Université de Poitiers, Année 2024-2025

3e année de Licence de Mathématiques, Anneaux

Corrigé du contrôle continu du mercredi 5 mars 2025

Exercice 1 – Questions de cours (5 points)

1. Donner la définition d'un idéal maximal d'un anneau commutatif.

   C'est la définition 4.1 du cours.

   Un idéal propre d'un anneau A est dit *maximal* s'il n'est contenu dans aucun autre idéal propre de A que lui-même.

2. Soit M un idéal d'un anneau commutatif A. Démontrer que, si A/M est un corps, alors M est un idéal maximal de A.

   Il s'agit de la réciproque de la proposition 4.2 du cours.

   Si A/M est un corps, alors A/M est non nul et M est donc un idéal propre de A. Si J est un idéal de A contenant strictement M, alors il existe $a \in J \setminus M$. En particulier $\overline{a}$ est non nul dans A/M, et comme A/M est un corps, il est inversible dans A/M : il existe $b \in A$ tel que $\overline{a}\overline{b} = 1_{A/M}$. On en déduit que $\overline{ab} = \overline{1_A}$ et que 1_A appartient à $ab + M$. Or ab appartient à J puisque J est un idéal de A, et J contient M, donc $ab + M$ est contenu dans J. Ainsi on a $1_A \in J$ d'où $J = A$, ce qui montre que M est un idéal maximal de A.

3. Énoncer le *Théorème d'isomorphisme*.

   *C'est le théorème principal de la section 6 "*Morphismes d'anneaux*" du cours.*

   Pour tout morphisme d'anneaux $f : A \to B$, les anneaux $A/\operatorname{Ker} f$ et $\operatorname{Im} f$ sont isomorphes.

Exercice 2 – Issu du TD (4 points)

On considère les deux anneaux $A = \mathbb{Z}/10\mathbb{Z}$ et $B = \mathbb{Z}/13\mathbb{Z}$.

1. L'application $A \to A \times B$ définie par $a \mapsto (a, 0)$ est-elle un morphisme d'anneaux ?
2. L'application $A \times B \to A$ définie par $(a, b) \mapsto a$ est-elle un morphisme d'anneaux ?
3. Déterminer l'unique morphisme d'anneaux $\mathbb{Z} \to A \times B$. Quelle est son image ? son noyau ?

C'est l'exercice 13 de la 1re fiche de TD. Il a été corrigé en TD le mardi 4 février.

Exercice 3 – Issu du TD (2 points)
Montrer qu'un élément x d'un anneau commutatif A est inversible si et seulement s'il n'est contenu dans aucun idéal maximal de A.
C'est l'exercice 3 de la 2e fiche de TD. Il a été corrigé en TD le mardi 11 février.

Exercice 4 – Le nombre d'or (9 points)
On note $\mathbb{Z}[\varphi]$ le sous-anneau de $\mathbb{R}$ engendré par $\mathbb{Z}$ et le *nombre d'or* $\varphi = \frac{1+\sqrt{5}}{2}$.

1. **L'anneau $\mathbb{Z}[\varphi]$**

   (a) Démontrer que l'ensemble $\{a + b\varphi \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.
   Notons $E = \{a + b\varphi \mid a, b \in \mathbb{Z}\}$. C'est une partie de $\mathbb{R}$. De plus, on a :
   - $1 = 1 + 0\varphi \in E$;
   - pour tous $x = a + b\varphi$ et $y = c + d\varphi$ des éléments de E, on a
     (i) $x - y = (a - c) + (b - d)\varphi \in E$;
     (ii)
     $$\begin{aligned} xy &= (a + b\varphi)(c + d\varphi) \\ &= ac + (ad + bc)\varphi + bd\varphi^2 \\ &= ac + (ad + bc)\varphi + bd\tfrac{6+2\sqrt{5}}{4} \\ &= ac + (ad + bc)\varphi + bd\tfrac{3+\sqrt{5}}{2} \\ &= ac + (ad + bc)\varphi + bd(1 + \varphi) \\ &= (ac + bd) + (ad + bc + bd)\varphi \in E. \end{aligned}$$

   Ceci montre que E est un sous-anneau de $\mathbb{R}$ (*voir proposition 3.3 du cours*).

