1e année, Algèbre 1

# TD n° 3 : Quotients et quaternions d'Hamilton

---

`À faire en priorité :  1 - 2 - 3 - 5 - 9 - 10`

La fin de la feuille comprend : le complément II du cours sur les quaternions d'Hamilton et quelques définitions.

## 1 Sous-groupes distingués et groupes quotients

**Exercice 1.**

Soient $H$ un sous-groupe distingué d'indice fini $n$ de $G$, et $g \in G$. Montrer $g^n \in H$.

**Exercice 2. Centre et automorphismes intérieurs**

Soit $G$ un groupe.

1. Montrer que $\mathrm{int} : G \to \mathrm{Aut}(G), g \mapsto \mathrm{int}_g$, est un morphisme de groupes de noyau $\mathrm{Z}(G)$.
2. En déduire que l'image, soit $\mathrm{Int}(G)$, est un sous-groupe de $\mathrm{Aut}(G)$ et que $\mathrm{Z}(G)$ est un sous-groupe distingué de $G$. Montrer finalement que $G/\mathrm{Z}(G) \cong \mathrm{Int}(G)$.
3. Montrer que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

**Exercice 3.**

1. Soit $G$ un groupe tel que $G/\mathrm{Z}(G)$ est monogène, montrer que $G$ est abélien.
2. Examiner le cas $G = \mathrm{H}_8$.

**Exercice 4.**

Soient $G$ un groupe et $H, K$ deux sous-groupes de $G$, . Rappelons $HK \coloneqq \{hk; h \in H,\ k \in K\}$.

1. Montrer que si $K$ est distingué $G$, alors $HK$ est un sous-groupe de $G$.
2. Soit $\mathrm{m}\colon H \times K \to HK$ l'application de multiplication définie par $(h, k) \mapsto hk$. Montrer que $m$ est une bijection si, et seulement si, $H \cap K = \{e_G\}$.
3. Montrer que m est un morphisme de groupe si, et seulement si, $\forall h \in H, \forall k \in K,\ hk = kh$.
4. Supposons maintenant que $H$ et $K$ sont distingués dans $G$. Montrer l'implication
$$H \cap K = \{e_G\} \implies \forall h \in H, k \in K,\ hk = kh$$
et conclure que m est un isomorphisme.
5. Montrer que $\mathrm{H}_8$ n'est pas de la forme $HK$ pour des sous-groupes non-triviaux.

**Exercice 5.**

Soient $G$ un groupe et $H$ une partie de $G$. Rappelons qu'on note $\mathrm{N}_G(H)$ (*resp.* $\mathrm{C}_G(H)$) le normalisateur (*resp.* centralisateur) de $H$ dans $G$.

1. Montrer que $\mathrm{C}_G(H)$ et $\mathrm{N}_G(H)$ sont des sous-groupes de $G$.
2. Montrer que $\mathrm{N}_G(H)$ est le plus grand sous-groupe de $G$ contenant $H$, et dans lequel $H$ est distingué.
3. Montrer aussi que $\mathrm{C}_G(H)$ est un sous-groupe distingué de $\mathrm{N}_G(H)$.
4. *(Exemple)* On suppose $G = \mathrm{GL}_2(k)$ avec $k$ un corps et $H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} ;\ x \in k \right\}$. Déterminer $\mathrm{C}_G(H)$ et $\mathrm{N}_G(H)$.

**Exercice 6.**

Soit $G$ un groupe fini de cardinal $n \geqslant 1$. Montrer[1] $|\mathrm{Hom}(G,G)| \leqslant n^{\log_2(n)}$.

**Exercice 7.**

Soit $G$ un groupe de type fini. Montrer que tout sous-groupe de $G$ d'indice fini est de type fini. Donner l'exemple d'un groupe $G$ de type fini, muni d'un sous-groupe qui n'est pas de type fini.

# 2 Matrices $2 \times 2$ et quaternions

**Exercice 8.**

On se place dans le groupe $\mathrm{GL}_2(\mathbb{Q})$ et on considère l'élément

$$g \coloneqq \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{et} \quad H \coloneqq \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} ;\ n \in \mathbb{Z} \right\}$$

1. Justifier que $H \subset G$ est un sous-groupe puis vérifier $gHg^{-1} \subsetneq H$.
2. Vérifier que $H' \coloneqq \bigcup_{n \geq 0} g^{-n} H g^{n}$ est le plus petit sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ contenant $H$ tel que $gH'g^{-1} = H'$. Puis, déterminer $H'$.

## 2.1 Quaternions

*Les deux exercices suivant concernent les quaternions. Le premier montre notamment que pour $p$ premier, $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ peut être vu comme un anneau de* quaternions modulo $p$.

**Exercice 9.**

Soit $p$ un nombre premier.

1. Montrer qu'il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^2 + y^2 = -1$.
   On considère les deux matrices $I, J \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$
   $$I \coloneqq \begin{bmatrix} x & y \\ y & -x \end{bmatrix}, \quad J \coloneqq \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$
2. Vérifier $I^2 = -1$, $J^2 = -1$ et $IJ + JI = 0$.
3. On suppose $p > 2$. Montrer que $\{1, I, J, IJ\}$ forme une base du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.
4. En déduire que $\mathrm{H}_8$ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout nombre premier $p > 2$.

**Exercice 10. Quaternions de Hurwitz**

On considère l'élément $\omega = \frac{1+I+J+K}{2}$ de $\mathbb{H}$ et on pose $\mathrm{Hur} \coloneqq \mathbb{Z} + \mathbb{Z}I + \mathbb{Z}J + \mathbb{Z}K + \mathbb{Z}\omega$.

