Fiche de lecture

-

weld

Table des matières

1 Central simple algebras and Galois cohomology

1.1 Basic properties

Definition 1.1.1, Remark 1.1.2

La première k-algèbre des quaternions qui est apparue est une $\mathbb{R}$-algèbre de base $1, i, j, k$ telle que :

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

$$ij = -ji = k$$

D'où on déduit les relations suivantes :

$$ij = k, jk = i, ki = j$$

C'est une algèbre à division ; en effet, chaque élément q de cette algèbre admet une quantité conjuguée qu'on note $\sigma(q)$ telle que :

$$\sigma : (a + bi + cj + dk) \mapsto (a - bi - cj - dk)$$

On définit la norme $N(q)$ comme étant le produit :

$$N(q) = q\sigma(q)$$

Ainsi, tout q différent de 0 admet un inverse multiplicatif $\sigma(q)/N(q)$.

On commence par introduire la notation $k^\times$. Ici, k désigne un corps quelconque des inversibles pour $\times$. La notation $k^{\times 2}$ désigne l'ensemble des carrés du corps k, c'est à dire :

$$k^{\times 2} = \{x^2 \mid x \in k^\times\}$$

En parlant des corps usuels, on a :

$$\mathbb{R}^{\times 2} = \left\{ x^2 \;\middle|\; x \in \mathbb{R}^\times \right\} = \mathbb{R}_+^\times$$

Puisque tout élément q de $\mathbb{Q}$ peut s'écrire comme le produit de nombres premiers, alors :

$$\mathbb{Q} = \left\{ (-1)^\epsilon \prod_p p^{(\nu_p)} \;\middle|\; \epsilon \in \{0,1\}, \nu_p \in \mathbb{Z}, p \in \mathbb{P} \right\}$$

Prenons le temps de définir $\mathbb{Q}^{\times 2}$. Avec la nouvelle notation de $\mathbb{Q}$ introduite à la ligne précédente, on a qu'un carré q de $\mathbb{Q}$ s'écrit :

$$q^2 = \left((-1)^\epsilon \prod_p p^{(\nu_p)} \right)^2 = \prod_p p^{2\nu_p}$$

Alors :

$$\mathbb{Q}^{\times 2} = \left\{ \prod_p p^{2\nu_p} \in \mathbb{Q}^\times \;\middle|\; \nu_p \in \mathbb{Z}, p \in \mathbb{P} \right\}$$

Il nous est à présent possible d'introduire la notation $k^\times/k^{\times 2}$. Il nous faut d'abord rappeler ce qu'est un groupe quotient. Soit G, un groupe et $H \subset G$, un sous-groupe de G. G/H désigne l'ensemble des classes de G suivant H.

$$G/H = \left\{ xH \;\middle|\; x \in G \right\}$$

Donnons également quelques mots sur les relations d'équivalence : soit $x, y \in G$. Si $\bar{x} = \bar{y}$, alors :

$$\bar{x} = \bar{y} \Leftrightarrow x = yH$$

$$\Leftrightarrow xy^{-1} \in H$$

Pour les réels, alors :

$$\mathbb{R}^\times/\mathbb{R}^{\times 2} = \left\{ x\mathbb{R}^{\times 2} \;\middle|\; x \in \mathbb{R}^\times \right\}$$

Ce qui implique que pour tout x, y de $\mathbb{R}^\times$, si $\bar{x} = \bar{y}$ alors $\frac{x}{y} \in \mathbb{R}_+^\times$.

Remarque: On peut montrer que $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Pour s'en rendre compte, on construit le morphisme canonique de $\mathbb{R}^\times$ vers $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ qui à x associe sa classe d'équivalence dans $\mathbb{R}^\times/\mathbb{R}^{\times 2}$. On voit ici que $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ peut se réduire à deux éléments $\{-1, 1\}$ selon que $x < 0$ ou $x > 0$.