   (b) En déduire que $\mathbb{Z}[\varphi] = \{a + b\varphi \mid a, b \in A\}$.
   Comme $\mathbb{Z}[\varphi]$ est un sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$ et φ, il contient tous les éléments de la forme $a + b\varphi$ pour $a, b \in \mathbb{Z}$ et on a donc $E \subseteq \mathbb{Z}[\varphi]$.
   Or on a vu que E est un sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$ et φ, donc comme $\mathbb{Z}[\varphi]$ est le sous-anneau de $\mathbb{R}$ engendré par $\mathbb{Z}$ et φ, on a aussi $\mathbb{Z}[\varphi] \subseteq E$ d'où $\mathbb{Z}[\varphi] = E = \{a + b\varphi \mid a, b \in A\}$.

   (c) Justifier que les éléments de $\mathbb{Z}[\varphi]$ s'écrivent de façon unique sous la forme $a + b\varphi$ pour $a, b \in \mathbb{Z}$.
   D'après ce qui précède, les éléments de $\mathbb{Z}[\varphi]$ s'écrivent tous sous la forme $a + b\varphi$ pour $a, b \in \mathbb{Z}$.
   Cette écriture est unique car, si on a $a + b\varphi = c + d\varphi$ pour $a, b, c, d \in \mathbb{Z}$, alors on a $a + b\frac{1+\sqrt{5}}{2} = c + d\frac{1+\sqrt{5}}{2}$, donc $2a + b + b\sqrt{5} = 2c + d + d\sqrt{5}$, d'où $(b - d)\sqrt{5} = 2c + d - 2a - b \in \mathbb{Z}$. Comme $\sqrt{5}$ est un nombre irrationnel, on en déduit que $b - d = 0$ et que $2c + d - 2a - b = 0$, d'où $b = d$ et $a = c$, ce qui prouve l'unicité de l'écriture.

(d) Soit $\varphi^* = \frac{1-\sqrt{5}}{2}$. Justifier que l'application $\omega : \mathbb{Z}[\varphi] \to \mathbb{Z}[\varphi]$, définie par $\omega(a + b\varphi) = a + b\varphi^*$, est un automorphisme de l'anneau $\mathbb{Z}[\varphi]$.

Remarque : *Comme on a* $\varphi^* = \frac{1-\sqrt{5}}{2} = 1 - \frac{1+\sqrt{5}}{2} = 1 - \varphi \in \mathbb{Z}[\varphi]$, *on a* $a + b\varphi^* \in \mathbb{Z}[\varphi]$ *pour tout* $a, b \in \mathbb{Z}$ *et* ω *est donc bien une application.*

Pour tous $x = a + b\varphi$ et $y = c + d\varphi$ des éléments de $\mathbb{Z}[\varphi]$, on a :

- $\omega(x+y) = \omega((a+c)+(b+d)\varphi) = (a+c)+(b+d)\varphi^* = (a+b\varphi^*)+(c+d\varphi^*) = \omega(x) + \omega(y)$;
- $\omega(xy) = \omega((ac+bd)+(ad+bc+bd)\varphi) = (ac+bd)+(ad+bc+bd)\varphi^*$, or on a $\omega(x)\omega(y) = (a+b\varphi^*)(c+d\varphi^*) = ac+(ad+bc)\varphi^*+bd\varphi^{*2} = ac+(ad+bc)\varphi^*+bd\frac{6-2\sqrt{5}}{4} = ac+(ad+bc)\varphi^*+bd(1+\varphi^*) = (ac+bd)+(ad+bc+bd)\varphi^*$, d'où $\omega(xy) = \omega(x)\omega(y)$.
- $\omega(1) = \omega(1+0\varphi) = 1 + 0\varphi^* = 1$.

