Actions, groupes cycliques et Lagrange

Travaux dirigés du 23 et du 26 septembre 2025

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 $|G|$.
   L'action de G sur X est transitive si et seulement si pour tout $x \in X$, $O_x = X$. Le cas échéant, on a donc pour x quelconque la relation $|G| = |X||G_x|$ par la formule orbite-stabilisateur, puis 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 $n!$.
   L'action de G sur X est fidèle si et seulement si le morphisme $m : G \to S_X$ associé à l'action est injectif. On a $G \simeq m(G)$, $m(G)$ sous-groupe de S_X, et $S_X = S_n$. On a donc que $|G|$ divise $n!$ par Lagrange.
3. On suppose l'action libre (c'est-à-dire que $G_x = \{1\}$ pour tout $x \in X$). Montrer que $|G|$ divise n.
   Soient $x_1, \dots, x_r$ des représentants des orbites de G dans X. On a donc $|X| = \sum_{i=1}^{r} |O_{x_i}|$ par l'équation aux classes. Mais on a $G_x = \{1\}$ pour tout $x \in X$ par hypothèse, et donc $|G| = |O_x|$ par la formule orbite-stabilisateur, puis $|X| = r|G|$ et $|G|$ 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 $g \in G$.
   Pour tout $h \in G$ on a $h \in G_{gx} \iff hgx = gx \iff g^{-1}hgx = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}$, ce qui conclut.
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 $\bullet$.
   Pour tout $x, y \in X$, il existe par transitivité un $g \in G$ tel que $g \bullet x = y$. Par la question précédente, G_x et G_y sont donc conjugués. On en déduit qu'il n'y a qu'une seule classe de conjugaison de sous-groupes de G.
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 $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$.
   Soit $f : X \to Y$ un isomorphisme entre $(X, \bullet)$ et $(Y, \star)$. Pour $x \in X$ et $g \in G$, $g \bullet x = x \iff f(g \bullet x) = f(x) \iff g \star f(x)$ par injectivité de f. On a donc $G_x = G_{f(x)}$, puis $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Supposons réciproquement $\mathrm{Stab}(X, \bullet) = \mathrm{Stab}(Y, \star)$. Il existe $x \in X$ et $y \in Y$ avec $G_x = G_y =: H$. On a alors $(X, \bullet) \simeq (G/H, \text{translations}) \simeq (Y, \star)$.

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.
   On peut supposer $G = \mu_n$. Soit d un diviseur de n. On fait agir G sur μ_d par $G \times \mu_d \to \mu_d$, $(g, x) \mapsto g^{n/d}x$. C'est une action transitive. On aurait aussi pu utiliser le point de vue $\mathbb{Z}/n\mathbb{Z}$, et observer que $\mathbb{Z}/n\mathbb{Z}$ agit sur $\mathbb{Z}/d\mathbb{Z}$ par $(m, x) \mapsto mx$.
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.
   On sait que deux actions transitives de G sont isomorphes si, et seulement si, elles ont un stabilisateur en commun. Mais on sait aussi que les sous-groupes du groupe cyclique μ_n sont les μ_d avec $d|n$. Le stabilisateur de 1 dans l'action ci-dessus est $\mu_{n/d}$. Cela conclut.

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.
   Le sous-groupe μ_n est bien cyclique engendré par $e^{\frac{2i\pi}{n}}$. Réciproquement, par Lagrange, tout sous-groupe d'ordre n est inclus dans μ_n, donc égal à μ_n (et donc cyclique) pour des raisons de cardinal.

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.)

   Considérons $H = \langle x\rangle \cap \langle y\rangle$. C'est un sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$. D'après Lagrange, $|H|$ divise $a = |\langle x\rangle|$ et $b = |\langle y\rangle|$ et donc $H = \{1\}$. (On peut d'ailleurs se passer de Lagrange ici en disant simplement que l'on a $h^a = h^b = 1$, et donc $h = 1$, pour tout h dans H.) Vérifions maintenant que xy est d'ordre ab. Soit $k \in \mathbb{Z}$. Comme $xy = yx$, on a $(xy)^k = x^k y^k$. En particulier, $(xy)^{ab} = 1$. Réciproquement, si $(xy)^k = 1$ alors $x^k = y^{-k} \in H = \{1\}$, et donc $x^k = y^{-k} = 1$. Ainsi, $a|k$ et $b|k$ puis $ab|k$ car $(a,b) = 1$.

