Actions, groupes cycliques et Lagrange

Travaux dirigés du 23 et du 26 septembre 2025

On corrigera en priorité les exercices marqués d'un ≪ ✾ ≫, dans l'ordre.

✾ Exercice 1. Actions transitives, fidèles et libres

Soit G un groupe fini agissant sur un ensemble fini X à $n \geq 1$ éléments.

1. On suppose l'action transitive. Montrer que n divise $|G|$.
2. On suppose l'action fidèle (c'est-à-dire que $\bigcap_{x \in X} G_x = \{1\}$). Montrer que $|G|$ divise $n!$.
3. On suppose l'action libre (c'est-à-dire que $G_x = \{1\}$ pour tout $x \in X$). Montrer que $|G|$ divise n.

✾ Exercice 2. Actions transitives et classes de conjugaison

Soit G un groupe.

1. Soit $(X, \bullet)$ une action de G. Montrer le *principe de conjugaison*, c'est-à-dire qu'on a $G_{g \bullet x} = gG_xg^{-1}$ pour tout $x \in X$ et tout $g \in G$.
2. En déduire que si $(X, \bullet)$ est une action transitive de G, les stabilisateurs associés G_x, avec $x \in X$, forment une classe de conjugaison de sous-groupes de G. On notera $\mathrm{Stab}(X, \bullet)$ cette classe de conjugaison de sous-groupes de G associé à $\bullet$.
3. On rappelle que si $(X, \bullet)$ est une action transitive de G et $x \in X$, alors $(X, \bullet)$ est isomorphe à l'action par translations de G sur G/G_x. Montrer que deux actions transitives $(X, \bullet)$ et $(Y, \star)$ d'un même groupe G sont isomorphes si, et seulement si, on a $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$.

Exercice 3. Actions transitives d'un groupe cyclique

Soient $n \geq 1$ un entier et G cyclique d'ordre n.

1. Pour tout diviseur d de n, définir une action transitive de G sur un ensemble à d éléments.
2. En utilisant le résultat de l'exercice précédent, montrer que toute action transitive de G est isomorphe à une et une seule des actions définies au 1.

✾ Exercice 4. Sous-groupes finis de $k^\times$

On va montrer que si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.

1. Montrer le cas $k = \mathbb{C}$ à l'aide du sous-groupe μ_n.
2. Montrer que si G un groupe et $x, y \in G$ deux éléments qui commutent, d'ordres finis a et b avec $(a, b) = 1$ alors xy est d'ordre ab. (Si on ne suppose plus que x et y commutent, alors xy peut être d'ordre quelconque, et ce même si G est fini : voir les exercices 5 et 6.)
3. Soient k un corps et $G \subseteq k^\times$ un sous-groupe fini. Montrer l'égalité suivante dans $k[X]$:

$$X^{|G|} - 1 = \prod_{g \in G} (X - g) \ .$$

   (On rappelle qu'un polynôme de degré n à coefficients dans un corps quelconque a au plus n racines)
4. Conclure.

✾ Exercice 5. Recherche d'exemples

1. Donner un exemple de groupe infini dont tous les éléments sont d'ordre fini.
2. Donner un exemple de groupe possédant deux éléments a, b avec $a^2 = 1$, $b^2 = 1$ et ab d'ordre infini.

Exercice 6. En général, on ne peut rien dire sur l'ordre du produit de deux éléments

Soient a et b des entiers avec $a, b \geq 3$. On pose $\xi_n = e^{2i\pi/n}$ pour $n \geq 1$ et l'on considère pour $a, b \geq 1$ et $t \in \mathbb{C}$ les éléments A, B et U_t de $SL_2(\mathbb{C})$ définis par

$$A = \begin{bmatrix} \xi_a & 0 \\ 0 & \xi_a^{-1} \end{bmatrix}, \quad B = \begin{bmatrix} 0 & -1 \\ 1 & \xi_b + \xi_b^{-1} \end{bmatrix}, \quad U_t = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

1. Montrer que A est d'ordre a dans le groupe $SL_2(\mathbb{C})$.
2. Observer que si $g \in SL_2(\mathbb{C})$ est de trace $x + x^{-1}$ avec $x \in \mathbb{C}^\times$, le polynôme caractéristique de g est $(X-x)(X-x^{-1})$. En déduire que B est d'ordre b, dans le groupe $SL_2(\mathbb{C})$.
3. On pose $B_t = U_t B U_t^{-1}$. Calculer la trace de AB_t.
4. On suppose $c \geq 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit AB_t est d'ordre c.
5. En admettant qu'il existe un nombre premier p tel que $p \equiv 1$ mod. abc (voir l'exercice suivant), et en travaillant dans $\mathbb{Z}/p\mathbb{Z}$ à la place du corps $\mathbb{C}$ (on rappelle que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, c.f. exercice 4), montrer qu'il existe un groupe fini possédant un élément d'ordre a et un autre d'ordre b, dont le produit est d'ordre c.

Exercice 7. Théorème de Dirichlet faible (complément à l'exercice précédent)

Soit $n \geq 1$ un entier. On se propose de montrer qu'il existe une infinité de nombres premiers $p \equiv 1$ mod. n. On considère le n-ème polynôme cyclotomique

$$\Phi_n = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

C'est un polynôme unitaire de degré $\varphi(n)$ dans $\mathbb{C}[X]$.

1. Montrer $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire $\Phi_n \in \mathbb{Z}[X]$ (on rappelle que si on a $P, Q \in \mathbb{Z}[X]$ avec Q unitaire, on dispose d'une division euclidienne $P = AQ + B$ avec $A, B \in \mathbb{Z}[X]$ et $\deg B < \deg Q$).
2. Montrer que si k est un corps dans lequel $n \cdot 1 \neq 0$, le polynôme $X^n - 1$ n'a pas de racine double dans k.
3. Soit $a \in \mathbb{N}$. Montrer que si p est un nombre premier divisant l'entier $\Phi_n(a)$, alors on a $p|n$ ou $p \equiv 1[n]$.
4. Conclure.

Exercice 8. Cauchy abélien

On va voir une autre preuve du théorème de Cauchy dans le cas abélien. On suppose que le groupe abélien fini G est engendré par des éléments $x_1, \ldots, x_n$, avec x_i d'ordre d_i.

1. Montrer que $|G|$ divise $d_1 \ldots d_n$.
2. En déduire que si p premier divise $|G|$, alors G admet un élément d'ordre p.

Exercice 9. Zoologie

Quel est le cardinal minimal d'un groupe non abélien ?