Corrigé du CC2

Exercice 1. 1. *Question de cours.* Soit n un entier supérieur ou égal à 2 et soit $k \in \mathbb{Z}$. Montrer que dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $\overline{k}$ est inversible (pour la loi $\times$) si et seulement si les entiers k et n sont premiers entre eux.

On a :

$$\begin{aligned}
\overline{k} \text{ est inversible} &\iff \exists u \in \mathbb{Z}\,,\ \overline{k}\,\overline{u} = \overline{1} \\
&\iff \exists u \in \mathbb{Z}\,,\ ku \equiv 1[n] \\
&\iff \exists u \in \mathbb{Z}\,,\ \exists v \in \mathbb{Z}\,,\ 1 - ku = nv \\
&\iff \exists u \in \mathbb{Z}\,,\ \exists v \in \mathbb{Z}\,,\ ku + nv = 1 \\
&\iff pgcd(k,n) = 1 \qquad \text{(d'après le théorème de Bézout)}
\end{aligned}$$

2. *Application* : donner la liste de tous les éléments inversibles de l'anneau $(\mathbb{Z}/12\mathbb{Z}, +, \times)$. Préciser l'inverse de chaque élément inversible.

D'après 1., les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. On a : $(\overline{1})^{-1} = \overline{1}$; $(\overline{5})^{-1} = \overline{5}$, car $5^2 = 25 \equiv 1[12]$; $(\overline{7})^{-1} = (-\overline{5})^{-1} = -\overline{5} = \overline{7}$; $(\overline{11})^{-1} = (-\overline{1})^{-1} = -\overline{1} = \overline{11}$

Exercice 2. Soit $(A, +, \times)$ un anneau commutatif intègre. On note $U(A)$ l'ensemble des éléments de A inversibles pour la loi $\times$ (ces éléments sont appelés des unités).

1. Soit p un entier supérieur ou égal à 1. Etant donné un élément quelconque a de A, démontrer l'équivalence suivante :

$$a \in U(A) \iff a^p \in U(A)\,.$$

Supposons a inversible : il existe $b \in A$ tel que $ab = 1$. Alors $a^p b^p = 1$, donc a^p est inversible, d'inverse b^p. Réciproquement supposons a^p inversible : il existe $s \in A$ tel que $a^p s = 1$. Alors, comme $p - 1 \in \mathbb{N}$, l'élément $a^{p-1}s$ de A est bien défini et

$$a(a^{p-1}s) = (aa^{p-1})s = a^p s = 1\,,$$

donc a est inversible, d'inverse $a^{p-1}s$.

2. On suppose dans cette question que l'anneau A ne possède qu'un nombre fini d'idéaux. Soit a un élément *non nul* de A.

a) Justifier qu'il existe $n, m \in \mathbb{N}$, avec $n < m$, tels que $a^n A = a^m A$.

Chaque ensemble $a^k A$ ($k \in \mathbb{N}$) est un idéal de l'anneau $(A, +, \times)$. Comme A ne possède qu'un nombre fini d'idéaux, les ensembles $a^k A$ ($k \in \mathbb{N}$) ne peuvent être deux à deux distincts. Donc il existe $n, m \in \mathbb{N}$, avec $n < m$, tels que $a^n A = a^m A$.

b) On pose $p = m - n$ ($p \in \mathbb{N}^*$). En utilisant le fait que a^n appartient à $a^m A$, montrer que $a^p \in U(A)$.

$a^n = a^n \times 1 \in a^n A$ donc $a^n \in a^m A$: il existe $b \in A$ tel que $a^n = a^m b$. On a

$$0 = a^m b - a^n = a^{n+p} b - a^n = a^n a^p b - a^n = a^n(a^p b - 1).$$

Or $a \neq 0$ et A est intègre, donc $a^p b - 1 = 0$: a^p est inversible, d'inverse b.

3. Que peut-on dire de A, si A ne possède qu'un nombre fini d'idéaux?

Si A ne possède qu'un nombre fini d'idéaux, d'après 2.b) et 1., tout élément non nul a de A est inversible. Donc $(A, +, \times)$ est un corps.

Exercice 3. 1. Trouver deux polynômes $U, V \in \mathbb{R}[X]$ tels que

$$U(X)(X^2 + X - 2) + V(X)(X^2 + 1) = 1\,.$$

On utilise l'algorithme d'Euclide (étendu), qui permet à la fois de déterminer le pgcd de deux polynômes et de trouver une relation de Bézout. On a

$$\begin{aligned} X^2 + X - 2 &= (X^2 + 1) + (X - 3) \\ X^2 + 1 &= (X + 3)(X - 3) + 10 \end{aligned}$$

On a donc $pgcd(X^2 + X - 2, X^2 + 1) \sim 10 \sim 1$ (dans $\mathbb{R}[X]$) : les polynômes $X^2 + X - 2$ et $X^2 + 1$ sont premiers entre eux.

On a

$$\begin{aligned} 10 &= (X^2 + 1) - (X + 3)(X - 3) \\ &= (X^2 + 1) - (X + 3)[(X^2 + X - 2) - (X^2 + 1)] \\ &= -(X + 3)(X^2 + X - 2) + [1 + (X + 3)](X^2 + 1) \\ &= -(X + 3)(X^2 + X - 2) + (X + 4)(X^2 + 1)\,. \end{aligned}$$

Posons

$$U(X) = -\frac{1}{10}(X + 3) \qquad \text{et} \qquad V(X) = \frac{1}{10}(X + 4)\,.$$

D'après ce qui précède, $U(X)(X^2 + X - 2) + V(X)(X^2 + 1) = 1$.

