

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

TD1 : GÉNÉRALITÉS SUR LES GROUPES

Exercice 1. Soit G groupe abélien d'ordre pq avec p, q deux nombres premiers distincts. Montrer que le groupe est cyclique.

Exercice 2. Soit G un groupe fini de cardinal n et m un entier premier avec n . Montrer que, pour tout y élément de G , il existe un unique x élément de G tel que $x^m = y$.

Exercice 3. Soit (G, \cdot) un groupe fini de cardinal n . On suppose que, tout x élément de G , satisfait l'égalité $x^2 = e$.

1. Montrer que G est un groupe commutatif.
2. Soit $A = \{a_1, \dots, a_p\}$ une partie génératrice de G , montrer que :

$$\forall x \in G, \quad \exists (\epsilon_1, \dots, \epsilon_p) \in (\mathbb{Z}/2\mathbb{Z})^p \text{ tels que, } x = a_1^{\epsilon_1} \dots a_p^{\epsilon_p}.$$

3. On suppose, dans les questions suivantes, que A est une partie génératrice de cardinal minimum p . Montrer que l'écriture :

$$x = a_1^{\epsilon_1} \dots a_p^{\epsilon_p}$$

est unique.

4. Soit Φ l'application définie par :

$$\begin{aligned} \Phi : G &\rightarrow (\mathbb{Z}/2\mathbb{Z})^p \\ x &\mapsto (\epsilon_1, \dots, \epsilon_p). \end{aligned}$$

Montrer que Φ est bien définie et que c'est un isomorphisme de groupes. En déduire que le cardinal de G est 2^p .

Exercice 4. Soit G un groupe abélien fini, a et b deux éléments de G . Le but de l'exercice est de voir quelles sont les valeurs que $|a.b|$ peut prendre en fonction de $|a|$ et $|b|$.

1. Soit p entier non nul tel que $(ab)^p = e$, soit m le ppcm de p et $|a|$, n le ppcm de p et $|b|$. Montrer que $|a|$ divise n et que $|b|$ divise m .
2. En déduire que lorsque $|a|$ et $|b|$ sont premiers entre eux, alors $|a.b| = |a|.|b|$.
3. Montrer que le résultat précédent est faux sans cette hypothèse.
4. Notons d le pgcd de $|a|$ et $|b|$ et M le ppcm de $|a|$ et $|b|$. En utilisant la première question, montrer que : $\frac{M}{d}$ divise $|a.b|$ et que $|a.b|$ divise M .
5. En choisissant des éléments convenables dans le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, vérifier que l'on peut avoir :

$$\frac{M}{d} < |a.b| < M.$$

6. Montrer qu'il existe toujours dans G un élément d'ordre M .
7. Si G est non abélien, donner un exemple avec a et b d'ordres 2 et $a.b$ d'ordre infini.

Exercice 5. Montrer que tout sous-groupe d'indice 2 est distingué.

Exercice 6. Soit p un nombre premier, on pose

$$U_p = \left\{ e^{\frac{2i\pi a}{p^\alpha}}, a \in \mathbb{Z}, \text{pgcd}(a, p) = 1, \alpha \in \mathbb{N} \right\}$$

1. Montrer que U_p est un groupe infini dont tous les éléments sont d'ordre fini. Trouver l'ordre de $e^{\frac{2i\pi a}{p^\alpha}}$, pour a entier premier avec p et $\alpha \in \mathbb{N}$.
2. On va montrer que tout sous-groupe strict de U_p est cyclique.
 - (a) Soit G_α le sous groupe engendré par $e^{\frac{2i\pi}{p^\alpha}}$. Montrer que si $\beta \leq \alpha$ alors $G_\beta \subset G_\alpha$.
 - (b) En déduire que $U_p = \bigcup G_\alpha$.
 - (c) Soit H un sous groupe distinct de G_α pour tout α . Considérer pour α fixé un $x \in H$ qui n'est pas dans G_α et le minimum des entiers n tels que x soit dans G_n . Montrer que $H = U_p$.
3. En déduire que U_p n'est pas le produit de deux sous-groupes.

Exercice 7. Faire la liste, à isomorphisme près, des groupes de cardinal inférieur ou égal à 7.

Exercice 8. Soit n un entier naturel supérieur ou égal à 2, montrer que le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (noté $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$) est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

Exercice 9. Montrer qu'un sous-groupe $H \subset G$ d'un groupe G est distingué ssi il existe un groupe G' et un morphisme de groupe $f: G \rightarrow G'$ tel que $H = \text{Ker}(f)$.

Exercice 10. Montrer que la relation \triangleleft définie sur les groupes n'est ni une relation d'équivalence, ni une relation d'ordre.

Exercice 11. Soit G_1 et G_2 deux groupes.

