèbre de $M_2(\mathbb{C})$ qui l'est.
- On rappelle qu'une algèbre associative et unitaire est en particulier un anneau.

I.1 Conjugaison, norme et inverse

Définition I.1.1. $\forall\, q \in \mathbb{H}$,
- q_1 est la partie réelle de q et $q - q_1 = q_2 i + q_3 j + q_4 k$ la partie pure de q, d'ailleurs un quaternion de partie réelle nulle sera appelé quaternion pur ;
- Et $\bar{q} := q_1 - q_2 i - q_3 j - q_4 k$ sera le conjugué de q.

Remarque. Les réels sont les quaternions égaux à leurs conjugués, tandis que les quaternions purs sont ceux opposés à leurs conjugués.

Propriété I.1.1. *La conjugaison $\overline{Id_H} : H \to H : q \mapsto \bar{q}$ est un anti-isomorphisme de $\mathbb{H} : \forall\, (q, r) \in \mathbb{H}^2$:*

$$\overline{q + r} = \overline{q} + \overline{r} \wedge \overline{qr} = \overline{r}\,\overline{q}$$

Démonstration.
- L'égalité de sommes suit de la définition ;
- Quant au produit, il est vérifié par tous les $(q, r) \in \{i, j, k\}^2$, et donc par distributivité pour tout couple de quaternions réels. □

Définition I.1.2. $\forall\, q \in \mathbb{H}$, *la* norme de q dans $\mathbb{H}$ *est* $N(q) := q\bar{q}$.

Propriété I.1.2. *La fonction norme quaternionique $N := Id_H \overline{Id_H}$ est :*
(i) À valeurs réelles : $N(\mathbb{H}) \subset \mathbb{R}$;
(ii) Et multiplicative : $\forall\, (q, r) \in \mathbb{H}^2$,

$$N(qr) = N(q)N(r).$$

Démonstration. En effet :

(i) $\forall\, q \in \mathbb{H}$,

$$N(q) := q\bar{q} = q_1^2 + q_2^2 + q_3^2 + q_4^2 \in \mathbb{R}.$$

(ii) $\forall\,(q,r)\in\mathbb{H}^2$,

$$\begin{aligned} N(qr) &:= qr\overline{qr} && \text{par définition de } N(qr)\,;\\ &= qr\bar{r}\bar{q} && \text{par la propriété 1}\,;\\ &= qN(r)\bar{q} && \text{par définition de } N(r)\,;\\ &= q\bar{q}N(r) && \text{par réalité de } N(r) \text{ et bilinéarité du produit}\,;\\ \Rightarrow\quad N(qr) &= N(q)N(r) && \text{par définition de } N(q). \end{aligned}$$

□

Théorème I.1.1. *$\mathbb{H}$ est un corps, et : $\forall\, q\in\mathbb{H}\backslash\{0\}$, $q^{-1}=N(q)^{-1}\bar{q}$.*

Démonstration. Il suffit de montrer le second point. Or, N est définie, puisque : $\forall\, q\in\mathbb{H}$,

$$q\neq 0\Leftrightarrow(q_1,q_2,q_3,q_4)\neq 0\Leftrightarrow N(q)\neq 0.$$

Ainsi, la norme de tout quaternion réel est inversible dans $\mathbb{R}$:

$$N(\mathbb{H}\backslash\{0\})\subset\mathbb{R}\backslash\{0\}=R^{\times}.$$

D'où (en utilisant l'associativité) : $\forall\, q\in\mathbb{H}\backslash\{0\}$,

$$q(N(q)^{-1}\bar{q}):=N(q)^{-1}q\bar{q}=N(q)^{-1}N(q)=1.$$

De plus, comme pour toute loi de composition interne associative unifère, en la notant par juxtaposition et son neutre 1, si tout élément a admet un inverse à droite a^{-1} alors c'est également son inverse à gauche, puisque :

$$a^{-1}a=a^{-1}a(a^{-1}(a^{-1})^{-1})=a^{-1}(aa^{-1})(a^{-1})^{-1}=a^{-1}(a^{-1})^{-1}=1.$$

Par conséquent on a $\forall\, q\in\mathbb{H}\backslash\{0\}$, $q(N(q)^{-1}\bar{q})=(N(q)^{-1}\bar{q})q=1$. □

I.2 Sous-corps et automorphismes de $\mathbb{H}$

Lemme I.2.1. *Les quaternions purs sont ceux de carré réel négatif.*

Démonstration. $\forall\, q\in\mathbb{H}$,

$$q^2\in\mathbb{R}\Leftrightarrow q^2=\overline{q^2}=\bar{q}^2\Leftrightarrow(q-\bar{q})(q+\bar{q})=0,$$

donc comme $\mathbb{H}$ est un corps, $q^2\in\mathbb{R}\Leftrightarrow q=\pm\bar{q}$.
Si alors $q=\bar{q}$, c'est-à-dire $q\in\mathbb{R}$, et bien comme l'on s'y attend $q^2=q\bar{q}=N(q)\geq 0$, et si $q=-\bar{q}$, c'est-à-dire q quaternion pur, $q^2=-q\bar{q}=-N(q)\leq 0$. Ainsi $q^2\in\mathbb{R}$ si et seulement si le quaternion q est réel ou pur, et en particulier réel négatif si et seulement si il est pur. □

Chapitre II

Les algèbres de quaternions généralisés $\binom{\alpha,\beta}{k}$

Sur le modèle des quaternions réels, on peut construire sur un corps de base commutatif k quelconque une algèbre associative unitaire quadridimensionnelle à deux paramètres que l'on notera α et β. On va ainsi pouvoir chercher à identifier des conditions nécessaires et suffisantes pour que ces k-algèbres soit des corps non commutatifs (dont k sera le centre). Il se trouve que la construction des algèbres de ce que l'on appelle en caractéristique différente de 2 « quaternions généralisés » donne en caractéristique 2 des algèbres commutatives. Pour le sujet qui nous intéresse, nous découvrirons donc dans une seconde partie la construction quelque peu différente de ce qu'il convient de désigner sous ce même terme en caractéristique 2.

II.1 En caractéristique différente de 2

Dans toute cette sous-section, k sera un corps commutatif de caractéristique différente de 2, et α et β deux éléments de k.

