Devoir libre $n°1$
correction

Exercice 1 **1.** $\mathbb{Z}[i\sqrt{3}]$ est une partie non vide de l'anneaux $(\mathbb{C},+,.)$. On vérifie facilement qu'il s'agit d'un sous-anneau de $(\mathbb{C},+,.)$, donc c'est un anneau.

2. (a) Soient $x=a+ib\sqrt{3}$ et $y=a'+ib'\sqrt{3}$ deux éléments de $\mathbb{Z}[i\sqrt{3}]$. On a :

$$N(xy)=N(aa'-3bb'+i(ab'+ba')\sqrt{3}=(aa'-3bb')^2+3(ab'+ba')^2$$

et

$$N(x)N(y)=(a^2+3b^2)(a'^2+3b'^2)=(aa'-3bb')^2+3(ab'+ba')^2.$$

Donc $N(xy)=N(x)N(y)$.

(b) Supposons que $x=a+ib\sqrt{3}$ est inversible dans $\mathbb{Z}[i\sqrt{3}]$, alors il existe $x'\in\mathbb{Z}[i\sqrt{3}]$ tel que $xx'=1$ et donc $1=N(1)=N(x)N(x')$ et comme $N(x)\in\mathbb{N}$, alors $N(x)=1$.
Inversement, si $N(x)=1$, alors $a^2+3b^2=1$ et donc $1-a^2=3b^2\geq 0$, d'où $a\in\{-1,0,1\}$.

- Si $a=0$, alors $3b^2=1$ ceci est impossible car $b\in\mathbb{Z}$.
- Si $a=1$, alors $3b^2=0$ et donc $b=0$.
- Si $a=-1$, alors $3b^2=0$ et donc $b=0$.

Donc les éléments inversibles sont 1 et -1.

(c) Soit $x=a+ib\sqrt{3}\in\mathbb{Z}[i\sqrt{3}]$. Supposons que $N(x)=2$, c'est-à-dire $a^2+3b^2=2$ et donc $2-a^2=3b^2\geq 0$, donc les valeurs possibles de a sont $-1,0$ et 1.

- Si $a=0$, alors $3b^2=2$ ceci est impossible car $b\in\mathbb{Z}$.
- Si $a=1$, alors $3b^2=1$ ceci est impossible car $b\in\mathbb{Z}$.
- Si $a=-1$, alors $3b^2=1$ ceci est impossible car $b\in\mathbb{Z}$.

Donc pour tout $x\in\mathbb{Z}[i\sqrt{3}]$, $N(x)\neq 2$.

3. Soit $x=yz$ avec $x\in\{1+i\sqrt{3},1-i\sqrt{3},2\}$, alors $N(x)=4$, donc $N(y)N(z)=4$ et par suite $N(y)\in\{1,2,4\}$.

- Si $N(y)=1$ alors y est inversible d'après 2)b).
- Si $N(y)=2$ ceci est impossible d'après 2)c).
- Si $N(y)=4$, alors $N(z)=1$ et z serait inversible.

Exercice 2 **1.** (a) • Si $G=\{\overline{0}\}$ le résultat est trivial.

- Soit maintenant G un sous-groupe de $\mathbb{Z}/_{n\mathbb{Z}}$ différent de $\{\overline{0}\}$. Soit x le plus petit élément positive tel que $\overline{x}\in G$, ainsi $\forall m\in\mathbb{Z}$, $m\overline{x}\in G$, donc $(\overline{x})$, le sous-groupe engendré par $\overline{x}$, est inclus dans G : $(\overline{x})\subset G$
Soit $y\in\mathbb{Z}$ tel que $\overline{y}\in G$, alors, par la division euclidienne, il existe $\alpha,r\in\mathbb{Z}$ tels que $y=\alpha x+r$ et $0\leq r<x$, donc $\overline{r}=\overline{y}-\alpha\overline{x}\in G$, donc $r=0$ et par conséquent $y=\alpha\overline{x}\in(\overline{x})$. D'où $G=(\overline{x})$.
D'autre part, il existe $q,r\in\mathbb{Z}$ tels que $n=qx+r$ avec $0\leq r<x$ et donc $\overline{r}=\overline{n}-q\overline{x}=-q\overline{x}\in G$, donc $r=0$ et $n=qx$, donc il suffit de prendre $p=x$.

