Exercices du chapitre 7

Exercice : 7.1. Les irréductibles de $\mathbb{Z}[i]$ sont de norme 2 (pour $1+i$), ou p premier $\equiv 1 \bmod 4$ (pour π et $\overline{\pi}$ dans l'écriture $p = \pi\overline{\pi}$), ou p^2 avec $p \equiv 3 \bmod 4$. On a donc une bonne idée de la factorisation en irréductibles d'un $z \in \mathbb{Z}[i]$ en factorisant d'abord $\mathrm{N}(z)$ dans $\mathbb{Z}$.

On a $-3+15i = 3(-1+5i)$ et $\mathrm{N}(-1+5i) = 1+25 = 26 = 2 \cdot 13$. On sait que $1+i$ doit diviser $-1+5i$, et c'est bien le cas

$$\frac{-1+5i}{1+i} = \frac{1}{2}(-1+5i)(1-i) = \frac{1}{2}(4-6i) = 2-3i.$$

De plus $2-3i$ est irréductible (de norme 13), on a donc la décomposition en irréductibles $-3+15i = 2(1+i)(2-3i)$.

De même, on a $\mathrm{N}(4+7i) = 16+49 = 65 = 5 \cdot 13$. On a $5 = 1^2+2^2 = (1+2i)(1-2i)$, et les deux irréductibles de $\mathbb{Z}[i]$ de norme 5 sont donc les associés de $1 \pm 2i$. Un seul des deux divise $4+7i$. On a en effet

$$\frac{4+7i}{1+2i} = \frac{1}{5}(4+7i)(1-2i) = \frac{1}{5}(18-i), \text{ et}$$

$$\frac{4+7i}{1-2i} = \frac{1}{5}(4+7i)(1+2i) = \frac{1}{5}(-10+15i) = -2+3i.$$

On a donc la décomposition en irréductibles $4+7i = (1-2i)(-2+3i)$ dans $\mathbb{Z}[i]$. On aurait pu éviter tout calcul en observant que l'on a $4+7i \equiv -1+2i \bmod 5\mathbb{Z}[i]$, et donc c'est $1-2i$ qui divise $4+7i$ (car il divise 5).

Exercice 7.2. On va montrer que la seule solution est $(x,y) = (1,0)$. Soit $(x,y) \in \mathbb{Z}^2$ avec $y^2 = x^3 - 1$. On a dans $\mathbb{Z}[i]$ la relation $x^3 = y^2+1 = (y-i)(y+i)$. Vérifions que $y-i$ et $y+i$ sont premiers entre eux dans $\mathbb{Z}[i]$.

Sinon, il existe un irréductible π de $\mathbb{Z}[i]$ divisant $y+i$ et $y-i$. On a alors $\pi \,|\, (y+i)-(y-i) = 2i$, donc π divise 2, puis $\pi \sim 1+i$ car on a $2 = -i(1+i)^2$. Mais alors π divise $y^2+1 = x^3$, et $2 = \mathrm{N}(\pi)$ divise x^6, et x est pair. C'est absurde car alors on a $y^2 \equiv -1 \bmod 4$.

Comme $\mathbb{Z}[i]$ est factoriel, on en déduit que l'on a $y+i = uz^3$ avec $z \in \mathbb{Z}[i]$ et $u \in \mathbb{Z}[i]^\times$. On a $u = (u^{-1})^3$, puis $y+i = (uz)^3$. Écrivons $uz = a+bi$ avec $a,b \in \mathbb{Z}$. On a donc

$$y+i \;=\; (a+bi)^3 \;=\; (a^3-3ab^2)+(3ba^2-b^2)i,$$

puis $1 = b(3a^2-b^2)$. Cela entraîne $b = \pm 1$, puis $3a^2 = 1+b$, $b=-1$, $a=0$, $y=0$ puis $x=1$.

Exercice 7.3. Montrons le (i). Comme $\mathbb{Z}[i]$ a pour $\mathbb{Z}$-base $1, i$, le groupe abélien sous-jacent à $(2+2i)$ est engendré par $2+2i$ et $i(2+2i) = -2+2i$, ou ce qui revient au même par 4 et $2+2i$. Ces éléments sont $\mathbb{R}$-linéairement indépendants, donc $\mathbb{Z}$-libres.

Comme $1, 1+i$ est une $\mathbb{Z}$-base de $\mathbb{Z}[i]$, et comme $c+d(1+i)$ est dans $(2+2i)$ si, et seulement si, on a $c \equiv 0 \bmod 4$ et $d \equiv 0 \bmod 2$ par le (i), on en déduit que le morphisme de groupes additifs $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}[i]/(2+2i), (\overline{a},\overline{b}) \mapsto \overline{c+d(1+i)}$, clairement bien défini et surjectif, est un isomorphisme. Pour la condition demandée dans l'énoncé, on écrit $a+bi = a-b+b(1+i)$ et on a donc $b \equiv 0 \bmod 2$ et $a-b \equiv 3 \bmod 4$.

