
Deuxième session
Vendredi 26 juin 2026 — 10h – 12h
Corrigé

Exercice 1 : (1+3 pts) Soit $(A, +, \cdot)$ un anneau commutatif unitaire. On note $B = \{x \in A : x^2 = x\}$.

1. Vérifier que pour tout $x \in B$ on a $1 - x \in B$.
2. On pose $x \circ y = x + y - 2xy$. Montrer que $\circ$ est une loi de composition interne sur B et que $(B, \circ, \cdot)$ est un anneau commutatif unitaire.

Solution.

1. Soit $x \in B$. Alors $x^2 = x$, et $(1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x$, d'où $1 - x \in B$.
2. Soient $x, y \in B$. Alors $x^2 = x$ et $y^2 = y$, et

   $$(x \circ y)^2 = (x+y-2xy)^2 = x^2+y^2+4x^2y^2+2xy-4x^2y-4xy^2 = x+y+4xy+2xy-4xy-4xy = x+y-2xy = x \circ y,$$

   d'où $x \circ y \in B$. Clairement $x \circ y = x + y - 2xy = y + x - 2yx = y \circ z$ et $\circ$ est commutative. On a

   $$(x \circ y) \circ z = (x+y-2xy) \circ z = x+y-2xy+z-2(x+y-2xy)z = x+y+z-2xy-2yz-2zx+4xyz,$$

   ce qui donne $x \circ (y \circ z) = (y \circ z) \circ x = x + y + z - 2xy - 2yz - 2zx + 4xyz$ par symétrie, et $\circ$ est associative. De plus $x \circ 0 = x + 0 - 2x0 = x$ et $0 = 0^2 \in B$ est élément neutre additif. Enfin, $x \circ x = x + x - 2x^2 = 2x - 2x = 0$ et x est son propre inverse additif. Ainsi $(B, 0, \circ)$ est un groupe abélien (d'exposant 2).
   Puisque $(B, +, \cdot)$ est un anneau commutatif unitaire, $\cdot$ est associatif, commutatif, avec élément neutre $1 = 1^2 \in B$. Vérifions la distributivité :

   $$x(y \circ z) = x(y + z - 2yz) = xy + xz - 2xyz = xy + xz - 2x^2yz = xy + xz - 2xyxz = (xy) \circ (xz).$$

   Ainsi $(B, \circ, \cdot)$ est un anneau commutatif unitaire.

Exercice 2 : (2+1+2 pts) Soient $f \leq -2$ un entier et ω, $\bar{\omega}$ les deux solutions complexes de $z^2 - z - f = 0$. On considère l'ensemble $A = \mathbb{Z} + \omega\mathbb{Z} \subseteq \mathbb{C}$.

1. Calculer $\omega + \bar{\omega}$ et $\omega\bar{\omega}$. Montrer que A est le sous-anneau $\mathbb{Z}[\omega]$ de $\mathbb{C}$ et est stable par conjugaison.
2. Montrer que $z\bar{z} \in \mathbb{N}$ pour tout $z \in A$.
3. Montrer qu'un élément $p + q\omega \in A$ est inversible dans A si et seulement si $p^2 + pq - fq^2 = 1$. En déduire que les seuls éléments inversibles de A sont 1 et -1.

Solution.

1. On remarque que $z^2 - z - f = 0$ est une équation quadratique réelle de discriminant $(-1)^2 - 4(-f) = 1 + 4f < 0$ puisque $f \leq -2$. Ainsi l'équation a deux racines complexes conjuguées ω et $\bar{\omega}$. D'après le relation racines-coefficients, on a $\omega + \bar{\omega} = 1$ et $\omega\bar{\omega} = -f$. Ainsi $-f = \omega\bar{\omega} = \omega(1-\omega) = \omega - \omega^2$, et $\omega^2 = \omega + f \in A$. Donc A est clos par multiplication par ω, ce qui signifie que $A = \mathbb{Z}[\omega]$ est un sous-anneau de $\mathbb{C}$. De plus, $\overline{p + q\omega} = p + q\bar{\omega} = p + q(1-\omega) = (p+q) - q\omega \in A$, et A est stable par conjugaison complexe : $\bar{A} \subseteq A$. Alors $A = \bar{\bar{A}} \subseteq \bar{A} \subseteq A$ et on a même égalité.
2. Soit $z = p + q\omega \in A$. Alors

   $$z\bar{z} = (p + q\omega)(p + q\bar{\omega}) = p^2 + pq(\omega + \bar{\omega}) + q^2\omega\bar{\omega} = p^2 + pq - fq^2 \in \mathbb{N}.$$

