# Théorie des groupes
# Un théorème de Frobenius

AFFALOU Étienne

Octobre 2023

## Table des matières

On va démontrer un théorème de Frobenius sur les groupes fini. Celui-ci fournit une condition suffisante pour qu'un sous-groupe d'un groupe fini $G$ soit normal dans $G$.
Dans toute la suite, $G$ est un groupe fini d'ordre différent de 1 et $H$ est un sous-groupe de $G$.

# 1 Une première proposition

On donne une première condition suffisante pour que $H \trianglelefteq G$.

Proposition Si $[G : H] = 2$, alors $H \trianglelefteq G$.

Preuve :
Comme $[G : H] = 2$, $G \setminus H \neq \emptyset$. On peut donc prendre $g \in G \setminus H$.
Par définition des classes à gauche et des classes à droite, on a

$$G = H \cup gH \text{ et } G = H \cup Hg$$

D'où l'égalité $H \cup gH = H \cup Hg$. Ainsi,

$$gH = H \setminus (H \cup gH) = H \setminus (H \cup Hg) = Hg$$

Donc $gH = Hg$ et on a bien $H \trianglelefteq G$, comme annoncé.

En fait, notre proposition ne s'applique que pour certains groupes. En effet, l'hypothèse $[G : H] = 2$ fournit que $G$ est un groupe d'ordre pair ($|G| = 2|H|$). Donc si $G$ n'est pas d'ordre pair, $[G : H] \neq 2$ et la proposition est inutile. L'objet du théorème de Frobenius est de généraliser cette proposition pour qu'elle soit toujours utile.

# 2 Théorème de Frobenius

L'idée est de considérer le plus petit diviseur premier de l'ordre de $G$. Le théorème suivant est un exercice de **[1]**.

Théorème de Frobenius Soit $p$ le plus petit diviseur premier de $|G|$ . Si $[G : H] = p$, alors $H \trianglelefteq G$.

Preuve :
Considérons l'action par translation à gauche de $H$ sur $G/H$ définie par $\forall h \in H, \forall g \in G$,

$$h.(gH) = (hg)H$$

Les orbites de cette action forment une partition de $G/H$. On a donc la partition

$$G/H = \bigcup_{i=1}^{p} A_i$$

où $\forall i \in \{1, \cdots, p\}$, $A_i$ est une orbite de l'action. Montrons que toutes les orbites sont en fait des singletons.
Tout d'abord, on sait que $\forall i \in \{1, \cdots, p\}$, $|A_i| \mid |H|$. Or, le plus petit diviseur différent de 1 de $|H|$ est au moins $p$ par hypothèse ($|G| = [G : H]|H| = p|H|$ avec $p$ le plus petit diviseur premier de $|G|$).
Cela prouve que si $\exists i \in \{1, \cdots, p\}$ tel que $|A_i| \neq 1$, alors on a $|A_i| \geqslant p$. Mais dans ce cas, étant donné que

$$p = |G/H| = \sum_{i=1}^{p} |A_i|$$

on obtient une contradiction (les orbites sont non vides et $p \geqslant 2$). Ainsi, $\forall i \in \{1, \cdots, p\}, |A_i| = 1$. Cela montre que

$$\forall h \in H, \forall g \in G, (hg)H = h.(gH) = gH$$

D'où $\forall h \in H, \forall g \in G, g^{-1}hg \in H$. Finalement, on a bien $H \trianglelefteq G$.

Dans le cas où $p = 2$, on retrouve bien la première proposition. Ce théorème peut désormais s'appliquer à tous les groupes finis (sauf un, lequel ?). Dans la suite, on donne quelques applications de ce théorème.

# 3 Applications

## 3.1 Groupes d'ordre $pq^\alpha$

Soient $p$ et $q$ deux nombres premiers distincts. On suppose par exemple que $p < q$.

Proposition Si $\exists \alpha \in \mathbb{N}^*, |G| = pq^\alpha$, alors $G$ n'est pas simple.

Preuve :
Le premier théorème de Sylow nous donne l'existence d'un $q$-Sylow $H$ d'ordre $q^\alpha$. Le théorème de Frobenius assure que $H$ est distingué dans $G$ étant donné que $[G : H] = p$ avec $p < q$. Donc $G$ n'est pas un groupe simple.

