EPFL - Automne 2020	Prof. Z. Patakfalvi
Structures algébriques	**Solutions de l'examen final**

Indications pour les correcteurs. Nous n'attendons pas des étudiants plus de détails que dans ces solutions.

Là où il y a lieu, nous donnons plusieurs solutions possibles et plausibles.

Nous mettons en gris certains calculs qui ne sont pas nécessaires, mais qu'il peut être utile d'avoir sous les yeux lors de la correction.

Nous utilisons souvent les résultats suivants des notes de cours : 3.5.7 (théorème de Lagrange), 3.5.25.2) (1e théorème d'isomorphisme), 3.5.37, 3.8.13 et 3.8.18. Nous n'en rappelons pas l'énoncé à chaque fois.

Exercice 1.
Considérons la fonction

$$\varphi\colon \mathbb{Z} \to \mathbb{Z} \setminus \{0\}, \quad n \mapsto \begin{cases} n+1 & \text{si } n \geq 0, \\ n & \text{si } n < 0. \end{cases}$$

alors φ est une bijection, ce qui montre que $|\mathbb{Z}| = |\mathbb{Z} \setminus \{0\}|$.

Solution alternative. On a l'inclusion canonique $\mathbb{Z}\setminus\{0\} \hookrightarrow \mathbb{Z}$, et l'inclusion

$$\mathbb{Z} \hookrightarrow \mathbb{Z} \setminus \{0\}, \quad n \mapsto 3n - 1.$$

On conclut avec le théorème de Cantor-Schröder-Bernstein.

Exercice 2. 1. On a $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

2. $\langle H, F\rangle$ est le plus petit sous-groupe de G qui contient H et F. Puisqu'il est stable par multiplication, il doit contenir $HF = \{hf \mid h \in H, f \in F\}$.

   Pour prouver que $\langle H, F\rangle = HF$, il suffit donc de montrer que HF est un sous-groupe de G. On va vérifier les critères de la Proposition 3.3.2.

   (a) Il est clair que $e_G \in HF$, donc HF **est non-vide**.

   (b) Montrons que HF **est stable par multiplication**. Prenons $h, h' \in H$ et $f, f' \in F$. Il faut montrer que $hfh'f' \in HF$. Puisque $f \in F \subseteq N_G(H)$, on a $fH = Hf$. En particulier il existe $\tilde{h}$ tel que $fh' = \tilde{h}f$. Ainsi

   $$hfh'f' = h\tilde{h}ff' \in HF$$

   comme désiré.

(c) Montrons pour finir que HF **contient les inverses de ses éléments**. Prenons $h \in H, f \in F$. Il faut montrer que $f^{-1}h^{-1} \in HF$. Puisque $f^{-1} \in F$, on voit comme précédemment qu'il existe $\tilde{h} \in H$ tel que

$$f^{-1}h^{-1} = \tilde{h}f^{-1} \in HF,$$

ce qui conclut.

Solution alternative. Montrons directement que $\langle H, F\rangle \subseteq HF$. On sait par la Proposition 3.7.6 que

$$\langle H, F\rangle = \{g_1 \cdots g_r \mid g_i \in H \cup F, r \geq 0\}$$

et donc il suffit de montrer que chaque mot $g_1 \cdots g_r$ appartient à HF. On procède par induction sur r. Le cas $r = 1$ est clair. Supposons ensuite le résultat prouvé pour $r - 1$. Alors $g_2 \cdots g_r = hf \in HF$. Si $g_1 \in H$, alors $g_1 h \in H$ et l'on a terminé. Si $g_1 \in F$, alors par hypothèse $g_1 H = H g_1$, et donc il existe un $h' \in H$ tel que $g_1 h = h' g_1$. On a ainsi $g_1 hf = h' g_1 f \in HF$, ce qui conclut.

Exercice 3.
Montrons que $R_H \subset G \times G$ est une relation d'équivalence.

1. **Réflexivité**. Soit $x \in G$. Alors $x^{-1}x = e_G \in H$, donc $(x, x) \in R_H$.
2. **Symétrie.** Soient $x, y \in G$ tels que $(x, y) \in R_H$. Donc $x^{-1}y \in H$. Puisque H est un sous-groupe de G, il contient des inverses (dans G) de ses éléments. Donc

   $$(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in H.$$

   Ainsi $(y, x) \in R_H$, ce qui établit la symétrie.
3. **Transitivité.** Supposons que $x, y, z \in G$ sont tels que $(x, y), (y, z) \in R_H$. Donc

   $$x^{-1}y \in H, \quad y^{-1}z \in H.$$

   Puisque H est stable par multiplication, on obtient

   $$x^{-1}yy^{-1}z = x^{-1}z \in H.$$

   Donc $(x, z) \in R_H$, comme voulu.

