Université Saclay-Paris-Sud Feuille de TD 3 M303

Exercice 1. Étant donnés un groupe G et H un sous-groupe de G, montrer que les équivalences suivantes sont vérifiées :

$$\forall g \in G,\ gHg^{-1} \subset H \iff \forall g \in G,\ gHg^{-1} = H.$$

Exercice 2. Soit G un groupe. Soient $x, y, z \in G$ et soit N un sous groupe distingué de G tels que

$$y^7 \in N,\ x^5 \in N \ \text{ et } \ y^{-1}zxz^{-1} \in N.$$

Montrer que x et y sont dans N.

Exercice 3.

1. Montrer que l'ensemble G des matrices de $M_2(\mathbb{Z}/5\mathbb{Z})$ triangulaires supérieures de déterminant non nul forme un sous-groupe de $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ qui est non commutatif.
2. Calculer le centre de G. Le groupe G est-il distingué dans $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$?
3. Calculer le cardinal de G et celui de $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$.
4. Montrer que le sous-ensemble K de G formé des matrices avec des 1 sur la diagonale est un sous-groupe commutatif distingué de G isomorphe au groupe additif $\mathbb{Z}/5\mathbb{Z}$.
5. Montrer que l'ensemble des matrices diagonales forme un sous-groupe commutatif de G qui n'est pas distingué dans G.

Exercice 4. Soit G un groupe non abélien et Z son centre. Montrer que G/Z n'est pas monogène.

Exercice 5. Résoudre dans $\mathbb{Z}$ l'équation $2^x \equiv 1 \mod 55$.

Exercice 6. Soit G un groupe, soit $H \triangleleft G$ et soit $\pi_H : G \to G/H$ la projection canonique. Montrer qu'il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H. Elle est donnée par $E \mapsto \pi_H(E)$ de réciproque $\mathcal{E} \mapsto \pi_H^{-1}(\mathcal{E})$.

Exercice 7. Soient G un groupe et

$$D(G) = \langle aba^{-1}b^{-1}, a, b \in G \rangle$$

le sous-groupe *engendré* par les commutateurs de G (éléments de la forme $aba^{-1}b^{-1}$) que l'on appelle également le groupe dérivé.

1. Montrer que pour tout morphisme f de G dans G, on a $f(D(G)) \subset D(G)$. En déduire que $D(G)$ est un sous-groupe distingué de G.
2. Montrer que $G/D(G)$ est abélien.
3. Soit N un sous-groupe distingué de G. Montrez que G/N est abélien si et seulement si $D(G) \subset N$.
4. Soit A un groupe abélien et $f : G \to A$ un morphisme de groupe. Montrer que $D(G) \subset Ker(f)$. En déduire qu'il existe un unique morphisme de groupes $\bar{f} : G/D(G) \to A$ tel que $\bar{f} \circ p = f$ où $p : G \to G/D(G)$ est la surjection canonique.

Exercice 8. Montrer que si G fini, et $H \subset G$ sous-groupe strict alors G n'est pas égal à l'union des conjugués de H.

Exercice 9. Soient G un groupe fini et p le plus petit facteur premier de l'ordre n de G. On suppose qu'il existe un sous-groupe H distingué dans G et d'ordre p. Montrer que H est dans le centre de G (on pourra faire opérer G par conjugaison sur H).

Exercice 10. p premier et G fini simple de Cardinal divisible par p^2. Montrer que tout sous-groupe strict de G a indice au moins $2p$. (*Indication : on pourra montrer qu'il n'y a pas de morphisme* $G \longrightarrow S_k$ *non trivial pour* $1 \leq k \leq 2p-1$.) Reciproquement, pour p impair, montrer qu'il existe un groupe simple de cardinal divisible par p^2 et un sous-groupe d'indice $2p$.

Exercice 11. On fait opérer le groupe multiplicatif $G = (\mathbb{Z}/8\mathbb{Z})^\times$ sur l'ensemble $X = \mathbb{Z}/8\mathbb{Z}$ par $a \cdot x = ax$.

