## CORRIGÉ (TRÈS) PARTIEL DE LA FICHE 7

**Exercice 4** — *L'anneau $\mathbb{Z}[i]$ des entiers de Gauss.*

0. L'application $\varphi : \mathbb{Z}[\mathrm{X}] \to \mathbb{C},\ \mathrm{P} \mapsto \mathrm{P}(i)$ est un homomorphisme d'anneaux. Par division euclidienne, tout polynôme $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ s'écrit (de manière unique) sous la forme $\mathrm{P} = (\mathrm{X}^2+1)\mathrm{Q} + a + b\mathrm{X}$ avec $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}]$ et $a, b \in \mathbb{Z}$. Comme $\mathrm{P}(i) = a + bi$, on obtient immédiatement :
- $\mathrm{P}(i) = 0$ si et seulement si $a = b = 0$, de sorte que le noyau de l'homomorphisme $\varphi$ est l'idéal engendré par le polynôme $\mathrm{X}^2 + 1$ ;
- $\varphi(\mathrm{P}) = a + bi$, de sorte que l'image de $\varphi$ est le sous-anneau $\mathbb{Z}[i]$ de $\mathbb{C}$, formé des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbb{Z}$.

L'homomorphisme $\varphi$ induit donc un isomorphisme d'anneaux entre l'anneau quotient $\mathbb{Z}[\mathrm{X}]/(\mathrm{X}^2+1)$ et le sous-anneau $\mathbb{Z}[i]$ de $\mathbb{C}$.

1. L'application $\mathrm{N} : \mathbb{Z}[i] \to \mathbb{N},\ z \mapsto \mathrm{N}(z) = z\bar{z}$ est multiplicative : $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ pour tous $z, z' \in \mathbb{Z}[i]$.

Si un élément $z$ de $\mathbb{Z}[i]$ est inversible, il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ ; on a alors $\mathrm{N}(z)\mathrm{N}(z') = \mathrm{N}(zz') = \mathrm{N}(1) = 1$ et donc $\mathrm{N}(z) = 1$ puisque $\mathrm{N}(z), \mathrm{N}(z') \in \mathbb{N}$. Réciproquement, si $z$ est un élément de $\mathbb{Z}[i]$ tel que $z\bar{z} = \mathrm{N}(z) = 1$, $z$ est inversible dans $\mathbb{Z}[i]$, d'inverse $\bar{z}$. Ainsi, les éléments inversibles de l'anneau $\mathbb{Z}[i]$ sont précisément les éléments de norme 1.

Les solutions de l'équation $a^2 + b^2 = 1$ dans $\mathbb{Z}^2$ étant les couples $(1,0)$, $(-1,0)$, $(0,1)$ et $(0,-1)$, $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

2. L'anneau $\mathbb{Z}[i]$ est *euclidien* : quels que soient les éléments $a, b \in \mathbb{Z}[i]$, il existe un couple $(q, r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ avec $\mathrm{N}(r) < \mathrm{N}(b)$. Ce résultat, démontré en cours, implique que l'anneau $\mathbb{Z}[i]$ est principal [(1)]

*Illustration* – Comme $z = \frac{5+5i}{3-4i} = \frac{(5+5i)(3+4i)}{25} = -\frac{1}{5} + \frac{7}{5}i$, $i$ est le point de $\mathbb{Z}[i]$ le plus proche de $z$ et

$$|z - i|^2 = \Big| -\frac{1}{5} + \frac{2}{5}i \Big|^2 = \frac{1}{25};$$

on a alors

$$\mathrm{N}(5 + 5i - (3-4i)i) = \mathrm{N}(3-4i)|z-i|^2 < \mathrm{N}(3-4i),$$

donc l'identité $5 + 5i = (3-4i)i + 1 + 2i$ est une division euclidienne de $5+5i$ par $3-4i$ et l'idéal $(5+5i, 3-4i)$ est égal à l'idéal $(3-4i, 1+2i)$.

