Corrigé du devoir 2

I

(1) $\mathbb{Z}[i]$ est stable par addition et par multiplication et contient 1. C'est un anneau intègre puisque $\mathbb{C}$ est intègre.

(2) $z \mapsto \overline{z}$ est un morphisme d'anneaux puisque la conjugaison respecte l'addition la multiplication et 1. C'est un isomorphisme parce que c'est une involution.

(3) On a $N(zz') = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z')$. Si z a un inverse z', on a $zz' = 1$, donc $N(z)N(z') = N(1) = 1$. Mais comme $N(z)$ et $N(z')$ sont des entiers, on a $N(z) = \pm 1$ (en fait $N(z) = 1$, puisque $N(z) \geq 0$).

(4) D'après la question précédente, il faut chercher les inversibles parmi les z tels que $N(z) = 1$. Or, pour $z = a + ib$, on a $N(z) = a^2 + b^2$. Comme a et b sont entiers, l'un de ces deux carrés doit être 0 et l'autre 1 ? Ceci laisse les quatre possibilites $(0,1), (0,-1), (1,0), (-1,0)$ pour le couple (a,b), ce qui montre que les inversibles sont parmi $1, -1, i$ et $-i$. Or, ces éléments ont pour inverses respectifs $1, -1, -i$ et i.

(5) Soit $u + iv$ un nombre complexe. Il existe un entier a tel que $|a - u| \leq 1/2$ et un entier v tel que $|b - v| \leq 1/2$. On a donc $|(u+iv) - (a+ib)|^2 = |(u-a) + i(v-b)|^2 = |u-a|^2 + |v-b|^2 \leq 1/4 + 1/4 = 1/2$. On a donc $|(u+iv) - (a+ib)| \leq 1/\sqrt{2} < 1$.

Comme $d \neq 0$, on peut considérer le nombre complexe z/d. Il existe un élément q de $\mathbb{Z}[i]$ tel que $|z/d - q| < 1$, ce qui entraîne $N(z/d - q) < 1$, puisque pour tout complexe x on a $N(x) = |x|^2$. En posant $b = z/d - q$, on a $z = qd + bd$, avec $r = bd \in \mathbb{Z}[i]$ car $z - dq \in \mathbb{Z}[i]$, et $N(r) = N(bd) = N(b)N(d) < N(d)$.

(6) ($N(x)$ est appelé la « norme » de x.) Soit $x \in I$. On a $x = qa + r$ avec $N(r) < N(a)$. Comme a est de norme minimale parmi les éléments non nuls de I, et comme $r \in I$ (car égal à $x - qa$), on doit avoir $r = 0$. Ainsi, x est un multiple de a. L'anneau $\mathbb{Z}[i]$ est donc commutatif intègre et tous ses idéaux sont principaux. Il est donc principal.

(7) C'est un cas particulier de la question **(b)** de l'exercice 7 de la feuille 6. Voir la solution de cette feuille. Cet homomorphisme envoie $X^2 + 1$ sur $i^2 + 1 = 0$. Son noyau contient donc l'idéal engendré par $X^2 + 1$. Réciproquement, si $P(X)$ est envoyé sur 0, on a $P(i) = 0$, autrement-dit, i est racine de $P(X)$, de même que $-i$ puisque $P(X)$ est à coefficients réels. Ainsi, $P(X)$ est divisible par $(X - i)(X + i) = X^2 + 1$. Toutefois, le quotient est a priori à coefficients rationnels. En fait il est à coefficients entiers, car quand on divise par un polynôme unitaire, on ne divise les coefficients que par 1. Ceci montre que le noyau de l'homomorphisme est inclus dans l'idéal engendré par $X^2 + 1$.

Comme 1 et i sont dans l'image de cet homomorphisme (ce sont les images de 1 et X) et comme 1 et i engendrent le groupe additif $\mathbb{Z}[i]$, l'homomorphisme est surjectif. La dernière affirmation résulte donc du théorème de passage au quotient.

II

(1) On a $2 = (1+i)(1-i)$, et $1+i$ et $1-i$ ne sont pas inversibles. 2 n'est donc pas irréductible dans $\mathbb{Z}[i]$.

(2) Si $p = a^2 + b^2$, on a $p = (a+ib)(a-ib)$. Or $a \pm ib$ ne peut pas être inversible puisque sa norme, qui est p, n'est pas 1.

