EPFL Automne 2024
Algebre Lineaire Avancee, MATH-110

Série 5

Exercice 1. 1. Si $\varphi^{(-1)}(\{h\})$ est vide, alors nous n'avons rien faire, supposons donc qu'il existe $g_0 \in G$ tel que $\varphi(g_0) = h$ c'est a dire : $g_0 \in \varphi^{(-1)}(\{h\})$ et montrons que

$$\varphi^{(-1)}(\{h\}) = g_0 \star \ker(\varphi)$$

— Tout d'abord on observe que $\forall g \in g_0 \star \ker(\varphi)$, il existe un $k \in \ker(\varphi)$ tel que $g = g_0 \star k$, ainsi en utilisant le fait que φ est un morphisme de groupe, on obtient :

$$\varphi(g) = \phi(g_0 \star k) = \phi(g_0) \cdot \varphi(k) = h \cdot e_H = h$$

Donc $g \in \varphi^{(-1)}(\{h\})$ et par consequent $\varphi^{(-1)}(\{h\}) \supseteq g_0 \star \ker(\varphi)$.

— Maintenant prenons $g \in \varphi^{(-1)}(\{h\})$, on peut ecrire $g = e_g \star g = g_0 \star g_0^{(-1)} \star g$ et on voit que $g_0^{(-1)} \star g$ appartient a $\ker \varphi$, en effet :

$$\varphi(g_0^{(-1)} \star g) = \varphi(g_0^{(-1)}) \cdot \varphi(g) = \varphi(g_0)^{(-1)} \cdot \varphi(g) = h^{(-1)} \cdot h = e_H$$

Donc $g = g_0 \star g_0^{(-1)} \star g$ est bien un element de $g_0 \star \ker(\varphi)$, ainsi $\varphi^{(-1)}(\{h\}) \subseteq g_0 \star \ker(\varphi)$

Par double inclusion, on a bien montre que $\varphi^{(-1)}(\{h\}) = g_0 \star \ker(\varphi)$.

2. — Tout d'abord on observe que $\forall g \in \ker(\varphi) \star g_0$, il existe un $k \in \ker(\varphi)$ tel que $g = k \star g_0$, on retrouve ainsi :

$$\varphi(g) = \phi(k) \cdot \varphi(g_0) = h \cdot e_H = h$$

Donc $g \in \varphi^{(-1)}(\{h\})$ et par consequent $\varphi^{(-1)}(\{h\}) \supseteq \ker(\varphi) \star g_0$.

— Maintenant prenons $g \in \varphi^{(-1)}(\{h\})$,cette fois-ci en ecrivant $g = g \star g_0^{(-1)} \star g_0$ on a egalement :

$$\varphi(g \star g_0^{(-1)}) = \varphi(g) \cdot \varphi(g_0^{(-1)}) = h \cdot h^{(-1)} = e_H$$

Donc g est bien un element de $\ker(\varphi) \star g_0$, ainsi $\varphi^{(-1)}(\{h\}) \subseteq \ker(\varphi) \star g_0$

Par double inclusion, on a bien montre que $\varphi^{(-1)}(\{h\}) = \ker(\varphi) \star g_0$.

3. On a montre au point 1. et 2. que si $g_0 \in \varphi^{(-1)}(\{h\})$ alors on a bien que :

$$\varphi^{-1}(\{h\}) = g_0 \star \ker(\varphi) = \varphi^{-1}(\{h\}) = \ker(\varphi) \star g_0$$

Maintenant, si $g_0 \notin \varphi^{(-1)}(\{h\})$, alors il existe un $h' \in H$ tel que $\varphi(g_0) = h' \neq h$. Si on considere $g = g_0 \star e_G \in g_0 \star \ker\varphi$ (car e_G est toujours un element du ker) on a que $g = g_0 \notin \varphi^{(-1)}(\{h\})$ donc les egalite precedantes ne sont pas respectees. Ainsi l'ensemble de tous les $g_0 \in G$ respectant les proprietes demandees est $\varphi^{(-1)}(\{h\})$.

