EPFL Automne 2024
Algebre Lineaire Avancee, MATH-110

Corrections Série 4

Exercice 1. 1. Le groupe $\mathfrak{S}_2$ ne possede que l'identite et la permutation qui echange 1 et 2, on peut les representer respectivement par

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Et ce groupe est commutatif car

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

2. On peut representer les elements de $\mathfrak{S}_3$ par

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Et ce groupe n'est pas commutatif car

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

3. On calcule

$$\tau \circ \theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

$$\theta \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\theta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\theta^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

On remarque aussi que

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Ainsi

$$\theta^n = \begin{cases} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} & \text{if } n = 3k+1,\ k \in \mathbb{Z} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} & \text{if } n = 3k+2,\ k \in \mathbb{Z} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \text{if } n = 3k,\ k \in \mathbb{Z} \end{cases}$$

Et

$$\tau^n = \begin{cases} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} & \text{if } n = 2k+1,\ k \in \mathbb{Z} \\ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \text{if } n = 2k,\ k \in \mathbb{Z} \end{cases}$$

4. Les elements de $\mathfrak{S}_{4,3}$ sont donnes par

$$\mathfrak{S}_{4,3} = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \right\}$$

Et on remarque que

$$\mathfrak{S}_{4,3} = \left\{ Id, \tau, \theta, \theta^2, \tau \circ \theta, \theta \circ \tau \right\}$$

Ainsi si on montre que $\mathfrak{S}_{4,3}$ est un sous-groupe de $\mathfrak{S}_4$, alors c'est le groupe engendre par θ et τ. Montrons alors que c'est un sous-groupe, il faut verifier les 3 points de la definition d'un sous groupe

- On a que $Id \in \mathfrak{S}_{4,3}$.
- Soient $\sigma, \sigma' \in \mathfrak{S}_{4,3}$, on a alors $\sigma(3) = \sigma'(3) = 3$, ainsi $\sigma \circ \sigma'(3) = \sigma(3) = 3$, donc $\sigma \circ \sigma' \in \mathfrak{S}_{4,3}$.
- Soit $\sigma \in \mathfrak{S}_{4,3}$, on a que $\sigma(3) = 3$, ainsi $\sigma^{-1}(3) = \sigma^{-1} \circ \sigma(3) = Id(3) = 3$, donc $\sigma^{-1} \in \mathfrak{S}_{4,3}$.

Donc $\mathfrak{S}_{4,3}$ est un sous-groupe de $\mathfrak{S}_4$.

Exercice 2. On doit verifier les 3 points de la definition d'un sous groupe

- On a par definition que $e_G.g = g = g.e_G$ pour tout $g \in G$, ainsi $e_G \in Z(G)$.
- Soient $z, z' \in Z(G)$, on a alors $z.z'.g = z.g.z' = g.z.z'$ pour tout $g \in G$, ainsi $z.z' \in Z(G)$.
- Soit $z \in Z(G)$, on a alors pour tout $g \in G$ que $z.g = g.z$, en multipliant par z^{-1} a gauche on obtient $g = z^{-1}.g.z$, et en multipliant par z^{-1} a droite on obtient $g.z^{-1} = z^{-1}.g$, ainsi $z^{-1} \in Z(G)$.

Donc $Z(G)$ est un sous-groupe de G.

Exercice 3. De nouveau, on doit verifier les 3 points de la definition d'un sous groupe

- On a que $Id(x_0) = x_0$ donc $Id \in \mathfrak{S}_{X,x_0}$.
- Soient $\sigma, \sigma' \in \mathfrak{S}_{X,x_0}$, on a alors $\sigma(x_0) = \sigma'(x_0) = x_0$, ainsi $\sigma \circ \sigma'(x_0) = \sigma(x_0) = x_0$, donc $\sigma \circ \sigma' \in \mathfrak{S}_{X,x_0}$.
- Soit $\sigma \in \mathfrak{S}_{X,x_0}$, on a que $\sigma(x_0) = x_0$, ainsi $\sigma^{-1}(x_0) = \sigma^{-1} \circ \sigma(x_0) = Id(x_0) = x_0$, donc $\sigma^{-1} \in \mathfrak{S}_{X,x_0}$.

