Introduction à l'arithmétique des algèbres de quaternions

Isabelle Pays
Université de Mons-Hainaut
B-7000 Mons

Jean-Pierre Tignol
Université Catholique de Louvain
B-1348 Louvain-la-Neuve

Les problèmes diophantiens, qui consistent à trouver les solutions en nombres entiers de certaines équations, sont parmi les plus fascinants et les plus anciens des mathématiques, et leur attrait ne s'est pas affaibli au cours des siècles, jusqu'à l'époque actuelle. On peut citer par exemple l'équation $X^2 + Y^2 = Z^2$, dont les Babyloniens connaissaient déjà un grand nombre de solutions, ou la célèbre équation de Fermat $X^n + Y^n = Z^n$, ou la démonstration de la conjecture de Mordell par Faltings en 1983. Certains de ces problèmes, qui concernent plus particulièrement les formes quadratiques binaires, ont donné naissance, entre les mains d'Euler, de Gauss, Kummer et Dedekind, à une partie importante de la théorie algébrique des nombres. Euler avait déjà observé que pour résoudre les équations du type

$$X^2 + Y^2 = n,$$

il y avait avantage à adjoindre à l'anneau des entiers une racine carrée de -1, de manière à factoriser le premier membre :

$$X^2 + Y^2 = (X + \sqrt{-1}\, Y)(X - \sqrt{-1}\, Y),$$

et à transformer le problème initial en un problème de factorisation dans $\mathbb{Z}[i]$:

$$n = (X + \sqrt{-1}\, Y)(X - \sqrt{-1}\, Y).$$

Une solution complète s'obtient alors à partir des propriétés arithmétiques de $\mathbb{Z}[i]$ (voir par exemple [7, Theorem 366]).

En 1886, Rudolf Lipschitz eut l'idée d'utiliser le même genre de procédé pour des formes quadratiques quaternaires ; on peut en effet factoriser par exemple :

$$X^2 + Y^2 + Z^2 + T^2 = (X + iY + jZ + kT)(X - iY - jZ - kT),$$

à condition que les éléments i, j, k satisfassent les relations :

$$i^2 = j^2 = k^2 = -1 \qquad ij = k = -ji.$$

L'anneau $\mathbb{Z}[i, j, k]$ est alors non commutatif ; c'est un sous-anneau de l'algèbre des quaternions découverte par Hamilton en 1843. Un peu plus tard, Adolf Hurwitz montrait que la théorie développée par Lipschitz pouvait se simplifier de manière très significative si l'on admettait parmi les quaternions "entiers" le quaternion $\frac{1+i+j+k}{2}$. Au début du

vingtième siècle, la notion d'anneau d'entiers (ou *ordre*) dans une algèbre non commutative est progressivement dégagée en vue de jouer le même rôle que les anneaux d'entiers dans les corps de nombres. Après être apparue à l'état d'ébauche dans le livre de Dickson [5, Chap.10], cette "arithmétique non commutative" a connu un développement très rapide, aboutissant en une dizaine d'années à un résultat spectaculaire : la classification des algèbres simples sur les corps de nombres par Brauer, Hasse, Noether et Albert, au début des années 30 (voir le livre de Deuring [4, Chap.6]). Depuis, la théorie des ordres a poursuivi sa croissance vigoureuse, trouvant même récemment des applications pratiques dans l'élaboration de réseaux téléphoniques (voir [2]).

Le but de ce travail est de présenter les fondements de "l'arithmétique non commutative", en introduisant la notion d'ordre dans une algèbre de quaternions et les notions qui lui sont associées, telles que discriminant, idéal, quotient. L'objectif qui sert de fil conducteur à cette introduction est de présenter une démonstration du théorème de Lagrange suivant lequel tout entier positif est somme de quatre carrés. Il s'agit en réalité plutôt d'un prétexte pour donner au lecteur une visite guidée des bases d'une théorie qui s'est développée bien au-delà de cette application particulière. Au lecteur qui est pressé de découvrir cette jolie démonstration du théorème de Lagrange et qui risque de s'impatienter en chemin, nous ne pouvons que recommander de consulter l'un des nombreux ouvrages où celle-ci apparaît sous une forme dépouillée, par exemple [3, Chap.1], [7, Theorem 369] ou [12, section 5.7].

Nous avons pris le parti de limiter notre discussion aux ordres des algèbres de quaternions rationnelles, de manière à disposer d'hypothèses qui apportent certaines simplifications sans dénaturer les idées essentielles. Chaque section est suivie de notes qui indiquent certains prolongements des résultats présentés. Nous espérons ainsi faciliter au lecteur l'abord de textes plus avancés, tels que les livres de Reiner [11] ou de Vignéras [13].

Pour limiter les pré-requis autant que possible, nous commençons par une étude algébrique des algèbres de quaternions. La deuxième section introduit la notion d'ordre dans les algèbres de quaternions rationnelles et la troisième celles d'idéaux et de quotients, le principal résultat donnant des indications sur la structure du quotient d'un ordre par l'idéal des multiples d'un nombre premier. Ce résultat est utilisé dans la section suivante pour démontrer le théorème de Lagrange et plus généralement pour montrer que tout entier positif est représenté par la forme norme d'un ordre principal, dans le cas où celle-ci est définie positive.

Ces notes reproduisent, avec un certain nombre de compléments, le texte du cours donné à Locarno en avril 1989 dans le cadre du CERFIM par le second auteur. Celui-ci tient à remercier le CERFIM, et en particulier Remo Moresi, pour son hospitalité, et ses auditeurs pour leur patience et l'intérêt qu'ils ont bien voulu lui témoigner. Georges Elencwajg, David Leep, Pasquale Mammone et Paul Van Praag ont bien voulu nous faire part de leurs commentaires sur une version préliminaire de ce texte ; nous les en remercions vivement.

1 Algèbres de quaternions

1. *Définition :* Soit F un corps commutatif de caractéristique différente de 2 (c'est-à-dire que $1+1 \neq 0$ dans F). On appelle *algèbre de quaternions* sur F toute algèbre (associative) sur F admettant une base de quatre éléments, notés 1, i, j, k, qui satisfont les relations suivantes : 1 est l'élément neutre pour la multiplication, et

$$i^2 = a.1, \quad j^2 = b.1, \quad ij = k = -ji,$$

pour certains éléments non nuls $a, b \in F$. Une telle algèbre est notée $(a,b)_F$. L'élément 1 est généralement omis dans les produits ; en particulier, on note habituellement $f.1 = f$ pour tout $f \in F$, ce qui conduit à identifier F à un sous-corps de $(a,b)_F$.

Bien sûr, un choix arbitraire de produits d'éléments de base ne définit généralement pas une structure d'algèbre associative sur un espace vectoriel ; si par exemple on avait posé : $j^2 = i + b.1$ au lieu de $j^2 = b.1$, les relations conduiraient à une contradiction puisque de $j(j^2 - b.1) = (j^2 - b.1)j$ on déduirait : $ji = ij$ alors que l'on demande par ailleurs $ij = -ji$; il faudrait donc avoir $ij = ji = 0$, d'où $ab.1 = i^2 j^2 = (ij)^2 = 0$, ce qui contredit l'hypothèse que a et b sont non nuls. Pour justifier la définition ci-dessus, et prouver l'existence d'algèbres de quaternions $(a,b)_F$ quels que soient les éléments $a, b \neq 0$, il suffit de considérer dans l'algèbre $M_4(F)$ des matrices carrées d'ordre 4 sur F les matrices suivantes :

$$I \text{ est la matrice unité : } I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\mathcal{I} = \begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 1 & 0 \end{pmatrix}, \mathcal{J} = \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & -b \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \mathcal{K} = \begin{pmatrix} 0 & 0 & 0 & -ab \\ 0 & 0 & b & 0 \\ 0 & -a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Une vérification directe montre que les matrices $I, \mathcal{I}, \mathcal{J}$ et $\mathcal{K}$ satisfont les relations requises ci-dessus de $1, i, j, k$. Ainsi, la sous-algèbre de $M_4(F)$ formée des combinaisons linéaires de $I, \mathcal{I}, \mathcal{J}$ et $\mathcal{K}$ est une algèbre de quaternions $(a,b)_F$.

Voici un exemple où la construction d'une algèbre de quaternions redonne une algèbre bien connue par ailleurs : l'algèbre de quaternions $(1,1)_F$ est isomorphe à l'algèbre $M_2(F)$ des matrices carrées d'ordre 2 sur F. Pour le voir, il suffit de trouver une base 1, i, j, k de $M_2(F)$ dont les éléments satisfont les relations ci-dessus, avec $a = b = 1$. Bien sûr, 1 est la matrice unité :

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

pour i et j, on peut prendre par exemple :

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Vu les relations ci-dessus, on doit prendre alors

$$k = ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Une vérification directe montre que les matrices 1, i, j, k ci-dessus forment bien une base de $M_2(F)$, et qu'elles satisfont les relations :

$$i^2 = 1; \quad j^2 = 1; \quad k = -ji.$$

Dès lors, comme annoncé, $M_2(F) \simeq (1,1)_F$.

2. *Conjugaison, trace et norme :* Le *conjugué* d'un quaternion

$$x = x_0 + x_1 i + x_2 j + x_3 k \in (a,b)_F$$

est le quaternion

$$\overline{x} = x_0 - x_1 i - x_2 j - x_3 k \in (a,b)_F.$$

La conjugaison est donc un opérateur F-linéaire sur l'algèbre $(a,b)_F$, et les quaternions invariants sous cet opérateur sont ceux qui appartiennent à F. Il est clair également que

$$\overline{\overline{x}} = x$$

pour tout $x \in (a,b)_F$. Un calcul direct montre de plus que, pour $x, y \in (a,b)_F$,

$$\overline{x.y} = \overline{y}.\overline{x}.$$

Dès lors, pour tout $x \in (a,b)_F$, les quaternions

$$T(x) = x + \overline{x} \quad \text{et} \quad N(x) = x\overline{x},$$

que l'on appelle respectivement *trace* et *norme* de x, sont des éléments de F. Explicitement, pour $x = x_0 + x_1 i + x_2 j + x_3 k \in (a,b)_F$, on trouve :

$$T(x) = 2x_0 \quad \text{et} \quad N(x) = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2.$$

Les propriétés de la conjugaison entraînent les propriétés suivantes pour la trace et la norme : T est une application F-linéaire de $(a,b)_F$ vers F, c'est-à-dire que

$$T(fx + gy) = fT(x) + gT(y)$$

pour $f, g \in F$ et $x, y \in (a,b)_F$, et

$$N(xy) = N(x)N(y)$$

pour $x, y \in (a,b)_F$.

Considérons, à titre d'exemple, l'algèbre de quaternions $(1,1)_F$, que l'on a identifiée à l'algèbre de matrices $M_2(F)$ à la fin du numéro précédent, par le choix de certaines matrices i, j et k :

$$x_0 + x_1 i + x_2 j + x_3 k = \begin{pmatrix} x_0 + x_1 & x_2 + x_3 \\ x_2 - x_3 & x_0 - x_1 \end{pmatrix},$$

d'où, inversement, toute matrice d'ordre 2 s'identifie à un quaternion de $(1,1)_F$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{a+d}{2} + \frac{a-d}{2} i + \frac{b+c}{2} j + \frac{b-c}{2} k.$$

Sous cette identification, la conjugaison de $(1,1)_F$ correspond à l'opérateur suivant sur $M_2(F)$:

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

de sorte que la trace et la norme sont données par :

$$T\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d \quad \text{et} \quad N\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc.$$

La trace est donc la trace usuelle des matrices d'ordre 2, et la norme est le déterminant. La propriété qu'une matrice est inversible si et seulement si son déterminant est non nul admet un analogue dans les algèbres de quaternions générales :

Proposition 1 *Un quaternion $x \in (a,b)_F$ est inversible si et seulement si sa norme $N(x) \in F$ est non nulle.*

Démonstration: Si $N(x) \neq 0$, alors $N(x)^{-1}\overline{x}$ est l'inverse de x, comme le montre un calcul direct. Réciproquement, si x est inversible, alors de la relation $xx^{-1} = 1$ on déduit :

$$N(x)N(x^{-1}) = N(1) = 1,$$

ce qui montre que $N(x) \neq 0$. ∎

3. *Structure des algèbres de quaternions :* A toute algèbre de quaternions $A = (a,b)_F$ on associe la quadrique Q_A d'équation :

$$Q_A : \ X_0^2 - aX_1^2 - bX_2^2 + abX_3^2 = 0.$$

L'ensemble $Q_A(F)$ des points de cette quadrique dans F^4 est donc l'ensemble des quadruplets $(x_0, x_1, x_2, x_3) \in F^4$ tels que $N(x_0 + x_1 i + x_2 j + x_3 k) = 0$. En identifiant A à F^4 au moyen de la base standard $(1, i, j, k)$, c'est-à-dire en identifiant $x = x_0 + x_1 i + x_2 j + x_3 k \in A$ au quadruplet $(x_0, x_1, x_2, x_3) \in F^4$, on peut donc aussi écrire :

$$Q_A(F) = \{x \in A \mid N(x) = 0\}.$$

La structure de l'algèbre A dépend de la manière suivante de l'ensemble $Q_A(F)$:

Théorème 1 *Si $Q_A(F) = \{0\}$ $(= \{(0,0,0,0)\})$, alors A est une algèbre à division (ou, en d'autres termes, un corps non commutatif) ; si $Q_A(F) \neq \{0\}$, alors A est isomorphe à l'algèbre $M_2(F)$ des matrices carrées d'ordre 2.*

Démonstration: La première affirmation est claire, car si $Q_A(F) = \{0\}$, alors la norme de tout élément non nul de A est non nulle, donc, vu la proposition 1, tout élément non nul de A est inversible. Pour établir la seconde affirmation, nous aurons besoin de quelques résultats préliminaires :

Lemme 1 *$Q_A(F)$ ne contient pas de sous-F-espace vectoriel de dimension strictement supérieure à 2.*

Démonstration: Soit B la forme bilinéaire sur F^4 associée à la quadrique Q_A :

$$B(x,y) = x_0y_0 - ax_1y_1 - bx_2y_2 + abx_3y_3$$

pour $x = (x_0, x_1, x_2, x_3)$ et $y = (y_0, y_1, y_2, y_3)$. (De manière équivalente, en identifiant F^4 à A, on peut définir B comme la forme bilinéaire associée à la forme quadratique N sur A :

$$B(x,y) = \frac{1}{2}[N(x+y) - N(x) - N(y)] = \frac{1}{2}(x\overline{y} + y\overline{x}).)$$

Dire qu'un sous-espace V est contenu dans $Q_A(F)$ revient à dire que la forme quadratique N, donc aussi la forme bilinéaire B, s'annule sur V ; le sous-espace V est alors contenu dans son orthogonal $V^\perp$ pour la forme B, d'où

$$\dim V \leq \dim V^\perp.$$

Or, comme B est non dégénérée, on a

$$\dim V^\perp = \dim A - \dim V;$$

dès lors, si $V \subseteq Q_A(F)$, alors $2 \dim V \leq \dim A = 4$. ∎

Pour achever la démonstration du théorème 1, nous aurons encore besoin du lemme suivant :

Lemme 2 *Pour tout $x \in A$, $x \neq 0$, on peut trouver $y \in A$ tel que $N(xy + yx) \neq 0$.*

Démonstration: Soit $x = x_0 + x_1i + x_2j + x_3k$; un calcul direct donne :

$$xi + ix = 2(x_0i + x_1a),$$

donc $N(xi+ix) = -4a(x_0^2 - ax_1^2)$. Cela prouve que l'on peut choisir $y = i$ si $x_0^2 - ax_1^2 \neq 0$. De même, $N(xj+jx) = -4b(x_0^2 - bx_2^2)$, de sorte que l'on peut choisir $y = j$ si $x_0^2 - bx_2^2 \neq 0$, et on peut choisir $y = k$ si $x_0^2 + abx_3^2 \neq 0$. Le seul cas où l'on n'a pas encore choisi y est donc celui où

$$x_0^2 = ax_1^2 = bx_2^2 = -abx_3^2;$$

mais alors

$$N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 = -2x_0^2,$$

donc $N(x) \neq 0$, sinon les relations précédentes donnent : $x_0 = x_1 = x_2 = x_3 = 0$, d'où $x = 0$, contrairement à l'hypothèse. On peut alors choisir $y = 1$. ∎