Définition II.1.1. *L'*algèbre $\binom{\alpha,\beta}{k}$ des quaternions généralisés *est le k-espace vectoriel k^4 muni de la multiplication bilinéaire (notée par juxtaposition) telle que, en notant $e := (1, e_1, e_2, e_3)$ sa base usuelle ordonnée :*
- 1 est élément neutre de cette multiplication (faisant ainsi de $\binom{\alpha,\beta}{k}$ une algèbre unitaire) ;
- Elle est associative et sont vérifiées les relations suivantes :

$$e_1^2 = \alpha.1;\ e_2^2 = \beta.1;\ e_1e_2 = -e_2e_1 = e_3.$$

Remarque. - La seconde condition est remplaçable par la donnée de la table

de multiplication de la base e :

$\times$	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	$\alpha.1$	e_3	αe_2
e_2	e_2	$-e_3$	$\beta.1$	$-\beta e_1$
e_3	e_3	$-\alpha.1$	βe_1	$-\alpha\beta.1$

- On vérifie sans peine par bilinéarité que la multiplication définie par cette table est associative, alors que l'associativité est nécessaire en plus des relations de la définition pour obtenir la table.
- Le corps des quaternions réels $\mathbb{H}$ est comme attendu un cas particulier d'algèbre de quaternions généralisés (ce qui justifie la terminologie) :

$$\mathbb{H} = \begin{pmatrix} -1, -1 \\ \mathbb{R} \end{pmatrix}$$

Nous pouvons dès à présent poser une condition suffisante à ce que $\binom{\alpha,\beta}{k}$ ne soit pas un corps, car même pas exempte de diviseur de zéro ($e_3^2 = -\alpha\beta.1$) :

Définition II.1.2. *La k-algèbre $\binom{\alpha,\beta}{k}$ est dite* dégénérée *sitôt que $\alpha\beta = 0_k$,* non dégénérée *sinon.*

La non dégénérescence de $\binom{\alpha,\beta}{k}$ est alors une condition nécessaire à ce quelle soit un corps, mais nullement suffisante, ainsi que l'on va le voir dans la suite.

Définition II.1.3. $\forall\, q \in \binom{\alpha,\beta}{k}$,

- *Le* conjugué de q dans $\binom{\alpha,\beta}{k}$, *si $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ avec $(x_0, x_1, x_2, x_3) \in k^4$, est $\bar{q} := x_0 - x_1e_1 - x_2e_2 - x_3e_3$, comme dans le cas réel;*

- *Et la* norme de q dans $\binom{\alpha,\beta}{k}$ *est :*

$$N(q) := x_0^2 - \alpha x_1^2 - \beta x_2^2 - \alpha\beta x_3^2$$

($N(q) = q\bar{q} = \bar{q}q$ si l'on identifie canoniquement $k.1$, dans lequel $N(q)$ est à valeurs, avec k).

Lemme II.1.1.
(i) La conjugaison dans $\binom{\alpha,\beta}{k}$ en est un anti-isomorphisme ;
(ii) Et la norme y est multiplicative.

Démonstration. C'est la même que dans le cas particulier du corps $\mathbb{H}$. □

Propriété II.1.1. *L'algèbre* $\binom{\alpha,\beta}{k}$ *est un corps si et seulement si l'équation :*

$$x_0^2 - \alpha x_1^2 - \beta x_2^2 - \alpha\beta x_3^2 = 0_k$$

n'a d'autre solution $(x_0, x_1, x_2, x_3) \in k^4$ *que la solution triviale* $x_0 = x_1 = x_2 = x_3 = 0_k$*, c'est-à-dire si la fonction norme dans* $\binom{\alpha,\beta}{k}$ *est anisotrope.*

Démonstration. $\forall\, q \in \binom{\alpha,\beta}{k}$,

- Si $q \neq 0_{\binom{\alpha,\beta}{k}}$ est de norme nulle dans $\binom{\alpha,\beta}{k}$, il est diviseur de zéro dans $\binom{\alpha,\beta}{k}$ puisque $N(q) := q\bar{q} = 0$.

- Si réciproquement la condition est vérifiée, alors $q \neq 0_{\binom{\alpha,\beta}{k}} \Rightarrow N(q) \neq 0_k$ donc $N(q)$ est inversible dans k, et exactement de la même manière que pour le Théorème 1, on montre que q est inversible et du même coup que $q^{-1} = N(q)^{-1}\bar{q}$. □

Lemme II.1.2. *Si le premier paramètre est* 1_k *et le second non nul, alors la* k*-algèbre de quaternions généralisés n'est autre que celle des matrices carrées d'ordre* 2 *à coefficients dans* k *:*

$$\beta \neq 0_k \Rightarrow \binom{1_k, \beta}{k} \cong_{Alg_k} M_2(k)$$

Démonstration. En effet, si $\beta \neq 0_k$,
L'application linéaire de $\binom{1_k,\beta}{k}$ dans $M_2(k)$ faisant correspondre à la base $(1_{\binom{1_k,\beta}{k}}, e_1e_2e_3)$ de la première, la base $\left(I_2(k),\, A := \left(\begin{smallmatrix} 1_k & 0_k \\ 0_k & -1_k \end{smallmatrix}\right),\, B := \left(\begin{smallmatrix} 0_k & 1_k \\ \beta & 0_k \end{smallmatrix}\right) \text{ et } C := \left(\begin{smallmatrix} 0_k & -1_k \\ \beta & 0_k \end{smallmatrix}\right)\right)$ de la seconde, est un isomorphisme de k-algèbres :
C'est un isomorphisme linéaire, et il commute aux multiplications au but et à la source, ainsi qu'il suffit de le vérifier pour les relations qui définissent celle de $\binom{1_k,\beta}{k}$:

$$A^2 = 1_k.I_2(k),\ B^2 = \beta.I_2(k) \text{ et } AB = -BA = C.$$

□

Théorème II.1.1. *Si* $\alpha\beta \neq 0_k$ *alors les assertions suivantes sont équivalentes :*

(i)	$(*)$ $\alpha x_1^2 + \beta x_2^2 = x_3^2$ *a une solution non triviale* $x \in k^3$
(ii)	$\binom{\alpha,\beta}{k} \cong_{Alg_k} M_2(k)$
(iii)	$\binom{\alpha,\beta}{k}$ *n'est pas un corps*
(iv)	$(**)$ $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0_k$ *a une solution non triviale* $(x_0, x_1, x_2, x_3) \in k^4$

Démonstration.

