Algèbre 2

Examen du 17/01/2017 – Corrigé

Calculatrices et documents non autorisés. Durée 3h

Exercice 1. Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre 180.

Solution. Soit G un groupe abélien d'ordre $180 = 2^2 \cdot 3^2 \cdot 5$. Sa décomposition primaire est donnée par $G = G_2 \times G_3 \times G_5$.

$\rightarrow$ La composante primaire G_2 est un groupe abélien d'ordre 2^2, donc G_2 est isomorphe l'un des groupes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ ou } \mathbb{Z}/2^2\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$$

$\rightarrow$ La composante primaire G_3 est un groupe abélien d'ordre 3^2, donc G_3 est isomorphe l'un des groupes

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ ou } \mathbb{Z}/3^2\mathbb{Z} = \mathbb{Z}/9\mathbb{Z}$$

$\rightarrow$ La composante primaire G_5 est un groupe cyclique d'ordre 5, donc isomoprohe à

$$\mathbb{Z}/5\mathbb{Z}$$

Il y a donc, à isomorphisme près, $2 \times 2 \times 1 = 4$ groupes abéliens d'ordre 180 qui sont

$$\begin{aligned}
(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} &= (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \\
&\simeq \boxed{\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}} \\
(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &= (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \\
&\simeq \boxed{\mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}} \\
\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} &= (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z} \\
&\simeq \boxed{\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}} \\
\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\simeq \boxed{\mathbb{Z}/180\mathbb{Z}}
\end{aligned}$$

Exercice 2. On considère le groupe $(\mathbb{Z}/13\mathbb{Z})^*$ des éléments inversibles de l'anneau $\mathbb{Z}/13\mathbb{Z}$.

(a) Le groupe $(\mathbb{Z}/13\mathbb{Z})^*$ est-il cyclique? Quel est son ordre?

(b) Combien le groupe $(\mathbb{Z}/13\mathbb{Z})^*$ admet-il de sous-groupes d'ordre 2 et de sous-groupes d'ordre 6? Ces sous-groupes sont-ils cycliques?

(c) Déterminer ces sous-groupes et leurs générateurs.

(d) Montrer que dans $\mathbb{Z}/13\mathbb{Z}$ les racines du polynôme $P = X^4 + X^2 + \bar{1}$ sont toutes des carrés. Déterminer une factorisation de P dans $\mathbb{Z}/13\mathbb{Z}$.

Solution. (a) Puisque 13 *est premier, le groupe* $(\mathbb{Z}/13\mathbb{Z})^\times$ *est un groupe cyclique d'ordre 12,*

$$\begin{aligned}(\mathbb{Z}/13\mathbb{Z})^\times = \mathbb{Z}/13\mathbb{Z} \setminus \{\bar{0}\} &= \{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\overline{10},\overline{11},\overline{12}\}\\ &= \{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},-\bar{6},-\bar{5},-\bar{4},-\bar{3},-\bar{2},-\bar{1}\}\\ &= \{\pm\bar{1},\pm\bar{2},\pm\bar{3},\pm\bar{4},\pm\bar{5},\pm\bar{6}\}\end{aligned}$$

(b) Puisque le groupe $(\mathbb{Z}/13\mathbb{Z})^\times$ *est cyclique et que 2 divise son ordre, alors il admet un unique sous-groupe* H_2 *d'ordre 2 et qui est cyclique.*
De même $(\mathbb{Z}/13\mathbb{Z})^\times$ *admet un unique sous-groupe cyclique* H_6 *d'ordre 6.*

(c) Par unicité $H_2 = \{\bar{1}\ -\bar{1}\}$. *De plus* $-\bar{1}$ *est son unique générateur (*H_2 *admet* $\varphi(2) = 1$ *générateur).*
D'autre part,

$$\begin{aligned}H_6 &= \{x \in (\mathbb{Z}/13\mathbb{Z})^\times \ :\ x^6 = \bar{1}\}\\ &= \{y \in (\mathbb{Z}/13\mathbb{Z})^\times \ :\ y = x^2,\ x \in (\mathbb{Z}/13\mathbb{Z})^\times\}\end{aligned}$$