Nous pouvons à présent terminer la démonstration du théorème 1. Supposons donc que $Q_A(F) \neq \{0\}$; il s'agit de montrer que A est isomorphe à $M_2(F)$. Considérons pour cela un élément $q \neq 0$ dans $Q_A(F)$, et le sous-espace vectoriel

$$Aq = \{xq \mid x \in A\} \subseteq A.$$

Ce sous-espace est contenu dans $Q_A(F)$, car de $N(q) = 0$ on déduit :

$$N(xq) = N(x)N(q) = 0.$$

La proposition 1 montre alors que $\dim Aq \leq 2$. Considérons encore l'application

$$\lambda : A \to \mathrm{End}_F Aq$$

qui envoie tout élément $x \in A$ sur la multiplication à gauche par x :

$$\begin{aligned} \lambda_x : Aq &\to Aq \\ yq &\mapsto xyq. \end{aligned}$$

L' application λ est un homomorphisme d'algèbres. Dès lors, si x est dans le noyau Ker λ, alors, quel que soit l'élément $y \in A$, on a aussi

$$N(xy + yx) = (xy + yx)\overline{(xy + yx)} \in \text{ Ker } \lambda,$$

puisque

$$\lambda_{N(xy+yx)} = (\lambda_x \lambda_y + \lambda_y \lambda_x)\lambda_{\overline{(xy+yx)}},$$

et que le second membre est nul si $\lambda_x = 0$. Si $x \neq 0$, on peut, d'après le lemme précédent, trouver $y \in A$ tel que $N(xy+yx) \neq 0$; alors le noyau de λ contient un élément non nul de F, ce qui est impossible. Cette contradiction montre que l'homomorphisme λ est injectif ; par conséquent,

$$\dim A \leq \dim \mathrm{End}_F(Aq).$$

Par ailleurs, comme $\dim Aq \leq 2$, on a

$$\dim \mathrm{End}_F(Aq) \leq 4 = \dim A;$$

dès lors, $\dim \mathrm{End}_F(Aq) = \dim A$. Cela entraîne que $\dim Aq = 2$ et que λ est un isomorphisme :

$$A \simeq \mathrm{End}_F(Aq).$$

Comme le choix d'une base de Aq permet d'établir un isomorphisme entre $\mathrm{End}_F(Aq)$ et $M_2(F)$, le théorème est démontré. ∎

4. *Corps de base particuliers :* L'exemple classique d'une algèbre de quaternions à division est dû à Hamilton (1843) : c'est $(-1,-1)_{\mathbb{R}}$. Il s'agit bien d'une algèbre à division, d'après le théorème 1, puisque la quadrique correspondante

$$X_0^2 + X_1^2 + X_2^2 + X_3^2 = 0$$

n'a pas de point non nul dans $\mathbb{R}^4$. Il n'est pas difficile de voir que toute algèbre de quaternions sur $\mathbb{R}$ est isomorphe soit à $(-1,-1)_{\mathbb{R}}$, soit à $M_2(\mathbb{R})$; en effet, si $a > 0$ ou $b > 0$, alors la quadrique

$$X_0^2 - aX_1^2 - bX_2^2 + abX_3^2 = 0$$

admet des points non nuls dans $\mathbb{R}^4$, et l'algèbre $(a,b)_{\mathbb{R}}$ est donc isomorphe à $M_2(\mathbb{R})$. Par ailleurs, si $a < 0$ et $b < 0$, alors les éléments $i' = \sqrt{-a}\, i$, $j' = \sqrt{-b}\, j$ et $k' = \sqrt{ab}\, k$ de $(a,b)_{\mathbb{R}}$ satisfont :

$$i'^2 = j'^2 = k'^2 = -1 \quad \text{et} \quad i'j' = k' = -j'i',$$

donc $(1, i', j', k')$ est base d'une algèbre de quaternions $(-1,-1)_{\mathbb{R}}$. Par conséquent,

$$\begin{array}{lcll}(a,b)_{\mathbb{R}} & \simeq & M_2(\mathbb{R}) & \text{si } a>0 \text{ ou } b>0\\ (a,b)_{\mathbb{R}} & \simeq & (-1,-1)_{\mathbb{R}} & \text{si } a<0 \text{ et } b<0.\end{array}$$

Le théorème 1 permet aussi de voir que, pour certains choix du corps de base F, toute algèbre de quaternions $(a,b)_F$ est isomorphe à $M_2(F)$:

Corollaire 1 *Toute algèbre de quaternions sur le corps $\mathbb{C}$ des nombres complexes ou sur un corps fini est isomorphe à l'algèbre des matrices carrées d'ordre 2.*

Démonstration: Quels que soient les nombres complexes a, b non nuls, la quadrique

$$X_0^2 - aX_1^2 - bX_2^2 + abX_3^2 = 0$$

possède des points non nuls dans $\mathbb{C}^4$ (par exemple $(\sqrt{a}, 1, 0, 0)$) ; on en déduit, par le théorème 1, que toute algèbre de quaternions $(a,b)_{\mathbb{C}}$ est isomorphe à $M_2(\mathbb{C})$.

Le principe de la démonstration est le même pour les corps finis. Soit $\mathbb{F}_q$ le corps fini à q éléments (avec q impair, puisque la caractéristique est toujours supposée différente de 2) ; il s'agit de prouver que pour $a, b \in \mathbb{F}_q^\times$ $(= \mathbb{F}_q \smallsetminus \{0\})$, la quadrique

$$X_0^2 - aX_1^2 - bX_2^2 + abX_3^2 = 0$$

possède des points non nuls dans $\mathbb{F}_q^4$. Commençons par compter le nombre de carrés de $\mathbb{F}_q$: l'ensemble des carrés non nuls est l'image de l'homomorphisme d'élévation au carré :

$$\begin{array}{rcl}\mathbb{F}_q^\times & \to & \mathbb{F}_q^\times\\ x & \mapsto & x^2.\end{array}$$

Comme le noyau de cet homomorphisme compte deux éléments (à savoir $+1$ et -1), le nombre d'éléments de l'image est la moitié du nombre d'éléments de $\mathbb{F}_q^\times$; il y a donc $\frac{q-1}{2}$ carrés non nuls dans $\mathbb{F}_q$. En ajoutant 0, on trouve $\frac{q+1}{2}$ carrés au total. Le nombre d'éléments de chacun des ensembles

$$\{x_0^2 - a \mid x_0 \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \quad \text{et} \quad \{bx_2^2 \mid x_2 \in \mathbb{F}_q\} \subseteq \mathbb{F}_q$$

est donc $\frac{q+1}{2}$. Dès lors, ces ensembles ne peuvent pas être disjoints, et l'on peut trouver $x_0, x_2 \in \mathbb{F}_q$ tels que

$$x_0^2 - a = bx_2^2.$$

Le point $(x_0, 1, x_2, 0)$ est alors sur la quadrique. ∎

Sur le corps $\mathbb{Q}$ des nombres rationnels (qui nous occupera particulièrement dans la suite), il est clair qu'il existe des algèbres de quaternions à division ; en effet, puisque la quadrique

$$X_0^2 + X_1^2 + X_2^2 + X_3^2 = 0$$

n'a pas de point non nul dans $\mathbb{R}^4$, elle n'en a pas non plus dans $\mathbb{Q}^4$, donc l'algèbre $(-1,-1)_{\mathbb{Q}}$ est à division. Il convient de remarquer que le raisonnement par lequel on a prouvé ci-dessus que toute algèbre de quaternions sur $\mathbb{R}$ est isomorphe à $M_2(\mathbb{R})$ ou à $(-1,-1)_{\mathbb{R}}$ ne s'applique pas sur $\mathbb{Q}$, car les nombres rationnels positifs ne sont pas tous des carrés. On peut d'ailleurs montrer qu'il y a des nombres rationnels $a, b > 0$ tels que l'algèbre $(a,b)_{\mathbb{Q}}$ soit à division. La classification des algèbres de quaternions sur $\mathbb{Q}$ est beaucoup plus malaisée que sur $\mathbb{R}$; on verra plus loin que les classes d'isomorphie d'algèbres de quaternions sur $\mathbb{Q}$ sont en correspondance bi-univoque avec les nombres rationnels positifs qui sont produits de nombres premiers deux à deux distincts. (Voir les notes de la section 2).

5. *Notes :* Les relations entre l'algèbre de quaternions A et la quadrique Q_A se prolongent bien au-delà de ce que l'on a fait voir ci-dessus. On pourra s'amuser à prouver, à titre d'exercice, que la quadrique Q_A, considérée comme quadrique projective dans l'espace projectif à trois dimensions, est doublement réglée, les droites passant par un point q étant les idéaux à gauche et à droite Aq et qA. (Voir aussi l'article de Witt [14]).

Pour plus de détails sur les algèbres de quaternions, on consultera avec profit le premier chapitre du livre de Blanchard [3], où l'on trouvera également une extension de la définition des algèbres de quaternions aux corps de caractéristique 2, ou le premier chapitre du livre de Vignéras [13]. Pour les relations avec la théorie algébrique des formes quadratiques, le livre de Lam [8] (en particulier le chapitre 3) est une excellente référence.

Le raisonnement utilisé dans la démonstration du théorème 1 pour prouver l'injectivité de l'homomorphisme λ montre plus généralement que les algèbres de quaternions ne contiennent pas d'idéal bilatère non trivial : on dit que ces algèbres sont *simples*. Le théorème 1 est un cas très particulier d'un théorème de structure pour les algèbres simples de dimension finie, dû à J.H.M. Wedderburn, suivant lequel ces algèbres sont isomorphes à une algèbre de la forme $M_n(D)$, où D est une algèbre à division. Pour la théorie générale des algèbres simples, on peut consulter, outre le livre de Blanchard [3] déjà cité, le chapitre 12 du livre de Pierce [10], le livre de Draxl [6] ou les références classiques : Albert [1] ou Deuring [4].

2 Ordres dans les algèbres de quaternions

Dans cette section, A désigne une algèbre de quaternions (à division ou non) sur le corps $\mathbb{Q}$ des nombres rationnels.

1. *Définition :* Un *ordre* de A (sur $\mathbb{Z}$) est un sous-anneau Λ de A, de la forme :

$$\Lambda = \{a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 \mid a_1 \ldots, a_4 \in \mathbb{Z}\},$$

où (e_1, e_2, e_3, e_4) est une base de A sur $\mathbb{Q}$.

Ainsi, si (e_1, e_2, e_3, e_4) est une base de A sur $\mathbb{Q}$, l'ensemble des combinaisons linéaires à coefficients entiers : $\Lambda = \{a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$ est un ordre de A si et seulement si cet ensemble est un anneau ; il suffit évidemment de vérifier que les produits d'éléments de base e_ie_j appartiennent à Λ, et que l'unité $1 \in A$ est dans Λ.

Par exemple, si $(1, i, j, k)$ est la base standard de l'algèbre de quaternions $A = (a, b)_{\mathbb{Q}}$, et si α, β sont des entiers tels que $\alpha^2 a \in \mathbb{Z}$ et $\beta^2 b \in \mathbb{Z}$, alors l'ensemble des combinaisons linéaires à coefficients entiers de $1, \alpha i, \beta j, \alpha\beta k$ est un ordre de A, comme on le vérifie aisément.

Il est clair que la base (e_1, e_2, e_3, e_4) dont il est question dans la définition n'est pas déterminée de manière unique par Λ, mais il n'est pas difficile de trouver une condition pour que deux bases définissent le même ordre. Si (f_1, f_2, f_3, f_4) est une autre base de A, alors on peut former la matrice de changement de base $(a_{ij})_{1 \leq i,j \leq 4} \in M_4(\mathbb{Q})$, définie par les relations :

$$f_j = \sum_{i=1}^{4} e_i a_{ij} \quad \text{pour } j = 1, \ldots, 4.$$

Pour que le $\mathbb{Z}$-module $\{a_1f_1 + \cdots + a_4f_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$ soit contenu dans Λ, il faut et il suffit que chacun des éléments de base f_i soit dans Λ, ce qui revient à : $a_{ij} \in \mathbb{Z}$

pour $i, j = 1, \ldots, 4$, ou : $(a_{ij})_{1 \leq i,j \leq 4} \in M_4(\mathbb{Z})$. De même, comme l'expression de $e_1, \ldots, e_4$ comme combinaisons linéaires de $f_1, \ldots, f_4$ s'obtient à l'aide de la matrice inverse de (a_{ij}), l'inclusion réciproque

$$\Lambda \subseteq \{a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

est équivalente à la condition que la matrice inverse de (a_{ij}) soit dans $M_4(\mathbb{Z})$. Par conséquent, (f_1, f_2, f_3, f_4) est une autre base de A telle que

$$\Lambda = \{a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

si et seulement si la matrice de passage (a_{ij}) de la base (e_1, e_2, e_3, e_4) à la base (f_1, f_2, f_3, f_4) est dans $\mathrm{GL}_4(\mathbb{Z})$, le groupe multiplicatif des matrices de $M_4(\mathbb{Z})$ qui sont inversibles (dans $M_4(\mathbb{Z})$).

On se propose de montrer pour commencer que l'on peut toujours supposer, quitte à changer de base, que l'unité $1 \in A$ est un des éléments de base, disons $e_1 = 1$.

Lemme 3 *Si Λ est un ordre de A (sur $\mathbb{Z}$), alors $\Lambda \cap \mathbb{Q} = \mathbb{Z}$ et*

$$\Lambda = \{a_1 1 + a_2 f_2 + a_3 f_3 + a_4 f_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

pour certains éléments $f_2, f_3, f_4 \in A$ tels que $(1, f_2, f_3, f_4)$ soit une base de A sur $\mathbb{Q}$.

Démonstration: Puisque Λ est un module sur $\mathbb{Z}$ contenant 1, il contient $\mathbb{Z}$; l'inclusion $\mathbb{Z} \subseteq \Lambda \cap \mathbb{Q}$ est donc claire. Pour démontrer l'inclusion réciproque, on écrit

$$\Lambda = \{a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \mid a_1 \ldots, a_4 \in \mathbb{Z}\}$$

pour une certaine base (e_1, e_2, e_3, e_4) de A sur $\mathbb{Q}$, et on considère un élément $u \in \Lambda \cap \mathbb{Q}$. Soit $u = \frac{a}{b}$ avec $a, b \in \mathbb{Z}$, $b \neq 0$. Quitte à diviser a et b par leur plus grand commun diviseur, on peut supposer que a et b sont premiers entre eux. Il s'agit de prouver que $u \in \mathbb{Z}$, c'est-à-dire que $b = \pm 1$. C'est clair si $u = 0$; on peut donc supposer de plus $a \neq 0$. Comme $u \in \Lambda$, on a :

$$\frac{a}{b} = a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4$$

pour certains $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. Puisque Λ est un anneau contenant u, il contient aussi toutes les puissances de u, donc $(\frac{a}{b})^n \in \Lambda$ pour tout entier $n > 0$. Or, en multipliant par $(\frac{a}{b})^{n-1}$ les deux membres de l'égalité précédente, on trouve :

$$\left(\frac{a}{b}\right)^n = \frac{a^{n-1}a_1}{b^{n-1}} e_1 + \frac{a^{n-1}a_2}{b^{n-1}} e_2 + \frac{a^{n-1}a_3}{b^{n-1}} e_3 + \frac{a^{n-1}a_4}{b^{n-1}} e_4.$$

D'après la définition de Λ, une combinaison linéaire de (e_1, e_2, e_3, e_4) ne peut être contenue dans Λ que si tous ses coefficients sont dans $\mathbb{Z}$; dès lors,

$$b^{n-1} \text{ divise } a^{n-1}a_i \text{ pour } i = 1, \ldots, 4 \text{ et pour tout } n > 0.$$

Comme b et a sont premiers entre eux, il en est de même de b^{n-1} et a^{n-1}, donc la relation précédente donne :

$$b^{n-1} \text{ divise } a_i \text{ pour } i = 1, \ldots, 4 \text{ et pour tout } n > 0.$$

Or, il y a au moins un des a_i qui est non nul, puisque $u \neq 0$; cette dernière relation n'est donc possible que si $b = \pm 1$, ce qui démontre la première partie de l'énoncé.