(b) On a $G=(\overline{p})$ est un sous-groupe de $\mathbb{Z}/_{n\mathbb{Z}}$. De plus si $\overline{x}\in\mathbb{Z}/_{n\mathbb{Z}}$ et $\overline{y}=\alpha\overline{p}\in G$, alors $\overline{xy}=(\alpha x)\overline{p}\in G$. Donc G est un idéal de l'anneau $(\mathbb{Z}/_{n\mathbb{Z}},+,.)$

2. (a) $\mathbb{Z}_p$ est une partie non vide de $\mathbb{Q}$, car elle contient $\mathbb{Z}$.
Soient $\dfrac{m}{n}$ et $\dfrac{m'}{n'}$ deux éléments de $\mathbb{Z}_p$, alors

$$\frac{m}{n} - \frac{m'}{n'} = \frac{mn' - m'n}{nn'}.$$

Comme p ne divise pas n et n', alors p ne divise pas nn' et donc $\dfrac{m}{n} - \dfrac{m'}{n'} \in \mathbb{Z}_p$.
D'autre part, $\dfrac{m}{n} \times \dfrac{m'}{n'} = \dfrac{mm'}{nn'} \in \mathbb{Z}_p$. Donc $(\mathbb{Z}_p, +, .)$ est un sous-anneau de l'anneau $(\mathbb{Q}, +, .)$, donc c'est un anneau.

(b) Soit G un idéal de $\mathbb{Z}_p$, alors $G \cap Z_p$ est un sous-groupe de $\mathbb{Z}$, donc il est de la forme $r\mathbb{Z}$, $r \geq 0$.

- Si $G = \{0\}$ le résultat est évident.
- Supposons maintenant que $G \neq \{0\}$, alors il existe $x = \dfrac{m}{n} \in G$ non nul, donc $nx = m \in G \cap \mathbb{Z}$. Donc $G \cap \mathbb{Z} \neq \{0\}$.
Posons $r = p^\alpha \beta$ avec $\alpha \geq 0$ et p ne divise pas β. (décomposition d'un entier en facteurs premiers).
Montrons que $G = p^\alpha \mathbb{Z}_p$.
Soit $\dfrac{a}{b} \in Z_p$ où $a \in \mathbb{Z}$ et p ne divise pas b.

$$\begin{aligned} r = \beta p^\alpha \in G &\implies \frac{a}{b\beta}(\beta p^\alpha) = \frac{a}{b} p^\alpha \in G, \quad (p \text{ ne divise pas } b\beta) \\ &\implies p^\alpha \mathbb{Z}_p \in G \end{aligned}$$

Soit $x = \dfrac{a}{b} \in G$, donc $bx = a \in \mathbb{Z} \cap G = \beta p^\alpha \mathbb{Z}$, donc $x \in \dfrac{\beta}{b} p^\alpha \mathbb{Z}$ ou encore $x \in p^\alpha \dfrac{\beta}{b} \mathbb{Z} \subset p^\alpha \mathbb{Z}_p$.
D'où $G = p^\alpha Z_p$.

Exercice 3 **1.** Puisque 0 est dans l'intérieur de K, alors il existe $r > 0$ tel que $B(0, r) \subset K$. Donc pour tout $x \in \mathbb{R}^d \backslash \{0\}$, $\dfrac{r}{2} \dfrac{x}{\|x\|} \in B(0, r) \subset K$, donc $\dfrac{r}{2\|x\|} \in \{\alpha / \dfrac{x}{\alpha} \in K\}$, donc $\inf\{\alpha / \frac{x}{\alpha} \in K\}$ existe.
Si $x = 0$, alors $\{\alpha / \dfrac{x}{\alpha} \in K\} =]0, +\infty[$ car 0 est un point intérieur.
L'égalité est vraie si $x = 0$. Soit $\lambda \in \mathbb{R}^{*+}$. Alors pour tout $x \in \mathbb{R}^d$ non nul :

$$\begin{aligned} j_K(\lambda x) &= \inf\{\alpha > 0 / \frac{\lambda x}{\alpha} \in K\} \\ &= \inf\{\alpha > 0 / \frac{x}{\frac{\alpha}{\lambda}} \in K\} \end{aligned}$$

Donc $j_K(\lambda x) = \inf\{\lambda \alpha' \in \mathbb{R}_*^+, \ \frac{x}{\alpha'} \in K\}$, en posant $\alpha' = \dfrac{\alpha}{\lambda}$. Soit finalement :

$$\begin{aligned} j_K(\lambda x) &= \lambda \inf\{\alpha' \in \mathbb{R}_+^* / \frac{x}{\alpha'} \in K\} \\ &= \lambda j_K(x) \end{aligned}$$

et cette égalité reste évidement vraie pour $\lambda = 0$.

