UNIVERSITÉ DE RENNES 1

**Théorie des Groupes et Géométrie**

*Feuille n°1*

# Sous-groupes distingués

## Exercice 1 (Sous-groupes d'indice 2)

Démontrez que dans un groupe, tout sous-groupe d'indice 2 est distingué.

## Exercice 2 (Produit de sous-groupes)

Soit $G$ un groupe. Si $S, T$ sont deux sous-groupes de $G$, on note $ST = \{st \in G; s \in S, t \in T\}$ l'ensemble des produits.

**1.** Démontrez que si $S$ ou $T$ est distingué dans $G$, alors $ST$ est un sous-groupe mais que ce n'est pas le cas en général. *Utilisez par exemple la règle d'or du contre-exemple : commencer par la situation la plus simple possible et la compliquer progressivement jusqu'à trouver un contre-exemple.*

**2.** Démontrez que : si $S$ *et* $T$ sont distingués, alors $ST$ aussi ; si de plus $S \cap T = 1$, on a un isomorphisme $ST \simeq S \times T$.

**3.** Démontrez que si $S$ et $T$ sont finis, alors $ST$ est fini et on a l'égalité de cardinaux : $|ST| = |S||T|/|S \cap T|$.
*Introduisez et étudiez une application $f : S \times T \to ST$.*

## Exercice 3 (Sous-groupe de Frattini des $p$-groupes)

Soit $G$ un groupe et $p$ un nombre premier.

**1.** Démontrez que le sous-groupe $G'$ engendré par les commutateurs $[x, y] := xyx^{-1}y^{-1}$ est distingué, et que le groupe quotient $G/G'$ est abélien.

**2.** Démontrez que le sous-groupe $G^p$ engendré par les puissances $p$-ièmes $x^p$ est distingué, et que le groupe quotient $G/G^p$ est « tué par $p$ » au sens où chacun de ses éléments a une puissance $p$-ième nulle.

**3.** Démontrez que $G/G'G^p$ est un $\mathbb{F}_p$-espace vectoriel.

*Si $G$ est un $p$-groupe fini, l'entier $r := \dim_{\mathbb{F}_p}(G/G'G^p)$ est fini et un théorème classique affirme que ses parties génératrices minimales sont toutes de même cardinal égal à $r$.*

## Exercice 4 (Lemme de Zassenhaus ou lemme du papillon)

Soient $G$ un groupe et $H', H, K', K$ des sous-groupes tels que $H' \lhd H$ et $K' \lhd K$. Montrez qu'on a un isomorphisme :

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{K'(H \cap K)}{K'(H' \cap K)}.$$

*On pourra démontrer que les deux membres sont isomorphes à $(H \cap K)/((H \cap K')(H' \cap K))$.*

## Exercice 5 (Groupes simples abéliens)

Démontrez qu'un groupe abélien est simple si et seulement s'il est cyclique d'ordre premier.

## Exercice 6 ($p$-groupes élémentaires abéliens)

Un $p$-groupe $G$ est dit *élémentaire abélien* s'il est abélien et vérifie $px = 0$ pour tout $x \in G$ (on dit que $G$ est *d'exposant* $p$).

**1.** Montrez qu'un $p$-groupe élémentaire abélien peut être muni d'une unique structure de $\mathbb{F}_p$-espace vectoriel compatible avec sa structure de groupe.

**2.** Montrez qu'un morphisme entre deux $p$-groupes élémentaires abéliens est $\mathbb{F}_p$-linéaire.

**3.** Calculez le groupe des automorphismes d'un $p$-groupe élémentaire abélien.

**4.** Soit $V = (\mathbb{Z}/2\mathbb{Z})^2$ le groupe de Klein. Calculez $\mathrm{Aut}(V)$ et démontrez que n'importe quelle permutation de l'ensemble $V \setminus \{1\}$ définit un automorphisme de $V$.

# Résolubilité

## Exercice 7 (Étude de $\mathfrak{S}_3$)

**1**. Donner les structures de cycles possibles dans $\mathfrak{S}_3$, le nombre d'éléments de $\mathfrak{S}_3$ ayant cette structure, et leur signature.

