CHAPITRE 4

Arithmétique des entiers quadratiques imaginaires

Le but de ce chapitre est d'introduire l'arithmétique des anneaux engendrés par des entiers algébriques (l'*arithmétique transcendante*, selon Gauss) en étudiant de manière détaillée le cas des anneaux $\mathbb{Z}[\sqrt{d}]$, où $d < 0$ est entier, et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ lorsque de plus $d \equiv 1 \bmod 4$. Nous en donnerons aussi quelques applications à l'étude des équations diophantiennes.

Cette famille infinie d'exemples, historiquement la première étudiée, permet déjà de rendre compte de la diversité des phénomènes qui distinguent l'arithmétique de $\mathbb{Z}$ de celle des anneaux plus généraux. Même dans ce cas particulier, il est important pour ne pas s'y perdre de commencer par dégager les propriétés fondamentales que peut posséder la relation de divisibilité dans un anneau commutatif général, et c'est par là que nous commencerons. C'est de toutes façon une étape incontournable avant de dégager les propriétés plus fines de factorisation des idéaux démontrées par Kummer et Dedekind, qui feront l'objet d'un chapitre ultérieur.

RÉFÉRENCES : On pourra consulter le chapitre 4 du livre de Stewart & Tall, le chapitre 1 du livre de Samuel, où encore le chapitre du *Cours d'algèbre* de Perrin concernant l'arithmétique des anneaux.

1. Vocabulaire de l'arithmétique des anneaux

Dans tout ce paragraphe, A désigne un anneau commutatif unitaire. On supposera que A est *intègre*, ce qui signifie qu'il est non nul, et que pour tout $a, b \in A$, $ab = 0$ entraîne $a = 0$ ou $b = 0$.

1.1. Divisibilité. Si $a, b \in A$, on dit que a divise b, ou que b est multiple de a, et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ac$. L'intégrité de A assure que c est alors unique si $a \neq 0$. La relation de divisibilité est une relation de préordre sur A au sens de Bourbaki : pour tout $a, b, c \in A$, alors $a|a$, et si $a|b$ et $b|c$ alors $a|c$. L'étude de cette relation est appelée parfois *arithmétique de* A.

1.2. Unités. Les diviseurs de 1 jouent un rôle particulier puisqu'ils divisent tous les éléments de A ; ils sont appelés *unités* ou *inversibles* de A. L'ensemble des unités de A est noté $A^\times$ (à ne pas confondre avec $A\backslash\{0\}$), c'est un groupe (commutatif) pour la multiplication de A.

1.3. Éléments associés. Par intégrité de A, on constate que si $a, b \in A$, on a $a|b$ et $b|a$ si, et seulement si, $a = bu$ avec $u \in A^\times$. On dit alors que a et b sont *associés*, c'est une relation d'équivalence sur A, que l'on notera $a \sim b$. Par exemple, l'arithmétique d'un corps est inintéressante, car tous les éléments non nuls sont associés...

1.4. Pgcd, ppcm. Si $a_1, \ldots, a_n$ est une famille d'éléments de A, on appelle *plus grand diviseur commun* (ou pgcd) des a_i un élément $d \in A$ tel que d divise a_i pour tout i, et tel que si $b \in A$ divise a_i pour tout i alors b divise d.

Autrement dit, c'est un élément maximal de A parmi les éléments inférieurs aux a_i pour la relation d'ordre de divisibilité. De même on définit un plus petit multiple commun (ou ppcm) des a_i comme étant un élément minimal parmi les éléments plus grands que les a_i pour la relation de divisibilité.

En toute généralité, les pgcd et ppcm n'existent pas toujours, nous en verrons des exemples plus loin. En revanche, il découle de la définition que si deux pgcd (resp. ppcm) existent alors il sont associés.

1.5. Éléments premiers entre eux. Des éléments $a_1, \ldots, a_n \in A$ sont dits premiers entre eux si leurs seuls diviseurs communs sont les unités, ou ce qui revient au même si l'élément 1 est un pgcd des a_i.

1.6. Éléments irréductibles. Un élément *non nul* $\pi \in A$ est dit irréductible si ce n'est pas une unité, et si pour tout $a, b \in A$, la relation $\pi = ab$ entraîne que a ou b est une unité. Autrement dit, aux unités près, ce sont les éléments ayant exactement deux diviseurs, à savoir 1 et eux-même.

Si π est irréductible, il en va de même de tout élément associé. Il est souvent commode de choisir un ensemble de représentants des éléments irréductibles pour la relation d'association. Par exemple, les unités de $\mathbb{Z}$ sont ± 1, et les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p un nombre premier (sous entendu positif), un système de représentants étant précisément donné par l'ensemble des nombres premiers. Par la suite, on désignera par P un tel ensemble de représentants.

1.7. Anneaux factoriels. La définition suivante est fondamentale.

Définition 4.1. *On dit que A a la propriété de factorisation si pour tout $a \in A$ ni nul ni inversible, alors il existe $u \in A^\times$, $n \geq 1$ et $\pi_1, \ldots, \pi_n \in \mathrm{P}$ tels que $a = u\pi_1 \cdots \pi_n$. On dit que A est factoriel si de plus, pour tout a comme précédemment, une telle écriture est unique à permutation près.*

Autrement dit, cette seconde propriété est que si $u\pi_1 \cdots \pi_n = u'\pi'_1 \cdots \pi'_m$ avec $u, u' \in A^\times$, $\pi_i, \pi'_j \in \mathrm{P}$, alors $m = n$, $\exists \sigma \in \mathfrak{S}_n$ tel que $\pi'_i = \pi_{\sigma(i)}$ pour tout $i = 1, \cdots, n$, et donc $u = u'$. Il est facile de voir qu'autant la propriété de factorisation que celle d'être factoriel ne dépendent pas du choix de l'ensemble de représentants P des irréductibles de A.

1.8. Arithmétique des anneaux factoriels. Supposons A factoriel. Si $a \in A$ est non nul et si $\pi \in \mathrm{P}$, le caractère factoriel assure que le nombre $v_\pi(a) \in \mathbb{N}$ d'occurences de π dans l'écriture de a comme produit d'une unité et d'éléments de P est bien défini, on l'appelle la valuation en π de A. Par définition, $v_\pi(a) = 0$ pour tout π sauf un nombre fini et il y a donc un sens a écrire

$$a = u \prod_{\pi \in \mathrm{P}} a^{v_\pi(a)}$$

avec $u \in A^\times$, avec la convention $a^0 = 1$ pour tout $a \in A$.

La propriété d'unicité entraîne $v_\pi(ab) = v_\pi(a) + v_\pi(b)$ pour tout $a, b \in A\backslash\{0\}$. En particulier, $a|b$ si et seulement si $v_\pi(a) \leq v_\pi(b)$ pour tout $\pi \in \mathrm{P}$, de sorte que l'arithmétique de A est essentiellement triviale.