2. Il est clair que $j_K(x) = 0$ si $x = 0$.
Soit $x \in \mathbb{R}^d$ tel que $j_K(x) = 0$. Par définition de la borne inférieure :

$$\forall \varepsilon > 0, \exists \alpha \in]0, \varepsilon[\text{ tel que } \frac{x}{\alpha} \in K.$$

Or K est bornée, donc il existe $M>0$ tel que $\forall y\in K$, $\|y\|\leq M$. On a donc

$$\forall\varepsilon>0, \exists\alpha\in]0,\varepsilon[\ \text{ tel que }\ \|x\|\leq\alpha M$$

D'où $\forall\varepsilon>0$, $\|x\|\leq\varepsilon M$. Ainsi $\|x\|=0$ puis $x=0$.

3. Soient $x,y\in\mathbb{R}^d$. Pour tous $\alpha,\beta>0$ tels que $\dfrac{x}{\alpha}\in K$ et $\dfrac{y}{\beta}\in K$, on a $x=\alpha c$ et $y=\beta c'$ avec $(c,c')\in K^2$. D'où

$$x+y=\alpha c+\beta c'=(\alpha+\beta)\left(\frac{\alpha}{\alpha+\beta}c+\frac{\beta}{\alpha+\beta}c'\right)\in(\alpha+\beta).K$$

Donc, par définition de j_K : $j_K(x+y)\leq\alpha+\beta$. Cette inégalité étant valable pour tous α et β tels que $\dfrac{x}{\alpha}\in K$ et $\dfrac{y}{\beta}\in K$. On en déduit

$$j_K(x+y)\leq j_K(x)+j_K(y).$$

4. Reste à montrer que $\forall\lambda\in\mathbb{R}$, $\forall x\in\mathbb{R}^d$, on a $j_K(\lambda x)=|\lambda|j_K(x)$. L'égalité est déjà démontrée pour $\lambda\geq 0$.
Soit $\lambda\in\mathbb{R}^*$. Alors pour tout $x\in\mathbb{R}^n$:

$$\begin{array}{rcl} j_K(\lambda x) & = & \inf\{\alpha>0/\dfrac{\lambda x}{\alpha}\in K\} \\ & = & \inf\{\alpha>0/x\in\dfrac{\alpha}{\lambda}.K\} \end{array}$$

Or $x\in\dfrac{\alpha}{\lambda}.K\iff x\in\dfrac{\alpha}{|\lambda|}.K$, car K est symétrique par rapport à 0.
Donc $j_K(\lambda x)=\inf\{|\lambda|\alpha'\in\mathbb{R}_*^+/\dfrac{x}{\alpha'}\in K\}$, en posant $\alpha'=\dfrac{\alpha}{|\lambda|}$. Soit finalement :

$$\begin{array}{rcl} j_C(\lambda x) & = & |\lambda|\inf\{\alpha'\in\mathbb{R}_+^*/\dfrac{x}{\alpha'}\in K\} \\ & = & |\lambda|j_K(x) \end{array}$$

Tout ce qui précède montre que j_K est une norme sur $\mathbb{R}^d$.
Si $x\in K$, $\dfrac{x}{1}\in K$ d'où $j_K(x)\leq 1$. Ainsi $K\subset\overline{B}_{j_K}$. ($\overline{B}_{j_K}$ désigne la boule fermée unité pour la norme j_K).
Soit $x\in\overset{\circ}{\widehat{\overline{B}}}_{j_K}$, c'est-à-dire $j_K(x)<1$. Par définition de la borne supérieure, il existe $\lambda>0$ tel que $j_K(x)\leq\lambda<1$ et $x\in\lambda.K$, soit $x=\lambda.c$ avec $c\in K$. On a alors $x\in[0,c]$ d'où $x\in K$ puisque K est convexe. D'où

$$\overset{\circ}{\widehat{\overline{B}}}_{j_K}\subset K\subset\overline{B}_{j_K}.$$

Donc $\overline{\overset{\circ}{\widehat{\overline{B}}}_{j_K}}\subset\overline{K}\subset\overline{B}_{j_K}$. Mais $\overline{\overset{\circ}{\widehat{\overline{B}}}_{j_K}}=\overline{\overline{B}_{j_K}}$ et $K=\overline{K}$ d'où, en conclusion $K=\overline{B}_{j_K}$.

• • • • • • • • • • •