CHAPITRE

15

Groupes

Mon cher Ami,

J'ai fait en analyse plusieurs choses nouvelles. [...] cela m'a donné l'occasion [...] de décrire toutes les transformations possibles d'une équation même si elle n'est pas soluble par les radicaux. [...] Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance de ces théorèmes.

Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis. Je t'embrasse avec effusion.

– Évariste Galois. Le 29 Mai 1832

On est frappé de l'allure étrangement moderne de [la] pensée [d'Évariste Galois]. [...] Il est piquant que ses mémoires si concis soient pour nous plus clairs que les filandreux exposés que croyaient devoir en donner ses successeurs immédiats.

– Jean Dieudonné.

Programme

L'étude des structures algébriques permet d'approfondir plusieurs points abordés en première année : groupe symétrique, groupes issus de l'algèbre linéaire et de la géométrie des espaces euclidiens. Ce chapitre gagne à être illustré par de nombreux exemples.

— Groupes. Produit fini de groupes. Exemples issus de l'algèbre et de la géométrie.

— Sous-groupe. Caractérisation, intersection de sous-groupes, sous-groupe engendré par une partie, sous-groupes du groupe $(\mathbf{Z}, +)$.

— Morphisme de groupes. Exemples : signature, déterminant. Image et image réciproque d'un sous-groupe par un morphisme. Image et noyau d'un morphisme. Condition d'injectivité d'un morphisme. Exemple : groupe spécial orthogonal d'un espace euclidien. Isomorphisme de groupes. Réciproque d'un isomorphisme.

— Groupe $(\mathbf{Z}/n\mathbf{Z}, +)$, générateurs. Groupe monogène, groupe cyclique. Groupe des racines n-ièmes de l'unité. Tout groupe monogène infini est isomorphe à $(\mathbf{Z}, +)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbf{Z}/n\mathbf{Z}, +)$.

— Élément d'ordre fini d'un groupe, ordre d'un tel élément. Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x. Si x est d'ordre fini d et si e désigne l'élément neutre de G, alors, pour n dans $\mathbf{Z}$, on a $x^n = e \iff d|n$. L'ordre d'un élément d'un groupe fini divise le cardinal du groupe (démonstration exigible uniquement pour G commutatif).

1 Exemples, premières propriétés

Un groupe est, rappelons-le, un magma associatif unifère dont tous les éléments sont inversibles. Il est dit abélien ou commutatif si la loi est commutative. On note par la suite G un groupe. Sauf mention explicite du contraire, il est supposé multiplicatif.

Propriétés 15 - 1

L'élément neutre de G est unique.
Le symétrique d'un élément de G est unique.

Démonstration. Si e et e' sont deux éléments neutres, on a $e = ee' = e'$ par définition (e est neutre à gauche et e' est neutre à droite), d'où $e = e'$.

Si g est dans G et x et y sont inverses de g, on a $x = x(gy) = (xg)y = y$, d'où $x = y$. □

Proposition 15 - 1

Tout élément d'un groupe est régulier (on dit aussi simplifiable) :

$$\forall g \in G\,, \qquad \big(\forall (x,y) \in G^2\ (gx = gy \vee xg = yg) \Longrightarrow x = y\big)\ .$$

Démonstration. Il suffit de multiplier les égalités par l'inverse de g pour montrer l'implication. □

Définition 15 - 1

Pour $x \in G$ et $n \in \mathbf{N}$, on définit x^n par récurrence via $x^0 = 1_G$ et $x^{n+1} = x^n x$.

Proposition 15 - 2

Pour $x \in G$ et $n \in \mathbf{N}$, on a $(x^n)^{-1} = \left(x^{-1}\right)^n$. On note x^{-n} cette valeur commune, ce qui définit donc x^m pour m dans $\mathbf{Z}$.

Démonstration. C'est direct en utilisant l'associativité. □

Remarque 15 - 1

En notation additive on définit de même na pour n dans $\mathbf{Z}$ et a dans G.

Notations

En l'absence d'ambiguïté on note :

- xy au lieu de $x \cdot y$
- 1_G, ou tout simplement 1, le neutre en notation multiplicative.
- 0_G, ou tout simplement 0, le neutre en notation additive.
- En notation multiplicative, le symétrique de x est noté x^{-1} et on l'appelle aussi l'inverse de x.
- En notation additive, le symétrique de x est noté $-x$ et on parle alors d'opposé.

Exemples 15 - 1

Les groupes $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont des groupes additifs (donc abéliens). Les groupes $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{U}$ (l'ensemble des nombres complexes de module 1) et $\mathbf{C}^*$ sont des groupes multiplicatifs abéliens.

Voici quelques exemples de groupes pour le produit de composition : $SO_2(\mathbf{R})$, les rotations vectorielles du plan ; les rotations affines du plan ; S_E les permutations de l'ensemble E ; S_n les permutations sur $[\![1;n]\!]$. Seul le premier est commutatif, les autres ne le sont que si $n \leq 2$ ou $\text{Card}(E) \leq 2$.

Dans les groupes de matrices, on trouve le groupe abélien $\mathscr{M}_n(\mathbf{K})$ et le groupe non abélien (dès qu'on a $n \geq 2$) $GL_n(\mathbf{K})$.

En analyse on peut citer le groupe additif des suites réelles convergentes.

En géométrie les groupes des isométries préservant le carré ou le cercle ne sont pas abéliens.

2 Morphismes de groupes

Un (homo)morphisme de groupes est une application entre groupes préservant la structure.

Définition 15 - 2

Soit G et H deux groupes (notés multiplicativement), on appelle morphisme de groupes toute application $f : G \to H$ satisfaisant à

$$\forall (x,y) \in G^2, \quad f(xy) = f(x)f(y) .$$

On note $\text{Hom}(G,H)$ l'ensemble de ces morphismes.

On appelle endomorphisme du groupe G tout morphisme de G dans lui-même et on note $\text{End}(G)$ leur ensemble.

Exemple 15 - 2

Le déterminant de $\mathrm{GL}_n(\mathbf{K})$ dans $\mathbf{K}^*$ est un morphisme de groupes multiplicatifs.

La signature de S_n dans $\{\pm 1\}$ est un morphisme de groupes multiplicatifs.

Propriétés 15 - 2

— Si 1_G et 1_H sont les éléments éléments neutres respectifs de G et H, on a $f(1_G) = 1_H$.

— $\forall x \in G,\ f\left(x^{-1}\right) = f(x)^{-1}$.

— $\forall x \in G,\ \forall n \in \mathbf{Z},\ f\left(x^n\right) = f(x)^n$.

Démonstration. Soit x dans G, on a $f(x) = f(1_G x) = f(1_G)f(x)$ et donc, par régularité de $f(x)$, on a $f(1_G) = 1_H$. Il en résulte que si $xy = 1$, alors $f(x)f(y) = 1$ et donc f préserve les inverses. La dernière propriété résulte d'une récurrence immédiate. □

Définition 15 - 3

On appelle noyau d'un morphisme de groupes $f : G \to H$, et on le note $\mathrm{Ker}(f)$, l'ensemble $f^{-1}\left(\{1_H\}\right)$.

On appelle image de f, et on le note $\mathrm{Im}(f)$, l'ensemble $f(G)$.

Avec cette définition, on a

Proposition 15 - 3

Soit $f : G \to H$ un morphisme de groupes ; on a

$$\begin{aligned} f \text{ surjective} &\iff \mathrm{Im}(f) = H\,, \\ f \text{ injective} &\iff \mathrm{Ker}(f) = \{1_G\}\ . \end{aligned}$$

Démonstration. En ce qui concerne la surjectivité, il s'agit de la définition même. Quant à l'injectivité, puisque $f(1_G) = 1_H$, l'implication est directe. Par ailleurs on a, pour x et y dans G,

$$f(x) = f(y) \iff f(x)f(y)^{-1} = 1_H \iff f(xy^{-1}) = 1_H$$

et donc, si $\mathrm{Ker}(f) = \{1_G\}$, il vient $f(x) = f(y) \iff xy^{-1} = 1_G$, et cette dernière propriété équivaut à $x = y$. D'où le critère d'injectivité. □

Définition 15 - 4

On appelle isomorphisme de groupes de G sur H tout morphisme bijectif et on note $f : G \cong H$ un tel isomorphisme. Si de plus $G = H$, on parle d'automorphisme.

On note $\mathrm{Isom}(G, H)$ et $\mathrm{Aut}(G)$ les ensembles correspondants.

Théorème 15 - 1

Si φ est un isomorphisme de groupes de G sur H, alors φ^{-1} est un isomorphisme de groupes de H sur G.

Démonstration. En effet φ^{-1} est par définition bijectif et, pour x et y dans H, on a

$$\varphi\left(\varphi^{-1}(x)\varphi^{-1}(y)\right) = \varphi \circ \varphi^{-1}(x)\varphi \circ \varphi^{-1}(y) = xy$$

et donc $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$, ce qui montre que φ^{-1} est un morphisme de groupes. □

On dit aussi (plus rarement) monomorphisme pour morphisme injectif et épimorphisme pour morphisme surjectif.

Exemple 15 - 3

$\mathrm{Hom}(\mathbf{Z}) = \{x \mapsto ax \,|\, a \in \mathbf{Z}\} \cong \mathbf{Z}$ et $\mathrm{Aut}(\mathbf{Z}) \cong \{\pm 1\}$.

