Echanges

Sur les anneaux $\mathbf{Z}[\sqrt{a}]$

Jacques Bouteloup
Rouen

L'article de Guy Heuzé, dans le *Bulletin* n°381, a le mérite d'attirer l'attention sur des anneaux qui, dans un cas particulier évoqué ci-dessous, ne sont pas usuellement considérés. Mais il utilise une définition de $\mathbf{Z}[\sqrt{a}]$ qui n'est pas la définition classique, ce qui risque d'entraîner une confusion.

Tous les auteurs que j'ai lus à ce sujet, et notamment Châtelet, Bourbaki et Le Lionnais, sont d'accord pour désigner par $\mathbf{Z}[\sqrt{a}]$, a étant un élément de $\mathbf{Z}$ *sans facteur carré* (appelé par Châtelet *semi-premier*), l'anneau des entiers du corps quadratique $\mathbf{Q}[\sqrt{a}]$ (ensemble des $x + y\sqrt{a}$, $x \in \mathbf{Q}$, $y \in \mathbf{Q}$), ce qui est un cas particulier d'une notion générale, se caractérisant ici comme l'ensemble des éléments α du corps, de conjugué $\overline{\alpha}$, dont la trace $\alpha + \overline{\alpha}$ et la norme $N(\alpha) = \alpha.\overline{\alpha}$ sont éléments de $\mathbf{Z}$.

On démontre aisément que, lorsque *a n'est pas multiple de 4 plus 1*, c'est l'ensemble des $x + y\sqrt{a}$, $x \in \mathbf{Z}$, $y \in \mathbf{Z}$, mais que lorsque *a est multiple de 4 plus 1*, il faut ajouter à l'ensemble précédent celui des $\frac{x}{2} + \frac{y\sqrt{a}}{2}$ avec x et y impairs. Bien entendu, lorsque a est négatif, on peut introduire $b = -a$, notant l'anneau $\mathbf{Z}[i\sqrt{b}]$. Le cas particulier est donc dans ce cas b multiple de 4 plus 3.

L'intérêt de la définition usuelle, qui diffère donc de celle de Guy Heuzé pour $a \equiv 1 \pmod 4$, est, non seulement d'obtenir un cas particulier d'une notion générale, mais aussi d'aboutir à la structure d'*anneau de Dedekind*, entraînant des conséquences très intéressantes. Dans la suite, nous nous limiterons à $\mathbf{Z}[i\sqrt{b}]$ avec $b > 0$, distinguant $b = 3$ et $b \equiv 3$, modulo 4.

Un anneau de Dedekind est notamment *intégralement clos*. Par contre, l'anneau **A** des $x + iy\sqrt{4k+3}$ ($x \in \mathbf{Z}$, $y \in \mathbf{Z}$, k fixé sur **N**) ne possède pas cette propriété, l'élément du corps obtenu pour $x = y = 1/2$ étant racine de $x^2 - x + k + 1$ à coefficients dans **Z**, bien que n'appartenant pas à **A**.

La démonstration de Guy Heuzé sur l'anneau des $x + iy\sqrt{b}$ ($x \in \mathbf{Z}$, $y \in \mathbf{Z}$, b fixé sur N) est en fait valable pour tout b impair ≥ 3. Il n'est pas difficile de l'étendre au cas de b pair, 2 étant toujours irréductible et ne divisant pas $2 + i\sqrt{b}$ et $2 - i\sqrt{b}$, puisque $2(x + iy\sqrt{b}) = 2 + i\sqrt{b}$ conduit à $2y = 1$ impossible, bien qu'il divise le produit égal à $4 + b$, pair.

Un anneau de Dedekind est *principal* lorqu'il est *factoriel*. Il y a donc 3 cas possibles : *euclidien, principal non euclidien et non factoriel*. La démonstration de Guy Heuzé ainsi complétée prouve donc que, à part les cas usuels de $b = 1$ ou 2, le premier et le deuxième cas ne peuvent être obtenus que lorque $b \equiv 3$, modulo 4.

Dans *«Les nombres remarquables»*, Le Lionnais indique que $\mathbf{Z}[i\sqrt{b}]$, au sens usuel, est *euclidien* pour $b = 1, 2, 3, 7, 11$, *principal sans être euclidien* pour $b = 19, 43, 67, 163$, *non factoriel* dans tous les autres cas. La démonstration date de 1966, mais on savait déjà avant cette date que les 5 premières valeurs indiquées de b conduisaient à des anneaux euclidiens, avec la fonction $N(\alpha)$. C'est notamment proposé en exercice dans *l'Algèbre* de Bourbaki, chapitre VII, paragraphe 1, exercice 11, dans l'édition de 1952.

Je ne comprends donc pas que Dieudonné (dont je n'ai pas lu le livre), déclare qu'il se pose un problème d'anneau euclidien pour les valeurs 3, 7, 11 de b, la réponse étant *positive* avec la définition usuelle, dans Bourbaki, dont Dieudonné est l'un des plus illustres fondateurs, et négative dans le sens de Guy Heuzé, de façon évidente, un anneau euclidien étant principal, donc de Dedekind, donc intégramlement clos, contrairement à ce qui a été montré de façon immédiate ci-dessus.

L'utilisation de la définition usuelle justifie l'emploi constant dans les exemples de $\mathbf{Z}[i\sqrt{5}]$, 5 étant la plus petite valeur de b caractérisant un cas non factoriel.

N.D.L.R.

D'intéressantes précisions nous sont également apportées par Michel GUILLEMOT (Toulouse), qui rappelle tout d'abord la citation exacte de Jean DIEUDONNÉ : *«Lorsqu'on veut généraliser de la même manière la division euclidienne dans l'anneau* $\mathbb{Z}[\sqrt{D}]$, *on en déduit des théorèmes tout à fait analogues, malheureusement on a démontré que ce n'est possible que pour un nombre* ***fini*** *d'entiers D non divisibles par un carré ; pour* $D < 0$, *les valeurs possibles de D sont -1, -3, -7 et -11. En fait, il y a une infinité de valeurs de D pour lesquelles il n'y a pas de décomposition unique en facteurs premiers ; par exemple pour* $D = -5$, *on a* $9 = 3.3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ *et on peut prouver que* 3, $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ *sont premiers» (p.191)*

M.GUILLEMOT donne par ailleurs l'excellente référence bibliographique de François LE LIONNAIS :"Les nombres remarquables", où l'on peut lire : *«Corps quadratiques complexes : Il existe neuf valeurs de d telles que le nombre de classes de diviseurs de* $\mathbb{Q}[\sqrt{-d}]$ *soit égal à 1, c'est-à-dire dans lesquels tout entier se décompose de manière unique, à l'ordre près, en un produit de facteurs premiers. Ce sont d = 1, 2, 3, 7, 11, 19, 43, 67 et 163. Gauss avait déjà déterminé ces valeurs, mais il a fallu attendre 1966 pour que l'on démontre qu'il n'en existait pas d'autres. On notera également que* $\mathbb{Q}[\sqrt{-d}]$ *n'est pas euclidien» (p.67)*

Notre collègue cite enfin le «Défi algébrique» de Claude Mutafian, qui démontre (volume 2) de nombreux résultats sur les extensions quadratiques d'entiers :

«Pour $n \leq -3$ *ou* $n = 1 \pmod 4$, $\mathbb{Z}[\sqrt{n}]$ *n'est pas factoriel»* (p.253) ; *«Si 2 est irréductible dans* $\mathbb{Z}[\sqrt{n}]$, *cet anneau n'est pas factoriel.»*