Algèbre 2

Partiel CCI3 – Corrigé

14 décembre 2021 – durée 3h

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

Corrigé l'exercice 1. Soit G un groupe abélien d'ordre $180 = 2^2 \cdot 3^2 \cdot 5$. Sa décomposition primaire est donnée par $G = G_2 \times G_3 \times G_5$.

$\to$ La composante primaire G_2 est un groupe abélien d'ordre 2^2, donc G_2 est isomorphe à l'un des groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2^2\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$

$\to$ La composante primaire G_3 est un groupe abélien d'ordre 3^2, donc G_3 est isomorphe à l'un des groupes $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/3^2\mathbb{Z} = \mathbb{Z}/9\mathbb{Z}$

$\to$ La composante primaire G_5 est un groupe cyclique d'ordre 5, donc isomorphe à $\mathbb{Z}/5\mathbb{Z}$

Au total, à isomorphisme près, il y a $2 \times 2 \times 1 = 4$ groupes abéliens d'ordre 180 qui sont :

$$\begin{array}{rcl}
\to & & (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} \\
& = & (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \\
& \simeq & \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \text{ d'invariants } (6, 30) \\
\to & & (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
& = & (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \\
& \simeq & \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ d'invariants } (2, 90) \\
\to & & \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} \\
& = & (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z} \\
& \simeq & \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ d'invariants } (3, 60) \\
\to & & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
& \simeq & \mathbb{Z}/180\mathbb{Z} \text{ d'invariant } (180)
\end{array}$$

Exercice 2. Soit $\mathbb{Z}_7 := \mathbb{Z}/7\mathbb{Z}$ l'anneau des classes d'équivalences modulo 7 et $(\mathbb{Z}_7)^\times$ l'ensemble de ses éléments inversibles (pour le produit). Soit $\mathbb{U}_6$ le groupe cyclique des racines 6-ièmes de l'unité.

(1) Déterminer tous les générateurs de $\mathbb{U}_6$.

(2) Dire pourquoi $(\mathbb{Z}_7)^\times$ est un groupe cyclique et déterminer son ordre. Donner ses éléments explicitement.

(3) (a) Montrer que $\bar{3}$ est un générateur de $(\mathbb{Z}_7)^\times$.

(b) Déterminer alors les autres générateurs.

(4) Soit f l'application définie, pour tout $k \in \mathbb{Z}$, par

$$f(\bar{3}^k) = \mathrm{e}^{\frac{ik\pi}{3}}$$

Montrer que f est bien définie.

(5) (a) Montrer que f est un morphisme de groupes multiplicatifs de $(\mathbb{Z}_7)^\times$ vers $\mathbb{U}_6$.

(b) Ce morphisme est-il surjectif ?

(6) Déterminer le noyau de f.

(7) En déduire que les groupes $(\mathbb{Z}_7)^\times$ et $\mathbb{U}_6$ sont isomorphes.

Corrigé l'exercice 2. (1) $\mathbb{U}_6$ est cyclique d'ordre 6 et engendré par $\xi = e^{2i\pi/6} = e^{i\pi/3}$. Ce groupe admet $\varphi(6) = \varphi(2)\varphi(3) = 2$ générateurs, qui sont de la forme ξ^k avec $k \leq 5$ et $k \wedge 9 = 1$. On trouve alors $\xi^1 = \xi = e^{i\pi/3}$ et $\xi^5 = e^{5i\pi/3}$.

(2) Comme 7 est premier, $(\mathbb{Z}_7)^\times$ est un groupe cyclique, d'ordre 6 et $(\mathbb{Z}_7)^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

(3) (a) On a

$$\begin{array}{rcl}
\bar{3}^0 & = & \bar{1} \\
\bar{3}^1 & = & \bar{3} \\
\bar{3}^2 & = & \bar{9} = \bar{2} \\
\bar{3}^3 & = & \bar{3}^2 \times \bar{3} = \bar{2} \times \bar{3} = \bar{6} \\
\bar{3}^4 & = & \bar{3}^2 \times \bar{3}^2 = \bar{2} \times \bar{2} = \bar{4} \\
\bar{3}^5 & = & \bar{3}^4 \times \bar{3} = \bar{4} \times \bar{3} = \overline{12} = \bar{5} \\
\bar{3}^6 & = & \bar{3}^5 \times \bar{3} = \bar{5} \times \bar{3} = \overline{15} = \bar{1}
\end{array}$$

La dernière égalité peut aussi se déduire du petit théorème de Fermat. Il s'ensuit que $\bar{3}$ est d'ordre 6 (et que $(\mathbb{Z}_7)^\times = \{\bar{3}^k : 0 \leq k \leq 5\}$) ce qui implique que le groupe $(\mathbb{Z}_7)^\times$ est engendré par $\bar{3}$.