Pour le (iii), on renvoie au Complément 8 pour la structure d'anneau quotient, et on note $f : \mathbb{Z}[i] \to A$ la projection canonique (un morphisme d'anneaux). Posons $\epsilon = f(1+i)$. On a $i(2+2i) = (1+i)^3$ dans $\mathbb{Z}[i]$, et donc $\epsilon^3 = 0$ en appliquant f. On a aussi $(1+i)\mathbb{Z}[i] = 2\mathbb{Z}+(1+i)\mathbb{Z}$, et donc ϵA est l'ensemble des classes des $c+d(1+i)$ avec c pair. Il y a 4 tels éléments, tous non inversibles car $\epsilon^3 = 0$. Les 4 éléments restants sont ± 1 et $\pm 1+\epsilon \equiv \pm i$.

Montrons enfin le (iv). Soit π un irréductible de $\mathbb{Z}[i]$ non associé à $1+i$. On sait alors qu'il est premier à $1+i$, et donc par Bezout qu'il existe $u, v \in \mathbb{Z}[i]$ avec $u\pi + v(1+i) = 1$. En appliquant f on en déduit que $f(\pi)$ est inversible dans A. D'après le (iv), il existe une unique unité u de $\mathbb{Z}[i]$ tel que $f(u\pi) = f(u)f(\pi) \equiv 1 \bmod (2+2i)$ (noter que l'on a $3 \equiv -1$ dans A). Ainsi, $u\pi$ est l'unique associé de π qui est congru à 3 modulo $(2+2i)$.

Exercice 7.4. (i) Soit $n \in \mathbb{Z}$ et $(a,b) \in \mathbb{Z}^2$. On a $(a,b) \in \Sigma_n \iff n = \mathrm{N}(a+bi)$. Mais tout élément de $\mathbb{Z}[i]$ est produit d'une unité, de norme 1, et d'iréductibles, de norme 2, p premier $\equiv 1 \bmod 4$, ou p^2 avec p premier $\equiv 3 \bmod 4$. On en déduit que si σ_n est non vide alors pour tout premier $p \equiv 3 \bmod 4$ dans $\mathbb{Z}$ on a $\mathrm{v}_p(n)$ pair. Réciproquement, cette condition implique bien que n est somme de deux carrés. En effet, le produit de deux sommes de deux carrés est une somme de deux carré par la formule $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, de plus 2, les $p \equiv 1 \bmod 4$, et les p^2 avec $p \equiv 3 \bmod 4$, sont tous sommes de deux carrés (évident pour 2 et p^2, du cours pour les $p \equiv 1 \bmod 4$).

(ii) Pour $n \geqslant 1$ donné, le nombre $|\Sigma_n|$ d'éléments de $\mathbb{Z}[i]$ de norme n est de la forme $4a_n$ avec $a_n \geqslant 0$, à cause des 4 unités de $\mathbb{Z}[i]$. En utilisant que $\mathbb{Z}[i]$ est factoriel, la multiplicativité de la norme, et que la norme de chacun de ses irréductibles est une puissance d'un nombre premier, on constate que pour m et n premiers entre eux, et $z \in \Sigma_{mn}$, il existe une décomposirion $z = z_1 z_2$, avec z_1 et z_2 uniques modulo les unités, vérifiant $z_1 \in \Sigma_m$ et $z_2 \in \Sigma_n$. En particulier, on a $a_{mn} = a_m a_n$.

Pour $m, n \geqslant 1$ premiers entre eux, tout diviseur d de mn s'écrit de manière unique sous la forme ab avec $a|m$ et $b|n$. Regardant les restes modulo 4, on constate donc $\sigma_1(mn) = \sigma_1(m)\sigma_1(n) + \sigma_3(m)\sigma_3(n)$ et $\sigma_3(mn) = \sigma_1(m)\sigma_3(n) + \sigma_3(n)\sigma_1(n)$. Autrement dit, la fonction $n \mapsto b_n = \sigma_1(n) - \sigma_3(n)$ est multiplicative.

(iii) Il suffit donc de vérifier $a_n = b_n$ pour n une puissance d'un nombre premier.

– Les éléments de $\mathbb{Z}[i]$ de norme 2^k sont les $u(1+i)^k$ avec u unité, car l'unique irréductible (modulo unités) de norme une puissance de 2 est $1+i$, de norme 2. On a donc $a_{2^k} = 1$ pour tout $k \geqslant 0$. On a aussi $\sigma_1(2^k) = 1$ et $\sigma_3(2^k) = 0$, donc $b_{2^k} = 1$.

– Pour $p \equiv 1 \bmod 4$, disons $p = \pi\overline{\pi}$, les éléments de $\mathbb{Z}[i]$ de norme p^k sont les $u\pi^a\overline{\pi}^b$ avec u unité et $a+b=k$, car les uniques irréductibles (modulo unités) de norme une puissance de p sont π et $\overline{\pi}$, de norme p. On a donc $a_{p^k} = k+1$. On a aussi $\sigma_1(p^k) = k+1$ et $\sigma_3(p^k) = 0$, donc $b_{p^k} = k+1$.

