UNIVERSITÉ DE RENNES 1

Théorie des Groupes et Géométrie

TD 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 (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 4 (Groupes simples abéliens)

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

Résolubilité

Exercice 5 (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 6 (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 7 (Groupe triangulaire supérieur)

1. Montrer que le groupe de Heisenberg $H = U_3(k)$ des matrices carrées triangulaires supérieures de taille 3 avec des 1 sur la diagonale est résoluble.
2. Montrer que le groupe B des matrices carrées triangulaires supérieures de taille 3 inversibles est résoluble.

Bien entendu, le résultat est aussi vrai pour les matrices triangulaires de taille n.

Exercice 8 (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.

p-groupes

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

Exercice 9 (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 10 (p-groupes élémentaires abéliens)

Un p-groupe G est dit *élémentaire abélien* s'il est abélien et vérifie $x^p = 1$ 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.

Exercice 11 (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 12 (Sous-groupes de $U_3(\mathbb{F}_3)$)

On note $U = U_3(\mathbb{F}_3)$ le groupe des matrices carrées triangulaires supérieures de taille 3 avec des 1 sur la diagonale.

1. Montrer que U est un groupe non abélien dans lequel $x^3 = 1$ pour tout x, et calculer son cardinal.
2. Calculez le centre Z de U.
3. Décrivez les sous-groupes d'ordre 3 et donnez leur nombre.
4. Montrez que les sous-groupes d'ordre 9 contiennent tous le centre. En vous ramenant à U/Z, déduisez-en qu'ils sont tous distingués et donnez leur nombre.
5. Décrivez les sous-groupes d'ordre 9 de la manière suivante : notez $f : U \to (\mathbb{Z}/3\mathbb{Z})^2$ le morphisme qui à une matrice A associe les deux coefficients de sa première surdiagonale, et montrez que la considération des noyaux $H = \ker(\varphi \circ f)$ fournit suffisamment de sous-groupes d'ordre 9 à partir de formes $\mathbb{F}_3$-linéaires φ sur l'espace $E = (\mathbb{F}_3)^2$.

Actions de groupes

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 $X \smallsetminus \{x\}$ 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 $X \smallsetminus \{x\}$ est $(k-1)$-transitive.

Exercice 16 (Lemme du ping-pong)

Soit G un groupe agissant sur un ensemble E. Soit E_1, E_2 deux parties non vides et disjointes de E et $g, h \in G$ deux éléments tels que $g^k(E_1) \subset E_2$ et $h^k(E_2) \subset E_1$ pour tout $k \in \mathbb{Z} \smallsetminus \{0\}$.

1. Montrer qu'aucun « mot » de la forme $g^{k_1}h^{l_1}g^{k_2}h^{l_2}\cdots g^{k_d}h^{l_d}g^{k_{d+1}}$, avec $k_i, l_j \neq 0$, n'est égal à l'élément neutre.

2. En déduire en utilisant une conjugaison, qu'aucun mot du groupe engendré par g et h autre que le mot vide n'est égal à l'élément neutre. On dit alors que le groupe engendré par g et h est un *groupe libre*.

3. Montrer le sous groupe de $SL(2, \mathbb{Z})$ engendré par

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ et } B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

est libre, en considérant l'action naturelle sur $\mathbb{R}^2$ et les domaines $\{(x, y) \in \mathbb{R}^2, |x| < |y|\}$ et $\{(x, y) \in \mathbb{R}^2, |x| > |y|\}$ délimités par les diagonales.

Ordre des éléments

Exercice 17 (Ordre d'un produit)

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 xy est d'ordre mn.

2. Peut-on étendre ce résultat au cas où m et n ne sont pas premiers entre eux ?

3. Peut-on étendre ce résultat au cas où x et y ne commutent pas ?

Exercice 18 (Sous-groupes finis du groupe multiplicatif d'un corps)

On note $\varphi(n)$ l'indicateur d'Euler de n, égal à $|(\mathbb{Z}/n\mathbb{Z})^\times|$ ou encore au nombre d'entiers $1 \leq k \leq n$ premiers avec n.

1. Rappeler pourquoi $\sum_{d|n} \varphi(d) = n$.
Partitionner $\mathbb{Z}/n\mathbb{Z}$ en fonction de l'ordre de ses éléments.

2. Démontrer que tout sous-groupe fini H du groupe multiplicatif d'un corps (commutatif) k est cyclique :

(i) montrez que pour chaque $d|n$ l'ensemble $H_d = \{x \in H, x^d = 1\}$ est d'ordre au plus d,

(ii) montrez que l'ensemble H_d^* des éléments d'ordre d dans H est d'ordre 0 ou $\varphi(d)$,

(iii) concluez en regardant la partition $H = \amalg_{d|n} H_d^*$.

Théorème de Sylow et produit semi-direct

Exercice 19 (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 20 (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.

Groupes symétriques et alternés

Exercice 21 ($\mathfrak{A}_4$ 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 22 (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 23 (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 $\mathfrak{S}_n$..