Exercice 4. 1. On a $|R| = \sum_i |R_i|^2$.

Pour prouver cette égalité, il suffit d'observer que

$$R = \bigsqcup_i (R_i \times R_i)$$

comme sous-ensembles de $A \times A$. En effet :

(a) **L'union $\bigcup_i (R_i \times R_i)$ est disjointe.** On a en général

$$(R_i \times R_i) \cap (R_j \times R_j) \subseteq (R_i \cap R_j) \times (R_i \cap R_j).$$

Donc si $i \neq j$, on a $R_i \cap R_j = \emptyset$ et ainsi $(R_i \times R_i) \cap (R_j \times R_j) = \emptyset$.

(b) **R est inclus dans $\bigcup_i (R_i \times R_i)$.** En effet, soit $(x, y) \in R$. Alors par définition x, y appartiennent à la classe d'équivalence de x, qui est un R_i pour un certain indice i. Ainsi $(x, y) \in R_i \times R_i$.

(c) **R contient $\bigcup_i (R_i \times R_i)$.** Prenons $(x, y) \in R_i \times R_i$. Si R_i est la classe d'équivalence de $a \in A$, alors $(x, a), (y, a) \in R$. Par symétrie $(x, a), (a, y) \in R$ et par transitivité $(x, y) \in R$.

2. Puisque $|A| = \sum_{i=1}^{3} |R_i|$ et que $|R_i| \geq 1$, on trouve, quitte à renommer les R_i, les possibilités suivantes pour $(|R_1|, |R_2|, |R_3|)$:

- $(1, 1, 5)$ et donc $|R| = 27$;
- $(1, 2, 4)$ et donc $|R| = 21$;
- $(1, 3, 3)$ et donc $|R| = 19$;
- $(2, 2, 3)$ et donc $|R| = 17$.

Exercice 5. 1. On a

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}.$$

2. Prouvons que H est normal. Prenons une matrice quelconque

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in G.$$

Les calculs du point précédents impliquent que

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}.$$

Ainsi :

$$\begin{aligned} \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y+u \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H \end{aligned}$$

ce qui montre que H est normal.

Solution alternative. On prétend que $Z(G) = H$. En effet :

$$\begin{pmatrix}1&0&x\\0&1&0\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}=\begin{pmatrix}1&d&e+x\\0&1&f\\0&0&1\end{pmatrix}=\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&0&x\\0&1&0\\0&0&1\end{pmatrix}.$$

Donc $H \subseteq Z(G)$. Inversément, si

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \in Z(G),$$

alors l'égalité

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}=\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \quad \forall x,y,z \in \mathbb{F}_p$$

entraîne l'égalité

$$y + az + b = y + cx + b, \quad \text{donc} \quad az = cx.$$

Prenons $z = 1, x = 0$, on obtient $a = 0$. Prenons $x = 1, z = 0$, on trouve $c = 0$. Donc $Z(G) \subseteq H$.

En particulier, H est normal.

3. Considérons la fonction

$$g\colon G \to (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}, \quad \begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix} \mapsto (x,z).$$

Le calcul du premier point implique que g est un morphisme.

Voici le calcul détaillé :

$$\begin{aligned} g\left(\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&x'&y'\\0&1&z'\\0&0&1\end{pmatrix}\right) &= g\left(\begin{pmatrix}1&x+x'&*\\0&1&z+z'\\0&0&1\end{pmatrix}\right)\\ &= (x+x', z+z')\\ &= g\left(\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\right) + g\left(\begin{pmatrix}1&x'&y'\\0&1&z'\\0&0&1\end{pmatrix}\right). \end{aligned}$$

De plus, il est clair que $\ker(g) = H$ et que g est surjective. Donc par le premier théorème d'isomorphisme,

$$g\colon G/H \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}.$$

Solution alternative. Considérons la fonction

$$f\colon (\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \to G/H, \quad (x,y) \mapsto \left[\begin{pmatrix} 1 & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}\right].$$

