Algèbre 2, L3
Partiel du 08/11/2022 à 9h
Documents/calculatrices interdits
Durée : 2h

Exercice 1. On rappelle que $\mathbb{C}^*$ muni de la multiplication est un groupe. On note $\mathbb{U} \subset \mathbb{C}^*$ l'ensemble des éléments de norme complexe 1 et, pour n un entier naturel, $\mathbb{U}_n$ l'ensemble des éléments z tels que $z^n = 1$.

1. Montrer que $\mathbb{U}$ et $\mathbb{U}_n$ sont des sous-groupes de $\mathbb{C}^*$.
2. Soit $G = \langle a \rangle$ un groupe cyclique de générateur a. Rappeler la formule donnant l'ordre de a^k. Puis déterminer tous les éléments d'ordre 4 dans $\mathbb{U}_{20}$.
3. Lorsque G_1, G_2 sont deux groupes finis, montrer que l'élément (a, b) du groupe $G_1 \times G_2$ est d'ordre $o(a, b) = \text{ppcm}(o(a), o(b))$. Puis étendre ce résultat au cas d'un produit de la forme $G_1 \times \cdots \times G_n$ avec $n \geq 2$.
4. Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre $540 = 2^2 3^3 5$. On indiquera dans chaque cas la suite d'invariants.
5. Montrer que tout groupe abélien d'ordre 540 admet au moins un élément d'ordre 30.
6. Montrer qu'il existe un groupe abélien d'ordre 540 ne contenant aucun élément d'ordre 60.

Solution :

1. Le produit de deux nombres complexes de norme 1 est de norme 1, ainsi que l'inverse d'un nombre complexe de norme 1. Ainsi, $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$. Si $z_1, z_2 \in \mathbb{U}_n$, alors $z_1^n = z_2^n = 1$, de sorte que $(z_1/z_2)^n = z_1^n/z_2^n = 1/1 = 1$, et donc $z_1/z_2 \in \mathbb{U}_n$. Donc, $\mathbb{U}_n$ est bien un sous-groupe de $\mathbb{C}^*$.
2. L'ordre de a^k est $\frac{n}{\text{pgcd}(k,n)}$. Pour $n = 20$ et $\zeta = e^{2i\pi/20}$ un générateur de $\mathbb{U}_{20}$, l'ordre de ζ^k vaut 4 si et seulement si le pgcd de k et 20 vaut 5, ce qui arrive exactement lorsque k appartient à l'ensemble $\{5, 15\}$. Donc l'ensemble des éléments d'ordre 4 est $\{\zeta^5, \zeta^{15}\}$, soit $\{e^{10i\pi/20} = i, e^{30i\pi/20} = -i\}$.
3. Soit k un entier naturel, et $(a, b) \in G_1 \times G_2$. Alors $(a, b)^k = (a^k, b^k)$ par définition de la structure de groupe sur $G_1 \times G_2$. On note e_1, e_2 les éléments neutres de G_1, G_2. On a donc l'équivalence
$$(a, b)^k = (e_1, e_2) \iff a^k = e_1 \text{ et } b^k = e_2 \iff o(a) \mid k \text{ et } o(b) \mid k \iff \text{ppcm}(o(a), o(b)) \mid k$$
L'ensemble de ces entiers k est $o(a, b)\mathbb{Z}$ par un résultat du cours, d'où $o(a, b) = \text{ppcm}(o(a), o(b))$.
En utilisant la formule $\text{ppcm}(o(g_1), \text{ppcm}(o(g_2), \ldots, o(g_n)) = \text{ppcm}(o(g_1), \ldots, o(g_n)$, on déduit par récurrence sur n que $o(g_1, \ldots, g_n) = \text{ppcm}(o(g_1), \ldots, o(g_n))$ dans un produit de n groupes finis.
4. D'après le cours, les groupes abéliens d'ordre $2^2 3^3 5$ sont associés aux couples (λ, μ) avec λ une partition de 2 et μ une partition de 3 : $\lambda = (2)$ ou $\lambda = (1, 1)$ et $\mu = (3)$ ou $\mu = (2, 1)$ ou $\mu = (1, 1, 1)$. On trouve les groupes suivants (on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ et on indique λ sur la première ligne et μ sur la première colonne) :

	(2)	(11)
(3)	$\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5 \simeq \mathbb{Z}_{540}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{270}$
(21)	$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{180}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_6 \times \mathbb{Z}_{90}$
(111)	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{60}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$

Les invariants de ces groupes sont :

	(2)	(11)
(3)	(540)	(2, 270)
(21)	(3, 180)	(6, 90)
(111)	(3, 3, 60)	(3, 6, 30)

5. La décomposition primaire d'un groupe G abélien d'ordre 540 est $G = G_2 \times G_3 \times G_5$, où G_2 est d'ordre $2^2 = 4$, G_3 est d'ordre $3^3 = 27$ et G_5 est d'ordre 5. Par le théorème de Cauchy, G_2

admet un élément d'ordre 2, qu'on note x_2, et on définit similairement x_3 d'ordre 3 et x_5 d'ordre 5. Alors, (x_2, x_3, x_5) est d'ordre $\text{ppcm}(2,3,5) = 30$, d'parès la question 3.

