Algèbre 2

Examen du 19 Janvier 2018 – Corrigé

Calculatrices et documents non autorisés. Durée 3h

Exercice 1. On considère l'anneau $\mathbb{Z}[i\sqrt{p}] = \{z = a + ib\sqrt{p};\quad a, b \in \mathbb{Z}\}$, où $p \in \mathbb{N}$ est un nombre premier et $\langle 1 + i\sqrt{p}\rangle = (1 + i\sqrt{p})\mathbb{Z}[i\sqrt{p}] = \{(1 + i\sqrt{p})z;\quad z \in \mathbb{Z}[i\sqrt{p}]\}$ l'idéal de $\mathbb{Z}[i\sqrt{p}]$ engendré par $1 + i\sqrt{p}$.
Soit l'application

$$\begin{array}{rccc} f: & \mathbb{Z}[i\sqrt{p}] & \to & \mathbb{Z}/(p+1)\mathbb{Z} \\ & a + ib\sqrt{p} & \mapsto & \overline{a + pb} \end{array}$$

(1) Montrer que f est un morphisme d'anneaux surjectif.
(2) Montrer que $p + 1 \in \langle 1 + i\sqrt{p}\rangle$.
(3) En déduire que $\operatorname{Ker} f = \langle 1 + i\sqrt{p}\rangle$.
(4) On suppose que $p = 2$.
  (a) L'idéal $\langle 1 + i\sqrt{2}\rangle$ de $\mathbb{Z}[i\sqrt{2}]$ est-il maximal?
  (b) L'élément $1 + i\sqrt{2}$ est-il irréductible dans $\mathbb{Z}[i\sqrt{2}]$?
(5) On suppose que $p \neq 2$.
  (a) L'idéal $\langle 1 + i\sqrt{p}\rangle$ de $\mathbb{Z}[i\sqrt{p}]$ est-il premier?
  (b) L'élément $1 + i\sqrt{p}$ est-il irréductible dans $\mathbb{Z}[i\sqrt{p}]$?

Corrigé. (1) Il est claire que f est surjectif. Montrons que c'est un morphisme d'anneaux. Soient $x = a + ib\sqrt{p}$, $x' = a' + ib'\sqrt{p}$ deux éléments de $\mathbb{Z}[i\sqrt{p}]$. On a

$$\begin{aligned} f(x + x') &= f(a + a' + i(b + b')\sqrt{p}) = \overline{a + a' + p(b + b')} = \overline{a + pb} + \overline{a' + pb'} \\ &= f(x) + f(x') \end{aligned}$$

et

$$\begin{aligned} f(xx') &= f(aa' - bb'p + i(ab' + a'b)\sqrt{p}) = \overline{aa' - bb'p + p(ab' + a'b)} \\ &= \overline{aa' + bb'p^2 + p(ab' + a'b)} \quad car\ p^2 \equiv -p[p+1] \\ &= \overline{(a + pb)(a' + pb')} = \overline{a + pb} \times \overline{a' + pb'} \\ &= f(x)f(x') \end{aligned}$$

On en déduit que f est un morphisme d'anneaux surjectif.

(2) On a $1 + p = (1 + i\sqrt{p})(1 - i\sqrt{p}) \in (1 + i\sqrt{p})\mathbb{Z}[i\sqrt{p}]$, donc $p + 1 \in \langle 1 + i\sqrt{p}\rangle$.

(3) Il est claire que $1 + i\sqrt{p} \in \operatorname{Ker}(f)$, car $f(1 + i\sqrt{p}) = \overline{1 + p} = \overline{0}$. Réciproquement, si $x = a + ib\sqrt{p} \in \operatorname{Ker}(f)$, alors $\overline{a + pb} = \overline{0}$ et il existe $k \in \mathbb{Z}$ tel que $a + bp = k(p + 1)$. Donc

$$\begin{aligned} x = a + ib\sqrt{p} &= k(p+1) - bp + ib\sqrt{p} \\ &= k(p+1) - bp - b + b + ib\sqrt{p} \\ &= (k - b)(p + 1) + b(1 + i\sqrt{p}) \end{aligned}$$