Comme $\frac{3-4i}{1+2i} = \frac{(3-4i)(1-2i)}{5} = -1-2i$, $1+2i$ divise $3-4i$ dans $\mathbb{Z}[i]$ et donc finalement

$$(5+5i, 3-4i) = (3-4i, 1+2i) = (1+2i).$$

3. Soit $p$ un nombre premier. En vertu de l'exercice 3 (question 2) et de la question 0 ci-dessus,

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[\mathrm{X}]/(\mathrm{X}^2+1, p) \simeq \big(\mathbb{Z}[\mathrm{X}]/(p)\big)/(\mathrm{X}^2+1) \simeq \mathbb{F}_p[\mathrm{X}]/(\mathrm{X}^2+1).$$

4. (i) Supposons $p > 2$. Il est facile de voir que $-1$ est un carré dans $\mathbb{F}_p$ si et seulement s'il existe un élément d'ordre 4 dans le groupe multiplicatif $\mathbb{F}_p^\times$. En effet : s'il existe $x \in \mathbb{F}_p$ tel que $x^2 = -1$, $x^4 = 1$ et, comme $-1 \neq 1$ dans $\mathbb{F}_p$ puisque $p > 2$, $x$ est d'ordre 4 dans $\mathbb{F}_p^\times$ ; réciproquement, si $x$ est un élément d'ordre 4 de $\mathbb{F}_p^\times$, $(x^2-1)(x^2+1) = x^4 - 1 = 0$ et donc $x^2 = -1$ car, $x$ étant d'ordre 4, $x^2 \neq 1$.

Comme le groupe $\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$, il contient un élément d'ordre 4 si et seulement si $4 | p-1$. Ainsi, $-1$ est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \pmod 4$. [(2)]

---

(1) Soit en effet I un idéal non nul de $\mathbb{Z}[i]$. La fonction $\mathrm{N} : \mathrm{I} - \{0\} \to \mathbb{N} - \{0\}$ atteint son minimum en un élément non nul $f$ de I ; quel que soit alors $a \in \mathrm{I} - \{0\}$, $a = qf + r$ avec $\mathrm{N}(r) < \mathrm{N}(f)$ et, puisque $r = a - qf \in \mathrm{I}$, $r = 0$ vu le choix de $f$. L'idéal $\mathrm{I} = (f)$ est ainsi principal.

(2) Noter par ailleurs que $-1 = 1$ est un carré dans $\mathbb{F}_2$.

(ii) L'anneau $\mathbb{Z}[i]$ étant principal, un élément non nul $z$ est irréductible si et seulement si l'idéal $(z)$ est premier. Un nombre premier $p$ est par suite irréductible dans $\mathbb{Z}[i]$ si et seulement si l'anneau quotient $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[\mathrm{X}]/(\mathrm{X}^2+1)$ est intègre, donc si et seulement si le polynôme $\mathrm{X}^2+1$ est irréductible dans $\mathbb{F}_p[\mathrm{X}]$. Cette dernière est équivalente au fait que $\mathrm{X}^2+1$ n'ait pas de racine dans $\mathbb{F}_p$, c'est-à-dire que $-1$ ne soit pas un carré dans $\mathbb{F}_p$. Conclusion : $p$ est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \pmod 4$.

(iii) La décomposition $2 = (1-i)(1+i)$ montre que 2 n'est pas irréductible dans $\mathbb{Z}[i]$ car ni $1-i$ ni $1+i$ ne sont inversibles dans $\mathbb{Z}[i]$ puisque $\mathrm{N}(1-i) = \mathrm{N}(1+i) = 2$. En fait, $1-i = -i(1+i)$ et donc $2 = (-i)(1+i)^2$.

Soit d'autre part $p$ un nombre premier congru à 1 modulo 4. Vu la question (ii), $p$ n'est pas irréductible dans l'anneau $\mathbb{Z}[i]$ ; il existe donc $z, z' \in \mathbb{Z}[i]$ tels que $p = zz'$ et $\mathrm{N}(z), \mathrm{N}(z') > 1$. On a alors $p^2 = \mathrm{N}(p) = \mathrm{N}(z)\mathrm{N}(z')$, d'où $\mathrm{N}(z) = \mathrm{N}(z') = p$ ; en particulier, $p = z\overline{z}$.