Remarque : En utilisant le second théorème de Sylow, on obtient que le nombre $n_q$ de $q$-Sylow de $G$ vérifie

$$n_q \mid p \text{ et } n_q \equiv 1 \ [q]$$

On obtient alors $n_q = 1$ et donc $G$ n'est pas simple (voir par exemple l'exercice E de **[2]**).
Le second théorème de Sylow permet aussi de conclure. Cependant, on a réussi à montrer la proposition sans avoir recours à ce théorème de Sylow.

## 3.2 Dans le groupe symétrique $\mathfrak{S}_4$

Notons $\mathfrak{V}_4$ le sous-groupe de $\mathfrak{S}_4$ des doubles transpositions (c'est le groupe de Klein).

Proposition $\mathfrak{U}_4 \trianglelefteq \mathfrak{S}_4$ et $\mathfrak{V}_4 \trianglelefteq \mathfrak{U}_4$.

Preuve :
$\mathfrak{U}_4$ est d'indice 2 dans $\mathfrak{S}_4$ et $\mathfrak{V}_4$ est d'indice 2 dans $\mathfrak{U}_4$.

Remarque : En fait, le fait que $\mathfrak{U}_4 \trianglelefteq \mathfrak{S}_4$ vient du fait que $\mathfrak{U}_4$ est le noyau d'un morphisme de groupes (la signature). De plus, on a même $\mathfrak{V}_4 \trianglelefteq \mathfrak{S}_4$. Le résultat n'est donc pas très intéressant, mais la preuve est très courte.

## 3.3 Dans le groupe des quaternions $Q_8$

On va montrer que $Q_8$ est un groupe hamiltonien.

Définition Un groupe non abélien dont tous les sous-groupes sont distingués est dit hamiltonien.

Donnons d'abord les sous-groupes de $Q_8$.

Proposition Les sous-groupes de $Q_8$ sont

$$\{1\}, \{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}, Q_8$$

Preuve :
D'après le théorème de Lagrange, l'ordre des sous-groupes de $Q_8$ peut valoir $1, 2, 4$ ou $8$.
Il n'y a qu'un seul sous-groupe d'ordre 1 ($\{1\}$) et qu'un seul sous-groupe d'ordre 2 ($\{\pm 1\}$).
Les groupes d'ordre 4 sont les sous-groupes engendrés par 1 et $i$, $j$ ou bien $k$.
Enfin, $Q_8$ est le seul sous-groupe d'ordre 8.

Proposition $Q_8$ est un groupe hamiltonien.

Preuve :
On sait que $Q_8$ n'est pas abélien ($ij = -ji$ par exemple). De plus, tous ses sous-groupes sont distingués.
$\{1\}$ et $Q_8$ sont bien entendu distingués dans $Q_8$.
Étant donné que $i^2 = j^2 = k^2 = -1$, $\{\pm 1\} \trianglelefteq Q_8$ car $i \times (\pm 1) \times (-i) = -i^2 \times (\pm 1) = \pm 1$ par exemple.
Enfin, les trois sous-groupes qui restent sont distingués dans $Q_8$ d'après le théorème de Frobenius (ils sont d'indice 2).

Remarque : On aurait pu se passer du théorème de Frobenius pour la preuve, mais ce dernier raccourcit considérablement la longueur de la preuve (on se passe de longs calculs pour les trois derniers sous-groupes).

### 3.4 Dans le groupe diédral $D_n$

Pour tout $n \in \mathbb{N}^*$, on note $D_n$ le groupe diédral d'ordre $2n$.

Proposition $\forall n \in \mathbb{N}^*$, $D_n$ n'est pas simple.

Preuve :
Le sous-groupe engendré par la rotation $r$ est de cardinal $n$, donc d'indice 2 dans $D_n$, donc distingué dans $D_n$.

Remarque : Notre première proposition permet là encore de prouver le résultat rapidement.

Le théorème que l'on a démontré donne donc un critère de non simplicité (par exemple des groupes d'ordre $pq^\alpha$) et rend certaines démonstrations plus courtes.

Références :


— **[1]** Oraux X-ENS mathématiques vol. 1, *Serge Francinou, Hervé Gianella, Serge Nicolas*

— **[2]** Cours d'algèbre, *Daniel Perrin*