L'algèbre des quaternions

1 Définition

Pour définir l'algèbre des quaternions $\mathbb{H}$, on fixe un $\mathbb{R}$-espace vectoriel de dimension 4 et une base que l'on note $\{1, i, j, k\}$. On définit une application $\mathbb{R}$-bilinéaire $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ pour laquelle 1 est élément neutre, en posant :

$$i^2 = j^2 = k^2 = -1 \quad ; \quad ij = -ji = k \quad ; \quad ik = -ki = -j \quad ; \quad jk = -kj = i \ .$$

Il est facile de vérifier que cette multiplication munit $\mathbb{H}$ d'une structure de $\mathbb{R}$-algèbre associative.

Le sous-espace vectoriel de $\mathbb{H}$ engendré par 1 est noté simplement $\mathbb{R}$; c'est une sous-algèbre. Le sous-espace vectoriel de $\mathbb{H}$ engendré par i, j, k est noté P ; il n'est pas stable par multiplication. Un quaternion de $\mathbb{R}$ est dit *réel* et un quaternion de P est dit *imaginaire pur*. On a évidemment $\mathbb{H} = \mathbb{R} \oplus P$ donc on peut parler de la *partie réelle* et de la *partie imaginaire* d'un quaternion.

L'algèbre $\mathbb{H}$ n'est pas commutative ; son centre noté $Z(\mathbb{H})$ est la sous-algèbre engendrée par 1, c'est-à-dire $Z(\mathbb{H}) = \mathbb{R}$.

Il y a sur $\mathbb{H}$ une *conjugaison* qui est définie ainsi : si $q = a + bi + cj + dk$ alors son conjugué est $\overline{q} = a - bi - cj - dk$. On vérifie aisément que c'est un anti-automorphisme, c'est-à-dire que c'est un automorphisme d'espace vectoriel et que $\overline{q_1 q_2} = \overline{q_2 q_1}$. Dit autrement, la conjugaison est un isomorphisme entre $\mathbb{H}$ et l'algèbre *opposée* à $\mathbb{H}$, c'est-à-dire l'algèbre $\mathbb{H}^\circ$ dans laquelle le produit de deux éléments q_1 et q_2 est par définition $q_2 q_1$ (produit dans $\mathbb{H}$).

Soit un quaternion $q \in \mathbb{H}$. Il est facile de voir que $q \in \mathbb{R}$ ssi $\overline{q} = q$, et $q \in P$ ssi $\overline{q} = -q$. Mais il existe une autre caractérisation des quaternions réels et imaginaires purs, un peu plus surprenante et purement algébrique. Précisément, un simple calcul montre que $q \in \mathbb{R}$ ssi $q^2 \in \mathbb{R}_{\geq 0}$, et $q \in P$ ssi $q^2 \in \mathbb{R}_{\leq 0}$. Notons à ce propos que la relation d'ordre total de $\mathbb{R}$ ne s'étend pas à $\mathbb{H}$. De ce fait, la notation « $q \geq 0$ » est ambigüe et c'est pourquoi nous préférons écrire $q \in \mathbb{R}_{\geq 0}$.

On définit ensuite la norme d'un quaternion $q \in \mathbb{H}$ par $N(q) = q\overline{q}$. On vérifie que si $q = a + bi + cj + dk$ alors $N(q) = a^2 + b^2 + c^2 + d^2$. En particulier $N(q) \in \mathbb{R}$, $N(\overline{q}) = N(q)$, et $N(q) = 0$ si et seulement si $q = 0$. Il s'ensuit que si $q \neq 0$, alors $N(q)^{-1}\overline{q}$ est inverse à gauche et à droite pour q. Donc $\mathbb{H}$ est ce que l'on appelle une *algèbre à division* ou encore parfois un *corps gauche*. On a donc une application multiplicative $N : \mathbb{H} \to \mathbb{R}$ et un morphisme de groupes induit $\mathbb{H}^* \to \mathbb{R}^*$. Le fait que le corps $\mathbb{H}$ soit non commutatif introduit parfois certaines subtilités par rapport à la théorie des corps commutatifs. Nous essaierons de les mettre en lumière au fur et à mesure.

