Algèbre 2

# Examen final du 16/01/2019
# Corrigé – Barème/31,

Calculatrices et documents non autorisés. Durée 3h

**Exercice 1.** [4 point : 1 + 1 + 1 + 1] Donner, à isomorphisme près, la liste des groupes abéliens d'ordre 36.

Corrigé. Soit $G$ un groupe abélien d'ordre $36 = 2^2 \cdot 3^2$, donc $G = G_2 \times G_3$ où $G_2$ est sa composante primaire (d'ordre $2^2$) et $G_3$ est sa composante primaire (d'ordre $3^2$).

$G_2$ est isomorphe à l'un des groupes : $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$;

$G_3$ est isomorphe à l'un des groupes : $\mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9$;

Donc $G$ est isomorphe à l'un des 4 groupes

$$\begin{aligned} G &\simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \simeq \boxed{\mathbb{Z}_6 \times \mathbb{Z}_6} \\ &\simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_9 \simeq \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_9) \simeq \boxed{\mathbb{Z}_2 \times \mathbb{Z}_{18}} \\ &\simeq \mathbb{Z}_4 \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \simeq \mathbb{Z}_3 \times (\mathbb{Z}_3 \times \mathbb{Z}_4) \simeq \boxed{\mathbb{Z}_3 \times \mathbb{Z}_{12}} \\ &\simeq \mathbb{Z}_4 \times \mathbb{Z}_9 \simeq \boxed{\mathbb{Z}_{36}} \end{aligned}$$

**Exercice 2.** [3 point : (a) = 1 + (b) = 2] (a) Quel est le nombre d'éléments $x \in (\mathbb{Z}/17\mathbb{Z})^\times$ tels que $x^4 = 1$?

(b) Résoudre $x^4 = 1$ dans $(\mathbb{Z}/17\mathbb{Z})^\times$.

Corrigé. (a) Puisque 17 est un nombre premier, le groupe $\mathbb{Z}_{17}^\times$ est cyclique d'ordre 16. L'ensemble

$$H = \{x \in \mathbb{Z}_{17}^\times,\ x^4 = 1\}$$

est le seul sous-groupe de $\mathbb{Z}_{17}^\times$ d'ordre 4 : il contient donc 4 éléments.

(b) On peut déterminer les éléments de $H$, c-à-d les solutions de $x^4 = \bar{1}$, pour cela il faut déterminer un générateur de $\mathbb{Z}_{17}^\times$ (ce groupe admet en fait $\varphi(16) = 6$ générateurs) : on peut par exemple vérifier que $\bar{3}^2 = \bar{9}, \cdots, \bar{3}^8 = -\bar{1}$ et $\bar{3}^{16} = \bar{1}$ et 16 et le plus petit entier vérifiant cette dernière égalité. Donc $\bar{3}$ est un élément d'ordre 16 et c'est un générateur de $\mathbb{Z}_{17}^\times$. On en déduit que

$$\begin{aligned} H = \langle \bar{3}^{\frac{16}{4}} \rangle &= \langle \bar{3}^4 \rangle \\ &= \{\bar{3}^4 = \boxed{-\bar{4}}, (\bar{3}^4)^2 = \bar{3}^8 = \boxed{-\bar{1}}, (\bar{3}^4)^3 = \bar{3}^{12} = \boxed{\bar{4}}, (\bar{3}^4)^4 = \boxed{\bar{1}}\} \end{aligned}$$

**Exercice 3.** [3 point : $(a) = 1 + (b) = 1 + (c) = 1$] Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, ou sinon donner un argument pour justifier qu'il en existe pas :

(a) Le groupe linéaire $GL_2(\mathbb{R})$;

(b) Le groupe alterné $A_8$;

(c) Un groupe d'ordre 16 (ici il s'agit de décider si tout groupe d'ordre 16 admet un élément d'ordre 4).

Corrigé. (a) La matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est un élément d'ordre 4 de $GL_2(\mathbb{R})$

(b) On peut prendre $(1234)(5678)$ ou $(1234)(56)$.

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ est un groupe d'ordre 16 qui ne contient que des éléments d'ordre 2 (à part l'élément neutre).