Théorème 15 - 2

Pour x dans G et p et q dans $\mathbf{Z}$, on a

$$x^{p+q} = x^p x^q \ .$$

Autrement dit $n \mapsto x^n$ appartient à $\mathrm{Hom}(\mathbf{Z}, G)$.

Démonstration. Par disjonction de cas :

a. Si on a $p \geq 0$ et $q \geq 0$ (et donc $p+q \geq 0$), cela résulte de la définition et d'une récurrence immédiate (par exemple sur q).

b. Si $p \geq 0$, $p+q \geq 0$ mais $q < 0$, alors $-q > 0$ et il vient $x^{p+q}x^{-q} = x^p$. En multipliant à droite membre à membre par x^q, inverse de x^{-q}, on obtient la relation voulue.

c. Si $p+q \geq 0$, $q \geq 0$ mais $p < 0$, on applique ce qui précède en échangeant les rôles de p et q et donc de la droite et de la gauche.

d. Si $p+q < 0$, on part de la relation $x^{-p-q} = x^{-q}x^{-p}$ et on passe aux inverses.

□

Théorème 15 - 3

Automorphismes intérieurs

Pour a dans G, l'application $f_a : x \mapsto axa^{-1}$ est un automorphisme de G.

Un tel automorphisme est dit intérieur et on note $\mathrm{Int}(G)$ leur ensemble et alors l'application

$$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Aut}(G) \\ & a & \mapsto & f_a \end{array}$$

est un morphisme de groupes dont l'image est $\mathrm{Int}(G)$ et le noyau est $\mathcal{Z}(G)$ égal à $\{a \in G \,|\, \forall x \in G\,,\ ax = xa\}$ et appelé centre de G.

Démonstration. Soit a, b, x et y dans G.

a. On a $f_a(xy) = a(xy)a^{-1} = axaa^{-1}ya^{-1} = f_a(x)f_a(y)$. Donc $f_a \in \mathrm{End}(G)$.

b. On a $f_a \circ f_b(x) = f_a\left(f_b(x)\right) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$ et donc $f_a \circ f_b = f_{ab}$, i.e. $\varphi(ab) = \varphi(a)\varphi(b)$. En particulier on a $f_a \circ f_{a^{-1}} = f_1 = \mathrm{Id}_G$ et donc $f_a \in \mathrm{Aut}(G)$, d'une part, et $\varphi \in \mathrm{Hom}(G, \mathrm{Aut}(G))$, d'autre part.

c. L'image de φ est $\mathrm{Int}(G)$ par définition et on a $a \in \mathrm{Ker}(\varphi)$ si et seulement si $f_a = 1_{\mathrm{Aut}(G)} = \mathrm{Id}_G$, ou encore $\forall x \in G$, $f_a(x) = axa^{-1} = x$, i.e. $\forall x \in G$, $ax = xa$.

□

Définition 15 - 5

Pour x et a dans G, axa^{-1} est appelé conjugué de x par a. L'ensemble des conjugués de x s'appelle la classe de conjugaison de x dans G.

La relation de conjugaison est une relation d'équivalence dans G.

Remarques 15 - 2

L'ensemble des classes de conjugaison forme une partition de G.

Si G est commutatif, le seul automorphisme intérieur est Id_G.

3 Produit direct de groupes

Théorème 15 - 4

Soit G et H deux groupes (notés multiplicativement), la loi de composition interne définie sur $G \times H$ par $(x, y)(x', y') = (xx', yy')$ confère à $G \times H$ une structure de groupe d'élément neutre $(1_G, 1_H)$, où 1_G et 1_H sont les éléments neutres respectifs de G et H.

De plus les projections sur G et H sont des morphismes de groupes.

Démonstration. C'est direct. □

Plus généralement

Définition 15 - 6

Soit $(G_i)_{i\in I}$ une famille finie de groupes. Le produit cartésien $\prod_{i\in I} G_i$ est muni d'une structure de groupe en multipliant coordonnées par coordonnées.

Pour aller plus loin

Soit G un groupe et A un ensemble non vide. L'ensemble G^A peut être muni d'une structure de groupe par la formule $(g_a)_{a\in A} \cdot (h_a)_{a\in A} = (g_a h_a)_{a\in A}$ et les projections sur G données par l'évaluation en un élément a de A, sont des morphismes de groupes.

Remarque 15 - 3

Dans $G \times H$, on a $G \cong G \times \{1_H\}$ et $H \cong \{1_G\} \times H$.

Il arrive que G et H soient tous deux sous-groupes d'un autre groupe. Dans ce cas le produit cartésien $G \times H$ n'a a priori aucun rapport avec le produit GH défini comme l'ensemble des produits gh pour g dans G et h dans H.

La formule $ghg'h'$ n'est pas exprimée sous la forme d'un élément de GH. Si néanmoins les éléments de G et de H commutent entre eux, alors GH est stable par multiplication [a].

Par ailleurs pour que l'écriture gh d'un élément de GH soit unique, il faut $G \cap H = \{1\}$. Dans ce cas les deux produits de groupes sont en fait identiques : si G et H sont deux sous-groupes d'un groupe abélien et si $G \cap H = \{1\}$, alors $G \times H \cong GH$ et l'isomorphisme est donné par $(g, h) \mapsto gh$.

a. Attention néanmoins, cette condition n'est pas nécessaire !

Aparté

Dans des cas plus compliqués, on construit des produits plus « tordus », appelés produits semi-directs. Par exemple la formule $ghg'h' = gg' \cdot (g'^{-1}hg')h'$ peut définir une loi interne si, par exemple, $g'^{-1}hg'$ appartient à H, autrement dit si H est stable par $\mathrm{Int}(G)$. On dit alors que G opère ou agit sur H.

Un exemple est donné par $H = \mathfrak{A}_n$ et G le groupe engendré par une transposition. Dans ce cas le groupe obtenu par produit semi-direct est tout simplement S_n.

4 Sous-groupes

Un sous-groupe de G est un sous-ensemble de G qui, muni de la même loi [a], est un groupe.

Remarque 15 - 4

C'est une notion essentielle : si on a à démontrer qu'un ensemble est un groupe, il est souvent plus intéressant de l'inclure dans un groupe connu et de vérifier qu'on a affaire à un sous-groupe : on est ainsi dispensé(e) de vérifications fastidieuses, notamment de l'associativité.

Notations

On note $H < G$ le fait que H soit un sous-groupe de G.

Attention ! Cette notation n'est pas universelle. Bien que courante, il faut donc en préciser le sens quand on l'utilise dans une copie.

Théorème 15 - 5

Caractérisation des sous-groupes

Soit H une partie d'un groupe multiplicatif G. Les propositions suivantes sont équivalentes :

1. H est un sous-groupe de G.
2. H est non vide et $\forall (x,y) \in H^2$, $(xy \in H$ et $x^{-1} \in H)$.
3. H est non vide et $\forall (x,y) \in H^2$, $xy^{-1} \in H$.
4. $1_G \in H$ et $\forall (x,y) \in H^2$, $xy^{-1} \in H$.

Dans ce cas l'élément neutre de H est 1_G et le symétrique d'un élément de H dans H est son symétrique dans G.

Démonstration. (1) $\Longrightarrow$ (2) résulte de la définition.

(2) $\Longrightarrow$ (3) s'obtient en remarquant que l'on peut appliquer la seconde propriété à y et donc la première à (x, y^{-1}).

(3) $\Longrightarrow$ (4) s'obtient en spécialisant la propriété générale au couple (x,x) (qui existe car H est non vide).

(4) $\Longrightarrow$ (1) résulte de l'application de la propriété à $(1_G, x)$ puis à (x, y^{-1}).

Comme H contient 1_G, par unicité de l'élément neutre il en résulte $1_H = 1_G$. Et l'unicité du symétrique entraîne alors que le symétrique dans H est aussi celui dans G. □

Exemples 15 - 4

$\{1_G\}$ et G lui-même sont des sous-groupes (triviaux) de G. Il en va de même pour $\mathcal{Z}(G)$.

$\{1_G\} \times H$ et $G \times \{1_H\}$ sont des sous-groupes de $G \times H$ et, plus généralement, pour G' et H' des sous-groupes respectivement de G et H, $G' \times H'$ est un sous-groupe de $G \times H$.

$\mathrm{Aut}(G)$ est un sous-groupe de S_G.

On vérifie directement qu'un morphisme préserve la notion de sous-groupe.

a. ou plus précisément de sa bi-restriction au sous-ensemble

Théorème 15 - 6

Soit G et H deux groupes, f dans $\mathrm{Hom}(G,H)$, G' un sous-groupe de G et H' un sous-groupe de H.

Alors $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-groupes respectivement de G et H et, plus généralement, il en est de même de $f^{-1}(H')$ et $f(G')$.

Démonstration. Si x et y appartiennent à G', alors $f(xy^{-1}) = f(x)f(y)^{-1}$ montre que $f(x)f(y)^{-1}$ appartient à $f(G')$ et, puisqu'on a aussi $1_H = f(1_G)$ et $1_G \in G'$, 1_H appartient à $f(G')$ et donc $f(G') < H$.