Pour démontrer la seconde partie, on commence par écrire

$$1 = c_1 e_1 + c_2 e_2 + c_3 e_3 + c_4 e_4$$

pour certains $c_1, c_2, c_3, c_4 \in \mathbb{Z}$. Ces entiers sont premiers entre eux, car s'ils admettaient un commun diviseur $d \neq \pm 1$, alors en divisant par d les deux membres de l'égalité précédente, on obtiendrait : $\frac{1}{d} \in \Lambda$, contrairement à la partie de l'énoncé déjà démontrée. Comme c_1, c_2, c_3, c_4 sont premiers entre eux, on peut, d'après le "théorème de Bezout", trouver des entiers d_1, d_2, d_3, d_4 tels que

$$c_1 d_1 + c_2 d_2 + c_3 d_3 + c_4 d_4 = 1.$$

Considérons alors l'application $\phi : \Lambda \to \mathbb{Z}$ définie par :

$$\phi(a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4) = a_1 d_1 + a_2 d_2 + a_3 d_3 + a_4 d_4.$$

Comme cette application est $\mathbb{Z}$-linéaire, son noyau est un sous-module de Λ. De plus, comme $\phi(1) = 1$, un calcul direct montre que pour tout $\lambda \in \Lambda$ on a

$$\lambda - \phi(\lambda).1 \in \text{ Ker } \phi.$$

Dès lors, l'égalité :

$$\lambda = \phi(\lambda).1 + (\lambda - \phi(\lambda).1)$$

montre que tout élément de Λ se décompose en somme d'un élément de $\mathbb{Z}$ et d'un élément de Ker ϕ. Cette décomposition est unique, car si

$$a.1 + \kappa = a'.1 + \kappa'$$

avec $a, a' \in \mathbb{Z}$ et $\kappa, \kappa' \in$ Ker ϕ, alors, en appliquant ϕ aux deux membres de cette égalité on obtient : $a = a'$, et l'on en déduit immédiatement en revenant à l'égalité précédente : $\kappa = \kappa'$.

Les arguments précédents montrent que

$$\Lambda = \mathbb{Z}.1 \oplus \text{ Ker } \phi.$$

Dès lors, si (f_2, f_3, f_4) est une base de Ker ϕ (comme module sur $\mathbb{Z}$), alors $(1, f_2, f_3, f_4)$ est une base de Λ et la démonstration est achevée. ■

Proposition 2 *Tout ordre Λ est stable par conjugaison : $\Lambda = \overline{\Lambda}$; de plus, la trace et la norme de tout élément d'un ordre sont entiers : pour tout $\lambda \in \Lambda$, $T(\lambda) \in \mathbb{Z}$ et $N(\lambda) \in \mathbb{Z}$.*

Démonstration: D'après le lemme, on peut écrire :

$$\Lambda = \{a_1 1 + a_2 f_2 + a_3 f_3 + a_4 f_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

pour certains éléments $f_2, f_3, f_4 \in A$ tels que $(1, f_2, f_3, f_4)$ soit une base de A sur $\mathbb{Q}$. Comme $f_2 \in \Lambda$ et que Λ est un anneau, on doit avoir : $f_2^2 \in \Lambda$, donc les coordonnées de

f_2^2 par rapport à la base $(1, f_2, f_3, f_4)$ doivent être dans $\mathbb{Z}$. Or, f_2 est évidemment racine du polynôme

$$(X - f_2)(X - \overline{f_2}) = X^2 - T(f_2)X + N(f_2),$$

donc

$$f_2^2 = -N(f_2).1 + T(f_2).f_2;$$

par conséquent, $T(f_2)$ et $N(f_2)$ sont entiers. L'égalité :

$$\overline{f_2} = T(f_2) - f_2$$

montre alors que $\overline{f_2} \in \Lambda$, car Λ contient $\mathbb{Z}$ et f_2. Le même raisonnement montre que $\overline{f_i} \in \Lambda$ pour $i = 3, 4$. Si maintenant λ est un élément quelconque de Λ, soit

$$\lambda = a_1 1 + a_2 f_2 + a_3 f_3 + a_4 f_4,$$

alors

$$\overline{\lambda} = a_1 1 + a_2 \overline{f_2} + a_3 \overline{f_3} + a_4 \overline{f_4}$$

et comme Λ est un $\mathbb{Z}$-module contenant 1 et $\overline{f_i}$ pour $i = 2, 3, 4$, on voit que $\overline{\lambda} \in \Lambda$. Cela prouve : $\overline{\Lambda} \subseteq \Lambda$. En conjugant les deux membres de cette relation, on trouve :

$$\Lambda = \overline{\overline{\Lambda}} \subseteq \overline{\Lambda},$$

donc $\Lambda = \overline{\Lambda}$.

Pour tout élément $\lambda \in \Lambda$, la trace $T(\lambda) = \lambda + \overline{\lambda}$ (resp. la norme $N(\lambda) = \lambda\overline{\lambda}$) est alors somme (resp. produit) de deux éléments de Λ, donc $T(\lambda)$, $N(\lambda) \in \Lambda$. Comme de plus ces éléments sont dans $\mathbb{Q}$, on déduit du lemme 3 :

$$T(\lambda), N(\lambda) \in \mathbb{Z}.$$

■

2. *Discriminant d'un ordre :* Le discriminant d'une base (e_1, e_2, e_3, e_4) de A sur $\mathbb{Q}$ est le déterminant de la matrice des traces des produits deux à deux des éléments de base :

$$\mathrm{disc}(e_1, e_2, e_3, e_4) = \mathrm{dét}(T(e_i e_j)_{1 \leq i,j \leq 4}) \in \mathbb{Q}.$$

Par exemple, pour la base standard $(1, i, j, k)$ d'une algèbre de quaternions $(a, b)_{\mathbb{Q}}$, on trouve :

$$\mathrm{disc}(1, i, j, k) = \mathrm{dét} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & -2ab \end{pmatrix} = -2^4 a^2 b^2.$$

Si deux bases (e_1, e_2, e_3, e_4) et (f_1, f_2, f_3, f_4) sont liées par les relations :

$$f_i = \sum_{k=1}^{4} e_k a_{ki}, \quad \text{pour } i = 1, \ldots, 4,$$

alors

$$T(f_i f_j) = \sum_{k,\ell=1}^{4} a_{ki} T(e_k e_\ell) a_{\ell j},$$

donc

$$(T(f_i f_j))_{1\leq i,j\leq 4} = \mathcal{A}^t (T(e_k e_\ell))_{1\leq k,\ell\leq 4} \mathcal{A},$$

où $\mathcal{A} = (a_{ij})_{1\leq i,j\leq 4}$ est la matrice de changement de base. En prenant le déterminant des deux membres, on obtient la relation suivante entre les discriminants des bases (e_1, e_2, e_3, e_4) et (f_1, f_2, f_3, f_4) :

$$\mathrm{disc}(f_1, \ldots, f_4) = \mathrm{disc}(e_1, \ldots, e_4)(\text{dét } \mathcal{A})^2.$$

Si (e_1, e_2, e_3, e_4) est une base d'un ordre Λ de A (sur $\mathbb{Z}$), c'est-à-dire si l'ensemble

$$\Lambda = \{a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

est un ordre de A, alors $e_i e_j \in \Lambda$ pour $i, j = 1, \ldots, 4$ et la proposition précédente montre que $T(e_i e_j) \in \mathbb{Z}$ pour $i, j = 1, \ldots, 4$. Par conséquent,

$$\mathrm{disc}(e_1, \ldots, e_4) \in \mathbb{Z}.$$

Si (f_1, f_2, f_3, f_4) est une autre base du même ordre, alors, d'après ce qui a été dit au début de cette section, la matrice $\mathcal{A}$ de changement de base est une matrice de $\mathrm{GL}_4(\mathbb{Z})$, donc dét $\mathcal{A}$ est un élément inversible de $\mathbb{Z}$:

$$\text{dét } \mathcal{A} = \pm 1.$$

Il en résulte que $\mathrm{disc}(e_1, \ldots, e_4) = \mathrm{disc}(f_1, \ldots, f_4)$. On peut donc définir sans ambiguïté le *discriminant* de l'ordre Λ comme le discriminant de l'une quelconque de ses bases :

$$\mathrm{disc}\ \Lambda = \mathrm{disc}(e_1, \ldots, e_4) \in \mathbb{Z}.$$

Proposition 3 *Le discriminant d'un ordre est l'opposé du carré d'un nombre entier :*

$$\mathrm{disc}\ \Lambda = -r^2$$

pour un certain $r \in \mathbb{N}$.

Démonstration: Soit $A = (a, b)_{\mathbb{Q}}$, de base standard $(1, i, j, k)$, et soit (e_1, e_2, e_3, e_4) une base de A telle que

$$\Lambda = \{a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}.$$

D'après ce qui précède, on a :

$$\mathrm{disc}\ \Lambda = \mathrm{disc}(e_1, \ldots, e_4) = \mathrm{disc}(1, i, j, k)(\text{dét } \mathcal{A})^2 = -2^4 a^2 b^2 (\text{dét } \mathcal{A})^2,$$

où $\mathcal{A}$ est la matrice de passage de la base $(1, i, j, k)$ à la base $(e_1, \ldots, e_4)$. Par conséquent, $\mathrm{disc}\ \Lambda = -r^2$ pour $r = 2^2 ab(\text{dét } \mathcal{A}) \in \mathbb{Q}$. Comme $\mathrm{disc}\ \Lambda \in \mathbb{Z}$, on doit avoir $r \in \mathbb{Z}$. ∎

Etant donné la relation directe qui existe entre le discriminant $\mathrm{disc}\ \Lambda$ et l'entier positif r, on préfère habituellement utiliser ce dernier, que l'on appelle *discriminant réduit* de Λ, et que l'on note $d(\Lambda)$. On a donc, par définition :

$$\mathrm{disc}\ \Lambda = -d(\Lambda)^2.$$

Proposition 4 *Soient Λ et Λ' deux ordres de A. Si $\Lambda \supseteq \Lambda'$, alors $d(\Lambda)$ divise $d(\Lambda')$. De plus, si $\Lambda \supseteq \Lambda'$ et $d(\Lambda) = d(\Lambda')$, alors $\Lambda = \Lambda'$.*

Démonstration: Soient $(e_1, \ldots, e_4)$ et $(e'_1, \ldots, e'_4)$ des bases de A sur $\mathbb{Q}$ telles que

$$\Lambda = \{a_1 e_1 + \cdots + a_4 e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

et

$$\Lambda' = \{a_1 e'_1 + \cdots + a_4 e'_4 \mid a_1 \ldots, a_4 \in \mathbb{Z}\}.$$

Si $\Lambda \supseteq \Lambda'$, alors les éléments de la base $(e'_1, \ldots, e'_4)$ sont combinaisons linéaires à coefficients entiers de $(e_1, \ldots, e_4)$: soit

$$e'_i = \sum_{k=1}^{4} e_k a_{ki} \qquad \text{pour } i = 1, \ldots, 4,$$

avec $a_{ki} \in \mathbb{Z}$ pour $k, i = 1, \ldots, 4$. Comme précédemment, on a :

$$\operatorname{disc}(e'_1, \ldots, e'_4) = \operatorname{disc}(e_1, \ldots, e_4)(\text{dét } \mathcal{A})^2,$$

où $\mathcal{A} = (a_{ij})_{1 \leq i,j \leq 4} \in M_4(\mathbb{Z})$, c'est-à-dire :

$$-d(\Lambda')^2 = -d(\Lambda)^2(\text{dét } \mathcal{A})^2.$$

Comme les éléments de la matrice $\mathcal{A}$ sont entiers, il en est de même du déterminant dét $\mathcal{A}$, et la relation ci-dessus montre que $d(\Lambda)$ divise $d(\Lambda')$.

Si $d(\Lambda) = d(\Lambda')$, alors dét $\mathcal{A} = \pm 1$, par conséquent $\mathcal{A}$ est inversible dans $M_4(\mathbb{Z})$. A l'aide de l'inverse de $\mathcal{A}$, on peut exprimer $e_1, \ldots, e_4$ comme combinaisons linéaires à coefficients entiers de $e'_1, \ldots, e'_4$, d'où $\Lambda \subseteq \Lambda'$. Comme on avait supposé $\Lambda \supseteq \Lambda'$, on a bien $\Lambda = \Lambda'$. ∎

Comme tout nombre entier a un nombre fini de diviseurs, la proposition précédente montre qu'il est impossible de former une suite d'ordres strictement croissante infinie :

$$\Lambda_1 \subsetneq \Lambda_2 \subsetneq \cdots \subsetneq \Lambda_n \subsetneq \cdots$$

Dès lors, tout ordre est contenu dans un ordre *maximal*, c'est-à-dire un ordre qui n'est pas contenu strictement dans un autre.

3. *Exemples :* **a)** Dans l'algèbre $A = M_2(\mathbb{Q})$, que l'on peut considérer comme une algèbre de quaternions, comme on l'a vu au numéro 1 de la section 1, il est clair que l'anneau $\Lambda = M_2(\mathbb{Z})$ est un ordre. Un calcul direct, en prenant par exemple comme base de Λ sur $\mathbb{Z}$ la suite

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

montre que $\operatorname{disc}(\Lambda) = -1$, donc $d(\Lambda) = 1$. Il en résulte que Λ est un ordre maximal de A, car s'il était contenu proprement dans un autre ordre Λ', le discriminant réduit $d(\Lambda')$ devrait être un diviseur propre de $d(\Lambda)$, ce qui est impossible.

b) Soit à présent $A = (-1,-1)_{\mathbb{Q}}$, et soit

$$\Lambda = \{a_1 1 + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\},$$

où $(1, i, j, k)$ est la base standard de A. Une vérification directe montre que Λ est un ordre de A. Comme $\mathrm{disc}(1, i, j, k) = -16$, on a $d(\Lambda) = 4$.