On prétend que f est un morphisme. En effet,

$$f(x,y)\cdot f(a,b) = \left[\begin{pmatrix} 1 & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\right] = \left[\begin{pmatrix} 1 & a+x & bx \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}\right]$$

et dans G on a

$$\begin{pmatrix} 1 & a+x & 0 \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & 0 & bx \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\in H} = \begin{pmatrix} 1 & a+x & bx \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}$$

d'où dans G/H

$$\left[\begin{pmatrix} 1 & a+x & 0 \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}\right] = \left[\begin{pmatrix} 1 & a+x & bx \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix}\right]$$

et ainsi

$$f(x,y)\cdot f(a,b) = f((x,y)+(a,b)).$$

On a $f((x,y)) = e_{G/H}$ si et seulement si

$$\begin{pmatrix} 1 & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in H,$$

si et seulement si $x = 0 = y$. Donc f est injective.

On a montré que f est un morphisme injectif. Comme $|G/H| = |G|/|H| = p^2 = |(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}|$, on en déduit que f est un isomorphisme.

Exercice 6. 1. Ecrivons $H = \langle\tau\rangle$ et $F = \langle\rho\rangle$. On a $o(\tau) = 2 = o(\rho)$, et donc $H \cong \mathbb{Z}/2\mathbb{Z} \cong F$. Puisque τ et ρ sont à supports disjoints, ils commutent entre eux. Donc F est contenu dans le normalisateur de H. De plus $H \cap F$ est un sous-groupe d'ordre divisant 2, et si l'ordre vaut 2 alors $H = H \cap F = F$. Or $H \neq F$, donc $H \cap F$ est trivial. On peut alors appliquer le Théorème 3.8.13 ainsi que l'Exercice 2 pour obtenir

$$\langle H, F\rangle \cong HF \cong H \rtimes_{\mathrm{Ad}_F^H} F.$$

Mais puisque les éléments de H commutent avec ceux de F, le morphisme Ad_F^H est trivial. Donc

$$\langle H, F\rangle \cong H \times F \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}.$$

Solution alternative. Puisque τ et ρ sont à supports disjoints, ils commutent entre eux. Puisque $o(\tau) = 2 = o(\rho)$, on en déduit que

$$J := \langle \tau, \rho\rangle = \{\tau^a \rho^b \mid 0 \leq a, b \leq 1\} \subset S_n.$$

Donc la fonction

$$f\colon (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} \to J, \quad ([a], [b]) \mapsto \tau^a \rho^b$$

est bien définie et surjective, et c'est un morphisme puisque τ et ρ commutent entre eux.

La description $J = \{\tau^a \rho^b \mid 0 \leq a, b \leq 1\}$ implique que $|J| \leq 4$. Le groupe $\{e_{S_n}, \tau\}$ est un sous-groupe de J, donc par Lagrange on en déduit que $|J| \in \{2, 4\}$. Or $\rho \in J \setminus \{e_{S_n}, \tau\}$, donc $|J| \geq 3$ et ainsi $|J| = 4$.

Donc f est un morphisme surjectif entre deux groupes de même ordre fini. C'est donc un isomorphisme.

Solution alternative. Sans perte de généralité, on peut supposer que $\tau = (12)$ et $\rho = (34)$. On prétend que

$$\langle (12), (34)\rangle = \{e, (12), (34), (12)(34)\}.$$

Il suffit de montrer que l'ensemble de droite, appelons-le K, est un sous-groupe de S_n. Puisque (12) et (34) commutent et sont leur propre inverse, on voit que K est stable par multiplication et que chaque élément de H est son propre inverse. Donc $K \leq S_n$.

Puisque (12) et (34) commutent entre eux, il s'ensuit aussi que K est abélien.

Puisque tous les éléments de K sont leur propre inverse, chaque élément est 2-torsion, donc K n'est pas cyclique.

On conclut en utilisant l'Exercice 8.1 de la série 9.

2. Sans perte de généralité, on peut supposer que $\tau = (12)$ et $\rho = (23)$. Par l'Exercice 2.1 de la série 10, on sait que (12) et (23) génèrent S_3.

   Solution alternative. Le sous-groupe de S_3 généré par (12) et (23) contient au moins 4 éléments (par exemple l'identité, $(12), (23)$ et $(123) = (12)(23)$), et par Lagrange cela implique que ce sous-groupe est égal à S_3.

