5. Groupes quotients, actions de groupes et compléments

Exercice 1. (*Signature*) Cet exercice a pour objet la définition de la *signature* d'une permutation.

1. Étant donnée une permutation $\sigma \in \mathfrak{S}_n$, on pose $\varepsilon(\sigma) = (-1)^{n-k}$, où k est le nombre d'orbites de σ dans $\{1,\dots,n\}$.

(i) Déterminer explicitement $\varepsilon(\sigma)$ lorsque $\sigma = 1$ puis lorsque σ est un cycle.

(ii) Étant données une permutation $\sigma \in \mathfrak{S}_n$ et une transposition $\tau \in \mathfrak{S}_n$, démontrer que l'on a $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$. (*Indication : si $\tau = (i,j)$, distinguer le cas où i et j appartiennent à des σ-orbites distinctes et le cas où i et j appartiennent à la même σ-orbite.*)

(iii) Quelles que soient les transpositions $\tau_1,\dots,\tau_r \in \mathfrak{S}_n$, démontrer que l'on a $\varepsilon(\tau_1\dots\tau_r) = (-1)^r$.

2. En utilisant la question précédente, prouver que l'application $\varepsilon : \mathfrak{S}_n \to \{-1,1\}$ est un homomorphisme de groupes.

3. Démontrer que, si $f : \mathfrak{S}_n \to \{-1,1\}$ est un homomorphisme de groupes surjectif tel que $f(\tau) = -1$ pour toute transposition τ, alors $f = \varepsilon$.

4. Justifier les trois interprétations suivantes de la signature $\varepsilon(\sigma)$ d'une permutation $\sigma \in \mathfrak{S}_n$.

(i) Si $\sigma = \tau_1\dots\tau_r$ est une expression de σ comme un produit de transpositions, la parité de m ne dépend pas du choix des transpositions et $\varepsilon(\sigma) = (-1)^m$.

(ii) Une *inversion* de σ est une paire $\{i,j\}$ d'éléments de $\{1,\dots,n\}$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. Démontrer que l'on a :

$$\varepsilon(\sigma) = (-1)^{\text{nombre d'inversions de }\sigma} = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}.$$

(*Indication : multiplier σ par des transpositions convenables pour faire baisser le nombre d'inversions et vérifier que la seule permutation n'ayant aucune inversion est l'identité.*)

(iii) Soit $\rho : \mathfrak{S}_n \to \mathrm{GL}(n,\mathbb{Q})$ l'homomorphisme de groupes envoyant une permutation σ sur l'application linéaire définie par

$$\rho(\sigma)(e_i) = e_{\sigma(i)}.$$

Démontrer que l'on a $\varepsilon = \det\circ\rho$.

Exercice 2. (*Formule de Burnside*) Soit G un groupe fini opérant sur un ensemble fini X. Pour tout élément $g \in \mathrm{G}$, on pose

$$\mathrm{X}^g = \{x \in \mathrm{X} \mid gx = x\}.$$

1. Démontrer la formule

$$\sum_{x\in\mathrm{X}} |\mathrm{Stab}_{\mathrm{G}}(x)| = \sum_{g\in\mathrm{G}} |\mathrm{X}^g|.$$

(*Indication : compter combien de fois un point x de* X *apparaît dans l'un des ensembles* X^g, $g \in \mathrm{G}$...)

2. En déduire la *formule de Burnside* :

$$\text{Nombre d'orbites de G dans X } = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} |\mathrm{X}^g|.$$

3. Soit C un carré de sommets a, b, c, d et de centre o. On considère le groupe G d'isométries du plan engendré par la rotation de centre o et d'angle $\frac{\pi}{2}$ et par la symétrie (orthogonale) par rapport à la diagonale (ac). Démontrer que G est isomorphe à un sous-groupe d'ordre 8 de $\mathfrak{S}_4$.

4. On colorie les sommets du carré C à l'aide de $m \geq 1$ couleurs. Deux coloriages de C sont identifiés s'il existe un élément h de H envoyant l'un sur l'autre.

(i) Énumérer tous les coloriages possibles lorsque $m = 2$.

(ii) En appliquant la formule de Burnside, démonter qu'il y a

$$\frac{m^4+2m^3+3m^2+2m}{8}$$

coloriages possibles.

Exercice 3. (*Groupes diédraux*) Étant donné un entier $n \geq 1$, on désigne par P_n le polygône régulier à n côtés dans un plan euclidien orienté et on note D_n le groupe des isométries du plan qui préservent P_n, c'est-à-dire les isométries f

telles que $f(\mathrm{P}_n) = \mathrm{P}_n$. Soit O le centre de P_n. On désigne par r la rotation de centre O et d'angle $\frac{2\pi}{n}$ et par s la réflexion par rapport à un axe de symétrie Δ de P_n.

1.Démontrer que D_n est un groupe fini d'ordre $2n$ ayant pour éléments les isométries $s^\varepsilon r^k$, $0 \leq k \leq n-1$ et $\varepsilon \in \{0,1\}$.

2. Vérifier l'identité $srs^{-1} = r^{-1}$. En déduire la table de multiplication du groupe D_n. Pour quelles valeurs de n ce groupe est-il commutatif ?

3. Déterminer l'ordre de chacun des éléments de D_n. En déduire que le groupe D_4 n'est pas isomorphe au groupe $\mathbb{H}_8$ des quaternions.