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.)

   Posons $n = |G|$ et considérons le polynôme $P = X^n - 1 \in k[X]$. Le théorème de Lagrange assure que les n éléments de G sont racines de P. Or, P a au plus n racines, donc P est scindé à racines simples les éléments de G.

4. Conclure.

   Il suffit de démontrer que, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, alors G possède un élément g_i d'ordre $p_i^{\alpha_i}$ pour tout i. En effet, la question 2 assurera alors que l'élément $g_1 g_2 \dots g_r$ est d'ordre n. Remarquons que si d est un diviseur de n, alors $X^d - 1$ divise $X^n - 1$ dans $k[X]$, le quotient étant $\sum_{i=0}^{n/d-1} X^{id}$. En particulier, $X^d - 1$ est aussi scindé à racines distinctes dans G. Pour tout i, il existe donc au moins une racine g_i de $X^{p_i^{\alpha_i}} - 1$ dans G qui n'est pas racine de $X^{p_i^{\alpha_i - 1}} - 1$. Un tel élément est donc d'ordre $p_i^{\alpha_i}$, ce qui conclut la démonstration.

Exercice 5. Recherche d'exemples

1. Donner un exemple de groupe infini dont tous les éléments sont d'ordre fini.

   Le sous-groupe μ de $\mathbb{C}^\times$ constitué des racines de l'unité d'ordre arbitraire, i.e. $\mu = \bigcup_{n \geq 1} \mu_n$, convient. Un autre exemple est $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, dont tous les éléments sont d'ordre 1 ou 2 (ou plus généralement, tout produit infini de groupes d'ordres bornés)

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

   On peut regarder les réflexions $s_0(x) = -x$ et $s_1(x) = 1 - x$ dans le groupe d'isométries de l'espace euclidien $\mathbb{R}$. Elles sont d'ordre 2, mais $s_0 \circ s_1$ est la translation $x \mapsto x + 1$, qui est d'ordre infini. Un autre exemple du même type est obtenu en considérant deux réflexions orthogonales s et t du plan euclidien. On a $s^2 = t^2 = 1$, et st est la rotation d'angle le double de l'angle θ entre les deux axes. Ainsi, st est d'ordre fini si, et seulement si, $\theta \in \mathbb{Q}\pi$. On pouvait aussi regarder le groupe $\mathbb{Z}$ muni de la loi $x \cdot y = x + (-1)^x y$.

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

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

1. Montrer que A est d'ordre a dans le groupe $SL_2(\mathbb{C})$.

   La matrice $A^k = \mathrm{diag}(\xi_a^k, \xi_a^{-k})$ est l'identité si et seulement si $\xi_a^k = 1$, i.e. a divise k.

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 $SL_2(\mathbb{C})$.

   La matrice g étant une matrice 2×2, on a la formule $\chi_g(X) = X^2 - \mathrm{tr}(g)X + \det g$, et comme $g \in SL_2(\mathbb{C})$ on a $\det g = 1$. On en déduit que $\chi_g(X) = X^2 - (x + x^{-1})X + 1 = (X - x)(X - x^{-1})$. Comme la trace de B est $\xi_b + \xi_b^{-1}$, on déduit du calcul précédent que $\chi_B(X)$ est scindé à racines simples ξ_b et ξ_b^{-1} (car $b > 2$), et donc que B est semblable à $\mathrm{diag}(\xi_b, \xi_b^{-1})$. Donc B est d'ordre b par la question précédente.

