ARITHMÉTIQUE DES ANNEAUX EUCLIDIENS

Trois niveaux de difficulté/longueur :

— Piste bleue : questions **1)** à **9)**.

— Piste rouge : questions **1)** à **11)**.

— Piste noire : tout le devoir (éventuellement sans les questions **10)** et **11)**).

On s'intéresse dans ce devoir à des anneaux, dits *euclidiens*, dans lesquels une forme de division euclidienne peut être effectuée comme dans $\mathbb{Z}$, et à leur application à la résolution de certaines équations diophantiennes.

1 ANNEAUX EUCLIDIENS

Définition **(Anneau euclidien)** Soit A un anneau commutatif intègre. On dit que A est *euclidien* s'il existe une application $\varphi : A \longrightarrow \mathbb{N}$, appelée *stathme*, pour laquelle :

(i) $\forall a \in A,\quad \forall b \in A\setminus\{0_A\},\quad \exists q, r \in A,\quad a = bq + r \quad \text{et} \quad \varphi(r) < \varphi(b)$,

(ii) $\varphi(0_A) = 0 \quad \text{et} \quad \varphi(1_A) = 1$,

(iii) $\forall a, b \in A\setminus\{0_A\},\quad \varphi(a) \leqslant \varphi(ab)$.

D'après le théorème de la division euclidienne, $\mathbb{Z}$ est euclidien pour le stathme $x \longmapsto |x|$.

On pose à présent $\mathbb{Z}\big[i\sqrt{n}\big] = \Big\{a + ib\sqrt{n} \mid \quad a, b \in \mathbb{Z}\Big\}$ pour tout $n \in \mathbb{N}^*$. On admet que $\mathbb{Z}\big[i\sqrt{n}\big]$ est un sous-anneau de $\mathbb{C}$. À ce titre, il est commutatif et intègre.

1) On a vu en cours que $\mathrm{U}\big(\mathbb{Z}[i]\big) = \mathbb{U}_4$. Déterminer $\mathrm{U}\big(\mathbb{Z}\big[i\sqrt{n}\big]\big)$ pour tout $n \geqslant 2$.

2) Soit $n \in \{1, 2\}$.

a) Vérifier que l'application $x \longmapsto |x|^2$ est à valeurs dans $\mathbb{N}$ et satisfait les assertions (ii) et (iii) de la définition d'un stathme.

b) En approximant $\dfrac{a}{b}$ par un élément de $\mathbb{Z}\big[i\sqrt{n}\big]$, montrer que pour tous $a \in \mathbb{Z}\big[i\sqrt{n}\big]$ et $b \in \mathbb{Z}\big[i\sqrt{n}\big]\setminus\{0\}$, il existe deux éléments $q, r \in \mathbb{Z}\big[i\sqrt{n}\big]$ pour lequel $a = bq + r$ et $|r|^2 < |b|^2$.

c) Montrer, pour $n = 1$, que les éléments q et r de la question **a)** ne sont pas forcément uniques.

En résumé, $\mathbb{Z}[i]$ et $\mathbb{Z}\big[i\sqrt{2}\big]$ sont euclidiens pour le stathme $x \longmapsto |x|^2$, qui est bien à valeurs dans $\mathbb{N}$. On montrera plus loin que $\mathbb{Z}\big[i\sqrt{n}\big]$ ne l'est pas pour $n \geqslant 3$.

Dans les questions **3)** à **7)**, A est un anneau euclidien fixé de stathme φ.

3) Déterminer $\varphi^{-1}\big(\{0\}\big)$ et montrer que $\varphi^{-1}\big(\{1\}\big) = \mathrm{U}(A)$.

Définition **(Divisibilité et éléments associés)** Soient $a, b \in A$.

- On dit que a *divise* b ou que a est un *diviseur de* b si $b = ak$ pour un certain $k \in A$.
- On dit que b est *associé à* a si $b = au$ pour un certain $u \in \mathrm{U}(A)$.