1. Montrer que Hur est un sous-anneau de $\mathbb{H}$ et $\forall q \in \mathrm{Hur},\ \chi_q \in \mathbb{Z}[t]$.
2. Montrer $\mathrm{Hur}^\times = \{q \in \mathrm{Hur} \mid \mathrm{n}(q) = 1\}$. En déduire $|\mathrm{Hur}^\times| = 24$, puis lister les 24 éléments de Hur, ainsi que leurs polynômes caractéristiques.
3. On suppose $p$ premier impair. En utilisant l'exercice précédent, exhiber un morphisme d'anneaux surjectif $\varphi : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$. Vérifier que l'on a $\mathrm{tr}(\varphi(q)) = \mathrm{tr}(q) \bmod p$, et donc $\det \varphi(q) = \mathrm{n}(q) \bmod p$, pour tout $q \in \mathrm{Hur}$.
4. En déduire $\mathrm{Hur}^\times \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.
5. Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout $p > 2$ premier (un fait assez surprenant!).

[1] On pourra commencer par expliquer que pour $g_1, \ldots, g_r \in G$ une famille génératrice un morphisme $\varphi \colon G \to G$ est déterminé par la famille $\varphi(g_1), \ldots, \varphi(g_r) \in G$. Il faudra ensuite en construire une adaptée...

# 3 Rappels et notations

## 3.1 Définitions et notations

- Rappelons que $\mathrm{H}_8$ est le groupe fini des quaternions unités caractérisé comme le groupe d'ordre 8 contenant un élément d'ordre 2 et six éléments d'ordre 4.
- Soit $\mathrm{Z}(G) \coloneqq \{g \in G \mid gh = hg,\ \forall h \in G\}$ le *centre* de $G$. C'est un sous groupe distingué et on dit parfois qu'un élément de $G$ est *central* si $g \in \mathrm{Z}(G)$.
- Pour $G$ un groupe on note $\mathrm{Aut}(G)$ le groupe des automorphismes de $G$ dont les *automorphismes* intérieurs sont ceux obtenus comme conjugaison de $G$ par un élément de $G$.
- Pour $G$ un groupe et $H$ une partie[2] de $G$ on a respectivement, le *normalisateur* de $H$ dans $G$ et le *centralisateur* de $H$ dans $G$ définis par

$$\mathrm{N}_G(H) \coloneqq \left\{g \in G \mid gHg^{-1} = H\right\} \quad \text{et} \quad \mathrm{C}_G(H) \coloneqq \{g \in G \mid gh = hg,\ \forall h \in H\}\,.$$

## 3.2 Quaternions de Hamilton

Pour nous, les *quaternions d'Hamilton* sont définis comme le sous-anneau[3] de $\mathrm{M}_2(\mathbb{C})$ contenant $\mathbb{R}$ et engendré par les matrices $I$, $J$ et $K = IJ$ telles que $I^2 = J^2 = -1$ et $IJ = -JI$, i.e.

$$\mathbb{H} = \mathbb{R} \cdot 1 \ +\ \mathbb{R} \cdot I \ +\ \mathbb{R} \cdot J \ +\ \mathbb{R} \cdot K.$$

C'est un sous-espace vectoriel du $\mathbb{R}$-espace vectoriel $\mathrm{M}_2(\mathbb{C})$, dont les 4 générateurs $1, I, J, K$ forment en fait une base :

$$\forall x, y, z, t \in \mathbb{R}, \quad t\,1 + x\,I + y\,J + z\,K \ =\ \begin{bmatrix} t + ix & -y - iz \\ y - iz & t - ix \end{bmatrix}$$

Soit $q = t\,1 + x\,I + y\,J + z\,K \in \mathbb{H}$ comme ci-dessus, on pose :

1. $\mathrm{t}(q) \coloneqq \mathrm{tr}\, q = 2t$, la *trace* de $q$,
2. $\mathrm{n}(q) \coloneqq \det q = t^2 + x^2 + y^2 + z^2$, la *norme* de $q$,
3. $\chi_q \coloneqq t^2 - \mathrm{t}(q)t + \mathrm{n}(q)$ *le polynôme caractéristique* de $q$. Notons qu'il vérifie $\chi_q(q) = 0$ par Cayley-Hamilton dans $\mathrm{M}_2(\mathbb{C})$,
4. $q^\star \coloneqq t\,1 - x\,I - y\,J - z\,K \ =\ \mathrm{t}(q) - q$, le *conjugué* de $q$, un élément de $\mathbb{H}$.

La trace $\mathrm{t}\colon \mathbb{H} \to \mathbb{R}$ est donc $\mathbb{R}$-linéaire et la norme $\mathrm{n}\colon \mathbb{H} \to \mathbb{R}$ est multiplicative : on a $\mathrm{n}(qq') = \mathrm{n}(q)\mathrm{n}(q')$ car det est multiplicatif. Le théorème de Cayley-Hamilton dans $\mathrm{M}_2(\mathbb{C})$ s'écrit $q^2 - \mathrm{t}(q)q + \mathrm{n}(q) \cdot 1 = 0$. Il est donc aussi valable dans $\mathbb{H}$ et s'écrit encore

$$\forall q \in \mathbb{H}, \quad qq^\star = q^\star q = \mathrm{n}(q) \cdot 1.$$

Ainsi, tout quaternion $q \neq 0$ est inversible et $q^{-1} = \frac{1}{\mathrm{n}(q)} q^\star$ dans $\mathbb{H}$. On a montré :

**Proposition 3.1.** $\mathbb{H}$ *est un corps gauche.*

[2] En pratique, $H$ sera souvent un sous-groupe de $G$.

[3] Un sous-anneau d'un anneau $A$ est une partie $B \subset A$ contenant 1 et telle que pour tout $x, y \in B$ on a $xy \in B$, $x + y \in B$ et $-x \in B$.