- $(i) \Rightarrow (ii)$:
• Si une solution $x \in k^3$ de $(*)$ est telle que $x_3 \neq 0_k$, alors on a une solution non triviale $y \in k^2$ de $\alpha y_1^2 + \beta y_2^2 = 1_k$. Ainsi en posant $\varepsilon_1 := y_1 e_1 + y_2 e_2$, $\varepsilon_2 := e_3$ et $\varepsilon_3 := \varepsilon_1 \varepsilon_2$, on a en particulier $\varepsilon_3 = -\beta y_2 e_1 + \alpha y_1 e_2$ et il n'est donc pas colinéaire à ε_1, faute de quoi on aurait soit $y_1 y_2 = 0_k$, auquel cas $\varepsilon_3 \,//\, e_1$ ou $\varepsilon_3 \,//\, e_2$ (vecteurs nullement colinéaires à ε_1 d'où une contradiction), soit $\dfrac{\alpha y_1}{y_2} = -\dfrac{\beta y_2}{y_1}$ et donc $\alpha y_1^2 + \beta y_2^2 = 0_k$ ce qui est absurde car $0_k \neq 1_k$ puisque k est non nul.
Par conséquent, nous disposons là d'une base $(1, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ de $\left(\frac{\alpha,\beta}{k}\right)$ telle que :

$$\varepsilon_1^2 = 1, \varepsilon_2^2 = -\alpha\beta \text{ et } \varepsilon_3 = -\varepsilon_1\varepsilon_2,$$

i.e. d'un isomorphisme de k-algèbre entre $\left(\frac{\alpha,\beta}{k}\right)$ et $\left(\frac{1_k,-\alpha\beta}{k}\right)$ qui est elle-même isomorphe à $M_2(k)$ (puisque par hypothèse $\alpha\beta \neq 0_k$) par le lemme **II.2.1.2** précédent.
• Si à l'inverse pour toute solution $x \in k^3$ de $(*)$ on a $x_3 = 0_k$, en supposant sans perte de généralité que $x_2 \neq 0_k$, c'est que $-\dfrac{\alpha}{\beta} = \left(\dfrac{x_1}{x_2}\right)^2$ ou encore $-\alpha\beta = \left(\beta\dfrac{x_1}{x_2}\right)^2$ est carré. Or, $\forall\, \lambda \in k$,

$$\left(\frac{\alpha,\beta}{k}\right) \cong_{Alg_k} \left(\frac{\alpha,\lambda^2\beta}{k}\right)$$

via l'isomorphisme par lequel l'image de e_2 est λe_2 et qui laisse fixes les autres vecteurs de la base e. Donc ici :

$$\left(\frac{\alpha,-\alpha\beta}{k}\right) \cong_{Alg_k} \left(\frac{\alpha,1_k}{k}\right).$$

De même l'envoi de e sur la base $\left(1_{\left(\frac{\alpha,\beta}{k}\right)}, e_2, e_1, -e_3\right)$ de $\left(\frac{\alpha,\beta}{k}\right)$ donne l'isomorphisme :

$$\left(\frac{\alpha,\beta}{k}\right) \cong_{Alg_k} \left(\frac{\beta,\alpha}{k}\right),$$

et en l'envoyant si $\alpha \neq 0_k$ sur $\left(1_{\left(\frac{\alpha,\beta}{k}\right)}, e_1, e_3, \alpha e_3\right)$, l'isomorphisme :

$$\left(\frac{\alpha,\beta}{k}\right) \cong_{Alg_k} \left(\frac{\alpha,-\alpha\beta}{k}\right);$$

Donc finalement, comme $\alpha\beta \neq 0_k$, en utilisant en sus le lemme précédent **II.2.1.2** :

$$\left(\frac{\alpha,\beta}{k}\right) \cong_{Alg_k} \left(\frac{\alpha,-\alpha\beta}{k}\right) \cong_{Alg_k} \left(\frac{\alpha,1_k}{k}\right) \cong_{Alg_k} \left(\frac{1_k,\alpha}{k}\right) \cong_{Alg_k} M_2(k).$$

- $(ii) \Rightarrow (iii)$:
Cette implication provient de ce qu'une algèbre de matrice comporte toujours

un élément non nul mais néanmoins non inversible, tel ici que $\begin{pmatrix} 0_k & 1_k \\ 0_k & 0_k \end{pmatrix}$ qui est même diviseur de zéro dans $M_2(k)$.

- $(iii) \Rightarrow (iv)$:
Cette implication constitue, avec sa réciproque, la propriété **II.2.1.1**.

- $(iv) \Rightarrow (i)$:
Si $\exists\, \lambda \in k$, $\alpha = \lambda^2$, alors comme vu en démontrant la première implication :

$$\begin{pmatrix} \alpha, \beta \\ k \end{pmatrix} = \begin{pmatrix} \lambda^2, \beta \\ k \end{pmatrix} \cong_{Alg_k} \begin{pmatrix} \beta, \lambda^2 \\ k \end{pmatrix} \cong_{Alg_k} \begin{pmatrix} \beta, 1_k \\ k \end{pmatrix} \cong_{Alg_k} M_2(k).$$

Si α n'est pas carré dans k, soit $(x_0, x_1, x_2, x_3) \in k^4$ est une solution non triviale de l'équation $(**)$. Si $x_3 = 0_k$, $(**)$ devient au signe près $(*)$ et la première implication donne le résultat. Sinon, le quaternion $x_2 - x_3 e_1$ est inversible, car sa norme $x_2^2 - \alpha x_3^2$ ne peut être nulle ; sans quoi α serait égal à $\left(\frac{x_2}{x_3}\right)^2$ et donc carré. Ainsi :

$$(x_2 - x_3 e_1)(x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3) = x_2 x_0 - \alpha x_1 x_3 + (x_1 x_2 - x_0 x_3) e_1 + (x_2^2 - \alpha x_3^2) e_2$$

est non nul (comme produit d'un élément inversible par un non nul), mais de norme

$$(x_0 x_2 - \alpha x_1 x_3)^2 - \alpha (x_1 x_2 - x_0 x_3)^2 - \beta (x_2^2 - \alpha x_3^2)^2$$

nulle par $(**)$; d'où la solution $(x_1 x_2 - x_0 x_3, x_2^2 - \alpha x_3^2, x_0 x_2 - \alpha x_1 x_3) \in k^3$ de $(*)$, non triviale car $x_2^2 - \alpha x_3^2 \neq 0_k$.

