

Groupes

I. Lois de composition interne et notion de groupe

Vous connaissez déjà plusieurs opérations très différentes : l'addition des entiers, le produit des matrices inversibles, la composition des bijections. Pourtant, elles partagent les mêmes règles de calcul. La notion de groupe isole ces règles communes. Ainsi, un théorème démontré une fois pour tous les groupes s'applique aussitôt à chacun de ces exemples.

Définition :

Une **loi de composition interne** sur un ensemble E est une application $E \times E \rightarrow E$, notée $(x, y) \rightarrow x * y$. Elle est **associative** si $(x * y) * z = x * (y * z)$ pour tous x, y, z de E . Elle est **commutative** si $x * y = y * x$ pour tous x, y . Un élément e est **neutre** si $e * x = x * e = x$ pour tout x .

Définition :

Un **groupe** est un couple $(G, *)$ où $*$ est une loi de composition interne sur G telle que :

- la loi $*$ est associative ;
- il existe un élément neutre e ;
- tout $x \in G$ admet un **symétrique** x' : $x * x' = x' * x = e$.

Le groupe est dit **abélien** (ou commutatif) si la loi est de plus commutative. Si G est fini, son cardinal $|G|$ s'appelle l'**ordre** du groupe.

Propriété :

Dans un groupe G , le neutre est unique et chaque élément a un unique symétrique, noté x^{-1} . De plus, $(xy)^{-1} = y^{-1}x^{-1}$ et $(x^{-1})^{-1} = x$. Enfin, tout élément est simplifiable : $ax = ay \Rightarrow x = y$ et $xa = ya \Rightarrow x = y$.

Démonstration :

Si e et e_1 sont neutres, alors $e = e e_1 = e_1$. Ensuite, si y et z sont deux symétriques de x , l'associativité donne $y = y(xz) = (yx)z = z$. De plus, $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e$, et le produit dans l'autre ordre vaut aussi e . Enfin, on multiplie $ax = ay$ à gauche par a^{-1} pour obtenir $x = y$.

Notation :

En notation multiplicative, on écrit xy , x^{-1} et x^n pour $n \in \mathbb{Z}$, avec $x^0 = e$ et $x^{-n} = (x^{-1})^n$. On a alors $x^m x^n = x^{m+n}$ et $(x^m)^n = x^{mn}$. Pour un groupe abélien, on utilise souvent la notation additive : $x + y$, $-x$, nx et le neutre 0 .

Les exemples suivants reviendront tout au long du chapitre. En effet, ils couvrent les trois familles annoncées : nombres, classes de congruence et transformations.

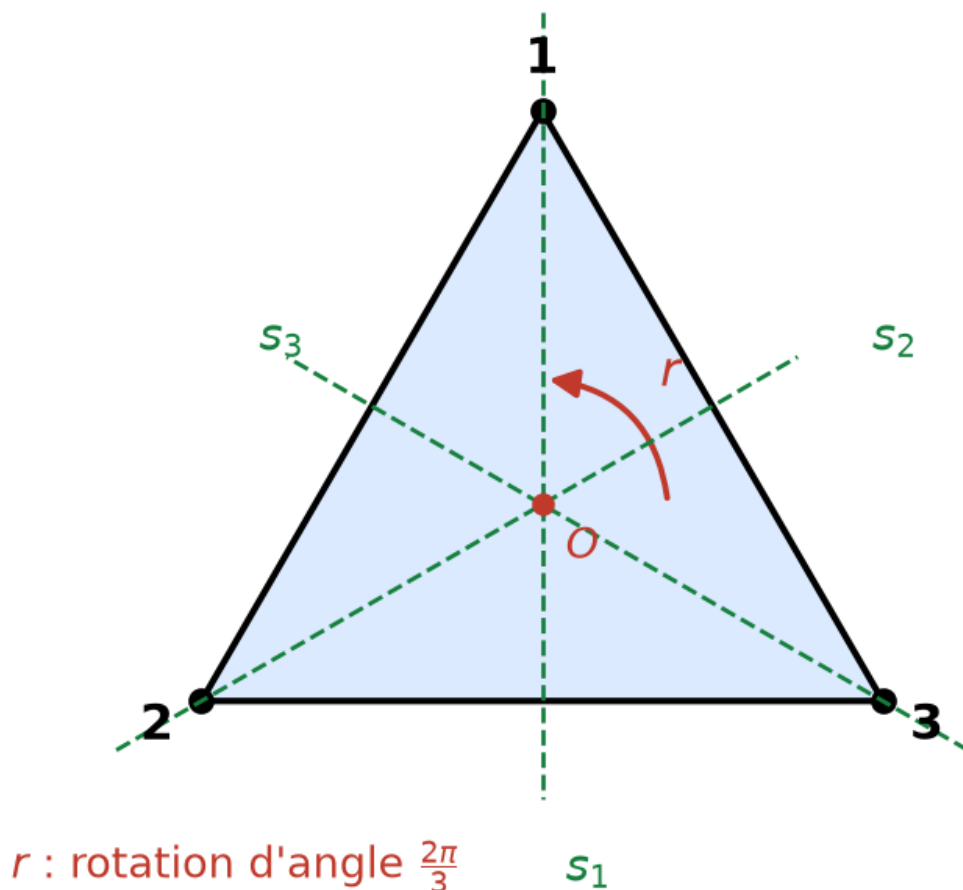
Exemple :

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ et $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des

groupes abéliens.

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien d'ordre n , de neutre $\bar{0}$.
- $\text{GL}_n(\mathbb{R})$, les matrices inversibles pour le produit, est un groupe non abélien dès que $n \geq 2$.
- L'ensemble $\mathcal{S}(E)$ des bijections de E dans E , muni de la composition, est un groupe de neutre Id_E .
- Les isométries du plan qui conservent un triangle équilatéral forment un groupe à six éléments : l'identité, deux rotations et trois symétries axiales.

