Université de Bourgogne
Département de mathématiques
UFR Sciences et Techniques

Licence 3
UE LMo6C : Algèbre 2

devoir maison n°1

Exercice 1. Soit G un groupe finiment engendré et $g_1, g_2, \dots, g_k$ des générateurs. Soit H un autre groupe et $\varphi : G \to H$ un homomorphisme.

1. Montrer que φ est complètement déterminé par les images des générateurs $g_1, g_2, \dots, g_k$.
2. Montrer que :
   (a) si $x \in G$ est d'ordre fini p alors l'ordre de $\varphi(x)$ divise p ;
   (b) si H est fini d'ordre n, alors l'ordre de $\varphi(x)$ divise le pgcd de p et de n.
3. Montrer que si φ est un isomorphisme, et si $x \in G$ est d'ordre fini p, alors l'ordre de $\varphi(x)$ est égal à p.

Solution de l'exercice 1.

1. Notons $\Gamma = \{g_1, \dots, g_k\}$ l'ensemble constitué de ces générateurs. Tout élément x de G peut s'écrire sous la forme :
$$x = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \cdots g_{i_r}^{\varepsilon_r}$$
où $r \in \mathbb{N}^*$ et $g_{i_j} \in \Gamma$, $\varepsilon_j \in \{-1; 1\}$ pour tout $j \in [\![1; r]\!]$. Mais puisque $\varphi : G \to H$ un homomorphisme, on a :
$$\varphi(x) = \varphi(g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \cdots g_{i_r}^{\varepsilon_r}) = \varphi(g_{i_1})^{\varepsilon_1} \varphi(g_{i_2})^{\varepsilon_2} \cdots \varphi(g_{i_r})^{\varepsilon_r}.$$
Par conséquent, si on connaît $\varphi(g)$ pour tout $g \in \Gamma$, on connaît $\varphi(x)$ pour tout $x \in G$.
2. (a) Si x est d'ordre fini p alors p est le plus petit entier $n \in \mathbb{N}^*$ (au sens de la division) tel que $x^n = 1_G$, où 1_G désigne l'élément neutre de G, autrement dit tout entier n satisfaisant cette propriété est un multiple de p. En particulier, $x^p = 1_G$ et donc $\varphi(x^p) = \varphi(x)^p = \varphi(1_G) = 1_H$, où 1_H désigne l'élément neutre de H. Mais alors l'ordre de $\varphi(x)$ divise p.
   (b) En vertu du théorème de Lagrange, si H est fini d'ordre n, l'ordre de $\varphi(x)$ divise n donc combiné avec ce qui précède, l'ordre de $\varphi(x)$ divise à la fois p et n, donc divise le pgcd de p et n.
3. Si φ est un isomorphisme et si x est d'ordre fini alors l'ordre de $\varphi(x)$ divise l'ordre de x (question 2(a)) et de la même manière pour $y = \varphi(x)$, qui est d'ordre fini, l'ordre de $\varphi^{-1}(y) = x$ divise l'ordre de $y = \varphi(x)$. Ainsi, x et $\varphi(x)$ ont même ordre.

Exercice 2. Soit G un groupe et Γ un système de générateurs de G. Soit H un sous-groupe de G.

1. Montrer l'équivalence : $\quad (H \lhd G) \iff \big(\forall g \in \Gamma \quad gHg^{-1} = H\big)$.
2. Soit Σ un système de générateurs de H.
   (a) Soit $x \in G$. Montrer l'équivalence : $\quad (xHx^{-1} \subset H) \iff \big(\forall h \in \Sigma \quad xhx^{-1} \in H\big)$.
   (b) En déduire l'équivalence : $\quad (H \lhd G) \iff \big(\forall g \in \Gamma \quad \forall h \in \Sigma \quad ghg^{-1} \in H \text{ et } g^{-1}hg \in H\big)$.
3. On note $Z(G)$ le centre de G : $Z(G) = \{x \in G : \forall y \in G \quad xy = yx\}$.
   (a) Montrer l'équivalence : $\quad \big(x \in Z(G)\big) \iff \big(\forall g \in \Gamma \quad gx = xg\big)$.
   (b) Application. On note $\mathrm{GL}_2(\mathbb{Z})$ le groupe des matrices inversibles à coefficients entiers (muni du produit des matrices).
      i. Donner une condition nécessaire et suffisante pour que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}$ appartienne à $\mathrm{GL}_2(\mathbb{Z})$.
      ii. Montrer que les matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ engendrent $\mathrm{GL}_2(\mathbb{Z})$.
      iii. Déterminer le centre $\mathrm{GL}_2(\mathbb{Z})$.