Action de groupes

Soit X un ensemble, G un groupe et soit $G \curvearrowright X$ une action a gauche de G sur X. On representera (comme on prefere) cette action, soit sous la forme d'un morphisme

$$\varphi : G \mapsto \mathrm{Bij}(X),$$

soit sous la forme d'une loi de composition externe

$$\odot : (g, x) \in G \times X \mapsto g \odot x \in X$$

verifiant les proprietes convenables.

Exercice 2. Soit $x \in X$, la G-orbite de x est le sous-ensemble des transformes de x par les elements de G :

$$G \odot x = \{g \odot x,\ g \in G\} \subset X.$$

On dit que x' est dans la G-orbite de x ssi

$$\text{il existe } g \in G, \text{ tel que } x' = g \odot x (= \varphi(g)(x))$$

ou en d'autre termes ssi

$$x' \in = G \odot x\ (= \varphi(G)(x)).$$

On note cette relation

$$x' \sim_G x$$

1. On note par $\mathcal{R} \subset X \times X$ la relation

$$\mathcal{R} = \{(x, x') \in X \times X : \exists g \in G\, x' = \varphi(g)(x)\}.$$

et on verifie que c'est bien une relation d' equivalence :

— Reflexivité : Soit $x \in X$. Comme $\varphi : G \to \mathrm{Bij}(X)$ est un morphisme, on a $\varphi(e_G) = \mathrm{Id}_X$, Donc

$$x = \mathrm{Id}_X(x) = \varphi(e_G)(x)$$

et donc $(x, x) \in \mathcal{R}$.

— Symmetrie : Soit $(x, x') \in \mathcal{R}$. Donc il existe par définition $g \in G$ tel que $x' = \varphi(g)(x)$. Par conséquent

$$\begin{aligned} x = \varphi(e_G)(x) = \varphi(g^{-1}g)(x) &= \big(\varphi(g^{-1}) \circ \varphi(g)\big)(x) \\ &= \varphi(g^{-1})\big(\varphi(g)(x)\big) = \varphi(g^{-1})(x') \end{aligned}$$

et donc $(x', x) \in \mathcal{R}$.

— Transitivité : Soit $(x, x'), (x', x'') \in \mathcal{R}$. Par conséquent il existe $g, g' \in G$ tel que $x' = \varphi(g)(x)$ et $x'' = \varphi(g')(x')$. On déduit

$$\begin{aligned} x'' = \varphi(g')(x') = \varphi(g')\big(\varphi(g)(x)\big) &= \big(\varphi(g') \circ \varphi(g)\big)(x) \\ &= \varphi(g'g)(x). \end{aligned}$$

Ainsi $\mathcal{R}$ est bien une relation d' equivalence.

2. Soit $x \in X$, on va montrer que $G_x = \{g \in G,\ \varphi(g)(x) = g \odot x = x\} \subset G$ est un sous-groupe de G :

— D'abord, on voit que G_x n'est pas vide, en effet, $e_G \in G_x$ car $\forall y \in X$, on a $\varphi(e_G)(y) = \mathrm{Id}_X(y) = y$ en particulier$\varphi(g)(x) = x$.

— Soient $g, h \in G_x$ alors :

$$\varphi(g \star h)(x) = \varphi(g) \circ \varphi(h)(x) = \varphi(g)(x) = x$$

Donc $g \star h \in G_x$. (On a utilise dans la premiere egalite le fait que φ est un morphisme, dans la deuxieme, le fait que $h \in G_x$ et dans la derniere le fait que $g \in G_x$.)

— Soit $g \in G_x$, alors comme $\varphi(g) \in \mathrm{Bij}(X)$ et que φ est un morphisme , on a que $\varphi(g^{(-1)}) \circ \varphi(g) = \varphi(g)^{(-1)}\varphi(g) = \mathrm{Id}_X$, ainsi :

$$\varphi(g^{(-1)})(x) = \varphi(g^{(-1)})\varphi(g)(x) = \mathrm{Id}_X(x) = x$$

Donc $g^{(-1)} \in G_x$.