La figure ci-dessous montre ce dernier groupe. D'abord, la rotation r de centre O et d'angle $\frac{2\pi}{3}$ envoie le sommet 1 sur le sommet 2. Ensuite, chaque symétrie s_k fixe le sommet k et échange les deux autres. Par exemple, on vérifie que $r \circ s_1 \neq s_1 \circ r$: ce groupe n'est donc pas abélien.



Attention :

$(\mathbb{N}, +)$ n'est pas un groupe, car 1 n'a pas d'opposé dans $\mathbb{N}$. De même, $(\mathbb{Z}, \times)$ n'est pas un groupe, car 2 n'a pas d'inverse entier. Enfin, $\mathbb{Z}/6\mathbb{Z} \setminus \{\bar{0}\}$ n'est pas stable par produit, puisque $\bar{2} \times \bar{3} = \bar{0}$.

II. Sous-groupes et sous-groupe engendré

La plupart des groupes utiles vivent à l'intérieur d'un groupe plus gros. C'est pourquoi on démontre rarement les axiomes de groupe directement. On prouve plutôt qu'une partie est un sous-groupe d'un groupe connu.

Définition :

Une partie H d'un groupe G est un **sous-groupe** de G si $e \in H$, si $xy \in H$ pour tous $x, y \in H$, et si $x^{-1} \in H$ pour tout $x \in H$. La loi de G induit alors sur H une structure de groupe.

Proposition :

Une partie H de G est un sous-groupe si et seulement si $H \neq \emptyset$ et, pour tous $x, y \in H$, $xy^{-1} \in H$.

Démonstration :

Le sens direct est clair. Réciproquement, soit $a \in H$. D'abord, $e = aa^{-1} \in H$. Ensuite, pour $y \in H$, on obtient $y^{-1} = ey^{-1} \in H$. Enfin, pour $x, y \in H$, on a $xy = x(y^{-1})^{-1} \in H$.

Méthode :

Pour montrer qu'un ensemble H muni d'une loi est un groupe :

- repérez un groupe connu G qui contient H avec la même loi ;
- vérifiez que $e \in H$, puis que $x, y \in H \Rightarrow xy^{-1} \in H$;
- ou bien reconnaissez H comme le noyau ou l'image d'un morphisme (partie III).

Pour montrer au contraire que H n'est pas un sous-groupe, un seul contre-exemple suffit : neutre

absent, produit ou inverse qui sort de H .

Exemple :

Le cercle $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$. En effet, $1 \in \mathbb{U}$, et si $|z| = |w| = 1$, alors $|zw^{-1}| = |z|/|w| = 1$. De même, $\mathrm{SL}_n(\mathbb{R}) = \{A : \det A = 1\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, et $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Propriété :

Toute intersection de sous-groupes de G est un sous-groupe de G . En revanche, une réunion de deux sous-groupes n'est en général pas un sous-groupe : $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ et $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, mais $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Définition :

Soit A une partie de G . Le **sous-groupe engendré** par A , noté $\langle A \rangle$, est l'intersection de tous les sous-groupes de G contenant A . C'est le plus petit sous-groupe de G qui contient A .

Proposition :

$\langle A \rangle$ est l'ensemble des produits finis $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$ avec $x_i \in A$ et $\varepsilon_i \in \{-1, 1\}$ (le produit vide valant e). En particulier, $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Démonstration :

Notons P l'ensemble de ces produits. D'abord, P contient e et A . Ensuite, le produit de deux tels produits en est encore un, et l'inverse de $x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$ vaut $x_k^{-\varepsilon_k} \dots x_1^{-\varepsilon_1}$. Donc P est un sous-groupe contenant A , d'où $\langle A \rangle \subset P$. Inversement, tout sous-groupe contenant A contient ces produits, donc $P \subset \langle A \rangle$.

Exemple :

Dans $(\mathbb{Z}, +)$, $\langle 4, 6 \rangle = \{4u + 6v : u, v \in \mathbb{Z}\} = 2\mathbb{Z}$, car $2 = 6 - 4$. Dans le groupe des isométries du triangle, $\langle r \rangle = \{\text{Id}, r, r^2\}$, tandis que $\langle r, s_1 \rangle$ est le groupe entier.

III. Morphismes de groupes, noyau et image

Un morphisme transporte la structure d'un groupe dans un autre. Il permet de comparer deux groupes, et surtout de fabriquer des sous-groupes sans calcul.

Définition :

Soient G et G' deux groupes. Une application $f : G \rightarrow G'$ est un **morphisme de groupes** si $f(xy) = f(x)f(y)$ pour tous $x, y \in G$. Un morphisme bijectif est un **isomorphisme** ; un isomorphisme de G dans lui-même est un **automorphisme**.

Propriété :

Si f est un morphisme, alors $f(e) = e'$, $f(x^{-1}) = f(x)^{-1}$ et $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$. La composée de deux morphismes est un morphisme, et la réciproque d'un isomorphisme est un isomorphisme.

Démonstration :

On a $f(e) = f(ee) = f(e)f(e)$, donc $f(e) = e'$ après simplification. Ensuite, $f(x)f(x^{-1}) = f(xx^{-1}) = e'$, d'où $f(x^{-1}) = f(x)^{-1}$. Enfin, si f est bijective, posons $x = f^{-1}(u)$ et $y = f^{-1}(v)$. Alors $f(xy) = uv$, donc $f^{-1}(uv) = xy = f^{-1}(u)f^{-1}(v)$.

Exemple :

- $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un isomorphisme, de réciproque $\ln$.
- $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ est un morphisme, car $\det(AB) = \det A \det B$.
- La projection $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $k \rightarrow \bar{k}$, est un morphisme surjectif.

Définition :

Le **noyau** d'un morphisme $f : G \rightarrow G'$ est $\ker f = \{x \in G : f(x) = e[\text{primeme?}]\}$. Son **image** est $\text{Im } f = f(G) = \{f(x) : x \in G\}$.