Solution de l'exercice 2.

1. On rappelle la définition de $H \lhd G$ que l'on utilise :

$$(\star) \qquad (H \lhd G) \iff \big(\forall x \in G \quad xHx^{-1} = H\big).$$

L'implication

$$(H \lhd G) \implies \big(\forall g \in \Gamma \quad gHg^{-1} = H\big)$$

est immédiate : ce n'est qu'un cas particulier du sens direct de $(\star)$ (on ne prend que les éléments de $x = g \in \Gamma$).

Pour l'implication réciproque, remarquons que pour $a, b \in G$ on a les implications

$$(aHa^{-1} = H) \implies (a^{-1}Ha = H) \qquad \text{et} \qquad (aHa^{-1} = H \quad \text{et} \quad bHb^{-1} = H) \implies (abH(ab)^{-1} = H).$$

Comme tout élément $x \in G$ est un produit d'éléments de Γ ou de leurs inverses, une simple récurrence sur le nombre de facteurs dans ce produit nous donne :

$$\big(\forall g \in \Gamma \quad gHg^{-1} = H\big) \implies \big(\forall x \in G \quad gHg^{-1} = H\big) \implies (H \lhd G).$$

2. (a) L'implication

$$(xHx^{-1} \subset H) \implies \big(\forall h \in \Sigma \quad xhx^{-1} \in H\big)$$

est évidente.

Pour l'implication réciproque, remarquons que pour $a_1, a_2 \in G$ et $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$ on a :

$$xa_1^{\varepsilon_1}a_2^{\varepsilon_2}x^{-1} = (xa_1x^{-1})^{\varepsilon_1}(xa_2x^{-1})^{\varepsilon_2}$$

Comme tout élément de H s'écrit comme produit d'éléments de H et de leurs inverse, une simple récurrence sur le nombre de facteurs dans ce produit nous donne :

$$(\forall h \in \Sigma \quad xhx^{-1} \in H) \implies (\forall h \in H \quad xhx^{-1} \in H) \implies (xHx^{-1} \subset H).$$

Remarque. Attention, on n'obtient pas l'égalité. Pour avoir l'égalité, il faudrait que $x^{-1}Hx \subset H$ donc remplacer x par x^{-1} mais x est fixé ! Cependant, si x est d'ordre fini p alors on a l'égalité car $x^{-1} = x^{p-1}$ et

$$(xHx^{-1} \subset H) \implies (\forall k \in \mathbb{N}^* \quad x^kHx^{-k} \subset H) \implies (x^{p-1}Hx^{1-p} \subset H) \implies (H \subset xHx^{-1}).$$

(b) On cumule les résultats des deux questions précédentes :

$$\begin{aligned}
(H \lhd G) &\iff \big(\forall x \in G \quad xHx^{-1} = H\big) \\
&\iff \big(\forall x \in \Gamma \quad xHx^{-1} = H\big) \\
&\iff \big(\forall x \in \Gamma \quad xHx^{-1} \subset H \quad \text{et} \quad x^{-1}Hx \subset H\big) \\
&\iff \big(\forall x \in \Gamma \quad \forall h \in \Sigma \quad xhx^{-1} \in H \quad \text{et} \quad x^{-1}hx \in H\big)
\end{aligned}$$

3. (a) L'implication

$$\big(x \in Z(G)\big) \implies \big(\forall g \in \Gamma \quad gx = xg\big)$$

est évidente.

On remarque que si $xa = ax$ et $xb = bx$ alors $xa^{-1} = a^{-1}x$ et $xab = abx$. Comme tout élément $g \in G$ est un produit d'éléments de Γ ou de leurs inverses, une simple récurrence sur le nombre de facteurs dans ce produit nous donne :

$$\big(\forall g \in \Gamma \quad gx = xg\big) \implies \big(\forall a \in G \quad ax = xa\big) \implies \big(x \in Z(G)\big).$$

(b) Soit $A \in \mathrm{GL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{R})$. Alors A est inversible donc :

$$\det A \in \mathbb{Z}^* \quad \text{et} \quad A^{-1} \in \mathrm{GL}_2(\mathbb{Z}) \quad \text{donc} \quad \det(A^{-1}) = (\det A)^{-1} \in \mathbb{Z}^*.$$

Ainsi $\det A \in \{-1; 1\}$. Autrement dit, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}$ est dans $\mathrm{GL}_2(\mathbb{Z})$ alors $ad - bc \in \{-1, 1\}$.

Réciproquement, si $ad - bc \in \{-1, 1\}$ l'inverse de A est $\pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ qui est bien dans $\mathrm{GL}_2(\mathbb{Z})$.