Comme $1+p$ *et* $1+i\sqrt{p}$ *appartiennent à l'idéal* $\langle 1+i\sqrt{p}\rangle$*, on a* $x \in \langle 1+i\sqrt{p}\rangle$*. Par conséquent* $\mathrm{Ker}(f) = \langle 1+i\sqrt{p}\rangle$*.*

(4) On suppose $p = 2$*.*

(a) On a $\mathrm{Ker}(f) = \langle 1+i\sqrt{2}\rangle$ *et* $\mathrm{Im}(f) = \mathbb{Z}/3\mathbb{Z}$*. Donc d'après le théorème d'isomorphisme* $\mathbb{Z}[i\sqrt{2}]/\langle 1+i\sqrt{2}\rangle \simeq \mathbb{Z}/3\mathbb{Z}$*. Comme* $\mathbb{Z}/3\mathbb{Z}$ *est un corps, l'idéal* $\langle 1+i\sqrt{2}\rangle$ *est maximal dans l'anneau* $\mathbb{Z}[i\sqrt{2}]$*.*

(b) L'ideal $\langle 1+i\sqrt{2}\rangle$ *étant maximal, il est premier, par suite l'élément* $\langle 1+i\sqrt{2}$ *est irréductible dans* $\mathbb{Z}[i\sqrt{2}]$*.*

(5) On suppose $p \neq 2$.

(a) On a dans ce cas $\mathbb{Z}[i\sqrt{p}]/\langle 1+i\sqrt{p}\rangle \simeq \mathbb{Z}/(p+1)\mathbb{Z}$. Or p est premier et $p \neq 2$, donc $p+1$ est pair. On en déduit que l'anneau $\mathbb{Z}/(p+1)\mathbb{Z}$ n'est pas intègre, donc $\mathbb{Z}[i\sqrt{p}]/\langle 1+i\sqrt{p}\rangle$ n'est pas intègre.

(b) Comme l'anneau $\mathbb{Z}[i\sqrt{p}]/\langle 1+i\sqrt{p}\rangle$ n'est pas intègre, l'idéal $\langle 1+i\sqrt{2}\rangle$ n'est pas premier et donc $1+i\sqrt{2}$ n'est pas irréductible dans $\mathbb{Z}[i\sqrt{p}]$.

Exercice 2.

(1) Soit K un corps et $P \in K[X]$ un polynôme de degré 2 ou 3. Montrer que P est irréductible dans $K[X]$ si, et seulement si, P n'a pas de racines dans K.
Montrer que cette caractérisation ne s'applique plus pour $d^\circ(P) \geq 4$.

(2) Déterminer la liste des polynômes unitaires irréductibles de degré ≤ 2 dans $\mathbb{Z}/3\mathbb{Z}[X]$.

(3) Décomposer les polynômes suivants en facteurs irréductibles dans $\mathbb{Z}/3\mathbb{Z}[X]$

$$(i)\ X^2+X+\bar{1},\ \ (ii)\ X^3+X+\bar{2},\ (iii)\ X^4+X^3+X+\bar{1}$$

(4) On considère le polynôme $P(X) = X^5 - X + 1 \in \mathbb{Z}[X]$.

(a) On note $\bar{P}$ la réduction de P modulo 3 (image de $P(X)$ dans $\mathbb{Z}/3\mathbb{Z}[X]$). Montrer que $\bar{P}$ est un polynôme irréductible dans $\mathbb{Z}/3\mathbb{Z}[X]$.

(b) En déduire que $(\mathbb{Z}/3\mathbb{Z}[X])/\langle\bar{P}\rangle$ est un corps.

(c) Le polynôme P est-il irréductible dans $\mathbb{Z}[X]$, dans $\mathbb{R}[X]$, dans $\mathbb{C}[X]$?