Par exemple, pgcd et ppcm existent dans un anneau factoriel. En effet, un pgcd de $a_1, \ldots, a_n$ est $\prod_{\pi \in \mathrm{P}} \pi^{\mathrm{Min_i v_\pi(a_i)}}$, et un ppcm s'obtient de même en remplaçant le Min par un Max.

1.9. Éléments premiers. Un élément non nul $\pi \in A$ est dit premier si ce n'est pas une unité et s'il satisfait à la propriété d'Euclide-Gauss : pour tout $a, b \in A$, π divise ab entraîne π divise a ou π divise b.

Un élément premier est irréductible. En effet, si $\pi = ab$ alors π divise a ou b. Si par exemple $\pi|a$, de sorte que $a = \pi c$ où $c \in A$, alors $\pi = \pi cb$ puis $1 = cb$, et donc b est une unité.

1.10. Caractérisation d'Euclide-Gauss des anneaux factoriels. Il n'est pas vrai en général qu'un irréductible est premier. C'est vrai toutefois si A est factoriel, car si $\pi \in \mathrm{P}$ divise ab, alors $1 \leq v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et donc soit $v_\pi(a) \geq 1$ soit $v_\pi(b) \geq 1$. Plus précisément, on a la propriété suivante :

Proposition 4.2. *Si A satisfait la propriété de factorisation, alors A est factoriel si et seulement si tout irréductible de A est premier.*

Démonstration — Supposons que tout irréductible de A est premier. Supposons qu'il existe $u, u' \in A^\times$, $n, m \geq 1$, ainsi que $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_m \in \mathrm{P}$ tels que

$$u\pi_1 \ldots \pi_n = u'\pi'_1 \ldots \pi'_m.$$

Alors π_1 divise $u'\pi'_1 \ldots \pi'_m$. Si π_1 ne divise aucun des π'_i alors π_1 divise u' par la propriété d'Euclide-Gauss appliquée m fois, et donc π_1 est une unité : absurde. Quitte à permuter les π'_i on peut donc supposer que π_1 divise π'_1, c'est-à-dire $\pi_1 = \pi'_1$ car π'_1 est irréductible, et donc associé à π_1. Ainsi, on peut diviser l'égalité ci-dessus par π_1 (A intègre). On conclut par récurrence sur n à moins que $m > n$ et qu'un produit de $m - n$ éléments parmi les π'_i soit une unité, ce qui est impossible car un diviseur d'une unité est une unité. □

1.11. Idéaux. On rappelle qu'un idéal est un sous-groupe additif $I \subset A$ tel que $aI \subset I$ pour tout $a \in A$. L'ensemble aA des multiples de a dans A est un idéal appelé idéal principal engendré par $a \in A$. On note aussi $(a) = aA$. On a $bA \subset aA$ si et seulement $b \in aA$, i.e. si, et seulement si, $a|b$ ("contenir c'est diviser"). En particulier $aA = A$ si, et seulement si, $a \in A^\times$.

Si $(I_j)_{j\in J}$ sont des idéaux, on désigne par $\sum_j I_j$ le plus petit idéal contenant les I_j, c'est-à-dire l'ensemble des sommes finies d'éléments de $\bigcup_j I_j$. Si $a_1, \dots, a_n \in A$ on pose aussi

$$(a_1, \dots, a_n) = a_1A + a_2A + \cdots + a_nA = \{\sum_{i=1}^{n} a_i x_i, x_i \in A \ \forall i\},$$

Un idéal est dit finiment engendré ou de type fini s'il est de la forme $(a_1, \dots, a_n)$.

De même, $\cap_j I_j$ est un idéal : c'est le plus grand idéal inclus dans chacun des I_j. Les notions de somme et d'intersection sont donc les analogues dans le langage des d'idéaux des notions respectives de pgcd et ppcm pour les éléments.

1.12. Anneaux noethérien. Un anneau est dit noethérien si tout idéal de A est finiment engendré. Une propriété importante (en fait caractéristique) des anneaux noethériens est que toute suite $(I_m)_{m\geq 1}$ d'idéaux qui est croissante, c'est-à-dire $I_m \subset I_{m+1}$ pour tout $m \geq 1$, est constante à partir d'un certain rang.

En effet, on vérifie immédiatement que $I = \bigcup_{m\geq 1} I_m$ est un idéal de A, donc de la forme $(a_1, \dots, a_n)$ pour certains éléments $a_i \in A$. Si N est assez grand de sorte que $a_i \in I_N$ pour $i = 1, \dots, n$, on constate que $I_m \subset I \subset I_N$ pour tout $m \geq 1$, d'où l'on tire $I_m = I_N$ si $m \geq N$.

Proposition 4.3. *Si A est noethérien alors A admet la propriété de factorisation.*

Démonstration — Soit $S \subset A\backslash\{0\}$ l'ensemble des éléments qui sont produits d'unités et d'irréductibles. Si $a \notin S$, alors a n'est pas irréductible en particulier, et donc il est de la forme bc avec b et c non unités. Comme S est stable par produits, soit b soit c n'est pas dans S ! Si $S \neq A\backslash\{0\}$, on construit donc récursivement une suite d'éléments non nuls $(a_m)_{m\geq 1}$ avec $a_m \in A\backslash S$, a_{m+1} divise a_m, et a_m non associé à a_{m+1}. Ainsi, $I_m = (a_m)$ est une suite strictement croissante d'idéaux de A, ce qui est absurde par noethérianité . □

1.13. Anneaux principaux. Un anneau est dit principal si tous ses idéaux sont principaux.

Lemme 4.4. (Relation de Bézout) *Si A est principal, et si $a, b \in A$, alors a et b admettent un pgcd d et il existe $u, v \in A$ tels que $au + bv = d$.*

En effet, il existe $d \in A$ tel que l'idéal $Aa + Ab$ (donc principal) soit de la forme Ad. Un tel d est évidemment un pgcd de a, b, et de la forme $au + bv$ avec $u, v \in A$.

Proposition 4.5. *Un anneau principal est factoriel.*

Démonstration — Un anneau principal est évidemment noethérien, de sorte que A satisfait la propriété de factorisation. Il suffit de vérifier la caractérisation d'Euclide-Gauss. Soit π un irréductible. Supposons $\pi|ab$ avec $a, b \in A$. Si π ne divise pas a alors a et π sont premiers entre eux, et donc il existe $u, v \in A$ tels que $au + \pi v = 1$ d'après le lemme ci-dessus. Mais alors $abu + \pi bv = b$ et donc π divise b. □

1.14. Anneaux euclidiens. L'anneau A est dit euclidien s'il possède une fonction $\varphi : A\backslash\{0\} \to \mathbb{N}$ telle que $\forall a, b \in A\backslash\{0\}$, il existe q et $r \in A$ tels que :

(i) $a = bq + r$,

(ii) si $r \neq 0$ alors $\varphi(r) < \varphi(b)$.