Ainsi on a montre que G_x est bien un sous groupe de G.

3. Soient $x, x' \in X$ tel que $x, x' \in G \odot y$, ainsi, comme R est une relation d'equivalence, on peut supposer sans perte de generalite que $x' \in G \odot x$ ainsi, il existe $g \in G$ tel que $x' = \varphi(g)(x) = g \odot x$.

— Soit $h \in G_{x'}$, i-e $\varphi(h)(x') = x'$, alors on peut ecrire $h = g \star g^{(-1)} \star h \star g \star g^{(-1)}$, montrons que $g' = g^{(-1)} \star h \star g \in G_x$, ainsi on aura $h = g \star g' \star g^{(-1)} \in g \star G_x \star g^{(-1)}$:

$$\varphi(g^{(-1)} \star h \star g)(x) = \varphi(g^{(-1)}) \circ \varphi(h) \circ \varphi(g)(x) = \varphi(g^{(-1)}) \circ \varphi(h)(x') = \varphi(g^{(-1)})(x') = x$$

On a donc bien que $g' = g^{(-1)} \star h \star g \in G_x$. (La derniere egalite viens du fait que $\varphi(g)$ est une bijection tel que $\varphi(g)(x) = x'$, ainsi comme $\varphi(g^{(-1)}) = \varphi(g)^{(-1)}$ est son inverse, on a bien que $\varphi(g^{(-1)})(x') = x$.)
On vient de montrer que $G_{x'} \subseteq g \star G_x \star g^{(-1)}$.

— Soit $h = g \star h' \star g^{(-1)} \in g \star G_x \star g^{(-1)}$, i-e $h' \in G_x$, montrons que $h \in G_{x'}$:

$$\varphi(h)(x') = \varphi(g) \circ \varphi(h') \circ \varphi(g^{(-1)}(x') = \varphi(g) \circ \varphi(h')(x) = \varphi(g)(x) = x'$$

Ainsi on a On vient de montrer que $G_{x'} \supseteq g \star G_x \star g^{(-1)}$.

Par double inclusion on a bien que $G_{x'} = g \star G_x \star g^{(-1)}$.

4. On ecrit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix}$$

Calculons donc l'orde σ :

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}$$
$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 6 & 5 & 4 & 2 \end{pmatrix}$$
$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 6 & 5 & 4 & 2 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}$$
$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 6 & 3 & 4 & 2 \end{pmatrix}$$

$$\sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 6 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 6 & 3 & 4 & 2 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \mathrm{Id}$$

Ainsi $n_\sigma = 6$.

5. On remarque que l'on peut decomposer σ en trois cycles $\sigma_1, \sigma_2, \sigma_3$ tel que si on ecrit $D_i = \{x \in X; \sigma_i(x) \neq x\}$ pour $i = 1, 2, 3$ alors on a que D_1, D_2 et D_3 sont deux a deux disjoints, en effet :

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 3 & 4 & 5 & 6 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

Ainsi on peut facilement voir que

$$G(1) = G(3) = G(5) = \{\sigma^n(1); n = 1, ..., 5\} = \{1, 3, 5\}$$
$$G(2) = G(7) = \{\sigma^n(2); n = 1, ..., 5\} = \{2, 7\}$$
$$G(4) = G(6) = \{\sigma^n(4); n = 1, ..., 5\} = \{4, 6\}$$

Ou $G(i)$ avec $i \in X$ est l'orbite de i. Cela nous donne donc la decomposition suivante de $X = G(1) \sqcup G(2) \sqcup G(4)$

6. En reprenant nos calcul de la question 4, on trouve que

$$G_1 = G_3 = G_5 = \{\mathrm{Id}, \sigma^3\}$$
$$G_2 = G_7 = \{\mathrm{Id}, \sigma^2, \sigma^4\}$$
$$G_4 = G_6 = \{\mathrm{Id}, \sigma^2, \sigma^4\}$$

Ainsi on a $n_1 = 2$ et $n_2 = n_4 = 3$ ou n_i est l'ordre de G_i, $i = 1, 2, ..., 7$.