Il reste à voir que les décompositions de 2 et de tout nombre premier $p \in 1+4\mathbb{Z}$ que l'on vient d'obtenir font intervenir des éléments irréductibles de $\mathbb{Z}[i]$.

Lemme – *Un entier de Gauss $z$ dont la norme $\mathrm{N}(z)$ est un nombre premier est irréductible.*
*Preuve.* Une décomposition $z = z'z''$ dans $\mathbb{Z}[i]$ implique $\mathrm{N}(z) = \mathrm{N}(z')\mathrm{N}(z'')$, donc $\mathrm{N}(z') = 1$ ou $\mathrm{N}(z'') = 1$ puisque $\mathrm{N}(z)$ est un nombre premier ; ainsi, $z'$ ou $z''$ est inversible en vertu de la question 1 et $z$ est bien irréductible.

5. À l'issue de la question 4, nous savons que les éléments suivants de $\mathbb{Z}[i]$ sont irréductibles :
– les entiers de Gauss de la forme $up$, avec $u \in \mathbb{Z}[i]^\times$ et $p$ un nombre premier congru à 3 modulo 4 ;
– les entiers de Gauss $a+ib$ dont la norme $a^2+b^2$ est un nombre premier.

Ceci épuise la liste des éléments irréductibles de $\mathbb{Z}[i]$. Considérons en effet un élément irréductible $z$ de $\mathbb{Z}[i]$. Comme $z$ n'est pas inversible, $\mathrm{N}(z)$ est un nombre entier strictement supérieur à 1 et donc est divisible par un nombre premier $p$ : $p | z\overline{z}$.

Si $p \equiv 3 \pmod 4$, $p$ est irréductible dans $\mathbb{Z}[i]$ ; on a alors $p|z$ ou $p|\overline{z}$ en vertu du lemme de Gauss (qui s'applique dans tout anneau factoriel) et, puisque $\overline{p} = p$, $p|z$. Comme nous avons supposé $z$ irréductible, il en découle $z = up$ avec $u \in \mathbb{Z}[i]^\times$.

Si $p = 2$ ou si $p \equiv 1 \pmod 4$, $p$ s'écrit sous la forme $p = \pi\overline{\pi}$ avec $\pi \in \mathbb{Z}$ irréductible ; on a alors $\pi\overline{\pi} | z\overline{z}$, donc $\pi | z\overline{z}$, et nécessairement $\pi | z$ ou $\pi | \overline{z}$ puisque $\pi$ est irréductible ; de manière équivalente, $\pi | z$ ou $\overline{\pi} | z$. Comme $z$ est irréductible, il en découle $z = u\pi$ ou $z = u\overline{\pi}$ avec $u \in \mathbb{Z}[i]^\times$ et finalement $\mathrm{N}(z) = \mathrm{N}(u\pi) = \mathrm{N}(\pi) = p$ est un nombre premier.

*Éléments irréductibles associés* — Rappelons que deux éléments $a$ et $b$ d'un anneau sont dits *associés* s'il existe un élément inversible $u$ de A tel que $b = ua$ ; de manière équivalente, $a$ et $b$ sont associés s'ils engendrent le même idéal dans A.

Pour utiliser de manière efficace le fait que l'anneau $\mathbb{Z}[i]$ est factoriel, il faut savoir précisément quels sont les éléments irréductibles associés. La situation est la suivante :
– À chaque nombre premier $p$ congru à 3 modulo 4 correspondent exactement quatre éléments irréductibles associés dans $\mathbb{Z}[i]$ : $p$, $-p$, $ip$ et $-ip$.
– Au nombre premier 2 correspondent également quatre éléments irréductibles associés dans $\mathbb{Z}[i]$ : $1+i$, $-1-i$, $-1+i$ et $1-i$.
– À chaque nombre premier $p$ congru à 1 modulo 4 correspondent deux familles de quatre éléments irréductibles associés : $\pi$, $-\pi$, $i\pi$ et $-i\pi$ d'une part, $\overline{\pi}$, $-\overline{\pi}$, $i\overline{\pi}$ et $-i\overline{\pi}$ d'autre part, où $\pi$ est un entier de Gauss de norme $p$.

