

Groupes et actions

I. Sous-groupes distingués et groupe quotient

Dans tout le chapitre, G désigne un groupe noté multiplicativement, de neutre e . On note $|G|$ son ordre lorsqu'il est fini. L'objectif est double : d'abord fabriquer de nouveaux groupes par passage au quotient, ensuite étudier un groupe à travers la façon dont il agit sur un ensemble.

1. Classes à gauche et théorème de Lagrange

Soit H un sous-groupe de G . La relation $x \sim y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence. Sa classe de x est la **classe à gauche** $xH = \{xh \mid h \in H\}$. L'ensemble des classes se note G/H , et son cardinal $[G:H]$ s'appelle l'**indice** de H dans G .

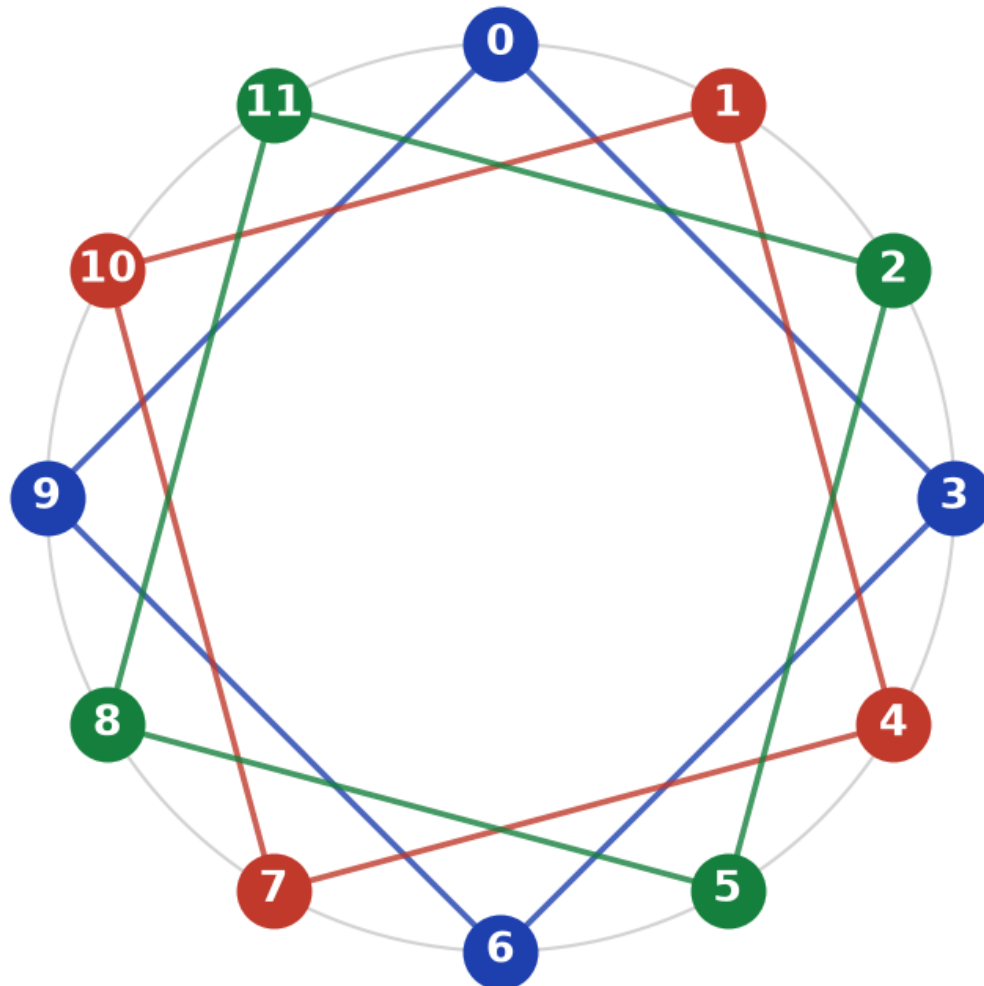
Théorème :

(Lagrange) Si G est fini et H est un sous-groupe de G , alors $|G| = [G:H] |H|$. En particulier, l'ordre de H divise l'ordre de G , et l'ordre de tout élément de G divise $|G|$.

Démonstration :

Les classes à gauche forment une partition de G . De plus, l'application $h \rightarrow xh$ est une bijection de H sur xH , de réciproque $y \rightarrow x^{-1}y$. Ainsi, chaque classe a exactement $|H|$ éléments. Il y a $[G:H]$ classes, d'où la formule. Enfin, l'ordre d'un élément g est l'ordre du sous-groupe $\langle g \rangle$.

Par exemple, dans $\mathbb{Z}/12\mathbb{Z}$, le sous-groupe $H = \{0, 3, 6, 9\}$ possède trois classes. La figure ci-dessous place les douze éléments sur un cercle et colore chaque classe : on voit trois carrés disjoints de même taille, conformément au théorème de Lagrange.