Pour des raisons que l'auteur ignore, une telle fonction s'appelle un *stathme euclidien*. Les deux exemples fondamentaux d'anneaux euclidiens sont les anneaux $\mathbb{Z}$ et $k[X]$ quand k est un corps. Un stathme euclidien sur $\mathbb{Z}$ est donné par $\varphi(a) = |a|$ (valeur absolue) et un stathme euclidien sur $k[X]$ étant la fonction degré d'un polynôme non nul. La vérification de (i) et (ii) dans les deux cas est le fruit de l'algorithme classique de division euclidienne.

Théorème 4.6. (Gauss) *Un anneau euclidien est principal, et donc factoriel.*

Démonstration — L'idéal nul étant principal, il suffit de voir que tout idéal non nul I de A est principal. Soit φ un stathme euclidien sur A, la partie $\varphi(I\backslash\{0\}) \subset \mathbb{N}$ est non vide, on peut donc trouver un élément $b \in I\backslash\{0\}$ pour lequel $\varphi(b)$ soit minimal. Bien entendu, $bA \subset I$ et nous allons vérifier l'inclusion réciproque. Mais si $a \in I$, il existe $q, r \in A$ tels que $a = bq + r$, et que de plus si $r \neq 0$ alors $\varphi(r) < \varphi(b)$. Mais $r = a - bq \in I$ car I est un idéal, donc ce second cas ne se produit pas par minimalité de $\varphi(b)$. Ainsi, $a = bq$ puis $I \subset bA$ et $I = bA$. □

Corollaire 4.7. *Les anneaux $\mathbb{Z}$ et $k[X]$ quand k est un corps sont principaux, et donc factoriels.*

Les inversibles de $k[X]$ quand k est un corps étant les constantes dans $k^\times$, on prend en général les polyômes unitaires non constants comme ensemble P des représentants des irréductibles dans ce cas. De la factorialité de $k[X]$ et du lemme du contenu de Gauss on déduit aussi la proposition importante suivante, pour laquelle nous renvoyons à l'exercice 4.12. On rappelle qu'un polynôme $P \in A[X]$ est dit primitif si ses coefficients sont premiers entre eux dans leur ensemble. On note aussi $K = \mathrm{Frac}(A)$ le corps de fractions [1] de A.

1. Lorsque A est un sous-anneau d'un corps C, on rappelle que le corps de fractions de A est simplement l'ensemble des $\frac{a}{b} \in C$ avec $a, b \in A$ et $b \neq 0$. C'est un sous-corps de C noté $\mathrm{Frac}(A)$. En général, on considère l'ensemble X des couples $(a, b) \in A^2$ tels que $b \neq 0$. La relation $(a, b) \sim (a', b') \Leftrightarrow ab' = ba'$ est une relation d'équivalence sur X dont l'ensemble des classes est noté Frac$A$. La classe de $(a, b) \in X$ est notée $\frac{a}{b}$. On munit $\mathrm{Frac}(A)$ d'une structure de corps en posant $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$ et $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+ba'}{bb'}$. C'est un exercice de vérifier que ces lois sont bien définies indépendamment des choix de représentants et qu'elle définissent une loi de corps sur $\mathrm{Frac}(A)$. L'anneau A se plonge alors dans K via $\iota : a \mapsto \frac{a}{1}$ (un morphisme injectif d'anneau), et tout élément de $\mathrm{Frac}(A)$ est de la forme $\frac{\iota(a)}{\iota(b)} = \frac{a}{b}$ pour certains $a, b \in A$ et $b \neq 0$. Dans les fondements des mathématiques, c'est ainsi que l'on définit $\mathbb{Q}$ à partir de $\mathbb{Z}$!

Proposition 4.8. (Gauss) *Si A est factoriel alors $A[X]$ est factoriel. De plus, les irréductibles de $A[X]$ sont exactement les irréductibles de A ainsi que les polynômes primitifs irréductibles dans $K[X]$.*

2. Anneaux d'entiers quadratiques imaginaires euclidiens

Fixons $D \equiv 0, 1 \bmod 4$ un entier que l'on supposera < 0. On considère le nombre complexe α défini par $\alpha = \sqrt{D/4}$ si $D \equiv 0 \bmod 4$, ou $\alpha = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \bmod 4$. Pour lever l'ambiguïté sur la racine carrée intervenant dans sa définition nous supposerons que l'on choisit celle de partie imaginaire > 0. C'est un entier algébrique : on a $\alpha^2 = D/4 \in \mathbb{Z}$ dans le premier cas, et $\alpha^2 - \alpha + \frac{1-D}{4} = 0$ dans le second. On considère alors le réseau $A_D \subset \mathbb{C}$ de base $1, \alpha$, i.e.

$$A_D = \mathbb{Z} + \mathbb{Z}\alpha.$$

La remarque précédente montre que *c'est un sous-anneau de* $\mathbb{C}$, ou encore que $A_D = \mathbb{Z}[\alpha]$ au sens du premier chapitre. Par exemple, $A_{-4} = \mathbb{Z}[i]$ (entiers de Gauss) et $A_{-3} = \mathbb{Z}[j]$ où $j = e^{2i\pi/3} = \frac{1+\sqrt{-3}}{2} - 1$ (entiers d'Eisenstein). Nous allons nous intéresser à l'arithmétique de l'anneau A_D.

Une application qui jouera un rôle important par la suite est l'application norme. Si $z \in \mathbb{C}$, on pose $\mathrm{N}(z) = z\overline{z} \in \mathbb{R}_{\geq 0}$: c'est le carré de la norme usuelle. Bien sûr, $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ pour tout $z, z' \in \mathbb{C}$ et on constate de plus que pour tout $x, y \in \mathbb{Z}$, alors

$$\mathrm{N}(x + y\alpha) = \begin{cases} x^2 - \frac{D}{4}y^2, & \text{si } D \equiv 0 \bmod 4, \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{si } D \equiv 1 \bmod 4. \end{cases}$$

La fonction $(x, y) \mapsto \mathrm{N}(x + y\alpha)$ est donc la forme principale de discriminant D. En particulier, $\mathrm{N}(\mathbb{Z}[\alpha]) \subset \mathbb{N}$. Notons de plus que $z \mapsto \overline{z}$ préserve $\mathbb{Z}[\alpha]$, car $\overline{\alpha}$ vaut $-\alpha$ ou $1 - \alpha$.