Bilan : Du cycle d'implication ainsi fermé résultent bien les équivalences requises. □

II.2 En caractéristique 2

Dans cette seconde sous-section, nous noterons K un corps non commutatif de dimension 4 sur son centre k de dimension 2, et nous tenterons de déterminer sa nécessaire structure pour en venir à ce que nous pourrons définir comme étant les algèbres de quaternions généralisés en cette caractéristique.

Définition II.2.1. *Soit $\mathbb{K}$ un corps commutatif et A une $\mathbb{K}$-algèbre associative. $\forall\, x \in A$, comme dans le cas des extensions de corps commutatifs,*
- Le degré de x dans A sur $\mathbb{K}$ *sera la dimension de la sous-$\mathbb{K}$-algèbre de A engendrée par x, encore notée $\mathbb{K}_A(x)$;*
- Et le polynôme minimal de x dans A sur $\mathbb{K}$ *sera $P_x^{\mathbb{K},A}$ l'unique générateur*

unitaire de l'idéal de $\mathbb{K}[X]$ *annulateur de* x *;*
- x *est alors* séparable dans A sur $\mathbb{K}$ *dès que* $P_x^{\mathbb{K},A}$ *est séparable, et* inséparable dans A sur $\mathbb{K}$ *sinon.*

Notation. *Soit* $\mathbb{K}$ *un corps commutatif.*
- Pour toute $\mathbb{K}$*-algèbre* A*,* $Z(A)$ *sera le centre de* A *;*
- Pour toute extension (commutative) $\mathbb{L}$ *de* $\mathbb{K}$ *et polynôme* P *à coefficients dans* $\mathbb{K}$*,* $Z_{\mathbb{L}}(P)$ *sera l'ensemble des racines de* P *dans* $\mathbb{L}$*.*

Lemme II.2.1. *Tout élément non central de* K *est de degré* 2 *sur* k *:*

$$\forall\, x \in K,\ [k_K(x) : k] = 2.$$

Démonstration. En effet, $\forall\, x \in K\backslash k$, on a par multiplicativité des degrés (qui a toujours cours ici comme dans le cas des extensions de corps) :

$$4 = [K : k] = [K : k_K(x)][k_K(x) : k];$$

or l'on ne peut avoir ni $[K : k_K(x)] = 1$ car $k_K(x)$ est commutatif et K ne l'est pas, ni $[k_K(x) : k] = 1$ car $x \notin k$. Donc $[K : k_K(x)] = [k_K(x) : k] = 2$. □

Lemme II.2.2. $\forall\, x \in K\backslash k$*, si* x *est séparable dans* K *sur* k*, alors :*

$$\exists\,(e,(\alpha,\beta)) \in K^2 \times k^2,\ k_K(x) = k_K(e_1)\ \textit{et}\ (**)_e \begin{cases} P_{e_1}^{k,K} = X^2 + X + \alpha & (1) \\ e_2^{-1} e_1 e_2 = e_1 + 1 & (2) \\ e_2^2 = \beta & (3) \end{cases}$$

Démonstration. En effet, soit x un élément de $K\backslash k$ séparable dans K sur k :

$$\exists\, a \in k^* \times k,\ P_x^{k,K} = X^2 + a_1 X + a_2,$$

puisque $x \notin k$, donc $deg(P_x^{k,K}) = [k_K(x) : k] = 2$ par le lemme **II.2.2.1** précédent, et de plus x étant séparable dans K sur k, $a_1 \notin 0$ faute de quoi on aurait $P_x^{k,K} = X^2 + a_2$ qui a une racine double, dans une extension convenable de k.
On a alors $P_{a_1^{-1}x}^{k,K} = X^2 + X + a_2/a_1^2$, et on peut donc poser $(e_1, \alpha) := (a_1^{-1}x, a_2/a_1^2)$.
Maintenant $\forall\, y \in K\backslash k_K(e_1)$, $ye_1 \neq e_1 y$, sinon $K = k_K(e_1, y)$ serait commutatif ; cela revient à dire que $z := ye_1 + e_1 y \neq 0_K$. Ainsi :

$$\begin{aligned} & ze_1 + e_1 z &=& \ ye_1^2 + e_1 y e_1 + e_2 y e_2 + e_1^2 y && \text{par définition de } z \text{ et distributivité}\,; \\ & &=& \ y(e_1 + \alpha) + (e_1 + \alpha)y && \text{car } P_{e_1}^{k,K} = X^2 + X + \alpha \text{ et } car(k) = 2\,; \\ \Rightarrow\ & ze_1 + e_1 z &=& \ z && \text{car } \alpha \in k = Z(K), \end{aligned}$$

soit : $z^{-1}e_1z = e_1 + 1_K$. Par suite :

$$z^{-2}e_1z^2 = z^{-1}e_1z + 1 = e_1 + 1_K + 1_K = e_1,$$

et donc z^2 commute avec e_1 d'où $z^2 \in k_K(e_1)$ (sinon $K = k_K(e_1, z^2)$ serait commutatif). Or $k_K(e_1) \bigcap k_K(z) = k$ donc $z^2 \in k$. On peut ainsi poser $e_2 := z^2$ et $\beta := z$. □

Lemme II.2.3. *$\forall\, z \in K\backslash k$, si z est inséparable dans K sur k, alors $\exists\, u \in K$ tel que $z^{-1}uz = u + 1_K$ et les propriétés $(**)_{(u,z)}$ soient vérifiées, c'est-à-dire que u et z aient les mêmes propriétés que e_1 et e_2 dans le lemme **II.2.2.2** précédent.*