- $H = \{0, 3, 6, 9\}$
- $1 + H = \{1, 4, 7, 10\}$
- $2 + H = \{2, 5, 8, 11\}$

2. Sous-groupes distingués

Définition :

Un sous-groupe H de G est **distingué** (ou normal) si $gHg^{-1} \subset H$ pour tout $g \in G$. On note alors $H \trianglelefteq G$. De façon équivalente, $gH = Hg$ pour tout $g \in G$: classes à gauche et à droite coïncident.

Dans un groupe abélien, tout sous-groupe est distingué. En revanche, dans S_3 , le sous-groupe $\{\text{id}, (1\ 2)\}$ n'est pas distingué. En effet, $(1\ 3)(1\ 2)(1\ 3) = (2\ 3)$ n'appartient pas à ce sous-groupe.

Proposition :

Les sous-groupes suivants sont toujours distingués :

- le noyau $\ker f$ de tout morphisme de groupes $f : G \rightarrow G'$;
- le centre $Z(G) = \left\{ z \in G \mid \forall g \in G, gz = zg \right\}$;
- tout sous-groupe d'indice 2 ;
- l'intersection d'une famille de sous-groupes distingués.

Démonstration :

Si $f(h) = e$, alors $f(ghg^{-1}) = f(g)f(g)^{-1} = e$. Pour le centre, $gzg^{-1} = z$. Enfin, si $[G:H] = 2$, les deux classes à gauche sont H et $G \setminus H$; de même pour les classes à droite. Donc, pour $g \notin H$, on a $gH = G \setminus H = Hg$. Le cas de l'intersection est immédiat.

Méthode :

Pour montrer que H est distingué dans G , on dispose de quatre stratégies :

- calculer ghg^{-1} et vérifier qu'il est dans H , en se limitant si besoin à des générateurs g de G ;

- reconnaître H comme le noyau d'un morphisme bien choisi (déterminant, signature, projection) ;
- observer que H est d'indice 2 ;
- montrer que H est une réunion de classes de conjugaison de G .

3. Construction du groupe quotient

Théorème :

Soit $H \triangleleft G$. La loi $(xH)(yH) = xyH$ est bien définie sur G/H et en fait un groupe, de neutre H . La **projection canonique** $\pi : G \rightarrow G/H, x \rightarrow xH$, est un morphisme surjectif de noyau H .

Démonstration :

Supposons $xH = x'H$ et $yH = y'H$. On écrit $x' = xh$ et $y' = yk$ avec $h, k \in H$. Alors $x'y' = xy(y^{-1}hy)k$. Or $y^{-1}hy \in H$, car H est distingué. Donc $x'y'H = xyH$, et la loi ne dépend pas des représentants. Les axiomes de groupe se déduisent alors de ceux de G .

Attention :

Si H n'est pas distingué, la formule $(xH)(yH) = xyH$ n'a pas de sens. Par exemple, avec $H = \{\text{id}, (1\ 2)\}$ dans S_3 , on a $(1\ 3)H = (1\ 3)(1\ 2)H$. Pourtant, en multipliant à droite par $(1\ 3)$, le premier représentant donne $(1\ 3)(1\ 3)H = H$, tandis que le second donne $(1\ 3)(1\ 2)(1\ 3)H = (2\ 3)H \neq H$.

II. Les théorèmes d'isomorphisme

Le groupe quotient n'est utile que si l'on sait l'identifier. C'est le rôle des théorèmes d'isomorphisme. Ils reposent tous sur une même propriété de factorisation.

Théorème :

(Propriété universelle) Soit $H \trianglelefteq G$ et $f : G \rightarrow G'$ un morphisme tel que $H \subset \ker f$. Il existe un unique morphisme $\bar{f} : G/H \rightarrow G'$ tel que $f = \bar{f} \circ \pi$, donné par $\bar{f}(xH) = f(x)$.

Théorème :

(Premier théorème d'isomorphisme) Pour tout morphisme $f : G \rightarrow G'$, l'application $\bar{f}$ induit un isomorphisme

$$G/\ker f \simeq \operatorname{Im} f.$$

Démonstration :

On prend $H = \ker f$. D'abord, $\bar{f}$ est bien définie : si $xH = yH$, alors $x^{-1}y \in \ker f$, donc $f(x) = f(y)$. Ensuite, $\bar{f}(xH) = e$ équivaut à $x \in \ker f$, c'est-à-dire $xH = H$; donc $\bar{f}$ est injective. Enfin, son image est $\operatorname{Im} f$.

Théorème :

(Deuxième théorème) Si H est un sous-groupe de G et $N \trianglelefteq G$, alors HN est un sous-groupe, $H \cap N \trianglelefteq H$ et $HN/N \simeq H/(H \cap N)$.

(Troisième théorème) Si $N \subset K$ sont deux sous-groupes distingués de G , alors $K/N \trianglelefteq G/N$ et

$$(G/N)/(K/N) \simeq G/K.$$

Les deux derniers énoncés se démontrent en appliquant le premier théorème. Pour le deuxième, on utilise $h \mapsto hN$, de H dans HN/N , qui est surjectif de noyau $H \cap N$. Pour le troisième, on factorise la projection $G \rightarrow G/K$ par G/N .

