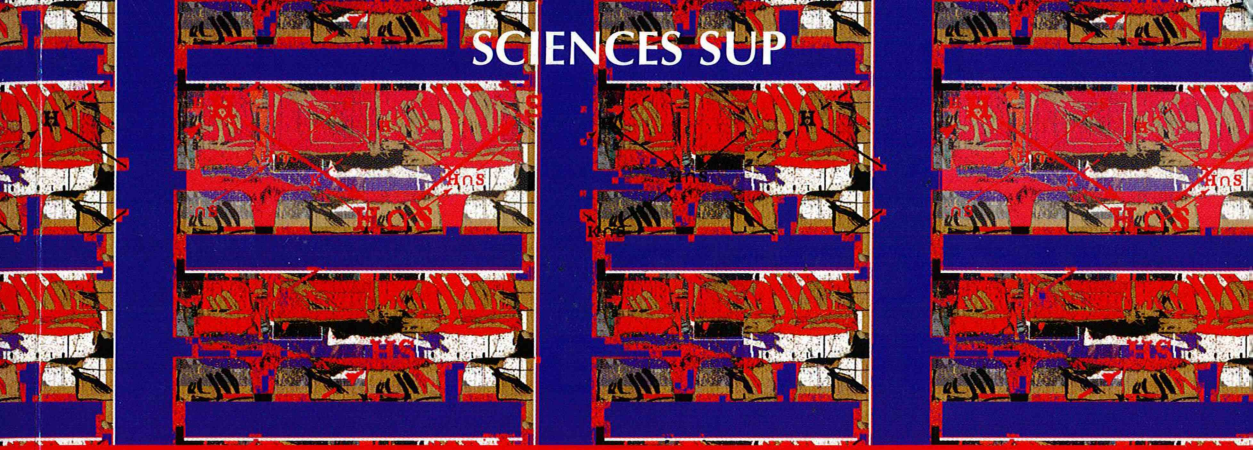


Rappels de cours, exercices et problèmes corrigés

Licence 3 • Master • CAPES • Agrégation

THÉORIE DES GROUPES

2e édition

Jean Delcourt

DUNOD

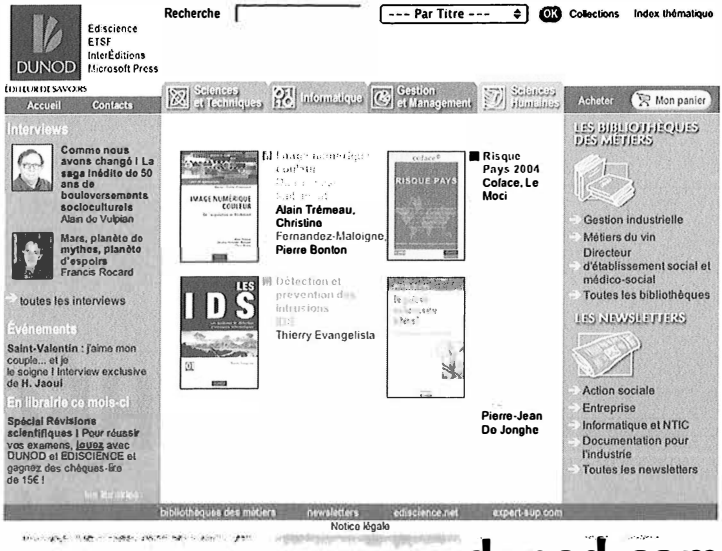
THÉORIE DES GROUPES

Jean Delcourt
Professeur agrégé à l'université
de Cergy-Pontoise

2e édition

DUNOD

Consultez nos catalogues sur le Web



www.dunod.com

Illustration de couverture : D'après *Lionel Auvergne*

© Dunod, Paris, 2001, 2007
ISBN 978-2-10-050667-5

À Michèle, Sophie et Marie

Préface

Ce livre est consacré aux groupes. Les ouvrages traitant de cette théorie sont nombreux, notamment en langue anglaise ; pour la langue française, on citera ceux de J. Calais ([6]), de N. Bouvier ([5]) entièrement consacrés aux groupes ; d'autres, comme le Cours d'algèbre de D. Perrin ([21]), et la « somme » de J.-M. Arnaudiès et J. Bertin ([3]) traitent une large part de la théorie, entre autres thèmes d'algèbre.

Notre livre vise à compléter ces textes, mais il prétend à une certaine originalité.

- C'est un livre de **cours par les exercices** qui tente de suivre une démarche d'auto-enseignement. Ainsi, l'étudiant devra lire cet ouvrage crayon en main, et sera amené à démontrer la plupart des théorèmes lui-même. Bien sûr, ces exercices sont corrigés de façon très détaillée.
- Nous y avons inclus un certain nombre de problèmes, également corrigés. Bien que d'une ampleur moindre qu'un problème de Capes ou d'Agrégation, ils visent à concrétiser, sur des exemples précis, les concepts de la théorie.
- Le plus souvent possible nous avons utilisé le langage de la géométrie qui donne un éclairage saisissant à des propriétés qui paraissent purement algébriques[1].
- Enfin l'ouvrage offre la palette la plus large possible d'exemples réels de groupes. Notre conviction est, en effet, qu'on ne comprend bien une théorie que lorsqu'on est assez familiarisé avec le domaine auquel elle s'applique, avec les êtres qui la peuplent... Et nous n'avons pas hésité à détailler au maximum les corrections, afin de ne laisser aucun point obscur ; enfin nous l'espérons.

Bien sûr, il a fallu faire des choix. Nous avons été amené à renoncer à toute présentation de la théorie de Galois, alors même que c'est l'origine historique de la théorie des groupes ; et nous n'avons pas abordé les développements passionnants que sont la théorie des extensions de groupes, ainsi que celle des représentations de groupes. Enfin, il n'est pas non plus question des propriétés topologiques des groupes.

1. Lire et relire l'excellent [20].

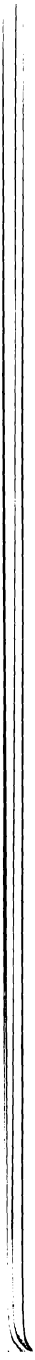
Quelques remarques sur les notations. Le groupe diédral est très présent dans les exercices, car suffisamment simple et compliqué pour être exemplaire. Ayant $2n$ éléments, avec n entier, il est parfois noté $\mathbb{D}_n$, car il est groupe de symétrie du polygone régulier à n éléments, et contient le groupe cyclique à n éléments... Nous avons choisi de le noter $\mathbb{D}_{2n}$, l'indice étant alors le cardinal ; cela nous paraît en effet plus conforme aux habitudes récentes. De la même façon, nous notons $\mathbb{Z}/n$ le groupe additif quotient de $\mathbb{Z}$ par le sous-groupe des multiples de n ; c'est un compromis entre la notation $\mathbb{Z}/n\mathbb{Z}$ un peu longue, et $\mathbb{Z}_n$ qui peut prêter à confusion (avec nombres p-adiques). Plus important, et discutable, nous faisons souvent jouer au groupe noté $\mathbb{Z}/n$ le rôle du prototype d'un groupe cyclique d'ordre n. Or, ce n'en est qu'une réalisation particulière, additive, avec un générateur privilégié (la classe de 1), de même que le groupe des racines n-ièmes de l'unité en représente une autre réalisation. Il aurait sans doute été préférable d'avoir une notation différente pour « le » groupe cyclique d'ordre n, compris comme le groupe engendré par un élément x d'ordre n, de présentation $\langle x \mid x^n \rangle$. On trouve parfois une écriture comme $\mathbf{C}_n$. Notre choix risque de dérouter, surtout qu'il nous arrive de jongler entre notation additive et multiplicative, mais ce type d'écriture « à isomorphisme près » est fréquent... et a des avantages. On nous pardonnera aussi, peut-être, certains « ssi » mis pour « si et seulement si ».

Pour terminer, parlons de notre public, enfin du public souhaité : les connaissances nécessaires pour nous suivre sont celles qu'a acquises un étudiant de Deug. Il lui est demandé une certaine familiarité avec l'algèbre linéaire, et avec les rudiments de l'algèbre générale. Ce livre devrait donc être utile aux étudiants de licence et de maîtrise, ainsi, bien sûr, qu'aux candidats aux concours Capes et Agrégation. Espérons également qu'il saura plaire aux simples amateurs de mathématiques.

Ce livre ne serait pas ce qu'il est sans les conseils éclairés que m'ont donnés de nombreux collègues et amis, spécialistes ou non de la théorie des groupes. Je remercie en particulier Dong Ye pour sa relecture attentive, mais il va de soi que les nombreuses erreurs qui subsistent sont entièrement de mon fait. Merci également aux éditions Dunod pour la qualité de leur travail éditorial.

Cette seconde édition a permis de corriger certaines erreurs et d'ajouter des précisions : merci à François Digne pour ses remarques. Nous avons également proposé quelques problèmes supplémentaires.

Table des matières



Chapitre 1

Groupes
Groupes cycliques

1.1 GROUPES, SOUS-GROUPES, ORDRE

Un groupe $\mathbf{G}$ ou $(\mathbf{G}, *)$ est un ensemble muni d'une loi $*$ associative qui admet un élément neutre et pour laquelle tout élément a un symétrique. Cela s'écrit :

$$\forall x, y, z \in \mathbf{G},\ x * (y * z) = (x * y) * z$$
$$\exists e \in \mathbf{G},\ x * e = e * x = x$$
$$\forall x \in \mathbf{G},\ \exists x' \in \mathbf{G},\ x * x' = x' * x = e$$

Si, de plus :

$$\forall x, y \in \mathbf{G},\ x * y = y * x$$

on dit que la loi est **commutative**, $\mathbf{G}$ est commutatif ou **abélien**. On note la loi de composition par $*$, par $\times$, ou par... rien du tout. Si la loi est commutative, on écrit plutôt $+$. On montre facilement que l'élément neutre est unique, il est noté e, 1 ou 0 dans le cas d'une loi commutative ; le symétrique de x est également unique, il est noté x^{-1} ou $-x$ (cas commutatif).

Un sous-groupe de $\mathbf{G}$ est un sous-ensemble de $\mathbf{G}$ qui est lui-même un groupe (pour la même loi de composition). Ainsi $\{e\}$ et $\mathbf{G}$ lui-même sont des sous-groupes de $\mathbf{G}$, appelés **sous-groupes triviaux**. Si $\mathbf{H}$ est un sous-groupe de $\mathbf{G}$, on écrit : $\mathbf{H} \leqslant \mathbf{G}$.

Exercice 1.1.1

Montrer qu'un ensemble $\mathbf{G}$ muni d'une loi associative est un groupe si et seulement si

$$\exists e \in \mathbf{G},\ \forall a \in \mathbf{G},\ e * a = a$$
$$\forall a \in \mathbf{G},\ \exists b \in \mathbf{G},\ b * a = e$$

Autrement dit, il suffit qu'il existe un élément neutre à gauche et un symétrique à gauche.

Exercice 1.1.2

Soit **G** un groupe fini, $\mathbf{G} = \{e, x_1, x_2, \ldots, x_{n-1}\}$ où e est l'élément neutre. On appelle **table** du groupe la matrice $T = (a_{i,j})$ où $a_{i,j} = x_i * x_j$. Montrer que T est un « carré latin », c'est-à-dire que sur chaque ligne et sur chaque colonne il y a un et un seul élément de **G**. Réciproquement, est-ce que tout carré latin est la table d'un groupe ?

Exercice 1.1.3

Soit **G** un groupe et S un sous-ensemble. Pourquoi peut-on parler du « sous-groupe engendré par **la** partie S » ? On le note $\langle S \rangle$ ou gr(S).

Exercice 1.1.4

Si **H** est un sous-ensemble **fini** d'un groupe **G**, **stable** pour la loi. Montrer que **H** est un sous-groupe de **G**. Contre-exemple dans le cas de cardinal infini.

Après ces généralités, nous arrivons au premier résultat important de la théorie des groupes, connu sous le nom de **théorème de Lagrange** : tout sous-groupe d'un groupe fini a pour cardinal un diviseur du cardinal du groupe. En démontrant ce théorème, on introduit des définitions très importantes, celle de l'ensemble quotient **G**/**H**, celle de l'indice d'un sous-groupe.

Exercice 1.1.5

Soit **G** un groupe, **H** un sous-groupe et x un élément de **G**. On note $x\mathbf{H}$ l'ensemble des éléments de **G** qui s'écrivent xh, avec $h \in \mathbf{H}$.

1) Montrer que la relation $x\mathcal{R}y \iff y \in x\mathbf{H}$ est une relation d'équivalence.
2) Montrer que les classes d'équivalence sont de la forme $x\mathbf{H}$ et sont toutes en bijection avec **H**. L'ensemble quotient, c'est-à-dire l'ensemble des classes d'équivalence est noté **G**/**H**. Son cardinal s'appelle l'indice de **H** dans **G**, et il s'écrit [**G** : **H**].
3) À quelle condition a-t-on $x\mathbf{H} = \mathbf{H}$? Quelles sont les classes d'équivalence qui sont des sous-groupes ?
4) Démontrer le **théorème de Lagrange**, si **H** est un sous-groupe d'un groupe fini **G**, alors le cardinal de **H** est un diviseur du cardinal de **G**.
5) On définit de même les classes d'équivalence à droite, de la forme $\mathbf{H}x$. Montrer que les classes à droite sont toutes en bijection avec **H**, et que l'ensemble quotient est en bijection avec l'ensemble des classes à gauche.

Exercice 1.1.6

Soit **H** un sous-groupe d'indice fini de **G**, et **K** un sous-groupe de **G** contenant **H**. Montrer qu'il est d'indice fini dans **G** et que :

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}][\mathbf{K} : \mathbf{H}]$$

Premiers exemples de groupes, les groupes cycliques. Ils apparaîtront sous différents aspects dans toute la théorie.

Exercice 1.1.7

On appelle **groupe monogène** un groupe engendré par un élément $\mathbf{G} = \langle x \rangle$. Montrer que $\mathbf{G}$ est infini, de la forme $\mathbf{G} = \{\ldots, x^{-1}, 1, x, x^2, x^3, \ldots\}$ ou fini de la forme $\mathbf{G} = \{1, x, x^2, \ldots, x^{n-1}\}$.[1] Un exemple du premier cas est $(\mathbb{Z},+)$, de générateur 1 ; le second cas est illustré par $(\mathbb{Z}/n\mathbb{Z},+)$, noté également $\mathbb{Z}/n$, ou par $\mathbb{U}_n$, groupe multiplicatif des racines n-ièmes de l'unité dans $\mathbb{C}$. Dans le cas fini, on dit que $\mathbf{G}$ est un **groupe cyclique**.

La notion d'**ordre** d'un élément est liée aux groupes cycliques. Rappelons qu'on appelle ordre d'un ensemble fini le nombre de ses éléments (on dit aussi cardinal). Il s'agit de deux emplois différents du mot ordre... Mais il y a quand même un lien.

Exercice 1.1.8

On appelle **ordre** d'un élément x d'un groupe $\mathbf{G}$ le plus petit entier $n > 0$ tel que $x^n = e$. Si n n'existe pas, on dit que x est d'ordre infini. L'ordre de x est souvent noté $|x|$ comme le cardinal d'un ensemble.

1) Montrer que l'ordre de x est l'ordre (i.e. le cardinal) du sous-groupe engendré par x.
2) Montrer que si l'ordre de x est n, alors $x^p = e \iff p \in n\mathbb{Z}$.
3) Si l'ordre de x est n, quel est l'ordre de x^k ?
4) Si a et b commutent, que peut-on dire de l'ordre de ab en fonction des ordres de a et de b ? On examinera le cas où les ordres de a et de b sont premiers entre eux.
5) Comparer les ordres de ab et de ba.
6) Dans un groupe fini, l'ordre de tout élément est fini. Réciproque ?

Exercice 1.1.9

Déterminer les sous-groupes d'un groupe cyclique. Traiter le cas infini, puis le cas d'un groupe cyclique d'ordre n ; il y a alors un sous-groupe de cardinal d pour chaque entier d divisant n. Que peut-on dire si n est premier ?

Exercice 1.1.10

Soit $\mathbf{G}$ un groupe cyclique d'ordre n engendré par x. On dit qu'un élément y de $\mathbf{G}$ est un **générateur** si $\mathbf{G} = \langle y \rangle$.
Montrer que les générateurs de $\mathbf{G}$ sont les éléments de la forme x^k où k est premier avec n. Détailler le cas où $n = 12$ puis où n est premier. On note $\phi(n)$ le nombre des générateurs d'un groupe cyclique d'ordre n ; il s'appelle **indicateur d'Euler**.

Exercice 1.1.11

Calculer $\phi(p)$, $\phi(p^\alpha)$ (avec p premier). Démontrer que :

$$\forall x \in \mathbb{N}^*, \sum_{d|n} \phi(d) = n$$

1. On note x^k le produit de x par lui-même k fois, avec les conventions habituelles pour $x^0 = e$ et pour $x^k = (x^{-1})^{-k}$ si k est négatif.

Exercice 1.1.12

Montrer qu'un groupe fini de cardinal n est cyclique ssi pour tout d divisant n, il existe un seul sous-groupe de cardinal d. On utilisera l'exercice précédent. Montrer de même que tout sous-groupe fini (multiplicatif) d'un corps commutatif est cyclique.

Exercice 1.1.13

On suppose que $\mathbf{G}$ est un groupe tel que : $\forall x \in \mathbf{G},\ x^2 = e$; autrement dit, tous les éléments différents de e sont d'ordre 2. Montrer que $\mathbf{G}$ est commutatif.

Exercice 1.1.14

Montrer que si le cardinal d'un groupe $\mathbf{G}$ est pair, alors il existe dans $\mathbf{G}$ un élément d'ordre 2. Réciproque ? On verra une généralisation dans le chapitre 3 (lemme de Cauchy).

Exercice 1.1.15

Démontrer qu'un groupe est fini ssi il a un nombre fini de sous-groupes.

Nous sommes maintenant en mesure de classer tous les groupes finis ayant moins de sept éléments. Cette classification des groupes finis se poursuivra tout au long de cet ouvrage ; en annexe, un tableau regroupe les principaux résultats concernant ces groupes finis de petit cardinal.

Exercice 1.1.16

Montrer que tout groupe ayant p éléments, où p est premier, est un groupe cyclique. Ainsi, nous connaissons les groupes à 2, 3, 5 et 7 éléments. Ainsi, bien sûr, que le groupe à 1 seul élément, que l'on notera souvent e, 1, ou même 0 dans un contexte commutatif.

Exercice 1.1.17

Montrer qu'il y a deux groupes à quatre éléments, tous les deux commutatifs. Celui qui n'est pas cyclique se note $\mathcal{V}$ et s'appelle **groupe de Klein**, ou **groupe du rectangle**.

Exercice 1.1.18

Démontrer qu'il y a deux groupes à six éléments, dont l'un n'est pas commutatif.

Après les groupes cycliques et nos petits groupes, nous allons construire de nouveaux exemples à l'aide de l'algèbre linéaire.

Exercice 1.1.19 (Des sous-groupes de matrices)

On note $\mathcal{M}(n, \mathbb{K})$ l'espace vectoriel des matrices carrées à coefficients dans le corps $\mathbb{K}$. Montrer que les ensembles suivants sont des groupes pour la multiplication :

1) L'ensemble des matrices de déterminant non nul, $\mathbf{GL}(n, \mathbb{K})$ (groupe linéaire).

2) L'ensemble des matrices de déterminant égal à 1, $\mathbf{SL}(n, \mathbb{K})$ (groupe spécial linéaire).

3) L'ensemble des matrices triangulaires supérieures, $\mathbf{T}(n, \mathbb{K})$ (matrices inversibles dont tous les coefficients d'indice $i > j$ sont nuls) ou des matrices triangulaires unipotentes, $\mathbf{TU}(n, \mathbb{K})$, c'est-à-dire les matrices triangulaires supérieures n'ayant que des 1 sur la diagonale.

Exercice 1.1.20

L'ensemble des matrices symétriques inversibles est-il un sous-groupe de l'ensemble des matrices inversibles ? Montrer que l'ensemble des matrices qui s'écrivent $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ avec $a^2 \neq b^2$ est un groupe pour le produit.

Exercice 1.1.21

Trouver les sous-groupes engendrés par les matrices suivantes (la loi est le produit des matrices) :

1) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

2) $B = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ avec $j = e^{\frac{2i\pi}{3}}$

3) Étudier le groupe engendré par A et B. On vérifiera qu'il a douze éléments, et l'on en cherchera les sous-groupes.

Exercice 1.1.22

Soient $\mathbb{E}$ un $\mathbb{K}$-espace vectoriel et $\mathbb{F}$ un sous-espace vectoriel. Montrer que $\mathbb{F}$ est un sous-groupe additif de $\mathbb{E}$. Réciproquement, est-ce que tout sous-groupe additif de $\mathbb{E}$ est un sous-espace vectoriel ? Donner des contre-exemples, mais examiner aussi le cas où $\mathbb{K}$ est un corps fini.

L'exercice suivant est important. Il montre comment construire un groupe à l'aide de deux autres. Nous rencontrerons à nouveau, et à plusieurs reprises, ce genre de construction.

Exercice 1.1.23

Soit $\mathbf{G}$ un groupe et $\mathbf{H} \leqslant \mathbf{G}$, $\mathbf{K} \leqslant \mathbf{G}$ deux sous-groupes. On s'intéresse à l'ensemble des éléments de la forme hk où $h \in \mathbf{H}$, $k \in \mathbf{K}$, ensemble que l'on note $\mathbf{HK}$.

1) Démontrer que $\mathbf{HK}$ est un sous-groupe si et seulement si $\mathbf{HK} = \mathbf{KH}$.

2) Quel est le cardinal de $\mathbf{HK}$ quand les deux groupes $\mathbf{H}$ et $\mathbf{K}$ sont finis ?

3) Montrer que si $\mathbf{H} \cap \mathbf{K} = \{e\}$, alors tout élément de $\mathbf{HK}$ s'écrit de façon unique comme produit hk.

4) Soit $\mathbf{G} = \mathbb{Z}/6$ et $\mathbf{H} = \langle \overline{2} \rangle$, $\mathbf{K} = \langle \overline{3} \rangle$. Vérifier que $\mathbf{G} = \mathbf{HK}$ et qu'il y a unicité de l'écriture comme dans la question précédente.

SOLUTIONS

1.1.1 Si b est inverse à gauche de a, montrons qu'il est aussi inverse à droite, $b * (a * b) = (b*a)*b = e*b = b$; si c est l'inverse à gauche de b, $(c*b)*(a*b) = e*(a*b) = a*b = c*b = e$, donc $a*b = e$. Montrons maintenant que e est aussi neutre à droite : $a*e = a*b*a = e*a = a$.

1.1.2 La ligne i de la matrice est l'ensemble des images des éléments de **G** par l'application $x \mapsto x_i * x$. Or cette application, que l'on nomme translation à gauche, et qu'on note L_{x_i}, est bijective, puisque l'équation $x_i * x = y$ a pour seule solution $x = x_i^{-1} * y$. On traite de même les colonnes de la matrice.
Tous les carrés latins ne sont pas des tables de groupe, même si l'on impose que la première ligne et la première colonne correspondent à l'élément neutre :

$*$	e	a_1	a_2	a_3	a_4
e	e	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_4	e	a_3
a_2	a_2	a_3	a_1	a_4	e
a_3	a_3	a_4	e	a_2	a_1
a_4	a_4	e	a_3	a_1	a_2

Sur ce tableau on constate par exemple que : $(a_1 * a_2) * a_3 = a_4 * a_3 = a_1$ et que $a_1 * (a_2 * a_3) = a_1 * a_4 = a_3$. La loi n'est pas associative.

1.1.3 Tout repose sur la propriété suivante. L'intersection de groupes est un groupe. Si donc S est un sous-ensemble de **G**, l'intersection des sous-groupes de **G** qui contiennent S est un sous-groupe, le plus petit contenant S. Comme **G** lui-même est un sous-groupe contenant S, cette intersection est bien définie et est non vide. Il est ensuite facile de montrer que ce sous-groupe est l'ensemble des produits de la forme : $s_1^{e_1} s_2^{e_2} \dots s_k^{e_k}$ où les s_i sont dans S et $e_i = \pm 1$. Comparer cette notion avec celle de « sous-espace vectoriel engendré par une partie ».

1.1.4 Soit $x \in \mathbf{H}$ et $\phi : g \mapsto xg$. Par hypothèse, si l'on restreint ϕ à **H**, l'ensemble d'arrivée est bien **H**. De plus, ϕ est injective (un antécédent de y est $x^{-1}y$). Comme **H** est fini, elle est bijective, et donc e admet un antécédent, x est inversible dans **H**. **H** est donc bien un sous-groupe de **G**. Pour un contre-exemple, regarder $\mathbb{N}$, stable pour la somme, mais qui n'est pas un sous-groupe de $\mathbb{Z}$.

1.1.5 1) $x\mathcal{R}x$ pour tout x, car $x = xe \in x\mathbf{H}$; si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x = yh$, $y = zh'$ donc $x = zh'h$ et $x \in z\mathbf{H}$. Enfin si $x = yh$ alors $y = xh^{-1}$. On a montré que la relation est réflexive, transitive et symétrique lorsque **H** est un sous-groupe. Remarquons que la relation $\mathcal{R}$ peut aussi être définie par : $x\mathcal{R}y \iff x^{-1}y \in \mathbf{H}$.

2) La définition même de la relation montre que les éléments en relation avec x sont tous dans $x\mathbf{H}$; de plus, l'application de **H** dans $x\mathbf{H}$ définie par $h \mapsto xh$ est bijective, surjective par définition de $x\mathbf{H}$ et injective car $xh = xh' \Rightarrow h = h'$, en composant à gauche par l'inverse de x.

3) $x\mathbf{H} = \mathbf{H}$ équivaut à x est en relation avec e, soit $x \in \mathbf{H}$. Si une classe est un sous-groupe, alors elle contient l'élément neutre e. C'est donc la classe de e, c'est-à-dire **H**. Toutes les autres classes ne sont pas des sous-groupes.

4) Comme pour toute relation d'équivalence, les classes d'équivalence forment une partition du groupe **G**. Leur ensemble s'écrit $\mathbf{G}/\mathbf{H}$ son cardinal, $[\mathbf{G} : \mathbf{H}]$ s'appelle l'indice de **H**

dans $\mathbf{G}$. Il peut être fini quand $\mathbf{G}$ et $\mathbf{H}$ sont infinis : c'est le cas de l'indice de $n\mathbb{Z}$ dans $\mathbb{Z}$ (qui vaut n). Quand $\mathbf{G}$ est fini, toutes les classes d'équivalence ont autant d'éléments que $\mathbf{H}$ et :

$$\text{card}(\mathbf{G}) = [\mathbf{G} : \mathbf{H}]\ \text{card}(\mathbf{H})$$

En particulier, on en déduit le **théorème de Lagrange** : le cardinal d'un sous-groupe d'un groupe de cardinal fini n est un diviseur de n.

5) On peut, pour définir les classes à droite, considérer la relation d'équivalence :

$$x\mathcal{S}y \iff y \in \mathbf{H}x \iff yx^{-1} \in \mathbf{H}$$

La relation $\mathcal{R}$ et la relation $\mathcal{S}$ sont alors reliées par :

$$x\mathcal{R}y \iff x^{-1}\mathcal{S}y^{-1}$$

Si donc on note, comme cela se fait parfois, $\mathbf{G} \setminus \mathbf{H}$ l'ensemble des classes d'équivalence à droite, il y a bijection entre les deux ensembles quotients par :

$$x\mathbf{H} \mapsto \mathbf{H}x^{-1}$$

1.1.6 Supposons que la famille $(g_i)_{i\in I}$ soit une famille de représentants des classes de $\mathbf{G}$ modulo $\mathbf{K}$ et que $(k_j)_{j\in J}$ soit une famille de représentants des classes de $\mathbf{K}$ modulo $\mathbf{H}$. Alors,

$$\mathbf{G} = \bigcup_{i\in I} g_i\mathbf{K} = \bigcup_{(i,j)\in I\times J} g_ik_j\mathbf{H}$$

Par ailleurs, si $g_ik_j\mathbf{H} = g_{i'}k_{j'}\mathbf{H}$, il vient $g_i^{-1}g_{i'} \in \mathbf{K}$ puisque $\mathbf{H} \subset \mathbf{K}$, et donc $g_i\mathbf{K} = g_{i'}\mathbf{K}$, soit $g_i = g_{i'}$. On a alors $k_j\mathbf{H} = k_{j'}\mathbf{H}$ d'où $k_j = k_{j'}$. On en déduit que les $(g_ik_j)_{(i,j)\in I\times J}$ constituent une famille de représentants des classes de $\mathbf{G}$ modulo $\mathbf{H}$. Et donc, si l'indice $[\mathbf{G} : \mathbf{H}]$ est fini, le cardinal de $I \times J$ est fini, I et J sont finis et

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}]\,[\mathbf{K} : \mathbf{H}]$$

1.1.7 $\langle x\rangle$ contient tous les éléments de la forme x^i, $i \in \mathbb{Z}$. S'il est fini, il existe i et j distincts (par exemple $i > j$) tels que $x^i = x^j$. On en déduit $x^{i-j} = e$. Définissons maintenant n comme étant le plus petit des entiers strictement positifs tels que $x^n = e$. Alors :

- $x^p = e \iff p \in n\mathbb{Z}$
- $\mathbf{G} = \{e, x, x^2, \ldots, x^{n-1}\}$

En effet, si $x^p = e$ et si $p = nq + r$ est la division euclidienne de p par n, alors $x^r = (x^p)(x^n)^{-q} = e$; au vu de la définition de n, on doit avoir $r = 0$, donc p est un multiple de n. On vérifie que les éléments indiqués sont distincts, sinon on aurait une égalité de la forme $x^{i-j} = e$ avec $0 < i - j < n$. De plus, $\mathbf{G}$ ainsi décrit est bien un groupe, l'inverse de x^i est x^{n-i}.
Dans le cas infini, toutes les puissances de x sont distinctes, sinon l'argumentation ci-dessus conduirait à $\mathbf{G}$ fini. Alors, l'ensemble $\{\ldots, x^{-2}, x^{-1}, e, x, x^2, x^3, \ldots\}$ est bien un groupe.

1.1.8 Cet exercice ressemble beaucoup au précédent. On ne reprendra pas le détail des arguments.

1) Si x est d'ordre n, alors le sous-groupe engendré par x est $\{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Ces éléments sont distincts, au nombre de n. On a bien $|x| = |\langle x\rangle|$. Si x n'est pas d'ordre fini, le sous-groupe engendré par x est en bijection avec $\mathbb{Z}$, il a une infinité d'éléments.

2) Déjà vu dans l'exercice précédent.

3) Soit ℓ l'ordre de x^k. Alors, $\left(x^k\right)^\ell = e$, donc $\exists\lambda \in \mathbb{Z}/\ k\ell = n\lambda$. Ce nombre est donc un multiple commun de k et de n, la plus petite valeur positive de ℓ est par conséquent celle

qui donne $k\ell = \text{ppcm}(k, n)$; or, on sait que :

$$\text{ppcm}(k, n) = k \vee n = \frac{kn}{k \wedge n}$$

On en déduit que

$$|x^k| = \frac{n}{k \wedge n}$$

Remarquons que x^k est de même ordre que x lorsque k et n sont premiers entre eux.

4) Le fait que a et b commutent permet d'écrire : $(ab)^k = a^k b^k$. Soient alors n et m les ordres respectifs de a et b. On a bien sûr $(ab)^{mn} = a^{mn}b^{mn} = e$. Supposons maintenant que $(ab)^\ell = a^\ell b^\ell = e$. Élevons cette égalité à l'exposant n, $a^{\ell n}b^{\ell n} = b^{\ell n} = e$. On en déduit que ℓn est un multiple de m. Comme n et m sont premiers entre eux, il vient, par le théorème de Gauss, que ℓ est un multiple de m. De même, on montre que ℓ est un multiple de n, et ℓ est un multiple du ppcm de m et n, c'est-à-dire de mn. Si m et n ne sont pas premiers entre eux, l'ordre de ab peut être plus petit que le ppcm des ordres ; si a est d'ordre 4, alors a^3 est d'ordre 4 et leur produit est d'ordre... 1.

5) Si ab est d'ordre n, alors :

$$(ba)^n = b(ab)^{n-1}a = b(ab)^{-1}a = bb^{-1}a^{-1}a = e$$

et ba est d'ordre m inférieur à n. Le même calcul montre que n est inférieur à m d'où l'égalité des ordres.

6) La réciproque est fausse. Autrement dit, il existe des groupes infinis dont tout élément est d'ordre fini. Nous aurons l'occasion d'en rencontrer plusieurs, mais voici un premier exemple. Soit **G** le groupe des suites à valeurs dans $\mathbb{Z}/2$; il est muni d'une structure de groupe additif en posant $(u + v)_n = u_n + v_n$, et tout élément est d'ordre fini égal à 2 (1 pour la suite constante nulle).

1.1.9 On reprend le même genre d'arguments que dans l'exercice précédent. Soit **H** un sous-groupe (autre que $\{e\}$) et $x^k \in \mathbf{H}$ tel que $k > 0$ (il y a de tels k car **H** est stable pour la prise d'inverse) soit minimum. Alors, $x^p \in \mathbf{H} \iff p \in k\mathbb{Z}$ par division euclidienne de p par k. Si **G** est infini, $\mathbf{H} = \langle x^k \rangle$ est alors un sous-groupe de **G**, et est aussi cyclique infini. Si **G** est fini d'ordre n, le théorème de Lagrange (1.1.5) permet d'affirmer que $\text{card}(\mathbf{H})$ est un diviseur d de n.
Soit alors d un diviseur quelconque de n. Alors $\langle x^{\frac{n}{d}} \rangle$ est un sous-groupe d'ordre d (puisque $x^{\frac{n}{d}}$ est exactement d'ordre d, cf. 1.1.8). Donc il existe toujours un sous-groupe d'ordre d. Montrons maintenant qu'il n'y en a qu'un seul, si $\langle x^k \rangle$ est un sous-groupe d'ordre d, alors $x^{kd} = e$, donc $n|kd$ et $\frac{n}{d}|k$. Cela montre que x^k appartient à $\langle x^{\frac{n}{d}} \rangle$. On a donc $\langle x^k \rangle \subset \langle x^{\frac{n}{d}} \rangle$. Mais comme ces deux groupes ont même ordre, ils coïncident.
Il y a donc un seul sous-groupe d'ordre d. Si n est premier, il n'y a donc aucun sous-groupe autre que e et **G** lui-même.

1.1.10 On peut utiliser l'exercice 1.1.8 pour trouver les générateurs de $\langle x \rangle$ où x est d'ordre n : l'ordre de x^k est $\frac{n}{k \wedge n}$, il faut et suffit que k soit premier à n pour que x^k soit d'ordre n et donc générateur de **G**. Le nombre des générateurs de **G** est donc le nombre des entiers k plus petit que n et premiers à n, noté $\phi(n)$. Ainsi, pour $n = 12$, sont générateurs x, x^5, x^7, x^{11} et $\phi(12) = 4$. Si $n = p$ est un nombre premier, tous les $k \neq 0$ conviennent et $\phi(p) = p - 1$.

1.1.11 Dans l'exercice précédent, on a montré que $\phi(p) = p - 1$. Cherchons maintenant les entiers inférieurs à p^α qui sont non premiers à p^α. Ce sont les nombres divisibles par p de la forme kp pour $0 \leqslant k < p^{\alpha-1}$. Il y en a donc $p^{\alpha-1}$, et l'on en déduit $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Pour la dernière formule, on considère $\mathbf{G} = \langle x \rangle$ un groupe cyclique d'ordre n et on classe ses éléments suivant leur ordre, c'est un entier d diviseur de n, et chaque élément d'ordre d est un générateur du (seul) sous-groupe d'ordre d. Le nombre des éléments d'ordre d est donc le nombre des générateurs d'un groupe cyclique d'ordre d, soit $\phi(d)$. Cette partition donne donc l'égalité :

$$n = \sum_{d|n} \phi(d)$$

1.1.12 On sait déjà qu'un groupe cyclique a cette propriété. Réciproquement, soit $\mathbf{G}$ d'ordre n un groupe ayant un seul sous-groupe d'ordre d pour tout d diviseur de n. On note $\psi(d)$ le nombre des éléments de $\mathbf{G}$ qui sont d'ordre d, nombre qui peut être éventuellement nul. Soit d tel que $\psi(d) \neq 0$ et x un élément d'ordre d. Alors $\langle x \rangle$ est le seul sous-groupe d'ordre d, il est cyclique, et tout élément d'ordre d engendre ce même groupe : on a donc $\psi(d) = \phi(d)$ chaque fois que $\psi(d)$ est non nul. Mais, en classant les éléments de $\mathbf{G}$ suivant leur ordre, on obtient une partition de $\mathbf{G}$ et :

$$n = \sum_{d|n} \psi(d) = \sum_{d|n} \phi(d)$$

il est donc impossible que pour un d, $\psi(d)$ soit nul ; on a, pour tout d, $\psi(d) = \phi(d)$, en particulier $\psi(n) = \phi(n)$, et est non nul, il existe un élément d'ordre n et $\mathbf{G}$ est cyclique.
Avec les mêmes notations, supposons maintenant que $\mathbf{G}$ soit un sous-groupe fini du groupe multiplicatif d'un corps. Soit g un élément d'ordre d, s'il en existe, et $\mathbf{H} = \langle g \rangle$. Alors tout élément d'ordre d vérifie l'égalité $x^d = 1$, et les d éléments de $\mathbf{H}$ vérifient aussi cette égalité. Mais dans un corps, une équation de degré d admet au plus d solutions ; tous les éléments d'ordre d sont donc dans $\mathbf{H}$ et en sont des générateurs. On termine comme ci-dessus.

1.1.13 Suppposons que tout carré soit égal à l'élément neutre :

$$(xy)^2 = xyxy = e \Rightarrow x(xyxy)y = x(e)y \Rightarrow yx = xy$$

Le groupe est donc commutatif.

1.1.14 On peut partitionner $\mathbf{G}$ en deux sous-ensembles, l'ensemble des éléments égaux à leur inverse, et l'ensemble de ceux qui sont différents de leur inverse. Le cardinal de ce dernier ensemble est pair (on regroupe par paires x et x^{-1}) ; le premier ensemble contient au moins l'élément neutre. Si donc le cardinal $\mathbf{G}$ est pair, ce premier ensemble contient au moins un élément $x \neq e$, tel que $x = x^{-1}$ soit $x^2 = e$, x est d'ordre 2. La réciproque est contenue dans le théorème de Lagrange : si x est d'ordre 2 dans un groupe fini, son ordre divise le cardinal du groupe.

1.1.15 Dans un sens, pas de problème... Pour l'autre sens, une idée est de se ramener aux groupes monogènes. Supposons que $\mathbf{G}$ ait un nombre fini de sous-groupes, il y a alors un nombre fini de sous-groupes de la forme $\langle x \rangle$. Si $\mathbf{G}$ avait une infinité d'éléments, parmi ces sous-groupes un serait monogène infini, ce qui est absurde car un tel groupe a une infinité de sous-groupes.

1.1.16 Nous avons déjà remarqué qu'un groupe cyclique ayant p éléments, p premier, n'a aucun sous-groupe non trivial. Pour un groupe $\mathbf{G}$ quelconque, d'ordre p premier, c'est la

même idée. Soit $x \neq e$. Son ordre est un diviseur de p différent de 1, c'est p. Le groupe **G** est donc engendré par p et est cyclique. Un groupe à 2 éléments sera cyclique, de modèle $\mathbb{Z}/2 = \{\overline{0}, \overline{1}\}$ s'il est noté additivement, ou $\{1, -1\}$ s'il est multiplicatif. De même, un groupe à trois éléments sera $\mathbb{Z}/3$ ou $\{1, j, j^2\}$, avec $j = e^{\frac{2i\pi}{3}}$, racine cubique de l'unité. De même pour cinq ou sept éléments. La suite nous prouvera que p premier n'est pas le seul cas où il existe un seul type de groupe ayant p éléments ; voir le tableau dans l'annexe B2.

1.1.17 Parmi les groupes ayant quatre éléments, il y a le groupe cyclique $\mathbb{Z}/4$ ou en version multiplicative $\{1, -1, i, -i\}$. Si **G** a quatre éléments et n'est pas cyclique, tous les éléments différents de e ont pour ordre 2. **G** est donc commutatif d'après l'exercice 1.1.13. Soit x et y deux éléments distincts et différents de e. Alors $x^2 = y^2 = e$ et $xy \neq x, xy \neq y$ car ni x ni y ne sont neutres. Comme le groupe est d'ordre 4, il n'y a pas d'autre élément. La table suivante s'en déduit, compte-tenu de la commutativité et de l'ordre 2 de xy :

$*$	e	x	y	xy
e	e	x	y	xy
x	x	e	xy	y
y	y	xy	e	x
xy	xy	y	x	e

C'est un carré latin. Reste à vérifier, il n'y a pas beaucoup de cas, l'associativité... Une autre méthode pour vérifier cette associativité est de trouver un « modèle » : dans le plan euclidien, (Oxy) repère orthogonal, on prend pour x la réflexion d'axe Ox, pour y la réflexion d'axe Oy. xy est alors la symétrie de centre O et le groupe obtenu est le groupe des isométries qui conservent un rectangle centré en O et d'axes de symétrie Ox et Oy. D'où le nom de **groupe du rectangle** pour ce groupe $\mathcal{V}$ (de l'allemand « vier », quatre). On le nomme également **groupe de Klein**[1].

1.1.18 Il y a le groupe cyclique. Soit **G** non cyclique d'ordre 6 et x un élément d'ordre 2. Il en existe d'après l'exercice 1.1.14. Si tous les éléments différents de e étaient d'ordre 2, on retrouverait un sous-groupe d'ordre 4 comme dans l'exercice précédent, ce qui est absurde (théorème de Lagrange). Il existe un élément y d'ordre 3. **G** contient donc déjà e, x, y, y^2, et $y^2 \neq x$ car il est d'ordre 3. Soit alors l'élément xy. Il est différent de e, car l'inverse de x est lui-même, de x et de y, car x et y sont différents de e. Il est différent de y^2 car x est différent de y. Enfin, les mêmes arguments montrent que xy^2 est distinct des précédents. Reste à définir les autres produits : yx ne peut être égal à e, x, y, y^2, il peut être xy ou yx. Compte-tenu de l'associativité, on voit rapidement que chacune des hypothèses permet de remplir la table ; dans le premier cas, on obtient :

$\times$	e	y	y^2	x	xy	xy^2
e	e	y	y^2	x	xy	xy^2
y	y	y^2	e	$\boldsymbol{xy}$	$\boldsymbol{xy^2}$	$\boldsymbol{x}$
y^2	y^2	e	y	$\boldsymbol{xy^2}$	$\boldsymbol{x}$	$\boldsymbol{xy}$
x	x	xy	xy^2	e	y	y^2
xy	xy	xy^2	x	$\boldsymbol{y}$	$\boldsymbol{y^2}$	$\boldsymbol{e}$
xy^2	xy^2	x	xy	$\boldsymbol{y^2}$	$\boldsymbol{e}$	$\boldsymbol{y}$

1. Dans le chapitre suivant, nous retrouverons ce groupe sous la forme $\mathbb{Z}/2 \times \mathbb{Z}/2$.

On « reconnaît » le groupe cyclique à six éléments ; il est commutatif et les puissances de xy, par exemple, redonnent tous les éléments du groupe. Dans le second cas, on obtient :

$\times$	e	y	y^2	x	xy	xy^2
e	e	y	y^2	x	xy	xy^2
y	y	y^2	e	$\mathbf{xy^2}$	$\mathbf{x}$	$\mathbf{xy}$
y^2	y^2	e	y	$\mathbf{xy}$	$\mathbf{xy^2}$	$\mathbf{x}$
x	x	xy	xy^2	e	y	y^2
xy	xy	xy^2	x	$\mathbf{y^2}$	$\mathbf{e}$	$\mathbf{y}$
xy^2	xy^2	x	xy	$\mathbf{y}$	$\mathbf{y^2}$	$\mathbf{e}$

C'est un groupe non commutatif ; il a deux éléments d'ordre 3, y et y^2, et trois d'ordre 2, x, xy, xy^2. Pour vérifier l'associativité, on peut prendre le modèle suivant, y est la rotation de centre O et d'angle $\frac{2\pi}{3}$, x est la réflexion d'axe Ox. On vérifie alors qu'on a bien $xy = y^2x$. Ce groupe, que l'on peut appeler groupe du triangle équilatéral, va réapparaître sous de nouveaux déguisements[1], on le notera $\mathcal{S}_3$.

1.1.19 Les connaissances classiques d'algèbre linéaire donnent la réponse aux deux premières questions. $\mathbf{GL}(n, \mathbb{K})$ est un groupe, car une matrice est inversible ssi son déterminant est non nul. $\mathbf{SL}(n, \mathbb{K})$ en est un sous-groupe, car le produit de deux matrices de déterminant 1 est une matrice de déterminant 1. Il en va de même pour l'inverse. Pour la dernière question, utilisons une méthode « géométrique » ; si une matrice de $\mathbf{T}(n, \mathbb{K})$ est interprétée comme la matrice d'un automorphisme u de $\mathbb{K}^n$ dans la base canonique, celui-ci est caractérisé parce qu'il conserve les espaces engendrés par e_1, par $e_1, e_2, \ldots$, par $e_1, e_2, \ldots, e_n$. L'ensemble de tels automorphismes est stable pour la composition et pour l'inverse. On peut aussi montrer la stabilité de cet ensemble par le calcul ; on vérifie alors que si $A, B \in \mathbf{T}(n, \mathbb{K})$ alors, si $C = AB$ on a $c_{ii} = a_{ii}b_{ii}$. Cette observation montre que $\mathbf{TU}(n, \mathbb{K})$ est un sous-groupe.

1.1.20 Les matrices symétriques forment un sous-espace vectoriel donc un sous-groupe **additif** de l'ensemble des matrices carrées. En revanche, elles ne forment pas un sous-groupe multiplicatif en se restreignant à celles qui sont inversibles. En effet, le produit de deux matrices symétriques est symétrique ssi ces matrices commutent :

$$ {}^t(AB) = AB \iff {}^tB{}^tA = AB \iff BA = AB $$

et dès la dimension 2, on trouve des matrices symétriques inversibles qui ne commutent pas. Pour les mêmes raisons, l'inverse d'une matrice symétrique est une matrice symétrique.
Les matrices de la forme indiquée commutent et forment un sous-groupe de $\mathbf{GL}(n, \mathbb{K})$; il faut en particulier vérifier que le produit de deux matrices de cet ensemble est encore une matrice de la même forme.

1.1.21 1) Le groupe engendré par A est cyclique ; comme A est d'ordre 4, c'est le groupe cyclique à quatre éléments ou $\mathbb{Z}/4$.

2) Le groupe engendré par B est cyclique d'ordre 3.

3) La question est plus délicate. Un groupe engendré par deux éléments d'ordre fini peut être assez compliqué... Ici, le théorème de Lagrange prouve que le groupe engendré a au moins douze éléments, car il contient deux sous-groupes ayant quatre et trois éléments. Le calcul

1. Voir dans le chapitre 2, le paragraphe Groupes de permutations.

montre que $AB = B^2A$, ce qui permet rapidement de voir que le groupe obtenu a bien douze éléments qui sont :

$$I,\ A,\ A^2,\ A^3,\ B,\ B^2,\ AB,\ A^2B,\ A^3B,\ AB^2,\ A^2B^2,\ A^3B^2$$

Le groupe obtenu est non commutatif, nous aurons l'occasion d'en donner d'autres descriptions. Disons tout de suite qu'on le note T, et qu'il fait partie des « groupes dicycliques ». Il contient : un élément d'ordre 2, deux éléments d'ordre 3, six éléments d'ordre 4, et deux d'ordre 6.
On trouve alors six sous-groupes non triviaux qui contiennent tous le groupe à deux éléments. Pour une suite, voir l'exercice 3.3.6

1.1.22 Par définition même, un sous-espace vectoriel doit être lui-même un espace vectoriel, donc doit être un sous-groupe pour l'addition. En revanche, un sous-groupe additif de l'espace vectoriel $\mathbb{E}$ n'est pas forcément un $\mathbb{K}$-sous-espace vectoriel de $\mathbb{E}$. C'est par exemple le cas de $\mathbb{Q}$, sous-groupe additif du $\mathbb{R}$-espace vectoriel $\mathbb{R}$.
Si néanmoins $\mathbb{K} = \mathbb{F}_p$ est un corps fini à p éléments[1] où p est premier, alors les deux notions coïncident. En effet, la multiplication par un scalaire est, en ce cas, une addition répétée ; si $\mathbb{F}$ est un sous-groupe additif de $\mathbb{E}$,

$$\forall \lambda \in \mathbb{F}_p,\ \forall x \in \mathbb{F},\ \lambda.x = (1+1+1+\ldots+1).x = x+x+\ldots+x \in \mathbb{F}$$

On a noté 1 la classe de 1 et utilisé que $\mathbb{F}_p$ est additivement cyclique.

1.1.23 1) Utilisons pour résoudre cette question le « lemme » : $\mathbf{H}$ non vide est un sous-groupe de $\mathbf{G}$ ssi $\mathbf{HH} = \mathbf{H}$ et $\mathbf{H}^{-1} = \mathbf{H}$. On rédigera alors ainsi $\mathbf{HKHK} = \mathbf{HHKK} = \mathbf{HK}$ et $(\mathbf{HK})^{-1} = \mathbf{K}^{-1}\mathbf{H}^{-1} = \mathbf{KH} = \mathbf{HK}$ pour démontrer une implication. Pour l'autre, on dira :

$$\mathbf{K} \subset \mathbf{HK},\ \mathbf{H} \subset \mathbf{HK} \Rightarrow \mathbf{KH} \subset \mathbf{HK}, \qquad \mathbf{HK} = (\mathbf{HK})^{-1} \subset \mathbf{K}^{-1}\mathbf{H}^{-1} = \mathbf{KH}$$

ce qui prouve que $\mathbf{HK}$ est un sous-groupe de $\mathbf{G}$ implique $\mathbf{HK} = \mathbf{KH}$.

2) Soit ϕ l'application surjective définie par :

$$\begin{aligned} \phi :\ & \mathbf{H} \times \mathbf{K} \to \mathbf{HK} \\ & (h,k) \mapsto hk \end{aligned}$$

alors

$$\phi(h,k) = \phi(h',k') \iff hk = h'k' \iff kk'^{-1} = h^{-1}h' = w \in \mathbf{H} \cap \mathbf{K}$$

et si $w \in \mathbf{H} \cap \mathbf{K}$, alors $\phi(h,k) = \phi(hw, w^{-1}k)$. L'ensemble des antécédents d'un élément de $\mathbf{HK}$ est donc de cardinal $|\mathbf{H} \cap \mathbf{K}|$ et

$$|\mathbf{HK}| = \frac{|\mathbf{H}|\,|\mathbf{K}|}{|\mathbf{H} \cap \mathbf{K}|}$$

3)

$$hk = h'k' \Rightarrow kk'^{-1} = h^{-1}h' \in \mathbf{H} \cap \mathbf{K} = \{e\}$$

donc $k = k'$ et $h = h'$.

4) La vérification est immédiate (attention, on est en notation additive).

1. Lorsque qu'on considère sa structure de corps, l'anneau $\mathbb{Z}/p$ est plutôt noté $\mathbb{F}_p$.

1.2 MORPHISMES, SOUS-GROUPES NORMAUX, GROUPES QUOTIENTS

Un **morphisme de groupes** est une application ϕ d'un groupe $\mathbf{G}$ dans un groupe $\mathbf{H}$ qui respecte les opérations :

$$\forall g, g' \in \mathbf{G},\ \phi(gg') = \phi(g)\phi(g')$$

Tout morphisme transporte l'élément neutre en l'élément neutre, le symétrique de l'image de x est l'image du symétrique de x. De plus, ϕ et ϕ^{-1} transportent les sous-groupes en des sous-groupes.

Comme en algèbre linéaire, on appelle **noyau** d'un morphisme ϕ, noté $\mathrm{Ker}(\phi)$, l'ensemble des antécédents de l'élément neutre. Un morphisme est injectif ssi son noyau est réduit au neutre.

Si un morphisme de $\mathbf{G}$ vers $\mathbf{G}'$ est bijectif, son application réciproque est aussi un morphisme. Les deux groupes sont dits **isomorphes**, et l'on écrit :

$$\mathbf{G} \cong \mathbf{G}'$$

Un isomorphisme d'un groupe dans lui-même s'appelle un **automorphisme**. L'ensemble des automorphismes de $\mathbf{G}$ est un groupe pour la loi de composition ou loi rond ; il est noté $\mathrm{Aut}(\mathbf{G})$.

Exercice 1.2.1

Quel est l'effet d'un morphisme (d'un isomorphisme) sur l'ordre d'un élément ?

Exercice 1.2.2

Les groupes $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ munis de l'addition sont-ils isomorphes ?

Exercice 1.2.3

Soit x un élément quelconque de $\mathbf{G}$. On note i_x l'application :

$$\begin{array}{rccc} i_x : & \mathbf{G} & \to & \mathbf{G} \\ & g & \mapsto & i_x(g) = xgx^{-1} \end{array}$$

Montrer que i_x est un automorphisme de $\mathbf{G}$. On l'appelle **automorphisme intérieur**. Montrer que l'ensemble des automorphismes intérieurs est un sous-groupe de l'ensemble des automorphismes de $\mathbf{G}$. On le note $\mathrm{Int}(\mathbf{G})$.

Exercice 1.2.4

Montrer que $x \mapsto x^2$ de $\mathbf{G}$ dans $\mathbf{G}$ est un morphisme ssi $\mathbf{G}$ est commutatif. Lorsque $\mathbf{G}$ est fini, à quelle condition est-ce un automorphisme ?

Un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ est **normal** (ou **distingué**) dans $\mathbf{G}$ si toute classe à gauche est une classe à droite, ou, plus précisément, si $\forall x \in \mathbf{G},\ x\mathbf{H} = \mathbf{H}x$. On écrit alors :

$$\mathbf{H} \lhd \mathbf{G}$$

Dans le cas commutatif, tous les sous-groupes de $\mathbf{G}$ sont normaux dans $\mathbf{G}$. Dans le cas général, les deux sous-groupes « triviaux » de $\mathbf{G}$, i.e. $\{e\}$ et $\mathbf{G}$ sont normaux dans $\mathbf{G}$. Un groupe qui n'a pas de sous-groupe normal autre que les sous-groupes triviaux est un **groupe simple**.[1]

Exercice 1.2.5

Montrer que les seuls groupes commutatifs simples sont les groupes isomorphes à $\mathbb{Z}/p$ où p est premier.

Exercice 1.2.6

Montrer que $\forall x \in \mathbf{G},\ x\mathbf{H} \subset \mathbf{H}x \iff \forall x \in \mathbf{G},\ x\mathbf{H} = \mathbf{H}x$, et donc $\mathbf{H}$ est normal dans $\mathbf{G}$.

Si $\mathbf{H}$ est un sous-groupe normal dans $\mathbf{G}$, alors l'ensemble quotient $\mathbf{G}/\mathbf{H}$ peut être muni d'une structure de groupe compatible avec celle de $\mathbf{G}$; il suffit de définir le produit des deux classes $x\mathbf{H}$ et $y\mathbf{H}$ par $x\mathbf{H}y\mathbf{H} = xy\mathbf{H}$. Le fait que $\mathbf{H}$ est normal dans $\mathbf{G}$ montre que cette définition a un sens. La **projection** de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$ définie par $g \mapsto g\mathbf{H}$ est un morphisme de groupe.

Exercice 1.2.7

Démontrer qu'on peut caractériser un sous-groupe normal $\mathbf{H}$ dans $\mathbf{G}$ par l'une des conditions suivantes :

a) c'est le noyau d'un morphisme de $\mathbf{G}$ dans un autre groupe ;

b) il est stable par tout automorphisme intérieur.

Exercice 1.2.8

Montrer que l'intersection de deux sous-groupes normaux dans $\mathbf{G}$ est un sous-groupe normal dans $\mathbf{G}$.

Exercice 1.2.9

On suppose que $\mathbf{K} \leqslant \mathbf{H} \leqslant \mathbf{G}$. Dire quelles implications sont toujours vraies :

$$\mathbf{K} \lhd \mathbf{G} \Rightarrow \mathbf{K} \lhd \mathbf{H}$$
$$\mathbf{K} \lhd \mathbf{H} \Rightarrow \mathbf{K} \lhd \mathbf{G}$$
$$\mathbf{K} \lhd \mathbf{H} \text{ et } \mathbf{H} \lhd \mathbf{G} \Rightarrow \mathbf{K} \lhd \mathbf{G}$$

Exercice 1.2.10

Si f est un morphisme de $\mathbf{G}$ dans $\mathbf{G}'$ que dire de l'image réciproque (resp. l'image directe) d'un sous-groupe normal dans $\mathbf{G}'$ (resp. dans $\mathbf{G}$) ?

1. Les groupes simples sont les « briques » qui permettent, en grande partie, de reconstituer tous les autres groupes. Les groupes simples finis sont tous connus, mais l'étude complète de leur classification occupe plusieurs centaines de pages de démonstration.

Exercice 1.2.11

Montrer que le groupe des matrices triangulaires unipotentes, $\mathbf{TU}(n, \mathbb{K})$ est normal dans $\mathbf{T}(n, \mathbb{K})$. Est-il normal dans $\mathbf{GL}(n, \mathbb{K})$?

Exercice 1.2.12

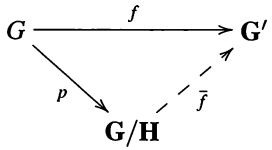
Montrer que $\mathrm{Int}(\mathbf{G})$ est un sous-groupe normal dans $\mathrm{Aut}(\mathbf{G})$.

Exercice 1.2.13 (Théorème de correspondance)

Soit $\mathbf{H} \lhd \mathbf{G}$. Montrer que l'application $\mathbf{K} \mapsto \mathbf{K}/\mathbf{H}$ est une bijection de l'ensemble des sous-groupes $\mathbf{K}$ tels que $\mathbf{H} \leqslant \mathbf{K} \leqslant \mathbf{G}$ sur l'ensemble des sous-groupes de $\mathbf{G}/\mathbf{H}$. Montrer que c'est aussi une bijection de l'ensemble de tels sous-groupes $\mathbf{K}$ normaux dans $\mathbf{G}$ dans l'ensemble des sous-groupes normaux dans $\mathbf{G}/\mathbf{H}$.
Retrouver ainsi les sous-groupes de $\mathbb{Z}/n$.

Exercice 1.2.14 (Théorème de factorisation)

Soit $f : \mathbf{G} \to \mathbf{G}'$ un morphisme de groupe. Soit $\mathbf{H} \lhd \mathbf{G}$. On suppose que $\mathbf{H} \subset \mathrm{Ker} f$. Montrer que l'on peut définir un morphisme $\bar{f} : \mathbf{G}/\mathbf{H} \mapsto \mathbf{G}'$ tel que $\bar{f} \circ p = f$ où p est la projection de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$. On dit que le morphisme f « passe au quotient ». Vérifier que f et $\bar{f}$ ont même image. Ce théorème se symbolise par le schéma suivant :



Dans ce type de diagramme, on convient que si l'on peut aller d'un groupe à un autre par plusieurs chemins, les morphismes composés correspondant à ces chemins seront égaux ; on dit parfois que l'on a un **diagramme commutatif**.

Exercice 1.2.15 (Premier théorème d'isomorphisme)

Montrer que si f est un morphisme de $\mathbf{G}$ dans $\mathbf{G}'$, alors on peut en déduire un isomorphisme de $\mathbf{G}/\mathrm{Ker} f$ dans $\mathrm{Im} f$. On pourra appliquer le théorème de factorisation.

Exercice 1.2.16

On suppose que $\mathbf{H} \lhd \mathbf{G}$ et $\mathbf{K} \leqslant \mathbf{G}$. Démontrer que le sous-groupe engendré par $\mathbf{H}$ et $\mathbf{K}$ est $\mathbf{HK}$.

Exercice 1.2.17 (Deuxième théorème d'isomorphisme)

$\mathbf{H}$ et $\mathbf{K}$ sont deux sous-groupes de $\mathbf{G}$. On suppose que $\mathbf{K} \lhd \mathbf{G}$. Montrer que :

$$\mathbf{H} \cap \mathbf{K} \lhd \mathbf{H} \text{ et } \mathbf{H}/\mathbf{H} \cap \mathbf{K} \cong \mathbf{HK}/\mathbf{K}$$

Exercice 1.2.18 (Troisième théorème d'isomorphisme)

K et **H** sont tous les deux normaux dans **G**. On suppose que $\mathbf{K} \subset \mathbf{H}$. Montrer que :

$$\mathbf{H}/\mathbf{K} \lhd \mathbf{G}/\mathbf{K} \text{ et } (\mathbf{G}/\mathbf{K})/(\mathbf{H}/\mathbf{K}) \cong \mathbf{G}/\mathbf{H}$$

À présent, quelques exercices supplémentaires qui tournent autour des mêmes idées, les relations entre un groupe et ses sous-groupes.

Exercice 1.2.19 (Lemme de Poincaré)

On suppose que $\mathbf{H} \leqslant \mathbf{G}$, $\mathbf{K} \leqslant \mathbf{G}$ et qu'ils sont tous deux d'indice fini. Démontrer que leur intersection est encore d'indice fini. On prouvera :

$$[\mathbf{G} : \mathbf{H} \cap \mathbf{K}] \leqslant [\mathbf{G} : \mathbf{H}][\mathbf{G} : \mathbf{K}]$$

Donner un exemple où la relation est une inégalité stricte, puis où la relation est une égalité.

Exercice 1.2.20 (Doubles classes)

H et **K** sont deux sous-groupes de **G**. Si $g \in \mathbf{G}$, une double classe est l'ensemble $\mathbf{H}g\mathbf{K} = \{hgk / \ h \in \mathbf{H},\ k \in \mathbf{K}\}$.

1) Montrer qu'une double classe est la réunion de classes à gauche et aussi une réunion de classes à droite. Montrer que les doubles classes partitionnent **G**.
2) Lorsque **G** est fini, calculer le cardinal d'une double classe. On pourra introduire $x\mathbf{K}x^{-1}$.
3) Que dire si l'un des sous-groupes est normal dans **G** ?

Exercice 1.2.21

Montrer qu'un sous-groupe d'indice 2 dans **G** est toujours normal dans **G**.

SOLUTIONS

1.2.1 Si x est d'ordre $n \in \mathbb{N}$, alors $\phi(x^n) = \phi(x)^n$ prouve que $\phi(x)$ est d'ordre d diviseur de n. Si ϕ est un isomorphisme, alors le même raisonnement avec ϕ^{-1} prouve que n divise d, et donc que x et $\phi(x)$ ont même ordre.

1.2.2 $\mathbb{Z}$ et $\mathbb{Q}$ ne peuvent être en bijection avec $\mathbb{R}$; ils sont dénombrables ce qui n'est pas le cas de $\mathbb{R}$. Par ailleurs, si $\mathbb{Q}$ était isomorphe à $\mathbb{Z}$, il serait monogène, et il existerait un générateur $\frac{p}{q}$ tel que tout rationnel puisse s'écrire $r = n\frac{p}{q}$ où $n \in \mathbb{Z}$. Or cela est impossible. Par exemple, tout rationnel de la forme $\frac{1}{q'}$ où q' n'est pas diviseur de q ne peut s'écrire ainsi.

1.2.3 $i_x(yy') = xyy'x^{-1} = xyx^{-1}xy'x^{-1} = i_x(y)i_x(y')$, $\qquad i_x(e) = xex^{-1} = e$
prouve qu'un automorphisme intérieur est un morphisme de groupe. C'est également une bijection car on a immédiatement $i_x^{-1} = i_{x^{-1}}$. Enfin, l'ensemble des automorphismes intérieurs est un groupe :

$$i_x \circ i_{x'}(y) = i_x(x'yx'^{-1}) = xx'y(xx')^{-1} = i_{xx'}(y)$$

en ajoutant que i_e est le neutre et $(i_x)^{-1} = i_{x^{-1}}$.

1.2.4 Si ϕ est un morphisme :

$$\forall x, y\ (xy)^2 = x^2y^2 \iff xyxy = xxyy \iff yx = xy$$

le groupe est commutatif, et réciproquement. Si maintenant $\mathbf{G}$ est fini, ϕ sera un isomorphisme ssi il est injectif ; or le noyau de ϕ est formé des éléments d'ordre 2 et de l'identité. On sait qu'un groupe admet des éléments d'ordre 2 ssi son cardinal est pair (voir 1.1.14), et la condition recherchée est donc $|\mathbf{G}|$ est impair.

1.2.5 L'étude des sous-groupes des groupes cycliques nous a montré que $\mathbb{Z}/n$ n'est simple que si n est premier. Il n'a pas de sous-groupe non trivial de même que n n'a pas de diviseur non trivial. Si $\mathbf{G}$ est un groupe commutatif non réduit à $\{e\}$, prenons $x \neq e$: $\langle x \rangle$ est un sous-groupe normal et $\mathbf{G}$ ne peut être simple que s'il est monogène. Enfin $\mathbb{Z}$, le groupe monogène infini n'est pas simple, il a une infinité de sous-groupes normaux.

1.2.6 Supposons $x\mathbf{H} \subset \mathbf{H}x$ pour tout x, et écrivons : $hx = xx^{-1}hx = xh'x^{-1}x = xh'$, (on a utilisé l'hypothèse avec x^{-1}) ; on a donc $\mathbf{H}x \subset x\mathbf{H}$. De la même façon, il suffit de vérifier $x\mathbf{H}x^{-1} \subset \mathbf{H}$ pour tout $x \in \mathbf{G}$, pour assurer que $\mathbf{H}$ est normal dans $\mathbf{G}$.

1.2.7 Dire que $\mathbf{H}$ est normal dans $\mathbf{G}$, c'est dire que pour tout $x \in \mathbf{G}$, $x\mathbf{H} = \mathbf{H}x$ soit aussi $x\mathbf{H}x^{-1} = \mathbf{H}$, c'est-à-dire $i_x(\mathbf{H}) = \mathbf{H}$ d'où b). Par ailleurs, si l'on considère la projection de $\mathbf{G}$ sur le groupe $\mathbf{G}/\mathbf{H}$, son noyau est $\mathbf{H}$; réciproquement, si ϕ est un morphisme de $\mathbf{G}$ dans $\mathbf{G}'$, alors :

$$\forall h \in \operatorname{Ker}\phi,\ \forall x \in \mathbf{G},\ \phi(xhx^{-1}) = \phi(x)\phi(h)\phi(x^{-1}) = \phi(x)\phi(x^{-1}) = e$$

et donc $xhx^{-1} \in \operatorname{Ker}\phi$, on a montré $x \operatorname{Ker}\phi\, x^{-1} \subset \operatorname{Ker}\phi$ ce qui prouve que le noyau d'un morphisme est toujours un sous-groupe normal.

1.2.8 Il suffit de l'écrire, soit x dans $\mathbf{G}$ et $y \in \mathbf{H} \cap \mathbf{K}$. Alors $xyx^{-1} \in \mathbf{H}$ car $\mathbf{H} \lhd \mathbf{G}$ et $xyx^{-1} \in \mathbf{K}$ car $\mathbf{K} \lhd \mathbf{G}$.

1.2.9 Seule la première implication est vraie ; si $x \in \mathbf{H}$, alors $x \in \mathbf{G}$ et $x\mathbf{K}x^{-1} = \mathbf{K}$ puisque $\mathbf{K}$ est normal dans $\mathbf{G}$. La deuxième implication est fausse ; si $x\mathbf{K}x^{-1} = \mathbf{K}$ est vrai pour tout x de $\mathbf{H}$, il n'y a pas de raison que cela reste vrai pour tout x de $\mathbf{G}$. L'hypothèse supplémentaire de la troisième implication ne permet pas non plus d'obtenir une implication. Voici un contre-exemple, qui utilise le groupe alterné $\mathcal{A}_4$ que nous verrons dans le chapitre suivant (2.4.11) :

$$\mathbf{G} = \mathcal{A}_4$$
$$\mathbf{H} = \{e, (12)(34), (13)(24), (14)(23)\}$$
$$\mathbf{K} = \{e, (12)(34)\}$$

On a alors $\mathbf{K} \lhd \mathbf{H}$, $\mathbf{H} \lhd \mathbf{G}$ et $\mathbf{K}$ n'est pas normal dans $\mathbf{G}$.

1.2.10 Soit ϕ un morphisme de $\mathbf{G}$ vers $\mathbf{G}'$; l'image réciproque d'un sous-groupe normal dans $\mathbf{G}'$ est un sous-groupe normal dans $\mathbf{G}$. En effet, si $\mathbf{H}' \lhd \mathbf{G}'$,

$$\forall x \in \mathbf{G}, \forall h \in \phi^{-1}(\mathbf{H}'),\ \phi(xhx^{-1}) = \phi(x)\phi(h)\phi(x)^{-1} \in \phi(x)\mathbf{H}'\phi(x)^{-1} = \mathbf{H}'$$

On a bien montré que $xhx^{-1} \in \phi^{-1}(\mathbf{H}')$. Cas particulier, si $\mathbf{H}' = \{e\}$, on retrouve le fait que le noyau d'un morphisme est toujours normal dans $\mathbf{G}$.
Si, en revanche, $\mathbf{H} \lhd \mathbf{G}$, alors $\phi(\mathbf{H}) \lhd \phi(\mathbf{G})$ par :

$$\phi(\mathbf{H}) = \phi(x\mathbf{H}x^{-1}) = \phi(x)\phi(\mathbf{H})\phi(x)^{-1}$$

et, donc, on n'a pas forcément $\phi(\mathbf{H}) \lhd \mathbf{G}'$.

1.2.11 Soit U une matrice triangulaire unipotente et T une matrice triangulaire supérieure (inversible). Alors TUT^{-1} est encore triangulaire supérieure, et les termes diagonaux sont égaux à 1. En effet, lorsqu'on fait le produit de deux matrices triangulaires supérieures, les éléments diagonaux du produit sont les produits des éléments diagonaux de chacun des facteurs.
Autre version de ce raisonnement, l'application :

$$\begin{array}{rccc} \phi : & \mathbf{T}(n,\mathbb{K}) & \to & \mathbb{K}^{*n} \\ & T=(t_{ij}) & \mapsto & (t_{11},\ldots,t_{nn}) \end{array}$$

est un morphisme de groupe (en comprenant que dans l'ensemble d'arrivée on multiplie composant par composant). Le groupe des matrices triangulaires unipotentes est le noyau de ce morphisme.
En revanche, le même groupe n'est pas normal dans $\mathbf{GL}(n,\mathbb{K})$. Il existe des matrices de la forme MUM^{-1} qui ne sont pas triangulaires unipotentes si U est triangulaire unipotente. Pour s'en convaincre, on peut voir qu'une telle matrice est semblable à U ; or on peut trouver des matrices semblables à une matrice triangulaire unipotente qui ne sont pas triangulaires. Bien sûr, on s'est placé dans le cas où $n > 1$.

1.2.12 Soit ϕ un automorphisme quelconque et i_x un automorphisme intérieur. Alors, pour $y \in \mathbf{G}$, on a :

$$\phi \circ i_x \circ \phi^{-1}(y) = \phi(x\phi^{-1}(y)x^{-1}) = \phi(x)y\phi(x)^{-1} = i_{\phi(x)}(y)$$

ce qui prouve que $\phi \circ i_x \circ \phi^{-1} = i_{\phi(x)}$ et que le sous-groupe des automorphismes intérieurs est normal dans le groupe des automorphismes.

1.2.13 Si $\mathcal{G}$ est l'ensemble des sous-groupes de $\mathbf{G}$ contenant $\mathbf{H}$, et $\mathcal{H}$ est l'ensemble des sous-groupes de $\mathbf{G}/\mathbf{H}$, on peut définir une application ϕ de $\mathcal{G}$ dans $\mathcal{H}$ par :

$$\phi(\mathbf{K}) = \mathbf{K}/\mathbf{H}$$

En effet, si l'on note p la projection de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$, on a $\phi(\mathbf{K}) = p(\mathbf{K})$. L'image de $\mathbf{K}$ est bien un sous-ensemble de $\mathbf{G}/\mathbf{H}$. C'est un sous-groupe de $\mathbf{G}/\mathbf{H}$ car

$$\mathbf{H} \lhd \mathbf{G} \text{ et } \mathbf{H} \leqslant \mathbf{K} \leqslant \mathbf{G} \Rightarrow \mathbf{H} \lhd \mathbf{K}$$

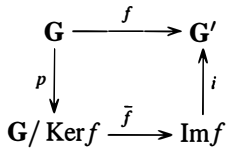
qui se voit en reprenant la définition d'un sous-groupe normal dans un groupe. Montrons que ϕ est bijective ; si $\mathbf{L}$ est un sous-groupe de $\mathbf{G}/\mathbf{H}$, alors $p^{-1}(\mathbf{L}) = \mathbf{K}$ est un sous-groupe de $\mathbf{G}$ (car p est un morphisme) qui contient $p^{-1}(e) = \mathbf{H}$. De plus, $\phi(\mathbf{K}) = p(\mathbf{K}) = p(p^{-1}(\mathbf{L})) = \mathbf{L}$ car p est surjective ; on a ainsi montré que tout élément de $\mathcal{H}$ avait un antécédent unique, ϕ est bijective.
Cette correspondance induit aussi une bijection entre sous-groupes normaux. En effet, l'image inverse et l'image directe par un morphisme surjectif d'un sous-groupe normal est un sous-groupe normal.
Les sous-groupes de $\mathbb{Z}/n$ sont ainsi en correspondance bijective avec les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Ce sont les $d\mathbb{Z}$ où $d|n$. On retrouve un résultat déjà obtenu.

1.2.14 Comme $\bar{f} \circ p = f$, il faut que $\bar{f}(g\mathbf{H})$ soit défini par $\bar{f}(g\mathbf{H}) = f(g)$. Mais pour que cette définition soit cohérente, il faut que le résultat soit le même quand on change de représentant. Si $g\mathbf{H} = g'\mathbf{H}$ alors $g^{-1}g' \in \mathbf{H} \subset \mathrm{Ker} f$ donc $f(g'^{-1}g) = e$ soit $f(g') = f(g)$. De plus, $\bar{f}$ est bien un morphisme, car

$$\bar{f}(g\mathbf{H}g'\mathbf{H}) = \bar{f}(gg'\mathbf{H}) = f(gg') = f(g)f(g') = \bar{f}(g\mathbf{H})\bar{f}(g'\mathbf{H})$$

Enfin, $\bar{f}$ a même image que f car l'ensemble des $\bar{f}(g\mathbf{H})$ est l'ensemble des $f(g)$.

1.2.15 Il suffit d'appliquer le théorème de factorisation au cas où $\mathbf{H} = \mathrm{Ker} f$ et de restreindre l'ensemble d'arrivée. On symbolise ce théorème par le schéma suivant, où i est l'inclusion de $\mathrm{Im} f$ dans $\mathbf{H}$.