– Pour $p \equiv 3 \bmod 4$, les éléments de $\mathbb{Z}[i]$ de norme p^k sont les $up^{k/2}$ avec u unité si k est pair, et il n'y en a pas si k est impair, car l'unique irréductible (modulo unités) de norme une puissance de p est p, de norme p^2. On a donc $a_{p^k} = 1$ ou 0 selon que k est pair ou impair. Pour k pair, on a $\sigma_1(p^k) = 1 + k/2$ et $\sigma_3(p^k) = k/2$. Pour k impair, on a $\sigma_1(p^k) = \sigma_3(p^k) = (1+k)/2$. On a toujours $a_{p^k} = b_{p^k}$.

Exercice 7.5. (i) On a vu en cours que $\mathbb{Z}[\sqrt{-3}]$ est non factoriel, donc non principal, en examinant l'identité $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. De même, $\mathbb{Z}[\sqrt{-4}] = \mathbb{Z} + 2\mathbb{Z}i$ est non factoriel à cause de l'identité $2 \cdot 2 = -(2i)(2i)$. En effet, $\mathbb{Z}[\sqrt{-4}]$ n'a pas d'élément de norme ± 2, puisque $x^2 + 4y^2 = \pm 2$ n'a aucune solution $x, y \in \mathbb{Z}$. Cela montre que ± 2 et $\pm 2i$ sont irréductibles. Ils sont non associés (!) car les inversibles de $\mathbb{Z}[2i]$ sont ± 1 (bien noter que $\pm i$ n'est pas dans $\mathbb{Z}[2i]$!).

(ii) L'équation $x^2 - dy^2 \leqslant 4$ avec $x, y \in \mathbb{Z}$ implique bien $y = 0$ et $x = 1$ ou 2.

(iii) On a clairement $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\alpha$. Ainsi, l'idéal $(2, \alpha) = 2(\mathbb{Z} + \alpha\mathbb{Z}) + \alpha(\mathbb{Z} + \alpha\mathbb{Z})$ est engendré comme groupe abélien par $2, \alpha, 2\alpha$ et α^2. Mais les éléments 2α et α^2 sont dans $2\mathbb{Z} + \alpha\mathbb{Z}$ (si d est pair on a $\alpha^2 = d$, et si d est impair on a $\alpha^2 = d - 1 + 2(1+\sqrt{d})$). On a donc bien $(2, \alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.

(vi) On déduit du (iii) que l'on a $(2,\alpha) \neq \mathbb{Z}[\sqrt{d}]$, car 1 n'est pas de la forme $2n+\alpha m$ avec $m,n \in \mathbb{Z}$ (on aurait $m=0$). Ainsi, si on suppose $(2,\alpha)=(z)$ avec $z \in \mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(z)>1$. Mais on a aussi $z|2$ car $2 \in (z)$, et donc $\mathrm{N}(z) \,|\, \mathrm{N}(2)=4$ dans $\mathbb{Z}$. D'après le (ii), cela implique $z=\pm 2$. Mais on a aussi $z|\,\alpha$ car $\alpha \in (z)$. Mais il est clair que 2 ne divise pas α (les multiples de 2 dans $\mathbb{Z}+\mathbb{Z}\alpha$ ont leurs coefficients en 1 et α qui sont des entiers pairs).

Exercice 7.6. (i) Soit $z \in I$ non nul. On constate $\mathrm{N}(z)=\overline{z}z \in I$. Mais $\mathrm{N}(z)$ est un entier non nul.

(ii) Comme on a $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}^2$, on a aussi $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. En particulier, c'est un groupe fini, et il n'a donc qu'un nombre fini de sous-groupes. On conclut car les sous-groupes de $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}]$ sont en bijection naturelle avec ceux de $\mathbb{Z}[\sqrt{d}]$ contenant $n\mathbb{Z}[\sqrt{d}]$ (dont les idéaux contenant n font partie).

(iii) Soit I un idéal non nul de A. On a vu que I contient $(n)=nA$ pour un certain entier $n \geqslant 1$. Observons que les sous-groupes de $\mathbb{Z}^2$ contenant $n\mathbb{Z}^2$ sont clairement de type fini, engendrés par $(n,0)$, $(0,n)$ et par un sous-ensemble de l'ensemble fini des (a,b) avec $0 \leqslant a,b<n$. On en déduit que tout idéal de A (isomorphe à $\mathbb{Z}^2$ comme groupe abélien) est finiment engendré comme groupe abélien, et donc *a fortiori* de type fini comme idéal. On a $nA \subset I$ et nA d'indice fini dans A, donc I est d'indice fini dans A (en clair, on a une surjection $A/nA \to A/I$).

(iv) On peut supposer $\mathrm{N}(z)$ non nul. On a $z \in zA$ donc $\mathrm{N}(z) \in zA$ et on a vu qu'il n'y a qu'un nombre fini d'ideaux de A contenant $\mathrm{N}(z)$.

Exercice 7.7. (i) C'est l'argument classique dû à Dirichlet. On regarde les $N+1$ éléments $k\alpha-[k\alpha]$ de $[0,1[$, avec $0 \leqslant k \leqslant N$. Consirérant la partition de $[0,1[$ en les N parties $[q/N,(q+1)/N[$ avec $0 \leqslant q<N$, on en déduit qu'il existe $0 \leqslant i<j \leqslant N$ avec $|(j\alpha-[j\alpha])-(i\alpha-[i\alpha])|<1/N$. Posons $q=j-i$ et $p=[j\alpha]-[i\alpha]$, on a $1 \leqslant q<N$ et $|p-q\alpha|<1/N$.