(b) Puisque l'ordre du groupe cyclique $(\mathbb{Z}_7)^\times$ est égal à 6 et que $\bar{3}$ en est un générateur, on en déduit que tous les générateurs sont de la forme $\bar{3}^k$ avec $k \leq 5$ et $k \wedge 6 = 1$. On trouve alors $\bar{3}^1 = \bar{3}$ et $\bar{3}^5 = \bar{4}$.

(4) Il faut vérifier que pour tout $k, h \in \mathbb{Z}$, si $\bar{3}^k = \bar{3}^k$, alors $f(\bar{3}^k) = f(\bar{3}^h)$. Or,

$$\begin{array}{rcll}
\bar{3}^k = \bar{3}^k & \iff & \bar{3}^{k-h} = \bar{1} & \\
& \iff & 6|(k-h) & \text{car } o(\bar{3}) = 6 \\
& \iff & \exists \ell \in \mathbb{Z},\ h = k + 6\ell &
\end{array}$$

Donc

$$\begin{aligned} f(\bar{3}^h) &= f(\bar{3}^{k+6\ell}) = \mathrm{e}^{\frac{i(k+6\ell)\pi}{3}} \\ &= \mathrm{e}^{\frac{ik\pi}{3}}\mathrm{e}^{2i\ell\pi} \\ &= \mathrm{e}^{\frac{ik\pi}{3}} = f(\bar{3}^k) \end{aligned}$$

Par conséquent, l'application f est bien définie.

(5) D'abord, pour tout entier k, $1 \leq k \leq 5$, on a $f(\bar{3}^k) \in \mathbb{U}_6$, car $\left(\mathrm{e}^{\frac{ik\pi}{3}}\right)^6 = 1$. Donc $f\colon (\mathbb{Z}_7)^\times \to \mathbb{U}_6$.

Soient $a, b \in (\mathbb{Z}_7)^\times$, alors il existe un unique couple d'entier (k, j) avec $0 \leq k, j \leq 5$ et tels que $a = \bar{3}^k$ et $b = \bar{3}^j$. On a

$$\begin{aligned} f(ab) &= f(\bar{3}^k\bar{3}^j) = f(\bar{3}^{k+j}) \\ &= \mathrm{e}^{\frac{i(k+j)\pi}{3}} = \mathrm{e}^{\frac{ik\pi}{3}}\mathrm{e}^{\frac{ij\pi}{3}} \\ &= f(\bar{3}^k)f(\bar{3}^j) = f(a)f(b) \end{aligned}$$

Il s'ensuit que f est un morphisme de groupes.

Exercice 3. Soit G un groupe abélien fini, soient H et K deux sous-groupes d'ordres respectifs r et s. Soit l'ensemble $HK = \{hk : h \in H,\ k \in K\}$.

(1) Montrer que HK est un sous-groupe de G ayant au plus rs éléments.

(2) On suppose r et s premiers entre eux. Montrer que HK a exactement rs éléments dans ce cas.

(3) On suppose maintenant que r et s sont deux nombres premiers distincts. Montrer qu'alors HK est un groupe cyclique.

Corrigé l'exercice 3. (1) On a

$HK \subset G$,

$HK \neq \emptyset$, car $e \in HK$,

Pour tout $x_1, x_2 \in HK$, il existe $(h_1, h_2) \in H^2$ et $(k_1, k_2) \in K^2$ tels que $x_1 = h_1k_1$ et $x_2 = h_2k_2$. Comme G est abélien, on a

$$x_1x_2^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = (h_1h_2^{-1})(k_1k_2^{-1}) \in HK$$

Il s'ensuit alors que HK est un sous-groupe de G.

