Université de Poitiers, Année 2023-2024

3$^{\text{e}}$ année de Licence de Mathématiques, Anneaux

**Corrigé de l'examen du lundi 6 mai 2024**

---

## Exercice 1 – Questions de cours (5 points)

1. Démontrer que tout anneau euclidien est principal.

   *C'est le théorème 5.2.7 du cours.*

   Soient $A$ un anneau euclidien, $\varphi : A^* \to \mathbb{N}$ un stathme euclidien sur $A$ et $I$ un idéal de $A$. Soit $n$ le plus petit entier naturel pour lequel il existe $b \in I$ non nul tel que $\varphi(b) = n$. En particulier, on a $(b) \subseteq I$. L'application $\varphi$ étant un stathme euclidien, il existe pour tout $a \in I$ des éléments $q$ et $r$ de $A$ tels que $a = bq + r$ et soit $r = 0_A$, soit $\varphi(r) < \varphi(b)$. Or on a $r = a - bq \in I$, donc le choix de $b$ impose $r = 0_A$. Ainsi $b$ divise $a$ et $a$ appartient à $(b)$. Ceci démontre que $I$ est contenu dans $(b)$, d'où $I = (b)$ et $A$ est principal.

2. Donner la définition d'un $PGCD$ de deux éléments d'un anneau intègre et d'un anneau à $PGCD$.

   *Il s'agit des définitions 6.2.1 et 6.3.1 du cours.*

   Un $PGCD$ de deux éléments $a$ et $b$ d'un anneau intègre $A$ est un diviseur commun $d$ à $a$ et $b$ tel que tout autre diviseur de $a$ et $b$ divise $d$.

   Un anneau intègre est dit *à $PGCD$* si tout couple de ses éléments admet un $PGCD$.

3. Soit $A$ un anneau intègre. Montrer que, si $a \in A$ est irréductible, alors tout $b \in A$ est

   - soit premier avec $a$ ;
   - soit divisible par $a$.

   *Il s'agit du lemme 6.1.7 du cours.*

   Si $b$ n'est pas premier avec $a$, alors $a$ et $b$ ont un diviseur commun non inversible $d$. En particulier, il existe $u \in A$ tel que $a = du$, et comme $a$ est irréductible, $u$ est inversible. On obtient $d = au^{-1}$, donc $a$ divise $d$. Comme $d$ divise $b$, on en déduit que $a$ divise $b$.

**Exercice 2 – L'anneau $\mathbb{Z} + X\mathbb{Q}[X]$ – *Exercice issu des fiches de TD* (7 points)**

*L'exercice est extrait de l'exercice 7 de la fiche "Anneaux euclidiens, principaux, factoriels", donc pour les questions 1 et 3, se référer à la correction faite en TD. Une correction des questions 2 et 4 est donnée car elles ne sont pas formulées comme sur la fiche TD.*

Soit $A = \mathbb{Z} + X\mathbb{Q}[X]$ l'ensemble des polynômes de $\mathbb{Q}[X]$ dont le terme constant est un entier.

1. Montrer que $A$ est un anneau. Quels sont ses éléments inversibles ?

2. (a) Justifier que les polynômes constants de la forme $P(X) = p$ pour un nombre premier $p$ sont des éléments irréductibles de $A$.
   Si $P = UV$ pour deux polynômes $U$ et $V$ de $A$, alors comme $\deg P = 0$, on a $\deg U = \deg V = 0$, ce sont donc des polynômes constants non nuls et il existe des éléments $u$ et $v$ non nuls de $\mathbb{Z}$ tels que $U = u$ et $V = v$. On obtient $p = uv$, et $p$ étant un nombre premier, on a $u$ ou $v$ égal à $\pm 1$, donc $U$ ou $V$ est inversible dans $A$ et $P$ est irréductible.