Exercice 7. 1. Remarquons que $f^{-1} = f$. Un calcul simple montre alors que

$$fhf^{-1} = (15432) = (12345)^4 = h^4.$$

Ainsi pour $i \in \mathbb{Z}$

$$fh^i f^{-1} = (fhf^{-1})^i = h^{4i} \in \langle h \rangle.$$

Donc $f \in N_{S_7}(\langle h \rangle)$, puisque $\langle h \rangle = \{h^i \mid i \in \mathbb{Z}\}$.

2. Ecrivons $F = \langle f \rangle, H = \langle h \rangle$. Puisque $f \in N_{S_7}(H)$ et que $N_{S_7}(H)$ est un sous-groupe, on a $F \subseteq N_{S_7}(H)$. Par l'Exercice 2, on a $P = HF$.

   De plus, par le théorème de Lagrange, l'ordre du sous-groupe $I := H \cap F$ doit diviser à la fois $|H| = 5$ et $|F| = 2$, donc $I = \{e_{S_7}\}$ (cela peut s'obtenir sans le théorème de Lagrange, en listant explicitement les éléments de H et de F : il suffit d'observer que $f \notin H$).

   Par le Théorème 3.8.13 du cours, on a ainsi

$$P = HF \cong H \rtimes_{\mathrm{Ad}_F^H} F \tag{1}$$

   ce qui implique en particulier que $|P| = |H| \cdot |F| = 2 \cdot 5$.

   Alternativement, on peut utiliser le corollaire 3.8.2 qui établit une bijection $HF \leftrightarrow H \times F$, que donne également $|P| = |HF| = 2 \cdot 5 = 10$.

   Il est également possible de lister explicitement les éléments de P, mais il est important de vérifier que les éléments sont deux-à-deux distincts avant d'affirmer que $|P| = 10$.

   À partir de là, on propose trois solutions :

   A) Par le Corollaire 3.8.18 (qui est applicable puisque $(\mathbb{Z}/5\mathbb{Z})^\times$ est cyclique, engendré par [3]) – ou par le tableau de classification vu ans le cours –, on obtient que $P \cong \mathbb{Z}/10\mathbb{Z}$ ou que $P \cong D_{10}$. Excluons le premier cas : s'il y avait un tel isomorphisme, P serait abélien, et donc $fhf^{-1} = h$; or on a calculé au point précédent que $fhf^{-1} = h^4 \neq h$. Donc $P \cong D_{10}$.

   B) Par l'argument ci-dessus, on peut énumérer

$$P = \{h^j, h^j f \mid 0 \leq j \leq 4\}, \tag{2}$$

   et ces éléments sont deux-à-deux distincts.
   On définit une application $\phi : P \to D_{10}$ par

$$\phi(h^j) := \sigma^j, \quad \phi(h^j f) = \sigma^j \cdot \tau \qquad (0 \leq j \leq 4). \tag{3}$$

   Il est assez clair que ϕ est bijective, mais le plus dur est de montrer que ϕ est un homomorphisme. Soient $x = h^n f^m$ et $y = h^r f^s$ deux éléments de P, où $0 \leq m, s \leq 1$ et $0 \leq n, r \leq 4$. On distingue deux cas :

- Si $m = 0$, on trouve

$$\begin{aligned}\phi(xy) &= \phi(h^{n+r} f^s) \\ &= \phi(h^{n+r \bmod 5} \cdot f^s) \\ &= \sigma^{n+r \bmod 5} \cdot \tau^s \\ &\overset{\star}{=} \sigma^n \sigma^r \tau^s \\ &= \phi(x)\phi(y),\end{aligned}$$

  où $\star$ utilise le fait que $\sigma \in D_{10}$ est d'ordre 5.
- Si $m = 1$, on a

$$\begin{aligned}\phi(xy) &= \phi(h^n \cdot f \cdot h^r \cdot f^{-1+s+1}) \\ &= \phi(h^n \cdot h^{-r} \cdot f^{s+1}) \\ &= \phi(h^{n-r \bmod 5} \cdot f^{s+1 \bmod 2}) \\ &= \sigma^{n-r \bmod 5} \cdot \tau^{s+1 \bmod 2} \\ &\overset{\star\star}{=} \sigma^{n-r} \tau^{s+1} \\ &\overset{\star\star\star}{=} \sigma^n \cdot (\tau \sigma^r \tau^{-1}) \cdot \tau^{s+1} \\ &= (\sigma^n \tau) \cdot (\sigma^r \tau^s) \\ &= \phi(x)\phi(y),\end{aligned}$$

  où $\star\star$ utilise le fait que $\sigma \in D_{10}$ est d'ordre 5 et τ est d'ordre 2, et $\star\star\star$ utilise la relation $\tau\sigma\tau^{-1} = \sigma^{-1}$.

