L3 Mathématiques et Mathématiques/Enseignement **Université Paris Diderot**
2015/2016

Eléments de corrigé du Partiel d'algèbre du 18 novembre 2015

Exercice 1.

1. Il suffit de trouver deux matrices qui ne commutent pas dans H par exemple

$$\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}, \quad \text{alors que} \quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}=\begin{pmatrix}1 & 2\\ 0 & 2\end{pmatrix}$$

2. Notons M_u la matrice $\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$. Un calcul rapide donne $M_uM_{u'}=M_{u+u'}$ donc le morphisme est un morphisme de groupes, qui est surjectif car tout élément de T s'écrit M_u pour un certain $u\in\mathbb{R}$. Le noyau du morphisme est constitué des réels u tel que $M_u=\mathrm{Id}$ donc est réduit à 0. Conclusion: on a bien un isomorphisme de groupes.

3. Il faut montrer que pour tout $h\in H, M_u\in T$ on a $hM_uh^{-1}\in T$. Calculons

$$\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\frac{1}{ac}\begin{pmatrix}c & -b\\ 0 & a\end{pmatrix}=\frac{1}{ac}\begin{pmatrix}a & au+b\\ 0 & c\end{pmatrix}\begin{pmatrix}c & -b\\ 0 & a\end{pmatrix}=\frac{1}{ac}\begin{pmatrix}ac & a^2u\\ 0 & ac\end{pmatrix}=\begin{pmatrix}1 & \frac{a}{c}u\\ 0 & 1\end{pmatrix}\in T$$

Le contre-exemple ci-dessous prouve que T n'est pas distingué dans $GL_2(\mathbb{R})$.

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}=\begin{pmatrix}1 & u\\ 1 & 1+u\end{pmatrix}\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}=\begin{pmatrix}1-u & u\\ -u & 1+u\end{pmatrix}\notin T, \text{ pour } u\neq 0$$

s

4. Comme H est distingué dans T on a H/T est un groupe. Par ailleurs prenons $\overline{h}$ et $\overline{h'}$ deux éléments de H/T. Montrons que $\overline{hh'h^{-1}h'^{-1}}=\overline{\mathrm{Id}}$ ce qui est équivalent à montrer que $hh'h^{-1}h'^{-1}\in T$. On a:

$$hh'=\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}a' & b'\\ 0 & c'\end{pmatrix}=\begin{pmatrix}aa' & ab'+bc'\\ 0 & cc'\end{pmatrix}, \quad \text{et } h'h=\begin{pmatrix}aa' & a'b+b'c\\ 0 & cc'\end{pmatrix}$$

Donc

$$(h'h)^{-1}=\frac{1}{aa'cc'}\begin{pmatrix}cc' & -a'b-b'c\\ 0 & aa'\end{pmatrix} \text{ et } hh'h^{-1}h'^{-1}=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix},$$

Pour un certain $\beta\in\mathbb{R}$, donc cet élément se trouve dans T.

Exercice 2.

1. Soient $\sigma,\tau\in\Sigma_p$. On a $\varphi(\sigma,\varphi(\tau,(a_1,\dots,a_p)))=\varphi(\sigma,(a_{\tau^{-1}(1)},\dots,a_{\tau^{-1}(p)}))$. Posons $b_i=a_{\tau^{-1}(i)}$. Ainsi

$$\varphi(\sigma,\varphi(\tau,(a_1,\dots,a_p)))=(b_{\sigma^{-1}(1)},\dots,b_{\sigma^{-1}(p)})=(a_{\tau^{-1}(\sigma^{-1}(1))},\dots,a_{\tau^{-1}(\sigma^{-1}(p))})=\varphi(\sigma\tau,(a_1,\dots,a_p)).$$

2. (a) K est un groupe cyclique d'ordre l'ordre du cycle $(1...p)$ qui vaut p.

   (b) $(a_1, \ldots, a_p)$ est un point fixe pour l'action de K si et seulement si $(a_1, \ldots, a_p) = (a_p, a_1, \ldots, a_{p-1})$, si et seulement si $a_p = a_1 = a_2 = a_3 = \ldots = a_{p-1}$.

   (c) La formule des classes donne

$$Card(A^p) = Card((A^p)^K) + \sum_{i=1}^{r} O(x_i)$$

   où $O(x_i)$ est l'orbite de x_i et $x_1, \ldots, x_r$ sont des représentants des orbites ayant $n > 1$ éléments. Comme le cardinal de $O(x_i)$ divise p on a $O(x_i) = p$. Donc $n^p = n + rp$ c'est-à-dire n^p est congru à n modulo p.

Exercice 3.

1. On a $\alpha z + \beta = z'$ si et seulement si $z = \frac{1}{\alpha}(z' - \beta)$. Donc $f_{(\alpha,\beta)}$ est une bijection de $\mathbb{C}$ d'application réciproque $f_{(\frac{1}{\alpha}, \frac{-\beta}{\alpha})}$.

2. F est non vide ($f_{(1,0)} = Id_{\mathbb{C}}$) et on a montré que $f \in F \Rightarrow f^{-1} \in F$ dans la question précédente. Par ailleurs

$$(f_{(\alpha,\beta)} \circ f_{(\alpha',\beta')})(z) = \alpha(\alpha' z + \beta') + \beta = f_{(\alpha\alpha', \alpha\beta' + \beta)}(z) \quad (1)$$

   donc F est stable par composition. En conséquence, F est un sous-groupe des bijections de $\mathbb{C}$.