1.2.16 Le sous-groupe engendré par $\mathbf{H}$ et $\mathbf{K}$ doit contenir l'ensemble $\mathbf{HK}$. Pour que ce soit un groupe, d'après l'exercice 1.1.23, il suffit de vérifier que, lorsque $\mathbf{H} \lhd \mathbf{G}$, on a $\mathbf{HK} = \mathbf{KH}$. Or,

$$\mathbf{HK} = \bigcup_{k \in \mathbf{K}} \mathbf{H}k = \bigcup_{k \in \mathbf{K}} k\mathbf{H} = \mathbf{KH}$$

1.2.17 $\mathbf{H}$ et $\mathbf{K}$ sont deux sous-groupes de $\mathbf{G}$. On suppose que $\mathbf{K} \lhd \mathbf{G}$. Rappelons d'abord que le groupe engendré par $\mathbf{H}$ et $\mathbf{K}$ est alors $\mathbf{HK}$ puisque $\mathbf{K}$ est normal dans $\mathbf{G}$. De plus, $\mathbf{K}$ est normal dans $\mathbf{HK}$, car il est normal dans le groupe plus grand $\mathbf{G}$; considérons alors la restriction à $\mathbf{H}$ de la projection de $\mathbf{G}$ sur $\mathbf{HK}/\mathbf{K}$:

$$\begin{array}{rccc} \phi : & \mathbf{H} & \to & \mathbf{HK}/\mathbf{K} \\ & h & \mapsto & h\mathbf{K} \end{array}$$

Alors ϕ est surjective, car $hk\mathbf{K} = h\mathbf{K} = \phi(h)$. Son noyau est défini par :

$$\mathrm{Ker}\,\phi = \{h \in \mathbf{H} / \; h\mathbf{K} = \mathbf{K}\} = \{h \in \mathbf{H} / \; h \in \mathbf{K}\} = \mathbf{H} \cap \mathbf{K}$$

Le premier théorème d'isomorphisme donne alors :

$$\mathbf{H}/\mathbf{H} \cap \mathbf{K} \cong \mathbf{HK}/\mathbf{K}$$

1.2.18 Soit p la projection de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$. Comme $\mathbf{K} \leqslant \mathbf{H} = \mathrm{Ker} p$, le théorème de factorisation montre qu'il existe un morphisme $\bar{p}$ défini par :

$$\begin{array}{rccc} \bar{p} : & \mathbf{G}/\mathbf{K} & \to & \mathbf{G}/\mathbf{H} \\ & g\mathbf{K} & \mapsto & g\mathbf{H} \end{array}$$

De plus, ce morphisme est surjectif, car p est surjectif. Enfin,

$$\mathrm{Ker}\{\bar{p}\} = \{g\mathbf{K} |\; g\mathbf{H} = \mathbf{H}\} = \{g\mathbf{K} |\; g \in \mathbf{H}\} = \mathbf{H}/\mathbf{K}$$

D'où, en appliquant le premier théorème d'isomorphisme,

$$(\mathbf{G}/\mathbf{K})/(\mathbf{H}/\mathbf{K}) \cong \mathbf{G}/\mathbf{H}$$

Ainsi, par exemple :

$$(\mathbb{Z}/12)/(3\mathbb{Z}/12) \cong \mathbb{Z}/3$$

1.2.19 Il suffit de trouver une injection de l'ensemble quotient $\mathbf{G}/\mathbf{H}\cap\mathbf{K}$ dans un ensemble fini. Soit en effet :

$$f : g(\mathbf{H}\cap\mathbf{K}) \mapsto (g\mathbf{H}, g\mathbf{K})$$

dont l'ensemble d'arrivée est l'ensemble fini $\mathbf{G}/\mathbf{H}\times\mathbf{G}/\mathbf{K}$. L'application est bien définie, car si $g' = gh$, où $h\in\mathbf{H}\cap\mathbf{K}$, alors $g\mathbf{H} = g'\mathbf{K}$ et $g\mathbf{K} = g'\mathbf{K}$. Elle est injective, car si $g\mathbf{H} = g'\mathbf{H}$ et $g\mathbf{K} = g'\mathbf{K}$, on a $g' = gh = gk$ où $h\in\mathbf{H}$ et $k\in\mathbf{K}$, ce qui donne $h = k\in\mathbf{H}\cap\mathbf{K}$.
Pour que l'inégalité soit stricte, il suffit de prendre $\mathbf{H} = \mathbf{K}$, deux sous-groupes non triviaux de $\mathbf{G}$. Pour un cas d'égalité, prendre, par exemple, $\mathbf{G} = \mathbb{Z}$, $\mathbf{H} = 2\mathbb{Z}$ et $\mathbf{K} = 3\mathbb{Z}$.

1.2.20 1)

$$\mathbf{H}x\mathbf{K} = \bigcup_{h\in\mathbf{H}} hx\mathbf{K} = \bigcup_{k\in\mathbf{K}} \mathbf{H}xk$$

prouve qu'une double classe est réunion de classes à gauche et de classes à droite. Pour montrer que les doubles classes partitionnent $\mathbf{G}$, il suffit de vérifier que la relation :

$$x\mathcal{R}y \iff \mathbf{H}x\mathbf{K} = \mathbf{H}y\mathbf{K} \iff \exists h\in\mathbf{H},\ \exists k\in\mathbf{K},\ y = hxk$$

est une relation d'équivalence, ce qui est immédiat.

2) On voit d'abord que l'application $hxk \mapsto hxkx^{-1}$ est une bijection (translation à droite) de la double classe $\mathbf{H}x\mathbf{K}$ vers l'ensemble $\mathbf{H}x\mathbf{K}x^{-1}$. Or, cet ensemble est de la forme $\mathbf{H}\mathbf{K}'$ où $\mathbf{K}'$ est un sous-groupe de $\mathbf{G}$, image de $\mathbf{K}$ par un automorphisme intérieur. On en déduit :

$$|\mathbf{H}x\mathbf{K}| = \frac{|\mathbf{H}||\mathbf{K}'|}{|\mathbf{H}\cap\mathbf{K}'|} = \frac{|\mathbf{H}||\mathbf{K}|}{|\mathbf{H}\cap\mathbf{K}'|}$$

car $\mathbf{K}$ et $\mathbf{K}'$ sont isomorphes et ont même cardinal. Comme $\mathbf{K}'$ dépend de x, les doubles classes ont en général des cardinaux différents, à cause du cardinal du dénominateur.

3) Si l'un des deux groupes, par exemple $\mathbf{K}$, est normal dans $\mathbf{G}$, les doubles classes sont de même cardinal car, dans ce cas, $\mathbf{K}' = \mathbf{K}$. Mais en fait, la notion de double classe est très simplifiée... puisqu'alors $\mathbf{H}x\mathbf{K} = \mathbf{H}\mathbf{K}x$ et que $\mathbf{H}\mathbf{K}$ est un sous-groupe dès que $\mathbf{K}\lhd\mathbf{G}$.

1.2.21 Un sous-groupe $\mathbf{H}$ est d'indice 2 s'il y a seulement deux classes à gauche ; ces classes sont donc $\mathbf{H}$ et $x\mathbf{H}$ où $x\notin\mathbf{H}$. Mais il y a également seulement deux classes à droites, qui sont donc $\mathbf{H}$ et $\mathbf{H}x$. La classe à gauche de x et la classe à droite sont donc toutes les deux le complémentaire de $\mathbf{H}$ et coïncident. $\mathbf{H}$ est donc normal dans $\mathbf{G}$.

1.3 PROBLÈMES

1.3.1 Sous-groupes caractéristiques, centre

Rappelons qu'une caractérisation possible d'un sous- groupe normal (ou distingué) dans $\mathbf{G}$ est qu'il est stable par tout automorphisme intérieur. On dit qu'un sous-groupe $\mathbf{H}$ est **caractéristique** dans $\mathbf{G}$ s'il est stable par tout automorphisme de $\mathbf{G}$. On note $\mathbf{H}\sqsubset\mathbf{G}$ pour dire que $\mathbf{H}$ est caractéristique dans $\mathbf{G}$, et, bien sûr, un sous-groupe caractéristique dans $\mathbf{G}$ est aussi normal dans $\mathbf{G}$.

1) Démontrer que :

$$\mathbf{H} \sqsubset \mathbf{K} \sqsubset \mathbf{G} \Rightarrow \mathbf{H} \sqsubset \mathbf{G}$$

Cette propriété, nous l'avons vu, n'est pas vraie pour la relation de « normalité ».

2) Démontrer que :

$$\mathbf{H} \sqsubset \mathbf{K} \lhd \mathbf{G} \Rightarrow \mathbf{H} \lhd \mathbf{G}$$

3) Si $\mathbf{G}$ est un groupe, on appelle **centre** de $\mathbf{G}$ l'ensemble des éléments de $\mathbf{G}$ qui commutent avec tous les éléments de $\mathbf{G}$. On le note $\mathcal{Z}(\mathbf{G})$ et l'on peut écrire :

$$\mathcal{Z}(\mathbf{G}) = \{z \in \mathbf{G} | \forall x \in \mathbf{G},\ xz = zx\}$$

Bien sûr le centre contient toujours e et est égal à $\mathbf{G}$ ssi $\mathbf{G}$ est commutatif. D'une certaine façon, la taille du centre mesure le degré de commutativité de $\mathbf{G}$.
Démontrer que le centre d'un groupe est toujours un sous-groupe caractéristique. Est-ce encore le cas des sous-groupes du centre ?

4) On note $\mathbf{G}'$ ou $D(\mathbf{G})$ le sous-groupe engendré par les **commutateurs**, c'est-à-dire les éléments de la forme $xyx^{-1}y^{-1}$. Démontrer que c'est un sous-groupe caractéristique de $\mathbf{G}$. Ce sous-groupe, appelé **groupe dérivé**, sera étudié plus longuement dans le chapitre 4. Il mesure également le degré de commutativité de $\mathbf{G}$, et est réduit au neutre quand $\mathbf{G}$ est commutatif.

5) On note $\mathbf{G}^n$ le sous-groupe de $\mathbf{G}$ engendré par les éléments de la forme x^n où $x \in \mathbf{G}$[1]. Démontrer que pour tout n ce sous-groupe est caractéristique.

6) Une notion encore plus forte est celle de **sous-groupe pleinement invariant** de $\mathbf{G}$. Ce sont les groupes qui sont invariants par tous les morphismes de $\mathbf{G}$ dans $\mathbf{G}$ (appelés parfois endomorphismes). Démontrer que les groupes $\mathbf{G}'$ et $\mathbf{G}^n$ sont pleinement invariants. On peut montrer que le centre d'un groupe n'est pas toujours pleinement invariant.

7) Quelle relation y a t-il entre le centre de $\mathbf{G}$ et le centre d'un de ses sous-groupes ?

8) Montrer que le centre de $\mathbf{GL}(n, \mathbb{K})$, groupe des matrices inversibles à coefficient dans le corps $\mathbb{K}$, est le groupe des matrices scalaires, c'est-à-dire de la forme λI où λ est un scalaire non nul. On pourra utiliser les matrices de la forme $T_{ij} = I + E_{ij}$ où I est la matrice identité et E_{ij} est la matrice dont tous les coefficients sont nuls, sauf le coefficient d'indices i, j qui est égal à 1.
Chercher le centre de $\mathbf{T}(2, \mathbb{K})$, groupe des matrices triangulaires supérieures et de $\mathbf{TU}(2, \mathbb{K})$, groupe des matrices triangulaires unipotentes. Généraliser à une dimension quelconque.

9) Soit ϕ l'application qui à $x \in \mathbf{G}$ associe i_x automorphisme intérieur. Montrer que c'est un morphisme de groupe. Déterminer son noyau. En déduire :

$$\mathbf{G}/\mathcal{Z}(\mathbf{G}) \cong \mathrm{Int}(\mathbf{G})$$

1. Cette notation est ambiguë. Dans un autre contexte, elle représente le produit cartésien de n exemplaires de $\mathbf{G}$.

1.3.2 Le groupe modulaire $\mathcal{M}$

Soit $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ l'ensemble des complexes prolongé d'un point supplémentaire, noté ∞. À toute matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ d'entiers relatifs vérifiant $ad - bc = 1$, on associe l'homographie $f = \phi(A)$, de $\hat{\mathbb{C}}$ dans lui-même définie par :

$$f(z) = \frac{az + c}{bz + d}$$

pour z n'annulant pas le dénominateur. On pose de plus :

$$f(\infty) = \frac{a}{b}, \qquad f(-\frac{d}{b}) = \infty \quad \text{si } b \text{ n'est pas nul ;} \qquad f(\infty) = \infty \text{ si } b = 0$$

1) Vérifier que l'on a bien défini ainsi une bijection, et que l'ensemble de ces bijections constitue un groupe. Ce groupe s'appelle le **groupe modulaire** et est noté $\mathcal{M}$. Il a une grande importance en arithmétique, dans la théorie des fonctions elliptiques...

2) On note $\mathbf{G} = \mathbf{SL}(2, \mathbb{Z})$ le groupe des matrices 2×2 à coefficients dans $\mathbb{Z}$ et de déterminant 1. Vérifier que l'application ϕ de $\mathbf{G}$ dans $\mathcal{M}$ définie ci-dessus est bien un morphisme de groupe. En chercher le noyau et déduire :

$$\mathcal{M} \cong \mathbf{SL}(2, \mathbb{Z})/\{I, -I\}$$

Le groupe $\mathcal{M}$ est aussi noté $\mathbf{PSL}(2, \mathbb{Z})$.

3) Notre objectif est de montrer que $\mathcal{M}$ est engendré par les bijections $t : z \mapsto z+1$ et $s : z \mapsto -\frac{1}{z}$. Vérifier que ce sont des éléments de $\mathcal{M}$. On notera $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ des représentants de ces éléments de $\mathcal{M}$ dans $\mathbf{SL}(2, \mathbb{Z})$. Déterminer l'ordre de S. Étudier le groupe engendré par T et montrer qu'il est isomorphe à $\mathbb{Z}$.

4) Soit A une matrice 2×2. Montrer que $T^k A$ se déduit de A par la règle suivante : la ligne 2 est inchangée, la ligne 1 est remplacée par elle-même plus k fois la ligne 2. Montrer que SA se déduit de A par la règle, les lignes 1 et 2 sont échangées, puis la ligne 1 est multipliée par -1. Examiner ce qui se passe pour AT^k et AS.

5) En utilisant l'algorithme d'Euclide, montrer que l'on peut multiplier à gauche une matrice A à coefficients dans $\mathbb{Z}$ par un produit de puissances de T et de puissances de S de sorte que la matrice obtenue soit triangulaire supérieure.

6) Montrer qu'une matrice de $\mathbf{SL}(2, \mathbb{Z})$ triangulaire supérieure est de la forme T^k ou S^2T^k où $k \in \mathbb{Z}$.

7) En déduire que $\mathbf{SL}(2, \mathbb{Z})$ est engendré par S et T, puis que $\mathcal{M}$ est engendré par s et t.

8) Effectuer l'algorithme décrit dans les deux dernières questions pour prouver que :

$$\begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix} = T^3 S^{-1} T^{-2} S T^3$$

On a montré que $\mathcal{M}$ est engendré par deux éléments, l'un s étant d'ordre 2, l'autre t d'ordre infini. On va montrer qu'il est engendré aussi par deux éléments d'ordre fini.

On définit l'homographie u par $u(z) = \dfrac{1}{1-z}$ et l'on note U la matrice $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ qui représente u. Vérifier que $u^3 = e$ et que $\mathcal{M}$ est engendré par u et s. Écrire l'homographie a de matrice A, en fonction de s et de u.

9) Montrer que tout élément m de $\mathcal{M}$ peut s'écrire :

$$m = s^{i_1} u^{j_1} s^{i_2} \dots s^{i_k} u^{j_k} \qquad (*)$$

où les i_ℓ sont égaux à 1 sauf i_1 qui peut être nul, les j_ℓ sont égaux à 1 ou 2, sauf j_k qui peut aussi être nul. On va montrer que cette écriture est unique.

10) On pose $x = su$ et $y = su^2$. Vérifier que ce sont les classes des matrices X et Y données par :

$$X = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

Montrer que l'ensemble M des matrices de la forme $X^{a_1} Y^{b_1} \dots X^{a_k} Y^{b_k}$ où les exposants sont des entiers naturels dont un au moins est strictement positif, ne contient que des matrices dont les termes diagonaux sont supérieurs à 1, les autres étant négatifs, l'un au moins strictement. En déduire qu'une écriture de la forme (*) ne peut donner l'identité que si $k = 1$ et $i_1 = j_1 = 0$. Conclure, en montrant que l'écriture (*) est unique.

Chapitre **2**

Exemples de groupes

2.1 GROUPES PRODUITS

Dans le chapitre 1, nous avons rencontré le groupe des entiers modulo n, noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/n$, ainsi que quelques autres groupes finis ou infinis. Pour enrichir notre panoplie, nous allons commencer par définir ce qu'on appelle les « groupes produits ».
On définit le produit de deux groupes $\mathbf{K}$ et $\mathbf{H}$ par :

$$\mathbf{K} \times \mathbf{H} = \{(k, h) |\ k \in \mathbf{K},\ h \in \mathbf{H}\}$$

C'est donc le « produit cartésien » des deux ensembles. On le munit de la loi :

$$(k, h)(k', h') = (kk',\ hh')$$

Il est facile de vérifier que cette loi est bien une loi de groupe.

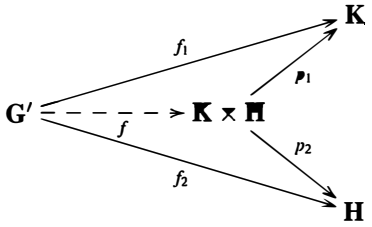
Exercice 2.1.1

Faire cette vérification. On note p_1 (resp. p_2) l'application de $\mathbf{K} \times \mathbf{H}$ dans $\mathbf{K}$ (resp. dans $\mathbf{H}$) définie par : $p_1(k, h) = k$ (resp. $p_2(k, h) = h$). Démontrer que ces applications, appelées **projections**, sont des morphismes de groupe. Comment définir le produit de n groupes, d'une famille de groupes ? Préciser alors les projections.

Exercice 2.1.2 (Propriété universelle du produit)

Soit $\mathbf{G} = \mathbf{K} \times \mathbf{H}$ et $\mathbf{G}'$ un groupe quelconque. Alors, si l'on se donne deux morphismes $f_1 : \mathbf{G}' \to \mathbf{K}$ et $f_2 : \mathbf{G}' \to \mathbf{H}$, il existe un seul morphisme $f : \mathbf{G}' \to \mathbf{G}$ tel que :

$$p_1 \circ f = f_1, \quad p_2 \circ f = f_2$$



Généraliser cette propriété à un produit quelconque de groupes. Elle est « universelle » en ce sens qu'elle caractérise le produit de groupes (à isomorphisme près). Le démontrer.

Exercice 2.1.3

Montrer que le produit de deux groupes commutatifs est commutatif. Est-ce que le produit de deux groupes cycliques est cyclique ?

Exercice 2.1.4 (Théorème des restes chinois)

Démontrer que :

$$\mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \ldots \times \mathbb{Z}/n_k \cong \mathbb{Z}/n_1 n_2 \ldots n_k$$

lorsque les entiers n_i sont premiers entre eux deux à deux. Préciser l'isomorphisme et son application réciproque.

Comme le théorème chinois le montre, un groupe donné peut être isomorphe à un produit. On dit alors qu'il est **décomposable**. C'est donc le cas des groupes $\mathbb{Z}/n$ quand n n'est pas premier et de $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ puisqu'ils sont isomorphes respectivement à $\mathbb{R}_+^* \times \{-1, 1\}$ et $\mathbb{R}_+^* \times \mathbb{U}$. La bijection, dans le second cas, est celle qui, à un complexe z, associe le couple $(z, e^{i\theta})$ où θ est un argument. Tout groupe décomposable en produit de deux groupes contient des sous-groupes isomorphes à ces groupes. Examinons de plus près cette situation.

Exercice 2.1.5

Soit $\mathbf{G} = \mathbf{K} \times \mathbf{H}$, muni de la structure produit. On pose $\mathcal{K} = \mathbf{K} \times \{e\}$, $\mathcal{H} = \{e\} \times \mathbf{H}$.

Montrer que :

a) $\mathcal{K}$ (resp. $\mathcal{H}$) est un sous-groupe de $\mathbf{G}$, isomorphe à $\mathbf{K}$ (resp. à $\mathbf{H}$).

b) $\mathcal{K}$ et $\mathcal{H}$ sont normaux dans $\mathbf{G}$.

c) $\mathcal{K} \cap \mathcal{H} = (e, e)$, élément neutre de $\mathbf{G}$.

d) $\mathbf{G} = \mathcal{K}\mathcal{H}$.

Énoncer une réciproque.

Regardons maintenant une généralisation de l'exercice précédent.

Exercice 2.1.6

Soit $(\mathbf{G}_i)_{i=1..n}$ une famille de sous-groupes normaux de $\mathbf{G}$, telle que :

$$\mathbf{G} = \langle \bigcup_{i=1..n} \mathbf{G}_i \rangle$$

Démontrer que $\mathbf{G}$ est isomorphe au produit des $\mathbf{G}_i$ ssi l'une des conditions suivantes est réalisée :

1) $\mathbf{G}_i \cap \langle \bigcup_{j \neq i} \mathbf{G}_j \rangle = \{e\}$ pour tout i.

2) Tout élément g de $\mathbf{G}$ s'écrit de façon unique comme produit $g = g_1 g_2 \dots g_n$ où $g_i \in \mathbf{G}_i$.

Exercice 2.1.7

Soit $\mathbf{G}$ un groupe commutatif fini dont tous les éléments différents du neutre sont d'ordre p (premier). Montrer que $\mathbf{G}$ est isomorphe au produit $\mathbb{Z}/p \times \mathbb{Z}/p \times \dots \times \mathbb{Z}/p$. Ce produit s'appelle **p-groupe élémentaire**.

Voici maintenant deux exemples de groupes définis à partir d'un produit cartésien, mais avec une opération différente.

Exercice 2.1.8

Soit $\mathbf{G}$ l'ensemble défini par $\mathbf{G} = \mathbb{Z}/2 \times \mathbb{Z}$. On définit dans $\mathbf{G}$ une opération $*$ par :

$$\begin{aligned} (a,b) * (a',b') &= (\overline{0},\ b+b'-1) \quad \text{si } a = a' = \overline{1} \\ &= (a+a',\ b+b') \quad \text{sinon.} \end{aligned}$$

Vérifier, qu'avec cette opération, $\mathbf{G}$ est bien un groupe commutatif, puis démontrer qu'il est isomorphe à $(\mathbb{Z}, +)$.

Exercice 2.1.9

Soit $\mathbf{G}$ l'ensemble défini par :

$$\mathbf{G} = \mathbb{Z}/n \times \mathbb{Z}/2$$

avec la loi suivante :

$$(a,b) * (a',b') = (a + (-1)^b a', b + b')$$

avec la convention que $(-1)^b$ sera 1 si $b = \overline{0}$ et -1 si $b = \overline{1}$.
Montrer que c'est bien un groupe. Quels sont les éléments d'ordre 2 ?
Reprendre l'étude avec l'ensemble :

$$\mathbf{G}' = \mathbb{Z} \times \mathbb{Z}/2$$

la loi étant définie par la même règle. Ces groupes s'appellent **groupes diédraux**, et sont notés respectivement $\mathbb{D}_{2n}$ et $\mathbb{D}_{\infty}$. On les retrouvera dans la section suivante.

Après ces deux exemples, on conviendra que la notation $\mathbf{G} \times \mathbf{H}$ représentera le produit de deux groupes muni de sa structure de produit direct. On choisira une autre notation lorsque la loi sera définie autrement. Passsons maintenant à une autre question : que peut-on dire des sous-groupes d'un groupe produit ?

Exercice 2.1.10

Démontrer que :

$$\mathbf{H} \leqslant \mathbf{G} \text{ et } \mathbf{H}' \leqslant \mathbf{G}' \Rightarrow \mathbf{H} \times \mathbf{H}' \leqslant \mathbf{G} \times \mathbf{G}'$$

puis que :

$$\mathbf{H} \lhd \mathbf{G} \text{ et } \mathbf{H}' \lhd \mathbf{G}' \Rightarrow \mathbf{H} \times \mathbf{H}' \lhd \mathbf{G} \times \mathbf{G}' \text{ et } (\mathbf{G} \times \mathbf{G}')/(\mathbf{H} \times \mathbf{H}') \cong (\mathbf{G}/\mathbf{H}) \times (\mathbf{G}/\mathbf{H}')$$

On a donc vu que le produit de sous-groupes est un sous-groupe du produit ; de tels sous-groupes sont appelés « sous-groupes rectangles ». Mais il y peut y avoir d'autres sous-groupes du produit qui ne sont pas de cette forme. L'essentiel sera vu dans un problème, contentons-nous d'un exemple.

Exercice 2.1.11

Chercher tous les sous-groupes de $\mathbb{Z}/4 \times \mathbb{Z}/4$, en précisant ceux qui sont « rectangles ».

Pour terminer, voici une autre construction d'un groupe à partir d'une famille de groupes, la somme directe de groupes.[1]

Exercice 2.1.12

Soit $(\mathbf{G}_i)_{i\in\mathcal{I}}$ une famille de groupes et soit $\mathbf{H}$ le sous-ensemble du produit formé des $(x_i)_{i\in\mathcal{I}}$ avec $x_i = e_i$ (élément neutre) sauf pour un nombre fini d'indices. Vérifier que $\mathbf{H}$ est un sous-groupe du produit $\prod_{i\in\mathcal{I}} G_i$. On le note parfois $\sum_{i\in\mathcal{I}} G_i$ et l'on l'appelle **somme directe** des groupes $\mathbf{G}_i$. Que dire si $\mathcal{I}$ est fini ? On définit les applications j_i par :

$$\begin{array}{rccc} j_i : & \mathbf{G}_i & \longrightarrow & \mathbf{H} \\ & a & \mapsto & x = (x_k)_{k\in\mathcal{I}} \end{array}$$

où $x_k = e_k$, élément neutre, pour tous les indices différents de i, et où $x_i = a$. Montrer que ce sont des morphismes injectifs.

Exercice 2.1.13

On considère un groupe $\mathbf{G}'$ commutatif et une famille de morphismes $(f_i)_{i\in\mathcal{I}}$ de chacun des $\mathbf{G}_i$ tous commutatifs dans $\mathbf{G}'$. Si $\mathbf{H}$ est la somme directe définie dans l'exercice précédent, montrer qu'il existe un unique morphisme f de $\mathbf{H}$ dans $\mathbf{G}'$ tel que $f \circ j_i = f_i$ pour tous les indices i.

SOLUTIONS

2.1.1 Les vérifications sont faciles. L'associativité par exemple résulte de :

$$\begin{array}{rcccl} (a,b)((a',b')(a'',b'')) & = & (a,b)(a'a'',\, b'b'') & = & (a(a'a''),\, b(b'b'')) \\ & = & ((aa')a'',(bb')b'') & = & ((a,b)(a',b'))(a'',b'') \end{array}$$

1. L'expression **somme** n'est pas heureuse. On parle parfois de « produit restreint ».

La projection p_1 est un morphisme :

$$p_1((a,b)(a',b')) = p_1(aa', bb') = aa' = p_1(a,b)p_1(a',b')$$

et l'on peut remarquer que c'est un morphisme surjectif, tout élément a de $\mathbf{K}$ est l'image de $(a, 1)$, par exemple.
Pour définir le produit d'une famille quelconque de groupes, $(\mathbf{G}_i)_{i\in\mathcal{I}}$, il suffit de prendre :

$$(g_i)_{i\in\mathcal{I}}(g'_i)_{i\in\mathcal{I}} = (g_i g'_i)_{i\in\mathcal{I}}$$

Les projections p_i sont définies par $p_i(g) = g_i$ où $g = (g_i)_{i\in\mathcal{I}}$, et le produit est noté $\prod_{i\in\mathcal{I}} G_i$.

> ***Remarque :*** l'ensemble des applications d'un ensemble X non vide dans un groupe est muni d'une structure de groupe par cette méthode. Cet ensemble n'est autre, en effet, que le produit d'une famille indexée par les éléments de X de groupes égaux à $\mathbf{G}$. On le note $\mathbf{G}^X$. Nous avons déjà rencontré $(\mathbb{Z}/2)^{\mathbb{N}}$, groupe des suites à valeurs dans $\mathbb{Z}/2$, comme exemple de groupe infini dont tous les éléments sont d'ordre fini.

2.1.2 Posons $f(g) = (f_1(g), f_2(g))$. On vérifie immédiatement que c'est un morphisme et que $p_1 \circ f = f_1$, de même $p_2 \circ f = f_2$. D'une certaine façon, f est le « produit » de f_1 et de f_2, et il est unique, sa définition ne peut être différente. On vérifie facilement que $\mathbf{G} = \mathbf{K} \times \mathbf{H}$ est le seul groupe ayant cette propriété. Si $\widetilde{\mathbf{G}}$ a la même propriété, on a alors deux projections π_1 et π_2 et il existe un morphisme f de $\widetilde{\mathbf{G}}$ dans $\mathbf{G}$ tel que $p_i \circ f = \pi_i (i = 1, 2)$, et d'un morphisme g de $\mathbf{G}$ dans $\widetilde{\mathbf{G}}$ tel que $\pi_i \circ g = p_i (i = 1, 2)$. Ainsi, $p_i \circ f \circ g = p_i$ pour $i = 1, 2$. Mais l'identité vérifie aussi cette égalité, et l'unicité anoncée ci-dessus donne $f \circ g = id$; de même en échangeant les rôles, et f est un isomorphisme.

2.1.3 $(g,h)(g',h') = (gg', hh') = (g'g, h'h) = (g',h')(g,h)$
De plus, le produit n'est commutatif que si les deux facteurs sont commutatifs, car le produit $\mathbf{G} \times \mathbf{H}$ contient comme sous-groupes $\mathbf{G} \times \{1\}$ et $\{1\} \times \mathbf{H}$. En revanche, le produit de deux groupes cycliques n'est pas toujours cyclique. Ainsi, $\mathbb{Z} \times \mathbb{Z}$ ne l'est pas car il contient un sous-groupe propre d'indice infini $(\mathbb{Z} \times \{0\})$. $\mathbb{Z} \times \mathbb{Z}/n$ ne l'est pas pour la même raison, avec le même exemple. Enfin, si $m \wedge n = d$ (i.e. le pgcd de n et m est d) alors les sous-groupes engendrés par $(\frac{n}{d}, 0)$ et $(0, \frac{m}{d})$ sont deux sous-groupes de même cardinal d de $\mathbb{Z}/n \times \mathbb{Z}/m$, qui sont distincts quand d est différent de 1 ; cela est contradictoire avec le fait qu'un groupe cyclique fini n'a qu'un seul sous-groupe de cardinal donné.
Reste à examiner le cas où $m \wedge n = 1$. Alors, le produit est cyclique ; en effet, considérons le morphisme :

$$\begin{array}{rccl} \phi & : \mathbb{Z} & \to & \mathbb{Z}/n \times \mathbb{Z}/m \\ & a & \mapsto & (\overline{a} \mod n, \overline{a} \mod m) \end{array}$$

c'est un morphisme « produit » des projections canoniques. Son noyau est formé des entiers multiples communs de m et de n, ce sont donc les multiples de mn puisque m et n sont premiers entre eux. On en déduit, par le premier théorème d'isomorphisme, un morphisme injectif de $\mathbb{Z}/mn$ dans $\mathbb{Z}/n \times \mathbb{Z}/m$. Ce morphisme est surjectif car les deux ensembles ont même cardinal.

2.1.4 On utilise le même « truc » que dans l'exercice précédent. Si ϕ est le morphisme qui, à l'entier a, associe $(\overline{a} \mod n_i)_{i=1..k}$, alors son noyau est formé des entiers qui sont multiples communs des n_i. Comme les n_i sont premiers entre eux deux à deux, leur ppcm est leur

produit (cela se démontre facilement en appliquant le théorème de Gauss). On obtient la surjectivité par l'étude des cardinaux. Un complément : il est possible de prouver la surjectivité directement ; les n_i étant premiers entre eux deux à deux, posons $n = n_1 n_2 \dots n_k$. Alors les $m_i = \frac{n}{n_i}$ sont premiers entre eux dans leur ensemble, ce qui implique qu'il existe des entiers u_i tels que :

$$\sum_{i=1}^{k} u_i m_i = 1$$

Mais alors

$$u_i m_i \equiv 1 \mod n_i \text{ pour tout } i, \quad u_i m_i \equiv 0 \mod n_j \text{ pour } i \neq j$$

et si l'on pose $x = \sum_{i=1}^{k} x_i u_i m_i$ alors on aura :

$$\forall i \in \{1, \dots, k\},\ x \equiv x_i \mod n_i$$

On a obtenu l'application réciproque demandée, et résolu des congruences simultanées par rapport à des entiers premiers entre eux deux à deux.

2.1.5 a) et b) Le plus rapide est d'observer que $\mathcal{K}$ est le noyau de la deuxième projection, $p_2 : (k, h) \mapsto h$, c'est donc un sous-groupe normal du produit. Quant à l'isomorphisme de $\mathcal{K}$ avec $\mathbf{K}$, c'est la restriction à $\mathcal{K}$ de la première projection.

c) Le seul élément commun est bien (e, e).

d) $(h, k) = (h, e)(e, k)$, donc $\mathbf{G} = \mathcal{K}\mathcal{H}$. On a également $\mathbf{G} = \mathcal{H}\mathcal{K}$, et, par ailleurs, tout élément de $\mathcal{K}$ commute avec tout élément de $\mathcal{H}$; ce qui n'implique pas que $\mathbf{G}$ soit commutatif.

Démontrons une réciproque, que l'on peut appeler **reconnaissance des produits directs internes**.

Si $\mathcal{H} \lhd G$, $\mathcal{K} \lhd G$, $\mathcal{K} \cap \mathcal{H} = \{e\}$, $\mathbf{G} = \mathcal{K}\mathcal{H}$ *alors* $\mathbf{G}$ *est isomorphe au produit* $\mathcal{K} \times \mathcal{H}$.

Montrons d'abord que tout élément k de $\mathcal{K}$ commute avec tout élément h de $\mathcal{H}$:

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

En utilisant le fait que $\mathcal{K}$ et $\mathcal{H}$ sont normaux dans $\mathbf{G}$, on voit que cet élément est à la fois dans $\mathcal{K}$ et dans $\mathcal{H}$, c'est donc e, et $hk = kh$. Maintenant définissons ϕ par :

$$\begin{array}{rccc} \phi : & \mathcal{K} \times \mathcal{H} & \to & \mathbf{G} \\ & (k, h) & \mapsto & kh \end{array}$$

On a :

$$\phi((k, h)(k'h')) = \phi(kk', hh') = kk'hh' = khk'h' = \phi((k, h))\phi((k', h'))$$

et ϕ est un morphisme. Il est bijectif car tout élément de $\mathbf{G}$ s'écrit sous la forme kh, c'est dans l'hypothèse, et le noyau est réduit au neutre car $kh = e$ prouve que k est l'inverse de h et est donc à la fois dans $\mathcal{K}$ et dans $\mathcal{H}$, c'est e.

2.1.6 1) Tout repose sur la propriété que $g_i g_j = g_j g_i$ dès que ces deux éléments sont dans des groupes $\mathbf{G}_i$ et $\mathbf{G}_j$ distincts. La démonstration est la même que pour l'exercice précédent. $g_i g_j g_i^{-1} g_j^{-1}$ est à la fois dans $\mathbf{G}_i$ et $\mathbf{G}_j$, et vaut donc e. Du fait que $\mathbf{G}$ est engendré par les

$\mathbf{G}_i$, on en déduit que tous les éléments de $\mathbf{G}$ peuvent s'écrire $g = g_1 g_2 \dots g_n$, en regroupant les élements provenant de chaque groupe. Enfin, si :

$$g_1 g_2 \dots g_n = g'_1 g'_2 \dots g'_n$$

où $g_i \in \mathbf{G}_i$, on peut écrire $g_1^{-1} g'_1$ comme élément du groupe engendré par les $\mathbf{G}_i$, pour $i \neq 1$, on a donc $g_1 = g'_1$ et ainsi de suite. C'est ici qu'on a besoin de l'hypothèse, et non de simples intersections deux à deux.

On peut alors définir une application de $\prod_{i=1..n} \mathbf{G}_i$ dans $\mathbf{G}$ par :

$$\phi(g_1, g_2, \dots, g_n) = g_1 g_2 \dots g_n$$

C'est un morphisme, grâce à la première propriété démontrée, il est surjectif par hypothèse, et injectif, par l'unicité vue ci-dessus.

2) Par rapport au cas précédent, il suffit de montrer que $g_i g_j = g_j g_i$. Pour cela, cherchons l'intersection de $\mathbf{G}_i$ avec $\mathbf{G}_j$. Soit x un élément de cette intersection, et écrivons :

$$x = ee \dots g_i \dots e = e \dots g_j \dots e$$

où g_i et g_j sont à leur place. L'unicité prouve que $\mathbf{G}_i \cap \mathbf{G}_j = \{e\}$, et l'on conclut comme ci-dessus.

2.1.7 Montrons que $\mathbf{G}$ est alors un $\mathbb{Z}/p$-espace vectoriel, et notons additivement l'opération dans $\mathbf{G}$. C'est un groupe commutatif. Pour définir la multiplication par un scalaire, posons pour commencer $k.g = g + g + \dots + g$ où il y a k exemplaires de g. Pour tout g d'ordre p, le résultat ne dépend pas de la classe modulo p. On peut poser $\overline{k}.g = k.g$ où $\overline{k}$ est la classe modulo p de k. Cette définition convient également lorsque g est nul. Pour terminer, remarquons que si $\mathbf{G}$ est fini, il est de dimension finie et donc isomorphe à $(\mathbb{Z}/p)^n$, en tant qu'espace vectoriel et donc en tant que groupe.

2.1.8 Soit $\mathbf{G}$ l'ensemble défini dans l'énoncé. L'opération $*$ est interne. On peut montrer « à la main » qu'elle définit bien une structure de groupe commutatif sur $\mathbf{G}$, mais il est plus économique de trouver directement l'isomorphisme avec $\mathbb{Z}$. Posons :

$$\phi(\overline{a}, b) = 2b - a$$

avec $a = 0$ ou $a = 1$. C'est bien une bijection, les éléments de la forme $(\overline{0}, b)$ sont envoyés sur les nombres pairs, ceux de la forme $(\overline{1}, b)$ sont envoyés sur les impairs. Montrons que c'est un morphisme :

$$\phi((\overline{a}, b) + (\overline{a'}, b')) = \phi(\overline{a} + \overline{a'}, b + b') = 2b + 2b' - a - a' = \phi(\overline{a}, b) + \phi(\overline{a'}, b')$$

si a et a' ne sont pas tous les deux égaux à 1.

$$\phi((\overline{1}, b) + (\overline{1}, b')) = \phi(\overline{0}, b + b' - 1) = 2b + 2b' - 2 = \phi(\overline{1}, b) + \phi(\overline{1}, b')$$

dans le dernier cas. C'est donc un isomorphisme de groupe ; toutes les propriétés de groupe sont vérifiées par « transport ». Cet exercice montre qu'il faut prendre garde qu'un ensemble, qui est un produit cartésien de groupes, n'est pas toujours muni de la structure produit ; ici, notre groupe $\mathbf{G}$ n'est pas isomorphe au groupe produit $\mathbb{Z}/2 \times \mathbb{Z}$.

2.1.9
$$\begin{aligned}((a,b)*(a',b'))\,(a'',b'') &= (a+(-1)^b a', b+b')*(a'',b'')\\ &= (a+(-1)^b a'+(-1)^{b+b'}a'', b+b'+b'')\\ (a,b)*((a',b')*(a'',b'')) &= (a,b)*(a'+(-1)^{b'}a'', b'+b'')\\ &= (a+(-1)^b(a'+(-1)^{b'}a''), b+b'+b'')\end{aligned}$$

Il y a bien égalité. On a utilisé le fait que lorsque $b \in \mathbb{Z}/2$, $(-1)^b$ est défini sans ambiguité, et que les règles de calcul habituelles sur les exposants restent valides. On trouve facilement que le neutre est $(\overline{0},\overline{0})$, et que :

$$(a,\overline{1})^{-1} = (a,\overline{1}) \quad \text{et} \quad (a,\overline{0})^{-1} = (-a,\overline{0})$$

On voit après ce calcul que tous les éléments de la forme $(a,\overline{1})$ sont d'ordre 2, ainsi que les couples $(a,\overline{0})$ pour a vérifiant $2a = 0$. Cela fait donc un élément supplémentaire lorsque n est pair.
Les mêmes calculs montrent que $\mathbf{G}'$ est un groupe dont les éléments d'ordre 2 sont les couples $(a,\overline{1})$.

2.1.10 $(h_1,h_1')(h_2,h_2')^{-1} = (h_1,h_1')(h_2^{-1},h_2'^{-1}) = (h_1h_2^{-1}, h_1'h_2'^{-1}) \in \mathbf{H}\times\mathbf{H}'$
prouve que le produit de sous-groupes est un sous-groupe. Pour la deuxième propriété, on considère l'application ϕ définie par :

$$\phi(a,b) = (a\mathbf{H}, b\mathbf{H}')$$

où $a \in \mathbf{G}$, $b \in \mathbf{G}'$. C'est un morphisme (car chaque « composante » est un morphisme), et le noyau est formé de $\mathbf{H}\times\mathbf{H}'$. L'application ϕ est surjective de $\mathbf{G}\times\mathbf{G}'$ sur $\mathbf{G}/\mathbf{H}\times\mathbf{G}'/\mathbf{H}'$, et l'on applique le théorème d'isomorphisme.

2.1.11 Nous noterons a la classe de a modulo 4.

1) Le seul groupe à un élément est $\{(0,0)\}$, il est rectangle.
2) Les groupes à deux éléments sont engendrés par des éléments d'ordre 2. On trouve les groupes :
$$\langle(2,0)\rangle, \langle(0,2)\rangle, \langle(2,2)\rangle$$
Les deux premiers sont rectangles, mais pas le troisième.
3) Les groupes à quatre éléments sont de deux types ; ceux qui sont cycliques sont engendrés par les éléments d'ordre 4. Il y en a six :
$$\langle(1,0)\rangle, \langle(0,1)\rangle, \langle(1,2)\rangle, \langle(2,1)\rangle, \langle(1,3)\rangle, \langle(1,1)\rangle$$
Les deux premiers sont rectangles. Le dernier s'appelle le sous-groupe diagonal. On trouve également un autre sous-groupe à quatre éléments, formés du neutre et de tous les éléments d'ordre 2 :
$$\{(0,0),\ (2,0),\ (0,2),\ (2,2)\}$$
Il est rectangle.
4) Il y a deux groupes à huit éléments qui sont rectangles, $\langle(2,0),(0,1)\rangle$ et $\langle(1,0),(0,2)\rangle$. On peut ajouter $\langle(1,1),(2,0)\rangle$ formé de tous les couples ayant même parité.
5) Le seul sous-groupe à seize éléments est $\mathbb{Z}/4\times\mathbb{Z}/4$. On compte ainsi quinze sous-groupes. Voir également le premier problème, à la fin de ce chapitre.

2.1.12 Le produit de deux éléments de $\mathbf{H}$ est encore dans $\mathbf{H}$: appelons **support** de h l'ensemble des indices pour lesquels $h_i \neq e_i$. Deux éléments de $\mathbf{H}$ ont un support fini, et leur produit a un support inclus dans la réunion des supports, ce support est donc fini. On voit également que ghg^{-1} a un support inclus dans celui de h, $\mathbf{H}$ est donc normal dans le groupe produit $\mathbf{G}$.
Les j_i sont des morphismes injectifs : $j_i(ab)$ est une famille $(x_k)_{k\in\mathcal{I}}$ où tous les x_k sont neutres sauf $x_i = ab$. Par définition de la loi produit, $j_i(ab) = j_i(a)j_i(b)$. On vérifie également l'injectivité. Les images des $\mathbf{G}_i$ sont des sous-groupes de $\mathbf{H}$, et $\mathbf{H}$ est engendré par ces images. Cette somme directe de groupe est très proche de la somme directe de sous-espaces vectoriels que l'on rencontre en algèbre linéaire.

2.1.13 Si $h \in \mathbf{H}$, on pose $f(h) = \prod_{i\in\mathcal{I}} f_i(h_i)$. Cette définition a un sens car ce produit est en réalité fini, seul un nombre fini des h_i étant différent du neutre.

2.2 GROUPES LIBRES, GROUPES DÉFINIS PAR GÉNÉRATEURS ET RELATIONS

Soit X un ensemble non vide. Première définition, informelle, du groupe libre engendré par X : c'est le « plus grand groupe » engendré par X. On le note $\mathbf{L}(X)$.

Exercice 2.2.1

Lorsque $X = \{x\}$, quel est $\mathbf{L}(X)$?

Dans le cas général, on définit $\mathbf{L}(X)$ de la façon suivante :

- On note X^{-1} un ensemble en bijection avec X, et disjoint de X. L'image de $x \in X$ est notée x^{-1}.
- $\mathcal{L}(X)$ est l'ensemble des suites finies d'éléments de $X \cup X^{-1}$, auquel on ajoute la suite vide, notée e. Ces suites sont appelées **mots**, et le nombre de symboles qui constituent un mot z s'appelle sa longueur, notée $l(z)$.
- On dit qu'un mot est **réduit** s'il ne contient aucune sous-suite formée de deux termes consécutifs de la forme xx^{-1} ou $x^{-1}x$, et l'on note $\mathbf{L}(X)$ l'ensemble des mots réduits.
- Soit alors l'opération $*$ définie par :

$$e * w = w * e = w$$

et

$$\text{si } w = a_1a_2\dots a_k,\ w' = b_1b_2\dots b_l,\ \text{alors } w * w' = a_1a_2\dots a_kb_1b_2\dots b_l$$

lorsque a_kb_1 n'est pas de la forme xx^{-1} ou $x^{-1}x$. Sinon, on applique l'opération à $a_1a_2\dots a_{k-1}$ et $b_2\dots b_l$ (avec cas particulier quand l'un est vide).

$\mathbf{L}(X)$ s'appelle le **groupe libre engendré par** X.

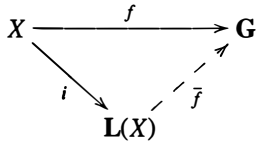
Exercice 2.2.2

Vérifier que c'est bien un groupe, montrer que X s'injecte dans $\mathbf{L}(X)$ et que $\mathbf{L}(X)$ est engendré par l'image de X (que l'on confondra avec X).

Voyons maintenant pourquoi le groupe obtenu est bien le « plus grand » engendré par X.

Exercice 2.2.3

Soit $\mathbf{G}$ un groupe et f une **application** de X dans $\mathbf{G}$. Montrer qu'il existe un seul morphisme $\bar{f}$ de $\mathbf{L}(X)$ dans $\mathbf{G}$ qui prolonge f. En déduire que tout groupe engendré par X est un quotient de $\mathbf{L}(X)$.



Certaines propriétés des groupes libres sont aisées à obtenir ; par exemple qu'un groupe libre est caractérisé par la propriété décrite dans l'exercice précédent ; de même, on vérifie que deux ensembles X et Y en bijection conduisent à des groupes libres isomorphes. Néanmoins, la structure d'un groupe libre, même engendré par un petit nombre d'éléments, est assez riche.

Exercice 2.2.4

Décrire les éléments de $\mathbf{L}(x, y)$. Montrer que $\mathbf{L}(x, y)$ contient des sous-groupes isomorphes à $\mathbf{L}(X)$ où X est n'importe quel ensemble fini ou dénombrable. On pourra utiliser les mots a_n définis par $a_n = x^n y^n$, pour n entier naturel.

Exercice 2.2.5

Soit encore le groupe libre $\mathbf{L}(x, y)$. Montrer que le groupe $\mathbf{H}$ engendré par x^2, y^2, xy, yx n'est pas librement engendré par ces éléments. Comment caractériser les éléments de $\mathbf{H}$?

Exercice 2.2.6

Combien y a t-il de mots réduits de longueur ℓ si X contient k éléments ?

Exercice 2.2.7

Montrer que tout élément (autre que e) d'un groupe libre est d'ordre infini. Vérifier également que si deux éléments d'un groupe libre commutent, ils sont puissances d'un même élément.

Voyons maintenant comment on définit un groupe « par générateurs et relations ». Si $\mathbf{G} = \mathbf{L}(X)$ est un groupe libre et $\mathcal{R}$ un ensemble de mots réduits, on appelle $\mathbf{H}$ le sous-groupe normal engendré par $\mathcal{R}$, et l'on note $\langle X|\mathcal{R}\rangle$ le groupe quotient $\mathbf{G}/\mathbf{H}$. On dit également que $\langle X|\mathcal{R}\rangle$ est une **présentation** de ce groupe quotient.

Exercice 2.2.8

Montrer qu'il existe bien un plus petit sous-groupe normal de $\mathbf{G}$ qui contient l'ensemble des mots de $\mathcal{R}$, ce qui justifie l'expression « sous-groupe normal » engendré par $\mathcal{R}$.

Exercice 2.2.9

Reconnaître le groupe $\mathbf{G} = \langle x, y \mid x \rangle$.

Lorsque $\mathcal{R}$ contient un mot comme xy^{-1}, on écrira $x = y$ à la place. Cela s'explique car dans l'ensemble quotient tous les éléments de $\mathcal{R}$ ont pour image l'élément neutre, et $xy^{-1} = e$ équivaut à $x = y$. On fait, bien sûr, l'abus de notation de confondre un mot avec sa classe.

Exercice 2.2.10

Reconnaître $\langle x \mid x^n = e \rangle$.

Tout groupe peut ainsi être défini par « générateurs et relations ». Il n'est pas toujours facile pour autant de reconnaître un groupe à partir d'une présentation. Voici une démarche possible.

Exercice 2.2.11 (Théorème de Von Dyck)

Soit $\mathbf{G} = \langle X|\mathcal{R} \rangle$ et $\mathbf{H} = \langle X|\mathcal{S} \rangle$. On suppose que $\mathcal{R} \subset \mathcal{S}$. Démontrer qu'on peut définir un morphisme surjectif de $\mathbf{G}$ sur $\mathbf{H}$ laissant fixes les éléments de X et dont le noyau est le sous-groupe normal engendré par les images dans $\mathbf{G}$ de $\mathcal{S} \setminus \mathcal{R}$.
Si maintenant $\mathbf{H}$ est un groupe engendré par Y en bijection avec X, et tel que toute relation de $\mathcal{R}$ ait pour image une relation satisfaite dans $\mathbf{H}$, alors la bijection s'étend en un morphisme surjectif de $\mathbf{G}$ sur $\mathbf{H}$.

Exercice 2.2.12

On désire démontrer que le groupe $\mathbf{G}$ de présentation $\langle x, y \mid x^2 = y^3 = e,\ xy = yx \rangle$ est le groupe cyclique $\mathbb{Z}/6$. Montrer qu'il existe un morphisme de $\mathbf{G}$ sur $\mathbb{Z}/6$. En utilisant les cardinaux, montrer que c'est un isomorphisme. Reconnaître également les groupes diédraux dans la présentation :

$$\langle x, y \mid x^n = y^2 = e,\ yxy = x^{-1} \rangle$$

et le groupe de Klein dans :

$$\langle x, y \mid x^2 = y^2 = xyx^{-1}y^{-1} = e \rangle$$

Exercice 2.2.13

Soit $\mathbf{G}$ le groupe défini par :

$$\mathbf{G} = \langle x, y \mid x^2 = y^2 = 1 \rangle$$

1) Montrer que **G** est infini et décrire ses éléments ; on montrera qu'il s'écrivent de façon unique sous une des formes suivantes :

$$(xy)^k,\ (yx)^k,\ (xy)^k x,\ (yx)^k x$$

2) Montrer que **G** contient une infinité d'éléments d'ordre 2.

3) Montrer que **G** est isomorphe au groupe diédral infini 2.1.9.

Exercice 2.2.14

Soit **G** le groupe défini par la présentation

$$\langle x, y, z \mid x^2 = y^3 = z^3 = xyz \rangle$$

1) Démontrer que xyz commute à tous les éléments de **G**, et identifier le quotient $\mathbf{G}/\langle xyz \rangle$.

2) Démontrer que **G** est d'ordre 24. Le groupe **G** s'appelle le groupe « binaire tétraédral ». Pour une généralisation, voir le problème du dernier chapitre.

Exercice 2.2.15

Démontrer que le groupe **G** de présentation :

$$\mathbf{G} = \langle x, y \mid xy = yx^2,\ yx = xy^2 \rangle$$

est réduit à l'élément neutre.

Exercice 2.2.16

Soit $\mathbf{B}_3$ le groupe défini par :

$$\mathbf{B}_3 = \langle x, y \mid xyx = yxy \rangle$$

C'est ce qu'on appelle un « groupe de tresses ». Montrer que ce groupe est isomorphe au groupe de présentation $\langle a, b \mid a^3 = b^2 \rangle$.

SOLUTIONS

2.2.1 C'est le plus « grand » groupe monogène, donc le groupe monogène infini, isomorphe à $\mathbb{Z}$.

2.2.2 L'inverse de $w = a_1 a_2 \dots a_k$ est $a_k^{-1} \dots a_2^{-1} a_1^{-1}$, en observant que $(x^{-1})^{-1} = x$ (il est bien réduit si w est réduit). L'élément neutre est le mot vide e. Reste à montrer l'associativité. Cela peut se faire en examinant à la main tous les cas correspondant aux simplifications possibles. $\mathbf{L}(X)$ contient, comme mots de longueur 1, tous les mots de la forme $w = x$ ou $w = x^{-1}$ où $x \in X$, d'où l'injection de X dans $\mathbf{L}(X)$.

2.2.3 Convenons que si $x \in X$, on pose $f(x^{-1}) = f(x)^{-1}$; alors si $w = a_1 a_2 \dots a_k$, il suffit de définir $\overline{f}(w) = f(a_1) f(a_2) \dots f(a_k)$. On vérifie que $\overline{f}$ est un morphisme de groupe de façon récursive.
Supposons maintenant que **G** est engendré par X, et que f est l'injection de X dans **G**. On définit le morphisme de $\mathbf{L}(X)$ dans **G**, comme-ci dessus, et ce morphisme est surjectif, car

tout élément de **G** s'écrit comme produit de puissances d'éléments de X et de leurs inverses ; il est donc l'image du mot correspondant de $\mathbf{L}(X)$. Le théorème d'isomorphisme assure donc que **G** est un quotient de $\mathbf{L}(X)$. D'où l'importance des groupes libres, leurs quotients sont des modèles de **tous** les groupes.

2.2.4 En convenant que le mot $xx\ldots x$ avec n termes s'écrit x^n, et avec une convention analogue pour les exposants négatifs, $\mathbf{L}(x, y)$ est formé des mots de la forme $x^{n_1}y^{m_1}x^{n_2}y^{m_2}\ldots x^{n_k}y^{m_k}$, les exposants étant des entiers relatifs non nuls, sauf éventuellement le premier et le dernier. On voit facilement qu'alors une telle écriture est unique, en procédant par récurrence sur la longueur. Le groupe engendré par $a_1, a_2, \ldots, a_l$ est un sous-groupe de $\mathbf{L}(x, y)$, qui est isomorphe à un groupe libre engendré par l éléments. En effet, tout produit $a_{i_1}^{\alpha_1}\ldots a_{i_k}^{\alpha_k}$ s'écrit sous la forme

$$x^{k_1}y^{p_1}x^{k_2}\ldots y^{p_n}$$

et l'on peut reconstituer le produit, de façon unique, à partir de cette forme réduite, si k_1 est non nul, il est positif, et le produit commençe par a_{k_1}. On fait alors apparaître y^{k_1}. Si k_1 est nul, p_1 est négatif et le produit commence par $a_{p_1}^{-1}$. Tout repose sur le fait que les seules simplifications possibles sont :

$$x^p y^p y^{-q}x^{-q} = x^p y^{p-q}x^{-q} \quad \text{et} \quad y^{-p}x^{-p}x^q y^q = y^{-p}x^{q-p}y^q$$

Le groupe engendré par tous les a_k est libre de base un ensemble dénombrable. Cela montre à quel point un groupe libre est « grand ».

2.2.5 Il y a une relation entre les quatre générateurs :

$$x^2(yx)^{-1}y^2 = xy$$

et donc le groupe en question, noté **H**, n'est pas isomorphe à un groupe libre engendré par quatre éléments. On constate que les éléments de **H** ont un nombre pair d'éléments dans leur écriture réduite. La réciproque est également vraie, et l'on peut démontrer que **H** est librement engendré par x^2, xy, y^2.

2.2.6 On dispose de $2k$ symboles, mais il ne faut pas que deux symboles consécutifs soient formés de x et x^{-1}. Pour $\ell > 0$ on trouve donc $2k(2k-1)^{\ell-1}$ mots.

2.2.7 Soit w un mot réduit de longueur $\ell = \ell(w)$. Alors le carré de w est de longueur $2\ell - 2k$, où k est le nombre de simplifications qui peuvent avoir lieu. Ainsi, avec $w = xyzy^{-1}x^{-1}$, de longueur 5, le carré est de longueur 6. Il suffit de montrer que $k < \frac{\ell(w)}{2}$ pour assurer $\ell(w^2) > \ell(w)$. Il y a une simplification si x_ℓ et x_1 sont inverses l'un de l'autre... et k simplifications si $x_{\ell-k+1}$ et x_k sont inverses. Ainsi, lorsque $\ell = 2n$, il y a n simplifications si x_{n+1} et x_n sont inverses ; c'est impossible car on part d'un mot réduit. On traite de même le cas impair. On a donc $\ell(w^2) > \ell(w)$, ce qui assure que w est d'ordre infini.
Supposons maintenant $ww' = w'w$. S'il n'y a aucune simplification dans chacun des produits, on voit facilement que w et w' sont puissances d'un même mot ; tout dépend de la différence des longueurs de w et w', en particulier, s'ils ont même longueur, $w = w'$. S'il y a une ou plusieurs simplifications, il faut procéder par récurrence sur la somme des longueurs.

2.2.8 On utilise le fait que l'intersection de sous-groupes normaux dans **G** est un sous-groupe normal dans **G**. Ainsi, le sous-groupe normal engendré par $\mathcal{R}$ est l'intersection des groupes normaux le contenant. Comme **G** est normal dans lui-même et contient $\mathcal{R}$, cette intersection est non vide et contient $\mathcal{R}$.

On peut caractériser ce sous-groupe (que l'on peut appeler **clôture normale** de $\mathcal{R}$), comme étant le sous-groupe engendré par les éléments de la forme grg^{-1} où g est quelconque dans $\mathbf{G}$, et $r \in \mathcal{R}$.

2.2.9 Le groupe engendré par x est le groupe monogène infini ; mais il n'est pas normal dans $\mathbf{L}(x, y)$. La clôture normale est le groupe $\mathbf{H}$ engendré par les mots de la forme wxw^{-1}. On doit alors identifier le groupe $\mathbf{L}(x, y)/\mathbf{H}$. On peut vérifier que c'est le groupe libre $\mathbf{L}(y)$, car $\mathbf{H}$ est le noyau du morphisme défini par $\phi(x) = 1$, $\phi(y) = y$. On a donc :

$$\langle x, y \mid x \rangle = \langle y \rangle$$

Bien sûr, dans ce cas particulier, la méthode « intuitive » fonctionne ; on remplace x par 1 dans les mots de $\mathbf{L}(x, y)$.

2.2.10 C'est le groupe cyclique d'ordre n. Le groupe normal $\mathbf{H}$ engendré par x^n est formé des x^{kn}, et le quotient $\mathbf{L}(x)/\mathbf{H}$ est isomorphe à $\mathbb{Z}/n$.

2.2.11 On sait que :

$$\mathbf{L}(X)/\mathbf{R} \cong \mathbf{G} \quad \text{et } \mathbf{L}(X)/\mathbf{S} \cong \mathbf{H}$$

où $\mathbf{R}$ et $\mathbf{S}$ sont les sous-groupes normaux engendrés par les relations $\mathcal{R}$ et $\mathcal{S}$. Puisque $\mathcal{R} \subset \mathcal{S}$, on a $\mathbf{R} \subset \mathbf{S}$. Il suffit d'appliquer le théorème de factorisation, il existe un morphisme surjectif de $\mathbf{L}(X)$ dans $\mathbf{H}$, de noyau $\mathbf{S}$. Ce morphisme se factorise donc en un morphisme surjectif de $\mathbf{G}$ sur $\mathbf{H}$. La deuxième partie de l'énoncé se traite de la même façon, il suffit de dire que l'hypothèse faite sur $\mathbf{H}$ implique que les relations, définissant $\mathbf{H}$ comme quotient d'un groupe libre, contiennent les relations $\mathcal{R}$.

2.2.12 1) On définit un morphisme surjectif de $\mathbf{G}$ dans $\mathbb{Z}/6$ en utilisant l'exercice précédent ; x doit avoir pour image un élément d'ordre 2, y un élément d'ordre 3, et ces images doivent commuter. On prendra par exemple $x \mapsto \overline{3}$ et $y \mapsto \overline{2}$, éléments qui engendrent bien $\mathbb{Z}/6$. Reste à voir que les éléments de $\mathbf{G}$ sont au maximum 6 ; il y a en effet e, x, y, y^2, xy, xy^2, les autres éléments se réduisant à l'un de ceux-là à l'aide des relations. On a donc bien un isomorphisme entre $\mathbf{G}$ et $\mathbb{Z}/6$.

2) Même démarche. Le groupe $\mathbb{D}_{2n}$ vu dans l'exercice 2.1.9 est engendré par les éléments $a = (1, 0)$ et $b = (0, 1)$ qui sont respectivement d'ordre n et 2. De plus, $bab^{-1} = (0, 1) * (1, 0) * (0, 1) = (-1, 1) * (0, 1) = (-1, 0) = a^{-1}$. Donc les éléments a et b satisfont les relations. Enfin, le cardinal de $\mathbb{D}_{2n}$ est $2n$, et dans le groupe $\langle x, y \mid x^n = y^2, yxy = x^{-1} \rangle$, les éléments sont, au plus, ceux de la liste

$$e, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y$$

puisque la relation $yx = x^{-1}y$ permet de mettre les puissances de x en tête de n'importe quel produit. Enfin pour le dernier groupe, on vérifie que $x \mapsto (1, 0)$ et $y \mapsto (0, 1)$ donnent un morphisme surjectif et l'on termine en utilisant le nombre des éléments.

2.2.13 1) Comme $x^2 = y^2 = 1$, toute puissance de x se réduit à x, de même pour y. Tout élément du groupe peut donc s'écrire comme une suite $...xyxy...$. Si la suite commence par x, elle sera de la forme $(xy)^k$ ou $(xy)^k x$ suivant la façon dont elle se termine. De même pour les suites commençant par y, et cette écriture est unique, avec k dans $\mathbb{N}$, $\mathbf{G}$ est donc infini. Pour $k = 0$, bien sûr, les deux premières formules donnent toutes deux e.

2) Les éléments de $\mathbf{G}$ qui sont de la forme $(xy)^k x$ ou $(yx)^k y$ sont d'ordre deux, comme le montre l'exemple suivant :

$$\big((xy)^3 x\big)^2 = (xyxyxy)x(xyxyxy)x = e$$

en utilisant $x^2 = y^2 = e$. On peut d'ailleurs faire le calcul général comme suit :

$$x(xy)^k x = (yx)^k = (y^{-1}x^{-1})^k = (xy)^{-k} \Rightarrow (xy)^k x = x^{-1}(xy)^{-k}$$

Il y a donc une infinité d'éléments d'ordre deux. Par ailleurs, xy et yx sont d'ordre infini, et inverse l'un de l'autre.

3) D'où l'isomorphisme avec $\mathbb{D}_\infty$:

$$\begin{cases} (xy)^k & \mapsto & (k,0) \\ (yx)^k & \mapsto & (-k,0) \\ (xy)^k x & \mapsto & (k,1) \\ (xy)^k y & \mapsto & (-k,1) \end{cases}$$

qui est une bijection et dont on vérifie aisément que c'est un morphisme.

2.2.14 1)

$$(xyz)x = x^2 x = xx^2 = x(xyz)$$

de même, xyz commute avec les autres générateurs (et leurs inverses) et est donc dans le centre de $\mathbf{G}$. Étudions le quotient par le groupe engendré par xyz. Il a pour présentation :

$$\langle x, y, z \mid x^2 = y^3 = z^3 = xyz = e \rangle = \langle y, z \mid y^3 = z^3 = (yz)^2 = e \rangle$$

Son nombre maximum d'éléments est 12. En effet, soit la liste :

$$1,\ y,\ y^2,\ z,\ z^2,\ yz,\ y^2z,\ yz^2,\ zy,\ zy^2,\ z^2y,\ yz^2y$$

elle représente tous les mots contenant au plus deux occurences de y et z, puisque $z^2y^2 = yz$ et $y^2z^2 = zy$. Il reste à vérifier à la main qu'il n'y a pas d'autres éléments possibles, en effectuant les produits de ces douze éléments par les générateurs[1]. Enfin, si $a = (1,2,3)$ et $b = (2,3,4)$ sont des 3-cycles du groupe alterné $\mathcal{A}_4$, on voit immédiatement qu'ils vérifient les relations $a^3 = b^3 = (ab)^2 = e$. Comme $\mathcal{A}_4$ a douze éléments, on a obtenu l'isomorphisme de $\mathbf{G}/\langle xyz \rangle$ avec $\mathcal{A}_4$.

2) Montrons que $\mathbf{G}$ a 24 éléments. Pour cela, il suffit de vérifier que xyz est d'ordre 2. Voici un exemple de calcul qui le montre ; il utilise les relations $y^2 = zyz$ et $z^2 = yzy$ issues de la présentation de $\mathbf{G}$:

$$y^4 = (zyz)(zyz) = zy^2zy^2z = z^2yz^3yz^2 = z^2y^5z^2 = yzy^7zy \Rightarrow y^2 = zy^7z = zyz$$

On en déduit $y = y^7$ donc $y^6 = e = (xyz)^2$. Comme $\langle xyz \rangle$ est d'indice 12, l'ordre de $\mathbf{G}$ est 24.

1. Il existe des méthodes systématiques pour obtenir la liste ci-dessus, voir par exemple [18].

2.2.15 Multiplions les deux relations entre elles

$$xy^2x = yx^3y^2$$

En utilisant $xy^2 = yx$ on en déduit :

$$yx^2 = yx^3y^2 \Rightarrow e = xy^2 = yx$$

Donc x et y sont inverses l'un de l'autre et une des deux relations donne $x = y = e$. Il n'est pas toujours facile de montrer qu'un groupe, dont on connaît la présentation, est réduit à l'élément neutre. On peut montrer qu'il n'y a pas d'algorithme général pour ce faire.

2.2.16 Posons $a = xy$ et $b = yxy$. Alors $a^3 = xyxyxy = (xyx)(yxy) = (yxy)^2 = b^2$. Réciproquement, on récupère x et y par $y = ba^{-1}$ et $x = a^2b^{-1}$. On vérifie alors $xyx = b = yxy$.

2.3 QUELQUES GROUPES FINIS

Nous avons déjà vu que :

- Les groupes à 1, 2, 3 , 5 et 7 éléments sont cycliques.
- Il y a deux groupes à quatre éléments, tous les deux commutatifs.
- Il y a un groupe à six éléments commutatif, et un non commutatif (qui est le plus petit groupe non commutatif).

Progressons dans notre étude en nous intéressant aux groupes ayant huit éléments.

Exercice 2.3.1

1) Décrire les groupes ayant huit éléments construits à l'aide des $\mathbb{Z}/n$

2) Le groupe diédral $\mathbb{D}_8$ est défini par :

$$\mathbb{D}_8 = \langle a, b \mid a^4 = b^2 = e,\ ba = a^3b \rangle$$

Vérifier qu'il correspond bien au groupe de l'exercice 2.1.9 Donner l'ordre de chacun des ses éléments.

3) Montrer que le groupe $\mathbb{H}_8$, appelé **groupe quaternionique** défini par :

$$\mathbb{H}_8 = \langle a, b \mid a^4 = e,\ b^2 = a^2,\ ba = a^3b \rangle$$

admet huit éléments. Quels sont les ordres de ses éléments ?

4) Montrer que les groupes précédents sont isomorphes aux groupes engendrés par les matrices :

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Exercice 2.3.2

Dresser le graphe des sous-groupes de $\mathbb{D}_8$, ainsi que ceux de $\mathbb{H}_8$. Préciser ceux qui sont normaux dans le groupe. On vérifiera, en particulier, que les sous-groupes de $\mathbb{H}_8$ sont tous normaux dans $\mathbb{H}_8$. Un tel groupe est appelé **hamiltonien**, du nom de l'inventeur des quaternions. Les groupes finis hamiltoniens sont tous connus.

N.B. On démontrera (3.4.1) qu'il n'y a pas d'autres groupes ayant huit éléments.

Exercice 2.3.3 (Une autre présentation de $\mathbb{H}_8$)

Soit $\mathbb{H}$ un $\mathbb{R}$-espace vectoriel de base $(1, i, j, k)$. On munit $\mathbb{H}$ d'une structure d'algèbre [1] par :

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$$

On convient bien sûr d'identifier $\mathbb{R}$ à la droite vectorielle engendrée par 1 qui, de plus, est l'élément neutre. Montrer que l'opération ainsi définie est associative ; on pourra faire toutes les vérifications ou montrer qu'il y a isomorphisme avec l'ensemble des matrices :

$$\left\{ z = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} / (a, b) \in \mathbb{C}^2 \right\}$$

Montrer que $\mathbb{H}$ est de plus un corps, non commutatif, contenant une infinité de corps isomorphes à $\mathbb{C}$. Montrer que $\mathbb{H}_8$ s'identifie à un sous-groupe multiplicatif de $\mathbb{H}$. En déduire une « version » matricielle (à coefficients dans $\mathbb{C}$, puis à coefficients dans $\mathbb{R}$) de $\mathbb{H}_8$.

Exercice 2.3.4 (Les groupes quaternioniques $\mathbb{H}_{2^n}$)

On appelle **groupe quaternionique** d'ordre 2^n le groupe défini par :

$$\mathbb{H}_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1,\ bab^{-1} = a^{-1},\ b^2 = a^{2^{n-2}} \rangle$$

Montrer que $\mathbb{H}_{2^n}$ admet la présentation plus simple :

$$\mathbb{H}_{2^n} = \langle a, b \mid bab^{-1} = a^{-1},\ b^2 = a^{2^{n-2}} \rangle$$

puis démontrer que $\mathbb{H}_{2^n}$ est de cardinal 2^n, et a pour modèle le groupe engendré par les matrices :

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

où ζ est une racine primitive 2^{n-1}-ième de l'unité. Vérifier qu'il n'y a qu'un élément d'ordre 2 ; déterminer le centre, ainsi que le quotient par le centre.

Exercice 2.3.5 (Les groupes dicycliques)

On appelle **dicyclique** un groupe qui a la présentation :

$$\mathbf{G} = \langle a, b, c \mid a^2 = b^2 = c^m = abc \rangle$$

1) Montrer que les groupes quaternioniques sont dicycliques. On commencera par montrer que $a^4 = 1$.

2) Démontrer qu'un groupe dicyclique est d'ordre $4m$, et donner l'ordre de ses éléments.

1. Une algèbre sur $\mathbb{R}$ est un espace vectoriel muni d'une multiplication « compatible » avec la structure d'espace vectoriel ; un exemple, l'algèbre des matrices carrées de dimension n.

3) Donner une version « matricielle » d'un groupe dicyclique. On s'inspirera de l'exercice 1.1.21

4) Reconnaître les groupes dicycliques pour $m = 1$, $m = 2$, $m = 3$.

SOLUTIONS

2.3.1 1) Les trois groupes $\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ sont des groupes à huit éléments ; ils ne sont pas isomorphes, il suffit pour s'en convaincre de considérer les éléments d'ordre 2. Nous verrons dans le chapitre 4 qu'il n'y a pas d'autre groupe commutatif ayant huit éléments.

2) La formule $ba = a^3b$, ainsi que l'ordre de a et de b permet de calculer tous les produits formés de puissances consécutives de a et de b. On voit alors que les éléments de $\mathbb{D}_8$ et de $\mathbb{H}_8$ sont e, a, a^2, a^3, b, ab, a^2b, a^3b. Et l'on obtient facilement les tables. Pour $\mathbb{D}_8$:

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Il y a un élément d'ordre un, e, deux éléments d'ordre quatre, a et a^3, et les cinq autres éléments sont d'ordre deux.

3) Pour $\mathbb{H}_8$:

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

Il y a, cette fois, un élément d'ordre un, e, un élément d'ordre deux seulement, a^2, les six autres sont d'ordre quatre. Ces considérations d'ordre prouvent que $\mathbb{D}_8$ et $\mathbb{H}_8$ ne sont pas isomorphes.

4) Il suffit de vérifier que les éléments a et b donnés par ces matrices satisfont aux conditions de chacune des définitions. On a ainsi une réalisation concrète de chacun des deux groupes.

Dès que le nombre d'éléments est un peu grand, la méthode d'étude qui consiste à écrire la table du groupe est inopérante. Il vaut mieux, par exemple pour prouver ou infirmer que deux groupes sont isomorphes, étudier l'ordre des éléments, ou l'architecture des sous-groupes. Mais cela ne suffit pas toujours.

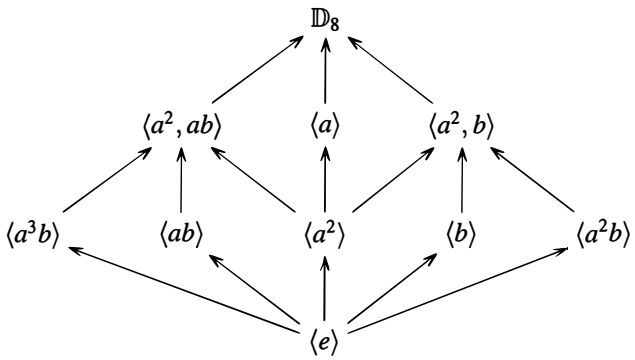
2.3.2 Pour déterminer les sous-groupes d'un groupe fini, il y a une méthode « systématique » mais parfois un peu fastidieuse. On considère les groupes engendrés par un élément (ils sont donc tous cycliques), puis on considère les sous-groupes obtenus en ajoutant un nouvel élément à tous ces sous-groupes, et ainsi de suite.
Dans le cas du groupe diédral, on obtient donc d'abord :

- Cinq sous-groupes à deux éléments engendrés par les cinq éléments d'ordre 2 ; ce sont :

$$\{e,b\},\{e,ab\},\{e,a^2b\},\{e,a^3b\},\{e,a^2\}$$

  Ils sont tous les cinq isomorphes à $\mathbb{Z}/2$.
- Un sous-groupe d'ordre 4 engendré par l'un des deux éléments d'ordre 4, (a ou a^3). C'est donc le groupe cyclique $\{e, a, a^2, a^3\}$ isomorphe à $\mathbb{Z}/4$.
- Deux sous-groupes d'ordre 4 obtenus en ajoutant a^2 à l'un des quatre premiers groupes de deux éléments. On obtient ainsi le groupe $\{e, a^2, b, a^2b\}$ et le groupe $\{e, a^2, ab, a^3b\}$. Ces deux groupes à quatre éléments ne sont pas cycliques (pas d'élément d'ordre 4) et sont donc isomorphes à $\mathbb{Z}/2 \times \mathbb{Z}/2$.