**Exercice 4.** [5 point : $(a) = 2 + (b) = 0 + (c) = 1 + (d) = 2$] Considérons les deux éléments suivants du groupe symétrique $S_9$

$$\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9), \quad \sigma' = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9).$$

(a) Justifier pourquoi $\sigma$ et $\sigma'$ sont conjugués, puis exhiber une permutation $\omega \in S_9$ telle que $\sigma' = \omega\sigma\omega^{-1}$.

(b) Quel est le cardinal de la classe de conjugaisons de $\sigma$ dans $S_9$?

(c) Calculer l'ordre de $\sigma$.

(d) Calculer $\sigma^{2019}$.

Corrigé. (a) Les deux permutations $\sigma$ et $\sigma'$ sont présentées sous forme de produits de cycles disjoints d'ordres respectivement 2, 3 et 4. Les cycles de même ordre étants conjugués dans $\mathbb{S}_9$, on peut donc (par composition) conjuguer $\sigma$ et $\sigma'$ par un élément $\omega \in S_9$. Pour cela on écrit

$$\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9), \quad \sigma' = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

et prendre la permutation (parmi tant d'autres)

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 5 & 6 & 7 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$$

qui vérifie $\sigma' = \omega\sigma\omega^{-1}$.

(c) $o(\sigma) = \text{ppcm}(2, 3, 4) = 12$

(d) $2019 \equiv 15 \mod 12$, donc $\sigma^{2019} = \sigma^{15}$ et comme $15 \equiv 1 \mod 2$, $15 \equiv 0 \mod 3$ et $15 \equiv -1 \mod 4$, on a

$$\sigma^{2019} = \sigma^{15} = (1\ 2)^1(3\ 4\ 5)^0(6\ 7\ 8\ 9)^{-1} = (1\ 2)(9\ 8\ 7\ 6)$$

**Exercice 5.** [10 point : $(a) = 1 + (b) = 2 + (c) = 1 + (d) = 2 + (e) = 2 + (f) = 2$] Soit $A = \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10},\ a, b \in \mathbb{Z}\}$, sous-anneau de $\mathbb{R}$. On note $N(x)$ la norme d'un élément $x = a + \sqrt{10}b$ de $A$, donnée par $N(x) = a^2 - 10b^2$.

(a) Vérifier que pour tous $x, y \in A$, $N(xy) = N(x)N(y)$.

(b) Montrer qu'un élément $x \in A$ est inversible si et seulement si $N(x) \in \{1, -1\}$.

(c) Donner un exemple d'élément inversible $x \notin \{1, -1\}$.

(d) Montrer que pour $a \in \mathbb{Z}/10\mathbb{Z}$ la condition $a^2 \in \{-3, 3\}$ n'a pas de solution. Montrer de même que la condition $a^2 \in \{-2, 2\}$ n'a pas de solution.

(e) A l'aide de la question (d), montrer que les éléments 2, 3 et $4+\sqrt{10}$ sont irréductibles dans $A$.

(f) En déduire que $A$ n'est pas factoriel.

Corrigé. (a) Un calcul direct montre que $\forall x, y \in A$, $N(xy) = N(x)N(y)$.

(b) Si $x \in A^\times$, alors $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$. Comme $N(x)$ et $N(x^{-1})$ sont des éléments de $\mathbb{Z}$, on a $N(x) \in \{1, -1\}$. Réciproquement, si $N(x) \in \{1, -1\}$, alors en notant $\bar{x} = a - b\sqrt{10}$ pour $x = a + b\sqrt{10}$, on a $z \times \pm\bar{z} = \pm 1$. Donc $x \in A^\times$, puisque $\pm\bar{x} \in A$.

(c) On peut prendre par exemple $x = 3 + \sqrt{10}$ pour lequel $N(x) = -1$ et dont l'inverse est $-\bar{x} = -3 + \sqrt{10}$, ou $x = 19 + 6\sqrt{10}$ pour lequel $N(x) = 1$ et dont l'inverse est $\bar{x} = 19 - 6\sqrt{10}$.

(d) Il suffit de calculer les carrés des éléments de $\mathbb{Z}/10\mathbb{Z}$ et voir que les seules valeurs possibles obtenues sont $\bar{0}, \bar{4}, \bar{5}, \bar{6}, \bar{9}$. Donc ni $\pm\bar{2}$ ni $\pm\bar{3}$ ne sont des carrés dans $\mathbb{Z}/10\mathbb{Z}$.