4. Soit G un groupe engendré par des éléments a et b tels que $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = 2$ et $\mathrm{ord}(ab) = 2$. Démontrer que G est isomorphe au groupe D_n.

Exercice 4. (*Classification des groupes abéliens finis*) L'objet de cet exercice est la détermination de tous les groupes abéliens finis à isomorphisme près ; en particulier, on va démontrer que tout groupe abélien est isomorphe à un produit de groupes abéliens cycliques.

I. Soit p un nombre premier et soit G un groupe abélien fini dont l'ordre est une puissance de p. Quel que soit $r \geq 0$, on désigne par G_r le sous-groupe de G formé des éléments g tels que $g^{p^r} = e$; cela définit une suite croissante

$$\{e\} = \mathrm{G}_0 \subset \mathrm{G}_1 \subset \ldots \subset \mathrm{G}_r \subset \mathrm{G}_{r+1} \subset \ldots \mathrm{G}$$

de sous-groupes de G et $\mathrm{G}_r = \mathrm{G}$ si r est suffisamment grand. Enfin, pour $r \geq 1$, on pose $\mathrm{V}_r = \mathrm{G}_r / \mathrm{G}_{r-1}$.

1. Déterminer explicitement les suites $(\mathrm{G}_r)_{r\geq 0}$ et $(\mathrm{V}_r)_{r\geq 1}$ dans chacun des trois cas suivants :

$$\mathrm{G} = \mathbb{Z}/p^3\mathbb{Z}, \;\; \mathrm{G} = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \;\; \text{ et } \;\; \mathrm{G} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

2. Soit $r \geq 1$. Justifier que l'on a $x^p = 1$ pour tout élément x du groupe V_r puis en déduire que l'application

$$\mathbb{Z}/p\mathbb{Z} \times \mathrm{V}_r \to \mathrm{V}_r, \;\; (\overline{m}, x) \mapsto x^m$$

fait de V_r un espace vectoriel de dimension finie sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On pose $\delta(r) = \dim_{\mathbb{F}_p}(\mathrm{V}_r)$.

3. Soient $1 \leq s \leq r$. Vérifier que l'homomorphisme de groupes $\mathrm{G} \to \mathrm{G}$, $g \mapsto g^{r-s}$ induit une application $\mathbb{F}_p$-linéaire injective $u_r^s : \mathrm{V}_r \to \mathrm{V}_s$. La suite $(\delta(r))_{r\geq 1}$ est par conséquent décroissante.

4. Fixons $r \geq 1$ tel que $\mathrm{G} = \mathrm{G}_r$. On choisit $d(r) = \delta(r)$ éléments $g_{r,1}, \ldots, g_{r,\delta(r)}$ de G_r dont les images par la projection canonique $\mathrm{G}_r \to \mathrm{V}_r$ forment une base de V_r sur $\mathbb{F}_p$; ensuite, pour tout $s \in \{1, \ldots, r-1\}$, on choisit $d(s) = \delta(s) - \delta(s+1)$ éléments $g_{s,1}, \ldots, g_{s,d(s)}$ de G_s dont les images par la projection canonique $\mathrm{G}_s \to \mathrm{V}_s$ constituent une base d'un supplémentaire de $u_{s+1}^s(\mathrm{V}_{s+1})$ dans V_s.

(i) Étant donnés des entiers naturels $m_{s,i}$, $1 \leq s \leq r$ et $1 \leq i \leq d(s)$, démontrer que l'identité

$$g_{r,1}^{m_{r,1}} \ldots g_{r,d(r)}^{m_{r,d(r)}} \ldots g_{s,1}^{m_{s,1}} \ldots g_{s,d(s)}^{m_{s,d(s)}} \ldots g_{1,1}^{m_{1,1}} \ldots g_{1,d(1)}^{m_{1,d(1)}} = 1$$

implique

$$m_{s,i} \equiv 0 \pmod{p^s}$$

pour tout $1 \leq s \leq r$ et $1 \leq i \leq d(s)$.

(ii) En déduire que le groupe G est isomorphe au groupe produit

$$\prod_{s\geq 1} (\mathbb{Z}/p^s\mathbb{Z})^{d(s)}.$$

5. Étant donné $r \geq 1$, démontrer que l'on a $|G_r| = p^{\delta(1)+\ldots+\delta(r)}$. En déduire que G contient exactement $(p^{\delta(r)} - 1)p^{\delta(1)+\ldots+\delta(r-1)}$ éléments d'ordre p^r.

6. Soient H un autre groupe abélien fini d'ordre une puissance de p et soit $\delta'(r)$ la dimension du $\mathbb{F}_p$-espace vectoriel $\mathrm{H}_r/\mathrm{H}_{r-1}$ $(r \geq 1)$. Démontrer que le groupe H est isomorphe à G si et seulement si $\delta(r) = \delta'(r)$ pour tout $r \geq 1$.

II. Soit G un groupe abélien fini.

1. En utilisant la seconde question de l'exercice 2 de la fiche 4, déduire de ce qui précède que G est isomorphe à un produit de groupes cycliques.

2. Démontrer qu'un groupe abélien fini H est isomorphe à G si et seulement si, pour tout nombre entier naturel m, G et H ont le même nombre d'éléments d'ordre m.