Théorème :

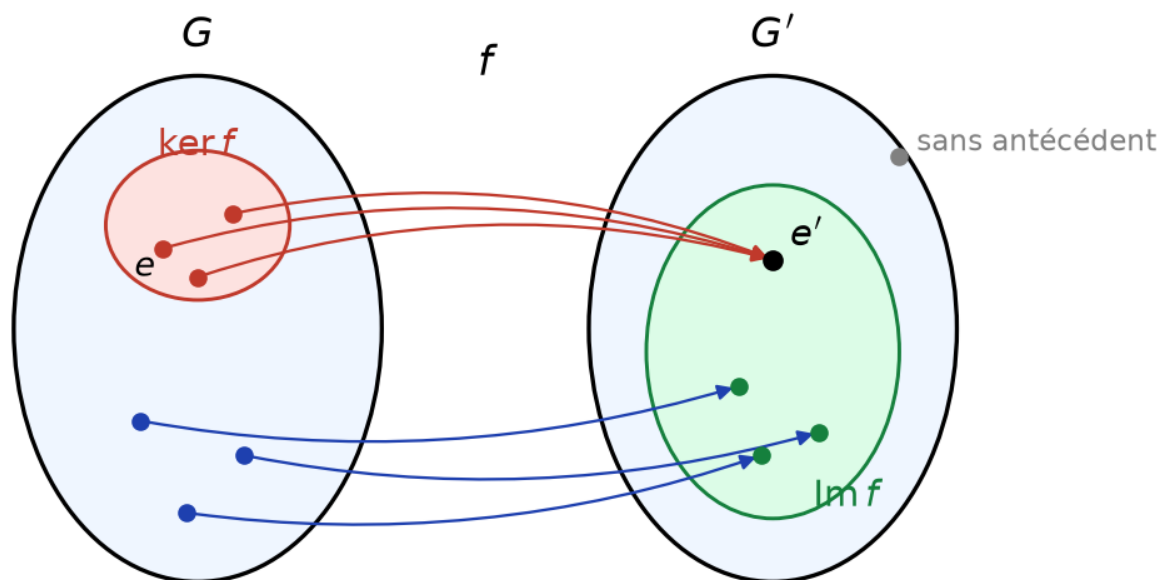
Soit $f : G \rightarrow G'$ un morphisme. L'image directe d'un sous-groupe de G est un sous-groupe de G' , et l'image réciproque d'un sous-groupe de G' est un sous-groupe de G . En particulier, $\ker f$ est un sous-groupe de G et $\text{Im } f$ un sous-groupe de G' . De plus :

$$f \text{ injective} \Leftrightarrow \ker f = \{e\}.$$

Démonstration :

Soit H un sous-groupe de G . D'abord, $e' = f(e) \in f(H)$. Ensuite, $f(x)f(y)^{-1} = f(xy^{-1}) \in f(H)$ pour $x, y \in H$. De même, si H' est un sous-groupe de G' et $x, y \in f^{-1}(H')$, alors $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$. Pour l'injectivité, supposons $\ker f = \{e\}$. Si $f(x) = f(y)$, alors $f(xy^{-1}) = e'$, donc $xy^{-1} = e$ et $x = y$. La réciproque vient de $f(e) = e'$.

Comme le montre la figure ci-dessous, tout le noyau est envoyé sur le seul neutre e' . En revanche, l'image peut ne pas remplir G' : certains éléments n'ont pas d'antécédent.



Méthode :

Pour identifier le noyau et l'image d'un morphisme f :

- vérifiez d'abord que f est bien un morphisme ;
- pour le noyau, résolvez l'équation $f(x) = e'$;

- pour l'image, cherchez pour quels y l'équation $f(x) = y$ a une solution ;
- concluez sur l'injectivité par le critère $\ker f = \{e\}$.

Exemple :

Soit $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \times)$, $t \mapsto e^{it}$. C'est un morphisme, car $e^{i(s+t)} = e^{is} e^{it}$.
 Ensuite, $e^{it} = 1 \Leftrightarrow t \in 2\pi\mathbb{Z}$, donc $\ker f = 2\pi\mathbb{Z}$. Enfin, tout complexe de module 1 s'écrit e^{it} , donc $\text{Im } f = \mathbb{U}$. Par conséquent, f n'est pas injective.

IV. Ordre d'un élément et groupes cycliques

1. Ordre d'un élément

Définition :

Soit $x \in G$. S'il existe un entier $n \geq 1$ tel que $x^n = e$, le plus petit d'entre eux est l'**ordre** de x . Sinon, on dit que x est d'ordre infini.

Théorème :

Soit x d'ordre fini n . Alors, pour tout $k \in \mathbb{Z}$, $x^k = e \Leftrightarrow n \mid k$. De plus,
 $\langle x \rangle = \{e, x, \dots, x^{n-1}\}$ a exactement n éléments. Si x est d'ordre infini, les x^k ,
 $k \in \mathbb{Z}$, sont deux à deux distincts.

Démonstration :

Écrivons la division euclidienne $k = qn + r$ avec $0 \leq r < n$. Alors

$x^k = (x^n)^q x^r = x^r$. Donc $x^k = e$ équivaut à $x^r = e$, c'est-à-dire à $r = 0$ par minimalité de n . Le même calcul montre que $\langle x \rangle = \{x^r : 0 \leq r < n\}$. Ces éléments sont distincts : si $x^r = x^s$ avec $0 \leq r < s < n$, alors $x^{s-r} = e$ avec $0 < s - r < n$, ce qui est exclu. Enfin, si x est d'ordre infini, $x^k = x^l$ avec $k < l$ donnerait $x^{l-k} = e$, ce qui est impossible.

Proposition :

Si x est d'ordre n et $k \in \mathbb{Z}$, alors x^k est d'ordre $\frac{n}{\text{pgcd}(n, k)}$.

Démonstration :

Posons $d = \text{pgcd}(n, k)$, $n = dn_1$ et $k = dk_1$, avec n_1 et k_1 premiers entre eux. Pour $m \geq 1$, on a $(x^k)^m = e \Leftrightarrow n \mid km \Leftrightarrow n_1 \mid k_1 m$. Par le lemme de Gauss, cela équivaut à $n_1 \mid m$. Le plus petit tel m est donc $n_1 = n/d$.