*Justifications* – La première assertion est claire. Supposons que $z$ soit un entier de Gauss dont la norme est un nombre premier $p$ ; $z$ est alors irréductible (cf. question 4 (iii)).

Si $p = 2$, $z\overline{z} = 2 = (-i)(1+i)^2$, donc $z | 1+i$, puis $z = u(1+i)$ avec $u \in \mathbb{Z}[i]^\times$ puisque $1+i$ est irréductible et finalement $z \in \{1+i, -1-i, -1+i, 1-i\}$.

Si $p \equiv 1 \pmod 4$, fixons $\pi \in \mathbb{Z}[i]$ irréductible tel que $p = \pi\overline{\pi}$. On a alors $z\overline{z} = \pi\overline{\pi}$, donc $z | \pi\overline{\pi}$ puis $z|\pi$ ou $z|\overline{\pi}$ et finalement $z = u\pi$ ou $z = u\overline{\pi}$ avec $u \in \mathbb{Z}[i]^\times$. Il reste à vérifier que $\pi$ et $\overline{\pi}$ ne sont pas associés. Posant $\pi = a+ib$, il s'agit de vérifier que $\overline{\pi} = a-ib$ est distinct de $-a-ib$, $-b+ia$ et $-b-ia$. Le premier cas implique $a = 0$ puis $p = a^2+b^2 = b^2$, ce qui est absurde ; les deux autres cas impliquent $a = \pm b$ puis $p = a^2+b^2 = 2a^2$, ce qui contredit l'hypothèse $p \equiv 1 \pmod 4$.

On peut lever l'ambiguïté due aux éléments inversibles en fixant une normalisation des éléments irréductibles. Cela revient à choisir une application

$$\lambda : \{\text{nombres premiers}\} \to \{\text{éléments irréductibles de } \mathbb{Z}[i]\}$$

telle que :

– $\lambda(2)$ soit associé à $1+i$ ;
– $\lambda(p)$ soit associé à $p$ si $p \equiv 3 \pmod 4$ ;
– $\lambda(p)$ soit un entier de Gauss de norme $p$ si $p \equiv 1 \pmod 4$.

Une fois ceci fait, le caractère factoriel de l'anneau $\mathbb{Z}[i]$ garantit que tout entier de Gauss non nul $z$ s'écrit d'une manière et d'une seule sous la forme

$$z = u\lambda(2)^{v_2(z)} \prod_{p\equiv 3 \pmod 4} \lambda(p)^{v_p(z)} \prod_{p\equiv 1 \pmod 4} \lambda(p)^{v_p(z)} \prod_{p\equiv 1 \pmod 4} \overline{\lambda(p)}^{v'_p(z)},$$

avec $u \in \mathbb{Z}[i]^\times$, $v_p(z), v'_p(z) \in \mathbb{N}$ et $v_p(z), v'(z) = 0$ pour tout nombre premier $p$ sauf au plus un nombre fini.

**Exercice 5** — *Deux applications arithmétiques.*

1. *Première application : un nombre naturel $n \geq 2$ peut s'écrire sous la forme $a^2+b^2$ avec $a, b \in \mathbb{Z}$ si et seulement si, dans sa décomposition en produit de nombres premiers, tout facteur $p \equiv 3 \pmod 4$ intervient avec une multiplicité paire.*

(i) Étant donné un entier naturel $n$, l'existence d'entiers $a$ et $b$ tels que $a^2+b^2 = n$ équivaut évidemment à l'existence d'entiers $a$ et $b$ tels que $n = (a+ib)(a-ib)$, c'est-à-dire à l'existence d'un entier de Gauss $z$ tel que $n = z\overline{z}$.