2 Sous-corps de $\mathbb{H}$

2.1 L'équation $X^2 + 1 = 0$

Dans ce qui suit, on notera G le sous-groupe de $\mathbb{H}^*$ formé des quaternions de norme 1. On note que $q^2 = -1$ ssi on a simultanément $q^2 \in \mathbb{R}_{\leq 0}$ et $q \in G$. D'après ce que l'on a dit plus haut, cela veut donc dire que $q \in P \cap G$. L'espace vectoriel euclidien P est de dimension 3 et $P \cap G$ est sa sphère unité. On obtient donc que l'équation $X^2 + 1 = 0$ possède dans $\mathbb{H}$ un ensemble de solutions isomorphe à la sphère S^2. En particulier, on constate que la finitude du nombre de racines d'un polynôme, phénomène classique de la théorie des corps commutatifs, est prise en défaut ici.

2.2 Formes polaires

Tout quaternion non nul peut donc s'écrire $q = tp$ où $t = N(q)$ et $p \in G$. Cette écriture sera appelée la *forme polaire* de q, en analogie avec le cas complexe.

Pour les quaternions non réels, une autre écriture nous sera aussi utile : partant de la décomposition en partie réelle et partie imaginaire $q = r + q'$, on peut considérer la forme polaire de q' et obtenir

$$q = r + tp \quad \text{où} \quad r \in \mathbb{R},\ p \in P \cap G,\ t = N(q - r)\ .$$

2.3 Commutants

Étant donné $q \in \mathbb{H}$, on définit le commutant de q, noté $Z(q)$, comme étant l'ensemble des quaternions $x \in \mathbb{H}$ tels que $qx = xq$. C'est un sous-corps de $\mathbb{H}$ contenant $\mathbb{R}$, que nous allons calculer. Notons K le sous-corps de $\mathbb{H}$ engendré par q, c'est le corps des polynômes en q, qui est monogène donc évidemment commutatif. On a les formules de produit des dimensions d'espaces vectoriels $[\mathbb{H} : \mathbb{R}] = [\mathbb{H} : K]\,[K : \mathbb{R}]$ et $[Z(q) : \mathbb{R}] = [Z(q) : K]\,[K : \mathbb{R}]$. Il s'ensuit que $[K : \mathbb{R}]$ vaut 1 ou 2, puis que $[Z(q) : \mathbb{R}]$ vaut aussi 1, 2 ou 4.

Si $q \in \mathbb{R}$, on a $K = \mathbb{R}$ et $Z(q) = \mathbb{H}$. Sinon, q n'est pas central, donc $Z(q) \neq \mathbb{H}$. On a $[Z(q) : \mathbb{R}] = [K : \mathbb{R}] = 2$. Dans ce cas $Z(q)$ est un corps commutatif isomorphe à $\mathbb{C}$. Si on écrit $q = r + tp$ avec r la partie réelle de q et $t = N(q - r)$, on a $p^2 = -1$ donc on définit un isomorphisme de $\mathbb{R}$-algèbres explicite $f : \mathbb{C} \to Z(q)$ en posant $f(i) = p$.

Notons qu'en particulier, la $\mathbb{R}$-algèbre $\mathbb{H}$ elle-même n'est pas monogène. Ceci est à comparer au fait que toute $\mathbb{R}$-algèbre de dimension finie qui est un corps commutatif est monogène, d'après le théorème de l'élément primitif.

2.4 Structures de $\mathbb{C}$-algèbre sur $\mathbb{H}$

Une structure de $\mathbb{C}$-algèbre sur $\mathbb{H}$ est donnée par un morphisme $f : \mathbb{C} \to \mathbb{H}$. Un tel morphisme est déterminé par l'image de i par f, qui doit être un élément de carré -1. On voit donc que les structures de $\mathbb{C}$-algèbre sur $\mathbb{H}$ sont en bijection avec $P \cap G$.