Proposition 4.9. *(i) Les unités de A_D sont les éléments $u \in A_D$ tels que $\mathrm{N}(u) = 1$. En particulier, hormis les exceptions $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$ on a $A_D = \{\pm 1\}$.*

(ii) Soient $a, b \in A_D$ non nuls tels que $a \mid b$ dans $\mathbb{Z}[\alpha]$. Alors $\mathrm{N}(a) \mid \mathrm{N}(b)$ dans $\mathbb{Z}$, et $\mathrm{N}(a) = \mathrm{N}(b)$ si et seulement si a et b sont associés.

(iii) Pour que $\pi \in A_D$ non nul et non unité soit irréductible, il suffit qu'aucun diviseur propre de $\mathrm{N}(\pi)$ ne soit de la forme $\mathrm{N}(z)$ avec $z \in A_D$. C'est en particulier le cas si $\mathrm{N}(\pi)$ est premier.

Démonstration — Soient $a, b \in A_D$ tels que $ab = 1$. Alors $\mathrm{N}(a), \mathrm{N}(b) \in \mathbb{N}$ et $\mathrm{N}(a)\mathrm{N}(b) = 1$, donc $\mathrm{N}(a) = 1$. Réciproquement, si $a \in A_D$ est tel que $\mathrm{N}(a) = 1$ alors $a\overline{a} = 1$ mais $\overline{a} \in A_D$ et donc $a \in A_D^\times$. Le "en particulier" découle de l'étude des représentations de 1 par une forme principale, que nous avons déjà traitée en exercice.

Si $a = bc$ avec $a, b, c \in A_D$ non nuls, alors $\mathrm{N}(a) = \mathrm{N}(b)\mathrm{N}(c)$ et donc $\mathrm{N}(b) \mid \mathrm{N}(a)$ dans $\mathbb{Z}$. Il y a égalité si, et seulement si, $\mathrm{N}(c) = 1$, i.e. $c \in A_D^\times$. Le (iii) en découle immédiatement. □

Corollaire 4.10. *A_D a la propriété de factorisation.*

Démonstration — En effet, on constate que si $a, b \in A_D$ sont non nuls et tels que a est un diviseur propre de b (i.e. $b = ac$ avec ni a ni c une unité), alors $N(a) < N(b)$. On conclut donc par récurrence sur la norme de l'élément. □

Théorème 4.11. *Si $D \in \{-3, -4, -7, -8, -11\}$ alors A_D est euclidien pour le stathme* N*. En particulier, il est principal et factoriel. Pour les autres valeurs de D, l'anneau A_D n'est pas euclidien (pour aucun stathme).*

La première partie du théorème est due à Gauss, la dernière à P. Samuel [2].

Démonstration — Commençons par vérifier le premier point. Il suffit de montrer la propriété d'approximation suivante : si $z \in \mathbb{C}$, il existe un $t \in A_D$ tel que $|z - t| < 1$. En effet, si a et b sont non nuls et dans A_D, et si $t \in A_D$ est tel que $\mathrm{N}(\frac{a}{b} - t) < 1$, alors $\mathrm{N}(a - tb) < \mathrm{N}(b)$ (multiplicativité de N), et donc $\mathrm{N} : A_D \to \mathbb{N}$ définit un stathme euclidien. Il ne reste qu'à vérifier la propriété d'approximation ci-dessus pour les valeurs de l'énoncé. Il ne serait pas difficile de procéder géométriquement. Donnons un argument algébrique.

Soit q la forme principale de discriminant $D < 0$. Soient $x, y \in \mathbb{R}$ fixés. On cherche $u, v \in \mathbb{Z}$ tels que $q(x - u, y - v) < 1$. Supposons $D \equiv 0 \bmod 4$. On peut choisir $u, v \in \mathbb{Z}$ tels que $|x - u|, |y - v| \leq \frac{1}{2}$, auquel cas

$$q(x - u, y - v) = (x - u)^2 - \frac{D}{4}(y - v)^2 \leq \frac{1 - D/4}{4}$$

qui est < 1 si $D = -4, -8$. Supposons $D \equiv 1 \bmod 4$, auquel cas on rappelle l'identité $4q(\alpha, \beta) = (2\alpha + \beta)^2 - D\beta^2$. On choisit alors $v \in \mathbb{Z}$ tel que $|y - v| \leq 1/2$, puis $u \in \mathbb{Z}$ tel que $|2u + \frac{v - 2x - y}{2}| \leq 1$, c'est bien sur possible ! On a alors $4q(x - u, y - v) \leq 1 - \frac{D}{4}$ qui est < 4 dès que $-D < -12$, ce qui conclut le premier point.

Pour voir que A_D n'est pas euclidien nous avons besoin de la proposition suivante.

Proposition 4.12. *(i) Tout idéal non nul de A_D admet une $\mathbb{Z}$-base à deux éléments. En particulier, A_D est noethérien.*

(ii) Tout idéal non nul I de A_D est d'indice fini dans A_D, noté $\mathrm{N}(I)$ *("norme de I").*

(iii) Si $z \in A_D$ est non nul, alors $\mathrm{N}((z)) = \mathrm{N}(z)$.

Démonstration — Si I est un idéal de A_D, il est donc discret dans $\mathbb{C} \simeq \mathbb{R}^2$, comme partie d'un réseau. C'est en fait un réseau s'il est non nul. En effet, si $x \neq 0 \in I$ on constate que $x, \alpha x \in I$ est encore une $\mathbb{R}$-base de $\mathbb{C}$, ce qui conclut. En particulier, I admet une $\mathbb{Z}$-base à deux éléments (c'est la caractérisation algébrique des réseaux, i.e. le théorème 2.4) et est d'indice fini dans A_D (Proposition 2.17). De plus, l'indice de I dans A_D est égal à son covolume. Mais la multiplication par $z \in \mathbb{C}^\times$ est la composée d'une rotation et d'une homothétie de rapport $|z|$, qui multiplie donc les covolumes par $|z|^2 = N(z)$. En particulier, $\mathrm{N}((z)) = \mathrm{N}(z)$. □

2. P. Samuel, *About euclidean rings*, Journal of Algebra 19, 282-301 (1971).

Terminons la démonstration du théorème. Supposons que A_D admette un stathme euclidien φ. Soit $x \in A$ qui n'est ni nul, ni une unité, et tel que $\varphi(x)$ est minimal. On en déduit que tout $a \in A_D$ est de la forme $bx + r$ avec $r = 0$ ou $r \in A_D^\times$. En particulier $1 < \mathrm{N}(x) = \mathrm{N}((x)) \leq 1 + |A_D^*|$. Mais $|D| > 4$, donc $A_D^* = \{\pm 1\}$, puis $\mathrm{N}(x) \in \{2, 3\}$. En particulier la forme principale de discriminant $-D$ représente 2 ou 3. Il est clair que cela entraîne $|D/4| \leq 3$ si $D \equiv 0 \bmod 4$, et $|D| \leq 12$ si $D \equiv 1 \bmod 4$ (car $4(x^2 + xy + \frac{1-D}{4}) = (2x + y)^2 - Dy^2$)). Il ne reste qu'à exclure $A_{-12} = \mathbb{Z}[\sqrt{-3}]$, mais il n'est pas euclidien car non factoriel (voir §4). □

3. Digression : application aux équations diophantiennes

Avant de continuer notre analyse, donnons une application typique de la factorialité des anneaux de la forme $\mathbb{Z}[\alpha]$ à l'étude des équations diophantiennes. La proposition suivante avait été formulée par Fermat, on prétend qu'il l'avait lancée en défi aux mathématiciens anglais de son époque (le milieu du 17$^{\text{eme}}$ siècle). Nombreux sont les contemporains de Fermat qui considéraient ce problème comme étant insoluble !