On en déduit que ω est un endomorphisme de l'anneau $\mathbb{Z}[\varphi]$.

De plus, on a

$$\begin{aligned} \operatorname{Ker}\omega &= \{a + b\varphi \mid a, b \in \mathbb{Z} \text{ et } \omega(a + b\varphi) = 0\} \\ &= \{a + b\varphi \mid a, b \in \mathbb{Z} \text{ et } a + b\varphi^* = 0\} \\ &= \{a + b\varphi \mid a, b \in \mathbb{Z} \text{ et } a + b(1 - \varphi) = 0\} \\ &= \{a + b\varphi \mid a, b \in \mathbb{Z} \text{ et } a + b - b\varphi = 0\} \end{aligned}$$

qui vaut $\{0\}$ par unicité de l'écriture $0 = 0 + 0\varphi$. On en déduit que ω est injectif.

En outre, pour tout $x = a + b\varphi \in \mathbb{Z}[\varphi]$, on a $\omega(a + b - b\varphi) = a + b - b\varphi^* = a + b - b(1 - \varphi) = a + b\varphi = x$, ce qui prouve que ω est surjectif.

Ainsi, l'endomorphisme ω est un automorphisme de l'anneau $\mathbb{Z}[\varphi]$.

2. L'application N

(a) Pour tout $z \in \mathbb{Z}[\varphi]$, on note $N(z) = z\omega(z)$. Vérifier que, pour tous $x, y \in \mathbb{Z}[\varphi]$, on a $N(xy) = N(x)N(y)$.

On a vu que ω est un automorphisme de $\mathbb{Z}[\varphi]$, donc pour tous $x, y \in \mathbb{Z}[\varphi]$, on a $N(xy) = xy\omega(xy) = xy\omega(x)\omega(y) = x\omega(x)y\omega(y) = N(x)N(y)$.

(b) Montrer que $N(z) = a^2 + ab - b^2$ pour tout $z \in \mathbb{Z}[\varphi]$.

Pour tout $z = a + b\varphi \in \mathbb{Z}[\varphi]$, on a $N(z) = (a + b\varphi)(a + b\varphi^*) = a^2 + ab(\varphi + \varphi^*) + b^2\varphi\varphi^*$. Or, comme $\varphi^* = 1 - \varphi$, on a $\varphi + \varphi* = 1$. Comme on a aussi $\varphi\varphi^* = \frac{1+\sqrt{5}}{2}\frac{1-\sqrt{5}}{2} = \frac{1-\sqrt{5}^2}{4} = -1$, on obtient $N(z) = a^2 + ab - b^2$.

(c) En déduire que, pour tout $z \in \mathbb{Z}[\varphi]$, on a $N(z) \in \mathbb{Z}$ et que l'élément z est inversible dans $\mathbb{Z}[\varphi]$ si et seulement si $N(z) \in \{+1, -1\}$.

Pour tout $z \in \mathbb{Z}[\varphi]$, on a $N(z) = a^2 + ab - b^2 s$ d'après la question précédente, d'où $N(z) \in \mathbb{Z}$.

Par conséquent, si z est inversible dans $\mathbb{Z}[\varphi]$, ce qui signifie que z est non nul et que $z^{-1} \in \mathbb{Z}[\varphi]$, alors les nombres $N(z)$ et $N(z^{-1})$ sont des entiers. De plus

on a $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$ d'après ce qui précède, donc on a $N(z) \in \{+1, -1\}$.
Réciproquement, si $N(z) \in \{+1, -1\}$, alors on a $z \neq 0$, donc $\omega(z) \neq 0$ puisque ω est un automorphisme de $\mathbb{Z}[\varphi]$, d'où $\frac{1}{z} = \frac{\omega(z)}{z\omega(z)} = \frac{\omega(z)}{N(z)} = \pm\omega(z) \in \mathbb{Z}[\varphi]$. Ainsi z est inversible dans $\mathbb{Z}[\varphi]$.