   (b) Remarquer que tous les polynômes de cette forme divisent $X$ dans $A$ et en déduire que $A$ n'est pas factoriel.
   Soit $P$ un polynôme constant de la forme $P(X) = p$ pour un nombre premier $p$. Alors on a $X = \frac{1}{p}XP(X)$, avec $\frac{1}{p}X \in A$, donc $P$ divise $X$ dans $A$.
   Si $p$ et $q$ sont deux nombres premiers distincts, alors les polynômes constants $P = p$ et $Q = q$ de $A$ ne sont pas associés. On obtient donc une infinité d'éléments irréductibles deux à deux non associés qui divisent $X$ dans $A$. Comme $X$ est non nul, il n'est pas possible que l'anneau $A$ soit factoriel.

3. On considère $P, Q \in A$ tels que $P(0)$ et $Q(0)$ ne soient pas nuls simultanément.

   (a) Pourquoi existe-t-il $R \in \mathbb{Q}[X]$ tel que $R\mathbb{Q}[X] = P\mathbb{Q}[X] + Q\mathbb{Q}[X]$ ?

   (b) Vérifier que $R(0)$ est non nul.
   On pose $S = \frac{d}{R(0)}R$ où $d$ désigne le *pgcd* des entiers relatifs $P(0)$ et $Q(0)$.

   (c) Montrer que $S$ divise $P$ et $Q$ dans $\mathbb{Q}[X]$, puis dans $A$.

4. Soit $T \in A$ un diviseur commun de $P$ et $Q$ dans $A$.

   (a) Montrer qu'il existe $U \in \mathbb{Q}[X]$ tel que $S = UT$ et que $T(0)$ divise $P(0)$ et $Q(0)$.
   On a vu à la question 3 (a) que $R\mathbb{Q}[X] = P\mathbb{Q}[X] + Q\mathbb{Q}[X]$, donc comme $S = \frac{d}{R(0)}R$, il existe des polynômes $G$ et $H$ sur $\mathbb{Q}$ tels que $S = PG + QH$. Comme $T$ divise $P$ et $Q$ dans $\mathbb{Q}[X]$, on en déduit que $T$ divise $S$ dans $\mathbb{Q}[X]$. Ainsi il existe $U \in \mathbb{Q}[X]$ tel que $S = UT$.
   Comme $T$ divise $P$ dans $A$, il existe $F \in A$ tel que $P = FT$. On en déduit que $P(0) = F(0)T(0)$. Or on $F(0) \in \mathbb{Z}$ puisque $F \in A$, donc $T(0)$ divise $P(0)$ et, de même, $T(0)$ divise $Q(0)$.

   (b) En déduire que $U$ appartient à $A$ et que $S$ est un $PGCD$ de $P$ et $Q$ dans $A$.
   Comme $S = UT$, on a $S(0) = U(0)T(0)$. De plus, on a $S(0) = \frac{d}{R(0)}R(0) = d$, or $T(0)$ divise $P(0)$ et $Q(0)$, donc $T(0)$ divise $d = S(0)$. Ceci montre que $U(0)$ est un entier relatif, d'où $U \in A$.
   On a vu à la question 3 (c) que $S$ divise $P$ et $Q$ dans $A$, et on vient de montrer que, dans $A$, tout diviseur commun à $P$ et $Q$ divise $S$, donc $S$ est un $PGCD$ de $P$ et $Q$.

*Remarque : on peut montrer que lorsque $P, Q \in A$ vérifient $P(0) = Q(0) = 0$, ils admettent aussi un $PGCD$ dans $A$, et ainsi démontrer que $A$ est un* anneau à *$PGCD$.*

**Exercice 3 – Anneaux d'entiers quadratiques (12 points)**

1. **Généralités**

On fixe $\alpha$ un nombre complexe n'appartenant pas à $\mathbb{Q}$ et qui est racine d'un polynôme unitaire $U_\alpha = X^2 + rX + s$ de degré 2 à coefficients dans $\mathbb{Z}$.