En ajoutant le groupe réduit à $\{e\}$ et $\mathbb{D}_8$ lui-même, on obtient donc dix sous-groupes, et tous les sous-groupes propres sont commutatifs.
Lesquels de ces groupes sont normaux dans $\mathbb{D}_8$? Les trois sous-groupes à quatre éléments le sont. Le groupe $\{e, a^2\}$ qui est le centre, est également normal dans $\mathbb{D}_8$, mais ce n'est pas vrai des autres. On obtient ainsi le schéma suivant :



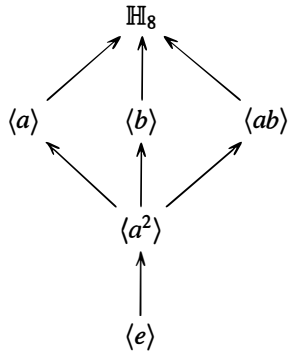
Dans le cas du groupe quaternionique :

- Un sous-groupe à deux éléments engendré par l'élément d'ordre deux $a^2 = b^2$; c'est $\{e, a^2\}$ isomorphe à $\mathbb{Z}/2$.
- Trois sous-groupes d'ordre quatre engendrés par l'un des six éléments d'ordre quatre. Ce sont : $\{e, a, a^2, a^3\}$, $\{e, b, a^2, a^2b\}$,$\{e, ab, a^2, a^3b\}$, tous les quatre sont isomorphes à $\mathbb{Z}/4$, et contiennent le groupe d'ordre deux qui est le centre.

Soit au total six sous-groupes. Il est remarquable que :

- tous ces sous-groupes propres sont commutatifs ;
- ils sont tous normaux dans $\mathbb{H}_8$.

Voici le graphe des sous-groupes :



2.3.3 La structure d'algèbre est bien définie par les produits des quatre éléments d'une base. On peut vérifier l'associativité de tous les produits comme $(ij)k = kk = -1$, $i(jk) = ii = -1$. Mais il est plus éclairant d'utiliser la bijection suggérée. Commençons par observer que l'ensemble des matrices est un $\mathbb{R}$-espace vectoriel de dimension 4 et engendré par les matrices :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

On vérifie que ces matrices vérifient les relations définissant les produits de i, j, k, la première étant associée à 1. Définissons donc la bijection en associant à ces quatre matrices les éléments $1, i, j, k$. On a ainsi un isomorphisme d'algèbre, l'associativité du produit de matrices se transporte dans $\mathbb{H}$. Pour être plus précis, la bijection s'écrit :

$$\begin{pmatrix} x+iy & z+it \\ -z+it & x-iy \end{pmatrix} \mapsto x + iy + jz + kt$$

Une matrice est inversible ssi son déterminant est non nul ; or ce déterminant est

$$|x+iy|^2 + |z+it|^2 = x^2 + y^2 + z^2 + t^2$$

donc non nul pour tout élément de $\mathbb{H}$ autre que le vecteur nul. De plus, l'inverse d'un élément de $\mathbb{H}$ est bien dans $\mathbb{H}$ et s'écrit :

$$q = x + iy + jz + kt \Rightarrow q^{-1} = \frac{x - iy - jz - kt}{x^2 + y^2 + z^2 + t^2}$$

et $\mathbb{H}$ est un corps non commutatif. On peut remarquer que si $\overline{q} = x - iy - jz - kt$, on a $q\overline{q} = x^2 + y^2 + z^2 + t^2$. De plus, cette conjugaison est l'image dans $\mathbb{H}$ de l'application $A \mapsto {}^t\overline{A}$ dans l'ensemble des matrices complexes, et en a les propriétés. D'après les propriétés de la multiplication, on voit que les sous-ensembles $\mathrm{vect}(1, i)$, $\mathrm{vect}(1, j)$ et $\mathrm{vect}(1, k)$ sont des corps isomorphes à $\mathbb{C}$, mais ce ne sont pas les seuls, tous les quaternions de la forme $q = yi + zj + tk$ ont un carré égal au réel $-y^2 - z^2 - t^2$, et $\mathrm{vect}(1, q)$ est alors un corps isomorphe à $\mathbb{C}$.
Si l'on considère maintenant l'ensemble $\{\pm 1, \pm i, \pm j, \pm k\}$, c'est un sous-groupe multiplicatif de $\mathbb{H}^*$, isomorphe à $\mathbb{H}_8$. On fait par exemple correspondre a à i et b à j. On trouve donc deux représentations matricielles de $\mathbb{H}_8$, celle issue de la définition de $\mathbb{H}$:

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

représentation qui ressemble à celle vue dans l'exercice précédent, et que nous retrouverons dans l'exercice suivant ; enfin, on peut aussi écrire :

$$i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

en utilisant la version matricielle des nombres complexes.

2.3.4 Montrons que la première relation se déduit des deux autres. Puisque $b^2 = a^{2^{n}-2}$, b commute avec $a^{2^{n}-2}$. On a donc

$$(bab^{-1})^{2n-2} = ba^{2n-2}b^{-1} = a^{2n-2} = a^{-2n-2} \Rightarrow a^{2n-1} = 1$$

Il est facile de voir que le groupe $\mathbf{G}$ a au plus 2^n éléments qui sont ceux du groupe cyclique $\langle a \rangle$ et ceux de la forme ba^k où k va de 0 à $2^{n-1} - 1$. En effet, $bab^{-1} = a^{-1}$ implique $ba^k = a^{-k}b$ et, par ailleurs, $b^2 = a^{2^{n}-2}$. On vérifie aisément que les matrices A et B satisfont les relations $A^{2^{n-1}} = I$, $B^2 = A^{2^{n-2}} (= -I)$, $BAB^{-1} = A^{-1}$. Comme ce groupe de matrices admet 2^n éléments, le théorème de Von Dyck assure qu'on a modélisé les groupes quaternioniques. Pour être plus précis, avec ce modèle,

$$A^k = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix} \qquad BA^k = \begin{pmatrix} 0 & \zeta^{-k} \\ -\zeta^k & 0 \end{pmatrix}$$

et, en particulier, $B^2 = A^{2^{n-2}} = -I$. Cherchons les éléments d'ordre 2 ; $(ba^k)^2 = ba^kba^k = ba^ka^{-k}b = b^2$, tous ces éléments sont d'ordre 4. Le seul élément d'ordre 2 est donc à chercher dans $\langle a \rangle$, c'est $a^{2^{n-2}} = b^2$. Quant au centre, cherchons si a^k commute avec $ba^{k'}$:

$$ba^{k'}a^k = a^kba^{k'} \iff ba^{k+k'} = ba^{k'-k}$$

seul donc convient $a^{2^{n-2}} = b^2$. On vérifie également qu'aucun élément de la forme ba^k n'est dans le centre qui est donc réduit à deux éléments. Pour identifier le quotient de $\mathbb{H}_{2^n}$ par son centre $Z(\mathbb{H}_{2^n})$, utilisons la présentation, les classes $\overline{a}$ et $\overline{b}$ vérifient :

$$\overline{a}^{2^{n-2}} = \overline{b}^2 = 1, \ \overline{b}\,\overline{a}\,\overline{b}^{-1} = \overline{a}^{-1}$$

on reconnaît la présentation du groupe diédral, $\mathbb{D}_{2^{n-1}}$, (qui a le bon nombre d'éléments).

2.3.5 1) Observons d'abord que $a = bc$ et donc $b^2 = bcbc$ d'où $bcb^{-1} = c^{-1}$. Faisons ensuite le calcul suivant :

$$c^m = b^2 = bb^2b^{-1} = bc^mb^{-1} = (bcb^{-1})^m = c^{-m}$$

On en déduit $c^{2m} = b^4 = e$, et que le groupe dicyclique admet la présentation :

$$\mathbf{G} = \langle b, c \mid c^{2m} = 1, \ c^m = b^2, \ bcb^{-1} = c^{-1} \rangle$$

Dans le cas où m est une puissance de 2, on retrouve les groupes quaternioniques.

2) En s'inspirant de l'exercice précédent, une liste exhaustive des $4m$ éléments de $\mathbf{G}$ sera :

$$1, c, c^2, \ldots, c^{2m-1}, b, bc, \ldots, bc^{2m-1}$$

3) Pour une version matricielle, prenons

$$C = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

où ω est une racine primitive $2m$-ième de l'unité.

4) Pour $m = 1$, les relations $c^2 = 1$, $c = b^2$, $bcb^{-1} = c^{-1}$ impliquent que le groupe est engendré par un élément b tel que $b^4 = 1$. On reconnaît le groupe cyclique $\mathbb{Z}/4$. Pour $m = 2$, c'est le groupe quaternionique à huit éléments. Enfin, pour $m = 3$, c'est le groupe T rencontré dans l'exercice 1.1.21.

2.4 GROUPES DE PERMUTATIONS

On note $\mathcal{S}_n$ l'ensemble des bijections de $\{1, 2, \ldots, n\}$ dans lui-même ; ses éléments sont aussi appelés **permutations**. Les groupes de permutations sont également appelés **groupes symétriques**. Ils sont à l'origine de la création de la théorie des groupes ; Évariste Galois les a introduits en étudiant les permutations des racines d'une équation polynomiale.
La convention que nous appliquons pour le produit de permutations est la convention habituelle de la composition d'applications ; on écrira parfois $\sigma\tau$ pour $\sigma \circ \tau$. Une permutation σ peut-être représentée de la façon suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

expression qui signifie que $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ et $\sigma(4) = 4$.

Exercice 2.4.1

Reconnaître les groupes symétriques $\mathcal{S}_1$, $\mathcal{S}_2$, et $\mathcal{S}_3$.

Exercice 2.4.2 (Décomposition en cycles)

1) On appelle **r-cycle**, où $r \in \{2, 3, \ldots, n\}$, une permutation c telle qu'il existe $(i_1, i_2, \ldots, i_r)$ entiers distincts pris dans $\{1, 2, \ldots, n\}$ et tels que :

$$c(i_1) = i_2,\ c(i_2) = i_3,\ \ldots,\ c(i_r) = i_1$$

tous les autres entiers étant invariants. Le r-cycle c est noté $c = (i_1, i_2, \ldots, i_r)$ et s'appelle aussi une **permutation circulaire**. Démontrer qu'un r-cycle est d'ordre r.

2) On appelle **support** du r-cycle c l'ensemble des entiers $\{i_1, i_2, \ldots, i_r\}$. Démontrer que si deux cycles ont des supports disjoints, alors ils commutent.

3) Démontrer que toute permutation est composée de façon unique de cycles de supports disjoints. On conviendra que l'identité est composée de 0 cycle.

4) Un exemple, soit σ la permutation de $\{1, 2, \ldots, n\}$ définie par, $\sigma(i) = n + 1 - i$. Donner sa décomposition en cycles.

Exercice 2.4.3

Démontrer que le r-cycle $c = (i_1, i_2, \ldots, i_r)$ est composé de $r - 1$ 2-cycles. En déduire que $\mathcal{S}_n$ est engendré par les 2-cycles (appelés **transpositions**).

Parlons maintenant de la **conjugaison** des permutations. On dit que σ et σ' sont conjuguées s'il existe une permutation ρ telle que $\sigma' = \rho \circ \sigma \circ \rho^{-1}$. Autrement dit, ce sont des

éléments images l'un de l'autre par un automorphisme intérieur. C'est clairement une relation d'équivalence. De façon intuitive, deux permutations sont conjuguées si elles représentent la même transformation à une bijection de $\{1, 2, \ldots, n\}$ près (à un « changement de repère près »). La notion de conjugaison sera approfondie et généralisée dès le chapitre suivant.

Exercice 2.4.4

1) On note $c = (i_1, i_2, \ldots, i_r)$ un cycle de longueur r. Étant donné σ élément quelconque de $\mathcal{S}_n$, montrer que :
$$\sigma \circ c \circ \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_r))$$
2) Donner une condition nécessaire et suffisante pour que deux permutations soient conjuguées.
3) Montrer que le nombre de classes de conjugaison de $\mathcal{S}_n$ est égal au nombre des partitions de n, i.e. le nombre de façons d'écrire n comme somme d'entiers.
4) Détailler les classes de conjugaison de $\mathcal{S}_n$ quand $n = 2, 3, 4, 5$ en précisant l'ordre de chaque élément.

La décomposition en cycles permet également d'étudier l'ordre des éléments d'un groupe symétrique.

Exercice 2.4.5

Quel est l'ordre d'une permutation dont on connaît la décomposition en cycles ? Quel est l'ordre maximal d'un élément de $\mathcal{S}_{20}$?

Exercice 2.4.6

Si p est premier, décrire tous les éléments d'ordre p du groupe $\mathcal{S}_n$. Les dénombrer. Si a_n est leur nombre, on pourra démontrer que :
$$\sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n = e^{x + \frac{x^p}{p}}$$

Exercice 2.4.7 (Étude des puissances d'un cycle)

Soit σ un r-cycle, montrer que σ^k est un cycle ou un produit de cycles de même taille. Déterminer alors cette taille. Réciproquement, si une permutation est produit de cycles disjoints de même taille, montrer que c'est la puissance d'un cycle.

Le groupe symétrique est engendré par les transpositions, mais ce n'est pas la seule possibilité.

Exercice 2.4.8

Montrer que $\mathcal{S}_n$ est engendré par chacun des ensembles suivants :

- les transpositions du type $(1, i)$;
- les transpositions du type $(i, i+1)$;
- le cycle $\sigma = (1, 2, \ldots, n)$ et la transposition $(1, 2)$.

Exercice 2.4.9

Est-ce que $\sigma = (1, 2, \ldots, n)$ et une transposition quelconque engendrent $\mathcal{S}_n$? On constatera que c'est faux pour $n = 4$, et on pourra montrer que c'est vrai lorsque n est premier.

La signature est un outil très important pour l'étude des permutations. Elle intervient chaque fois qu'une transposition de deux éléments amène un changement de signe, par exemple dans la théorie des déterminants en algèbre linéaire.

Exercice 2.4.10 (Signature)

1) Montrer que :

$$\begin{aligned}(ab)(ax_1x_2\ldots x_kby_1y_2\ldots y_l) &= (ax_1x_2\ldots x_k)(by_1y_2\ldots y_l)\\ (ab)(ax_1\ldots x_k)(by_1\ldots y_l) &= (ax_1\ldots x_kby_1\ldots y_l)\end{aligned}$$

en supposant que tous les éléments qui interviennent sont distincts.

2) On définit une application, nommée **signature** de $\mathcal{S}_n$ dans $\{-1, 1\}$ par :

$$\varepsilon(\sigma) = (-1)^{n-k}$$

où k est le nombre de cycles augmenté du nombre de points fixes de σ. Ce nombre k s'appelle le nombre d'orbites de σ : c'est le nombre des orbites dans l'action de $\langle\sigma\rangle$ sur l'ensemble $\{1..n\}$, voir le chapitre suivant. Ainsi, si σ est une transposition, $k = 1 + (n-2)$ car il y a un 2-cycle et $n-2$ points fixes. La signature d'une transposition est alors -1. Montrer que la signature est un morphisme.

3) Lorsque la signature est 1, on dit que la permutation est **paire**, impaire sinon. Quelle est la parité d'un r-cycle ? Comment trouver la parité connaissant la décomposition en cycles ?

4) On appelle **groupe alterné** le noyau de la signature ; c'est donc un sous-groupe distingué d'indice 2 de $\mathcal{S}_n$. On le note $\mathcal{A}_n$. Montrer qu'il est engendré par les 3-cycles (pour $n > 2$).

5) Démontrer que $\mathcal{A}_n$ est aussi engendré par les 3-cycles de la forme $(1, 2, i)$.

Exercice 2.4.11

Détailler le groupe alterné $\mathcal{A}_4$; en préciser notamment les sous-groupes. Lesquels sont normaux dans $\mathcal{A}_4$?

Exercice 2.4.12

Montrer que le centre de $\mathcal{S}_n$ est réduit à id pour $n > 2$.

Exercice 2.4.13

Soit σ un élément de $\mathcal{S}_n$. On suppose que dans sa décomposition en cycles, il y a k_i cycles d'ordre i, k_1 étant le nombre des points fixes.

1) Montrer que :

$$n = \sum_{i=1}^{n} i\,k_i$$

2) On définit :

$$\mathcal{C}_{\mathcal{S}_n}(\sigma) = \{g \in \mathcal{S}_n \;/\; g\sigma = \sigma g\}$$

(centralisateur de σ). Montrer que :

$$\text{Card}\left(\mathcal{C}_{\mathcal{S}_n}(\sigma)\right) = \prod_{i=1}^{n} i^{k_i} k_i!$$

Exercice 2.4.14

Soit $s(n,k)$ le nombre des permutations de $\mathcal{S}_n$ qui ont exactement k orbites. Montrer que :

$$\sum_{k=1}^{n} s(n,k)X^k = X(X+1)\ldots(X+n-1)$$

(ce sont les nombres de Stirling de première espèce). On démontrera et utilisera la relation de récurrence :

$$s(n+1,k) = s(n,k-1) + ns(n,k)$$

SOLUTIONS

2.4.1 $\mathcal{S}_1$ est le groupe trivial, $\mathcal{S}_2$ contient l'identité et la bijection échangeant 1 et 2, qui est d'ordre 2, il est bien sûr isomorphe au groupe cyclique $\mathbb{Z}/2$. Quant à $\mathcal{S}_3$, il a six éléments. C'est le groupe à six éléments qui n'est pas commutatif, voir 1.1.18. Il contient trois éléments d'ordre 2, les trois permutations qui échangent deux nombres et laissent fixe le troisième, deux éléments d'ordre 3 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

ainsi que l'identité.

2.4.2 1) Une récurrence immédiate montre que :

$$\text{pour } k \leqslant r \quad \begin{cases} c^k(i_l) = i_{k+l} & \text{si } k+l \leqslant r \\ c^k(i_l) = i_{k+l-r} & \text{si } k+l > r \end{cases}$$

On en déduit que pour ces valeurs de k, $c^k = e$ seulement si $k = r$. Un r-cycle est bien d'ordre r. On peut choisir d'écrire $c = (i_2, \ldots, i_r, i_1)$, etc. Il y a donc r façons d'écrire un cycle de support donné. On convient en général de mettre en tête le plus petit élément du support.

2) Il suffit d'utiliser que tout cycle laisse invariant un entier qui n'est pas dans son support.

3) Prenons une démarche algorithmique. Soit σ une permutation. On cherche l'image de 1, s'il n'est pas fixe on cherche l'image de cette image jusqu'à retrouver 1. Cela donne un premier cycle. Puis on prend le plus petit entier qui n'est pas encore apparu ; on cherche son image... et cela donne un nouveau cycle, de support disjoint du premier. Il reste à prouver l'unicité ; elle résulte de ce que les supports des cycles sont entièrement déterminés par σ, car tout cycle contenant un entier doit contenir toutes ses images successives par les puissances de σ (c'est ici qu'intervient notamment que les supports sont disjoints). Le même argument montre que le cycle correspondant à ce support est bien déterminé.

4) Cette permutation « renverse l'ordre » des entiers de 1 à n. Elle vérifie $\sigma \circ \sigma = \mathrm{id}$ de par sa définition même. Si n est impair, il y a un nombre invariant $\frac{n+1}{2}$ et σ se décompose en :

$$\sigma = (1,n)(2,n-1)(3,n-2)\dots(\frac{n-1}{2},\frac{n+3}{2})$$

si n est pair :

$$\sigma = (1,n)(2,n-1)(3,n-2)\dots(\frac{n}{2},\frac{n}{2}+1)$$

2.4.3 On vérifie immédiatement que :

$$(i_1,i_2,\dots,i_r) = (i_1,i_2)(i_2,i_3)\dots(i_{r-1},i_r)$$

(il y a d'autres solutions, et rappelons que l'on compose de la droite vers la gauche). Comme toute permutation est composée de cycles, on en déduit que $\mathcal{S}_n$ est engendré par les transpositions.

2.4.4 1) Si $i \neq \sigma(i_k)$, pour un entier k, alors $\sigma^{-1}(i)$ n'est pas dans l'ensemble $\{i_1,\dots,i_r\}$, et il est fixé par $c\,\sigma \circ c \circ \sigma^{-1}(i) = i$. Sinon, $\sigma^{-1}(i) = i_k$, et $\sigma \circ c \circ \sigma^{-1}(i) = \sigma(i_{k+1})$, ou $\sigma(i_1)$ si $k = r$. On a bien la relation demandée, facile à retenir, le conjugué de c est un r-cycle mais portant sur un ensemble « transporté » par σ. On appellera cela **principe de conjugaison**.

2) Deux permutations sont conjuguées ssi elles ont même structure dans leur décomposition en cycles. La question précédente, appliquée à un produit de cycles disjoints, le montre. Et si deux permutations sont de même structure, elles sont conjuguées. Ainsi, $(1,2)(3,4,5)$ est conjuguée de $(i,j)(k,l,m)$ par toute permutation qui transforme 1 en i, 2 en j, etc.

3) C'est une conséquence de la question précédente, en n'oubliant pas les points invariants. Ainsi, si $n = 7$, $7 = 1+1+2+3$ correspond à la classe de $(1,2)(3,4,5)$. Le nombre de partitions d'un entier n ne se calcule pas facilement... On peut, suivant Hardy et Ramanujan, donner l'équivalent quand n tend vers $+\infty$:

$$\frac{1}{4n\sqrt{3}}e^{\pi\sqrt{2n/3}}$$

4) Voilà le travail ! La « structure » indique les points fixes (chiffre 1) et les r-cycles (autres chiffres). On a indiqué la parité des permutations (notion définie un peu plus loin).

- Cas $n = 3$

Structure	Nombre de permutations	Ordre	Parité
1+1+1	1	1	paire
2+1	3	2	impaire
3	2	3	paire

- Cas $n = 4$

Structure	Nombre de permutations	Ordre	Parité
1+1+1+1	1	1	paire
2+1+1	6	2	impaire
3+1	8	3	paire
4	6	4	impaire
2+2	3	2	paire

- Cas $n = 5$

Structure	Nombre de permutations	Ordre	Parité
1+1+1+1+1	1	1	paire
2+1+1+1	10	2	impaire
3+1+1	20	3	paire
4+1	30	4	impaire
5	24	5	paire
2+2+1	15	2	impaire
3+2	20	6	paire

- Cas $n = 6$

Structure	Nombre de permutations	Ordre	Parité
1+1+1+1+1+1	1	1	paire
2+1+1+1+1	15	2	impaire
3+1+1+1	40	3	paire
4+1+1	90	4	impaire
5+1	144	5	paire
6	120	6	impaire
2+2+1+1	45	2	paire
2+3+1	120	6	impaire
2+4	90	4	paire
2+2+2	15	2	impaire
3+3	40	3	paire

Quelques explications complémentaires. L'ordre d'un cycle est le ppcm des ordres de chacun des cycles qui le composent, comme le prouve l'exercice suivant. Pour le dénombrement, on utilise par exemple que le nombre des p-cycles est $(p-1)!C_n^p$, en comptant les supports possibles, puis les images successives d'un nombre choisi dans ce support.

2.4.5 Soient r_i les ordres des cycles c_i formant une permutation σ et m leur ppcm. Alors $\sigma^m = id$ parce que $c_i^m = id$ et que ces cycles commutent. Réciproquement, si $\sigma^p = id$, alors pour chaque i, $c_i^p = id$. En effet, si x est dans le support de c_i, il est invariant par tous les autres cycles et $\sigma^p(x) = c_i^p(x)$. Comme $c_i(y) = y$ quand y n'est pas dans le support de c_i, on en déduit $c_i^p = id$. Ainsi, p doit être multiple commun des r_i. Dans le cas $n = 20$, il faut chercher le maximum du ppcm d'une partition de 20. Par tâtonnements, on trouve que c'est 420, issu de la partition $20 = 1 + 3 + 4 + 5 + 7$.

2.4.6 Une permutation sera d'ordre p ssi c'est un p-cycle ou un composé de p-cycles de supports disjoints ; de cette façon seulement p sera le ppcm des ordres. Sachant que le nombre des p-cycles est $(p-1)!C_n^p$, on trouve au total une expression :

$$a_n = (p-1)!C_n^p + \frac{1}{2!}(p-1)!^2 C_n^p C_{n-p}^p + \frac{1}{3!}(p-1)!^3 C_n^p C_{n-p}^p C_{n-2p}^p + \dots$$

la somme s'arrêtant à $E(n/p)$ termes au maximum (E désigne la partie entière). On peut simplifier ce résultat et l'écrire :

$$a_n = \sum_{0 \leqslant k \leqslant n/p} \frac{n!}{p^k k!(n-kp)!}$$

Démontrons maintenant que :

$$\sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n = e^{x+\frac{x^p}{p}}$$

Le plus direct est de partir du résultat :

$$e^{x+\frac{x^p}{p}} = e^x e^{\frac{x^p}{p}} = \sum_{k=0}^{\infty} \frac{x^k}{k!} \sum_{j=0}^{\infty} \frac{x^{pj}}{p^j j!} = \sum_{n=0}^{\infty} b_n \frac{x^k}{k!}$$

alors les b_n sont donnés par :

$$b_n = n! \sum_{k+pj=n} \frac{1}{k!j!p^j} = \sum_{0 \leqslant j \leqslant n/p} \frac{n!}{j!p^j(n-pj)!} = a_n$$

Une généralisation : le nombre $c_{n,m}$ des permutations de $\mathcal{S}_n$ vérifiant $\sigma^m = id$ vérifie :

$$\sum_{n=0}^{+\infty} \frac{c_n}{n!} x^n = \exp\left(\sum_{d|m} \frac{x^d}{d} \right)$$

2.4.7 Supposons $\sigma = (1, \dots, r)$. Alors $\sigma^k(1) = k+1 \pmod r$ (en prenant le représentant qui est dans $\{1, \dots, r\}$). Alors l'image de 1 sera dans un cycle de longueur d, si $(\sigma^k)^d(1) = 1 \pmod r$, avec d minimum. On trouve donc $d = \frac{r}{k \wedge r}$. Comme ce calcul marche bien sûr pour tous les autres, on en déduit que σ^r est constitué de $k \wedge r$ cycles de longueur $\frac{r}{k \wedge r}$. En particulier, les puissances d'un p-cycle sont toujours des p-cycles (ou id) si p est premier. Ces calculs sont à mettre en relation avec l'étude des groupes cycliques.
Réciproquement, donnons-nous un produit de p cycles disjoints de longueur q, avec $n > pq$. Avec les notations précédentes, on doit avoir $r = pq$ et $k = pq'$ où $q \wedge q' = 1$. Il y a donc au moins la possibilité de prendre $k = p$, et l'on construit facilement une solution parmi celles possibles. Ainsi, $(1,2,3)(4,5,6)(7,8,9)(10,11,12)$ est la puissance 4 de $(1,4,7,10,3,6,9,12,2,5,8,11)$ et de cinq autres, mais aussi la puissance 8 de $(1,4,7,10,3,6,9,12,2,5,8,11)$.

2.4.8 – Si ni i ni j ne sont égaux à 1, $(ij) = (1i)(1j)(1i)$. Le lecteur informaticien aura reconnu la procédure pour échanger le contenu de deux variables.
– Contentons-nous d'un exemple qui éclaire le cas général :

$$(1,5) = (1,2)(2,3)(3,4)(4,5)(3,4)(2,3)(1,2)$$

Voir le principe de conjugaison introduit dans l'exercice précédent.

– Il faut utiliser les puissances de $\sigma = (1, 2, \ldots, n)$. Comme σ^k transforme 1 en $k+1$, on a $\sigma^k \circ (1,2) \circ \sigma^{-k} = (k+1, k+2)$. On conclut, grâce à la question précédente.

2.4.9 Soit donc $\sigma = (1,2,3,4)$ et prenons $\tau = (1,3)$. Alors le groupe engendré n'est pas $\mathcal{S}_4$ mais le groupe diédral $\mathbb{D}_8$. On peut le voir en remarquant $\sigma^4 = \tau^2 = id$, $\tau \circ \sigma \circ \tau = \sigma^{-1}$, qui est la présentation du groupe diédral. Le groupe engendré est donc de cardinal inférieur à huit, on vérifie qu'il est bien égal à huit.
En revanche, si p est premier, et $\sigma = (1, 2, \ldots, p)$, alors n'importe quelle permutation $\tau = (i,j)$ unie à σ engendre $\mathcal{S}_p$. En fait, il suffit que si $d = j - i$, $d \wedge n = 1$. On le vérifie en étudiant les conjugués de (i,j) par σ^k, puis en conjuguant (i,j) avec $(j, j+d)$, ce qui donne $(i, j+d)$. En itérant, on voit bien qu'on obtient une transposition entre deux éléments consécutifs s'il existe k tel que $kd \equiv 1 \pmod{n}$.

2.4.10 1) Il suffit de suivre les images successives des éléments ; a donne x_1 qui donne... puis x_k redonne a par l'intermédiaire de a. De même, pour tous les autres, sans oublier que l'on compose de la droite vers la gauche.

2) Montrons que la signature est un morphisme. Soit σ une permutation, (a,b) une transposition, et considérons $\tau = (a,b)\sigma$. Il y a deux possibilités, a et b sont dans un même cycle dans la décomposition de σ, et la première formule de la seconde question montre que τ contient un cycle de plus que σ. Si a et b sont dans deux cycles disjoints, la seconde formule montre qu'il y a un cycle de moins. Et si a ou b sont fixés par σ, la seconde formule convient encore en convenant que la liste des x_i ou des y_i est vide. D'ailleurs, si a est fixe par σ, on peut écrire que σ contient le 1-cycle (a). Ainsi, $\varepsilon(\tau) = -\varepsilon\sigma = \varepsilon((a,b))\varepsilon(\sigma)$. Comme le groupe symétrique est engendré par les permutations, la preuve est complète.

3) Un r-cycle contient 1 cycle et $n - r$ points fixes. Sa signature est donc $(-1)^{r-1}$, elle est paire si... r est impair (pas de chance). Et pour un produit de cycles, il suffit d'utiliser le fait que la signature est un morphisme. Ainsi, les transpositions sont impaires, les doubles transpositions sont paires.

4) Les 3-cycles et leurs composés sont des permutations paires. Réciproquement, il suffit de considérer les produits de la forme $(a,b)(c,d)$ les quatre lettres représentant des éléments distincts. Or :

$$(a,b)(b,c) = (a,b,c) \qquad (a,b)(c,d) = (a,c,b)(a,c,d)$$

ce qui prouve que tout composé d'un nombre pair de transpositions est aussi composé de 3-cycles.

5) Il s'agit donc de fabriquer n'importe quel 3-cycle avec les n 3-cycles de la forme $(1,2,i)$. Prenons i,j,k distincts et distincts de 1 et 2. Le principe de conjugaison donne :

$$\begin{aligned}(1,2,i)(1,2,j)(1,2,i)^{-1} &= (i,j,2)\\ (1,2,i)(i,j,2)(1,2,i)^{-1} &= (1,j,i)\\ (1,2,k)(i,j,2)(1,2,k)^{-1} &= (i,j,k)\end{aligned}$$

2.4.11 Comme le montre le tableau de la réponse à l'exercice 2.4.4 (cas $n = 4$), $\mathcal{A}_4$ contient trois doubles transpositions, $u = (1,2)(3,4)$, $v = (1,3)(2,4)$ et $w = (1,4)(2,3)$. Il en résulte trois groupes d'ordre 2, inclus dans un groupe d'ordre 4 formé de l'identité et de ces trois doubles transpositions. Il est isomorphe au groupe de Klein $\mathcal{V}$. Il y a également huit 3-cycles, avec l'identité, le compte est bon. Chaque 3-cycle est d'ordre trois, et forme un groupe

cyclique avec son carré. Il y a ainsi quatre sous-groupes d'ordre 3 ; tout autre sous-groupe a deux générateurs. S'il contient deux 3-cycles dont l'un n'est pas le carré de l'autre, alors ces 3-cycles sont $(1,2,3)$ et $(1,2,4)$, à un changement de notation près, dont on sait qu'ils engendrent $\mathcal{A}_4$. Enfin, s'il contient un 3-cycle σ et une double transposition τ, il contient une autre double transposition $\sigma\tau\sigma^{-1}$, donc un sous-groupe d'ordre 4 et un sous-groupe d'ordre 3. D'après le théorème de Lagrange, il a au moins douze éléments, c'est $\mathcal{A}_4$. Remarquons que le groupe $\mathcal{A}_4$ est le plus petit qui donne un contre-exemple au théorème de Lagrange ; d'ordre douze, il n'a pas de sous-groupe d'ordre six. Les sous-groupes d'ordre deux ne sont pas normaux, comme le montre le calcul du conjugué d'une double transposition par un 3-cycle. Les sous-groupes d'ordre trois sont aussi conjugués deux à deux (images l'un de l'autre par un automorphisme intérieur), et ne sont pas normaux: En revanche, le groupe à quatre éléments est forcément normal dans $\mathcal{A}_4$, étant seul de son cardinal.

2.4.12 Soit σ un élément du centre de $\mathcal{S}_n$. Alors, si a et b sont deux entiers distincts, on doit avoir $(a,b)\sigma(a,b) = (\sigma(a),\sigma(b)) = \sigma$. La permutation σ doit donc fixer tous les autres entiers, et l'on a $\sigma(a) = a$,$\sigma(b) = b$ ou $\sigma(a) = b$,$\sigma(b) = a$. Dans le premier cas, σ est l'identité. Si le second était possible, soit c un autre entier (d'où $n > 2$), $(a,c)\sigma(a,c) = (\sigma(a),\sigma(c)) = \sigma$ prouverait que $\sigma(a) = c$, ce qui est absurde.

2.4.13 1) Pour la permutation σ, tout élément de l'ensemble $\{1,\ldots,n\}$ est soit fixe, et contribue dans k_1, soit fait partie du support d'un i-cycle. Ces supports étant disjoints, les éléments concernés sont au nombre de $i \times k_i$, d'où la formule.

2) Supposons que τ commute avec σ. Soit $(a_1,a_2,\ldots,a_k)$ un k-cycle de σ, et notons $b_i = \tau(a_i)$. Alors :

$$\sigma(b_i) = \sigma\tau(a_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1} \text{ et } \sigma(b_k) = b_1$$

et donc $(b_1,b_2,\ldots,b_k)$ est un k-cycle de σ, τ transforme le support d'un k-cycle de σ en un k-cycle de σ. Réciproquement, construisons τ de la façon suivante :

- pour chaque i, on choisit une des $k_i!$ permutations des i-cycles de σ ;
- pour chaque i-cycle, il faut choisir l'image d'un élément, mettons a, dans le support d'un autre i-cycle ; cela ce fait de i façons, et l'image des autres est alors déterminée, car :

$$\tau(\sigma^k(a)) = \sigma^k(\tau(a))$$

Il est alors facile de vérifier qu'une telle permutation commute bien avec σ. Le nombre des choix possibles est donc :

$$\text{Card}\left(\mathcal{C}_{\mathcal{S}_n}(\sigma)\right) = \prod_{i=1}^{n} i^{k_i} k_i!$$

Attention, dans ce qui précède, il faut tenir compte des points fixes. Si σ est une transposition, la formule donne $2(n-2)!$ permutations, ce qu'on vérifie facilement.

2.4.14 1) Montrons la relation de récurrence. Si l'on ajoute un $n+1$-ième élément, les permutations ayant k cycles se partitionnent en deux :

- celles pour lesquelles cet élément est fixe, il y en a $s(n,k-1)$;

– les autres ; elles sont obtenues en insérant le nouvel élément dans un des cycles. Or cela peut se faire de r façons différentes dans un r-cycle. Comme la somme des longueurs des cycles est n, il y a n façons de prolonger une permutation des n premiers éléments. On a donc :

$$s(n+1,k) = s(n,k-1) + ns(n,k)$$

Cette formule convient pour $k = 1$ également, si l'on considère que $s(n,0) = 0$.

On peut initialiser cette relation en dénombrant les permutations circulaires :

$$s(n,1) = \frac{n!}{n} = (n-1)! ;$$

on constate également que $s(n,n) = 1$. Voici la table des premières valeurs des $s(n,k)$ que l'on obtient :

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 11 & 6 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
24 & 50 & 35 & 10 & 1 & 0 & 0 & 0 & 0 & 0 \\
120 & 274 & 225 & 85 & 15 & 1 & 0 & 0 & 0 & 0 \\
720 & 1764 & 1\,624 & 735 & 175 & 21 & 1 & 0 & 0 & 0 \\
5\,040 & 13\,068 & 13\,132 & 6\,769 & 1\,960 & 322 & 28 & 1 & 0 & 0 \\
40\,320 & 109\,584 & 118\,124 & 67284 & 22\,449 & 4\,536 & 546 & 36 & 1 & 0 \\
362\,880 & 1\,026\,576 & 1\,172\,700 & 723\,680 & 269\,325 & 63\,273 & 9\,450 & 870 & 45 & 1
\end{bmatrix}$$

2) Montrons maintenant la formule demandée, par récurrence sur n et posons

$$g_n(X) = \sum_{k=1}^{n} s(n,k)X^k$$

Alors :

$$\begin{aligned}
g_{n+1}(X) &= \textstyle\sum_{k=1}^{n+1} s(n+1,k)X^k \\
&= \textstyle\sum_{k=1}^{n} s(n,k-1)X^k + n\sum_{k=0}^{n} s(n,k)X^k + X^{n+1} \\
&= \textstyle\sum_{k=0}^{n-1} s(n,k)X^{k+1} + ng_n(X) + X^{n+1} \\
&= X(g_n(X) - X^n) + ng_n(X) + X^{n+1} \\
&= (X+n)g_n(X)
\end{aligned}$$

En tenant compte de $g_0(X) = 1$, on obtient bien :

$$\sum_{k=1}^{n} s(n,k)X^k = X(X+1)\dots(X+n-1)$$

2.5 PROBLÈMES

2.5.1 Les sous-groupes d'un produit

Soit $\mathbf{G} = \mathbf{H} \times \mathbf{K}$, muni de la structure de produit direct. Dans ce problème, on recherche tous les sous-groupes de $\mathbf{G}$. On conviendra d'identifier $\mathbf{H}$ avec le sous-groupe de $\mathbf{G}$ qui s'écrit $\mathbf{H} \times \{1\}$, de même pour $\mathbf{K}$.

1) Soit $\mathbf{L}$ un sous-groupe de $\mathbf{G}$. Si p_1 et p_2 sont les deux projections, on note :

$$\mathbf{L}_1 = \mathbf{L} \cap \mathbf{H}, \quad \mathcal{L}_1 = p_1(\mathbf{L})$$

$$\mathbf{L}_2 = \mathbf{L} \cap \mathbf{K}, \quad \mathcal{L}_2 = p_2(\mathbf{L})$$

Démontrer que :

$$\mathbf{L}_1 \lhd \mathcal{L}_1 \leqslant \mathbf{H} \qquad \text{et} \qquad \mathbf{L}_2 \lhd \mathcal{L}_2 \leqslant \mathbf{K}$$

2) Montrer que :

$$\mathcal{L}_1/\mathbf{L}_1 \cong \mathcal{L}_2/\mathbf{L}_2$$

3) On étudie maintenant une réciproque. Soient quatre groupes $\mathbf{L}_1, \mathcal{L}_1, \mathbf{L}_2, \mathcal{L}_2$ tels que :

$$\mathbf{L}_1 \lhd \mathcal{L}_1 \leqslant \mathbf{H} \qquad \text{et} \qquad \mathbf{L}_2 \lhd \mathcal{L}_2 \leqslant \mathbf{K}$$

et tels qu'il existe un isomorphisme θ :

$$\theta : \mathcal{L}_1/\mathbf{L}_1 \to \mathcal{L}_2/\mathbf{L}_2$$

Montrer qu'on peut alors construire un sous-groupe $\mathbf{L}$ de $\mathbf{G}$ tel que les quatre groupes $\mathbf{L}_1, \mathcal{L}_1, \mathbf{L}_2, \mathcal{L}_2$ soient issus de $\mathbf{L}$ comme dans la première question.

4) Dans la situation précédente, quand un sous-groupe de $\mathbf{G}$ est-il rectangle ?

5) *Applications.* Vérifier les résultats obtenus dans l'exercice 2.1.11 sur les sous-groupes de $\mathbb{Z}/4 \times \mathbb{Z}/4$. Que peut-on dire des sous-groupes de $\mathbb{Z}/p \times \mathbb{Z}/p$ lorsque p est premier ?

6) Rechercher les sous-groupes de :

a) $\mathbb{Z} \times \mathbb{Z}$

b) $\mathbb{Z}/2 \times \mathbb{Z}/6$

c) $\mathcal{S}_3 \times \mathcal{S}_3$

2.5.2 Les groupes de Prüfer

Soit p un nombre premier. On note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité (dans le corps des nombres complexes $\mathbb{C}$).

1) Rappeler pourquoi $\mathbb{U}_n$ est un groupe pour le produit.

2) On appelle ***p*-groupe de Prüfer** l'ensemble

$$\mathbb{U}_{p^\infty} = \bigcup_{k=0..\infty} \mathbb{U}_{p^k}$$

Vérifier que c'est un groupe pour le produit et que les $\mathbb{U}_{p^k}$ forment une suite croissante de sous-groupes.

3) Soit **H** un sous-groupe strict de $\mathbb{U}_{p^\infty}$. Démontrer que l'ensemble des ordres des éléments de **H** est fini, et en déduire que **H** est un des $\mathbb{U}_{p^n}$.

4) Démontrer que le quotient de $\mathbb{U}_{p^\infty}$ par $\mathbb{U}_{p^k}$ est isomorphe à $\mathbb{U}_{p^\infty}$.

5) Trouver un autre modèle (additif) du p-groupe de Prüfer.

6) Examiner l'ensemble des endomorphismes de $\mathbb{U}_{p^\infty}$.

7) Regardons maintenant un autre exemple de groupe construit suivant le même principe. On note $\mathcal{S}_{(\mathbb{N})}$ le groupe formé des bijections σ de $\mathbb{N}^*$ telles que $\sigma(i) = i$ pour tout i suffisamment grand. Démontrer que $\mathcal{S}_{(\mathbb{N})}$ est un groupe.

8) Pour chaque n, on considère l'ensemble des σ de $\mathcal{S}_{(\mathbb{N})}$ telles que :

$$\forall i > n,\ \sigma(i) = i$$

Montrer que cet ensemble est un groupe isomorphe à $\mathcal{S}_n$, que l'on notera encore $\mathcal{S}_n$. Vérifier que $\mathcal{S}_{(\mathbb{N})}$ est l'union des $\mathcal{S}_n$.

9) Montrer que l'on peut « prolonger » la signature et définir un groupe alterné $\mathcal{A}_{(\mathbb{N})}$ normal dans $\mathcal{S}_{(\mathbb{N})}$. Montrer que c'est un groupe simple.

10) Soit **K** le sous-groupe de $\mathcal{S}_{(\mathbb{N})}$ engendré par les transpositions $\tau_i = (2i-1, 2i)$, pour $i \in \mathbb{N}^*$. Le décrire et vérifier qu'il est commutatif.

Chapitre **3**

Actions de groupes Groupes de Sylow

Une **action** d'un groupe $\mathbf{G}$ sur un ensemble X est une « loi externe », c'est-à-dire une application ϕ :

$$\begin{array}{rcl} \phi : \mathbf{G} \times X & \to & X \\ (g, x) & \mapsto & g.x \end{array}$$

qui vérifie :

$$\forall g, g' \in \mathbf{G},\ \forall x \in X, \qquad g'.(g.x) = (g'g).x$$
$$\forall x \in X, \qquad e.x = x$$

On peut présenter cette notion différemment, en disant qu'une action est un morphisme Φ de $\mathbf{G}$ dans le **groupe symétrique** de X, c'est-à-dire le groupe des bijections de X dans lui-même. Pour retrouver alors la première définition, on écrit : $\Phi(g)(x) = \phi(g, x) = g.x$. La notion d'action de groupe est très présente en théorie des groupes, mais aussi en géométrie, algèbre linéaire... Elle fournit plus généralement un langage unifié et très parlant pour beaucoup de situations mathématiques.

Exercice 3.1.1

Montrer qu'un groupe $\mathbf{G}$ agit sur lui-même par :

$g.x$	$=$	gx	translation à gauche
$g.x$	$=$	xg^{-1}	translation à droite
$g.x$	$=$	gxg^{-1}	automorphisme intérieur

Dans quel(s) cas $\Phi(g)$ est-il toujours un automorphisme de $\mathbf{G}$? On dit alors que c'est une **action par morphismes**

Quelques définitions :

1. Si $x \in X$, son **orbite**, notée $\mathbf{G}x$ est définie par :
$$\mathbf{G}x = \{y \in X / \exists g \in \mathbf{G},\ y = g.x\}$$
Le mot orbite fait image, penser à l'orbite d'un point du plan lorsque $\mathbf{G}$ est le groupe des rotations de centre O.
2. Si $x \in X$, son **stabilisateur**, souvent noté $\mathbf{G}_x$ est défini par :
$$\mathbf{G}_x = \{g \in \mathbf{G} / \ g.x = x\}$$
3. Le **noyau** de l'action est l'ensemble des éléments de $\mathbf{G}$ tels que, pour tout x de X, $g.x = x$. C'est bien sûr le noyau de Φ. Une action est dite **fidèle** si son noyau est réduit au neutre. Ce cas est fréquent, et $\mathbf{G}$ est alors isomorphe à un sous-groupe du groupe symétrique de X (ou est même un sous-groupe de ce groupe symétrique).

Exercice 3.1.2

Montrer que le stabilisateur d'un élément de X est toujours un sous-groupe de $\mathbf{G}$. Comment décrire le noyau d'une action à l'aide des stabilisateurs ? Montrer que si une action n'est pas fidèle, on peut définir une action de $\mathbf{G}/\operatorname{Ker}\Phi$ qui le sera.

Exercice 3.1.3

Montrer que les orbites d'une action forment une partition de X. Décrire les orbites et les stabilisateurs pour les actions de translation à gauche et d'automorphisme intérieur de l'exercice 3.1.1.

Exercice 3.1.4

Soient $\mathbf{G} = \mathbf{GL}(n, \mathbb{K})$ et $X = \mathcal{M}_n(\mathbb{K})$. $\mathbf{G}$ agit sur X par « automorphisme intérieur » (c'est un prolongement de la définition) :
$$P.M = PMP^{-1}$$
Que sont les orbites ? Les décrire dans le cas particulier de $\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$.

Exercice 3.1.5

L'action que nous avons définie est une action « à gauche » ; on peut également définir une action à droite. Examiner ce qui change (en particulier, ce que deviennent translations et automorphismes intérieurs).

Exercice 3.1.6

Soit $\mathcal{E}$ un espace vectoriel. On peut y définir des formes bilinéaires symétriques ϕ. Définir une action *à droite* de $\mathbf{GL}(\mathcal{E})$ sur l'ensemble noté $\mathcal{L}_2(\mathcal{E})$ des formes bilinéaires. En se plaçant en dimension finie et dans le cas des formes bilinéaires symétriques, quelles sont les orbites de cette action ? On répondra dans le cas réel et dans le cas complexe.

Exercice 3.1.7

Soit **G** un groupe agissant sur un ensemble X. Dans quelles conditions et comment obtient-on une action dans les cas suivants :

- Un sous-groupe de **G** sur X.
- **G** sur un sous-ensemble de X.
- **G** sur $\mathcal{P}(X)$, ensemble des sous-ensembles de X.
- $\mathbf{G} \times \mathbf{G}$ sur X.
- **G** sur $X \times X$.
- $\mathbf{H} \times \mathbf{G}$ sur Y^X.

Pour le dernier cas, on suppose que **H** agit sur Y et l'on rappelle que Y^X désigne l'ensemble des applications de X dans Y.

Exercice 3.1.8

Décrire des actions de $\mathcal{S}_n$ sur :

- $\mathbb{E}^n$ où $\mathbb{E}$ est un ensemble quelconque.
- $\mathbb{K}[X_1, X_2, \ldots, X_n]$, anneau des polynômes à n indéterminées sur un corps $\mathbb{K}$. Quels sont alors les polynômes qui sont seuls dans leur orbite ? Donner des exemples où l'orbite contient un élément, deux éléments, trois éléments...

Soit $X = \mathcal{M}_n(\mathbb{K})$. On peut faire agir le groupe symétrique $\mathcal{S}_n$ en permutant lignes ou colonnes. Voici une vision différente.

Exercice 3.1.9

1) Si $\sigma \in \mathcal{S}_n$, on pose $P_\sigma = (p_{ij})$ où

$$p_{ij} = \delta_{i\sigma(j)}$$

On rappelle que δ_{ij} vaut 1 si $i = j$ et 0 sinon.
Vérifier que l'ensemble **P** des matrices de cette forme est un groupe isomorphe à $\mathcal{S}_n$. On les appelle **matrices de permutation**.

2) Montrer que **P** agit sur $\mathcal{M}_n(\mathbb{K})$ par translation à gauche. Comment caractériser cette action ? Que dire de matrices qui sont dans une même orbite ?

3) Comment décrire la multiplication à droite par une matrice de permutation ?

Il existe une relation entre **G**, l'orbite $\mathbf{G}x$ d'un élément et $\mathbf{G}_x$ son stabilisateur. C'est le point de départ d'une étude qui montre que, finalement, toute action de groupe se traduit entièrement dans le groupe **G**.

Exercice 3.1.10

On considère le quotient $\mathbf{G}/\mathbf{G}_x$, qui n'est pas un groupe en général, car le stabilisateur d'un élément n'est pas forcément normal.

1) Montrer que l'application :

$$\begin{array}{rccc} f: & \mathbf{G}/\mathbf{G}_x & \to & \mathbf{G}x \\ & g\mathbf{G}_x & \mapsto & g.x \end{array}$$

est bien définie et est bijective.

2) Vérifier ce résultat sur l'exemple simple suivant. Soit $\mathbf{G}$ le groupe engendré par les deux applications :

$$g : z \mapsto 1 - z,\ h : z \mapsto \frac{1}{z}$$

considérées comme des bijections de $X = \mathbb{C} \setminus \{0, 1\}$. Vérifier qu'il a six éléments. Lorsqu'on le fait opérer sur X, décrire les orbites et les stabilisateurs.

Exercice 3.1.11

Soit $\mathbf{G}$ un groupe agissant sur deux ensembles X et Y. On dit que les deux actions Φ et Ψ sont **isomorphes** s'il existe une bijection f de X sur Y telle que :

$$\forall g \in \mathbf{G},\ f \circ \Phi(g) = \Psi(g) \circ f$$

Ce qui peut se schématiser :

$$\begin{array}{ccc} X & \xrightarrow{\Phi(g)} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[\Psi(g)]{} & Y \end{array}$$

Autrement dit, en notant par un point les deux actions,

$$\forall g \in \mathbf{G},\ f(g.x) = g.f(x)$$

Démontrer que, dans la première question de l'exercice précédent, f est un isomorphisme d'actions.

En conclusion : toute action de groupe se réduit à des actions sur des orbites, et chacune de ces actions est isomorphe à l'action de $\mathbf{G}$ sur un ensemble quotient $\mathbf{G}/\mathbf{H}$. Pour être complet :

Exercice 3.1.12

1) Soient x et y deux éléments de X qui sont dans la même orbite. Comparer leurs stabilisateurs respectifs.

2) Soient $\mathbf{H}$ et $\mathbf{H}'$ deux sous-groupes de $\mathbf{G}$. Montrer que les actions de $\mathbf{G}$ sur les quotients $\mathbf{G}/\mathbf{H}$ et $\mathbf{G}/\mathbf{H}'$ sont isomorphes si et seulement si $\mathbf{H}$ et $\mathbf{H}'$ sont conjugués, c'est-à-dire s'il existe $g \in \mathbf{G}$ tel que $\mathbf{H} = g\mathbf{H}'g^{-1}$.

Exercice 3.1.13

Soit $\mathbf{SL}(2, \mathbb{R})$ le groupe « unimodulaire » des matrices 2×2 à coefficients réels et de déterminant égal à 1. Montrer qu'il opère sur le demi-plan de Poincaré par :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} .z = \frac{az + c}{bz + d}$$

Quel est le stabilisateur de i ? Et son orbite ? (Le demi-plan de Poincaré est l'ensemble des complexes de partie imaginaire strictement positive).

Exercice 3.1.14 (Formule des classes)

Dans cet exercice, on suppose que X est fini. On considère un ensemble Ω d'éléments de X tel que toute orbite rencontre Ω en un seul point ; on dit parfois que Ω est une **transversale**. Démontrer que :

$$|X| = \sum_{x \in \Omega} \frac{|\mathbf{G}|}{|\mathbf{G}_x|}$$

En théorie des groupes, voici une importante application de la « formule des classes ». On dit qu'un groupe fini $\mathbf{G}$ est un p-groupe (p premier) si son cardinal est une puissance de p. L'exercice qui suit donne une propriété des centres des p-groupes.

Exercice 3.1.15

On considère un groupe $\mathbf{G}$ qui agit sur lui-même par automorphisme intérieur.

1) Si $x \in \mathcal{Z}(\mathbf{G})$ (centre de $\mathbf{G}$), quelle est l'orbite de x ?

2) Montrer que :

$$|\mathbf{G}| = |\mathcal{Z}(\mathbf{G})| + \sum_{x \in A} \frac{|\mathbf{G}|}{|\mathbf{G}_x|}$$

où A est une transversale pour l'ensemble des orbites non réduites à un point.

3) En déduire que tout groupe de cardinal p^n où p est premier a un centre non trivial (i.e. ne contenant pas que l'élément neutre). Comme le centre est un sous-groupe normal, on en déduit qu'un p-groupe non commutatif n'est jamais simple.

Exercice 3.1.16

Une action est dite **doublement transitive** si chaque fois qu'on se donne deux couples (x, y) et (x', y') de X, avec $x \neq y$ et $x' \neq y'$, il existe $g \in \mathbf{G}$ tel que $x' = g.x$ et $y' = g.y$.

1) Donner des exemples d'actions doublement transitives. On utilisera des espaces vectoriels ou des espaces affines.

2) Démontrer que si une action est doublement transitive, tous les stabilisateurs sont des sous-groupes maximaux.[1]

3) Comment définir des actions multiplement transitives ? Soit $\mathbf{G}$ le groupe linéaire d'un espace vectoriel $\mathcal{E}$ de dimension deux ; montrer qu'il agit triplement transitivement sur les droites vectorielles mais pas quadruplement.

4) Montrer que si la dimension est trois, alors le groupe linéaire agit doublement transitivement mais pas triplement... Examiner son action sur les plans vectoriels. En dimension finie quelconque ?

1. Un sous-groupe $\mathbf{H}$ est **maximal** dans $\mathbf{G}$ s'il n'existe aucun sous-groupe strictement compris entre $\mathbf{H}$ et $\mathbf{G}$.

Exercice 3.1.17 (Formule de Burnside)

Soit $\mathbf{G}$ un groupe fini agissant sur un ensemble fini X. On note N le nombre des orbites, et $\mathrm{Fix}(g)$ l'ensemble des points fixes de g (i.e. des x tels que $g.x = x$). Montrer :

$$N = \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} |\mathrm{Fix}(g)|$$

Pour cela, on dénombrera l'ensemble des couples (g, x) où $g.x = x$ de deux façons différentes.

Exercice 3.1.18

Un exemple d'application. Une roue de loterie est partagée en n secteurs ; chacun d'eux est colorié d'une couleur parmi p couleurs différentes. Quel est le nombre des roues de loterie possibles, sachant qu'on ne distingue pas deux coloriages s'ils se déduisent l'un de l'autre par rotation ? On modélisera la situation en considérant qu'un coloriage est une application de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$ et en faisant agir le groupe des rotations. On peut commencer par des cas particuliers, $(n = 4, 5, 6)$. La formule à obtenir est :

$$\frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) p^d$$

où $\phi(d)$ est le nombre des entiers de $\{1, \ldots, d\}$ qui sont premiers avec d.

SOLUTIONS

3.1.1 $g.(g'.x) = g.(g'x) = gg'x = (gg').x$ $\qquad e.x = ex = x$

$g.(g'.x) = g.(xg'^{-1}) = xg'^{-1}g^{-1} = x(gg')^{-1} = (gg').x$ $\qquad e.x = xe^{-1} = x$

$g.(g'.x) = g.(g'xg'^{-1}) = gg'xg'^{-1}g^{-1} = (gg')x(gg')^{-1} = gg'.x$ $\qquad e.x = exe^{-1} = x$

S'agit-il d'une action par morphismes ? Ce n'est pas le cas des translations à droite ou à gauche, (*cf.* l'image de l'élément neutre) ; En revanche, $gxx'g^{-1} = gxg^{-1}gx'g^{-1}$ prouve que l'action par automorphisme intérieur est une action par morphisme.

3.1.2 Si g et g' sont dans le stabilisateur de x, alors $(gg').x = g.(g'.x) = g.x = x$, et $g^{-1}.x = g^{-1}.(g.x) = x$ prouvent que $\mathbf{G}_x$ est stable par le produit et par la prise d'inverse. C'est donc un sous-groupe de $\mathbf{G}$; (il contient au moins e).
Le noyau d'une action, formé de tous les g tels que, pour tout x, $g.x = x$, est l'intersection de tous les stabilisateurs. Enfin, si une action n'est pas fidèle, c'est que Φ n'est pas un morphisme injectif de $\mathbf{G}$ dans le groupe symétrique de X. Le premier théorème d'isomorphisme assure alors qu'on peut définir un morphisme injectif de $\mathbf{G}/\mathrm{Ker}\,\Phi$ dans le groupe symétrique de X.

3.1.3 Les orbites forment une partition de X. Il suffit pour cela de vérifier que la relation :

$$x \mathcal{R} y \iff \exists g \in \mathbf{G},\ y = g.x$$

est une relation d'équivalence (associée à l'action), ce qui n'offre aucune difficulté.
Pour la translation à gauche, il n'y a qu'une seule orbite. En effet, si x et y sont dans $\mathbf{G}$, $y = (yx^{-1})x$. De même, $x = gx$ implique $g = e$, le stabilisateur de tout élément est réduit au neutre. Il en va de même pour la translation à droite.

En revanche, pour l'action par automorphisme intérieur, la situation est plus riche. Le stabilisateur de x est l'ensemble des g tels que $g.x = gxg^{-1} = x$ c'est-à-dire tels que : $gx = xg$. C'est le **centralisateur** de x, l'ensemble des éléments qui commute avec x ; on le note $\mathcal{C}_{\mathbf{G}}(x)$. Les éléments de l'orbite de x sont les y tels qu'il existe g tels que $y = gxg^{-1}$. La relation d'équivalence associée porte alors le nom de **conjugaison**. On l'a déjà rencontrée lors de l'étude du groupe symétrique.
Dans la plupart des cas, cette notion de conjuguaison s'avère très intéressante : des éléments conjugués ont beaucoup de propriétés communes. Bien sûr, pour un groupe commutatif, la conjugaison se réduit à l'identité.

3.1.4 En algèbre linéaire, on apprend que M et $P.M$ représentent le même endomorphisme, mais dans des bases différentes. La relation de conjugaison s'appelle la **similitude**, et les orbites sont formées de matrices semblables. Dans le cas d'un corps algébriquement clos, on peut étudier les réduites de Jordan pour classer ces orbites. Dans le cas particulier de $\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$, il y a 16 matrices.

- Celles qui sont seules dans leur orbite :

$$\begin{pmatrix}0&0\\0&0\end{pmatrix} \quad \begin{pmatrix}1&0\\0&1\end{pmatrix}$$

  Ce sont d'ailleurs les matrices du centre de l'anneau.
- Celles de valeurs propres 0 et 1 qui sont donc diagonalisables et toutes semblables :

$$\begin{pmatrix}1&0\\0&0\end{pmatrix} \quad \begin{pmatrix}1&1\\0&0\end{pmatrix} \quad \begin{pmatrix}1&0\\1&0\end{pmatrix} \quad \begin{pmatrix}0&0\\1&1\end{pmatrix} \quad \begin{pmatrix}0&1\\0&1\end{pmatrix} \quad \begin{pmatrix}0&0\\1&1\end{pmatrix}$$

- Dans une autre classe, voici les matrices nilpotentes non nulles :

$$\begin{pmatrix}0&1\\0&0\end{pmatrix} \quad \begin{pmatrix}0&0\\1&0\end{pmatrix} \quad \begin{pmatrix}1&1\\1&1\end{pmatrix}$$

- Puis la classe des matrices de seule valeur propre 1, mais non diagonalisables :

$$\begin{pmatrix}1&1\\0&1\end{pmatrix} \quad \begin{pmatrix}1&0\\1&1\end{pmatrix} \quad \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

- Enfin, une classe de matrices n'ayant aucune valeur propre :

$$\begin{pmatrix}1&1\\1&0\end{pmatrix} \quad \begin{pmatrix}0&1\\1&1\end{pmatrix}$$

On peut continuer à examiner cet exemple, en cherchant les stabilisateurs. Le groupe agissant, formé des matrices inversibles, n'a que six éléments et est isomorphe à $\mathcal{S}_3$.

3.1.5 On peut définir une action à droite comme un « antihomomorphisme » d'un groupe $\mathbf{G}$ dans le groupe symétrique d'un ensemble X, c'est-à-dire Φ vérifiant :

$$\forall g,\ g' \in \mathbf{G},\ \Phi(g) \circ \Phi(g') = \Phi(g'g)$$

Au lieu de la notation $g.x$, on utilise $x.g$ ou bien x^g (notation exponentielle) de sorte que la propriété de définition s'écrive $(x.g).g' = x.(gg')$. L'exemple le plus simple d'action à droite est l'action de $\mathbf{G}$ sur lui-même donnée par $x.g = xg$. Enfin, à toute action à droite, on

peut associer une action à gauche par $g.x = x.g^{-1}$. Ainsi, on peut définir un automorphisme intérieur « à droite » par $x \mapsto g^{-1}xg$. [1]

3.1.6 Soit ϕ une forme bilinéaire sur $\mathcal{E}$ et u un automorphisme de $\mathcal{E}$. On est conduit naturellement à considérer ψ définie par :

$$\psi(x, y) = \phi(u(x), u(y))$$

et ψ est bien une forme bilinéaire sur $\mathcal{E}$. En posant $\psi = u.\phi$, on définit une action **à droite** de $\mathbf{GL}(\mathcal{E})$ sur $\mathcal{L}_2(\mathcal{E})$, espace des formes bilinéaires sur $\mathcal{E}$. En effet,

$$v.(u.\phi)(x, y) = v.\phi(u(x), u(y)) = v.\psi(x, y) = \psi(v(x), v(y)) = \phi(u(v(x)), u(v(y))$$

et donc $v.(u.\phi) = (u \circ v).\phi$. Supposons que $\mathcal{E}$ est de dimension finie, et limitons-nous aux formes bilinéaires symétriques. Si M est la matrice de ϕ dans une base $\mathcal{B}$, et U la matrice de u dans la même base, alors la matrice de ψ est ${}^tUMU$. En effet,

$$\psi(x, y) = {}^t(UX)MUY = {}^tX({}^tUMU)Y$$

on reconnaît la relation de **congruence** entre matrices symétriques. Dans le cas réel, un résultat classique (loi d'inertie de Sylvester) est que les classes d'équivalence sont caractérisées par la signature de la forme quadratique associée, ces classes d'équivalence étant les orbites pour l'action considérée. Dans le cas complexe, les orbites sont simplement classées par le rang.
Enfin, le stabilisateur d'une forme bilinéaire donnée est un groupe, c'est le **groupe orthogonal** de la forme bilinéaire symétrique.

3.1.7 **Cas 1.** L'action d'un sous-groupe de $\mathbf{G}$ se définit par restriction sans aucun problème ; c'est la restriction du morphisme Φ de $\mathbf{G}$ dans le groupe symétrique de X. Remarquons qu'en général les orbites sont alors plus nombreuses. Ainsi, regardons l'exercice précédent ; si $\mathcal{E}$ est muni d'une structure euclidienne, on peut étudier l'action du groupe orthogonal de cette structure euclidienne sur les formes bilinéaires symétriques. Les orbites sont alors classées par les n-uples croissants de valeurs propres réelles ; c'est le théorème spectral.

Cas 2. $\mathbf{G}$ n'agit pas toujours par restriction sur un sous-ensemble Y de X. Il faut pour cela que Y soit stable par **toutes** les bijections de X définies par les éléments de $\mathbf{G}$. Un exemple, si $\mathbf{G}$ agit sur lui-même par automorphismes intérieurs, alors $\mathbf{G}$ agit sur son centre (mais cette action est triviale). Et les sous-groupes qui, comme le centre, sont stables par **tous** les automorphismes intérieurs sont les sous-groupes normaux dans $\mathbf{G}$.

Cas 3. $\mathbf{G}$ agit naturellement sur l'ensemble $\mathcal{P}(X)$ de tous les sous-ensembles de X (en convenant que l'image de l'ensemble vide est vide). On peut également trouver des actions de $\mathbf{G}$ sur des sous-ensembles de $\mathcal{P}(X)$. Ainsi, le groupe linéaire de $\mathcal{E}$ agit sur tous les sous-ensembles de $\mathcal{E}$; il agit aussi sur l'ensemble des droites de $\mathcal{E}$, et plus généralement sur l'ensemble des sous-espaces de dimension k.

Cas 4. $\mathbf{G} \times \mathbf{G}$ n'agit pas naturellement sur X ; il faudrait donner un sens à $(g, g').x$. Si l'on suppose que c'est $(gg').x$, alors

$$(u, u').((g, g').x) = (u, u').(gg'.x) = uu'gg'.x \neq (ug, u'g').x$$

en général.

1. On pourrait donc penser qu'il est possible de se passer totalement des actions à droite, mais il y a des circonstances où elles sont plus naturelles que les actions à gauche.

Cas 5. En revanche, **G** définit naturellement une action sur $X \times X$ par $g.(x, x') = (g.x, g.x')$. La considération de cette action (et de ses généralisations) est utile, voir plus loin les questions de transitivité.

Cas 6. $\mathbf{H} \times \mathbf{G}$ agit à gauche sur Y^X par :

$$\forall f \in Y^X,\ \forall x \in X,\ ((h, g).f)(x) = h.(f(g^{-1}.x))$$

Il suffit de le vérifier. En fait, toute action à gauche sur l'ensemble de départ conduit à une action à droite sur l'ensemble des applications, ce que traduit le g^{-1}. Cet exemple est courant : on le retrouve dans l'exercice précédent et dans celui qui suit.

3.1.8 $\mathcal{S}_n$ agit **à gauche** sur $\mathbb{E}^n$ par :

$$\sigma.(x_1, x_2, \ldots, x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)})$$

C'est un cas particulier de l'exercice précédent, dans la mesure où l'ensemble des n-uples est en bijection avec l'ensemble des applications de $\{1, 2, \ldots, n\}$ dans $\mathbb{E}$. Prenons un exemple, avec $\sigma = (1, 2, 3)$ (permutation circulaire).

$$\sigma.(x_1, x_2, x_3) = (x_3, x_1, x_2)$$

On voit bien que les indices sont transformés par σ^{-1}, mais que les « valeurs » tournent suivant σ.

$\mathcal{S}_n$ agit à gauche sur $\mathbb{K}[X_1, X_2, \ldots, X_n]$ par :

$$\sigma.P(x_1, x_2, \ldots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Cela résulte de ce que l'anneau des polynômes est l'ensemble des applications (presque nulles, c'est-à-dire nulles sauf pour un nombre fini d'indices) de $\mathbb{N}^n$ dans $\mathbb{K}$. L'ensemble des polynômes qui sont seuls dans leur orbite, et sont donc fixés par tous les éléments de $\mathcal{S}_n$ est un sous-anneau, celui des polynômes symétriques. Les polynômes **antisymétriques**, c'est-à-dire qui vérifient $\sigma.P = P$ si σ est paire, $\sigma.P = -P$ sinon, sont dans des orbites à deux éléments. Il n'y a pas d'autre possibilité, car une orbite à deux éléments est liée à un stabilisateur d'indice deux ; et le seul groupe d'indice deux du groupe symétrique est le groupe alterné qui stabilise les polynômes symétriques. Un exemple de polynôme à trois variables dont l'orbite a trois éléments : $X_1X_2 + X_3$. Voir le lien avec les sous-groupes d'indice 3 de $\mathcal{S}_3$.

3.1.9 1) $P_\sigma \circ P_\tau = P_{\sigma\circ\tau}$. En effet, si l'on appelle c_{ij} le coefficient courant de cette matrice :

$$c_{ij} = \sum_{k=1}^{n} \delta_{i\sigma(k)}\delta_{k\tau(j)} = \delta_{i\sigma(\tau(j))}$$

L'application $\sigma \mapsto P_\sigma$ est donc un morphisme ; elle est surjective par définition de l'ensemble des matrices de permutations ; elle est injective car $P_\sigma = I$ ssi $\delta_{i\sigma(j)} = \delta_{ij}$ pour tout i, j ; σ est donc l'identité.

2) Soit $M = (m_{ij})$. Alors $P_\sigma M$ a pour coefficient :

$$d_{ij} = \sum_{k=1}^{n} \delta_{i\sigma(k)}m_{kj} = m_{\sigma^{-1}(i)j}$$

Une façon de comprendre ce résultat est de considérer la matrice M formée des lignes (L_i). Alors $P_\sigma M$ est la matrice $(L_{\sigma^{-1}(i)})$. Cette écriture confirme que l'on a bien une action à gauche, ce que montre aussi le calcul de la première question. Un exemple, si

$\sigma = (1,2,3)$, la matrice $P_\sigma M$ est $\begin{pmatrix} L_3 \\ L_1 \\ L_2 \end{pmatrix}$. Un truc : pour avoir la matrice P_σ, il suffit de faire subir cette transformation à la matrice de l'identité.

3) Cette fois, MP_σ a pour coefficients $(m_{i\sigma(j)})$, il s'agira d'une permutation des colonnes, et d'une action à droite. Si $\sigma = (1,2,3)$, la matrice MP_σ est : (C_2, C_3, C_1).

3.1.10 1) L'application f est bien définie si $g\mathbf{G}_x = g'\mathbf{G}_x$, c'est que $g^{-1}g' \in \mathbf{G}_x$, donc $g^{-1}g'.x = x$ soit $g'.x = g.x$. Ce même calcul, fait à l'envers, montre que f est injective. De plus, f est surjective par définition même de l'orbite de x.

2) $\mathbf{G}$ est un groupe à six éléments. Si l'on pose $r = g \circ h$, $r(z) = 1 - \frac{1}{z}$ et $r^2(z) = \frac{1}{1-z}$, $r^3(z) = z$. Le dernier élément du groupe est $k = h \circ r : z \mapsto \frac{z}{z-1}$, il est d'ordre 2 comme g et h. On reconnaît ainsi le groupe $\mathcal{S}_3$. Faisons agir $\mathbf{G}$ sur $\mathbb{C} \setminus \{0,1\}$. L'orbite de z contient donc au maximum six éléments qui sont :

$$z,\ \frac{1}{z},\ \frac{z}{z-1},\ \frac{z-1}{z},\ 1-z,\ \frac{1}{1-z}$$

Si ces éléments sont distincts, le stabilisateur est réduit à l'identité. En cherchant si certains de ces éléments sont égaux, on trouve qu'il y a deux cas particuliers. Si z est égal à -1, à $\frac{1}{2}$ ou à 2, l'orbite a trois éléments (qui sont ces trois complexes) et les stabilisateurs sont les sous-groupes à deux éléments $\{e,h\}, \{e,g\}, \{e,k\}$. Si z est $-j$ ou $-j^2$ (j et j^2 sont les racines cubiques de l'unité), l'orbite a deux éléments, et le stabilisateur est $\{e, r, r^2\}$. On vérifie bien qu'il y a dans tous les cas, bijection de $\mathbf{G}/\mathbf{G}_z$ avec $\mathbf{G}z$. Cette action est liée à la notion de birapport, rencontrée en géométrie.

3.1.11 f est définie par :

$$f : h\mathbf{G}_x \mapsto h.x$$

Les actions de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{G}_x$ et de $\mathbf{G}$ sur $\mathbf{G}x$ sont définies par :

$$g.(h\mathbf{G}_x) = (gh)\mathbf{G}_x$$
$$g.(h.x) = (gh).x$$

On a alors :

$$f(g.h\mathbf{G}_x) = f(gh\mathbf{G}_x) = gh.x \text{ et } g.f(h\mathbf{G}_x) = g.h.x$$

Comme par ailleurs f est bijective, c'est bien un isomorphisme d'action. Ainsi, toute action de $\mathbf{G}$ se résume à une action sur chacune des orbites, et chacune de ces actions est isomorphe à l'action de $\mathbf{G}$ sur un de ses quotients.

3.1.12 1) Si x et y sont dans la même orbite, c'est qu'il existe un $g \in \mathbf{G}$ tel que $y = g.x$. Alors, $h \in \mathbf{G}$ laisse y invariant et s'écrit $h.y = y \iff h.(g.x) = g.x \iff g^{-1}hg \in \mathbf{G}_x$ et donc

$$\mathbf{G}_y = g\mathbf{G}_x g^{-1}$$

Les deux stabilisateurs sont conjugués.

2) On a vu que l'action d'un groupe $\mathbf{G}$ sur l'orbite de x est isomorphe à l'action de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{G}_x$. Si l'on prend un autre représentant y de la même orbite, on obtient un autre isomorphisme avec l'action de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{G}_y = \mathbf{G}/g\mathbf{G}_x g^{-1}$. Donc si $\mathbf{H}' = g\mathbf{H}g^{-1}$, les actions

de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$ et sur $\mathbf{G}/\mathbf{H}'$ sont isomorphes. ($\mathbf{H}$ est alors le stabilisateur de $x = \mathbf{H}$). Réciproquement, soit f un isomorphisme d'action entre $\mathbf{G}/\mathbf{H}'$ et $\mathbf{G}/\mathbf{H}$. Alors :

$$g \in \mathbf{G}_{f(x)} \iff g.f(x) = f(x) \iff f(g.x) = f(x) \iff g.x = x \iff g \in \mathbf{G}_x$$

prouve que x et $f(x)$ ont même stabilisateur (on a utilisé que f était bijective). Si l'on applique cela à $x = \mathbf{H}'$, en posant $f(x) = g\mathbf{H}$, on trouve que le stabilisateur de x qui est $\mathbf{H}'$, est aussi le stabilisateur de $g\mathbf{H}$, qui est $g\mathbf{H}g^{-1}$. Remarquons que l'application f est alors définie par $f : k\mathbf{H}' \mapsto kg\mathbf{H}$.

