TD1 : Groupes et actions de groupes

Exercices $\star$: exercices indispensables, applications directes du cours.
Exercices $\star\star$: exercices un peu plus difficiles.
Exercices $\star\star\star$: exercices difficiles, pour aller plus loin.

Exercice 1 : $\star$
Soit A un groupe abélien.

a) Montrer que tout morphisme de groupes $f : \mathbb{Z} \to A$ est de la forme $f(k) = k \cdot a_0$ pour un certain $a_0 \in A$.

b) Montrer que le groupe $\mathrm{Hom}(\mathbb{Z}, A)$ est isomorphe à A.

c) Montrer que $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$ est isomorphe au sous-groupe de n-torsion de A (i.e. au noyau de la multiplication par n dans A).

d) Identifier le groupe $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ à un groupe usuel.

Exercice 2 : (Sous-groupes de $\mathbb{R}$) $\star$

a) Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit monogènes, soit denses.

b) Donner un exemple de sous-groupe dense et de type fini dans $(\mathbb{R}, +)$.

c) Tous les sous-groupes de $\mathbb{R}$ sont-ils de type fini ?

d) ($\star\star$) Montrer qu'un sous-groupe du cercle unité $\mathbb{U}$ est soit fini cyclique, soit dense.

Exercice 3 : $\star$

a) Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

b) Donner un exemple de groupe d'exposant 3 qui n'est pas abélien.

Exercice 4 : $\star$

a) Montrer que les groupes $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes. Que dire des groupes $\mathbb{Q}$ et $\mathbb{Q}^2$?

b) Montrer que les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_{>0}, \cdot)$ sont isomorphes. Sont-ils isomorphes à $(\mathbb{R}^\times, \cdot)$?

c) Les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_{>0}, \cdot)$ sont-ils isomorphes ?

d) Montrer que tout élément du groupe $G = (\mathbb{Q}/\mathbb{Z}, +)$ est d'ordre fini. Montrer que G contient des éléments d'ordre arbitrairement grand.

Exercice 5 : $\star$
Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Exercice 6 : $\star$

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.

b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Exercice 7 : (Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$) $\star\star$
Si A est un anneau, on note $A^\times$ le groupe (multiplicatif) des éléments inversibles de A.

a) Soit G un groupe monogène. Montrer que le groupe des automorphismes de G est en bijection avec l'ensemble des générateurs de G.

b) Montrer que pour tout $n \in \mathbb{N}$, on a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

c) Soit p un nombre premier impair et soit $\alpha \geq 1$. Quel est l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$? (On pourra montrer que pour tout k, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, avec λ premier à p).

d) En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

e) Expliciter $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ pour $\alpha \geq 1$. (On pourra calculer l'ordre de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$).

f) En déduire $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \mathbb{N}$.

g) Déterminer une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit un groupe cyclique.

Exercice 8 : $\star$

a) Montrer que le groupe des automorphismes de groupe de $(\mathbb{Z}/p\mathbb{Z})^n$ est naturellement isomorphe à $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

b) Le groupe des automorphismes de groupe de $\mathbb{C}^n$ est-il isomorphe à $\mathrm{GL}_n(\mathbb{C})$?

Exercice 9 : $\star\star$

Décrire les groupes $\mathrm{Aut}(\mathfrak{S}_3)$ et $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$.

Exercice 10 : $\star$

a) Donner la liste de tous les groupes (à isomorphisme près) de cardinal inférieur ou égal à 7.

b) ($\star\star$) Déterminer tous les groupes de cardinal 8.

Exercice 11 : $\star\star$

Soit G un groupe tel que le quotient par son centre est monogène. Prouver que G est abélien.

Exercice 12 : $\star$

Soit G un groupe fini.

a) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{S}_n$.

b) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{A}_n$.

c) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathrm{GL}_n(k)$, pour tout corps k.

Exercice 13 : $\star$

Soit G un groupe, et soient H et K des sous-groupes de G. On suppose que :

a) $H \triangleleft G$ et $K \triangleleft G$.

b) $HK = G$.

c) $H \cap K = \{1\}$.

Montrer que G est isomorphe à $H \times K$.

Exercice 14 : (Théorèmes d'isomorphisme) $\star\star$

Soit G un groupe et soit $H \triangleleft G$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de G/H en fonction de ceux de G.

b) Soit K un sous-groupe de G.

   i) Si K est distingué dans G et contient H, montrer que l'on a un isomorphisme $(G/H)/(K/H) \cong G/K$.

   ii) Montrer que HK est un sous-groupe de G égal à KH.

   iii) Montrer que H est distingué dans HK.

   iv) Montrer que l'on a un isomorphisme $K/(K \cap H) \cong (HK)/H$.

Exercice 15 : $\star$

Soit G un groupe et soit H un sous-groupe de G.

a) Si H est d'indice 2 dans G, montrer que H est distingué dans G.

b) ($\star\star$) Si l'indice de H dans G est le plus petit facteur premier du cardinal de G, montrer que H est distingué dans G.

Exercice 16 : $\star\star\star$

Soit H un sous-groupe dans $\mathfrak{S}_n$. On suppose son indice k compris entre 2 et n. Montrer que $k = 2$ et $H = \mathfrak{A}_n$, ou alors $k = n$ et H est isomorphe à $\mathfrak{S}_{n-1}$.

Exercice 17 : $\star\star$

On se propose de démontrer l'énoncé utile suivant de « simplification par G ». Si G, H et K sont trois groupes finis tels que $G \times H \simeq G \times K$, alors $H \simeq K$.

a) Donner un contre-exemple avec des groupes infinis.

b) Pour deux groupes finis L et G, on note $h(L, G)$ (resp. $i(L, G)$) le nombre de morphismes (resp. de morphismes injectifs) de L dans G. Démontrer les identités suivantes :

$$h(L, G \times K) = h(L, G) \cdot h(L, K)$$

et

$$h(L, G) = \sum_{N \triangleleft L} i(L/N, G)\,,$$

où la somme porte sur tous les sous-groupes distingués de L.

c) En déduire le résultat souhaité.

Exercice 18 : (Action de groupes et p-groupes) $\star$

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

$$|X^G| \equiv |X| \text{ (mod. } p)\,.$$

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

$$\begin{aligned} i : (x, y, z) \mapsto \quad & (x + 2z, z, y - x - z) \text{ si } x < y - z\,, \\ & (2y - x, y, x - y + z) \text{ si } y - z < x < 2y\,, \\ & (x - 2y, x - y + z, y) \text{ si } x > 2y\,. \end{aligned}$$

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

Exercice 20 : (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 21 : $\star\star\star$
Soit G un groupe fini.

a) Soit H un sous-groupe de G d'indice n. On note $x_1, \dots, x_n \in G$ un ensemble de représentants de G modulo H. L'action de G sur G/H induit une action de G sur $\{1, \dots, n\}$, et pour tout $g \in G$ et $1 \leq i \leq n$, il existe $h_{i,g \cdot i} \in H$ tel que $gx_i = x_{g \cdot i} h_{i,g \cdot i}$. On note enfin $\pi : H \to H/D(H)$ la projection canonique. Montrer que la formule
$$V(g) := \pi \left(\prod_{i=1}^{n} h_{i,g \cdot i} \right)$$
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 $g_1, \dots, g_r$ 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.