Penchons-nous sur le cas des rationnels et la définition de $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Prenons deux éléments x, y de $\mathbb{Q}^\times$. Alors, comme vu précédemment, on peut les écrire :

$$x = (-1)^{\epsilon_x} \prod_p p^{(\nu_{x,p})} \quad (\epsilon_x \in \{0,1\}, \nu_{x,p} \in \mathbb{Z}, p \in \mathbb{P})$$

$$y = (-1)^{\epsilon_y} \prod_p p^{(\nu_{y,p})} \quad (\epsilon_y \in \{0,1\}, \nu_{y,p} \in \mathbb{Z}, p \in \mathbb{P})$$

On a alors :

$$x\mathbb{Q}^{\times 2} = \left\{ (-1)^{\epsilon_x} \prod_p p^{\nu_p} \;\middle|\; \epsilon_x \in \{0,1\},\ \nu_p = \nu_{x,p} \mod 2,\ p \in \mathbb{P} \right\} \text{ et,}$$

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2} = \left\{ x\mathbb{Q}^{\times 2} \;\middle|\; x \in \mathbb{Q}^\times \right\} = \left\{ (-1)^{\epsilon} \prod_p p^{\nu_p} \;\middle|\; \epsilon, \nu_p \in \{0,1\} \right\}$$

De même :

$$\begin{aligned} \bar{x} = \bar{y} &\Leftrightarrow x = y\mathbb{Q}^{\times 2} \\ &\Leftrightarrow \frac{x}{y} \in \mathbb{Q}^{\times 2} \\ &\Leftrightarrow \left[(-1)^{(\epsilon_x - \epsilon_y)} \prod_p p^{(\nu_{x,p} - \nu_{y,p})} \right] \in \mathbb{Q}^{\times 2} \end{aligned}$$

Revenons à la définition **1.1.1**. Pour tout élément a, b de $k^\times$, on peut construire une algèbre de quaternion sur $k^\times$ notée (a, b), de base $1, i, j, ij$ telle que la multiplication soit définie comme :

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

On appelle alors l'ensemble $\{1, i, j, ij\}$ la base quaternionique de (a, b).

S'en suit la remarque **1.1.2** qui nous dit qu'on peut trouver des algèbres de quaternions isomorphes à (a, b) ; ces dernières ne dépendent que des classes d'équivalence de a et de b dans $k^\times/k^{\times 2}$.

Autrement dit, tous les éléments de $k^\times$ qui partagent la même classe d'équivalence dans $k^\times/k^{\times 2}$ engendreront la même algèbre de quaternions. On montre en particulier que (a, b) est isomorphe à (b, a).

C'est en partie de là qu'émerge la richesse de la théorie : on a notamment montré en remarque que $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ se réduisait à l'ensemble $\{-1, 1\}$. C'est-à-dire qu'on ne peut construire que trois algèbres de quaternions différentes sur $\mathbb{R}^\times$:

1. (1,1)
2. (1,-1) isomorphe à (-1,1)
3. (-1,-1)

En anticipant l'exemple **1.1.5**, on finira par montrer que $(1, 1)$ et $(1, -1)$ sont isomorphes à $M_2(\mathbb{R})$ et donc qu'on ne peut finalement construire que deux algèbres de quaternions sur $\mathbb{R}^\times$.

A REVOIR: → Le cas de $\mathbb{Q}^\times$ est différent. Réfléchissons au quotient $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Posons par exemple que si un nombre est un carré parfait, alors sa classe d'équivalence est 1, sinon 0.

Revenons à la définition d'un nombre rationnel comme un produit de nombres premiers. Les "copies" de nombres premiers vont se simplifier entre elles (puisqu'elles formeront alors un carré parfait).

On pourra réduire alors notre rationnel à un produit de nombres premiers uniques qui seront, ou non, un carré. On peut alors renvoyer chacun de ces termes premiers à sa classe d'équivalence et affecter comme cela un rationnel à un ensemble de

coordonnées de $(0, 1, 1, ...)$.