**2**. Décrire les sous-groupes de $\mathfrak{S}_3$, et ceux qui sont distingués dans $\mathfrak{S}_3$. Déterminer les sous-groupes de Sylow de $\mathfrak{S}_3$.

**3**. Trouver une suite de composition à facteurs abéliens de $\mathfrak{S}_3$.

## Exercice 8 (Suite dérivée de $\mathfrak{S}_4$)

On note $V$ le sous-groupe de $\mathfrak{S}_4$ composé des double-transpositions (produits de transpositions à supports disjoints) et 1.

**1**. Montrer que $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$.

**2**. Calculer les commutateurs $(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}$ et $(1,2,3)(1,2,4)(1,2,3)^{-1}(1,2,4)^{-1}$.

**3**. Montrer que $D(\mathfrak{S}_4) = \mathfrak{A}_4$.

**4**. Montrer que $V \subset D(\mathfrak{A}_4)$.

**5**. Vérifier que $V$ est distingué dans $\mathfrak{A}_4$ et que le quotient $\mathfrak{A}_4/V$ est un groupe abélien. En déduire que $D(\mathfrak{A}_4) \subset V$.

**6**. En déduire $D^2(\mathfrak{S}_4)$.

**7**. Calculer les autres sous-groupes dérivés de $\mathfrak{S}_4$.

## Exercice 9 (Transformations affines de la droite)

Soient $k$ un corps et $G$ l'ensemble des applications $f : k \to k$ de la forme $f(x) = ax + b$ avec $a, b \in k$, $a \neq 0$. Démontrez que $G$ est un groupe résoluble.

## Exercice 10 (Théorème de Feit-Thompson)

Montrer que les assertions suivantes sont équivalentes :

**1**. Tout groupe d'ordre impair est résoluble.

**2**. Tout groupe fini simple non-abélien est d'ordre pair.

*Le théorème de Feit-Thompson (1962) montre qu'elles sont vraies.*

# Actions de groupes

Si $p$ est un nombre premier, on appelle *p-groupe* un groupe fini non trivial d'ordre une puissance $p$.

## Exercice 11 (Centre d'un $p$-groupe)

Montrer que le centre d'un $p$-groupe n'est pas réduit à l'élément neutre.
*Regardez la partition en orbites pour l'action de $G$ par conjugaison sur lui-même.*

## Exercice 12 (Groupes d'ordre $p^2$ et $p^3$)

**1**. Montrer que si le quotient d'un groupe par son centre est cyclique alors le groupe est abélien, donc égal à son centre.

**2**. Montrer qu'un groupe d'ordre $p^2$ est abélien. En déduire la liste des groupes d'ordre $p^2$.

**3**. Soit $G$ un groupe non abélien d'ordre $p^3$ et $Z$ son centre. Montrez que :

$$\text{(i) } Z \text{ est d'ordre } p, \qquad \text{(ii) } G/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2, \qquad \text{(iii) } D(G) = Z.$$

## Exercice 13 (Théorème de Cauchy)

Démontrez que tout groupe fini d'ordre divisible par un nombre premier $p$ possède un élément d'ordre $p$. *On pourra faire agir par permutation circulaire le groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des $p$-uplets $(x_1, \ldots, x_p)$ de $G$ tels que $x_1 \cdots x_p = 1$.*

### **Exercice 14** (Application des formules de comptage)

On fixe une action d'un groupe $G$ sur un ensemble fini $E$.

1. On suppose que l'ordre de $G$ est 15, que le cardinal de $E$ est 17 et que $E$ n'a pas de point fixé par tous les éléments du groupe $G$. Déterminer le nombre d'orbites et le cardinal de chacune d'elles.
2. Montrer que toute action d'un groupe d'ordre 143 sur un ensemble de cardinal 25 possède un point fixe.

### **Exercice 15** (Sur la transitivité multiple)

Soit $k \geq 2$ entier. On dit que l'action d'un groupe $G$ sur un ensemble $X$ de cardinal au moins $k$ est *$k$-transitive* si pour tout $x_1 \ldots, x_k \in X$ distincts et tout $y_1, \ldots, y_k \in X$ distincts, il existe $g \in G$ tel que $gx_i = y_i$ pour $i = 1, \ldots, k$.