(ii) On choisit $p_n \in \mathbb{Z}$ et $1 \leqslant q_n$ avec $|p_n-q_n\sqrt{d}|<1/n$ et $1 \leqslant q_n \leqslant n$. On a donc $|p_n|<1/n+|q_n|\sqrt{d} \leqslant 1/n+n\sqrt{d}$ puis $|\mathrm{N}(p_n-q_n\sqrt{d})|<1/n(1/n+n\sqrt{d})<1+\sqrt{d}$. On conclut en posant $x_n=p_n-q_n\sqrt{d}$ (nécessairement non nul car $q_n \neq 0$).

(iii) Comme l'ensemble des $\mathrm{N}(x_n)$ est fini (des entiers bornés), quitte à extraire (x_n) on peut supposer qu'il existe $k \in \mathbb{Z}$ avec $\mathrm{N}(x_n)=k$ pour tout n et $x_n \to 0$. De même, comme on a $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}]=\mathbb{Z}/k\mathbb{Z}\overline{1} \oplus \mathbb{Z}/k\mathbb{Z}\overline{\sqrt{d}}$, un ensemble fini, on peut supposer que $x_n \bmod k\mathbb{Z}[\sqrt{d}]$ est constante. Comme $k\mathbb{Z}[\sqrt{d}]$ est un idéal de $\mathbb{Z}[\sqrt{d}]$, on peut multiplier les congruences, et on en déduit que la classe $x_m\overline{x_n} \bmod k\mathbb{Z}[\sqrt{d}]$ ne dépend pas de $n,m \geqslant 1$. Pour $m=n$ on a $x_n\overline{x_n}=\mathrm{N}(x_n)=k \equiv 0 \bmod k\mathbb{Z}[\sqrt{d}]$. On a donc $x_m\overline{x_n} \in k\mathbb{Z}[\sqrt{d}]$ pour tout $m,n \geqslant 1$.

(iv) Posons $x_m\overline{x_n}=ky_{m,n}$ pour un certain $y_{m,n} \in \mathbb{Z}[\sqrt{d}]$. En prenant la norme on a $k^2=\mathrm{N}(x_m)\mathrm{N}(x_n)=k^2\mathrm{N}(y_{m,n})$, puis $y_{m,n} \in \mathbb{Z}[\sqrt{d}]^\times$ pour tout m,n. On a $y_{m,n} \to 0$ et $y_{m,n} \neq 0$, on a donc construit une infinité d'unités.

Exercice 7.8. (i) Soit $M=\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ la matrice dont les colonnes sont les deux vecteurs donnés. Son déterminant est $ad-bc$, non nul par hypothèse. Soit $G \subset \mathbb{Z}^2$ le sous-groupe engendré par (a,b) et (c,d). On veut montrer qu'il est d'indice fini $|\det M|$. Pour $P \in \mathrm{GL}_2(\mathbb{Z})=\mathrm{Aut}(\mathbb{Z}^2)$, $P(G)$ a même indice que G dans $\mathbb{Z}^2$. Il est engendré par les deux colonnes de PM, qui est de déterminant $\det P \det M=\pm\det M$. On peut donc à loisir multiplier à gauche M par des éléments de $\mathrm{GL}_2(\mathbb{Z})$. En utilisant des transvections standards, on peut remplacer (a,b) par (a,b') (resp. (a',b)) où b' est le reste de la division

euclidienne de b par a (resp. de a par b). Après un nombre fini d'itérations, on se ramène donc au cas $a = 0$ ou $b = 0$. Par symétrie, on peut donc supposer $b = 0$, et on a $ad \neq 0$. Mais le sous-groupe H de $\mathbb{Z}^2$ engendré par $(1, 0)$ et (c, d) est d'indice $|d|$ dans $\mathbb{Z}^2$, car c'est le noyau de $(x, y) \mapsto y \bmod d$, et G est d'indice $|a|$ dans H, car c'est le noyau de $x(1, 0) + y(c, d) \mapsto x \bmod a$. Ainsi, G est bien d'indice $|ad|$ dans $\mathbb{Z}^2$.

(ii) Le groupe abélien A est libre de rang 2 engendré par 1 et $\sqrt{d}$. Écrivons $z = a+b\sqrt{d}$ avec $a, b \in \mathbb{Z}$. Le sous-groupe Az de A est engendré par $z = a + b\sqrt{d}$ et $z\sqrt{d} = bd + a\sqrt{d}$. Mais le sous-groupe de $\mathbb{Z}^2$ engendré par (a, b) et (bd, a) est d'indice fini égal à $a^2 - db^2 \neq 0$ par le (i). On conclut car $\mathrm{N}(z) = a^2 - db^2$.