Donc $\mathfrak{S}_{X,x_0}$ est un sous-groupe de $\mathfrak{S}_X$.

Exercice 4. Par definition du sous-groupe engendre par un sous-ensemble, il est clair que pour $C \subset D \subset G$, on a $\langle C \rangle \subset \langle D \rangle$. Ainsi on a que $\langle A \rangle \subset \langle \langle B \rangle \rangle$. Mais puisque $\langle B \rangle$ est un groupe, on a que $\langle \langle B \rangle \rangle = \langle B \rangle$. Donc

$$\langle A \rangle = G \subset \langle B \rangle \subset G$$

Et ainsi

$$\langle B \rangle = G$$

Exercice 5.

1. On a que $3 - 2 = 1 \in \langle 2, 3 \rangle$, et de plus il est clair que $\langle 1 \rangle = \mathbb{Z}$, donc grace a l'exercice 4 on en deduit que $\langle 2, 3 \rangle = \mathbb{Z}$.
2. De la meme maniere, $73 - 24.3 = 73 - 72 = 1 \in \langle 3, 73 \rangle$, donc grace a l'exercice 4 on en deduit que $\langle 3, 73 \rangle = \mathbb{Z}$
3. Tout d'abord, soit $\alpha \in \langle m, n \rangle$, on peut l'ecrire sous la forme $\alpha = xm + yn$ avec $x, y \in \mathbb{Z}$. Par definition $pgcd(m, n)$ divise m et n, donc il divise α et ainsi $\langle m, n \rangle$ est un sous-groupe de $pgcd(m, n).\mathbb{Z}$. De plus par le theoreme de Bezout il existe $x, y \in \mathbb{Z}$ tels que $xm + yn = pgcd(m, n) \in \langle m, n \rangle$. Ainsi en utilisant l'exercice 4 avec $G = pgcd(m, n).\mathbb{Z}$, $A = \{pgcd(m, n)\}$ et $B = \{m, n\}$ on obtient que $\langle m, n \rangle = pgcd(m, n).\mathbb{Z}$.

Exercice 6. Etendre la notation de l'exercice aux cas suivants : si $n = 0$ on pose $n.(x, y) = (0, 0)$, si $n < 0$ on pose $n.(x, y) = (-n).(-x, -y) = (-x, -y) + \cdots + (-x, -y)$ pour $|n|$-fois.

1. Avec la notation de l'exercise on a :

$$(n, m) = n.(1, 0) + m.(0, 1).$$

Dans tous les cas, c'est un element de $\langle \{(1, 0), (0, 1)\} \rangle$. Et alors $\mathbb{Z}^2 = \langle \{(1, 0), (0, 1)\} \rangle$.

2. Pour $x = 0 = y$ on a, comme φ est un morphisme des groupes, que $\varphi((0,0)) = 1 = h_1^0 h_2^0$. Par induction on peut montrer que pour des entiers positifs x, y on a $\varphi(x.(1,0)) = \varphi((1,0))^x = h_1^x$ et $\varphi(y.(0,1)) = h_2^y$. Pour un entier *negatif* x (resp. y), comme $x.(1,0)$ (resp. $y.(0,1)$) est l'inverse de $(-x,0)$ (resp. $((0,-y))$ on a $\varphi(x.(1,0)) = \varphi(-x,0))^{-1} = (h_1^{-x})^{-1} = h_1^x$ (resp. $\varphi(y.(0,1)) = h_2^y$). En conclusion

$$\varphi(x,y) = \varphi(x.(1,0) + y.(0,1)) = \varphi(x.(1,0)) \star \varphi(y.(0,1)) = h_1^x \star h_2^y.$$