Exercice 3. 1. On commence par montrer que $t_\bullet$ est bien definie c'est a dire que pour tout $g \in G$ l'application t_g est bien une bijection. Soit $h_1, h_2 \in G$ tel que $t_g(h_1) = t_g(h_2)$. Alors on a

$$h_1 = g^{(-1)}.g.h_1 = g^{-1}.t_g(h_1) = g^{-1}.t_g(h_2) = g^{-1}.g.h_2 = h_2,$$

ce qui montre l'injectivité de t_g.

Soit $h \in G$ arbitraire. Donc

$$h = g.(g^{-1}.h) = t_g(g^{-1}.h)$$

ce qui montre la surjectivité de t_g.

Comme $g \in G$ ést arbitraire, on en déduit que pour tout $g \in G$ l'application t_g est une bijection. Montrons maintenant que $t_\bullet$ est un morphisme de groupe : Soient $g, h, \in G$. On veut montrer que e $t_{g.h} = t_g \circ t_h$. Pour cela, on considere $x \in G$ quelconque et grâce à l'associativité de la composition interne dans G, on a :

$$t_{g.h}(x) = (g.h).x = g.(h.x) = t_g(h.x) = t_g\big(t_h(x)\big) = (t_g \circ t_h)(x).$$

Comme $x \in G$ ést arbitraire, on en déduit que $t_{g.h} = t_g \circ t_h$. On en déduit que $t_\bullet$ est un morphisme.

2. Soit $g \in G$ tel que $t_g = \mathrm{Id}_G$. Donc

$$g = g.e_G = t_g(e_G) = \mathrm{Id}(e_G) = e_G$$

Donc on a montré que $\ker(t_\bullet) \subset \{e_G\}$. Comme $t_\bullet$ est un morphisme, sait que $t_{e_G} = \mathrm{Id}_G$ et on déduit que $\ker(t_\bullet) = \{e_G\}$ et donc que $t_\bullet$ est bien injectif.

Exercice 4. On rappelle que si $\psi : G \to H$ et $\psi' : H \to K$ deux morphismes de groupes bijectif , alors $\psi^{(-1)} : H \to G$ et $\psi' \circ \psi : G \to K$ sont aussi des morphismes de groupes bijectifs.

1. Montrons que $\simeq$ est une relation d'equivalence :
   (a) Reflexivite : Pour un groupe G on a $G \simeq G$ en considerant l'isomorphisme $\mathrm{Id}_G : G \to G$.
   (b) Symetrie : Soient G, H deux groupes tel que $G \simeq H$ donc il existe $\psi : G \to H$ un isomorphisme, comme ψ est un isomorphisme, on peut considerer $\psi^{(-1)} : H \to G$ qui est aussi un isomorphisme et ainsi, on a bien $H \simeq G$.
   (c) Transitivite : Soient G, H, K trois groupes, tel que $G \simeq H$ et $H \simeq K$ via $\psi : G \to H$ et $\psi' : H \to K$ respectivement, alors comme $\psi' \circ \psi : G \to K$ est aussi un isomorphisme, on a bien $G \simeq K$.
2. On pose :

$$\begin{array}{rcl} \theta : \mathrm{Aut}_{Gr}(G) \to \mathrm{Bij}(\mathrm{Isom}_{Gr}(G,H)) & & \\ \varphi \longmapsto & \theta_\varphi : \mathrm{Isom}_{Gr}(G,H) & \to \mathrm{Isom}_{Gr}(G,H) \\ & \psi & \mapsto \theta_\varphi = \psi \circ \varphi \end{array}$$

   Et on verifie que cela definie une action a droite :
   (a) Neutralite : Pour tout $\psi \in \mathrm{Isom}_{Gr}(G,H)$, on a bien $\theta_{\mathrm{Id}_G}(\phi) = \phi \circ \mathrm{Id}_G = \psi$

