6 Anneaux euclidiens, principaux, factoriels

On cherche à dégager et étudier des classes d'anneaux intègres qui ont des propriétés arithmétiques similaires à celles de $\mathbf{Z}$ et $\mathbf{K}[X]$ (où $\mathbf{K}$ est un corps).

Parmi les motivations que l'on peut dégager :

- c'est joli et intéressant !
- cela peut permettre de résoudre des problèmes d'arithmétique sur $\mathbf{Z}$ (*cf.* la section consacrée à la motivation historique ci-dessous, ainsi que la section 6.4) ;
- (à plus long terme) dans le cadre de la géométrie algébrique, ces classes correspondent à des objets ayant de très bonnes propriétés géométriques ;
- cela peut *ne pas* permettre de résoudre des problèmes d'arithmétique sur $\mathbf{Z}$ (*cf.* encore une fois la section consacrée à la motivation historique ci-dessous, ainsi que la section 6.4...) ; cela apporte un éclairage instructif et conceptuel sur le fait que l'arithmétique est difficile, et peut entraîner le développement d'outils nouveaux et utiles (la notion abstraite d'idéal d'un anneau est née comme cela)

6.1 Motivation historique

Cette partie peut être réservée à une seconde lecture.

Lorsque l'on souhaite démontrer des résultats portant sur l'arithmétique de $\mathbf{Z}$, il peut s'avérer extrêmement utile de travailler sur un anneau plus gros ; ceci est illustré notamment dans la section 6.4 ci-dessous.

Une autre illustration frappante de ce procédé est la tentative de démonstration du « dernier théorème de Fermat » proposée en 1847 par le mathématicien Gabriel Lamé. Rappelons qu'il s'agit de démontrer l'énoncé suivant : pour tout entier $n \geqslant 3$, l'équation

$$x^n + y^n = z^n$$

n'a pas de solutions $(x, y, z) \in \mathbf{Z}^3$ non triviales (une solution (x, y, z) est dite triviale si $x\,y\,z = 0$, c'est-à-dire l'une des trois inconnues est nulle). L'approche proposée par Lamé était erronée [12], mais l'erreur commise était assez subtile, tout à fait « digne » du grand mathématicien qu'était Lamé et au final très intéressante, puisqu'elle est concomitante à la naissance de concepts fondamentaux en théorie des anneaux.

Avant d'expliquer les grandes lignes de l'idée de Lamé, rappelons l'énoncé suivant :

Proposition. *Soit $n \geqslant 2$ un entier, b et c des entiers relatifs premiers entre eux et $a = b\,c$. On suppose que $|a|$ est une puissance n-ème (c'est-à-dire s'écrit α^n où α est un entier relatif). Alors $|b|$ et $|c|$ sont aussi des puissances n-ème.*

La proposition se généralise à un produit quelconque de facteurs supposés premiers entre eux 2 à 2. Cette proposition ainsi que sa généralisation se démontrent à partir du théorème de

12. En fait l'énoncé ci-dessus n'a finalement été démontré dans toute sa généralité qu'en 1994 par Andrew Wiles.

décomposition en facteurs premiers. L'un des aspects les plus cruciaux de la démonstration est que l'on utilise l'*unicité* de la décomposition. Cette proposition se généralise à tout anneau intègre admettant une théorème de décomposition en irréductibles aux propriétés similaires à celui qui existe sur $\mathbf{Z}$; en particulier, et c'est absolument fondamental, on doit avoir en un certain sens unicité d'une telle décomposition. De tels anneaux sont appelés *anneaux factoriels* et seront définis plus précisément ci-dessous.

De fait, on a la généralisation de la proposition ci-dessus.

Proposition. *Soit A un anneau factoriel, soit $n \geqslant 2$ un entier, b et c des éléments de A premiers entre eux et $a = bc$. On suppose que a est associé à une puissance n-ème (c'est-à-dire à un élément qui s'écrit α^n où $\alpha \in A$). Alors b et c sont aussi associés à des puissances n-ème.*

Là encore, on peut généraliser à un produit fini de facteurs supposés premiers entre eux deux à deux.

L'idée de Lamé pour démontrer qu'il n'y a pas de solutions entières non triviales à l'équation $x^p + y^p = z^p$ pour p premier impair [13] est d'écrire l'équation sous la forme

$$\prod_{i=0}^{p-1} (x + \zeta_p^i\, y) = z^p \tag{6.1}$$

où ζ_p est une racine primitive p-ème de l'unité.

Ceci permet de voir l'équation (6.1) comme une égalité dans l'anneau noté $\mathbf{Z}[\zeta_p]$, défini comme le sous-anneau de $\mathbf{C}$ image de $\mathbf{Z}[X]$ par l'unique morphisme $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur ζ_p. Ainsi $\mathbf{Z}[\zeta_p] = \{P(\zeta_p), \quad P \in \mathbf{Z}[X]\}$.

Par des manipulations relativement standards, on montre que s'il existe un triplet $(x, y, z) \in \mathbf{Z}^3$ vérifiant (6.1), alors il en existe un tel que les éléments de $\mathbf{Z}[\zeta]$

$$x + \zeta_p\, y,\ x + \zeta_p^2\, y, \ldots, x + \zeta_p^{p-1}\, y \tag{6.2}$$

sont premiers entre eux deux à deux. Comme leur produit est d'après (6.1) une puissance p-ème, chacun de ces éléments est associés à une puissance p-ème. De ce dernier fait on arrive à déduire une contradiction.

L'idée de Lamé est très séduisante. Sa faiblesse fondamentale réside cependant dans l'étape consistant à montrer que les éléments (6.2) sont des puissances p-ème. En fait, on applique à ce stade la (généralisation de la) proposition 6.1. Le (*gros !*) problème est que l'anneau $\mathbf{Z}[\zeta_p]$ n'est en général pas factoriel. À l'époque où Lamé propose sa démonstration, l'existence d'anneaux non factoriels n'était vraiment pas une évidence, et il semblait naturel

13. Rappelons que sachant que le dernier théorème de Fermat est vrai pour $n = 4$, pour démontrer le théorème en toute généralité, il suffit de considérer des exposants premiers impairs

de penser que les propriétés de $\mathbf{Z}$ se généralisaient aisément [14] aux anneaux $\mathbf{Z}[\zeta_p]$. La stratégie de Lamé s'applique quand même dans certains cas.

Insistons lourdement sur le fait que le problème des anneaux $\mathbf{Z}[\zeta_p]$ en général n'est pas le défaut d'*existence* d'une décomposition en produit d'irréductibles. Cette propriété d'existence est en fait vraie pour *tous* les anneaux $\mathbf{Z}[\zeta_p]$. Ce qui fait défaut, ce qui est vraiment exigeant, est la propriété d'*unicité* de la décomposition.

Il est à noter également que le défaut de factorialité d'anneaux tel que les anneaux $\mathbf{Z}[\zeta_p]$ est justement ce qui a poussé KUMMER et DEDEKIND à dégager la notion d'*idéal*, fondement de l'approche algébrique de la théorie des nombres et de l'algèbre moderne en général.

14. Bien sûr, en toute rigueur, LAMÉ aurait dû penser à le vérifier ; que celui qui n'est jamais tombé dans le piège d'une généralisation hâtive lui jette la première pierre... En fait, KUMMER avait peu de temps auparavant justement démontré que cette généralisation n'était pas valide, mais LAMÉ n'était pas au courant de ce travail ; à l'époque, la circulation des nouvelles découvertes scientifiques n'était évidemment pas aussi aisée qu'actuellement !