On montre alors qu'avec une telle application, $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. $\leftarrow$

On voit alors qu'on peut construire autant d'algèbres de quaternions différentes sur $\mathbb{Q}^\times$, contrairement au corps $\mathbb{R}^\times$ qui n'en générait que deux.

Norm, Lemma 1.1.3, Remark 1.1.4

Le texte poursuit avec la construction d'une norme sur une k-algèbre de quaternions.

Prenant un élément $q = x + yi + zj + wij$ de (a, b), on définit le nombre conjugué de q comme étant :

$$\bar{q} = x - yi - zj - wij$$

L'application σ qui à un élément de (a, b) associe sa quantité conjuguée réalise un automorphisme dans (a, b). Notons également que $\sigma(\sigma(q)) = q$: autrement dit, l'application σ est involutive.

On peut par ailleurs montrer que σ est la seule application linéaire telle que :

$$\sigma(1) = 1 \text{ et } \sigma(q)q \in k, \ \ \forall q \in (a, b)$$

Preuve: Commençons par vérifier ces propriétés : $\sigma(1) = 1$ est immédiat, par définition.

$$\sigma(q)q = (x - yi - zj - wij)(x + yi + zj + wij) = x^2 - y^2a - z^2b + w^2ab$$

On a donc $\sigma(q)q \in k$, puisque composé de sommes et produits de termes dans k. On cherche à montrer que σ est unique.

Supposons alors qu'il existe une autre application qui vérifie ces propriétés et définissons s une application linéaire de (a, b) dans (a, b). On a trivialement que si $s(1) = 1$, alors $s(1) = \sigma(1)$.

Si $s(q)q \in k$, alors il existe un p dans k tel que :

$$s(q)q = p$$
$$\Leftrightarrow \frac{1}{p}s(q)q = 1$$
$$\Leftrightarrow s(\frac{q}{p})q = 1 \ \text{ (linéarité de } s)$$

Ce qui veut dire que $s(\frac{q}{p})$ est un inverse pour q.

Tâchons de montrer que cet inverse est unique ; on suppose qu'il existe $q_1, q_2 \in (a, b)$ tels que :

$$q_1q = qq_1 = 1 \text{ et } q_2q = qq_2 = 1$$

Alors $q_1 = 1 \times q_1 = (q_2q)q_1 = q_2(qq_1) = q_2 \times 1 = q_2$. On peut en déduire les choses suivantes :

Si $\sigma(q)q = p_\sigma \in k$, alors $\sigma(\frac{q}{p_\sigma})q = 1$. De même, si $s(q)q = p_s \in k$, alors $s(\frac{q}{p_s})q = 1$.

On a démontré plus tôt que tout élément q de (a, b) admettait un unique inverse, d'où on tire l'égalité :

$$s(\frac{q}{p_s}) = \sigma(\frac{q}{p_\sigma})$$

Sachant que l'application σ est involutive et linéaire, on a :

$$\sigma(s(\frac{q}{p_s})) = \sigma(\sigma(\frac{q}{p_\sigma}))$$
$$\Leftrightarrow \frac{q}{p_s} = \frac{q}{p_\sigma}$$
$$\Leftrightarrow \frac{p_\sigma}{p_s}q = q$$

On a ici une disjonction de cas : soit $q = 0$, soit $q \neq 0$.

Si $q = 0$, alors $s(q)q = \sigma(q)q = 0 \in k$. Enfin, si $q \neq 0$, alors :

$$\frac{p_\sigma}{p_s} = 1 \Leftrightarrow p_\sigma = p_s = p \in k$$

Donc, par linéarité des applications σ et s :

$$\begin{aligned} & s(\frac{q}{p})q = \sigma(\frac{q}{p})q \\ \Leftrightarrow & \frac{1}{p}s(q)q = \frac{1}{p}\sigma(q)q \\ \Leftrightarrow & s(q)q = \sigma(q)q \\ \Rightarrow & s(q) = \sigma(q), \ \ \forall q \in (a,b) \end{aligned}$$

Concluant sur le fait que σ soit bien la seule application linéaire respectant ces propriétés.