Pour déterminer si cet ordre est maximal, supposons avoir trouvé un ordre $\Lambda' \supsetneq \Lambda$ et soit

$$a = a_1 1 + a_2 i + a_3 j + a_4 k \in \Lambda' \quad (a_1, \ldots, a_4 \in \mathbb{Q}).$$

D'après la proposition 2, on doit avoir $T(a) \in \mathbb{Z}$ et $N(a) \in \mathbb{Z}$, donc :

$$2a_1 \in \mathbb{Z} \qquad \text{et} \qquad a_1^2 + a_2^2 + a_3^2 + a_4^2 \in \mathbb{Z}. \tag{1}$$

De plus, puisque Λ' contient Λ, il contient i, j, k, donc aussi ai, aj et ak. Dès lors, on doit avoir $T(ai) \in \mathbb{Z}$, $T(aj) \in \mathbb{Z}$ et $T(ak) \in \mathbb{Z}$, ce qui donne :

$$-2a_2 \in \mathbb{Z}, \quad -2a_3 \in \mathbb{Z} \quad \text{et} \quad -2a_4 \in \mathbb{Z}.$$

On peut donc poser $a_i = \frac{\alpha_i}{2}$ pour un certain entier α_i $(i = 1, \ldots, 4)$. La condition (1) impose de plus :

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 \in 4\mathbb{Z},$$

ce qui entraîne que $\alpha_1, \ldots, \alpha_4$ sont soit tous quatre pairs, soit tous quatre impairs. Dans le premier cas, $a \in \Lambda$; dans le second, on trouve en posant $\alpha_i = 1 + 2\lambda_i$ pour $i = 1, \ldots, 4$:

$$a = \frac{1}{2}(1 + i + j + k) + \lambda$$

où $\lambda = \lambda_1 1 + \lambda_2 i + \lambda_3 j + \lambda_4 k \in \Lambda$. Ces calculs suggèrent que l'on peut ajouter à Λ l'élément $\varepsilon = \frac{1}{2}(1 + i + j + k)$; en tous cas, ils montrent que si Λ' est un ordre contenant Λ, alors

$$\Lambda' \subseteq \{b_1\varepsilon + b_2 i + b_3 j + b_4 k \mid b_1, \ldots, b_4 \in \mathbb{Z}\},$$

car les éléments $a \in \Lambda'$ trouvés ci-dessus sont soit de la forme

$$a = a_1 1 + a_2 i + a_3 j + a_4 k \qquad \text{avec } a_1, \ldots, a_4 \in \mathbb{Z}$$

(c'est-à-dire $a \in \Lambda$), et alors $a = 2a_1\varepsilon + (a_2 - a_1)i + (a_3 - a_1)j + (a_4 - a_1)k$, soit de la forme

$$a = \varepsilon + (\lambda_1 1 + \lambda_2 i + \lambda_3 j + \lambda_4 k) \qquad \text{avec } \lambda_1, \ldots, \lambda_4 \in \mathbb{Z},$$

et alors $a = (1 + 2\lambda_1)\varepsilon + (\lambda_2 - \lambda_1)i + (\lambda_3 - \lambda_1)j + (\lambda_4 - \lambda_1)k$. Une simple vérification montre qu'en fait l'ensemble

$$\Theta = \{b_1\varepsilon + b_2 i + b_3 j + b_4 k \mid b_1, \ldots, b_4 \in \mathbb{Z}\}$$

est bien un ordre. Le discriminant réduit de cet ordre est : $d(\Theta) = 2$, donc il n'y a pas d'ordre Λ' contenu strictement dans Θ et contenant strictement Λ, puisqu'il n'y a pas d'entier positif qui soit multiple strict de 2 et diviseur strict de 4. En conclusion, l'ordre Θ est l'unique ordre de A contenant strictement Λ ; il est donc bien sûr maximal.

c) Soit à présent $B = (-1,-3)_{\mathbb{Q}}$. Comme les produits deux à deux d'éléments de la base standard sont des combinaisons linéaires à coefficients entiers des éléments de cette base, l'ensemble

$$\Gamma = \{a_1 1 + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

est un ordre de B. Un calcul direct donne son discriminant réduit : $d(\Gamma) = 12$.

Pour déterminer si Γ est maximal et, le cas échéant, pour trouver un ordre maximal contenant Γ, on raisonne comme dans l'exemple précédent : supposons avoir trouvé un ordre $\Gamma' \supsetneq \Gamma$ et soit

$$a = a_1 1 + a_2 i + a_3 j + a_4 k \in \Gamma' \quad (a_1, \ldots, a_4 \in \mathbb{Q}).$$

Les conditions : $T(a), T(ai), T(aj), T(ak) \in \mathbb{Z}$ donnent :

$$2a_1, 2a_2, 6a_3, 6a_4 \in \mathbb{Z}.$$

Par ailleurs, on doit aussi avoir $N(a) \in \mathbb{Z}$, donc

$$a_1^2 + a_2^2 + 3a_3^2 + 3a_4^2 \in \mathbb{Z}.$$

Ecrivons : $a_1 = \frac{\alpha_1}{2}, a_2 = \frac{\alpha_2}{2}, a_3 = \frac{\alpha_3}{6}, a_4 = \frac{\alpha_4}{6}$ pour certains entiers $\alpha_1, \ldots, \alpha_4$. La condition précédente s'écrit alors :

$$3\alpha_1^2 + 3\alpha_2^2 + \alpha_3^2 + \alpha_4^2 \in 12\mathbb{Z},$$

ce qui entraîne : $\alpha_3^2 + \alpha_4^2 \in 3\mathbb{Z}$. Comme les carrés modulo 3 sont représentés par 0 et 1, cette dernière relation entraîne à son tour : $\alpha_3 \equiv \alpha_4 \equiv 0 \bmod 3$. Soit $\alpha_3 = 3\alpha'_3$ et $\alpha_4 = 3\alpha'_4$ pour certains entiers α'_3, α'_4. La condition sur la norme de a s'écrit à présent :

$$\alpha_1^2 + \alpha_2^2 + 3\alpha'^2_3 + 3\alpha'^2_4 \in 4\mathbb{Z}.$$

En examinant les différentes solutions, on voit que Γ' doit contenir l'un des éléments suivants :

$$\tfrac{1}{2}(1+j), \tfrac{1}{2}(1+k), \tfrac{1}{2}(i+j), \tfrac{1}{2}(i+k), \tfrac{1}{2}(1+i+j+k).$$

S'il contient $\frac{1}{2}(1+j)$, alors il doit contenir aussi $i.\frac{1}{2}(1+j) = \frac{1}{2}(i+k)$, et il contient alors aussi $\frac{1}{2}(1+j) + \frac{1}{2}(i+k) = \frac{1}{2}(1+i+j+k)$. De même, s'il contient $\frac{1}{2}(1+k)$, alors il doit aussi contenir $i.\frac{1}{2}(1+k) + j = \frac{1}{2}(i+j)$ et $\frac{1}{2}(1+k) + \frac{1}{2}(i+j) = \frac{1}{2}(1+i+j+k)$. Par ailleurs, Γ' ne peut contenir les cinq éléments ci-dessus, car alors il contiendrait aussi $\frac{1}{2}(1+j) - \frac{1}{2}(i+j)$, dont la norme est $\frac{1}{2}$.

Par ce genre d'arguments, on parvient à la conclusion que Γ' est l'un des ensembles suivants, dont on peut vérifier qu'ils sont bien des ordres de B :

$$\begin{aligned}
\Delta &= \left\{ a_1 1 + a_2 i + a_3 \frac{1+j}{2} + a_4 \frac{i+k}{2} \mid a_1, \ldots, a_4 \in \mathbb{Z} \right\} \\
\Phi &= \left\{ a_1 1 + a_2 i + a_3 \frac{i+j}{2} + a_4 \frac{1+k}{2} \mid a_1, \ldots, a_4 \in \mathbb{Z} \right\} \\
\Psi &= \left\{ a_1 1 + a_2 i + a_3 j + a_4 \frac{1+i+j+k}{2} \mid a_1, \ldots, a_4 \in \mathbb{Z} \right\}.
\end{aligned}$$

Les ordres Δ et Φ sont maximaux, et $\Psi = \Delta \cap \Phi$. Les discriminants réduits se calculent aisément : $d(\Delta) = d(\Phi) = 3$; $d(\Psi) = 6$.

4. *Notes :* On peut tirer de la démonstration de la proposition 4 une précision supplémentaire : si Λ et Λ' sont deux ordres tels que $\Lambda \supseteq \Lambda'$, alors $(\Lambda : \Lambda') = \frac{d(\Lambda')}{d(\Lambda)}$.

Tous les résultats de cette section (et leurs démonstrations) se généralisent presque sans modification au cas des ordres sur un anneau principal R dans une algèbre de quaternions sur le corps des fractions de R. Il faut cependant être attentif au fait que le discriminant d'un ordre n'est alors défini qu'à un facteur près dans $R^{\times 2}$, le groupe des carrés d'éléments inversibles de R. (Le cas où $R = \mathbb{Z}$ est particulièrement simple à cet égard, vu que $\mathbb{Z}^\times = \{\pm 1\}$ et $\mathbb{Z}^{\times 2} = \{1\}$).

Les résultats de cette section se généralisent encore au cas où R est un anneau intègre non nécessairement principal et où l'algèbre de quaternions est remplacée par une algèbre à division quelconque dont le centre est le corps de fractions de R, mais les modifications à apporter sont alors assez importantes, à commencer par la définition d'ordre : un ordre est alors un sous-anneau qui est de type fini comme module sur R et qui contient une base de l'algèbre. Lorsque R est principal, ce module est libre, de sorte que l'on peut se ramener à la définition donnée au début de la section. Lorsque l'ordre n'est pas un module libre, la définition du discriminant doit bien sûr être revue également. Pour ces généralisations, on consultera avec profit les livres de Reiner [11] et de Deuring [4].

Un cas particulier important, directement lié au sujet traité ici, est celui où l'anneau de base R est l'anneau $\mathbb{Z}_p$ des nombres p-adiques, pour un certain nombre premier p. Cet anneau est principal et son seul élément irréductible est p (à la multiplication près par des éléments inversibles). De plus, il contient l'anneau $\mathbb{Z}$, de sorte que son corps de fractions $\mathbb{Q}_p$ contient le corps $\mathbb{Q}$. Toute algèbre de quaternions rationnelle $A = (a, b)_{\mathbb{Q}}$ se plonge naturellement dans une algèbre de quaternions p-adique :

$$A \hookrightarrow A_p = (a, b)_{\mathbb{Q}_p},$$

et si $\Lambda = \{a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$ est un ordre de A, alors

$$\Lambda_p = \{a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 \mid a_1, \ldots, a_4 \in \mathbb{Z}_p\}$$

est un ordre de A_p sur $\mathbb{Z}_p$. Comme $(e_1, \ldots, e_4)$ est à la fois base de Λ sur $\mathbb{Z}$ et base de Λ_p sur $\mathbb{Z}_p$, il est clair que $d(\Lambda)$ est un représentant de $d(\Lambda_p)$ (ce dernier élément n'étant défini qu'à un facteur inversible de $\mathbb{Z}_p$ près).

La classification des algèbres de quaternions p-adiques est très simple (et particulièrement aisée lorsque p est impair) : à isomorphisme près, il n'y a qu'une seule algèbre de quaternions à division sur $\mathbb{Q}_p$. (Voir [8, Ch.6, Theorem 2.10]). De plus, cette algèbre de quaternions à division contient un unique ordre maximal : c'est l'ensemble des éléments dont la norme a une valuation p-adique non négative (voir [11, §12]) ; le discriminant réduit de cet ordre est p (à la multiplication près par un élément inversible de $\mathbb{Z}_p$). Dès lors, si p est un nombre premier qui ne divise pas le discriminant réduit $d(\Lambda)$, alors l'algèbre A_p est une algèbre de matrices ; en effet, cette algèbre contient l'ordre Λ_p de discriminant réduit inversible dans $\mathbb{Z}_p$, donc elle ne peut pas être à division. Par ailleurs, si Λ est un ordre maximal de A, alors on peut prouver au moyen d'un principe "local-global" (voir [13, p.83]) que Λ_p est un ordre maximal de A_p pour tout p premier. Il en résulte que $d(\Lambda)$ est le produit des nombres premiers p tels que l'algèbre A_p soit à division ; par conséquent, tous les ordres maximaux de A ont le même discriminant réduit, que l'on appelle aussi (par abus de langage) *discriminant de l'algèbre A*.

Un théorème célèbre dû à Brauer-Hasse-Noether et Albert établit que ce discriminant classifie les algèbres de quaternions rationnelles à isomorphisme près. (Voir [11, Ch.8] ; il y

a un énoncé analogue pour les algèbres simples centrales de dimension finie quelconque sur un corps de nombres arbitraire. Si le corps de nombres admet plusieurs plongements dans le corps des réels, le discriminant ne suffit pas ; il faut aussi tenir compte du comportement de l'algèbre par les différentes extensions des scalaires à $\mathbb{R}$). Voici pour terminer une démonstration élémentaire d'une partie de ce résultat (pour le cas particulier des algèbres de quaternions rationnelles), due à E. Witt [14] :
Théorème : Si A est une algèbre de quaternions rationnelle de discriminant 1*, alors* $A \simeq M_2(\mathbb{Q})$.

Démonstration (E. Witt) : Soit $A = (a, b)_{\mathbb{Q}}$ une algèbre de quaternions rationnelle à division et soit Λ un ordre de A (sur $\mathbb{Z}$). Il s'agit de prouver : $d(\Lambda) \neq 1$. On considère pour cela le plongement :

$$A \hookrightarrow A_\infty = (a, b)_{\mathbb{R}}.$$

D'après le numéro 4 de la première section, l'algèbre A_∞ est isomorphe soit à $(-1, -1)_{\mathbb{R}}$, soit à $(1, -1)_{\mathbb{R}}$ ($\simeq M_2(\mathbb{R})$). Au moyen de la base standard $(1, i_\infty, j_\infty, k_\infty)$ de $(-1, -1)_{\mathbb{R}}$ ou de $(1, -1)_{\mathbb{R}}$, on peut établir un isomorphisme d'espaces vectoriels $f : A_\infty \to \mathbb{R}^4$ par : $f(x_1 + x_2 i_\infty + x_3 j_\infty + x_4 k_\infty) = (x_1, x_2, x_3, x_4)$. Cet isomorphisme possède la propriété suivante : pour $x = x_1 + x_2 i_\infty + x_3 j_\infty + x_4 k_\infty$,

$$|N(x)| = |x_1^2 \pm x_2^2 + x_3^2 \pm x_4^2| \leq x_1^2 + x_2^2 + x_3^2 + x_4^2 = \|f(x)\|^2,$$

où $\|.\|$ désigne la norme usuelle sur $\mathbb{R}^4$. L'ordre Λ est ainsi identifié à un réseau de $\mathbb{R}^4$. Le disque ouvert D de $\mathbb{R}^4$ centré en 0 et de rayon 1 ne contient pas d'autre point de ce réseau que 0, car pour $x \in \Lambda$, $x \neq 0$, la norme $N(x)$ est un entier non nul, donc $|N(x)| \geq 1$ et, d'après la relation ci-dessus, $\|f(x)\| \geq 1$. D'après un théorème de Minkowski ([12, Corollaire, p.67]), le volume du disque D est lié à la maille du réseau Λ par la relation :

$$v(D) \leq 2^4 m(\Lambda);$$

or, le volume du disque unité de $\mathbb{R}^4$ est : $v(D) = \frac{\pi^2}{2}$ et la maille du réseau Λ est $\frac{d(\Lambda)}{4}$, le dénominateur 4 provenant du discriminant de la base $(1, i_\infty, j_\infty, k_\infty)$; dès lors, on a :

$$d(\Lambda) \geq \frac{\pi^2}{8} > 1.$$

■

3 Idéaux et quotients d'ordres

Par comparaison aux algèbres de quaternions, les ordres présentent l'avantage de se prêter à un plus grand nombre de constructions algébriques. Dans cette section, on se propose d'examiner en particulier la construction d'anneaux quotients, qui est rendue impossible dans les algèbres de quaternions par l'absence d'idéaux bilatères (voir les notes de la première section). Commençons par rappeler la notion d'*idéal*; le fait que la multiplication dans un ordre n'est pas commutative conduit à introduire une distinction entre idéaux à gauche, à droite et bilatères :

1. *Définitions :* Une partie I d'un ordre Λ d'une algèbre de quaternions A est un *idéal à gauche* de Λ si elle satisfait les conditions suivantes :

1. $0 \in I$.
2. I est stable pour l'addition : $x + y \in I$ si $x, y \in I$.
3. I est stable par les multiplications à gauche par les éléments de Λ : $\lambda x \in I$ pour $\lambda \in \Lambda$ et $x \in I$.

On définit de même la notion d'*idéal à droite*, en remplaçant la condition 3 par celle-ci : $x\lambda \in I$ pour $\lambda \in \Lambda$ et $x \in I$. Enfin, on appelle *idéal bilatère* tout idéal à gauche qui est également idéal à droite.