1. Calculer les orbites et le stabilisateur de chacun des éléments de X.
2. Soit n un entier > 1. On fait opérer le groupe $G = (\mathbb{Z}/n\mathbb{Z})^\times$ sur l'ensemble $X = \mathbb{Z}/n\mathbb{Z}$ par $a \cdot x = ax$. Écrire la formule des classes correspondante (on pourra définir une bijection entre l'ensemble des orbites et les diviseurs de n).

Exercice 12. Soit $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ que l'on dispose dans un carré

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array}$$

Soit G le groupe de symétrie du carré. On fait agir G sur X à travers le carré. Écrire l'équation aux classes dans ce contexte.

Exercice 13. Soit E un ensemble fini muni d'une action $G \times E \to E$ d'un groupe fini G. On note

$$E_G := \{x \in E \mid \forall g \in G,\ g \cdot x = x\}$$

qu'on appelle l'*ensemble des points fixes pour l'action* de G sur E.

1. On suppose que
$$E_G = \emptyset\ ,\ \mathrm{card}(G) = 15 \text{ et } \mathrm{card}(E) = 17.$$
Quel est alors le nombre d'orbites et le cardinal de chacune d'elles ?
2. On suppose que
$$\mathrm{card}(G) = 33 \text{ et } \mathrm{card}(E) = 19.$$
Montrer que E_G ne peut pas être vide.

Exercice 14. Soit H un sous-groupe distingué d'un groupe G qui agit transitivement sur un ensemble X. Montrer que les orbites de l'action (induite de l'action de G) de H sur X ont toutes même cardinal.

Exercice 15. Soit une action d'un groupe G sur un ensemble. Montrer que tous les éléments d'une même orbite ont même stabilisateur si et seulement si ce stabilisateur est un sous-groupe distingué de G.

Exercice 16. Soit G un groupe de cardinal pq avec p et q premiers et distincts. On suppose que G opère sur un ensemble X de cardinal $n = pq - p - q$. Montrer qu'il existe au moins un point fixe par cette action.

Exercice 17. Soit $(G, \cdot)$ un groupe dont on note 1 l'élément neutre et E un G-ensemble, c'est-à-dire un ensemble muni d'une action de G notée $G \times E \to E$, $(g, x) \mapsto g \cdot x$. On suppose que G et E sont finis.

1. Pour tout $x \in E$ rappeler (sans démonstration) la relation liant $\mathrm{card}(G)$, $\mathrm{card}(\mathrm{Stab}_G(x))$ et $\mathrm{card}(O(x))$.

   Pour tout $g \in E$, on note $\mathrm{Fix}(g) = \{x \in E \mid g \cdot x = x\}$ On note $F = \{(g, x) \in G \times E \mid g \cdot x = x\}$.

   $$p : F \to G, \quad (g, x) \mapsto g, \quad \text{et} \quad q : F \to E, \quad (g, x) \mapsto x.$$

2. Montrer que
   $$F = \coprod_{x \in E} q^{-1}(\{x\}) = \coprod_{g \in G} p^{-1}(\{g\}).$$

3. Établir la *formule de Burnside* :
   $$k = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g)).$$

Exercice 18. Soit G un groupe fini. On laisse G agir sur lui même par conjugaison et on appelle *classe de conjugaison* une orbite pour cette action, et on note $C(x)$ la classe de conjugaison (i.e. l'orbite) de x. Pour $x \in G$ on note $Z(x)$ le stabilisateur (ou le commutant) de x dans G.

1. Pour quels $x \in G$ a t'on $|C(x)| = 1$?

2. Montrer que $|C(x)|$ divise $|G|$.

3. On note $Z(G)$ le centre de G. Montrer que $|C(x)|$ divise $|G|/|Z(G)|$ et même qu'il ne peut y avoir égalité que si G est abélien.

4. Ecrire (formellement) l'équation aux classes (pour l'action considérée ici). Justifier que si l'on ordonne les cardinaux des orbites de manières croissante, alors le premier terme est 1.

5. Quels sont les groupes avec une unique classe de conjugaison ?

6. Montrer que si l'équation pour les classes de conjugaison de G est $1+n$ alors $G = \mathbb{Z}/2\mathbb{Z}$.

7. On veut caractériser les groupes G dont l'équation pour les classes de conjugaison est de la forme $1 + n + m$ avec $n \geq m$.

