Université de Bordeaux
Licence de Sciences et Technologies
2016-2017

Structures Algébriques 1

Devoir surveillé

3 mars 2017, Durée 1h30
Documents non autorisés.

Exercice 1. On note $\mathrm{GL}_2(\mathbb{C})$ l'ensemble des matrices 2×2 inversibles à coefficients dans $\mathbb{C}$. Il s'agit d'un groupe pour la multiplication des matrices, propriété qu'on utilisera dans la suite *sans la redémontrer*. Dans $\mathrm{GL}_2(\mathbb{C})$, on considère les matrices :

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ A=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ B=\begin{pmatrix}0&i\\i&0\end{pmatrix}\text{ et }C=\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

et on pose $G=\{I,-I,A,-A,B,-B,C,-C\}$.

1. Dresser la table de multiplication de G et en déduire que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$.
   On vérifie facilement que
   $$A^2=B^2=C^2=-I$$
   et
   $$AB=-BA=C,\ BC=-CB=A,\ CA=-AC=B$$
   d'où l'on déduit la table suivante :

	I	-I	A	-A	B	-B	C	-C
I	I	-I	A	-A	B	-B	C	-C
-I	-I	I	-A	A	-B	B	-C	C
A	A	-A	-I	I	C	-C	-B	B
-A	-A	A	I	-I	-C	C	B	-B
B	B	-B	-C	C	-I	I	A	-A
-B	-B	B	C	-C	I	-I	-A	A
C	C	-C	B	-B	-A	A	-I	I
-C	-C	C	-B	B	A	-A	I	-I

   En particulier, G est stable par produit et passage à l'inverse (chaque ligne et chaque colonne contient l'élément neutre) ; c'est donc un sous-groupe.
2. Le groupe G est-il cyclique ? Abélien ? Justifier.
   Il n'est pas abélien, car $AB\neq BA$ par exemple, donc a fortiori pas cyclique.
3. Énumérer tous les sous-groupes de G. *On prendra soin de justifier que la liste obtenue est complète.*
   Les ordres possibles pour un sous-groupe de G sont, en vertu du théorème de Lagrange, 1, 2, 4 et 8. Examinons ces différentes possibilités :
   - Ordre 1 : il y a un seul sous-groupe, à savoir $\{I\}$.
   - Ordre 2 : les éventuels sous-groupes d'ordre 2 sont nécessairement cycliques, et il y en a autant que d'éléments d'ordre 2. Or $-I$ est le seul élément d'ordre 2, donc $<-I>=\{I,-I\}$ est le seul sous-groupe d'ordre 2.

- Ordre 4 : chaque élément d'ordre 4 engendre un sous-groupe cyclique d'ordre 4. Inversement, chaque sous-groupe cyclique d'ordre 4 contient exactement deux éléments d'ordre 4. D'après la table, il y a 6 éléments d'ordre 4 et donc exactement $3 = \frac{6}{2}$ sous-groupes d'ordre 4, à savoir
$$< A >= \{I, -I, A, -A\},$$
$$< B >= \{I, -I, B, -B\}$$
et
$$< C >= \{I, -I, C, -C\}.$$
Il existe des groupes d'ordre 4 non cycliques, mais G n'en contient pas : en effet, un tel groupe contient nécessairement 3 éléments d'ordre 2, et G n'en possède qu'un.
- Ordre 8 : il y a un seul sous-groupe, à savoir G lui-même.

Exercice 2. Pour tout $n \in \mathbb{N}^*$, on note S_n le groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$. La permutation identité, qui applique chaque élément sur lui-même, est notée Id.

1. Dans S_6, on considère les éléments $\alpha = (1\ 2)(4\ 5)$ et $\beta = (1\ 6\ 5\ 3\ 2)$. Calculer $\beta\alpha\beta^{-1}$.
   On peut faire un calcul direct ou (mieux !) remarquer que $\beta\alpha\beta^{-1} = \beta(1\ 2)\beta^{-1}\beta(4\ 5)\beta^{-1}$ et appliquer la formule de conjugaison des cycles vue en cours. On trouve : $\beta\alpha\beta^{-1} = (6\ 1)(4\ 3)$
2. Soit $\gamma = (1\ 2\ 3\ 4\ 5\ 6) \in S_6$. Calculer γ^2, γ^3, γ^4, γ^5 et γ^6. Déterminer l'ensemble des entiers $m \in \mathbb{Z}$ tels que γ^m soit un cycle de longueur 6.
   $\gamma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\gamma^3 = (1\ 4)(2\ 5)(3\ 6)$, $\gamma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\gamma^5 = (1\ 6\ 5\ 4\ 3\ 2)$, $\gamma^6 = \mathrm{Id}$. Pour un entier m quelconque, on a $\gamma^m = \gamma^r$ où r désigne le reste de la division euclidienne de m par 6. Par conséquent, γ^m est un cycle de longueur 6 si et seulement si $m \equiv 1$ ou $5 \mod 6$.
3. Montrer que S_5 ne contient pas d'élément d'ordre 8.
   On sait que l'ordre d'une permutation est égal au PPCM des longueurs des cycles de sa décomposition en cycles à supports disjoints. Pour qu'il soit égal à 8, il faut donc en particulier que cette décomposition contienne un cycle de longueur 8, ce qui est impossible dans S_5, où les cycles sont de longueur au plus 5..
4. Montrer que pour tout $n \in \mathbb{N}^*$, le nombre d'éléments α de S_n tels que $\alpha^3 = \mathrm{Id}$ est impair.
   Un élément α de S_n vérifie $\alpha^3 = \mathrm{Id}$ si et seulement si il est d'ordre 1 ou 3. L'identité est le seul élément d'ordre 1. Un élément est d'ordre 3 si et seulement si son inverse l'est. On peut donc grouper les éléments d'ordre 3 par paires $\{\alpha, \alpha^{-1}\}$, et leur nombre est donc pair. Le nombre total d' éléments α tels que $\alpha^3 = \mathrm{Id}$ est donc bien impair.

