

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

DEVOIR SURVEILLÉ 1
 correction

Exercice 1.

- Si H est caractéristique, il est clair qu'on a bien l'inclusion. Supposons donc que $\varphi(H) \subset H$ pour tout automorphisme. On a alors $\varphi^{-1}(H) \subset H$. Or $H = \varphi(\varphi^{-1}(H))$ puisque φ est surjective, et donc $H = \varphi(\varphi^{-1}(H)) \subset \varphi(H)$. On a donc bien $\varphi(H) = H$.
- Soit $\varphi \in \text{Aut}(G)$.
 On a $\varphi(\{e_G\}) = \{e_G\}$ et $\varphi(G) = G$, donc $\{e_G\}$ et G sont caractéristiques.
 Soit $g \in Z(G)$. Pour tout $h \in G$, il existe $\tilde{h} \in G$ tel que $h = \varphi(\tilde{h})$ et donc $\varphi(g).h = \varphi(g).\varphi(\tilde{h}) = \varphi(g.\tilde{h}) = \varphi(\tilde{h}.g) = \varphi(\tilde{h}).\varphi(g) = h.\varphi(g)$. On a donc $\varphi(g) \in Z(G)$ et donc $\varphi(Z(G)) \subset Z(G)$. On en conclut que $Z(G)$ est caractéristique.
 Pour montrer que $\varphi(D(G)) \subset D(G)$, il suffit de vérifier que l'image d'un commutateur $[g_1.g_2]$ est un commutateur. Or clairement $\varphi([g_1.g_2]) = [\varphi(g_1), \varphi(g_2)]$. On en conclut que $D(G)$ est caractéristique.
- Considérons la conjugaison φ_g par $g \in G$. C'est un automorphisme, on en déduit que $\varphi_g(H) = H$, et ce pour tout $g \in G$. On en déduit que H est stable par conjugaison, il est donc distingué.
- On prend $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et on considère le sous-groupe $H = \{(0, 0), (1, 0)\} \subset G$. Puisque G est abélien, H est distingué, mais en considérant l'automorphisme $\varphi : (x, y) \mapsto (x, y + x)$, on voit que H n'est pas caractéristique car $\varphi(H) = \{(0, 0), (1, 1)\} \not\subset H$.
- On a vu que, pour tout groupe G , G est caractéristique dans G . Il est clair que si G_1 et G_2 sont respectivement des sous-groupes (caractéristiques) l'un de l'autre, alors $G_1 = G_2$. Il ne reste donc plus qu'à montrer la transitivité. On considère pour cela trois groupes $K \subset H \subset G$ avec K caractéristique dans H et H caractéristique dans G . Soit φ un automorphisme de G . Puisque H est caractéristique dans G , on a $\varphi(H) = H$ et on peut donc considérer $\varphi|_H : H \rightarrow H$ qui est de fait surjective et toujours injective. On a donc $\varphi|_H \in \text{Aut}(H)$ et, puisque K est caractéristique dans H , $\varphi(K) = \varphi|_H(K) = K$. On en conclut que K est caractéristique dans G .
- On considère le groupe alterné $\mathcal{A}_4$ et le sous-groupe $G := \{\text{Id}, (12)(34), (13)(24), (14)(23)\}$ formé des produits de transpositions à supports disjoints. Il est distingué car la conjugaison préserve la taille des cycles. De plus, il contient le sous-groupe $H := \{\text{Id}, (12)(34)\}$ qui est distingué dans G car d'indice 2. Par contre, H n'est pas distingué dans $\mathcal{A}_4$ car le conjugué de $(12)(34)$ par $(123) \in \mathcal{A}_4$ vaut $(14)(23) \notin H$.

Exercice 2.

- On commence par remarquer que $\det(a_k) = \det(b_k) = 1 \neq 0$ et donc $D_n \subset \text{SL}_2(\mathbb{C})$. Par calcul direct, on voit que

$$a_k^{-1} = a_{-k} ; \quad b_k^{-1} = b_{n+k} (= -b_k) ;$$

$$a_{k_1} a_{k_2} = a_{k_1+k_2} ; \quad a_{k_1} b_{k_2} = b_{k_1+k_2} ; \quad b_{k_1} a_{k_2} = b_{k_1-k_2} ; \quad b_{k_1} b_{k_2} = a_{n+k_1-k_2} (= -a_{k_1-k_2}).$$

En particulier, D_n est stable par produit et par inverse, c'est donc un sous-groupe de $\text{SL}_2(\mathbb{C})$, donc un groupe.

- (a) D'après les règles de calcul de la question précédente, on a clairement
 - $\langle a_1 \rangle = \{a_1^k = a_k \mid k \in \llbracket 0, 2n-1 \rrbracket\} \cong \mathbb{Z}/2n\mathbb{Z}$, on en déduit que $|a_k| = \frac{2n}{\text{pgcd}(2n, k)}$;
 - $b_k^2 = -\text{Id}$, on en déduit que $|b_k| = 4$.
- (b) D'après les règles de calcul de la question 1, on a $a_1.b_0.a_1 = a_1.b_{-1} = a_0$.