Si x et y appartiennent à G avec $f(x)$ et $f(y)$ dans H', alors $f(xy^{-1}) = f(x)f(y)^{-1}$ montre que xy^{-1} appartient à $f^{-1}(H')$ et, puisqu'on a aussi $1_H = f(1_G)$ et $1_H \in H'$, 1_G appartient à $f^{-1}(H')$ et donc $f^{-1}(H') < G$. □

Exemple 15 - 5

En posant $\mathrm{SL}_n(\mathbf{K}) = \{A \in \mathrm{GL}_n(\mathbf{K}) \,|\, \det A = 1\}$, $\mathrm{SL}_n(\mathbf{K})$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{K})$ en tant que noyau du morphisme déterminant.

Exemple 15 - 6

Si f est un endomorphisme de G, alors l'ensemble de ses points fixes est un sous-groupe de G puisque $f(1_G) = 1_G$ et si, pour x et y dans G, on a $f(x) = x$ et $f(y) = y$, alors $f(xy^{-1}) = f(x)f(y)^{-1} = xy^{-1}$ et donc xy^{-1} est point fixe de f, i.e. $G^f < G$.

Exemple 15 - 7

En posant $\mathscr{O}_n(\mathbf{R}) = \{M \in \mathscr{M}_n(\mathbf{R}) \,|\, {}^tMM = I_n\}$, $\mathscr{O}_n(\mathbf{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$, appelé groupe orthogonal. En effet, puisque det est multiplicatif et invariant par transposition, pour M dans $\mathscr{O}_n(\mathbf{R})$, on a $\det(M)^2 = 1$ et en particulier $\det(M) \neq 0$, donc $\mathscr{O}_n(\mathbf{R}) \subset \mathrm{GL}_n(\mathbf{R})$. Or $M \in \mathscr{O}_n(\mathbf{R})$ si et seulement si $M = {}^tM^{-1}$ et $M \mapsto {}^tM^{-1}$ est un morphisme et donc $\mathscr{O}_n(\mathbf{R})$ en est l'ensemble des points fixes et est donc un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$.

Il résulte de la caractérisation des sous-groupes que cette notion est stable par intersection.

Théorème 15 - 7

Toute intersection de sous-groupes de G est un sous-groupe de G.

Démonstration. Comme 1_G appartient à tous les sous-groupes, il appartient à leur intersection. Pour x et y dans G appartenant à tous les sous-groupes, il en va de même pour xy^{-1}, puisqu'on a affaire à des sous-groupes, et donc xy^{-1} appartient à leur intersection. □

Exemple 15 - 8

En posant $\mathrm{SO}_n(\mathbf{R}) = \{A \in \mathscr{O}_n(\mathbf{R}) \,|\, \det A = 1\}$, $\mathrm{SO}_n(\mathbf{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$ en tant qu'intersection de $\mathscr{O}_n(\mathbf{R})$ et $\mathrm{SL}_n(\mathbf{R})$.

5 Sous-groupe engendré par une partie

Définition 15 - 7

Soit A une partie de G. On note $\langle A\rangle$ l'ensemble défini par

$$\langle A\rangle = \bigcap_{\substack{H<G\\ H\supset A}} H\ ,$$

i.e. $\langle A\rangle$ est l'intersection de tous les sous-groupes de G contenant A (l'ensemble de ces sous-groupes est non-vide puisqu'il y a au moins G lui-même). On dit que c'est le sous-groupe engendré par la partie A.

Théorème 15 - 8

Soit A une partie de G. Alors $\langle A\rangle$ est un sous-groupe de G contenant A et c'est le plus petit sous-groupe de G contenant A (au sens de l'inclusion). De plus on a

$$\langle A\rangle = \left\{ g\in G \;\middle|\; \exists n\in\mathbf{N}^*, \exists (a_1,\cdots,a_n)\in \left(A\cup A^{-1}\right)^n\ , g=\prod_{i=1}^{n} a_i \right\}$$

ou encore

$$\langle A\rangle = \left\{ g\in G \;\middle|\; \exists n\in\mathbf{N}^*, \exists (a_1,\cdots,a_n)\in A^n\ , \exists (k_1,\cdots,k_n)\in\mathbf{Z}^n\ , g=\prod_{i=1}^{n} a_i^{k_i} \right\}\ .$$

Démonstration. Le sous-ensemble $\langle A\rangle$ est un sous-groupe en tant qu'intersection de tels objets. Il contient A puisque A est contenu dans chacun des ensembles dont on prend l'intersection. C'est donc un sous-groupe contenant A et, par définition même, il est inclus dans tout tel sous-groupe. C'est donc le plus petit tel sous-groupe au sens de l'inclusion.

On vérifie directement que les ensembles proposés contiennent A, sont stables par passage à l'inverse et par multiplication. Ce sont donc des sous-groupes de G contenant A. Il en résulte qu'ils contiennent $\langle A\rangle$. Mais, réciproquement, tout groupe contenant A contient aussi les inverses d'éléments de A, par stabilité par passage à l'inverse, et les produits d'éléments de A et de A^{-1}, par stabilité par produit. On a donc l'inclusion réciproque. □

D'après le théorème 15 - 2, pour a dans G, l'application φ_a qui à n associe a^n est un morphisme de groupes, i.e. $\varphi_a\in \mathrm{Hom}(\mathbf{Z},G)$. La seconde caractérisation des sous-groupes et le théorème précédent fournissent immédiatement :

Théorème 15 - 9

Pour a dans G, on a $\langle\{a\}\rangle = \mathrm{Im}(\varphi_a) = \{a^n \,|\, n\in\mathbf{Z}\}$.

6 Groupes monogènes, ordre

Définition 15 - 8

On dit que G est monogène s'il est engendré par un seul élément, i.e. s'il existe a dans G (a priori non unique) tel que $G = \langle\{a\}\rangle$. Les éléments a qui réalisent cette propriété sont appelés générateurs de G.

Plus généralement si A est une partie de G telle que $G = \langle A\rangle$, on dit que G est engendré par A ou que A est une partie génératrice de G.

Exemple 15 - 9

Le groupe additif $\mathbf{Z}$ est monogène et admet 1 et -1 comme générateurs.

Définition 15 - 9

Soit n dans $\mathbf{N}^*$. On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes d'équivalences dans $\mathbf{Z}$ pour la relation donnée par : $x \equiv y \pmod n$ si et seulement si $n \mid (y-x)$. Cet ensemble est naturellement muni d'une structure de groupe induite par l'addition dans $\mathbf{Z}$, i.e. $cl(x)+cl(y) = cl(x+y)$, le résultat ne dépendant pas du choix de x et de y dans une classe d'équivalence. On parle de classe d'équivalence modulo n.

On notera indifféremment $cl_n(a)$, $cl(a)$, $\overline{a}$ ou $a+n\mathbf{Z}$ la classe d'équivalence de a modulo n, i.e. l'ensemble $\{a+kn \mid k \in \mathbf{Z}\}$.

Démonstration. Si $x \equiv x' \pmod n$ et $y \equiv y' \pmod n$, alors n divise $x-x'$ ainsi que $y-y'$, donc aussi $(x+y)-(x'+y')$ et donc $x+y \equiv x'+y' \pmod n$, ce qui montre que l'addition est une loi interne dans $\mathbf{Z}/n\mathbf{Z}$, d'élément neutre $cl(0)$ et de symétrique donné par $cl(x) \mapsto cl(-x)$. L'associativité résulte de l'associativité dans $\mathbf{Z}$. □

Proposition 15 - 4

Le groupe $\mathbf{Z}/n\mathbf{Z}$ est monogène et si k est dans $\mathbf{Z}$, alors $cl(k)$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$ s et seulement si $k \wedge n = 1$.

Démonstration. Puisque 1 engendre $\mathbf{Z}$, $cl(1)$ engendre $\mathbf{Z}/n\mathbf{Z}$ et donc ce dernier est monogène.

Si $cl(k)$ engendre $\mathbf{Z}/n\mathbf{Z}$, en particulier on dispose a dans $\mathbf{Z}$ tel que $a \cdot cl(k) = cl(1)$, i.e. $cl(ak) = cl(1)$ ou encore $n \mid (ak-1)$. On dispose alors de b dans $\mathbf{Z}$ tel que $ak+bn = 1$ et donc, puisqu'on a affaire à une relation de Bézout, $k \wedge n = 1$.

Réciproquement une relation de Bézout entre k et n permet montrer que $cl(1)$ appartient au sous-groupe engendré par $cl(k)$ et donc que le sous-groupe engendré par $cl(1)$ est inclus dans celui engendré par $cl(k)$. Comme le premier est le groupe tout entier, il en va de même pour le second, i.e. $cl(k)$ engendre $\mathbf{Z}/n\mathbf{Z}$. □

Exemple 15 - 10

Le groupe $\mathbf{U}_n$ des racines n^{e} de l'unité est monogène de générateur $e^{2i\pi/n}$ (et plus généralement $e^{2ik\pi/n}$ avec k premier avec n).

Le groupe additif $\mathbf{Q}$ ne contient aucune partie génératrice finie. En effet, par réduction au même dénominateur, le groupe engendré par une partie finie A de $\mathbf{Q}$ ne contient que des rationnels dont le dénominateur est borné par une constante ne dépendant que de A.