Méthode :

Pour établir un isomorphisme $G/H \simeq G'$, on procède en trois temps :

- on cherche un morphisme $f : G \rightarrow G'$ naturel (exponentielle, déterminant, module, réduction modulo n) ;
- on vérifie que f est surjectif ;
- on calcule $\ker f$ et on vérifie qu'il vaut H .

Le premier théorème d'isomorphisme conclut alors, sans jamais manipuler de classes.

Exemple :

Le morphisme $t \mapsto e^{2i\pi t}$, de $(\mathbb{R}, +)$ dans le groupe $\mathbb{U}$ des complexes de module 1, est surjectif de noyau $\mathbb{Z}$. Donc $\mathbb{R}/\mathbb{Z} \simeq \mathbb{U}$. De même, le déterminant, de $\mathrm{GL}_n(\mathbb{K})$ dans $\mathbb{K}^*$, est surjectif de noyau $\mathrm{SL}_n(\mathbb{K})$. Par conséquent, $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \simeq \mathbb{K}^*$.

III. Groupes cycliques et $\mathbb{Z}/n\mathbb{Z}$

Un groupe est **monogène** s'il est engendré par un seul élément, et **cyclique** s'il est de plus fini. Ces groupes sont entièrement classés.

Théorème :

Tout groupe monogène infini est isomorphe à $\mathbb{Z}$. Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration :

Soit $G = \langle g \rangle$. Le morphisme $k \rightarrow g^k$, de $\mathbb{Z}$ dans G , est surjectif. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. Si $n = 0$, on obtient $G \simeq \mathbb{Z}$. Sinon, le premier théorème d'isomorphisme donne $G \simeq \mathbb{Z}/n\mathbb{Z}$, et alors $|G| = n$.

Proposition :

Soit $n \geq 1$.

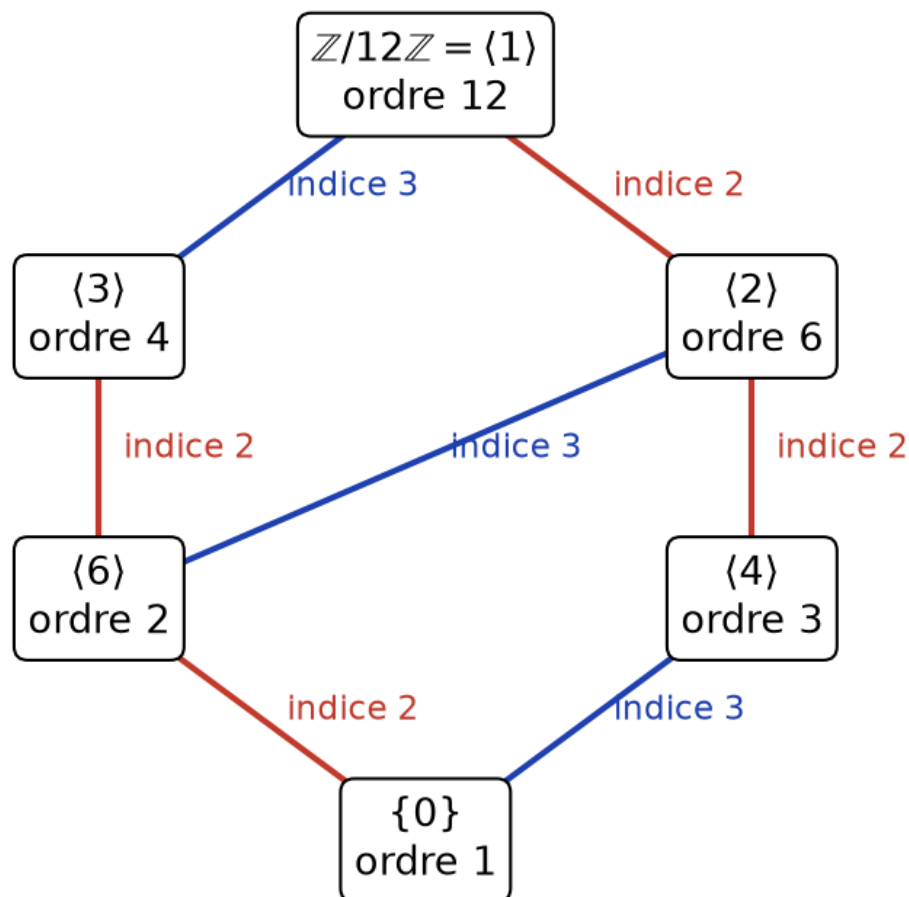
- Pour chaque diviseur d de n , $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d , à savoir $\langle \overline{n/d} \rangle$. Il n'y en a pas d'autre.
- L'ordre de $\overline{k}$ est $n / (k \wedge n)$. Ainsi, $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$; il y a $\varphi(n)$ générateurs.
- (Lemme chinois) Si $m \wedge n = 1$, alors $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Démonstration :

Un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est l'image d'un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$, c'est-à-dire $a\mathbb{Z}$ avec a divisant n . Son ordre vaut n/a , d'où l'unicité. Ensuite, $j\overline{k} = \overline{0}$ équivaut à $n \mid jk$, soit $\frac{n}{k \wedge n} \mid j$. Enfin, le morphisme $x \rightarrow (x \bmod m, x \bmod n)$ a pour noyau $\text{ppcm}(m, n)\mathbb{Z} = mn\mathbb{Z}$. Il est donc injectif sur $\mathbb{Z}/mn\mathbb{Z}$, puis bijectif par égalité des cardinaux.