Par exemple, pour $x \in \Lambda$, l'ensemble des multiples à gauche de x :

$$\Lambda x = \{\lambda x \mid \lambda \in \Lambda\}$$

est un idéal à gauche de Λ ; de même,

$$x\Lambda = \{x\lambda \mid \lambda \in \Lambda\}$$

est un idéal à droite et

$$\Lambda x \Lambda = \{\textstyle\sum_i \lambda_i x \mu_i \mid \lambda_i, \mu_i \in \Lambda\}$$

est un idéal bilatère. Bien sûr, si $x \in \mathbb{Z}$, alors x commute avec tout élément de A, donc

$$\Lambda x = x\Lambda = \Lambda x \Lambda.$$

Plus généralement, pour $x_1, \ldots, x_n \in \Lambda$, l'ensemble

$$\Lambda x_1 + \cdots + \Lambda x_n = \{\lambda_1 x_1 + \cdots + \lambda_n x_n \mid \lambda_1, \ldots, \lambda_n \in \Lambda\}$$

est un idéal à gauche ; on peut encore construire d'autres exemples en formant des intersections, car toute intersection d'idéaux à gauche (resp. à droite, resp. bilatères) est un idéal à gauche (resp. à droite, resp. bilatère).

Comme tout ordre Λ est stable par la conjugaison de l'algèbre de quaternions (voir la proposition 2), il est clair que pour tout idéal à gauche I de Λ, le conjugué

$$\overline{I} = \{\overline{\lambda} \mid \lambda \in I\}$$

est un idéal à droite de Λ, vu que le conjugué d'un produit est égal au produit des conjugués dans l'ordre inverse. Réciproquement, le conjugué de tout idéal à droite de Λ est un idéal à gauche de Λ.

La particularité des idéaux bilatères est de permettre la construction d'anneaux quotients, sur le même modèle que l'anneau des classes résiduelles $\mathbb{Z}/n\mathbb{Z}$: si I est un idéal bilatère d'un ordre Λ, l'ensemble

$$\Lambda/I = \{\lambda + I \mid \Lambda \in \Lambda\},$$

dans lequel l'égalité de deux éléments $\lambda + I = \mu + I$ est définie par la condition : $\lambda - \mu \in I$, hérite de Λ une structure d'anneau, l'addition et la multiplication étant définies par :

$$\begin{aligned} (\lambda + I) + (\mu + I) &= (\lambda + \mu) + I \\ (\lambda + I)(\mu + I) &= \lambda\mu + I. \end{aligned}$$

(La condition que I est un idéal bilatère garantit que ces opérations sont bien définies, c'est-à-dire que si $\lambda + I = \lambda' + I$ et $\mu + I = \mu' + I$, alors $(\lambda + \mu) + I = (\lambda' + \mu') + I$ et $\lambda\mu + I = \lambda'\mu' + I$).

Dans cette section, on se propose d'examiner en particulier les quotients d'ordres des algèbres de quaternions rationnelles par les idéaux (bilatères) des multiples des nombres premiers $p \in \mathbb{Z}$. Remarquons pour commencer que si Λ est un ordre, alors l'anneau quotient $\Lambda/p\Lambda$ est une algèbre de dimension 4 sur le corps à p éléments $\mathbb{F}_p$ $(= \mathbb{Z}/p\mathbb{Z})$; en effet, si $(e_1, \ldots, e_4)$ est une base de Λ sur $\mathbb{Z}$, alors $(e_1 + p\Lambda, \ldots, e_4 + p\Lambda)$ est une base de $\Lambda/p\Lambda$ sur $\mathbb{F}_p$. La détermination de la structure de $\Lambda/p\Lambda$ se fonde principalement sur la forme bilinéaire symétrique t déduite de la trace :

$$t : \ (\Lambda/p\Lambda) \times (\Lambda/p\Lambda) \to \mathbb{F}_p$$

définie par :

$$t(x + p\Lambda, y + p\Lambda) = T(xy) + p\mathbb{Z}.$$

Si $(e_1, \ldots, e_4)$ est une base de Λ sur $\mathbb{Z}$, alors la matrice de la forme bilinéaire symétrique t par rapport à la base $(e_1 + p\Lambda, \ldots, e_4 + p\Lambda)$ est :

$$(t(e_i + p\Lambda, e_j + p\Lambda))_{1 \leq i,j \leq 4} = (T(e_i e_j) + p\mathbb{Z})_{1 \leq i,j \leq 4};$$

le déterminant de cette matrice est donc $\mathrm{disc}(\Lambda) + p\mathbb{Z} = -d(\Lambda)^2 + p\mathbb{Z}$. Il est donc naturel de poursuivre la discussion en considérant séparément le cas où p divise $d(\Lambda)$.

2. *Cas où p ne divise pas le discriminant :* Dans ce cas, on obtient un théorème de structure très précis :

Théorème 2 *Soit Λ un ordre (sur $\mathbb{Z}$) dans une algèbre de quaternions A (sur $\mathbb{Q}$). Si p est un nombre premier qui ne divise pas le discriminant réduit $d(\Lambda)$, alors $\Lambda/p\Lambda$ est une algèbre de matrices sur le corps $\mathbb{F}_p$ à p éléments :*

$$\Lambda/p\Lambda \simeq M_2(\mathbb{F}_p).$$

Démonstration: Comme p ne divise pas $d(\Lambda)$, la forme bilinéaire t est non dégénérée. Comme les formes bilinéaires et les algèbres de quaternions en caractéristique 2 possèdent des propriétés assez particulières, nous traiterons séparément le cas où $p = 2$. Supposons d'abord p impair ; le principe de la démonstration dans ce cas est de montrer que $\Lambda/p\Lambda$ est une algèbre de quaternions sur $\mathbb{F}_p$; le résultat découle alors du corollaire 1.

Comme p est supposé impair, $1 + p\Lambda$ est anisotrope pour la forme t ; on peut donc trouver une base orthogonale de $\Lambda/p\Lambda$ qui contient $1 + p\Lambda$. Soit $(1 + p\Lambda, \lambda_1 + p\Lambda, \lambda_2 + p\Lambda, \lambda_3 + p\Lambda)$ une telle base ; on a donc, en particulier :

$$t(1 + p\Lambda, \lambda_1 + p\Lambda) = 0,$$

c'est-à-dire :

$$T(\lambda_1) \in p\mathbb{Z}. \tag{2}$$

On a aussi $t(\lambda_1 + p\Lambda, \lambda_1 + p\Lambda) \neq 0$, car la forme bilinéaire t est non dégénérée, c'est-à-dire :

$$T(\lambda_1^2) \notin p\mathbb{Z}. \tag{3}$$

Comme λ_1 est racine du polynôme

$$(X - \lambda_1)(X - \overline{\lambda_1}) = X^2 - T(\lambda_1)X + N(\lambda_1),$$

on a :

$$\lambda_1^2 = T(\lambda_1)\lambda_1 - N(\lambda_1), \tag{4}$$

d'où

$$T(\lambda_1^2) = T(\lambda_1)^2 - 2N(\lambda_1).$$

Les relations (2) et (3) ci-dessus donnent alors : $N(\lambda_1) \notin p\mathbb{Z}$, d'où, par (4) :

$$(\lambda_1 + p\Lambda)^2 = -N(\lambda_1).(1 + p\Lambda) \neq 0.$$

De même, on trouve :

$$(\lambda_2 + p\Lambda)^2 = -N(\lambda_2).(1 + p\Lambda) \neq 0.$$

Enfin, comme $\lambda_1 + p\Lambda$ et $\lambda_2 + p\Lambda$ sont orthogonaux pour la forme t, on a $T(\lambda_1\lambda_2) \in p\mathbb{Z}$, c'est-à-dire : $\lambda_1.\lambda_2 + \overline{\lambda_2}.\overline{\lambda_1} \in p\mathbb{Z}$, ou :

$$(\lambda_1 + p\Lambda)(\lambda_2 + p\Lambda) + (\overline{\lambda_2} + p\Lambda)(\overline{\lambda_1} + p\Lambda) = 0. \tag{5}$$

De (2), on déduit de même :

$$\overline{\lambda_1} + p\Lambda = -\lambda_1 + p\Lambda.$$

Comme la même relation vaut pour λ_2, l'équation (5) donne :

$$(\lambda_1 + p\Lambda)(\lambda_2 + p\Lambda) = -(\lambda_2 + p\Lambda)(\lambda_1 + p\Lambda).$$

En utilisant les relations précédentes, on voit que l'élément $\lambda_1\lambda_2 + p\Lambda$ de $\Lambda/p\Lambda$ est orthogonal à $1 + p\Lambda, \lambda_1 + p\Lambda$ et $\lambda_2 + p\Lambda$ pour la forme t ; par conséquent, les éléments $1 + p\Lambda, \lambda_1 + p\Lambda, \lambda_2 + p\Lambda, \lambda_1\lambda_2 + p\Lambda$ forment une base de $\Lambda/p\Lambda$ et satisfont les relations qui définissent une algèbre de quaternions. On a donc $\Lambda/p\Lambda \simeq M_2(\mathbb{F}_p)$, par le corollaire 1.

Supposons maintenant $p = 2$. L'élément $1 + 2\Lambda$ est alors isotrope pour la forme t ; cependant, le lemme 3 montre que $1 + 2\Lambda \neq 0$, donc l'orthogonal de cet élément dans $\Lambda/2\Lambda$ est de dimension 3 sur $\mathbb{F}_2$. Soit $\lambda_1 + 2\Lambda$ un élément de cet orthogonal, différent de $0\ (= 0 + 2\Lambda)$ et de $1 + 2\Lambda$. On a donc

$$T(\lambda_1) \in 2\mathbb{Z}.$$

De plus, comme $N(1 + \lambda_1) = 1 + T(\lambda_1) + N(\lambda_1)$, on a $N(1 + \lambda_1) \in 2\mathbb{Z}$ si et seulement si $N(\lambda_1) \in 1 + 2\mathbb{Z}$. Quitte à remplacer λ_1 par $1 + \lambda_1$, on peut donc supposer de plus : $N(\lambda_1) \in 2\mathbb{Z}$. La relation (4) donne alors :

$$(\lambda_1 + 2\Lambda)^2 = 0,$$

ce qui entraîne aussi que $\lambda_1 + 2\Lambda$ est isotrope pour la forme t.

Soit $\lambda_2 + 2\Lambda$ un élément de l'orthogonal de $1 + 2\Lambda$ qui ne soit pas orthogonal à $\lambda_1 + 2\Lambda$. (Il en existe, car $1 + 2\Lambda$ et $\lambda_1 + 2\Lambda$ ne sont pas multiples l'un de l'autre). On a donc :

$$T(\lambda_2) \in 2\mathbb{Z}, \qquad T(\lambda_1\lambda_2) \in 1 + 2\mathbb{Z}.$$

Encore une fois, quitte à remplacer λ_2 par $1+\lambda_2$, on peut supposer de plus : $N(\lambda_2) \in 2\mathbb{Z}$, d'où, comme précédemment :

$$(\lambda_2 + 2\Lambda)^2 = 0.$$

Pour la commodité des notations, posons : $e_0 = 1 + 2\Lambda$, $e_1 = \lambda_1 + 2\Lambda$, $e_2 = \lambda_2 + 2\Lambda$ et $e_3 = \lambda_1\lambda_2 + 2\Lambda$. Montrons que (e_0, e_1, e_2, e_3) est une base de $\Lambda/2\Lambda$ sur $\mathbb{F}_2$. Il suffit bien sûr de prouver que ces éléments sont linéairement indépendants. Si

$$(\alpha_0 + 2\mathbb{Z})e_0 + (\alpha_1 + 2\mathbb{Z})e_1 + (\alpha_2 + 2\mathbb{Z})e_2 + (\alpha_3 + 2\mathbb{Z})e_3 = 0,$$

c'est-à-dire si

$$\alpha_0 1 + \alpha_1\lambda_1 + \alpha_2\lambda_2 + \alpha_3\lambda_1\lambda_2 \in 2\Lambda,$$

alors $T(\alpha_0 1 + \alpha_1\lambda_1 + \alpha_2\lambda_2 + \alpha_3\lambda_1\lambda_2) \in 2\mathbb{Z}$, ce qui donne, vu que $T(1)$, $T(\lambda_1)$, $T(\lambda_2) \in 2\mathbb{Z}$ et $T(\lambda_1\lambda_2) \in 1 + 2\mathbb{Z}$:

$$\alpha_3 \in 2\mathbb{Z}.$$

Par ailleurs, il est impossible que e_2 soit combinaison linéaire de e_0 et e_1, car e_2 n'est pas orthogonal à e_1 ; on doit donc avoir $\alpha_2 \equiv 0 \bmod 2$. Dès lors, on obtient également $\alpha_0 \equiv \alpha_1 \equiv 0 \bmod 2$, car e_1 n'est pas multiple de e_0.

Déterminons à présent la table de multiplication des éléments $e_0, \ldots, e_3$. On sait que e_0 est l'unité ; par ailleurs, on a déjà obtenu ci-dessus les relations :

$$e_1^2 = e_2^2 = 0.$$

Comme la norme est multiplicative et que $N(\lambda_1) \in 2\mathbb{Z}$, on a $N(\lambda_1\lambda_2) \in 2\mathbb{Z}$, d'où, puisque tout élément $a \in A$ est racine du polynôme $(X - a)(X - \overline{a}) = X^2 - T(a)X + N(a)$,

$$e_3^2 - e_3 = 0.$$

Par ailleurs, de la relation $T(\lambda_1\lambda_2) \in 1 + 2\mathbb{Z}$, on déduit aussi :

$$(\lambda_1 + 2\Lambda)(\lambda_2 + 2\Lambda) + (\overline{\lambda_2} + 2\Lambda)(\overline{\lambda_1} + 2\Lambda) = 1 + 2\Lambda.$$

De même, les relations $T(\lambda_1), T(\lambda_2) \in 2\mathbb{Z}$ donnent :

$$\overline{\lambda_1} + 2\Lambda = -\lambda_1 + 2\Lambda = \lambda_1 + 2\Lambda, \quad \overline{\lambda_2} + 2\Lambda = -\lambda_2 + 2\Lambda = \lambda_2 + 2\Lambda,$$

si bien que la relation précédente s'écrit aussi :

$$e_1e_2 + e_2e_1 = e_0.$$

De ces relations, la table de multiplication des éléments $e_0, \ldots, e_3$ se déduit facilement :

	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	0	e_3	0
e_2	e_2	$e_0 + e_3$	0	e_2
e_3	e_3	e_1	0	e_3

Un calcul direct montre alors que l'application $\Lambda/2\Lambda \to M_2(\mathbb{F}_2)$ définie par :

$$a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3 \mapsto \begin{pmatrix} a_0 + a_3 & a_1 \\ a_2 & a_0 \end{pmatrix}$$

est un isomorphisme. ∎

3. *Cas où p divise le discriminant :* La structure de $\Lambda/p\Lambda$ ne se décrit pas de manière aussi simple dans ce cas. Pour notre objet, le résultat suivant est suffisant :

Théorème 3 *Soit Λ un ordre (sur $\mathbb{Z}$) dans une algèbre de quaternions A sur $\mathbb{Q}$. Si p est un nombre premier qui divise le discriminant réduit $d(\Lambda)$, alors $\Lambda/p\Lambda$ admet un idéal bilatère non trivial (c'est-à-dire différent de $\{0\}$ et de $\Lambda/p\Lambda$).*

Démonstration: Considérons le radical de la forme bilinéaire t :

$$\text{rad } t = \{\xi \in \Lambda/p\Lambda \mid t(\xi, \eta) = 0 \text{ pour tout } \eta \in \Lambda/p\Lambda\}.$$

Vu la définition de la forme t :

$$t(\xi, \eta) = T(xy) + p\mathbb{Z} \quad \text{pour } \xi = x + p\Lambda \text{ et } \eta = y + p\Lambda,$$

et vu les propriétés de la trace T, il est clair que pour $\xi, \eta, \zeta \in \Lambda/p\Lambda$:

$$t(\xi\eta, \zeta) = t(\xi, \eta\zeta) = t(\eta, \zeta\xi).$$

Dès lors, rad t est un idéal de $\Lambda/p\Lambda$. Cet idéal n'est pas réduit à $\{0\}$ dans le cas présent, puisque la forme t est dégénérée lorsque p divise $d(\Lambda)$.