Méthode :

Pour déterminer l'ordre d'un élément x :

- calculez les puissances successives $x, x^2, x^3, \dots$ jusqu'à trouver e ;
- si vous savez que $x^N = e$, l'ordre divise N : testez seulement les diviseurs de N ;
- dans $\mathbb{Z}/n\mathbb{Z}$, l'ordre de $\bar{k}$ vaut $n/\text{pgcd}(n, k)$;

- dans $\mathbb{C}^*$, $e^{2i\pi p/q}$ avec $\text{pgcd}(p, q) = 1$ est d'ordre q , et un complexe de module différent de 1 est d'ordre infini.

Exemple :

Dans $\mathbb{Z}/12\mathbb{Z}$, l'élément $\bar{8}$ est d'ordre $12/\text{pgcd}(12, 8) = 3$. En effet, $\bar{8} + \bar{8} + \bar{8} = \bar{24} = \bar{0}$. Dans $\text{GL}_2(\mathbb{R})$, la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 4, car son carré vaut $-I_2$.

2. Sous-groupes de $\mathbb{Z}$

Théorème :

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$, et l'entier n est unique.

Démonstration :

Soit H un sous-groupe. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un entier non nul, donc aussi son opposé : $H \cap \mathbb{N}^*$ est non vide. Soit n son plus petit élément. D'abord, $n\mathbb{Z} \subset H$. Ensuite, pour $h \in H$, écrivons $h = qn + r$ avec $0 \leq r < n$. Alors $r = h - qn \in H$, donc $r = 0$ par minimalité. Ainsi $H = n\mathbb{Z}$. Enfin, n est le plus petit élément strictement positif de H , d'où l'unicité.

Corollaire :

Pour $a, b \in \mathbb{Z}$, on a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ avec $d = \text{pgcd}(a, b)$, et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ avec

$$m = \text{ppcm}(a, b).$$

3. Groupes monogènes et cycliques

Définition :

Un groupe G est **monogène** s'il existe $a \in G$ tel que $G = \langle a \rangle$; un tel a est un **générateur**. Un groupe monogène fini est dit **cyclique**.

Théorème :

Soit $G = \langle a \rangle$ un groupe monogène. Si G est infini, il est isomorphe à $(\mathbb{Z}, +)$. Si G est d'ordre n , il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ par $\bar{k} \rightarrow a^k$.

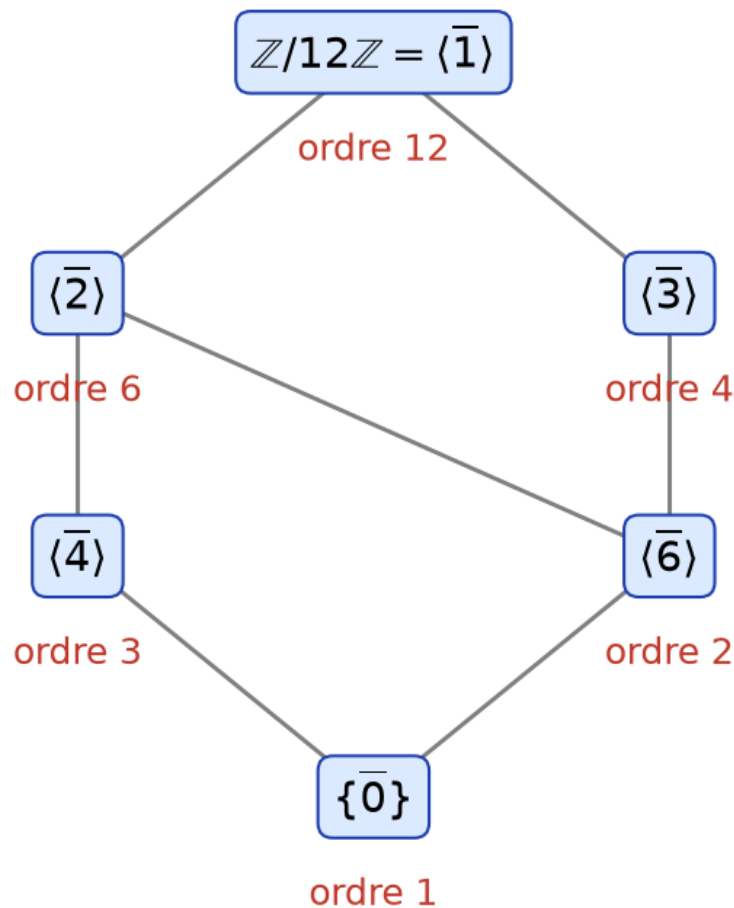
Démonstration :

L'application $\varphi: \mathbb{Z} \rightarrow G, k \rightarrow a^k$, est un morphisme surjectif. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. Si $n = 0$, φ est injective, donc c'est un isomorphisme. Sinon, a est d'ordre n , et $a^k = a^l \Leftrightarrow n \mid k - l$. Par conséquent, $\psi(\bar{k}) = a^k$ est bien défini et injectif. De plus, ψ est un morphisme surjectif, donc un isomorphisme.

Propriété :

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $\text{pgcd}(k, n) = 1$; il y en a $\varphi(n)$, où φ est l'indicatrice d'Euler. De plus, pour chaque diviseur d de n , $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d , à savoir $\langle \overline{n/d} \rangle$, et il n'en a pas d'autre.

En effet, $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il est d'ordre n , c'est-à-dire si $\text{pgcd}(n, k) = 1$. La seconde affirmation est démontrée dans la fiche d'exercices. La figure ci-dessous représente les six sous-groupes de $\mathbb{Z}/12\mathbb{Z}$: un trait relie deux sous-groupes quand le plus bas est inclus dans le plus haut.