La figure suivante représente les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, ordonnés par inclusion. On y lit les six

diviseurs de 12 : chaque arête relie un sous-groupe à un sous-groupe qui le contient avec un indice premier.



Remarque :

Un groupe d'ordre premier p est cyclique : tout élément différent de e est d'ordre p d'après Lagrange. En revanche, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique, car tous ses éléments sont d'ordre au plus 2.

IV. Actions de groupes, orbites et stabilisateurs

1. Définition

Définition :

Une **action** de G sur un ensemble X est une application $G \times X \rightarrow X$, $(g, x) \rightarrow g \cdot x$, telle que $e \cdot x = x$ et $g \cdot (h \cdot x) = (gh) \cdot x$ pour tous $g, h \in G$ et $x \in X$.

Autrement dit, une action est un morphisme $\rho: G \rightarrow \mathcal{S}(X)$, où $\rho(g): x \rightarrow g \cdot x$. L'action est **fidèle** si ρ est injectif. Trois exemples reviennent sans cesse :

- l'action de G sur lui-même par translation, $g \cdot x = gx$;
- l'action par conjugaison, $g \cdot x = gxg^{-1}$;
- l'action sur les classes à gauche G/H , $g \cdot (xH) = gxH$.

Théorème :

(Cayley) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Démonstration :

L'action par translation est fidèle, car $gx = x$ entraîne $g = e$. Le morphisme ρ est donc injectif, et $G \simeq \rho(G) \subset \mathcal{S}(G) \simeq \mathcal{S}_n$.

2. Orbites et stabilisateurs

Définition :

L'**orbite** de x est $G \cdot x = \{g \cdot x \mid g \in G\}$. Le **stabilisateur** de x est $G_x = \{g \in G \mid g \cdot x = x\}$; c'est un sous-groupe de G . Les orbites forment une partition de X . L'action est **transitive** s'il n'y a qu'une orbite.

Théorème :

(Relation orbite-stabilisateur) L'application $gG_x \rightarrow g \cdot x$ est une bijection de G/G_x sur $G \cdot x$. Si G est fini,

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

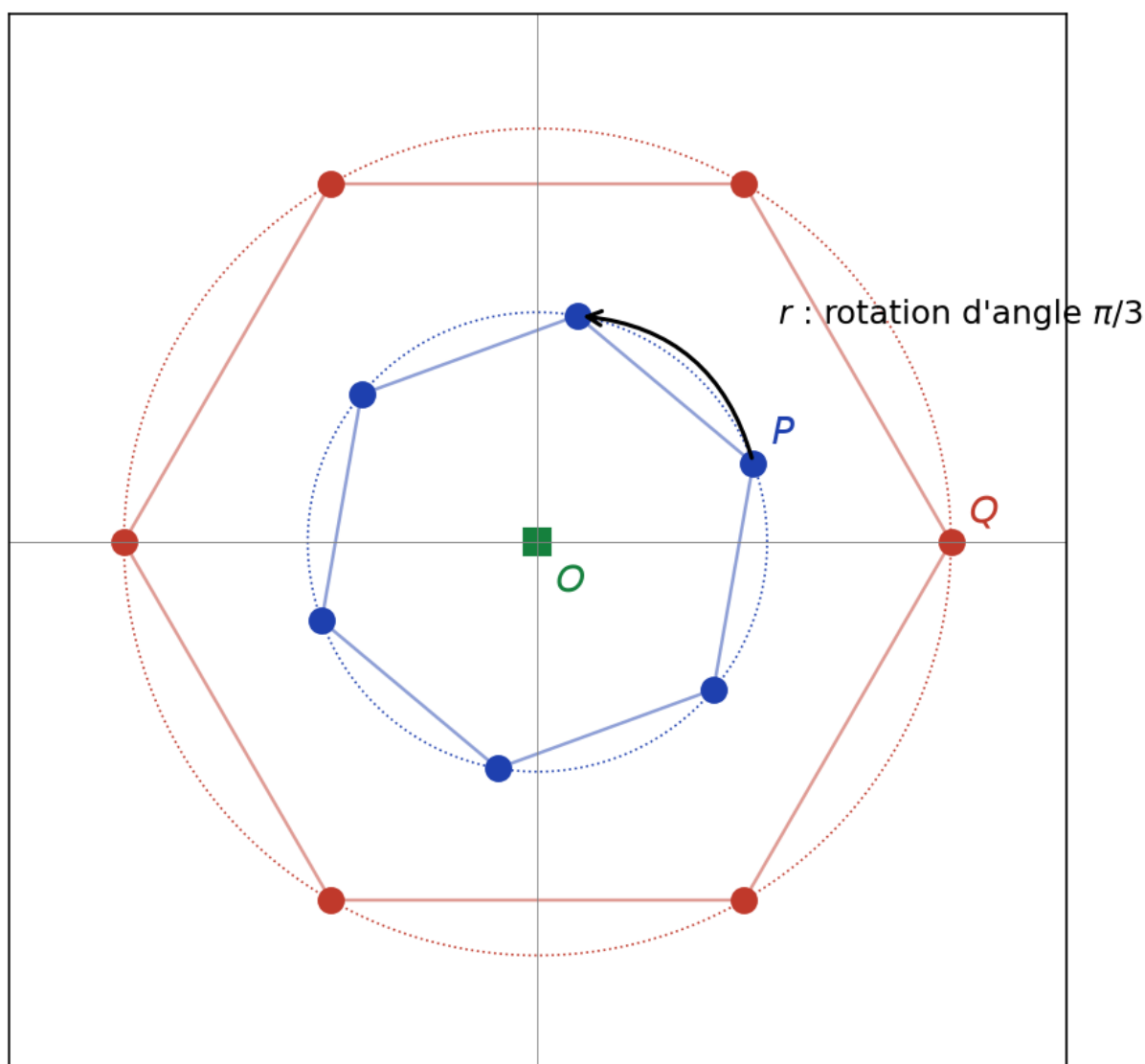
De plus, $G_{g \cdot x} = g G_x g^{-1}$.