(a) Pour tout sous-anneau $A$ de $\mathbb{C}$, on note $A[\alpha]$ le sous-anneau de $\mathbb{C}$ engendré par $A$ et $\alpha$. *On admet que* $A[\alpha] = \{a + b\alpha \mid a, b \in A\}$ *et que les éléments de* $\mathbb{Q}[\alpha]$ *s'écrivent de façon unique sous la forme* $a + b\alpha$ *pour* $a, b \in \mathbb{Q}$.

i. Justifier que l'autre racine $\alpha^*$ de $U_\alpha$ vérifie $\alpha^* = -r - \alpha$ et qu'elle est différente de $\alpha$.
Comme $U_\alpha = X^2 + rX + s$ a pour racines $\alpha$ et $\alpha^*$, on a $U_\alpha = (X - \alpha)(X - \alpha^*) = X^2 - (\alpha + \alpha^*)X + \alpha\alpha^*$, d'où $r = -(\alpha + \alpha^*)$ et $\alpha^* = -r - \alpha$.
Aussi, si on avait $\alpha^* = \alpha$, on aurait $r = -2\alpha \in \mathbb{Z}$, ce qui contredirait $\alpha \notin \mathbb{Q}$.

ii. Prouver que l'application $\omega : \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha]$ qui, à tout $z = a + b\alpha \in \mathbb{Q}[\alpha]$, associe $\omega(z) = a + b\alpha^*$, est un automorphisme de l'anneau $\mathbb{Q}[\alpha]$.
Notons d'abord que, comme $\alpha^* = -r - \alpha$, on a $a + b\alpha^* = a - br - b\alpha \in \mathbb{Q}[\alpha]$ pour tout $z = a + b\alpha \in \mathbb{Q}[\alpha]$, donc $\omega$ est bien une application.
Pour tous éléments $a + b\alpha$ et $c + d\alpha$ de $\mathbb{Q}[\alpha]$, on a $\omega((a + b\alpha) + (c + d\alpha)) = \omega(a + c + (b + d)\alpha) = a + c + (b + d)\alpha^*$ et $\omega(a + b\alpha) + \omega(c + d\alpha) = (a + b\alpha^*) + (c + d\alpha^*) = a + c + (b + d)\alpha^*$, donc on a $\omega((a + b\alpha) + (c + d\alpha)) = \omega(a + b\alpha) + \omega(c + d\alpha)$.
Comme $\alpha$ est une racine de $U_\alpha$, on a $\alpha^2 + r\alpha + s = 0$ donc $\alpha^2 = -s - r\alpha$. De même, on a $\alpha^{*2} = -s - r\alpha^*$. On a donc

$$\begin{aligned}\omega((a + b\alpha)(c + d\alpha)) &= \omega(ac + (ad + bc)\alpha + bd\alpha^2)\\ &= \omega(ac + (ad + bc)\alpha + bd(-s - r\alpha))\\ &= \omega(ac - bds + (ad + bc - bdr)\alpha)\\ &= ac - bds + (ad + bc - bdr)\alpha^*\end{aligned}$$

$$\begin{aligned}\omega((a + b\alpha)\omega(c + d\alpha)) &= (a + b\alpha^*)(c + d\alpha^*)\\ &= ac + (ad + bc)\alpha^* + bd\alpha^{*2}\\ &= ac + (ad + bc)\alpha^* + bd(-s - r\alpha^*)\\ &= ac - bds + (ad + bc - bdr)\alpha^*\end{aligned}$$

Ainsi on a bien $\omega((a + b\alpha)(c + d\alpha)) = \omega((a + b\alpha)\omega(c + d\alpha))$.
Aussi, on a $\omega(1) = \omega(1 + 0\alpha) = 1 + 0\alpha^* = 1$, donc $\omega$ est un morphisme d'anneaux de $\mathbb{Q}[\alpha]$ vers $\mathbb{Q}[\alpha]$ : c'est un endomorphisme de $\mathbb{Q}[\alpha]$.
Comme on a $\alpha^* = -\alpha - r$ et $\alpha = -\alpha^* - r$, alors pour tout $z = a + b\alpha \in \operatorname{Ker}\omega$, on a $0 = \omega(z) = a + b\alpha^* = a + b(-\alpha - r) = a - br - b\alpha$, d'où $a - br = 0$ et $-b = 0$, ce qui implique $a = b = 0$ et $z = 0$. On en déduit que $\operatorname{Ker}\omega = \{0\}$, donc $\omega$ est un endomorphisme injectif.
De plus, pour tout $z = a + b\alpha \in \mathbb{Q}[\alpha]$, on a $z = a + b(-\alpha^* - r) = a - br - b\alpha^* = \omega(a - br - b\alpha) \in \operatorname{Im}\omega$, donc $\omega$ est un endomorphisme surjectif. On en déduit que $\omega$ est un automorphisme de $\mathbb{Q}[\alpha]$.