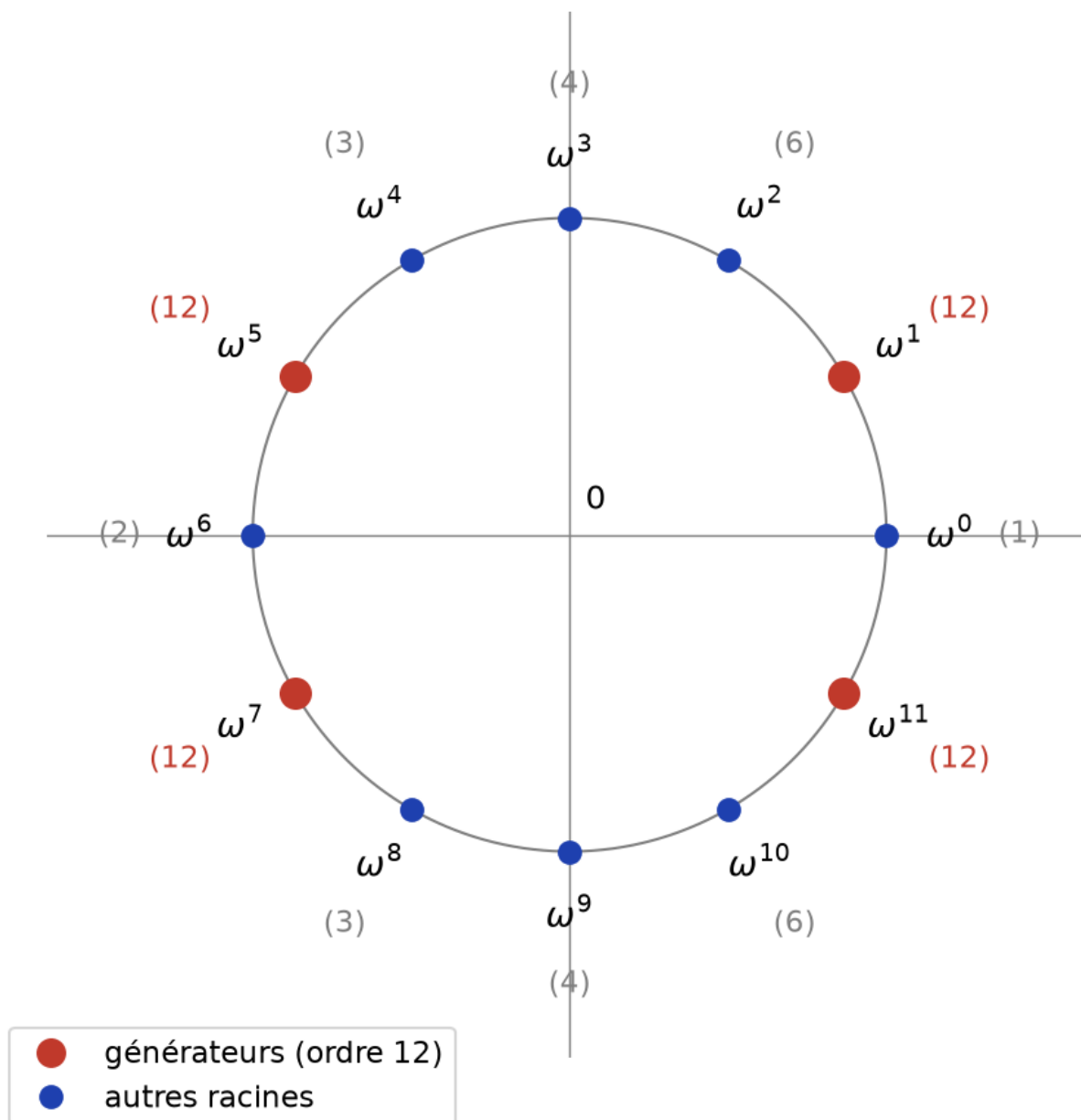


Exemple :

Le groupe $\mathbb{U}_n$ des racines n -ièmes de l'unité est cyclique d'ordre n , engendré par $\omega = e^{2i\pi/n}$. L'isomorphisme $\bar{k} \rightarrow \omega^k$ montre que ω^k est d'ordre $n/\text{pgcd}(n, k)$. Ainsi, les générateurs de $\mathbb{U}_{12}$ sont ω , ω^5 , ω^7 et ω^{11} : ce sont les racines primitives douzièmes de l'unité.

Sur la figure suivante, chaque racine ω^k de $\mathbb{U}_{12}$ porte son ordre entre parenthèses. Les quatre

générateurs apparaissent en rouge.



V. Classes modulo un sous-groupe et théorème de Lagrange

Un sous-groupe H découpe le groupe G en morceaux de même taille. Ce découpage donne le résultat le plus utile de la théorie des groupes finis : le théorème de Lagrange.

Définition :

Soit H un sous-groupe de G . On pose $x \sim y \Leftrightarrow x^{-1}y \in H$. La **classe à gauche** de x modulo H est $xH = \{xh : h \in H\}$. On définit de même la classe à droite Hx . L'ensemble des classes à gauche se note G/H .

Proposition :

La relation $\sim$ est une relation d'équivalence sur G , et la classe de x est xH . Par conséquent, les classes à gauche forment une partition de G . De plus, $h \rightarrow xh$ est une bijection de H sur xH .