(e) On a $N(4 + \sqrt{10}) = 6$, donc $4 + \sqrt{10}$ n'est pas inversible (d'après la question (b). Cet élément n'est pas non plus nul. Montrons qu'il ne peut être réductible, pour conclure qu'il est irréductible. Si on avait $4 + \sqrt{10} = xy$ avec $x$ et $y$ non inversibles, alors $N(x), N(y) \notin \{\pm 1\}$ et $N(x)N(y) = 6$, ce qui laisse deux possibilités $\{N(x), N(y)\} = \{2, 3\}$. Mais si $x = a + b\sqrt{10}$ alors $N(x) = a^2 - 10b^2 \equiv a^2 \mod 10$ et la question (d) montre que cela est impossible. On en déduit que $4 + \sqrt{10}$ est irréductible.

(f) On montre de même que $4 - \sqrt{10}$, 2 et 3 sont irréductibles dans $A$.

Les éléments $4 \pm \sqrt{10}$ et 2 ne sont pas associés, car sinon il existerait $u \in A^\times$ tel que $2 = u(4 \pm \sqrt{10})$. En appliquant $N$, on trouve $6u = 4$ ce qui est impossible comme égalité dans $\mathbb{Z}$. On montre de même que $4 \pm \sqrt{10}$ et 3 ne sont pas associés.

Mais $2 \times 3 = 6 = (4+\sqrt{10})(4-\sqrt{10})$, ce qui veut dire que 6 admet deux décompositions distinctes (non associées). Ceci montre que l'anneau $A$ n'est pas factoriel.

**Exercice 6.** [6 point : $(1) = 1 + (2)(a) = 2 + (2)(b) = 1 + (2)(c) = 1 + 0,5 + 0,25 + 0,25$]
(1) Déterminer les polynômes irréductibles de degré 2 dans $\mathbb{Z}/2\mathbb{Z}[X]$.

(2) On considère le polynôme $P(X) = 2019X^5 + 2018X^4 + 2016X^3 + 2015X^2 + 2014X + 2013 \in \mathbb{Z}[X]$.

(a) Soit $\bar{P}$ la réduction du polynôme $P$ modulo 2. Montrer que $\bar{P}$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

(b) Soit $\langle \bar{P} \rangle$ l'idéal $\mathbb{Z}/2\mathbb{Z}[X]$ de engendré par $\bar{P}$. Montrer que $\mathbb{Z}/2\mathbb{Z}[X]/\langle \bar{P} \rangle$ est un corps.

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

Corrigé. (1) Il n'y a qu'un seul polynôme irréductible de degré 2 dans $\mathbb{Z}/2\mathbb{Z}$, à savoir $X^2 + X + \bar{1}$.

(2) (a) La réduction de $P$ modulo 2 est $\bar{P}(X) = X^5 + X^2 + \bar{1} \in \mathbb{Z}/2\mathbb{Z}[X]$. Si ce polynôme était réductible alors il doit avoir un facteur irreducible de degré 1 et donc une racine dans $\mathbb{Z}/2\mathbb{Z}[X]$ ou un facteur irréductible de degré 2 qui est forcement $X^2 + X + \bar{1}$. On voit immédiatement que $\bar{P}$ n'a pas de racine de $\mathbb{Z}/2\mathbb{Z}[X]$. D'autre part (par division euclidienne) on a $X^5 + X^2 + \bar{1} = (X^2 + X + \bar{1})(X^3 + X^2) + \bar{1}$, ce qui montre que $X^5 + X^2 + \bar{1}$ n'est pas divisible par $X^2 + X + \bar{1}$. En conclusion $\bar{P}(X) = X^5 + X^2 + \bar{1}$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

(b) Comme $\bar{P}$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$, l'idéal $\langle \bar{P} \rangle$ est maximal et par conséquent l'anneau quotient $\mathbb{Z}/2\mathbb{Z}[X]/\langle \bar{P} \rangle$ est un corps.

(c) Comme $\bar{P}$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$, le polynôme $P$ est irréductible dans $\mathbb{Q}[X]$. Puisque $P$ est primitif, il est irréductible irréductible dans $\mathbb{Z}[X]$. Les seuls polynômes irréductibles dans $\mathbb{R}[X]$ sont ceux de degré 1 ou de degré 2 à discriminant négatif, et les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. On en déduit que $P$ n'est irréductible ni dans $\mathbb{R}[X]$ ni dans $\mathbb{C}[X]$.