(ii) Fixons un nombre entier naturel non nul $n$ et reprenons les notations introduites à la fin de l'exercice précédent.

S'il existe $z \in \mathbb{Z}[i]$ tel que $n = z\overline{z}$, alors $z$ est non nul et s'écrit donc (de manière unique) sous la forme

$$z = u\lambda(2)^{v_2(z)} \prod_{p\equiv 3 \pmod 4} \lambda(p)^{v_p(z)} \prod_{p\equiv 1 \pmod 4} \lambda(p)^{v_p(z)} \prod_{p\equiv 1 \pmod 4} \overline{\lambda(p)}^{v'_p(z)},$$

avec $u \in \mathbb{Z}[i]^\times$, $v_p(z), v'_p(z) \in \mathbb{N}$ et $v_p(z), v'(z) = 0$ pour tout nombre premier $p$ sauf au plus un nombre fini. Il en découle

$$\begin{aligned} n &= z\overline{z} \\ &= (u\overline{u})\mathrm{N}(1+i)^{v_2(z)} \prod_{p\equiv 3 \pmod 4} p^{2v_p(z)} \prod_{p\equiv 1 \pmod 4} \mathrm{N}(\lambda(p))^{v_p(z)+v'_p(z)} \\ &= 2^{v_2(z)} \prod_{p\equiv 3 \pmod 4} p^{2v_p(z)} \prod_{p\equiv 1 \pmod 4} p^{v_p(z)+v'_p(z)} \end{aligned}$$

et nous constatons que chaque facteur premier $p \equiv 3 \pmod 4$ apparaît avec une multiplicité paire dans la décomposition de $n$ en produit de nombres premiers.

Supposons réciproquement que tout facteur premier $p \equiv 3 \pmod 4$ apparaisse avec une multiplicité paire dans la décomposition de $n$ en produit de nombre premiers. On a alors

$$\begin{aligned} n &= 2^{v_2(n)} \prod_{p\equiv 1 \pmod 4} p^{v_p(n)} \prod_{p\equiv 3 \pmod 4} p^{2\tilde{v}_p(n)} \\ &= \mathrm{N}(\lambda(2))^{v_2(n)} \prod_{p\equiv 1 \pmod 4} \mathrm{N}(\lambda(p))^{v_p(n)} \prod_{p\equiv 3 \pmod 4} \mathrm{N}(\lambda(p))^{\tilde{v}_p(n)} \\ &= z\overline{z} \end{aligned}$$

avec

$$z = \lambda(2)^{v_2(n)} \prod_{p\equiv 1 \pmod 4} \lambda(p)^{v_p(n)} \prod_{p\equiv 3 \pmod 4} \lambda(p)^{\tilde{v}_p(n)}.$$

2. *Seconde application : détermination des solutions entières de l'équation de Pythagore $x^2+y^2 = z^2$.*

(i) Étant donné un triplet $(x,y,z) \in \mathscr{E}$, écrivons $x = dx'$ et $y = dy'$ avec $d = \mathrm{pgcd}(x,y)$ et $x',y' \in \mathbb{Z}$ des entiers premiers entre eux. On a alors $z^2 = x^2 + y^2 = d^2(x'^2 + y'^2)$, donc $d^2$ divise $z^2$ puis $d$ divise $z$ ; posant $z = dz'$, on obtient finalement $x'^2 + y'^2 = z'^2$ et, puisque $x'y'z' \neq 0$, le triplet $(x',y',z')$ appartient à $\mathscr{E}$.

On considère dans ce qui suit un triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $x^2 + y^2 = z^2$, $xyz \neq 0$ et $\mathrm{pgcd}(x,y) = 1$. L'identité $x^2 + y^2 = z^2$ s'écrit de manière équivalente sous la forme

$$z^2 = (x+iy)(x-iy)$$

dans l'anneau $\mathbb{Z}[i]$.

