TD5 : Actions de groupes et théorèmes de Sylow

Exercices $\star$: à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices $\star\star$: seront traités en classe en priorité.
Exercices $\star\star\star$: plus difficiles.

Exercice 1 : $\star$
Soit p un nombre premier.

a) Montrer qu'un groupe de cardinal p^2 est commutatif.

b) Combien d'éléments d'ordre p y a-t-il dans un groupe de cardinal p ? Et dans un groupe de cardinal p^2 ?

Exercice 2 :
Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E := \{(g, x) \in G \times X : g \cdot x = x\},$$

calculer le nombre moyen de point fixes d'un élément de G.
Que dire en particulier si l'action est transitive ? Que dire de la moyenne du nombre de points fixes d'une permutation aléatoire ?

Exercice 3 : (Lemme de Cauchy) $\star$
Soit G un groupe fini et soit p un nombre premier divisant le cardinal de G. En utilisant une action convenable de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble

$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

prouver que G admet un élément d'ordre p (sans utiliser les théorèmes de Sylow !).

Exercice 4 : $\star$
Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

Exercice 5 : $\star\star$
Soit G un groupe.

a) On suppose que G est fini et on note p le plus petit nombre premier divisant le cardinal de G. Montrer que tout sous-groupe de G d'indice p est distingué.

b) On suppose que G est infini et qu'il admet un sous-groupe strict H d'indice fini. Montrer que G n'est pas un groupe simple.

Exercice 6 :

a) Montrer que si G est un groupe fini et H un sous-groupe strict de G, alors la réunion des conjugués de H n'est pas égale à G tout entier. Que dire si le groupe G est infini et si H est d'indice fini dans G ? Et si on ne suppose plus H d'indice fini ?

b) Soit G un groupe fini agissant transitivement sur un ensemble fini X tel que $|X| \geq 2$. Montrer qu'il existe $g \in G$ ne fixant aucun point de X.

Exercice 7 :
Soit G un groupe fini non trivial agissant sur un ensemble fini X. On suppose que pour tout $g \neq e \in G$, il existe un unique $x \in X$ tel que $g \cdot x = x$. On souhaite montrer que X admet un point fixe sous G (nécessairement unique).

a) On note $Y := \{x \in X : \mathrm{Stab}_G(x) \neq \{e\}\}$. Montrer que Y est stable par G.

b) On note $n = |Y/G|$ et $y_1, \dots, y_n$ un système de représentants de Y/G. Pour tout i, on note m_i le cardinal de $\mathrm{Stab}_G(y_i)$. En considérant l'ensemble $Z := \{(g, x) \in (G \setminus \{e\}) \times X : g \cdot x = x\}$, montrer que
$$1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right) .$$

c) En déduire que $n = 1$.

d) Conclure.

Exercice 8 : $\star\star$

a) Soit G un p-groupe fini agissant sur un ensemble fini X. On note X^G l'ensemble des points fixes de X sous G. Montrer que
$$|X^G| \equiv |X| \ (\mathrm{mod.}\ p) .$$

b) Soit G un p-groupe agissant sur un ensemble fini X dont le cardinal n'est pas divisible par p. Montrer que X admet un point fixe sous G.

c) Soit G un p-groupe fini et $H \neq \{e\}$ un sous-groupe distingué de G. Montrer que l'intersection de H avec le centre de G n'est pas réduite à l'élément neutre.

d) Montrer qu'un groupe d'ordre p^n admet des sous-groupes d'ordre p^i pour tout $0 \leq i \leq n$.

e) Soit p un nombre premier congru à 1 modulo 4. On souhaite montrer que p est somme de deux carrés d'entiers. On note
$$X := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\} .$$

   i) On définit $i : X \to X$ par les formules suivantes
$$i : (x,y,z) \mapsto \begin{array}{l} (x + 2z, z, y - x - z) \text{ si } x < y - z \,, \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y \,, \\ (x - 2y, x - y + z, y) \text{ si } x > 2y \,. \end{array}$$
   Vérifier que i est bien définie.

   ii) Montrer que i est une involution.

   iii) Montrer que i a un unique point fixe.

   iv) Montrer que $|X|$ est impair.

   v) Montrer que l'application $j : X \to X$ définie par $j(x, y, z) := (x, z, y)$ admet un point fixe.

   vi) Conclure.