(3) Si $a + ib$ (tel que $p = a^2 + b^2$) était un produit uv dans $\mathbb{Z}[i]$, on aurait $p = N(a+ib) = N(u)N(v)$. Mais comme p est premier, ceci implique que $N(u) = 1$ ou $N(v) = 1$, autrement-dit que u ou v est inversible. $a + ib$ (qui n'est pas inversible) est donc irréductible.

(4) On a par hypothèse $p = (a+ib)(c+id)$ dans $\mathbb{Z}[i]$, avec $a+ib$ et $c+id$ non inversibles. On a donc $p^2 = N(p) = N(a+ib)N(c+id) = (a^2+b^2)(c^2+d^2)$. Ainsi, a^2+b^2 et c^2+d^2, qui ne peuvent pas être 1, divisent p^2. Comme p est premier, la seule possibilité est $a^2 + b^2 = c^2 + d^2 = p$.

(5) En réduisant modulo 4 l'égalité $p = a^2 + b^2$, on obtient $3 = \alpha^2 + \beta^2$ (où $\alpha, \beta \in \mathbb{Z}/4\mathbb{Z}$, puisque p vaut 3 modulo 4. Toutefois, les carrés de $0, 1, 2, 3$ dans $\mathbb{Z}/4\mathbb{Z}$ sont $0, 1, 0, 1$. En faisant la somme de deux d'entre eux, il est impossible de faire 3.

(6) Rappelons que le nombre de racines d'un polynôme sur un corps commutatif ne peut pas excéder le degré de ce polynôme. Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre 4, il est racine du polynome $X^4 - 1 = (X-1)(X+1)(X^2+1)$. Or, 1 est d'ordre 1, -1 est d'ordre 2 (car p est impair). Un élément d'ordre 4 ne peut donc être qu'une racine du polynôme $X^2 + 1$. Si x est une racine de ce polynôme, il en est de même de $-x$. Or 0 est le seul élément égal à son opposé dans $\mathbb{Z}/p\mathbb{Z}$ puisque 2 est inversible (p est impair). Ainsi, $X^2 + 1$ ne peut pas avoir une racine double. Il ne peut donc y avoir dans $(\mathbb{Z}/p\mathbb{Z})^*$ que zéro ou deux éléments d'ordre 4. Il nous suffit donc de montrer qu'il y en a au moins un.

On a $p = 4k + 1$. Comme le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$ est $4k$ ($\mathbb{Z}/p\mathbb{Z}$ est un corps), il y a un 2-Sylow (d'ailleurs unique). Ce sous-groupe contient au moins 4 éléments puisque 4 divise $4k$. Or $(\mathbb{Z}/p\mathbb{Z})^*$ ne peut pas contenir plus de deux éléments d'ordre 2, puisque ces éléments doivent être des racines de $X^2 - 1$ (-1 est donc en fait le seul élément d'ordre 2). Il doit donc exister dans ce 2-Sylow un élément d'ordre 2^j pour un certain j, et donc un élément d'ordre 4.

(7) Notons α et β les deux éléments d'ordre 4 de $(\mathbb{Z}/p\mathbb{Z})^*$, c'est-à-dire les deux éléments distincts de 1 et de -1 qui sont racines du polynôme $X^4 - 1$ modulo p. Comme α et β sont les racines de $X^2 + 1$, on voit que leur somme est 0 et que leur produit est 1.

Considérons maintenant les éléments 1, -1, α, β, $i\alpha$ et $i\beta$ de $\mathbb{Z}[i]/p\mathbb{Z}[i]$. Ils sont deux à deux distincts. En effet, si dans cet anneau on a $a + ib = c + id$ c'est que $(a + c) + i(b + d) \in p\mathbb{Z}[i]$. Or $p\mathbb{Z}[i]$ est l'ensemble des $x + iy$ tels que les entiers x et y soient divisibles par p. Ainsi, comme groupe additif, $\mathbb{Z}[i]/p\mathbb{Z}[i]$ s'identifie à $(\mathbb{Z}/p\mathbb{Z})[i]$. Il en résulte que les 6 éléments ci-dessus sont distincts dans ce groupe. Or, ils vérifient tous l'équation $x^4 = 1$.

(8) Comme le polynôme $X^4 - 1$ a au moins 6 racines distinctes sur l'anneau $\mathbb{Z}[i]/p\mathbb{Z}[i]$ ce dernier ne peut pas être un corps. Il en résulte que p est réductible sur $\mathbb{Z}[i]$, autrement-dit que $p = uv$, où u et v sont deux éléments non inversibles de $\mathbb{Z}[i]$. On conclut comme dans la question II **(4)**.