Démonstration :

On a $g \cdot x = g' \cdot x$ si et seulement si $g^{-1}g' \in G_x$, c'est-à-dire $gG_x = g'G_x$. Ainsi, l'application est bien définie et injective. Elle est surjective par définition de l'orbite. Enfin, $h \cdot (g \cdot x) = g \cdot x$ équivaut à $g^{-1}hg \in G_x$.

Exemple :

Soit G le groupe des six rotations de centre O et d'angle $k\pi/3$, agissant sur le plan. L'orbite d'un point $P \neq O$ compte six points : ce sont les sommets d'un hexagone régulier. Son stabilisateur est donc trivial, car $6 = 6/1$. En revanche, l'orbite de O est $\{O\}$, de stabilisateur G tout entier. La figure ci-dessous montre ces orbites.



- orbite de P : 6 points, stabilisateur $\{id\}$
- orbite de Q : 6 points, stabilisateur $\{id\}$
- orbite de O : $\{O\}$, stabilisateur G entier

Méthode :

Pour calculer l'ordre d'un groupe fini G de transformations, on choisit un objet x sur lequel il agit (sommet, face, arête). On détermine son orbite, souvent tout l'ensemble par transitivité, puis son stabilisateur, plus petit et plus facile à décrire. On conclut par $|G| = |G \cdot x| \times |G_x|$.

3. Formule des classes et formule de Burnside

Supposons X fini, et choisissons un représentant $x_1, \dots, x_r$ par orbite. La partition en orbites donne aussitôt la **formule des classes**.

Théorème :

(Formule des classes)

$$|X| = \sum_{i=1}^r [G : G x_i].$$

En particulier, pour l'action de G fini sur lui-même par conjugaison, les orbites sont les classes de conjugaison, les stabilisateurs sont les centralisateurs $C(x)$, et

$$|G| = |Z(G)| + \sum_j [G : C(x_j)],$$

où la somme porte sur les classes de conjugaison non réduites à un élément.

Corollaire :

Soit p premier. Tout groupe d'ordre p^k , avec $k \geq 1$, a un centre non trivial.

Démonstration :

Chaque indice $[G : C(x_j)]$ divise p^k et est différent de 1. Il est donc divisible par p . Par conséquent, $|Z(G)| = |G| - \sum_j [G : C(x_j)]$ est divisible par p . Comme $e \in Z(G)$, on a $|Z(G)| \geq 1$, donc $|Z(G)| \geq p$.

Proposition :

(Formule de Burnside) Si G et X sont finis, le nombre d'orbites vaut

$$r = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|, \text{ où } \text{Fix}(g) = \{x \in X \mid g \cdot x = x\}.$$

Démonstration :

On compte de deux façons les couples (g, x) tels que $g \cdot x = x$. D'une part, leur nombre vaut $\sum_g |\text{Fix}(g)|$. D'autre part, il vaut $\sum_x |G_x| = \sum_x |G|/|G \cdot x|$. Or chaque orbite Ω contribue $\sum_{x \in \Omega} 1/|\Omega| = 1$ à la somme $\sum_x 1/|G \cdot x|$. D'où le résultat.

V. Le groupe symétrique

1. Cycles et décomposition

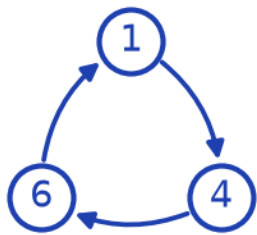
Un **cycle** de longueur $k \geq 2$ est une permutation $(a_1 a_2 \dots a_k)$ qui envoie a_1 sur a_2 , puis a_2 sur a_3 , et ainsi de suite jusqu'à $a_k \rightarrow a_1$, en fixant les autres points. Une **transposition** est un cycle de longueur 2.

