Corrigé du contrôle continu n°2

Exercice 1. Soit H_1 l'ensemble des matrices de type $\begin{pmatrix} x & x \\ -x & -x \end{pmatrix}$ où $x \in \mathbb{R}$, et soit H_2 l'ensemble des matrices de type $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ où $x \in \mathbb{R}$.

(1) Les ensembles H_1 ou H_2 ne sont pas des sous-anneaux de l'anneau de matrices $\mathcal{M}_2(\mathbb{R})$ car ils ne contiennent pas la matrice identité qui est le neutre multiplicatif de l'anneau $\mathcal{M}_2(\mathbb{R})$.

(2) On remarque que $\begin{pmatrix} x & x \\ -x & -x \end{pmatrix}\begin{pmatrix} y & y \\ -y & -y \end{pmatrix}$ est toujours égale à la matrice nulle. Donc la loi produit n'a pas de neutre dans H_1. Ainsi, H_1 muni de la somme et du produit de matrices usuels n'est pas un anneau.

(3) Posons $M(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ pour tout $x \in \mathbb{R}$. On calcule facilement $M(x)+M(y) = M(x+y)$ et $M(x)M(y) = M(xy)$. Donc H_2 est stable par les lois $+$ et $\times$, qui sont donc les lois induites de celles de $\mathcal{M}_2(\mathbb{R})$. Ainsi, H_2 est facilement un sous-groupe de $(\mathcal{M}_2(\mathbb{R}), +)$, et la loi $\times$ est associative et distributive par rapport à $+$. Le neutre pour $+$ est la matrice nulle et pour $\times$ c'est $M(1)$. Ainsi, H_2 muni de la somme et du produit de matrices usuels est un anneau. Il est commutatif puisque $M(x)M(y) = M(xy) = M(yx) = M(y)M(x)$.

(4) En fait, $\varphi(x) = M(x)$. Donc, $\varphi(1) = M(1)$, $\varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$. On a donc un morphisme d'anneaux. Il est trivialement surjectif. Puisque $\varphi(x) = 0$ équivaut à $x = 0$, il est injectif. Donc, on a bien un isomorphisme d'anneaux.

Exercice 2. Posons $A = \{a + jb \mid a, b \in \mathbb{Z}\}$ où $j = \exp(\frac{2i\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ est un nombre complexe satisfaisant $j^3 = 1$ et $1 + j + j^2 = 0$.

(1) Déjà $A \subset \mathbb{C}$ et $1 = 1 + j0 \in A$.
Soit $a, b, a', b' \in \mathbb{Z}$. Alors, $(a+jb) - (a'+jb') = (a-a') + j(b-b')$ avec $a-a'$ et $b-b'$ des entiers relatifs. Donc, $(a+jb) + (a'+jb') \in A$, et A est un sous-groupe de $(\mathbb{C}, +)$.
Puis, $(a+jb)(a'+jb') = (aa'-bb') + j(ab'+a'b-bb')$ avec $aa'-bb'$ et $ab'+a'b-bb'$ des entiers relatifs. Donc, $(a+jb)(a'+jb') \in A$ et A est stable par le produit. En conclusion, A est un sous-anneau de l'anneau $(\mathbb{C}, +, \times)$.

(2) Posons $N(z) = |z|^2$ pour tout $z \in \mathbb{C}$. Rappelons que $|z|$ désigne le module du nombre complexe z et que $|z|^2 = z\overline{z}$ où $\overline{z}$ est le conjugué de z. De plus, $N(zz') = N(z)N(z')$ pour tous complexes z et z'.

(a) Soit $z \in A$ que l'on écrit $a + jb$ avec a et b entiers relatifs. Déjà, $N(z)$ étant un module c'est un réel positif. On calcule

$$N(z) = z\overline{z} = (a+jb)(a+\overline{j}b) = a^2 + b^2 - ab \in \mathbb{Z}.$$

Donc, $N(z)$ est un entier positif : $N(z) \in \mathbb{N}$.