3.1.13 Soit h la matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Alors

$$h.z = \frac{az+c}{bz+d} = \frac{ab|z|^2 + (bc\bar{z} + adz) + cd}{|bz+d|^2}$$

La partie imaginaire de $h.z$ est donc :

$$\frac{(ad-bc)\,\mathrm{Im}(z)}{|bz+d|^2}$$

Comme par hypothèse, le déterminant de h est 1, on voit que tout complexe de partie imaginaire strictement positive a pour image un complexe de partie imaginaire strictement positive. De plus, un calcul simple montre bien qu'il s'agit d'une action, avec des notations évidentes :

$$h.(h'.z) = \frac{a\frac{a'z+c'}{b'z+d'} + c}{b\frac{a'z+c'}{b'z+d'} + d} = \frac{(aa' + cb')z + ac' + cd'}{(a'b + db')z + bc' + dd'} = (hh').z$$

Cette action n'est pas fidèle, on voit facilement que son noyau est formé de la matrice de l'identité et de son opposée. Le stabilisateur de i est formé des matrices h telles que :

$$ai + c = -b + di \iff a = d \text{ et } b = -c$$

Comme le déterminant est égal à 1, on trouve toutes les matrices orthogonales directes. Enfin l'orbite de i est le demi-plan de Poincaré tout entier, puisque le complexe $x + iy$ où x est réel et y est réel strictement positif est l'image de i par h de matrice $\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix}$. L'action est donc transitive.

3.1.14 Si $\mathbf{G}$ agit sur X, les orbites sont des classes d'équivalence. Elles sont donc disjointes, et forment une partition de X ; reste à évaluer le cardinal d'une classe, c'est ce qui est fait dans l'exercice 3.1.10. On obtient alors la formule demandée.

3.1.15 1) Si x est dans le centre de $\mathbf{G}$, $gxg^{-1} = x$ pour tout g, x est seul dans son orbite.

2) L'orbite de x a pour cardinal $|\mathbf{G}|/|\mathbf{G}_x|$, la formule des classes donne le résultat demandé :

$$|\mathbf{G}| = |\mathcal{Z}(\mathbf{G})| + \sum_{x \in A} \frac{|\mathbf{G}|}{|\mathbf{G}_x|}$$

3) Dans l'égalité précédente $|\mathbf{G}|$, $\dfrac{|\mathbf{G}|}{|\mathbf{G}_x|}$ sont des multiples de p (puisque x n'étant pas dans le centre, $\mathbf{G}_x$ n'est pas $\mathbf{G}$ tout entier). On en déduit que le cardinal du centre est multiple de p. Puisqu'il est non vide (*cf.* l'élément neutre), il contient au moins p éléments.

3.1.16 1) Des exemples en géométrie affine. Le groupe des translations agit sur un espace affine de façon transitive, étant donnés deux points distincts A et B, il existe un vecteur $\overrightarrow{u}$ tel que $B = t_{\overrightarrow{u}}(A)$. Le vecteur $\overrightarrow{u}$ est d'ailleurs unique et s'écrit $\overrightarrow{u} = \overrightarrow{AB}$. En revanche, il n'agit pas doublement transitivement. Mais dès la dimension un, le groupe affine agit doublement transitivement. En dimension un, cela se traduit par l'énoncé : il existe toujours une application affine prenant des valeurs données en deux points distincts donnés.

2) Soit $\mathbf{H}$ le stabilisateur d'un élément x. Commençons par remarquer qu'une action doublement transitive est... transitive. Les stabilisateurs de tous les éléments sont donc des groupes conjugués (et donc isomorphes). Soit $\mathbf{H}$ le stabilisateur de x et g un élément de $\mathbf{G}$ qui n'est pas dans $\mathbf{H}$. On va montrer que $\mathbf{G} = \mathbf{H} \cup \mathbf{H}g\mathbf{H}$, ce qui montrera que tout groupe contenant $\mathbf{H}$ et g est égal à $\mathbf{G}$, et donc que $\mathbf{H}$ est maximal. Posons $g.x = y$ et soit g' quelconque qui n'est pas dans $\mathbf{H}$; on pose $g'.x = y'$. Alors il existe $h \in \mathbf{H}$ tel que :

$$h.x = x \text{ et } h.y = y'$$

puisque l'action est doublement transitive et $x \neq y$ et $x \neq y'$. Mais alors $g'^{-1}hg$ vérifie :

$$g'^{-1}hg.x = g'^{-1}h.y = g'^{-1}.y' = x$$

et est donc dans $\mathbf{H}$. On en déduit que $g' \in \mathbf{H}g\mathbf{H}$.
La réciproque de notre énoncé est fausse, voilà un contre-exemple. Prenons pour $\mathbf{G}$ le groupe cyclique engendré par la permutation $\sigma = (1, 2, 3, 4, 5)$. Alors le stabilisateur de 1 est l'identité, qui est un sous-groupe maximal de $\mathbf{G} \cong \mathbb{Z}/5$, mais l'action n'est pas doublement transitive, $1 \mapsto 2$ et $2 \mapsto 4$ sont incompatibles.[1]

3) Une action est triplement transitive si, pour trois éléments distincts x_1, x_2, x_3 de X, et trois éléments y_1, y_2, y_3 de X, il existe un élément g de $\mathbf{G}$ tel que $y_1 = g.x_1, y_2 = g.x_2, y_3 = g.x_3$. Exemple, le groupe symétrique agit triplement transitivement sur les triplets d'éléments distincts de $\{1, 2, \ldots, n\}$. En fait, le groupe symétrique agit même n fois transitivement sur le même ensemble... Et c'est exceptionnel.

4) On se donne trois droites vectorielles distinctes du plan. Appelons u, v, w des vecteurs directeurs. Alors, u et v sont indépendants, et l'on peut écrire w sous la forme :

$$w = \alpha u + \beta v, \qquad \alpha, \beta \in \mathbb{K}^*$$

De même, si l'on se donne encore trois droites, dirigées par u', v', w' on peut de même écrire

$$w' = \alpha' u' + \beta' v', \qquad \alpha, \beta \in \mathbb{K}$$

Il suffit alors de définir $f \in \mathbf{G}$ par $f(\alpha u) = \alpha' u'$ et $f(\beta v) = \beta' v'$. En revanche, cela ne marche plus forcément avec quatre droites ; prendre celles dirigées par $u, v, u + v, u - v$ et essayer de les transformer en celles dirigées par $u, v, u + v, u - 2v$.

En dimension 3, l'action n'est plus triplement transitive. Si l'on se donne trois droites distinctes coplanaires, elles ne peuvent être transformées en trois droites distinctes non coplanaires. L'action sur les plans est également doublement transitive, mais non triplement : considérer trois plans ayant une droite en commun qui ne peuvent être envoyés sur trois plans distincts quelconques.

1. Les groupes de permutations transitifs, qui ont la propriété que les stabilisateurs sont maximaux, sont néanmoins importants ; on les appelle **groupes primitifs**. Voir le problème 4 du dernier chapitre.

3.1.17 Soit E l'ensemble des couples (g, x) où $g.x = x$. Alors,

$$|E| = \sum_{g \in \mathbf{G}} |\mathrm{Fix(g)}| = \sum_{x \in X} |\mathbf{G}_x|$$

Si A est une transversale de X, on a donc :

$$|E| = \sum_{x \in A} |\mathbf{G}x||\mathbf{G}_x| = |\mathbf{G}||A|$$

Le nombre des orbites, soit $|A|$, est donc :

$$|A| = \frac{1}{|\mathbf{G}|} \sum_{g \in \mathbf{G}} |\mathrm{Fix(g)}|$$

3.1.18 Le groupe symétrique $\mathcal{S}_n$ agit sur l'ensemble des coloriages (applications de $\{1, \ldots, n\}$ dans $\{1, \ldots, p\}$), mais pour ce qui nous concerne, on se limite au sous-groupe cyclique engendré par la permutation circulaire $\sigma = (1, 2, \ldots, n)$. Deux roues seront en effet identiques si elles se déduisent l'une de l'autre par une puissance de σ, c'est-à-dire si elles sont dans la même orbite. Le nombre de roues est donc le nombre d'orbites. Pour appliquer la formule précédente, reste à déterminer le nombre des points fixes par une permutation τ. Supposons que τ soit produit de k cycles (y compris les points fixes, comptant pour un cycle). Alors, un coloriage doit être constant sur chacun de ces cycles pour être fixe par τ ; le nombre de coloriages fixes est donc p^k. Ainsi, pour la permutation circulaire σ, il y a p coloriages fixes, les roues dont tous les secteurs ont la même couleur.
Il faut ensuite déterminer le nombre de cycles que contient la puissance m de σ, c'est 1 ssi m est premier avec n, $m \wedge n$ en général. On peut indexer la somme sur les diviseurs de n, en tenant compte que le nombre d'exposants m tels que $m \wedge n = d$ est $\phi(n/d)$ (voir l'étude des sous-groupes des groupes cycliques). En définitive :

$$\text{nombre de roues} = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) p^d$$

Par exemple, avec p couleurs et trois secteurs, on trouve $\frac{1}{3}(2p + p^3)$, pour quatre secteurs $\frac{1}{4}(2p + p^2 + p^4)$ ce que confirment des dénombrements directs.

3.2 LES THÉORÈMES DE SYLOW

Ils sont très importants pour les groupes finis. Ils permettent d'affirmer l'existence de sous-groupes ayant un cardinal donné, et donc fournissent une réciproque – partielle – au théorème de Lagrange. Plus précisément, soit $\mathbf{G}$ un groupe fini de cardinal $n = p^k m$ où p est un nombre premier qui ne divise pas m. Alors il existe au moins un sous-groupe d'ordre p^k. Un tel sous-groupe sera appelé un **p-Sylow** de $\mathbf{G}$. On rappelle qu'un **p-groupe** fini est un groupe dont le cardinal est une puissance de p, et on montrera que tout p-sous groupe de $\mathbf{G}$ est inclus dans un p-Sylow de $\mathbf{G}$.

Les démonstrations des théorèmes de Sylow sont un florilège d'actions de groupes. Avant de les aborder, un point de vocabulaire. On appelle **normalisateur** de $\mathbf{H}$ dans $\mathbf{G}$ l'ensemble des éléments g de $\mathbf{G}$ tels que $g\mathbf{H}g^{-1} = \mathbf{H}$. Il sera noté $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$.

Exercice 3.2.1

1) Montrer que le normalisateur de **H** est le plus grand sous-groupe de **G** dans lequel **H** est normal.
2) On appelle **conjugué** du sous-groupe **H** son image par un automorphisme intérieur. En utilisant l'action de **G** sur ses sous-groupes par automorphisme intérieur, démontrer que le nombre des conjugués de **H** est l'indice de son normalisateur (dans le cas où cet indice est fini). Montrer, de même, que le nombre des conjugués d'un élément de **G** est l'indice de son centralisateur.
3) Étudier le normalisateur dans $\mathcal{S}_n$ du groupe engendré par une transposition.

L'exercice suivant utilise encore cette action par conjugaison.

Exercice 3.2.2

Si **G** est un groupe fini, démontrer qu'il n'existe aucun sous-groupe strict qui contienne au moins un représentant de chaque classe de conjugaison des éléments de **G**. Trouver un contre-exemple dans le cas d'un groupe infini.

L'exercice suivant propose une des démonstrations de l'existence des p-Sylow d'un groupe fini, mais aussi des deux autres théorèmes de Sylow.

Exercice 3.2.3

Soit **G** un groupe ayant $p^k m$ éléments, où $m \geqslant 1$ n'est pas divisible par p premier.

1) On appelle $\mathcal{X}$ l'ensemble des sous-ensembles de **G** ayant p^k éléments. Alors **G** agit sur $\mathcal{X}$ par translation à gauche. Calculer le cardinal de $\mathcal{X}$ et démontrer qu'il existe au moins une orbite dont le cardinal n'est pas divisible par p.
2) Soit alors A une telle orbite, $\mathbf{G}_X$ le stabilisateur d'un élément X de A. Démontrer que $\mathbf{G}_X$ est un p-Sylow de **G**. En déduire le **premier théorème de Sylow** : tout groupe fini dont le cardinal est divisible par p admet un p-Sylow.
3) Changeons d'action. Soit **S** un p-Sylow de **G**, et **H** un p-groupe de **G**. En faisant agir **H** sur **G**/**S** par translation à gauche, démontrer que **H** est inclus dans un conjugué de **S**. En particulier, tous les p-Sylow de **G** sont des conjugués de **S**. Ce résultat constitue le **second théorème de Sylow**.
4) En déduire que si un groupe admet un seul p-Sylow, celui-ci est normal dans **G**, et réciproquement si **G** a p-Sylow normal, c'est le seul p-Sylow de **G**.
5) Utiliser cette fois l'action de conjugaison de **S** sur les p-Sylow, et démontrer que le nombre c_p de ces p-Sylow est congru à 1 modulo p. Démontrer également que c_p est un diviseur de m. C'est le **troisième théorème de Sylow**.

On peut commencer par « vérifier » nos trois théorèmes, en cherchant les p-Sylow de groupes déjà connus.

Exercice 3.2.4

1) Déterminer les p-Sylow de $\mathbb{Z}/n$, (pour p diviseur de n), de $\mathbb{Z}/6 \times \mathbb{Z}/12$, de $\mathbb{D}_{2n}$ ($p = 2$ ou p diviseur de n).
2) Chercher les 2-Sylow de $\mathcal{S}_4$ et de $\mathcal{S}_5$ et les reconnaître.

Le charme des théorèmes de Sylow est qu'ils n'utilisent que le cardinal du groupe $\mathbf{G}$, cela permet parfois de donner un résultat général concernant tous les groupes ayant un cardinal donné. Commençons par examiner le problème de la simplicité.[1]

Exercice 3.2.5

1) En utilisant le troisième théorème de Sylow, démontrer qu'il n'y a pas de groupe simple ayant 30, 42, ou 105 éléments.
2) Généraliser aux groupes ayant pqr éléments, où p, q et r sont distincts et premiers. On pourra raisonner par l'absurde, et poser $p > q > r$.

Exercice 3.2.6

Démontrer qu'il n'y a pas de groupe simple d'ordre 300. On pourra étudier le normalisateur d'un 5-Sylow.

Exercice 3.2.7

Montrer qu'un groupe simple d'ordre au moins $r!$ ne peut avoir de sous-groupe d'indice r.

Voici maintenant d'autres applications, et pour commencer des applications au groupe symétrique.

Exercice 3.2.8 (Étude du groupe $\mathcal{A}_5$)

Ce groupe est formé des permutations paires de 5 éléments. Rappelons qu'il contient :

- 15 éléments d'ordre 2 (les doubles transpositions) ;
- 20 éléments d'ordre 3 (les 3-cycles) ;
- 24 éléments d'ordre 5 (les 5-cycles) ;
- et l'identité, bien sûr.

1) Démontrer que les 3-cycles forment une classe de conjugaison dans $\mathcal{A}_5$. Étudier également les doubles transpositions.
2) Démontrer que si $\mathbf{H} \lhd \mathcal{A}_5$, alors s'il contient un élément d'ordre 5, il les contient tous. On utilisera les théorèmes de Sylow.
3) En utilisant qu'un sous-groupe normal est réunion de classes de conjugaison, démontrer que $\mathcal{A}_5$ est simple.

1. Rappelons qu'un groupe est simple s'il n'a pas d'autre sous-groupe normal que lui-même ou l'élément neutre.

L'exercice suivant montre que le groupe alterné est simple pour lorsque $n > 5$. Les cas $n = 2, 3, 4$ se traitent facilement : $n = 2$, le groupe alterné est trivial, $n = 3$, le groupe alterné est d'ordre 3, il est simple ; pour $n = 4$, le groupe alterné contient un sous-groupe normal, le groupe des doubles transpositions.

Exercice 3.2.9 (Simplicité du groupe alterné (cas général))

On suppose donc que $n > 5$ et que $\mathbf{H} \lhd \mathcal{A}_n$. Soit τ un élément de $\mathbf{H}$, différent de l'identité.

1) Si σ est une permutation quelconque de $\mathcal{A}_n$, montrer que $\sigma\tau\sigma^{-1}\tau^{-1}$ est dans $\mathbf{H}$.
2) En prenant i tel que $\tau(i) = j, j \neq i$, et en utilisant k distinct de $i, j, \tau(j)$, construire un 3-cycle σ, tel que $\sigma\tau\sigma^{-1}\tau^{-1}$ laisse fixes au moins $n - 5$ éléments.
3) En déduire que $\mathbf{H}$ contient un 3-cycle, puis que $\mathbf{H} = \mathcal{A}_n$.

Le groupe $\mathcal{S}_n$ n'est pas simple, mais il contient très peu de sous-groupes normaux.

Exercice 3.2.10

Montrer que, pour $n \geqslant 5$, les seuls sous-groupes normaux de $\mathcal{S}_n$ sont les sous-groupes « triviaux » et le groupe alterné.

Exercice 3.2.11

1) Soit $\mathbf{G}$ un groupe, $\mathbf{H}$ un sous-groupe. On a déjà utilisé le fait que $\mathbf{G}$ agit sur l'ensemble quotient $\mathbf{G}/\mathbf{H}$ par translation à gauche. Montrer que le noyau de cette action est l'intersection des conjugués de $\mathbf{H}$.
2) Vérifier que c'est le plus grand sous-groupe normal dans $\mathbf{G}$ et inclus dans $\mathbf{H}$.
3) En déduire que si $\mathbf{H}$ est un sous-groupe d'indice n de $\mathcal{S}_n$, alors il est isomorphe à $\mathcal{S}_{n-1}$.

Après cet intermède sur les groupes symétriques et alternés, revenons à des applications variées des théorèmes de Sylow.

Exercice 3.2.12

Démontrer que si p est le plus petit facteur premier du cardinal de $\mathbf{G}$, alors un sous-groupe d'indice p (s'il en existe), est forcément normal dans $\mathbf{G}$.

Exercice 3.2.13

Soit $\mathbf{S}$ un p-groupe de Sylow d'un groupe $\mathbf{G}$. On note $\mathbf{N}$ son normalisateur dans $\mathbf{G}$. Démontrer que $\mathbf{N}$ est un groupe autonormalisant, c'est-à-dire que son normalisateur dans $\mathbf{G}$ est lui-même. Que dire si $\mathbf{S}$, lui-même, est autonormalisant ? Donner des exemples.
Soit plus généralement $\mathbf{H}$ un sous-groupe tel que $\mathbf{N} \leqslant \mathbf{H} \leqslant \mathbf{G}$. Démontrer que $\mathbf{H}$ est également autonormalisant.

Exercice 3.2.14 (Lemme de Frattini)

Soit $\mathbf{N} \lhd \mathbf{G}$ où $\mathbf{G}$ est fini. On se donne un p-Sylow $\mathbf{S}$ de $\mathbf{N}$. Vérifier que les conjugués de $\mathbf{S}$ dans $\mathbf{G}$ sont aussi dans $\mathbf{N}$, et en déduire que :

$$\mathbf{G} = \mathbf{N}\mathcal{N}_{\mathbf{G}}(\mathbf{S})$$

Parlons un peu des p-groupes, groupes finis ayant p^k éléments. Tout p-Sylow est un p-groupe, et l'on constate que, dès que k est un peu grand, il y a énormément de p-groupes non isomorphes. Par exemple, il y a 51 groupes à 32 éléments, et 10 494 213 groupes ayant 512 éléments...

Exercice 3.2.15 (Théorème de Cauchy)

Montrer que si $\mathbf{G}$ est un groupe fini de cardinal n et si p est un facteur premier de n, alors il existe un élément d'ordre p dans $\mathbf{G}$. On pourra introduire

$$\mathbb{E} = \{(x_1, x_2, \ldots, x_p) / \; x_1 x_2 \ldots x_p = 1\}$$

et passer par les étapes suivantes :

1) Calculer le cardinal de $\mathbb{E}$.
2) Montrer que $\mathbb{Z}/p$ agit naturellement sur $\mathbb{E}$, et que chaque orbite a un ou p éléments. À quoi correspondent les orbites à un élément ?
3) En déduire le résultat.
4) Retrouver le théorème de Cauchy en utilisant le théorème de Sylow.

La notion de p-groupe n'a pas de sens dans le cas d'un groupe infini ; on décide d'appeler p-groupe un groupe dont tout élément est d'ordre une puissance de p (avec encore bien sûr p premier). La première chose à faire est de vérifier que cette nouvelle définition coïncide avec la précédente dans le cas fini.

Exercice 3.2.16

Soit p un nombre premier. Montrer que pour un groupe fini $\mathbf{G}$, il y a équivalence entre :
(i) L'ordre de tout élément est une puissance de p.
(ii) Le cardinal de $\mathbf{G}$ est une puissance de p.

Nous avons déjà montré qu'un p-groupe fini a toujours un centre non trivial (*cf.* 3.1.15). Voici un lemme important qui suit le même type de démonstration.

Exercice 3.2.17

Démontrer que si $\mathbf{H}$ est un sous-groupe propre d'un p-groupe $\mathbf{G}$ alors soit $\mathbf{H}$ est normal dans $\mathbf{G}$, soit il existe un conjugué de $\mathbf{H}$, distinct de $\mathbf{H}$, qui est inclus dans le normalisateur dans $\mathbf{G}$ de $\mathbf{H}$. On pourra utiliser l'action par conjugaison de $\mathbf{H}$ sur ses conjugués.

Exercice 3.2.18

1) En utilisant l'exercice précédent, démontrer que tout sous-groupe maximal d'un p-groupe fini $\mathbf{G}$ est normal dans $\mathbf{G}$ et est d'indice p. Que dire si $\mathbf{G}$ n'est pas un p-groupe ?

2) Démontrer également que si $\mathbf{G}$ est d'ordre p^n, il admet des sous-groupes normaux d'ordre p^i où i est quelconque inférieur à n. On pourra raisonner par récurrence en utilisant le centre.

3) Démontrer qu'entre tout sous-groupe $\mathbf{H}$ et $\mathbf{G}$, il existe une suite de sous-groupes $\mathbf{H} = \mathbf{H}_0, \mathbf{H}_1, \mathbf{H}_2, \ldots \mathbf{H}_n = \mathbf{G}$ chacun étant normal et d'indice p dans le suivant. Examiner l'exemple des groupes à huit éléments. Que dire quand $\mathbf{G}$ n'est pas un p-groupe ?

Enfin, deux exercices qui introduisent des généralisations de la notion de sous-groupe normal.

Exercice 3.2.19

Un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ est dit **pronormal** dans $\mathbf{G}$ si pour tout x, le groupe $x\mathbf{H}x^{-1}$ est conjugué de $\mathbf{H}$ dans $\langle \mathbf{H}, x\mathbf{H}x^{-1} \rangle$. Bien sûr, tout groupe normal dans $\mathbf{G}$ est pronormal dans $\mathbf{G}$. On se limitera à $\mathbf{G}$ fini.

1) Démontrer que tout p-Sylow de $\mathbf{G}$ est pronormal dans $\mathbf{G}$.

2) Plus généralement, montrer que si $\mathbf{S}$ est un p-Sylow d'un sous-groupe $\mathbf{K}$ normal dans $\mathbf{G}$, alors $\mathbf{S}$ est pronormal dans $\mathbf{G}$.

3) Démontrer qu'un p-sous-groupe $\mathbf{H}$ de $\mathbf{G}$ est pronormal dans $\mathbf{G}$ ssi tout p-Sylow ne contient qu'un seul conjugué de $\mathbf{H}$.

4) Donner un exemple de groupe pronormal dans $\mathbf{G}$ qui n'est pas normal dans $\mathbf{G}$.

Exercice 3.2.20

Un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ est dit **sous-normal** dans $\mathbf{G}$ s'il existe une suite $(\mathbf{H}_i)$ de sous-groupes de $\mathbf{G}$ telle que :

$$\mathbf{H} \lhd \mathbf{H}_1 \lhd \mathbf{H}_2 \lhd \ldots \lhd \mathbf{H}_{n-1} \lhd \mathbf{G}$$

La sous-normalité est donc transitive, contrairement à la normalité, et un sous-groupe normal dans $\mathbf{G}$ est sous-normal dans $\mathbf{G}$.

1) Si $\mathbf{G}$ est un p-groupe fini, démontrer que tous ses sous-groupes sont sous-normaux.

2) Donner un exemple de groupe sous-normal dans $\mathbf{G}$ sans être normal dans $\mathbf{G}$. Quels sont les groupes sous-normaux de $\mathcal{S}_n$?

3) Si ϕ est un morphisme de groupe et si $\mathbf{H}$ est sous-normal dans $\mathbf{G}$, est-ce que $\phi(\mathbf{H})$ est sous-normal dans $\phi(\mathbf{G})$?

4) Montrer que si $\mathbf{H} \lhd \mathbf{G}$, et si $\mathbf{S}$ est un p-Sylow de $\mathbf{G}$, alors $\mathbf{H} \cap \mathbf{S}$ est un p-Sylow de $\mathbf{H}$.

5) Montrer que la propriété précédente subsiste si l'on suppose seulement $\mathbf{H}$ sous-normal dans $\mathbf{G}$.

6) Montrer qu'un groupe, qui est à la fois pronormal et sous-normal dans $\mathbf{G}$, est aussi normal dans $\mathbf{G}$.

SOLUTIONS

3.2.1 1) C'est pratiquement la définition. Si $\mathbf{H}$ est normal dans $\mathbf{K}$, avec $\mathbf{H} \leqslant \mathbf{K} \leqslant \mathbf{G}$, c'est que $g\mathbf{H}g^{-1} = \mathbf{H}$ pour tout g de $\mathbf{K}$. Il reste à vérifier que l'ensemble de tels g est bien un sous-groupe, ce qui est immédiat et résulte également de la question suivante.

2) Dans l'action considérée, $\mathcal{N}_{\mathbf{G}}(\mathbf{H})$ est le stabilisateur de $\mathbf{H}$. L'orbite de $\mathbf{H}$, qui est formée de ses conjugués, contient donc $[\mathbf{G} : \mathcal{N}_{\mathbf{G}}(\mathbf{H})]$ éléments.
Si l'on considère l'action par conjugaison non pas sur les sous-groupes mais sur les éléments eux-mêmes, le stabilisateur est le centralisateur, et le nombre des conjugués est l'indice de ce centralisateur (3.1.3).

3) Soit $\mathbf{H} = \{e, (i,j)\}$. Puisque $\sigma \circ (i,j) \circ \sigma^{-1} = (\sigma(i), \sigma(j))$, un élément du normalisateur fixe i et j, ou les échange. Si $\mathbf{K}$ est le groupe des permutations qui fixent i et j (de cardinal $(n-2)!$), le normalisateur de $\mathbf{H}$ dans $\mathbf{G}$ est $\mathbf{HK} = \mathbf{K} \subset (i,j)\mathbf{K}$. Il est de cardinal $2(n-2)!$, car formé de deux ensembles disjoints ayant chacun $(n-2)!$ éléments. Cela donne $\frac{n(n-1)}{2}$ conjugués pour $\mathbf{H}$... Ce sont tous les groupes engendrés par une transposition.

3.2.2 Soit $\mathbf{G}$ de cardinal n ; supposons que $\mathbf{H}$, distinct de $\mathbf{G}$ et de cardinal p, contienne au moins un élément de chaque classe de conjugaison de $\mathbf{G}$. Si nous appelons k le nombre des conjugués de $\mathbf{H}$, $k > 1$; en effet, si $\mathbf{H}$ était normal dans $\mathbf{G}$, il serait réunion de classes de conjugaisons, et avec notre hypothèse, il serait donc égal à $\mathbf{G}$. En outre, l'hypothèse implique également que l'union des conjugués de $\mathbf{H}$ est égale à $\mathbf{G}$. De plus, cette union est formée de e et de la réunion des conjugués des autres éléments de $\mathbf{H}$; son cardinal est donc inférieur ou égal à $1 + k(p-1)$. On a donc :

$$n \leqslant 1 + k(p-1) \Rightarrow \frac{n}{k} \leqslant p - 1 + \frac{1}{k}$$

Comme k est différent de 1, cela donne $p' = \frac{n}{k} < p$ ce qui est absurde car $p' = \frac{n}{k}$ est le cardinal du normalisateur de $\mathbf{H}$. Or ce normalisateur contient $\mathbf{H}$.
Voici un exemple en cardinal infini. Si $\mathbf{G}$ est l'ensemble des matrices carrées à coefficients complexes, en dimension supérieure à 1, la conjugaison est la similitude, et le sous-groupe des matrices triangulaires supérieures contient un élément de chaque classe, d'après le théorème de trigonalisation.

3.2.3 1) Le cardinal de $\mathcal{X}$ est $C^{p^k}_{p^k m}$. Or ce nombre n'est pas divisible par p. En effet, il peut s'écrire :

$$C^{p^k}_{p^k m} = \frac{p^k m(p^k m - 1)(p^k m - 2)\dots(p^k m - p^k + 1)}{p^k(p^k - 1)\dots(1)}$$

Numérateur et dénominateur contiennent le même nombre d'exemplaires du facteur premier p puisque $p^k m - i \equiv p^k - i \pmod{p^j}$ pour $j \leqslant k$. Le cardinal de $\mathcal{X}$ n'est pas divisible par p et les orbites forment une partion de $\mathcal{X}$, donc il existe une orbite de cardinal non divisible par p.

2) Les éléments de A sont formés de p^k éléments de $\mathbf{G}$. Soit $X \in A$, son stabilisateur $\mathbf{G}_X$ est d'indice non divisible par p puisque $|A| = |\mathbf{G}/\mathbf{G}_X|$. Son cardinal est donc égal à $p^k m'$ où p ne divise pas m'. Mais si x_1 est un élément de X, les gx_1 où $g \in \mathbf{G}_X$ sont distincts et sont dans X. Il y en a moins de p^k, le stabilisateur $\mathbf{G}_X$ a donc moins de p^k éléments, donc exactement p^k éléments, c'est un p-Sylow. On comprendra mieux cette démonstration si on la fait fonctionner sur un exemple, disons le groupe diédral $\mathbb{D}_{10}$, avec $p = 2$. Il y a

45 parties à deux éléments qui se découpent en deux orbites à 10 éléments et trois à 5 éléments. Par exemple, l'orbite de $\{s, r\}$ (avec les notations habituelles) a 5 éléments, et le stabilisateur de $x_1 = \{s, r\}$ est $\langle sr \rangle$, qui a deux éléments...

3) Dans cette action, les orbites ont pour cardinal l'indice dans **H** du stabilisateur d'un élément, donc une puissance de p. Mais comme $\mathbf{G}/\mathbf{S}$ est de cardinal m, il y a au moins une orbite de taille $p^0 = 1$. Soit $x\mathbf{S}$ élément de cette orbite. On a donc $hx\mathbf{S} = x\mathbf{S}$ pour tout $h \in \mathbf{H}$, ce qui équivaut à $\mathbf{H} \subset x\mathbf{S}x^{-1}$. Si maintenant **H** est un p-Sylow, il a même cardinal que **S** donc que $x\mathbf{S}x^{-1}$, il y a donc égalité. On a prouvé que tous les p-Sylow sont conjugués.

4) C'est une conséquence directe, les p-Sylow sont les conjugués de l'un d'entre eux **S** ; si donc il y a un seul p-Sylow, ce groupe coïncide avec ses conjugués, il est normal dans **G**. Réciproquement, si **S** est un p-Sylow normal dans **G**, il coïncide avec ses conjugués, et il n'y a qu'un seul p-Sylow.

5) On fait agir **S** sur l'ensemble des p-Sylow, par conjugaison cette fois. Les orbites sont encore de cardinal une puissance de p. Il y a une orbite ayant un seul élément, celle constituée de **S** lui-même. Reste à montrer qu'il n'y en a pas d'autre. Si en effet **Q** est seul dans son orbite, c'est que $x\mathbf{Q}x^{-1} = \mathbf{Q}$ pour tout x de **S**. Donc **S** est un sous-groupe du normalisateur de **Q** dans **G**. C'est alors un p-Sylow de ce normalisateur... Mais **Q** est le seul p-Sylow de son normalisateur (question précédente), donc $\mathbf{S} = \mathbf{Q}$. On a donc bien une seule orbite à un élément, et le nombre c_p de p-Sylow vérifie :

$$c_p \equiv 1 \pmod{p}$$

Comme, par ailleurs, c'est aussi le nombre des conjugués de **S**, c'est l'indice du normalisateur de **S**, donc un diviseur de m.

3.2.4 1) Les groupes commutatifs n'ont qu'un seul p-Sylow, puisque tous les sous-groupes sont normaux. Ainsi, si $n = p^k m$, dans $\mathbb{Z}/n$, il y a un seul groupe à p^k éléments, ce qu'on savait déjà. En revanche, il est moins direct de vérifier que $\mathbb{Z}/6 \times \mathbb{Z}/12$ n'a qu'un sous-groupe d'ordre 9, qui ne peut être que le groupe « rectangle » $2\mathbb{Z}/6 \times 4\mathbb{Z}/12$.
Si $p \neq 2$, le groupe diédral $\mathbb{D}_{2n}$ a un seul p-Sylow. Posons

$$\mathbb{D}_{2n} = \langle r, s \mid r^n = s^2 = e,\ srs = r^{-1} \rangle \text{ avec } n = p^k m \text{ où } p \text{ ne divise pas } m$$

Le groupe engendré par r^m est un p-Sylow, et il est normal dans $\mathbb{D}_{2n}$.
Si $p = 2$, et le groupe engendré par r^m et s est un 2-Sylow, mais il n'est pas normal, et il existe d'autres 2-Sylow, engendrés par r^m et un élément d'ordre deux $r^k s$. On peut vérifier qu'il y a alors m 2-Sylow de cette forme.

2) Les 2-Sylow de $\mathcal{S}_4$ ont huit éléments. On en trouve un en utilisant les éléments d'ordre 2 ou 4, le groupe cyclique engendré par $(1, 2, 3, 4)$ peut être complété en un 2-Sylow en utilisant $\tau = (1, 3)$. Comme $\tau(1, 2, 3, 4)\tau = (1, 2, 3, 4)^{-1}$, on reconnaît le groupe diédral $\mathbb{D}_8$.
Le nombre des 2-Sylow peut être 1 ou 3. Le premier cas est exclu, car le groupe obtenu ne contient pas tous les éléments d'ordre 2 ou 4. Il y a donc trois 2-Sylow, isomorphes à $\mathbb{D}_8$. Ils sont égaux à leur normalisateur, car l'indice du normalisateur est 3.
Les 2-Sylow de $\mathcal{S}_5$ ont aussi huit éléments, et ils se décrivent de la même façon que pour $\mathcal{S}_4$. Leur nombre est impair, diviseur de 15. Il y en a effectivement 15, puisqu'il y en a 5 fois plus que dans le cas $n = 4$. La structure des p-Sylow de $\mathcal{S}_n$ est connue, elle utilise la notion de « produit en couronne » : voir le problème correspondant du dernier chapitre.

3.2.5 1) Pour $n = 42 = 2 \times 3 \times 7$, le nombre des 7-Sylow vérifie $s_7 \equiv 1 \pmod 7$ et $s_7|6$. La seule solution est 1, il y a un seul 7-Sylow qui est normal.
Pour les autres groupes, c'est un peu moins direct. Pour $n = 105 = 3 \times 5 \times 7$, le nombre des 7-Sylow divise 15, et est congru à 1 modulo 7, c'est 1 ou 15. Mais si c'était 15, il y aurait 6 éléments d'ordre 7 dans chaque 7-Sylow, donc, comme ils ne peuvent s'intersecter qu'en l'élément neutre (Lagrange), un total de $6 \times 15 = 90$ éléments. Comptons alors les 5-Sylow, leur nombre divise 21 et est congru à 1 modulo 5, si c'est 21, comme chaque 5-Sylow contient 4 éléments d'ordre 5, on dépasse l'effectif du groupe.
De la même façon, pour $n = 30$, $s_2 = 1, 3, 5, 15$, $s_3 = 1, 10$, $s_5 = 1, 6$, et l'hypothèse $s_5 = 6$ donne 24 éléments d'ordre 5, l'hypothèse $s_3 = 10$ donne 20 éléments d'ordre 3, ce qui est absurde.

2) Cette question généralise le cas 105. Supposons $p > q > r$ et que le groupe soit simple. Alors le nombre de p-Sylow est un diviseur de qr différent de 1. Comme il est plus grand que p, car congru à 1 modulo p, c'est qr. De même, le nombre de q-Sylow divise pr et est plus grand que q, c'est donc au moins p, le nombre des r-Sylow divise pq et est au moins égal à q. Si l'on additionne les nombres des éléments d'ordre p, q, r, et le neutre, on trouve :

$$\begin{aligned}(p-1)qr + (q-1)p + (r-1)q + 1 &= pqr + pq - p - q + 1 \\ &= pqr + (p-1)(q-1) > pqr\end{aligned}$$

ce qui est absurde.

3.2.6 $300 = 2^2 \times 3 \times 5^2$; le nombre des 5-Sylow est donc 1 ou un diviseur de 12 congru à 1 modulo 5. Supposons le groupe $\mathbf{G}$ non simple, il y a six 5-Sylow, et le normalisateur $\mathbf{N}$ d'un de ces 5-Sylow est d'indice 6. Ainsi, $\mathbf{G}$ agit par translation sur $\mathbf{G}/\mathbf{N}$, ensemble de six éléments. Cette action est forcément fidèle, car son noyau est un sous-groupe normal de $\mathbf{G}$ qui ne peut être égal à $\mathbf{G}$. Le groupe $\mathbf{G}$, de cardinal 300 est isomorphe à un sous-groupe de $\mathcal{S}_6$, de cardinal 720, ce qui est absurde.

3.2.7 Si $\mathbf{G}$ a un sous-groupe $\mathbf{H}$ d'indice r, alors il agit par translations sur le quotient $\mathbf{G}/\mathbf{H}$. Le noyau de cette action est un sous-groupe normal de $\mathbf{G}$. Ce ne peut être $\mathbf{G}$, car l'action n'est pas triviale, c'est donc $\{e\}$, et $\mathbf{G}$ est isomorphe à un sous-groupe du groupe des permutations d'un ensemble à r éléments. Or cela est incompatible avec l'hypothèse sur le cardinal. Ainsi un groupe simple n'a pas de « grand » sous-groupe. Par exemple, un groupe simple d'ordre 60 (il en existe un, c'est $\mathcal{A}_5$) n'a pas de sous-groupe d'indice 2, 3 ou 4, donc pas de sous-groupe de cardinal 30, 15 ou 20.

3.2.8 1) Il faut démontrer que deux 3-cycles quelconques sont conjugués dans $\mathcal{A}_5$. Si l'on prend cinq entiers distincts, les calculs suivants de conjugués :

$$\begin{aligned}(il)(jm)(ijk)(jm)(il) &= (lmk) \\ (ilm)(ijk)(ilm)^{-1} &= (ljk) \\ (ik)(lm)(ijk)(lm)(ik) &= (ikj)\end{aligned}$$

montrent que tout 3-cycle est conjugué d'un 3-cycle quelconque par un élément de $\mathcal{A}_n$. Et cela ne marche pas pour $n = 3$, les deux 3-cycles ne sont pas conjugués dans $\mathcal{A}_3$. De même, dans $\mathcal{A}_4$, il y a deux classes de conjugaison pour les 3-cycles (en particulier, un 3-cycle n'est pas conjugué à son carré). Pour les doubles transpositions, on rappelle (2.4.4) qu'elles sont conjuguées dans $\mathcal{S}_n$ c'est-à-dire qu'il existe σ telle que $\sigma(1,2)(3,4)\sigma^{-1} = (ij)(kl)$. Il suffit de prendre une permutation qui transforme 1 en i, 2 en j... Si σ est paire, c'est

terminé, sinon, il suffit de considérer $(ij)\sigma$. Remarquons qu'ici $n \geqslant 4$ suffit, les doubles transpositions ne forment qu'une classe dans $\mathcal{A}_4$. Cette classe est d'ailleurs le sous-groupe normal de $\mathcal{A}_4$.

2) Soit $\mathbf{H}$ normal dans $\mathcal{A}_5$. Alors $\mathbf{H}$ est formé de classes de conjugaison. S'il contient un élément d'ordre 5, il contient le sous-groupe engendré qui est un 5-Sylow. Mais alors il contient tous les conjugués, donc tous les autres 5-Sylow, soit les 24 éléments d'ordre 5.

3) Par la première question, si $\mathbf{H}$ normal dans $\mathcal{A}_5$ contient un élément d'ordre 2, il les contient tous (ce sont les doubles transpositions, il y en a 15). Enfin, s'il contient des éléments d'ordre 3, il les contient tous, cela fait 20. Mais, en ajoutant l'identité, on obtient comme cardinaux possibles : 16, 21, 25, 36, 40, 45 qui ne sont pas des diviseurs de 60. Les seules solutions sont $\mathbf{H} = \{id\}$ ou $\mathbf{H} = \mathcal{A}_5$, $\mathcal{A}_5$ est donc simple.

3.2.9 1) Il suffit d'écrire $(\sigma\tau\sigma^{-1})\tau^{-1}$, le terme entre parenthèses est un conjugué de τ et est donc dans $\mathbf{H}$.

2) Remarquons que le choix proposé est possible, si l'on prend bien sûr $\tau \neq id$. Prenons $\sigma = (i, k, j)$. Alors :

$$\sigma(\tau\sigma^{-1}\tau^{-1}) = (i, k, j)(j, \tau(j), \tau(k))$$

et donc seuls $(i, j, k, \tau(k), \tau(j))$ sont transformés, ce qui fait au plus 5 éléments.

3) La permutation précédente, notée ρ, est donc (elle est paire), soit l'identité, soit un 3-cycle, soit un 5-cycle, soit une double transposition. Si ρ était l'identité, on aurait $(i, j, k) = (\tau(k), j, \tau(j))$ et donc $k = \tau(j)$ ce qui est exclu par hypothèse. Supposons que ρ soit un 3-cycle, $\mathbf{H}$ contient un 3-cycle... Dans le cas où $\rho = (a, b, c, d, e)$:

$$(a, b, c)\rho(a, b, c)^{-1}\rho^{-1} = (a, b, d)$$

et $\mathbf{H}$ contient aussi un 3-cycle. Enfin, si $\rho = (a, b)(c, d)$

$$(a, b, e)\rho(a, b, e)^{-1}\rho^{-1} = (a, e, b)$$

et $\mathbf{H}$ contient également un 3-cycle. Comme $\mathbf{H}$ est normal dans $\mathcal{A}_n$, il contient tous les 3-cycles, (puisque, d'après l'exercice précédent, tous les 3-cycles sont conjugués dans $\mathcal{A}_n$) ; or les 3-cycles engendrent $\mathcal{A}_n$ (2.4.10). $\mathbf{H}$ est donc égal à $\mathcal{A}_n$, et $\mathcal{A}_n$ est simple.

3.2.10 On est donc dans le cas où $\mathcal{A}_n$ est simple puisque $n \geqslant 5$. Soit $\mathbf{H}$ un sous-groupe normal de $\mathcal{S}_n$. Alors $\mathbf{H} \cap \mathcal{A}_n$ doit être un sous-groupe normal de $\mathcal{A}_n$; le conjugué d'un élément pair de $\mathbf{H}$ est encore un élément pair de $\mathbf{H}$. Si cette intersection est $\mathcal{A}_n$, alors $\mathbf{H} = \mathcal{A}_n$, puisque le groupe alterné est d'indice 2, et donc maximal, ou bien $\mathbf{H} \cap \mathcal{A}_n = \{id\}$. Mais dans ce cas, $\mathbf{H}$ ne peut contenir que l'identité et des permutations impaires. Soit x une telle permutation. Alors, si y en est une autre, $xy \in \mathbf{H}$ est paire, donc est l'identité. Donc $\mathbf{H}$ ne peut contenir que id, x, x^{-1}, et l'on a forcément $x = x^{-1}$ car une permutation impaire ne peut pas être d'ordre 3. Mais alors, $\mathbf{H}$ normal implique que $zxz^{-1} \in \{id, x\}$, et si x était différent de id, il serait dans le centre de $\mathcal{S}_n$... qui est réduit à id. C'est terminé, $\mathcal{S}_n$ ne contient, comme sous-groupe normal, que les sous-groupes triviaux et le groupe alterné.

3.2.11 1) $\mathbf{G}$ agit donc par $g.x\mathbf{H} = gx\mathbf{H}$; et donc g est dans le noyau si, pour tout $x \in \mathbf{G}$, $gx\mathbf{H} = x\mathbf{H}$, c'est-à-dire $g \in x\mathbf{H}x^{-1}$. Le noyau de l'action est donc l'intersection des conjugués de $\mathbf{H}$. Le cas particulier où $\mathbf{H}$ est normal dans $\mathbf{G}$ donne un noyau égal

à $\mathbf{H}$; c'est ...normal, on a alors une action fidèle de $\mathbf{G}/\mathbf{H}$ sur $\mathbf{G}/\mathbf{H}$ qui est la translation à gauche de ce groupe.

2) Soit :
$$\mathbf{K} = \bigcap_{x \in \mathbf{G}} x\mathbf{H}x^{-1}$$
Alors $y\mathbf{K}y^{-1}$ est égal à $\mathbf{K}$ car $y \mapsto yx$ est une bijection de $\mathbf{G}$, donc $\mathbf{K} \lhd \mathbf{G}$. Par ailleurs, si $\mathbf{N} \lhd \mathbf{G}$, et $\mathbf{N} \leqslant \mathbf{H}$, alors
$$\forall x \in \mathbf{G},\ x\mathbf{N}x^{-1} = \mathbf{N} \leqslant x\mathbf{H}x^{-1}$$
et donc $\mathbf{N}$ est inclus dans l'intersection des conjugués de $\mathbf{H}$ [1].

3) Nous ne traiterons pas les valeurs de $n \leqslant 5$. Cela se fait « à la main ». Considérons l'action de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$, on en déduit un morphisme de $\mathbf{G}$ dans le groupe symétrique de $\mathbf{G}/\mathbf{H}$ qui possède n éléments. Le noyau de cette action est normal dans $\mathbf{G}$, et c'est aussi l'intersection des conjugués de $\mathbf{H}$; il est donc inclus dans $\mathbf{H}$, et ne peut être égal au groupe alterné qui est d'indice 2 alors que $\mathbf{H}$ est d'indice n. D'après l'exercice précédent, ce ne peut être que l'identité. On en déduit que $\mathbf{G}$ est isomorphe à un groupe symétrique d'un ensemble de n éléments... Mais $\mathbf{H}$ se présente alors comme un stabilisateur, celui de la classe de e. C'est le stabilisateur d'un élément dans un groupe de permutation de n éléments. C'est donc un groupe isomorphe à $\mathcal{S}_{n-1}$. Pour terminer, il faut comprendre que $\mathbf{H}$ peut bien sûr être déjà dans $\mathbf{G}$ le stabilisateur d'un point (il y a n tels groupes). Ce que nous avons montré c'est que, dans tous les cas, $\mathbf{H}$ est isomorphe à $\mathcal{S}_{n-1}$. Cela dit... il n'est pas sûr qu'il existe beaucoup de sous-groupes d'indice n qui ne soient pas stabilisateur d'un élément. Nous aurons l'occasion d'y revenir dans l'exercice 3.3.8.

3.2.12 On considère à nouveau l'action par translation de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$ où $\mathbf{H}$ est d'indice p. Alors le noyau de cette action est un sous-groupe $\mathbf{N}$ normal dans $\mathbf{G}$ et inclus dans $\mathbf{H}$. Mais alors $\mathbf{G}/\mathbf{N}$ est isomorphe à un sous-groupe du groupe symétrique $\mathcal{S}_p$. Comme l'indice de $\mathbf{N}$ est aussi un diviseur du cardinal de $\mathbf{G}$, ce ne peut-être que 1 ou p. Le cas 1 est exclu, car $\mathbf{N}$ est inclus dans $\mathbf{H}$. C'est donc que $\mathbf{N} = \mathbf{H}$, $\mathbf{H}$ est normal dans $\mathbf{G}$. Rappelons que nous avons déjà démontré (plus directement) que tout sous-groupe d'indice 2 dans $\mathbf{G}$ est normal dans $\mathbf{G}$ (1.2.21).

3.2.13 Soit $\mathbf{N}$ le normalisateur dans $\mathbf{G}$ d'un p-Sylow $\mathbf{S}$ et soit $g \in \mathbf{G}$ qui normalise $\mathbf{N}$, $g\mathbf{N}g^{-1} = \mathbf{N}$. Considérons alors $g\mathbf{S}g^{-1}$. C'est un sous-groupe de $\mathbf{N}$. Mais $\mathbf{S}$ est un p-Sylow de $\mathbf{G}$, donc un p-Sylow de $\mathbf{N}$ (puisque $\mathbf{S} \leqslant \mathbf{N} \leqslant \mathbf{G}$) ; et, par définition du normalisateur, $\mathbf{S}$ est normal dans $\mathbf{N}$. Donc $\mathbf{N}$ ne contient qu'un seul p-Sylow et $g\mathbf{S}g^{-1} = \mathbf{S}$ ce qui prouve qu'en fait g normalise aussi $\mathbf{S}$ et donc $g \in \mathbf{N}$. On a bien prouvé que $\mathbf{N}$ est son propre normalisateur. Si $\mathbf{S}$ est autonormalisant, il est son propre normalisateur, et le nombre de ses conjugués est maximum (il vaut $\frac{|\mathbf{G}|}{|\mathbf{S}|}$). C'est, par exemple, le cas des 2-Sylow de $\mathcal{S}_4$ ou de $\mathcal{S}_5$.

Étudions maintenant le cas d'un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ qui contient le normalisateur $\mathbf{N}$ du p-Sylow $\mathbf{S}$. Soit x normalisant $\mathbf{H}$. Alors, $x\mathbf{S}x^{-1}$ est un p-Sylow de $\mathbf{H}$, donc (théorème de Sylow), conjugué de $\mathbf{S}$ dans $\mathbf{H}$. Cela signifie qu'il existe $y \in \mathbf{H}$ tel que :
$$x\mathbf{S}x^{-1} = y\mathbf{S}y^{-1}$$

1. Ce plus grand sous-groupe normal de $\mathbf{G}$ inclus dans $\mathbf{H}$ se nomme en anglais le *core* de $\mathbf{H}$, ce qui peut se traduire par cœur.

Mais alors x et y sont conjugués modulo $\mathbf{N} \subset \mathbf{H}$. Comme $y \in \mathbf{H}$, on en déduit que $x \in \mathbf{H}$.

3.2.14 Soit g quelconque dans $\mathbf{G}$. On a $g\mathbf{S}g^{-1} \leqslant g\mathbf{N}g^{-1} = \mathbf{N}$, d'où la première affirmation. Mais $\mathbf{S}$ étant un p-Sylow de $\mathbf{N}$, $g\mathbf{S}g^{-1}$ en est aussi un p-Sylow, et il existe $n \in \mathbf{N}$ tel que $g\mathbf{S}g^{-1} = n\mathbf{S}n^{-1}$. Or cette égalité équivaut à $n^{-1}g \in \mathbf{N_G}(\mathbf{S})$ d'où le résultat :

$$\mathbf{G} = \mathbf{N}\mathcal{N}_{\mathbf{G}}(\mathbf{S})$$

3.2.15 1) $\mathbb{E}$ est de cardinal n^{p-1}, car les $p-1$ premiers éléments de la liste $(x_1, x_2, \ldots, x_p)$ déterminent le dernier, $x_p = (x_1 \ldots x_{p-1})^{-1}$.

2) $\mathbb{Z}/p$ agit par :

$$k.(x_1, x_2, \ldots, x_p) = (x_{k+1}, x_{k+2}, \ldots, x_{k+p})$$

avec la convention que les indices sont définis « modulo p ». C'est l'action naturelle de $\langle\sigma\rangle$ où $\sigma = (1, 2, \ldots, p)$ est une permutation circulaire. Il faut néanmoins vérifier que l'on a encore

$$x_{k+1}x_{k+2} \ldots x_{k+p} = 1$$

Cela se voit facilement par récurrence :

$$x_1x_2 \ldots x_p = 1 \Rightarrow x_2x_3 \ldots x_1 = 1$$

car x_1 est le symétrique de $x_2x_3 \ldots x_p$. On peut également remarquer que tous ces éléments sont conjugués. Une orbite aura un élément lorsque $x_1 = x_2 = \ldots = x_p = x$. Un tel élément x vérifie dont $x^p = e$. Soit c'est e, soit c'est un élément d'ordre p, puisque p est premier. Si $x_1 \neq x_2$, alors l'orbite a p éléments ; pour s'en convaincre, on peut voir que le stabilisateur d'un élément est soit $\mathbb{Z}/p$, soit $\{e\}$ puisque p est premier.

3) La formule des classes s'écrit donc :

$$n^{p-1} = r + ps$$

où r est le nombre des orbites à un élément, s celui des orbites à p éléments. Le nombre r est multiple de p. Comme il est non nul (à cause de e), il est strictement plus grand que 1 et il y a au moins un élément d'ordre p.

4) Les hypothèses faites sur p assurent l'existence d'un p-Sylow. Dans ce p-Sylow, un élément différent du neutre engendre un groupe cyclique d'ordre une puissance de p qui contient un élément d'ordre p ; la démonstration est beaucoup plus simple, mais le théorème de Cauchy sert aussi de base à d'autres démonstrations des théorèmes de Sylow, d'où l'intérêt de le démontrer indépendamment des théorèmes de Sylow.

3.2.16 Si le cardinal est une puissance de p, alors tout élément a pour ordre une puissance de p, par le théorème de Lagrange. Réciproquement, si le cardinal de $\mathbf{G}$ contient un autre facteur premier que p, mettons q, alors il existe un élément d'ordre q (théorème de Cauchy). Donc $\mathbf{G}$ n'est pas un p-groupe.
Un p-groupe infini intéressant est le p-groupe de Prüfer, ensemble des racines p^n-ièmes de l'unité lorsque n parcourt $\mathbb{N}$. Voir le second problème du chapitre 2. Un produit infini de p-groupes finis conviendra également, l'ensemble des suites à valeurs dans $\mathbb{Z}/2$ est un 2-groupe pour l'addition.

3.2.17 $\mathbf{H}$ agit sur ses conjugués par $h.x\mathbf{H}x^{-1} = hx\mathbf{H}x^{-1}h^{-1}$. Dans cette action, $\mathbf{H}$ est seul dans son orbite. Comme $\mathbf{H}$ est un p-groupe, l'équation des classes montre qu'il existe une autre orbite à un seul élément, mettons $g\mathbf{H}g^{-1} \neq \mathbf{H}$. Mais alors

$$\forall h \in \mathbf{H},\ hg\mathbf{H}g^{-1}h^{-1} = g\mathbf{H}g^{-1} \Rightarrow g^{-1}hg\mathbf{H}g^{-1}h^{-1}g = \mathbf{H}$$

prouve que tout élément de $g^{-1}\mathbf{H}g$ normalise $\mathbf{H}$. Il y a un conjugué inclus dans le normalisateur. Donc, si $\mathbf{H}$ n'est pas normal dans $\mathbf{G}$, on a prouvé :

$$\mathbf{H} < \mathcal{N}_{\mathbf{G}}(\mathbf{H}) < \mathbf{G}$$

et $\mathbf{H}$ n'est pas autonormalisant.

3.2.18 1) La fin de l'exercice précédent montre en effet que si $\mathbf{H}$ est maximal parmi les sous-groupes de $\mathbf{G}$, alors il est normal dans $\mathbf{G}$. Le quotient $\mathbf{G}/\mathbf{H}$ est alors un p-groupe qui n'a pas de sous-groupe non trivial (sinon $\mathbf{H}$ ne serait pas maximal, *cf.* le théorème de correspondance), c'est donc un groupe cyclique à p éléments, et $\mathbf{H}$ est d'indice p. Ce résultat est faux si $\mathbf{G}$ n'est pas un p-groupe, il suffit de prendre comme exemple un groupe simple non commutatif.

2) Faisons un raisonnement par récurrence. Supposons que tout p-groupe de cardinal p^k où $k < n$ vérifie la propriété. La récurrence est amorcée sans problème pour $k = 1$, et soit $\mathbf{G}$ un groupe d'ordre p^n. Nous savons que le centre $\mathcal{Z}(\mathbf{G})$ est non trivial. Il contient un élément x d'ordre p (parce qu'il est commutatif, mais on peut aussi utiliser le théorème de Cauchy), et $\langle x\rangle$ sous-groupe du centre est normal dans $\mathbf{G}$. On peut alors considérer $\mathbf{G}/\langle x\rangle$, qui est différent de $\mathbf{G}$, et lui appliquer l'hypothèse de récurrence. Cela (par le théorème de correspondance) donne des sous-groupes normaux de tout ordre p^k contenant $\langle x\rangle$. En ajoutant $\langle x\rangle$ lui-même, la propriété est démontrée.

3) Soit maintenant $\mathbf{K}$ un sous-groupe strict d'un p-groupe $\mathbf{G}$. Alors $\mathbf{K}$ est inclus dans un sous-groupe maximal $\mathbf{K}_0$ de $\mathbf{G}$. On considère en effet l'ensemble des sous-groupes contenant $\mathbf{K}$, et l'on prend un de ceux qui ont le cardinal maximal. Ce sous-groupe est normal dans $\mathbf{G}$ d'après l'exercice précédent, et d'indice p. Si ce n'est pas $\mathbf{K}$, on recommence...
Dans les cas de $\mathbb{H}_8$, les chaînes de sous-groupes sont du type :

$$\{e\} \lhd \langle -e\rangle \lhd \langle i\rangle \lhd \mathbb{H}_8$$

en utilisant les notations $\mathbb{H}_8 = \{e, -e, i, j, k, -i, -j, -k\}$.

Dans le cas du groupe diédral $\mathbb{D}_8$ engendré par a d'ordre 4 et b d'ordre 2, il y a deux types de chaînes :

$$\{e\} \lhd \langle a^2\rangle \lhd \langle a\rangle \lhd \mathbb{D}_8 \quad \text{et} \quad \{e\} \lhd \langle b\rangle \lhd \langle a^2, b\rangle \lhd \mathbb{D}_8$$

3.2.19 De façon intuitive, un groupe est pronormal dans $\mathbf{G}$ s'il est « assez proche » de ses conjugués. Mais cette idée est vague, et l'exercice est un peu rude à résoudre.

1) Un p-Sylow $\mathbf{S}$ de $\mathbf{G}$ est pronormal dans $\mathbf{G}$, pour tout x de $\mathbf{G}$, $x\mathbf{S}x^{-1}$ est un p-Sylow d'un groupe qui le contient, donc de $\mathbf{H} = \langle \mathbf{S}, x\mathbf{S}x^{-1}\rangle$; il est donc conjugué de $\mathbf{S}$ dans $\mathbf{H}$, par le second théorème de Sylow.

2) C'est pratiquement le même argument. Si $\mathbf{S} \leqslant \mathbf{K} \lhd \mathbf{G}$ alors pour tout x de $\mathbf{G}$, $x\mathbf{S}x^{-1} \leqslant x\mathbf{K}x^{-1} = \mathbf{K}$. Si donc $\mathbf{S}$ est un p-Sylow de $\mathbf{K}$, c'est aussi le cas de $x\mathbf{S}x^{-1}$ et $\mathbf{S}$ et son conjugué sont des p-Sylow de $\mathbf{H} = \langle \mathbf{S}, x\mathbf{S}x^{-1}\rangle$ puisque ce groupe est inclus dans $\mathbf{K}$. On continue comme dans la première question.

3) • Supposons que $\mathbf{H}$ soit un p-groupe pronormal dans $\mathbf{G}$. Alors $\mathbf{H}$ est un sous-groupe d'un p-Sylow $\mathbf{S}$, en utilisant encore le second théorème de Sylow. Montrons que tout conjugué $x\mathbf{H}x^{-1}$, qui est inclus dans $\mathbf{S}$, est confondu avec $\mathbf{H}$. En effet, soit $\mathbf{K} = \langle \mathbf{H}, x\mathbf{H}x^{-1} \rangle$. C'est un sous-groupe de $\mathbf{S}$, donc un p-groupe. Si $\mathbf{H}$ est un sous-groupe strict de $\mathbf{K}$, il existe alors un sous-groupe $\mathbf{K}_1$ maximal dans $\mathbf{K}$, normal dans $\mathbf{K}$, contenant $\mathbf{H}$, et donc ne contenant pas $x\mathbf{H}x^{-1}$. Comme $\mathbf{H}$ est pronormal dans $\mathbf{G}$, il existe $y \in \mathbf{K}$ tel que $x\mathbf{H}x^{-1} = y\mathbf{H}y^{-1}$. Mais alors, $\mathbf{H} \leqslant \mathbf{K}_1 \Rightarrow y\mathbf{H}y^{-1} \leqslant y\mathbf{K}_1y^{-1} = \mathbf{K}_1$ ce qui est absurde. On en déduit que $\mathbf{S}$ contient un seul des conjugués de $\mathbf{H}$, et, par conjugaison, que tout p-Sylow de $\mathbf{G}$ contient un seul conjugué de $\mathbf{H}$.
• Supposons maintenant que $\mathbf{H}$ soit un p-groupe, et que chaque p-Sylow de $\mathbf{G}$ ne contienne qu'un de ses conjugués (il y en a au moins un car tous les p-Sylow sont conjugués). Soit alors $x\mathbf{H}x^{-1}$ un conjugué de $\mathbf{H}$ distinct de $\mathbf{H}$, et $\mathbf{K} = \langle \mathbf{H}, x\mathbf{H}x^{-1} \rangle$. Alors $\mathbf{K}$ n'est pas un p-groupe (sinon il serait contenu dans un p-Sylow, ce qui contredit l'hypothèse sur $\mathbf{H}$). Soit donc $\mathbf{T}$ un p-Sylow de $\mathbf{K}$ contenant $\mathbf{H}$. Alors $x\mathbf{H}x^{-1}$ est contenu dans un p-Sylow de $\mathbf{K}$, qui est de la forme $y\mathbf{T}y^{-1}$ où $y \in \mathbf{K}$. Considérons maintenant le p-Sylow $\mathbf{S}$ de $\mathbf{G}$ contenant $\mathbf{H}$. Alors $y\mathbf{S}y^{-1}$ est un p-Sylow de $\mathbf{G}$ qui contient $y\mathbf{T}y^{-1}$, et donc $x\mathbf{H}x^{-1}$. Mais il contient aussi $y\mathbf{H}y^{-1}$; par l'hypothèse, on en conclut $x\mathbf{H}x^{-1} = y\mathbf{H}y^{-1}$, qu'il fallait démontrer. Pour suivre, faire un dessin.

4) Un exemple de sous-groupe qui est pronormal sans être normal. $\mathbf{H} = \langle (1,2) \rangle$, sous-groupe de $\mathcal{S}_3$; ce n'est pas un sous-groupe normal de $\mathcal{S}_3$, mais il est pronormal car maximal, $\langle \mathbf{H}, x\mathbf{H}x^{-1} \rangle$ est égal à $\mathcal{S}_3$ pour tout x non dans $\mathbf{H}$.

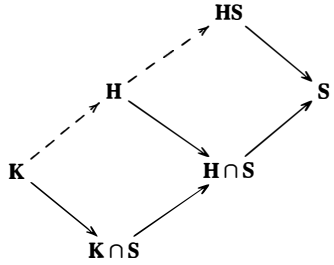
3.2.20 1) C'est exactement le résultat de la dernière question de l'exercice 3.2.18.

2) Prenons un exemple dans le 2-groupe $\mathbb{D}_8$. Le sous-groupe engendré par b d'ordre 2 n'est pas normal, mais il est sous-normal. Les groupes symétriques ont très peu de groupes sous-normaux, dès que $n \geqslant 5$, le groupe alterné est simple et il est le seul sous-groupe normal de $\mathcal{S}_n$; il n'y a pas d'autre sous-groupe sous-normal non trivial.

3) Si ϕ est un morphisme surjectif, il transforme un sous-groupe normal en un sous-groupe normal, et donc conserve la sous-normalité. En particulier, les conjugués d'un groupe sous-normal dans $\mathbf{G}$ sont sous-normaux dans $\mathbf{G}$. Si ϕ n'est plus surjectif, l'image d'un sous-groupe sous-normal est sous-normale dans l'image.

4) Le plus direct est d'utiliser le second théorème d'isomorphisme : $\mathbf{S}$ est un p-Sylow de $\mathbf{HS}$ et donc $|\mathbf{HS}| = p^n m$ où m est premier à p. Si donc m' est le cardinal de $\mathbf{H}$ et p^k celui de $\mathbf{H} \cap \mathbf{S}$, l'isomorphisme :
$$\mathbf{HS}/\mathbf{H} \cong \mathbf{S}/\mathbf{H} \cap \mathbf{S}$$
prouve que $mp^n/m' = p^n/p^k$ et donc $m' = mp^k$ qui prouve que $\mathbf{H} \cap \mathbf{S}$ est un p-Sylow de $\mathbf{H}$.

5) Il suffit de refaire le même calcul en utilisant le schéma suivant :



et d'itérer. Remarquons que le résultat ne subsiste plus si l'on ne fait aucune hypothèse sur **H**. Cependant, on peut montrer que si **H** est un sous-groupe quelconque de **G**, et **S** un p-Sylow, alors il existe un p-Sylow $a\mathbf{S}a^{-1}$ tel que $a\mathbf{S}a^{-1} \cap \mathbf{H}$ soit un p-Sylow de **H**. C'est le point de départ d'une démonstration du premier théorème de Sylow [21].

6) Soit **K** un sous-groupe à la fois pronormal et sous-normal dans **G**. Supposons que $\mathbf{K} \lhd \mathbf{H} \lhd \mathbf{L}$ et considérons $x\mathbf{K}x^{-1}$ où $x \in \mathbf{L}$. Alors $\mathbf{K} \leqslant \mathbf{H} \Rightarrow x\mathbf{K}x^{-1} \leqslant x\mathbf{H}x^{-1} = \mathbf{H}$ puisque **H** est normal dans **L**. Et donc le sous-groupe engendré par **K** et $x\mathbf{K}x^{-1}$ est inclus dans **H** ; comme **K** est pronormal, il existe $y \in \mathbf{H}$ tel que $x\mathbf{K}x^{-1} = y\mathbf{K}y^{-1} = \mathbf{K}$, car **K** est normal dans **H**. On a donc montré que **K** est normal dans **L**, d'où, en itérant, le résultat demandé : la pronormalité peut être redéfinie comme étant ce qui manque à un groupe sous-normal pour être normal...

3.3 PRODUITS SEMI-DIRECTS

Introduisons un vocabulaire bien utile pour étudier les groupes, et plus précisément les morphismes. Si a et b sont deux morphismes tels que $b \circ a$ existe, on schématise :

$$\mathbf{N} \xrightarrow{a} \mathbf{G} \xrightarrow{b} \mathbf{K}$$

On dit que cette suite est **exacte en G** si

$$\operatorname{Ker} b = \operatorname{Im} a$$

Le cas le plus intéressant est celui d'une suite :

$$e \longrightarrow \mathbf{N} \xrightarrow{a} \mathbf{G} \xrightarrow{b} \mathbf{K} \longrightarrow e$$

qui est exacte en **N**, **G** et **K**. On dit alors que c'est une **suite exacte courte**. Par abus, on note e le groupe réduit à un élément ; on écrira au besoin aussi 0 ou 1.

Exercice 3.3.1

1) Montrer que dans le cas d'une suite exacte courte, a est injectif et b est surjectif.
2) Montrer que $a(\mathbf{N}) \lhd \mathbf{G}$ et $\mathbf{K} \cong \mathbf{G}/a(\mathbf{N})$.
3) Montrer que tout morphisme entre deux groupes permet de définir une suite exacte.

Examinons le cas où **G** est produit direct de ses sous-groupes **N** et **K**.

Exercice 3.3.2

1) Démontrer qu'on peut définir un morphisme i de **N** dans $\mathbf{N} \times \mathbf{K}$ et un morphisme p de $\mathbf{N} \times \mathbf{K}$ dans **K**, de sorte que la suite

$$e \longrightarrow \mathbf{N} \xrightarrow{i} \mathbf{N} \times \mathbf{K} \xrightarrow{p} \mathbf{K} \longrightarrow e$$

soit exacte.

2) Peut-on échanger les rôles de **N** et de **K** ?

On va considérer maintenant une situation plus générale que le produit direct, où **G** sera encore le produit ensembliste de **N** et de **K**, et où il y aura encore une suite exacte. Prenons **N** et **K** deux groupes, et ϕ un morphisme de **K** dans Aut(**N**), c'est-à-dire une action de **K** sur **N**, mais une action « par automorphismes ». On notera donc $\phi(k)(n)$ ou $k.n$ l'image de n sous cette action et **G** le produit cartésien (ensembliste) de **N** par **K**.

Exercice 3.3.3

1) On définit alors une loi dans **G** par :

$$(n, k) * (n', k') = (n\phi(k)(n'),\ kk') = (n(k.n'),\ kk')$$

Montrer que **G** est un groupe.

2) Montrer que la suite :

$$1 \longrightarrow \mathbf{N} \xrightarrow{i} \mathbf{G} \xrightarrow{p} \mathbf{K} \longrightarrow 1$$

où $i(n) = (n, 1)$ et $p(n, k) = k$, est une suite exacte.

3) Que se passe t-il si $\phi(k) = \mathrm{id}$ pour tout $k \in \mathbf{K}$?

Cette construction est très pratique pour fabriquer des groupes, et aussi pour « démonter » des groupes que l'on connaît déjà. On appellera **produit semi-direct** ce groupe et l'on le notera $\mathbf{G} = \mathbf{N} \rtimes_\phi \mathbf{K}$ pour ne pas le confondre avec le produit direct $\mathbf{N} \times \mathbf{K}$. Le morphisme ϕ sera parfois sous-entendu. Voici un premier exemple.

Exercice 3.3.4

Démontrer que le groupe diédral $\mathbb{D}_{2n}$ est le produit semi-direct du groupe cyclique $\mathbb{Z}/n$ par $\mathbb{Z}/2$.

Avant de poursuivre les exemples, donnons une autre caractérisation des produits semi-directs avec un autre point de vue. Il s'agit maintenant de savoir si un groupe donné est un produit semi-direct de deux de ses sous-groupes. Une condition nécessaire est, bien sûr, qu'il admette au moins un sous-groupe normal, mais elle ne suffit pas. On va obtenir une condition nécessaire et suffisante, à rapprocher du critère de produit direct vu dans l'exercice 2.1.5. Ce résultat s'appellera « critère du produit semi-direct ».

Exercice 3.3.5

1) Soit $\mathbf{G} = \mathbf{N} \rtimes_\phi \mathbf{K}$ un produit semi-direct, et la suite exacte associée :

$$1 \longrightarrow \mathbf{N} \xrightarrow{i} \mathbf{G} \xrightarrow{p} \mathbf{K} \longrightarrow 1$$

On note $\mathcal{N}$ l'image de i, $\mathcal{K}$ l'ensemble des couples $(1, k)$ où $k \in \mathbf{K}$; démontrer que :

$$\mathcal{N} \lhd \mathbf{G} \qquad \mathcal{N} \cap \mathcal{K} = 1 \qquad \mathbf{G} = \mathcal{N}\mathcal{K}$$

2) Démontrer que l'action de $\mathbf{K}$ sur $\mathbf{N}$ se traduit, dans $\mathbf{G}$, par une action par automorphismes intérieurs.

3) Réciproquement, montrer que si deux sous-groupes $\mathbf{N}$ et $\mathbf{K}$ d'un groupe $\mathbf{G}$ satisfont :

$$\mathbf{N} \lhd \mathbf{G} \qquad \mathbf{N} \cap \mathbf{K} = 1 \qquad \mathbf{G} = \mathbf{NK}$$

alors $\mathbf{G}$ est isomorphe au produit semi-direct $\mathbf{N} \rtimes_\phi \mathbf{K}$ où $\phi(k)(n) = knk^{-1}$.

4) Avec les hypothèses de la question précédente, quand le produit semi-direct se révèle-t-il être un produit direct ?

5) À quelle condition un produit semi-direct est-il commutatif ?

6) Utiliser ce qui précède pour montrer que le groupe symétrique est produit semi-direct du groupe alterné et du groupe engendré par une transposition.

Continuons maintenant des exemples, d'abord avec des groupes cycliques.

Exercice 3.3.6

Soit $\mathbf{N} = \mathbb{Z}/3$ et $\mathbf{K} = \mathbb{Z}/4$, et l'on adoptera la notation multiplicative. Si y est générateur de $\mathbf{K}$, on définit une action par morphisme sur $\mathbf{N} = \langle x \rangle$ par $y.x = x^{-1}$.

1) Vérifier que cette condition définie bien une action par morphismes de $\mathbf{K}$ sur $\mathbf{N}$.

2) Montrer que le produit semi-direct ainsi obtenu est un groupe non commutatif à douze éléments non isomorphe au groupe diédral $\mathbb{D}_{12}$ ni au groupe alterné $\mathcal{A}_4$. On le note T. En donner une présentation.

3) Montrer que T est isomorphe au groupe de matrices de l'exercice 1.1.21, et au groupe dicyclique à douze éléments de l'exercice 2.3.5.

Pour définir des produits semi-directs, il est nécessaire de bien connaître les automorphismes ; continuons à nous intéresser aux groupes cycliques.

Exercice 3.3.7

1) Soit $\mathbf{G} = \mathbb{Z}/n$. Démontrer qu'un morphisme de $\mathbf{G}$ dans un groupe est déterminé par l'image d'un générateur.

2) En déduire que le groupe des automorphismes de $\mathbb{Z}/n$ est isomorphe à l'ensemble des inversibles de l'**anneau** $\mathbb{Z}/n$.

Parmi les groupes dont on peut obtenir le groupe des automorphismes, il y a les groupes symétriques.

Exercice 3.3.8

1) Examiner le cas de $\mathcal{S}_2$, $\mathcal{S}_3$ et $\mathcal{S}_4$.

2) Montrer que $\mathrm{Int}(\mathcal{S}_n) \cong \mathcal{S}_n$, pour $n > 2$.

3) Montrer que si ϕ est un automorphisme qui conserve les transpositions, alors ϕ est un automorphisme intérieur. On rappelle que $\mathcal{S}_n$ est engendré par les transpositions de la forme $(1,2),(1,3),\ldots,(1,n)$.
4) Montrer que si $n > 4$ et $n \neq 6$, il est nécessaire qu'un automorphisme conserve les transpositions. On pourra utiliser le fait que l'image d'une transposition est une permutation d'ordre 2, et utiliser des arguments de dénombrement. Conclure, dans ce cas, sur $\mathrm{Aut}(\mathcal{S}_n)$.
5) Montrer que si $\mathcal{S}_n$ contient un sous-groupe d'indice n qui n'est pas le stabilisateur d'un entier $1, 2, \ldots, n$, alors $\mathrm{Aut}(\mathcal{S}_n)$ contient un automorphisme intérieur.
6) Que dire sur le groupe $\mathrm{Aut}(\mathcal{S}_6)$?

Étudions maintenant des produits semi-directs fabriqués avec des groupes cycliques.

Exercice 3.3.9

Démontrer que pour qu'il existe un produit semi-direct non direct, $\mathbb{Z}/n \rtimes \mathbb{Z}/m$, il faut qu'il existe r, tel que $r^n \equiv 1 \pmod{m}$. Examiner les cas $m = 2$, puis $m = 3$. Existe t-il un produit semi-direct non trivial de la forme $\mathbb{Z}/4 \rtimes \mathbb{Z}/3$?