Mais $(\pm\bar{1})^2 = \bar{1}$, $(\pm\bar{2})^2 = \bar{4}$, $(\pm\bar{3})^2 = \bar{9} = -\bar{4}$, $(\pm\bar{4})^2 = \overline{16} = \bar{3}$, $(\pm\bar{5})^2 = \overline{25} = \overline{12} = -\bar{1}$, $(\pm\bar{6})^2 = \overline{36} = \overline{10} = -\bar{3}$,
D'où

$$H_6 = \{\pm 1, \pm 3, \pm 4\}.$$

Le sous-groupe H_6 *admet* $\varphi(6) = 2$ *générateurs. Ce sont les éléments d'ordre 6 dans* H_6. *Déterminons ces générateurs.*
Il faut exclure $\bar{1}$, *car c'est le neutre, et* $-\bar{1}$, *car cet élément est d'ordre 2. Par ailleurs,*
$\bar{3}^2 = \bar{9}$ *et* $\bar{3}^3 = \overline{27} = \bar{1}$, *donc* $o(\bar{3}) = 3$.
$\bar{4}^2 = \bar{3}$, $\bar{4}^3 = \overline{12} = -\bar{1}$, $\bar{4}^4 = -\bar{4}$, $\bar{4}^5 = -\overline{16} = -\bar{3}$ *et* $\bar{4}^6 = -\overline{12} = \bar{1}$, *donc* $o(\bar{4}) = 6$.
On montre de même que $o(-\bar{4}) = 3$ *et que* $o(-\bar{3}) = 6$.
Ainsi les générateurs [1] *de* H_6 *sont* $\bar{4}$ *et* $-\bar{3} = \overline{10}$.

(d) Soit $x \in \mathbb{Z}/13\mathbb{Z}$, *on a* $x \in H_6$ *ssi* $x^6 = \bar{1}$ *ssi* $x^6 - \bar{1} = \bar{0}$ *ssi* $(x^2-\bar{1})(x^4+x^2+\bar{1}) = \bar{0}$ *ssi* $x^2 - \bar{1} = \bar{0}$ *ou* $x^4 + x^2 + \bar{1} = \bar{0}$ *car* $\mathbb{Z}/13\mathbb{Z}$ *est intègre puisque 13 est premier. On en déduit que les solutions de* $x^4 + x^2 + \bar{1} = \bar{0}$ *sont les éléments de* H_6 *qui sont différents de* $\pm\bar{1}$ *(les racines de* $x^2 - \bar{1} = \bar{0}$*), et donc ces racines sont toutes des carrés car appartiennent à* H_6. *Par conséquent, les racines du polynôme* $X^4 + X^2 + \bar{1}$ *dans* $\mathbb{Z}/13\mathbb{Z}$ *sont* $\pm\bar{3}$ *et* $\pm\bar{4}$ *et* $X^4 + X^2 + \bar{1} = (X - \bar{3})(X + \bar{3})(X - \bar{4})(X + \bar{4})$.

Exercice 3. Soit $n \in \mathbb{N}^*$. On note $\mathcal{A}_n$ le groupe alterné, c-à-d. le sous-groupe du groupe symétrique $\mathcal{S}_n$ formé des permutations paires.

[1] En fait une fois le premier générateur $\bar{4}$ est trouvé, le deuxième générateur est $\bar{4}^k$ où $k \wedge 6 = 1$ et $k \neq 1$, c-à-d, $k = 5$ et par conséquent ce générateur est $\bar{4}^5 = -\bar{3}$.

(a) Montrer que $\mathcal{A}_3$ est un groupe cyclique et déterminer ses générateurs.

(b) Montrer que si $f : \mathcal{S}_3 \to \mathcal{A}_3$ est un morphisme de groupes, alors $\forall \gamma \in \mathcal{S}_3$, $f(\gamma) = \mathrm{Id}_{\mathcal{S}_3}$.

(c) Soit G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n (donc d'indice 2). Montrer que

$$\forall g \in G, \quad g^2 \in H$$

(d) En déduire que $\mathcal{A}_3$ (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.

Solution. (a) $\mathcal{A}_n$ *est un groupe d'ordre* $\frac{3!}{2} = 3$, *donc il est cyclique et admet* $\varphi(3) = 2$ *générateurs qui sont les 3-cycles* $\sigma = (1,2,3)$ *et* $\sigma^2 = (1,3,2)$.

(b) Soit $f : \mathcal{S}_3 \to \mathcal{A}_3$ *un morphisme de groupes. Si* $\tau \in \mathcal{S}_3$ *est une transposition alors* $f(\tau)^2 = f(\tau^2) = f(\mathrm{Id}_{\mathcal{S}_3}) = \mathrm{Id}_{\mathcal{A}_3} = \mathrm{Id}_{\mathcal{S}_3}$ *(car une transposition est d'ordre 2). On en déduit que* $f(\tau)$ *est un élément d'ordre 1 ou 2 dans* $\mathcal{A}_3$. *Or* $\mathcal{A}_3 = \langle \sigma \rangle = \{\mathrm{Id}_{\mathcal{S}_3}, \sigma, \sigma^2\}$ *et aucun de ces éléments n'est d'ordre 2, donc forcément* $f(\tau)$ *est d'ordre 1 et par suite* $f(\tau) = \mathrm{Id}_{\mathcal{S}_3}$. *Comme* $\mathcal{S}_3$ *est engendré par les transpositions, on déduit que pour tout élément* $\gamma \in \mathcal{S}_3$, $f(\gamma) = \mathrm{Id}_{\mathcal{S}_3}$, *ce qui veut dire que* f *est l'application constante* $\mathrm{Id}_{\mathcal{S}_3}$. *Par conséquent, il n'existe pas de morphisme de groupes surjectif de* $\mathcal{S}_3$ *sur* $\mathcal{A}_3$.