Proposition 4.13. *Les seules solutions $x, y \in \mathbb{Z}$ de l'équation $y^2 = x^3 - 2$ sont $(x, y) = (\pm 5, 3)$.*

Démonstration — Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^3 - 2$. Comme 2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$, on constate que x et y sont impairs. On déduit de $y^2 = x^3 - 2$ qu'ils sont en fait premiers entre eux. Considérons la factorisation

$$(y + i\sqrt{2})(y - i\sqrt{2}) = x^3$$

dans $\mathbb{Z}[i\sqrt{2}] = A_{-8}$. Ce dernier est euclidien d'après la proposition précédente, donc factoriel. Vérifions que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$. Il suffit de voir qu'il n'y a pas d'irréductible π divisant $y + i\sqrt{2}$ et $y - i\sqrt{2}$. Mais un tel π diviserait $2i\sqrt{2} = -(i\sqrt{2})^3$, et donc $i\sqrt{2}$ (car π est également premier), et donc y. Mais alors $\mathrm{N}(i\sqrt{2}) = 2$ diviserait $N(y) = y^2$, ce qui est absurde.

Si dans un anneau factoriel A, on a une relation $a^n = bc$ avec b et c premier entre eux, et n un entier ≥ 1, on constate en décomposant b et c en irréductibles qu'il existe $d \in A$ et $u \in A^\times$ tels que $b = d^n u$. Comme $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, on en déduit l'existence de $u, v \in \mathbb{Z}$ tels que

$$\pm(y + i\sqrt{2}) = (u + iv\sqrt{2})^3 = u^3 - 6uv^2 + (3u^2v - 2v^3)i\sqrt{2}.$$

En prenant la coordonnée en $i\sqrt{2}$, on obtient $\pm 1 = v(3u^2 - 2v^2)$, d'où l'on tire $v = \pm 1$ puis $3u^2 = \pm v + 2$ et donc $u = 1$ et $v = \pm 1$. En particulier, $\pm y = u^3 - 6uv^2 = -5$, ce qui conclut ! □

Cette méthode admet de multiples applications. La plus célèbre est certainement la stratégie qu'elle fournit pour montrer que l'équation de Fermat $x^n + y^n = z^n$, qui s'écrit aussi

$$x^n = \prod_{i=0}^{n-1} (z - \zeta^i y)$$

où $\zeta = e^{\frac{2i\pi}{n}}$, n'a pas de solution non triviale ($xyz = 0$) quand $n \neq 2$. Si l'on sait que $\mathbb{Z}[\zeta]$ est factoriel, et si l'on arrive à se ramener au cas où les $z-\zeta^i y$ sont premiers entre eux, cela fournit un point de départ pour l'étude de l'équation, à savoir que $z - \zeta y$ est une puissance n^{ieme} dans $\mathbb{Z}[\zeta]$ fois une unité de $\mathbb{Z}[\zeta]$, ce qui fournit $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ identités distinctes au lieu d'une !

L'idée même que $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$ puisse ne pas être factoriel a en fait mis très longtemps à émerger dans l'esprit des mathématiciens. Sous une autre forme peut-être, c'est aussi l'erreur présumée de la démonstration jamais retrouvée par Fermat de son "théorème" ("cette marge est trop petite pour la contenir."...). Fermat en a vraiment démontré le cas $n = 4$ par sa méthode de descente infinie, et le cas second cas historiquement effectivement démontré, à savoir $n = 3$ a dû attendre Euler. Dans ce cas, $\mathbb{Z}[j] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ est factoriel d'après le théorème ci-dessus, et la stratégie fonctionne en effet : nous renvoyons au chapitre 17 du livre de Ireland et Rosen pour une démonstration utilisant ces idées. Cette stratégie a aussi ses limites, on peut en fait montrer que le plus petit entier n impair tel que $\mathbb{Z}[\zeta]$ n'est pas factoriel est $n = 23$, et aussi qu'il n'y a qu'un nombre fini d'entiers n tels que $\mathbb{Z}[\zeta]$ est factoriel ! Il faut alors se plonger dans les travaux de Kummer pour aller plus loin dans cette direction... Mais ceci anticipe sur le cheminement du cours... revenons donc à l'anneau $\mathbb{Z}[\alpha]$ étudié ici.

4. Anneaux d'entiers quadratiques imaginaires factoriels

Donnons des exemples de D pour lesquels $A_D = \mathbb{Z}[\alpha]$ n'est pas factoriel. Vérifions par exemple que $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel. En effet, on a la relation

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

bien que 2 et $1 \pm \sqrt{-3}$ soient des irréductibles non associés dans $\mathbb{Z}[\sqrt{3}]$. Le seul point non trivial est cette dernière assertion, vérifions-là à l'aide de la proposition 4.9. Les unités de $\mathbb{Z}[\sqrt{-3}]$ étant ± 1, il sont deux à deux non associés. Ils sont aussi irréductibles. En effet, chacun est de norme 4 et 2 n'est pas une norme de $\mathbb{Z}[\sqrt{-3}]$, i.e. n'est pas de la forme $a^2 + 3b^2$ avec $a, b \in \mathbb{Z}$. Cela conclut. De même, on vérifierait que les factorisations

$$2 \cdot 2 = -(2i)^2, \;\; 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \;\; 2 \cdot 3 = -\sqrt{-6}^2$$

entraînent que $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-4}] = \mathbb{Z}[2i]$, $\mathbb{Z}[\sqrt{-5}]$ et $\mathbb{Z}[\sqrt{-6}]$ ne sont pas factoriels. Par exemple, 2, 3 et $1 \pm \sqrt{-5}$ sont de normes respectives 4, 9 et 6, ils sont donc irréductibles car il n'y a pas d'élément de norme 2 ou 3 dans $\mathbb{Z}[\sqrt{-5}]$, non associés car $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Un premier résultat général est le suivant, englobant notamment les exemples précédents sauf $d = -5$.