Revenons sur les suites exactes. Il est parfois possible de repérer sur une suite exacte si le groupe **G** est produit direct, ou semi-direct, des groupes **N** et **K**. Cela est très pratique quand on connaît seulement **N** et le morphisme dont il est le noyau.

Exercice 3.3.10

Soit une suite exacte :

$$e \longrightarrow \mathbf{N} \xrightarrow{i} \mathbf{G} \xrightarrow{p} \mathbf{K} \longrightarrow e$$

1) Démontrer que **G** est le produit semi-direct de **N** et de **K** ssi il existe un morphisme s : $\mathbf{K} \to \mathbf{G}$ tel que $p \circ s = id$. Ce morphisme s'appelle une **section**.
2) Démontrer que se donner une section équivaut à se donner un sous-groupe de **G** isomorphe à **K**, et dont les éléments sont dans des classes différentes modulo **N**. Ce sous-groupe s'appelle un **relèvement** de **K**.
3) Examiner à nouveau le cas du groupe symétrique et du groupe alterné.

Exercice 3.3.11

Soit $\mathbf{G} = \mathcal{A}_4$ le groupe alterné, et $\mathcal{V} = \{e, u, v, w\}$ le sous-groupe des doubles transpositions. On utilise les notations de 2.4.11.
Montrer que si $\mathbf{K} = \langle (1,2,3) \rangle$, alors $\mathcal{V}$ et **K** satisfont le critère de produit semi-direct, et en déduire que :

$$\mathcal{A}_4 \cong (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes_\phi \mathbb{Z}/3$$

À tout groupe on peut associer un produit semi-direct privilégié, son **holomorphe**.

Exercice 3.3.12

Soit **G** un groupe, Aut(**G**) le groupe de ses automorphismes. On appelle **holomorphe** de **G** et on note Hol(**G**) le produit semi-direct $\mathbf{G} \rtimes_\phi \mathrm{Aut}(\mathbf{G})$.

1) Préciser l'action ϕ.
2) Déterminer les holomorphes de $\mathbb{Z}$, $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/4$
3) Vérifier également que l'holomorphe du groupe de Klein est $\mathcal{S}_4$. On pourra commencer par établir que le groupe d'automorphismes du groupe de Klein est $\mathcal{S}_3$.
4) Étudier le groupe des automorphismes du groupe diédral. On vérifiera que le sous-groupe cyclique $\langle a \rangle$ doit être invariant, et l'on en déduira que :

$$\mathrm{Aut}(\mathbb{D}_{2n}) = \mathrm{Hol}(\mathbb{Z}/n)$$

Regardons maintenant des exemples de groupes qui ne sont pas des produits semi-directs. Dans le cas d'un groupe commutatif, la situation n'est pas très intéressante. Un produit semi-direct est forcément direct ; par ailleurs, un groupe comme $\mathbb{Z}/4$ n'est pas produit de son sous-groupe $2\mathbb{Z}/4$ avec un autre sous-groupe. Un autre contre-exemple est donné par le groupe quaternionique.

Exercice 3.3.13

1) Démontrer que le groupe quaternionique $\mathbb{H}_8$ n'est pas produit semi-direct de deux de ses sous-groupes (en éliminant bien sûr les cas « triviaux »).
2) Généraliser dans le cas d'un groupe dicyclique quelconque.

SOLUTIONS

3.3.1 1) Le premier morphisme est défini par $e \mapsto e$, donc le noyau de a est réduit à e, et a est injectif. Le dernier morphisme arrive dans e, c'est donc le morphisme constant à valeur e ; son noyau est **K** et c'est l'image de b. b est surjectif.

2) **N** est le noyau d'un morphisme, donc est normal dans **G** ; par ailleurs, le premier théorème d'isomorphisme permet de dire que **G**/**N** est isomorphe à l'image de b donc à **K**.

3) C'est encore le théorème d'isomorphisme. Si b est un morphisme de **G** dans **H**, il donne lieu à la suite exacte :

$$e \longrightarrow \mathrm{Ker}\, b \xrightarrow{i} \mathbf{G} \xrightarrow{b} \mathrm{Im}\, b \longrightarrow e$$

où i est l'injection.

3.3.2 1) Il suffit de poser $i(n) = (n, e)$ et $p(n, k) = k$. Alors, comme on l'a vu dans les exercices 2.1.1 et 2.1.12, i et p sont des morphismes respectivement injectif et surjectif. De plus, le noyau de p est formé des éléments de la forme (n, e), qui est bien l'image de i.

2) Les groupes **K** et **N** jouent le même rôle, et la suite,

$$e \longrightarrow \mathbf{K} \xrightarrow{j} \mathbf{N} \times \mathbf{K} \xrightarrow{q} \mathbf{N} \longrightarrow e$$

avec définition similaire de j et q, est également exacte.

3.3.3 1) Montrons l'associativité :

$$\begin{aligned}
\big((n,k)*(n',k')\big)*(n'',k'') &= (n(k.n'),kk')*(n'',k'') \\
&= (n(k.n')(kk'.n''),(kk')k'') \\
&= (n(k.n')(k.(k'.n'')),kk'k'') \\
(n,k)*\big((n',k')*(n'',k'')\big) &= (n,k)*(n'(k'.n''),k'k'') \\
&= (nk.(n'(k'.n'')),kk'k'') \\
&= (n(k.n')(k.(k'.n'')),kk'k'')
\end{aligned}$$

Pour bien comprendre la fin du calcul, rappelons-nous que l'action est une action par **morphismes**, et donc $k.(ab) = (k.a)(k.b)$. Ici, $k.(n'(k'.n'')) = (k.n')(k.(k'.n''))$ et l'associativité est démontrée.

$$(n,k)*(1,1) = (nk.1,k) = (n,k) \qquad (1,1)*(n,k) = (1.n,k) = (n,k)$$

en remarquant que la première égalité est due à ce que c'est une action par morphismes, donc $k.1 = 1$, la seconde à ce que c'est une action, et $1.k = k$. Enfin on vérifiera que $(n,k)^{-1} = (k^{-1}.n^{-1},k^{-1})$.

2) Il faut d'abord vérifier que i et p sont des morphismes :

$$i(n)*i(n') = (n,1)*(n',1) = (n1.n',1) = (nn',1) = i(nn')$$

$$p((n,k)*(n',k')) = p(nk.n',kk') = kk' = p(n,k)p(n',k')$$

Et le noyau de i est bien **N**, tandis que p est bien surjective, tout $k \in \mathbf{K}$ est l'image de $(1,k)$. Enfin, $\mathrm{Ker}p$ est formé des couples $(n,1)$, c'est bien l'image de i.

3) La loi est alors la loi habituelle du produit direct.

3.3.4 Si l'on se donne une action ϕ différente de l'identité de $\mathbb{Z}/2$ sur $\mathbb{Z}/n$, $\phi(1)$ doit être un automorphisme d'ordre 2. On sait que les automorphismes de $\mathbb{Z}/n$ sont donnés par $x \mapsto kx$ ou, en notation multiplicative, $x \mapsto x^k$, avec k premier à n. Il faut donc $k^2 \equiv 1 \pmod{n}$, ce qui sera toujours satisfait pour $k = -1$. Considérons alors le produit semi-direct

$$\mathbf{G} = \mathbb{Z}/n \rtimes_\phi \mathbb{Z}/2$$

En notant r un générateur de $\mathbb{Z}/n$ et σ un générateur de $\mathbb{Z}/2$, et en identifiant r avec $(r,1)$ et σ avec $(1,\sigma)$, on aura :

$$r^p\sigma = (r^p,1)(1,\sigma) = (r^p,\sigma)$$

mais également :

$$\sigma r^{-p} = (1,\sigma)(r^{-p},1) = (\sigma.r^{-p},\sigma) = (r^p,\sigma)$$

On a donc $r^p\sigma = \sigma r^{-p}$ reconnaît les générateurs et règles de calcul du groupe diédral, et l'on conclut en disant que les deux groupes ont le même nombre d'éléments.

$$\mathbb{D}_{2n} \cong \mathbb{Z}/n \rtimes_\phi \mathbb{Z}/2$$

Pour terminer, signalons que notre construction fonctionne *mutatis mutandis* dans le cas du groupe diédral infini :

$$\mathbb{D}_\infty \cong \mathbb{Z} \rtimes_\phi \mathbb{Z}/2$$

3.3.5 1) L'image $\mathcal{N}$ de i est aussi le noyau de p et c'est donc un sous-groupe normal de $\mathbf{G}$. Le groupe $\mathcal{K}$ est lui-même un sous-groupe de $\mathbf{G}$ isomorphe à $\mathbf{K}$, la loi de $\mathbf{G}$ permet en effet d'écrire :

$$(1,k)(1,k') = (1,kk') \qquad (1,k)^{-1} = (1,k^{-1})$$

Comme $\mathcal{N}$ est formé de couples de la forme $(n,1)$ tandis que $\mathcal{K}$ est formé de couples $(1,k)$, leur intersection est réduite au neutre de $\mathbf{G}$. Enfin, la loi de $\mathbf{G}$ permet également de voir que :

$$(n,1)(1,k) = (n,k)$$

ce qui prouve $\mathbf{G} = \mathcal{N}\mathcal{K}$. Comme $\mathbf{K}$ et $\mathcal{K}$ sont isomorphes, de même que $\mathbf{N}$ et $\mathcal{N}$, on procédera souvent à l'identification de $(n,1)$ avec n et de $(1,k)$ avec k.

2) En utilisant la loi de $\mathbf{G}$:

$$(1,k)(n,1)(1,k^{-1}) = (k.n,1)(1,k^{-1}) = (k.n,1)$$

Avec les identifications :

$$knk^{-1} = k.n$$

3) Les hypothèses étant :

$$\mathbf{N} \lhd \mathbf{G} \qquad \mathbf{N} \cap \mathbf{K} = e \qquad \mathbf{G} = \mathbf{N}\mathbf{K}$$

on définit une application :

$$\psi : (n,k) \mapsto nk$$

du produit semi-direct $\mathbf{N} \rtimes_\phi \mathbf{K}$ dans $\mathbf{G}$. C'est un morphisme :

$$\begin{aligned} \psi\left((n,k)(n',k')\right) &= \psi(nk.n', kk') \\ &= \psi(nkn'k^{-1}, kk') \\ &= nkn'k^{-1}kk' \\ &= nkn'k' \\ &= \psi(n,k)\psi(n'k') \end{aligned}$$

Il est surjectif par hypothèse, et injectif car son noyau est formé des (n,k) tels que $nk = 1$, et cette égalité implique $n = k^{-1} \in \mathbf{N} \cap \mathbf{K} = \{1\}$. Donc $n = k = 1$. Nous laissons toutes les autres vérifications au lecteur. Remarquons néanmoins que l'on a obtenu l'unicité de l'écriture sous la forme nk.

4) Pour que le produit semi-direct se réduise à un produit direct, il faut et suffit que $k.n = knk^{-1} = n$ pour tout k et n, autrement dit, tout élément de $\mathbf{K}$ commute à tout élément de $\mathbf{N}$. Montrons que cela équivaut à $\mathbf{K} \lhd \mathbf{G}$. Si l'on commence par supposer $\mathbf{K} \lhd \mathbf{G}$, alors $nkn^{-1}k^{-1} = (nkn^{-1})k^{-1}$ est le produit de deux éléments de $\mathbf{K}$ donc est dans $\mathbf{K}$. On voit de même que cet élément est dans $\mathbf{N}$, donc dans $\mathbf{N} \cap \mathbf{K}$ donc est 1, œ qui montre la commutativité. Réciproquement, soit $g = nk \in \mathbf{G}$. Alors $g\mathbf{K}g^{-1} = \mathbf{K}$ puisque $nkk'k^{-1}n^{-1} = kk'k^{-1} \in \mathbf{K}$, et $\mathbf{K}$ est normal dans $\mathbf{G}$ comme déjà $\mathbf{N}$.

5) Pour que **G** soit commutatif, il est d'abord nécessaire que **N** et **K** le soient, puisqu'ils sont isomorphes à des sous-groupes de **G**. De plus :

$$(n,1)(1,h) = (n,h) \qquad (1,h)(n,1) = (h.n,h)$$

prouve que les deux éléments commutent ssi l'action est triviale. Le produit doit donc être direct. Cela montre que la structure de produit semi-direct permet de fabriquer très facilement des groupes non commutatifs.

6) Soit $\mathbf{G} = \mathcal{S}_n$, $\mathbf{N} = \mathcal{A}_n$ et $\mathbf{K} = \langle(1,2)\rangle$ le groupe à deux éléments engendré par une transposition. Alors $\mathbf{N} \cap \mathbf{K} = \{e\}$ et $\mathbf{NK} = \mathbf{G}$ puisque **N** est d'indice 2 et ne contient pas $(1,2)$. Conclusion, le groupe symétrique est un produit semi-direct.

3.3.6 1) Les seuls automorphismes de $\mathbb{Z}/3$ sont donnés par $x \mapsto x$ et $x \mapsto x^{-1}$. L'application $x \mapsto y.x = x^{-1}$ est donc bien un automorphisme. Par ailleurs, $y^2.x = y.(y.x) = y.x^{-2} = x$ donc y^2 agit comme l'identité. Enfin $y^3.x = y.x$; on a donc défini une action, non fidèle, de $\mathbb{Z}/4$ sur $\mathbb{Z}/3$.

2) Ce produit semi-direct est un groupe dont les éléments s'écrivent $(x^\ell, y^k) = x^\ell y^k$ par abus de notation, en notant y un générateur de $\mathbb{Z}/4$ et x un générateur de $\mathbb{Z}/3$; il n'est pas commutatif car $yxy^{-1} = y.x = x^{-1}$. Une façon, un peu laborieuse, de montrer qu'il n'est pas isomorphe à $\mathbb{D}_{12}$, ni à $\mathcal{A}_4$ est d'examiner l'ordre de ses éléments. On constate que ce groupe a un seul élément d'ordre 2, $(1,y^2) = y^2$, deux d'ordre 3, six d'ordre 4 et deux d'ordre 6. On pourra vérifier ces affirmations en faisant les calculs comme celui-ci :

$$(x^2y)^2 = x^2y.x^2y^2 = x^2x^{-2}y^2 = y^2$$

et donc x^2y est d'ordre 4. Dans ce cas, le produit semi-direct $\mathbb{Z}/3 \rtimes_\phi \mathbb{Z}/4$ n'est donc pas isomorphe à $\mathbb{D}_{12}$, qui a huit éléments d'ordre 2, ni à $\mathcal{A}_4$ qui en a trois.
Pour conclure, si l'on considère le groupe de présentation :

$$\mathbf{G} = \langle x,y \mid x^3 = y^4 = 1,\ yxy^{-1} = x^{-1}\rangle$$

alors ce groupe a, au plus, douze éléments qui sont de la forme $x^k y^{k'}$ où $0 \leqslant k \leqslant 2$ et $0 \leqslant k' \leqslant 3$. En effet, la relation $yx = x^2y$ permet toujours de se ramener à cette forme. On conclut, par le théorème de Von Dyck que notre produit semi-direct est bien **G**.

3) Il suffit de définir l'isomorphisme par l'image des générateurs $x \mapsto B$ et $y \mapsto A$. Les deux matrices sont bien d'ordres respectifs 3 et 4 et vérifient la relation $ABA^{-1} = B^{-1}$. Enfin, T est bien un groupe dicyclique. Trouvons un élément d'ordre 6, $z = xy^2$ convient. Alors $z^6 = y^4 = (yz)^4 = 1$ on reconnaît une des présentations d'un groupe dicyclique.

3.3.7 1) Soit ϕ un morphisme d'un groupe **G** dans un groupe **H** ; si **G** est engendré par un élément x, alors on peut choisir pour $\phi(x)$ un élément quelconque de **H**, ϕ sera déterminé car, nécessairement, $\phi(x^k) = \phi(x)^k$. Tout choix de $\phi(x)$ convient.

2) Il suffit que ϕ soit surjective pour être bijective (ensembles finis). Ainsi, comme l'image de ϕ est engendrée par $\phi(x)$, celui-ci doit être un générateur de $\mathbb{Z}/n$, c'est-à-dire un inversible de l'anneau $\mathbb{Z}/n$. Il y a donc $\phi(n)$ automorphismes de $\mathbb{Z}/n$. Si x est un générateur, un morphisme sera déterminé par r premier à n et $x \mapsto rx$ (en notation additive) ou $x \mapsto x^r$ (en notation multiplicative).

3.3.8 1) Le seul automorphisme de $\mathcal{S}_2$ est l'identité. Pour $\mathcal{S}_3$, les automorphismes sont plus nombreux : comme les trois transpositions sont génératrices, il suffit de déterminer leur image, qui est d'ordre deux, donc une transposition. On vérifie facilement que cela permet de définir six automorphismes de $\mathcal{S}_3$, mais cela résulte également de la question suivante. De même, il y a 24 automorphismes de $\mathcal{S}_4$.

2) Il suffit d'utiliser que le centre de $\mathcal{S}_n$ est réduit au neutre dès que $n > 2$, et donc $\mathrm{Int}(\mathbf{G}) \cong \mathbf{G}$; voir le premier problème du chapitre 1.

3) Commençons par remarquer que :

- un automorphisme transforme un élément d'ordre deux en un élément d'ordre deux ;
- un automorphisme intérieur transforme un cycle en un cycle de même longueur, donc une transposition en une transposition.

Soit donc ϕ qui transforme toute transposition en une transposition. En particulier, $\phi(1,2) = (a_1, a_2)$ où a_1 et a_2 sont des entiers distincts. De la même façon, l'image de $(1,3)$ est une transposition ; ce ne peut être la transposition de deux éléments distincts de a_1 et a_2, sinon les images de $(1,2)$ et de $(1,3)$ commuteraient, ce qui n'est pas le cas de $(1,2)$ et $(1,3)$. On a donc $\phi(1,3) = (a_1, a_3)$ par exemple (puisque a_1 et a_2 jouent encore le même rôle), avec a_3 distinct des précédents (ϕ est bijective). Passons à $\phi(1,4)$. Il faut que cette transposition ait un élément commun avec les deux précédentes, d'où $\phi(1,4) = (a_1, a_4)$ ou $\phi(1,4) = (a_2, a_3)$. Mais ce dernier cas est exclu, car $(1,2)(1,3)(1,4)$ est un 4-cycle alors que $(a_1,a_2)(a_1,a_3)(a_2,a_3)$ est une transposition. On en déduit de même que $\phi(1,i) = (a_1, a_i)$. Comme les a_i sont distincts, on a fabriqué une permutation, et

$$a \circ (1,i) \circ a^{-1} = (a_1, a_i)$$

prouve que ϕ coïncide avec l'automorphisme intérieur défini par a sur toutes les transpositions $(1,i)$ donc sur tout le groupe $\mathcal{S}_n$.

4) L'image par un automorphisme ϕ d'une transposition est nécessairement un élément d'ordre deux, et comme les transpositions sont conjuguées, on ne peut arriver que dans une même classe de conjugaison. Comme ϕ est bijectif, on obtient toute cette classe de conjugaison. Il faut donc examiner s'il est possible qu'il y ait bijection entre l'ensemble des transpositions, et l'ensemble des doubles transpositions, des triples transpositions... or ces ensembles sont de cardinaux respectifs :

$$\frac{n(n-1)}{2} \qquad \frac{4!}{2!2!2!}C_n^4 \qquad \frac{(2k)!}{(2!)^k k!}C_n^{2k}$$

On a appliqué le « principe du berger » pour ce dénombrement ; on part d'un ensemble de $2k$ entiers, on considère toutes ses permutations, et, en regroupant deux éléments consécutifs, on obtient k transpositions de supports disjoints. Mais il faut diviser par $k!$ car l'ordre n'importe pas, et k fois par 2! car les deux éléments d'une transposition jouent le même rôle. Ce nombre est égal à $\frac{n(n-1)}{2}$ ssi

$$(n-2)(n-4)\dots(n-2k+1) = k!2^{k-1}$$

après simplifications. On utilise d'abord que $n \geqslant 2k$ pour minorer le premier membre par $(2k-2)!$. Mais on montre par récurrence que $(2k-2)! > k!2^{k-1}$ dès que $k > 4$. Il y a, en revanche, égalité lorsque $k = 3$, et donc en prenant $n = 6$, on voit qu'il y a

autant de transpositions que de triples transpositions. Reste à voir $k = 2$ ou $k = 3$, mais le second membre de l'égalité ci-dessus est constant, le premier croît avec n, ce qui permet rapidement de prouver qu'il n'y a pas d'autre possibilité.
Conclusion. Sauf pour $n = 6$ et $n = 2$, le groupe des automorphismes de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_n$. Comme son centre est trivial, c'est bien un **groupe complet**.

5) On retrouve la situation étudiée dans l'exercice 3.2.11 : Si $\mathbf{H}$ est un sous-groupe d'indice n dans $\mathcal{S}_n$, l'action par translation de $\mathcal{S}_n$ sur le quotient $\mathcal{S}_n$ est fidèle, donc $\mathcal{S}_n$ est isomorphe à un sous-groupe de $\mathcal{S}_n$, donc à lui-même. Dans cet isomorphisme, l'image de $\mathbf{H}$ est un stabilisateur (celui de $\mathbf{H}$) ; si donc $\mathbf{H}$ n'est pas le stabilisateur d'un entier, il a une image qui n'est pas un sous-groupe conjugué, et donc l'isomorphisme n'est pas intérieur. On en déduit qu'un tel $\mathbf{H}$ ne peut exister que si $n = 6$.

6) Il n'est pas très aisé de montrer que $\mathcal{S}_6$ est bien une exception. Nous nous contenterons de donner un exemple d'automorphisme non intérieur[1], en demandant au lecteur de faire les vérifications. Il suffit de définir les images des cinq transpositions $(1,2)$, $(1,3),\ldots,$ $(1,6)$. Ces images doivent être des triples transpositions, comme $(1,2)(3,4)(5,6)$. Il y a au moins une restriction, puisque le produit de deux transpositions $(1,i)(1,j)$ est un 3-cycle, il est nécessaire que leurs images aient le même ordre. Or, quand on considère deux triples transpositions, il n'y a que deux cas, soit elles ont un cycle en commun, et leur composé est une double transposition (ou l'identité), soit elles n'ont aucun cycle commun, et leur composé est le produit de deux 3-cycles de supports disjoints. C'est ce dernier cas qui convient. Il suffit de constater qu'on peut trouver cinq triples transpositions ayant la propriété de n'avoir aucun cycle commun deux à deux. Par exemple :

$$(1,2)(3,4)(5,6)\quad (1,3)(2,5)(4,6)\quad (1,4)(2,6)(3,5)\quad (1,5)(2,4)(3,6)\quad (1,6)(2,3)(4,5)$$

et l'on peut vérifier... avec un bon logiciel, que les 5! applications envoyant les $(1,i)$ sur une de ces triples transpositions donnent un automorphisme extérieur. Au total, il y aura 6! automorphismes extérieurs, autant que d'intérieurs. Il y a des justifications plus convaincantes, et souvent géométriques, de l'existence d'automorphismes extérieurs dans $\mathcal{S}_6$; voir [21] ou [15].

3.3.9 Nous ne faisons que généraliser ce qui a été vu dans les exercices précédents. Il s'agit de trouver un morphisme de $\mathbb{Z}/m$ dans le groupe des automorphismes de $\mathbb{Z}/n$. On doit donc associer à un générateur de $\mathbb{Z}/m$, noté y, un entier r premier à n, et l'action sera $y.x = x^r$, en notation multiplicative. Mais il faut que l'on ait une action de groupe, et donc que le morphisme $\phi(y)$ associé à y soit d'ordre m ; or :

$$x = \phi(y) \circ \ldots \phi(y)(x) = \phi(y)^m(x) = y^m.x = x^{r^m}$$

et donc que $r^m \equiv 1 \pmod{n}$. Remarquons que cette congruence implique r premier à n.

- Dans le cas $m = 2$. Il s'agit de trouver r tel que $r^2 \equiv 1 \pmod{n}$. Une solution évidente est $r = -1$. L'action est donnée par $y.x = x^{-1}$; et l'on a :

$$x^n = 1,\ y^2 = 1,\ yxy^{-1} = x^{-1}$$

1. Un tel automorphisme est appelé **automorphisme extérieur**.

et comme le groupe a $2n$ éléments, c'est le groupe diédral $\mathbb{D}_{2n}$. Notre produit semi-direct a en général la présentation :

$$\mathbf{G} = \langle x^n = 1,\ y^m = 1,\ yxy^{-1} = x^r \rangle$$

Un tel groupe fait partie des groupes **métacycliques**. On appelle ainsi un groupe qui a un sous-groupe normal cyclique, ici isomorphe à $\mathbb{Z}/n$ avec un quotient cyclique, isomorphe à $\mathbb{Z}/m$. Pour le cas $m = 2$, hormis les groupes diédraux, on a une autre famille infinie :

$$\mathbf{G} = \langle x^{4n} = 1,\ y^2 = 1,\ yxy^{-1} = x^{2n-1} \rangle$$

en effet, dans ce cas $r = 2n - 1$ et $r^2 = (2n-1)^2 \equiv 1 \pmod{4n}$. Pour $n = 1$, on trouve un produit direct $\mathbb{Z}/4 \times \mathbb{Z}/2$, pour $n = 2$, on trouve un groupe non commutatif à 16 éléments.

- Pour le cas $m = 3$, le premier exemple non trivial est un produit semi-direct de $\mathbb{Z}/7$ avec $\mathbb{Z}/3$, avec $r = 2$. Il a 21 éléments. Enfin, il n'existe pas de produit semi-direct non direct de la forme $\mathbb{Z}/4 \rtimes \mathbb{Z}/3$ car les automorphismes de $\mathbb{Z}/4$ sont l'identité ou $x \mapsto x^{-1}$ d'ordre 2, alors que les éléments non nuls de $\mathbb{Z}/3$ sont d'ordre 3.

3.3.10 1) Supposons que $\mathbf{G}$ soit produit semi-direct de $\mathbf{N}$ et $\mathbf{K}$. Alors une section est tout simplement donnée par :

$$s(k) = (1, k)$$

dont on vérifie immédiatement qu'elle est un morphisme et que $p \circ s = id$.
Supposons maintenant donnée s. Alors s est injective puisque $p \circ s = id$. On en déduit que son image $\mathcal{K} = s(K)$ est isomorphe à $\mathbf{K}$. Si l'on note $\mathcal{N}$ l'image de $\mathbf{N}$ par i, on peut vérifier le critère de produit semi-direct. Soit $g \in \mathbf{G}$, et posons $k = s \circ p(g) \in \mathcal{K}$. Alors, par l'hypothèse sur s, $p(k) = p(g)$, et donc, si l'on pose $n = gk^{-1}$,

$$p(n)p(k) = p(g) = p(k) \Rightarrow p(n) = 1 \Rightarrow n \in \mathcal{N}$$

puisque la suite est exacte. On a donc $\mathbf{G} = \mathcal{N}\mathcal{K}$. Enfin,

$$\mathcal{N} \cap \mathcal{K} = \mathrm{Ker}\, p \cap \mathcal{K} = \mathrm{Ker}\, p|_{\mathcal{K}} = \{1\}$$

car la restriction de p à $\mathcal{K}$ est injective puisque $p \circ s = id$, $p(g) = 1$.

2) Montrons d'abord qu'avec les notations précédentes, $\mathcal{K}$ est bien un relèvement de $\mathbf{K}$, il suffit de vérifier que deux éléments de $\mathcal{K}$ congrus modulo $\mathcal{N}$ sont égaux. Or :

$$k \equiv k' \pmod{\mathcal{N}} \iff p(k) = p(k') \iff k = k'$$

puisque p restreinte à $\mathcal{K}$ est injective. Réciproquement, soit $\mathcal{K}$ un relèvement de $\mathbf{K}$, alors la restriction de p à $\mathcal{K}$ est bijective, puisque $\mathcal{K}$ est une transversale de $\mathcal{N}$ puisque $\mathcal{K}$ est une transversale[1] de $\mathcal{N}$. Il suffit de définir s comme l'application réciproque de cette projection.

3) Dans le cas de $\mathcal{S}_n$, on a la suite exacte :

$$e \longrightarrow \mathcal{A}_n \xrightarrow{i} \mathcal{S}_n \xrightarrow{\epsilon} \{1, -1\} \longrightarrow e$$

Un relèvement sera un sous-groupe de $\mathcal{S}_n$ à deux éléments, donc engendré par une permutation τ d'ordre 2. Mais ce doit être une transversale du groupe alterné, donc cette permutation doit être impaire. On peut prendre une transposition. On aura donc :

$$\mathcal{S}_n \cong \mathcal{A}_n \rtimes_\phi \langle \tau \rangle$$

où l'action est définie par $\tau.\sigma = \tau \circ \sigma \circ \tau$.

1. autrement dit, les éléments de $\mathcal{K}$ représentent toutes les classes de $\mathbf{G}$ modulo $\mathcal{N}$.

3.3.11 Ces sous-groupes sont d'intersection e, car $\mathbf{K}$ ne contient pas de double-transposition mais seulement le 3-cycle $(1,2,3)$ et son carré $(1,3,2)$ (et le neutre bien sûr). De plus, nous savons que $\mathcal{V}$ est normal dans $\mathcal{A}_4$. On peut en déduire que ces deux groupes forment un produit semi-direct, et ce produit est $\mathcal{A}_4$, car il a douze éléments :

$$\mathcal{A}_4 \cong (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes_\phi \mathbb{Z}/3$$

Notons que dans ce cas, il y a quatre relèvements différents.

3.3.12 1) L'action est définie « naturellement » par : $\phi.g = \phi(g)$, où $\phi \in \mathrm{Aut}(\mathbf{G})$ et $g \in \mathbf{G}$.

2) Les automorphismes des groupes cycliques ont été étudiés. Dans le cas de $\mathbb{Z}$, l'holomorphe est donc $\mathbb{Z} \rtimes \mathbb{Z}/2$, avec les lois :

$$(a,0)(b,0) = (a+b,0) \quad (a,0)(b,1) = (a+b,1)$$
$$(a,1)(b,0) = (a-b,1) \quad (a,1)(b,1) = (a-b,0)$$

On reconnaît le groupe diédral infini, engendré par $x = (1,0)$ et $y = (0,1)$ avec :

$$\mathbb{D}_\infty = \langle x, y \mid y^2 = 1,\ yxy = x^{-1} \rangle$$

qui est aussi le groupe des transformations de $\mathbb{Z}$ données par $z \mapsto \pm z + a$.
Dans le cas de $\mathbb{Z}/2$, l'holomorphe est $\mathbb{Z}/2$ lui-même car il n'y a pas d'autre automorphisme que l'identité. Pour $\mathbb{Z}/3$ et $\mathbb{Z}/4$, le groupe d'automorphismes est $\mathbb{Z}/2$ engendré par $x \mapsto x^{-1}$ en notation multiplicative. La présentation des holomorphes est donc :

$$\langle x, y \mid x^n = 1,\ y^2 = 1,\ yxy = x^{-1} \rangle$$

pour $n = 3$ ou $n = 4$. On reconnaît les groupes diédraux $\mathbb{D}_6 = \mathcal{S}_3$ et $\mathbb{D}_8$.

3) Le groupe $\mathcal{V}$ de Klein a pour groupe d'automorphismes $\mathcal{S}_3$. Un automorphisme induit en effet une permutation des 3 éléments d'ordre 2 de $\mathcal{V}$. Réciproquement, si l'on se donne une permutation quelconque de ces trois éléments u, v et w, on fixe l'image de deux générateurs du groupe $\mathcal{V}$, par exemple u et v, et l'image du troisième est automatiquement celui qui reste. L'holomorphe est donc le produit semi-direct $\mathcal{V} \rtimes_\phi \mathcal{S}_3$, à 24 éléments.
Montrons que ce groupe est isomorphe à $\mathcal{S}_4$. Pour cela, montrons qu'il coïncide avec le produit semi-direct :

$$\mathcal{S}_4 = \mathcal{V} \rtimes \mathbf{K}$$

où $\mathbf{K}$ est le stabilisateur de 4, donc isomorphe à $\mathcal{S}_3$. Il est immédiat que ces deux sous-groupes satisfont le critère de produit semi-direct. Par ailleurs, l'action de $\mathbf{K}$ sur $\mathcal{V}$ peut être étudiée grâce aux transpositions :

$$(1,2)(1,2)(3,4)(1,2) = (1,2)(3,4)$$
$$(1,2)(1,3)(2,4)(1,2) = (1,4)(2,3)$$
$$(1,2)(1,4)(2,3)(1,2) = (1,3)(2,4)$$

ainsi, $(1,2)$ fixe u et échange v et w ; ainsi, de même, pour les autres automorphismes. Le bilan est :

$$\mathrm{Hol}(\mathcal{V}) = \mathcal{S}_4$$

4) Posons

$$\mathbb{D}_{2n} = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1} \rangle$$

Un automorphisme est déterminé par l'image de r qui est de la forme r^k où k est premier à n, car cette image doit être d'ordre n, et par l'image de s qui est de la forme $r^\ell s$, car ce doit

être un élément d'ordre 2 non dans $\langle r\rangle$. Il y a donc bijection entre $\mathrm{Aut}(\mathbb{D}_{2n})$ et le produit semi-direct $\mathbb{Z}/n \rtimes \mathrm{Aut}(\mathbb{Z}/n)$, la bijection est donnée par :

$$\phi \mapsto (r^\ell, \phi')$$

en notant ϕ' la restriction de ϕ à $\langle r\rangle$. Il reste à montrer que c'est un morphisme, soit ψ un autre automorphisme, avec $\psi(r) = r^{k'}$ et $\psi(s) = r^{\ell'}s$. Alors

$$\psi(\phi(s)) = \psi(r^\ell s) = r^{k'\ell} r^{\ell'} s$$

et

$$\psi \circ \phi \mapsto (r^{\ell'+k'\ell}, \psi' \circ \phi') = (r^{\ell'}, \psi')(r^\ell, \phi')$$

en utilisant la loi du produit semi-direct. On a donc :

$$\mathrm{Aut}(\mathbb{D}_{2n}) = \mathrm{Hol}(\mathbb{Z}/n)$$

3.3.13 1) Les sous-groupes normaux de $\mathbb{H}_8$ sont le centre, à deux éléments, et les trois sous-groupes d'ordre 4. $\mathbb{H}_8$ ne peut être produit semi-direct car aucun couple de sous-groupe n'est d'intersection réduite au neutre. Voir l'exercice 2.3.2.

2) Rappelons qu'un groupe dicyclique quelconque admet la présentation :

$$\mathbf{G} = \langle x, y \mid x^{2n} = y^4 = 1,\ y^2 = x^n,\ yxy^{-1} = x^{-1}\rangle$$

Ses $4n$ éléments peuvent s'écrire x^k ou $x^k y$, et un calcul facile montre que tous les éléments de la forme $x^k y$ ont pour carré $y^2 = x^n$. On en déduit que tout sous-groupe de $\mathbf{G}$ contient le sous-groupe à deux éléments $\{e,\ y^2\}$ qui est d'ailleurs le centre de $\mathbf{G}$. Ce groupe ne peut donc être produit semi-direct, pour la même raison que ci-dessus, bien qu'il admette des sous-groupes normaux.

3.4 D'AUTRES GROUPES FINIS

Les théorèmes de Sylow, ainsi que la notion de produit semi-direct vont nous permettre d'avancer encore dans notre connaissance des groupes finis ayant peu d'éléments. Nous nous concentrerons sur les groupes non commutatifs, les autres étant étudiés dans le chapitre suivant, et nous essaierons de compléter notre connaissance des groupes d'ordre inférieur à 30.

Exercice 3.4.1 (Groupes d'ordre huit)

On poursuit l'exercice 2.3.1 du chapitre précédent en vérifiant qu'il n'y a pas d'autre groupe non commutatif à huit éléments que les groupes diédraux et quaternioniques. Soit $\mathbf{G}$ un groupe non commutatif à huit éléments.

1) Démontrer qu'il existe un élément a d'ordre 4. Soit $\mathbf{H} = \langle a\rangle$. Vérifier que $\mathbf{H} \lhd \mathbf{G}$, et que si $b \in \mathbf{G} \setminus \mathbf{H}$, alors $b^2 = e$ ou $b^2 = a^2$.

2) Démontrer que, dans le premier cas, $\mathbf{G}$ est isomorphe à $\mathbb{D}_8$, dans le second cas, il est isomorphe à $\mathbb{H}_8$.

L'exercice suivant démonte la structure des groupes d'ordre $2p$, ce qui règle le cas des groupes d'ordre 6, déjà connus, 10, 14, 22, 26...

Exercice 3.4.2 (Groupes d'ordre $2p$)

On suppose que p est premier différent de 2. En étudiant les p-Sylow et les 2-Sylow, montrer qu'il n'y a que deux sortes de groupes d'ordre $2p$, le groupe cyclique $\mathbb{Z}/2p$ et le groupe diédral $\mathbb{D}_{2p}$.

Parmi les groupes d'ordre petit, il manque encore l'ordre 9. Réglons le cas des ordres p^2, ce qui donnera également le cas des groupes d'ordre $25, 49\ldots$

Exercice 3.4.3 (Groupe d'ordre p^2)

Démontrer qu'un groupe d'ordre p^2, où p est premier, est nécessairement commutatif. Vérifier ainsi qu'il n'y a que deux groupes d'ordre p^2.

Voici traités deux exemples de groupes d'ordre p^2q.

Exercice 3.4.4 (Groupes d'ordre douze)

L'objectif de cet exercice est de montrer qu'il n'y a pas d'autre groupe non commutatif d'ordre douze que ceux que l'on connaît déjà, soit $\mathcal{A}_4$, $\mathbb{D}_{12}$ et T. Soit $\mathbf{G}$ un groupe non commutatif ayant 12 éléments.

1) Démontrer que s'il y a plus d'un 3-Sylow dans $\mathbf{G}$, alors $\mathbf{G}$ est isomorphe $\mathcal{A}_4$. Ce cas sera exclu par la suite. Combien y a t-il alors d'éléments d'ordre 3 ?
2) En déduire qu'il y a un élément a d'ordre 6 (contrairement au cas de $\mathcal{A}_4$), et que $\langle a\rangle$ est normal dans $\mathbf{G}$.
3) Montrer que si $\mathbf{G}$ est produit semi-direct de $\mathbb{Z}/6$ par $\mathbb{Z}/2$, alors $\mathbf{G}$ est isomorphe à $\mathbb{D}_{12}$.
4) Examiner le dernier cas, vérifier qu'il y a alors un seul élément d'ordre 2.

Exercice 3.4.5 (Groupes d'ordre dix-huit)

Nous verrons dans le chapitre suivant qu'il n'y a que deux groupes commutatifs d'ordre 18, $\mathbb{Z}/18$ et $\mathbb{Z}/3 \times \mathbb{Z}/6$. Il existe également trois groupes non commutatifs. Soit $\mathbf{G}$ un groupe non commutatif d'ordre 18.

1) Montrer que $\mathbf{G}$ a un seul 3-Sylow, et que c'est donc un produit semi-direct de $\mathbb{Z}/9$ par $\mathbb{Z}/2$, ou de $\mathbb{Z}/3 \times \mathbb{Z}/3$ par $\mathbb{Z}/2$.
2) Déterminer le groupe des automorphismes de $\mathbb{Z}/9$. En déduire un groupe d'ordre 18.
3) Étudier le groupe des automorphismes de $\mathbb{Z}/3 \times \mathbb{Z}/3$, en déduire deux nouveaux groupes d'ordre 18.
4) Montrer que les trois groupes obtenus sont bien distincts (à isomorphisme près). Retrouver lequel est isomorphe à $\mathcal{S}_3 \times \mathbb{Z}/2$.

Il manque encore le cas des groupes d'ordre pq, et ainsi sera réglé le cas des ordres 15, 21, 28... Cet exercice généralise le cas des groupes d'ordre $2p$ vus ci-dessus.

Exercice 3.4.6 (Groupes d'ordre pq)

On suppose que p et q sont premiers distincts. On pourra supposer $p < q$. Soit $\mathbf{G}$ un groupe d'ordre pq.

1) Montrer que $\mathbf{G}$ contient un q-Sylow normal.
2) Montrer que si $p \not\equiv 1 \pmod{q}$, alors $\mathbf{G}$ est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ et est donc cyclique. Combien y a-t-il de cas de ce type si $pq < 100$?
3) Dans l'autre cas, montrer que $\mathbf{G}$ est soit cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, ou est produit semi-direct de la forme $\mathbb{Z}/q \rtimes_\phi \mathbb{Z}/p$. On admettra que, dans ce cas, il existe une seule structure semi-directe. Combien y a-t-il de situations de ce type si $pq < 100$?

Pour l'ordre 27, il nous faut étudier les groupes d'ordre p^3.

Exercice 3.4.7 (Les groupes non commutatifs d'ordre p^3)

1) Soit $\mathbf{N}$ le groupe $\mathbb{Z}/p \times \mathbb{Z}/p$, que nous considérerons comme engendré par les deux éléments a et b :

$$\mathbf{N} = \langle a, b \mid a^p = b^p = 1,\ ab = ba \rangle$$

et $\mathbf{K}$ le groupe $\mathbb{Z}/p = \langle c \rangle$. On définit une action par automorphismes de $\mathbf{K}$ sur $\mathbf{N}$ par :

$$c.a = ab,\ c.b = b$$

Vérifier que l'on obtient bien une action, et en reconnaître la nature géométrique (si $\mathbf{N}$ est considéré comme un espace vectoriel).

2) Vérifier que le produit semi-direct $\mathbf{G} = \mathbf{N} \rtimes_\phi \mathbf{K}$ admet la présentation :

$$\mathbf{G} = \langle a, b, c \mid a^p = b^p = c^p = 1,\ b = cac^{-1}a^{-1},\ ab = ba,\ bc = cb \rangle$$

et que tous les éléments de $\mathbf{G}$ vérifient $x^p = 1$ (si p est impair).

3) Montrer que le cas $p = 2$ donne une nouvelle structure semi-directe pour le groupe diédral $\mathbb{D}_8$.
4) On suppose maintenant que $p > 2$. $\mathbf{N} = \mathbb{Z}/p^2 = \langle a \rangle$ et $\mathbf{K} = \mathbb{Z}/p = \langle b \rangle$. On considère l'action par automorphismes définie par :

$$b.a = a^{p+1}$$

Vérifier que l'on définit bien ainsi une action, et que le produit semi-direct $\mathbf{G} = \mathbf{N} \rtimes_\phi \mathbf{K}$ admet la présentation :

$$\mathbf{G} = \langle a, b \mid a^{p^2} = b^p = 1,\ bab^{-1} = a^{p+1} \rangle$$

5) On suppose que $p \geqslant 3$, montrer qu'il n'y a pas d'autre groupe non commutatif d'ordre p^3 que ceux décrits ci-dessus. On pourra distinguer deux cas, suivant qu'il existe un élément d'ordre p^2 ou non.

Enfin, des exemples de groupes d'ordre 16.

Exercice 3.4.8

Soit **N** le groupe cyclique d'ordre 8 engendré par a, et **K** le groupe cyclique d'ordre 2 engendré par b.

1) Montrer que $b.a = a^3$ définit une action par morphisme ϕ de **K** sur **N**.
2) Soit $\mathbf{G} = \mathbf{N} \rtimes_\phi \mathbf{K}$ le produit semi-direct obtenu. Déterminer son centre.
3) Montrer qu'il admet trois sous-groupes d'indice 2, deux à deux non isomorphes. Pourquoi sont-ils caractéristiques dans **G** ?
4) Vérifier que le produit semi-direct obtenu n'est pas isomorphe au groupe diédral $\mathbb{D}_{16}$. On le nomme **groupe semi-diédral**.
5) Y a-t-il d'autres produits semi-directs de la forme $\mathbb{Z}/8 \rtimes_\psi \mathbb{Z}/2$?

SOLUTIONS

3.4.1 1) Si tout élément vérifie $x^2 = e$, on sait que le groupe est commutatif. Voir 1.1.13. Soit un élément a (différent de e) qui n'est pas d'ordre 2, il est d'ordre 4 (car s'il était d'ordre 8, le groupe serait cyclique et commutatif). Le groupe $\mathbf{H} = \langle a \rangle$ est d'indice 2, donc normal dans **G**. (1.2.21). Si b n'est pas dans **H**, $\overline{b}^2 = e$ dans le quotient **G**/**H** qui est d'ordre 2, donc $b^2 \in \mathbf{H}$. Si b est d'ordre 2, $b^2 = e$, sinon, b est d'ordre 4, et b^2, d'ordre 2 dans $\langle a \rangle$ ne peut être que a^2. En définitive, $b^2 = e$ ou $b^2 = a^2$.

2) Remarquons que, dans les deux cas, les huit éléments de **G** sont :

$$e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b$$

car ils sont distincts, comme on le vérifie aisément. Cherchons le conjugué de a par b ; il est de même ordre que a, et est dans $\langle a \rangle$, mais ce ne peut être a, sinon le groupe est commutatif ; c'est donc a^3 et $bab^{-1} = a^3 = a^{-1}$. Si $b^2 = e$, on retrouve la définition par générateurs et relations du groupe diédral. Si $b^2 = a^2$ c'est celle du groupe quaternionique (2.3.1).

3.4.2 Il y a un seul p-Sylow, car un p-Sylow est d'indice 2 donc normal dans **G**. Nous avons vu deux démonstrations de ce résultat, 3.2.12 et 1.2.21. De plus, ce p-Sylow est d'ordre p donc isomorphe à $\mathbb{Z}/p$. Le nombre de 2-Sylow est impair et diviseur de p ; c'est un ou p.

- Si c'est un, ce 2-Sylow est normal, son intersection avec le p-Sylow est réduite à un élément (p impair), on peut appliquer le critère du produit direct, **G** est $\mathbb{Z}/p \times \mathbb{Z}/2$, isomorphe à $\mathbb{Z}/2p$.
- Si c'est p, on a toujours une intersection réduite au neutre, mais le produit est semi-direct non direct. $\mathbb{Z}/2$ ne peut agir d'une façon non triviale que par $x \mapsto x^{-1}$ (en notation multiplicative)[1] ; on reconnaît le groupe diédral $\mathbb{D}_{2p}$.

3.4.3 Soit **G** un groupe d'ordre p^2. Si un de ses éléments est d'ordre p^2, il engendre **G**, qui est cyclique. Sinon, tous les éléments (sauf e) sont d'ordre p. Soit $\mathbf{H} = \langle x \rangle$ le sous-groupe d'ordre p engendré par un élément (différent de e) de **G**. Alors **H** est normal dans **G**, en tant

1. En effet, quand p est premier, l'équation $r^2 \equiv 1 \pmod{p}$ n'a pour solution que 1 ou -1.

que groupe d'indice p, où p est le plus petit premier divisant l'ordre de $\mathbf{G}$. Si y est un élément de $\mathbf{G}$ qui n'est pas dans $\mathbf{H}$, il engendre un groupe $\mathbf{K}$ tel que $\mathbf{H} \cap \mathbf{K} = \{e\}$, par le théorème de Lagrange. Donc $\mathbf{HK}$ est un produit direct et il est isomorphe à $\mathbb{Z}/p \times \mathbb{Z}/p$. De plus, $\mathbf{HK}$ est $\mathbf{G}$, pour des raisons de cardinal. Il y a ainsi deux groupes d'ordre p^2, tous les deux commutatifs. Parmi les « petits » groupes, cela concerne donc l'ordre 4, 9, 25, 49,...

3.4.4 1) $\mathbf{G}$ est un groupe non commutatif d'ordre 12, et $\mathbf{S}$ un 3-Sylow, de cardinal 3. Alors $\mathbf{G}$ agit par translation sur $\mathbf{G}/\mathbf{S}$, de cardinal 4. Le noyau de l'action est inclus dans $\mathbf{S}$. S'il est trivial, $\mathbf{G}$ est isomorphe à un sous-groupe de $\mathcal{S}_4$, et comme il est de cardinal 12, ce ne peut être que $\mathcal{A}_4$. On sait qu'il y a alors quatre 3-Sylow, engendré par les 3-cycles. Autre possibilité, le noyau est $\mathbf{S}$, qui est donc normal dans $\mathbf{G}$, et $\mathbf{G}$ n'a qu'un seul 3-Sylow. Il y a alors deux éléments d'ordre 3.

2) On a donc maintenant $\mathbf{G} \neq \mathcal{A}_4$, Soit x l'un des deux éléments d'ordre 3. Alors il existe un élément y d'ordre 2 qui commute avec x. En effet, le centralisateur de x a pour indice le nombre des conjugués de x, (3.2.1) donc, soit 1, soit 2. Ce centralisateur a un cardinal pair, il a un élément d'ordre 2 noté y. Le produit $a = xy$ est d'ordre 6, puisque x et y commutent. Le groupe $\langle a \rangle$ est normal dans $\mathbf{G}$ puisque d'indice 2.

3) Le groupe $\langle a \rangle$ contient un élément d'ordre 2, en l'occurence a^3. S'il existe dans $\mathbf{G}$ un autre élément d'ordre 2, mettons b, alors $\langle a \rangle \cap \langle b \rangle = \{e\}$, de plus, pour des raisons de cardinal, $\langle a \rangle \langle b \rangle = \mathbf{G}$, et comme $\langle a \rangle$ est normal dans $\mathbf{G}$, celui-ci est produit semi-direct de $\langle a \rangle$ et de $\langle b \rangle$. Hormis le cas commutatif, la seule action possible est donnée par $bab^{-1} = a^{-1}$, puisque c'est le seul automorphisme de $\mathbb{Z}/6$ différent de l'identité. On reconnaît le groupe diédral $\mathbb{D}_{12}$.

4) Dans ce cas, les éléments de $\mathbf{G} \setminus \langle a \rangle$ sont d'ordre 4, puisque 2, 3 et 6 sont à rejeter ; (on exclut le cas 6 en remarquant que si c est d'ordre 6, c^2 est d'ordre 3 donc est a^2 ou a^4 et c^3 d'ordre 2 est a^3 donc $c = a$ ou $c = a^{-1}$). Soit b l'un de ces éléments d'ordre 4. Alors b^2 est d'ordre 2, ce ne peut être que a^3, et bab^{-1} est un élément d'ordre 6 de $\langle a \rangle$, ce ne peut être que a^{-1}, car si c'était a, a et b commuteraient, et $\mathbf{G}$ serait commutatif. On reconnaît ainsi une des présentations du groupe dicyclique $\mathcal{T}$:

$$\mathcal{T} = \langle a, b, \mid a^6 = e,\ b^2 = a^3,\ bab^{-1} = a^{-1} \rangle$$

3.4.5 1) Un 3-Sylow a neuf éléments. Le nombre des 3-Sylow est congru à 1 modulo 3 et diviseur de 2, c'est donc 1. Le seul 3-Sylow $\mathbf{H}$ est donc normal dans $\mathbf{G}$. Soit a un élément d'ordre 2 de $\mathbf{G}$. Alors $\mathbf{H} \cap \langle a \rangle = \{1\}$, car a n'est pas dans $\mathbf{H}$, qui ne contient pas d'éléments d'ordre 2. De plus, $\mathbf{H}$ et a engendrent $\mathbf{G}$, car $\mathbf{H}$ est d'indice 2 ; on en déduit que $\mathbf{G}$ est produit semi-direct de $\mathbf{H}$ et de $\mathbb{Z}/2$, par le critère de produit semi-direct.

2) On suppose que $\mathbf{H} = \mathbb{Z}/9$. Les automorphismes de $\mathbb{Z}/9$ sont, en notation multiplicative, $x \mapsto x$, $x \mapsto x^2$, $x \mapsto x^4$, $x \mapsto x^5 = x^{-4}$, $x \mapsto x^7 = x^{-2}$, $x \mapsto x^8 = x^{-1}$. Parmi ces automorphismes, seul le dernier est d'ordre 2 ; il y a donc une seule structure semi-directe qui est celle du groupe diédral $\mathbb{D}_{18}$.

3) Les automorphismes de $\mathbb{Z}/3 \times \mathbb{Z}/3$ sont beaucoup plus nombreux. Ce sont, en effet, les applications linéaires bijectives de l'espace vectoriel [1] $(\mathbb{F}_3)^2$ dans lui-même, puisque tout

1. Rappelons qu'on note $\mathbb{F}_p$ le corps à p éléments.

morphisme est forcément $\mathbb{F}_3$-linéaire. Dans ce groupe de 48 éléments, il y en a 12 d'ordre 2, ce sont $-I$ et les matrices de trace nulle et de déterminant -1 ; elles sont toutes semblables à la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. En dimension 2, deux matrices sont semblables si elles ont même trace et même déterminant. Il y a donc deux structures de produit semi-direct. La première est définie par :

$$\mathbf{G}_1 = (\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes_{\phi_1} \mathbb{Z}/2 \text{ où } \phi_1(1)(a,b) = (-a,-b)$$

et la seconde :

$$\mathbf{G}_2 = (\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes_{\phi_2} \mathbb{Z}/2 \text{ où } \phi_2(1)(a,b) = (b,a)$$

Ce dernier cas est un exemple de **produit en couronne**, celui de $\mathbb{Z}/3$ par $\mathbb{Z}/2$. Voir le problème en fin de chapitre pour plus de précision sur cette notion.

4) Comment reconnaître que ces groupes sont différents ? Ici encore, l'étude des ordres des éléments va suffir.

Dans le cas du groupe diédral $\mathbb{D}_{18}$, on trouve :

– un élément d'ordre 1, neuf d'ordre 2, deux d'ordre 3, six d'ordre 9.

Dans le cas du groupe $\mathbf{G}_1$:

– un élément d'ordre 1, neuf d'ordre 2, huit d'ordre 3.

Dans le cas du groupe $\mathbf{G}_2$:

– un élément d'ordre 1, trois d'ordre 2, huit d'ordre 3, six d'ordre 6.

Le groupe à 18 éléments $\mathcal{S}_3 \times \mathbb{Z}/3$ coïncide avec ce groupe $\mathbf{G}_2$ comme le montre l'ordre de ses éléments. Remarquons, pour conclure, que le groupe $\mathbf{G}_1$ peut être engendré par ses éléments

$$a = ((1,0),1),\ b = ((0,1),1),\ c = ((0,0),1)$$

avec la présentation :

$$\mathbf{G}_1 = \langle a,b,c \mid a^2 = b^2 = c^2 = (abc)^2 = (ab)^3 = (ac)^3 = 1 \rangle$$

3.4.6 1) Supposons $p < q$. Le nombre de q-Sylow est s_q, de la forme $1 + kq$ et c'est un diviseur de p ; ce ne peut donc qu'être 1. Il y a donc un seul q-Sylow qui est normal dans $\mathbf{G}$.

2) Avec les mêmes hypothèses, soit s_p le nombre des p-Sylow. Alors $s_p \equiv 1 \pmod{p}$ et $s_p \mid q$. Si donc $q \not\equiv 1 \pmod{p}$, il n'y a qu'un seul p-Sylow qui est normal dans $\mathbf{G}$. Les deux sous-groupes de Sylow sont cycliques puisqu'ils ont pour ordres respectifs q et p et ils satisfont le critère de produit direct. Leur intersection ne peut être que e car leurs ordres sont premiers. On peut donc affirmer que $\mathbf{G}$ est isomorphe au produit direct $\mathbb{Z}/p \times \mathbb{Z}/q$ qui est lui même cyclique, par le théorème chinois.
Les cas qui correspondent à cette situation sont :

$p = 3 : q = 5, 11, 17, 23, 29...$	d'où les ordres : $15, 33, 51, 69, 87...$
$p = 5 : q = 7, 13, 17, 19...$	d'où les ordres :$35, 65, 83, 95...$
$p = 7 : q = 11, 13...$	d'où les ordres :$77, 91...$

On obtient ainsi des entiers n, tel qu'il n'existe, à isomorphisme près, qu'un seul groupe d'ordre [1] n.

3) Si $q \equiv 1 \pmod{p}$, alors il peut y avoir plusieurs p-Sylow. Soit $\mathbf{K}$ un de ces groupes, et $\mathbf{N}$ l'unique q-Sylow. Ces deux groupes satisfont le critère du produit semi-direct comme ci-dessus et leur produit ne peut être que $\mathbf{G}$.
Étudions maintenant l'action de $\mathbf{K}$ sur $\mathbf{N}$; le groupe $\mathrm{Aut}(\mathbb{Z}/q)$ est d'ordre $q-1$: notre action est définie par un morphisme de $\mathbb{Z}/p$ dans $\mathbb{Z}/q-1$. Si ce morphisme n'est pas trivial, ce qui donne le cas du produit direct, il est injectif puisque p est premier. $\mathbb{Z}/p$ a pour image sur un sous-groupe d'ordre p de $\mathbb{Z}/q-1$, ce groupe existe car $p \mid q-1$, et il existe un élément d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q)$ (lemme de Cauchy). Par exemple, si $p=3$ et $q=7$, on obtient deux structures semi-directes, données par :

$$\langle a, b \mid a^7 = b^3 = 1,\ bab^{-1} = a^2 \rangle \text{ et } \langle a, b \mid a^7 = b^3 = 1,\ bab^{-1} = a^4 \rangle$$

car $2^3 \equiv 4^3 \equiv 1 \pmod{7}$. Ces produits semi-directs sont isomorphes : dans la première présentation, en remplaçant b par b^2, on a $(b^2)^3 = 1$ et $b^2ab^{-2} = a^4$, on retrouve la seconde présentation.

Les cas qui correspondent à cette situation sont :

$$p = 2 : q = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47...$$

d'où les ordres : 6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86, 94...

$p = 3 : q = 7, 13, 19, 31...$ d'où les ordres :21, 39, 57, 93...
$p = 5 : q = 11...$ d'où l'ordre : 55...

En ajoutant les groupes d'ordre p^2 et les groupes d'ordre 99, on obtient tous les n inférieurs à 100, tel qu'il existe deux groupes d'ordre n.

3.4.7 1) Considérons $\mathbf{N}$ muni de sa structure de $\mathbb{F}_p$-espace vectoriel. Alors tout automorphisme du groupe additif est automatiquement un automorphisme d'espace vectoriel, et réciproquement. L'application définie par

$$c.a = a,\ c.b = ab$$

a, pour matrice, dans la base (a, b) :

$$\mathrm{Mat}(\phi(c)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

C'est donc la matrice d'une transvection. On est bien dans le cas d'une action car cette matrice est d'ordre p. Plus précisément, $\mathbb{Z}/p$ est isomorphe au groupe des matrices de la forme :

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

2) Il suffit de traduire l'action par des automorphismes intérieurs. $c.b = b$ s'écrit $cbc^{-1} = b$ soit $bc = cb$, de même $c.a = ab$ s'écrit $b = cac^{-1}a^{-1}$. Enfin, la présentation de $\mathbf{N}$ est :

$$\mathbf{N} = \langle a, b \mid a^p = b^p = 1,\ ab = ba \rangle$$

1. En ajoutant le cas où l'ordre de $\mathbf{G}$ est premier, on obtient tous les cas où $n < 100$ et où il n'y a qu'un seul groupe d'ordre n. Cela ne se poursuit pas ; il y a un seul groupe d'ordre $255 = 3 \times 5 \times 17$.

On obtient donc pour le produit semi-direct :

$$\mathbf{G} = \langle a, b, c \mid a^p = b^p = c^p = 1,\ ab = ba,\ bc = cb,\ b = cac^{-1}a^{-1} \rangle$$

en effet, comme a et c commutent avec b, et que $ca = abc$, les éléments de $\mathbf{G}$ peuvent s'écrire $x = a^k b^\ell c^m$ (où les exposants sont positifs) et sont donc en nombre inférieur à p^3. On conclut par le théorème de Von Dyck. De plus, le calcul des puissances successives de x montre que :

$$x^p = a^{pk} b^{p\ell + p(p-1)mk/2} c^{pm}$$

ce qui montre que tout élément est d'ordre p quand p est impair.

3) Lorsque $p = 2$, les éléments ac et abc sont d'ordre 4, comme le montre le calcul précédent. Tous les autres (sauf e) étant d'ordre 2, on reconnaît le groupe diédral $\mathbb{D}_8$, qui peut donc s'écrire :

$$\mathbb{D}_8 = \mathcal{V} \rtimes_\phi \mathbb{Z}/2$$

l'action étant définie par :

$$1.(a, b) = (a + b, b)$$

4) Vérifions que c'est une action :

$$b.a = a^{p+1} \Rightarrow b^p.a = a^{(p+1)^p} = a$$

car

$$(1 + p)^p = 1 + p^2 + C_p^2 p^2 + \ldots \equiv 1 \pmod{p^2}$$

La traduction de l'action par automorphisme intérieur montre que le produit semi-direct satisfait les mêmes relations que

$$\mathbf{G} = \langle a, b \mid a^{p^2} = b^p = 1,\ bab^{-1} = a^{p+1} \rangle$$

et l'on voit, comme toujours, que les éléments de $\mathbf{G}$ peuvent s'écrire $a^k b^\ell$ où $0 \leqslant k \leqslant p^2 - 1$ et $0 \leqslant \ell \leqslant p - 1$, ce qui prouve que $\mathbf{G}$ contient au maximum p^3 éléments ; on conclut par le théorème de Von Dyck. Dans le cas $p = 2$, on retrouve encore le groupe diédral, mais dans les autres cas, il s'agit d'un groupe différent du précédent, car ses éléments non triviaux ne sont pas tous d'ordre p.

5) Supposons pour commencer qu'il existe un élément, a, d'ordre p^2. Soit $\mathbf{N} = \langle a^2 \rangle$, alors $\mathbf{N}$ est normal dans $\mathbf{G}$, puisqu'il est d'indice p, plus petit facteur premier de p^3. Soit $b \notin \mathbf{N}$. Alors $b^p \in \mathbf{N}$, puisque le quotient est d'ordre p, et $bab^{-1} \in \mathbf{N}$. On désire retrouver la présentation précédente et donc avoir $b^p = 1$ et $bab^{-1} = a^{p+1}$, mais ce n'est pas immédiat, il faut « changer » b.
Posons pour commencer $bab^{-1} = a^r$. Alors

$$a = b^p ab^{-p} = a^{r^p}$$

puisque $b^p \in \mathbf{N}$ commute avec a. On en déduit que $r^p \equiv 1 \pmod{p^2}$. Un théorème d'arithmétique dit que $r^p \equiv r \pmod{p}$. Par soustraction, on en déduit $r = 1 + sp$. Mais alors,

$$b^j ab^{-j} = a^{r^j} = a^{(1+sp)^j} = a^{1+spj}$$

puisque a est d'ordre p^2. Si l'on choisit j de sorte que $sj \equiv 1 \pmod{p}$, on obtient $b^j ab^{-j} = a^{p+1}$. On peut donc remplacer b par $b' = b^j$, on aura toujours $b^j \notin \mathbf{N}$ puisque j est premier à p.

On a alors $b'^p \in \mathbf{N}$ donc $b'^p = a^k$. Mais k est multiple de p, sinon a^k serait d'ordre p^2 et b' d'ordre p^3 et le groupe serait cyclique. Posons $b'^p = a^{pu}$. Considérons alors $b'' = a^u b$:

$$b''^p = a^u b' a^u b \dots a^u b' = b'^{-p} p a^{u(1+(1+p)+(1+p)^2+\dots+(1+p)^{p-1}} = b'^{-p} a^{up} = e$$

en effet,

$$1 + (1+p) + (1+p)^2 + \dots + (1+p)^{p-1} \equiv p + p(1 + 2 + 3 + \dots + p - 1) \equiv p \pmod{p^2}$$

On a également utilisé $b'^j a = a^{1+p} b'^j$, et l'on peut vérifier qu'on a toujours $b'' a b''^{-1} = a^{1+p}$. En définitive, on a bien obtenu la présentation :

$$\mathbf{G} = \langle a, b \mid a^{p^2} = b^p = 1,\ bab^{-1} = a^{p+1} \rangle$$

Supposons pour terminer qu'il n'y ait aucun élément d'ordre p^2. Alors le centre $\mathcal{Z}(\mathbf{G})$ est d'ordre p, car il n'est pas trivial ($\mathbf{G}$ est un p-groupe) et ne peut être d'ordre p^2, sinon il commuterait avec tous les sous-groupes d'ordre p, et $\mathbf{G}$ serait produit direct et commutatif. Le quotient $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est d'ordre p^2, et ne contient que des éléments d'ordre p (et le neutre), car $\mathbf{G}$ ne contient pas d'élément d'ordre supérieur. Il est donc du type

$$\mathbf{G}/\mathcal{Z} = \langle \alpha, \beta \mid \alpha^p = \beta^p = 1,\ \alpha\beta = \beta\alpha \rangle$$

Si l'on note a et b des représentants des classes α et β, alors :

$$a^p = b^p = 1,\ aba^{-1}b^{-1} \in \mathcal{Z}(\mathbf{G})$$

et l'on note c ce dernier élément qui n'est pas égal à 1, sinon $\mathbf{G}$ serait commutatif. En définitive, $\mathbf{G}$ est engendré par a, b, c vérifiant :

$$a^p = b^p = c^p = 1,\ ac = ca,\ bc = cb,\ c = aba^{-1}b^{-1}$$

ce qui correspond bien à la présentation du groupe décrit plus haut.

3.4.8 1) D'après les études précédentes, il suffit de vérifier que $3^2 \equiv 1 \pmod 8$ ce qui est vrai.

2) Comme dans les exercices ci-dessus, les seize éléments de notre produit semi-direct s'écrivent $a^k b^\ell$ où $0 \leqslant k \leqslant 7$ et $0 \leqslant \ell \leqslant 1$. La loi se transcrit :

$$(a^k b^\ell)(a^{k'} b^{\ell'}) = a^{k+k'3^\ell} b^{\ell'-\ell}$$

On en déduit aisément que le centre est le groupe à deux éléments $\langle a^4 \rangle$.

3) $\mathbf{G}$ admet le sous-groupe normal $\mathbf{N}$ isomorphe à $\mathbb{Z}/8$, le sous-groupe $\langle a^2, b \rangle$ est isomorphe au groupe diédral $\mathbb{D}_8$ puisque $ba^2b^{-1} = (a^3)^2 = a^{-2}$, et l'on obtient la présentation du groupe diédral. Enfin, $\langle a^2, ab \rangle$ engendré par deux éléments d'ordre 4 est isomorphe à $\mathbb{H}_8$, et contient :

$$e,\ a^2,\ a^4,\ a^6,\ ab,\ a^3b,\ ,a^5b,\ a^7b$$

On vérifie aisément qu'il n'y a pas d'autre groupe à 8 éléments. Comme ces sous-groupes sont deux à deux non isomorphes, ils sont caractéristiques dans $\mathbf{G}$.

4) $\mathbf{G}$ n'est pas diédral car $\mathbb{D}_{2n}$ ne contient qu'un sous-groupe d'indice 2.

5) L'équation $r^2 \equiv 1 \pmod 8$ a pour solution $r = 1, 3, 5, 7$. Le premier cas donne le produit direct, le dernier donne le groupe diédral ; reste à examiner le troisième. Il est donné par la présentation :

$$\langle a, b \mid a^8 = b^2 = 1,\ bab^{-1} = a^5 \rangle$$

et un rapide examen des ordres de ses éléments montre qu'il n'est pas isomorphe aux deux produits semi-directs précédents.

3.5 PROBLÈMES

3.5.1 Les groupes $\mathbf{GL}(n,\mathbb{K})$, $\mathbf{PGL}(n,\mathbb{K})$, $\mathbf{SL}(n,\mathbb{K})$, $\mathbf{PSL}(n,\mathbb{K})$

Ce problème est consacré au début de l'étude de ces groupes géométriques qui font partie de ce qu'on nomme les **groupes classiques**. Dans tout le problème, $\mathbb{K}$ est un corps commutatif, fini ou infini.

1) **Préliminaires**

a) Soit $\mathbf{GL}(n,\mathbb{K})$ le groupe des matrices carrées inversibles de dimension n (groupe linéaire), et soit $\mathbf{SL}(n,\mathbb{K})$ formé des matrices de déterminant 1. Montrer que c'est un sous-groupe normal dans $\mathbf{GL}(n,\mathbb{K})$. On l'appelle groupe spécial linéaire.

b) Le groupe linéaire est-il produit semi-direct du groupe spécial linéaire et d'un autre groupe ?

c) On sait que le centre de $\mathbf{GL}(n,\mathbb{K})$ est formé des matrices scalaires ; (*cf.* le premier problème du chapitre 1). Quel est le centre de $\mathbf{SL}(n,\mathbb{K})$?

d) On note $\mathbf{PGL}(n,\mathbb{K})$ et $\mathbf{PSL}(n,\mathbb{K})$ les quotients de $\mathbf{GL}(n,\mathbb{K})$ et de $\mathbf{SL}(n,\mathbb{K})$ par leur centre respectif. Démontrer que ces groupes ont un centre réduit à l'élément neutre. Ces groupes sont dits groupes **projectifs linéaires** et **spécial projectif linéaire**.

e) On note $\mathbb{P}(\mathbb{E})$ l'ensemble des droites d'un espace vectoriel $\mathbb{E}$, et en particulier $\mathbb{P}^{n-1}(\mathbb{K})$ l'ensemble des droites vectorielles de $\mathbb{K}^n$. Démontrer que $\mathbf{PGL}(n,\mathbb{K})$ et $\mathbf{PSL}(n,\mathbb{K})$ agissent fidèlement et transitivement sur $\mathbb{P}^{n-1}(\mathbb{K})$ (appelé **espace projectif** de dimension $n-1$).

2) **Calculs des cardinaux ; premiers cas particuliers**

a) On suppose que $\mathbb{K}$ est un corps fini de cardinal q (qui est donc de la forme $q = p^m$, avec p premier) ; on sait qu'il y a unicité (à isomorphisme près) d'un tel corps [1], que l'on note $\mathbb{F}_q$. Calculer le cardinal de chacun des groupes $\mathbf{GL}(n,\mathbb{K})$, $\mathbf{PGL}(n,\mathbb{K})$, $\mathbf{SL}(n,\mathbb{K})$.

b) On rappelle que $\mathbb{K}^*$ est un groupe cyclique de cardinal $q-1$ (1.1.12). Montrer que l'équation $x^n = 1$ admet $d = n \wedge (q-1)$ solutions dans le corps $\mathbb{F}_q$. En déduire le cardinal de $\mathbf{PSL}(n,\mathbb{K})$.

c) Dresser une table des « petits » cardinaux de ces groupes pour $q \leqslant 9$ et $n \leqslant 3$, et donner la liste des groupes ayant mêmes cardinaux.

d) On considère le cas du corps à deux éléments, noté $\mathbb{F}_2$. Montrer que les quatre groupes $\mathbf{GL}(n,\mathbb{F}_2)$, $\mathbf{PGL}(n,\mathbb{F}_2)$, $\mathbf{SL}(n,\mathbb{F}_2)$, $\mathbf{PSL}(n,\mathbb{F}_2)$ sont isomorphes.

e) Cas particulier : $\mathbf{GL}(2,\mathbb{F}_2)$. En utilisant une action de ce groupe sur les droites de $(\mathbb{F}_2)^2$, démontrer qu'il est isomorphe à $\mathcal{S}_3$.

f) Que dire de $\mathbf{GL}(3,\mathbb{F}_2)$? Préciser, en particulier, les 2-Sylow.

1. *cf.* notamment l'ouvrage de D. Perrin [21].

3) **Autres cas particuliers. $\mathbf{GL}(2,\mathbb{F}_3)$, $\mathbf{GL}(2,\mathbb{F}_4)$, $\mathbf{GL}(2,\mathbb{F}_5)$**

a) On considère le cas du corps à trois éléments, $\mathbb{F}_3 = \{-1, 0, 1\}$, où on confond un entier avec sa classe modulo 3. Montrer, par la méthode vue à la question précédente, que $\mathbf{PGL}(2,\mathbb{F}_3)$ est isomorphe à $\mathcal{S}_4$.

b) Montrer que $\mathbf{SL}(2,\mathbb{F}_3)$, bien qu'ayant le même cardinal, n'est pas isomorphe à $\mathbf{PGL}(2,\mathbb{F}_3)$. Montrer enfin que $\mathbf{PSL}(2,\mathbb{F}_3)$ est isomorphe à $\mathcal{A}_4$.

c) Montrer que $\mathbf{PGL}(2,\mathbb{F}_4)$ est isomorphe à $\mathcal{A}_5$. On utilisera l'exercice 3.2.10. Que dire des groupes $\mathbf{SL}(2,\mathbb{F}_4)$ et $\mathbf{PSL}(2,\mathbb{F}_4)$?

d) Montrer que $\mathbf{PGL}(2,\mathbb{F}_5)$ est isomorphe à $\mathcal{S}_5$. Même méthode, et on utilisera l'exercice 3.2.11. Que dire de $\mathbf{PSL}(2,\mathbb{F}_5)$?

e) Deux questions concernant des sous-groupes de Sylow. Démontrer que le groupe des matrices triangulaires unipotentes supérieures est un p-Sylow de $\mathbf{GL}(n,\mathbb{F}_p)$. Déterminer le nombre de ces p-Sylow et regarder, par exemple, le nombre des 3-Sylow de $\mathbf{GL}(2,\mathbb{F}_3)$.

3.5.2 Produits semi-directs en géométrie

Dans ce problème, nous allons rencontrer des produits semi-directs dans un cadre géométrique. Ce n'est pas un hasard, car qui dit produit semi-direct dit action de groupe, et la notion d'action de groupe est la géométrisation de la notion de groupe ; un produit semi-direct a très souvent une interprétation en tant que groupe géométrique. Nous noterons $\mathcal{E}$ un espace affine de dimension finie, de direction un espace vectoriel $\mathbb{E}$. Si f est une application affine de $\mathcal{E}$ dans $\mathcal{E}$, on note $\overrightarrow{f}$ l'application linéaire associée à f, mais nous ne rappellerons pas tous les théorèmes de géométrie utilisés.

1) **Le groupe affine**

a) Montrer que le groupe des translations $\mathcal{T}(\mathcal{E})$ est normal dans le groupe affine $\mathbf{GA}(\mathcal{E})$ et que le quotient est isomorphe à $\mathbf{GL}(\mathbb{E})$.

b) Trouver un « relèvement » de $\mathbf{GL}(\mathbb{E})$ dans le groupe affine. En déduire que le groupe affine est produit semi-direct. Donner une version « interne » et une version « externe » de cette structure.

c) On suppose que $\mathcal{E}$ est muni d'un repère ; pour simplifier les écritures on se placera dans le cas de la dimension 3. On appelle **matrice augmentée** d'un point x la matrice colonne :

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 1 \end{pmatrix}$$

où (x_1, x_2, x_3) sont les coordonnées de x. Si f est dans le groupe affine, montrer qu'il existe une matrice M, telle que la matrice augmentée de $x' = f(x)$ soit

$$X' = MX$$

On fera intervenir $\mathcal{M}$ la matrice de $\overrightarrow{f}$, ainsi que la matrice des coordonnées de O', image de l'origine. Retrouver, dans cette écriture, la structure de produit semi-direct du groupe affine.

d) Montrer que le sous-groupe des homothéties-translations peut aussi s'écrire comme produit semi-direct.

e) Reconnaître des groupes affines en petite dimension et avec des corps finis. Y a-t-il un lien avec l'holomorphe d'un groupe ?

