Correction devoir maison 2

Exercice 1

(a) $Q(X) = 2X^5 + 5X^4 + 8X^3 + 7X^2 + 4X + 1$, donc $Q'(X) = 10X^4 + 20X^3 + 24X^2 + 14X + 4$. Par divisions euclidiennes successives, on trouve :

$$Q(X) = Q'(X)(\frac{1}{5}X + \frac{1}{10}) + \frac{3}{5}(2X^3 + 3X^2 + 3X + 1)$$
$$Q'(X) = (2X^3 + 3X^2 + 3X + 1)(5X + \frac{5}{2}) + \frac{3}{2}(X^2 + X + 1)$$
$$2X^3 + 3X^2 + 3X + 1 = (X^2 + X + 1)(2X + 1) \ .$$

Le dernier reste non nul est $\frac{3}{4}(X^2 + X + 1)$, donc le pgcd de Q et Q' est $X^2 + X + 1$. Les racines multiples de Q sont les racines de Q qui sont aussi racines de Q', donc ce sont les racines de leur pgcd $X^2 + X + 1 = (X - j)(X - j^2)$, où $j = \exp(\frac{2i\pi}{3}) \in \mathbb{C}$. Q a donc deux racines multiples dans $\mathbb{C}$, à savoir j et j^2.

(b) j et j^2 sont racines de Q de multiplicité au moins 2 , donc $(X-j)^2(X-j^2)^2 = (X^2+X+1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1$ divise Q. La division euclidienne donne alors la factorisation de Q en produit d'irréductibles de $\mathbb{R}[X]$:

$$Q(X) = (2X + 1)(X^2 + X + 1)^2 \ ,$$

vu que $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$ (son discriminant est < 0).

Exercice 2

(a) (i) On va montrer la *contraposée* de l'équivalence demandée : P est réductible si et seulement si P a une racine dans K.

$$\begin{aligned} P \text{ est réductible} &\Leftrightarrow \exists\, Q, R \in K[X] \text{ non inversibles tels que } P = QR \\ &\Leftrightarrow \exists\, Q, R \in K[X] \text{ avec } \deg(Q) = 1 \text{ ou } \deg(R) = 1 \text{ et } P = QR \\ &\Leftrightarrow P \text{ a une racine dans } K \ . \end{aligned}$$

On en déduit l'équivalence demandée car, si A et B sont deux propositions quelconques, l'implication $(A \Rightarrow B)$ est *équivalente* à l'implication $(\text{non}(B) \Rightarrow \text{non}(A))$.

(ii) Supposons $b^3 + ab^2 + a^3 = 0$ avec $(a, b) \in \mathbb{Z}^2$ premiers entre eux, alors $b^3 = -a(b^2 + a^2)$, si bien que tout diviseur premier de a divise b^3 ; il s'ensuit que a n'a pas de diviseur premier, c'est-à-dire $a = \pm 1$. On obtient de même que $b = \pm 1$, puis on vérifie que cela contredit l'hypothèse $b^3 + ab^2 + a^3 = 0$.
Cette équation n'a donc pas de solution $(a, b) \in \mathbb{Z}^2$ avec a et b premiers entre eux.

(iii) Supposons $1 + X + X^3$ réductible dans $\mathbb{Q}[X]$, alors ce polynôme a une racine dans $\mathbb{Q}$ d'après la question (a-i). Ecrivons celle-ci $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$ premiers entre eux, alors $1 + \frac{a}{b} + (\frac{a}{b})^3 = 0$, d'où $b^3 + ab^2 + a^3 = 0$. Mais ceci est impossible d'après la question (a-ii). Le polynôme $1 + X + X^3$ est donc irréductible dans $\mathbb{Q}[X]$.