   (a) Montrer que si $n = 1$ alors $m = 1$. Qui est donc G ?

   (b) On suppose que $n > 1$. Montrer que $1 + n = m$.

(c) En déduire que $n = 2$ et $m = 3$, et donc $G = \mathfrak{S}_3$.

8. Quels sont les groupes fini possédant au plus 3 classes de conjugaison ?
9. Montrer que l'on ne peut pas avoir une equation aux classes de la forme

$$|G| = 1+1+1+2+5, \quad |G| = 1+2+3+4 \quad |G| \; = 1+1+2+2+2+2.$$

10. Bonus : montrer que $|G| = 1+2+2+5$ est possible en choisissant un bon groupe.
11. Bonus : montrer qu'il n'existe au plus qu'un nombre fini de groupes fini avec au plus $n \in \mathbb{N}_{\geq 1}$ classes de conjugaison.

Solution

1.
2.
3. Si il y a égalité, le stabilisateur de x, c'est à dire $Z(x)/Z(G)$ est trivial, i.e. $Z(x) = Z(G)$. Mais x est dans $Z(x)$, donc dans $Z(G)$, donc $C(x) = \{x\}$ et $|G|/|Z(G)| = 1$ donc $G = Z(G)$.
4.
5. groupe trivial car neutre toujours seul dans sa propre classe
6. n divise $n+1$ donc n divise 1 donc $n = 1$.
7. (a) si $n = 1$ et $m \neq 1$ $|Z(G)| = 2$ donc m divise $(m+2)/2$ donc $m \leq m/2+1$, c'est possible que si $m = m/2+1$ i.e. $m = 2$. Mais si $m = 2$, $|G| \; = 4$ donc G abélien. Plus rapidement : par la question 2, m divise $m+2$ donc m divise 2 puis idem. (b) m divise $m+n+1$ donc $n+1$ et n divise $m+1$. On a donc $n \leq m \leq n+1$. Si $m = n$ alors $n = m|1$: impossible. (c) On a donc $n| \; 1+m = n+2$ donc $n = 2$ et $m = 3$.
8. Pour 3 classes : $\mathbb{Z}/3\mathbb{Z}$, et $\mathfrak{S}_3$.
9.
   - $|G| = 10$, $|Z(G)| = 3$, et $|Z(G)| \; \nmid |G$: impossible.
   - On a une classe telle que $|C(x)| = 3 \nmid 10 = |G|$: impossible.
   - $|G/Z(G)| = 10/2 = 5$, et $2 \nmid 5$: impossible.
10. On prend le groupe $D_5 \simeq \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$: il est engendré par r, s tels que $r^5 = 1, s^2 = 1$ et $r^{-1}sr = r^{-2}s$ i.e. $sr = r^{-1}s$. On a donc que 1 est dans sa propre classe, $r, r^{-1} = srs^{-1} = srs$ sont ensemble, $r^2, r^{-2} = r^3$ aussi, et $s, rs = r^{-2}sr^2, r^2s = rsr^{-1}, r^3s, r^4s$ aussi.

11. (dur : quitte à diviser par $|G|$, il faut montrer qu'il n'y a qu'un nombre fini de solutions à
$$\sum_{i=1}^{n} \frac{1}{n_i} = 1,$$
pour $n_i \in \mathbb{N}$. Clairement quitte à réordonner $n_1 \leq n$. Montrons par récurrence que $n_i \leq n^{1+1+2+\cdots+2^{i-1}}$, donc $n_i \leq n^{2^i}$ et donc $|G| \leq n^{2^{n-1}}$ (car le neutre a classe 1). On écrit
$$1/n_{i+1} + \cdots + 1/n_n = 1 - 1/n_1 - \cdots - 1/n_i = \frac{a}{n_1 \ldots n_i} \geq \frac{1}{n_1 \ldots n_i},$$
et donc $(n-i)/n_{i+1} \geq \frac{1}{n_1 \ldots n_i}$ et par HR, $n_{i+1} \leq n n_1 \ldots n_i = n^{1+1+\cdots+2^i}$, d'où le résultat.