Exercice 9 :
Soit $n \geq 1$ un entier. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphisme de groupes finis admettant exactement n classes de conjugaison.

Exercice 10 : $\star\star$

a) Calculer le groupe des isométries directes (resp. indirectes) d'un tétraèdre régulier dans l'espace euclidien de dimension trois (on pourra regarder l'action de ce groupe sur les sommets du tétraèdre).

b) Mêmes questions pour un cube et un octaèdre (on pourra regarder l'action du groupe des isométries du cube sur les diagonales de ce cube).

c) Mêmes questions pour un dodécaèdre et un icosaèdre (on pourra regarder l'action du groupe des isométries du dodécaèdre sur les "grands cubes" inscrits dans ce dodécaèdre).

Exercice 11 : (Théorème de Pólya) $\star\star\star$
Soit G un groupe fini, agissant sur un ensemble fini X de cardinal N.
Notons $Z_{G,X} := \frac{1}{|G|}\sum_{g\in G}\prod_{\omega\in X/\langle g\rangle} X_{|\omega|} \in \mathbb{Z}[X_1,\dots,X_N]$.
Soit $C_n := \{1,\dots,n\}$, appelé "ensemble des couleurs". On appelle "coloriage de X en $\leq n$ couleurs" une application $f : X \to C_n$. On note $\mathcal{C}(X,n)$ l'ensemble de ces coloriages. Si $f \in \mathcal{C}(X,n)$, on note $\mathrm{type}(f) := X_1^{|f^{-1}(1)|}\dots X_n^{|f^{-1}(n)|} \in \mathbb{Z}[X_1,\dots,X_n]$. Si $A \subset \mathcal{C}(X,n)$, on note $N_A := \sum_{f\in A}\mathrm{type}(f)$ la fonction génératrice de A.
On cherche à dénombrer les coloriages de X en n couleurs à l'action de G près.

a) Calculer $Z_{G,X}$ dans les exemples suivants :
   i) G agissant sur lui-même par translation.
   ii) $G = \mathfrak{S}_n$ agissant sur $X = \{1,\dots,n\}$.
   iii) $G = \mathbb{Z}/n\mathbb{Z}$ ou D_n agissant sur l'ensemble X des sommets d'un polygone régulier à n côtés.
   iv) G est le groupe des isométries (resp. des isométries directes) d'un polyèdre régulier agissant sur l'ensemble X des faces dudit polyèdre.
b) Montrer que G agit naturellement sur $\mathcal{C}(X,n)$ et que $\mathrm{type} : \mathcal{C}(X,n) \to \mathbb{Z}[X_1,\dots,X_n]$ est constante sur les orbites de G. On peut donc définir $\mathrm{type} : \mathcal{C}(X,n)/G \to \mathbb{Z}[X_1,\dots,X_n]$ et $N_{\bar{A}}$ pour une partie $\bar{A} \subset \mathcal{C}(X,n)/G$. Si $\bar{A} = \mathcal{C}(X,n)/G$, on notera $N_{X/G} := N_{\bar{A}}$.
c) Montrer que $N_{X/G}$ est un polynôme symétrique.
d) Montrer que $N_{X/G}(X_1,\dots,X_n) = Z_{G,X}(S_1,\dots,S_N)$ dans $\mathbb{Z}[X_1,\dots,X_n]$, où $S_i(X_1,\dots,X_n) := X_1^i + \dots + X_n^i$.
e) En déduire que $|\mathcal{C}(X,n)/G| = Z_{G,X}(n,\dots,n) = \frac{1}{N}\sum_{g\in G} n^{\lambda(g)}$, où $\lambda(g)$ désigne le nombre de cycles de g dans la décomposition de g vu comme permutation de X.
f) Dénombrer les coloriages des faces d'un cube en $\leq n$ couleurs à isométrie près. Et les coloriages en exactement n couleurs ? Donner enfin la répartition selon les types de coloriages (par exemple, le nombre de coloriage avec une face bleue, deux faces blanches et trois faces rouges).
g) Mêmes questions en remplaçant le cube par un icosaèdre.
h) Que dire du nombre de colliers de k perles avec au plus n couleurs ?