(d) Justifier que $\mathbb{Z}[\varphi]$ a une infinité d'éléments inversibles.
Indication : *calculer $N(\varphi)$ et considérer les puissances de φ.*
On a $N(\varphi) = N(0 + 1\varphi) = 0^2 + 0 \cdot 1 - 1^2 = -1$. On en déduit que, pour tout $n \in \mathbb{N}$, on a $N(\varphi^n) = N(\varphi)^n = (-1)^n$, donc φ^n est inversible pour tout $n \in \mathbb{N}$ d'après la question précédente. Or, on a $\varphi > \frac{1+2}{2} > 1$, donc les puissances φ^n de φ sont toutes distinctes, et $\mathbb{Z}[\varphi]$ a une infinité d'éléments inversibles.

3. **Éléments premiers de $\mathbb{Z}[\varphi]$**

(a) Montrer que 11 n'est pas premier dans $\mathbb{Z}[\varphi]$.
Indication : *calculer $(3 + 2\varphi)(5 - 2\varphi)$.*
On a

$$\begin{aligned}(3 + 2\varphi)(5 - 2\varphi) &= 15 + 4\varphi - 4\varphi^2 \\ &= 15 + 4\tfrac{1+\sqrt{5}}{2} - 4\tfrac{6+2\sqrt{5}}{4} \\ &= 15 + (2 + 2\sqrt{5}) - (6 + 2\sqrt{5}) \\ &= 11.\end{aligned}$$

Or, les nombres $\frac{3}{11} + \frac{2}{11}\varphi$ et $\frac{5}{11} - \frac{2}{11}\varphi$ n'appartiennent pas à $\mathbb{Z}[\varphi]$, donc 11 ne divise ni $3 + 2\varphi$, ni $5 - 2\varphi$, dans $\mathbb{Z}[\varphi]$. Ainsi 11 n'est pas premier dans $\mathbb{Z}[\varphi]$.

(b) Soit $z \in \mathbb{Z}[\varphi]$. Montrer que 2 divise z dans $\mathbb{Z}[\varphi]$ si et seulement si $N(z)$ est pair.
Indication : *pour $z = a + b\varphi$, il s'agit de montrer que a et b sont tous les deux pairs si et seulement si $N(z)$ est pair.*
Soit $z = a + b\varphi \in \mathbb{Z}[\varphi]$. Comme on a $\frac{z}{2} = \frac{a}{2} + \frac{b}{2}\varphi$, dire que 2 divise z équivaut à dire que $\frac{a}{2}$ et $\frac{b}{2}$ appartiennent à $\mathbb{Z}$, autrement dit que a et b sont des entiers pairs. Si c'est le cas, alors $N(z) = a^2 + ab - b^2$ est également pair.
Réciproquement, si $N(z) = a^2 + ab - b^2$ est pair, alors comme une somme de trois entiers impairs est impair, l'un des entiers a^2, ab, b^2 est pair, ce qui implique que a ou b est pair. Dans ce cas, au moins deux des entiers a^2, ab, b^2 sont pairs, donc comme $N(z) = a^2 + ab - b^2$ est pair, le troisième est aussi pair, ce qui implique que a et b sont pairs. Ainsi, 2 divise $z = a + b\varphi$.

(c) En déduire que 2 est un élément premier de $\mathbb{Z}[\varphi]$.
Le nombre 2 est non nul et, comme $N(2) = 4 \neq 0$, il est non inversible dans $\mathbb{Z}[\varphi]$.
Si 2 divise un produit xy déléments x et y de $\mathbb{Z}[\varphi]$, alors $N(xy)$ est pair d'après la question précédente. Or on a $N(xy) = N(x)N(y)$, donc l'un des entiers $N(x)$ ou $N(y)$ est pair, ce qui implique, d'après la question précédente, que 2 divise x ou y dans $\mathbb{Z}[\varphi]$. On en déduit que 2 est un élément premier de $\mathbb{Z}[\varphi]$.