Corrigé. (1) Soit $P \in K[X]$ *tel que* $\deg(P) = 2$ *ou* $\deg(P) = 3$*. Si* P *est réductible, il existe* $A, B \in K[X]$ *tels que* $\deg(A) = r \geq 1$*,* $\deg(B) = s \geq 1$ *et* $P = AB$*. On a* $r+s = \deg(P) = 2$ *ou* $= 3$*. L'un des degrés* r *ou* s *est égal à 1. Par exemple, si* $r = 1$*, alors* B *est de la forme* $B(X) = aX+b$*, où* $a \in K$ *et* $a \neq 0$*, et donc* a *est un élément inversible de* K*.* P *admet donc pour racine* ba^{-1}*. Réciproquement, si* P *a une racine* $\alpha \in K$*, il existe* $Q \in K[X]$*, avec* $\deg(Q) = \deg(P) - 1 \neq 0$*, tel que* $P(X) = (X-\alpha)Q(X)$ *et* P *n'est pas irréductible.*

(2) Dans $\mathbb{Z}/3\mathbb{Z}[X]$ *les polynômes irréductibles sont non inversibles donc de degré* ≥ 1*. Les polynômes unitaires de degré 1 sont irréductibles, ce sont* $\boxed{X}$*,* $\boxed{X+\bar{1}}$ *et* $\boxed{X-\bar{1}}$*. Les polynômes unitaires de degré 2 sont irréductibles si et seulement si ils n'ont pas de racine dans* $\mathbb{Z}/3\mathbb{Z}$*. Cette condition élimine* X^2*,* $X^2 \pm X$*,* $X^2 \pm \bar{1}$ *et* $X^2 \pm X + \bar{1}$*. Les polynômes unitaires irréductibles de degré 2 sont donc* $\boxed{X^2+\bar{1}}$ *et* $\boxed{X^2 \pm X - \bar{1}}$*.*

(3) On a

(a) $X^2 + X + \bar{1} = (X - \bar{1})^2$*;*

(b) $X^3 + X + \bar{2} = X^3 + X - \bar{1} = (X + 1)(X^2 - X - 1)$*;*

(c) $X^4 + X^3 + X + \bar{1} = (X + \bar{1})(X^3 + \bar{1}) = (X + \bar{1})(X + \bar{1})^3 = (X + \bar{1})^4$.

(4) (a) $P(X) = X^5 - X + 1 \in \mathbb{Z}[X]$. *Sa réduction modulo 3 est* $\bar{P}(X) = X^5 - X + \bar{1} = X^5 + \bar{2}X + \bar{1} \in \mathbb{Z}/3\mathbb{Z}[X]$ *est unitaire et n'a pas de racines dans* $\mathbb{Z}/3\mathbb{Z}[X]$. *Donc il n'est divisible pas aucun des polynômes irréductible* X, $X + \bar{1}$, $X - \bar{1}$.

S'il était réductible dans $\mathbb{Z}/3\mathbb{Z}[X]$, *il serait donc produit d'un facteur irréductible unitaire de degré 2 et d'un autre facteur irréductible unitaire de degré 3. Mais aucun des polynômes irréductibles* $X^2 + \bar{1}$, $X^2 + X - \bar{1}$ *et* $X^2 - X - \bar{1}$ *ne divise* $X^5 - X + \bar{1}$. *Il suffit pour cela d'effectuer trois les divisions euclidiennes.*

On en déduit que la réduction $\bar{P}(X) = X^5 - X + \bar{1}$ *est irréductible dans* $\mathbb{Z}/3\mathbb{Z}[X]$.

(b) Comme $\bar{P}$ *est irréductible dans* $\mathbb{Z}/3\mathbb{Z}[X]$, *l'idéal* $\langle \bar{P} \rangle$ *est premier dans* $\mathbb{Z}/3\mathbb{Z}[X]$ *et par conséquent l'anneau quotient* $\mathbb{Z}/3\mathbb{Z}[X]/\langle \bar{P} \rangle$ *est un corps.*

(c) Comme la réduction $\bar{P}$ *est irréductible dans* $\mathbb{Z}/3\mathbb{Z}[X]$, *le polynôme* P *est irréductible dans* $\mathbb{Q}[X]$ *et puisque* P *est primitif (car unitaire), il est irréductible dans* $\mathbb{Z}[X]$. *Le polynôme* P *n'est irréductible ni dans* $\mathbb{R}[X]$ *(car* $\deg(P) > 2$*), ni dans* $\mathbb{C}[X]$ *(car* $\deg(P) > 1$*).*

Exercice 3. (a) Donner la liste de tous les éléments du groupe alterné $\mathcal{A}_4$ en précisant leur ordre.