3. Si $z, z' \in A$ avec $zz' = 1$, alors $1 = zz'\overline{zz'} = z\bar{z}\,z'\bar{z}' = k\,\ell$ où $k = z\bar{z}$ et $\ell = z'\bar{z}'$ sont deux entiers non-nuls. Ceci implique $k = \ell = 1$, et en particulier $k = z\bar{z} = p^2 + pq - fq^2$, où $z = p + q\omega$. Donc si $p + q\omega$ est inversible, alors $p^2 + pq - fq^2 = 1$. Réciproquement, si $p^2 + pq - fq^2 = 1$ et $z = p + q\omega \in A$, alors $z\bar{z} = 1$ et z est inversible avec inverse $\bar{z}$.
   Cherchons les $(p, q) \in \mathbb{Z}^2$ tels que $p^2 + pq - fq^2 = 1$. Si $q = 0$ on a $p^2 = 1$ et $p = \pm 1$. Sinon, $\frac{p}{q}$ est une solution de $z^2 + z - f - 1 = 0$, de discriminant $1 + 4(f+1) \leq 1 - 4 < 0$. Il n'y a donc pas de solution réelle, et encore moins rationnelle. Ainsi les seuls élement inversibles sont ± 1.

Exercice 3 : (5+1+1 pts) On considère l'anneau $A = \mathbb{Z}[X]/(2(X^2-1))$, et on note x et $\bar{2}$ les classes de X et 2, respectivement.

1. On cherche à montrer que les seuls éléments inversibles de A sont les (classes de) ± 1. Soient donc $u, v \in A$ les classes de $U, V \in \mathbb{Z}[X]$, avec $uv = 1$.
   (a) Montrer que $A/(2) \cong F_2[X]$. En déduire que $U, V \equiv 1 \mod 2Z[X]$.
   (b) Si $U = 1 + 2P$ et $V = 1 + 2Q$ pour des $P, Q \in \mathbb{Z}[X]$, montrer que $X^2 - 1$ divise $P + Q + 2PQ$.
   (c) En déduire que pour $\ell = \pm 1$ on a $P(\ell) = Q(\ell) \in \{0, -1\}$.
   (d) En déduire que P est congru à 0 ou -1 modulo $X^2 - 1$.
   (e) En déduire que $U \equiv \pm 1 \mod 2(X^2-1)$.
2. Vérifier qu'il y a $a, b \in A$ avec $a\bar{2} = \bar{2}x$ et $b\bar{2}x = \bar{2}$.
3. Montrer que $\bar{2}$ et $\bar{2}x$ ne sont pas multiples l'un de l'autre par un élément inversible de l'anneau.

Solution.

1. (a) On a $(2(X^2-1)) \leq (2)$, d'où $A/2 = \mathbb{Z}[X]/(2(X^2-1))(2) = \mathbb{Z}[X]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[X] = \mathbb{F}_2[X]$. Les images de u et v dans $A/(\bar{2}) \cong \mathbb{F}_2[X]$ satisfont $(U + (2))(V + (2)) = 1$. Or, le seul élément inversible de $\mathbb{F}_2[X]$ est 1. Donc $U, V \in 1 + (2) = 1 + 2\mathbb{Z}[X]$.
   (b) On a $UV = (1 + 2P)(1 + 2Q) = 1 + 2P + 2Q + 4PQ$ est congru à 1 modulo $2(X^2 - 1)$. Alors $2(X^2 - 1)$ divise $2P + 2Q + 4PQ$, et $X^2 - 1$ divise $P + Q + 2PQ$.
   (c) On a
   $$0 = P(\ell) + Q(\ell) + 2P(\ell)Q(\ell) = P(\ell)(1 + Q(\ell)) + Q(\ell)(1 + P(\ell)).$$
   Puisque $P(\ell)$ et $1 + P(\ell)$ sont premiers entre eux, tout comme $Q(\ell)$ et $1 + Q(\ell)$, on a soit $P(\ell) = Q(\ell) = 0$, soit $1 + P(\ell) + 1 + Q(\ell) = 0$ (puisque $P(\ell) = Q(\ell) \notin \{0, -1\}$ est impossible, et $P(\ell) = -Q(\ell) \neq 0$ est impossible).
   (d) Soit $aX + b$ le reste de la division euclidienne de P par $X^2 - 1$. Alors $a + b = P(1) \in \{0, -1\}$ et $-a + b = P(-1) \in \{= 0, -1\}$. Ainsi $2a \in \{1, 0, -1\}$ d'où $a = 0$ et P est congru à 0 ou -1 modulo $X^2 - 1$.
   (e) D'après la question précédente, $U = 1 + 2P \equiv \pm 1 \mod 2(X^2 - 1)$.
2. On prend $a = x$ et $b = x$, puisque $X\,2X = 2X^2 \equiv 2 \mod 2(X^2 - 1)$.
3. $\bar{2}x \neq \pm\bar{2}$ puisque $2(X^2 - 1)$ ne divise pas $2X \mp 2$ dans $\mathbb{Z}[X]$.

