Groupes et géométrie, feuille 4

N. Perrin

À rendre le mercredi 04.03.2020

Correction le jeudi 05.03.2020

Exercice 1 ($2 \times 5 + 10 = 20$ Points) Soit K un corps. On note $B \subset \mathrm{GL}_2(K)$ le sous-groupe de matrices triangulaires supérieures, on note $T \subset B$ le sous-groupe des matrices diagonales et on note $U \subset B$ le sous-groupe des matrices triangulaires supérieures ayant un 1 sur la diagonale. Rappelons que l'on a vu (cf. TD 3) que $U \triangleleft B$ et $B/U \simeq T$.

On suppose maintenant que $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ est le corps ayant 2 éléments.

(i) Déterminer les ordres $|\mathrm{GL}_2(\mathbb{F}_2)|$, $|B|$, $|T|$ et $|U|$ des groupes G, B, T et U.

(ii) On définit les vecteurs suivants :

$$x_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ x_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ et } x_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

et on pose $X = \{x_1, x_2, x_3\}$. Montrer que $f(X) = X$ pour tout $f \in \mathrm{GL}_2(\mathbb{F}_2)$.

(iii) Soit $\varphi : \mathrm{GL}_2(\mathbb{F}_2) \to \mathrm{Bij}(X)$ l'application définie par $\varphi(f) : X \to X$, $x_i \mapsto f(x_i)$ pour $i \in [1,3]$. Montrer que φ est un isomorphisme de groupes.

Solution. (i) On cherche les matrices 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ qui sont inversibles. Commençons par décrire toutes les matrices 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Il s'agit de choisir combien de 0 (et donc combien de 1) on a dans la matrice et où ils sont placés. On a 4 "places" où mettre un 0 ou 1 donc 2^4 possibilités. Ces possibilités se décomposent en fonction du nombre de 0 :

- 4 zéros : $\binom{4}{4} = 1$ choix, la matrice nulle $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, elle n'est pas inversible
- 3 zéros : $\binom{4}{3} = 4$ choix, on a les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, aucune n'est inversible
- 2 zéros : $\binom{4}{2} = 6$ choix, on a les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, les deuxième et troisième sont inversibles ;

- 1 zéros : $\binom{4}{1} = 4$ choix, on a les matrices $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, elles sont toutes inversibles
- 0 zéros : $\binom{4}{0} = 1$ choix, la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, elle n'est pas inversible.

Finalement, on a

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$U = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

On a donc $\mathrm{GL}_2(\mathbb{F}_2)| = 6$, $|B| = 2 = |U|$ et $|T| = 1$.

(ii) On remarque que $X = \mathbb{F}^2 \setminus \{(0,0)\}$. De plus, tout élément $g \in \mathrm{GL}_2(\mathbb{F}_2)$ realise une bijection de $\mathbb{F}_2^2$ dans lui-même et envoie $(0,0)$ sur $(0,0)$. Ainsi ond doit avoir $g(X) = X$.

(iii) Montrons que φ est un morphisme de groupes. On a $\varphi(fg)(x_i) = (fg)(x_i) = f(g(x_i))$ donc $\varphi(fg) = f \circ g$ et φ est un morphisme de groupes. Montrons qu'il est injectif. Soit $f \in \ker(\varphi)$, on a $\varphi(f) = \mathrm{Id}_X$ donc $f(x_i) = x_i$ pour tout $i \in [1,3]$. Comme (x_1, x_2) est une base de $\mathbb{F}_2^2$ et que f est linéaire, le fait que $f(x_1) = x_1$ et $f(x_2) = x_2$ impose $f = I_2$. Finalement $|\mathrm{GL}_2(\mathbb{F}_2)| = 6 = |\mathfrak{S}_3|$ donc l'application injective φ est aussi surjective. ∎

Exercice 2 (20 Points) On note D_8 le groupe des isométries qui préservent un carré. Montrer que les groupes

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad D_8, \quad \mathbb{H},$$

sont deux-à-deux non isomorphes. Lesquels sont commutatifs ?

Solution. On regarde les ordres des éléments. Le seul groupe ayant un élément d'ordre 8 est $\mathbb{Z}/8\mathbb{Z}$ donc il n'est isomorphe à aucun autre (cf. plus bas pour D_8). Il est commutatif.

Le seul groupe ayant uniquement des éléments d'ordre 2 est $(\mathbb{Z}/2\mathbb{Z})^3$, il n'est isomorphe à aucun autre (cf. plus bas pour D_8). Il est commutatif.

Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est commutatif alors que D_8 et $\mathbb{H}$ ne le sont pas (cf. plus bas pour D_8 et TD 2 pour $\mathbb{H}$), il n'est donc isomorphe à aucun autre. Il est commutatif.

Le groupe D_8 des isométries d'un carré $ABCD$ de centre O contient la rotation r de centre O et d'angle $\frac{\pi}{2}$ qui est d'ordre 4. De plus il contient la symétrie s_{AB} par rapport à la médiatrice de $[AB]$. De plus, on a $rs_{AB}r^{-1} = s_{CB}$ la symétrie par rapport à la médiatrice de $[BC]$. Donc D_8 n'est pas commutatif. Enfin, le groupe D_8 contient s_{AB} et s_{BC} qui sont d'ordre 2 donc il contient 2 éléments d'ordre 2. Ce n'est pas le cas du groupe $\mathbb{H}$ donc D_8 n'est isomorphe à aucun autre. Il n'est pas commutatif.