(2) Soit G un sous-groupe du groupe symétrique $\mathcal{S}_4$. On fait opérer G sur l'ensemble $E = \{1, 2, 3, 4\}$ par l'action induite par l'action naturelle de $\mathcal{S}_4$. Pour $x \in E$ on note O_x l'orbite de x et G_x le stabilisateur de x pour cette action.
Déterminer O_x et G_x pour $x = 1, 2, 3, 4$ dans chacun des cas suivants :

(a) $G = \langle (1\,2\,3) \rangle$;

(b) $G = \langle (1\,2\,3\,4) \rangle$;

(c) $G = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$;

(d) $G = \{\mathrm{id}, (1\,2), (1\,2)(3\,4), (3\,4)\}$;

(e) $G = \mathcal{A}_4$.

Corrigé. (1) On a dans le groupe les $12 = \frac{4}{2}$ *éléments distincts suivants :*

(i) id*;*

(ii) les 3 éléments d'ordre 2 : $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(2\,3)(1\,4)$*;*

(iii) les 8 éléments d'ordre 3 : $(1\,2\,3)$, $(1\,3\,2)$, $(2\,3\,4)$, $(2\,4\,3)$, $(1\,3\,4)$, $(1\,4\,3)$, $(1\,2\,4)$, $(1\,4\,2)$.

(2) (a) $G = \langle (1\,2\,3) \rangle = \{\mathrm{id} = \sigma^3, (1\,3\,2) = \sigma^2, (1\,2\,3) = \sigma\}$, *groupe cyclique d'ordre 3 engendré par le 3-cycle* $\sigma = (1\,2\,3)$.

x	O_x	G_x
1	$\{1, 2, 3\}$	id
2	$\{1, 2, 3\}$	id
3	$\{1, 2, 3\}$	id
4	$\{4\}$	G

(b) $G = \langle(1\,2\,3\,4)\rangle = \{\mathrm{id} = \sigma^4, (1\,4\,3\,2) = \sigma^3, (1\,3)(2\,4) = \sigma^2, (1\,2\,3\,4) = \sigma\}$, *groupe cyclique d'ordre 4 engendré par le 4-cycle* $\sigma = (1\,2\,3\,4)$.

x	O_x	G_x
1	$\{1,2,3,4\}$	id
2	$\{1,2,3,4\}$	id
3	$\{1,2,3,4\}$	id
4	$\{1,2,3,4\}$	id

(c) $G = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, *groupe d'ordre 4, dont tous les éléments, sauf id, sont d'ordre 2.*

x	O_x	G_x
1	$\{1,2,3,4\}$	id
2	$\{1,2,3,4\}$	id
3	$\{1,2,3,4\}$	id
4	$\{1,2,3,4\}$	id

(4) $G = \{\mathrm{id}, (1\,2), (1\,2)(3\,4), (3\,4)\}$, *groupe d'ordre 4, dont tous les éléments, sauf id, sont d'ordre 2.*

x	O_x	G_x
1	$\{1,2\}$	$\langle(3\,4)\rangle = \{\mathrm{id}, (3\,4)\}$
2	$\{1,2\}$	$\langle(3\,4)\rangle = \{\mathrm{id}, (3\,4)\}$
3	$\{3,4\}$	$\langle(1\,2)\rangle = \{\mathrm{id}, (1\,2)\}$
4	$\{3,4\}$	$\langle(1\,2)\rangle = \{\mathrm{id}, (1\,2)\}$

(5) $G = \mathcal{A}_4$, *groupe alterné (voir (1)).*

x	O_x	G_x
1	$\{1,2,3,4\}$	$\langle(2\,3\,4)\rangle = \{\mathrm{id}, (2\,3\,4), (2\,4\,3)\}$
2	$\{1,2,3,4\}$	$\langle(1\,3\,4)\rangle = \{\mathrm{id}, (1\,3\,4), (1\,4\,3)\}$
3	$\{1,2,3,4\}$	$\langle(1\,2\,4)\rangle = \{\mathrm{id}, (1\,2\,4), (1\,4\,2)\}$
4	$\{1,2,3,4\}$	$\langle(1\,2\,3)\rangle = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$