Si rad $t \neq \Lambda/p\Lambda$, l'énoncé est donc démontré ; il ne reste donc qu'à envisager le cas où rad $t = \Lambda/p\Lambda$, c'est-à-dire celui où la forme t est nulle ou encore celui où $T(x) \in p\mathbb{Z}$ pour tout $x \in \Lambda$. Comme $T(1) = 2$, on doit avoir $p = 2$ dans ce cas. De plus, l'hypothèse que $T(x) \in 2\mathbb{Z}$ pour tout $x \in \Lambda$ entraîne :

$$x + \overline{x} \in 2\mathbb{Z} \subset 2\Lambda$$

et, comme $-1 = 1$ dans $\Lambda/2\Lambda$, on en déduit :

$$\overline{x} + 2\Lambda = x + 2\Lambda$$

pour tout $x \in \Lambda$. Dès lors, le quotient $\Lambda/2\Lambda$ est commutatif, puisque de la relation $\overline{x.y} = \overline{y}.\overline{x}$ on déduit en prenant les classes modulo 2Λ et en utilisant la propriété précédente :

$$xy + 2\Lambda = (y + 2\Lambda)(x + 2\Lambda).$$

De plus, on a pour tout $x \in \Lambda$:

$$(x + 2\Lambda)^2 = x\overline{x} + 2\Lambda = N(x) + 2\Lambda,$$

et, comme $N(x) \in \mathbb{Z}$, l'image de $N(x)$ dans $\Lambda/2\Lambda$ est $0 + 2\Lambda$ ou $1 + 2\Lambda$; par conséquent, pour tout $\xi \in \Lambda/2\Lambda$:

$$\xi^2 = 0 \text{ ou } 1.$$

Considérons alors

$$I = \{\xi \in \Lambda/2\Lambda \mid \xi^2 = 0\} \text{ et } I' = \{\xi \in \Lambda/2\Lambda \mid \xi^2 = 1\}.$$

Comme $\Lambda/2\Lambda$ est commutatif et que, dans $\Lambda/2\Lambda$,

$$(\xi + \eta)^2 = \xi^2 + 2\xi\eta + \eta^2 = \xi^2 + \eta^2,$$

l'ensemble I est un idéal (bilatère) de $\Lambda/2\Lambda$. De plus, I et I' ont le même nombre d'éléments, car la bijection $\xi \mapsto \xi + 1$ échange I et I' ; comme $\Lambda/2\Lambda$ est l'union de I et I', qui sont disjoints, on voit que I contient exactement la moitié des éléments de $\Lambda/2\Lambda$, donc c'est un idéal bilatère non trivial. ∎

4. *Exemple :* Soit $A = (-1,-1)_{\mathbb{Q}}$ et soit Λ l'ordre engendré par la base standard de A :

$$\Lambda = \{a_1 1 + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\}.$$

Le discriminant réduit de Λ a été calculé au numéro 3 de la section 2 : $d(\Lambda) = 4$. Dès lors, pour tout nombre premier $p \neq 2$, le quotient $\Lambda/p\Lambda$ est isomorphe à l'algèbre de matrices $M_2(\mathbb{F}_p)$. Par exemple, pour $p = 3$, on peut établir comme suit un isomorphisme explicite :

$$(a_1 1 + a_2 i + a_3 j + a_4 k) + 3\Lambda \mapsto \begin{pmatrix} a_1 + a_3 + a_4 + 3\mathbb{Z} & a_2 + a_3 - a_4 + 3\mathbb{Z} \\ -a_2 + a_3 - a_4 + 3\mathbb{Z} & a_1 - a_3 - a_4 + 3\mathbb{Z} \end{pmatrix}.$$

Pour $p = 2$, le quotient $\Lambda/2\Lambda$ se trouve dans la situation exceptionnelle décrite dans la démonstration du théorème 3, puisque $T(x) \in 2\mathbb{Z}$ pour tout $x \in \Lambda$. Le quotient $\Lambda/2\Lambda$ est l'algèbre commutative de dimension 4 sur $\mathbb{F}_2$ ayant pour base $(1{+}2\Lambda, i{+}2\Lambda, j{+}2\Lambda, k{+}2\Lambda)$. On observe que chaque élément de cette base a pour carré 1 ($= 1{+}2\Lambda$) ; dès lors l'idéal I des éléments de carré nul consiste en l'ensemble des éléments du type $(a_1 1{+}a_2 i{+}a_3 j{+}a_4 k){+}2\Lambda$ où $a_1 + a_2 + a_3 + a_4 \in 2\mathbb{Z}$. (Le quotient $\Lambda/2\Lambda$ est isomorphe à l'algèbre du groupe $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ sur $\mathbb{F}_2$).

5. *Notes :* Comme les ordres d'algèbres de quaternions admettent une "algèbre de fractions" (à savoir l'algèbre de quaternions elle-même), il est habituel et souvent commode d'élargir la notion d'idéal en y incluant les modules de la forme $d^{-1}I$ où I est un idéal (au sens de la définition donnée ci-dessus) et d est un entier non nul. Ces modules sont parfois appelés "idéaux fractionnaires", les idéaux au sens de la définition du numéro 1 étant alors désignés sous le terme d'idéaux "entiers". Par ailleurs, étant donné la grande variété d'ordres dans une algèbre de quaternions, il est aussi utile de *restreindre* la notion d'idéal pour renforcer la relation entre un ordre et ses idéaux. En effet, avec la définition donnée ci-dessus, tout idéal d'un ordre Λ est également un idéal (éventuellement fractionnaire) de tout ordre contenu dans Λ.

On est ainsi conduit à poser les définitions suivantes (voir [13, p.21]) : si A est une algèbre de quaternions rationnelle, on appelle ($\mathbb{Z}$-) *réseau* de A tout sous-$\mathbb{Z}$-module de type fini de A contenant une base de A (sur $\mathbb{Q}$) ; si R est un réseau de A, on définit :

$$\mathcal{O}_g(R) = \{a \in A \mid aR \subseteq R\} \quad \text{et} \quad \mathcal{O}_d(R) = \{a \in A \mid Ra \subseteq R\}.$$

Ces ensembles sont des ordres de A, que l'on appelle respectivement *ordre (des stabilisateurs) à gauche* et *ordre (des stabilisateurs à droite)* de R. Enfin, si Λ est un ordre de A (sur $\mathbb{Z}$), on appelle *idéal à gauche* (resp. *à droite*) de Λ tout réseau R de A tel que $\mathcal{O}_g(R) = \Lambda$ (resp. $\mathcal{O}_d(R) = \Lambda$).

Pour comparer cette notion à celle introduite au début de la section, posons momentanément les définitions suivantes : I est un idéal à gauche de Λ *au sens 1* s'il satisfait les conditions du numéro 1, c'est-à-dire : I est un sous-groupe additif de Λ stable par les multiplications à gauche par les éléments de Λ, et I est un idéal à gauche de Λ *au sens 2* si c'est un réseau de A tel que $\mathcal{O}_g(I) = \Lambda$. Les idéaux à gauche au sens 2 qui sont contenus dans Λ sont alors des idéaux au sens 1 ; plus généralement, si I est un idéal à gauche au sens 2, alors il existe un entier $d \neq 0$ tel que $dI \subseteq \Lambda$; l'ensemble dI est alors un idéal à gauche de Λ au sens 1. Inversement, si I est un idéal à gauche de Λ au sens 1, on ne peut pas conclure que I est un idéal à gauche au sens 2 : d'abord, si I ne contient que des éléments non inversibles de A — par exemple si $\Lambda = M_2(\mathbb{Z})$ et que $I \subseteq \Lambda$ est l'ensemble

des matrices dont la seconde colonne est nulle — alors I n'est certainement pas un idéal au sens 2 puisqu'il ne peut contenir une base de A. Cependant, si I contient un élément a inversible dans A, alors il doit contenir aussi $e_1a, \ldots, e_4a$, pour toute base $e_1, \ldots, e_4$ de Λ sur $\mathbb{Z}$, et ces éléments forment une base de A. Dès lors, si A est une algèbre à division, tout idéal à gauche I *non nul* au sens 1 contient une base de A. Comme I est contenu dans Λ, on peut dire de plus que I est un $\mathbb{Z}$-module de type fini. Par ailleurs, la condition de stabilité par les multiplications à gauche signifie seulement : $\Lambda \subseteq \mathcal{O}_g(I)$, et l'on n'a pas nécessairement l'égalité, sauf bien sûr si Λ est un ordre maximal. Par exemple, si $\Lambda \subseteq M_2(\mathbb{Q})$ est l'ordre défini par :

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ nc & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$$

pour un certain $n \in \mathbb{Z}$ fixé ($n \neq \pm 1$), alors l'ensemble

$$I = \left\{ \begin{pmatrix} a & b \\ nc & nd \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$$

est un idéal à gauche de Λ au sens 1 mais non au sens 2 car on peut vérifier :

$$\mathcal{O}_g(I) = \left\{ \begin{pmatrix} a & n^{-1}b \\ nc & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\} \supsetneq \Lambda.$$

On peut vérifier de plus que I n'est pas de la forme Λx avec $x \in \Lambda$, alors que tous les idéaux de Λ au sens 2 sont de la forme Λx (avec x inversible dans $M_2(\mathbb{Q})$). L'ordre Λ est donc principal, à condition de se limiter aux idéaux au sens 2.

En conclusion, si A est à division et si Λ est un ordre maximal de A, alors tout idéal à gauche non nul de Λ au sens 1 est un idéal à gauche au sens 2 et tout idéal à gauche au sens 2 est de la forme $d^{-1}I$ où d est un entier non nul et I est un idéal à gauche au sens 1.

Les définitions et les résultats de cette section se généralisent aux ordres des algèbres simples centrales quelconques sur $\mathbb{Q}$ ou plus généralement sur un corps de nombres arbitraire. Dans le cas général, où il n'y a pas nécessairement d'involution comme la conjugaison quaternionienne, la relation entre idéaux à gauche et à droite d'un ordre est donnée par l'inversion : à tout idéal à gauche I d'un ordre Λ, on associe un idéal à droite I^{-1} : voir [13, p.21].

4 Ordres principaux

Les ordres les plus simples à étudier et dont les propriétés ressemblent le plus à celles des entiers naturels sont ceux qui satisfont la condition suivante :

1. *Définition :* Un ordre Λ est *principal* si tout idéal à gauche de Λ est de la forme Λx pour un certain $x \in \Lambda$ ou, de manière équivalente, si tout idéal à droite de Λ est de la forme $x\Lambda$ pour un certain $x \in \Lambda$. L'équivalence de ces deux conditions résulte de la relation entre idéaux à gauche et à droite donnée par la conjugaison : si I est un idéal à droite de Λ, alors $\overline{I}$ est un idéal à gauche, et si $\overline{I} = \Lambda x$ pour un certain $x \in \Lambda$, alors $I = \overline{x}\Lambda$.

2. *Exemples :* **a)** L'ordre $\Lambda = M_2(\mathbb{Z})$ de $M_2(\mathbb{Q})$ est principal. Pour le prouver, considérons un idéal à gauche $I \subseteq \Lambda$. Comme $M_2(\mathbb{Z})$ est un module de rang 4 sur $\mathbb{Z}$, l'idéal I, considéré comme module sur $\mathbb{Z}$, est engendré par (au plus) quatre matrices $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$; soit

$$I = \mathbb{Z}.\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \mathbb{Z}.\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \mathbb{Z}.\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} + \mathbb{Z}.\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}.$$

Soit alors V le sous-module de $\mathbb{Z}^2$ engendré par les lignes des matrices $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$:

$$\begin{aligned} V =& \mathbb{Z}.(a_{11}\ \ a_{12}) + \mathbb{Z}.(a_{21}\ \ a_{22}) + \mathbb{Z}.(b_{11}\ \ b_{12}) + \mathbb{Z}.(b_{21}\ \ b_{22}) \\ &+ \mathbb{Z}.(c_{11}\ \ c_{12}) + \mathbb{Z}.(c_{21}\ \ c_{22}) + \mathbb{Z}.(d_{11}\ \ d_{12}) + \mathbb{Z}.(d_{21}\ \ d_{22}) \subseteq \mathbb{Z}^2 \end{aligned}$$

et soit J l'ensemble des matrices dont les deux lignes sont dans V :

$$J = \left\{ \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \ \mid \ (x_{11}\ \ x_{12}) \in V \text{ et } (x_{21}\ \ x_{22}) \in V \right\}.$$

Il est clair que $I \subseteq J$, puisqu'il résulte directement des définitions de V et de J que les matrices $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ sont dans J. Inversement, on a aussi $J \subseteq I$, car si $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in J$, alors :

$$(x_{11}\ \ x_{12}) = \alpha_{11}(a_{11}\ \ a_{12}) + \alpha_{12}(a_{21}\ \ a_{22}) + \beta_{11}(b_{11}\ \ b_{12}) + \cdots + \delta_{12}(d_{21}\ \ d_{22})$$

et

$$(x_{21}\ \ x_{22}) = \alpha_{21}(a_{11}\ \ a_{12}) + \alpha_{22}(a_{21}\ \ a_{22}) + \beta_{21}(b_{11}\ \ b_{12}) + \cdots + \delta_{22}(d_{21}\ \ d_{22})$$

pour certains entiers $\alpha_{11}, \ldots, \delta_{22}$, d'où

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \mathcal{A} + \cdots + \begin{pmatrix} \delta_{11} & \delta_{12} \\ \delta_{21} & \delta_{22} \end{pmatrix} \mathcal{D},$$

ce qui montre que $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in I$, car I est un idéal à gauche. Par conséquent, $I = J$.