- (c) Pour l'existence, on note que $a_k = a_1^k$ et que $b_k = a_k \cdot b_0 = a_1^k \cdot b_0$. De plus, a_1 étant d'ordre $2n$, on peut remplacer k par le reste de sa division euclidienne par $2n$.
 Pour l'unicité, on suppose que $a_1^r b_0^s = a_1^{r'} b_0^{s'}$. On a alors $a_1^{r-r'} = b_0^{s'-s}$ avec $s' - s \in \{-1, 0, 1\}$. Mais b_0 et b_0^{-1} ne sont pas diagonales comme les puissances de a_1 . On en déduit que $s - s' = 0$, c'est-à-dire que $a_1^{r-r'} = \text{Id}$, et donc $r - r' \in 2n\mathbb{Z}$. Au final, on a bien $s = s'$ et $r = r'$.
- (d) D'après la question précédente, D_n est en bijection avec $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On en déduit que $|D_n| = 4n$.
3. (a) D'après la question 2.(d), D_1 est un groupe à quatre éléments ; et d'après la question 2.(a), b_0 est d'ordre 4. On en déduit que $D_1 = \langle b_0 \rangle \cong \mathbb{Z}/4\mathbb{Z}$.
- (b) Si D_n était abélien on aurait $b_1 = a_1 \cdot b_0 = b_0 \cdot a_1 = b_{-1}$, et donc $\omega_n = \omega_n^{-1}$, c'est-à-dire $\omega_n^2 = 1$, ce qui n'est vrai que pour $n = 1$.
4. (a) D'après les règles de calcul de la question 1, on a

$$[a_{k_1}, a_{k_2}] = a_{k_1+k_2-k_1-k_2} = \text{Id} ;$$

$$[a_{k_1}, b_{k_2}] = a_{k_1} \cdot b_{k_2} \cdot a_{k_1}^{-1} \cdot b_{k_2}^{-1} = a_{k_1} \cdot b_{k_2} \cdot a_{-k_1} \cdot b_{n+k_2} = b_{k_1+k_2} \cdot b_{n+k_2-k_1} = a_{2k_1} = a_2^{k_1} ;$$

$$[b_{k_1}, a_{k_2}] = [a_{k_2}, b_{k_1}]^{-1} = a_2^{-k_2} ;$$

$$[b_{k_1}, b_{k_2}] = b_{k_1} \cdot b_{k_2} \cdot b_{k_1}^{-1} \cdot b_{k_2}^{-1} = b_{k_1} \cdot b_{k_2} \cdot b_{n+k_1} \cdot b_{n+k_2} = a_{n+k_1-k_2} \cdot b_{n+k_1-k_2} = a_{2k_1} = a_2.$$

On en déduit bien que $D(D_n) = \langle a_2 \rangle$.

- (b) D'après la question 2.(c), le quotient est le groupe $\{\overline{\text{Id}}, \overline{a_1}, \overline{b_0}, \overline{a_1 \cdot b_0}\}$ d'ordre 4. De plus, on a $\overline{a_1}^2 = \overline{\text{Id}}$ et $\overline{a_1 \cdot b_0}^2 = \overline{a_1 \cdot b_0 \cdot a_1 \cdot b_0} = \overline{b_0^2} = \overline{b_0}^2 = \overline{a_n}$. Donc si n est pair, tous les éléments sont d'ordre 2 et on a $D_n/D(D_n) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; et si n est impair, alors $\overline{b_0}$ est d'ordre 4, donc engendre le groupe quotient, et on a $D_n/D(D_n) \cong \mathbb{Z}/4\mathbb{Z}$.
5. (a) D'après les règles de calcul de la question 1, on a

$$b_0 \cdot a_{2k} \cdot b_0^{-1} = b_0 \cdot a_{2k} \cdot b_n = b_0 \cdot b_{2k+n} = a_{-2k} ;$$

$$b_0^3 \cdot a_{2k} \cdot b_0^{-3} = b_n \cdot a_{2k} \cdot b_0 = b_n \cdot b_{2k} = a_{-2k} ;$$

et, puisque $b_0^2 = a_n$, $b_0^0 \cdot a_{2k} \cdot b_0^{-0} = b_0^2 \cdot a_{2k} \cdot b_0^{-2} = a_{2k}$.

- (b) Puisque n est impaire, $D_n/D(D_n)$ est engendré par $\overline{b_0}$, on peut donc considérer l'application

$$\psi : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong D(D_n) \times D_n/D(D_n) & \longrightarrow & D_n \\ (k, r) \cong (a_{2k}, \overline{b_0}^r) & \longmapsto & a_{2k} \cdot b_0^r \end{array}.$$

Elle est injective car $a_{2k} \cdot b_0^r = a_{2k'} \cdot b_0^{r'}$ implique que $a_{2(k-k')} = b_0^{r'-r}$ avec $r' - r \in \llbracket -3, 3 \rrbracket$ et $2(k - k') \in \llbracket 2 - 2n, 2n - 2 \rrbracket$, or $b_0^{r'-r}$ n'est pas diagonale si $r' - r$ est impair, et $b_0^{\pm 2} = a_n$ n'est égal à $a_{2(k-k')}$ que si n et $2(k - k')$ sont congrus modulo $2n$, c'est-à-dire si $2(k - k') = \pm n$, ce qui n'est pas possible puisque n est impair ; on a donc $r = r'$ et de fait $k = k'$ par un argument similaire à celui de la question 2.(c). Par égalité des cardinaux des ensembles de départ et d'arrivée, on en déduit que ψ est bijective.

Enfin, on a

$$\begin{aligned} \psi(k, r) \cdot \psi(k', r') &= a_{2k} \cdot b_0^r \cdot a_{2k'} \cdot b_0^{r'} \\ &= a_{2k} \cdot b_0^r \cdot a_{2k'} \cdot b_0^{-r} \cdot b_0^r \cdot b_0^{r'} \\ &= a_{2k} \cdot a_{2k'}^{(-1)^r} \cdot b_0^{r+r'} \text{ (d'après la question précédente)} \\ &= a_{2(k+(-1)^r k')} \cdot b_0^{r+r'} = \psi(k + (-1)^r k', r + r'). \end{aligned}$$

L'application ψ est donc un isomorphisme entre D_n et $\mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z}$.