(c) Supposons $|G| = 2n$ *et* $|H| = n$, *et soit* $g \in G$. *Si* $g \in H$, *alors* $g^2 \in H$ *(car* H *est un sous-groupe de* G*). Supposons maintenant que* $g \notin H$, *alors* $gH \neq H$. *Or* $|G/H| = 2$, *donc* $G/H = \{gH, H\}$ *et* $G = gH \cup H$ *(les classes d'équivalences modulo* H *forment une partition de* G*). Comme* $g^2 \in G$, *alors soit* $g^2 \in gH$, *soit* $g^2 \in H$. *Mais si* $g^2 \in gH$, *alors il existe* $h \in H$ *tel que* $g^2 = gh$, *puis* $g = h \in H$ *ce qui contredit l'hypothèse* $g \notin H$. *Par conséquent,* $g^2 \in H$.

(d) Si H *est un sous-groupe d'ordre 6 de* $\mathcal{A}_3$ *qui est d'ordre 12, alors d'après (c)*

$$\forall \gamma \in \mathcal{A}_3, \quad \gamma^2 \in H.$$

Mais si $\gamma \in \mathcal{A}_3$ *est un 3-cycle, il est d'ordre 3 et* $\gamma^3 = \mathrm{Id}_{\mathcal{S}_3}$, *donc* $\gamma^{-1} = \gamma^2 \in H$. *On en déduit que forcément* $\gamma \in H$. *Ce qui veut dire que* H *contient tout les 3-cycles de* $\mathcal{A}_3$ *et donc contient* $\mathcal{A}_3$ *car* $\mathcal{A}_3$ *est engendré par les 3-cycles, c-à-d.* $\mathcal{A}_3 \subset H$ *ce qui est absurde. Par conséquent* $\mathcal{A}_3$ *n'admet pas de sous-groupes d'ordre 6.*

Exercice 4. On considère l'ensemble $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5};\ \ a, b \in \mathbb{Z}\}$.

(a) Montrer que $\mathbb{Z}[\sqrt{-5}]$ est un sous-anneau de $\mathbb{C}$.

(b) On pose pour tout $z \in \mathbb{Z}[\sqrt{-5}]$, $\theta(z) = z\bar{z} = |z|^2$. On note $(\mathbb{Z}[\sqrt{-5}])^*$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{-5}]$.

Montrer que $(\mathbb{Z}[\sqrt{-5}])^* = \{z \in \mathbb{Z}[\sqrt{-5}];\ \theta(z) = 1\}$, déterminer alors $(\mathbb{Z}[\sqrt{-5}])^*$.

(c) Montrer que 2, 3, 31, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$.

(d) Montrer que $1 + i\sqrt{5}$ n'est associé ni à 2 ni à 3 dans l'anneau $\mathbb{Z}[\sqrt{-5}]$.

(e) En déduire que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Solution. (a) Il est facile de montrer que $\mathbb{Z}[\sqrt{-5}]$ *est un sous-anneau de* $\mathbb{C}$.

(b) Soit $z \in (\mathbb{Z}[\sqrt{-5}])^\star$, *alors il existe* $w \in \mathbb{Z}[\sqrt{-5}]$ *tel que* $zw = 1$. *Donc* $\theta(z)\theta(w) = \theta(zw) = 1$. *De cette égalité entre entiers naturels on déduit que* $\theta(z) = 1$. *Réciproquement, soit* $z \in \mathbb{Z}[\sqrt{-5}]$ *tel que* $\theta(z) = 1$ *c'est-à-dire* $z\bar{z} = 1$. *Puisque*

l'anneau est stable par la conjugaison complexe, $\bar{z} \in \mathbb{Z}[\sqrt{-5}]$ et donc z est inversible d'inverse $\bar{z}$.

Soit $z = a + ib\sqrt{5} \in \mathbb{Z}[\sqrt{-5}]$. Alors

$$z \in (\mathbb{Z}[\sqrt{-5}])^\star \iff a^2 + 5b^2 = 1 \iff b = 0, a = \pm 1$$

On en déduit que $(\mathbb{Z}[\sqrt{-5}])^\star = \{\pm 1\}$.