1. Montrer qu'une action est $k$-transitive si et seulement si elle est transitive et que l'action du stabilisateur de tout point $x \in X$ sur $X \setminus \{x\}$ est $(k-1)$-transitive.
2. Montrer qu'une action est $k$-transitive si et seulement si elle est transitive et que l'action d'un stabilisateur d'un point $x \in X$ sur $X \setminus \{x\}$ est $(k-1)$-transitive.

## Produit semi-direct

Dans les deux exercices suivants, on utilisera librement les théorèmes de Sylow sur l'existence des sous-groupes de Sylow et les congruences classiques sur leur nombre.

### **Exercice 16** (Groupes d'ordre $pq$)

Soient $p < q$ deux nombres premiers. Soit $G$ un groupe d'ordre $pq$.

1. Montrer que $s_q = 1$ où le nombre $s_q$ est le nombre de $q$-Sylow de $G$.
2. En déduire que $G$ est un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.
3. Montrer que si $p \nmid q-1$ alors $G$ est cyclique.
4. Montrer que si $p|q-1$ alors il existe à isomorphisme près deux groupes d'ordre $pq$ : le groupe cyclique d'ordre $pq$ et le groupe non-abélien d'ordre $pq$. (Remarque : le groupe diédral est l'exemple le plus simple du second cas.)

### **Exercice 17** (Groupes finis résolubles)

1. Montrer par récurrence qu'un $p$-groupe est toujours résoluble.
2. Soient $p, q$ deux nombres premiers distincts. Montrer qu'un groupe de cardinal $pq$ est toujours résoluble.
   *Supposer $p > q$ et considérer un $p$-Sylow.*
3. Soit $G$ un groupe d'ordre 12. Montrer que $G$ est résoluble.
   *En supposant les 3-Sylow non distingués, compter le nombre d'éléments d'ordre 3.*
4. Soient $p, q$ deux nombres premiers distincts. Montrer qu'un groupe de cardinal $p^2q$ est toujours résoluble.

### **Exercice 18** (Groupe triangulaire supérieur)

1. Soit $k$ un corps. Montrez que le groupe de Heisenberg $G = U_3(k)$ des matrices carrées triangulaires supérieures de taille 3 avec des 1 sur la diagonale est résoluble.
2. On suppose désormais que $k = \mathbb{F}_3$. Montrez que tout élément $x \in G$ vérifie $x^3 = 1$ mais $G$ n'est pas abélien. (On rappelle que si tout élément vérifie $x^2 = 1$, alors est abélien. On ne peut donc pas remplacer 2 par 3 dans cet énoncé.)
3. Le groupe $G = U_3(\mathbb{F}_3)$ est-il un produit semi-direct ?

### **Exercice 19** (Holomorphe d'un groupe)

On appelle *holomorphe* d'un groupe de $G$ le produit semi-direct $\mathrm{Hol}(G) = G \rtimes_\varphi \mathrm{Aut}(G)$ défini par l'action tautologique $\varphi = \mathrm{Id} : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$ de $\mathrm{Aut}(G)$ sur $G$. Écrivez les formules décrivant le produit et l'inverse dans $\mathrm{Hol}(G)$.

### Exercice 20 (Sur-groupes et conjugaisons)

1. Soient $G$ un groupe et $f : G \to G$ un automorphisme. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que $f$ est la restriction à $G$ d'un automorphisme intérieur (ou conjugaison) de $G'$.
*On pourra prendre pour $G'$ l'holomorphe $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$.*
2. Soient $G$ un groupe fini et $x, y \in G$ deux éléments de même ordre. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que $x$ et $y$ sont conjugués dans $G'$.
*On pourra prendre pour $G'$ le groupe symétrique $\mathfrak{S}_G$.*

### Exercice 21 (Automorphismes du groupe diédral)

Soit $n \geq 3$ et $\mathbb{D}_n$ le groupe diédral engendré par deux élements $r, s$ satisfaisant les relations $r^n = s^2 = (rs)^2 = 1$.