3. On démontre le relation par récurrence sur n. Pour $n = 1$, la relation est vérifiée. Supposons que la relation soit vraie au rang n et calculons

$$(f_{(\alpha,\beta)})^{n+1} = f^n_{(\alpha,\beta)} \circ f_{(\alpha,\beta)} = f_{(\alpha^n\alpha, \alpha^n\beta + (\sum_{i=0}^{n-1} \alpha^i)\beta)} = f_{(\alpha^{n+1}, (\sum_{i=0}^{n} \alpha^i)\beta)}$$

   par hypothèse de récurrence et d'après l'équation (1). Donc la relation est vraie au rang $n + 1$. Le principe de récurrence permet de conclure que la formule est vraie pour tout $n \geq 1$.

4. $f_{(\alpha,\beta)}$ est d'ordre fini si et seulement si il existe $n \in \mathbb{N}^*$ tel que $(f_{(\alpha,\beta)})^n = Id_{\mathbb{C}} = f_{(1,0)}$, si et seulement si il existe $n \in \mathbb{N}$ tel que $\alpha^n = 1$ et $(\sum_{i=0}^{n-1} \alpha^i)\beta = 0$.

   Donc α^n est une racine n-ième de l'unité.

   Premier cas: $\alpha = 1$, alors nécessairement $\beta = 0$ et $f_{(1,0)} = Id_{\mathbb{C}}$ est d'ordre 1.

   Deuxième cas: $\alpha \neq 1$. Soit d l'ordre de α dans $\mathbb{C}^*$. On a d divise n et α est une racine primitive d-ième de l'unité, donc $\{\alpha^i, 0 \leq i \leq d-1\}$ est l'ensemble des racines d-ième de l'unité. Par conséquent $\sum_{i=0}^{d-1} \alpha^i = 0$ et donc $(f_{(\alpha,\beta)})^d = Id_{\mathbb{C}}$.

   Ainsi $f_{(\alpha,\beta)}$ est d'ordre fini si et seulement si α est une racine d-ième de l'unité pour un certain $d \geq 2$ ou $(\alpha, \beta) = (1, 0)$.

Exercice 4.

1. Soit G un groupe d'ordre p^2. D'après P2. $|Z(G)| \in \{p, p^2\}$. Si $|Z(G)| = p^2$ alors $Z(G) = G$ et G est abélien. Si $|Z(G)| = p$ alors $G/Z(G)$ est d'ordre p, donc cyclique par P3; alors P1. implique que G est un groupe abélien (et d'ailleurs cela implique que $Z(G) = G$ donc que $|Z(G)| \neq p$) .

2. (a) On connait deux groupes d'ordre 8 non abélien: le groupe des quaternions et le groupe diédral d'ordre 8.

   (b) Par P2., on a $|Z(G)| \in \{p, p^2, p^3\}$. On élimine le cas où $|Z(G)| = p^3$ car G n'est pas abélien, donc $G \neq Z(G)$; combinant P1. et P3. on élimine également le cas où $|Z(G)| = p^2$. Il reste donc $|Z(G)| = p$.

   (c) Ainsi $|G/Z(G)| = p^2$ et par la question précédente on obtient que $G/Z(G)$ est abélien.

   (d) Soit H est un sous-groupe distingué de G tel que G/H est abélien. Pour tous $x, y \in G$ on a donc $\overline{xyx^{-1}y^{-1}} = \overline{e}$ c'est-à-dire $xyx^{-1}y^{-1} \in H$. Comme $D(G)$ est engendré par les éléments de type $xyx^{-1}y^{-1}$ et que H est un sous-groupe de G on en déduit que $D(G) \subset H$.

   (e) En c) on a montré que $G/Z(G)$ était abélien donc d) implique que $D(G) \subset Z(G)$. Ceci implique que $|D(G)| \in \{1, p\}$. Par ailleurs, on a toujours $G/D(G)$ est un groupe abélien:
   en effet $D(G)$ est distingué dans G: si $xyx^{-1}y^{-1} \in D(G)$ et $t \in G$ on a

$$txyx^{-1}y^{-1}t^{-1} = (txt^{-1})(tyt^{-1})(tx^{-1}t^{-1})(ty^{-1}t^{-1}) \in D(G)$$

   et si $x_1 \cdots x_n$ est un élément de $D(G)$ avec chaque x_i de la forme $uvu^{-1}v^{-1}$ alors

$$tx_1 \cdots x_n t^{-1} = (tx_1t^{-1}) \cdots (tx_nt^{-1}) \in D(G)$$

   donc $D(G)$ est distingué dans G donc $G/D(G)$ est un groupe. Par ailleurs pour $x, y \in G$ on a $xyx^{-1}y^{-1} \in D(G)$ donc $\bar{x}\bar{y}\overline{x^{-1}y^{-1}} = \overline{e}$ ce qui implique que $\bar{x}$ commute avec $\bar{y}$ donc $G/D(G)$ est abélien. Ainsi comme G n'est pas abélien on ne peut avoir $D(G) = \{e\}$. Par conséquent $|D(G)| = p$ et $D(G) = Z(G)$.