Exercice 7.9. (i) Si on a $I = xA$ avec $x \neq 0$ alors on a clairement $I \sim A$. Réciproquement, si on a $aI = bA$ avec a, b non nuls, on a $b \in aI \subset aA$ et donc $b = ac$ pour un certain $c \in A$, puis $aI = acA$, et comme A est intègre, $I = cA$ est principal.

(ii) On a toujours $[A] \in \mathrm{Cl}(A)$, et par le (i) A est principal si, et seulement si, on a $\mathrm{Cl}(A) = \{[A]\}$.

Exercice 7.10. (i) Si la largueur du rectangle est 1, les disques roses sont de rayon 1 et centrés aux sommets du rectangle, les disques oranges sont de rayon 1/2. La longueur du rectangle est donc $\sqrt{3}/2 + 1 + \sqrt{3}/2 = 1 + \sqrt{3}$. Cela conclut.

(ii) On a $3 < 2\sqrt{3}$ et donc $\sqrt{|d|} \leqslant \sqrt{7} < 1 + \sqrt{3}$. On pose $z = a/b$. Par le (i), il existe $q \in A$ avec soit $\mathrm{N}(a/b - q) < 1$, soit $\mathrm{N}(a/b - q/2) < 1/4$. On a $\mathrm{N}(r) < \mathrm{N}(b)$ avec $r = a - qb$ dans le premier cas, et $r = 2a - qb$ dans le second.

(iii) On choisit $z \in I$ non nul et avec $\mathrm{N}(z)$ minimal. On a $Az \subset I$ car I est un idéal. Soit $a \in I$ non nul. Par le (ii), on peut écrire soit $a = qz + r$, soit $2a = qz + r$, avec $\mathrm{N}(r) < \mathrm{N}(z)$. On a $r \in I$ et donc $r = 0$ dans les deux cas, par choix de z. On a donc $z \,|\, 2a$ dans les deux cas, puis $2I \subset Az$. On a montré $zA \subset I \subset \frac{1}{2}zA$. En multipliant ces inclusions par l'élément $\frac{2}{z} \in \mathbb{Q}[\sqrt{d}]^\times$, elles s'écrivent aussi $2A \subset I' \subset A$ avec $I' = \frac{2}{z}I$, qui est donc un idéal non nul de A. Il vérifie $zI' = 2I$: il est équivalent à I.

(iv) Soit I un idéal de A contenant $2A$. On a $A = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Le groupe quotient $A/2A \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a donc pour représentants $0, 1, \alpha, \alpha + 1$. Si I contient 1 on a $I = A$. Si I contient α on a $J \subset I$, puis $I = J$ ou $I = A$ car J est d'indice 2. Enfin, si I contient $\alpha + 1$, alors I contient aussi $\alpha(\alpha + 1) = \alpha^2 + \alpha$. Si d est pair on a $\alpha^2 = d \in 2\mathbb{Z} \subset I$, donc I contient α, puis $1 = 1 + \alpha - \alpha$, et donc $I = A$. De même, si d est impair on a $\alpha^2 = 2\alpha + d - 1$ et donc $\alpha(\alpha + 1) + \alpha = 3\alpha + d - 1 \in \alpha + 2A$, et donc $\alpha \in I$ puis encore $1 \in I$ et donc $I = A$.

(v) D'après (iii) et (iv), tout idéal non nul de A est équivalent à $2A$, J ou A. Comme A et $2A$ sont principaux, on a $\mathrm{Cl}(A) = \{[A], [J]\}$. On en déduit que l'idéal J est principal si, et seulement si, A est principal, par l'Exercice 7.9. On a vu que J n'est pas principal pour $d < -4$ dans l'Exercice 7.5. Pour $d = -3$, on a vu que A est non factoriel en cours, donc non principal, donc J est non principal aussi dans ce cas.

Exercice 7.11. (i) On a $j^2 + j + 1 = 0$, donc $j^2 = -j - 1$, ce qui implique que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$. On observera que pour $z \in \mathbb{Z}[j]$, on a $\overline{z} \in \mathbb{Z}[j]$ (conjugaison complexe) car $\overline{j} = j^2 = -j - 1$.

(ii) On a $j^3 = 1$ donc les 6 éléments donnés sont dans $\mathbb{Z}[j]^\times$. Réciproquement, si on a $\alpha\beta = 1$ avec α, β dans $\mathbb{Z}[j]$, alors on a $|\alpha|^2|\beta|^2 = 1$ avec $|\alpha|^2, |\beta|^2 \in \mathbb{Z}$ par la formule ci-dessus, puis donc $|\alpha|^2 = 1$. Posons $\alpha = a+bj$ avec $a, b \in \mathbb{Z}$. Cela s'écrit aussi $a^2-ab+b^2 = 1$, et en multipliant par 4, $(2a - b)^2 + 3b^2 = 4$. Les seules solutions ce cette équation sont $(a, b) = (\pm 1, 0)$, $(a, b) = (0, \pm 1)$ et $(a, b) = \pm(1, 1)$, qui sont les 6 solutions déjà trouvées.