(c) On note $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ la matrice identité. Les trois matrices $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ et $-E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ont pour déterminants respectifs -1, -1 et 1 donc sont dans $\mathrm{GL}_2(\mathbb{Z})$. En outre, S et $-E$ sont d'ordre 2, donc égales à leur inverse. Considérons les matrices suivantes construites à partir de S et T :

$$T^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \quad U := ST = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad L := TS = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad F := UST^{-1}SL = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Alors pour tout $n \in \mathbb{Z}$ les matrices suivantes (calculées par récurrence sur $|n|$) et leurs opposées (toutes engendrées par S, T et $-E$) sont les seules matrices de $\mathrm{GL}_2(\mathbb{Z})$ qui ont un coefficient nul :

$$U^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad L^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \quad SU^n = \begin{pmatrix} 0 & 1 \\ 1 & n \end{pmatrix} \quad SL^n = \begin{pmatrix} n & 1 \\ 1 & 0 \end{pmatrix}$$

$$FU^n = \begin{pmatrix} 1 & n \\ 0 & -1 \end{pmatrix} \quad L^nF = \begin{pmatrix} 1 & 0 \\ n & -1 \end{pmatrix} \quad SFU^n = \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix} \quad SL^nF = \begin{pmatrix} n & -1 \\ 1 & 0 \end{pmatrix}$$

En effet, si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}$ est dans $\mathrm{GL}_2(\mathbb{Z})$ alors $ad - bc = \pm 1$. Si $a = 0$ ou $d = 0$ alors b et c sont dans $\{-1, 1\}$ et si $b = 0$ ou $c = 0$ alors a et d sont dans $\{-1, 1\}$.

Supposons maintenant $abcd \neq 0$. Quitte à multiplier A par F à gauche et/ou à droite, on peut supposer que $ad - bc = 1$ et $c > 0$. En vertu du lemme de Bézout, a et c sont premiers entre eux. Si on fait la division euclidienne de a par c, il existe des entiers $q_1 \in \mathbb{Z}$ et r_1 tels que $a = q_1c + r_1$ avec $0 < r_1 < c$, avec c et r_1 premiers entre eux. Alors :

$$SU^{-q_1}A = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & b_1 \\ r_1 & d_1 \end{pmatrix} \quad \text{avec } b_1 = d \text{ et } d_1 = b - q_1 d$$

On voit s'amorcer l'algorithme d'Euclide : en itérant le processus

$$a = q_1c + r_1 \qquad c = q_2r_1 + r_2 \qquad r_1 = q_3r_2 + r_3 \qquad \dots \qquad r_{n-2} = q_nr_{n-1} + 1$$

autrement dit si on pose $c = r_0$, il existe des entiers $q_2, \dots, q_n$ et $r_2, \dots r_n$ tels que

$$r_n = 1 \quad \text{et} \quad \forall i \in [\![1, n]\!] \quad r_{i-1} = q_{i+1}r_i + r_{i+1} \quad \text{et} \quad 0 < r_{i+1} < r_i \quad (\text{division de } r_{i-1} \text{ par } r_i)$$

(récurrence sur $k \geqslant \max\{|a|, c\}$). Il vient alors :

$$(SU^{-r_{n-1}})\left[(SU^{-q_n})\dots(SU^{-q_2})(SU^{-q_1})A\right] = \begin{pmatrix} 0 & 1 \\ 1 & -r_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-1} & \beta \\ 1 & \delta \end{pmatrix} = \begin{pmatrix} 1 & \delta \\ 0 & \beta - r_{n-1}\delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

avec $\beta, \delta \in \mathbb{Z}$. Nécessairement, compte tenu de ce qui précède $\beta - r_{n-1}\delta \in \{-1; 1\}$. Précisément $\beta - r_{n-1}\delta = (-1)^n$ puisque $\det A = 1$ donc :

$$\begin{pmatrix} 1 & \delta \\ 0 & \beta - r_{n-1}\delta \end{pmatrix} = \begin{pmatrix} 1 & \delta \\ 0 & (-1)^{n+1} \end{pmatrix} = F^{n+1}U^{\delta}.$$

Par conséquent

$$A = U^{q_1}SU^{q_2}\dots SU^{q_n}SU^{r_{n-1}}SF^{n+1}U^{\delta} \in \langle S, T, -E \rangle.$$

Exercice 3. Pour un entier $n \geqslant 2$, on note $\mathcal{S}_n$ le groupe des permutations de $\{1, 2, \dots, n\}$.