(b) Associativite : Soient $\varphi_1, \varphi_2 \in \mathrm{Aut}_{Gr}(G)$, et $\psi \in \mathrm{Isom}_{Gr}(G,H)$, on a bien :

$$\theta_{\varphi_1 \circ \varphi_2}(\psi) = \psi \circ \varphi_1 \circ \varphi_2 = \theta_{\varphi_2}(\psi \circ \varphi_1) = \theta_{\varphi_2} \circ \theta_{\varphi_1}(\psi)$$

(c) Simplification : Soient $\varphi \in \mathrm{Aut}_{Gr}(G)$, et $\psi \in \mathrm{Isom}_{Gr}(G,H)$, on a bien :

$$\theta_{\varphi}(\theta_{\varphi^{(-1)}}(\psi)) = \psi \circ \varphi^{(-1)} \circ \varphi = \psi = \psi \circ \varphi \circ \varphi^{(-1)} = \theta_{\varphi^{(-1)}}(\theta_{\varphi}(\psi))$$

C'est donc bien une action a droite.
On observe que pour G un groupe et X un ensemble tel que $\alpha : G \to \mathrm{Bij}(X)$ est une action a droite de G sur X, alors si on definie $\alpha^{(-1)}$ comme suivant :

$$\begin{array}{lll} \alpha^{(-1)} : G \to & & \mathrm{Bij}(X) \\ \quad g \longmapsto \alpha^{(-1)}(g) : & & X \to X \\ & & \quad x \mapsto \alpha^{(-1)}(g)(x) = \alpha(g^{(-1)})(x) \end{array}$$

Alors $\alpha^{(-1)}$ est une action a gauche de G sur X, en effet :

(a) Neutralite : Pour tout $x \in X$: $\alpha^{(-1)}(e_G)(x) = \alpha(e_G^{(-1)})(x) = \alpha(e_G)(x) = x$.

(b) Associativite : Soient $g, g' \in G$ et $x \in X$, alors en utilisant le fait que α est une action a droite, on obtient :

$$\alpha^{(-1)}(g.g')(x) = \alpha((g.g')^{(-1)})(x) = \alpha((g')^{(-1)}.g^{(-1)})(x) =$$

$$\alpha(g^{(-1)}) \circ \alpha((g')^{(-1)})(x) =$$

$$\alpha^{(-1)}(g) \circ \alpha^{(-1)}(g')(x)$$

(c) Simplification : Soient $g, \in G$ et $x \in X$, alors en utilisant le fait que α est une action a droite, on obtient facilement que la simplification est aussi satisfaite !

On peut aussi montrer que si α est une action a gauche, alors $\alpha^{(-1)}$ est une action a droite. Ainsi dans notre cas, $\theta^{(-1)}$ est une action a gauche de $\mathrm{Aut}_{Gr}(G)$ sur $\mathrm{Isom}_{Gr}(G,H)$. Cette action est definie pour tout $\varphi \in \mathrm{Aut}_{Gr}(G)$, et $\psi \in \mathrm{Isom}_{Gr}(G,H)$ comme $\theta^{(-1)}(\varphi)(\psi) = \psi \circ \varphi^{(-1)}$.

3. On pose :

$$\begin{array}{lll} \theta : \mathrm{Aut}_{Gr}(H) \to \mathrm{Bij}(\mathrm{Isom}_{Gr}(G,H)) & & \\ \quad \varphi \longmapsto & \theta_\varphi : \mathrm{Isom}_{Gr}(G,H) & \to \mathrm{Isom}_{Gr}(G,H) \\ & \quad \psi & \mapsto \theta_\varphi = \varphi \circ \psi \end{array}$$

et

$$\begin{array}{lll} \theta^{(-1)} : \mathrm{Aut}_{Gr}(H) \to \mathrm{Bij}(\mathrm{Isom}_{Gr}(G,H)) & & \\ \qquad\qquad \varphi \longmapsto & \theta_{\varphi}^{(-1)} : \mathrm{Isom}_{Gr}(G,H) & \to \mathrm{Isom}_{Gr}(G,H) \\ & \qquad\qquad \psi & \mapsto \theta_{\varphi}^{(-1)} = \varphi^{(-1)} \circ \psi \end{array}$$

On peut verifie de la meme maniere qu'au point precedant que θ est une action gauche et que par consequent $\theta^{(-1)}$ est une action a droite.