4) **a)** Justifier l'assertion : « $\mathrm{U}(A)$ est un groupe, donc la relation d'association est une relation d'équivalence sur A. »

b) Montrer que pour tous $a, b \in A$, a et b sont associés si et seulement s'ils se divisent mutuellement.

c) Montrer que pour tous $a, b \in A$, si a divise b et si $\varphi(a) = \varphi(b)$, alors a et b sont associés.

Définition **(Éléments premiers entre eux)** Soient $a, b \in A$. On dit que a et b sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de $\mathrm{U}(A)$.

5) Soient $a, b \in A$ premiers entre eux.

a) Montrer que l'ensemble $\varphi\Big((aA+bA)\setminus\big\{0_A\big\}\Big)$ possède un plus petit élément m.

On peut ainsi se donner un élément non nul $d \in aA+bA$ pour lequel $\varphi(d) = m$.

b) Montrer que d divise a, puis que $au + bv = 1_A$ pour certains $u, v \in A$ (*théorème de Bézout*).

Définition **(Élément irréductible)** Soit $a \in A$. On dit que a est *irréductible* si a n'est ni nul ni inversible et si ses seuls diviseurs sont 1, a et leurs associés.

6) Soient $p \in A$ irréductible et $a, b \in A$. Montrer que p divise ab si et seulement si p divise a ou b (*lemme d'Euclide*).

Il n'est pas dur de montrer que les associés d'un irréductible sont eux-mêmes irréductibles. On se donne à présent un ensemble quelconque P de représentants des classes d'équivalence d'irréductibles de A pour la relation d'association. En d'autres termes, P est une partie de A satisfaisant les trois conditions suivantes :

— tout élément de P est irréductible,

— tout irréductible de A est associé à un élément de P,

— les éléments de P sont deux à deux non associés.

7) Montrer que pour tout $a \in A\setminus\big\{0_A\big\}$, il existe un élément $u \in \mathrm{U}(A)$ et une famille presque nulle $(\alpha_p)_{p\in P}$ d'entiers naturels pour lesquels $a = u\displaystyle\prod_{p\in P} p^{\alpha_p}$. Cette relation est appelée une *factorisation irréductible de a*.

On admet finalement les résultats suivants, qui se démontrent comme leurs analogues dans $\mathbb{Z}$.

Définition-théorème **(Valuation p-adique et unicité de la factorisation irréductible)**

- Soit $p \in P$. L'ensemble $\Big\{n \in \mathbb{N} \mid \quad p^n \text{ divise } a\Big\}$ possède un plus grand élément pour tout $a \in A\setminus\big\{0_A\big\}$, appelé la *valuation p-adique de a* et noté $v_p(a)$. En outre, pour tous $a, b \in A\setminus\big\{0_A\big\}$: $\quad v_p(ab) = v_p(a) + v_p(b)$.
- La factorisation irréductible d'un élément de A est unique à l'ordre près des facteurs.

Théorème **(Une recette pour casser les puissances)** Soient $a, b \in A$ premiers entre eux et $k \geqslant 2$. Si $ab = z^k$ pour un certain $z \in A$, alors $a = ux^k$ et $b = vy^k$ pour certains $u, v \in \mathrm{U}(A)$ et $x, y \in A$.

8) Montrer que si A est l'un des anneaux euclidiens $\mathbb{Z}[\mathrm{i}]$ ou $\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$ et si k est impair, les éléments u et v du théorème précédent peuvent être choisis égaux à 1.

9) Soit $n \geqslant 3$. Montrer que 2 est irréductible dans $\mathbb{Z}\big[\mathrm{i}\sqrt{n}\big]$, puis que $\mathbb{Z}\big[\mathrm{i}\sqrt{n}\big]$ n'est pas euclidien. On pourra observer que 2 divise $\big(\mathrm{i}\sqrt{n}\big)^2$ ou $\big(1+\mathrm{i}\sqrt{n}\big)\big(1-\mathrm{i}\sqrt{n}\big)$.

2 Résolution d'une équation de Mordell

On appelle *équation de Mordell* toute équation diophantienne d'inconnue $(x,y)\in\mathbb{Z}^2$ de la forme $y^2=x^3+k$ avec $k\in\mathbb{Z}$ fixé, mais on ne s'intéresse dans cette partie qu'à l'équation $y^2=x^3-2$. Curieusement, la résolution de cette équation gagne à être effectuée dans $\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$.