(b) On obtient aisément que X^4+1 est irréductible sur $\mathbb{Q}$ si et seulement si il n'est divisible par aucun polynôme de degré 1 ou 2 de $\mathbb{Q}[X]$.
S'il était divisible par un polynôme de $\mathbb{Q}[X]$ de degré 1, il aurait une racine $\frac{a}{b}$ dans $\mathbb{Q}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}\setminus\{0\}$, ce qui entraînerait $a^4 = -b^4$, ce qui est impossible car $a^4 \geq 0$ et $-b^4 < 0$; X^4+1 n'est donc divisible par aucun polynôme de degré 1 de $\mathbb{Q}[X]$.
S'il était divisible par un polynôme de $\mathbb{Q}[X]$ de degré 2, on aurait

$$X^4+1 = (X^2+aX+b)(X^2+cX+d) = X^4+(a+c)X^3+(ac+b+d)X^2+(ad+bc)X+bd \ ,$$

avec $a,b,c,d \in \mathbb{Q}$. On en tire $a=-c$ et $bd=1$, puis $b+d=a^2$ et $a(d-b)=0$, donc $d=b$ ou $a=0$. Le cas $a=0$ est impossible car alors $b=-d$ d'où $b^2=-1$. Donc $b=d$, d'où $b^2=1$ donc $b=\pm 1$ et $2b=a^2$ donc $a^2=\pm 2$, ce qui est impossible pour $a \in \mathbb{Q}$. X^4+1 n'est donc divisible par aucun polynôme de degré 2 de $\mathbb{Q}[X]$, ce qui termine la preuve de son irréductibilité.

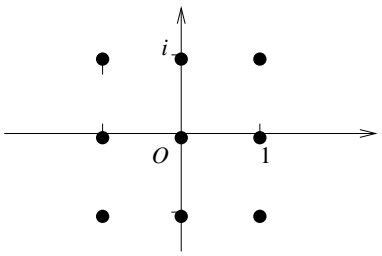
Exercice 3

1. Si $P \in \mathbb{R}[X]$ irréductible divise A et B, alors P divise $A^2+B^2=C^2$ donc P divise C par le lemme de Gauss ; ceci contredit l'hypothèse sur les diviseurs communs aux trois polynômes, donc aucun irréductible ne divise A et B, c'est-à-dire qu'ils sont premiers entre eux. On montre de même que A et C sont premiers entre eux, ainsi que B et C.
2. On raisonne par l'absurde : supposons que C ait une racine réelle α, alors $A(\alpha)^2+B(\alpha)^2=0$, donc $A(\alpha)=0=B(\alpha)$, ce qui entraîne que $X-\alpha$ divise A, B et C dans $\mathbb{R}[X]$ et contredit les hypothèses. Ainsi C n'a pas de racine réelle.
3. Soit P un diviseur commun à $C-B$ et $C+B$, alors P divise la somme $C-B+C+B=2C$ et la différence $C-B-C-B=-2B$, si bien que P est un diviseur commun à B et C, donc $P \in \mathbb{R}^\times$ d'après la question 1. Ceci montre que $C-B$ et $C+B$ sont premiers entre eux. A fortiori ils sont non nuls ; comme de plus ils sont de degrés ≤ 2 tandis que A^2 est de degré 4, aucun d'eux n'est divisible par A^2.
4. On note que $A^2=(C-B)(C+B)$ et A^2 ne divise aucun des deux facteurs. Donc, si A était irréductible, on aurait $A=u(C-B)=v(C+B)$ avec $u,v \in \mathbb{R}^\times$, par unicité de la décomposition en produits d'irréductibles, et $C-B$ ne serait pas premier à $C+B$, ce qui contredit le résultat de la question précédente. A est donc le produit de deux polynômes de degré 1. Ces deux polynômes sont distincts, car $A=P^2$ avec P irréductible entraîne que P est un diviseur commun à $C-B$ et $C+B$, par le même raisonnement que ci-dessus. A a donc deux racines réelles distinctes.
5. On a $A^2(X)=(X-a)^2(X-a')^2=(C-B)(C+B)$ donc, puisque $C-B$ et $C+B$ sont premiers entre eux, on obtient $C-B=u(X-a)^2$ et $C+B=\frac{1}{u}(X-a')^2$ avec $u \in \mathbb{R}^\times$ (quitte à échanger a et a'). On en tire $C=\frac{u}{2}(X-a)^2+\frac{1}{2u}(X-a')^2$ et $B=\frac{1}{2u}(X-a')^2-\frac{u}{2}(X-a)^2$. Si A n'est pas unitaire, B et C doivent avoir le même cœfficient dominant que A au signe près. Finalement, l'ensemble des triplets (A,B,C) solutions du problème est