4. Soit $\psi \in \mathrm{Isom}_{Gr}(G,H)$ un isomorphisme. on va montrer que

$$\mathrm{Isom}_{Gr}(G,H) = \psi \circ \mathrm{Aut}_{Gr}(G) = \mathrm{Aut}_{Gr}(H) \circ \psi$$

En procedant par double inclusion.
D'abord, on observe que comme $\psi \in \mathrm{Isom}_{Gr}(G,H)$, alors trivialement on a que $\psi \circ \mathrm{Aut}_{Gr}(G) \subseteq \mathrm{Isom}_{Gr}(G,H)$ et $\mathrm{Aut}_{Gr}(H) \circ \psi \subseteq \mathrm{Isom}_{Gr}(G,H)$ car la composition de deux isomorphisme de groupe est toujours un isomorphisme de groupes. Ensuite nous avons :

(a) $\mathrm{Isom}_{Gr}(G,H) \subseteq \psi \circ \mathrm{Aut}_{Gr}(G)$: Soit $\phi \in \mathrm{Isom}_{Gr}(G,H)$ alors, $\phi = \psi \circ \psi^{(-1)} \circ \phi$ et on a bien $\psi^{(-1)} \circ \phi \in \mathrm{Aut}_{Gr}(G)$ donc $\phi = \psi \circ \psi^{(-1)} \circ \phi \in \psi \circ \mathrm{Aut}_{Gr}(G)$. Ce qui montre que

$$\mathrm{Isom}_{Gr}(G,H) \subseteq \psi \circ \mathrm{Aut}_{Gr}(G)$$

(b) $\mathrm{Isom}_{Gr}(G,H) \subseteq \mathrm{Aut}_{Gr}(H) \circ \psi$: Soit $\phi \in \mathrm{Isom}_{Gr}(G,H)$ alors, $\phi = \phi \circ \psi^{(-1)} \circ \psi$ et on a bien $\phi \circ \psi^{(-1)} \in \mathrm{Aut}_{Gr}(H)$ donc $\phi = \psi \circ \psi^{(-1)} \circ \phi \in \mathrm{Aut}_{Gr}(H) \circ \psi$. Ce qui montre que

$$\mathrm{Isom}_{Gr}(G,H) \subseteq \mathrm{Aut}_{Gr}(H) \circ \psi$$

Ce qui montre bien les egalites voules.

Premiers exercices sur les anneaux

Exercice 5. 1. Montrons que les seuls sous-anneaux de $\mathbb{Z}$ sont $\{0\}$ ou $\mathbb{Z}$.
Fixons A un sous-anneau non-nul de $\mathbb{Z}$. Comme, A est non nul, par definition, $1 \in A$, et donc, vu que A est un sous-groupe additif de $\mathbb{Z}$, il contient le sous-groupe genere par 1, qui est donc $\mathbb{Z}$.

2. Montrons que les seuls anneaux de $\mathbb{Z}/q\mathbb{Z}$ sont $\{0 \pmod q\}$ et $\mathbb{Z}/q\mathbb{Z}$.
Fixons A un sous-anneau non-nul de $\mathbb{Z}/q\mathbb{Z}$. Comme, A est non nul, par definition, $1 \pmod q \in A$, et donc, vu que A est un sous-groupe additif de $\mathbb{Z}/q\mathbb{Z}$, il contient le sous-groupe genere par $1 \pmod q$, qui est donc $\mathbb{Z}/q\mathbb{Z}$.

Exercice 6. Soit A un anneau commutatif. Soit l'ensemble

$$M_2(A) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in A\}$$

des matrices 2×2 a coefficients dans A. On muni cet ensemble des lois d'addition et de multiplication des matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix},\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

1. Verifions que $M_2(A)$ est un anneau d'element nul la matrice nulle

$$0_{2(A)} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix}$$

et d'unite la matrice identite

$$\mathrm{Id}_2 = \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}.$$

En premier on montre que $(M_2(A), +, 0_2)$ est un groupe commutatif.