Exercice 4 : (2+2+1 pts) Soit $A = \mathcal{C}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions continues réelles, et I le sous-ensemble des fonctions réelles nulles en 0. On admet que A est un anneau, et que I est un idéal dans A.

1. Soient $f_1, \ldots, f_n \in A$. Montrer que tout élément g de l'idéal $(f_1, \ldots, f_n)$ vérifie $|g| = O(\sum |f_i|)$ au voisinage de 0 (où $g = O(h)$ au voisinage de 0 signifie qu'il existe une constante c telle que $g(x) \leq ch(x)$ pour $|x|$ suffisamment petit).
2. En déduire que I n'est pas engendré par un nombre fini d'éléments, et donc que A n'est pas noethérien.
3. Montrer que $I^2 = I$, où I^2 est l'idéal qui consiste des sommes des produits de deux éléments de I.

Solution.

1. Puisque $g \in (f_1, \ldots, f_n)$ il y a $g_1, \ldots, g_n \in \mathcal{C}(\mathbb{R}, R)$ avec $g = \sum_{i=1}^n g_i f_i$. Puisque les fonctions $|g_i|$ sont continues sur l'interval $[-1, 1]$, il y on un maximum m_i. Soit $m = \sum_i m_i$. Alors pour $x \in [-1, 1]$ on a
   $$|g(x)| = |\sum_i g_i(x) f_i(x)| \leq \sum_i |g_i(x)|\,|f_i(x)| \leq \sum_i m_i \sum_j |f_j(x)|,$$
   et on peut prendre $c = \sum_i m_i$.
2. Supposons pour une contradiction que $I = (f_1, \ldots, f_n)$ est finiment engendré. Puisque $\mathrm{id}_{\mathbb{R}} \in I$, les f_i n'ont aucun zéro commun sauf 0. Donc $f(x) = \sum_i |f_i(x)| > 0$ pour tout $x \neq 0$, et f est continue avec $f(0) = 0$. Soit $g(x) = \sqrt{f(x)}$. Alors g est continue sur $\mathbb{R}$ avec $g(0) = 0$, et donc $g \in I$. Mais $\lim_{x\to 0} \frac{g(x)}{f(x)} = \lim_{x\to 0} \frac{1}{g(x)} \to \infty$, ce qui contredit $g = O(f) = O(\sum_i |f_i|)$.
   Ainsi I n'est pas finiment engendré. D'après un théorème du cours, un anneau est noethérien si et seulement si tout idéal est finiment engendré. Donc A n'est pas noethérien.

3. Il est clair que $I^2 \leq I$. Soit donc $f \in I$. On pose $g = \sqrt{|f|}$ et $h = \sqrt{|f|}\mathrm{sgn}(f)$, où $\mathrm{sgn}(x) = 1$ si $f(x) > 0$, 0 si $f(x) = 0$ et -1 si $f(x) < 0$. Alors g et h sont continues, zéro en 0, et $gh = f$. Ainsi $f \in I^2$.

Exercice 5 : (1+2+1+1+2+1 pts) Soit $\alpha = \frac{1+i\sqrt{19}}{2} \in \mathbb{C}$ et $A = \mathbb{Z}[\alpha]$. On note $N : \mathbb{C} \to \mathbb{C}, z \mapsto z\overline{z}$ la *norme* sur $\mathbb{C}$.