Théorème :

Toute permutation $\sigma \in \mathcal{S}_n$ se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près, et les cycles commutent. Les supports des cycles sont les orbites non triviales de l'action de $\langle \sigma \rangle$ sur $\{1, \dots, n\}$. L'ordre de σ est le ppcm des longueurs des cycles.

Exemple :

Dans $\mathcal{S}_8$, soit σ définie par $\sigma(1) = 4$, $\sigma(4) = 6$, $\sigma(6) = 1$, $\sigma(2) = 7$, $\sigma(7) = 2$, $\sigma(5) = 8$, $\sigma(8) = 5$ et $\sigma(3) = 3$. On suit les flèches à partir de 1, puis du plus petit point non encore atteint. On obtient $\sigma = (1\ 4\ 6)(2\ 7)(5\ 8)$, d'ordre $\text{ppcm}(3, 2, 2) = 6$. La figure ci-dessous dessine ces cycles.



cycle (1 4 6)
longueur 3



transposition
(2 7)



transposition
(5 8)



point fixe
3

Proposition :

Pour tout cycle et toute permutation τ , on a $\tau(a_1 \dots a_k) \tau^{-1} = (\tau(a_1) \dots \tau(a_k))$. Par conséquent, deux permutations sont conjuguées dans $\mathcal{S}_n$ si et seulement si elles ont le même **type**, c'est-à-dire la même liste de longueurs de cycles.

2. Signature et groupe alterné

Théorème :

Les transpositions engendrent $\mathcal{S}_n$. Il existe un unique morphisme non trivial $\varepsilon : \mathcal{S}_n \rightarrow \{-1, 1\}$ pour $n \geq 2$, la **signature**. Il vérifie $\varepsilon(\tau) = -1$ pour toute transposition, et $\varepsilon(c) = (-1)^{k-1}$ pour un cycle de longueur k .

En pratique, on calcule la signature par la décomposition en cycles. En effet,

$(a_1 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ est un produit de $k-1$ transpositions. Ainsi, la permutation σ de l'exemple précédent a pour signature $(+1)(-1)(-1) = 1$.

Définition :

Le **groupe alterné** $\mathcal{A}_n$ est le noyau de la signature. C'est un sous-groupe distingué d'indice 2 de $\mathcal{S}_n$ pour $n \geq 2$, donc d'ordre $n!/2$.

Proposition :

Pour $n \geq 3$, le groupe $\mathcal{A}_n$ est engendré par les 3-cycles.

Démonstration :

Un élément de $\mathcal{A}_n$ est un produit d'un nombre pair de transpositions. Il suffit donc d'écrire un produit de deux transpositions distinctes à l'aide de 3-cycles. Si elles ont un point commun, $(a b)(a c) = (a c b)$. Sinon, $(a b)(c d) = (a b)(b c)(b c)(c d) = (b c a)(c d b)$.

Remarque :

Pour $n \geq 5$, le groupe $\mathcal{A}_n$ est **simple** : ses seuls sous-groupes distingués sont $\{\text{id}\}$ et lui-même. Le cas $n = 5$ est traité en exercice. En revanche, $\mathcal{A}_4$ contient le sous-groupe distingué $V_4 = \{\text{id}, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}$, réunion de deux classes de conjugaison.

VI. Groupes diédraux et groupes d'isométries

Soit $n \geq 3$ et P_n un polygone régulier à n sommets $A_0, \dots, A_{n-1}$, de centre O . Le **groupe diédral** D_n est le groupe des isométries du plan qui conservent P_n .

Théorème :