— Neutralité de 0_2 : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0_A+a & 0_A+b \\ 0_A+c & 0_A+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix}$$

Ici on a utilisé la neutralité de 0_A dans A.

— Inversibilité : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. L'inverse est $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \in M_2$ car

$$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a+a & -b+b \\ -c+c & -d+d \end{pmatrix} = \begin{pmatrix} 0_A & 0_A \\ 0_A & 0_A \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

Ici on a utilisé l'inversiblilité de $+$ dans A.

— Associativité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in M_2$ arbitraire. On a

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

$$= \begin{pmatrix} (a+a')+a'' & (b+b')+b'' \\ (c+c')+c'' & (d+d')+d'' \end{pmatrix} = \begin{pmatrix} a+a'+a'' & b+b'+b'' \\ c+c'+c'' & d+d'+d'' \end{pmatrix}$$

$$= \begin{pmatrix} a+(a'+a'') & b+(b'+b'') \\ c+(c'+c'') & d+(d'+d'') \end{pmatrix} = \ldots = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right)$$

Ici on a utilisé l'associativité de $+$ dans A.

— Commutativité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix} \in M_2$. On a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} = \begin{pmatrix} a'+a & b'+b \\ c'+c & d'+d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}+\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Ici on a utilisé la commutativité de $+$ dans A.

Maintenant il reste à verifier l'associativité et la neutralité de $\times$ ainsi que la distributivité de $+$ et de $\times$ pour prouver que M_2 est un anneau.

— Neutralité de Id_2 : Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1_A a + 0_A c & 1_A b + 0_A d \\ 0_A a + 1_A c & 0_A b + 1_A d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$= \begin{pmatrix} 1_A a + 0_A b & 0_A a + 1_A b \\ 1_A c + 0_A d & 0_A c + 1_A d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1_A & 0_A \\ 0_A & 1_A \end{pmatrix}$$

Ici on a utilisé la neutralité de 1_A dans A.

— Associativité de la multiplication : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in$ M_2 arbitraire. On a

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

$$= \begin{pmatrix} (aa'+bc')a''+(ab'+bd')c'' & (aa'+bc')b''+(ab'+bd')d'' \\ (ca'+dc')a''+(cb'+dd')c'' & (ca'+dc')b''+(cb'+dd')d'' \end{pmatrix}$$

$$= \begin{pmatrix} a(a'a''+b'c'')+b(c'a''+d'c'') & a(a'b''+b'd'')+b(c'b''+d'd'') \\ c(a'a''+b'c'')+d(c'a''+d'c'') & c(a'b''+b'd'')+d(c'b''+d'd'') \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'a''+b'c'' & a'b''+b'd'' \\ c'a''+d'c'' & c'b''+d'd'' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right)$$

Ici on a utilisé l'associativité de $\times$ dans A.

— Distributivité : Soient $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}, \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \in M_2$ arbitraire. On a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'+a'' & b'+b'' \\ c'+c'' & d'+d'' \end{pmatrix}$$

$$= \begin{pmatrix} a(a'+a'')+b(c'+c'') & a(b'+b'')+b(d'+d'') \\ c(a'+a'')+d(c'+c'') & c(b'+b'')+d(d'+d'') \end{pmatrix}$$
$$= \begin{pmatrix} aa'+bc'+aa''+bc'' & ab'+bd'+ab''+bd'' \\ ca'+dc'+ca''+dc'' & cb'+dd'+cb''+dd'' \end{pmatrix}$$
$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

et de maniére similaire on obtient

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \times \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}.$$

2. Montrons que l'ensemble des matrices triangulaires superieures

$$T_{\sup,2}(A) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ a, b, d \in A\} \subset M_2(A)$$

est un sous-anneau.
On a clairement que $0, 1 \in T_{\sup,2}(A)$. Soit $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ et $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ deux matrices arbitraires dans $T_{\sup,2}(A)$. Alors $-\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} \in T_{\sup,2}(A)$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ 0 & c+z \end{pmatrix} \in T_{\sup,2}(A)$, et pour finir, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} \in T_{\sup,2}(A)$, nous permettant de conclure.