Démonstration. En effet, soit z un élément de $K\backslash k$ inséparable dans K sur k :

$$\exists\, \beta \in k,\ P_z^{k,K} = X^2 + \beta,$$

puisque $z \notin k$ donc $deg(P_z^{k,K}) = 2$ toujours par le lemme **II.2.2.1**, et de plus si le terme a d'indice 1 (id est le ≪ coefficient devant X ≫) de $P_z^{k,K}$ était non nul, alors on aurait $(P_z^{k,K})' = a$ et donc $Z_{\mathbb{L}}(P_z^{k,K}) \bigcap Z_{\mathbb{L}}((P_z^{k,K})') = \emptyset$, c'est-à-dire la séparabilité de $P_z^{k,K}$.
Soit alors l'automorphisme intérieur de K $\sigma := z^{-1}Id_K z$; ce n'est pas l'identité de K (sinon $z \in Z(K) = k$ ce qui n'est pas), mais $\sigma^2 = Id_K$ puisque $z^2 = \beta \in k$. Maintenant, soit $x \in K\backslash k_K(z)$. Alors $zx \neq xz$ comme dans la démonstration précédente pour y et e_1 et donc $t := \sigma(x) + x \neq 0_K$, d'où :

$$\sigma(t) = \sigma^2(x) + \sigma(x) = x + \sigma(x) = t,$$

et ainsi $u := t^{-1}x$ répond à la question car :

$$\sigma(t^{-1}x) = \sigma(t)^{-1}\sigma(x) = t^{-1}(x + t) = t^{-1}x + 1_K.$$

En outre, u et $u+1_K$ qui sont par conséquent conjugués par un k-automorphisme de K ont par suite dans K le même polynôme minimal sur k ; qui a ainsi comme racines dans $k_K(u)$ ces deux éléments de somme 1 donc est de la forme $X^2 + X + \alpha$ pour un $\alpha \in k$ (en effet $k_K(u)$ est un sous-corps de K contenant k donc $P_u^{k,k_K(u)} = P_u^{k,K}$). Ceci termine de montrer $(**)_{(u,z)}$. □

Nous voyons donc que par le lemme **II.2.2.2**, l'existence dans $K\backslash k$ d'un élément x séparable de K sur k entraîne celle d'un élément e_2 inséparable de K sur k, et qu'inversement par le lemme **II.2.2.3**, celle d'un z inséparable entraîne celle d'un e_1 séparable. Par conséquent, le principe du tiers exclus nous confirme l'existence dans $K\backslash k$ à la fois d'un élément séparable et d'un autre inséparable de K sur k, et donc des éléments e_1 et e_2 du premier de ces deux lemmes, qui vérifient $(**)_{(e_1,e_2)}$ pour un certain couple $(\alpha, \beta) \in k$.

Théorème II.2.1. *Avec les notations précédentes, et en notant $e_3 := e_1e_2$,*
(i) $(1_K, e_1, e_2, e_3)$ forme une k-base de K ;
(ii) Et sa table de multiplication dans K est donnée par $(**)_{(e_1,e_2)}$.

Démonstration. En effet,

(i) Soit $(x_0, x_1, x_2, x_3) \in k^4$ tel que $x_0 + x_1e_1 + x_2e_2 + x_3e_3 = 0_K$.
Si $x_3 = 0_k$, la nullité de x_1, x_2 et x_3 résulte de ce que $e_2 \notin k_K(e_1)$ en raison du lemme **II.2.2.2**.
Si $x_3 \neq 0_k$, alors $x_2e_2 + x_3e_3 = (x_2 + x_3e_1)e_2 \neq 0_K$ et, en multipliant à gauche par $(x_2+x_3e_1)^{-1}$, on obtient $(x_2+x_3e_1)^{-1}(-x_0+x_1e_1) = e_2$ et donc une égalité du type $y_0 + y_1e_1 + e_2 = 0_K$ avec $y_0, y_1 \in k$, ce qui est absurde.

(ii) Énumérons ci-dessous les égalités manquant pour compléter la table de multiplication de la base e de K sur k :

$e_1^2 = \alpha + e_1$ par (2) ;

$$\begin{array}{rrcll} & e_3^2 & = & e_1(e_2e_1e_2) & \\ & & = & e_1\beta(e_2^{-1}e_1e_2) & \text{par (3)}, \\ & & = & e_1\beta(e_1 + 1_K) & \text{par (2)}, \\ & & = & \beta e_1^2 + \beta e_1 & \\ & & = & \beta(\alpha + e_1) + \beta e_1 & \text{(cela vient d'être montré)}, \\ \Rightarrow & e_3^2 & = & \alpha\beta & \text{car } car(k) = 2\,; \end{array}$$

$e_2e_1 = e_2(1_K + e_2^{-1}e_1e_2) = e_2 + e_3$ par (2) ;

$e_1e_3 = e_1^2e_2 = (\alpha + e_1)e_2 = \alpha e_2 + e_3$ par (2) ;

$$\begin{array}{rrcll} & e_3e_1 & = & e_1e_2e_1 & \text{par définition de } e_3, \\ & & = & e_2(e_2^{-1}e_1e_2)e_1 & \\ & & = & e_2e_1 + e_2e_1^2 & \text{par (2)}, \\ & & = & e_2e_1 + e_2\alpha + e_2e_1 & \text{par (1)}, \\ \Rightarrow & e_3e_1 & = & \alpha e_2 & \text{car } car(k) = 2; \end{array}$$

$e_2e_3 = e_2e_1e_2 = e_2^2(e_2^{-1}e_1e_2) = \beta(e_1 + 1_K) = \beta + \beta e_1$ par (2) ; et enfin :

$e_3e_2 = e_1e_2^2 = \beta e_1$ par (3).

On obtient donc la table suivante :

$\times$	1_K	e_1	e_2	e_3
1_K	1_K	e_1	e_2	e_3
e_1	e_1	$\alpha + e_1$	e_3	$\alpha e_2 + e_3$
e_2	e_2	$e_2 + e_3$	β	$\beta + \beta e_1$
e_3	e_3	αe_2	βe_1	$\alpha\beta$

□

On peut ainsi poser :

Définition II.2.2. *Soit k un corps commutatif de caractéristique 2 et $(\alpha, \beta) \in k^2$. L'*algèbre $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ de quaternions généralisés *est le k-espace vectoriel k^4 muni de la multiplication bilinéaire (notée par juxtaposition) telle que, en notant $e :=$*

$(1, e_1, e_2, e_3)$ *sa base usuelle ordonnée :*
- 1 *est élément neutre de cette multiplication (faisant ainsi de* $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ *une algèbre unitaire) ;*
- *Elle est associative et sont vérifiées les relations suivantes :*

$$e_1^2 = e_1 + \alpha.1;\ e_2^2 = \beta.1;\ e_1e_2 = e_3 = e_2e_1 + e_2.$$

Remarque*.*
- La seconde condition est remplaçable sous réserve de redondances par la table de multiplication de la base e. - Comme de coutume, on identifiera canoniquement $k.1$ à k pour noter, $\forall\, x \in k$, indifféremment les éléments $x.1$ de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ et x de k.