(c) $2 \notin (\mathbb{Z}[\sqrt{-5}])^\star$. De plus, si $2 = zw$ avec $z, w \in \mathbb{Z}[\sqrt{-5}]$, alors nécessairement $4 = \theta(z)\theta(w)$ (avec $\theta(z), \theta(w) \in \mathbb{N}$). Or si $\theta(z) = \theta(w) = 2$, alors on aurait $a^2 + 5b^2 = 2$ (avec $z = a + ib\sqrt{5}$). Mais dans cette égalité, nécessairement $b = 0$ (car sinon $a^2 + 5b^2 \geq 5$), donc $a^2 = 2$ ce qui est impossible dans $\mathbb{Z}$. On en déduit que $\theta(z) = 1$ et $\theta(w) = 4$ ou inversement. Ce qui veut dire $z \in (\mathbb{Z}[\sqrt{-5}])^\star$ ou $w \in (\mathbb{Z}[\sqrt{-5}])^\star$. Par conséquent 2 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$.

On montre de même que 3 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$

Montrons que 31 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$. On a $31 \notin (\mathbb{Z}[\sqrt{-5}])^\star$. De plus, si $31 = zw$ avec $z, w \in \mathbb{Z}[\sqrt{-5}]$, alors nécessairement $31^2 = \theta(z)\theta(w)$. Les seules possibilités de cette égalité sont $\theta(z) = \theta(w) = 31$ ou $\theta(z) = 1$ et $\theta(w) = 31^2$ ou inversement. Or si $\theta(z) = \theta(w) = 31$, alors on aurait $a^2 + 5b^2 = 31$ (avec $z = a + ib\sqrt{5}$). Dans cette équation, nécessairement $b \in \{-2, -1, 0, 1, 2\}$ et dans chaque cas on arrive à une contradiction. Par conséquent, on a nécessairement $\theta(z) = 1$ et $\theta(w) = 31^2$ (ou inversement) et cela entraîne que 31 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$.

On montre de même que $1 \pm i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$.

(d) Les éléments inversibles étant ± 1, l'élément $1 + i\sqrt{5}$ n'est associé ni à 2 ni à 3.

(e) On a $6 = 2 \times 3$ et $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Donc dans $\mathbb{Z}[\sqrt{-5}]$ l'élément 6 admet deux décompositions <u>différentes</u> en produit de facteurs irréductibles car $1+i\sqrt{5}$ n'est associé ni à 2 bi à 3. On en déduit que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Exercice 5. (a) Déterminer l'ensemble de solutions de l'équation $x^4 + \bar{2} = \bar{0}$ dans $\mathbb{Z}/5\mathbb{Z}$.

(b) Montrer que le polynôme $X^4 + \bar{2} \in \mathbb{Z}/5\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$.

(c) On considère le polynôme $P(X) = X^4 + 15X^3 + 7$. Montrer qu'il est irréductible dans $\mathbb{Z}[X]$.

Solution. (a) Les éléments de $\mathbb{Z}/5\mathbb{Z}$ sont $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$ et leur puissance 4^{eme} sont respectivement $\bar{0}$, $\bar{1}$, $\bar{1}$, $\bar{1}$, $\bar{1}$. Il en résulte que l'équation $x^4 + \bar{2} = \bar{0}$ n'a pas de solution dans $\mathbb{Z}/5\mathbb{Z}$.

(b) D'après (a) le polynôme $X^4 + \bar{2}$ n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$ et donc n'est pas divisible par un polynôme de degré 1 (ni par un polynôme de degré 3). S'il est réductible, il doit être produit de deux polynômes de degré 2,

$$X^4 + \bar{2} = (X^2 + aX + b)(X^2 + cX + d), \quad a, b, c, d \in \mathbb{Z}/5\mathbb{Z}$$

On peut en effet se ramener à des polynômes unitaires en divisant l'un des facteurs et en multipliant l'autre par un scalaire non nul (donc inversible) convenable. On a alors $a + c = \bar{0}$, $ac + b + d = \bar{0}$ et $bd = \bar{2}$, donc $b + d = a^2$. Mais les seuls carrés *de* $\mathbb{Z}/5\mathbb{Z}$ *sont* $\bar{0}$, $\bar{1}$ *et* $-\bar{1}$, *ce qui implique que* $-b^2 = \bar{2}$ *ou que* $b(\bar{1} - b) = \bar{2}$ *ou que* $b(\bar{1} + b) = -\bar{2}$. *En essayant toutes les valeurs possibles pour* b, *on voit qu'aucune de ces égalités ne peut avoir lieu. Par conséquent le polynôme* $X^4 + \bar{2}$ *est irréductible dans* $\mathbb{Z}/5\mathbb{Z}[X]$.

(c) La réduction du polynôme P *modulo le nombre premier* 5 *est* $\bar{P}(X) = X^4 + \bar{2}$, *qui est irréductible dans* $\mathbb{Z}/5\mathbb{Z}[X]$ *d'après (b). On en déduit que* P *est irréductible dans* $\mathbb{Q}[X]$ *et comme* P *est primitif (car unitaire), il est donc irréductible dans* $\mathbb{Z}[X]$.