(b) Pour tout $z \in \mathbb{Q}[\alpha]$, on note $N(z) = z\omega(z)$.

i. Justifier que, pour tout $z \in \mathbb{Q}[\alpha]$, on a $N(z) = 0$ si et seulement si $z = 0$.
On a $N(z) = 0$ si et seulement si $z = 0$ ou $\omega(z) = 0$. Or on a vu que $\omega$ est un automorphisme de $\mathbb{Q}[\alpha]$, donc $\omega$ ne s'annule que pour $z = 0$, d'où le résultat.

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

iii. Montrer que $N(z) = a^2 - abr + b^2 s$ pour tout $z \in \mathbb{Q}[\alpha]$.
Pour tout $z = a + b\alpha \in \mathbb{Q}[\alpha]$, on a $N(z) = (a + b\omega)(a + b\omega^*) = a^2 + ab(\omega + \omega^*) + b^2\omega\omega^*$. Or, comme $\alpha$ et $\alpha^*$ sont les deux racines de $U_\alpha$, on a $U_\alpha = (X - \alpha)(X - \alpha^*) = X^2 - (\alpha + \alpha^*) + \alpha\alpha^*$, d'où $r = -(\alpha + \alpha^*)$ et $s = \alpha\alpha^*$. Ainsi on obtient $N(z) = a^2 - abr + b^2 s$.

iv. En déduire que, pour tout $z \in \mathbb{Z}[\alpha]$, on a $N(z) \in \mathbb{Z}$ et que l'élément $z$ est inversible dans $\mathbb{Z}[\alpha]$ si et seulement si $N(z) \in \{+1, -1\}$.
Pour tout $z \in \mathbb{Z}[\alpha]$, on a $N(z) = a^2 - abr + b^2 s$ d'après la question précédente, d'où $N(z) \in \mathbb{Z}$.
Par conséquent, si $z$ est inversible dans $\mathbb{Z}[\alpha]$, ce qui signifie que $z^{-1}$ appartient aussi à $\mathbb{Z}[\alpha]$, 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 1 (b) ii., donc on a $N(z) \in \{+1, -1\}$.
Réciproquement, si $N(z) \in \{+1, -1\}$, on a $\frac{1}{z} = \frac{\omega(z)}{z\omega(z)} = \frac{\omega(z)}{N(z)}$. Or on a vu précédemment que $\omega(z) = a - br - b\alpha$, donc on a bien $\frac{1}{z} \in \mathbb{Z}[\alpha]$ et $z$ est inversible dans $\mathbb{Z}[\alpha]$.

v. Pourquoi l'anneau $\mathbb{Q}[\alpha]$ est-il un corps ?
Soit $z = a + b\alpha$ un élément non nul de $\mathbb{Q}[\alpha]$. Alors $N(z)$ est non nul d'après 1 (b) i., et on obtient $\frac{1}{z} = \frac{\omega(z)}{z\omega(z)} = \frac{\omega(z)}{N(z)} = \frac{a-br-b\alpha}{N(z)}$ avec $N(z) = a^2 - abr + b^2 s \in \mathbb{Q}$. Ainsi $\frac{1}{z}$ appartient à $\mathbb{Q}[\alpha]$ et $z$ est inversible dans $\mathbb{Q}[\alpha]$. Ceci montre que $\mathbb{Q}[\alpha]$ est un corps.

## 2. Le nombre d'or

On considère le *nombre d'or* $\varphi = \frac{1+\sqrt{5}}{2}$.