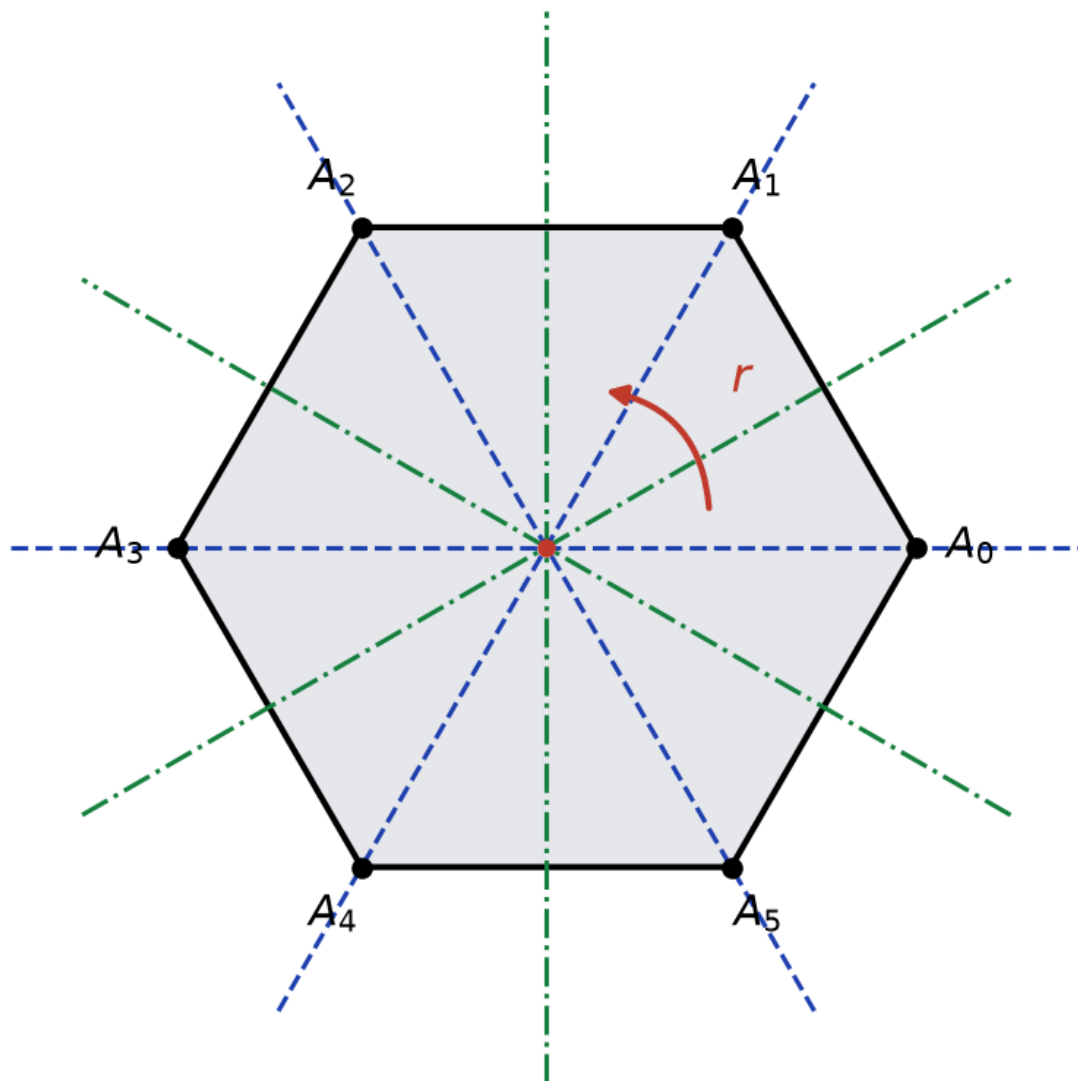
Le groupe D_n est d'ordre $2n$. Il est formé des n rotations r^k de centre O et d'angle $2k\pi/n$, et des n réflexions sr^k , où s est la réflexion d'axe (OA_0) . On a les relations

$$r^n = s^2 = \text{id}, \quad srs^{-1} = r^{-1}.$$

Démonstration :

Une isométrie qui conserve P_n fixe son centre de gravité O et permute les sommets. Le groupe D_n agit donc sur les n sommets. Cette action est transitive, grâce aux rotations r^k . Par ailleurs, le stabilisateur de A_0 fixe O et A_0 . C'est donc l'identité ou la réflexion s d'axe (OA_0) , car une isométrie fixant deux points distincts est l'identité ou la réflexion par la droite qui les joint. Par la relation orbite-stabilisateur, $|D_n| = n \times 2 = 2n$. Enfin, srs est une isométrie directe de D_n , donc une rotation r^k . Or elle envoie A_1 sur $s(r(A_{n-1})) = s(A_0) = A_0$. C'est donc r^{-1} .

La figure ci-dessous illustre le cas $n = 6$. Les six axes de symétrie sont de deux sortes : trois passent par deux sommets opposés, trois par les milieux de deux côtés opposés.



- axe par deux sommets opposés
- .- axe par les milieux de deux côtés opposés

Propriété :

Le sous-groupe $\langle r \rangle$ des rotations est cyclique d'ordre n et distingué dans D_n , car d'indice 2. Le quotient $D_n / \langle r \rangle$ est d'ordre 2. De plus, D_n n'est pas abélien, puisque $sr = r^{-1}s \neq rs$ dès que $n \geq 3$.

Exemple :

Calculons les classes de conjugaison des réflexions dans D_n . La relation $r^j (sr^k) r^{-j} = sr^{k-2j}$ montre que sr^k est conjuguée aux sr^{k+2m} . Si n est impair, toutes les réflexions sont conjuguées. En revanche, si n est pair, elles forment deux classes de $n/2$ éléments, qui correspondent aux deux sortes d'axes de la figure.

VII. Les théorèmes de Sylow

Le théorème de Lagrange donne une condition nécessaire sur l'ordre d'un sous-groupe. Sa réciproque est fautive en général : A_4 , d'ordre 12, n'a aucun sous-groupe d'ordre 6. Les théorèmes de Sylow fournissent une réciproque partielle.

Définition :

Soit G fini et p premier, avec $|G| = p^\alpha m$ et $p \nmid m$. Un **p -sous-groupe de Sylow** de G est un sous-groupe d'ordre p^α . On note n_p leur nombre.