Théorème 15 - 10

Les sous-groupes de $\mathbf{Z}$ sont monogènes. Ils sont tous de la forme $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

Démonstration. Soit H un sous-groupe de $\mathbf{Z}$.

a. Si $H = \{0\}$, alors il est bien monogène et $H = 0\mathbf{Z}$.

b. Sinon on peut définir $n = \min\{|p| \,|\, p \in H\,,\ p \neq 0\}$.

a. Comme H est stable par passage à l'opposé, en tant que sous-groupe de $\mathbf{Z}$, $n \in H$. Mézalor H est un sous-groupe de $\mathbf{Z}$ contenant n, et il contient donc $\langle n\rangle$, i.e. $\{kn \,|\, k \in \mathbf{Z}\}$, ce que l'on note $n\mathbf{Z}$. Ainsi $n\mathbf{Z} \subset H$.

b. Réciproquement, pour $a \in H$ on effectue la division enclidienne de a par n, i.e. on écrit $a = nq + r$ avec $0 \leq r < n$. Comme $n\mathbf{Z} \subset H$, $qn \in H$ et donc $r = p - nq \in H$. Comme $|r| < n$, on a donc $r = 0$ par définition de n et ainsi $a \in n\mathbf{Z}$ ou encore $H \subset n\mathbf{Z}$.

En résumé $H = n\mathbf{Z} = \langle n\rangle$ et donc H est bien monogène.

□

Soit a dans G, on a vu que l'application φ_a qui à n associe a^n est un morphisme de groupes. Son noyau est donc un sous-groupe de $\mathbf{Z}$.

Définition 15 - 10

Si $\mathrm{Ker}(\varphi_a)$ est réduit à $\{0\}$, on dit que a est d'ordre infini (dans G) et on note $\mathrm{ord}_G(a) = +\infty$. Sinon $\mathrm{Ker}(\varphi_a)$ est de la forme $n\mathbf{Z}$ pour un unique entier naturel non nul n. On dit que a est d'ordre n dans G et on note $\mathrm{ord}_G(a) = n$.

Exemple 15 - 11

Dans $\mathbf{C}^*$, i est d'ordre 4. Une symétrie est une involution, donc est d'ordre 2. Il revient au même de dire qu'une involution est son propre inverse.

Proposition 15 - 5

Soit x un élément d'ordre fini, n, dans G. On a

1. $\forall p \in \mathbf{Z}$, $(x^p = 1 \iff n|p)$,
2. $\forall (r,s) \in \mathbf{Z}^2$, $(x^r = x^s \iff n|(r-s) \iff r \equiv s \pmod n)$,
3. $n = \min\left\{k \in \mathbf{N}^* \;\middle|\; x^k = 1\right\}$,
4. $\mathrm{Im}(\varphi_x) = \left\{x^k \;\middle|\; k \in \mathbf{Z}\right\} = \left\{1, x, \cdots, x^{n-1}\right\}$ et $\mathrm{Card}\,(\mathrm{Im}(\varphi_x)) = n$.
5. $\mathrm{ord}_G(x) = \mathrm{ord}_G(x^{-1})$

Démonstration. La première assertion est une reformulation de $\mathrm{Ker}(\varphi_x) = n\mathbf{Z}$ et la seconde du lien entre le noyau et le défaut d'injectivité de φ_x. Les deux suivantes en découlent immédiatement.

Quant à la dernière, on a, pour p entier, $\varphi_x(p) = x^p = \varphi_{x^{-1}}(-p)$, de sorte que $p \in \mathrm{Ker}(\varphi_x) \iff -p \in \mathrm{Ker}(\varphi_{x^{-1}})$. Comme un noyau est stable par passage au symétrique, il vient $\mathrm{Ker}(\varphi_x) = \mathrm{Ker}(\varphi_{x^{-1}})$. □

Définition 15 - 11

Un groupe monogène fini est appelé cyclique.

Remarque 15 - 5

Si un groupe monogène G est infini et x est un de ses générateurs, on a $G = \mathrm{Im}(\varphi_x)$ et donc, d'après la proposition précédente, x est nécessairement d'ordre infini (sinon G serait fini). Par conséquent φ_x est injective et réalise donc un isomorphisme entre $\mathbf{Z}$ et G.

En d'autres termes il n'existe qu'un groupe monogène infini à isomorphisme près : $\mathbf{Z}$.

Théorème 15 - 11

Soit n un entier naturel non nul. A isomorphisme près il existe un unique groupe cyclique de cardinal n : $\mathbf{Z}/n\mathbf{Z}$.

Démonstration. On vérifie directement que φ_x permet de définir une application bijective de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathrm{Im}(\varphi_x)$: elle est bien définie parce que $\mathrm{Ker}(\varphi_x) \supset n\mathbf{Z}$, elle est injective parce que $\mathrm{Ker}(\varphi_x) \subset n\mathbf{Z}$ et elle est surjective par définition des groupes monogènes. □

Définition 15 - 12

Le cardinal d'un groupe s'appelle aussi son ordre. On le note indifféremment $\mathrm{Card}(G)$, $|G|$ ou encore parfois $\#G$.

Théorème 15 - 12

Lagrange

Soit G un groupe fini et H un sous-groupe de G, alors l'ordre de H divise celui de G. (Résultat hors-programme)

En particulier, l'ordre de tout élément de G divise le cardinal de G.

Joseph Louis, comte de Lagrange, 1736–1813.

Démonstration. Le point particulier résulte du résultat général appliqué à $\langle x\rangle$ dont le cardinal est l'ordre de x.

Soit H un sous-groupe de G. Pour x dans G, on note xH l'ensemble $\{xh \,|\, h \in H\}$. Puisque la multiplication par x est injective, on a $\mathrm{Card}(xH) = \mathrm{Card}(H)$. De plus, puisque H contient 1_G, $x \in xH$. Enfin, pour y dans G, on a $xH = yH$ si et seulement si $y \in xH$. En effet si $xH = yH$, en particulier $y \in yH$ et donc aussi $y \in xH$. Réciproquement on dispose de h_1 dans H tel que $y = xh_1$ et donc, pour h dans H, $yh = x(h_1h)$ avec $h_1h \in H$, donc $yH \subset xH$. Comme on a aussi $x = y(h_1)^{-1}$, on a $x \in yH$ et donc $xH \subset yH$.

Il en résulte que G admet une partition en des ensembles x_iH, pour i variant dans un ensemble I. On a donc $\mathrm{Card}(G) = \mathrm{Card}(I)\,\mathrm{Card}(H)$ et donc l'ordre de H divise celui de G. □

Remarque 15 - 6

La relation $xH = yH$ induit une relation d'équivalence. On note l'ensemble des classes d'équivalences G/H. On prendra garde que la relation $Hx = Hy$ induit aussi une relation d'équivalence mais elle est, en général, différente. L'ensemble des classes d'équivalence pour cette seconde relation se note $H\backslash G$. On a $\mathrm{Card}(G/H) = \mathrm{Card}(H\backslash G) = \dfrac{\mathrm{Card}(G)}{\mathrm{Card}(H)}$.

Lorsque G est commutatif, ces deux relations sont identiques et, de plus, G/H admet une structure de groupe induite par celle de G définie par la loi donnée par $(xH)(yH) = (xy)H$.

♠

Lorsque G n'est pas commutatif, G/H peut admettre une structure de groupe. Une fois encore cela n'est possible que si $G/H = H\backslash G$ ou encore si, pour tout x dans G, $xHx^{-1} = H$. On dit alors que H est un sous-groupe distingué, ou normal, de G. Par exemple, si $f \in \mathrm{Hom}(G, G')$ alors $\mathrm{Ker}(f)$ est dinstingué dans G et on a le théorème d'isomorphisme pour les groupes (l'équivalent du théorème du rang pour les espaces vectoriels) : $G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. En particulier si $G = \mathbf{Z}$, $G' = \mathbf{Z}/n\mathbf{Z}$ et $f(x) = cl(x)$, on a $\mathrm{Ker}(f) = n\mathbf{Z}$ et f surjective, d'où $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/n\mathbf{Z}$!

7 Le groupe symétrique

Pour n entier naturel non nul, le groupe S_n est par définition le groupe des permutations de l'ensemble $[\![1;n]\!]$, i.e. $S_n = S_{[\![1;n]\!]}$. Il résulte directement du principe des bergers qu'on a $\text{Card}(S_{n+1}) = (n+1)\,\text{Card}(S_n)$ et donc

Propriété 15 - 3

Pour n dans $\mathbf{N}^*$, $\text{Card}(S_n) = n!$.

Les éléments de S_n peuvent s'analyser « géométriquement » via leur action sur l'ensemble $[\![1;n]\!]$. On peut par exemple imaginer que les n entiers servent à numéroter des points dans l'espace. Ainsi S_3 peut être interprété comme agissant sur les sommets d'un triangle (pourquoi pas équilatéral), S_4 agit alors sur les sommets d'un tétraèdre et plus généralement S_n sur n points affinement indépendants dans un espace de dimension $n-1$.

On peut alors parler d'orbites, de stabilisateur, de fixateur etc. en se référant au sens géométrique de ces mots. Dans le cadre de notre étude, simplifiée, on se contentera des orbites :

Définition 15 - 13

Soit k un « point » de $[\![1;n]\!]$ et σ un élément de S_n, l'orbite de k sous l'action de σ est l'ensemble $\{\sigma^p(k) \,|\, p \in \mathbf{N}\}$.

L'ensemble des orbites sous σ forme une partition de $[\![1;n]\!]$ et une orbite réduite à un point correspond à un point fixe.