1. Montrer que $G_1 \times G_2 \cong G_2 \times G_1$.
2. Montrer que $G_1 \triangleleft G_1 \times G_2$ et que $G_1 \times G_2 / G_1 \cong G_2$.
3. (a) A-t-on $G_1 \triangleleft G_1 \rtimes_\varphi G_2$ et $G_1 \rtimes_\varphi G_2 / G_1 \cong G_2$ pour tout morphisme $\varphi: G_1 \rightarrow \text{Aut}(G_2)$?
 (b) A-t-on $G_2 \triangleleft G_1 \rtimes_\varphi G_2$ et $G_1 \rtimes_\varphi G_2 / G_2 \cong G_1$ pour tout morphisme $\varphi: G_1 \rightarrow \text{Aut}(G_2)$?

Exercice 12. Montrer qu'action transitive et fidèle par un groupe abélien est simplement transitive.

Exercice 13. Soit G un groupe. On appelle *commutateur* de G tout élément de la forme $[x, y] := x^{-1}.y^{-1}.x.y$ avec $x, y \in G$, et on note $D(G) \subset G$ le sous-groupe, appelé *dérivé*, engendré par ces commutateurs.

1. Montrer que $D(G) = \{E\}$ ssi G est abélien.
2. Montrer que $D(G) \triangleleft G$.
3. Montrer que $G/D(G)$ est abélien.
4. Montrer que, pour tout $H \triangleleft G$, G/H est abélien ssi $D(G) \subset H$.

Exercice 14. On dit qu'un groupe G est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$. On dit de plus qu'il est *cyclique* s'il est aussi de cardinal fini ; on appelle alors *ordre* de G le cardinal de G .

1. Soit G un groupe monogène et $H \subset G$ un sous-groupe.
 - (a) Montrer que, si G est non-cyclique, alors H est soit trivial, soit monogène non-cyclique.
 - (b) Montrer que, si G est cyclique, alors H est cyclique et l'ordre de H divise l'ordre de G .
2. Soit G un groupe monogène engendré par $g \in G$.
 - (a) Montrer que, si G est non-cyclique, alors les seuls générateurs de G sont g et g^{-1} .
 - (b) Montrer que, si G est cyclique d'ordre $n \in \mathbb{N}^*$, alors les seuls généralteurs de G sont les g^k , avec $k \in \llbracket 1, n-1 \rrbracket$ premier avec n .
3. Soit G un groupe d'ordre p premier.
 - (a) Montrer que G est cyclique.
 - (b) Montrer que tout élément non nul de G est générateur.

Exercice 15. Soit G un groupe. On dit que deux éléments $g_1, g_2 \in G$ sont *conjugués* s'il existe $h \in G$ tel que $g_1 = h^{-1}.g_2.h$.

1. Montrer que la relation définie par $(g_1 \sim g_2) \Leftrightarrow (g_1, g_2 \text{ conjugués})$ est une relation d'équivalence.

On appelle *classes de conjugaisons* les classes de la relation \sim et on note \mathcal{C} l'ensemble des classes d'équivalence.

Soit a une action de G sur un ensemble X .

2. Montrer que si $g_1, g_2 \in G$ sont conjugués, alors il existe une bijection entre les points fixes de g_1 pour a et ceux de g_2 .

Pour toute classe de conjugaison $c \in \mathcal{C}$, on note n_c son cardinal, et k_c le cardinal commun des ensembles des points fixes pour a de ses éléments. On note aussi N l'ordre de G et K le nombre d'orbite de a .

3. Montrer que $KN = \sum_{c \in \mathcal{C}} k_c n_c$.

Exercice 16. Soit G un groupe.

1. Montrer que, pour tout $g \in G$, l'application $\text{conj}_g : \begin{array}{ccc} G & \longrightarrow & G \\ g' & \longmapsto & g^{-1}.g'.g \end{array}$ est un automorphisme de groupe.

On note $\text{Int}(G) := \{\text{conj}_g \mid g \in G\}$ et on appelle *automorphismes intérieurs* ses éléments.

2. Montrer que $\text{Int}(G) \triangleleft \text{Aut}(G)$.
3. Montrer que $\text{Int}(G) \cong G/Z(G)$.

Exercice 17. Soit $p \in \mathbb{N}^*$ un nombre premier et G un groupe fini tel que p divise $|G|$. On note $\Omega := \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = e\}$.

1. Montrer que $\mathbb{Z}/p\mathbb{Z}$ agit sur Ω par permutation circulaire des termes des p -uplets.
2. Montrer que les orbites pour cette action sont de cardinal 1 ou p .
3. Déterminer le cardinal de l'orbite de (e, \dots, e) .
4. (théorème de Cauchy) En déduire qu'il existe au moins $p - 1$ éléments de G d'ordre p .