Comme V est un sous-module de $\mathbb{Z}^2$, il admet une base d'au plus deux éléments ; soit $(u_1\ \ u_2)$, $(v_1\ \ v_2)$ un système de générateurs de V comme module sur $\mathbb{Z}$, et $\mathcal{U} = \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix} \in \Lambda$. Montrons que $J = \Lambda\mathcal{U}$. D'abord, tout produit $\lambda\mathcal{U}$ est dans J, car les lignes de la matrice $\begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix}$ sont combinaisons linéaires de $(u_1\ \ u_2)$ et $(v_1\ \ v_2)$, et sont donc dans V. Réciproquement, si $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in J$, alors les lignes de cette matrice sont dans V, donc on a

$$\begin{aligned} (x_{11}\ \ x_{12}) &= \lambda_{11}(u_1\ \ u_2) + \lambda_{12}(v_1\ \ v_2) \\ (x_{21}\ \ x_{22}) &= \lambda_{21}(u_1\ \ u_2) + \lambda_{22}(v_1\ \ v_2) \end{aligned}$$

pour certains entiers $\lambda_{11}, \lambda_{12}, \lambda_{21}, \lambda_{22}$, d'où

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix} \in \Lambda\mathcal{U}.$$

Dès lors, $I = \Lambda\mathcal{U}$, ce qui montre que tout idéal à gauche de Λ est principal.

b) Soit $A = (-1,-1)_{\mathbb{Q}}$ et soit Λ l'ordre de A engendré par la base standard de A :

$$\Lambda = \{a_1 1 + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\}.$$

Pour montrer que Λ n'est pas principal, considérons l'idéal à gauche :

$$I = \Lambda(1+i) + \Lambda(i+j).$$

Si $I = \Lambda x$, alors on a en particulier :

$$1 + i = \lambda x \quad \text{et} \quad i + j = \mu x$$

pour certains $\lambda, \mu \in \Lambda$. En prenant la norme des deux membres de la première égalité, on obtient :

$$2 = N(\lambda)N(x),$$

d'où $N(\lambda) = 1$ ou 2. Dans le premier cas, on a, en multipliant les deux membres de la première égalité par le conjugué de λ :

$$\overline{\lambda}(1+i) = x,$$

d'où, en remplaçant dans la deuxième égalité :

$$i + j = \mu\overline{\lambda}(1+i).$$

Alors $(i+j)(1+i)^{-1} = \mu\overline{\lambda} \in \Lambda$. C'est une contradiction, puisque

$$(i+j)(1+i)^{-1} = \tfrac{1}{2}(i+j)(1-i) = \tfrac{1}{2}(1+i+j+k) \notin \Lambda.$$

Dans le second cas, on a $N(x) = 1$, donc $\Lambda x = \Lambda$ puisque tout élément $\lambda \in \Lambda$ s'écrit : $\lambda = (\lambda\overline{x})x$. Dans ce cas, $I = \Lambda$ et l'on peut dès lors trouver des éléments $\lambda, \mu \in \Lambda$ tels que

$$1 = \lambda(1+i) + \mu(i+j).$$

En prenant la norme des deux membres, on obtient alors :

$$1 = N(\lambda)N(1+i) + T(\lambda(1+i)(\overline{i+j})\overline{\mu}) + N(\mu)N(i+j);$$

mais la trace de tout élément de Λ est paire et $N(1+i) = N(i+j) = 2$, donc le deuxième membre de l'égalité précédente est un entier pair. Cette contradiction montre qu'il est absurde de supposer que I est de la forme Λx pour $x \in \Lambda$, donc Λ n'est pas principal. (Le corollaire 3 ci-dessous donne une autre manière de voir que Λ n'est pas principal : il suffit de remarquer que Λ n'est pas maximal (voir le numéro 3 de la section 2)).

c) Soit encore $A = (-1,-1)_{\mathbb{Q}}$ et considérons cette fois l'ordre Θ engendré par $\varepsilon = \frac{1}{2}(1+i+j+k), i, j$ et k :

$$\Theta = \{a_1\varepsilon + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\}$$

(voir l'exemple **b** du numéro 3 de la section 2).

Pour montrer que Θ est principal, on utilise le lemme suivant, qui permet d'établir un algorithme de division euclidienne dans Θ :

Lemme 4 *Pour tout $z \in A$ il existe un élément $\theta \in \Theta$ tel que $N(z-\theta) < 1$.*

Démonstration: Soit $z = z_1 1 + z_2 i + z_3 j + z_4 k \in A$, avec $z_1, \ldots, z_4 \in \mathbb{Q}$. On peut trouver $y_1, \ldots, y_4 \in \mathbb{Z}$ tels que $|z_i - y_i| \leq \frac{1}{2}$ pour $i = 1, \ldots, 4$. Si l'une au moins de ces inégalités est stricte, on pose $\theta = y_1 1 + y_2 i + y_3 j + y_4 k$; alors $\theta \in \Theta$ et $N(z-\theta) = \sum_{i=1}^{4} |z_i - y_i|^2 < 1$. Dans le cas contraire, on a $z_i - y_i = \pm\frac{1}{2}$ pour $i = 1, \ldots, 4$. Quitte à remplacer y_i par $y_i - 1$, on peut supposer $z_i = y_i + \frac{1}{2}$ pour $i = 1, \ldots, 4$; alors

$$z = (y_1 1 + y_2 i + y_3 j + y_4 k) + \varepsilon \in \Theta.$$

On peut donc choisir $\theta = z$. ∎

Remarques : 1) L'élément θ dont il est question ci-dessus n'est en général pas unique : si par exemple $z = \frac{1}{2}(1+i)$, on peut choisir indifféremment $\theta = 0$ ou $\theta = \varepsilon$.

2) Ce lemme entraîne la propriété de division euclidienne (avec reste) suivante : pour $x, y \in \Theta$ avec $y \neq 0$, il existe $q_1, q_2, r_1, r_2 \in \Theta$ tels que :

$$\begin{aligned} x &= yq_1 + r_1 \quad \text{et} \quad N(r_1) < N(y) \\ x &= q_2 y + r_2 \quad \text{et} \quad N(r_2) < N(y). \end{aligned}$$

En effet, le lemme donne des éléments $q_1, q_2 \in \Theta$ tels que $N(y^{-1}x - q_1) < 1$ et $N(xy^{-1} - q_2) < 1$, ce qui donne le résultat désiré avec $r_1 = x - yq_1$ et $r_2 = x - q_2 y$.

Prouvons à présent que Θ est principal. Soit I un idéal à gauche de Θ. Si $I = \{0\}$, alors bien sûr $I = \Theta.0$. Si $I \neq \{0\}$, soit $\lambda \in I$ un élément non nul de norme $N(\lambda)$ minimale. Pour tout $x \in I$ on peut trouver, d'après le lemme, un élément $\theta \in \Theta$ tel que $N(x\lambda^{-1} - \theta) < 1$; alors $x - \theta\lambda$ est un élément de I dont la norme est

$$N(x - \theta\lambda) = N(x\lambda^{-1} - \theta)N(\lambda) < N(\lambda).$$

Vu la minimalité de $N(\lambda)$, on doit avoir $x - \theta\lambda = 0$, donc $x \in \Theta\lambda$, ce qui prouve : $I = \Theta\lambda$.

d) Prenons encore pour exemple l'ordre

$$\Delta = \left\{ a_1 1 + a_2 i + a_3 \frac{1+j}{2} + a_4 \frac{i+k}{2} \mid a_1, \ldots, a_4 \in \mathbb{Z} \right\}$$

de l'algèbre de quaternions $B = (-1, -3)_{\mathbb{Q}}$ (voir l'exemple **c** du numéro 3 de la section 2). Le même raisonnement que dans l'exemple précédent permet de prouver que cet ordre est principal. La démonstration de la propriété de division euclidienne repose sur le lemme suivant :

Lemme 5 *Pour $x, y \in \mathbb{R}$ il existe des nombres entiers $x', y' \in \mathbb{Z}$ tels que*

$$(x - x')^2 + (x - x')(y - y') + (y - y')^2 \leq \tfrac{1}{3}.$$

Démonstration: La démonstration la plus simple est géométrique. Dans le plan $\mathbb{R}^2$, on considère le réseau R engendré par $(1, 0)$ et $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, c'est-à-dire :

$$R = (1, 0)\mathbb{Z} + (\tfrac{1}{2}, \tfrac{\sqrt{3}}{2})\mathbb{Z}.$$

La figure 1 montre quelques points de ce réseau. L'inspection de cette figure montre que

les points du plan qui sont les plus éloignés d'un point de R sont les centres de gravité des triangles équilatères dont les sommets sont les points de R ou, ce qui revient au même, les centres des cercles circonscrits à ces triangles. Or, le rayon du cercle circonscrit est $\frac{\sqrt{3}}{3}$; dès lors, tout point du plan est à une distance d'au plus $\frac{\sqrt{3}}{3}$ d'un point du réseau R. Par conséquent, pour $x, y \in \mathbb{R}$ on peut trouver $x', y' \in \mathbb{Z}$ tels que la distance entre les points $(1,0)x + (\frac{1}{2}, \frac{\sqrt{3}}{2})y$ et $(1,0)x' + (\frac{1}{2}, \frac{\sqrt{3}}{2})y'$ soit inférieure ou égale à $\frac{\sqrt{3}}{3}$, c'est-à-dire :

$$\left\| \Big((x-x') + \tfrac{1}{2}(y-y'), \tfrac{\sqrt{3}}{2}(y-y') \Big) \right\| \leq \tfrac{\sqrt{3}}{3}.$$

Le lemme en résulte, car la norme du vecteur au premier membre est :

$$\sqrt{\big((x-x') + \tfrac{1}{2}(y-y')\big)^2 + \tfrac{3}{4}(y-y')^2} = \sqrt{(x-x')^2 + (x-x')(y-y') + (y-y')^2}.$$

■

Corollaire 2 *Pour tout $z \in B$ il existe un élément $\delta \in \Delta$ tel que $N(z-\delta) < 1$.*

Démonstration: Soit $z = z_1 1 + z_2 i + z_3 \frac{1+j}{2} + z_4 \frac{i+k}{2} \in B$, avec $z_1, \ldots, z_4 \in \mathbb{Q}$. D'après le lemme, on peut trouver $z'_1, \ldots, z'_4 \in \mathbb{Z}$ tels que

$$\begin{aligned} (z_1 - z'_1)^2 + (z_1 - z'_1)(z_3 - z'_3) + (z_3 - z'_3)^2 &\leq \tfrac{1}{3} \\ (z_2 - z'_2)^2 + (z_2 - z'_2)(z_4 - z'_4) + (z_4 - z'_4)^2 &\leq \tfrac{1}{3}. \end{aligned}$$

On pose alors $\delta = z'_1 1 + z'_2 i + z'_3 \frac{1+j}{2} + z'_4 \frac{i+k}{2}$; un simple calcul donne :

$$\begin{aligned} N(z-\delta) =& (z_1 - z'_1)^2 + (z_1 - z'_1)(z_3 - z'_3) + (z_3 - z'_3)^2 \\ &+ (z_2 - z'_2)^2 + (z_2 - z'_2)(z_4 - z'_4) + (z_4 - z'_4)^2 \leq \tfrac{2}{3}. \end{aligned}$$

■

Le fait que l'ordre Δ est principal se déduit de ce résultat par les mêmes arguments que pour l'ordre Θ dans l'exemple précédent.

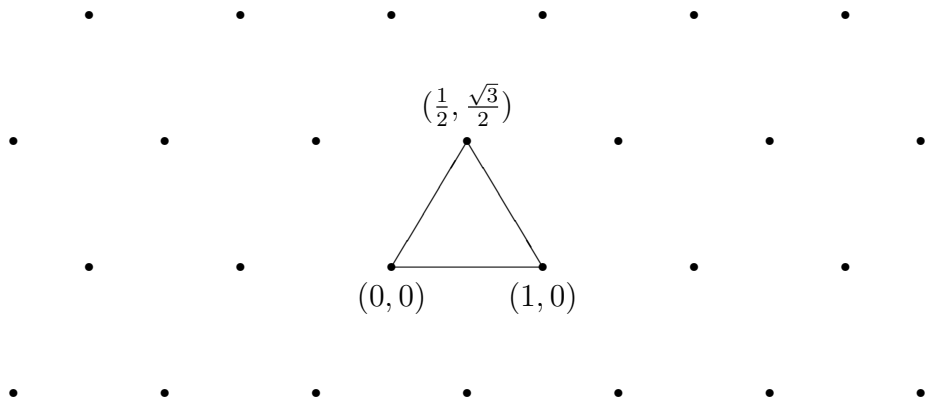

FIG. 1 – Quelques points de R

3. *Unicité des ordres principaux :* Il faut se garder de croire que toute algèbre de quaternions rationnelle contient un ordre principal ; l'existence d'un tel ordre est même tout-à-fait exceptionnelle parmi les algèbres de quaternions du type $(a, b)_{\mathbb{Q}}$ avec $a, b < 0$ (voir les notes à la fin de cette section). Cependant, lorsqu'un tel ordre existe, il possède des propriétés remarquables ; on se propose de prouver ici que les ordres principaux sont maximaux et qu'ils sont uniques (à conjugaison près par un élément inversible) dans leur algèbre de quaternions.

Théorème 4 *Soient Λ, Λ' deux ordres d'une algèbre de quaternions A. Si Λ est principal, alors il existe un élément inversible $a \in A$ tel que $a\Lambda' a^{-1} \subseteq \Lambda$. En particulier, le discriminant réduit $d(\Lambda)$ divise $d(\Lambda')$.*

Démonstration: La seconde affirmation découle directement de la première, par la proposition 4, car le discriminant de Λ' est égal au discriminant de $a\Lambda' a^{-1}$, puisque $T(a(e'_i e'_j)a^{-1}) = T(e'_i e'_j)$ pour toute base $(e'_1, \ldots, e'_4)$ de Λ'.

Pour démontrer la première affirmation, on considère l'ensemble

$$\Lambda\Lambda' = \{\textstyle\sum_i \lambda_i \lambda'_i \mid \lambda_i \in \Lambda, \lambda'_i \in \Lambda'\};$$

si $(e_1, \ldots, e_4)$ (resp. $(e'_1, \ldots, e'_4)$) est une base de Λ (resp. Λ') sur $\mathbb{Z}$, on peut aussi décrire $\Lambda\Lambda'$ de la manière suivante :

$$\Lambda\Lambda' = \{\textstyle\sum_{i,j=1}^{4} \alpha_{ij} e_i e'_j \mid \alpha_{ij} \in \mathbb{Z}\},$$

ce qui montre que cet ensemble est un sous-$\mathbb{Z}$-module de type fini de A. Comme $(e_1, \ldots, e_4)$ est aussi une base de A sur $\mathbb{Q}$, on peut écrire :

$$e_i e'_j = \sum_{k=1}^{4} \gamma_{ijk} e_k$$

pour certains nombres rationnels γ_{ijk}. Si d est un commun dénominateur de ces nombres rationnels, alors $de_i e'_j \in \Lambda$ pour $i, j = 1, \ldots, 4$, donc

$$d\Lambda\Lambda' \subseteq \Lambda.$$

Par ailleurs, la définition de $\Lambda\Lambda'$ montre clairement que pour tout $\lambda \in \Lambda$ et tout $x \in \Lambda\Lambda'$, le produit λx est dans $\Lambda\Lambda'$; donc $d\Lambda\Lambda'$ est un idéal à gauche de Λ. Comme on suppose que Λ est principal, on doit avoir

$$d\Lambda\Lambda' = \Lambda a$$

pour un certain $a \in \Lambda$. En particulier, comme $d = d.1.1 \in d\Lambda\Lambda'$, l'idéal Λa contient un élément non nul de $\mathbb{Q}$, donc a doit être inversible dans A. Considérons alors l'ensemble

$$\Gamma = \{\gamma \in A \mid d\Lambda\Lambda'\gamma \subseteq d\Lambda\Lambda'\}.$$

Il est clair que $\Lambda' \subseteq \Gamma$. D'autre part, pour $\gamma \in \Gamma$ on a, vu que $d\Lambda\Lambda' = \Lambda a$:

$$\Lambda a\gamma \subseteq \Lambda a;$$

en particulier,

$$a\gamma \in \Lambda a,$$

d'où $\gamma \in a^{-1}\Lambda a$ et donc

$$\Gamma \subseteq a^{-1}\Lambda a.$$

Par conséquent,

$$a\Lambda' a^{-1} \subseteq \Lambda.$$

■

Corollaire 3 *Tout ordre principal d'une algèbre de quaternions est maximal. Si une algèbre de quaternions A contient un ordre principal Λ, alors tout ordre maximal de A est de la forme $a\Lambda a^{-1}$ pour un certain élément inversible $a \in A$.*

Démonstration: Soit Λ un ordre principal d'une algèbre de quaternions A, et soit Θ un ordre maximal contenant Λ ; alors $d(\Theta)$ divise $d(\Lambda)$, par la proposition 4, et $d(\Lambda)$ divise $d(\Theta)$ par le théorème précédent. Dès lors $d(\Theta) = d(\Lambda)$, et $\Lambda = \Theta$ par la proposition 4, ce qui montre que Λ est maximal.

Si Λ' est un ordre maximal de A, alors le théorème précédent livre un élément inversible $a \in A$ tel que $a\Lambda' a^{-1} \subseteq \Lambda$. Alors $\Lambda' \subseteq a^{-1}\Lambda a$, et comme Λ' est maximal, les inclusions précédentes sont des égalités. ∎

Par exemple, dans l'algèbre de quaternions $B = (-1,-3)_{\mathbb{Q}}$, les ordres maximaux Δ et Φ décrits dans l'exemple **c** du numéro 3 de la section 2 sont conjugués par un élément inversible de B : on peut vérifier que $\Phi = a\Delta a^{-1}$ avec $a = 1 + i + j + k$.