2) **Le groupe orthogonal**

On appelle **matrice orthogonale** une matrice O de $\mathbf{GL}(n, \mathbb{R})$ qui vérifie :

$$O\,{}^tO = {}^tO\,O = I$$

Si l'on suppose l'espace vectoriel $\mathbb{R}^n$ muni d'une structure d'espace vectoriel euclidien orienté, la base canonique étant orthonormée directe, les matrices orthogonales sont celles des endomorphismes qui conservent le produit scalaire, on les appelle **transformations orthogonales**.

a) Vérifier que l'ensemble des matrices orthogonales est un groupe noté $\mathbf{O}(n, \mathbb{R})$ et appelé **groupe orthogonal**. Que reconnaît-on si $n = 1$, $n = 2$?

b) Montrer que l'ensemble des matrices orthogonales de déterminant positif est un sous-groupe normal de $\mathbf{O}(n, \mathbb{R})$. On le note $\mathbf{SO}(n, \mathbb{R})$ et on le nomme **groupe spécial orthogonal**. Le groupe orthogonal est-il produit (semi)-direct de son sous-groupe spécial avec un autre sous-groupe ?

c) Vérifier que $\mathbf{SO}(2, \mathbb{R})$ est commutatif, d'abord directement, puis en vérifiant et en utilisant que $\mathbf{O}(2, \mathbb{R}) \setminus \mathbf{SO}(2, \mathbb{R})$ est uniquement formé d'involutions.

d) Déterminer tous les sous-groupes finis de $\mathbf{SO}(2, \mathbb{R})$ et de $\mathbf{O}(2, \mathbb{R})$.

e) On considère l'ensemble des quaternions unitaires, c'est-à-dire l'ensemble des éléments q de $\mathbb{H}$ tels que :

$$q = \alpha + \beta i + \gamma j + \delta k, \text{ avec } \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$$

Vérifier que c'est un sous-groupe (non commutatif) de $\mathbb{H}$, en bijection avec la sphère[1] S^3.

f) Soit $\mathbb{E}$ l'espace vectoriel des quaternions purs, c'est-à-dire des éléments de $\mathbb{H}$ de la forme :

$$z = ci + dj + ek, \text{ avec } c,\ d,\ e \in \mathbb{R}$$

On munit $\mathbb{E}$ d'une structure d'espace vectoriel euclidien orienté de sorte que (i, j, k) soit orthonormée directe et on considère l'application ϕ définie par :

$$\phi(q) = z \mapsto qzq^{-1}$$

Vérifier que ϕ est un morphisme de S^3 sur $\mathbf{SO}(3, \mathbb{R})$. En préciser l'image et le noyau, et en déduire l'isomorphisme de groupe :

$$S^3/(\mathbb{Z}/2) \cong \mathbf{SO}(3, \mathbb{R})$$

1. De façon générale, on note S^n la sphère de rayon 1 dans le $\mathbb{R}$-espace vectoriel de dimension $n + 1$.

g) Est-ce que S^3 est produit direct ou semi-direct de $\mathbb{Z}/2$ avec $\mathbf{SO}(3,\mathbb{R})$?

3) **Le groupe des isométries**
On revient à l'espace affine $\mathcal{E}$, et l'on suppose que sa direction $\mathbb{E}$ est munie d'une structure d'espace vectoriel euclidien orienté. On appelle **isométrie** une application qui conserve les distances. On sait que les isométries sont les applications affines dont l'application linéaire est une transformation orthogonale. L'ensemble des isométries est un groupe noté $I(\mathcal{E})$.

a) Montrer que l'ensemble $I^+(\mathcal{E})$ des isométries directes (c'est-à-dire dont l'application linéaire associée est dans $\mathbf{SO}(\mathbb{E})$) est un sous-groupe normal de $I(\mathcal{E})$. Est-ce que $I(\mathcal{E})$ est un produit semi-direct de $I^+(\mathcal{E})$ avec un autre sous-groupe ?

b) Montrer que le groupe des translations $T(\mathcal{E})$ est un sous-groupe normal de $I^+(\mathcal{E})$. Peut-on en déduire une structure de produit semi-direct ?

c) En dimension 2, déterminer tous les sous-groupes finis de $I(\mathcal{E})$, et en donner une interprétation géométrique. On pourra commencer par montrer qu'il y a forcément un point invariant unique.

Chapitre **4**

Groupes commutatifs

Les groupes commutatifs sont assez agréables ; pour certains d'entre eux, on dispose d'un théorème de classification. De plus, les « briques » avec lesquelles on peut les construire sont assez peu variées. Il s'agit de $\mathbb{Z}$, des groupes cycliques, de $\mathbb{Q}$ et de quelques autres... Cela dit, les groupes commutatifs infinis ne se laissent pas apprivoiser si simplement. Intéressons-nous d'abord aux groupes commutatifs finis.

4.1 GROUPES COMMUTATIFS FINIS

Les groupes cycliques et leurs produits (directs) sont commutatifs. Commençons par étudier comment ils peuvent être engendrés.

Exercice 4.1.1

Soit $\mathbf{G} = \mathbb{Z}/2 \times \mathbb{Z}/12 \times \mathbb{Z}/15$. Trouver, en utilisant le théorème chinois (cf. 2.1.4), un groupe isomorphe à $\mathbf{G}$ qui soit produit direct de deux groupes cycliques seulement. En déduire que $\mathbf{G}$ peut être engendré par deux éléments. On donnera un exemple de tels éléments.

Étudions encore un groupe du même type et profitons-en pour définir ce qu'est un *p*-**groupe cyclique**. C'est un groupe cyclique d'ordre p^i où p est premier et $i \in \mathbb{N}^*$. On dit parfois aussi : groupe cyclique primaire.

Exercice 4.1.2

Soit $\mathbf{G}$ le groupe

$$\mathbf{G} = \mathbb{Z}/12 \times \mathbb{Z}/36 \times \mathbb{Z}/15 \times \mathbb{Z}/20$$

1) Montrer que $\mathbf{G}$ est isomorphe au produit de groupes cycliques primaires.
2) Montrer que $\mathbf{G}$ peut aussi s'écrire :
$$\mathbf{G} \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \dots \mathbb{Z}/d_k$$
où les entiers d_i vérifient :
$$\forall i \; d_i | d_{i+1}$$

Les exercices précédents nous ont donné des exemples où des groupes commutatifs finis sont des produits directs de groupes cycliques. Nous allons maintenant démontrer que c'est en fait général : tout groupe commutatif fini est isomorphe à un produit direct de p-groupes cycliques. Et nous obtiendrons, en prime, des propriétés d'unicité. Pour commencer, faisons une convention de notation. On sait que dans le cas d'un ensemble d'indice fini, le produit direct et la somme directe (2.1.12) de groupes coïncident. Comme les groupes commutatifs sont notés additivement, on préférera parler de somme plutôt que de produit, et l'on notera cette somme directe avec le symbole $\oplus$ utilisé également en algèbre linéaire. L'exercice suivant présente ce qu'on appelle la **décomposition primaire**.

Exercice 4.1.3

Soit $\mathbf{G}$ un groupe abélien fini, et p un nombre premier.

1) Démontrer que :
$$\mathbf{G}[p] = \{x \in \mathbf{G} \mid \exists n \in \mathbb{N}, \; p^n x = 0\}$$
est un sous-groupe de $\mathbf{G}$. Ses éléments sont donc ceux qui sont d'ordre une puissance de p. On dit aussi qu'ils sont annulés par une puissance de p. $\mathbf{G}[p]$ s'appelle la **p-torsion** de $\mathbf{G}$.
2) Démontrer que $\mathbf{G}$ est somme directe des $\mathbf{G}[p]$, lorsqu'on restreint p à l'ensemble des diviseurs premiers de $|\mathbf{G}|$. On sera amené à utiliser une relation de Bezout.

Exercice 4.1.4

1) Démontrer que si $\mathbf{G} = \bigoplus_{i \in \mathcal{I}} \mathbf{G}_i$, avec $\mathcal{I}$ fini, alors $\mathbf{G}[p] = \bigoplus_{i \in \mathcal{I}} \mathbf{G}_i[p]$.
2) Déterminer $\mathbb{Z}/n[p]$.
3) On suppose que $\mathbf{G}$ est fini et que p divise le cardinal de $\mathbf{G}$. Montrer que $\mathbf{G}[p]$ est l'unique p-Sylow de $\mathbf{G}$. L'exercice précédent montre donc qu'un groupe commutatif fini est somme directe de ses p-Sylow.

Il nous faut maintenant étudier la structure des groupes de la forme $\mathbf{G}[p]$ lorsque $\mathbf{G}$ est un groupe abélien fini. Commençons par une définition inspirée de l'algèbre linéaire : un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ admet un **supplémentaire** s'il existe $\mathbf{K} \leqslant \mathbf{G}$ tel que $\mathbf{G} = \mathbf{H} \oplus \mathbf{K}$. On dit aussi que $\mathbf{H}$ est **facteur direct** de $\mathbf{G}$.
Rappelons que cela équivaut à
$$\mathbf{G} = \mathbf{H} + \mathbf{K} \quad \text{et} \quad \mathbf{H} \cap \mathbf{K} = \{0\}$$
d'après ce que nous avons appelé le « critère de produit direct », et compte-tenu de ce que, dans le cas commutatif, tous les sous-groupes sont normaux.

Exercice 4.1.5

Dans cette question, le groupe $\mathbf{G}$ n'est pas nécessairement commutatif.

1) Montrer que si $\mathbf{H} \lhd \mathbf{G}$ et si $\mathbf{H}$ admet un supplémentaire $\mathbf{K}$, alors $\mathbf{G}/\mathbf{H} \cong \mathbf{K}$.
2) Montrer qu'aucun sous-groupe non trivial de $\mathbb{Z}$ n'admet de supplémentaire.
3) Si $\mathbf{G} = \mathbb{Z}/n$, chercher les sous-groupes de $\mathbf{G}$ qui ont un supplémentaire.

Passons aux deux exercices fondamentaux qui expliquent comment se décomposent les p-groupes commutatifs finis, puis les groupes commutatifs finis quelconques.

Exercice 4.1.6

1) Soit $\mathbf{G}$ un p-groupe abélien, et g un élément de $\mathbf{G}$ d'ordre maximal p^m. On veut montrer que $\langle g \rangle$ admet un supplémentaire. Soit $\mathbf{H}$ un sous-groupe de $\mathbf{G}$ maximal parmi ceux pour lesquels $\mathbf{H} \cap \langle g \rangle = \{0\}$. On raisonne par l'absurde, en supposant que $\mathbf{G} \neq \mathbf{H} + \langle g \rangle$. Soit x pris d'ordre minimal parmi les éléments de $\mathbf{G} \setminus (\mathbf{H} + \langle g \rangle)$.
   a) En utilisant la définition de x, montrer que $px \in \mathbf{H} + \langle g \rangle$.
   b) On peut donc écrire $px = h + ag$ où $h \in \mathbf{H}$ et $a \in \mathbb{Z}$. Montrer que a est divisible par p.
   c) En déduire qu'on peut trouver q entier non divisible par p tel que $qx \in \mathbf{H} + \langle g \rangle$ et aboutir à une contradiction.
2) Montrer qu'un p-groupe abélien fini se décompose comme somme directe de termes de la forme $\mathbb{Z}/p^{n_i}$. On procédera par récurrence.
3) Montrer que la suite des n_i est unique (à l'ordre près).

Exercice 4.1.7 (Facteurs invariants, diviseurs élémentaires)

Les exercices qui précèdent montrent que tout groupe abélien fini peut s'écrire :

$$\mathbf{G} \cong \left(\mathbb{Z}/p_1^{\alpha_1} \oplus \ldots \oplus \mathbb{Z}/p_1^{\alpha_i}\right) \oplus \ldots \oplus \mathbb{Z}/p_k^{\lambda_k}$$

Cette suite de puissances de nombres premiers est unique (à l'ordre près). On les appelle **diviseurs élémentaires** de $\mathbf{G}$. Démontrer que $\mathbf{G}$ s'écrit également de façon unique :

$$\mathbf{G} \cong \mathbb{Z}/d_1 \oplus \ldots \oplus \mathbb{Z}/d_\ell$$

où les d_i sont des entiers tels que $d_i | d_{i+1}$ pour tout i. Ce sont les **facteurs invariants**.

D'une certaine façon, les groupes commutatifs finis sont analogues aux nombres entiers qui se décomposent en facteurs premiers ; mais la situation est plus compliquée, les groupes de base sont non seulement les $\mathbb{Z}/p$ mais aussi les groupes $\mathbb{Z}/p^\alpha$. Retour à des exemples concrets pour lesquels nous aboutirons à une décomposition complète.

Exercice 4.1.8

Voici quelques quotients finis de $\mathbb{Z}^n$. En donner les diviseurs élémentaires et les facteurs invariants.

$$\mathbf{G}_1 = \mathbb{Z}^2/\langle 2e_1, 3e_2 \rangle \quad \mathbf{G}_2 = \mathbb{Z}^2/\langle 2e_1, 3e_1 + 4e_2 \rangle$$

$$\mathbf{G}_3 = \mathbb{Z}^2/\langle 2e_1 + 2e_2,\ 2e_1 + 6e_2\rangle$$

où (e_1, e_2) représente la base canonique de $\mathbb{Z}^2$.
On pourra commencer par démontrer le (petit) théorème :
Si $\mathbf{A} \lhd \mathbf{K}$ et $\mathbf{B} \lhd \mathbf{H}$, alors $\mathbf{A} \times \mathbf{B} \lhd \mathbf{K} \times \mathbf{H}$ et

$$(\mathbf{K} \times \mathbf{H})/(\mathbf{A} \times \mathbf{B}) \cong (\mathbf{K}/\mathbf{A}) \times (\mathbf{H}/\mathbf{B})$$

Une autre façon d'obtenir des groupes commutatifs finis est de partir d'un anneau fini et d'étudier le groupe de ses éléments inversibles.

Exercice 4.1.9

Déterminer le groupe des inversibles des anneaux $\mathbb{Z}/n$ pour $n = 1 \ldots 12$; comment déduire le groupe des inversibles de l'anneau $\mathbb{Z}/n$ de ses composantes primaires ? En déduire le groupe des inversibles de l'anneau $\mathbb{Z}/45$.

Pour sortir de ces cas particuliers, il est nécessaire d'étudier le groupe des inversibles de l'anneau $\mathbb{Z}/p^\alpha$. Et il s'avère que l'on doit distinguer le cas où $p = 2$ des autres.

Exercice 4.1.10

Dans cet exercice, nous noterons $\mathbf{G}_n$ le groupe des inversibles de l'anneau $\mathbb{Z}/n$.

1) Montrer que le groupe des inversibles des anneaux $\mathbb{Z}/5^\alpha$ est cyclique, pour $\alpha = 1, 2, 3...$ En préciser un générateur.
2) Rappeler pourquoi $\mathbf{G}_p$ est cyclique. (*cf.* 1.1.12).
3) On revient au cas général, où p est un premier différent de 2. Démontrer les congruences :
$$(1+p)^{p^m} \equiv 1 \pmod{p^{m+1}} \text{ et } (1+p)^{p^m} \not\equiv 1 \pmod{p^{m+2}}$$
4) En déduire que le groupe des inversibles de $\mathbb{Z}/p^m$ est cyclique, lorsque $p \neq 2$. On pourra chercher l'ordre de $1 + p$ et montrer qu'il existe des éléments d'ordre $p - 1$.
5) Examiner le cas où $p = 2$; on pourra étudier l'ordre de 5 et montrer que $\mathbf{G}_{2^m}$ est engendré par 5 et par -1.

Exercice 4.1.11

Soit $\mathbf{G}$ un groupe abélien fini et m l'ordre maximum d'un élément de $\mathbf{G}$. Montrer que tout élément g de $\mathbf{G}$ vérifie $mg = 0$. Et si $\mathbf{G}$ est fini non abélien ?

Exercice 4.1.12

Quel est le nombre des groupes commutatifs d'ordre p^n ? Quel est le nombre des groupes commutatifs d'ordre 2 160 ?

Exercice 4.1.13

Soit $\mathbf{G}$ un groupe abélien fini. On note $\widehat{\mathbf{G}}$ l'ensemble des morphismes de $\mathbf{G}$ dans $\mathbb{C}^*$ (muni de sa structure multiplicative). Démontrer que $\widehat{\mathbf{G}}$ est un groupe isomorphe à $\mathbf{G}$.

SOLUTIONS

4.1.1 Dans un premier temps, on peut décomposer $\mathbf{G}$:

$$\mathbf{G} = \mathbb{Z}/2 \times (\mathbb{Z}/4 \times \mathbb{Z}/3) \times (\mathbb{Z}/3 \times \mathbb{Z}/5)$$

et en déduire une écriture plus économique :

$$\mathbf{G} = (\mathbb{Z}/2 \times \mathbb{Z}/3) \times (\mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/5) = \mathbb{Z}/6 \times \mathbb{Z}/60$$

Bien sûr, on peut procéder autrement, et par exemple on trouve directement que $\mathbf{G} = \mathbb{Z}/12 \times \mathbb{Z}/30$.

Ce produit peut être engendré par deux éléments, par exemple $(1,0)$ et $(0,1)$. Cherchons de quels éléments ils proviennent par les isomorphismes ci-dessus :

$$(1,0) \leftarrow ((1,1),(0,0,0)) \leftarrow (1,(0,1),(0,0)) \leftarrow (1,4,0)$$

$$(0,1) \leftarrow ((0,0),(1,1,1)) \leftarrow (0,(1,0),(1,1)) \leftarrow (0,9,1)$$

Une explication, le 9 par exemple est un antécédent de $(1,0)$ dans $\mathbb{Z}/4 \times \mathbb{Z}/3 \cong \mathbb{Z}/12$ car il est congru à 1 modulo 4 et divisible par 3. Il y a bien sûr plusieurs solutions, ne serait-ce que parce que $\mathbf{G}$ contient plusieurs sous-groupes isomorphes à $\mathbb{Z}/3$.

4.1.2 1) Décomposons les nombres 12, 36, 15, 20 en facteurs premiers,

$$12 = 2^2 \times 3,\ 36 = 2^2 \times 3^2,\ 15 = 3 \times 5,\ 20 = 2^2 \times 5$$

et donc le théorème chinois permet de décomposer $\mathbb{Z}/12$ en $\mathbb{Z}/2^2 \times \mathbb{Z}/3$ etc. soit :

$$\mathbf{G} \cong \mathbb{Z}/2^2 \times \mathbb{Z}/2^2 \times \mathbb{Z}/2^2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3^2 \times \mathbb{Z}/5 \times \mathbb{Z}/5$$

Pour le moment, on ne sait pas s'il y a unicité (à l'ordre des facteurs près) de cette décomposition en groupes cycliques primaires. Ce sera fait dans un prochain exercice.

2) D'après le théorème chinois, les d_i vont être de la forme $2^{a_i}3^{b_i}5^{c_i}$, avec des exposants pouvant être nuls, et pris dans la liste ci-dessus. De plus, la relation $d_i | d_{i+1}$ implique $a_i \leqslant a_{i+1}$, $b_i \leqslant b_{i+1}$ et $c_i \leqslant c_{i+1}$. Il suffit de ranger les exposants dans un tableau, [1] :

$$\begin{pmatrix} 2 & 2 & 1 \\ 2 & 1 & 1 \\ 2 & 1 & 0 \end{pmatrix}$$

les colonnes correspondant aux facteurs premiers $2, 3, 5$. On lit les facteurs d_i sur chaque ligne en commençant par le bas $d_1 = 2^2 \times 3 = 12$, $d_2 = 2^2 \times 3 \times 5 = 60$, $d_3 = 2^2 \times 3^2 \times 5 = 180$ et donc

$$\mathbf{G} \cong \mathbb{Z}/12 \times \mathbb{Z}/60 \times \mathbb{Z}/180$$

4.1.3 1) Si $p^n x = 0$ et $p^m y = 0$ alors $p^{\sup(m,n)}(x - y) = 0$, donc $\mathbf{G}[p]$ est un sous-groupe de $\mathbf{G}$.

2) Montrons qu'un élément x d'ordre m où $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ est somme d'éléments d'ordre une puissance d'un premier. Il suffit d'utiliser une relation de Bezout :

$$u_1 m_1 + u_2 m_2 + \ldots + u_k m_k = 1$$

où m_i est le quotient de m par $p_i^{a_i}$; (il est immédiat que les m_i sont premiers entre eux). Alors

$$x = u_1(m_1 x) + u_2(m_2 x) + \ldots + u_k(m_k x)$$

1. C'est un exemple de tableau de Young, voir [20].

est bien une décomposition du type souhaité, puisque $m_i x$ est annulé par $p_i^{a_i}$, et donc aussi $u_i m_i x$. On peut remarquer que les composants de cette écriture sont des multiples de x. Reste à montrer que la somme est directe, c'est-à-dire que cette décomposition est unique. Il suffit, par linéarité, de montrer que :

$$0 = x_1 + x_2 + \ldots + x_k \Rightarrow x_1 = x_2 = \ldots = x_k = 0$$

dès lors que $x_i \in \mathbf{G}[p_i]$ pour tout i. Avec les notations précédentes, on écrit :

$$m_i \times 0 = 0 = m_i x_1 + m_i x_2 + \ldots + m_i x_k = m_i x_i$$

Mais, par définition, x_i est d'ordre une puissance de p_i, et m_i est premier à p_i, donc x_i doit être nul. Lorsque $\mathbf{G}$ est fini de cardinal n, tout élément a pour ordre un diviseur de n, on peut donc se limiter aux p_i diviseurs premiers de n et dire que $\mathbf{G}$ est isomorphe à la somme directe des $\mathbf{G}[p_i]$.

4.1.4 1) Si $x = (x_i)_{i\in\mathcal{I}} \in \mathbf{G}$, $p^n x = (p^n x_i)_{i\in\mathcal{I}}$. Si donc $x \in \mathbf{G}[p]$, alors $x_i \in \mathbf{G}_i[p]$ pour tout i. Réciproquement, si $x = (x_i)_{i\in\mathcal{I}}$ est tel que $x_i \in \mathbf{G}_i[p]$ pour tout i, alors chaque x_i a un ordre de la forme p^{a_i}. Comme la somme est finie, on voit que x est annulé par $p^{\sup(a_i)}$, et l'on a bien l'égalité d'ensemble indiquée. Cet argument ne fonctionne pas si $\mathcal{I}$ est infini, et l'on construit facilement un contre-exemple avec :

$$\mathbf{G} = \prod_{i\in\mathbb{N}^*} \mathbb{Z}/p^i$$

2) Supposons $n = p^\alpha m$ où $p \nmid m$. Tout repose sur l'étude des sous-groupes d'un groupe cyclique. L'ordre d'un élément x est un diviseur d de n, et x est dans le groupe engendré par la classe de $\frac{n}{d}$. Les éléments d'ordre une puissance de p sont donc exactement les éléments du sous-groupe engendré par $\overline{m}$, et ce sous-groupe est isomorphe à $\mathbb{Z}/p^\alpha$. Si p ne divise pas n, $\left(\mathbb{Z}/n\right)[p] = \{0\}$. On peut donc écrire :

$$\mathbb{Z}/n \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i} \qquad \text{si} \qquad n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

C'est bien sûr la décomposition de $\mathbb{Z}/n$ donnée habituellement par le théorème chinois.

3) Il suffit de dire que pour un groupe commutatif, il n'y a qu'un seul p-Sylow ; les p-Sylow sont tous conjugués, c'est-à-dire tous égaux... Tout élément du p-Sylow est d'ordre une puissance de p, et tout élément d'ordre une puissance de p est dans l'unique p-Sylow (puisqu'en général un élément d'ordre p est dans un p-Sylow).

4.1.5 1) C'est le second théorème d'isomorphisme qui s'applique ici, dans le cas particulier où $\mathbf{HK} = \mathbf{G}$ et où $\mathbf{H} \cap \mathbf{K} = \{e\}$, voir 1.2.17. On peut aussi tout redémontrer en partant de l'application qui, à g, associe h lorsque $g = h + k$ où $h \in \mathbf{H}$ et $k \in \mathbf{K}$.

2) Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$. Si $n \neq 0$ et $n \neq 1$, le quotient est fini et ne peut être isomorphe à un $m\mathbb{Z}$. Aucun sous-groupe non trivial de $\mathbb{Z}$ n'admet de supplémentaire.

3) On connaît les sous-groupes de $\mathbb{Z}/n$, si d est un diviseur de n, il existe un sous-groupe d'ordre d, formé des éléments x tels que $dx = 0$. Deux tels sous-groupes d'ordre d et d' ont une intersection réduite à 0 ssi d et d' sont premiers entre eux, et ils engendrent $\mathbb{Z}/n$ ssi de plus $dd' = n$. C'est encore un avatar du théorème chinois... Ainsi, dans $\mathbb{Z}/12$, les sous-groupes $\langle 2\rangle$ et $\langle 6\rangle$ n'ont pas de supplémentaire, mais $\langle 3\rangle$ et $\langle 4\rangle$ en ont. Dans le cas où n est

puissance d'un nombre premier, aucun sous-groupe non trivial n'admet de supplémentaire. Seuls les groupes cycliques primaires sont indécomposables en une somme directe.

4.1.6 1)

a) Si $px \notin \mathbf{H} + \langle g \rangle$, alors px serait d'ordre plus petit que l'ordre de x, contredisant la définition de x.

b) On sait que $p^m x = 0$, puisque $\mathbf{G}$ est un p-groupe avec un élément d'ordre maximal p^m. De $px = h + ag$, on déduit $0 = p^m x = p^{m-1}h + ap^{m-1}g$, d'où

$$ap^{m-1}g \in \mathbf{H} \cap \langle g \rangle = \{0\}$$

comme l'ordre de g est p^m, p divise a.

c) On a donc $px = h + pbg$. Alors $x - bg$ vérifie :

$$p(x - bg) \in \mathbf{H}, \qquad x - bg \notin \mathbf{H}$$

La deuxième affirmation venant de ce que x n'est pas dans $\mathbf{H} + \langle g \rangle$. Mais alors, par définition de $\mathbf{H}$, le groupe engendré par $\mathbf{H}$ et $x - bg$ doit rencontrer $\langle g \rangle$ en un élément non nul. Il existe des entiers k et q, et un élément h' de $\mathbf{H}$ tels que :

$$kg = q(x - bg) + h' \neq 0$$

et l'on a alors $qx \in \mathbf{H} + \langle g \rangle$.
Montrons que p ne divise pas q. Sinon, comme $p(x - bg) \in \mathbf{H}$, on aurait également $q(x - bg) \in \mathbf{H}$ et kg serait à la fois dans $\mathbf{H}$ et dans $\langle g \rangle$ et serait donc nul. Maintenant, à partir des nombres premiers entre eux p et q, on peut construire une relation de Bezout $pp' + qq' = 1$ et $(pp' + qq')x = x \in \mathbf{H} + \langle g \rangle$, c'est la contradiction.

2) On peut donc écrire :

$$\mathbf{G} = \langle g \rangle \oplus \mathbf{H}$$

et $\langle g \rangle$ est un sous-groupe d'ordre bien défini p^{n_1}, ordre maximal d'un élément de $\mathbf{G}$. Le sous-groupe $\mathbf{H}$ est lui-même un p-groupe, auquel on peut faire subir le même traitement. Comme $\mathbf{G}$ est fini, le processus engagé s'arrête, et l'on a obtenu une décomposition de $\mathbf{G}$ en un nombre fini de groupes cycliques d'ordres p^{n_i}.

3) Raisonnons par récurrence sur le cardinal de $\mathbf{G}$. Si $|\mathbf{G}| = p$, pas de problème. On fait l'hypothèse de l'unicité pour tout p−groupe de cardinal inférieur à $|\mathbf{G}|$, et l'on suppose que

$$\mathbf{G} = \mathbf{H}_1 \oplus \mathbf{H}_2 \oplus \ldots \oplus \mathbf{H}_k = \mathbf{K}_1 \oplus \mathbf{K}_2 \oplus \ldots \oplus \mathbf{K}_\ell$$

où les $\mathbf{H}_i$ (resp. les $\mathbf{K}_i$) sont cycliques d'ordre p^{a_i} (resp. p^{b_i}). Pour obtenir un groupe de cardinal plus petit, utilisons la multiplication par p. $p\mathbf{G}$ est un sous-groupe de $\mathbf{G}$ et

$$p\mathbf{G} \cong p\mathbf{H}_1 \oplus p\mathbf{H}_2 \oplus \ldots \oplus p\mathbf{H}_k \cong p\mathbf{K}_1 \oplus p\mathbf{K}_2 \oplus \ldots \oplus p\mathbf{K}_\ell$$

en utilisant les propriétés des sommes directes. Par ailleurs, $p\mathbb{Z}/p^\alpha \cong \mathbb{Z}/p^{\alpha-1}$. En appliquant l'hypothèse de récurrence, on en déduit l'égalité deux à deux des a_i et des b_i en se limitant aux $a_i \neq 1$ et aux $b_i \neq 1$. Mais ces cas exclus correspondent à des facteurs de la forme $\mathbb{Z}/p$; on montre qu'il y en a autant dans chaque décomposition en utilisant le cardinal $\mathbf{G}$.

4.1.7 L'unicité des diviseurs élémentaires résulte de la remarque suivante. Si $\mathbf{G}$ se décompose en produit direct de groupes cycliques, alors $\mathbf{G}[p]$ est le produit de facteurs de la forme $\mathbb{Z}/p^i$. On utilise ensuite l'unicité de la décomposition d'un p-groupe vue dans l'exercice précédent.
L'existence des facteurs invariants s'obtient par la méthode explicitée dans l'exercice 4.1.2, si $p_1, p_2, \ldots, p_k$ est la liste des nombres premiers qui interviennent dans les diviseurs élémentaires, on construit d_ℓ comme produit des p_i aux exposants les plus élevés, puis $d_{\ell-1}$ de la même façon. Le nombre des facteurs invariants est donc le maximum du nombre des groupes apparaissant dans une des p_i-composantes.
L'unicité des facteurs invariants peut s'obtenir ainsi ; on suppose que

$$\mathbf{G} = \mathbf{H}_1 \times \mathbf{H}_2 \times \ldots \times \mathbf{H}_\ell = \mathbf{K}_1 \times \mathbf{K}_2 \times \ldots \times \mathbf{K}_k$$

où $\mathbf{H}_i$ est cyclique d'ordre d_i, $\mathbf{K}_i$ cyclique d'ordre d'_i, avec de plus $d_i \mid d_{i+1}$ et $d'_i \mid d'_{i+1}$. Il suffit alors de considérer $\mathbf{G}[p]$ qui, d'après l'exercice 4.1.4, est le produit de groupes isomorphes à $\mathbb{Z}/p^{\alpha_i}$ (resp. $\mathbb{Z}/p^{\alpha'_i}$), les suites α_i et α'_i étant croissantes. L'unicité de la décomposition d'un p-groupe prouve donc que ces deux suites sont identiques, d'où l'unicité de la suite des facteurs invariants.

4.1.8 Le théorème se démontre en utilisant le morphisme

$$\begin{array}{cccc} \phi & \mathbf{H} \times \mathbf{K} & \to & \mathbf{H}/\mathbf{A} \to \mathbf{K}/\mathbf{B} \\ & (h, k) & \mapsto & h\mathbf{A} \times k\mathbf{B} \end{array}$$

qui est surjectif et dont le noyau est le produit $\mathbf{A} \times \mathbf{B}$; on applique alors le premier théorème d'isomorphisme.
Pour $\mathbf{G}_1$, il suffit d'écrire :

$$\mathbf{G}_1 = (\mathbb{Z}e_1 \oplus \mathbb{Z}e_2)/(\mathbb{Z}2e_1 \oplus \mathbb{Z}3e_2) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$$

en appliquant le théorème. Les diviseurs élémentaires sont 2 et 3, et le facteur invariant est 6.
Pour $\mathbf{G}_2$, commençons par remarquer, qu'il n'a que huit éléments, on constate que

$$(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)$$

sont dans des classes distinctes ; de plus, tout couple d'entiers est dans une de ces classes. Pour se ramener à une seconde coordonnée dans $\{0, \ldots, 3\}$, on utilise un multiple de $(3,4)$, puis un multiple de $(2,0)$ pour la première coordonnée. Enfin, la classe de $(0,1)$ est d'ordre huit, ce qui prouve que

$$\mathbf{G}_2 \cong \mathbb{Z}/8$$

Nous verrons une méthode plus géométrique dans le problème en fin de chapitre.
Pour $\mathbf{G}_3$, enfin, on pourrait procéder comme ci-dessus, mais observons que :

$$\mathbb{Z}(2e_1 + 2e_2) \oplus \mathbb{Z}(2e_1 + 6e_2) = \mathbb{Z}(2e_1 + 2e_2) \oplus \mathbb{Z}(4e_2)$$

et :

$$\mathbb{Z}^2 = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 = \mathbb{Z}(e_1 + e_2) \oplus \mathbb{Z}e_2$$

d'où le quotient :

$$\mathbf{G}_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/4$$

les diviseurs élémentaires et les facteurs invariants coïncident et valent 2, 4.

4.1.9 On sait que les inversibles de l'anneau $\mathbb{Z}/n$ sont les classes des entiers premiers à n. Cela résulte immédiatement de l'identité de Bezout, et le cardinal du groupe (multiplicatif) des inversibles est $\phi(n)$ où ϕ représente l'indicateur d'Euler (1.1.10). On obtient donc les cardinaux suivants, en notant $\mathbf{G}_n$ le groupe des inversibles de l'anneau $\mathbb{Z}/n$:

n	2	3	4	5	6	7	8	9	10	11	12
$\lvert\mathbf{G}_n\rvert$	1	2	2	4	2	6	4	6	4	10	4

Laissons les cas de cardinal 2 où sont inversibles 1 et -1 seulement ; on trouve que $\mathbf{G}_5$, $\mathbf{G}_7$, $\mathbf{G}_9$, $\mathbf{G}_{10}$ et $\mathbf{G}_{11}$ sont cycliques, engendrés respectivement par 2, 3, 2, 3, 2. Par exemple :

$$\mathbf{G}_9 = \{1,\ 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 7,\ 2^5 = 5\}$$

En revanche, $\mathbf{G}_8$ et $\mathbf{G}_{12}$ sont isomorphes à $\mathbb{Z}/2 \times \mathbb{Z}/2$, tous leurs éléments différents de 1 sont d'ordre 2.
Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition primaire de n, alors l'anneau $\mathbb{Z}/n$ est isomorphe au produit des anneaux $\mathbb{Z}/p_i^{\alpha_i}$; on dispose déjà de l'isomorphisme de groupe, les autres vérifications sont immédiates. De même, on montre rapidement que le groupe des inversibles d'un anneau produit est le produit des groupes d'inversibles de chaque facteur. Ainsi, le groupe des inversibles de $\mathbb{Z}/45$ sera isomorphe au groupe $\mathbf{G}_5 \times \mathbf{G}_9$ soit $\mathbb{Z}/4 \times \mathbb{Z}/6$ qui a pour facteurs invariants 2, 2^2, 3 et diviseurs élémentaires 2 et 12.

4.1.10 1) Les calculs sont un peu longs à conduire ; on a vu dans l'exercice précédent que 2 était générateur de $\mathbf{G}_5$. On constate qu'il est également générateur de $\mathbf{G}_{25}$, qui est de cardinal 20. Il suffit pour cela de vérifier que $2^{10} \equiv -1 \pmod{25}$, ce qui est immédiat. On constate de même que $\mathbf{G}_{125}$ est encore cyclique, d'ordre 100, et engendré par 2. On a en effet :

$$2^{10} = -1 + 25k \text{ donc } 2^{50} = (-1 + 25k)^5 \equiv -1 \pmod{125}$$

et l'on peut en déduire que 2 est d'ordre 100 dans $\mathbf{G}_{125}$. On a utilisé une propriété de congruence des coefficients binomiaux : si p est premier, alors

$$\forall k \in \{1, 2, \dots, p-1\},\ C_p^k \equiv 0 \pmod{p}$$

propriété qui est immédiate avec le théorème de Gauss, en écrivant :

$$k!(p-k)!C_p^k = p!$$

2) D'après l'exercice 1.1.12, tout sous-groupe fini d'un corps commutatif est cyclique ; et c'est bien le cas de $\mathbf{G}_p$, puisque l'anneau $\mathbb{Z}/p$ est un corps, ses éléments non nuls sont des classes de nombres premiers à p et sont inversibles.

3) Raisonnons par récurrence ; pour $m = 0$, on a bien

$$1 + p \equiv 1 \pmod{p} \quad \text{et} \quad 1 + p \not\equiv 1 \pmod{p^2}$$

L'hypothèse de récurrence peut s'écrire :

$$\exists k \in \mathbf{N},\ (1+p)^{p^m} = 1 + kp^{m+1}$$

avec k non divisible par p. On en déduit :

$$(1+p)^{p^{m+1}} = \left((1+p)^{p^m}\right)^p = (1 + kp^{m+1})^p \equiv 1 \pmod{p^{m+2}}$$

en utilisant la formule du binôme et la congruence rappelée ci-dessus. On a également :

$$(1+p)^{p^{m+1}} \equiv 1 + kp^{m+2} \pmod{p^{m+3}}$$

en utilisant les trois premiers termes de la formule du binôme, d'où

$$(1+p)^{p^{m+1}} \not\equiv 1 \pmod{p^{m+3}}$$

car k n'est pas divisible par p. Remarquons que cet argument suppose $p > 2$ pour qu'il y ait suffisamment de termes dans la formule du binôme.

4) On en déduit que la classe de $1+p$ est d'ordre p^{m-1} dans $\mathbf{G}_{p^m}$. Or, l'ordre de $\mathbf{G}_{p^m}$ est $p^{m-1}(p-1)$, nombre d'entiers inférieurs à p^m qui sont premiers avec lui. Reste à trouver un élément d'ordre $p-1$. Pour cela, utilisons le morphisme d'anneau de $\mathbb{Z}/p^n$ dans $\mathbb{Z}/p$ défini par :

$$x + p^n\mathbb{Z} \mapsto x + p\mathbb{Z}$$

Ce morphisme est bien défini car $p^n\mathbb{Z} \subset p\mathbb{Z}$. Il est surjectif, et l'image réciproque d'un générateur du groupe cyclique des inversibles de $\mathbb{Z}/p$ sera d'ordre (multiplicatif) multiple de $p-1$. Dans le groupe cyclique qu'il engendre, il y a un élément d'ordre $p-1$.
Conclusion. On dispose d'un élément d'ordre $p-1$, d'un élément $p+1$ d'ordre p^{m-1} ; comme ces ordres sont premiers entre eux, le produit sera d'ordre $p^m - p^{m-1}$ qui est le cardinal de $\mathbf{G}_{p^m}$.

5) Dans le cas $p = 2$, $\mathbf{G}_{2^m}$ est d'ordre 2^{m-1}. Pour trouver un élément d'ordre 2^{m-1}, $1+2 = 3$ ne convient pas toujours, par exemple 3 est d'ordre 2 dans $\mathbf{G}_8$[1]. Au contraire, on va montrer que 5 est d'ordre 2^{m-2} dans $\mathbf{G}_{2^m}$ (en laissant de côté les cas simples $m = 1$ et $m = 2$. On a en effet $5^2 \equiv 1 \pmod{2^3}$ et $5 \not\equiv 1 \pmod{2^3}$, ce qui amorce la récurrence. Ensuite, on voit que :

$$5^{2^{m-2}} = (1+4)^{2^{m-2}} \equiv 1 + 2^m \pmod{2^{m+1}}$$

et cette congruence donne $5^{2^{m-2}} \equiv 1 \pmod{2^m}$, mais aussi, en l'appliquant au rang précédent, $5^{2^{m-3}} \not\equiv \pmod{2^m}$. Le groupe engendré par 5 est donc cyclique d'ordre 2^{m-2}, celui engendré par -1 bien sûr d'ordre 2. Vérifions que ces deux groupes sont d'intersection réduite à 1. En effet, $5^k \equiv -1 \pmod{2^m}$ est impossible car $5 \equiv 1 \pmod 4$ d'où contradiction en élevant à la puissance k. Il y a donc produit direct de deux groupes cycliques et

$$\mathbf{G}_{2^m} \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{m-2}$$

avec les exceptions de $m = 1$ et $m = 2$.

4.1.11 Raisonnons par l'absurde. Soit x d'ordre maximum m, et g qui ne vérifie pas $mg = 0$. Alors, si n est l'ordre de g, on a $1 < n < m$ et si μ est le ppcm de n et m, il est strictement plus grand que m puisque m ne divise pas n. Or, on peut écrire ce ppcm comme produit dd' de deux diviseurs de n et de m premiers entre eux ; il suffit d'utiliser la décomposition en facteurs premiers et de construire d en prenant les facteurs premiers dont l'exposant est maximum dans n, d' avec ceux de m. Un multiple de g sera d'ordre d, un multiple de x sera d'ordre d', et comme la loi est commutative, dd' sera d'ordre μ, ce qui est absurde. Si $\mathbf{G}$ est fini non abélien, ce résultat est faux, il suffit de prendre l'exemple de $\mathcal{S}_3$.

1. Le lecteur est cependant invité à vérifier que 3 convient presque toujours...

4.1.12 Il y a autant de groupes commutatifs que de listes de diviseurs élémentaires qui sont ici de la forme p^i ; le produit des p^i devant être égal à p^n, il y a autant de groupes commutatifs d'ordre p^n que de façons d'écrire n comme somme d'entiers non nuls ; c'est le nombre des partitions de n, déjà rencontré dans l'exercice 2.4.4 et noté $p(n)$. Cela donne, pour les premières valeurs, de n les résultats suivants :

Valeur de n	2	3	4	5	6	7	8	9	10
$p(n)$	2	3	5	7	11	15	22	30	42

Même si ce nombre augmente rapidement, il y a, notamment dans le cas $p = 2$, beaucoup plus de groupes non commutatifs.
Le nombre 2 160 s'écrit $2\,160 = 2^4 3^3 5$ et les suites de facteurs invariants possibles sont au nombre de $p(4)p(3) = 15$.

4.1.13 Commençons par le cas où $\mathbf{G} = \mathbb{Z}/n$. Tout morphisme ϕ de $\mathbf{G}$ dans $\mathbb{C}^*$ est déterminé par l'image $\phi(1)$ du générateur de $\mathbf{G}$. Cette image doit vérifier $\phi(1)^n = 1$ et est donc une racine n-ième de l'unité, et toute racine n-ième de l'unité convient. De plus, si $\phi(1) = \omega^k$ et $\psi(1) = \omega^{k'}$ où ω est une racine primitive n-ième de l'unité, alors :

$$(\phi\psi)(1) = \omega^k \omega^{k'} = \omega^{k+k'}$$

montre qu'il y a isomorphisme entre $\widehat{\mathbf{G}}$ muni de la loi produit et le groupe $\mathbb{Z}/n$.
Pour le cas général d'un groupe fini, commençons par montrer que :

$$\widehat{\mathbf{A} \times \mathbf{B}} \cong \widehat{\mathbf{A}} \times \widehat{\mathbf{B}}$$

Il suffit d'établir une bijection entre ces deux ensembles :

$$(\phi, \psi) \mapsto \Phi \text{ où } \Phi(x, y) = \phi(x)\psi(y)$$

$$\Phi \mapsto (\phi, \psi) \text{ où } \phi(x) = \Psi(x, 0),\ \psi(y) = \Psi(0, y)$$

On peut également écrire cette bijection à l'aide des projections p_1 et p_2 et des inclusions définies par $i_1(x) = (x, 0)$ et $i_2(y) = (0, y)$. Il est alors immédiat que notre correspondance est bien une bijection et que c'est un morphisme.
En utilisant le fait que tout groupe commutatif fini est produit de groupes cycliques, on obtient l'isomorphisme entre $\mathbf{G}$ et $\widehat{\mathbf{G}}$ si $\mathbf{G}$ est abélien fini. Le résultat ne subsiste pas si $\mathbf{G}$ est infini. Ainsi $\widehat{\mathbb{Z}}$ est isomorphe à $(\mathbb{C}^*, \times)$.

4.2 GROUPES COMMUTATIFS DE TYPE FINI

Nous allons maintenant généraliser certains des résultats précédents à un type particulier de groupes infinis. Mais auparavant, intéressons-nous à l'ensemble des éléments d'ordre fini d'un groupe commutatif.

Exercice 4.2.1

1) Un groupe est **sans torsion** s'il n'a aucun élément d'ordre fini, à part le neutre. Il est **de torsion** si tous ses éléments sont d'ordre fini. Montrer qu'un groupe fini est de torsion ; donner un exemple de groupe infini qui est de torsion.

2) Un groupe qui contient à la fois des éléments d'ordre fini et des éléments d'ordre infini est un groupe **mixte**. Parmi les groupes suivants, reconnaître dans laquelle des trois catégories il faut les ranger :

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{R}^*, \times),\ (\mathbb{C}^*, \times),\ (\mathbb{Z} \times \mathbb{Z}/5, +)$$

Exercice 4.2.2

Si $\mathbf{G}$ est un groupe commutatif, on appelle **sous-groupe de torsion** de $\mathbf{G}$ l'ensemble des éléments d'ordre fini. On le note $\mathbf{T}$.

1) Montrer que c'est un sous-groupe normal et même un sous-groupe caractéristique de $\mathbf{G}$.

2) Montrer que le groupe quotient $\mathbf{G/T}$ est sans torsion.

3) Déterminer les sous-groupes de torsion des groupes de l'exercice précédent, ainsi que les quotients. Dans le cas de $\mathbb{C}^*$, on montrera que le groupe de torsion, noté $\mathbb{U}_\infty$ est isomorphe au quotient $\mathbb{Q}/\mathbb{Z}$ (muni de l'addition).

Exercice 4.2.3

Soit $\mathbf{G}$ abélien. Si p est premier, on note $\mathbf{G}[p]$ (p-torsion) l'ensemble des éléments dont l'ordre est une puissance de p. Montrer que c'est un sous-groupe de $\mathbf{G}$, et que le sous-groupe de torsion de $\mathbf{G}$ est somme directe des $\mathbf{G}[p]$. Étudier l'exemple de $\mathbb{U}_\infty$.

Parmi les groupes infinis, nous allons nous limiter maintenant aux groupes de **type fini**, c'est-à-dire aux groupes engendrés par un nombre fini d'éléments. Bien sûr, les groupes finis entrent aussi dans cette catégorie.

Exercice 4.2.4

1) Soit $\mathbf{G} = \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \ldots \times \mathbb{Z}/n_k \times \mathbb{Z} \times \ldots \times \mathbb{Z}$. Vérifier que $\mathbf{G}$ est engendré par un nombre fini d'éléments.

2) Parmi les groupes commutatifs suivants, lesquels sont de type fini :

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{U}_{p^\infty}, \times),\ (\mathbb{U}_\infty, \times)$$

Exercice 4.2.5

Démontrer que si $\mathbf{G}$ est de type fini et s'il est engendré par un ensemble S, alors il existe un sous-ensemble fini de S qui engendre $\mathbf{G}$; autrement dit, de tout ensemble générateur on peut extraire un sous-ensemble générateur fini.

Que peut-on appeler **groupe abélien libre** ? Il s'agit comme pour les groupes libres, du plus grand groupe abélien engendré par un ensemble X d'éléments. Pour être plus précis,

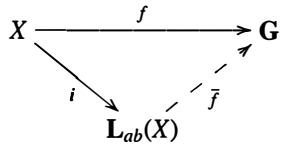
soit X un ensemble (de générateurs), on note $\mathbf{L}_{ab}(X)$ le groupe $\bigoplus_{x\in X}\mathbb{Z}_x$ où les $\mathbb{Z}_x$ sont des copies de $\mathbb{Z}$. Les éléments de ce groupe sont donc des familles d'entiers relatifs $(\alpha_x)_{x\in X}$ nuls sauf un nombre fini [1]. On conviendra, par abus de notation, de noter x la famille nulle sauf $\alpha_x = 1$, et tout élément g de $\mathbf{L}_{ab}(X)$ s'écrit de façon unique :

$$g = \sum_{x\in X} \alpha_x x$$

où les coefficients sont presque tous nuls. Les éléments de X, considérés comme éléments de $\mathbf{L}_{ab}(X)$, constituent ce qu'on appelle une **base** de ce groupe.

Exercice 4.2.6

Montrer que le groupe abélien libre engendré par X a la propriété (dite « universelle ») suivante, si $\mathbf{G}$ un groupe commutatif et f une **application** de X dans $\mathbf{G}$, alors il existe un seul morphisme $\bar{f}$ de $\mathbf{L}_{ab}(X)$ dans $\mathbf{G}$ qui prolonge f.



On se référera à l'exercice 2.2.3.

Exercice 4.2.7

De façon plus générale, un sous-ensemble Y d'un groupe libre $\mathbf{G}$ est une base ssi tout élément g s'écrit de façon unique $g = \sum_{y\in Y} \beta_y y$ où les β_y sont presque tous nuls.

1) Montrer que si $\mathbf{G}$ est libre et de type fini, alors toutes les bases ont un nombre fini d'éléments.
2) Montrer, de plus, qu'elles ont le même cardinal ; on pourra utiliser le quotient $\mathbf{G}/p\mathbf{G}$ où p est un nombre premier. Ce cardinal s'appelle le **rang** du groupe abélien libre.

Nous allons maintenant obtenir pour les groupes commutatifs de type fini un théorème de décomposition analogue au cas fini. Mais il faut commencer par étudier comment les notions de torsion, type fini, liberté se combinent. Et pour pouvoir faire des raisonnements par récurrence, commençons par étudier un certain type de suite exacte.

Exercice 4.2.8

Soit une suite exacte :

$$0 \longrightarrow \mathbf{N} \xrightarrow{a} \mathbf{G} \xrightarrow{b} \mathbf{L} \longrightarrow e$$

où $\mathbf{N}$, $\mathbf{G}$ et $\mathbf{L}$ sont commutatifs, et où $\mathbf{L}$ est libre. Démontrer que cette suite est scindée. En déduire qu'un sous-groupe $\mathbf{N}$ d'un groupe commutatif est facteur direct dès que le quotient $\mathbf{G}/\mathbf{N}$ est libre.

1. On dit alors souvent qu'ils sont presque tous nuls.

Exercice 4.2.9 (Théorème de Dedekind)

Démontrer que si $\mathbf{G}$ est un groupe abélien libre de rang n, alors tout sous-groupe de $\mathbf{G}$ est libre de rang $r \leqslant n$. Le quotient est-il un groupe libre ?

Exercice 4.2.10

1) Démontrer que si $\mathbf{G}$ est commutatif de type fini, alors $\mathbf{G}$ est isomorphe au quotient d'un groupe commutatif libre de type fini par un de ses sous-groupes.
2) Démontrer que tout quotient d'un groupe commutatif de type fini est de type fini.
3) Démontrer que tout sous-groupe d'un groupe commutatif de type fini est de type fini.

Exercice 4.2.11

1) Démontrer que si un groupe commutatif est de type fini et de torsion, alors il est fini.
2) Démontrer que si un groupe commutatif est de type fini et sans torsion, alors il est libre. Cette question est plus délicate. On pourra procéder par récurrence sur le nombre de générateurs.

SOLUTIONS

4.2.1 1) Tout élément x d'un groupe fini de cardinal n vérifie $x^n = e$, et est donc d'ordre fini (diviseur de n). Cela étant, il existe des groupes infinis dont tous les éléments sont d'ordre fini ; c'est le cas du groupe additif de toutes les suites à valeurs dans $\mathbb{Z}/2$, dont tous les éléments sont d'ordre 2. Nous l'avons rencontré dans l'exercice 1.1.8.

2) Les trois premiers groupes sont sans torsion, ils ne contiennent aucun élément d'ordre fini à part 0. Les éléments d'ordre fini de $\mathbb{R}^*$ sont 1 et -1. Il est mixte, de même que $\mathbb{C}^*$, dont les éléments d'ordre fini sont les complexes qui sont racines de l'unité. On note leur ensemble :

$$\mathbb{U}_\infty = \{z \in \mathbb{C} / \exists n \in \mathbb{N}^*,\ z^n = 1\}$$

Le dernier groupe est mixte, les éléments de la forme $(0, a)$ sont d'ordre fini, tous les autres sont d'ordre infini.

4.2.2 1) Si $nx = 0$, $my = 0$, où n et m sont des entiers, alors $mn(x + y) = 0$ et $m(-x) = -mx = 0$. L'ensemble $\mathbf{T}$ des éléments d'ordre fini est donc un sous-groupe ; si ϕ est un endomorphisme de $\mathbf{G}$, $n\phi(x) = \phi(nx) = 0$. C'est donc un sous-groupe (pleinement) caractéristique. En revanche, si $\mathbf{G}$ n'est pas commutatif, le produit de deux éléments d'ordre fini n'est pas forcément d'ordre fini. Un exemple géométrique est bien connu, celui de deux réflexions par rapport à des droites faisant entre elles un angle non commensurable à π, car le composé est alors une rotation d'ordre infini. Si l'ensemble des éléments d'ordre fini est un groupe, il est caractéristique.

2) Soit $\overline{g}$ un élément du quotient $\mathbf{G}/\mathbf{T}$. Alors $\overline{g}$ est d'ordre fini ssi il existe $k \in \mathbb{N}^*$ tel que $k\overline{g} = \overline{0}$, donc $kg \in \mathbf{T}$; mais dire que kg est d'ordre fini implique que g est d'ordre fini, $\overline{g} = \overline{e}$. Cela prouve que le groupe de torsion du quotient est trivial.

3) Regardons maintenant les exemples :

- $\mathbb{R}^*$ muni du produit a pour sous-groupe de torsion $\{-1, 1\}$. Le quotient est $\mathbb{R}_+^*$. Pour le montrer, on peut utiliser le morphisme donné par la valeur absolue.
- $\mathbb{C}^*$ muni du produit a pour sous-groupe de torsion $\mathbb{U}_\infty$. Pour identifier le quotient, commençons par montrer l'isomorphisme :

$$\mathbb{U}_\infty \cong \mathbb{Q}/\mathbb{Z}$$

Il résulte du morphisme

$$\frac{p}{q} \mapsto e^{2i\pi\frac{p}{q}}$$

qui est surjectif car tout élément de $\mathbb{U}_\infty$ s'écrit $e^{2i\pi\frac{p}{q}}$ si c'est une racine q-ième de l'unité. De plus, le noyau de ce morphisme est $\mathbb{Z}$; il ne reste qu'à appliquer le premier théorème d'isomorphisme. On peut alors montrer que :

$$\mathbb{C}^*/\mathbb{U}_\infty \cong \mathbb{R}_+^* \times (\mathbb{R}/\mathbb{Q})$$

en utilisant le morphisme

$$z \mapsto (|z|, \arg(z)\mathbb{Q})$$

ou en utilisant le fait que l'ensemble des nombres complexes de module 1, $\mathbb{U}$, est isomorphe au groupe $\mathbb{R}/\mathbb{Z}$[1].

- $\mathbb{Z} \times \mathbb{Z}/5$ a pour éléments de torsion $\{0\} \times \mathbb{Z}/5$, et le quotient est isomorphe à $\mathbb{Z}$.

4.2.3 Il n'y a aucune modification à faire dans la réponse à l'exercice 4.1.3. Le groupe de torsion d'un groupe commutatif est somme directe des $\mathbb{G}[p]$. Dans le cas où le groupe n'est pas fini, il s'agit ici d'une somme directe pouvant porter sur un ensemble infini d'indices. Pour $\mathbb{U}_\infty$, un élément est dans $\mathbb{U}_\infty[p]$ ssi c'est une racine p^k-ième de l'unité. L'ensemble formé par ces éléments est donc le groupe que nous avons déjà rencontré dans un problème du chapitre 2 ; le p-groupe de Prüfer, $\mathbb{U}_{p^\infty}$, appelé aussi groupe quasi-cyclique. On en déduit donc

$$\mathbb{U}_\infty = \bigoplus_{p\in\mathcal{P}} \mathbb{U}_{p^\infty}$$

4.2.4 1) **G** est engendré par $(1, 0, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)$, il est donc de type fini. Pour le moment, on ne peut affirmer que les générateurs décrits sont en nombre minimal.

2) $\mathbb{Z}$ est bien sûr de type fini, puisqu'il est monogène. Les groupes finis sont également de type fini, puisqu'ils sont engendrés par leurs éléments, en nombre fini. $\mathbb{Q}$ n'est pas de type fini. Voici un argument, si $\mathbb{Q}$ était engendré par un nombre fini d'éléments, ceux-ci auraient un nombre fini de facteurs premiers dans leurs dénominateurs, et il en serait de même pour tous les rationnels. Or l'ensemble des premiers est infini. On peut aussi, plus simplement, regarder les rationnels de la forme $\frac{1}{2^n}$. Les autres groupes sont aussi de type infini ; il suffit de le vérifier pour $\mathbb{U}_{p^\infty}$ qui est un sous-groupe du suivant, et il suffit encore de considérer les éléments de la forme $e^{\frac{2i\pi}{p^n}}$.

1. Au passage, notons l'isomorphisme $\mathbb{U}/\mathbb{U}_\infty \cong \mathbb{R}/\mathbb{Q} \cong \mathbb{R}$, le dernier obtenu par la théorie des espaces vectoriels.

4.2.5 C'est immédiat, si $\mathbf{G}$ est de type fini, il est engendré par un ensemble fini d'éléments $x_1, \ldots, x_k$. Si donc $(y_i)_{i\in\mathcal{I}}$ est une famille génératrice quelconque, il suffit d'écrire les x_i en fonctions d'éléments de la famille $(y_i)_{i\in\mathcal{I}}$, ce qui ne fera apparaître qu'un nombre fini d'éléments de cette famille, et l'on récupère ainsi une sous-famille génératrice finie.

4.2.6 Il est nécessaire de poser $\bar{f}(x) = f(x)$ pour les éléments de X, et pour tout élément de $\mathbf{L}_{ab}(X)$, on aura :

$$\bar{f}\left(\sum_{x\in X}\alpha_x x\right) = \sum_{x\in X}\alpha_x f(x)$$

où les α_x sont des éléments de $\mathbb{Z}$ presque tous nuls. Il y a donc unicité de $\bar{f}$ et on vérifie immédiatement que c'est un morphisme.

4.2.7 1) Si X est une base, il engendre $\mathbf{G}$; l'exercice ci-dessus montre que si $\mathbf{G}$ est de type fini, on peut extraire de X un sous-ensemble fini qui engendre encore $\mathbf{G}$. Mais on garde alors l'unicité de l'écriture et ce sous-ensemble fini est donc une base. En fait, X coïncide avec cet ensemble fini, puisque tout surensemble d'une base n'est plus une base (par unicité de l'écriture). Ce raisonnement vaut pour toutes les bases qui sont donc finies.

2) Supposons que $\mathbf{G}$ soit libre de base $(x_1, x_2, \ldots, x_n)$. Alors

$$\mathbf{G} = \bigoplus_{i=1}^{n}\mathbb{Z}x_i$$

et si p est un nombre premier :

$$\mathbf{G}/p\mathbf{G} \cong \bigoplus_{i=1}^{n}\mathbb{Z}x_i \Big/ \bigoplus_{i=1}^{n}\mathbb{Z}px_i \cong \bigoplus_{i=1}^{n}\mathbb{Z}/p\mathbb{Z}$$

et l'on termine par l'unicité de la dimension d'un espace vectoriel, ou par l'unicité de la décomposition d'un p-groupe fini. On a utilisé que, X étant une base :

$$p\mathbf{G} = \bigoplus_{i=1}^{n}\mathbb{Z}px_i$$

et pour l'isomorphisme l'exercice 4.1.8.

4.2.8 Il s'agit de trouver une section, soit $(e_i)_{i\in\mathcal{I}}$ une base de $\mathbf{L}$. Comme b est surjectif, tout e_i a un antécédent g_i dans $\mathbf{G}$, et l'on peut poser $s(e_i) = g_i$. Mais alors, par la propriété universelle des groupes libres, s se prolonge en un morphisme de $\mathbf{L}$ dans $\mathbf{G}$ et :

$$b\circ s(g) = b\circ s\left(\sum_{i\in\mathcal{I}}x_i e_i\right) = \sum_{i\in\mathcal{I}}x_i b(s(e_i)) = g$$

montre bien que s est une section.
Si l'on applique ce résultat à la suite exacte

$$0 \longrightarrow \mathbf{N} \xrightarrow{a} \mathbf{G} \xrightarrow{b} \mathbf{G}/\mathbf{N} \longrightarrow e$$

on voit que si $\mathbf{G}/\mathbf{N}$ est libre, alors $\mathbf{G}$ est produit semi-direct (donc direct dans le cas commutatif) et $\mathbf{N}$ admet un supplémentaire.

4.2.9 Commençons par le cas où $\mathbf{G}$ est de rang 1. Il est isomorphe à $\mathbb{Z}$, tous ses sous-groupes sont de la forme $n\mathbb{Z}$ et sont aussi de rang 1 (sauf si $n = 0$ où le rang est par convention nul). Supposons que le théorème soit vrai pour tous les groupes libres de rang n, et supposons que $\mathbf{G}$ soit de rang $n+1$; posons

$$\mathbf{G} = \bigoplus_{i=1}^{n+1} \mathbb{Z}e_i \text{ et } \mathbf{G}' = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$$

Soit alors $\mathbf{H}$ un sous-groupe de $\mathbf{G}$ et $\mathbf{H}' = \mathbf{H} \cap \mathbf{G}'$; alors par hypothèse de récurrence $\mathbf{H}'$ est libre de rang $\leqslant n$. Le second théorème d'isomorphisme (en notation additive) permet aussi d'écrire :

$$\mathbf{H}/\mathbf{H}' \cong \mathbf{H}/\mathbf{H} \cap \mathbf{G}' \cong (\mathbf{H} + \mathbf{G}')/\mathbf{G}' \leqslant \mathbf{G}/\mathbf{G}' \cong \mathbb{Z}$$

Donc $\mathbf{H}/\mathbf{H}'$ est isomorphe à un sous-groupe de $\mathbb{Z}$. Si c'est 0, alors $\mathbf{H}$ est isomorphe à $\mathbf{H}'$ donc libre, sinon, $\mathbf{H}/\mathbf{H}'$ est isomorphe à $\mathbb{Z}$, libre donc $\mathbf{H}'$ est facteur direct de $\mathbf{H}$ (exercice précédent). On peut écrire $\mathbf{H} = \mathbf{H}' \oplus \langle h \rangle$ car le supplémentaire est isomorphe au quotient donc de rang un. $\mathbf{H}$ est donc libre de rang $r + 1 \leqslant n + 1$.

> ***Remarque :*** ce **théorème de Dedekind** reste vrai dans le cas d'un groupe libre commutatif quelconque (i.e. non de type fini) avec une démonstration de même style. Il est vrai également pour un groupe libre quelconque, c'est le théorème de Nielsen-Schreier, de démonstration plus difficile. Il n'y a plus, alors, d'inégalité concernant le nombre des générateurs du sous-groupe.
> Le quotient d'un groupe libre par un de ses sous-groupes n'est pas libre (sauf cas triviaux), voir $\mathbb{Z}/n$ mais aussi l'exercice qui suit.

4.2.10 1) On applique la propriété universelle des groupes libres. Si $\mathbf{G}$ est engendré par $x_1, x_2, \ldots, x_n$, il existe un morphisme surjectif du groupe libre $\bigoplus_{i=1}^{n+1} \mathbb{Z}e_i$ sur $\mathbf{G}$, (dont le noyau est un groupe libre par le théorème de Dedekind), il ne reste qu'à appliquer le premier théorème d'isomorphisme pour obtenir que $\mathbf{G}$ est isomorphe au quotient d'un groupe libre.

2) Avec les mêmes notations, si $\mathbf{H}$ est un sous-groupe de $\mathbf{G}$, alors $\mathbf{G}/\mathbf{H}$ est engendré par les $x_i + \mathbf{H}$, donc est de type fini.

3) Soit $\mathbf{G}$ abélien de type fini ; il est isomorphe à un quotient de groupes libres $\mathbf{L}/\mathbf{M}$ de type fini, et, par le théorème de correspondance, un sous-groupe de $\mathbf{G}$ est isomorphe à un quotient de groupes libres de type fini $\mathbf{M}'/\mathbf{M}$ où $\mathbf{M} \leqslant \mathbf{M}' \leqslant \mathbf{L}$, ce sous-groupe de $\mathbf{G}$ est donc de type fini.

4.2.11 1) C'est direct. Les éléments de $\mathbf{G}$ s'écrivent comme combinaison à coefficients entiers des générateurs, et comme tous ces générateurs sont d'ordre fini, il y a un nombre fini de combinaisons distinctes.

2) On procède par récurrence sur le nombre des générateurs. Supposons que $\mathbf{G}$ soit engendré par un seul élément. Alors s'il est sans torsion, c'est que cet élément est d'ordre infini et $\mathbf{G}$ est libre, isomorphe à $\mathbb{Z}$. Si $\mathbf{G}$ est engendré par $e_1, e_2, \ldots, e_n$, soit $\mathbf{H}$ le sous-groupe défini par :

$$\mathbf{H} = \{x \in \mathbf{G} \mid \exists n \in \mathbb{Z},\ nx \in \langle e_1 \rangle\}$$

alors on vérifie aisément que $\mathbf{H}$ est un sous-groupe (qui contient $\langle e_1 \rangle$). Intuitivement, ce sont les éléments de $\mathbf{G}$ qui sont « colinéaires » à e_1. On voit également que $\mathbf{G}/\mathbf{H}$ est sans torsion, si $k(g + \mathbf{H}) = \mathbf{H}$, c'est que $kg \in \mathbf{H}$ et donc $g \in \mathbf{H}$. C'est cette propriété qui nous a fait choisir $\mathbf{H}$ plutôt que $\langle e_1 \rangle$ pour la récurrence. On voit maintenant en effet que $\mathbf{G}/\mathbf{H}$ étant engendré par $e_2 + \mathbf{H}, \ldots, e_n + \mathbf{H}$ est libre par hypothèse de récurrence. Et l'exercice 4.2.8 nous permet de dire que $\mathbf{H}$ est facteur direct de $\mathbf{G}$. On a donc :

$$\mathbf{G} = \mathbf{H} \oplus \mathbf{M}$$

où $\mathbf{M}$ est libre puisqu'isomorphe à $\mathbf{G}/\mathbf{H}$. On va montrer que $\mathbf{H}$ est également libre. Pour commencer, il est de type fini, car sous-groupe d'un groupe de type fini, et, par la définition même de $\mathbf{H}$, le quotient $\mathbf{H}/\langle e_1 \rangle$ est de torsion ; étant de type fini il est fini, d'ordre, par exemple, k. On en déduit que si $h \in \mathbf{H}$, alors $kh \in \langle e_1 \rangle$, et $\mathbf{H}$ s'injecte dans $k\mathbf{H}$ qui s'injecte dans $\langle e_1 \rangle$ lui-même isomorphe à $\mathbb{Z}$... $\mathbf{H}$ est isomorphe à un sous-groupe de $\mathbb{Z}$, donc est libre. On peut aussi avoir une vision plus géométrique, en considérant $\mathbf{H}$ comme un sous-groupe de type fini d'une « droite » dans un $\mathbb{Q}$-espace vectoriel, et les sous-groupes de type fini de $\mathbb{Q}$ sont isomorphes à $\mathbb{Z}$.

4.3 GROUPES DIVISIBLES

Dans ce paragraphe, nous allons étudier quelques propriétés des groupes commutatifs qui ne sont pas de type fini. Pour commencer, regardons les **groupes divisibles** ; cette notion est aussi importante que celle de groupe libre, et en est, en quelque sorte, la « symétrique ».

Exercice 4.3.1

Un groupe commutatif $\mathbf{G}$ est **divisible** si :

$$\forall g \in \mathbf{G},\ \forall n \in \mathbb{N}^*,\ \exists x \in \mathbf{G},\ nx = g$$

Le mot divisible se comprend, on peut diviser tout élément de $\mathbf{G}$ par n'importe quel entier. En notation multiplicative, on dira que tout élément admet (au moins) une racine n-ième.

1) Montrer que les groupes suivants sont divisibles :

$$(\mathbb{Q}, +),\ (\mathbb{R}_+^*, \times),\ (\mathbb{C}^*, \times),\ (\mathbb{U}_{p^\infty}, \times)$$

2) Montrer que le quotient d'un groupe divisible par un sous-groupe est divisible.

3) Montrer, par des exemples, que les sous-groupes d'un groupe divisible ne sont pas toujours divisibles.

Les deux dernières questions de l'exercice précédent montrent l'analogie avec les groupes libres, en échangeant quotient et sous-groupe. Les exercices suivants continuent la comparaison.

Exercice 4.3.2

Montrer que tout groupe commutatif est isomorphe à un sous-groupe d'un groupe divisible. On pourra commencer par les groupes libres.

Exercice 4.3.3

Montrer qu'un sous-groupe divisible d'un groupe commutatif **G** est toujours facteur direct de **G**. On pourra s'inspirer de l'exercice 4.1.6.

Il est possible de donner la structure des groupes divisibles.

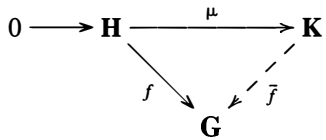
Exercice 4.3.4

Montrer qu'un groupe divisible est somme directe de groupes isomorphes à $\mathbb{Q}$ ou à un p-groupe de Prüfer. On cherchera surtout à étudier ce que donnent les éléments d'ordre infini et ceux d'ordre fini.

Encore une comparaison qui fait appel à la notion de groupe injectif et de groupe projectif.

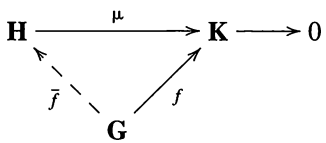
Exercice 4.3.5

1) Un groupe commutatif **G** est **injectif** s'il a la propriété suivante : pour chaque injection $\mu : \mathbf{H} \to \mathbf{K}$ entre groupes commutatifs, si l'on se donne un morphisme f de **H** vers **G**, il se prolonge en un morphisme $\bar{f}$ de **K** vers **G** :



Montrer qu'un groupe commutatif **G** est injectif ssi il est divisible. Pour la réciproque, il convient d'utiliser une méthode proche de celle de l'exercice 4.3.3.

2) Un groupe commutatif **G** est **projectif** s'il a la propriété suivante, pour chaque surjection $\mu : \mathbf{H} \to \mathbf{K}$ entre groupes commutatifs, si l'on se donne un morphisme f de **G** vers **K**, il existe un morphisme $\bar{f}$ de **G** vers **H** tel que $\mu \circ \bar{f} = f$:



Montrer qu'un groupe commutatif **G** est projectif ssi il est libre.

Enfin, pour en terminer avec les groupes commutatifs infinis, un exercice qui étudie un groupe infini indexé par les nombres premiers.

Exercice 4.3.6

Soit $\mathbf{G}$ le produit direct des $\mathbb{Z}/p$ pour tous les premiers p, et soit $\overline{\mathbf{G}}$ la somme directe de ces mêmes groupes, considérée comme sous-groupe de $\mathbf{G}$.

1) Montrer que $\overline{\mathbf{G}}$ est le sous-groupe de torsion de $\mathbf{G}$.

2) Montrer que le quotient $\mathbf{G}/\overline{\mathbf{G}}$ est divisible.

3) Montrer que le sous-groupe de torsion de $\mathbf{G}$ n'est pas facteur direct de $\mathbf{G}$.

SOLUTIONS

4.3.1 1) $\mathbb{Q}$ est divisible, l'équation $nx = \frac{p}{q}$ a pour solution $x = \frac{p}{nq}$. $\mathbb{R}_+^*$ est divisible car tout réel positif admet une racine n-ième, cela se montre par l'analyse, en étudiant la fonction réciproque de la fonction puissance. Enfin un complexe non nul admet n racines n-ièmes, c'est un cas particulier du théorème de d'Alembert-Gauss. Pour le groupe de Prüfer, il faut un peu de calcul. Soit à résoudre $x^n = e^{\frac{2ik\pi}{p^m}}$. Posons $n = p^i s$ où s est premier à p. Les solutions sont alors les complexes :

$$x_\ell = e^{\frac{2i\pi}{sp^{i+m}}(k+\ell p^m)}$$

où ℓ est entier. Une de ces racines sera dans le groupe de Prüfer s'il existe ℓ tel que $k + \ell p^m \equiv 0 \pmod{s}$. Or cela est possible car p^m est inversible modulo s. Le calcul fait peut être clarifié en prenant des exemples, dans $\mathbb{U}_{2^\infty}$, on cherchera une solution de $x^6 = i$.

2) Si $\mathbf{G}$ est divisible et $\mathbf{H}$ un sous-groupe, alors $n(x + \mathbf{H}) = g + \mathbf{H}$ équivaut à $nx - g \in \mathbf{H}$, et l'on peut toujours trouver x qui convienne puisque $\mathbf{G}$ est divisible.

3) Il suffit par exemple de considérer le sous-groupe $\mathbb{Z}$ de $\mathbb{Q}$, qui n'est pas divisible. La situation est un peu plus riche pour le sous-groupe $\mathbb{D}$ des décimaux, qui n'est pas divisible, $3x = 1$ n'a pas de solution, mais pour certaines valeurs de n comme 2 et 5 il y a toujours une solution.

4.3.2 Soit $\mathbf{L}$ un groupe abélien libre. On note $(e_i)_{i\in I}$ une base et

$$\overline{\mathbf{L}} = \bigoplus_{i\in I} \mathbb{Q}e_i$$

Alors $\mathbf{L}$ est un sous-groupe de $\overline{\mathbf{L}}$ qui est divisible. Comme tout groupe commutatif $\mathbf{G}$ est quotient d'un groupe abélien libre, il est isomorphe par le théorème de correspondance à un sous-groupe d'un quotient de $\overline{\mathbf{L}}$ qui est divisible.

4.3.3 Soit $\mathbf{N}$ un sous-groupe divisible d'un groupe $\mathbf{G}$. Considérons un sous-groupe $\mathbf{M}$ maximal parmi ceux vérifiant $\mathbf{N} \cap \mathbf{M} = \{0\}$[1] et supposons que la somme directe $\mathbf{N} \oplus \mathbf{M}$ ne soit pas $\mathbf{G}$. Appelons g un élément de $\mathbf{G} \setminus (\mathbf{N} \oplus \mathbf{M})$. Alors $\langle g\rangle$ rencontre $\mathbf{N} \oplus \mathbf{M}$ ailleurs qu'en 0, sinon $\mathbf{M} + \langle g\rangle$ contredit la maximalité de $\mathbf{M}$. Soit alors p le plus petit entier positif tel que $pg \in \mathbf{N} \oplus \mathbf{M}$ (le nombre p peut être choisi premier, s'il ne l'était pas, il suffirait de remplacer g par $g_1 = \frac{p}{q}g$ où q serait un diviseur premier de p).