1. On rappelle que tout élément $x \in \mathbb{D}_n$ peut s'écrire d'une unique manière sous la forme $x = s^\epsilon r^i$ avec $\epsilon \in \{0, 1\}$ et $i \in \mathbb{Z}/n\mathbb{Z}$. Montrez que le produit de $x = s^\epsilon r^i$ avec $y = s^\eta r^j$ est donné par la formule $xy = s^{\epsilon+\eta} r^{(1-2\eta)i+j}$.
2. Montrez que pour tout morphisme de groupes $f : \mathbb{D}_n \to H$, les éléments $R = f(r)$ et $S = f(s)$ vérifient les relations $R^n = S^2 = (RS)^2 = 1$. Réciproquement montrez que pour tout couple $(R, S) \in H^2$ tel que $R^n = S^2 = (RS)^2 = 1$ il existe un unique morphisme de groupes $f : \mathbb{D}_n \to H$ tel que $f(r) = R$ et $f(s) = S$.
3. Déduisez de la question précédente que les automorphismes $f : \mathbb{D}_n \to \mathbb{D}_n$ sont les morphismes $f = f_{i,j}$ déterminés par $f(r) = r^i$ et $f(s) = sr^j$, pour $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $j \in \mathbb{Z}/n\mathbb{Z}$.
4. Montrez que $\mathrm{Aut}(\mathbb{D}_n)$ est l'holomorphe de $\mathbb{Z}/n\mathbb{Z}$.
*On pourra montrer que $\mathrm{Aut}(\mathbb{D}_n) = N \rtimes H$ avec $N = \{f_{1,j};\ j \in \mathbb{Z}/n\mathbb{Z}\}$ et $H := \{f_{i,0};\ i \in (\mathbb{Z}/n\mathbb{Z})^\times\}$.*

### Exercice 22 (Ordre du produit de deux éléments)

Soit $G$ un groupe et $x, y$ deux éléments d'ordres finis égaux respectivement à $m$ et $n$.

1. On suppose que $x$ et $y$ commutent et que $m$ et $n$ sont premiers entre eux. Démontrez que le sous-groupe engendré par $x$ et $y$ est isomorphe au produit direct $\langle x \rangle \times \langle y \rangle$ et que $xy$ est d'ordre $mn$.
2. Peut-on étendre le résultat sur l'ordre au cas où $m$ et $n$ ne sont pas premiers entre eux ?
3. Peut-on étendre le résultat sur l'ordre au cas où $x$ et $y$ ne commutent pas ?

## Groupes symétriques et alternés

### Exercice 23 ($\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6)

1. Soit $H$ un sous-groupe d'ordre 6 de $\mathfrak{A}_4$. Montrer que pour tout $g \in \mathfrak{A}_4$, on a $g^2 \in H$.
2. En déduire que $H$ contient tous les 3-cycles.
3. Conclure (éventuellement de deux manières...).
*La réciproque au théorème de Lagrange est donc fausse. Il s'agit du plus petit contre-exemple.*

### Exercice 24 (Sous-groupes d'indice 2 de $\mathfrak{S}_n$)

1. Soit $f : \mathfrak{S}_n \to \{\pm 1\}$ un homomorphisme de groupes. Démontrer que les transpositions ont toutes la même image. En déduire que $f$ est soit constante soit la signature.
2. Soit $G$ d'indice 2 dans $\mathfrak{S}_n$. Démontrer que $G$ est distingué puis que $G = \mathfrak{A}_n$.

### Exercice 25 (Sous-groupes distingués de $\mathfrak{S}_n$)

Le but de l'exercice est de déterminer les sous-groupes distingués de $\mathfrak{S}_n$ (pour $n \geqslant 5$).

1. Soit $H$ un sous-groupe distingué de $\mathfrak{S}_n$. Montrer que $H \cap \mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{A}_n$. En déduire que $H$ contient $\mathfrak{A}_n$ ou que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$.
2. On suppose que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$. Montrer que la restriction à $H$ du morphisme signature est injective. Montrer que dans ce cas que tous les éléments de $H$ sont dans le centre de $\mathfrak{S}_n$ et en déduire que $H = \{\mathrm{Id}\}$.
3. On suppose que $H$ contient $\mathfrak{A}_n$. Montrer alors que $H = \mathfrak{S}_n$ ou $H = \mathfrak{A}_n$ suivant l'indice de $H$ dans $\mathfrak{S}_n$.
4. Conclure : si $n \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$..