1. Déterminer le polynôme minimal de α sur $\mathbb{Q}$.
2. Montrer que pour tous $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $r = 0$ ou $N(r) < N(b)$ et qui vérifient soit $a = bq + r$, soit $2a = bq + r$.
   (Indication : Si $a/b = u + \alpha v$ avec $u, v \in \mathbb{Q}$, on peut distinguer selon $|\lfloor v \rfloor + \frac{1}{2} - v| \leq \frac{1}{6}$ ou pas.)
3. Montrer que $A/(2) \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$.
4. En déduire que l'idéal engendré par 2 est maximal dans A.
5. Soit I un idéal non trivial de A, et soit $a \in I \setminus \{0\}$ de norme minimale. En utilisant les questions précédentes, montrer que $I = (a)$.
6. En déduire que A est principal.

Solution.

1. On a $\alpha^2 = \frac{1-19+2i\sqrt{19}}{4} = \frac{-20+2+2i\sqrt{19}}{4} = -5 + \alpha$. Puisque $\alpha \notin \mathbb{Q}$, le polynôme minimal de α sur $\mathbb{Q}$ est $X^2 - X + 5$. Il en découle que $A = \mathbb{Z} + \alpha\mathbb{Z}$. On note que $\bar{\alpha} = 1 - \alpha \in A$, et A est stable par conjugaison complexe.
2. Soit $x = a/b = u + \alpha v$ avec $u, v \in \mathbb{Q}$ et $n = \lfloor v \rfloor$.
   1er cas : $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$. Soient s et t les entiers les plus proches, respectivement, de u et v. Alors $|s - u| \leq \frac{1}{2}$ et $|t - v| \leq \frac{1}{2}$. On pose $q = s + \alpha t \in A$. Alors
   $$N(x - q) = (s - u)^2 + (s - u)(t - v) + 5(t - v)^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1.$$
   Donc avec $r = a - bq = b(x - q)$ on a bien $N(r) < N(b)$.
   2e cas : $v \in [n + \frac{1}{3}, n + \frac{2}{3}]$. Alors $2v \in [2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}]$. On prend s l'entier le plus proche de $2u$, et $t = n + 1$. Alors $|2u - t| \leq \frac{1}{2}$ et $|2v - t| \leq \frac{1}{3}$. Si $q = s + \alpha t$ et $r = 2a - bq$, on calcule comme ci-dessus que $N(r) < N(b)$.
3. On a $A \cong \mathbb{Z}[X]/(X^2 - X + 5)$, et donc
   $$A/(2) \cong \mathbb{Z}[X]/(2)(X^2 - X + 5) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 - X + \bar{5}) \cong \mathbb{F}_2[X]/(X^2 + X + 1).$$
4. $X^2 + X + 1$ est de degré 2 et n'a pas de racine dans $\mathbb{F}_2$; il est donc irréductible sur $\mathbb{F}_2$. Ainsi $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps, ce qui implique que $A/(2)$ est un corps, et (2) est maximal dans A.
5. On a $(a) \leq I$. Pour une contradiction, soit $b \in I \setminus (a)$. D'après 2. il y a $q, r \in A$ avec $b = aq + r$ ou $2b = aq + r$ et soit $r = 0$ soit $N(r) < N(a)$. Alors $r = b - aq$ ou $r = aq - 2b$ et $r \in I$; puisque $N(a)$ était minimal, on a $r = 0$ et soit $b = aq \in (a)$, soit $2b = aq$. Dans ce cas $aq \in (2)$ qui est premier, et soit $a \in (2)$ soit $q \in (2)$. Si $q \in (2)$ alors $q = 2q'$; par simplification ($A \leq \mathbb{C}$ est intègre) on a $b = aq' \in (a)$. Sinon $a = 2a'$ pour un $a' \in A$ et il y a $q' \in A$ avec $qq' - 1 \in (2)$, disons $qq' = 1 + 2p$ pour $p \in A$. Alors
   $$2bq' = aqq' = a(1 + 2p) = a + 2ap = 2a' + 2ap\,;$$
   par simplification on a $a' = bq' - ap \in I$. Puisque $N(a') = N(a)/4 < N(a)$, ceci contredit la minimalité de $N(a)$.
6. D'après la question précédente, tout idéal est engendré par un seul élément. Donc A est principal.