Théorème :

(Sylow) Avec ces notations :

- G possède au moins un p -sous-groupe de Sylow ;
- les p -sous-groupes de Sylow sont deux à deux conjugués, et tout p -sous-groupe de G est contenu dans l'un d'eux ;
- n_p divise m et $n_p \equiv 1 \pmod{p}$.

La démonstration, admise ici, repose entièrement sur des actions de groupes et sur la formule des classes. Retenons surtout la conséquence suivante, qui sert constamment.

Corollaire :

Un p -sous-groupe de Sylow P est distingué dans G si et seulement si $n_p = 1$. En effet, les conjugués de P sont exactement les p -sous-groupes de Sylow.

Méthode :

Pour montrer qu'un groupe d'ordre donné n'est pas simple, on factorise son ordre, puis on liste les valeurs possibles de chaque n_p avec les deux conditions de divisibilité et de congruence. Si l'une d'elles force $n_p = 1$, c'est terminé. Sinon, on compte les éléments d'ordre p : deux sous-groupes d'ordre premier p distincts ne partagent que e , ce qui donne $n_p(p-1)$ éléments d'ordre p . On aboutit souvent à trop d'éléments.

Exemple :

Soit G d'ordre $15 = 3 \times 5$. D'abord, n_5 divise 3 et $n_5 \equiv 1 \pmod{5}$, donc $n_5 = 1$. Ensuite, n_3 divise 5 et $n_3 \equiv 1 \pmod{3}$, donc $n_3 = 1$. Les sous-groupes P_3 et P_5 sont distingués, d'intersection triviale. Ainsi, pour $x \in P_3$ et $y \in P_5$, le commutateur $xyx^{-1}y^{-1}$ appartient à $P_3 \cap P_5 = \{e\}$. Par conséquent, xy est d'ordre 15 et $G \simeq \mathbb{Z}/15\mathbb{Z}$.

Ce qu'il faut retenir

- Un sous-groupe H est distingué si $gHg^{-1} \subset H$ pour tout g ; les noyaux, le centre et les sous-groupes d'indice 2 le sont toujours.
- Le quotient G/H n'est un groupe que si H est distingué ; la projection canonique a pour noyau H .
- Premier théorème d'isomorphisme : $G/\ker f \simeq \operatorname{Im} f$. C'est l'outil standard pour identifier un quotient.

- Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, qui a un unique sous-groupe par diviseur de n et $\varphi(n)$ générateurs.
- Relation orbite-stabilisateur : $|G \cdot x| = |G|/|G_x|$; elle calcule l'ordre des groupes de transformations.
- Formule des classes : $|G| = |Z(G)| + \sum [G : C(x_j)]$; un p -groupe non trivial a un centre non trivial.
- Dans S_n , on décompose en cycles disjoints ; ordre = ppcm des longueurs, signature = produit des $(-1)^{k-1}$, conjugaison = même type.
- D_n est d'ordre $2n$, engendré par r et s avec $srs^{-1} = r^{-1}$; ses rotations forment un sous-groupe distingué cyclique.
- Sylow : $n_p | m$ et $n_p \equiv 1 \pmod{p}$; si $n_p = 1$, le p -Sylow est distingué.

Questions fréquentes sur groupes et actions

Pourquoi faut-il qu'un sous-groupe soit distingué pour former un quotient ?

La loi $(xH)(yH) = xyH$ doit être indépendante des représentants choisis. Cette indépendance équivaut exactement à $gHg^{-1} \subset H$ pour tout g . Sans cette condition, deux représentants d'une même classe peuvent donner des produits dans des classes différentes.

Comment calcule-t-on l'ordre d'un groupe d'isométries ?

On fait agir le groupe sur un ensemble d'objets géométriques, par exemple les sommets. On détermine l'orbite d'un sommet, souvent tous les sommets, puis son stabilisateur. La relation

$$|G| = |G \cdot x| \times |G_x|$$

donne alors l'ordre, par exemple $2n$ pour le groupe diédral D_n .

À quoi servent les théorèmes de Sylow en pratique ?

Ils donnent l'existence de sous-groupes d'ordre p^α et des contraintes sur leur nombre n_p . Si les conditions $n_p | m$ et $n_p \equiv 1 \pmod{p}$ forcent $n_p = 1$, le sous-groupe est distingué. On montre ainsi qu'un groupe d'ordre 15 est cyclique, ou qu'un groupe d'ordre 30 n'est pas simple.

Comment reconnaître deux permutations conjuguées ?

Deux permutations de $\mathcal{S}_n$ sont conjuguées si et seulement si leurs décompositions en cycles disjoints ont les mêmes longueurs. Pour trouver un conjugué, on écrit les deux décompositions l'une sous l'autre et on envoie chaque élément sur celui qui occupe la même place.

Pour aller plus loin en L3

- Les énoncés : [exercices de maths en L3 sur groupes et actions](#)
- Chapitre précédent : [Espaces \$L^p\$](#)
- Chapitre suivant : [Anneaux, idéaux et arithmétique](#)
- Tester vos connaissances : [QCM de maths en L3 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L3](#) et la [licence de maths de L1 à L3](#)