Soit p un entier supérieur à 2. On appelle **cycle** de longueur p, ou encore p-cycle, un élément de S_n qui n'a qu'une seule orbite non triviale (i.e. non réduite à un point), celle-ci étant de cardinal p. On écrit $\sigma = (a_1 a_2 \cdots a_p)$ si $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_p) = a_1$.

Un 2-cycle est appelé **transposition**.

On appelle support d'un cycle son unique orbite non triviale, i.e. si $\sigma = (a_1 a_2 \cdots a_p)$, le support de σ est $\{a_1, a_2, \ldots, a_p\}$.

Propriété 15 - 4

Soit σ un p-cycle. On a $\sigma^p = Id$ et $\sigma^{-1} = \sigma^{p-1}$.

Par ailleurs, pour $\rho \in S_n$, $\rho\sigma\rho^{-1}$ est également un p-cycle. Ce cycle est l'image par f_ρ, automorphisme intérieur donné par ρ, de σ. De plus, si $\sigma = (a_1 a_2 \cdots a_p)$, $f_\rho(\sigma) = (\rho(a_1)\rho(a_2)\cdots\rho(a_p))$.

Démonstration. Si k appartient à l'unique orbite non triviale, on a, pour q dans $\mathbf{Z}$, $\sigma^q(k) = k \Longrightarrow p|q$ et donc $\sigma^p(k) = k$. Sinon σ fixe k et a fortiori σ^p en fait de même. Il vient donc $\sigma^p = Id$. L'autre assertion en découle.

On vérifie directement qu'on a $f_\rho(\sigma) = (\rho(a_1)\rho(a_2)\cdots\rho(a_p))$ en étudiant les images une par une, ce qui prouve que c'est un p-cycle. □

Théorème 15 - 13

Le groupe S_n admet comme parties génératrices :

1. L'ensemble des cycles. Plus précisément toute permutation s'écrit comme produit de cycles à supports disjoints, cette décomposition étant unique à l'ordre des facteurs près.
2. L'ensemble des transpositions. Il suffit plus précisément d'au plus n transpositions pour décomposer n'importe quel élément de S_n en produit de transpositions.
3. L'ensemble des transpositions de la forme $(1i)$, pour $2 \leq i \leq n$.
4. L'ensemble des transpositions de la forme $(i\ i+1)$, pour $1 \leq i \leq n-1$.
5. La partie formée de (12) et $(12\cdots n)$.

Démonstration. La première décomposition est une simple description de l'action d'un élément σ sur $[\![1;n]\!]$ et résulte du fait que l'ensemble des orbites sous σ en forme une partition.

La seconde s'obtient par récurrence : à mutiplication à gauche près par $(n\sigma(n))$, on peut supposer que σ fixe n et l'interpréter alors comme permutation de S_{n-1}.

On se ramène alors à cet ensemble : on a $(ij) = f_{(1j)}((1i)) = (1j)(1i)(1j)$, pour i et j distincts et tous deux distincts de 1. Ceci montre que les $(1i)$ suffisent pour engendrer S_n.

Comme, pour $i \geq 3$, on a $(1i) = \prod_{k=1}^{i-2} f_{(k\ k+1)}\left((i-1\ i)\right)$, les $(i\ i+1)$ engendrent S_n.

Enfin, si $\sigma = (12\cdots n)$, on a $\sigma^k(1) = k$ et $\sigma(2) = \sigma^{k+1}(1) = k+1$, donc $f_{\sigma^k}((12)) = (k\ k+1)$, ce qui montre que (12) et σ engendrent S_n. □

Pour conclure cette brève étude de S_n, en liaison avec la théorie du déterminant, on étudie les morphismes de S_n à valeurs dans $\mathbf{C}^*$.

Théorème 15 - 14

Pour $n \geq 2$, on a $\mathrm{Hom}(S_n, \mathbf{C}^*) = \mathrm{Hom}(S_n, \{\pm 1\}) \cong \mathrm{Hom}(S_n, \mathbf{Z}/2\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z}$.

L'unique homomorphisme non trivial est appelé homomorphisme signature. On le note ε et il est caractérisé par les propriétés suivantes :

1. Si σ est un p-cycle, $\varepsilon(\sigma) = (-1)^{p-1}$ et en particulier si τ est une transposition, $\varepsilon(\tau) = -1$.
2. Si σ est produit de k transpositions, alors $\varepsilon(\sigma) = (-1)^k$.
3. Si la décomposition en cycles disjoints fait apparaitre k cycles (en comptant pour l'occasion un point fixe comme étant un 1-cycle), alors $\varepsilon(\sigma) = (-1)^{n-k}$.
4. Si I_σ est défini comme l'ensemble des paires (ij) qui sont inversées par σ, i.e.
$$I_\sigma = \left\{(i,j) \in [\![1;n]\!]^2 \;\middle|\; i<j \text{ et } \sigma(i) > \sigma(j)\right\},$$
alors $\varepsilon(\sigma) = (-1)^{\#I_\sigma}$.

Démonstration. Soit τ une transposition et f dans $\mathrm{Hom}(S_n, \mathbf{C})$. Comme τ est involutive, $f(\tau)$ aussi et donc $f(\tau) = \pm 1$.

Par ailleurs si τ' est une autre transposition, il existe σ dans S_n tel que $\tau' = \sigma\tau\sigma^{-1}$, puisqu'il suffit que σ envoie le support de τ' sur celui de τ, ce qui est toujours possible puisque $n \geq 2$. Il en résulte $f(\tau') = f(\tau)$ puisque $f(\sigma)^{-1} = f(\sigma^{-1})$ et $\mathbf{C}^*$ est commutatif.

Comme les transpositions engendrent S_n, il en résulte d'une part que f est à valeurs dans $\{\pm 1\}$ et d'autre part que l'application $f \mapsto f(\tau)$ est injective, et qu'il y a donc au plus deux tels homomorphismes.

Si f est non trivial, il est donc nécessairement défini par la propriété (2) du théorème.

Par ailleurs, en considérant l'application ε donnée par

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

on montre que ε est un homomorphisme à valeurs dans $\mathbf{C}^*$ et $\varepsilon((12)) = -1$. C'est donc l'unique homomorphisme non trivial de S_n dans $\mathbf{C}^*$.

Les autres propriétés sont immédiates. □

Définition 15 - 14

Une permutation de signature $+1$ est appelée paire, et impaire dans le cas contraire.

L'ensemble des permutations paires est appelé groupe alterné, et est noté $\mathfrak{A}_n$. C'est le noyau de l'homomorphisme signature.

8 Compléments

♠

L'ensemble de cette section est pour la culture générale seulement !

8 1 Dualité de Pontrjagyn et transformée de Fourier

La dualité introduite par Lev Semenovich Pontrjagyn (1908–1988) permet d'expliquer la transformée de Fourier en unifiant les phénomènes issus des groupes finis, du groupe $\mathbf{R}$ ou du cercle $\mathbf{S}^1$.

L'objet central dans cette théorie est le groupe dual d'un groupe G, noté $\widehat{G}$ et égal par définition à $\mathrm{Hom}(G, \mathbf{U})$. Il s'agit bien d'un dual comme on peut l'entendre pour un espace vectoriel et on peut montrer que, sous certaines conditions, le dual du dual est égal au groupe de départ. La raison qui impose de se retreindre aux morphismes à valeurs dans $\mathbf{U}$ (et non $\mathbf{C}^*$) est le besoin de relation d'orthogonalité, via un produit scalaire (hermitien). Cette restriction est automatique si G est fini (ou compact).

Prenons quelques exemples. Si $G = \mathbf{Z}$, un homomorphisme est déterminé par l'image de 1 et donc $\widehat{\mathbf{Z}} = \mathbf{U}$. Par dualité, on a $\widehat{\mathbf{U}} \cong \mathbf{Z}$, les homomorphismes étant tout simplement les fonctions puissance : $z \mapsto z^n$.

Si on s'intéresse à $\mathbf{Z}/n\mathbf{Z}$, l'image de 1 est une racine n^{e} de l'unité et il vient $\widehat{\mathbf{Z}/n\mathbf{Z}} \cong \mathbf{Z}/n\mathbf{Z}$.

On considère maintenant $\mathbf{R}$. On a un morphisme naturel donné par l'exponentielle complexe, dont le noyau est $2\pi\mathbf{Z}$, ce qui permet de faire de tout endomorphisme de $\mathbf{R}$ un élément du dual. Il n'y a en fait pas d'autres possibilités, de sorte que $\widehat{\mathbf{R}} \cong \mathbf{R}$, les morphismes étant donnés par $x \mapsto \exp(2i\pi\lambda x)$, pour λ réel.

La dualité de Pontrjagyn associe à toute fonction sur G (en fait à une fonction intégrable), une fonction sur $\widehat{G}$. La formule est

$$\widehat{f}(\chi) = \int_G f(g)\overline{\chi(g)}dg$$

et on a une formule d'inversion qui permet de « récupérer » f à partir de la connaissance de $\widehat{f}$, la formule de Plancherel :

$$f(g) = \int_{\widehat{G}} \widehat{f}(\chi)\chi(g)d\chi \ .$$

Dans le cas d'une fonction périodique, $G = \mathbf{R}/T\mathbf{Z}$ est isomorphe à $\mathbf{U}$ et donc son dual est isomorphe à $\mathbf{Z}$. Les coefficients de Fourier sont définis par

$$\widehat{f}(n) = c_n(f) = \int_0^T f(x)e^{2in\pi x/T}\frac{dx}{T}$$

et on récupère la fonction par

$$f(x) = \sum_{n\in\mathbf{Z}} c_n(f)e^{2in\pi x/T} \ ,$$

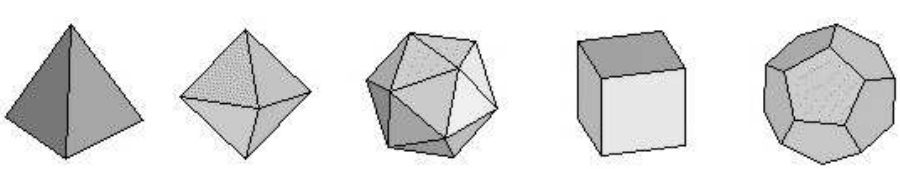
l'intégrale sur $\mathbf{Z}$ étant, comme on s'en doute, devenue une somme discrète.