(iii) En raisonnant comme dans le cours, il suffit de montrer que pour tout $z \in \mathbb{C}$ il existe $q \in \mathbb{Z}[j]$ tel que $|z-q|^2 < 1$. Posons $z = a+bj$, $u, v \in \mathbb{Z}$ et $q = u+vj$. On a

$$4|z-q|^2 = (2(a-u)-(b-v))^2 + 3(b-v)^2.$$

On peut choisir $v \in \mathbb{Z}$ tel que $|b-v| \leqslant 1/2$, puis $u \in \mathbb{Z}$ tel que $|2a-(b-v)-2u| \leqslant 1$. On a alors bien $4|z-q|^2 \leqslant 1+3/4 < 4$.

(iv) On a montré que $\mathbb{Z}[j]$ est euclidien, donc principal et factoriel. Soit $p \equiv 1 \bmod 3$ un nombre premier. On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ a un élément d'ordre 3 (Gauss ou Cauchy), de sorte que le polynôme $X^3-1 = (X-1)(X^2+X+1)$ a une racine $\neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi, il existe un entier $n \in \mathbb{Z}$ tel que $n^2+n+1 \equiv 0 \bmod p$. Mézalor p divise $n^2+n+1 = (n-j)(n-j^2)$ dans $\mathbb{Z}[j]$. Si p était irréductible, donc premier, il diviserait $n+j$ ou $n+j^2$: absurde car le coefficient en j de $n+j$ et $n+j^2$ est ± 1, qui n'est pas multiple de p dans $\mathbb{Z}$. Ainsi, p est réductible, et s'écrit donc $\alpha\beta$ avec $|\alpha|^2, |\beta|^2 > 1$ par le (ii). De $p^2 = |\alpha|^2|\beta|^2$, et $|\alpha|^2, |\beta|^2 \in \mathbb{Z}$, on déduit $p = |\alpha|^2$. On a donc $p = \alpha\overline{\alpha}$ pour un certain $\alpha \in \mathbb{Z}[j]$. Écrivons $\alpha = a+bj$ avec $a, b \in \mathbb{Z}$, et donc $p = a^2-ab+b^2$. Les associés de α sont

$$a+bj, -a-bj, -b+(a-b)j, b-(a-b)j, -(a-b)-aj \text{ et } (a-b)+aj.$$

On a aussi $\overline{\alpha} = (a-b)-jb$. Il n'est pas dans la liste ci-dessus ! En effet, sinon on aurait soit $b = -b = 0$, soit $b = 2a$, soit $a = 2b$, soit $b = \pm a$, et tous ces cas sont exclus par $a^2-ab+b^2 = p$ (premier impair).

(v) Comme dans le cours, $\mathbb{Z}[j]$ étant factoriel il y a exactement $6+6 = 12$ éléments de $\mathbb{Z}[j]$ de norme p, à savoir les $u\alpha$ et les $u\overline{\alpha}$ avec $u \in \mathbb{Z}[j]^\times$.

(vi) Si on a $p = a^2-ab+b^2$ avec $(a,b) \in \mathbb{Z}$. On a vu que les 12 écritures possibles sont obtenues en remplaçant (a,b) par les 6 couples suivants et leurs opposés :

$$(a,b),\ (-b,a-b),(a-b,a),(a-b,-b),(b,a) \text{ et } (-a,b-a).$$

Les couples (c,d) avec $p = c^2+3d^2$ correspondent bijectivement aux (a,b) avec $p = a^2-ab+b^2$ et b pair, via $(c,d) = (a-b/2, b/2)$, via l'identité

$$a^2-ab+b^2 = (a-b/2)^2+3(b/2)^2.$$

De plus, si on a (a,b) avec $p = a^2-ab+b^2$, alors a ou b est impair. En considérant (a,b), (b,a) et $(-b,a-b)$ on constate que l'un au moins des couples ci-dessus à sa seconde coordonnée paire. Quitte à prendre ce couple pour couple (a,b) de départ, on peut donc supposer b pair et a impair. On constate alors que parmi les 6 couples ci-dessus, seuls (a,b) et $(a-b,-b)$ ont leur seconde coordonnée paire. Ajoutant leurs opposés, les 4 uniques couples (c,d) avec $p = c^2+3d^2$ sont donc $\pm(a-b/2, b/2)$ et $\pm(a-b/2, -b/2)$. Autrement dit, si (c,d) est l'une de ces 4 écritures, les autres sont $(\pm c, \pm d)$: c'est l'assertion d'unicité cherchée.

Exercice 7.12. (i) On démontre comme pour $\mathbb{Z}[\sqrt{d}]$ que les unités de A_d sont ses éléments de norme ± 1. On a

$$4(x^2 + xy + \frac{1-d}{4}y^2) = (2x+y)^2 - dy^2.$$

Pour $d < -3$ et $x, y \in \mathbb{Z}$, le terme de droite est égal à 4 si, et seulement si, $y = 0$ et $x = \pm 1$. Cela prouve exactement $\mathrm{A}_d^\times = \{\pm 1\}$ dans ce cas. Pour $d = -3$, on a aussi $\pm(1,1)$ et $\pm(0,1)$ comme on l'a déjà vu dans l'Exercice 7.11, ce qui donne $\mathrm{A}_{-3} = \mu_6$.