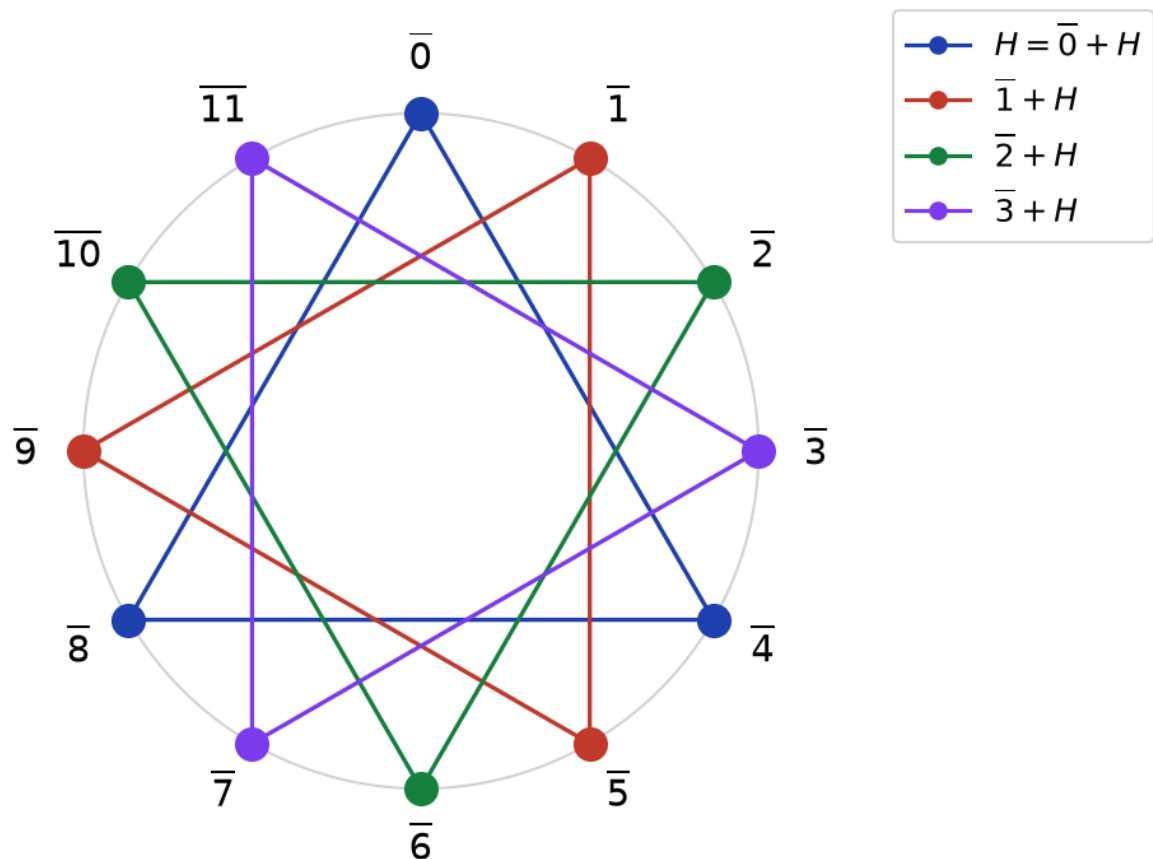
Démonstration :

D'abord, $x^{-1}x = e \in H$, donc $\sim$ est réflexive. Ensuite, si $x^{-1}y \in H$, son inverse $y^{-1}x$ est dans H : la relation est symétrique. De plus, si $x^{-1}y$ et $y^{-1}z$ sont dans H , leur produit $x^{-1}z$ aussi : elle est transitive. Par ailleurs, $y \sim x \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$. Enfin, $h \rightarrow xh$ est surjective sur xH par définition, et injective par simplification.

Exemple :

Dans $G = \mathbb{Z}/12\mathbb{Z}$, prenons $H = \langle \bar{4} \rangle = \{\overline{0\ 4}, \overline{0\ 8}\}$. En notation additive, les classes sont $\bar{0} + H$, $\bar{1} + H = \{\overline{1\ 5}, \overline{0\ 9}\}$, $\bar{2} + H$ et $\bar{3} + H$. On obtient ainsi 4 classes de 3 éléments, et $4 \times 3 = 12$.

La figure ci-dessous place les douze éléments sur un cercle. Chaque classe forme un triangle d'une couleur : les quatre triangles ne se chevauchent pas et recouvrent tout le groupe.



Théorème :

Théorème de Lagrange. Soit G un groupe fini et H un sous-groupe de G . Alors l'ordre de H divise l'ordre de G . Plus précisément, $|G| = |H| \times |G/H|$. L'entier $[G : H] = |G/H|$ s'appelle l'**indice** de H dans G .

Démonstration :

Les classes à gauche forment une partition de G . Notons $x_1H, \dots, x_kH$ ces classes, deux à deux distinctes, avec $k = |G/H|$. Chacune est en bijection avec H , donc possède $|H|$ éléments. Par conséquent, $|G| = \sum_{i=1}^k |x_iH| = k |H|$.

Corollaire :

Soit G un groupe fini d'ordre n .

- L'ordre de tout élément x divise n , et donc $x^n = e$.
- Si n est premier, G est cyclique, et tout élément différent de e l'engendre.

Démonstration :

L'ordre de x est le cardinal de $\langle x \rangle$, qui divise n par Lagrange. En écrivant $n = dm$, avec d l'ordre de x , on obtient $x^n = (x^d)^m = e$. Ensuite, si n est premier et $x \neq e$, l'ordre de x divise n et vaut au moins 2, donc il vaut n . Ainsi $\langle x \rangle = G$.

Méthode :

Pour utiliser le théorème de Lagrange :

- listez les diviseurs de $|G|$: ce sont les seuls ordres possibles pour un élément ou un sous-groupe ;
- pour calculer x^N , réduisez l'exposant N modulo l'ordre de x , ou modulo $|G|$;
- pour montrer qu'un sous-groupe est tout G , montrez que son ordre ne peut être qu'un diviseur de $|G|$ supérieur à $|G|/2$.

Exemple :

Pour p premier, $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe d'ordre $p - 1$. Donc $a^{p-1} = 1$ pour a non divisible par p : c'est le petit théorème de Fermat. Par exemple, $3^{100} = (3^{10})^{10}$ et $3^{10} \equiv 1 \pmod{11}$, donc $3^{100} \equiv 1 \pmod{11}$.

Remarque :

La réciproque du théorème de Lagrange est fausse : un diviseur de $|G|$ n'est pas toujours l'ordre d'un sous-groupe. Par exemple, le groupe alterné A_4 , d'ordre 12, n'a aucun sous-groupe d'ordre 6 (résultat admis ici). De plus, dans un groupe non abélien, la classe à gauche xH peut différer de la classe à droite Hx .

VI. Le groupe symétrique

1. Permutations et cycles

Définition :

Le **groupe symétrique** S_n est le groupe des bijections de $\{1, \dots, n\}$ dans lui-même, muni de la composition. Ses éléments s'appellent des **permutations**, et $|S_n| = n!$. On note $\sigma\tau = \sigma \circ \tau$: on applique d'abord τ , puis σ .

