Corrigé deuxième session Algèbre 3 (23 juin 2015)

Exercice 1. Décrire tous les sous-groupes du groupe additif $(\mathbb{Z}/12\mathbb{Z}, +)$.

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$ est cyclique d'ordre 12. Il contient donc un unique sous-groupe (cyclique) d'ordre d pour chaque diviseur d de 12, à savoir :

- $\langle\overline{0}\rangle = \{\overline{0}\}$ d'ordre 1,
- $\langle\overline{6}\rangle = \{\overline{0}, \overline{6}\}$ d'ordre 2,
- $\langle\overline{4}\rangle = \{\overline{0}, \overline{4}, \overline{8}\}$ d'ordre 3,
- $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ d'ordre 4,
- $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ d'ordre 6 et
- $\langle\overline{1}\rangle = \mathbb{Z}/12\mathbb{Z}$ d'ordre 12.

Exercice 2.

Soit $\mathbf{GL}_2(\mathbb{R})$ le groupe des matrices réelles de taille 2×2 inversibles, la loi de groupe étant le produit matriciel usuel et l'élément neutre la matrice identité $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

On ne demande pas de re-démontrer que $\mathbf{GL}_2(\mathbb{R})$ est bien un groupe.

On considère, dans $\mathbf{GL}_2(\mathbb{R})$, les éléments

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

1. Déterminer l'ordre de A et celui de B.
   A est d'ordre 2 et B d'ordre 4.
2. Montrer que $AB = B^{-1}A$.
   Calcul immédiat.
3. Soit $H = \langle A \rangle$ et $K = \langle B \rangle$ les sous-groupes de $\mathbf{GL}_2(\mathbb{R})$engendrés respectivement par A et B.
   (a) Montrer que $H \cap K = \{I\}$.
   $H \cap K$ est contenu dans $H = \{I, A\}$, donc d'ordre au plus 2. Comme $A \notin K = \{I, B, -I, -B\}$ on conclut que $H \cap K = \{I\}$.
   (b) Montrer que si i et j sont des entiers relatifs on a l'équivalence :
   $$B^i A^j = I \iff \begin{cases} i \equiv 0 \mod 4 \\ j \equiv 0 \mod 2 \end{cases}$$
   C'est une conséquence de la question précédente : si $B^i A^j = I$ alors $B^j = A^{-i} \in H \cap K = \{I\}$. Donc $B^j = A^{-i} = I$, ce qui n'est possible que si i (resp. j) est un multiple de l'ordre de B (resp. A).

4. Justifier que les éléments $I, B, B^2, B^3, A, BA, B^2A, B^3A$ sont deux à deux distincts et qu'ils forment un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$, noté G dans la suite.

   Le fait que ces 8 éléments soient deux à deux distincts est une conséquence immédiate de la question précedente. En effet, les éléments de cette liste sont de la forme B^iA^j avec $0 \leq i \leq 3$ et $0 \leq j \leq 1$ et si deux éléments $x = B^iA^j$ et $y = B^{i'}A^{j'}$ sont égaux, on a

   $$B^iA^j = B^{i'}A^{j'} \Rightarrow B^{i-i'} = A^{j'-j} \Rightarrow i \equiv i' \bmod 4 \text{ et } j \equiv j' \bmod 2 \text{ (question précédente)}$$

   moyennant quoi $x = y$.

   Pour vérifier que l'ensemble $G = \{I, B, B^2, B^3, A, BA, B^2A, B^3A\}$ est bien un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ il reste à s'assurer que pour tout $x \in G$ et tout $y \in G$ le produit xy^{-1} appartient lui aussi à G. Si $x = B^iA^j$ et $y = B^{i'}A^{j'}$, on a

   $$xy^{-1} = B^iA^j\left(B^{i'}A^{j'}\right)^{-1} = B^iA^{j-j'}B^{-i'}.$$

   Si $j - j' \equiv 0 \mod 2$ on trouve que $xy^{-1} = B^{i-i'}$ qui appartient bien à G. Sinon, c'est-à-dire si $j - j' \equiv 1 \mod 2$, alors la relation $AB = B^{-1}A$ établie précédemment permet de conclure que $xy^{-1} = B^{i+i'}A$, qui appartient aussi à G. L'ensemble G est bien un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$.

5. Combien y a-t-il d'éléments d'ordre 2 dans G ?

   Il y a 5 éléments d'ordre 2, à savoir B^2, A, BA, B^2A et B^3A.

6. Montrer que K un sous-groupe normal de G.

   $K = \langle B \rangle$ un sous-groupe normal de G car d'indice 2 dans G. On peut aussi le justifier directement en remarquant, grâce au résultat de la question 2, que $AB^iA^{-1} = B^{-i}$.