4. *Représentation d'entiers par la forme norme d'un ordre principal :* On se propose à présent de déterminer quels nombres entiers sont *représentables* par la forme norme d'un ordre Λ d'une algèbre de quaternions A, c'est-à-dire pour quels nombres $z \in \mathbb{Z}$ l'équation $N(\lambda) = z$ admet une solution $\lambda \in \Lambda$. Les résultats obtenus jusqu'à présent donnent une voie pour répondre à ce type de question pour $z = \pm p$ avec p premier, mais ils ne permettent pas de faire la distinction entre $+p$ et $-p$; dès lors, nous limiterons notre discussion au cas où $A = (a,b)_{\mathbb{Q}}$ avec $a, b < 0$: dans ce cas, la forme norme est définie positive et ne représente donc pas les nombres négatifs. (On trouvera dans les notes à la fin de cette section quelques indications sur le cas où la forme norme est indéfinie).

Théorème 5 *Soit Λ un ordre principal d'une algèbre de quaternions $A = (a,b)_{\mathbb{Q}}$ avec $a, b < 0$. Pour tout nombre entier $n > 0$, il existe un élément $\lambda \in \Lambda$ tel que $N(\lambda) = n$.*

Démonstration: Il suffit de démontrer le théorème pour n un nombre premier, car si $n = p_1 \dots p_r$ est la décomposition de n en produit de facteurs premiers (non nécessairement distincts) et si $\lambda_1, \dots, \lambda_r \in \Lambda$ sont tels que $N(\lambda_i) = p_i$ pour $i = 1, \dots, r$, alors, vu la multiplicativité de la norme :

$$N(\lambda_1 \dots \lambda_r) = n.$$

Soit donc $n = p$, un nombre premier. Si p ne divise pas le discriminant réduit $d(\Lambda)$, alors $\Lambda/p\Lambda \simeq M_2(\mathbb{F}_p)$, d'après le théorème 2. Or, $M_2(\mathbb{F}_p)$ contient des idéaux à gauche non triviaux — par exemple l'idéal des matrices dont la seconde colonne est nulle — donc il en est de même de $\Lambda/p\Lambda$. Soit I un idéal à gauche non trivial de $\Lambda/p\Lambda$ et soit J son image inverse dans Λ par l'application canonique $\Lambda \to \Lambda/p\Lambda$, c'est-à-dire :

$$J = \{\lambda \in \Lambda \mid \lambda + p\Lambda \in I\}.$$

L'ensemble J est alors un idéal à gauche de Λ, et comme I est non trivial on a

$$\Lambda \supsetneq J \supsetneq p\Lambda.$$

Comme Λ est principal, on peut trouver $x \in \Lambda$ tel que $J = \Lambda x$.

Montrons que $N(x) = p$. Comme $p \in p\Lambda \subset \Lambda x$, on peut écrire :

$$p = \lambda x \tag{6}$$

pour un certain $\lambda \in \Lambda$, d'où, en prenant la norme des deux membres :

$$p^2 = N(\lambda)N(x),$$

ce qui montre que $N(x)$ divise p^2. Si $N(x) = 1$, alors $\Lambda = \Lambda x$ puisque tout élément $y \in \Lambda$ s'écrit alors :

$$y = (y\overline{x})x \in \Lambda x;$$

cela contredit l'inclusion stricte $\Lambda \supsetneq J$.

De même, si $N(x) = p^2$, alors $N(\lambda) = 1$, d'où, en multipliant par le conjugué de λ les deux membres de l'égalité (6) :

$$x = p\overline{\lambda} \in p\Lambda,$$

ce qui entraîne : $J \subseteq p\Lambda$, contrairement à l'inclusion stricte $J \supsetneq p\Lambda$. Comme $N(x)$ est un diviseur propre de p^2, positif et différent de 1, on doit avoir $N(x) = p$, comme annoncé.

Dans le cas où le nombre premier p divise le discriminant réduit $d(\Lambda)$, le raisonnement est semblable : on utilise le théorème 3 pour obtenir un idéal non trivial I de $\Lambda/p\Lambda$ (l'idéal I est bilatère, cette fois), que l'on relève en un idéal J de Λ (encore bilatère) strictement compris entre Λ et $p\Lambda$. Comme Λ est principal, on peut trouver $x \in \Lambda$ tel que $J = \Lambda x$, et les mêmes arguments que ci-dessus montrent que $N(x) = p$. ■

Soit par exemple Θ l'ordre de l'algèbre de quaternions $(-1,-1)_{\mathbb{Q}}$ décrit dans le numéro 3 de la section 2, dont on a montré au numéro 2 ci-dessus qu'il est principal :

$$\Theta = \{a_1\varepsilon + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\},$$

où $\varepsilon = \frac{1+i+j+k}{2}$. un calcul direct donne la forme norme de Θ :

$$N(a_1\varepsilon + a_2 i + a_3 j + a_4 k) = a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_1a_2 + a_1a_3 + a_1a_4.$$

Dès lors, le théorème précédent montre que tout entier positif est représenté par cette forme, c'est-à-dire que pour tout entier $n > 0$ l'équation

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_1X_2 + X_1X_3 + X_1X_4 = n$$

admet une solution en nombres entiers.

De même, si l'on applique le théorème précédent à l'ordre

$$\Delta = \left\{ a_1 1 + a_2 i + a_3\frac{1+j}{2} + a_4\frac{i+k}{2} \mid a_1, \ldots, a_4 \in \mathbb{Z} \right\} \subset (-1,-3)_{\mathbb{Q}},$$

dont on a vu au numéro 2 ci-dessus qu'il est principal, on conclut que tout entier positif est représenté par la forme

$$N(\delta) = a_1^2 + a_1a_3 + a_3^2 + a_2^2 + a_2a_4 + a_4^2,$$

c'est-à-dire que pour tout entier $n > 0$ l'équation

$$X_1^2 + X_1X_3 + X_3^2 + X_2^2 + X_2X_4 + X_4^2 = n$$

admet une solution en nombres entiers.

5. *Le théorème des quatre carrés :* Le théorème 5 ne s'applique pas directement au cas de la forme quadratique $X_1^2 + X_2^2 + X_3^2 + X_4^2$, qui est la forme norme de l'ordre

$$\Lambda = \{a_1 1 + a_2 i + a_3 j + a_4 k \mid a_1, \ldots, a_4 \in \mathbb{Z}\} \subset (-1,-1)_{\mathbb{Q}},$$

puisque celui-ci n'est pas principal. Cependant, la relation suivante entre Λ et Θ permet d'en déduire le théorème des quatre carrés :

Lemme 6 *Pour tout élément $\theta \in \Theta$, il existe un élément $u \in \Theta$ tel que $N(u) = 1$ et $u\theta \in \Lambda$.*

Démonstration: Si $\theta \in \Lambda$, alors on peut évidemment choisir $u = 1$. Si $\theta \notin \Lambda$, soit

$$\theta = \theta_1 \varepsilon + \theta_2 i + \theta_3 j + \theta_4 k$$

avec θ_1 impair ; alors

$$2\theta = \theta_1 1 + (\theta_1 + 2\theta_2) i + (\theta_1 + 2\theta_3) j + (\theta_1 + 2\theta_4) k,$$

donc toutes les coordonnées de 2θ par rapport à la base standard sont impaires. Modulo 4, ces coordonnées peuvent donc toutes être représentées par $+1$ ou par -1. Il en est bien sûr de même du conjugué $2\overline{\theta}$; soit donc

$$2\overline{\theta} = \alpha + 4\lambda$$

pour un certain quaternion α de la forme $\pm 1 \pm i \pm j \pm k$ et un certain $\lambda \in \Lambda$. En posant $u = \frac{\alpha}{2}$, on a alors $u \in \Theta$ et $N(u) = 1$. De plus,

$$u\theta = (\overline{\theta} - 2\lambda)\theta = N(\theta) - \lambda(2\theta) \in \Lambda.$$

■

Théorème 6 (Lagrange) *Tout entier positif est somme de quatre carrés.*

Démonstration: D'après ce qui précède, l'équation $N(\theta) = n$ admet une solution $\theta \in \Theta$ pour tout entier $n > 0$. Si $u \in \Theta$ est tel que $N(u) = 1$ et $u\theta \in \Lambda$, alors $N(u\theta) = n$, ce qui montre que l'équation $N(\lambda) = n$ admet au moins une solution $\lambda \in \Lambda$. ■

6. *Notes :* Si Λ est un ordre quelconque d'une algèbre de quaternions A (ou plus généralement d'une algèbre simple centrale quelconque), on définit sur l'ensemble des idéaux à gauche (resp. à droite) de Λ une relation d'équivalence par homothétie : deux idéaux à gauche (resp. à droite) I et J sont équivalents s'il existe un élément inversible $a \in A$ tel que

$$I = Ja \qquad (\text{resp. } I = aJ).$$

(La notion d'idéal utilisée pour cette définition est de préférence celle indiquée dans les notes de la section 3). En utilisant la relation entre idéaux à gauche et à droite donnée par la conjugaison quaternionienne (ou, dans un cas plus général, par l'inversion : voir les notes de la section 3), on peut montrer que le nombre de classes d'équivalence d'idéaux à

gauche est le même que le nombre de classes d'équivalence d'idéaux à droite ; ce nombre est noté habituellement $h(\Lambda)$ et est appelé *nombre de classes de* Λ.

Si on se limite aux ordres maximaux des algèbres de quaternions à division, où les deux notions d'idéaux coïncident à peu près (voir les notes de la section 3), on voit qu'un ordre Λ est principal si et seulement si $h(\Lambda) = 1$, puisque cette dernière condition signifie que tout idéal à gauche de Λ est équivalent à Λ et est donc de la forme Λa pour un certain $a \in A$. (L'élément a est bien sûr dans Λ si l'idéal est contenu dans Λ).

Pour tout ordre Λ d'une algèbre de quaternions à division, le nombre de classes $h(\Lambda)$ est fini [11, §26] ; de plus, les ordres maximaux ont tous le même nombre de classes, appelé, par abus de langage, *nombre de classes de l'algèbre* A [13, p.26]. Il résulte d'un théorème d'Eichler [13, p.99] que ce nombre est 1 pour toute algèbre de quaternions $(a, b)_{\mathbb{Q}}$ avec $a > 0$ ou $b > 0$; dès lors, tout ordre maximal d'une algèbre de quaternions rationnelle dont la forme norme est indéfinie est principal. Dans le cas où $A = (a, b)_{\mathbb{Q}}$ avec $a, b < 0$, certaines formules donnent le nombre de classes de A : voir [13, p.152]. De ces formules, il ressort que seules cinq algèbres de ce type contiennent des ordres (maximaux) principaux : ce sont, outre les algèbres $(-1, -1)_{\mathbb{Q}}$ et $(-1, -3)_{\mathbb{Q}}$ déjà citées, les algèbres $(-2, -5)_{\mathbb{Q}}$, $(-1, -7)_{\mathbb{Q}}$ et $(-2, -13)_{\mathbb{Q}}$, de discriminants respectifs 5, 7 et 13.

En ce qui concerne la représentation des entiers par la forme norme d'un ordre maximal (principal) Λ d'une algèbre de quaternions $A = (a, b)_{\mathbb{Q}}$ avec $a > 0$ ou $b > 0$, la seule difficulté est de prouver que -1 est représenté. En effet, les arguments du numéro 4 de cette section montrent que pour tout entier n, l'un au moins des deux entiers $+n$ ou $-n$ est de la forme $N(\lambda)$ avec $\lambda \in \Lambda$. Si l'on montre que $-1 = N(\alpha)$ pour un certain $\alpha \in \Lambda$, alors on a : $n, -n = N(\lambda), N(\alpha\lambda)$, et par conséquent tout nombre entier, positif ou négatif, est représenté par la forme norme de Λ.

Nous ne connaissons malheureusement aucune démonstration élémentaire de ce résultat (qui est une conséquence d'un théorème général d'Eichler [13, p.90]). L'idée est de trouver, en appliquant le théorème chinois des restes, un entier $z \in \mathbb{Z}$ tel que $z^2 + 4$ soit non-carré modulo p pour tout nombre premier $p \neq 2$ qui divise le discriminant de A et tel que, de plus, $z \equiv 1 \bmod 8$ si le discriminant de A est pair. De cette manière, $z^2 + 4$ est non-carré dans le corps des nombres p-adiques $\mathbb{Q}_p$, pour tout p premier qui divise le discriminant de A. Soit alors $K = \mathbb{Q}(\sqrt{z^2 + 4})$. La partie non-élémentaire de la démonstration consiste à voir que la condition sur $z^2 + 4$ assure que l'algèbre A devient une algèbre de matrices si l'on étend les scalaires de $\mathbb{Q}$ à K. L'algèbre A contient alors un sous-corps isomorphe à K. On considère alors l'élément $\alpha = (z + \sqrt{z^2 + 4})/2 \in A$. Cet élément est racine de l'équation irréductible $X^2 - zX - 1$, donc sa norme est -1 et sa trace est $z \in \mathbb{Z}$. Cet élément est donc entier sur $\mathbb{Z}$, et l'on peut montrer qu'il existe un ordre maximal de A qui le contient. Comme tous les ordres maximaux de A sont principaux et conjugués, ils contiennent tous un élément de norme -1 (et de trace z).

Outre le nombre de classes, on définit aussi le nombre de types d'ordres maximaux d'une algèbre de quaternions A : c'est le nombre de classes de conjugaison d'ordres maximaux, c'est-à-dire le nombre de classes d'équivalence d'ordres maximaux, en considérant deux ordres Λ et Λ' comme équivalents s'il existe un élément inversible $a \in A$ tel que $\Lambda' = a\Lambda a^{-1}$. Il n'est pas difficile de montrer que ce nombre est inférieur ou égal au nombre de classes de A (voir [13, p.26] ou [4, Chap.6,§8]). Cela généralise le corollaire 3, suivant lequel tous les ordres maximaux d'une algèbre de quaternions sont conjugués si celle-ci contient un ordre principal.

Signalons enfin que les techniques développées dans ces notes peuvent aussi être uti-

lisées pour déterminer le nombre de représentations d'un entier comme somme de quatre carrés (formule de Jacobi) ou le nombre de représentations d'un entier par la forme norme d'un ordre principal [9].

Références

[1] Albert, A.A. : *Structure of Algebras*, Amer. Math. Soc. Coll. Pub. 24, Amer. Math. Soc., Providence, R.I., 1961.

[2] Bien, F. : Constructions of Telephone Networks by Group Representations, *Notices Amer. Math. Soc.* **36** (1989) 5–22.

[3] Blanchard, A. : *Les Corps non Commutatifs*, Coll. Sup, Presses Univ. France, Paris, 1972.

[4] Deuring, M. : *Algebren* (2.Auf.), Ergebnisse d. Math.41, Springer, Berlin, 1968.

[5] Dickson, L.E. : *Algebras and their Arithmetics*, Chicago, 1923.

[6] Draxl, P. : *Skew Fields*, London Math. Soc. Lecture Notes Series 81, Cambridge Univ. Press, Cambridge, 1983.

[7] Hardy, G.H. and Wright, E.M. : *An Introduction to the Theory of Numbers*, Oxford Univ. Press, Oxford, 1979.

[8] Lam, T.-Y. : *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading, Mass., 1973.

[9] Pays, I. : Arbres, ordres maximaux et formes quadratiques entières, en préparation.

[10] Pierce, R.S. : *Associative Algebras*, Graduate Texts in Math. 88, Springer, New York, 1982.

[11] Reiner, I. : *Maximal Orders*, Academic Press, London, 1975.

[12] Samuel, P. : *Théorie Algébrique des Nombres*, Coll. Méthodes, Hermann, Paris, 1967.

[13] Vignéras, M.-F. : *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Math. 800, Springer, Berlin, 1980.

[14] Witt, E. : Ueber ein Gegenbeispiel zum Normensatz, *Math. Z.* **39** (1935) 462–467.