1. On considère $n = 3$. On note $t = (1\,2)$ et $c = (1\,2\,3)$. Exprimer tous les éléments de $\mathcal{S}_3$ en fonction de t et c et déterminer le sous-groupe dérivé $[\mathcal{S}_3, \mathcal{S}_3]$.
2. On considère $n > 3$. On note $t = (1\,2)$ et $c = (1\,2\,3\,\dots\,n)$.
   (a) Montrer que $\Gamma = \{t, c\}$ est un système de générateurs de $\mathcal{S}_n$.
   (b) Déterminer le sous-groupe H de $\mathcal{S}_n$ engendré par les commutateurs des éléments de Γ.
   (c) Le sous-groupe dérivé $[\mathcal{S}_n, \mathcal{S}_n]$ est-il égal à H ?

Solution de l'exercice 3.

1. Remarquons que $\mathrm{id} = t^2 = c^3$, $c^2 = (3\,2\,1)$. De plus :

$$c \circ t = (1\,2\,3)(1\,2) = (1\,3) = (1\,2)(3\,2\,1) = t \circ c^2$$
$$t \circ c = (1\,2)(1\,2\,3) = (2\,3) = (3\,2\,1)(1\,2) = c^2 \circ t$$

donc $\mathcal{S}_3 = \{\mathrm{id}, \mathrm{c}, \mathrm{c}^2, \mathrm{t}, \mathrm{c} \circ \mathrm{t}, \mathrm{c}^2 \circ \mathrm{t}\}$ est le groupe diédral. Les seuls commutateurs éventuellement non triviaux sont $[c,t]$, $[c^2,t]$, $[c, c\circ t]$,$[c^2, c\circ t]$, $[c\circ t, t]$ et leurs inverses.

$$[c,t] = [c\circ t, t] = c^2 \qquad [c^2,t] = [c, c\circ t] = [c^2, c\circ t] = c$$

donc $[\mathcal{S}_3, \mathcal{S}_3] = \langle c \rangle$.

2. On suppose $n \geqslant 4$.

   (a) On rappelle que les transpositions forment un système de générateurs de $\mathcal{S}_n$: on procède par récurrence sur n. C'est évident pour $n = 2$. Soit $\sigma \in \mathcal{S}_n$.
   — Si σ fixe n, on peut la voir comme une permutation dans $\mathcal{S}_{n-1}$ et on applique l'hypothèse de récurrence.
   — Si $\sigma(n) = k \neq n$ alors $(k\,n)\sigma = \sigma'$ fixe n. On applique l'hypothèse de récurrence à σ' et on remarque que $\sigma = (k\,n)\sigma'$.
   Ce qui montre l'hérédité de la proposition. Ainsi cette proposition est vraie pour tout $n \geqslant 2$.

   En outre si p et q sont deux entiers distincts de $[\![1; n]\!]$, alors $(1\,p)(1\,q)(1\,p) = (p\,q)$ donc $\mathcal{S}_n$ est engendrée par les transpositions $(1\,k)$ $k \in [\![2; n]\!]$.

   D'autre part pour p dans $[\![1; n-1]\!]$,

$$(1\,p+1) = (1\,2)(2\,3)\dots(p-1\,p)(p\,p+1)(p-1\,p)(p-2\,p-1)\cdots(2\,3)(1\,2)$$

   (récurrence sur p) donc les transpositions $(p\,p+1)$ engendrent $\mathcal{S}_n$.

   Enfin, $(p\,p+1) = c^{p-1} \circ t \circ c^{-p+1}$ donc c et t engendrent $\mathcal{S}_n$.

   (b) $[c,t] = c\circ t \circ c^{-1} \circ t = (2\,3)(1\,2) = (1\,2\,3)$ et $[t,c] = [c,t]^{-1} = (1\,2\,3)^2 = (3\,2\,1)$ donc

$$H = \langle (1\,2\,3) \rangle = \{\mathrm{id}, (1\,2\,3), (3\,2\,1)\} \quad \text{sous-groupe isomorphe à } \mathbb{Z}/3\mathbb{Z}.$$

   (c) On peut remarquer que $(1\,2\,4) \notin H$ et pourtant $(1\,2\,4) = (4\,2\,1)^2 = (4\,2)(2\,1)(4\,2)(2\,1) \in [\mathcal{S}_n, \mathcal{S}_n]$. Précisément, le sous-groupe dérivé de $\mathcal{S}_n$ est $\mathcal{A}_n$ (sous-groupe des permutations de signature 1, engendré par les 3-cycles) qui est d'ordre $\frac{n!}{2} \neq 3$.