La transformée de Fourier intervient en physique lors de l'étude des phénomènes ondulatoires (chaleur, mécanique quantique) et ses avatars discrets et finis interviennent dans l'étude des phénomènes périodiques (électricité) ou dans la compression de données (JPEG, JPEG2000).

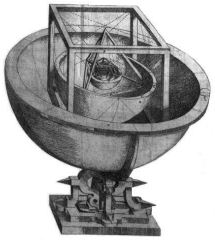
8 2 Isométries des polyèdres réguliers

Afin de mieux comprendre S_3, on peut le voir agir sur un triangle équilatéral. On peut alors s'apercevoir de liens forts entre la classifications des permutations et celle des isométries.

Le groupe des isométries directes préservant le triangle équilatéral est composé des rotations d'angle multiple de $2\pi/3$. Il est isomorphe à $\mathbf{Z}/3\mathbf{Z}$, ou encore à $\mathfrak{A}_3$. Quant aux isométries indirectes, ce sont les symétries par rapport aux médiatrices, et correspondent donc aux transpositions. Au final le groupe des isométries du triangle équilatéral est isomorphe à S_3. L'homomorphisme signature correpond alors au déterminant.

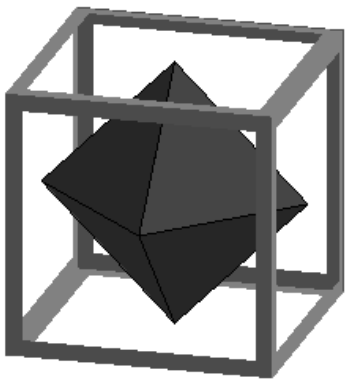


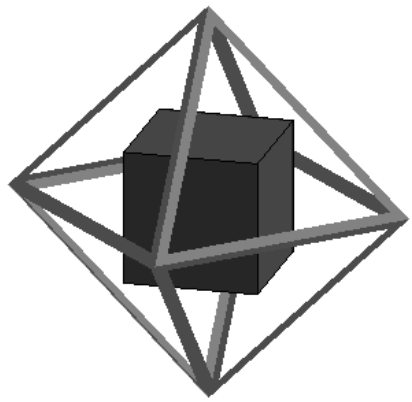
En dimension 3, on s'intéresse au groupe des isométries du tétraèdre régulier. Comme une telle isométrie préserve le centre de gravité, on peut la penser comme une isométrie vectorielle qui permute les quatre sommets, et donc ce groupe est un sous-groupe de S_4, et lui est en fait égal. Une fois encore les isométries directes correspondent à $\mathfrak{A}_4$. Il ne faut pourtant pas croire que c'est un phénomène général.



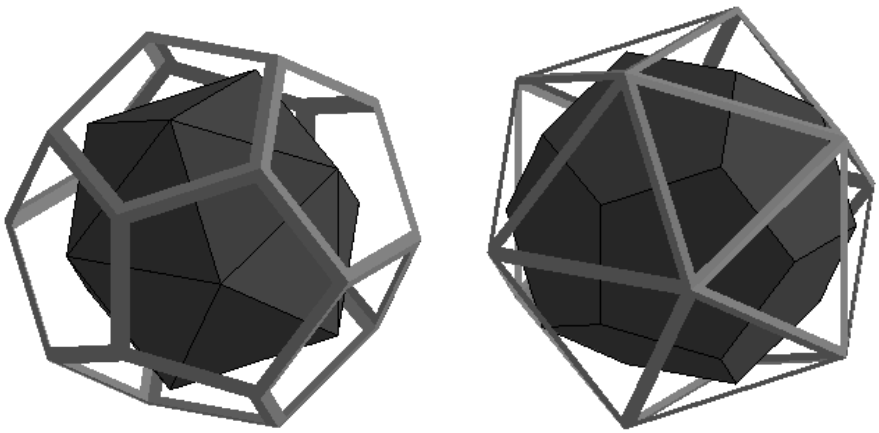
Le cube, tout comme l'octaèdre, a pour groupe d'isométries **directes** le groupe S_4. Le cube a huit sommets, mais comme son centre est fixe, elles sont appariées deux par deux. On peut donc faire agir S_4 sur le cube en le faisant agir sur ses diagonales. Comme un sommet et ses trois voisins correspondent à un repère orthonormé de l'espace, une isométrie (directe ou non) du cube tranforme ce repère en un autre. On a huit choix pour le centre du repère, trois pour la première direction, deux pour la seconde et un seul pour la dernière direction, ce qui fait 48 isométries. Il y en a 24 directes et 24 indirectes. En résumé le groupe des isométries **directes** du cube est S_4. Les autres sont le produit des isométries directes par la symétrie centrale de centre le centre du cube. De la sorte le groupe des isométries du cube est isomorphe au produit direct $S_4 \times \mathbf{Z}/2\mathbf{Z}$.

Le fait que ce produit soit direct est accidentel. Par exemple S_3 n'est pas isomorphe au produit direct $\mathfrak{A}_3 \times \mathbf{Z}/2\mathbf{Z}$, car ce dernier est isomorphe à $\mathbf{Z}/6\mathbf{Z}$ (c'est le théorème chinois) et S_3 ne contient évidemment aucun élément d'ordre 6.





Le fait que l'octaèdre et le cube aient même groupe d'isométries provient de ce qu'ils sont duaux au sens suivant : en prenant les centres des faces de l'un d'eux et en les reliant entre eux si (et seulement si) les deux faces en question ont une arête commune, on retrouve l'autre polyèdre. Cette dualité (on parle plutôt de figure polaire, au sens de la géométrie projective) est préservée par les isométries, et permet donc de voir que les groupes d'isométries sont en fait les mêmes.



Pour clore signalons que le groupe des isométries directes du dodécaèdre, ou de son dual, i.e. l'icosaèdre, est le groupe $\mathfrak{A}_5$. Or, une fois encore, la symétrie centrale préserve le polyèdre, et donc le groupe des isométries du dodécaèdre est le produit direct $\mathfrak{A}_5 \times \mathbf{Z}/2\mathbf{Z}$, et ce n'est donc pas le groupe S_5, bien qu'il ait 120 éléments.

Exercices

Généralités

15 - 1 Ⓢ ★ Transport de structure

Soit G un groupe multiplicatif et E un ensemble tel qu'il existe une bijection (ensembliste) φ de G sur E. Montrer que l'on définit une loi sur E via la formule

$$\forall (a,b) \in E^2\,, \quad a \star b = \varphi\left(\varphi^{-1}(a)\varphi^{-1}(b)\right)$$

et que $(E, \star)$ est un groupe.

On dit que $(E, \star)$ est le groupe obtenu par **transport de structure** à partir de G.

15 - 2 Ⓢ ★ Union

Soit H et K des sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

15 - 3 Ⓢ ★★ Partie stable ♥

Soit H une partie finie non vide d'un groupe $(G, .)$, stable pour le produit. Montrer que H est un sous-groupe de G.

Indication : on exploitera les translations $\tau_a : x \mapsto ax$.

15 - 4 Ⓢ ★★ Groupes abéliens ♥

Soit G un groupe multiplicatif. Montrer que G est abélien si et seulement si l'une des trois propriétés suivantes est vérifiée :

1. $x \mapsto x^{-1}$ est un endomorphisme de G,
2. $x \mapsto x^2$ est un endomorphisme de G.
3. $\forall (a,b) \in G^2,\ \exists k \in \mathbf{N},\ \forall i \in \{k-1, k, k+1\}$ $(ab)^i = a^i b^i$.

15 - 5 Ⓢ ★★ Caractérisation de l'inverse

Soit G un groupe fini muni d'un endomorphisme involutif f ayant 1_G comme unique point fixe.

a. Montrer que l'application $g \mapsto g^{-1}f(g)$ est une bijection de G dans lui-même.

b. En déduire que f est l'application inverse puis que G est abélien.

15 - 6 Ⓢ ★★ Produit de sous-groupes

Soit H et K des sous-groupes d'un groupe G. Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$, où la notation XY désigne l'ensemble de tous les produits xy avec $x \in X$ et $y \in Y$.

15 - 7 Ⓢ ★★ Morphismes injectifs †

Existe-t-il un morphisme injectif de $\left(\mathbf{Z}^2, +\right)$ dans $(\mathbf{Z}, +)$?