(a) Déterminer $U_\varphi$ et montrer que $\mathbb{Z}[\varphi]$ a une infinité d'éléments inversibles.
*Indication : calculer $N(\varphi)$ et considérer les puissances de $\varphi$.*
On a $\varphi^2 = \frac{3+\sqrt{5}}{2} = \varphi + 1$, donc on obtient $\varphi^2 - \varphi - 1 = 0$ et $U_\varphi = X^2 - X - 1$.
On en déduit que $\varphi^* = \frac{1-\sqrt{5}}{2}$ et que $N(\varphi) = \varphi\omega(\varphi) = \varphi\varphi^* = -1$. En particulier $\varphi$ est inversible dans $\mathbb{Z}[\varphi]$ d'après 1(b)iv., ses puissances sont donc aussi inversibles. Or $\varphi$ est un nombre réel strictement plus grand que 1, ses puissances sont donc toutes distinctes et il y a bien une infinité d'éléments inversibles dans $\mathbb{Z}[\varphi]$.

(b) Montrer que, pour tous $x, y \in \mathbb{Z}[\varphi]$ avec $y$ non nul, il existe $q \in \mathbb{Z}[\varphi]$ tel que $|N(\frac{x}{y} - q)| < 1$.
*Indication : est-il possible d'écrire $\frac{x}{y}$ sous la forme $\frac{x}{y} = a + b\varphi$ avec $a$ et $b$ dans $\mathbb{Q}$ ? Prendre alors $q = a' + b'\varphi$ avec $a'$ et $b'$ dans $\mathbb{Z}$ les plus proches possibles de $a$ et $b$.*
Comme $\mathbb{Q}[\varphi]$ est un corps d'après 1(b)v., on a $\frac{x}{y} \in \mathbb{Q}[\varphi]$ et il existe $a$ et $b$ dans $\mathbb{Q}$ tels que $\frac{x}{y} = a + b\varphi$. On considère des entiers relatifs $a'$ et $b'$ tels que $|a - a'| \leqslant \frac{1}{2}$ et

$|b-b'| \leqslant \frac{1}{2}$, et on note $q = a' + b'\varphi$. En utilisant 1(b)iii. et 2(a), on obtient

$$\begin{aligned} |N(\tfrac{x}{y} - q)| &= |N((a-a') + (b-b')\varphi)] \\ &= |(a-a')^2 + (a-a')(b-b') - (b-b')^2| \\ &\leqslant |a-a'|^2 + |a-a'||b-b'| + |b-b'|^2 \leqslant \tfrac{3}{4} < 1. \end{aligned}$$

(c) On note $\mathbb{Z}[\varphi]^* = \mathbb{Z}[\varphi] \setminus \{0\}$. Démontrer que l'application $N^* : \mathbb{Z}[\varphi]^* \to \mathbb{N}$ définie par $N^*(z) = |N(z)|$ est un stathme euclidien sur $\mathbb{Z}[\varphi]$.

On fixe d'abord un couple $(a, b)$ d'éléments de $\mathbb{Z}[\varphi]$ avec $b$ non nul. D'après 2(b), il existe $q \in \mathbb{Z}[\varphi]$ tel que $|N(\frac{a}{b} - q)| < 1$. On pose $r = a - bq$. Si $r$ est non nul, en utilisant 1(b)i. et la question précédente, on obtient $N^*(r) = |N(a-bq)| = |N((\frac{a}{b} - q)b)| = |N(\frac{a}{b} - q)||N(b)| < |N(b)| = N^*(b)$.

Pour montrer que $N^*$ est un stathme euclidien sur $\mathbb{Z}[\varphi]$, il reste à montrer que, si $(a, b)$ est un couple d'éléments non nuls de $\mathbb{Z}[\varphi]$ tel que $b$ divise $a$, alors on a $N^*(b) \leqslant N^*(a)$. Soit $(a, b)$ un tel couple et soit $d \in \mathbb{Z}[\varphi]$ tel que $a = bd$. Comme $a$ est non nul, on a $d \neq 0$ et $N(d)$ est aussi non nul d'après 1(b)i. Comme c'est un élément de $\mathbb{Z}$ d'après 1(b)iv., on obtient $N^*(d) \geqslant 1$. On obtient $N^*(a) = |N(bd)| = |N(b)||N(d)| = N^*(b)N^*(d) \geqslant N^*(b)$, ce qui démontre que $N^*$ est un stathme euclidien sur $\mathbb{Z}[\varphi]$.