Comme G est abélien, l'application

$$\begin{array}{rccc} f\colon & H \times K & \to & HK \\ & (h,k) & \mapsto & hk \end{array}$$

est clairement un morphisme de groupe. De plus, il est surjectif par construction. D'après le théorème de l'isomorphisme, les deux groupes $(H\times K)/\operatorname{Ker} f$ et KH sont isomorphe. Donc

$$|HK| = \frac{|H \times K|}{|\operatorname{Ker} f|}$$

Or $|H \times K| = |H|\ |K| = rs$ et $|\operatorname{Ker} f| \geq 1$, donc $|HK| = \frac{|H\times K|}{|\operatorname{Ker} f|} \leq rs$ On peut montrer[1] que $\operatorname{Ker} f \simeq H \cap K$ et ce sous-groupe n'est pas nécessairement réduit à $\{e\}$.

(3) Si $r \wedge s = 1$, alors $H \cap K = \{e\}$ et $\operatorname{Ker} f = \{(e, e)\}$. D'après la question précédente, $HK \simeq H \times K$ et donc $|HK| = rs$.

(4) On suppose que r et s sont premiers et distincts. Donc les deux sous-groupes H et K sont cycliques et leur produit cartésien $H \times K$ est cyclique. Comme $HK \simeq H \times K$, le groupe HK est aussi cyclique.

Exercice 4. Considérons les deux éléments suivants du groupe symétrique $\mathcal{S}_9$

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 6 & 1 & 7 & 8 & 9 & 2 & 5 \end{pmatrix}, \\ \sigma' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 9 & 5 & 2 & 8 & 3 & 6 & 1 \end{pmatrix}. \end{aligned}$$

(1) Décomposer les permutations σ et σ' en produit de cycles disjoints.

(2) Justifier pourquoi σ et σ' sont conjuguées dans $\mathcal{S}_9$, puis exhiber une permutation $\gamma \in \mathcal{S}_9$ telle que $\sigma' = \gamma \circ \sigma \circ \gamma^{-1}$.

(3) Determiner le nombre des permutation $\gamma \in \mathcal{S}_9$ qui conjuguent σ et σ'.

(4) Calculer l'ordre et la signature de σ.

(5) Calculer σ^{2021}.

Corrigé l'exercice 4. (1) On a

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

(2) Deux cycles de même longeurs sont conjugués. On peut conjuger

1. $\operatorname{Ker}(f) = \{(k, k^{-1}) : k \in H \cap K\} \simeq H \cap K$

$(1,4)$ et $(6,8)$,
$(5,7,9)$ et $(2,4,5)$,
$(2,3,6,8)$ et $(1,7,3,9)$.

On en déduit par compositions σ et σ' sont conjugués dans $\mathcal{S}_9$. On peut prendre par exemple comme permutation qui conjugue σ et σ' :

$$\begin{aligned}\gamma &= \begin{pmatrix}1&4&5&7&9&2&3&6&8\\6&8&2&4&5&1&7&3&9\end{pmatrix}\\ &= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&1&7&8&2&3&4&9&5\end{pmatrix}\end{aligned}$$

(3) Il y a :
2 façons de conjuguer $(1,4)$ et $(6,8)$
3 façons de conjuguer $(5,7,9)$ et $(2,4,5)$
4 façons de conjuguer $(2,3,6,8)$ et $(1,7,3,9)$
Donc au total, il y a $2\times3\times4=24$ permutations possibles qui conjuguent σ et σ'.

(4) On a $o(1,4)=2$, $o(5,7,9)=3$ et $o(2,3,6,8)=4$, donc $o(\sigma)=ppcm(2,3,4)=12$.
On a $\varepsilon(\sigma)=\varepsilon(1,4)\varepsilon(5,7,9)\varepsilon(2,3,6,8)=(-1)^{2-1}\times(-1)^{3-1}\times(-1)^{4-1}=1$.