On peut alors introduire la notion de norme, pour $q = x + yi + zj + wij$ dans (a,b) :

$$N : (a,b) \to k, \ \ q \mapsto (x^2 - y^2a - z^2b + w^2ab) \ \ [1]$$

Note: La norme est une forme quadratique non dégénérée.

On a la propriété suivante :

$$\forall q_1, q_2 \in (a,b), \ \ N(q_1q_2) = q_1q_2\overline{(q_2q_1)} = q_1q_2\bar{q_2}\bar{q_1} = q_1N(q_2)\bar{q_1} = N(q_1)N(q_2)$$

Le lemme **1.1.3** nous dit qu'un élément est inversible si et seulement si sa norme est différente de 0. Cela se comprend bien (voir la preuve plus haut) puisque pour tout q de (a,b), on a :

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

On peut donc dire que (a,b) est une algèbre à division ssi la norme ne s'annule pas pour les éléménts de (a,b) différents de 0.

La remarque **1.1.4** quant à elle généralise les notions de nombre conjugué et de norme, indépendemment des définitions qui usent de la base quaternionique. Pour cela, prenons un élément q de (a,b), une k-algèbre de quaternions. On dit que q est un quaternion pur si et seulement si $q^2 \in k$ et $q \notin k$.

On peut montrer que q est un quaternion pur si, pour $q = x + yi + zj + wij$, $x = 0$. Alors, chaque élément de (a,b) peut s'écrire comme la somme d'un quaternion pur et d'un élément de k. Posons $q = x + q_2$, avec $x \in k$ et $q_2 \in (a,b)$ tel que q_2 pur. On définit alors simplement :

$$\bar{q} = x - q_2$$

Example 1.1.5, Definition 1.1.6, Proposition 1.1.7

L'exemple **1.1.5** est assez explicite. Il permet de montrer qu'il existe un autre type de k-algèbre, isomorphe à $M_2(k)$. On définit l'application suivante :

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

Cette application est un isomorphisme de $(1,b)$ dans $M_2(k)$ puisque ces matrices, leurs compositions et la matrice identité forment une base de $M_2(k)$.

C'est précisément en utilisant cette définition qu'on montre qu'il n'existe en fait que deux $\mathbb{R}$-algèbres de quaternions : $(1,b)$ et $(-1,-1)$.

La définition **1.1.6** introduit le terme d'algèbre déployée. On dit qu'une k-algèbre de quaternions est déployée si elle est isomorphe à $M_2(k)$.

Nous allons nous arrêter un instant sur la proposition **1.1.7**. Elle nécessite pour la comprendre de faire une introduction aux extensions de corps, et plus particulièrement aux extensions quadratiques.

[1] On pressent l'arrivée, pour certaines algèbres, du théorème des quatre carrés

Tout d'abord, parlons de la notation. Soit K, k deux corps, tels que $k \subset K$. On note alors K/k l'extension de corps K de k. On dit que K est une extension simple de k s'il existe un α de K, tel que :

$$K = k(\alpha)$$

Le théorème fondamental de la théorie des corps nous dit qu'on peut représenter les éléments de $k(\alpha)$ par un polynôme de degré $(n-1)$, où n est le degré de K, à coefficients dans k.
(à revoir)
Prenons un exemple pour bien comprendre. Le corps des complexes $\mathbb{C}$ est une extension de $\mathbb{R}$ ($\mathbb{R} \subset \mathbb{C}$). On note alors $\mathbb{C}/\mathbb{R}$. Cette extension est dite simple, puisque :

$$\mathbb{C} = \mathbb{R}(\sqrt{-1} = i)$$

Puisque $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2, alors tout nombre de $\mathbb{R}(i)$ peut s'écrire comme un polynôme de degré au plus $(2-1=)$ 1, à coefficients dans $\mathbb{R}$. Alors on a, pour tout x de $\mathbb{R}(i)$:

$$x = a + bi, \quad (a, b \in \mathbb{R})$$

Et l'on retrouve bien là la notation habituelle d'un nombre complexe. On peut voir aussi que cet exemple répond à la définition d'extension quadratique : on dit qu'une extension K de k est une extension quadratique ssi $k \subset K$ et que K est de dimension 2 en tant que k-espace vectoriel.