3. On pose $B_t = U_t B U_t^{-1}$. Calculer la trace de AB_t.

   On calcule

$$B_t = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \xi_b + \xi_b^{-1} \end{bmatrix} \begin{bmatrix} 1 & -t \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \xi_b + \xi_b^{-1} - t \end{bmatrix} = \begin{bmatrix} t & * \\ 1 & \xi_b + \xi_b^{-1} - t \end{bmatrix},$$

donc

$$AB_t = \begin{bmatrix} \xi_a t & * \\ \xi_a^{-1} & \xi_a^{-1}(\xi_b + \xi_b^{-1} - t) \end{bmatrix},$$

d'où $\operatorname{tr} AB_t = \xi_a t + \xi_a^{-1}(\xi_b + \xi_b^{-1} - t) = (\xi_a - \xi_a^{-1})t + \xi_a^{-1}(\xi_b + \xi_b^{-1})$.

4. On suppose $c \geq 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit AB_t est d'ordre c.
   La trace ci-dessus est de la forme $\alpha t + \beta$ avec $\alpha \neq 0$. Si $c < \infty$, pour t bien choisi elle vaut donc $\xi_c + \xi_c^{-1}$ et AB_t est d'ordre c par l'observation de la question 2 (on utilise $c > 2$). Si $c = \infty$, pour un t bien choisi, on a $|\operatorname{tr} AB_t| > 2$, et donc AB_t est d'ordre infini (les valeurs propres d'une $M \in GL_n(\mathbb{C})$ d'ordre fini sont des racines de l'unité).

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.
   En effet, si $p \equiv 1$ mod. abc, le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est d'ordre $p-1$, contient des éléments d'ordre a, b et c, que l'on note encore ξ_a, ξ_b et ξ_c. L'argument précédent fonctionne alors verbatim dans $G = SL_2(\mathbb{Z}/p\mathbb{Z})$.

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

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

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 $\deg B < \deg Q$).
   On remarque que les $e^{\frac{2ik\pi}{n}}$ avec $1 \leq k \leq n$ et $(k,n) = 1$ sont exactement les racines de l'unité d'ordre n. Donc on a

$$X^n - 1 = \prod_{\substack{\zeta \in \mu \\ \zeta^n = 1}} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \mu \\ \zeta \text{ d'ordre } d}} (X - \zeta) = \prod_{d|n} \Phi_d .$$

   Pour montrer que $\Phi_n \in \mathbb{Z}[X]$, on procède par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$, c'est vrai car $\Phi_1 = X - 1$. Supposons le résultat vrai jusqu'au rang $n-1$ et montrons-le au rang n. D'après l'hypothèse de récurrence, le polynôme $Q = \prod_{\substack{d|n \\ d \neq n}} \Phi_d$ est dans $\mathbb{Z}[X]$ et on a $X^n - 1 = \Phi_n Q$. Comme Q est unitaire, on peut effectuer la division euclidienne de $X^n - 1$ par Q dans $\mathbb{Z}[X]$ et on écrit $X^n - 1 = AQ + B$ avec $A, B \in \mathbb{Z}[X]$ et $\deg B < \deg Q$. On a donc $AQ + B = \Phi_n Q$ donc $B = (\Phi_n - A)Q$ et en regardant les degrés on obtient $B = 0$ et $A = \Phi_n$, d'où $\Phi_n \in \mathbb{Z}[X]$, ce qui achève la récurrence.

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.
   Soit $\alpha \in k$ une racine double de $X^n - 1$, on a $(X - \alpha)^2 | X^n - 1$ donc $(X - \alpha) | nX^{n-1}$ en dérivant, puis $n\alpha^{n-1} = 0$. Or $n\alpha^{n-1} = (n \cdot 1)\alpha^{n-1}$ avec $n \cdot 1 \neq 0$, donc $\alpha = 0$ par intégrité. Or, 0 n'est pas racine de $X^n - 1$; on en déduit que $X^n - 1$ n'a pas de racine double.