6. Tout élément $x = (x_3, x_6, x_{30})$ du groupe $G = \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$ vérifie $30x = (30x_3, 30x_6, 30x_{30}) = (0,0,0)$, donc son ordre divise 30 et ne peut pas être égal à 60. Le groupe G est donc un exemple de groupe abélien d'ordre 540 qui ne contient pas d'élément d'ordre 60.

Exercice 2. Dans cet exercice, on note

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R}^*, b \in \mathbb{R} \right\} \quad \text{et} \quad U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

1. Montrer que G, muni de la multiplication matricielle, est un groupe.
2. Montrer que U est un sous-groupe distingué de G, qui de plus est abélien.
3. En déduire que l'ensemble quotient G/U a une structure de groupe.
4. On note $\phi : G \to \mathbb{R}^* \times \mathbb{R}^*$ l'application définie par
$$\phi : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d).$$
Montrer que ϕ est un morphisme de groupes surjectif.
On rappelle que la structure de groupe sur $\mathbb{R}^*$ est donnée par la multiplication et que la structure de groupe sur un produit est donnée composante par composante : la structure de groupe sur $\mathbb{R}^* \times \mathbb{R}^*$ est donc donnée par $(x_1, y_1) * (x_2, y_2) = (x_1 x_2, y_1 y_2)$.
5. En déduire que le groupe quotient G/U est isomorphe à $\mathbb{R}^* \times \mathbb{R}^*$ et qu'il est abélien.
6. Le groupe G est-il abélien ?

Solution :

1. Le cours nous indique que $\text{GL}_2(\mathbb{R})$ est un groupe. Pour montrer que G est un groupe, il est commode de montrer qu'il est un sous-groupe de $\text{GL}_2(\mathbb{R})$. Soit $g_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, g_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ deux éléments de G. Alors $g_2^{-1} = \begin{pmatrix} \frac{1}{a_2} & \frac{-b_2}{a_2 d_2} \\ 0 & \frac{1}{d_2} \end{pmatrix}$ et donc
$$g_1 g_2^{-1} = \begin{pmatrix} \frac{a_1}{a_2} & \frac{b_1}{d_2} - \frac{a_1 b_2}{a_2 d_2} \\ 0 & \frac{d_1}{d_2} \end{pmatrix},$$
de sorte que $g_1 g_2^{-1} \in G$.
2. Pour $u_1 = \begin{pmatrix} 1 & x_1 \\ 0 & 1 \end{pmatrix}$ et $u_2 = \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix}$, on a $u_1 u_2^{-1} = \begin{pmatrix} 1 & x_1 - x_2 \\ 0 & 1 \end{pmatrix}$, de sorte que U est bien un sous-groupe de G. De plus, $u_1 u_2 = \begin{pmatrix} 1 & x_1 + x_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_2 + x_1 \\ 0 & 1 \end{pmatrix} = u_2 u_1$, de sorte que U est abélien.
Pour $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ et $u = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U$, on a $gug^{-1} = \begin{pmatrix} 1 & \frac{ax}{d} \\ 0 & 1 \end{pmatrix}$, de sorte que $gug^{-1} \in U$. Ainsi, U est bien distingué.
3. Le cours dit que lorsqu'on quotiente un groupe par un sous-groupe distingué, le quotient acquière une structure de groupe. Ainsi, G/U a une structure de groupe.
4. Soit $g_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, g_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$. Alors $\phi(g_1)\phi(g_2) = (a_1, d_1) * (a_2, d_2) = (a_1 a_2, d_1 d_2)$. D'un autre côté, $g_1 g_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}$ et donc $\phi(g_1 g_2) = (a_1 a_2, d_1 d_2)$. On a donc bien $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$, ce qui signifie que ϕ est un morphisme.
Il est surjectif car étant donné $(a, d) \in \mathbb{R}^* \times \mathbb{R}^*$ et $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, on peut remarquer que $\phi(g) = (a, d)$, et que donc (a, d) a un antécédent.
5. Le noyau de ϕ est l'ensemble des matrices $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ telles que $\phi(g) = (1, 1)$, ce qui signifie $(a, d) = (1, 1)$: c'est donc U.