Attention cependant ! Dans la preuve qui suit, l'arithmétique de $\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$ est mise au service de l'arithmétique de $\mathbb{Z}$, donc les mots ont deux sens. Dire que a divise b dans $\mathbb{Z}$, c'est dire que $b=ak$ pour un certain $k\in\mathbb{Z}$, mais on peut aussi vouloir dire que a divise b dans $\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$, et cette fois $k\in\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$.

10) Soit $x,y\in\mathbb{Z}$ deux entiers pour lesquels $y^2=x^3-2$. Soit $d\in\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$ un diviseur commun de $y+\mathrm{i}\sqrt{2}$ et $y-\mathrm{i}\sqrt{2}$.

a) Montrer que $|d|^2$ divise à la fois 8 et x^3 dans $\mathbb{Z}$.

b) Montrer que x est impair, puis que $d\in\mathrm{U}\big(\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]\big)$. Conclusion ?

11) Montrer que $(3,5)$ et $(3,-5)$ sont les seules solutions de l'équation de Mordell étudiée.

3 Un cas particulier du théorème de Mihăilescu

Jusqu'en 2002, on a appelé *conjecture de Catalan* l'énoncé selon lequel l'équation diophantienne $x^m-y^n=1$ d'inconnues $x,y,m,n\geqslant 2$ admet pour seule solution le quadruplet $(x,y,m,n)=(3,2,2,3)$, autrement dit l'énoncé selon lequel 8 et 9 sont les seules puissances consécutives d'entiers. Proposée par le mathématicien français Catalan en 1844, cette conjecture est devenue en 2002 le *théorème de Mihăilescu*, du nom du mathématicien roumain qui l'a finalement démontrée.

Le résultat est trivial si m et n sont pairs. En effet, si $m=2m'$ et $n=2n'$ pour certains $m',n'\in\mathbb{N}^*$, alors $x^m-y^n\neq 1$ pour tous $x,y\geqslant 2$ car : $\big|x^m-y^n\big|=\big(x^{m'}+y^{n'}\big)\big|x^{m'}-y^{n'}\big|\geqslant 4\big(x^{m'}-y^{n'}\big)$. Ensuite, si p est un diviseur premier de m et q un diviseur premier de n, alors $m=pm'$ et $n=qn'$ pour certains $m',n'\in\mathbb{N}^*$ et tout couple (x,y) d'entiers supérieurs à 2 pour lequel $x^m-y^n=1$ satisfait aussi la relation $\big(x^{m'}\big)^p-\big(y^{n'}\big)^q=1$. Pour démontrer la conjecture de Catalan, il est par conséquent suffisant de la démontrer pour les seules équations $x^p-y^q=1$ avec $p,q\in\mathbb{P}$.

En 1850, le mathématicien français Le Besgue (1791-1875) a résolu le cas $q=2$ et c'est sa preuve que l'on suit ci-dessous. Pour information, il y a un autre Lebesgue en mathématiques (1875-1941), beaucoup plus important, à qui l'on doit la théorie moderne du calcul intégral.

12) Soit $p\in\mathbb{P}$ supérieur à 3. On suppose par l'absurde que $x^p-y^2=1$ pour certains entiers $x,y\geqslant 2$. On pose $q=\dfrac{p-1}{2}$.

a) Étudier la parité de x et y.

b) Montrer que $1+\mathrm{i}y=(a+\mathrm{i}b)^p$ pour certains $a,b\in\mathbb{Z}^*$, puis que $x=a^2+b^2$ et $\displaystyle\sum_{k=0}^{q}(-1)^k\binom{p}{2k}a^{p-2k}b^{2k}=1$.

c) Montrer que $a=1$ et que b est pair.

d) Montrer que pour tout $k\in[\![2,q]\!]$: $v_2\left(\binom{p}{2k}b^{2k}\right)>v_2\left(\binom{p}{2}b^2\right)$ et en déduire une contradiction.