Exercice 12 : $\star\star$
On suppose qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente-six 5-Sylow.
b) Montrer que G contient dix 3-Sylow, puis que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_G$. (Indication : on pourra considérer les ordres possibles pour le centralisateur de g ; on observera qu'un groupe d'ordre 18 admet un unique 3-Sylow.)
c) Conclure.

Exercice 13 : $\star\star$
Soient p et q deux nombres premiers distincts.

a) Montrer qu'un groupe d'ordre pq n'est pas simple.
b) Montrer que si $p < q$ et p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.
c) Soit G un groupe simple d'ordre $p^\alpha m$, avec $\alpha \geq 1$ et m non divisible par p. On note n_p le nombre de p-Sylow de G. Montrer que $|G|$ divise $n_p!$.
d) Montrer qu'un groupe d'ordre $p^m q^n$, avec $p < q$, $1 \leq m \leq 2$ et $n \geq 1$, n'est pas simple.
e) Montrer qu'un groupe d'ordre $p^2 q$ ou $p^3 q$ n'est pas simple.

Exercice 14 : $\star$
Montrer qu'un groupe non commutatif d'ordre < 60 n'est pas simple.

Exercice 15 : $\star\star$
On cherche à montrer que $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathfrak{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathfrak{A}_5$.

b) Montrer que $\mathfrak{A}_5$ est simple.

c) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

d) En déduire que G contient un sous-groupe d'ordre 12.

e) Conclure.

Exercice 16 : $\star\star\star$
Soit G un groupe fini.

a) Soit H un sous-groupe de G d'indice n. On note $x_1, \ldots, x_n \in G$ un ensemble de représentants de G modulo H. L'action de G sur G/H induit une action de G sur $\{1, \ldots, n\}$, et pour tout $g \in G$ et $1 \leq i \leq n$, il existe $h_{i,g} \in H$ tel que $gx_i = x_{g \cdot i} h_{i,g}$. On note enfin $\pi : H \to H/D(H)$ la projection canonique. Montrer que la formule

$$V(g) := \pi \left(\prod_{i=1}^{n} h_{i,g} \right)$$

définit un morphisme de groupes $G \to H/D(H)$ indépendant du choix des x_i.

b) Avec les notations précédentes, soit $h \in H$. On considère l'action de $\langle h \rangle$ sur $X = G/H$ et on note $g_1, \ldots, g_r$ des éléments de G tels que les classes $[g_i]$ des g_i dans X forment un ensemble de représentants pour cette action. Pour tout i, on note n_i l'entier minimal non nul tel que $h^{n_i} \cdot [g_i] = [g_i]$. Montrer que

$$V(h) = \pi \left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i \right) .$$

c) Soient S un p-Sylow de G et $A, B \subset S$ des parties stables par conjugaison dans S. Montrer que si A et B sont conjuguées dans G, alors elles le sont dans $N_G(S)$ (on pourra considérer deux p-Sylow de $N_G(A)$).

d) Soit S un p-Sylow de G tel que $S \subset Z(N_G(S))$. Montrer que le morphisme $V : G \to S$ défini à la question a) est surjectif. En déduire qu'il existe un sous-groupe distingué H de G tel que S soit isomorphe à G/H.

e) En déduire que si G est simple non cyclique, alors le cardinal de G est divisible par 12 ou son plus petit facteur premier apparaît au moins au cube dans sa décomposition en facteurs premiers.

Exercice 17 : $\star\star\star$

a) Montrer qu'un groupe d'ordre $60 < n < 168$ avec n non premier n'est jamais simple.

b) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$ sont d'ordre 168.

c) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ est simple.

d) Soit G simple d'ordre 168. Montrer que G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$.

e) Montrer que l'on a un isomorphisme entre $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$.