Exercice 18. Soit $p \in \mathbb{N}^*$ un nombre premier. On dit qu'un groupe est un p -groupe si son cardinal est une puissance de p . On dit qu'un sous-groupe $H \subset G$ est un p -Sylow de G si c'est un p -groupe de cardinal maximal, c'est-à-dire tel que $p \nmid \frac{|G|}{|H|}$.

1. (a) Montrer que le cardinal de $\text{GL}_n(\mathbb{F}_p)$ est $p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1} (p^k - 1)$.
(b) Montrer que les matrices triangulaires supérieures ayant des 1 sur la diagonale forment un p -Sylow de $\text{GL}_n(\mathbb{F}_p)$.
2. Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$, $H \subset G$ un sous-groupe et $S \subset G$ un p -Sylow de G . On considère l'action par translation à gauche de H sur l'ensemble des classes à gauche de S .
(a) Montrer que, pour toute classe à gauche $g.S$, $\text{Stab}(g.S) = g.S.g^{-1} \cap H$.
(b) Montrer que, pour tout $g \in G$, $\text{Stab}(g.S)$ est p -groupe dont le cardinal divise celui de H .
(c) Soit $g \in G$, montrer que, si $\text{Stab}(g.S)$ n'est pas un p -Sylow de H , alors p divise $|\mathcal{O}(g.S)|$.
(d) Montrer qu'il existe $g \in G$ tel que $g.S.g^{-1} \cap H$ est un p -Sylow de H .
3. (a) Montrer que, pour tout n , il existe un monomorphisme de groupe envoyant \mathfrak{S}_n dans $\text{GL}_n(\mathbb{F}_p)$.
(b) Montrer que, pour tout groupe G de cardinal $n \in \mathbb{N}^*$, il existe un monomorphisme de groupe envoyant G dans $\text{GL}_n(\mathbb{F}_p)$.
(c) (premier théorème de Sylow) Montrer que tout groupe fini possède au moins un p -Sylow.
4. (a) Montrer que si S_1 et S_2 sont deux p -Sylow d'un groupe fini G , alors il existe $g \in G$ tel que $g.S_1.g^{-1} \cap S_2$ soit un p -Sylow de S_2 .
(b) (deuxième théorème de Sylow) Montrer que tous les p -Sylow d'un groupe fini sont conjugués.
(c) Montrer qu'un p -Sylow d'un groupe fini G est distingué ssi il est l'unique p -Sylow de G .
(a) Montrer qu'un groupe fini G agit par conjugaison sur l'ensemble de ses p -Sylow et que cette action ne possède qu'une seule orbite.

- (b) (troisième théorème de Sylow, partie un) Montrer que le nombre de p -Sylow d'un groupe fini G divise $|G|$.
5. (a) Soit G un p -groupe agissant sur un ensemble X . Montrer que $|X| \cong |\text{Fix}(G)| \pmod{p}$.
- (b) Soit S un p -Sylow d'un groupe fini G . On considère l'action par conjugaison de S sur l'ensemble des p -Sylow de G et on fixe $S' \in \text{Fix}(S)$.
- Montrer que $S' \triangleleft \langle S \cup S' \rangle$.
 - Montrer que S et S' sont des p -Sylow de $\langle S \cup S' \rangle$ et en déduire que $S' = S$.
- (c) (troisième théorème de Sylow, partie deux) Montrer que le nombre de p -Sylow d'un groupe fini G est congru à 1 modulo p .
6. Soit G un groupe de cardinal p^2q avec p et q deux nombres premiers distincts.
- Montrer que G n'est pas simple.
 - Montrer que, si $q \nmid p^2 - 1$ et $p \nmid q - 1$, alors G est abélien.

Exercice 19. Montrer que le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ agit sur $\mathbb{Z}/8\mathbb{Z}$. Décrire les orbites et calculer leurs cardinaux en utilisant la formule des classes.

Exercice 20. Soit G un groupe fini à 21 éléments opérant sur un ensemble à 11 éléments. Montrer qu'il existe au moins un point fixe sous l'action de G .

Exercice 21. On cherche le nombre de colliers de 67 perles formés de 2 rouges, 7 bleues et 2 noires et 56 vertes.

- Montrer que l'on peut considérer les colliers comme des sommets colorés d'un polygone régulier à 67 côtés et que sur cet ensemble agit le groupe diédral D_{67} .
- Montrer que le nombre de colliers n est égal au nombre d'orbites dans l'action du groupe.
- Calculer $|\text{Fix}(g)|$ en séparant les cas suivants que g soit une symétrie, l'identité ou une rotation. On utilisera à bon escient que 67 est impair, premier, et que 7 est impair.
- Conclure.