Définition :

Soient $a_1, \dots, a_k$ des éléments distincts, avec $k \geq 2$. Le **cycle** $\begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}$ est la permutation qui envoie a_1 sur a_2 , a_2 sur a_3 , ..., a_k sur a_1 , et fixe les autres éléments. L'entier k est sa

longueur et $\{a_1, \dots, a_k\}$ son **support**. Un cycle de longueur 2 est une **transposition**.

Propriété :

Un cycle de longueur k est d'ordre k . Deux cycles de supports disjoints commutent. Enfin, $\mathcal{S}_n$

n'est pas abélien pour $n \geq 3$, car $(1\ 2)(1\ 3) = (1\ 3\ 2)$ alors que $(1\ 3)(1\ 2) = (1\ 2\ 3)$.

Théorème :

Toute permutation $\sigma \neq \text{Id}$ s'écrit comme un produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près. L'ordre de σ est alors le ppcm des longueurs de ces cycles.

Démonstration :

Posons $i \equiv j$ s'il existe $m \in \mathbb{Z}$ tel que $j = \sigma^m(i)$: c'est une relation d'équivalence, dont les classes sont les **orbites** de σ . Soit i et p le plus petit entier $p \geq 1$ tel que $\sigma^p(i) = i$.

L'orbite de i est alors $\{i, \sigma(i), \dots, \sigma^{p-1}(i)\}$, et σ y agit comme le cycle $(i\ \sigma(i)\ \dots\ \sigma^{p-1}(i))$. Le

produit des cycles associés aux orbites de plus d'un élément coïncide donc avec σ en tout point.

L'unicité vient de ce que chaque cycle est imposé par son orbite. Enfin, des cycles disjoints commutent : si $\sigma = c_1 \dots c_r$, alors $\sigma^m = c_1^m \dots c_r^m$, et ce produit vaut Id si et seulement si chaque $c_j^m = \text{Id}$.

Méthode :

Pour décomposer une permutation en cycles disjoints :

- partez du plus petit élément non encore traité et suivez les flèches $i \rightarrow \sigma(i)$ jusqu'à revenir au départ ;
- recommencez avec le plus petit élément restant ;
- oubliez les points fixes ;
- l'ordre est le ppcm des longueurs, et la signature vaut $(-1)^{\sum (k_j - 1)}$.

Exemple :

Soit $\sigma \in \mathcal{S}_8$ donnée par

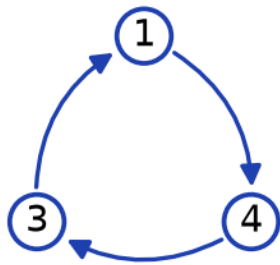
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 8 & 2 & 5 & 7 & 3 \end{pmatrix}.$$

On suit $1 \rightarrow 4 \rightarrow 3 \rightarrow 1$, puis $2 \rightarrow 6 \rightarrow 2$, puis $5 \rightarrow 8 \rightarrow 7 \rightarrow 5$. Donc

$$\sigma = (1, 4, 3)(2, 6)(5, 8, 7),$$

et son ordre vaut $\text{ppcm}(3, 2, 3) = 6$.

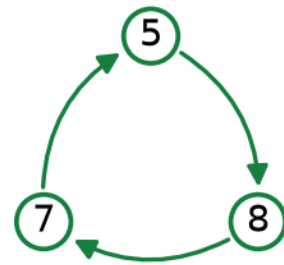
La figure ci-dessous dessine les trois orbites de cette permutation. Chaque flèche relie i à $\sigma(i)$: on lit directement les cycles.



(1 4 3) longueur 3



(2 6) longueur 2



(5 8 7) longueur 3

2. Transpositions et signature

Corollaire :

Toute permutation est un produit de transpositions. Plus précisément,

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} a_2 \\ a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} \\ a_k \end{pmatrix}.$$

Définition :

Une **inversion** de σ est un couple (i, j) avec $i < j$ et $\sigma(i) > \sigma(j)$. Si $I(\sigma)$ est leur nombre, la **signature** de σ est $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Théorème :

La signature $\varepsilon : \mathcal{S}_n \rightarrow \{-1, 1\}$ est un morphisme de groupes. Toute transposition a pour signature

-1 , et un cycle de longueur k a pour signature $(-1)^{k-1}$. Le noyau de ε est le **groupe alterné** $\mathcal{A}_n$.

Démonstration :

D'abord, on a la formule

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

En effet, le numérateur et le dénominateur contiennent les mêmes facteurs en valeur absolue, et chaque inversion apporte un signe moins. Ensuite, chaque quotient est symétrique en i et j . Donc, pour $\sigma, \tau \in \mathcal{S}_n$:

$$\varepsilon(\sigma\tau) = \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{i < j} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma) \varepsilon(\tau),$$

car les paires $\{\tau(i), \tau(j)\}$ décrivent une fois chaque paire. De plus, $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ n'a qu'une inversion, donc $\varepsilon\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = -1$. Toute transposition $\begin{pmatrix} a \\ b \end{pmatrix}$ s'écrit $\gamma \begin{pmatrix} 1 \\ 2 \end{pmatrix} \gamma^{-1}$ pour une permutation γ envoyant 1 sur a et 2 sur b . Par conséquent, $\varepsilon\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = -1$. Enfin, un k -cycle est un produit de $k - 1$ transpositions.

Exemple :

$\sigma = (1, 4, 3)(2, 6)(5, 8, 7)$
 Pour σ , on obtient $\varepsilon(\sigma) = (+1)(-1)(+1) = -1$. La permutation σ est donc impaire, et $\sigma \notin \mathcal{A}_8$.

VII. Anneaux, corps et idéaux

Beaucoup d'ensembles portent deux lois liées entre elles, comme $\mathbb{Z}$ avec l'addition et la multiplication. Le vocabulaire des anneaux décrit cette situation. Il prolonge le chapitre d'arithmétique sur $\mathbb{Z}/n\mathbb{Z}$.