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 $p \equiv 1[n]$.
   Dans $\mathbb{Z}$ on a la relation $a^n - 1 = \prod_{d|n} \Phi_d(a)$, donc $p | (a^n - 1)$, c'est à dire $a^n \equiv 1[p]$. On en déduit que a appartient au groupe $\mathbb{F}_p^\times$ et que si on note $m \in \mathbb{N}^*$ l'ordre de a dans ce groupe, on a $m | n$. Si $m = n$, alors n divise le cardinal de $\mathbb{F}_p^\times$ par le théorème de Lagrange, donc $n | p - 1$, c'est à dire $p \equiv 1[n]$. Si $m < n$, en désignant par I l'ensemble des entiers naturels $d \in \mathbb{N}$ vérifiant les propriétés $d | n$, $d \nmid m$ et $d \neq n$, alors on a

$$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \cdot \prod_{d|m} \Phi_d \cdot \prod_{d \in I} \Phi_d = \Phi_n \cdot (X^m - 1) \cdot \prod_{d \in I} \Phi_d$$

   Comme $p | \Phi_n(a)$ et $a^n \equiv 1[p]$, la réduction modulo p du polynôme $X^n - 1$ admet $a \in \mathbb{F}_p$ comme racine double. On en déduit par la question précédente que $n \cdot 1 = 0$ dans $\mathbb{F}_p$, c'est à dire $p | n$.

4. Conclure.
   Supposons qu'il n'y ait qu'un nombre fini de nombre premiers $p_1, \ldots, p_r \in \mathbb{N}$ vérifiant $p_k \equiv 1[n]$ pour tout $k \in \{1, \ldots, r\}$. On note $a = np_1 \ldots p_r$. Dans $\mathbb{Z}$ on a la relation $-1 = 0^n - 1 = \prod_{d|n} \Phi_d(0)$, et donc $\Phi_n(0) = \pm 1$. Comme $\Phi_n(a) \equiv \Phi_n(0)[a]$, on a $\Phi_n(a) \equiv \pm 1[a]$. On va supposer $n \geq 2$ (le cas $n = 1$ est connu, et de toute manière n'importe lequel des autres cas l'implique). On remarque que pour ζ racine de l'unité différente de 1, on a $|a - \zeta| > 1$, d'où $|\Phi_n(a)| > 1$ puis $|\Phi_n(a)| \geq 2$. Soit donc p un nombre premier divisant $\Phi_n(a)$. D'après la question précédente, on a $p | n$ ou $p \equiv 1[n]$. Dans les deux cas, on a $p | a$, donc $\Phi_n(a) \equiv \pm 1[p]$. Mais on a choisi p de sorte que $\Phi_n(a) \equiv 0[p]$; absurde.

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 $x_1, \dots, x_n$, avec x_i d'ordre d_i.

1. Montrer que $|G|$ divise $d_1 \dots d_n$.
   On remarque que comme on a $d_i x_i = 0$ dans G pour $i = 1, \dots, n$, on dispose d'un morphisme bien défini $f : \prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z}) \to G, (\overline{m_i}) \mapsto \sum_{i=1}^n m_i x_i$. Il est surjectif car les x_i engendrent G. On a donc $d_1 d_2 \dots d_n = |\prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z})| = |\operatorname{Im} f||\ker f| = |G||\ker f|$, et donc $|G|$ divise $d_1 d_2 \dots d_n$.
2. En déduire que si p premier divise $|G|$, alors G admet un élément d'ordre p.
   On constate que si p divise $|G|$, il divise l'un des d_i, disons $d_i = p m_i$, et donc $m_i x_i$ est d'ordre $d_i/m_i = p$.

Exercice 9. Zoologie

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

On sait que si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est l'unique groupe de cardinal p. Donc on va regarder les cardinaux non premiers. En cardinal 4, tout élément non trivial a ordre 2 ou 4. S'il existe un élément d'ordre 4, le groupe est cyclique donc abélien. Sinon, tout élément non trivial a ordre 2 et le groupe est abélien (c.f. TD n° 1). En cardinal 6, on a le groupe S_3 où les permutations $(1,2)$ et $(2,3)$ ne commutent pas. On en déduit que le cardinal minimal d'un groupe non abélien vaut 6.