D'après ce qui précède, le groupe $\mathbb{H}$ n'est isomorphe à aucun autre. Il n'est pas commutatif. ∎

Exercice 3 ($6 \times 6 = 30$ Points) Soit G un groupe fini d'ordre $|G|$ et soit p un facteur premier de $|G|$.

(i) Supposons que G est un groupe cyclique. Montrer qu'il existe un élément $g \in G$ tel que $\mathrm{ord}(g) = p$.

(ii) On suppose maintenant que G est commutatif.

(a) Soit $H \subset G$ un sous-groupe, montrer que $H \triangleleft G$.

(b) Soit $H \subset G$ un sous-groupe et soit $g \in G$ tel que p divise l'ordre de $[g] \in G/H$. Montrer que p divise $\mathrm{ord}(g)$.

(c) Montrer par récurrence sur $|G|$ qu'il existe un élément $g \in G$ tel que p divise $\mathrm{ord}(g)$.

(d) Montrer qu'il existe $g \in G$ tel que $\mathrm{ord}(g) = p$.

(iii) Montrer en donnant un exemple, que si n est un facteur non premier de $|G|$ alors il n'existe pas nécessairement d'élément d'ordre n (même si G est commutatif).

Solution. Posons $n = |G|$.

(i) Soit g un générateur de G. On a $G = \langle g \rangle$ et $\mathrm{ord}(g) = |G| = n$. On sait que $\mathrm{ord}(g^d) = \frac{n}{\mathrm{pgcd}(d,n)}$. Comme p divise n, on a $n = dp$ pour un $d \in \mathbb{Z}$. On a donc $\mathrm{ord}(x^d) = \frac{n}{\mathrm{pgcd}(d,n)} = \frac{n}{d} = p$.

(ii).(a) Comme le groupe est commutatif, tout sous-groupe est distingué.

(ii).(b) On a $[g]^{\mathrm{ord}(x)} = [x^{\mathrm{ord}(x)}] = [1]$ donc $\mathrm{ord}([x])$ divise $\mathrm{ord}(x)$ et comme p divise $\mathrm{ord}([x])$, on a que p divise $\mathrm{ord}(x)$.

(ii).(c) Si le groupe G est cyclique, le résultat est vrai par (i). Sinon, soit $g \in G$ avec $g \neq 1$. Alors $H = \langle g \rangle \subsetneq G$. On a $H \triangleleft G$ par (ii).(a) et $|H||G/H| = |G|$ donc p divise $|H||G/H|$ donc p divise $|H|$ ou $|G/H|$. Dans le premier cas, on conclue par récurrence car $|H| < |G|$. Dans le second cas, par récurrence (on a $|G/H| < |G|$), il existe $g' \in G$ tel que p divise $\mathrm{ord}([g'])$ et par (ii).(b) p divise $\mathrm{ord}(g')$.

(ii).(d) Soit g tel que p divise $\mathrm{ord}(g)$. Alors $\langle g \rangle$ est un cyclique groupe dont l'ordre est divisible par p donc il contient un élément d'ordre p par (i). ∎

Exercice 4 ($3 \times 10 = 30$ Points) Un sous-groupe $H \subset G$ est dit **caractéristique** si pour tout automorphisme $\varphi : G \to G$, on a $\varphi(H) = H$.

(i) Montrer que si $H \subset G$ est un sous-groupe caractéristique alors $H \triangleleft G$.

(ii) Soit $H \subset G$ un sous-groupe caractéristique de G et soit $K \subset H$ un sous-groupe caractéristique de H. Montrer que K est un sous-groupe caractéristique de G.

(iii) Soit $H \triangleleft G$ un sous-groupe distingué de G et soit $K \subset H$ un sous-groupe caractéristique de H. Montrer que $K \triangleleft G$.

Solution. (i) L'application de conjugaison $\mathrm{Int}_g : G \to G$, $h \mapsto ghg^{-1}$ est un automorphisme de groupes (TD 0). On a donc $H = \mathrm{Int}_g(H) = gHg^{-1}$ pour tout $g \in G$ et $H \triangleleft G$.

(ii) Soit φ un automorphisme de G. On a $\varphi(H) = H$ donc $\psi = \varphi|_H$ est un automorphisme de H. On a $\psi(K) = K$ et donc $\varphi(K) = \varphi|_H(K) = \psi(K) = K$. Ainsi K est un sous-groupe caractéristique de G.

(iii) Soit $g \in G$, l'application de conjugaison $\mathrm{Int}_g : G \to G$, $h \mapsto ghg^{-1}$ est un automorphisme de groupes et comme H est distingué, on a $H = gHg^{-1}\mathrm{Int}_g(H)$. Donc $\psi = \mathrm{Int}_g|_H$ est un automorphisme de H. On a $\psi(K) = K$ et donc $gKg^{-1} = \mathrm{Int}_g(K) = \psi(K) = K$. Ainsi K est un sous-groupe distingué de G. ■