15 - 8 Ⓢ ★★ Formule des classes

Soit G un groupe et X un ensemble ainsi qu'un morphisme de groupes φ de G dans S_X. On notera $g \cdot x$ au lieu de $\varphi(g)(x)$ et on définit une relation $\mathcal{R}$ sur X par $x \mathcal{R} y \equiv \exists g \in G,\ y = g \cdot x$.

a. Montrer que $\mathcal{R}$ est une relation d'équivalence. Les classes seront nommées orbites. L'orbite de x est notée $\mathcal{O}_G(x)$.

b. Montrer que, à x fixé, l'ensemble G_x défini par $G_x = \{g \in G \,|\, g \cdot x = x\}$ est un sous-groupe de G. On dit que G_x est le stabilisateur de x dans G.

c. Montrer que, au sein d'une même orbite, les stabilisateurs sont images les uns des autres par des automorphismes intérieurs.

d. Montrer que, si G est fini, on a $\mathrm{Card}(G) = \mathrm{Card}(G_x)\,\mathrm{Card}(\mathcal{O}_G(x))$.

15 - 9 Ⓢ ★★★ Groupes d'ordre p^2

On reprend l'exercice 15 - 8 et on suppose G fini et $\mathrm{Card}(G) = p^n$ avec p premier et $n \in \mathbf{N}^*$.

a. On suppose X fini et $\mathrm{Card}(X) \wedge p = 1$. Montrer qu'il existe x dans X tel que $\mathcal{O}_G(x) = \{x\}$, i.e. x est un point fixe sous G.

b. En déduire que le centre G, i.e. le sous-groupe de G donné par $\mathcal{Z}(G) = \{g \in G \,|\, \forall h \in G\,, hg = gh\}$ est distinct de $\{1\}$.

c. En déduire tous les groupes d'ordre p^2.

15 - 10 Ⓢ ★★★ Groupes de Sylow

a. Combien y a-t-il de familles $(x_1, \ldots, x_n)$ d'éléments de $\mathbf{F}_p^n$ linéairement indépendants ?

b. En déduire le cardinal de $\mathrm{GL}_n(\mathbf{F}_p)$.

c. En déduire le nombre de droites dans $\mathbf{F}_p^n$.

d. Soit $k = \mathrm{Card}\left(\mathrm{GL}_3(\mathbf{F}_2)\right)$. Exhiber pour tout nombre premier p un sous-groupe de $\mathrm{GL}_3(\mathbf{F}_2)$ de cardinal $p^{v_p(k)}$.

Ordre d'un élément et applications

15 - 11 Ⓢ ★ Ordre d'une image

Soit $\varphi : G \to H$ un morphisme de groupes finis et a un élément de G. Que dire de $\mathrm{ord}_H\left(\varphi(a)\right)$?

15 - 12 Ⓢ ★ Exposant

Soit a et b deux éléments d'un groupe abélien fini G. On note e le ppcm des ordres de a et b.

a. Soit p un nombre premier. Montrer qu'il existe x dans $\langle a \rangle$ ou $\langle b \rangle$ d'ordre $p^{v_p(e)}$.

b. En déduire qu'il existe y dans G d'ordre e.

c. En déduire qu'il existe un entier $e(G)$ qui est le plus grand des ordres des éléments de G au sens de l'ordre naturel et de l'ordre donné par la divisibilité, i.e. tel qu'il existe g dans G d'ordre $e(G)$ et tel que l'ordre de tout élément de G divise $e(G)$. L'entier $e(G)$ est appelé exposant de G.

d. Quel sont les exposants de $\mathbf{Z}/12\mathbf{Z}$, de $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$?

15 - 13 Ⓢ ★ Racines de l'unité

On note $\mu_\infty(\mathbf{C})$ la réunion des $\mu_n(\mathbf{C})$ pour n dans $\mathbf{N}^*$, i.e. l'ensemble $\{z\in\mathbf{C}\,|\,\exists n\in\mathbf{N}^* z^n=1\}$. Montrer qu'il est infini mais que tous ses éléments sont d'ordre fini.

15 - 14 Ⓢ ★★ Commutativité de l'ordre

Montrer que pour tous x, y dans un groupe G fini, xy et yx ont même ordre.

15 - 15 Ⓢ ★★ Vierergruppe

Étude des groupes d'ordre 4.

a. Soit G un groupe fini d'ordre pair. Montrer que le nombre d'éléments de G d'ordre 2 est impair.

Indication : utiliser la relation d'équivalence définie par $y\mathcal{R}x \iff y\in\{x,x^{-1}\}$.

b. En déduire, à un isomorphisme près, tous les groupes d'ordre 4.

15 - 16 Ⓢ ★★ Théorème de Cauchy

Soit G un groupe d'ordre $2p$ avec p premier. Montrer qu'il contient un élément d'ordre p.

15 - 17 Ⓢ ★★★ Ordre d'un produit

Soit G un groupe commutatif fini, et a, b deux éléments de G d'ordres respectifs p et q.

a. Que dire de l'ordre de ab ?

b. Préciser le cas où p et q sont premiers entre eux.

c. Préciser le cas où $\langle a\rangle\cap\langle b\rangle=\{e_G\}$. Le résultat est-il encore vrai si $\langle a\rangle\cap\langle b\rangle\neq\{e_G\}$?

d. Que peut-on dire si G n'est pas commutatif ?

15 - 18 U 2019 ★★★ Ordre maximal dans S_n

Soit $n\geq 1$ un entier naturel. On définit $g(n)=\max_{\sigma\in S_n}\mathrm{ord}_{S_n}(\sigma)$. Déterminer les entiers naturels n tels que $g(n)$ est impair.

Indication : Si G est un groupe fini commutatif, que dire de l'ordre de ab ? Peut-on avoir $g(n)=3^2\times 5$? Est-ce que $g(n)=p^\alpha$ est possible ? Si $g(n)$ est impair, montrez que si p divise $g(n)$ alors p^2 ne divise par $g(n)$.

Groupes cycliques

15 - 19 Ⓢ ★ Sous-groupes

Déterminer les sous-groupes de $2\mathbf{Z}$.

15 - 20 Ⓢ ★ Sous-groupes cycliques

Soit H et K deux sous-groupes cycliques d'un groupe G quelconque. Montrer que $H\cap K$ est cyclique.

15 - 21 Ⓢ ★★ Endomorphismes

Démontrer $\mathrm{End}(\mathbf{Z}/n\mathbf{Z})\simeq\mathbf{Z}/n\mathbf{Z}$.

15 - 22 Ⓢ ★★ Théorème de Wilson

Soit p un entier naturel non nul. Montrer que p est premier si et seulement si $(p-1)!\equiv -1\pmod p$.

15 - 23 Ⓢ ★★★ Morphismes additifs

Déterminer le nombre de morphismes additifs de $\mathbf{Z}/n\mathbf{Z}$ sur $\mathbf{Z}/m\mathbf{Z}$. (On pourra commencer par étudier le cas $n=4$ et $m=3$.)

15 - 24 ★★★ Développement décimal

Soit x un réel et $a_0+\sum_{n=1}^{+\infty}a_n10^{-n}$ son développement décimal propre, i.e. $a_0=\lfloor x\rfloor$ et, pour $n\in\mathbf{N}^*$, $a_n=\lfloor 10^n x\rfloor-10\lfloor 10^{n-1}x\rfloor$.

a. Montrer que x est décimal si et seulement si la suite $(a_n)_{n\in\mathbf{N}^*}$ est nulle à partir d'un certain rang.

b. Montrer que x est rationnel si et seulement si la suite $(a_n)_{n\in\mathbf{N}^*}$ est périodique à partir d'un certain rang.

c. On écrit $x=p/q$ avec $(p,q)\in\mathbf{Z}\times\mathbf{N}^*$, $\mathrm{pgcd}(p,q)=1$ et $q=2^\alpha 5^\beta Q$, pour α et β entiers naturels et Q premier à 10. Montrer que la suite $(a_n)_{n\in\mathbf{N}^*}$ est périodique à partir du rang $\max(\alpha,\beta)+1$ et que sa période γ est l'ordre de $\overline{10}$ dans $(\mathbf{Z}/Q\mathbf{Z})^\times$.

d. En déduire que, si q est premier et si $\overline{10}$ engendre le groupe cyclique $(\mathbf{Z}/q\mathbf{Z})^\times$, alors les développements décimaux de p/q, pour p dans $\mathbf{N}^*$, ont des périodes de longueur $q-1$ et diffèrent uniquement par une permutation circulaire.

e. Montrer que c'est le cas pour $q=7$.

f. Quel est nombre premier suivant parmi ceux qui ont la propriété précédente ?

15 - 25 Ⓢ X ★★★ Pell-Fermat

Soit $G=\left\{x+y\sqrt{2}\;\middle|\;(x,y)\in\mathbf{N}\times\mathbf{Z},\ x^2-2y^2=1\right\}$.

a. Montrer que G est un groupe.

b. Montrer que G est monogène

Indication : on pourra chercher le plus petit élément de G qui soit supérieur à 1.

15 - 26 Ⓢ X 05 ★★★ Théorème de Wolstenholme

Soit p un nombre premier. On écrit $\sum_{k=1}^{p-1}\frac{1}{k}=\frac{u_p}{v_p}$ avec $\mathrm{pgcd}(u_p,v_p)=1$.

a. En utilisant le théorème de Wilson, montrer que, pour $p>2$, u_p est divisible par p.

b. Pour $p > 3$, démontrer qu'en fait u_p est divisible par p^2.