(d) En déduire que l'anneau $\mathbb{Z}[\varphi]$ est euclidien, principal, factoriel et intégralement clos.

Comme il y a un stathme euclidien sur $\mathbb{Z}[\varphi]$, l'anneau $\mathbb{Z}[\varphi]$ est euclidien. On en déduit qu'il est de plus principal, factoriel et intégralement clos car tout anneau euclidien est principal, tout anneau principal est factoriel, tout anneau factoriel est à *PGCD* et tout anneau à *PGCD* est intégralement clos.

(e) i. Soit $z = a + b\varphi \in \mathbb{Z}[\varphi]$. Montrer que 7 divise $z$ dans $\mathbb{Z}[\varphi]$ si et seulement si 7 divise $N(z)$ dans $\mathbb{Z}$.

*Indication :* *pour la réciproque, montrer d'abord que $N(z) = a^2 + ab - b^2$, puis que $N(z)$ est congru à $(a+4b)^2 - 3b^2$ modulo 7. Calculer ensuite les carrés modulo 7, et donner les valeurs possibles de $3b^2$ et de $(a+4b)^2$ modulo 7. En déduire que, si $N(z)$ est nul modulo 7, alors $3b^2$ et $(a+4b)^2$ aussi.*

Si 7 divise $z$ dans $\mathbb{Z}[\varphi]$, alors on a $z = 7d$ pour $d \in \mathbb{Z}[\varphi]$. On a alors $N(z) = N(7)N(d) = 49N(d)$ avec $N(d)$ et $N(z)$ dans $\mathbb{Z}$ d'après 1(b)iv., ce qui montre que 7 divise $N(z)$ dans $\mathbb{Z}$.

Réciproquement, supposons que 7 divise $N(z)$ dans $\mathbb{Z}$. Comme on a $N(z) = a^2 + ab - b^2$ d'après 1(b)iii., alors $N(z)$ est congru modulo 7 à $(a+4b)^2 - 3b^2 = a^2 + 8ab + 13b^2$. Or les carrés modulo 7 sont 0,1,2 et 4, donc les valeurs possibles de $3b^2$ modulo 7 sont 0,3,5 et 6. Comme $(a+4b)^2$ est un carré, il est congru à 0,1,2 ou 4, et donc $N(z)$ ne peut être nul modulo 7 que si $3b^2$ et $(a+4b)^2$ sont nul modulo 7, ce qui implique que 7 divise $b$ et $a+4b$, donc 7 divise aussi $a$. Ceci montre que 7 divise $z = a + b\varphi$ dans $\mathbb{Z}[\varphi]$.

ii. En déduire que 7 est un élément premier et irréductible de $\mathbb{Z}[\varphi]$.

Si 7 divise un produit $xy$ d'éléments de $\mathbb{Z}[\varphi]$, alors on a $7d = xy$ pour $d \in \mathbb{Z}[\varphi]$ et on a $N(7d) = N(xy)$ donc on a $N(7)N(d) = N(x)N(y)$, d'où $49N(d) = N(x)N(y)$. Or $N(d)$, $N(x)$ et $N(y)$ sont des entiers d'après 1(b)iv., donc 7 divise $N(x)N(y)$ dans $\mathbb{Z}$, et comme 7 est un nombre premier, il divise $N(x)$ ou $N(y)$ (dans $\mathbb{Z}$). La question précédente montre que 7 divise $x$ ou $y$ dans $\mathbb{Z}[\varphi]$. Comme 7 est non nul et non inversible dans $\mathbb{Z}[\varphi]$ (car $N(7) = 49 \notin \{+1, -1\}$), on en déduit que 7 est un élément premier, et donc irréductible, de $\mathbb{Z}[\varphi]$.