3. On veut montrer que $(1,0)$ et $(0,1)$ sont contenus dans $\mathbb{Z}.(a,b) + \mathbb{Z}.(c,d)$, i.e. on doit trouver $n_1, m_1, n_2, m_2 \in \mathbb{Z}$ t.q.

$$m_1(a,b) + n_1(c,d) = (1,0),\ m_2(a,b) + n_2(c,d) = (0,1).$$

Si $ad - bc = 1$ on a que $m_1 = d, n_1 = -b$ et $m_2 = -c, n_2 = a$ est une solutione. Si $ad - bc = -1$ en peut choisir $m_1 = -d, n_1 = b$ et $m_2 = c, n_2 = -a$. Dans tous le cas on a que $(1,0), (0,1) \in \{\{(a,b),(c,d)\}\}$. Nous pouvons maintenant utiliser l'exercice 4 et le point (1) pour conclure.

4. Premierement, observons que $(1,0) \wedge (0,1) = 1$. Montrons que $1 \notin H \wedge H$. Cela nous permettra de conclure, parce que l'image de $H \times H$ par l'application $\wedge$ ne contient pas 1, donc H ne peut pas etre egal a $\mathbb{Z}^2$, parce que l'image de $\mathbb{Z}^2 \times \mathbb{Z}^2$ par $\wedge$ le contient. Prenons deux elements quelconques $n_1.(a,b)+m_1.(c,d), n_2.(a,b)+m_2.(c,d) \in H$ et calculons $(n_1.(a,b)+m_1.(c,d)) \wedge (n_2.(a,b) + m_2.(c,d)) = (n_1a + m_1c, n_1b + m_1d) \wedge (n_2a + m_2c, n_2b + m_2d) = (n_1a+m_1c)(n_2b+m_2d) - (n_1b+m_1d)(n_2a+m_2c) = n_1n_2ab+m_1m_2cd+n_1m_2ad+ m_1n_2bc + -n_1n_2ab - m_1m_2cd - n_1m_2bc - n_2m_1ad = (ad - bc)(n_1m_2 - m_1n_2)$. Clairement, ceci est divisible par $ad - bc$ et comme $ad - bc \neq 1$, ce resultat ne peut jamais etre egal a 1, ce qu'il fallait demontrer.

Exercice 7. 1. Soit $K = \{a \in G : \varphi(a) = \psi(a)\}$. Montrons que K est un sous-groupe de G en utilisant le critere de sous-groupe : soit $a, b \in K$ et montrons que $ab^{-1} \in K$. On a $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = \psi(a)\psi(b)^{-1} = \psi(a)\psi(b^{-1}) = \psi(ab^{-1})$, donc on a bien $ab^{-1} \in K$. Par hypothese, $A \subset K$, mais $< A >= G$ et donc on conclut par l'exercice 4 que $K = G$, ce qu'il fallait demontrer.

Exercice 8.

1. Pour $h, k \in G$ quelconques, on a $\mathrm{Ad}_g(hk) = ghkg^{-1} = ghe_Gkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1}) = \mathrm{Ad}_g(h)\mathrm{Ad}_g(k)$.

2. On observe que $\mathrm{Ad}_g \circ \mathrm{Ad}_{g^{-1}}(h) = h$, quelque soit $h \in G$. De maniere similaire, on a $\mathrm{Ad}_{g^{-1}} \circ \mathrm{Ad}_g(h) = h$, quelque soit $h \in G$. On a donc que $\mathrm{Ad}_g \circ \mathrm{Ad}_{g^{-1}} = Id_G$ et $\mathrm{Ad}_{g^{-1}} \circ \mathrm{Ad}_g = Id_G$, ce qui nous permet de deduire que Ad_g est surjectif et injectif, respectivement. Ad_g est donc une bijection.

Exercice 9.