(ii) Les démonstrations sont les même verbatim. Vérifions par exemple $|A/zA| = |\mathrm{N}(z)|$ pour $A = \mathrm{A}_d$ et $z \in \mathrm{A}_d$ non nul. Le groupe abélien A est libre de rang 2 engendré par 1 et τ_d. Écrivons $z = a+b\tau_d$ avec $a, b \in \mathbb{Z}$. Le sous-groupe Az de A est engendré par $z = a+b\tau_d$ et $z\tau_d = a\tau_d + b(\tau_d + \frac{d-1}{4}) = b\frac{d-1}{4} + (a+b)\tau_d$. Mais le sous-groupe de $\mathbb{Z}^2$ engendré par (a,b) et $(b\frac{d-1}{4}, a+b)$ est d'indice fini égal à $|a(a+b) + b^2\frac{1-d}{4}|$ par le (i) de l'Exercice 7.8, car on a $\mathrm{N}(z) = a^2+ab+\frac{1-d}{4}b^2 \neq 0$.

Exercice 7.13. C'est la même démonstration que pour la question (iii) de l'Exercice 7.11. On utilise au final que l'on a $1 + \frac{|d|}{4} < 4$ pour $|d| = 3, 7, 11$.

Exercice 7.14. (i) La méthode est la même que dans l'Exercice 7.10. Pour changer, on procède algébriquement plutôt que géométriquement. Soit $z \in \mathbb{C}$. Montrons qu' il existe $u, v \in \mathbb{Z}$ tel que l'on a soit $|z - (u + \alpha v)|^2 < 1$, soit $|z - (u + \alpha v)/2|^2 < 1/4$. Écrivons $z = x + y\,\alpha$ avec $x, y \in \mathbb{R}$. On a

$$|z - (u + \alpha v)|^2 \;=\; \frac{1}{4}\left(2(x-u) + (y-v))^2 + 19(y-v)^2\right).$$

Posons $r = \sqrt{\frac{3}{19}}$ (on a $r \simeq 0.397$). Supposons d'abord qu'il existe $v \in \mathbb{Z}$ tel que $|y - v| < r$. On peut bien sûr choisir $u \in \mathbb{Z}$ avec $|2x + (y - v) - 2u| \leqslant 1$, et on a alors

$$|z - (u + \alpha v)|^2 \leqslant \frac{1}{4}(1 + 19r^2) < 1.$$

(Cela explique bien sûr le choix de r). Sinon, la distance de y à $1/2 + \mathbb{Z}$ est $\leqslant s$ avec $s := 1/2 - r \simeq 0.103$. On peut donc trouver $v \in \mathbb{Z}$ avec $|y - v/2| \leqslant s$ et $u \in \mathbb{Z}$ tel que $|2(x - u/2) + (y - v/2)| \leqslant 1/2$, de sorte que l'on a

$$|z - (u + \alpha v)/2|^2 \;=\; \frac{1}{4}\left(2(x - u/2) + (y - v/2))^2 + 19(y - v/2)^2\right) \leqslant \frac{1}{4}\left(\frac{1}{4} + 19s^2\right).$$

On conclut car on a $1/4 + 19s^2 \simeq 0.26 < 1$.

(ii) Posons $\alpha = \tau_{-19}$ et $A = \mathrm{A}_{-19} = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Alors $A/2A$ a pour représentants $0, 1, \alpha$ et $1 + \alpha$. Mais on a $\alpha^2 - \alpha + 5 = 0$, et donc $\alpha(1 + \alpha) = -5 \in 1 + 2A$. Ainsi, si I est un idéal de A contenant $2A$, on a soit $I = 2A$, soit $1 \in I$, et donc $I = A$.

(iii) Le même argument que dans l'Exercice 7.10 montre, à partir du (i), que tout idéal non nul de A est équivalent à un idéal contenant $2A$, *i.e.* à A ou à $2A$. Donc tout idéal est équivalent à un idéal principal, *i.e.* est principal.

Exercice 7.15. (i) Par hypothèse, on a $\{0\} \cup A^\times \subsetneq A$. On peut donc trouver $z \in A$ non nul, et non unité, tel que l'entier $\varphi(z)$ est minimal. Soit $a \in A$. Comme A est euclidien pour φ, on peut écrire $a = qx + r$ avec soit $r = 0$, soit $r \neq 0$ et $\varphi(r) < \varphi(x)$. Dans le second cas, on en déduit que r est une unité. On a montré que $\{0\} \cup A^\times$ contient des représentants de A/xA.

(ii) Pour $d < 0$ et $x, y \in \mathbb{Z}$, on a $4\mathrm{N}(x + y\tau_d) = (2x - y)^2 + |d|y^2$. On cherche à savoir quand cette quantité peut être égale à $2.4 = 8$ ou $3.4 = 12$. Pour $|d| > 11$ et $d \equiv 1 \bmod 4$, et donc $|d| \geqslant 15$, cela force $y = 0$, et il n'y a pas de solution car ni 8 ni 12 n'est un carré.