On peut aussi munir d'autres corps pour former des extensions quadratiques. Posons d, un entier différent de 1, qui n'est pas un carré. Soit K = $\mathbb{Q}(\sqrt{d})$ une extension quadratique de $\mathbb{Q}$. On peut écrire alors :

$$K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$$

K est donc de degré 2 sur $\mathbb{Q}$. On peut définir également :

$$\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

On a de manière triviale $\mathbb{Z}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{d})$. On définit dans cette extension une opération de conjugaison, c'est-à-dire que pour tout $\alpha = x + y\sqrt{d} \in K$, le conjugué de α est :

$$\bar{\alpha} = x - y\sqrt{d}$$

On définit également deux applications de K () dans $\mathbb{Q}$:

$$\forall \alpha \in K,\ Tr(\alpha) = \alpha + \bar{\alpha} \text{ (trace de } \alpha)$$

$$N(\alpha) = \alpha\bar{\alpha} \text{ (norme de } \alpha)$$

La théorie des corps nous dit que tout élément α de K (une extension quadratique de $\mathbb{Q}$) est une racine d'un polynome de degré 2, à coefficients rationnels :

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha}X + \alpha\bar{\alpha}) = X^2 - Tr(\alpha)X + N(\alpha)$$

Avec ces résultats sommaires sur les extensions quadratiques, nous devrions être capable de comprendre la proposition **1.1.7**. Cette proposition montre l'équivalence entre plusieurs propositions :

(1) L'algèbre de quaternions (a, b) est déployée.

(2) L'algèbre de quaternions (a, b) n'est pas une algèbre à division.

(3) L'application norme $N : (a, b) \to k$ admet un zéro non-trivial.

(4) L'élément b est une norme pour l'extension quadratique $k(\sqrt{a})/k$.

$(1), (2), (3)$ sont relativement simples à comprendre. On peut tenter de résoudre l'exercice 2 assez simplement avec l'équivalence de ces propositions en tête, pour nous en convaincre.

On cherche à montrer qu'une algèbre de quaternions Q est déployée si et seulement si il existe une base (e, f, g, h) telle que la norme N soit définie, pour tout $q = xe + yf + zg + wh$ de Q, par :

$$N : q \mapsto xy - zw$$

Par l'absurde, supposons que Q n'est pas déployée et qu'il existe une base telle que la norme puisse y être définie comme ci-haut. Donc, d'après la proposition **1.1.7**, si Q n'est pas déployée, il n'existe pas de q dans Q ($q \neq 0$), tel que $N(q) = 0$. Or, quand $xy = zw$, on a $N(q) = 0$. Pour s'en convaincre, on prend $q_1 = (0, 1, 1, 0) \in Q$. Le quaternion q_1 est bien différent de zéro, et sa norme vaut :

$$N(q_1) = 0 \times 1 - 1 \times 0 = 0$$

Donc la proposition est absurde, on en déduit que pour toute algèbre de quaternions déployée, et pour tout élément q de Q, il existe une base (e, f, g, h) de Q telle que la norme de $q = xe + yf + zg + wh$ puisse s'écrire comme $N(q) = xy - zw$. [2]

Reste à écrire sur (4)

[2] Si Q est déployée, alors elle est par définition isomorphe à $M_2(k)$. C'est-à-dire, d'après la proposition **1.1.7**, que tous ses éléments n'y sont pas inversibles. Et on retrouve bien là le rapport avec la propriété du déterminant d'une matrice 2×2, où si pour $X \in M_2(k)$, $\det(X) = 0$, alors il n'existe pas de $X^{-1} \in M_2(k)$ tel que $X^{-1}X = XX^{-1} = Id$.