2. On note $\mathcal{S}$ le sous-ensemble de $\mathbb{R}[X]$ constituée des polynômes P tels que

$$\begin{cases} X^2 + 1 \text{ divise } P(X) \\ X^2 + X - 2 \text{ divise } P(X) - 1 \end{cases}$$

Utiliser 1. pour trouver un élément P_0 de $\mathcal{S}$. Montrer que tout élément P de $\mathcal{S}$ est de la forme

$$P(X) = P_0(X) + (X^2 + 1)(X^2 + X - 2)Q(X)\,, \quad \text{avec } Q \in \mathbb{R}[X]\,.$$

Considérons les polynômes U et V trouvés en 1 et posons

$$P_0(X) = V(X)(X^2 + 1) = \frac{1}{10}(X + 4)(X^2 + 1) = \frac{1}{10}(X^3 + 4X^2 + X + 4)$$

Le polynôme $X^2 + 1$ divise évidemment polynôme P_0 et d'après 1.,

$$P_0(X) - 1 = -U(X)(X^2 + X - 2)\,,$$

donc $X^2 + X - 2$ divise $P_0 - 1$. On a bien $P_0 \in \mathcal{S}$.

Soit $P \in \mathcal{S}$; P et P_0 sont divisibles par $X^2 + 1$ donc $P - P_0$ également; $P - 1$ et $P_0 - 1$ sont divisibles par $X^2 + X - 2$ donc $P - P_0 = (P - 1) - (P_0 - 1)$ également. $P - P_0$ est donc divisible par $X^2 + 1$ et $X^2 + X - 2$. Or les polynômes $X^2 + 1$ et $X^2 + X - 2$ sont premiers entre eux, donc leur produit $(X^2 + 1)(X^2 + X - 2)$ divise $P - P_0$. Ainsi il existe $Q \in \mathbb{R}[X]$ tel que

$$P(X) = P_0(X) + (X^2 + 1)(X^2 + X - 2)Q(X)\,.$$

Exercice 4. On considère le sous-ensemble suivant de $\mathbb{R}$:

$$B = \{a + b\sqrt{2}\,;\, a, b \in \mathbb{Z}\}\,.$$

1. Montrer que B est un sous-anneau de $(\mathbb{R}, +, \times)$.

(i) B est une partie non vide vide de $\mathbb{R}$. En particulier, $1 = 1 + 0 \times \sqrt{2} \in B$.

(ii) Soit $x, y \in B$. Il existe $a, b, a', b' \in \mathbb{Z}$ tels que $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. On a

$$x - y = (a - a') + (b - b')\sqrt{2} \qquad \text{avec} \quad a - a', b - b' \in \mathbb{Z}\,.$$

On a donc $\forall (x, y) \in B^2\,,\ x - y \in B$.

(iii) Avec les notations de la propriété précédente,

$$xy = (a+b\sqrt{2})(a'+b'\sqrt{2}) = (aa'+2bb')+(ab'+a'b)\sqrt{2} \qquad \text{avec} \quad aa'+2bb', ab'+a'b \in \mathbb{Z}\,.$$

On a donc $\forall (x, y) \in B^2\,,\ xy \in B$.

Par les propriétés établies en (i),(ii),(iii), B est un sous-anneau de $(\mathbb{R}, +, \times)$.

2. Pour $x = a + b\sqrt{2}$ (avec $a, b \in \mathbb{Z}$), on pose $N(x) = a^2 - 2b^2$. Montrer que

$$\forall (x, y) \in B \times B\,,\ N(xy) = N(x)N(y)$$

Soit $x = a+b\sqrt{2}\,,\ y = a'+b'\sqrt{2} \in B$, avec $a, b, a', b' \in \mathbb{Z}$. On a $N(x) = (a+b\sqrt{2})(a-b\sqrt{2})$ et $xy = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$. On a

$$\begin{aligned} N(x)N(y) &= (a + b\sqrt{2})(a - b\sqrt{2})(a' + b'\sqrt{2})(a' - b'\sqrt{2}) \\ &= [(a + b\sqrt{2})(a' + b'\sqrt{2})][(a - b\sqrt{2})(a' - b'\sqrt{2})] \\ &= [(aa' + 2bb') + (ab' + a'b)\sqrt{2}][(aa' + 2bb') - (ab' + a'b)\sqrt{2}] \\ &= N(xy)\,. \end{aligned}$$

3. Soit $x \in B$. Montrer que si $N(x) = \pm 1$, alors x est une unité de l'anneau B.

Posons $x = a + b\sqrt{2}$, avec $a, b \in \mathbb{Z}$, et posons $y = a - b\sqrt{2}$: y appartient aussi à B, et $xy = N(x)$. Si $N(x) = \pm 1$, $xy = 1$ ou $x(-y) = 1$ donc x est une unité de l'anneau B.

4. Soit $x \in B$. Montrer que si $N(x)$ est un nombre premier ou l'opposé d'un nombre premier, alors x est un élément irréductible de l'anneau B.

On suppose que $N(x) = \pm p$, où p est un nombre premier; x est irréductible dans $(B, +, \times)$ si :

$$\forall y, z \in B\,,\ x = yz \Longrightarrow y \in U(B) \text{ ou } z \in U(B)\,.$$

Supposons $yz = x$, avec $y, z \in B$. Alors $N(y)N(z) = N(yz) = N(x) = \pm p$ d'après 2. Comme p est premier, cela implique $N(y) = \pm 1$ ou $N(z) = \pm 1$; donc d'après 3. , $y \in U(B)$ ou $z \in U(B)$. Ainsi x est irréductible.