Définition II.2.3. *La* k*-algèbre* $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ *est dite* dégénérée *sitôt que* $\beta = 0_k$*,* non dégénérée *sinon.*

Comme dans le cas de la caractéristique différente de 2, la non dégénérescence de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ est alors une condition nécessaire à ce qu'elle soit exempte de diviseur de zéro et donc a fortiori un corps, mais sera tout aussi loin d'être suffisante. En revanche on a déjà le résultat suivant :

Théorème II.2.2. *Tout corps non commutatif de caractéristique* 2 *de dimension* 4 *sur son centre* k *est isomorphe en tant que* k*-algèbre à une algèbre de la forme* $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$*.*

Démonstration. Cela suit par l'étude menée dans cette sous-section **II.2.2** de la définition de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$. □

Définition II.2.4. $\forall\, q \in \left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$*,*

- *Le* conjugué de q dans $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$*, si* $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ *avec* $(x_0, x_1, x_2, x_3) \in k^4$*, est* $\bar{q} := x_0 + x_1 + x_1e_1 + x_2e_2 + x_3e_3$*.*

- *Et la* norme de q dans $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ *est :*

$$N(q) := x_0^2 + x_0x_1 + \alpha x_1^2 + \beta(x_2^2 + x_2x_3 + \alpha x_3^2)$$

($N(q) = q\bar{q} = \bar{q}q$ *toujours comme dans les précédents cas).*

Lemme II.2.4.
(i) La conjugaison dans $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ *en est un anti-isomorphisme ;*
(ii) Et la norme y est multiplicative.

Démonstration.

(i) En posant $\varepsilon_1 := e_1 + 1$, les relations reliant les éléments de la base e dans la définition de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ donnent que :
- $\varepsilon_1^2 = e_1^2 + 2e_1 + 1 = \alpha + e_1 + 1 = \alpha + \varepsilon_1$;
- $\varepsilon_1 e_2 + e_2\varepsilon_1 = e_1e_2 + e_2 + e_2e_1 + e_2 = e_2$;
- et : $e_2\varepsilon_1 = e_2e_1 + e_2 = e_3$.

Par conséquent, la multiplication *opposée* à celle de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ donne lieu à la même table que la multiplication pour e, en remplaçant e_1 par ε_1 ; et donc l'application linéaire ϕ envoyant e_1 sur ε_1 tout en fixant les autres vecteurs de e est un anti-isomorphisme de $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$. Or :

$$\begin{array}{rcl}\phi : q = x_0 + x_1e_1 + x_2e_2 + x_3e_3 & \longmapsto & x_0 + x_1\,(e_1 + 1) + x_2e_2 + x_3e_3\\ & = & x_0 + x_1 + x_1e_1 + x_2e_2 + x_3e_3\\ & = & \bar{q}\end{array}$$

n'est autre que la conjugaison dans $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$.

(ii) C'est encore la même que dans le cas du corps $\mathbb{H}$ et plus généralement des algèbres $\left(\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ de quaternions généralisés sur des corps de caractéristique différente de 2. □

Propriété II.2.1. *L'algèbre $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ est un corps si et seulement si l'équation :*

$$x_0^2 + x_0x_1 + \alpha x_1^2 + \beta(x_2^2 + x_2x_3 + \alpha x_3^2) = 0_k$$

n'a d'autre solution $(x_0, x_1, x_2, x_3) \in k^4$ que la solution triviale $x_0 = x_1 = x_2 = x_3 = 0_k$, c'est-à-dire si la fonction norme dans $\left[\begin{smallmatrix}\alpha,\beta\\ k\end{smallmatrix}\right)$ est définie.

Démonstration. Il s'agit encore une fois de la même démonstration qu'en caractéristique différente de 2. □

Exemple. *Un corps de quaternions en caractéristique 2 :*
On prend $k := \mathbb{F}_2(X)$. On peut vérifier que l'équation

$$x_0^2 + x_0x_1 + x_1^2 + (x_2^2 + x_2x_3 + x_3^2)X_{\mathbb{F}_2} = 0_{\mathbb{F}_2(X)}$$

n'admet pas de solution non triviale $(x_0, x_1, x_2, x_3) \in \mathbb{F}_2(X)^4$, et ainsi la $\mathbb{F}_2(X)$-algèbre $\left[\begin{smallmatrix}1_{\mathbb{F}_2(X)},X_{\mathbb{F}_2}\\ \mathbb{F}_2(X)\end{smallmatrix}\right)$ est un corps, non commutatif, de dimension 4 sur son centre $\mathbb{F}_2(X)$.

On peut montrer que les propriétés des algèbres de quaternions généralisés sont analogues en caractéristiques 2 et différente de 2, notamment que tout corps non commutatif de dimension 4 sur son centre en est un de quaternions généralisés. En particulier, on note que du théorème de Wedderburn, qui affirme que tout corps fini est commutatif (et donc est isomorphe à $\mathbb{F}_{p^n}$ pour un nombre premier p et un entier naturel non nul n), découle donc qu'une algèbre quadridimensionnelle sur le corps fini $\mathbb{F}_{p^n}$ est soit le corps commutatif $\mathbb{F}_{p^{4n}}$, soit isomorphe à la $\mathbb{F}_{p^n}$-algèbre des matrices carrées d'ordre 2 à coefficients dans $\mathbb{F}_{p^n}$.

Chapitre III

Un corps non commutatif de degré 9 sur son centre $\mathbb{Q}$

III.1 Étude d'un corps commutatif L

Tous les corps rencontrés dans les paragraphes précédents sont des corps de quaternions, ils sont de dimension 4 sur leur centre. Avant de présenter des constructions plus générales de corps non commutatifs, en voici un exemple tout à fait différent : un corps de dimension 9 sur son centre $\mathbb{Q}$.
Soit $L := \mathbb{Q}_{\mathbb{C}}\left(\cos\left(\frac{2\pi}{7}\right)\right)$ le sous-corps de $\mathbb{C}$ engendré par $\cos\left(\frac{2\pi}{7}\right)$.