Proposition 4.14. *Si A_D est factoriel, alors D est sans facteur carré, à mois que $D \equiv 0 \bmod 4$ auquel cas $D/4$ est sans facteur carré et n'est pas congru à 1 modulo 4.*

Un entier $D \equiv 0, 1 \bmod 4$ satisfaisant les conclusions de cette proposition est appelé *discriminant fondamental*. Il est équivalent de demander que D n'est pas de la forme $N^2 D'$ avec $D \equiv 0, 1 \bmod 4$ et $N \in \mathbb{Z}$, ou encore que toutes les formes binaires de discriminant D sont primitives (comparer avec l'exercice 3.2).

La première observation, cruciale, est dûe à Dedekind. Soit A un anneau intègre de corps de fractions K. On dit que A est *intégralement clos* (ou *normal*) si pour tout élément de K qui est entier sur A est en fait dans A. Autrement dit, si pour tout $x \in K$ tel qu'il existe $P \in A[X]$ unitaire vérifiant $P(x) = 0$ alors $x \in A$.

Proposition 4.15. *Si A est factoriel alors A est intégralement clos.*

Démonstration — En effet, supposons que $x \in K$ et qu'il existe un entier $n \geq 1$ et des éléments $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = x^n.$$

Comme A est factoriel on peut écrire $x = \frac{p}{q}$ avec $p, q \in A$ premiers entre eux, $q \neq 0$. Mais alors en multipliant l'équation par q^n on conclut que q divise p^n. Si π est un irréductible divisant q, il divise donc p car π est premier, ce qui est absurde car p et q sont premiers entre eux. Ainsi, q est une unité, et donc $x \in A$. □

Cette proposition généralise l'égalité $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ démontrée au premier chapitre. Un autre exemple important d'anneau intégralement clos est donné par la proposition suivante :

Proposition 4.16. *L'anneau $\overline{\mathbb{Z}}$ est intégralement clos.*

Démonstration — Soit $x \in \mathbb{C}$ et soit $P \in \overline{\mathbb{Z}}[X]$ unitaire de degré n satisfaisant $P(x) = 0$. Il faut montrer $x \in \overline{\mathbb{Z}}$. Soient $a_0, a_1, \ldots, a_{n-1} \in \overline{\mathbb{Z}}$ les coefficients de P, $A = \mathbb{Z}[a_0, \ldots, a_{n-1}]$ et $B = \mathbb{Z}[a_0, \ldots, a_{n-1}, x]$. On a $xB \subset B$. Il suffit donc de montrer que le groupe additif B est finiment engendré (Proposition 1.16 (ii)).

D'après la proposition 1.16 (i), le groupe additif de A est finiment engendré. Il suffit donc de montrer que tout élément de B est de la forme $\sum_{i=0}^{n} a_i x^i$ avec $a_i \in A$. Soit $y \in B$. On peut donc écrire $y = Q(x)$ avec $Q \in A[X]$. Comme P est unitaire à coefficients dans $\mathbb{Z}$, donc dans l'anneau A, on peut effectuer la division euclidienne de Q par P dans $A[X]$: on peut écrire $Q = SP + R$ avec $S, R \in A[X]$ et $\deg R < n$. On a alors $y = Q(x) = R(x)$, ce que l'on voulait démontrer. □

Proposition 4.17. *A_D est intégralement clos si, et seulement si, D est un discriminant fondamental.*

Démonstration — Nous ne démontrerons pour l'instant que la condition nécessaire, qui est celle dont on a besoin pour démontrer la proposition 4.14. La condition suffisante sera démontré au chapitre suivant.

Supposons $A_D = \mathbb{Z}[\alpha]$ intégralement clos. Il contient en particulier $\overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{d})$. Écrivons $d = d'm^2$ avec $m \geq 1$ et d' sans facteur carré. On a donc $\sqrt{d'} = \frac{1}{m}\sqrt{d} \in \mathbb{Z}[\alpha]$. En considérant la $\mathbb{Z}$-base $1, \alpha$ de $\mathbb{Z}[\alpha]$, on constate que cela entraîne $m = 1$, donc $d = d'$ est sans facteur carré. Dans le cas $\alpha = \frac{1+\sqrt{d}}{2}$, observera pour cela que $\frac{1}{m}\sqrt{d} = \frac{2}{m}\alpha - \frac{1}{m}$, donc $1/m \in \mathbb{Z}$. Enfin, si $d \equiv 1 \bmod 4$, on observe de plus $\frac{1+\sqrt{d}}{2} \in \overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{d}) \subset \mathbb{Z}[\alpha]$, et donc $\alpha = \frac{1+\sqrt{d}}{2}$. □

La proposition 4.14 peut en fait être sensiblement améliorée. Nous devons au préalable faire une remarque sur les différences entre "factoriel" et "principal" pour les anneaux $\mathbb{Z}[\alpha]$. Bien qu'il ne soit pas vrai en général qu'un anneau noethérien factoriel est principal (par exemple l'idéal $(2, X)$ de l'anneau factoriel $\mathbb{Z}[X]$ n'est pas principal), cela vaut pour les anneaux qui nous intéresseront majoritairement dans le cours, à savoir les $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. Nous reportons la vérification de ce fait à un chapitre ultérieur.

Il se trouve que la question de la principalité de $\mathbb{Z}[\alpha]$ est intimement reliée à la théorie des formes binaires étudiée au chapitre précédent. Ce lien peut-être inattendu sera étudié en détail un peu plus loin dans le cours. Le théorème suivant en sera un cas particulier.

Théorème 4.18. *Soit $D < 0$ un discriminant fondamental. L'anneau A_D est principal si, et seulement si, on a $\mathrm{h}(D) = 1$.*

Notre étude des formes binaires admet alors la conséquence suivante.

Corollaire 4.19. *Soit d un entier < 0.*

(i) L'anneau $\mathbb{Z}[\sqrt{d}]$ est principal si, et seulement si, $d = -1$ ou -2.

(ii) On suppose $d \equiv 1 \bmod 4$. L'anneau $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal si, et seulement si, l'entier d est dans l'ensemble $\{-3, -7, -11, -19, -43, -67, -163\}$.