1. L'existence de ce sous-groupe est assurée par le théorème de Zorn.

On a donc $pg = n + m$ où $n \in M$ et $m \in \mathbf{M}$. Comme $\mathbf{N}$ est divisible, on peut écrire $n = pn'$ où $n' \in \mathbf{N}$ et si l'on pose $g' = g - n'$, on a $pg' = m$. Mais $g' \notin \mathbf{N} \oplus \mathbf{M}$ (sinon g serait dans cette somme) et donc $\mathbf{N}$ rencontre le groupe engendré par g' et $\mathbf{M}$ en un élément non nul. Il existe $n'' \in \mathbf{N}$ tel que $n'' = kg' + m'$ où k est forcément non nul et plus petit strictement que p, donc est premier avec p. On dispose alors de pg' et kg' qui sont dans $\mathbf{N} \oplus \mathbf{M}$; mais alors une relation de Bezout donne $g' \in \mathbf{N} \oplus \mathbf{M}$, ce qui est absurde.

4.3.4 Soit $\mathbf{G}$ un groupe divisible.

- Si g est un élément d'ordre infini, alors $\mathbf{G}$ contient un sous-groupe isomorphe à $\mathbb{Q}$. En effet, il contient des éléments g_n tels que :

$$g_1 = g,\ 2g_2 = g_1,\ 3g_3 = g_2,\ 4g_4 = g_3 \ldots$$

  et si $\mathbf{H}$ est le sous-groupe engendré par les g_i, on peut montrer, à l'aide de présentations, qu'il est isomorphe à $\mathbb{Q}$. Contentons-nous de vérifier qu'il est sans torsion (sinon g serait d'ordre fini), et qu'il est donc un $\mathbb{Q}$-espace vectoriel, donc somme directe d'exemplaires de $\mathbb{Q}$.

- Si g est un élément d'ordre fini n, on peut, en le divisant par un facteur premier de n, obtenir un élément d'ordre premier p, alors $\mathbf{G}$ contient un sous-groupe isomorphe à $\mathbb{U}_{p^\infty}$. En effet, il contient des éléments g_n tels que :

$$pg_1 = 0,\ pg_2 = g_1,\ pg_3 = g_2 \ldots$$

  et cette fois, on obtient un groupe isomorphe à $\mathbb{U}_{p^\infty}$. On peut alors montrer (en utilisant une récurrence « transfinie ») que $\mathbf{G}$ est somme directe de ces deux types de groupes divisibles.

4.3.5 1) Montrons que tout groupe injectif est divisible. On prend pour morphisme injectif μ la multiplication par n de $\mathbb{Z}$ dans $\mathbb{Z}$, et l'on définit un morphisme f de $\mathbb{Z}$ dans $\mathbf{G}$ en posant $f(1) = g$. Alors ce morphisme se prolonge en un morphisme $\bar{f}$ de sorte que :

$$g = f(1) = \bar{f} \circ \mu(1) = \bar{f}(n) = n\bar{f}(1)$$

et, donc, le groupe est divisible.
Pour la réciproque, identifions $\mathbf{H}$ à un sous-groupe de $\mathbf{K}$ et considérons un prolongement maximal de f à un sous-groupe $\mathbf{S}$ tel que $\mathbf{H} \leqslant \mathbf{S} \leqslant \mathbf{K}$[1]. On note $\bar{f}$ ce prolongement et l'on va montrer que $\mathbf{S} = \mathbf{K}$ par l'absurde. Si $x \in \mathbf{K} \setminus \mathbf{S}$, il y a deux possibilités :

- soit $\mathbf{S} \cap \langle x \rangle = \{0\}$, alors on peut prolonger $\bar{f}$ à $\mathbf{S}' = \mathbf{S} \oplus \langle x \rangle$ en posant $\bar{f}(x) = 0$, et cela contredit la maximalité ;
- sinon, soit k entier positif minimum tel que $kx \in \mathbf{S}$. Comme $\mathbf{G}$ est divisible, l'image $\bar{f}(kx)$ peut être divisée par k, et soit g une solution. Tout élément de $\mathbf{S}'$ s'écrit de façon unique comme somme d'un élément de $\mathbf{S}$ et de ℓx pour $0 \leqslant \ell < k$, et l'on peut prolonger $\bar{f}$ au sous-groupe $\mathbf{S}' = \langle \mathbf{S}, x \rangle$ en posant :

$$\bar{f}(s + \ell x) = \bar{f}(s) + \ell g$$

  ce qui contredit aussi la maximalité.

2) Supposons que $\mathbf{G}$ soit projectif. Alors comme tout groupe commutatif il est quotient d'un groupe libre $\mathbf{L}$, et l'on dispose d'un morphisme p surjectif de $\mathbf{L}$ dans $\mathbf{G}$. Mais en appliquant

1. Existence encore assurée par le théorème de Zorn.

la propriété de projectivité au cas $f = \mathrm{id}_{\mathbf{G}}$, on dispose d'un morphisme $\bar{f}$ tel que $p \circ \bar{f} = \mathrm{id}_{\mathbf{G}}$. On en déduit que p est injectif, et donc que $\mathbf{G}$ est isomorphe à $\mathbf{L}$ et est libre.
La réciproque est plus simple ; avec les notations de l'énoncé, si $\mathbf{G}$ est de base (e_i), on définit $\bar{f}$ en posant $\bar{f}(e_i) = h_i$ où h_i est un antécédent par μ de $f(e_i)$. Cela définit bien un morphisme de $\mathbf{L}$ dans $\mathbf{H}$, par la propriété universelle des groupes libres, et ce morphisme répond bien à la condition imposée.

4.3.6 1) Un élément de $\mathbf{G}$ sera noté (x_p) où l'indice p parcourt l'ensemble $\mathcal{P}$ des nombres premiers et $x_p \in \mathbb{Z}/p$. Il sera d'ordre fini s'il existe n tel que :

$$\forall p \in \mathcal{P},\ nx_p = 0$$

Il est donc nécessaire que si $p \nmid n$, alors $x_p = 0$. Un élément d'ordre fini a ses coordonnées presque toutes nulles, et est donc dans la somme directe $\overline{\mathbf{G}}$. Réciproquement, un tel élément est d'ordre fini, en prenant pour n le produit des p tels que $x_p \neq 0$. On a donc trouvé le sous-groupe de torsion de $\mathbf{G}$.

2) Pour montrer que $\mathbf{G}/\overline{\mathbf{G}}$ est divisible, on doit résoudre $n(x + \overline{\mathbf{G}}) = g + \overline{\mathbf{G}}$ soit $nx - g \in \overline{\mathbf{G}}$. Mais si $p \nmid n$, alors n est inversible modulo p, et l'on peut trouver x_p tel que $nx_p - g_p = 0$, en prenant x_p quelconque pour $p|n$, on obtient $nx - g \in \overline{\mathbf{G}}$.

3) $\overline{\mathbf{G}}$ n'est pas facteur direct dans $\mathbf{G}$, sinon, il aurait un supplémentaire qui serait divisible (car isomorphe à $\mathbf{G}/\overline{\mathbf{G}}$). Mais cela est impossible, si g est un élément non nul de ce groupe, alors il existe p tel que $g_p \neq 0$ et l'équation $px = g$ ne peut avoir de solution.

4.4 PROBLÈMES

4.4.1 Groupes commutatifs définis par générateurs et relations

L'objectif de ce problème est d'étudier les groupes définis de la manière suivante :

$$\mathbf{G} = \langle X \mid S \rangle$$

où X est un ensemble de générateurs, S un ensemble de relations qui contient toutes les relations de la forme $x+y = y+x$ pour x et y distincts dans X. On notera alors la loi additivement, et l'on écrira :

$$\mathbf{G} = \mathrm{grab}\langle X \mid S' \rangle$$

où, dans S', on omet toutes les relations $x + y = y + x$.

1) Premiers exemples

Commençons à étudier des exemples de groupes commutatifs ayant un nombre infini de générateurs, groupes qui se ressemblent beaucoup mais sont différents.

a) Dire pourquoi un tel groupe est commutatif. Pourquoi tout groupe commutatif peut il être décrit ainsi ?

b) Reconnaître

$$\mathbf{G} = \mathrm{grab}\langle a \mid \rangle, \quad \mathbf{L} = \mathrm{grab}\langle a \mid 5a = 0 \rangle, \quad \mathbf{K} = \mathrm{grab}\langle a, b \mid 5a = 0,\ 7b = 0 \rangle$$

c) Des exemples de groupes commutatifs infinis.

- Soit $\mathbf{G}_1$ le groupe abélien engendré par les générateurs $x_0, x_1, \ldots, x_n, \ldots$ et les relations :

$$px_0 = 0,\ p^2x_1 = 0, \ldots,\ p^{n+1}x_n = 0, \ldots$$

- Soit $\mathbf{G}_2$ le groupe abélien engendré par les générateurs $x_0, x_1, \ldots, x_n, \ldots$ et les relations :

$$px_0 = 0,\ px_1 = x_0,\ p^2x_2 = x_0, \ldots,\ p^nx_n = x_0, \ldots$$

- Soit $\mathbf{G}_3$ le groupe abélien engendré par les générateurs $x_0, x_1, \ldots, x_n, \ldots$ et les relations :

$$px_0 = 0,\ px_1 = x_0,\ px_2 = x_1, \ldots,\ px_{n+1} = x_n, \ldots$$

i. On note S_1, S_2, S_3 les groupes engendrés par les relations de $\mathbf{G}_1$, $\mathbf{G}_2$ et $\mathbf{G}_3$. Comparer ces trois sous-groupes au sens de l'inclusion. Qu'en déduit-on pour les groupes $\mathbf{G}_1$, $\mathbf{G}_2$ et $\mathbf{G}_3$?

ii. Reconnaître le groupe $\mathbf{G}_1$.

iii. Reconnaître le groupe $\mathbf{G}_3$.

2) Cas fini

On veut maintenant étudier de façon systématique les groupes abéliens définis par un nombre fini de générateurs et par un nombre fini de relations.

a) Montrer qu'un tel groupe est isomorphe à un quotient de $\mathbb{Z}^n$ par un des ses sous-groupes $\mathbf{H}$.

b) On suppose que $(e_i)_{i=1..n}$ est une base de $\mathbb{Z}^n$ et que $(f_j)_{j=1..r}$ est un système générateur de $\mathbf{H}$; si l'on note $\mathcal{M}$ la matrice à n lignes et p colonnes définie par :

$$\mathcal{M} = (m_{ij}) \text{ avec } f_j = \sum_{i=1}^{n} m_{ij}e_i \text{ pour tout } j$$

on dit que $\mathcal{M}$ est une matrice **adaptée** à $\mathbf{H}$. Si l'on change de base et/ou de système générateur, on obtient une autre matrice adaptée à $\mathbf{H}$.
Montrer que les opérations suivantes transforment une matrice adaptée en une autre matrice adaptée.

- L'échange de deux lignes, de deux colonnes.
- Le remplacement d'une ligne L_i par elle-même additionnée de aL_j, où L_j est une autre ligne et a un entier.
- La même opération sur les colonnes.
- La multiplication d'une ligne (d'une colonne) par -1.

c) Étudier le cas où $\mathbf{H}$ est engendré par un seul élément f_1. On montrera qu'il existe une matrice adaptée de la forme :

$$\mathcal{M} = \begin{pmatrix} d \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

où d est le pgcd des coordonnées de f_1 dans la base initiale. À quel groupe est isomorphe $\mathbb{Z}^n/\mathbf{H}$? Que dire dans le cas où $d = 1$?

d) Montrer que, dans le cas général, il existe une matrice adaptée à $\mathbf{H}$ de la forme :

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \text{ où } D = \begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & & \vdots \\ 0 & \dots & \dots & d_k \end{pmatrix}$$

où $d_1 | d_2 | \dots | d_k$ et où dans la première écriture, 0 représente des matrices nulles. On raisonnera par récurrence sur le nombre de colonnes, et l'on commencera par obtenir une matrice adaptée dont la première colonne est :

$$\mathcal{M} = \begin{pmatrix} m_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

où m_1 est le pgcd des éléments de la première colonne de la matrice initiale, puis une matrice adaptée de la forme :

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & * & * & * \\ \vdots & * & * & * \\ 0 & * & * & * \end{pmatrix}$$

où les * désignent des entiers quelconques.

e) Trouver alors la décomposition du groupe abélien de type fini $\mathbb{Z}^n/\mathbf{H}$.

f) Traiter les exemples suivants :

i. $\mathbf{H}_1$ est le sous-groupe de $\mathbb{Z}^3$ engendré par :

$f_1 = 2e_1 - 2e_2$; $f_2 = 4e_1 + 2e_2 + 6e_3$; $f_3 = 6e_1 + 4e_2 + 12e_3$

ii. $\mathbf{H}_2$ est le sous-groupe de $\mathbb{Z}^3$ engendré par :

$f_1 = 12e_1 + 13e_2 + 6e_3$; $f_2 = 4e_1 + 6e_2 + 2e_3$; $f_3 = 4e_1 + 5e_2 + 2e_3$

g) Montrer que le groupe $\mathbf{G}/\mathbf{H}$ est fini ssi il existe une matrice adaptée qui est carrée et de déterminant non nul.

h) Montrer alors que le cardinal de $\mathbf{G}/\mathbf{H}$ est égal à ce déterminant.

Chapitre 5

Groupe dérivé, groupes nilpotents, groupes résolubles

5.1 CENTRE, GROUPE DÉRIVÉ

Après un chapitre consacré aux groupes commutatifs, revenons à des groupes quelconques ; la loi sera à nouveau notée multiplicativement. Il y a plusieurs façons de mesurer la non-commutativité d'un groupe $\mathbf{G}$. Comme nous l'avons déjà vu dans les premiers chapitres, on peut utiliser le **centre** de $\mathbf{G}$, ensemble des éléments de $\mathbf{G}$ qui commutent à tous les autres. Plus il est grand, plus $\mathbf{G}$ est proche d'un groupe commutatif. Rappelons un résultat important sur le centre, le centre d'un p-groupe n'est jamais trivial, *cf.* 3.1.15.
Il est également possible d'introduire ce qu'on appelle le **groupe dérivé** défini ainsi :
On note $[x, y] = xyx^{-1}y^{-1}$, le **commutateur** de x et y ; il est égal à 1 ssi x et y commutent.
On appelle **groupe dérivé** de $\mathbf{G}$ le groupe engendré par les commutateurs et on le note $\mathbf{G}'$. Plus il est petit, plus $\mathbf{G}$ est proche d'un groupe commutatif.
Revenons pour commencer sur le centre, en complément du premier problème du chapitre 2.

5.1.1 Quotient par le centre

Le centre de $\mathbf{G}$, noté $\mathcal{Z}(\mathbf{G})$ en est un sous-groupe normal. Le quotient $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est réduit à 1 ssi $\mathbf{G}$ est commutatif. D'une certaine façon, dans ce quotient, la commutativité de $\mathbf{G}$ est mise à zéro. Comme le centre est un sous-groupe normal de $\mathbf{G}$, le quotient est un groupe, et il arrive parfois que ce soit un groupe simple. C'est le cas des groupes $\mathbf{PSL}(n, \mathbb{F}_q)$, quotient des $\mathbf{SL}(n, \mathbb{F}_q)$ par leur centre, qui sont simples le plus souvent (*cf.* le problème du dernier chapitre). La dernière question du problème 1.3.1 montre que $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est isomorphe au groupe des automorphismes intérieurs de $\mathbf{G}$, ce qui justifie aussi son intérêt.

Exercice 5.1.1

Quelques questions élémentaires.

1) Montrer que le centre de $\mathbf{G}$ est l'intersection des centralisateurs de tous les éléments de $\mathbf{G}$[1].

2) Montrer que si xy est dans le centre de $\mathbf{G}$, alors x et y commutent.

3) Caractériser le centre du produit direct de groupes.

4) Montrer qu'un sous-groupe d'ordre 2, et normal dans $\mathbf{G}$, est inclus dans le centre.

Exercice 5.1.2

Déterminer $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ lorsque $\mathbf{G}$ est :

- le groupe diédral $\mathbb{D}_{2n}$;
- le groupe symétrique $\mathcal{S}_n$;
- le groupe quaternionique $\mathbb{H}_8$.

Exercice 5.1.3

Démontrer que $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ n'est jamais cyclique (ou monogène), ni réunion croissante de groupes cycliques. En déduire que ni $\mathbb{Q}$ ni un de ses quotients ne peuvent être des $\mathbf{G}/\mathcal{Z}(\mathbf{G})$.

Exercice 5.1.4

Chercher le centre de $\mathbf{TU}(n, \mathbb{K})$, groupe des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. Déterminer le quotient par le centre dans le cas $n = 2$ et $n = 3$.

Enfin un premier essai pour étudier une généralisation du centre, essai qui sera repris à la fin du chapitre.

Exercice 5.1.5

On pose $\mathcal{Z}_1 = \mathcal{Z}(\mathbf{G})$. Montrer qu'on peut définir un sous-groupe $\mathcal{Z}_2$ de $\mathbf{G}$ par :

$$\mathcal{Z}_2/\mathcal{Z}_1 = \mathcal{Z}(\mathbf{G}/\mathcal{Z}_1)$$

et que ce groupe est normal, et même caractéristique dans $\mathbf{G}$. Comment itérer cette construction ? Que donne-t-elle dans le cas d'un groupe diédral ? Vérifier que $\mathcal{Z}_2$ peut être défini par :

$$a \in \mathcal{Z}_2 \iff \forall b \in \mathbf{G},\ [a, b] \in \mathcal{Z}_1$$

SOLUTIONS

5.1.1 1) Si z est dans le centralisateur de x, alors $zx = xz$, et si z est dans tous les centralisateurs, il est dans le centre... Une simple question de quantificateur.

1. Le centralisateur de x est l'ensemble des éléments du groupe qui commutent à x.

2) Si $xy = z$, alors

$$xyx^{-1}y^{-1} = zx^{-1}y^{-1} = x^{-1}zy^{-1} = x^{-1}xyy^{-1} = e$$

et x et y commutent.

3) Si $\mathbf{G} = \mathbf{H} \times \mathbf{K}$, alors

$$(x, y)(x', y') = (x', y')(x, y) \iff xx' = x'x \text{ et } yy' = y'y$$

on en déduit

$$\mathcal{Z}(\mathbf{H} \times \mathbf{K}) = \mathcal{Z}(\mathbf{H}) \times \mathcal{Z}(\mathbf{K})$$

et ce résultat s'étend sans peine à un produit quelconque.

4) Si $\mathbf{H} = \{e, z\}$, alors $\mathbf{H} \lhd \mathbf{G}$ s'écrit :

$$\forall x \in \mathbf{G},\ x\mathbf{H} = \mathbf{H}x \iff xz = zx$$

et donc z est dans le centre de $\mathbf{G}$.

5.1.2 – Le centre du groupe diédral dépend de la parité de n. Écrivons en effet :

$$\mathbb{D}_{2n} = \langle r,\ s \mid r^n = s^2 = 1,\ srs^{-1} = r^{-1} \rangle$$

alors :

$$[r^k s,\ r^{k'} s] = r^{2k-2k'}, \qquad [r,\ r'] = 1, \qquad [r^k s,\ r^{k'}] = r^{-2k'}$$

un élément commute avec tous les autres ssi il est dans $\langle r \rangle$ et est d'ordre 2. Il faut donc que $n = 2m$ et le centre est alors $\mathcal{Z}(\mathbb{D}_{4m}) = \{1, r^m\}$. L'application $r^k b^i \mapsto r^{2k} b^i$ est alors un morphisme de $\mathbb{D}_{4m}$ dans $\langle r^2, b \rangle$, qui est isomorphe au groupe diédral $\mathbb{D}_{2m}$. On en conclut :

$$\mathbb{D}_{4m}/\mathcal{Z}(\mathbb{D}_{4m}) \cong \mathbb{D}_{2m} \qquad \mathbb{D}_{4m+2}/\mathcal{Z}(\mathbb{D}_{4m+2}) = \mathbb{D}_{4m+2}$$

– Comme le centre des groupes symétriques ($n \geqslant 3$) est réduit au neutre,

$$\mathcal{S}_n/\mathcal{Z}(\mathcal{S}_n) = \mathcal{S}_n$$

– Le quotient de $\mathbb{H}_8$ par son centre est isomorphe au groupe de Klein. Nous avons déjà traité le cas plus général des groupes quaternioniques dans l'exercice 2.3.4.

5.1.3 Supposons que $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ soit cyclique, engendré par la classe de x. Alors, tout g de $\mathbf{G}$ peut s'écrire $g = x^k z$ où z est dans le centre. Mais alors $\mathbf{G}$ est commutatif... En effet, avec les notations précédentes,

$$gg' = x^k z x^{k'} z' = x^{k+k'} zz' = g'g$$

et donc le centre de $\mathbf{G}$ est $\mathbf{G}$, et le quotient est trivial. La démonstration est la même dans le cas d'une réunion croissante de groupes cycliques, car deux éléments de $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ sont alors dans un même groupe cyclique, et donc commutent. Comme $\mathbb{Q}$ est la réunion croissante des groupes monogènes $\left\langle \frac{1}{n!} \right\rangle$, il ne peut être un $\mathbf{G}/\mathcal{Z}(\mathbf{G})$. Il en va de même pour ses quotients qui sont, eux-mêmes, réunion croissante de groupes monogènes.

5.1.4 Le plus simple, et le plus fastidieux, est de faire le calcul avec les matrices de transvections. Le centralisateur d'une transvection $T_{ij} = I + E_{ij}$ est formé des matrices dont la ligne j et la colonne i sont nulles (sauf éventuellement sur la diagonale où il y a deux éléments égaux). Comme les transvections de $\mathbf{TU}(n, \mathbb{K})$ correspondent à $1 \leqslant i < j \leqslant n$, on trouve que le centre est formé des matrices de la forme :

$$\begin{pmatrix} 1 & 0 & 0 & \dots & b \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

Le centre est alors isomorphe à $\mathbb{K}$ (groupe additif). Dans le cas $n = 2$, le groupe $\mathbf{TU}(2, \mathbb{K})$ est isomorphe au groupe additif $\mathbb{K}$, commutatif. Si $n = 3$, on peut étudier le quotient par le centre en considérant le morphisme :

$$\phi(M) = (m_{12}, m_{23})$$

On vérifie immédiatement que c'est un morphisme, son noyau est exactement le centre. Donc :

$$\mathbf{TU}(2, \mathbb{K})/\mathcal{Z}(\mathbf{TU}(2, \mathbb{K})) \cong \mathbb{K} \times \mathbb{K}$$

5.1.5 L'existence de $\mathcal{Z}_2$ provient tout simplement du théorème de correspondance. Il est l'image réciproque par le morphisme projection du centre du groupe $\mathbf{G}/\mathcal{Z}_1$. C'est l'image réciproque d'un sous-groupe caractéristique, et c'est donc lui-même un sous-groupe caractéristique de $\mathbf{G}$. On a également :

$$p(\mathcal{Z}_2) = \mathcal{Z}_2/\mathcal{Z}_1 = \mathcal{Z}(\mathbf{G}/\mathcal{Z}_1) \quad \text{et} \quad \mathcal{Z}_1 \lhd \mathcal{Z}_2$$

La première affirmation résulte de ce que $p(p^{-1}(\mathcal{Z}(\mathbf{G}/\mathcal{Z}_1)) = \mathcal{Z}(\mathbf{G}/\mathcal{Z}_1)$ puisque p est un morphisme surjectif. La seconde provient de ce que $\mathcal{Z}_1$ est normal dans $\mathbf{G}$ tout entier.
On peut itérer et obtenir ainsi une suite croissante de sous-groupes. Dans le cas d'un groupe diédral $\mathbb{D}_{2n}$, avec n impair, le centre est réduit au neutre, et donc la suite est stationnaire égal à $\{e\}$. Si $n = 2m$, le centre est $\{e, r^m\}$ et le quotient est isomorphe à $\mathbb{D}_{2m}$. Si donc $m = 2p + 1$, $\mathcal{Z}_2 = \mathcal{Z}_1$ et la suite est stationnaire. Si, au contraire, $m = 2p$, on trouve, en utilisant l'isomorphisme, que $\mathcal{Z}_2 = \{e, r^p, r^{2p}, r^{3p}\}$ et ainsi de suite. La longueur de la suite dépend de l'exposant de 2 dans la décomposition de n.
Enfin, $a \in \mathcal{Z}_2$, pour tout b de $\mathbf{G}$, $ab\mathcal{Z}_1 = ba\mathcal{Z}_1$ qui donne bien $\forall b \in \mathbf{G}$, $[a, b] \in \mathcal{Z}_1$. On peut bien sûr itérer cette caractérisation.

5.1.2 Le groupe dérivé

Commençons par quelques résultats techniques sur les commutateurs.

Exercice 5.1.6

Démontrer que le conjugué d'un commutateur est un commutateur. En déduire que le groupe dérivé de $\mathbf{G}$ est normal dans $\mathbf{G}$. Est-il caractéristique dans $\mathbf{G}$?

Exercice 5.1.7

Démontrer les formules suivantes :

$$[xy,z] = x[y,z]x^{-1}[x,z] \qquad [x,yz] = [x,y]y[x,z]y^{-1}$$

$$[x^{-1},y] = x^{-1}[y,x]x \qquad [x,y^{-1}] = y^{-1}[y,x]y$$

Exercice 5.1.8

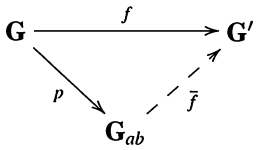
Rechercher, ou retrouver les groupes dérivés des groupes suivants :

- le groupe diédral $\mathbb{D}_{2n}$;
- le groupe symétrique $\mathcal{S}_n$ et le groupe alterné $\mathcal{A}_n$.

Le quotient d'un groupe $\mathbf{G}$ par son sous-groupe dérivé est « grand » quand $\mathbf{G}$ est commutatif, puisqu'alors le sous-groupe dérivé est réduit à l'élément neutre. C'est encore une mesure de la commutativité de $\mathbf{G}$. On l'appelle **abélianisé** de $\mathbf{G}$, et on le note $\mathbf{G}_{ab}$.

Exercice 5.1.9

1) Montrer que $\mathbf{G}_{ab}$ est abélien.
2) Soit $\mathbf{H} \lhd \mathbf{G}$ montrer que $\mathbf{G}/\mathbf{H}$ est commutatif ssi $\mathbf{H}$ contient le groupe dérivé.
3) Démontrer également que si $\mathbf{G}' \leqslant \mathbf{H} \leqslant \mathbf{G}$ alors $\mathbf{H} \lhd \mathbf{G}$.
4) Démontrer enfin que tout morphisme f de $\mathbf{G}$ dans un groupe commutatif $\mathbf{G}'$ se factorise par l'abélianisé suivant le diagramme :



où $\overline{f}$ est un morphisme unique tel que $\overline{f} \circ p = f$

Il est un cas où on détermine facilement l'abélianisé d'un groupe, c'est quand ce groupe est donné par une présentation.

Exercice 5.1.10

1) Montrer que l'abélianisé d'un groupe $\mathbf{G}$ donné par une présentation s'obtient en ajoutant aux relations initiales toutes les relations $x_i x_j = x_j x_i$ où x_i et x_j sont des générateurs de $\mathbf{G}$.
2) Utiliser ce résultat pour déterminer l'abélianisé des groupes suivants :

$$\mathbb{D}_{2n},\ \mathbf{G} = \langle a,b,c \mid a^2 = b^3 = c^5 = abc \rangle$$

ce dernier groupe est connu sous le non de **groupe binaire icosaédral**. Voir les problèmes, section 6.2.

3) Le **groupe des tresses** $\mathbb{B}_n$ est le groupe engendré par des éléments $x_1, x_2, \ldots, x_n$ qui commutent pour $|i-j|>1$, et vérifient les relations :

$$x_{i+1}x_ix_{i+1} = x_ix_{i+1}x_i$$

Nous avons déjà rencontré $\mathbb{B}_3$ dans l'exercice 2.2.16. Déterminer son abélianisé.

Il ne faut pas confondre le groupe dérivé qui est le groupe engendré par les commutateurs, et l'ensemble des commutateurs. Autrement dit, il peut exister des éléments du groupe dérivé qui ne sont pas des commutateurs. Mais il n'est pas facile de donner un exemple simple de cette situation. En voici un.

Exercice 5.1.11

Soit **G** l'ensemble des matrices de la forme :

$$A = \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix}$$

où f, g et h sont des polynômes à coefficients réels.

1) Montrer que **G** est un groupe pour le produit matriciel.

2) Déterminer les commutateurs des éléments de **G**.

3) Démontrer que le groupe dérivé de **G** est l'ensemble des matrices de la forme :

$$B = \begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

4) Démontrer que la matrice C définie par :

$$B = \begin{pmatrix} 1 & 0 & x^2+xy+y^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

n'est pas un commutateur.

Regardons maintenant une généralisation du groupe dérivé. Si **H** et **K** sont des sous-groupes de **G**, on note $[\mathbf{H},\mathbf{K}]$ le groupe engendré par les commutateurs $[h,k]$ où $h \in \mathbf{H}$ et $k \in \mathbf{K}$.

Exercice 5.1.12

Montrer que $[\mathbf{H},\mathbf{K}] = [\mathbf{K},\mathbf{H}]$ et que $[\mathbf{H},\mathbf{K}]$ est normal dans $\langle \mathbf{H},\mathbf{K}\rangle$. Si de plus **H** et **K** sont normaux dans **G**, $[\mathbf{H},\mathbf{K}]$ est-il normal dans **G** ?

Exercice 5.1.13

Soit $\mathbb{D}_\infty$ le groupe diédral infini, de présentation

$$\mathbb{D}_\infty = \langle a, b \mid b^2 = 1,\ bab^{-1} = a^{-1}\rangle$$

1) Chercher le centre, le sous-groupe dérivé, l'abélianisé.

2) Soit $\mathbf{H} = \langle b \rangle$ et $\mathbf{K} = \langle ab \rangle$. Quel est l'ordre de ces deux groupes ? Montrer que, néanmoins, $[\mathbf{H}, \mathbf{K}]$ est infini.

Exercice 5.1.14

1) Montrer que si $\mathbf{H} \lhd \mathbf{G}$ et $\mathbf{K} \lhd \mathbf{G}$, alors $[\mathbf{H}, \mathbf{K}] \leqslant \mathbf{H} \cap \mathbf{K}$. Quel résultat retrouve-t-on si, de plus, $\mathbf{H} \cap \mathbf{K} = \{e\}$?

2) De la même façon, montrer que :

$$\mathbf{H} \lhd \mathbf{G} \iff [\mathbf{H}, \mathbf{G}] \leqslant \mathbf{H}$$

3) Si les sous-groupes $\mathbf{K}$, $\mathbf{H}$ vérifient $\mathbf{K} \leqslant \mathbf{H} \leqslant \mathbf{G}$ et $\mathbf{K} \lhd \mathbf{G}$. Montrer que :

$$\mathbf{H}/\mathbf{K} \leqslant \mathcal{Z}(\mathbf{G}/\mathbf{K}) \iff [\mathbf{H}, \mathbf{G}] \leqslant \mathbf{K}$$

4) Avec trois sous-groupes maintenant, $\mathbf{F}$, $\mathbf{K}$ et $\mathbf{H}$ que l'on suppose normaux dans $\mathbf{G}$, montrer que :

$$[\mathbf{FK}, \mathbf{H}] = [\mathbf{F}, \mathbf{H}][\mathbf{K}, \mathbf{H}]$$

Un groupe est **parfait** s'il est égal a son groupe dérivé. Nous avons déjà vu que c'était le cas des groupes alternés (pour $n \geqslant 5$). Les groupes simples non commutatifs sont parfaits, et il existe des groupes parfaits non simples, mais ils sont relativement rares. C'est le cas du groupe binaire icosaédral rencontré dans l'exercice 5.1.10.

Exercice 5.1.15

Montrer que tout sous-groupe parfait d'un groupe $\mathbf{G}$ est inclus dans le groupe dérivé $\mathbf{G}'$.

Donnons une importante propriété des groupes parfaits, connue sous le nom de **lemme de Grün**.

Exercice 5.1.16

1) Soit $\mathbf{G}$ un groupe, $\mathcal{Z}_1$ son centre et $\mathcal{Z}_2$ le groupe défini par :

$$\mathcal{Z}_2/\mathcal{Z}_1 = \mathcal{Z}(\mathbf{G}/\mathcal{Z}_1)$$

(cf. l'exercice 5.1.5). Montrer que si $z \in \mathcal{Z}_2$, alors

$$\begin{array}{rccc} \phi_z : & \mathbf{G} & \to & \mathbf{G} \\ & x & \mapsto & [x, z] \end{array}$$

est un morphisme.

2) Vérifier que :

$$\mathbf{G}' \leqslant \operatorname{Ker} \phi_z \text{ et } \operatorname{Im} \phi_z \leqslant \mathcal{Z}_1$$

3) En déduire que si $\mathbf{G}$ est parfait, alors $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ a un centre trivial.

Pour terminer, un exercice qui relie la taille du groupe dérivé à celle du centre.

Exercice 5.1.17

Dans cet exercice, on suppose que $\mathcal{Z}(\mathbf{G})$ est d'indice n.

1) Montrer que le nombre des commutateurs est inférieur à n^2. On utilisera les classes de $\mathbf{G}$ modulo le centre.

2) Montrer que, pour tous x, y de $\mathbf{G}$, $[x, y]^n$ est dans le centre de $\mathbf{G}$. En déduire la relation :
$$[x, y]^{n+1} = [x, y^2][yxy^{-1}, y]^{n-1}$$

3) En déduire qu'un élément de $\mathbf{G}'$ est produit d'au plus n^3 commutateurs, $\mathbf{G}'$ est fini, donner un majorant de son cardinal.

SOLUTIONS

5.1.6 $x[a,b]x^{-1} = xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1} = [xax^{-1}, xbx^{-1}]$

et donc le conjugué d'un commutateur est encore un commutateur. Plus généralement, comme vu dans le problème 1.3.1, l'image d'un commutateur par un morphisme est un commutateur. On en déduit que le groupe dérivé est normal dans $\mathbf{G}$, caractéristique dans $\mathbf{G}$, et même pleinement invariant dans $\mathbf{G}$. [1]

5.1.7 Il s'agit de simples vérifications :
$$x[y,z]x^{-1}[x,z] = xyzy^{-1}z^{-1}x^{-1}xzx^{-1}z^{-1} = xyzy^{-1}x^{-1}z^{-1} = [xy,z]$$
$$[x,y]y[x,z]y^{-1} = xyx^{-1}y^{-1}yxzx^{-1}z^{-1}y^{-1} = [x,yz]$$
$$[x,y^{-1}] = xy^{-1}x^{-1}y = y^{-1}yxy^{-1}x^{-1}y = y^{-1}[y,x]y$$
$$[x^{-1},y] = x^{-1}yxy^{-1} = x^{-1}[y,x]x$$

5.1.8 – Le calcul fait dans l'exercice 5.1.7 montre que tout commutateur dans le groupe diédral est le carré d'une rotation. Le sous-groupe dérivé est donc le groupe engendré par les carrés. Si n est impair, c'est $\langle r\rangle \cong \mathbb{Z}/n$, si $n = 2m$, c'est $\langle r^2\rangle \cong \mathbb{Z}/m$.

– Un commutateur est forcément une permutation paire, car produit de quatre permutations. Le groupe dérivé est donc inclus dans le groupe alterné. Montrons que tout 3-cycle est un commutateur. En effet, le carré d'un 3-cycle est encore un 3-cycle. Or, tous les 3-cycles sont conjugués. On en déduit qu'il existe ρ telle que :
$$\sigma^2 = \rho\sigma\rho^{-1}$$
qui peut s'écrire :
$$\sigma = \sigma^{-1}\rho\sigma\rho^{-1} = [\sigma^{-1}, \rho]$$
Comme de plus (3.2.8), on peut prendre ρ dans le groupe alterné, on vient de démontrer que
$$\mathcal{S}_n' = \mathcal{A}_n \quad \text{et} \quad \mathcal{A}_n' = \mathcal{A}_n$$
au moins pour $n \geqslant 5$ dans le dernier cas. Une autre méthode consiste bien sûr à utiliser la

1. Voir le problème 1.3.1.

simplicité du groupe alterné et sa non-commutativité ; le groupe dérivé étant normal, il ne peut que coïncider avec $\mathcal{A}_n$. Enfin, pour être complet, regardons les cas $n = 3$ et $n = 4$:

$$\mathcal{A}_3' = \{e\} \quad \text{et} \quad \mathcal{A}_4' = \mathcal{V}$$

ce dernier groupe est le groupe des doubles transpositions.

5.1.9 1) $\mathbf{G}_{ab}$ est abélien car $xy\mathbf{G}' = yx\mathbf{G}' \iff x^{-1}y^{-1}xy \in \mathbf{G}'$ ce qui est bien vrai.

2) Supposons $\mathbf{G}/\mathbf{H}$ commutatif. Alors la projection $p : \mathbf{G} \to \mathbf{G}/\mathbf{H}$ envoie $\mathbf{G}'$ sur l'élément neutre puisque le groupe d'arrivée est commutatif. Donc $\mathbf{G}' \leqslant \mathbf{H}$. Réciproquement, tout commutateur du quotient est l'image d'un commutateur :

$$x\mathbf{H}y\mathbf{H}x^{-1}\mathbf{H}y^{-1}\mathbf{H} = xyx^{-1}y^{-1}\mathbf{H}$$

et donc le quotient est commutatif dès que $\mathbf{H}$ contient tous les commutateurs.

3) Si $\mathbf{G}' \leqslant \mathbf{H} \leqslant \mathbf{G}$, $\mathbf{H}$ est l'image réciproque par p d'un sous-groupe forcément normal du groupe commutatif $\mathbf{G}/\mathbf{G}'$, donc il est normal dans $\mathbf{G}$.

4) Cette factorisation est tout simplement une application du théorème général de factorisation (1.2.14). En effet, si f est un morphisme de $\mathbf{G}$ dans un groupe commutatif :

$$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = 1$$

puisque le groupe d'arrivée est commutatif. Le noyau de f contient donc le groupe dérivé.

5.1.10 1) Notons C l'ensemble des relations $x_ix_j = x_jx_i$ et $\mathbf{H}$ le sous-groupe normal engendré par ces relations. Le théorème de Von Dyck nous assure que si $\mathbf{G} = \langle X \mid R\rangle$, alors

$$\langle X \mid R,\ C\rangle \cong \mathbf{G}/\mathbf{H}$$

Il suffit de montrer que $\mathbf{H}$ est bien le sous-groupe dérivé $\mathbf{G}'$. Le sous-groupe normal engendré par les commutateurs des générateurs est inclus dans le groupe dérivé. Mais les formules de l'exercice 5.1.7 prouvent que ce groupe contient tous les commutateurs d'éléments de $\mathbf{G}$: il est donc égal au groupe dérivé.

2) De la présentation du groupe diédral, on déduit :

$$\begin{aligned}(\mathbb{D}_{2n})_{ab} &= \langle r, s \mid r^n = s^2 = 1,\ srs^{-1} = r^{-1},\ rs = sr\rangle \\ &= \langle r, s \mid r^n = s^2 = 1,\ rss^{-1} = r^{-1},\ rs = sr\rangle \\ &= \langle r, s \mid r^n = r^2 = 1,\ s^2 = 1,\ rs = sr\rangle\end{aligned}$$

Il y a donc deux cas :

- si n est pair, il s'agit du produit direct $\mathbb{Z}/2 \times \mathbb{Z}/2$;
- si n est impair, $r = 1$ et l'abélianisé est $\mathbb{Z}/2$.

Pour le second groupe, on obtient :

$$a^2 = b^3 = c^5 = abc,\ ab = ba,\ ac = ca,\ bc = ac \Rightarrow a = bc,\ b^3 = abc = b^2c^2$$
$$\Rightarrow b = c^2 \Rightarrow b^3 = c^6 = c^5$$

et donc $c = 1 = a = b$. L'abélianisé est trivial, donc $\mathbf{G} = \mathbf{G}'$[1].

1. Ce groupe, à 120 éléments, est le groupe « binaire icosaédral ».

3) Si l'on ajoute les relations $x_i x_{i+1} = x_{i+1} x_i$, on obtient $x_i = x_{i+1}$ et l'abélianisé de groupe des tresses $\mathbb{B}_n$ est donc $\mathbb{Z}$.

5.1.11 1) Le produit de deux éléments de **G** est donné par :

$$\begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f'(x) & h'(x,y) \\ 0 & 1 & g'(y) \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & f(x)+f'(x) & h(x,y)+h'(x,y)+f(x)g'(y) \\ 0 & 1 & g(y)+g'(y) \\ 0 & 0 & 1 \end{pmatrix}$$

Il en résulte que **G** est un groupe. L'inverse d'une matrice est donné par :

$$\begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -f(x) & f(x)g(y)-h(x,y) \\ 0 & 1 & -g(y) \\ 0 & 0 & 1 \end{pmatrix}$$

2) Le commutateur de deux matrices est de la forme :

$$\begin{pmatrix} 1 & 0 & f(x)g'(y)-f'(x)g(y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

3) En choisissant bien les matrices, par exemple avec $f'(x) = 0$, on voit que le groupe dérivé contient toutes les matrices dont l'élément en haut à droite est de la forme $x^k y^l$. Par ailleurs :

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ce qui prouve que le groupe dérivé est formé des matrices de la forme

$$\begin{pmatrix} 1 & 0 & h(x,y) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et qu'il est isomorphe à $\mathbb{R}[x, y]$ muni de l'addition.

4) Il suffit donc de montrer que le polynôme $x^2 + xy + y^2$ ne peut se mettre sous la forme :

$$x^2 + xy + y^2 = p(x)q(y) + r(x)s(y)$$

La démonstration utilise de l'algèbre linéaire. Si l'on pose $q(y) = \sum_i a_i y^i$ et $s(y) = \sum_i b_i y^i$, alors l'identification des coefficients de y dans les deux membres donne :

$$x^2 = a_0 p(x) + b_0 q(x)$$
$$x = a_1 p(x) + b_1 q(x)$$
$$1 = a_2 p(x) + b_2 q(x)$$

et dans l'espace vectoriel $\mathbb{R}[x]$, les polynômes indépendants 1, x et x^2 seraient combinaisons linéaires de deux polynômes $p(x)$ et $q(x)$.

5.1.12 $[\mathbf{H},\mathbf{K}]$ est engendré par les commutateurs de la forme $[h,k] = hkh^{-1}k^{-1}$. Mais $[h,k]^{-1} = [k,h]$ et donc $[\mathbf{H},\mathbf{K}] = [\mathbf{K},\mathbf{H}]$.
Utilisant une des formules de l'exercice 5.1.7, on peut écrire :

$$h[h',k]h^{-1} = [hh',k][h,k]^{-1}$$

où h et h' sont dans $\mathbf{H}$ et k dans $\mathbf{K}$. Ce conjugué d'un élément de $[\mathbf{H},\mathbf{K}]$ est donc dans $[\mathbf{H},\mathbf{K}]$. De même, le conjugué par un élément de $\mathbf{K}$, et donc par un élément de $\langle \mathbf{H},\mathbf{K}\rangle$. On a bien :

$$[\mathbf{H},\mathbf{K}] \lhd \langle \mathbf{H},\mathbf{K}\rangle$$

En général, le groupe $[\mathbf{H},\mathbf{K}]$ n'est pas normal dans $\mathbf{G}$, mais :

$$g[h,k]g^{-1} = [ghg^{-1}, gkg^{-1}]$$

prouve que le groupe est normal dans $\mathbf{G}$ si $\mathbf{H}$ et $\mathbf{K}$ sont normaux dans $\mathbf{G}$.

> ***Remarque :*** Ici comme dans d'autres exercices, nous raisonnons seulement sur des **générateurs** du groupe des commutateurs. Il faut se convaincre que cela suffit.

5.1.13 1) Les calculs de conjugués faits dans l'exercice 5.1.2 pour le groupe diédral restent valables dans ce cas et prouvent que le centre est réduit à e. Comme tout commutateur est une puissance paire de a, le groupe dérivé est $\mathbb{D}'_\infty = \langle a^2\rangle \cong \mathbb{Z}$. De plus,

$$\begin{aligned}(\mathbb{D}_\infty)_{ab} &= \langle a,b \mid b^2 = 1,\ bab^{-1} = a^{-1},\ ab = ba\rangle \\ &= \langle a,b \mid b^2 = 1,\ a^2 = 1,\ ab = ba\rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2\end{aligned}$$

2) b et ab sont d'ordre 2, comme donc $\mathbf{H}$ et $\mathbf{K}$. En revanche, $[ab,b] = a^2$ et $[\mathbf{H},\mathbf{K}] = \mathbb{D}'_\infty$, donc d'ordre infini.

5.1.14 1) $[h,k] = (hkh^{-1})k^{-1} \in \mathbf{K}$

$$= h(kh^{-1}k^{-1}) \in \mathbf{H}$$

(avec des notations évidentes). Donc $[\mathbf{H},\mathbf{K}] \leqslant \mathbf{H} \cap \mathbf{K}$. Si cette intersection est réduite au neutre, on voit que tout élément de $\mathbf{H}$ commute à tout élément de $\mathbf{K}$, fait déjà observé dans les exercices concernant le produit direct, voir 1.1.23, par exemple.

2) C'est le même calcul :

$$[h,g] \in \mathbf{H} \iff ghg^{-1} \in \mathbf{H}$$

et comme cela doit être vrai pour tous les éléments, cela équivaut à $\mathbf{H} \lhd \mathbf{G}$.

3) Par le théorème de correspondance, on sait que $\mathbf{H}/\mathbf{K}$ est un sous-groupe de $\mathbf{G}/\mathbf{K}$. Il sera inclus dans le centre ssi :

$$hg\mathbf{K} = gh\mathbf{K} \iff [h,g] \in \mathbf{K}$$

ce qui donne bien $[\mathbf{H},\mathbf{G}] \leqslant \mathbf{K}$.

4) L'exercice 5.1.7 donne :

$$[fk,h] = f[k,h]f^{-1}[f,h]$$

et comme les sous-groupes sont normaux dans $\mathbf{G}$, les groupes de commutateurs le sont aussi, on en déduit :

$$[\mathbf{FK},\mathbf{H}] \subset [\mathbf{K},\mathbf{H}][\mathbf{F},\mathbf{H}] = [\mathbf{F},\mathbf{H}][\mathbf{K},\mathbf{H}]$$

L'autre inclusion se déduit immédiatement du fait que $\mathbf{K}$ et $\mathbf{F}$ sont des sous-groupes de $\mathbf{FK}$.

5.1.15 Si $\mathbf{H} = \mathbf{H}'$, cela signifie que tout élément de $\mathbf{H}$ est un produit de commutateurs faits à partir d'éléments de $\mathbf{H}$, et c'est donc en particulier un élément du groupe dérivé $\mathbf{G}'$.

5.1.16 1) On va encore utiliser une des formules de l'exercice 5.1.7 :

$$\phi_z(xy) = [z, xy] = [z, x]x[z, y]x^{-1}$$

Mais on sait que $z \in \mathcal{Z}_2$, et par définition de $\mathcal{Z}_2$:

$$zy\mathcal{Z}_1 = yz\mathcal{Z}_1 \iff [z, y] \in \mathcal{Z}_1$$

et $[z, y]$ commute avec x, donc

$$\phi(xy) = \phi(x)\phi(y)$$

On peut aussi utiliser la troisième question de l'exercice 5.1.14 ou l'exercice 5.1.5.

2) Nous venons de voir que tout les éléments de la forme $[z, y]$ sont dans le centre, on a bien $\mathrm{Im}(\phi_z) \leqslant \mathcal{Z}_1$. En appliquant le premier théorème d'isomorphisme, le quotient $\mathbf{G}/\mathrm{Ker}(\phi_z)$ est donc commutatif, ce qui implique que $\mathbf{G}' \subset \mathrm{Ker}(\phi_z)$.

3) Si $\mathbf{G} = \mathbf{G}'$, alors pour tout z de $\mathcal{Z}_2$, $\mathrm{Ker}(\phi_z) = \mathbf{G}$, donc $[z, x] = e$ pour tout x, ce qui implique $z \in \mathcal{Z}_1$. On en déduit que $\mathcal{Z}_2/\mathcal{Z}_1$ est trivial, ce qui signifie que le centre de $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est trivial.

5.1.17 1) Si le centre est d'indice n, $\mathbf{G}$ est la réunion de n classes à gauche de la forme $x_i\mathcal{Z}(\mathbf{G})$, et un commutateur quelconque $[a, b]$ peut s'écrire $[x_iz, x_jz']$ où z et z' sont dans le centre ; mais alors ce commutateur est égal à $[x_i, x_j]$ et il y a moins de n^2 commutateurs distincts.

2) Puisque $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est d'ordre n, le théorème de Lagrange permet de dire que la classe de $[x, y]$ est d'ordre n, c'est-à-dire que $[x, y]^n \in \mathcal{Z}$. En utilisant ce résultat, on obtient :

$$\begin{aligned}
[x, y]^{n+1} &= xyx^{-1}[x, y]^n y^{-1} \\
&= xyx^{-1}xyx^{-1}y^{-1}[x, y]^{n-1}y^{-1} \\
&= [x, y^2]y[x, y]^{n-1}y^{-1} \\
&= [x, y^2][yxy^{-1}, y]^{n-1}
\end{aligned}$$

3) Un élément x du groupe dérivé est produit de commutateurs choisis parmi les (au plus) n^2. Supposons que ce produit contienne k commutateurs. Si un des commutateurs c apparaît plus de n fois dans cette écriture, on peut, par conjugaison, écrire x sous la forme $x = c^{n+1}c_1c_2 \ldots c_\ell$ où les c_1 c_2 sont des conjugués de commutateurs et sont donc des commutateurs. Mais la relation précédente prouve alors qu'on peut écrire x comme produit de $k - 1$ commutateurs. Ainsi, x s'écrit comme produit d'au plus n^3 commutateurs. Comme il y a au plus n^2 commutateurs, le groupe dérivé $\mathbf{G}'$ a au plus $(n^2)^{n^3}$ éléments. On peut améliorer sérieusement ce majorant...

5.2 RÉSOLUTION DE GROUPES

Comme tout nombre entier se décompose en facteurs premiers, on peut essayer de décomposer en éléments « simples ». Nous avons vu un premier exemple de cette décomposition dans le cas des groupes commutatifs finis, ou de type fini. Nous allons essayer

de généraliser, mais nous n'obtiendrons pas dans cette première approche des résultats aussi définitifs. L'idée est de poursuivre ce qui a été fait dans le paragraphe sur les suites exactes.

Commençons par définir une **suite de composition** d'un groupe $\mathbf{G}$; c'est une suite finie $(\mathbf{H}_i)_{i=0..n}$, de sous-groupes de $\mathbf{G}$ telle que :

i) $\mathbf{H}_0 = \{e\}$ $\mathbf{H}_n = \mathbf{G}$

ii) $\mathbf{H}_i \lhd \mathbf{H}_{i+1}$ pour tout i de 0 à $n-1$

Les quotients sont souvent appelés **facteurs** de la suite de composition. Si, de plus, la condition suivante est satisfaite :

iii) $\mathbf{H}_{i+1}/\mathbf{H}_i$ est un groupe simple non trivial pour tout i de 0 à $n-1$

alors on parle de **suite de Jordan-Hölder**. Commençons par quelques exemples faciles.

Exercice 5.2.1

1) Quelles sont les suites de composition, de Jordan-Hölder, des groupes simples ?
2) Décrire les suites de composition, de Jordan-Hölder, des groupes cycliques $\mathbb{Z}/n$.
3) Trouver les suites de composition, de Jordan-Hölder, des groupes $\mathbb{D}_{2n}$, $\mathbb{H}_8$ et $\mathcal{V} = \mathbb{Z}/2 \times \mathbb{Z}/2$.
4) Étudier le cas de $\mathbb{Z}$ et des groupes commutatifs infinis.

Exercice 5.2.2

Quelles sont les suites de Jordan-Hölder de $\mathbb{S}_n$?

Exercice 5.2.3

Donner un exemple de groupe infini admettant une suite de Jordan-Hölder.

Les sous-groupes qui interviennent dans une suite de composition sont normaux les uns dans les autres, mais pas forcément normaux dans $\mathbf{G}$; ce sont des sous-groupes sous-normaux, pour reprendre la terminologie de l'exercice 3.2.20.

Exercice 5.2.4

Si tous les sous-groupes $(\mathbf{H}_i)$ d'une suite de composition sont normaux dans $\mathbf{G}$, ils définissent une suite de composition **normale**. Donner un exemple de suite de composition qui n'est pas normale.

Nous allons maintenant montrer que les suites de Jordan-Hölder sont, dans une certaine mesure, toutes les mêmes. Une définition pour commencer.

On appelle **raffinement** d'une suite de composition $(\mathbf{H}_i)$, une suite $(\mathbf{K}_i)$ dont la suite $(\mathbf{H}_i)$ est une sous-suite. Commençons par un lemme technique.

Exercice 5.2.5 (Lemme de Zassenhaus)

Soient deux paires de sous-groupes de $\mathbf{G}$, $\mathbf{H}_1 \lhd \mathbf{H}_2$ et $\mathbf{K}_1 \lhd \mathbf{K}_2$. Démontrer que :

$$\mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_1) \lhd \mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_2) \quad \text{et} \quad \mathbf{K}_1(\mathbf{K}_2 \cap \mathbf{H}_1) \lhd \mathbf{K}_1(\mathbf{K}_2 \cap \mathbf{H}_2)$$

et que les groupes quotients sont isomorphes. On montrera que chacun de ces quotients est isomorphe au groupe

$$(\mathbf{H}_2 \cap \mathbf{K}_2)/(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{K}_1)$$

Il pourra aussi être utile de dessiner l'organisation des groupes qui interviennent dans la démonstration... Et l'on comprendra pourquoi ce lemme s'appelle aussi le **lemme du papillon**.

Encore une définition. Deux suites de compositions sont dites **équivalentes** si elles ont même longueur et des facteurs isomorphes deux à deux, sans tenir compte de l'ordre dans lequel ils apparaissent.

Exercice 5.2.6

1) Démontrer que deux suites de composition ont des raffinements équivalents. Ce résultat constitue le théorème de Schreier, et l'on pourra utiliser le lemme du papillon pour le démontrer.

2) En déduire que si un groupe admet une suite de Jordan-Hölder, alors toutes les suites de composition ont un raffinement qui est une suite de Jordan-Hölder, et toutes les suites de Jordan-Hölder sont équivalentes. Ce résultat constitue le **théorème de Jordan-Hölder**.

SOLUTIONS

5.2.1 1) La seule suite de composition sans répétition d'un groupe simple $\mathbf{G}$ est « triviale » $\{e\} \leqslant \mathbf{G}$, car le premier groupe $\mathbf{H}_{n-1}$ doit être normal dans $\mathbf{G}$. Elle peut être plus longue si l'on autorise les répétitions. C'est bien sûr une suite de Jordan-Hölder.

2) Les sous-groupes d'un groupe cyclique $\mathbb{Z}/n$ sont cycliques d'ordre d, où $d|n$. Et le quotient est isomorphe à $\mathbb{Z}/\frac{n}{d}$. Il sera simple ssi $\frac{n}{d}$ est premier. Une suite de composition est donc déterminée par une suite d'entiers $(d_i)_{i=0..k}$, tels que

$$1 = d_0|d_1| \ldots |d_{k-1}|d_k = n$$

et une suite de Jordan-Hölder est une suite de composition pour laquelle tous les quotients $\frac{d_{i+1}}{d_i}$ sont premiers.

3) $e \leqslant \langle r \rangle \leqslant \mathbb{D}_{2n}$

où $r^n = e$, est une suite de composition du groupe diédral. Le premier facteur est isomorphe à $\mathbb{Z}/2$; comme $\langle r \rangle$ est un groupe cyclique, on obtient des suites de composition (et de Jordan-Hölder) à l'aide de la question précédente.

Les sous-groupes du groupe quaternionique $\mathbb{H}_8$ sont tous normaux. En écrivant

$$\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

une suite de composition est :

$$1 \leqslant \langle -1 \rangle \leqslant \langle i \rangle \leqslant \mathbb{H}_8$$

Remarquons que les facteurs sont tous isomorphes à $\mathbb{Z}/2$, c'est une suite de Jordan-Hölder. On obtient d'autres suites avec j et k.
Il y a trois éléments d'ordre 2 dans $\mathcal{V}$. Il y a donc trois suites de Jordan-Hölder différentes, dont les facteurs sont isomorphes à $\mathbb{Z}/2$; c'est donc différent de $\mathbb{Z}/4$ qui n'a qu'une suite de Jordan-hölder, avec les mêmes facteurs.

4) $\mathbb{Z}$ n'a pas de suite de Jordan-Hölder. Rappelons en effet que tout groupe commutatif simple est isomorphe à $\mathbb{Z}/p$ où p est premier (1.2.5). On en déduit que tout groupe commutatif admettant une suite de Jordan-Hölder est fini, car chaque facteur de la décomposition est fini. $\mathbb{Z}$ a, en revanche, des suites de composition aussi longues qu'on veut :

$$0 \leqslant 8\mathbb{Z} \leqslant 4\mathbb{Z} \leqslant 2\mathbb{Z} \leqslant \mathbb{Z}$$

5.2.2 Commençons par le plus simple. Si $n \geqslant 5$, $\mathcal{S}_n$ a un seul sous-groupe normal non trivial, son sous-groupe alterné, et ce sous-groupe est simple. Il y a donc une seule suite de Jordan-Hölder (et une seule suite de composition non triviale) :

$$\{e\} \leqslant \mathcal{A}_n \leqslant \mathcal{S}_n$$

On obtient d'ailleurs le même résultat pour $n = 3$. Dans le cas $n = 4$, on obtient :

$$\{e\} \leqslant \langle u \rangle \leqslant \mathcal{V} \leqslant \mathcal{A}_4 \leqslant \mathcal{S}_4$$

où u est une double transposition et $\mathcal{V}$ le groupe de Klein des doubles transpositions. On obtient d'autre suites en changeant de double transposition.

5.2.3 Un premier exemple peut être donné par le groupe $\mathcal{S}_{\mathbb{N}}$ qui généralise l'exemple précédent. Il a un sous-groupe simple d'indice 2, le groupe alterné $\mathcal{A}_{\mathbb{N}}$, voir le problème 1.3.2.

5.2.4 La suite de Jordan-Hölder du groupe $\mathcal{S}_4$ présentée ci-dessus est un exemple. Le groupe $\langle u \rangle$ n'est pas normal dans $\mathcal{S}_4$, car il ne contient pas tous les éléments d'une classe de conjugaison.

5.2.5 Commençons par observer qu'on a les inclusions suivantes :

$$\mathbf{H}_1 \cap \mathbf{K}_1 \leqslant \mathbf{H}_1 \cap \mathbf{K}_2 \leqslant \mathbf{H}_1 \leqslant \mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_1) \lhd \mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_2) \leqslant \mathbf{H}_2$$

Ces inclusions sont claires, et les ensembles indiqués sont bien des sous-groupes, à cause de la normalité de $\mathbf{H}_1$ dans $\mathbf{H}_2$. La normalité sera prouvée plus loin.
Montrons également que

$$(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{K}_1) \lhd \mathbf{H}_2 \cap \mathbf{K}_2$$

D'abord

$$\mathbf{H}_1 \lhd \mathbf{H}_2 \Rightarrow \mathbf{H}_1 \cap \mathbf{K}_2 \lhd \mathbf{H}_2 \cap \mathbf{K}_2$$

car $g(\mathbf{H}_1 \cap \mathbf{K}_2)g^{-1}$ est inclus dans $\mathbf{H}_1$ si g est dans $\mathbf{H}_2$ (normalité) et dans $\mathbf{K}_2$ si g est dans $\mathbf{K}_2$. De même, en échangeant les rôles. Enfin, si deux sous-groupes sont normaux dans un groupe, leur produit est aussi normal dans le groupe[1], d'où :

$$(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{H}_1) \lhd \mathbf{H}_2 \cap \mathbf{K}_2$$

1. $a\mathbf{H}\mathbf{K}a^{-1} = a\mathbf{H}a^{-1}a\mathbf{K}a^{-1} = \mathbf{H}\mathbf{K}$.

On peut maintenant prouver les isomorphismes demandés à l'aide du premier théorème d'isomorphisme, soit $x \in \mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_2)$. Alors $x = hg$ où $h \in \mathbf{H}_1$ et $g \in \mathbf{H}_2 \cap \mathbf{K}_2$. On définit un morphisme ϕ de $\mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_2)$ dans $\mathbf{H}_2 \cap \mathbf{K}_2/(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{K}_1)$ par

$$\phi(x) = g(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{H}_1)$$

Cette application est bien définie :

$$x = hg = h'g' \Rightarrow g'g^{-1} = h'^{-1}h \in (\mathbf{H}_2 \cap \mathbf{K}_2) \cap \mathbf{H}_1 = \mathbf{H}_1 \cap \mathbf{K}_2 \subset (\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{H}_1)$$

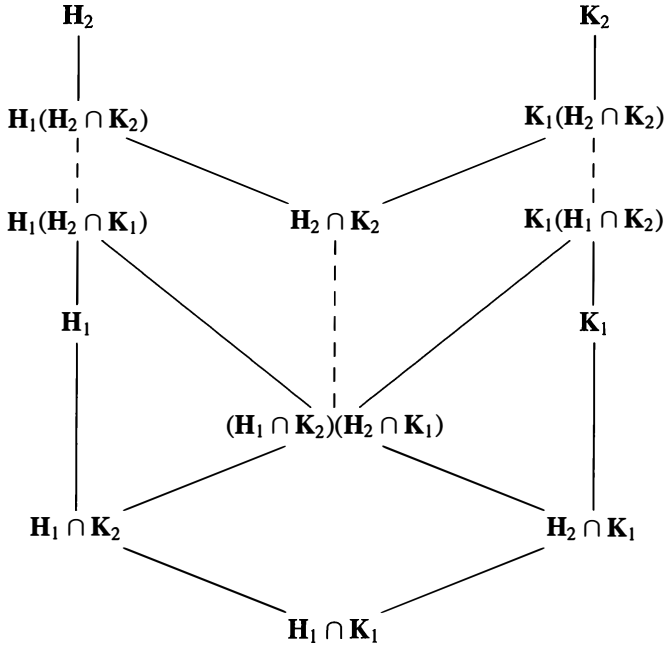
et $\phi(x)$ ne dépend pas de la décomposition de x. Par ailleurs ϕ est bien un morphisme, par définition de la loi dans le quotient, surjectif, car g peut parcourir $\mathbf{H}_2 \cap \mathbf{K}_2$. Cherchons enfin le noyau :

$$x = hg \in \operatorname{Ker}\phi \iff g = uv \text{ où } u \in \mathbf{H}_1 \cap \mathbf{K}_2 \text{ et } v \in \mathbf{H}_2 \in \mathbf{K}_1$$

On a donc $x = (hu)v \in \mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_1)$ et le premier théorème d'isomorphisme donne :

$$\mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_2)/\mathbf{H}_1(\mathbf{H}_2 \cap \mathbf{K}_1) \cong (\mathbf{H}_2 \cap \mathbf{K}_2)/(\mathbf{H}_1 \cap \mathbf{K}_2)(\mathbf{H}_2 \cap \mathbf{K}_1)$$

En échangeant les rôles, on obtient l'autre isomorphisme demandé. Pour mieux suivre la démonstration, contempler le « papillon » dessiné par les sous-groupes :



5.2.6 1) Supposons que $\mathbf{G}$ ait deux suites de compositions $(\mathbf{H}_i)$ de longueur n et $(\mathbf{K}_j)$ de longueur m. Alors le lemme précédent permet d'insérer entre $\mathbf{H}_i$ et $\mathbf{H}_{i+1}$ les groupes $\mathbf{H}_i(\mathbf{H}_{i+1} \cap \mathbf{K}_j)$ et $\mathbf{H}_i(\mathbf{H}_{i+1} \cap \mathbf{K}_{j+1})$ le premier étant normal dans le suivant. On obtient une suite de mn termes dont la suite initiale est une sous-suite. Mais si l'on fait la même opération avec la suite $(\mathbf{K}_j)$, on obtient une suite de même longueur et les isomorphismes issus du lemme de Zassenhaus prouvent que nos deux suites sont équivalentes. Bien sûr, si on « simplifie » ces suites de composition en ôtant les groupes superflus (égaux au suivant), on aura en général un raffinement de longueur inférieure à mn.

2) Entre deux termes consécutifs d'une suite de Jordan-Hölder, on ne peut insérer aucun sous-groupe (normal dans le plus grand), car le quotient est simple. Si donc on applique le théorème précédent à deux suites de Jordan-Hölder, on obtient des raffinements équivalents mais qui contiennent, une fois enlevées les répétitions, les mêmes sous-groupes que les suites initiales. Les deux suites sont donc équivalentes. Les facteurs d'une suite de Jordan-Hölder sont donc indépendants de la suite et ne dépendent que du groupe.

5.3 GROUPES NILPOTENTS, GROUPES RÉSOLUBLES

Parmi les groupes admettant une suite de composition, il en est qui ont une propriété supplémentaire ; nous commencerons par le cas des groupes **nilpotents**, bien que leur définition paraisse, de prime abord, peu naturelle.

On dit qu'un groupe est nilpotent s'il admet une suite de composition

$$\{e\} = \mathbf{H}_0 \lhd \mathbf{H}_1 \lhd \mathbf{H}_2 \lhd \ldots \lhd \mathbf{H}_n = \mathbf{G}$$

telle que :

$$\mathbf{H}_{i+1}/\mathbf{H}_i \leqslant \mathcal{Z}\left(\mathbf{G}/\mathbf{H}_i\right)$$

pour tout i de 0 à $n-1$. Une telle suite s'appelle **suite centrale**.

Exercice 5.3.1

Montrer que les groupes commutatifs et les p-groupes finis sont nilpotents.

Exercice 5.3.2

On note $(\mathcal{Z}_i)$ la suite des sous-groupes d'un groupe $\mathbf{G}$ définis par :

$$\mathcal{Z}_0 = \{e\}, \qquad \mathcal{Z}_{i+1}/\mathcal{Z}_i = \mathcal{Z}\left(\mathbf{G}/\mathcal{Z}_i\right)$$

Montrer que cette suite est croissante et que $\mathbf{G}$ est nilpotent ssi il existe n tel que $\mathcal{Z}_n = \mathbf{G}$.

Exercice 5.3.3

On note $(\Gamma^{(i)})$ la suite des groupes définie par :

$$\Gamma^{(0)} = \mathbf{G}, \qquad \Gamma^{i+1} = [\Gamma^i, \mathbf{G}]$$

Montrer que cette suite est décroissante et que $\mathbf{G}$ est nilpotent ssi il existe n tel que $\Gamma^{(n)} = \{e\}$. On pourra utiliser l'exercice 5.1.14.

Exercice 5.3.4

Montrer que tout sous-groupe d'un groupe nilpotent est nilpotent. Vérifier que tout quotient d'un groupe nilpotent l'est aussi, ainsi que tout produit direct de deux groupes nilpotents.

Exercice 5.3.5

Montrer que le groupe $\mathbf{TU}(n, \mathbb{K})$ des matrices triangulaires unipotentes est nilpotent. On pourra introduire des sous-ensembles de matrices dont les « surdiagonales » (en un sens à préciser...) sont nulles.

Une propriété importante des groupes nilpotents est qu'ils n'ont pas de sous-groupe propre autonormalisant.

Exercice 5.3.6

Montrer que si $\mathbf{G}$ est nilpotent, et si $\mathbf{H} < \mathbf{G}$, alors $\mathbf{H} < \mathcal{N}_{\mathbf{G}}(\mathbf{H})$[1]. On pourra introduire le plus grand k tel que $\mathcal{Z}_k \leqslant \mathbf{H}$.

En utilisant l'exercice précédent, nous allons maintenant caractériser les groupes nilpotents finis par leurs p-Sylow. On retrouve ainsi encore une propriété des groupes commutatifs.

Exercice 5.3.7

Montrer qu'un sous-groupe fini $\mathbf{G}$ est nilpotent si et seulement si il satisfait l'une des conditions suivantes :

- Tout p-Sylow de $\mathbf{G}$ est normal dans $\mathbf{G}$.
- $\mathbf{G}$ est le produit direct de ses p-Sylow.
- Tout sous-groupe maximal dans $\mathbf{G}$ est normal dans $\mathbf{G}$.

Voici maintenant une catégorie de groupes très renommée, celle des groupes **résolubles**. Sans que nous puissions le montrer dans le cadre de cet ouvrage, disons que ces groupes sont liés à la question de la résolubilité d'une équation algébrique « par radicaux » ; voir tout ouvrage traitant de la théorie de Galois.
On dit qu'un groupe $\mathbf{G}$ est **résoluble** s'il admet une suite de composition à facteurs commutatifs. La notion de groupe résoluble est encore une de celles qui généralisent la notion de groupe commutatif, car, bien sûr, tout groupe commutatif est résoluble.

Exercice 5.3.8

1) Montrer qu'un groupe simple non commutatif n'est pas résoluble.
2) Montrer qu'un groupe nilpotent est résoluble.
3) Examiner la résolubilité des groupes $\mathcal{S}_n$ et donner un exemple de groupe résoluble non nilpotent.

Comme pour les groupes nilpotents, il existe une suite de composition particulière qui permet de tester la résolubilité d'un groupe.

1. En utilisant le symbole $<$, on veut signaler que c'est un sous-groupe strict.

Exercice 5.3.9

On note $(\mathbf{G}^{(i)})$ la suite des groupes définie par :

$$\mathbf{G}^{(0)} = \mathbf{G}, \qquad \mathbf{G}^{i+1} = (\mathbf{G}^{i})'$$

C'est donc la suite des groupes dérivés successifs du groupe $\mathbf{G}$. On l'appelle **suite dérivée** du groupe $\mathbf{G}$. Montrer que cette suite est décroissante et que $\mathbf{G}$ est résoluble ssi il existe n tel que $\mathbf{G}^{(n)} = \{e\}$.

Démontrons des propriétés générales qui montrent que la propriété de résolubilité est très partagée ; on peut voir, par ailleurs, qu'il n'y a qu'un seul groupe non résoluble de cardinal inférieur à 100, que tout groupe d'ordre impair est résoluble... Mais ce dernier résultat est l'aboutissemement d'une très longue démonstration (Feit et Thompson).

Exercice 5.3.10

Montrer que si $\mathbf{G}$ est résoluble et si $\mathbf{H}$ est un sous-groupe de $\mathbf{G}$, alors $\mathbf{H}$ est résoluble. Si $\mathbf{H}$ est normal dans $\mathbf{G}$ résoluble, montrer que $\mathbf{G}/\mathbf{H}$ est aussi résoluble.

Exercice 5.3.11

Montrer que si l'on a une suite exacte :

$$0 \longrightarrow \mathbf{N} \xrightarrow{a} \mathbf{G} \xrightarrow{b} \mathbf{H} \longrightarrow 0$$

où $\mathbf{N}$ et $\mathbf{H}$ sont résolubles, alors $\mathbf{G}$ est aussi résoluble. En déduire que le produit direct ou un produit semi-direct de groupes résolubles est résoluble. A-t-on la même propriété pour les groupes nilpotents ?

Parmi les groupes linéaires, en voici deux qui sont résolubles.

Exercice 5.3.12

1) Vérifier que $\mathbf{GL}(2, \mathbb{F}_2)$ est résoluble.

2) Montrer également que $\mathbf{GL}(2, \mathbb{F}_3)$ est résoluble. On pourra construire une suite de composition.

Regardons encore un exemple de suite de composition particulière. On dit qu'un groupe est **polycyclique** s'il admet une suite de composition dont tous les facteurs sont cycliques.

Exercice 5.3.13

1) Donner des exemples de groupes polycycliques, et montrer que pour un groupe fini, polycyclique et résoluble sont synonymes.

2) Montrer qu'un sous-groupe d'un groupe polycyclique est polycyclique, qu'un quotient de groupes polycycliques est polycyclique.

3) Montrer que, dans une suite de composition d'un groupe polycyclique, le nombre des facteurs monogènes infinis est constant.

4) Montrer que si $\mathbf{G}$ est un groupe polycyclique qui admet une suite de composition cyclique de longueur n, alors il est engendré par n éléments.

Les groupes polycycliques sont très étudiés et utilisés car on peut standardiser leur présentation. Il est également possible pour ces groupes de généraliser les théorèmes de Sylow ; si $\mathbf{G}$ est un groupe résoluble fini de cardinal $n = kk'$ avec k et k' premiers entre eux, alors il existe au moins un sous-groupe de $\mathbf{G}$ d'ordre k. De tels sous-groupes s'appellent des **sous-groupes de Hall** et jouissent de propriétés analogues aux sous-groupes de Sylow.

SOLUTIONS

5.3.1 En ce qui concerne les groupes commutatifs, il n'y a rien à faire. La suite de composition $\{e\} \leqslant \mathbf{G}$ convient. Pour un p-groupe $\mathbf{G}$, on utilise le fait que le centre est non trivial, voir 3.1.15, et l'on raisonne par récurrence sur l'ordre du groupe. On a donc :

$$\{e\} \leqslant \mathcal{Z}(\mathbf{G}) \leqslant \mathbf{G}$$

et le rapport $\mathcal{Z}(\mathbf{G})/\{e\}$ est bien dans le centre de $\mathbf{G}/\{e\}$. Par ailleurs, $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est un p-groupe d'ordre strictement plus petit que l'ordre de $\mathbf{G}$. On peut lui appliquer l'hypothèse de récurrence. On dispose donc d'une suite centrale pour le groupe $\mathbf{G}/\mathcal{Z}(\mathbf{G})$. Cette suite se relève en une suite entre $\mathcal{Z}(\mathbf{G})$ et $\mathbf{G}$, et par le troisième théorème d'isomorphisme, ce relèvement est encore central.

5.3.2 Cette suite est croissante car, par le théorème de correspondance, le centre de $\mathbf{G}/\mathcal{Z}_i$ peut se mettre sous la forme $\mathcal{Z}_{i+1}/\mathcal{Z}_i$ où $\mathcal{Z}_{i+1}$ vérifie $\mathcal{Z}_i \leqslant \mathcal{Z}_{i+1} \leqslant \mathbf{G}$. Remarquons bien sûr que $\mathcal{Z}_1$ est le centre de $\mathbf{G}$. S'il existe n tel que $\mathcal{Z}_n = \mathbf{G}$, alors

$$\{e\} \leqslant \mathcal{Z}_1 \leqslant \ldots \leqslant \mathcal{Z}_n = \mathbf{G}$$

est une suite centrale et $\mathbf{G}$ est nilpotent. La définition d'une suite centrale est vérifiée avec = à la place de $\leqslant$. Réciproquement, supposons $\mathbf{G}$ nilpotent, soit $(\mathbf{H}_i)$ une suite centrale. Montrons que $\mathbf{H}_i \leqslant \mathcal{Z}_i$. C'est vrai pour $i = 0$ et même pour $i = 1$ puisque la suite est centrale :

$$\mathbf{H}_1 = \mathbf{H}_1/\{e\} \leqslant \mathcal{Z}(\mathbf{G}/\{e\}) = \mathcal{Z}(\mathbf{G}) = \mathcal{Z}_1$$

Raisonnons ensuite par récurrence. Si l'on suppose $\mathbf{H}_i \leqslant \mathcal{Z}_i$, soit $x \in \mathbf{H}_{i+1}$, alors $x\mathbf{H}_i$ commute avec tous les $g\mathbf{H}_i$, soit $[x, g] \in \mathbf{H}_i$, mais alors $[x, g] \in \mathcal{Z}_i$, ce qui prouve que $x \in \mathcal{Z}_{i+1}$, et l'on a bien $\mathbf{H}_{i+1} \leqslant \mathcal{Z}_{i+1}$. On peut maintenant achever le raisonnement. Si la suite $(\mathbf{H}_i)$ est centrale, il existe n tel que $\mathbf{H}_n = \mathbf{G}$ et alors $\mathcal{Z}_n = \mathbf{G}$.