$$\Big\{\Big(\alpha(X-a)(X-a'), \frac{\varepsilon_1\alpha}{2u}(X-a')^2-\frac{\varepsilon_1\alpha u}{2}(X-a)^2, \frac{\varepsilon_2\alpha u}{2}(X-a)^2+\frac{\varepsilon_2\alpha}{2u}(X-a')^2\Big), \\ \alpha,u \in \mathbb{R}^\times, a \neq a' \in \mathbb{R}, \varepsilon_1,\varepsilon_2 \in \{-1,1\}\Big\} \ .$$

Exercice 4

1. Les nombres $a \in \mathbb{Z}[i]$ avec $-1 \leq \mathrm{Re}(a) \leq 1$ et $-1 \leq \mathrm{Im}(a) \leq 1$ sont représentés par les points suivants du plan complexe :



   Les autres éléments de $\mathbb{Z}[i]$ s'obtiennent à partir d'un de ces 9 points en lui appliquant les translations horizontales et verticales de longueurs entières (par exemple).

2. Soit $z \in \mathbb{C}$, alors $k(z)$ est le nombre de points de $\mathbb{Z}[i]$ à l'intérieur du disque de centre z et de rayon 1 (le bord étant exclus). La distance entre deux points de $\mathbb{Z}[i]$ étant toujours ≥ 1, on en conclut que $k(z) = 1$ lorsque $z \in \mathbb{Z}[i]$.

3. Soit $z \in \mathbb{C}$:

   (i) La translation $z \mapsto z - 1$ est une application de $\mathbb{Z}[i]$ dans lui-même, qui admet une application réciproque $(z \mapsto z + 1)$; c'est donc une bijection. On en déduit :

$$\begin{aligned} k(z+1) &= \mathrm{Card}\,\{a \in \mathbb{Z}[i],\ |z+1-a| < 1\} \\ &= \mathrm{Card}\,\{a \in \mathbb{Z}[i],\ |z-(a-1)| < 1\} \\ &= \mathrm{Card}\,\{a' \in \mathbb{Z}[i],\ |z-a'| < 1\} = k(z)\ , \end{aligned}$$

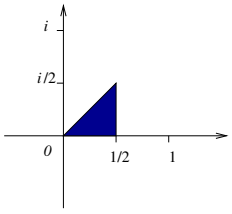
   car $a \mapsto a - 1$ est une bijection de $\mathbb{Z}[i]$ dans lui-même.

   (ii) On note que $z \mapsto z + i$ est une bijection de $\mathbb{Z}[i]$ dans lui-même et on en déduit comme ci-dessus que $k(z) = k(z + i)$; de même $z \mapsto -iz$ est une bijection de $\mathbb{Z}[i]$ dans lui-même, d'où

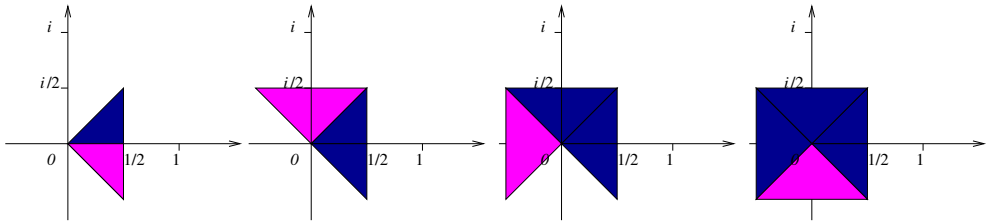
$$\begin{aligned} k(iz) &= \mathrm{Card}\,\{a \in \mathbb{Z}[i],\ |iz-a| < 1\} \\ &= \mathrm{Card}\,\{a \in \mathbb{Z}[i],\ |i||z-(-ia)| < 1\} \\ &= \mathrm{Card}\,\{a' \in \mathbb{Z}[i],\ |z-a'| < 1\} \\ &= k(z)\ . \end{aligned}$$

   Enfin $z \mapsto \overline{z}$ est une bijection de $\mathbb{Z}[i]$ dans lui-même, ce qui entraîne que $k(z) = k(\overline{z})$ en utilisant $|\overline{z}| = |z|$.