Démonstration — Supposons que $\mathbb{Z}[\sqrt{d}]$ est principal. La proposition 4.14 entraîne que d est sans facteur carré ainsi que la congruence $d \equiv 3 \bmod 4$ si d est impair. Si on a $d = ab$ avec $a < b$, la forme binaire $(a, 0, b)$ est de discriminant $4d$, réduite au sens de Gauss, et primitive : c'est donc la forme principale par le théorème 4.18, *i.e.* $a = 1$. On a donc soit $d = -1$, soit $-d$ est un nombre premier. Si c'est un premier impair, on observe de même que la forme binaire $(2, 2, \frac{1-d}{2})$ est de discriminant $4d$, réduite au sens de Gauss, et primitive car on a $d \equiv 3 \bmod 4$, ce n'est donc pas la forme principale : c'est absurde par le théorème 4.18. Les seules possibilités sont donc $d = -1$ ou $d = -2$. Réciproquement, on a déjà vu que pour ces valeurs de d l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien, donc principal.

De même, la condition suffisante du (ii) se déduit du théorème 4.18 et de la proposition 3.26. La condition nécessaire, la plus intéressante peut-être, est par contre absolument non élémentaire : elle se déduit du théorème 3.27 de Heegner-Stark-Baker. Un argument élémentaire semblable à celui du (i), consistant à considérer des formes réduites ambiguës, démontre par contre que si $\mathrm{h}(d) = 1$ avec $d \equiv 1 \bmod 4$ sans facteur carré, alors d est premier. □

Nous renvoyons à l'exercice 4.6 pour une démonstration du (i) qui ne repose pas sur le théorème 4.18. Observons que si l'on a $d = -19, -43, -67, -163$ alors l'anneau $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal mais non euclidien, d'après le théorème 4.11 (Samuel).

Le théorème 4.18 conclut ce chapitre sur une note un peu pessimiste : il n'y a en particulier qu'un nombre fini d'entiers quadratiques imaginaires α tels que $\mathbb{Z}[\alpha]$ est un anneau factoriel. Cependant, comme Dedekind et Kummer l'ont remarqué,

et comme nous le verrons ultérieurement, tous ceux d'entre eux qui sont intégralement clos (classifiés par la proposition 4.17) possèdent la propriété de factorisation unique de leurs idéaux en produit d'idéaux premiers. Comme on le verra aussi, cette propriété sera souvent suffisante pour les applications arithmétiques !

Remarque 4.20. (D'après le livre de Stewart et Tall, chapitre 4) La détermination des entiers $d > 0$ et $\alpha = \sqrt{d}$ ou $\frac{1+\sqrt{d}}{2}$ et $d \equiv 1 \bmod 4$ tels que $\mathbb{Z}[\alpha]$ est euclidien est en fait un problème ouvert. Par exemple, il n'est pas difficile de vérifier que $\mathbb{Z}[\sqrt{2}]$ est euclidien pour la valeur absolue de la norme de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Un résultat plus profond est que les seuls autres α tels que $\mathbb{Z}[\alpha]$ est euclidien pour la norme sont $\alpha = \sqrt{3}, \sqrt{6}$ et les $\alpha = \frac{1+\sqrt{d}}{2}$ avec

$$d = 5, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73$$

(Chatland-Davenport, Inkeri). Il semble que l'on ne connaisse pas d'exemple de $\mathbb{Z}[\alpha]$ qui soit euclidien et mais pour lequel la valeur absolue de la norme de $\mathbb{Q}(\alpha)/\mathbb{Q}$ ne soit pas un stathme euclidien, un candidat selon Samuel est $\mathbb{Z}[\sqrt{14}]$ (qui est principal).

5. Exercices

Les quatre premiers exercices concernent l'arithmétique de l'anneau $\mathbb{Z}[i]$ avec $i^2 = -1$ (anneau des "entiers de Gauss"). On rappelle que cet anneau est euclidien.

Exercice 4.1. (Irréductibles de $\mathbb{Z}[i]$)

(i) Montrer que $1 + i$ est irréductible dans $\mathbb{Z}[i]$ et que $2 = -i(1 + i)^2$.

(ii) Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, alors $p = \pi\overline{\pi}$ où π et son conjugué complexe $\overline{\pi}$ sont des irréductibles non associés de $\mathbb{Z}[i]$.

(iii) Montrer que si $p \equiv 3 \bmod 4$ est un nombre premier, alors p est irréductible dans $\mathbb{Z}[i]$.

(iv) Montrer que si π est un irréductible de $\mathbb{Z}[i]$ alors $\pi\mathbb{Z}[i] \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ engendré par un nombre premier. En déduire que si π est un irréductible de $\mathbb{Z}[i]$ alors π divise un et un seul nombre premier usuel.

(v) En déduire une classification des irréductibles de $\mathbb{Z}[i]$.

Exercice 4.2. *Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, il existe exactement 8 couples $(a, b) \in \mathbb{Z}^2$ tels que $p = a^2 + b^2$.*

Exercice 4.3. *Factoriser $-3 + 15i$ en irréductibles dans $\mathbb{Z}[i]$.*

Exercice 4.4. (Un choix de représentants des irréductibles)

(i) Montrer que l'idéal $(2(1 + i))$ de $\mathbb{Z}[i]$ admet pour $\mathbb{Z}$-base $4, 2(1 + i)$.

(ii) En déduire un isomorphisme de groupes abéliens $\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i] = \mathbb{Z}/4\mathbb{Z}\cdot\overline{1}\oplus \mathbb{Z}/2\mathbb{Z}\cdot\overline{1+i}$. À quelle condition sur $a, b \in \mathbb{Z}$ est-ce que $a+bi \equiv 3 \bmod 2(1+i)$?

(iii) Montrer qu'un ensemble de représentants des irréductibles de $\mathbb{Z}[i]$ est donné par $1 + i$ et l'ensemble des irréductibles de $\mathbb{Z}[i]$ congrus à 3 modulo $2(1 + i)$.

Exercice 4.5. *Soit p un nombre premier et soit $\alpha = \sqrt{-p}$.*

(i) Montrer que $\alpha\,\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}, a \equiv 0 \bmod p\}$.

(ii) En déduire que α est un élément premier de $\mathbb{Z}[\alpha]$.

Exercice 4.6. *On se propose de démontrer élémentairement que si $\mathbb{Z}[\sqrt{d}]$ est principal (où $d < 0$), alors $d = -1$ ou -2. On suppose donc $\mathbb{Z}[\sqrt{d}]$ principal.*

(i) Rappeler pourquoi d est sans facteur carré, et $d \not\equiv 1 \bmod 4$.

(ii) On pose $\beta = \sqrt{d}$ si d est pair, $1 + \sqrt{d}$ si d est impair, et on désigne par I l'idéal de $\mathbb{Z}[\alpha]$ engendré par 2 et β. Monter que $2, \beta$ est une $\mathbb{Z}$-base de I.

(iii) En déduire que $\mathrm{N}(I) = 2$ et conclure.

Dans l'esprit de l'exercice précédent, le lecteur pourra essayer de démontrer que si $d \equiv 1 \bmod 4$ et si $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal, alors d est un nombre premier. Pour cela, on pourra considérer un facteur premier minimal p de d et observer que l'idéal de $\mathbb{Z}[\alpha]$ engendré par p et $\frac{p+\sqrt{d}}{2}$ est de norme p.