Lemme III.1.1.
- Le degré de L sur $\mathbb{Q}$ vaut trois :

$$[L : \mathbb{Q}] = 3.$$

Démonstration. Il est commode de poser $\theta := e^{\frac{2i\pi}{7}}$ se placer dans $\mathbb{Q}_{\mathbb{C}}(\theta)$; on a alors $\theta^7 = 1$ ainsi que :

$$\theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1 = 0$$

Posons alors :

$$\begin{aligned} u &:= \theta + \theta^6 = 2cos\left(\tfrac{2\pi}{7}\right) \\ v &:= \theta^2 + \theta^5 = 2cos\left(\tfrac{4\pi}{7}\right) \quad \text{et} \\ w &:= \theta^3 + \theta^4 = 2cos\left(\tfrac{6\pi}{7}\right), \end{aligned}$$

On a alors : $u + v + w = -1$; mais aussi :

$$u^2 = 2 + v,\ v^2 = 2 + w \text{ et } w^2 = 2 + u;$$

ainsi que :

$$uv = u + w,\ vw = u + v \text{ et } uw = v + w;$$

d'où : $uv + vw + wu = -2$, puis :

$$uvw = uw + w^2 = v + w + u + 2 = 1.$$

On voit alors par le truchement des relations coefficients-racines que u, v et w sont les trois racines dans $\mathbb{Q}_{\mathbb{C}}(\theta)$ et donc dans $\mathbb{C}$ du polynôme $P := X^3 + X^2 - 2X - 1$.

Montrons que P est irréductible dans $\mathbb{Q}[X]$.
Par l'absurde dans le cas contraire, P aurait un facteur de degré 1, donc une racine rationnelle, or, $\forall\,(p,q) \in \mathbb{Z} \times \mathbb{N}^*$:

$$P\left(\frac{p}{q}\right) = \frac{p^3 + p^2 - 2pq^2 - q^3}{q^3}$$

Partant, si $\frac{p}{q}$ est irréductible, alors la considération de trois cas suffira :

• $|q| > 1 \Rightarrow p^3 + p^2 - 2pq^2 - q^3 \equiv p^3\ [|q|] \Rightarrow P\left(\frac{p}{q}\right) \neq 0$, donc $q = \pm 1$ et $\frac{p}{q} \in \mathbb{Z}$;

• $|p| > 1 \Rightarrow p^3 + p^2 - 2pq^2 - q^3 \equiv -q^3\ [|p|] \Rightarrow P\left(\frac{p}{q}\right) \neq 0$;

• Et enfin comme $1, -1$ et 0 ne sont pas non plus racines de P, ce dernier est sans racine rationnelle et en conséquence irréductible dans $\mathbb{Q}[X]$. Par conséquent P, unitaire, est le polynôme minimal de u de $\mathbb{Q}$ dans $\mathbb{C}$, est il est de degré 3 donc $L = \mathbb{Q}_{\mathbb{C}}\left(cos\left(\frac{2\pi}{7}\right)\right) = \mathbb{Q}_{\mathbb{C}}\left(\frac{u}{2}\right) = \mathbb{Q}_{\mathbb{C}}(u)$ est bien de degré 3 sur $\mathbb{Q}$.
La famille $(1, u, u^2)$ est alors une $\mathbb{Q}$-base de L, et donc (u, v, w) aussi, puisque $v = u^2 - 2$ et $w = v^2 - 2$ sont dans L, et qu'avec u ils l'engendrent :

$$1 = -u - v - w$$

$$u = u \qquad \text{et}$$

$$u^2 = 2 + v = -2u - v - 2w.$$

□

Définition III.1.1. *$\forall\,\xi \in L$, la* norme de ξ dans L *sera* $N(\xi) := det(\Xi)$ *où* Ξ *note l'endomorphisme $\mathbb{Q}$-linéaire de L de multiplication par ξ.*

Lemme III.1.2. *L'automorphisme $\mathbb{Q}$-linéaire σ de L tel que :*

$$\sigma(u) = v,\ \sigma(v) = w,\ \textit{et } \sigma(w) = u$$

est un automorphisme d'ordre 3 *de L.*

Démonstration. En effet,

$$\sigma(uv) = \sigma(u+w) = \sigma(u) + \sigma(w) = v + u = vw = \sigma(u)\sigma(v),$$

$$\sigma(vw) = \sigma(u+v) = \sigma(u) + \sigma(v) = v + w = wu = \sigma(v)\sigma(w),$$

$$\text{et } \sigma(uw) = \sigma(v+w) = \sigma(v) + \sigma(w) = w + u = vu = \sigma(u)\sigma(w);$$

et de plus σ permutant cycliquement les éléments de la base (u, v, w) dans cet ordre, $\sigma^2 \neq Id_L$ et $\sigma^3 = Id_L$, son ordre est donc bien 3. □

Propriété III.1.1. $\forall\, \xi \in L$,

$$N(\xi) = \xi\sigma(\xi)\sigma^2(\xi).$$

Démonstration.
Si $\xi \in \mathbb{Q}$ alors Ξ étant l'homothétie de rapport ξ,

$$det(\Xi) = \xi^3 = \xi\sigma(\xi)\sigma^2(\xi).$$

Si $\xi \notin \mathbb{Q}$, ξ est racine du polynôme caractéristique χ_Ξ de Ξ, et $\sigma(\xi)$ et $\sigma^2(\xi)$ qui ont le même polynôme minimal en sont en conséquence les deux autres racines ; donc $\xi\sigma(\xi)\sigma^2(\xi)$ est le terme constant de χ_Ξ, c'est-à-dire $det(\Xi)$. □

Lemme III.1.3. $\forall\, (x, y, z) \in \mathbb{Q}^3$,

$$N(xu+yv+zw) = x^3+y^3+z^3-4(x^2z+y^2x+z^2y)+3(x^2y+y^2z+z^2x)-xyz$$

Démonstration. Cela suit du calcul explicite de l'expression de la norme démontrée dans la propriété précédente **II.3.1.1**. □

Lemme III.1.4. $\forall\, x, y, z \in \mathbb{Z}$ *non tous pairs,* $N(xu + yv + zw)$ *est entier et impair.*

Démonstration. On le vérifie en calculant ce que vaut $N(xu+yv+zw)$ modulo 2 , i.e. dans $\mathbb{F}_2$. En effet,

$$N(xu+yv+zw) \equiv x+y+z+(xy+yz+zx)+xyz \equiv (x-1)(y-1)(z-1)+1\ [2],$$

qui est pair, soit nul dans $\mathbb{F}_2$, si et seulement si $x \equiv y \equiv z\ [2]$, c'est-à-dire x, y et z tous pairs. □

Lemme III.1.5. *$\forall\, x, y, z \in \mathbb{Q}$ non tous nuls,*
$N(xu + yv + zw) \neq 0$ et est le produit d'une puissance (entière) de 8 par une fraction de numérateur et dénominateur impairs.