   (iii) L'ensemble $D = \{z' \in \mathbb{C} \mid 0 \leq \mathrm{Im}(z') \leq \mathrm{Re}(z') \leq 1/2\}$ a la représentation suivante :



   En lui adjoignant son image par les transformations $z \mapsto \overline{z}$, puis $z \mapsto iz$ (rotation de 90° vers la droite), répétée trois fois, on obtient successivement les ensembles :



Il est clair qu'en appliquant de façon itérative les translations $z \mapsto z+1$ et $z \mapsto z+i$ au carré final, on peut recouvrir entièrement le plan complexe. Autrement dit, pour tout $z \in \mathbb{C}$, il existe $z' \in D$ tel que z' soit l'image de z par une composée f des transformations listées ci-dessus et de leurs inverses. Or $k(f(z)) = k(z)$ d'après la question précédente, c'est-à-dire $k(z') = k(z)$ et $z' \in D$ comme demandé.

(iv) Le point de l'ensemble D le plus éloigné de 0 est $\frac{1}{2} + \frac{i}{2}$, dont le module vaut $1/\sqrt{2}$, ce qui entraîne $|z'| \leq 1/\sqrt{2}$ pour tout $z' \in D$. De même, le point de D le plus éloigné de 1 est 0, donc $|z'-1| \leq 1$ pour tout $z' \in D$, et l'égalité n'est satisfaite que pour $z' = 0$, d'où le résultat.

4. D'après la question 3(iii), il suffit de montrer que pour tout $z' \in D$:

$$1 \leq k(z') \leq 4 \quad \text{et} \quad k(z') = 1 \Leftrightarrow z' = 0 \ .$$

Or, on sait par 3(iv) que $k(z') \geq 1$ pour tout $z' \in D$ (puisque $|z'| = |z'-0| < 1$) et que $k(z') \geq 2$ pour tout $z' \in D \setminus \{0\}$ (puisque $|z'-1| < 1$ pour $z' \neq 0$), ce qui prouve l'équivalence ci-dessus. Enfin, D est inclus dans le carré de sommets les points d'affixes $0, 1, i, 1+i$, et tous les points de $\mathbb{Z}[i] \setminus \{0, 1, i, 1+i\}$ sont à une distance ≥ 1 de ce carré. Il s'ensuit que $k(z') \leq 4$ pour tout $z' \in D$, et le résultat demandé en découle.

5. On trouve $k(\frac{1+i}{3}) = 4$, $k(\frac{1+i}{4}) = 3$ et $k(\frac{5+i}{12}) = 2$, si bien que toutes les valeurs possibles d'après la question précédente sont effectivement prises.

6. Soit $(z_1, z_2) \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0\}$, alors $k(\frac{z_1}{z_2}) \geq 1$, donc soit $a \in \mathbb{Z}[i]$ tel que $|\frac{z_1}{z_2} - a| < 1$. On vérifie immédiatement que $q = a$ et $r = z_1 - az_2$ satisfont les conditions demandées.

7. On a déjà vu (TD4, exercice 1) que $\mathbb{Z}[i]$ est intègre, il reste donc à montrer que tout idéal de $\mathbb{Z}[i]$ est principal. Soit I un idéal de $\mathbb{Z}[i]$ non réduit à $\{0\}$. On remarque que l'ensemble

$$\{|a|^2, \ a \in I, \ a \neq 0\}$$

est non vide et inclus dans $\mathbb{N} \setminus \{0\}$, donc il a un plus petit élément, qui est un entier strictement positif. Notons x un élément de $I \setminus \{0\}$ où ce minimum est atteint. Pour $y \in I$, soit $(q, r) \in \mathbb{Z}[i]^2$ tel que

$$y = qx + r \text{ et } |r| < |x| \ .$$

Alors $r = y - qx \in I$ et $|r| < |x|$, donc $r = 0$ pour ne pas contredire la définition de x, si bien que $y = qx \in x\mathbb{Z}[i]$. Ceci montre que $I = x\mathbb{Z}[i]$ est principal, et il s'ensuit que l'anneau $\mathbb{Z}[i]$ est principal.