(iii) Pour $d < -3$ on a aussi $|\mathrm{A}_d^\times| = 2$. On en déduit que si x est comme au (i), on a A/xA de cardinal $1, 2$ ou 3. Mais $A = xA$ est impossible car x n'est pas une unité, on a donc $|A/xA| = 2$ ou 3. Mais d'après l'exercice 7.12 (ii) on a $|A/xA| = |\mathrm{N}(x)|$, ce qui contredit le (ii).

Exercice 7.25. (i) On a $\varphi(n) \leqslant |n|$ pour tout $n \in \mathbb{Z}$. Pour $m, n \in \mathbb{Z}$ avec $n \neq 0$, la division euclidienne de m par n sécrit $m = qn + r$ avec $0 \leqslant r < |n|$. Cela conclut si n est pair. Si n est impair, disons $|n| = 2k + 1$, on constate que quitte à remplacer q par $q \pm 1$ et r par $r - |n|$ si nécessaire, on peut supposer $|r| \leqslant k$, et donc $\varphi(r) \leqslant |r| \leqslant k = \varphi(n)$.

(ii) On pose $\varphi(2) = x$ avec $x \geqslant 2$. Pour $m, n \in \mathbb{Z}$ avec $n \neq 0$, la division euclidienne de m par n sécrit $m = qn + r$ avec $0 \leqslant r < |n|$. Si on a $n = 2$, alors $0 \leqslant r \leqslant 1$ et donc $\varphi(r) = r < 2 \leqslant \varphi(x)$. On suppose donc $n \neq 2$, en particulier $\varphi(n) = |n|$. Si on a $r \neq 2$, ou $r = 2$ et $|n| > x$, on a bien $\varphi(r) < \varphi(n)$. Dans le cas restant on a $r = 2$ et $3 \leqslant |n| \leqslant x$. Mais alors l'égalité $m = (q \pm 1)n + 2 - |n|$, et l'inégalité $2 - x \leqslant 2 - |n| \leqslant -1$ montre $\varphi(2 - |n|) = |n| - 2 < \varphi(n) = |n|$.

Exercice 7.27. (i) On constate que l'on a $\mathrm{E}_n(\mathbb{Z}) = \{k \in \mathbb{Z} \mid 0 < |k| < 2^n\}$. En effet, c'est clair pour $n = 0$. De plus, pour $m \in \mathbb{Z}$ on constate que $\mathbb{Z}/m\mathbb{Z}$ est recouvert par les classes des entiers $\pm k$ avec $|k| < 2^n$ si, et seulement si, on a $0 < |m| < 2^{n+1}$, et on conclut par récurrence. Enfin, pour $m \in \mathbb{Z}$ non nul on a montré que $\upsilon(m)$ est le plus petit entier n tel que $|m| < 2^{n+1}$. Autrement dit, $\upsilon(m)$ vaut le nombre de chiffres de m dans son écriture en base 2, moins 1.

(ii) Par division euclidienne, on constate par récurrence sur $n > 0$ que $\mathrm{E}_n(k[X])$ est l'ensemble des polynômes non nuls et de degré $\leqslant n$ dans $k[X]$. On a donc $\nu = \deg$.

(iii) On a $x \in \mathrm{E}_1(A) \iff Ax = A \iff x \sim 1 \iff x \in A^\times$. On a clairement $\mathrm{E}_0(A) \subset \mathrm{E}_1(A)$ et $\mathrm{E}_1(A) = A^\times \subset \mathrm{E}_2(A)$. Mais pour $X, Y \subset A$ avec $X \subset Y$, et $a \in A$, alors $aA + X = A$ implique évidemment $aA + Y = A$. On en déduit $\mathrm{E}_n(A) \subset \mathrm{E}_{n+1}(A)$ pour tout $n \geqslant 0$ par récurrence sur n.

(iv) Soit $a \in A$ non nul avec $\varphi(a) \leqslant n$. Il suffit de montrer que l'on a $\upsilon(a) \leqslant n$, *i.e.* $a \in \mathrm{E}_{n+1}(A)$. On procède par récurrence sur $n \geqslant 0$. Supposons $n = 0$. Par euclidianité et $\varphi(a) = 0$, on a $1 = aq + r$ avec $r = 0$, donc $a \in A^\times = \mathrm{E}_1(A)$ par le (i). Pour n général, on constate par euclidianité que A/aA est recouvert par les classes de 0 et des $b \in A$ non nuls avec $\varphi(b) < \varphi(a) \leqslant n$. Par récurrence et le (iv), un tel b est dans $\mathrm{E}_n(A)$, ce qui montre bien que a est dans $\mathrm{E}_{n+1}(A)$.

(v) Supposons enfin $A = \mathrm{Eucl}(A) \cup \{0\}$, de sorte que υ est bien définie sur $A \smallsetminus \{0\}$. Soient $a, b \in A$ avec $b \neq 0$. Posons $n = \nu(b)$. On a $b \in \mathrm{E}_{n+1}(A)$ donc la classe de a dans A/bA est soit nulle, soit celle d'un certain $r \in \mathrm{E}_n(A)$. Autrement dit, on a $a - r \in bA$ avec soit $r = 0$, soit $\upsilon(r) < n = \upsilon(b)$.