Démonstration. x, y et z n'étant pas tous nuls,

$$\exists\,(h,p,q) \in \mathbb{Z} \times \mathbb{Z}^3 \times (2\mathbb{Z}+1),\ (x,y,z) = 2^h \frac{p}{q} = \left(2^h \frac{p_1}{q}, 2^h \frac{p_2}{q}, 2^h \frac{p_3}{q}\right)$$

avec p_1, p_2, p_3 non tous pairs. On a alors :

$$N(xu + yv + zw) = 2^{3h} \frac{N(p_1 u + p_2 v + p_3 w)}{q^3}$$

et $N(p_1u+p_2v+p_3w)$ et q^3 sont impairs, respectivement par le lemme précédent **II.3.1.4** et parce que q l'est. □

III.2 Définition d'un corps non commutatif K de dimension 9 sur $\mathbb{Q}$

Définition III.2.1. *La $\mathbb{Q}$-algèbre K est le $\mathbb{Q}$-espace vectoriel* à droite *L^3 muni de la multiplication $\mathbb{Q}$-bilinéaire (notée par . ou juxtaposition) telle que, en notant $(1, a, b)$ sa base usuelle ordonnée :*
- 1 est élément neutre de cette multiplication (faisant ainsi de K une algèbre unitaire) ;
- Elle est associative, L-linéaire par rapport au second argument et vérifie les relations suivantes, $\forall\, \xi \in L$:

$$a^2 = b,\ ab = a^3 = 2 \text{ et } \xi a = a\sigma(\xi).$$

Remarque.
- $\forall\,(\xi,\eta,\zeta),(\xi',\eta',\zeta') \in L^3$,

$$\begin{aligned}(\xi + a\eta + a^2\zeta)(\xi' + a\eta' + a^2\zeta') \quad = \quad & \xi\xi' + 2(\sigma(\zeta)\eta' + \sigma^2(\eta)\zeta') \\ + \quad & a(\eta\xi' + \sigma(\xi)\eta' + 2\sigma^2(\zeta)\zeta') \\ + \quad & a^2(\zeta\xi' + \sigma(\eta)\eta' + \sigma^2(\xi)\zeta')\end{aligned}$$

- $(u, v, w, au, av, aw, a^2u, a^2v, a^2w)$ est alors une $\mathbb{Q}$-base de K, qui étant tridimensionnel sur L, lui-même tridimensionnel sur $\mathbb{Q}$, est de dimension 9 sur $\mathbb{Q}$.

Propriété III.2.1. *L'algèbre K définie ci-dessus est un corps.*

Démonstration. Soit $(\xi, \eta, \zeta) \in L^3$,
Par L-linéarité par rapport au second argument de la multiplication dans K, la multiplication *à gauche* par $\xi + a\eta + a^2\zeta \in K$ est un endomorphisme du L-espace vectoriel K. Montrons alors la non nullité de son déterminant, dès que $\xi + a\eta + a^2\zeta \neq 0$:

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

$\in L$, or $\xi + a\eta + a^2\zeta \neq 0 \Leftrightarrow m := \xi' + a\eta' + a^2\zeta' \neq 0$ où ξ', η', ζ' sont les éléments de L dont les composantes rationnelles en u, v, w sont les numérateurs de celles de ξ, η et ζ respectivement, donc sont entières, et premières entre elles dans leur ensemble en les divisant sans perte de généralité par leur *pgcd* commun. Et cet élément m de K est non nul si et seulement si am ou a^2m l'est, ce qui permet de se ramener au cas plus particulier où ξ a ses composantes non toutes nulles, non toutes paires. On sait alors par le lemme **II.3.1.4** que $N(\xi)$ est un entier impair, le reste de l'expression ci-dessus étant un entier pair puisque σ stabilise $\mathbb{Z}$ (c'est un automorphisme de $\mathbb{Q}$-algèbre) ; le déterminant en question est donc impair et en particulier non nul.
L'endomorphisme considéré est par conséquent bijectif, i.e. $\xi + a\eta + a^2\zeta \neq 0$ inversible à droite, et par suite à gauche comme déjà vu dans la démonstration du théorème **II.1.1.1**. K est bien un corps. □

Propriété III.2.2.
(i) $Z(K) = \mathbb{Q}$ *;*
(ii) Et : $\forall\, x \in K\backslash\mathbb{Q}$, $[\mathbb{Q}_K(x) : \mathbb{Q}] = 3$.

Démonstration. En effet,

(ii) $\forall\, x \in K\backslash\mathbb{Q}$, on a par multiplicativité des degrés :

$$9 = [K : \mathbb{Q}] = [K : \mathbb{Q}_K(x)][\mathbb{Q}_K(x) : \mathbb{Q}];$$

or l'on ne peut avoir ni $[K : \mathbb{Q}_K(x)] = 1$ car $\mathbb{Q}_K(x)$ est commutatif ce que K n'est pas, ni $[\mathbb{Q}_K(x) : \mathbb{Q}] = 1$ car $x \notin \mathbb{Q}$. Donc $[K : \mathbb{Q}_K(x)] = [\mathbb{Q}_K(x) : \mathbb{Q}] = 3$.

(i) Les sous-corps de la forme $\mathbb{Q}_K(x)$ pour $x \in K\backslash\mathbb{Q}$ sont en conséquence sous-corps commutatifs maximaux de K ; tout élément non rationnel de K n'est donc pas dans son centre, car en ce cas on aurait pour un tel x : $\forall\, y \in K\backslash\mathbb{Q}_K(x)$,

$$Z(K)_K(y) = \mathbb{Q}_K(x)_K(y) = \mathbb{Q}_K(x, y) = K$$

par égalité des degrés sur $\mathbb{Q}$, et donc K est commutatif ce qui est absurde. Ainsi $Z(K) = \mathbb{Q}$. □