(ii) Soit $\pi$ un élément irréductible de $\mathbb{Z}[i]$ divisant $x+iy$. Vu l'identité ci-dessus, $\pi$ divise $z^2$ et donc $\pi$ divise $z$ ; par suite, la multiplicité de $\pi$ dans $z^2 = (x+iy)(x-iy)$ est paire. Pour en déduire que la multiplicité de $\pi$ dans $x+iy$ est également paire, il suffit de vérifier que $\pi$ ne divise pas $x-iy$.

Tout diviseur commum de $x+iy$ et $x-iy$ divise $2x = (x+iy)+(x-iy)$ et $2y = i((x+iy)-(x-iy))$, donc divise $\mathrm{pgcd}(2x,2y) = 2\mathrm{pgcd}(x,y) = 2$. Puisque les seuls éléments irréductibles de $\mathbb{Z}[i]$ divisant 2 sont les quatre entiers de Gauss associés à $1+i$, nous en déduisons que, si $\pi$ n'est pas associé à $1+i$, $\pi$ ne divise pas $x-iy$ et apparaît donc avec une multiplicité paire dans $x+iy$.

(iii) Par conjugaison, la multiplicité de $1-i$ dans $x-iy$ est la même que celle de $1+i$ dans $x+iy$ ; comme $1+i$ et $1-i = (-i)(1+i)$ sont associés, nous en déduisons que la multiplicité de $1+i$ est la même dans $x+iy$ et dans $x-iy$. Notant $m$ la multiplicité de $(1+i)$ dans $x+iy$, il découle de ce que l'on vient de dire que la multiplicité de $1+i$ dans $z^2 = (x+iy)(x-iy)$ est égale à $2m$.

D'un autre côté, si l'on écrit $z$ sous la forme $z = 2^\alpha z'$ avec $z' \in \mathbb{Z}$ et $2 \nmid z'$, alors $z = (-i)(1+i)^{2\alpha} z'$ et $1+i$ ne divise pas $z'$ dans $\mathbb{Z}[i]$ puisque $2 = \mathrm{N}(1+i)$ ne divise pas $z'^2 = \mathrm{N}(z')$ dans $\mathbb{Z}$. La multiplicité de $1+i$ dans $z$ est donc paire.

Finalement, la multiplicité $2m$ de $1+i$ dans $z^2$ est un multiple de 4 et $m$ est donc pair.

(iv) Avec les notations introduites à la fin de l'exercice 4, il découle de ce qui précède que $x+iy$ s'écrit sous la forme $u\lambda^2$ avec $u \in \mathbb{Z}[i]^\times$ et $\lambda \in \mathbb{Z}[i]$. On a alors $z^2 = u\lambda^2\overline{u\lambda^2} = (\lambda\overline{\lambda})^2$, donc $z = \pm\lambda\overline{\lambda}$.

Posant $\lambda = a+ib$, $\lambda^2 = (a^2-b^2)+2iab$ et donc $(x,y,z)$ est l'un des huit triplets suivants :

$$(a^2-b^2, 2ab, \pm(a^2+b^2)),\ \ (b^2-a^2, -2ab, \pm(a^2+b^2),\ \ (-2ab, a^2-b^2, \pm(a^2+b^2)),\ \ (2ab, b^2-a^2, \pm(a^2+b^2)).$$

Il est clair que tous ces triplets fournissent des solutions de l'équation de Pythagore.

*Conclusion* — En tenant compte des redondances et de (i), nous avons finalement déterminé toutes les solutions $(x,y,z)$ de l'équation de Pythagore $x^2+y^2=z^2$ avec $xyz \neq 0$ : ce sont tous les triplets de la forme $(d(a^2-b^2), 2dab, \pm d(a^2+b^2))$ ou $(2dab, d(a^2-b^2), \pm d(a^2+b^2))$ avec $d \in \mathbb{N} - \{0\}$ et $a,b \in \mathbb{Z} - \{0\}$ tels que $a^2 \neq b^2$.