3. Pour prouver que M_2 est non commutatif dans le cas oú $0_A \neq 1_A$, il suffit de calculer

$$\begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} = \begin{pmatrix} 1_A+1_A & 1_A \\ 1_A & 1_A \end{pmatrix} \neq \begin{pmatrix} 1_A & 1_A \\ 1_A & 1_A+1_A \end{pmatrix} = \begin{pmatrix} 1_A & 0_A \\ 1_A & 1_A \end{pmatrix} \times \begin{pmatrix} 1_A & 1_A \\ 0_A & 1_A \end{pmatrix}.$$

Si $0_A = 1_A$ on a $0_2 = Id_2$ et M_2 ne posséde qu'un seul élément. Ainsi dans ce cas, M_2 est commutatif.

Exercice 7. Soit $(A, +, ., 0_A, 1_A)$ un anneau . On a dit qu'un element $a \in A$ est inversible a gauche (resp. a droite) si il existe $b \in A$ (resp. $c \in A$) tel que

$$b.a = 1_A\ (resp.\ a.c = 1_A).$$

On dit que b est un inverse a gauche (resp. c est un inverse a droite)

1. On suppose que a est inversible a gauche ET inversible a droite (avec des inverses a gauche et a droite notes respectivement b et c). Montrons qu'alors
$$b = c$$
de sorte que a est inversible au sens du cours (les inverses a droite et a gauche etant les memes). On a :
$$a.b.a = a.c.a \implies a.(b-c).a = 0 \implies b.a.(b-c).a.c = b.0.c \implies b - c = 0$$
, nous permettant de conclure.
2. On va maintenant donner un exemple d'un anneau possedant un element inversible a gauche mais qui n'est pas inversible a droite. Soit $\mathcal{F}(\mathbb{Z},\mathbb{Z})$ l'ensemble des fonctions (toutes les fonctions, par seulement les morphismes de groupes) de $\mathbb{Z}$ sur $\mathbb{Z}$. Alors avec l'addition et la *composition* des fonctions, on obtient un anneau
$$(\mathcal{F}(\mathbb{Z},\mathbb{Z}), +, \circ, \underline{0}, \mathrm{Id}_{\mathbb{Z}})$$
Remarque. Dans cet exercice la "multiplication" est la composition des fonctions pas la multiplication sur les fonctions induite par la multiplication dans $\mathbb{Z}$.

   En particulier l'anneau etudie ici est non commutatif.

   (a) On considere la fonction de doublement
   $$D : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & D(n) = 2n \end{array}$$
   Soit $[\bullet] : \mathbb{R} \mapsto \mathbb{Z}$ la fonction partie entiere ($[x]$ est le plus grand entier inferieur ou egal a x). Montrer que la fonction
   $$H := [\frac{\bullet}{2}] : n \in \mathbb{Z} \mapsto [\frac{n}{2}] \in \mathbb{Z}$$
   est un inverse a gauche de D. On rappelle que l'element neutre multiplicatif est l'identite sur $\mathbb{Z}$. Calculons donc la composition. Soit $n \in \mathbb{Z}$.
   $$H \circ D(n) = [\frac{2n}{2}] = [n] = n.$$
   Nous pouvons donc conclure.

   (b) Montrons que D n'admet pas d'inverse a droite : il n'existe pas de $H' : \mathbb{Z} \mapsto \mathbb{Z}$ telle que
   $$D \circ H' = \mathrm{Id}_{\mathbb{Z}}.$$

   Supposons par l'absurde qu'une telle fonction existe. Cela impliquerai que $D \circ H'$ est surjective, et donc, que D est surjective, or $1 \notin \mathrm{im}(D)$.
   Un autre argument aurait pu etre fait en justifiant, par unicite de l'inverse, que $H' = H$ mais que $D \circ H(1) = D(0) = 0 \neq 1$.