C) On sait que $H \cong \mathbb{Z}/5\mathbb{Z}$ et $F \cong \mathbb{Z}/2\mathbb{Z}$. D'après l'équation (1), on déduit alors que $P \cong \mathbb{Z}/5\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ pour un certain morphisme $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$. Or, il y a exactement 2 tels morphismes, correspondant aux éléments de 2-torsion de $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$. Ceci dit, ϕ ne peut pas être le morphisme trivial car P n'est pas abélien – voir l'argument en A). Ainsi, P est l'unique produit semi-direct non-trivial de $\mathbb{Z}/5\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Puisque $D_{10} \cong \mathbb{Z}/5\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ par l'exemple 3.8.14.3, on en déduit que $P \cong D_{10}$.

Exercice 8.
Soient $G = D_{28}, H \trianglelefteq \langle \sigma^2 \rangle$ et $F = \langle \sigma^7, \tau \rangle$. Puisque H est normal, le morphisme $\phi := \mathrm{Ad}_F^H : F \to \mathrm{Aut}(H)$ est bien défini. Commençons par calculer les ordres des groupes de départ et d'arrivée de ϕ.

1. Puisque H est cyclique et que $o(\sigma) = 28/2 = 14$, on obtient que $|H| = o(\sigma^2) = 14/2 = 7$. Par le Corollaire 3.5.37, on obtient que $H \cong \mathbb{Z}/7\mathbb{Z}$, et donc que

$$\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$$

et ainsi $|\mathrm{Aut}(H)| = 6$ par l'Exemple 3.5.33 (ou en combinant l'Exercice 3 de la série 5 et l'Exercice 3 de la série 7).

Identifions explicitement les automorphismes de $\mathbb{Z}/7\mathbb{Z}$. On prétend que

$$\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) = \{m_x \colon [n] \mapsto [nx] \mid 1 \leq x \leq 6\}.$$

Puisque $\mathbb{Z}/7\mathbb{Z}$ est généré par $[1]$, un morphisme $f \colon \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ est entièrement défini par $f([1])$, dans le sens où $f = m_x$ avec $[x] = f([1])$. L'entier x est déterminé modulo 7, donc on peut choisir $x \in \{0, 1, \ldots, 6\}$. Si f est un morphisme non-trivial (par exemple, un automorphisme), alors $f([1]) \neq [0]$ et donc $x \neq 0$. Ceci établit l'inclusion $\subseteq$. Inversément, prenons $1 \leq x \leq 6$. Alors

$$m_x([n]) = [0] \Leftrightarrow 7|xn \Leftrightarrow 7|n \Leftrightarrow [n] = 0$$

où la deuxième équivalence découle du fait que 7 est premier. Donc m_x est injective ; et puisque le groupe de départ et d'arrivée de m_x ont le même cardinal, on déduit que m_x est un automorphisme. Ceci établit l'inclusion $\supseteq$.

2. Le groupe F doit nécessairement contenir l'ensemble $\{e, \sigma^7, \tau, \sigma^7\tau\}$. Inversément, on voit facilement que cet ensemble est un sous-groupe. Ainsi $|F| = 4$.

   En effet, chaque élément est son propre inverse. Pour montrer que l'ensemble est stable par multiplication, les seules vérifications à faire sont

   $$\sigma^7\tau\sigma^7 = \sigma^0\tau = \tau, \quad \sigma^7\tau\tau = \sigma^7.$$

Par le théorème de Lagrange, $|\mathrm{im}(\phi)|$ doit diviser à la fois $|F| = 4$ et $|\mathrm{Aut}(H)| = 6$. Donc $|\mathrm{im}(\phi)|$ vaut soit 1, soit 2. On prétend que $\phi(e) \neq \phi(\tau)$. Puisque $\phi(e) = \mathrm{id}_H$, il suffit de montrer que $\phi(\tau)$ est distinct de l'identité sur H. On a :

$$\phi(\tau)(\sigma^{2i}) = \tau\sigma^{2i}\tau = \tau^2\sigma^{-2i} = \sigma^{-2i}.$$

Cependant $\sigma^{2i} \neq \sigma^{-2i}$ pour $1 \leq i \leq 6$, puisque $o(\sigma) = 14$. On a bien obtenu que $\phi(\tau) \neq \phi(e)$. Il en découle donc que $|\mathrm{im}(H)| = 2$.