La factorisation canonique de ϕ est donc un isomorphisme de groupes

$$\overline{\phi} : G/\operatorname{Ker}(\phi) = G/U \to \operatorname{Im}(\phi) = \mathbb{R}^* \times \mathbb{R}^* .$$

Ainsi, G/U est isomorphe à $\mathbb{R}^* \times \mathbb{R}^*$, produit de deux groupes abéliens, donc abélien.

6. Si on prend $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ et $g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, alors $g_1 g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ et $g_2 g_1 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$, de sorte que G n'est pas abélien.

   Cet exercice donne donc l'exemple d'un groupe "construit à partir de groupes abéliens" (à savoir U et $\mathbb{R}^* \times \mathbb{R}^*$) mais qui n'est pas abélien. Plus précisément, G est produit semi-direct (cette notion n'a pas été étudiée en cours) de U et $\mathbb{R}^* \times \mathbb{R}^*$.

Exercice 3. Soit G un groupe fini d'ordre n. Soit p le plus petit nombre premier qui divise n. On suppose que H est un sous-groupe de G d'indice p. Le but de cet exercice est de montrer que H est distingué.

1. Donner la définition d'un sous-groupe distingué, donner un exemple de sous-groupe distingué dans un groupe et donner un autre exemple de sous-groupe non distingué.
2. On rappelle que l'indice de H dans G est le cardinal de G/H. Rappeler les définitions de G/H et $H\backslash G$ et expliquer pourquoi on a toujours $H \in G/H$ et $H \in H\backslash G$. Quel est le cardinal de $H\backslash G$?
3. On suppose d'abord que $p = 2$: H est donc un sous-groupe d'indice 2. Montrer que dans ce cas, H est bien distingué. On pourra pour cela considérer les quotients G/H et $H\backslash G$ et en déduire deux partitions de G.

Dans les questions suivantes, on ne fait plus l'hypothèse que $p = 2$.

4. Montrer que la formule $g \cdot xH = gxH$ définit une action de G sur G/H.
5. En restreignant cette action à H, montrer qu'on obtient un morphisme de groupes $\varphi : H \to \mathfrak{S}(G/H)$, où $\mathfrak{S}(G/H)$ désigne le groupe des permutations de l'ensemble G/H.
6. Montrer que les éléments de $\varphi(H)$ préservent l'élément $H \in G/H$, et que donc on obtient plus précisément un morphisme $H \to \mathfrak{S}(E)$, où E désigne l'ensemble G/H privé de H.
7. Montrer que le cardinal de $\mathfrak{S}(E)$ est $(p-1)!$.
8. Montrer que le cardinal de $\varphi(H)$ divise n.
9. Déduire des deux questions précédentes et de l'hypothèse que le cardinal de $\varphi(H)$ est égal à 1.
10. Conclure que H est distingué.

Solution :

1. cf cours
2. cf cours
3. Soit $x \in G$. Si $x \in H$, on a $xH = Hx = H$. Sinon, on a $G = H \amalg xH$ et $G = H \amalg Hx$, d'où on en déduit que $xH = Hx$. Ainsi, H est distingué.
4. Tout d'abord $g(xh)H = gxH$ donc cette définition ne dépend pas du choix (implicite) de x. Ensuite, $(g_1 g_2) \cdot xH = g_1 g_2 xH = g_1 \cdot (g_2 \cdot xH)$.
5. Une action de H est un tel morphisme de groupes, cf cours.
6. $h \cdot eH = hH = H$ pour $h \in H$, donc H préserve l'élément $H \in G/H$. Il préserve donc aussi son complémentaire, E.
7. $\mathfrak{S}(E)$ est isomorphe à $\mathfrak{S}_{p-1}$, donc de cardinal $(p-1)!$.
8. On sait que $|\varphi(H)|$ divise $|H|$, par le théorème de factorisation canonique ($\varphi(H) \simeq H/\operatorname{Ker}(\varphi)$). Comme $|H|$ divise n par le théorème de Lagrange, $f(H)$ divise n.
9. Comme p est le plus petit nombre premier divisant n, tous les facteurs premiers de $(p-1)!$ ne divisent pas n. Ainsi, $(p-1)!$ et n sont premiers entre eux. Donc comme $|f(H)|$ divise ces deux entiers, il est égal à 1.
10. Ceci signifie que $\forall h \in H, \varphi(h) = Id_{G/H}$. Autrement dit, $hxH = xH$ pour tout $h \in H$, donc $HxH = xH$, donc $Hx = xH$.