(b) Soit $z \in A$. Alors $\overline{z} \in A$. Si $N(z) = 1$, on a $z\overline{z} = 1$, donc $z \in U(A)$ et $\overline{z}$ est l'inverse de z pour le produit.
Réciproquement, si $z \in U(A)$, alors il existe $y \in U(A)$ tel que $zy = 1$ et on obtient $1 = N(zy) = N(z)N(y)$ avec $N(y)$ et $N(z)$ entiers naturels. Donc $N(z) = 1$. Ainsi, $z \in U(A) \iff N(z) = 1$.

(3) Soit $a, b \in \mathbb{Z}$ tel que $N(a+jb) = 1$. Alors $a^2 + b^2 = 1 + ab \geqslant 0$. Si $ab = -1$ comme a et b sont des entiers, $a^2 = b^2 = 1$ et $N(a+jb) = 3 \neq 1$, impossible ! ! Donc, ab est un entier > -1, autrement dit $ab \geqslant 0$.

(4) On remarque que $N(a+jb) = a^2+b^2-ab = (a-b)^2+ab$ somme de deux entiers positifs. Si $z = a+jb \in U(A)$ alors $N(a+jb) = 1$, ce qui entraîne soit $(a-b)^2 = 1$ et $ab = 0$, soit $(a-b)^2 = 0$ et $ab = 1$. Donc, $a = 0$ et $b = \pm 1$, ou $a = \pm 1$ et $b = 0$, ou $a = b = \pm 1$, c'est-à-dire $z = \pm j$ ou $z = \pm 1$ ou $z = \pm(1+j) = \mp\overline{j}$. Tous ces éléments ont bien un module qui vaut 1 donc ce sont des unités de A. Ainsi,

$$U(A) = \{1, -1, j, -j, \overline{j}, -\overline{j}\}.$$

Dans le groupe multiplicatif $U(A)$, les éléments j et $\overline{j}$ sont d'ordre 3, 1 est d'ordre 1, -1 est d'ordre 2, $-j$ et $-\overline{j}$ sont d'ordre 6.

(5) On admet que A est un anneau principal.

(a) Soit $z \in A$ tel que $N(z)$ est un nombre premier. Alors, $z \neq 0$ et $z \notin U(A)$. Si $z = z_1 z_2$, il vient $N(z_1)N(z_2) = N(z) = p$ avec $N(z_1)$ et $N(z_2)$ entiers naturels. Donc $N(z_1)$ ou $N(z_2)$ vaut 1, autrement dit z_1 ou z_2 est une unité de A. Par conséquant, z est un élément irréductible de A.

(b) On calcule $N(2+j) = 4+1-2 = 3$ nombre premier, donc $2+j$ est un élément irréductible de A. Puis $N(2+3j) = 4+9-6 = 7$ nombre premier, donc $2+3j$ est un élément irréductible de A. Enfin $N(3+8j) = 9+64-24 = 49 = 7^2$ n'est pas un nombre premier. On remarque que $3+8j = (2+3j)(3+j)$ avec $2+3j$ et $3+j$ qui sont deux éléments irréductibles. Donc $3+8j$ n'est pas irréductible.

Exercice 3. Soit $(A, +, .)$ un anneau commutatif, I et J deux idéaux de A. On définit le quotient de l'idéal I par l'idéal J de la manière suivante :

$$(I : J) = \{x \in A \mid xJ \subset I\}$$

où $xJ = \{x.y \mid y \in J\}$.

(1) Déjà, $(I : J) \subset A$ et $(I : J)$ contient 0 puisque $0J = \{0\} \subset I$.
Soit $x, y \in (I : J)$. Pour tout $z \in J$ on a par distributivité

$$(x+y)z = xz + yz \in I$$

car I est un sous-groupe de $(A, +)$. Donc $(x+y)J \subset I$. Ainsi, $x+y \in (I : J)$.
Soit $x \in (I : J)$ et $a \in A$. Pour tout $z \in J$ on a par associativité, commutativité et propriété d'absorption de I

$$(ax)z = a(xz) \in I$$

car $xz \in xJ \subset I$. Donc $(ax)J \subset I$. Ainsi, $ax \in (I : J)$.
De plus, si $x \in I$, par absorption, $xJ \subset I$.
Ainsi, $(I : J)$ est un idéal de A contenant I.