7. Le sous-groupe H est-il normal ?

   $H = \langle A \rangle$ n'est pas un sous-groupe normal car, par exemple, $BAB^{-1} = B^2A \notin H$.

Exercice 3.

1. On considère, dans S_8, la permutation

   $$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 4 & 8 & 1 & 3 & 2 \end{pmatrix}.$$

   (a) Quel est son support ? $\{1, 2, 3, 5, 6, 7, 8\}$

   (b) Quel est son ordre ? Le plus efficace est de décomposer p en produit de cycles à supports disjoints :

   $$p = (15826)\,(37)$$

   d'où l'on déduit que l'ordre de p vaut $5 \times 2 = 10$.

2. Calculer p^{10000}.

   En conséquence, $p^{10000} = Id$

3. Le groupe S_8 contient-t-il des éléments d'ordre 15 ?

   Oui : par exemple $\sigma = (123)\,(45678)$

4. Le groupe S_8 contient-t-il des éléments d'ordre 14 ?

   Non : si un tel élément existait alors sa décomposition en cycle à supports disjoints contiendrait au moins un cycle de longueur 7, et un cycle de longueur 2 puisque le ppcm des longueurs de ces cycles doit valoir 14. Son support aurait alors au moins 9 éléments, ce qui est absurde (on est dans S_8).

Exercice 4. On étudie dans cet exercice le sous-ensemble A de $\mathbb{R}$ constitué des nombres réels qui s'écrivent sous la forme d'une somme $m + n\sqrt{2}$ avec m et n entiers relatifs. Autrement dit

$$A = \left\{ x \in \mathbb{R} \mid \exists (m,n) \in \mathbb{Z}^2, x = m + n\sqrt{2} \right\}.$$

1. Montrer que A est un sous-anneau de $\mathbb{R}$.

   C'est clair car le produit et la différence de deux éléments de A sont bien des éléments de A, comme on le vérifie par un calcul élémentaire.

2. Soit $\phi : A \to A$ l'application qui à $x = m + n\sqrt{2}$ associe $\phi(x) = m - n\sqrt{2}$. Montrer que ϕ est un morphisme d'anneaux.

$$\begin{aligned}
\phi\left((m+n\sqrt{2})(m'+n'\sqrt{2})\right) &= \phi\left(mm' + 2nn' + (mn' + m'n)\sqrt{2}\right) \\
&= mm' + 2nn' - (mn' + m'n)\sqrt{2} \\
&= (m - n\sqrt{2})(m' - n'\sqrt{2}) \\
&= \phi\left(m + n\sqrt{2}\right)\phi\left(m' + n'\sqrt{2}\right).
\end{aligned}$$

3. Pour tout $x \in A$, on pose $N(x) = x\phi(x)$

   (a) Montrer que $N(x)$ appartient à $\mathbb{Z}$ pour tout $x \in A$.
   Si $x = m + n\sqrt{2} \in A$, alors $N(x) = m^2 - 2n^2$ appartient à $\mathbb{Z}$.

   (b) Montrer que l'application $N : A \to \mathbb{Z}$ est *multiplicative*, c'est-à-dire qu'elle vérifie :
   $$\forall x \in A, \forall y \in A, N(xy) = N(x)N(y).$$
   C'est un calcul immédiat, du fait que l'on a déjà vérifié que ϕ était un morphisme :
   $$N(xy) = xy\phi(xy) = xy\phi(x)\phi(y) = x\phi(x)y\phi(y) = N(x)N(y).$$

   (c) Montrer que si $N(x) = \pm 1$, alors x est inversible dans A.
   Comme l'image par ϕ d'un élément x de A appartient également à A, il est clair que si $x\phi(x) = 1$ alors x est inversible d'inverse $\phi(x)$ et si $x\phi(x) = -1$ alors x est inversible d'inverse $-\phi(x)$

   (d) Inversement, montrer que si x est inversible dans A, alors $N(x) = \pm 1$.
   Si $x \in A$ est inversible d'inverse $y \in A$, alors $xy = 1$ et $1 = N(xy) = N(x)N(y)$ puisque l'application N est multiplicative. Puisque $N(x)$ et $N(y)$ sont des entiers, la seule façon que leur produit soit égal à 1 et qu'ils soient simultanément égaux à 1 ou -1.

   (e) Montrer que l'élément $(3 - 2\sqrt{2})^4$ est inversible dans A et calculer son inverse.
   $N(3 - 2\sqrt{2}) = 1$, donc $3 - 2\sqrt{2}$ est inversible dans A, d'inverse $\phi(3 - 2\sqrt{2}) = 3 + 2\sqrt{2}$. Par suite, $(3 - 2\sqrt{2})^4$ est inversible dans A, d'inverse $(3 + 2\sqrt{2})^4$.