Exercice 3. On rappelle que l'ensemble $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ des nombres complexes non nuls est un groupe pour la multiplication *(on ne demande pas de le redémontrer)*.

Si $z_1, z_2, \ldots, z_k$ sont des nombres complexes non nuls, le sous-groupe de $\mathbb{C}^\times$ qu'ils engendrent est noté $\langle z_1, z_2, \ldots, z_k \rangle$.

Enfin, pour tout entier naturel n non nul, on définit
$$U_n = \left\{ z \in \mathbb{C} \mid z^n = 1 \right\}.$$

1. Montrer que U_n est un sous-groupe cyclique d'ordre n de $\mathbb{C}^\times$, engendré par $e^{2i\pi/n}$.

En posant $z = re^{i\theta}$, avec $r > 0$ et $\theta \in \mathbb{R}$, on a :

$$\begin{aligned} z^n = 1 &\Leftrightarrow r^n e^{in\theta} = 1 \\ &\Leftrightarrow \begin{cases} r = 1 \\ n\theta \in 2\pi\mathbb{Z} \end{cases} \\ &\Leftrightarrow \begin{cases} r = 1 \\ \theta \in \dfrac{2\pi}{n}\mathbb{Z} \end{cases} \\ &\Leftrightarrow z \in < e^{2i\pi/n} > . \end{aligned}$$

2. Soient a et b deux entiers naturels, , dont on note respectivement d et m le PGCD et le PPCM. Soit $n \in \mathbb{N}^*$ un multiple commun de a et de b. On pose $\rho = e^{2i\pi/n}$.
Montrer que
$$< \rho^a > \cap < \rho^b > = < \rho^m > \quad \text{et} \quad < \rho^a, \rho^b > = < \rho^d > .$$

   - Si ρ^k est un élément de U_n, on a les équivalences :
$$\begin{aligned} \rho^k \in < \rho^a > &\Leftrightarrow \exists q \in \mathbb{Z}, \rho^k = \rho^{aq} \\ &\Leftrightarrow \exists q \in \mathbb{Z}, \rho^{k-aq} = 1 \\ &\Leftrightarrow \exists q \in \mathbb{Z}, k - aq \in n\mathbb{Z} \\ &\Leftrightarrow k \in a\mathbb{Z} + n\mathbb{Z} = a\mathbb{Z} \text{ puisque } a \text{ divise } n. \end{aligned}$$
     De même, $\rho^k \in < \rho^b >$ si et seulement si $k \in b\mathbb{Z}$, d'où finalement, $\rho^k \in < \rho^a > \cap < \rho^b >$ si et seulement si $k \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

   - De la même façon,
$$\begin{aligned} \rho^k \in < \rho^a, \rho^b > &\Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, \rho^k = \rho^{au+bv} \\ &\Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, \rho^{k-(au+bv)} = 1 \\ &\Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, k - (au+bv) \in n\mathbb{Z} \\ &\Leftrightarrow k \in a\mathbb{Z} + b\mathbb{Z} + n\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}. \end{aligned}$$

3. Montrer que la réunion de tous les U_n est un sous-groupe de $\mathbb{C}^\times$. Est-il de type fini (c'est-à-dire engendré par un nombre fini d'éléments) ? Justifier.
La réunion, pour tous les $n \in \mathbb{N}^*$, des U_n est non vide (elle contient 1). Si x et y sont deux éléments de $\bigcup_{n\in\mathbb{N}^*} U_n$, alors il existe $\ell \in \mathbb{N}^*$ tel que $x^\ell = 1$ et $m \in \mathbb{N}^*$ tel que $y^m = 1$. On a alors $(xy^{-1})^{\ell m} = 1$, donc $xy^{-1} \in U_{\ell m} \subset \bigcup_{n\in\mathbb{N}^*} U_n$, ce qui prouve que $U := \bigcup_{n\in\mathbb{N}^*} U_n$ est un sous-groupe de $\mathbb{C}^\times$. Si U était de type fini, il existerait des nombres complexes non nuls z_1, z_2, …, z_k, appartenant respectivement à U_{n_1}, U_{n_2}, …, U_{n_k} tels que $U = \langle z_1, z_2, \ldots, z_k \rangle$. Tout élément z de U s'écrirait alors sous la forme
$$z = z_1^{a_1} z_2^{a_2} \ldots z_k^{a_k}$$
avec a_1, a_2, …, a_k dans $\mathbb{Z}$ et en posant $N = \text{PPCM}(n_1, n_2, \ldots, n_k)$ on aurait $z^N = 1$. Autrement dit, U serait contenu dans U_N ce qui est absurde puisque, par exemple, $e^{2i\pi/(N+1)}$ appartient à U mais pas U_N.