(2) On se place dans le cas où $A = \mathbb{Z}$. Si $x \in (18\mathbb{Z} : 3\mathbb{Z})$, alors $3x\mathbb{Z} \subset 18\mathbb{Z}$, autrement dit $18 \big| 3x$, ie $6 \big| x$, donc $x \in 6\mathbb{Z}$. Inversement, si $x \in 6\mathbb{Z}$, il existe $y \in \mathbb{Z}$ tel que $x = 6y$ et donc, $x(3z) = 18yz \in 18\mathbb{Z}$ pour tout entier z, autrement dit $x \in (18\mathbb{Z} : 3\mathbb{Z})$. Ainsi

$$(18\mathbb{Z} : 3\mathbb{Z}) = 6\mathbb{Z}.$$

Si $x \in (18\mathbb{Z} : 6\mathbb{Z})$, alors $6x\mathbb{Z} \subset 18\mathbb{Z}$, autrement dit $18 \big| 6x$, ie $3 \big| x$, donc $x \in 3\mathbb{Z}$. Inversement, si $x \in 3\mathbb{Z}$, il existe $y \in \mathbb{Z}$ tel que $x = 3y$ et donc, $x(6z) = 18yz \in 18\mathbb{Z}$ pour tout entier z, autrement dit $x \in (18\mathbb{Z} : 6\mathbb{Z})$. Ainsi

$$(18\mathbb{Z} : 6\mathbb{Z}) = 3\mathbb{Z}.$$

De manière générale, soit I et J deux idéaux de $\mathbb{Z}$. Si $J = \{0\}$, alors $(I : J) = A$, et si $I = \{0\}$, alors $(I : J) = \{0\}$.
Supposons désormais J et I non nuls. J et I étant des idéaux de $\mathbb{Z}$, il existe $m, n \in \mathbb{N}^\star$ tels que $J = n\mathbb{Z}$ et $I = m\mathbb{Z}$. Si $x \in (m\mathbb{Z} : n\mathbb{Z})$, alors $m|nx$. Posons d le pgcd de m et n, $m' = m/d$ et $n' = n/d$. Il vient après simplification : $m'|n'x$. Or m' et n' sont premiers entre eux. Par le théorème de Gauss, $m'|x$, ie. $x \in m'\mathbb{Z}$.
Inversement, soit $x \in m'\mathbb{Z}$. Il existe $y \in \mathbb{Z}$ tel que $x = m'y$ et donc, $x(nz) = m'nyz = mn' \in m\mathbb{Z}$ pour tout entier z, autrement dit $x \in (m\mathbb{Z} : n\mathbb{Z})$. Ainsi

$$(m\mathbb{Z} : n\mathbb{Z}) = m'\mathbb{Z} \text{ où } m' = m/(m \wedge n).$$

Exercice 4. Soit $(A, +, .)$ un anneau fini intègre. Pour tout $a \in A$ on considère l'application $\varphi_a : A \to A$ par définie $\varphi_a(x) = a.x$.

(1) Soit a un élément non nul de A. Pour tout $x, y \in A$, on a par distributivité, $\varphi_a(x+y) = a.(x+y) = a.x + a.y = \varphi_a(x) + \varphi_a(y)$. Donc, φ_a est un endomorphisme du groupe $(A, +)$. Comme A est intègre son noyau est $\{0\}$. Donc φ_a est injective de A dans A. Comme A est fini, elle est bijective. Donc, φ_a est un automorphisme du groupe $(A, +)$.

(2) Pour tout $a \neq 0$, φ_a étant bijective, 1 a un unique antécédent (qui est l'inverse de a). Donc a est inversible pour le produit. Par conséquent, A est un corps.