Exercice 4.7. *(Points entiers d'une certaine courbe elliptique) On se propose de montrer que les $x, y \in \mathbb{Z}$ tels que $y^2 + y = x^3 - 2$ sont exactement $(x, y) = (2, 2)$ ou $(2, -3)$.*

(i) Montrer que $\sqrt{-7}$ est premier dans $\mathbb{Z}[\alpha]$ où $\alpha = \frac{1+\sqrt{-7}}{2}$.

(ii) Montrer que si $y^2 + y = x^3 - 2$ alors $y + \alpha$ n'est pas divisible par $\sqrt{-7}$ dans $\mathbb{Z}[\alpha]$.

(iii) Conclure.

On peut démontrer qu'il y a une infinité de $x, y \in \mathbb{Q}$ tels que $y^2 + y = x^3 - 2$. Par exemple, en considérant la tangente à la courbe $y^2 + y = x^3 - 2$ au point $(2, 2)$ on constate que l'autre point d'intersection, à savoir $(x, y) = (\frac{44}{25}, \frac{178}{125})$, est aussi solution ! On peut itérer ce procédé et les solutions deviennent vite gigantesques, par exemple au deuxième coup on obtient la solution

$$\left(\frac{13373096}{5784025}, \frac{38354841394}{13910580125}\right).$$

Exercice 4.8. *(i) Trouver toutes les solutions $x, y \in \mathbb{Z}$ de $y^2 + y = x^3 - k$ sous l'hypothèse que $p = 4k - 1$ est un nombre premier > 3 et que $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ est factoriel.*

(ii) (difficile) Étudier le cas $k = 1$ (attention aux unités de $\mathbb{Z}[j]$).

Dans ce qui suit, A désignera un anneau commutatif unitaire intègre, sauf mention du contraire.

Exercice 4.9. (Pgcd et ppcm : quelques généralités) *Soient $a, b \in A$ non nuls.*

(i) Montrer que l'idéal $(a) \cap (b)$ est principal engendré par $m \in A$ si, et seulement si, m est un ppcm de a et b.

(ii) On suppose a premier et que a ne divise pas b, montrer que ab est un ppcm de a et b.

(iii) On suppose que $(a)+(b)=(d)$. Montrer que d est un pgcd de a et b.

(iv) On suppose a irréductible et que a ne divise pas b. Montrer que 1 est un pgcd de a et b.

Exercice 4.10. (Pgcd et ppcm : exemples et contre-exemples dans l'anneau non factoriel $\mathbb{Z}[\sqrt{-5}]$).

(i) Montrer que $\sqrt{-5}$ et $1+\sqrt{-5}$ admettent un ppcm et un pgcd.

(ii) Montrer que 2 et $1+\sqrt{-5}$ n'admettent pas de ppcm. On pourra remarquer qu'un tel ppcm m satisferait $12 \,|\, \mathrm{N}(m)$, puis qu'il serait associé à $2+2\sqrt{-5}$.

(iii) Montrer que $3(1+\sqrt{-5})$ et $3(1-\sqrt{-5}) = (1+\sqrt{-5})(-2-\sqrt{-5})$ n'admettent pas de pgcd.

Soit I l'idéal $(2, 1+\sqrt{-5})$ de $\mathbb{Z}[\sqrt{-5}]$.

(iv) Montrer que I admet pour $\mathbb{Z}$-base $2, 1+\sqrt{-5}$.

(v) En déduire que $\mathrm{N}(I)=2$, puis que I n'est pas principal.

(vi) En déduire que la réciproque du (iii) de l'exercice précédent est fausse.

(vii) Montrer que $(2)\cap(1+\sqrt{-5}) = (1+\sqrt{-5})\cdot I$.

Exercice 4.11. *Soient A un anneau intègre et $\varphi : A\backslash\{0\} \to \mathbb{N}$ un stathme euclidien. On dit que φ est* fort *si $\forall a, b \in A$, "$a \neq 0$ et b divise a" entraîne "$\varphi(b) \leq \varphi(a)$". Si I est un idéal non nul de A, on pose $\mathrm{m}_\varphi(I) = \mathrm{Min}\{\varphi(a), a \in I - \{0\}\}$ (justifier).*

(i) Vérifier que les stathmes euclidiens rencontrés jusque-là sont forts.

(ii) Montrer que si φ est fort alors A admet la propriété de factorisation (et donner un algorithme).

(iii) On suppose φ fort. Soient $I \neq 0$ un idéal de A et $x \in I - \{0\}$. Montrer que $I = Ax$ si, et seulement si, $\varphi(x) = \mathrm{m}_\varphi(I)$.

(iv) Montrer que tout anneau euclidien admet un stathme euclidien fort (Motzkin). *Un stathme euclidien φ étant donné, on pourra considérer $a \mapsto \mathrm{m}_\varphi(aA)$.*

Exercice 4.12. (Lemme du contenu de Gauss) *Soit A un anneau factoriel de corps de fractions K. Si $P \in A[X]$ est non nul, on note $\mathrm{c}(P)$ le pgcd des coefficients de P, c'est un élément de A bien défini aux unités près. On dit que P est primitif si $\mathrm{c}(P)$ est une unité.*

(i) Montrer que $A[X]^\times = A^\times$.

(ii) Montrer que si $P, Q \in A[X]$ sont primitifs alors PQ est primitif.

(iii) En déduire que si $P, Q \in A[X]$ sont non nuls, alors $\mathrm{c}(PQ) = \mathrm{c}(P)\mathrm{c}(Q)$ (aux unités près).

(iv) Montrer que si $P \in A[X]$ est non constant, alors P est irréductible dans $A[X]$ si, et seulement si, $\mathrm{c}(P) = 1$ et P est irréductible dans $K[X]$.

(v) En déduire que les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs non constants qui sont irréductibles dans $K[X]$.

(vi) Montrer que $A[X]$ est factoriel.

(vii) En déduire que $\mathbb{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$ sont factoriels si $n \geq 1$ et si k est un corps.

(viii) Vérifier que $\mathbb{Z}[X]$ n'est pas principal (bien que factoriel par le (vii)).

Exercice 4.13. *Soit A l'anneau des fonctions holomorphes sur $\mathbb{C}$ tout entier.*

(i) Montrer que A est intègre.

(ii) Montrer que les unités de A sont les fonctions holomorphes sur $\mathbb{C}$ qui ne s'annulent pas, et que les irréductibles de A sont, aux unités près, les $z - a$ avec $a \in \mathbb{C}$.

(iii) En déduire que A n'a pas la propriété de factorisation (en particulier, A n'est pas noethérien).