15 - 27 ★★★★ Théorème de Wolstenholme

On reprend l'exercice 15 - 26. On écrit $\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{x_p}{y_p}$ avec $\text{pgcd}(x_p, y_p) = 1$.

a. Pour $p > 3$, démontrer que x_p est divisible par p.

b. En déduire, toujours pour $p > 3$, $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$.

Groupe symétrique

15 - 28 Ⓢ Magistère 2017 ★★ Ordre maximal

Déterminer l'ordre maximal d'un élément de S_{10}.

15 - 29 Ⓢ ★★ Classes de conjugaisons

Soit G un groupe fini d'ordre n. Pour tout y dans G on pose $cl(y) = \left\{xyx^{-1} \;\middle|\; x \in G\right\}$. Montrer que pour tout y, le cardinal de $cl(y)$ divise n. À quelle condition nécessaire et suffisante ce cardinal ne dépend-il pas de y ? Étudier le cas particulier de S_3.

15 - 30 Ⓢ ★★★ Isométries du cube

Soit G le groupe des isométries du cube, i.e. le groupe des isométries de $\mathbf{R}^3$ qui laissent le cube globalement invariant (on ne demande pas de vérifier que c'est un groupe).

a. Déterminer un morphisme surjectif φ de G sur S_4.

b. Déterminer $\text{Ker}(\varphi)$.

c. Caractériser $\varphi^{-1}(\tau_{1,2} \circ \tau_{3,4})$.

Sous-groupes additifs de R

On reprendra au passage l'exercice 2 - 10.

15 - 31 Ⓢ ★★ Homomorphismes réels

Déterminer $\text{Hom}(\mathbf{Z}, \mathbf{R})$ et $\text{Hom}(\mathbf{R}, \mathbf{Z})$. Que dire de $\text{Hom}(\mathbf{Q}, \mathbf{Z})$?

15 - 32 Ⓢ ★★ Homomorphismes continus

Déterminer les morphismes continus de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$, et réciproquement.

15 - 33 Ⓢ M 2013 ★★★ Écriture décimale

Montrer qu'il existe une infinité de puissances relatives de 2 dont l'écriture décimale commence par 2013.

15 - 34 Ⓢ X ★★★ Triangles entiers

Soit E l'ensemble des réels x appartenant à $\left[0; \frac{\pi}{2}\right]$ tels qu'il existe un triangle dont les sommets sont des points du plan à coordonnées entières (i.e. des points dans $\mathbf{Z}^2$) dont l'un des angles admet x comme mesure.

a. Montrer que E est dense dans $\left[0; \frac{\pi}{2}\right]$.

b. Montrer que, si x et y appartiennent à E et si on a $x + y \leq \frac{\pi}{2}$, alors on a $x + y \in E$.

c. En déduire qu'il existe G sous-groupe de $\mathbf{R}$ tel que $G \cap \left[0; \frac{\pi}{2}\right] = E$.

Géométrie

15 - 35 Ⓢ ★★ Groupe du carré ♥

a. Démontrer que l'ensemble des isométries du plan qui laissent (globalement) invariant un carré (i.e. ses sommets) forme un groupe d'ordre 8. On le note D_4.

b. Montrer qu'il admet deux générateurs x et y tels que $x^4 = y^2 = e$ et $xy = yx^3$.

c. En déduire $D_4 = \left\{x^i y^j \;\middle|\; 0 \leq i \leq 3\,,\ 0 \leq j \leq 1\right\}$.

d. Déterminer tous les sous-groupes de D_4 et en donner une interprétation géométrique.

15 - 36 Ⓢ ★★ Groupe de l'hexagone

a. Démontrer que l'ensemble des isométries du plan qui laissent (globalement) invariant un hexagone (i.e. ses sommets) forme un groupe d'ordre 12. On le note D_6.

b. Montrer qu'il admet deux générateurs x et y tels que $x^6 = y^2 = e$ et $xy = yx^5$.

c. En déduire $D_6 = \left\{x^i y^j \;\middle|\; 0 \leq i \leq 5\,,\ 0 \leq j \leq 1\right\}$.

d. Déterminer tous les sous-groupes de D_6 et en donner une interprétation géométrique.

15 - 37 Ⓢ ★★★ Groupes d'ordre 8

Soit G un groupe d'ordre 8.

a. Montrer que si tous ses éléments sont d'ordre inférieur à 2, alors $G \simeq (\mathbf{Z}/2\mathbf{Z})^3$.

b. On suppose que G admet au moins un élément d'ordre strictement supérieur à 2. Montrer que si G est commutatif, alors $G \simeq \mathbf{Z}/8\mathbf{Z}$ ou $G \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

c. On suppose G non commutatif.

i. Montrer que si G n'a que deux éléments d'ordre 4, alors $G \simeq D_4$.

ii. Montrer que, sinon, G est engendré par trois éléments d'ordre 4 i, j et k tels que $i^2 = j^2 = k^2$, $ij = k$, $jk = i$ et $ki = j$, et en dresser la table de multiplication. On le note H_8.

d. Déterminer les sous-groupes de tous ces groupes d'ordre 8.

Compléments

Si $H < G$, on note

$$[G : H] = |G|/|H|$$

et ce nombre est appelé indice de H dans G.

Pour x et y dans G, on note $x\mathcal{R}_d y$ si $xH = yH$ (classes à droite) et $x\mathcal{R}_d y$ si $Hx = Hy$ (classes à gauche).

On dit de plus que H est distingué dans G (ou normal) si les classes à gauche et à droite sont égales, i.e. si, pour g dans G, $gH = Hg$ ou encore

$$f_g(H) = gHg^{-1} = H\ .$$

15 - 38 **L 2018** ★★★ **Groupe dual**

Soit G un groupe abélien fini de cardinal q noté multiplicativement. On note E l'ensemble des applications de G vers $\mathbf{C}$ et $\hat{G} = \mathrm{Hom}(G, \mathbf{C}^*)$. Enfin, pour $(f, g) \in E^2$, on pose $\langle f \,|\, g\rangle = \dfrac{1}{q}\displaystyle\sum_{x\in G} \overline{f(x)}g(x)$.

a. (♠) Montrer que l'application qui à f dans E associe $\sqrt{\langle f \,|\, f\rangle}$ est bien définie et est une norme sur le $\mathbf{C}$-espace vectoriel E.

b. Montrer que $\hat{G}$ est une famille orthonormée, i.e. $\langle f \,|\, g\rangle = \delta_{f,g}$.

c. Soit H un sous-groupe de G. Pour φ dans $\hat{G}$, on note $\widetilde{\varphi}$ la restriction de φ à H. Montrez que l'application définie sur $\hat{G}$ qui à φ associe $\widetilde{\varphi}$ est surjective.

15 - 39 Ⓢ ★★★ **Sous-groupes distingués**

a. Soit H un sous-groupe distingué de G. Montrer que l'ensemble des classes d'équivalences pour $\mathcal{R}_d$ forme un groupe. On le note G/H.

b. Montrer que l'application canonique de G dans G/H est un morphisme de groupe surjectif et de noyau H. En déduire que H est distingué dans G si et seulement s'il existe un groupe G' et un morphisme φ de G dans G' tels que $H = \mathrm{Ker}(\varphi)$.

c. Montrer que l'intersection de deux sous-groupes distingués l'est aussi.

d. Montrer que l'image réciproque d'un sous-groupe distingué par un morphisme de groupe l'est aussi.

e. On appelle groupe dérivé le sous-groupe $D(G)$ de G engendré par les commutateurs, i.e. par les éléments de la forme $xyx^{-1}y^{-1}$. Montrer que c'est un sous-groupe distingué et que, pour tout sous-groupe distingué H de G, G/H est commutatif si et seulement si $D(G) \subset H$.

f. Premier théorème d'isomorphisme. Soit f un morphisme de groupe de G dans G'. Montrer $G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.

g. Déterminer les sous-groupes distingués de tous les groupes d'ordre 8.

15 - 40 Ⓢ ★★★★ **Groupes résolubles**

Si $H < G$ et $K < G$, on note $[H, K]$ le sous-groupe de G engendré par les commutateurs $xyx^{-1}y^{-1}$ avec $x \in H$ et $y \in K$. On pose $D(G) = [G, G]$ et, pour n dans $\mathbf{N}$, $D^{n+1}(G) = D(D^n(G))$.

a. Montrer que les conditions suivantes sont équivalentes :

  a. Il existe un entier n tel que $D^{n+1}(G) = \{e\}$.

  b. On peut construire une suite finie et croissante de sous-groupes de G, $H_0 \subset H_1 \subset \cdots \subset H_r$, avec $H_0 = \{e\}$, $H_r = G$ et, pour $1 \leq k \leq r$, H_{k-1} est distingué dans H_k et H_k/H_{k-1} est commutatif.

  c. On peut construire une suite finie et croissante de sous-groupes distingués de G, $H_0 \subset H_1 \subset \cdots \subset H_r$, avec $H_0 = \{e\}$, $H_r = G$ et, pour $1 \leq k \leq r$, H_k/H_{k-1} est commutatif.

b. Un tel groupe est appelé résoluble. Montrer qu'un sous-groupe d'un groupe résoluble l'est aussi.

c. Soit H un sous-groupe distingué d'un groupe G. Montrer que si H et G/H sont résolubles alors G l'est aussi.

d. Montrer qu'un p-groupe (i.e. un groupe dont le cardinal est une puissance d'un nombre premier p) est résoluble.