1. On suppose que G est commutatif. Soit $g, h \in G$. Alors :
$$[g,h] = g \cdot h \cdot g^{-1} \cdot h^{-1} = g \cdot g^{-1} \cdot h \cdot h^{-1} = e_G \cdot e_G = e_G$$
donc $D(G) =< e_G >= \{e_G\}$.
2. Soit $k, g, h \in G$ quelconques. Alors :
$$\begin{aligned} Ad_k([g,h]) = k \cdot [g,h] \cdot k^{-1} = k \cdot g \cdot h \cdot g^{-1} \cdot h^{-1} \cdot k^{-1} = \\ = k \cdot g \cdot k^{-1} \cdot k \cdot h \cdot k^{-1} \cdot k \cdot g^{-1} \cdot k^{-1} \cdot k \cdot h^{-1} \cdot k^{-1} = \\ = (k \cdot g \cdot k^{-1}) \cdot (k \cdot h \cdot k^{-1}) \cdot (k \cdot g^{-1} \cdot k^{-1}) \cdot (k \cdot h^{-1} \cdot k^{-1}) = \\ = Ad_k(g) \cdot Ad_k(h) \cdot Ad_k(g)^{-1} \cdot Ad_k(h)^{-1} = [Ad_k(g), Ad_k(h)] \end{aligned}$$
ou on a utilise que $Ad_k(g^{-1}) = Ad_k(g)^{-1}$, puisque Ad_k est un homomorphisme de groupes.
3. Soit $k, g, h \in G$ quelconques. Il s'agit de montrer que $Ad_k(D(G)) = D(G)$. Par le 2), on sait que $Ad_k([g,h]) = [Ad_k(g), Ad_k(h)]$. Soit $d \in D(G)$, tel que $d = [g_1, h_1] \cdot \cdots \cdot [g_n, h_n]$ pour un $n \in \mathbb{N}$, $n \geqslant 1, g_i, h_i \in G \ \forall i \in 1, ..., n$. Alors $Ad_k([d]) = Ad_k([g_1, h_1]) \cdot \cdots \cdot Ad_k[g_n, h_n] = [Ad_k(g_1), Ad_k(h_1)] \cdot \cdots \cdot [Ad_k(g_n), Ad_k(h_n)] \in D(G)$ donc $Ad_k(D(G)) \subseteq D(G)$.

   D'un autre cote, on a
$$[g,h] = (\mathrm{Ad}_k \circ \mathrm{Ad}_{k^{-1}})[g,h] = \mathrm{Ad}_k\big([\mathrm{Ad}_{k^{-1}}(g), \mathrm{Ad}_{k^{-1}}(h)]\big) \in \mathrm{Ad}_k\big(D(G)\big).$$
   Donc
$$\{[g,h] : g, h \in G\} \subset \mathrm{Ad}_k\big(D(G)\big).$$
   En utilisant la minimalite du sous-groupe engendre par un sous-ensemble, on deduit $D(G) \subseteq \mathrm{Ad}_k\big(D(G)\big)$, ce qui nous permet de conclure.
4. Il s'agit de montrer que $D(G) \subseteq ker(\varphi)$. Soit $g, h \in G$ quelconques. On souhaite montrer que $\varphi(g.h.g^{-1}.h^{-1}) = e_Z$. Utilisant que Z est commutatif, on obtient
$$\begin{aligned} \varphi(g.h.g^{-1}.h^{-1}) = \varphi(g).\varphi(h).\varphi(g)^{-1}.\varphi(h)^{-1} \\ = \varphi(g).\varphi(g)^{-1}.\varphi(h).\varphi(h)^{-1} = e_Z. \end{aligned}$$
   Donc on a montre que
$$\{[g,h] : g, h \in G\} \subset \ker(\varphi).$$
   Comme $\ker(\varphi)$ est un sous-groupe, la minimalite du groupe engendre par un sous-ensemble implique que $D(G) \subseteq \ker(\varphi)$.