Définition :

Un **anneau** $(A, +, \times)$ est un ensemble muni de deux lois telles que $(A, +)$ est un groupe abélien, $\times$ est associative, possède un neutre 1_A , et est distributive sur $+$ des deux côtés. L'anneau est **commutatif** si $\times$ l'est. Les **inversibles** de A forment un groupe multiplicatif noté $A^\times$.

Définition :

Un **corps** est un anneau commutatif K tel que $1_K \neq 0_K$ et dont tout élément non nul est inversible. Autrement dit, $K^\times = K \setminus \{0\}$.

Exemple :

$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}[X]$ et $\mathbb{R}^{\mathbb{R}}$ sont des anneaux commutatifs. En revanche, $\mathcal{M}_n(\mathbb{R})$ est un anneau non commutatif pour $n \geq 2$. Enfin, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, tandis que

$$\mathbb{Z}^\times = \{-1, 1\}.$$

Théorème :

Dans $\mathbb{Z}/n\mathbb{Z}$, la classe $\bar{k}$ est inversible si et seulement si $\text{pgcd}(k, n) = 1$. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Démonstration :

Si $\bar{k} \bar{u} = \bar{1}$, alors $ku + nv = 1$ pour un entier v , donc $\text{pgcd}(k, n) = 1$. Réciproquement, le théorème de Bézout fournit u, v avec $ku + nv = 1$, et $\bar{u}$ est l'inverse de $\bar{k}$. Ainsi, tous les $\bar{k} \neq \bar{0}$ sont inversibles si et seulement si n est premier avec $1, \dots, n-1$, c'est-à-dire si n est premier.

Définition :

Soit A un anneau commutatif. Un **idéal** de A est un sous-groupe I de $(A, +)$ tel que $ax \in I$ pour tous $a \in A$ et $x \in I$. Pour $x \in A$, l'ensemble xA est l'idéal engendré par x . Un **morphisme d'anneaux** $f: A \rightarrow B$ vérifie $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1_A) = 1_B$.

Propriété :

- Le noyau d'un morphisme d'anneaux commutatifs est un idéal.
- Un idéal qui contient un inversible est l'anneau entier ; les seuls idéaux d'un corps sont $\{0\}$ et le corps.
- Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

Démonstration :

Le noyau est un sous-groupe additif, et si $f(x) = 0$, alors $f(ax) = f(a) \times 0 = 0$. Ensuite, si $u \in I$ est inversible, alors $1 = u^{-1}u \in I$, puis $a = a \times 1 \in I$ pour tout a . Dans un corps, tout idéal non nul contient un inversible. Enfin, un idéal de $\mathbb{Z}$ est un sous-groupe, donc de la forme $n\mathbb{Z}$; réciproquement, $n\mathbb{Z}$ est stable par multiplication par un entier.

Exemple :

L'évaluation $\text{ev}_1: \mathbb{R}[X] \rightarrow \mathbb{R}, P \mapsto P(1)$, est un morphisme d'anneaux. Son noyau est l'idéal des polynômes qui s'annulent en 1. Par la division euclidienne, c'est exactement $(X - 1)\mathbb{R}[X]$.

VIII. Ce qu'il faut retenir

- Un groupe est un ensemble muni d'une loi associative, avec un neutre et des symétriques ;
 $(xy)^{-1} = y^{-1}x^{-1}$.
- Pour prouver qu'un ensemble est un groupe, montrez que c'est un sous-groupe d'un groupe connu :
 $e \in H$ et $xy^{-1} \in H$.
- Le noyau et l'image d'un morphisme sont des sous-groupes, et f est injective si et seulement si
 $\ker f = \{e\}$.
- L'ordre de x est le plus petit $n \geq 1$ tel que $x^n = e$; alors $x^k = e \Leftrightarrow n \mid k$, et x^k est d'ordre $n/\text{pgcd}(n, k)$.
- Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$; tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$.
- Les classes xH partitionnent G en parts de même cardinal : c'est le théorème de Lagrange,
 $|H|$ divise $|G|$.

- Dans un groupe fini d'ordre n , $x^n = e$; un groupe d'ordre premier est cyclique.
- Toute permutation se décompose en cycles disjoints ; son ordre est le ppcm des longueurs.
- La signature est un morphisme de S_n dans $\{-1, 1\}$; un k -cycle a pour signature $(-1)^{k-1}$.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier ; les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$.

Questions fréquentes sur groupes

Comment montrer rapidement qu'un ensemble est un groupe ?

Le plus souvent, on ne vérifie pas les axiomes un par un. On montre que l'ensemble est un sous-groupe d'un groupe connu : il contient le neutre et, pour tous x, y de l'ensemble, xy^{-1} y appartient aussi. On peut aussi le reconnaître comme le noyau ou l'image d'un morphisme, ce qui donne le résultat sans calcul.

Le théorème de Lagrange a-t-il une réciproque ?

Non. Si d divise l'ordre d'un groupe fini, il n'existe pas forcément de sous-groupe d'ordre d : le groupe alterné A_4 , d'ordre 12, n'a pas de sous-groupe d'ordre 6. En revanche, dans un groupe cyclique d'ordre n , il existe exactement un sous-groupe d'ordre d pour chaque diviseur d de n .

Comment calculer l'ordre d'une permutation ?

On la décompose d'abord en produit de cycles à supports disjoints, en suivant les flèches $i \rightarrow \sigma(i)$.

L'ordre est alors le ppcm des longueurs des cycles. Par exemple, $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}$ est d'ordre $\text{ppcm}(4, 5) = 20$.

Quelle différence entre un groupe monogène et un groupe cyclique ?

Un groupe est monogène s'il est engendré par un seul élément. Il est cyclique s'il est de plus fini. Un groupe monogène infini est isomorphe à $\mathbb{Z}$, et un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Pour aller plus loin en L2

- Les énoncés : [exercices de maths en L2 sur groupes](#)
- À maîtriser avant : [Arithmétique et anneau \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre précédent : [Arithmétique et anneau \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre suivant : [Normes et topologie de \$\mathbb{R}^n\$](#)
- Le même thème en maths spé : [groupes, cours de maths spé](#)
- Tester vos connaissances : [QCM de maths en L2 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L2](#) et la [licence de maths de L1 à L3](#)