(5) Comme les cycles $(1,4)$, $(5,7,9)$ et $o(2,3,6,8)$ sont deux à deux disjoints,

$$\sigma^{2021}=(1,4)^{2021}(5,7,9)^{2021}(2,3,6,8)^{2021}$$

On a
$2021\equiv1[2]$, donc $(1,4)^{2021}=(1,4)$;
$2021\equiv3[3]$, donc $(5,7,9)^{2021}=(5,7,9)^2=(5,7,9)^{-1}=(5,9,7)$,
$2021\equiv1[4]$, donc $(2,3,6,8)^{2021}=(2,3,6,8)$.
Ainsi

$$\sigma^{2021}=(1,4)(5,9,7)(2,3,6,8).$$

Exercice 5. On considère l'ensemble $\mathbb{Z}[\sqrt{-5}]=\{a+ib\sqrt{5}\,:\,a,b\in\mathbb{Z}\}$.
(1) Montrer que $\mathbb{Z}[\sqrt{-5}]$ est un sous-anneau de $\mathbb{C}$.
$\mathbb{Z}[\sqrt{-5}]$ est-il commutatif ? unitaire ? intègre ?
(2) On pose, pour tout $z\in\mathbb{Z}[\sqrt{-5}]$, $\theta(z)=z\bar{z}=|z|^2$. On désigne par $(\mathbb{Z}[\sqrt{-5}])^\times$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{-5}]$.
(a) Montrer que $(\mathbb{Z}[\sqrt{-5}])^\times=\{z\in\mathbb{Z}[\sqrt{-5}]\,:\,\theta(z)=1\}$.
(b) Déterminer alors $(\mathbb{Z}[\sqrt{-5}])^\times$.
(3) Montrer que 2, 3, 31, $1+i\sqrt{5}$ et $1-i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$.
(4) Montrer que $1+i\sqrt{5}$ n'est associé ni à 2, ni à 3 dans l'anneau $\mathbb{Z}[\sqrt{-5}]$.
(5) En déduire que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Corrigé l'exercice 5. (1) Il est facile de montrer que $\mathbb{Z}[\sqrt{-5}]$ est un sous-anneau de $\mathbb{C}$. Il est commutatif, unitaire et intègre.
(2) (a) Soit $z\in(\mathbb{Z}[\sqrt{-5}])^\times$, alors il existe $w\in\mathbb{Z}[\sqrt{-5}]$ tel que $zw=1$. On a $\theta(z)\theta(w)=\theta(zw)=1$. 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 $\mathbb{Z}[\sqrt{-5}]$ est stable par la conjugaison complexe, $\bar{z}\in\mathbb{Z}[\sqrt{-5}]$ et donc z est inversible d'inverse $\bar{z}$. Ainsi $z\in(\mathbb{Z}[\sqrt{-5}])^\times$.
(b) Soit $z=a+ib\sqrt{5}\in\mathbb{Z}[\sqrt{-5}]$. Alors

$$z\in(\mathbb{Z}[\sqrt{-5}])^\times \iff a^2+5b^2=1 \iff b=0, a=\pm1$$

On en déduit que $(\mathbb{Z}[\sqrt{-5}])^\times=\{\pm1\}$.
(3) $2\notin(\mathbb{Z}[\sqrt{-5}])^\times$. De plus, si $2=zw$ avec $z,w\in\mathbb{Z}[\sqrt{-5}]$, alors nécessairement $4=\theta(2)=\theta(z)\theta(w)$ (avec $\theta(z),\theta(w)\in\mathbb{N}$). Or si $\theta(z)=\theta(w)=2$, on aurait, en posant $z=a+ib\sqrt{5}$, $a^2+5b^2=2$. Mais dans cette égalité, nécessairement $b=0$ (car sinon $a^2+5b^2\geq5$), 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 $z\in(\mathbb{Z}[\sqrt{-5}])^\times$ ou $w\in(\mathbb{Z}[\sqrt{-5}])^\times$. Par conséquent 2 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$.
On montre de même que 3, $1+\pm i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$. Pour 31, on raisonne aussi de la même façon pour aboutir à l'équation $a^2+5b^2=31$. Dans cette équation, nécessairement $b\in\{-2,-1,0,1,2\}$ et dans chaque cas on arrive à une contradiction.
(4) Les éléments inversibles étant ±1, l'élément $1+i\sqrt{5}$ n'est associé ni à 2, ni à 3.
(5) On a $6\in\mathbb{Z}[\sqrt{-5}]$, $6=2\times3$ et $6=(1+i\sqrt{5})(1-i\sqrt{5})$. Aucun facteur irréductible de la première décomposition n'est associé à un facteur irréductible de la seconde décomposition.On en déduit que l'anneau $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.