5.3.3 Montrons que cette suite est bien une suite décroissante formée de sous-groupes normaux dans $\mathbf{G}$. À l'étape 1, $\Gamma_1 = [\mathbf{G}, \mathbf{G}]$ est le groupe dérivé $\mathbf{G}'$, dont on sait qu'il est normal dans $\mathbf{G}$. Supposons $\Gamma_i \lhd \mathbf{G}$. Alors $\Gamma_{i+1} = [\Gamma_i, \mathbf{G}] \leqslant \Gamma_i$ d'après l'exercice 5.1.14. De plus, $\Gamma_{i+1} \lhd \mathbf{G}$ cette fois d'après l'exercice 5.1.12.

Si la suite obtenue s'arrête à l'élément neutre $\{e\}$, elle constitue une suite de composition. Mais on a :

$$\Gamma_i/\Gamma_{i+1} \leqslant \mathcal{Z}(\mathbf{G}/\Gamma_{i+1})$$

En effet, l'exercice 5.1.14 prouve que cela équivaut à $[\Gamma_i, \mathbf{G}] \leqslant \Gamma_{i+1}$ ce qui est vrai. Il s'agit bien d'une suite centrale, et le groupe $\mathbf{G}$ est nilpotent. Réciproquement, donnons-nous une série centrale que nous numérotons en décroissant pour faciliter la comparaison :

$$\{e\} = \mathbf{H}_n \leqslant \mathbf{H}_{n-1} \leqslant \ldots \leqslant \mathbf{H}_0 = \mathbf{G}$$

Montrons qu'alors $\Gamma_i \leqslant \mathbf{H}_i$. C'est vrai pour 0 et faisons l'hypothèse que $\Gamma_i \leqslant \mathbf{H}_i$. Comme la suite $(\mathbf{H}_i)$ est centrale, $\mathbf{H}_i/\mathbf{H}_{i+1} \leqslant \mathcal{Z}(\mathbf{G}/\mathbf{H}_{i+1})$ ce qui équivaut à $[\mathbf{H}_i, \mathbf{G}] \leqslant \mathbf{H}_{i+1}$. On a donc :

$$\Gamma_{i+1} = [\Gamma_i, \mathbf{G}] \leqslant [\mathbf{H}_i, \mathbf{G}] \leqslant \mathbf{H}_{i+1}$$

On en déduit que la suite (Γ_i) s'achève en $\{e\}$. De façon intuitive, la suite (Γ_i) est la suite centrale qui décroît le plus rapidement, tandis que la suite $(\mathcal{Z}_i)$ est la suite centrale qui croît le plus rapidement.

5.3.4 Soit $\mathbf{H} \leqslant \mathbf{G}$. Alors $\Gamma_1(\mathbf{H}) = [\mathbf{H}, \mathbf{H}] \leqslant \Gamma_1(\mathbf{G})$, et, par récurrence, on a aussi

$$\Gamma_i(\mathbf{H}) = [\Gamma_{i-1}(\mathbf{H}), \mathbf{H}] \leqslant [\Gamma_{i-1}(\mathbf{G}), \mathbf{G}]$$

Si donc la suite des $\Gamma_i(\mathbf{G})$ stationne en e, il en va de même pour la suite des $\Gamma_i(\mathbf{H})$.
Supposons maintenant $\mathbf{H}$ normal dans $\mathbf{G}$, et soit $(\mathbf{G}_i)$ une suite décroissante centrale. La suite image par la projection de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$ est $(\mathbf{G}_i\mathbf{H}/\mathbf{H})$. Mais on a

$$[\mathbf{G}_i\mathbf{H}/\mathbf{H}, \mathbf{G}/\mathbf{H}] = [\mathbf{G}_i, \mathbf{G}]\mathbf{H}/\mathbf{H} \leqslant \mathbf{G}_{i-1}\mathbf{H}/\mathbf{H}$$

car un commutateur $[x\mathbf{H}, y\mathbf{H}]$ peut s'écrire $[x, y]\mathbf{H}$. D'après l'exercice 5.1.14, la suite obtenue est donc centrale, et le groupe quotient est nilpotent.
Soient $\mathbf{G}$ et $\mathbf{K}$ deux groupes nilpotents, de suites centrales respectives $(\mathbf{G}_i)$ et $(\mathbf{K}_j)$. En insérant éventuellement des répétitions dans la suite la plus courte (ce qui ne change pas le fait d'être centrale), on dispose de deux suites de même longueur, et $(\mathbf{G}_i \times \mathbf{K}_i)$ est une suite de composition de $\mathbf{G} \times \mathbf{K}$ (*cf.* 2.1.10). De plus,

$$[\mathbf{G}_i \times \mathbf{K}_i, \mathbf{G} \times \mathbf{K}] = [\mathbf{G}_i, \mathbf{G}] \times [\mathbf{K}_i, \mathbf{K}] \leqslant \mathbf{G}_{i-1} \times \mathbf{K}_{i-1}$$

ce qui assure qu'il s'agit d'une suite centrale.

5.3.5 On va construire une suite de composition pour $\mathbf{TU}(n, \mathbb{K})$. Soit en effet $\mathbf{TU}^m(n, \mathbb{K})$ le sous-groupe de $\mathbf{TU}(n, \mathbb{K})$ formé des matrices dont les éléments vérifient :

$$a_{i,j} = 0 \text{ pour tous les couples } i, j \text{ tels que } 0 < j - i < m$$

les éléments diagonaux restant égaux à 1. On montre par récurrence que chacun de ces groupes est normal dans le précédent en considérant le morphisme :

$$\begin{array}{ccc} \mathbf{TU}^m(n, \mathbb{K}) & \to & \mathbb{K} \oplus \mathbb{K} \oplus \ldots \oplus \mathbb{K} \\ M & \mapsto & (m_{1,m+1}, m_{2,m+2}, \ldots, m_{n-m,n}) \end{array}$$

On vérifie en effet aisément que c'est un morphisme, dont le noyau est $\mathbf{TU}^{m+1}(n, \mathbb{K})$. Il en résulte une suite de composition

$$\mathbf{TU}(n, \mathbb{K}) = \mathbf{TU}^1(n, \mathbb{K}) \geqslant \mathbf{TU}^2(n, \mathbb{K}) \geqslant \ldots \geqslant \mathbf{TU}^n(n, \mathbb{K}) = \{e\}$$

Pour montrer que cette suite est centrale, il faut faire quelques calculs... Utilisons les matrices de transvection :

$$T_{ij}(\alpha) = I + \alpha E_{ij}$$

où α est un élément du corps, et E_{ij} la matrice nulle sauf l'élément e_{ij} qui vaut 1. On vérifie alors que $E_{ij}E_{jk} = E_{ik}$, le produit étant nul dans tous les autres cas. On en déduit :

$$[T_{ij}(\alpha), T_{jk}(\beta)] = T_{ik}(\alpha\beta), \qquad [T_{ij}(\alpha), T_{ki}(\beta)] = T_{kj}(-\alpha\beta)]$$

le commutant est l'identité dans tous les autres cas. Comme le groupe $\mathbf{TU}^m(n, \mathbb{K})$ est engendré par les transvections $T_{ij}(\alpha)$ pour lesquels $j - i > m$, le calcul précédent montre que :

$$[\mathbf{TU}^m(n, \mathbb{K}), \mathbf{TU}(n, \mathbb{K})] \leqslant \mathbf{TU}^{m+1}(n, \mathbb{K})$$

ce qui prouve que la suite est centrale.

5.3.6 L'existence d'un tel k est assuré par la nilpotence du groupe. Soit donc $x \in \mathcal{Z}_{k+1} \setminus \mathbf{H}$, qui existe par définition de k. Montrons que x normalise $\mathbf{H}$, soit $h \in \mathbf{H}$, alors, par définition de $\mathcal{Z}_{k+1}$, on a :

$$xh\mathcal{Z}_k = hx\mathcal{Z}_k \iff xhx^{-1}h^{-1} \in \mathcal{Z}_k \leqslant \mathbf{H}$$

d'où $xhx^{-1} \in \mathbf{H}$.

5.3.7 Soit $\mathbf{G}$ fini. On supposera que $\mathbf{G}$ n'est pas un p-groupe, cas où on sait déjà que $\mathbf{G}$ est nilpotent et où les assertions qui suivent sont sans grand intérêt.

1) On suppose $\mathbf{G}$ nilpotent et l'on applique l'exercice précédent. Si $\mathbf{S}$ est un p-Sylow, alors c'est un sous-groupe strict de son normalisateur $\mathcal{N}_{\mathbf{G}}(\mathbf{S})$. Mais le normalisateur d'un p-Sylow est autonormalisant (3.2.13). On en déduit que notre normalisateur coïncide avec $\mathbf{G}$ et donc que le p-Sylow $\mathbf{S}$ est normal dans $\mathbf{G}$.

2) On peut alors montrer que $\mathbf{G}$ est produit direct de ses p-Sylow, c'est le même résultat que dans le cas commutatif, dans l'exercice 4.1.3. Il suffit de voir que le produit des p-Sylow est direct. En effet, le produit de deux p-Sylow est direct puisqu'ils sont normaux dans $\mathbf{G}$ et que leur intersection est réduite au neutre (Lagrange) ; ce produit est encore normal dans $\mathbf{G}$, on achève par récurrence, et le produit de tous les p-Sylow est bien $\mathbf{G}$ tout entier, puisque ces deux groupes ont le même cardinal.

3) Si $\mathbf{G}$ est produit direct de ses p-Sylow, alors il est nilpotent. En effet, le produit direct de groupes nilpotents est nilpotent, et les p-Sylow sont nilpotents en tant que p-groupes.
Supposons maintenant que tout sous-groupe maximal d'un groupe fini $\mathbf{G}$ soit normal, et soit $\mathbf{S}$ un p-Sylow. Alors son normalisateur $\mathcal{N}_{\mathbf{G}}(\mathbf{S})$ n'est pas strictement inclus dans $\mathbf{G}$, sinon il serait inclus dans un sous-groupe maximal $\mathbf{H}$, normal dans $\mathbf{G}$. Or, tout sous-groupe contenant le normalisateur est auto-normalisant (3.2.13), donc ne peut être normal dans $\mathbf{G}$. Il y a une contradiction, donc le normalisateur d'un p-Sylow est égal à $\mathbf{G}$, tout p-Sylow est normal et $\mathbf{G}$ est nilpotent. La réciproque est immédiate, toujours en appliquant l'exercice précédent.
Il existe d'autres caractérisations des groupes nilpotents finis. Par exemple, on peut montrer que ce sont les groupes dont tout sous-groupe est sous-normal.

5.3.8 1) C'est immédiat, car un groupe simple non commutatif $\mathbf{G}$ n'a qu'une suite de composition, $e \leqslant \mathbf{G}$ dont le facteur $\mathbf{G}$ n'est pas commutatif.

2) Une suite centrale a pour facteur des sous-groupes inclus dans un centre, et qui sont donc commutatifs.

3) Pour $n = 2$, S_2 est commutatif. Pour $n = 3$, la suite $e \leqslant \langle\sigma\rangle \leqslant \mathcal{S}_3$ où σ est une permutation circulaire, a des quotients commutatifs $\mathbb{Z}/2$ et $\mathbb{Z}/3$. Pour $n = 4$, la suite $e \leqslant \mathcal{V} \leqslant \mathcal{A}_4 \leqslant \mathcal{S}_4$ a pour quotients $\mathcal{V}$, $\mathbb{Z}/3$, $\mathbb{Z}/2$ et $\mathcal{S}_4$ est résoluble. En revanche, à partir de $n = 5$, la seule suite de composition est : $e \leqslant \mathcal{A}_n \leqslant \mathcal{S}_n$ et le groupe symétrique $\mathcal{S}_n$ n'est pas résoluble car $\mathcal{A}_n$ est simple non commutatif. Enfin, l'exemple de $\mathcal{S}_3$ est l'exemple le plus simple de groupe résoluble qui n'est pas nilpotent.

5.3.9 La suite dérivée est par définition décroissante, chaque groupe dérivé est caractéristique dans le suivant et donc normal dans $\mathbf{G}$, et le quotient d'un groupe par son groupe dérivé est commutatif, c'est l'abélianisé de $\mathbf{G}$. Si donc la suite dérivée aboutit à $\{e\}$, le groupe $\mathbf{G}$ est résoluble.
Réciproquement, supposons $\mathbf{G}$ résoluble et soit

$$\mathbf{H}_0 = \{e\} \leqslant \mathbf{H}_1 \leqslant \dots \mathbf{H}_n = \mathbf{G}$$

dont les facteurs sont abéliens. Alors

$$\mathbf{G}/\mathbf{H}_{n-1} \text{ abélien } \Rightarrow \mathbf{G}' \leqslant \mathbf{H}_{n-1}$$

comme vu dans l'exercice 5.1.9, et de même, par récurrence pour tous les groupes suivants. Si donc $\mathbf{G}$ est résoluble, la suite dérivée stationne en $\{e\}$.

5.3.10 Si $\mathbf{K}$ est un sous-groupe de $\mathbf{G}$ et si $(\mathbf{H}_i)$ est une suite de composition cyclique, alors $(\mathbf{H}_i \cap \mathbf{K})$ est une suite de composition de $\mathbf{K}$ décroissante ; le fait que $\mathbf{H}_i \cap \mathbf{K} \lhd \mathbf{H}_{i+1} \cap \mathbf{K}$ résulte du second théorème d'isomorphisme, on peut écrire en effet :

$$\mathbf{H}_i \lhd \mathbf{H}_{i+1} \Rightarrow \mathbf{H}_i \cap \mathbf{K} = \mathbf{H}_i \cap (\mathbf{H}_{i+1} \cap \mathbf{K}) \lhd \mathbf{H}_{i+1} \cap \mathbf{K}$$

de plus

$$(\mathbf{H}_{i+1} \cap \mathbf{K})/(\mathbf{H}_i \cap \mathbf{K}) \cong \mathbf{H}_i(\mathbf{H}_{i+1} \cap \mathbf{K})/\mathbf{H}_i \leqslant \mathbf{H}_{i+1}/\mathbf{H}_i$$

et le sous-groupe d'un groupe commutatif est commutatif : $\mathbf{H}$ est résoluble.
Considérons maintenant un quotient d'un groupe résoluble par un sous-groupe normal $\mathbf{G}/\mathbf{K}$. Alors l'image par projection d'une suite de composition cyclique est une suite de composition. La projection est surjective, ce qui assure la normalité (cette suite est $(\mathbf{H}_i\mathbf{K}/\mathbf{K})$)). Le troisième théorème d'isomorphisme donne ensuite :

$$(\mathbf{H}_{i+1}\mathbf{K}/\mathbf{K})/(\mathbf{H}_i\mathbf{K}/\mathbf{K}) \cong \mathbf{H}_{i+1}\mathbf{K}/\mathbf{H}_i\mathbf{K}$$

Poursuivons.

$$\mathbf{H}_{i+1}\mathbf{K}/\mathbf{H}_i\mathbf{K} \cong \mathbf{H}_i/(\mathbf{H}_{i+1}\mathbf{K}) \cap \mathbf{H}_i$$

par le second théorème d'isomorphisme ; mais $(\mathbf{H}_{i+1}\mathbf{K}) \cap \mathbf{H}_i = \mathbf{H}_{i+1}(\mathbf{K} \cap \mathbf{H}_i)$ puisque $\mathbf{H}_{i+1} \leqslant \mathbf{H}_i$. Ainsi, notre quotient est isomorphe à $\mathbf{H}_i/\mathbf{H}_{i+1}(\mathbf{K} \cap \mathbf{H}_i)$ qui est un quotient de $\mathbf{H}_i/\mathbf{H}_{i+1}$, et est donc commutatif.

5.3.11 On dispose d'une suite de composition à facteurs commutatifs pour $\mathbf{N}$, notée $(\mathbf{N}_i)$, et d'une suite de composition à facteurs commutatifs de $\mathbf{G}/\mathbf{N}$, puisque ce groupe est isomorphe à $\mathbf{H}$. Mais d'après le théorème de correspondance, cette suite provient d'une suite $(\mathbf{G}_i)$ de sous-groupes telle que :

$$\mathbf{N} = \mathbf{G}_n \leqslant \mathbf{G}_{n-1} \leqslant \dots \leqslant \mathbf{G}_n = \mathbf{G}$$

De plus, si $(\mathbf{G}_{i+1}/\mathbf{N})/(\mathbf{G}_i/\mathbf{N})$ est commutatif, il en va de même pour $\mathbf{G}_{i+1}/\mathbf{G}_i$ d'après le troisième théorème d'isomorphisme. La réunion des deux suites $(\mathbf{N}_i)$ et $(\mathbf{G}_i)$ donne une suite de composition à facteurs commutatifs pour $\mathbf{G}$.
On peut conclure de ce raisonnement qu'une extension de groupes résolubles est un groupe résoluble : un produit direct, un produit semi-direct de groupes résolubles, est résoluble.
Il n'en va pas de même pour les groupes nilpotents (à part le cas du produit direct), et le groupe résoluble $\mathcal{S}_3$ sert encore de contre-exemple. Bien qu'extension de deux groupes commutatifs, donc nilpotents, ($\mathbb{Z}/3$ et $\mathbb{Z}/2$), il n'est pas nilpotent.

5.3.12 1) En ce qui concerne $\mathbf{GL}(2,\mathbb{F}_2)$, c'est vite réglé car ce groupe est isomorphe à $\mathcal{S}_3$ qui est résoluble, *cf.* 5.3.8.

2) Reprenons des arguments utilisés dans le problème 3.5.1 du chapitre 3. Le groupe linéaire $\mathbf{GL}(2,\mathbb{F}_3)$ agit sur l'ensemble des quatre droites du plan $\mathbb{F}_3^2$; le noyau de cette action est le centre qui a deux éléments $\pm id$. On en déduit une action fidèle de $\mathbf{GL}(2,\mathbb{F}_3)/\{\pm id\}$ qui a 24 éléments sur l'ensemble des quatre droites. En définitive, ce quotient est isomorphe à $\mathcal{S}_4$ et notre groupe est résoluble en tant qu'extension de deux groupes résolubles.

5.3.13 1) Les groupes finis commutatifs ont des suites de composition avec des facteurs cycliques, voir les décompositions du chapitre 4. Mais, plus généralement, tout groupe fini résoluble est polycyclique. À partir d'une suite de composition commutative, on peut construire une suite de Jordan-Hölder par raffinement ; mais cette suite aura des facteurs qui sont des quotients des facteurs initiaux commutatifs, et qui sont simples. Ce sont donc des groupes cycliques d'ordre premier.

2) Il suffit de reprendre mot pour mot les démonstrations faites pour les groupes résolubles, en changeant « commutatif » en « cyclique ».

3) On considère une suite de composition cyclique d'un groupe $\mathbf{G}$ qui admet k facteurs monogènes infinis. Alors tout raffinement admet encore k facteurs monogènes infinis. En effet, si $\mathbf{H} \lhd \mathbf{K}$, avec $\mathbf{K}/\mathbf{H}$ isomorphe à $\mathbb{Z}$. Alors un raffinement non trivial $\mathbf{H} \lhd \mathbf{N} \lhd \mathbf{K}$ contient deux facteurs $\mathbf{K}/\mathbf{N}$, isomorphe à un sous-groupe de $\mathbb{Z}$ donc monogène infini, et $\mathbf{N}/\mathbf{H}$ isomorphe à un quotient de $\mathbb{Z}$, donc cyclique. On a conservé le nombre des facteurs monogènes infinis. Si maintenant on considère deux suites de compositions cycliques, elles ont des raffinements équivalents, et, donc, même nombre de facteurs monogènes infinis.

4) Examinons le cas où la suite est de longueur deux :

$$\{e\} \longrightarrow \mathbf{H} \longrightarrow \mathbf{G}$$

avec donc $\mathbf{H}$ cyclique et $\mathbf{G}/\mathbf{H}$ cyclique. Si un générateur de $\mathbf{H}$ est x et un générateur de $\mathbf{G}/\mathbf{H}$ est $y\mathbf{H}$, tout élément de $\mathbf{G}$ est dans une classe $y^k\mathbf{H}$ et peut donc s'écrire $y^k x^\ell$, le groupe est engendré par deux éléments. Cette analyse s'étend rapidement au cas d'une suite de composition cyclique de longueur n.
On déduit de ce résultat qu'il existe des groupes résolubles qui ne sont pas polycycliques, il suffit de prendre des groupes résolubles qui ne sont pas de type fini. C'est possible, ne serait-ce qu'en prenant un groupe commutatif qui n'est pas de type fini.

Chapitre 6

Problèmes supplémentaires

Les problèmes que nous proposons ici ne se rattachent pas directement à l'un des chapitres. De difficulté variée et de longueur raisonnable, ils constituent un bon entraînement qui met en pratique les techniques et les notions déjà rencontrées.

6.1 LES PRODUITS EN COURONNE

6.1.1 Un exemple

1) Fixons l'entier n, et soit $\mathbf{G}_n$ le groupe des matrices de permutations, (*cf.* 3.1.9). On définit un nouvel ensemble de matrices, $\mathbf{B}_n$, en posant :

$$M \in \mathbf{B}_n \iff \exists \sigma \in \mathcal{S}_n,\ \exists (a_i) \in \{-1, 1\}^n,\ \begin{cases} m_{ij} = 0 & \text{si } i \neq \sigma(j) \\ m_{ij} = a_i & \text{si } i = \sigma(j) \end{cases}$$

où on a noté m_{ij} les coefficients de la matrice M. Vérifier que $\mathbf{B}_n$ est un groupe. Quel est son cardinal ? On le nomme **groupe hyperoctaédral**.

2) Montrer que $\mathbf{G}_n$ est un sous-groupe de $\mathbf{B}_n$. Est-il normal dans $\mathbf{B}_n$? Soit $\mathbf{D}_n$ l'ensemble des matrices diagonales dont les coefficients diagonaux sont pris dans $\{1, -1\}$. Montrer que c'est un sous-groupe de $\mathbf{B}_n$. Est-il normal dans $\mathbf{B}_n$?

3) Montrer que $\mathbf{B}_n = \mathbf{D}_n \rtimes_\phi \mathbf{G}_n$. On précisera l'action ϕ.

4) Reconnaître les groupes $\mathbf{B}_1$ et $\mathbf{B}_2$.

5) On suppose ici que $n = 3$. Montrer que l'ensemble $\mathbf{B}_3^+$ des matrices de $\mathbf{B}_3$ ayant un déterminant égal à 1 est un sous-groupe normal de $\mathbf{B}_3$, et que $\mathbf{B}_3 \cong \mathbf{B}_3^+ \times \mathbb{Z}/2$.

6) Vérifier que $\mathbf{B}_3^+$ est isomorphe au groupe des isométries directes qui conservent un cube, tandis que $\mathbf{B}_3$ est isomorphe au groupe de toutes les isométries qui conservent un cube. Interpréter, dans ce cadre, les sous-groupes $\mathbf{D}_3$ et $\mathbf{G}_3$. On l'appelle **groupe octaédral**.

7) Peut-on généraliser la définition géométrique de la question précédente ? On cherchera à définir un « hypercube » dans un espace de dimension quelconque.

6.1.2 Un cas plus général

On considère $\mathbf{G}$ un sous-groupe de $\mathcal{S}_n$, $n \geqslant 2$, et $\mathbf{H}$ un groupe quelconque. On appelle **produit en couronne** de $\mathbf{H}$ par $\mathbf{G}$ le produit semi-direct $\mathbf{W} = \mathbf{H}^n \rtimes_\phi \mathbf{G}$ où l'action de $\mathbf{G}$ sur $\mathbf{H}^n$ est l'action à gauche :

$$\sigma.(h_1, h_2, \ldots, h_n) = (h_{\sigma^{-1}(1)}, h_{\sigma^{-1}(2)}, \ldots, h_{\sigma^{-1}(n)})$$

(cf. 3.1.8). Nous noterons le produit en couronne $\mathbf{W} = \mathbf{H} \wr \mathbf{G}$[1].

1) Montrer que les groupes $\mathbf{B}_n$ entrent dans cette description.

2) Montrer qu'il existe dans $\mathbf{W}$ des sous-groupes isomorphes à $\mathbf{G}$, à $\mathbf{H}$. Sont-ce des sous-groupes normaux ?

3) On considère les groupes cycliques $\mathbb{Z}/n$ comme sous-groupes de $\mathcal{S}_n$, engendrés par la permutation circulaire $(1, 2, \ldots, n)$. Définir les groupes $\mathbb{Z}/m \wr \mathbb{Z}/n$. « produit en couronne ».

4) Soit Γ un graphe, autrement dit un ensemble fini formé de sommets (S_i) muni d'une relation $\mathcal{R}$ d'adjacence ; $\mathcal{R}$ est symétrique, et l'on n'a jamais $S\mathcal{R}S$. Si les sommets sont des points du plan, on peut représenter cette relation en reliant les sommets adjacents, l'arête étant une paire de sommets distincts. On appelle alors **automorphisme de graphe** une bijection ϕ de l'ensemble des sommets dans lui-même, telle que :

$$\forall S_i, S_j,\ S_i \mathcal{R} S_j \Rightarrow \phi(S_i) \mathcal{R} \phi(S_j)$$

Les produits en couronne sont souvent représentables comme des groupes d'automorphismes de graphes, comme le montrent les exemples suivants :

a) Déterminer les groupes d'automorphismes des deux arbres de la figure 6.1, et les identifier comme produits en couronne.

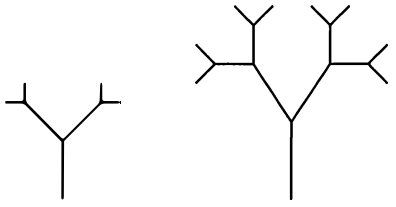


Figure 6.1 Arbres

b) Déterminer, de même, le groupe d'automorphisme de la « couronne » de la figure 6.2.

1. W est l'initiale de « wreath », le mot anglais pour couronne.

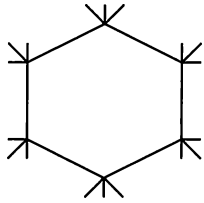


Figure 6.2 Couronne hexagonale

5) Montrer que $\mathcal{S}_m \wr \mathcal{S}_n$ peut s'identifier à un sous-groupe de $\mathcal{S}_{nm}$. En déduire que $(mn)!$ est divisible par $(m!)^n n!$.

6.1.3 Le cas général

Pour généraliser encore notre construction, on se donne :

– un groupe $\mathbf{G}$ agissant (à gauche) sur un ensemble X ;

– un groupe $\mathbf{H}$.

Rappelons que l'on note $\mathbf{H}^X$ l'ensemble des applications de X dans $\mathbf{H}$. C'est un groupe pour l'opération induite par $\mathbf{H}$. Si f et f' sont des éléments de $\mathbf{H}^X$, alors ff' est l'application définie par $ff'(x) = f(x)f'(x)$.
Considérons alors le produit semi-direct $\mathbf{W} = \mathbf{H}^X \rtimes_\phi \mathbf{G}$ où l'action est définie par :

$$\forall f \in \mathbf{H}^X, \forall \sigma \in \mathbf{G},\ \sigma.f : x \mapsto f(\sigma^{-1}.x)$$

On note ce produit semi-direct : $\mathbf{H} \wr_X \mathbf{G}$. Le groupe $\mathbf{H}^X \times \{e\}$ que l'on identifie à $\mathbf{H}^X$ s'appelle **groupe de base** du produit semi-direct. C'est, comme dans tout produit semi-direct, un sous-groupe normal de $\mathbf{W}$.

1) Vérifier que les constructions précédentes entrent dans ce cadre.

2) Montrer que $\mathbf{G}$ s'identifie à un sous-groupe $\mathbf{G}^*$ de $\mathbf{W}$, que l'on précisera. Montrer aussi qu'il existe des sous-groupes de $\mathbf{W}$ isomorphes à $\mathbf{H}$.

3) On note $\mathbf{H}^*$ le sous-groupe du groupe de base formé des applications f_h, telles que :

$$\forall x \in X,\ f_h(x) = h \quad \text{où } h \in \mathbf{H}$$

Ce sont donc les applications constantes. Montrer que c'est un sous-groupe de $\mathbf{W}$, isomorphe à $\mathbf{H}$. Que dire de $\mathbf{H}^*\mathbf{G}^*$?

4) On suppose que $\mathbf{H}$ agit sur un ensemble Y. Montrer que le produit en couronne $\mathbf{W}$ agit sur Y^X, par :

$$(f, g).\psi = \widetilde{\psi} \text{ où } \widetilde{\psi}(x) = f(x).\psi(g^{-1}.x)$$

où ψ est un élément de Y^X. Reconnaître les actions par restriction de $\mathbf{G}^*$ et de $\mathbf{H}^*$.

5) Si l'on note $\mathbf{H}^{(X)}$ l'ensemble des applications de X dans $\mathbf{R}$ qui prennent la valeur e pour presque tous les éléments de X, on obtient, par la même construction, un produit en couronne dit **restreint**. Montrer que c'est un sous-groupe du produit en couronne, que l'on peut alors appeler produit **complet**. Le produit en couronne restreint est-il un sous-groupe normal du produit complet ?

6) On suppose que l'action de **G** sur X est fidèle et transitive. Rechercher le centre de **W**. On traitera le cas restreint et le cas complet. En prenant pour **H** le groupe $\mathbb{Z}/p$ et pour **G** le p-groupe de Prüfer, montrer que le produit en couronne restreint est un exemple de p-groupe dont le centre est trivial.

7) Soit **W** le produit en couronne $\mathbb{Z}/2 \wr_{\mathbf{w}} \mathbb{Z}$, où l'on prend $X = \mathbb{Z}$ que l'on fait agir sur lui-même par translation à gauche ; ce produit s'appelle le produit en couronne **régulier**. Les éléments de **W** sont donc des couples $((u_n), k)$ où (u_n) est une suite indexée par $\mathbb{Z}$ à valeur dans $\mathbb{Z}/2$, et k un élément de $\mathbb{Z}$. Soit **K** l'ensemble des couples pour lesquels (u_n) est nulle sur les entiers strictement négatifs, et k est toujours nul. Montrer que **K** est un sous-groupe de **W** et étudier ses conjugués. En déduire un exemple de sous-groupe contenant strictement un de ses conjugués.

6.2 GROUPES POLYÉDRAUX ET BINAIRES POLYÉDRAUX

Dans ce problème, nous allons étudier des groupes qui ont une grande importance en géométrie ; ils sont liés aux célèbres **solides de Platon** (dans l'ordre tétraèdre, cube ou hexaèdre, octaèdre, dodécaèdre et icosaèdre) qui sont les cinq seuls polyèdres réguliers. On admettra leur existence et leurs propriétés géométriques de base. À chacun de ces polyèdres, on associe le groupe des isométries qui le conservent. Bien que nous soyons surtout intéressés par l'aspect « groupe » de ce problème, un minimum de connaissances géométriques est prérequis.

6.2.1 Groupe d'isométries conservant un ensemble

Soit $\mathcal{E}$ un espace affine euclidien, S un sous-ensemble. Une façon mathématique de mesurer le « degré de symétrie de S » est de déterminer l'ensemble des isométries g qui conservent S, c'est-à-dire qui vérifient $g(S) = S$.

1) Traduire l'énoncé précédent en termes d'action de groupe. En déduire que l'ensemble des isométries qui conservent S est un groupe, que l'on notera I_S, et qu'on appellera **groupe d'isométries** de S.

2) $\mathcal{E}$ est un plan. Déterminer le groupe d'isométries des figures ci-dessous.
   - Une droite.
   - Un cercle.
   - Un carré.
   - Un rectangle.
   - Un triangle « quelconque ».

3) Vérifier que le groupe des isométries qui conservent un polygone régulier à n côtés est un groupe isomorphe au groupe diédral $\mathbb{D}_{2n}$.

4) On suppose que S est un ensemble fini. Montrer que les éléments de I_S ont un point fixe commun. À quelle condition I_S est-il fini ?

5) Montrer que toutes les isométries d'un sous-groupe fini ont un point invariant commun.

6) La question précédente permet de ramener la recherche des groupes finis d'isométries aux sous-groupes finis de $\mathbf{O}(n)$, groupe des transformations orthogonales de l'espace vectoriel euclidien de dimension n. Démontrer que les sous-groupes finis de $\mathbf{O}(2)$ sont isomorphes aux groupes cycliques ou aux groupes diédraux.

6.2.2 Sous-groupes finis de SO(3)

On rappelle que les éléments de $\mathbf{SO}(3)$ sont les rotations, caractérisées par un axe (orienté) et un angle, ainsi que l'identité.

1) Soit $\mathbf{G}$ un sous-groupe fini de $\mathbf{SO}(3)$. On appelle **pôle** d'une rotation un des points d'intersection de l'axe de la rotation avec la sphère unité S^2. Montrer que $\mathbf{G}$ agit sur l'ensemble P des pôles de $\mathbf{G}$.

2) Soit k le nombre des orbites pour cette action, n le cardinal de $\mathbf{G}$. On considère un élément x de P, et l'on note $\mathbf{G}_x$ son stabilisateur. Montrer que $\mathbf{G}_x$ est cyclique et que son cardinal n_x vérifie :

$$2 \leqslant n_x \leqslant n$$

3) Soient $x_1, x_2, \ldots x_k$ des représentants des différentes orbites et n_i le cardinal du stabilisateur de x_i. En utilisant la formule de Burnside (3.1.17), démontrer la relation :

$$n \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) = 2(n-1)$$

4) En utilisant des « considérations arithmétiques », montrer que $k = 1$ puis $k \geqslant 4$ sont impossibles, puis que la relation qui vient d'être trouvée ne peut être satisfaite que dans les cas suivants :

   – il y a deux orbites et $n_1 = n_2 = n$;

   – il y a trois orbites et les stabilisateurs ont pour cardinaux :

      a) 2, 2, $\frac{n}{2}$, et donc n est pair.

      b) 2, 3, 3, et $n = 12$.

      c) 2, 3, 4, et $n = 24$.

      d) 2, 3, 5, et $n = 60$.

5) Dans le premier cas, montrer que le groupe $\mathbf{G}$ est formé de rotations de même axe, le décrire et proposer un objet de l'espace dont ce soit le groupe des rotations.

6) Étudier de même le a) du second cas.

7) Vérifier que le groupe des rotations d'un tétraèdre régulier correspond bien à la description b), et prouver qu'il n'y a pas d'autre possibilité.

8) Vérifier de même que les cas c) et d) correspondent respectivement au groupe des rotations conservant un cube (ou un octaèdre) et un dodécaèdre (ou un icosaèdre) réguliers. À quels groupes « connus » sont-ils isomorphes ?

6.2.3 Sous-groupes finis de O(3)

On s'intéresse maintenant aux sous-groupes finis de $\mathbf{O}(3)$. Il y a donc, en plus des rotations, les réflexions, et les **réflexions rotatoires** qui, comme leur nom l'indique, sont des composés

(commutatifs) d'une réflexion et d'une rotation d'axe orthogonal au plan de la réflexion ; dans le cas particulier d'un demi-tour (rotation d'angle π), on obtient $-id$.

1) Soit $\mathbf{G}$ un tel sous-groupe fini. Montrer que $\mathbf{G}^+ = \mathbf{G} \cap \mathbf{SO}(3)$ est un sous-groupe d'indice 1 ou 2 de $\mathbf{G}$.

2) Si $\mathbf{G} = \mathbf{G}^+$, on obtient donc les sous-groupes finis vus ci-dessus. Décrire quelques objets qui admettent ces sous-groupes comme groupes d'isométries.

3) On suppose que $\mathbf{G}^+$ est d'indice 2 dans $\mathbf{G}$. Montrer que si $\mathbf{G}$ contient $-id$, alors $\mathbf{G}$ est un produit direct de $\{\pm id\}$ avec un des groupes de la section précédente. Préciser les groupes obtenus.

4) On suppose toujours que $\mathbf{G}^+$ est d'indice 2 dans $\mathbf{G}$, mais que $\mathbf{G}$ ne contient pas $-id$. Étudier le groupe $\Gamma = \langle \mathbf{G}, -id \rangle$ et en déduire que $\mathbf{G}$ est de la forme $\mathbf{G} = \mathbf{H} \cup -id\mathbf{H}$ où $\mathbf{H}$ est un sous-groupe d'indice 2 d'un sous-groupe fini de $\mathbf{SO}(3)$. Préciser, le plus possible, les groupes obtenus.

5) Rechercher les groupes d'isométrie des solides de Platon parmi les groupes décrits précédemment.

6.2.4 Groupes polyédraux

Soient p, q, r trois entiers. On note (p, q, r) le groupe de présentation :

$$\langle a, b, c \mid a^p = b^q = c^r = abc = 1 \rangle$$

et l'on appelle **groupes polyédraux** les groupes ayant une telle présentation.

1) Trouver une présentation ayant seulement deux générateurs.

2) Reconnaître $(p, p, 1)$.

3) Montrer que $(2, 2, r)$ est le groupe $\mathbb{D}_{2r}$.

4) On considère les groupes polyédraux suivants : $(2, 3, 3)$; $(2, 3, 4)$; $(2, 3, 5)$. Montrer que le premier est fini et est isomorphe au groupe tétraédral $\mathbf{T}$.

5) Montrer que le second est fini, isomorphe au groupe octaédral $\mathbf{O}$. On pourra chercher un sous-groupe normal isomorphe au groupe tétraédral.

6) En admettant que le troisième groupe est fini d'ordre 60, montrer qu'il est isomorphe au groupe icosaédral $\mathbf{I}$. On peut montrer que ce sont les seuls groupes polyédraux finis ; chercher un modèle du groupe $(3, 3, 3)$ en utilisant des rotations planes.

6.2.5 Groupes binaires polyédraux

Dans ce paragraphe, on s'intéresse aux sous-groupes finis du groupe multiplicatif des quaternions non nuls, $\mathbb{H}^*$. On utilisera, pour cela, les résultats du problème 3.5.2. Soit $\mathbf{G}$ un sous-groupe fini du groupe des quaternions.

1) Montrer que $\mathbf{G}$ est un sous-ensemble du groupe des quaternions unitaires. On notera $\mathbf{H}$ ce groupe.

2) Soit ϕ l'application de $\mathbf{H}$ dans $\mathbf{SO}(3, \mathbb{R})$ définie par $\phi(q) = r$ où r est la rotation :

$$r(x) = qxq^{-1}$$

Que peut-on dire de $\phi(\mathbf{G})$? En déduire tous les sous-groupes finis de $\mathbb{H}^*$ qui ne contiennent pas -1.

3) Dans le cas où $\mathbf{G}$ contient -1, montrer qu'il admet la présentation :

$$\mathbf{G} = \langle a,\ b,\ c \mid a^p = b^q = c^r = abc,\ (abc)^2 = 1\rangle$$

avec (p, q, r) de la forme $(p, p, 1)$, $(2, 2, r)$, $(2, 3, 3)$, $(2, 3, 4)$ et $(2, 3, 5)$. On note parfois ces groupes $\langle p, q, r\rangle$ et l'on les appelle **groupes binaires polyédraux**.

4) Reconnaître $\langle p, p, 1\rangle$, et montrer que $\langle 2, 2, 2\rangle$ est un groupe dicyclique (*cf.* 2.3.5). Les trois autres groupes $\langle 3, 3, 2\rangle$, $\langle 4, 3, 2\rangle$, $\langle 5, 3, 2\rangle$ ont respectivement 24, 48 et 120 éléments, et se nomment groupes binaires tétraédral, octaédral, icosaédral.

5) Montrer directement que si $\mathbf{G}'$ est le groupe défini par :

$$\mathbf{G}' = \langle a,\ b,\ c \mid a^p = b^3 = c^2 = abc\rangle$$

alors $(abc)^2 = 1$. En déduire une présentation plus économique des groupes binaires polyédraux.

6.3 TRANSITIVITÉ, BLOCS, GROUPES PRIMITIFS

6.3.1 Groupes transitifs

Ici, nous nous intéresserons à l'action de groupes finis, en étudiant de nouvelles notions liées à la transitivité. Le cadre général du problème sera plus précisément l'action des sous-groupes de $\mathcal{S}_n$ sur $X = \{1, 2, \ldots, n\}$. Rappelons que $\mathcal{S}_n$ et $\mathcal{A}_n$ agissent transitivement sur X. On dira plus rapidement qu'ils sont **transitifs**.

1) Pour $n = 3$, vérifier que ce sont les seuls sous-groupes transitifs.

2) Pour n quelconque, montrer que le cardinal d'un groupe transitif est un multiple de n.

3) Montrer que les sous-groupes transitifs de $\mathcal{S}_4$ sont, outre $\mathcal{S}_4$ lui-même et $\mathcal{A}_4$:
   - $\langle(1, 2, 3, 4)\rangle$ et ses conjugués.
   - $\mathcal{V} = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, le groupe engendré par les doubles transpositions.
   - $\langle(1, 2, 3, 4), (1, 3)\rangle$ et ses conjugués, qui sont les 2-Sylow, isomorphes à $\mathbb{D}_8$.

Cas $n = 5$:

1) Montrer que le normalisateur dans $\mathcal{S}_5$ de $\langle(1, 2, 3, 4, 5)\rangle$ est le groupe à 20 éléments $\langle(1, 2, 3, 4, 5), (1, 4, 2, 3)\rangle$, isomorphe à l'holomorphe de $\mathbb{Z}/5$ c'est-à-dire à $\mathbf{GA}(1, \mathbb{F}_5)$.

2) Montrer que $\mathcal{S}_5$ n'a pas de sous-groupe transitif à plus de 20 éléments, autre que le groupe alterné. On utilisera l'action de $\mathcal{S}_5$ sur le quotient.

3) En déduire que les sous-groupes transitifs de $\mathcal{S}_5$ sont :
   - $\langle(1, 2, 3, 4, 5)\rangle$ de cardinal 5 et ses conjugués.
   - $\langle(1, 2, 3, 4, 5), (1, 2)(4, 3)\rangle$ de cardinal 10 et ses conjugués.
   - $\langle(1, 2, 3, 4, 5), (1, 4, 2, 3)\rangle$ de cardinal 20 et ses conjugués.

6.3.2 Blocs

Soit un groupe transitif $\mathbf{G}$ agissant sur un ensemble X. On peut faire agir $\mathbf{G}$ sur les sous-ensembles de X et l'on appelle **bloc** un sous-ensemble B de X tel que :

$$\forall g \in \mathbf{G},\ g.B = B \text{ ou } g.B \cap B = \emptyset$$

1) Montrer qu'alors l'ensemble des $g.B$ forme une partition de X par des blocs. On nomme parfois cette partition un **système de blocs**. Dans le cas où X et $\mathbf{G}$ sont finis, que peut-on dire du cardinal d'un bloc ?
2) On fait agir le groupe diédral sur les sommets d'un carré, quels sont tous les systèmes de blocs ?
3) Soit x un élément de X, $\mathbf{G}_x$ son stabilisateur. Montrer que tout bloc contenant x est de la forme $\mathbf{H}.x$ où $\mathbf{H}$ est un sous-groupe de $\mathbf{G}$ vérifiant $\mathbf{G}_x \leqslant \mathbf{H} \leqslant \mathbf{G}$.
4) Examiner les blocs déterminés par l'action du groupe cyclique engendré par une permutation circulaire.
5) Un groupe transitif est dit **primitif** s'il n'a aucun système de blocs non trivial (i.e. formé de singletons ou de X tout entier). Montrer qu'un groupe $\mathbf{G}$ est primitif ssi le stabilisateur d'un élément est un sous-groupe maximal de $\mathbf{G}$.
6) Montrer qu'un groupe 2-transitif est primitif. Un groupe est 2-transitif s'il agit sur un ensemble X de sorte que

$$\forall x, x', y, y' \in X,\ x \neq y,\ x' \neq y' \Rightarrow \exists g \in \mathbf{G}\ g.x = x' \text{ et } g.y = y'$$

On pourra se reporter à l'exercice 3.1.16 pour cette définition.

6.3.3 Simplicité des groupes spéciaux projectifs linéaires

Nous allons utiliser les notions précédentes pour trouver une nouvelle famille de groupes simples, les groupes $\mathbf{PSL}(n, \mathbb{K})$. Pour une définition, voir le problème 3.5.1.

1) On suppose que $\mathbf{G}$ est égal à son groupe dérivé (il est donc **parfait**), et qu'il agit fidèlement sur un ensemble X, par une action transitive et primitive.
Soit x un élément de X ; on suppose également qu'il existe un sous-groupe $\mathbf{A}$ commutatif et normal dans $\mathbf{G}_x$, tel que $\mathbf{G}$ soit engendré par l'union des conjugués de $\mathbf{A}$. Avec toutes ces hypothèses... $\mathbf{G}$ est un groupe simple. Cela constitue le critère d'Iwasawa. On appellera $\mathbf{N}$ un sous-groupe normal de $\mathbf{G}$, non trivial, et l'on passera par les étapes suivantes :
   - montrer que $\mathbf{N}.x$ est un bloc, et en déduire que $\mathbf{N}$ agit transitivement sur X ;
   - montrer que $\mathbf{N}\mathbf{G}_x = \mathbf{G}$;
   - montrer que $\mathbf{N}\mathbf{A} = \mathbf{G}$;
   - montrer que $\mathbf{G}/\mathbf{N}$ est commutatif.
2) On veut montrer que les groupes $\mathbf{PSL}(n, \mathbb{K})$ sont simples, sauf dans les deux cas $\mathbf{PSL}(2, \mathbb{F}_2)$ et $\mathbf{PSL}(2, \mathbb{F}_3)$. Il est bien entendu que $n \geqslant 2$.
   a) Montrer que $\mathbf{PSL}(n, \mathbb{K})$ agit 2-transitivement sur les droites de $\mathbb{K}^n$, et en déduire qu'il est primitif. Vérifier également que l'action est fidèle.

b) Montrer que $\mathbf{PSL}(n, \mathbb{K})$ est égal à son groupe dérivé, sauf les deux exceptions $\mathbf{PSL}(2, \mathbb{F}_2)$ et $\mathbf{PSL}(2, \mathbb{F}_3)$. On utilisera :
- le fait que $\mathbf{SL}(n, \mathbb{K})$ est engendré par les matrices de transvection ;
- le fait qu'une matrice de transvection est un commutateur, en dimension supérieure ou égale à trois.

et l'on sera amené à étudier, à part, le cas $n = 2$.

c) Soit $\mathbf{A}$ l'ensemble des projections des matrices de la forme :

$$A = \begin{pmatrix} 1 & \ell \\ 0 & I_{n-1} \end{pmatrix}$$

où ℓ est une matrice ligne avec $n-1$ colonnes et 0 représente une matrice colonne nulle de $n-1$ lignes. Montrer que $\mathbf{A}$ est un groupe commutatif, normal dans le stabilisateur de la droite engendré par le premier vecteur de base. Montrer enfin que $\mathbf{PSL}(n, \mathbb{K})$ est engendré par les conjugués des éléments de $\mathbf{A}$; on pourra pour cela vérifier que les éléments de $\mathbf{A}$ sont des matrices de transvection. Conclure.

6.4 SUR LES SOUS-GROUPES

1) On suppose que $\mathbf{H}$, $\mathbf{K}$ et $\mathbf{L}$ sont des sous-groupes de $\mathbf{G}$ tels que $\mathbf{H} \leqslant \mathbf{K}$. Démontrer que :

$$\text{Si} \quad \mathbf{H} \cap \mathbf{L} = \mathbf{K} \cap \mathbf{L} \quad \text{et} \quad \mathbf{HL} = \mathbf{KL} \quad \text{alors} \quad \mathbf{H} = \mathbf{K}$$

C'est la **loi modulaire**. On pourra l'écrire en notation additive et voir comment elle se traduit dans le cadre des espaces vectoriels (pour la loi d'addition).

2) On suppose que $\mathbf{H}$, $\mathbf{K}$ et $\mathbf{L}$ sont des sous-groupes de $\mathbf{G}$ tels que $\mathbf{H} \leqslant \mathbf{K}$. Démontrer que :

$$\mathbf{HL} \cap \mathbf{K} = \mathbf{H}(\mathbf{L} \cap \mathbf{K})$$

C'est la **loi de Dedekind**. Donner une traduction dans le cadre des espaces vectoriels, et montrer par un exemple que l'hypothèse $\mathbf{H} \leqslant \mathbf{K}$ est nécessaire.

3) Soit $\mathbf{G}$ un groupe et $\mathcal{L}(\mathbf{G})$ l'ensemble des sous-groupes de $\mathbf{G}$, muni de la relation d'ordre $\subset$. Montrer que cet ensemble est un **treillis** c'est-à-dire que :

$$\forall (\mathbf{H}, \mathbf{K}) \in \mathcal{L}(\mathbf{G})^2, \ \exists \mathbf{M} \in \mathcal{L}(\mathbf{G}), \ \mathbf{M} = \sup(\mathbf{H}, \mathbf{K})$$

et

$$\forall (\mathbf{H}, \mathbf{K}) \in \mathcal{L}(\mathbf{G})^2, \ \exists \mathbf{N} \in \mathcal{L}(\mathbf{G}), \ \mathbf{N} = \inf(\mathbf{H}, \mathbf{K})$$

On note alors $\mathbf{H} \vee \mathbf{K} = \sup(\mathbf{H}, \mathbf{K})$ et $\mathbf{H} \wedge \mathbf{K} = \inf(\mathbf{H}, \mathbf{K})$.

4) Montrer que

$$\mathbf{H} \leqslant \mathbf{K} \iff \mathbf{K} = \mathbf{H} \vee \mathbf{K} \quad \text{et} \quad \mathbf{H} \leqslant \mathbf{K} \iff \mathbf{H} = \mathbf{H} \wedge \mathbf{K}$$

et observer que ces équivalences sont valables dans tout treillis.

5) Soit $\mathbf{G} = \mathbb{Z}/n$ le groupe cyclique d'ordre n : comment décrire le treillis de ses sous-groupes ?

6) On dit qu'un sous-ensemble d'un treillis est un sous-treillis s'il est stable pour les opérations $\vee$ et $\wedge$. Montrer que l'ensemble $\mathcal{N}(\mathbf{G})$ des sous-groupes de $\mathbf{G}$ qui sont normaux dans $\mathbf{G}$ est un sous-treillis de $\mathcal{L}(\mathbf{G})$.

6.5 DES GROUPES D'ORDRE 12

1) Il y a trois groupes d'ordre 12 non commutatifs, $\mathbb{D}_{12}$, $\mathcal{A}_4$ et $\mathcal{T}$ (voir l'exercice 3.4.4). Déterminer dans chacun de ces trois cas l'ensemble de leurs sous-groupes.

2) Soit $\mathbf{H} = \mathbf{T}(2, \mathbb{F}_3)$ le groupe des matrices triangulaires supérieures inversibles d'ordre 2, à coefficients dans $\mathbb{F}_3 = \mathbb{Z}/3$. Vérifier que ce groupe a douze éléments, et préciser son centre. Auquel des groupes précédents est-il isomorphe ?

3) Déterminer les automorphismes intérieurs de $\mathbf{H}$.

4) Déterminer tous les automorphismes de $\mathbf{H}$.

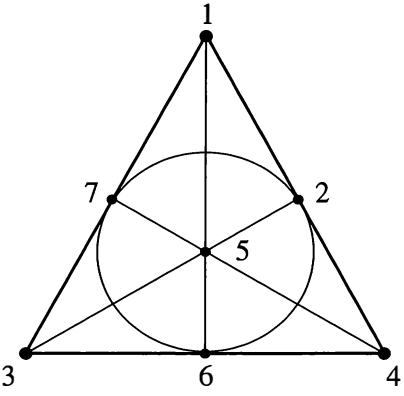
5) On appelle $\mathbf{G}$ le groupe de toutes les matrices inversibles d'ordre 2 à coefficients dans $\mathbb{F}_3$. Quel est le cardinal de $\mathbf{G}$?

6) Soit $\mathcal{Z}(\mathbf{G})$ le centre de $\mathbf{G}$. En considérant l'action de $\mathbf{G}$ sur $\mathbf{G}/\mathbf{H}$, montrer que $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est isomorphe au groupe symétrique $\mathcal{S}_4$. Retrouver ainsi un résultat du problème 3.5.1.

7) Encore un. Vérifier que le groupe $\mathbf{K}$, formé des matrices triangulaires supérieures de dimension deux, à coefficients dans le corps $\mathbb{F}_4$ et de déterminant 1, est aussi un groupe à douze éléments. À quel groupe est-il isomorphe ? On rappelle qu'il n'existe, à isomorphisme près, qu'un seul corps à quatre éléments. On peut le réaliser par l'anneau quotient $\mathbb{F}_2[X]/(X^2 + X + 1)$, et si l'on note α la classe de X, ce quotient peut s'écrire $\{0, 1, \alpha, 1 + \alpha\}$.

6.6 UN GROUPE D'ORDRE 168

On considère le graphe dessiné ci-dessous :



et on s'intéresse au groupe $\mathbf{G}$ des automorphismes de ce graphe, que l'on appelle « plan de Fano[1]. »

1) Le graphe est formé de sept points : le groupe des automorphismes est donc un sous-groupe du groupe $\mathcal{S}_7$. On considère aussi l'ensemble des sept « droites », colonnes du

1. Gino Fano, mathématicien italien (1871-1952), spécialiste de géométrie finie.

tableau ci-dessous :

$$\mathbb{D} = \begin{array}{|ccccccc|} \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ \hline \end{array}$$

(remarquer que $2, 6, 7$ est considéré comme une droite...) Montrer que $\mathbf{G}$ est de cardinal 168 : on s'intéressera au stabilisateur d'un point puis de deux points...

2) Soit $\sigma = (1,2,3,4,5,6,7)$ et $\tau = (3,7)(5,6)$. Montrer que $\mathbf{H} = \langle \sigma, \tau \rangle$ est un sous-groupe de $\mathbf{G}$, de $\mathcal{A}_7$, et que son cardinal est un multiple de 168. On cherchera un élément d'ordre 7, puis un élément d'ordre 3 et on montrera que $\mathbf{H}$ contient un groupe à huit éléments. En déduire que $\mathbf{H} = \mathbf{G}$.

3) On cherche à montrer que $\mathbf{G}$ est un groupe simple, c'est-à-dire qu'il n'a pas de sous-groupe normal non trivial. Pour cela, on va vérifier que $\mathbf{G}$ est isomorphe à $\mathbf{PSL}(3, \mathbb{F}_2) = \mathbf{PGL}(3, \mathbb{F}_2)$: montrer en effet que le plan de Fano est isomorphe au graphe formé des points et des droites du plan projectif construit sur le corps à deux éléments $\mathbb{F}_2$, et que $\mathbf{G}$ s'identifie au groupe des homographies de ce plan.

6.7 SOUS-GROUPES MAXIMAUX

Soit $\mathbf{G}$ un groupe. On dit que $\mathbf{M}$ est un sous-groupe maximal de $\mathbf{G}$ lorsque :

$$\forall \mathbf{L} \leqslant \mathbf{G}, \qquad \mathbf{M} \leqslant \mathbf{L} \leqslant \mathbf{G} \Rightarrow \mathbf{L} = \mathbf{M} \text{ ou } \mathbf{L} = \mathbf{G}$$

1) Quels sont les sous-groupes maximaux de $(\mathbb{Z}, +)$? Quels sont les sous-groupes maximaux de $\mathbb{Z}/n$?

2) Montrer que tout groupe fini $\mathbf{G}$ admet au moins un sous-groupe maximal.

3) Montrer que $(\mathbb{Q}, +)$ n'admet pas de sous-groupe maximal.

4) On suppose maintenant, et dans toutes les questions suivantes, que $\mathbf{G}$ est un groupe fini. Montrer que si $\mathbf{M}$ est un sous-groupe d'indice p (p premier), alors $\mathbf{M}$ est un sous-groupe maximal. Montrer que $\mathbb{S}_4$ admet un sous-groupe maximal d'indice 4.

5) Si $\mathbf{M}$ est un sous-groupe normal de $\mathbf{G}$, montrer qu'il est maximal si et seulement si il est d'indice p où p est premier.

6) À quelle condition $\mathbf{G}$ n'admet-il qu'un seul sous-groupe maximal ?

7) Soit $\mathbf{G}$ un groupe fini. On appelle **sous-groupe de Frattini** de $\mathbf{G}$ l'intersection des sous-groupes maximaux de $\mathbf{G}$. On le note $\Phi(\mathbf{G})$. Montrer que c'est un sous-groupe caractéristique de $\mathbf{G}$, et déterminer le sous-groupe de Frattini du groupe cyclique $\mathbb{Z}/n$, du groupe symétrique $\mathcal{S}_n$.

8) Montrer que $\Phi(\mathbf{G})$ est l'ensemble des non-générateurs de $\mathbf{G}$. La définition d'un « non-générateur » de $\mathbf{G}$ est la suivante : soit S une partie génératrice quelconque de $\mathbf{G}$, x est non-générateur si $\mathbf{G} = \langle S \setminus \{x\} \rangle$.

9) Montrer que $\Phi(\mathbf{G})$ est nilpotent. On montrera que $\Phi(\mathbf{G})$ est produit direct de ses sous-groupes de Sylow, et on sera amené à utilisé l'argument (ou lemme) de Frattini : voir 3.2.14

Solutions des problèmes

1.3.1 Sous-groupes caractéristiques, centre

1) Soit ϕ un automorphisme quelconque de $\mathbf{G}$. Alors $\phi(\mathbf{K}) = \mathbf{K}$ car $\mathbf{K}$ est caractéristique dans $\mathbf{G}$. On en déduit que la restriction de ϕ à $\mathbf{K}$ est un automorphisme de $\mathbf{K}$, et que $\phi(\mathbf{H}) = \mathbf{H}$. $\mathbf{H}$ est donc un sous-groupe caractéristique de $\mathbf{G}$. Dans le cas où on tente de remplacer « caractéristique » par « normal », ce qui ne fonctionne pas, c'est que la restriction d'un automorphisme intérieur est un automorphisme, mais pas forcément intérieur.

2) C'est le même argument. Si ϕ est un automorphisme intérieur de $\mathbf{G}$, $\mathbf{K}$ est stable par ϕ car il est normal dans $\mathbf{G}$, et la restriction de ϕ, qui n'est pas forcément intérieure dans $\mathbf{K}$, laisse invariant $\mathbf{H}$.

3) Soit $\phi \in \mathrm{Aut}(\mathbf{G})$ et $z \in \mathcal{Z}(\mathbf{G})$. Alors, si x est quelconque dans $\mathbf{G}$ et y son antécédent par ϕ, on écrit $\phi(z)x = \phi(z)\phi(y) = \phi(zy) = \phi(yz) = x\phi(z)$. Ainsi, $\phi(z)$ est dans le centre de $\mathbf{G}$, qui est donc un sous-groupe caractéristique de $\mathbf{G}$. Si $\mathbf{H}$ est un sous-groupe de $\mathcal{Z}(\mathbf{G})$, on ne peut ainsi montrer qu'il est caractéristique dans $\mathbf{G}$. En revanche, il est toujours normal dans $\mathbf{G}$, car tout automorphisme intérieur se réduit à l'identité quand on est dans le centre.

4) Soit ϕ un automorphisme. $\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1}$ et donc l'image d'un commutateur est un commutateur. Le sous-groupe dérivé est stable par tout automorphisme.

5) Même type de calcul $\phi(x^n) = \phi(x)^n$.

6) Il suffit d'observer que la bijectivité de ϕ n'est pas utilisée dans les deux questions précédentes. À l'opposé, cela a été nécessaire pour le centre.

7) Si $\mathbf{H} \leqslant \mathbf{G}$, alors $\mathcal{Z}(\mathbf{G}) \cap \mathbf{H} \subset \mathcal{Z}(\mathbf{H})$. Mais l'inclusion peut-être stricte. Ainsi, si $\mathbf{H}$ est un sous-groupe commutatif de $\mathbf{G}$, son centre est lui-même, alors que le centre de $\mathbf{G}$ peut être plus petit. Ainsi $\mathcal{A}_4$ a un centre de cardinal 2 et contient un sous-groupe commutatif à 4

éléments. Ne pas confondre le centre de **H**, qui est inclus dans **H**, avec son **centralisateur**, ensemble des éléments de **G** qui commutent avec tous les éléments de **H**.

8) Soit $C = (c_{ij})$ une matrice du centre et soit $T_{ij} = I + E_{ij}$ pour $i \neq j$. Alors $CT_{ij} = T_{ij}C$ pour tous les couples équivaut à la ligne j, et la colonne i est nulle sauf sur la diagonale. De plus, on doit avoir $c_{ii} = c_{jj}$. En utilisant les autres matrices T_{ii}, on voit que le centre ne peut contenir que les matrices scalaires, et qu'elles conviennent. Remarquons que le même calcul donne le centre de $\mathbf{SL}(n, \mathbb{K})$, puisque les matrices T_{ij} sont de déterminant 1. Passons au groupe des matrices triangulaires supérieures inversibles, pour $n = 2$, un calcul direct montre que le centre est formé des matrices scalaires, et cela se généralise en dimension quelconque. En revanche, le centre du groupe des matrices triangulaires unipotentes est formé des matrices unipotentes de la forme :

$$I + aE_{1n} = \begin{pmatrix} 1 & 0 & & 0 & a \\ 0 & 1 & & 0 & 0 \\ 0 & 0 & & 0 & 0 \\ 0 & 0 & & 0 & 0 \\ \vdots & & & \cdots & \vdots \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & & 0 & 1 \end{pmatrix}$$

Ce centre est un groupe isomorphe au groupe additif de $\mathbb{K}$.

9)

$$\phi(xy) = i_x \circ i_y \text{ et } i_x \circ i_y(g) = x(ygy^{-1})x^{-1} = i_{xy}(g)$$

donc ϕ est un morphisme. De plus, $i_x(g) = g$ pour tout g équivaut à $xgx^{-1} = g$, c'est-à-dire que x est dans le centre de **G**. On en déduit l'isomorphisme :

$$\mathbf{G}/\mathcal{Z}(\mathbf{G}) \cong \mathrm{Int}(\mathbf{G})$$

D'où l'intérêt de l'étude du quotient $\mathbf{G}/\mathcal{Z}(\mathbf{G})$.

1.3.2 Le groupe modulaire $\mathcal{M}$

1) Il suffit de montrer que f admet une application réciproque. Posons $f^{-1}(z) = \frac{dz-c}{-bz+a}$ avec les mêmes conventions pour ∞. Un simple calcul montre que cela convient, et le déterminant est encore 1.

$$f' \circ f(z) = \frac{a'f(z) + c'}{b'f(z) + d'} = \frac{\frac{a'az+a'c}{bz+d} + c'}{\frac{b'az+b'c}{bz+d} + d'} = \frac{(aa' + bc')z + ca' + dc'}{(ab' + bd')z + cb' + dd'}$$

prouve la stabilité (à la vérification des cas particuliers près). On peut également observer que le déterminant de la matrice obtenue est bien 1. L'ensemble de ces transformations est donc un groupe.

2) Dans le calcul ci-dessus, on « remarque » que les coefficients du composé de deux homographies sont ceux de la matrice produit [1]. C'est exactement dire que ϕ est un morphisme.

1. Ce n'est pas tout à fait un hasard... C'est la géométrie projective qui éclaire la relation entre homographie et matrices.

De plus, si $f(z) = z$ pour tout z, alors $bz^2 + (d-a)z + c = 0$ pour tout z, ce qui donne $b = c = 0$ et $a = d$. La condition sur le déterminant conduit bien aux solutions I et $-I$.

3) Les matrices T et S sont à coefficients entiers et de déterminant 1. De plus :

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad ; \quad S^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad ; \quad S^4 = I$$

S est donc d'ordre 4. Par ailleurs, une récurrence immédiate montre que

$$T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

pour k dans $\mathbb{Z}$. Le groupe engendré par T est isomorphe à $\mathbb{Z}$.

4)

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + ka_{21} & a_{12} + ka_{22} \\ a_{21} & a_{22} \end{pmatrix}$$

qui vérifie bien la règle indiquée[1]. Par ailleurs :

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{21} & -a_{22} \\ a_{11} & a_{12} \end{pmatrix}$$

Enfin les produits de l'autre côté donnent le même type de résultat mais pour les colonnes :

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} + ka_{11} \\ a_{21} & a_{22} + ka_{21} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{12} & -a_{11} \\ a_{22} & -a_{21} \end{pmatrix}$$

5) Soit :

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

une matrice de $\mathbf{SL}(2,\mathbb{Z})$. Si $b = 0$, A est triangulaire supérieure. Sinon, la division euclidienne de a par b s'écrit $a = bq + r$ et le produit de A à gauche par ST^{-q} donne une matrice de première colonne $\begin{pmatrix} -b \\ r \end{pmatrix}$. Comme $|r| < |b|$, en itérant comme dans l'algorithme d'Euclide, on parvient à un dernier reste nul, et on se ramène à une matrice triangulaire supérieure notée B.

6) Une matrice de la forme

$$B = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}$$

dans $\mathbf{SL}(2,\mathbb{Z})$, vérifie $\det(B) = ad = 1$. Elle peut donc s'écrire :

$$B = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = T^c \text{ ou } B = \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix} = S^2T^{-c}$$

En prémultipliant la matrice B de la question précédente par les inverses des matrices qui ont fait passer de A à B, on voit que toute matrice de $\mathbf{SL}(2,\mathbb{Z})$ est produit de puissances

1. Ce calcul est très général, il a déjà été utilisé dans le problème précédent avec les matrices T_{ij} qui sont des matrices de **transvections**.

de T et de puissances de S. En passant au quotient, le groupe modulaire est engendré par s et t.

7)
$$A = \begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}$$
$7 = 2 \times 3 + 1$. Multiplions à gauche par T^{-3} :
$$T^{-3}A = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}$$
Multiplions à gauche par S pour échanger les lignes :
$$ST^{-3}A = \begin{pmatrix} -2 & -7 \\ 1 & 3 \end{pmatrix}$$
Encore une combinaison de lignes :
$$T^2ST^{-3}A = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$$
et un échange de lignes :
$$ST^2ST^{-3}A = \begin{pmatrix} -1 & -3 \\ 0 & -1 \end{pmatrix}$$
On reconnaît la matrice S^2T^3, d'où :
$$A = T^3S^{-1}T^{-2}S^{-1}S^2T^3 = T^3S^{-1}T^{-2}ST^3$$
En passant au quotient, on aura $a = t^3st^{-2}st^3$. Bien sûr, il existe d'autres procédés du même type ; on aurait pu utiliser les colonnes... Une question se pose, arrive-t-on alors au même résultat ?

8) La matrice U vérifie :
$$U^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad U^3 = -I$$
donc $u^3 = e$, u est d'ordre 3. De plus, on vérifie que $T = U^{-1}S^{-1}$. On en déduit que $\mathcal{M}$ est engendré par s et u qui sont respectivement d'ordre 2 et 3 ; par exemple, on trouve $a = (u^2s)^3s(u^2s)^{-2}s(u^2s)^3$.

9) Cette écriture s'obtient tout simplement en développant les calculs de puissances, et en tenant compte de l'ordre de u et de s. Ainsi $a = u^2su^2su^2susususu^2su^2su^2s$.

10) L'ensemble M est stable pour le produit matriciel, comme le montre le calcul suivant :
$$\begin{pmatrix} a & -c \\ -b & d \end{pmatrix}\begin{pmatrix} a' & -c' \\ -b' & d' \end{pmatrix} = \begin{pmatrix} aa' + cb' & -ac' - cd' \\ -ba' - db' & bc' + dd' \end{pmatrix}$$
où tous les coefficients sont des entiers positifs. Si a, d, a', d' sont supérieurs à 1, les coefficients diagonaux du produit sont supérieurs à 1 et si $b + c \neq 0$ de même que $b' + c'$, les coefficients diagonaux de la matrice produit ne sont pas tous les deux nuls. L'ensemble M ne contient donc pas la matrice de l'identité. Donc toute matrice A de $\mathbf{SL}(2, \mathbb{Z})$ peut s'écrire sous la forme :
$$A = I,\ A = S^k,\ A = U^k,\ A = U^KN,\ A = NS^l,\ A = U^kNS^l$$

où N est un produit d'éléments de M, k et l inférieurs à l'ordre de U (resp. de S). Reste à chercher quand A est égal à I ou à $-I$. Cela ne se produit pas dans les trois derniers cas, sinon, par exemple, U^{-k} ou $-U^{-k}$ serait dans M, ce qui n'est pas vrai. On vérifie de même les autres possibilités. Enfin, deux décompositions différentes de A donneraient, en multipliant par l'inverse de l'une, une écriture non banale de I ou de $-I$. En passant à l'ensemble quotient, on voit donc que l'écriture $(*)$ est unique.

2.5.1 Les sous-groupes d'un produit

1) $\mathbf{L}_1$ et $\mathcal{L}_1$ sont des sous-groupes comme intersection de groupes, pour le premier, et comme image d'un groupe par un morphisme, pour le second. De plus, les éléments de $\mathcal{L}_1$ sont caractérisés par :

$$x \in \mathcal{L}_1 \iff \exists (x,y) \in \mathbf{L}$$

où (x,y) est bien sûr dans $\mathbf{G}$. On en déduit que $\mathbf{L}_1$, qui est formé des éléments de la forme $(x,1) \in \mathbf{L}$, est inclus dans $\mathcal{L}_1 \times \{1\}$. En identifiant $(x,1)$ avec x, $\mathbf{L}_1$ est un sous-groupe de $\mathcal{L}_1$. De même pour l'indice 2. Montrons que $\mathbf{L}_1$ est normal dans $\mathcal{L}_1$, soit $(x_0,1)$ dans $\mathbf{L}_1$, x dans $\mathcal{L}_1$ provenant d'un couple (x,y) de $\mathbf{L}$. Alors :

$$(x,1)(x_0,1)(x,1)^{-1} = (xx_0x^{-1},1) = (x,y)(x_0,1)(x,y)^{-1}$$

Comme ce dernier élément est dans $\mathbf{L}$, le conjugué de $(x_0,1)$ est dans $\mathbf{L}_1$. On peut aussi raisonner plus gobalement, en utilisant le fait que $\mathbf{L}_1$ est le noyau de la seconde projection.

2) Définissons une application par :

$$\begin{array}{rccc} \phi : & \mathcal{L}_1 & \longrightarrow & \mathcal{L}_2/\mathbf{L}_2 \\ & p_1(x,y) = (x,1) & \mapsto & y\mathbf{L}_2 \end{array}$$

Elle est bien définie car y est dans $\mathcal{L}_2$ et si (x,y) et (x,y') sont dans $\mathbf{L}$, alors $(1,y^{-1}y') \in \mathbf{L}$, et donc $y\mathbf{L}_2 = y'\mathbf{L}_2$. De plus, si $\phi(x,1) = \mathbf{L}_2$, alors $(1,y) \in \mathbf{L}$ et $(x,y) \in \mathbf{L}$, d'où $(x,yy^{-1}) \in \mathbf{L}$ et $x \in \mathbf{L}_1$. On en déduit l'isomorphisme demandé.

3) Il suffit de définir $\mathbf{L}$ ainsi :

$$\mathbf{L} = \{(x,y) \mid x \in \mathcal{L}_1,\ y \in \theta(x)\}$$

On vérifie immédiatement que c'est un groupe en utilisant le fait que θ est un morphisme. Le reste des vérifications est immédiat.

4) Si $\mathbf{L}$ est « rectangle », il est de la forme $\mathbf{H}_1 \times \mathbf{K}_1$. Et alors, $\mathbf{L}_1 = \mathcal{L}_1 = \mathbf{H}_1$. Le quotient est donc trivial, et il en va de même pour l'autre quotient. La réciproque est immédiate.

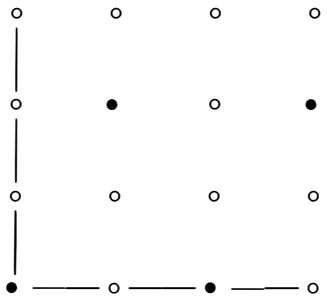
5) $\mathbf{G} = \mathbb{Z}/4$ a trois sous-groupes : $\langle\overline{0}\rangle$, $\langle\overline{2}\rangle$ et $\langle\overline{1}\rangle$. Il y a donc neuf groupes rectangles que nous ne détaillerons pas. Le quotient $\mathbf{G}/\langle\overline{0}\rangle$ conduit à deux automorphismes, l'identité, et le groupe $\mathbf{L}$ donné par la théorie précédente est le groupe diagonal, à quatre éléments. L'autre automorphisme, donné par $\overline{1} \mapsto \overline{3}$, conduit au sous-groupe :

$$\{(0,0),(1,3),(2,2),(3,1)\}$$

Les autres quotients sont $\mathbf{G}/\langle\overline{2}\rangle$ et $\langle\overline{2}\rangle/\langle\overline{0}\rangle$ qui sont isomorphes d'une seule façon ; cela donne quatre isomorphismes et quatre sous-groupes. À titre d'exemple, l'isomorphisme $\mathbf{G}/\langle\overline{2}\rangle \to \langle\overline{2}\rangle/\overline{0}$ donne le sous-groupe :

$$\{(0,0),(1,2),(2,0),(3,2)\}$$

comme on peut le vérifier sur le schéma ci-dessous :



Les sous-groupes de $\mathbb{Z}/p \times \mathbb{Z}/p$ sont rectangles, il y en a alors quatre, le sous-groupe trivial, le sous-groupe plein et les deux axes ($\overline{0} \times \mathbb{Z}/p$ et $\mathbb{Z}/p \times \overline{0}$). Les autres sont issus des automorphismes de $\mathbb{Z}/p$ dans lui-même ; ce sont les droites engendrées par $(\overline{1}, a)$ où a est inversible. Tout cela est compatible avec le fait que les sous-groupes de $\mathbb{Z}/p \times \mathbb{Z}/p$ en sont les sous-espaces vectoriels. Voir l'exercice 1.1.22.

6) a) $\mathbb{Z} \times \mathbb{Z}$. Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, et $m\mathbb{Z} \leqslant n\mathbb{Z}$ si et seulement si $n|m$, le quotient est isomorphe à $\mathbb{Z}/d$ où $d = \frac{m}{n}$. Les sous-groupes sont donc :

- les sous-groupes rectangles de la forme $n\mathbb{Z} \times m\mathbb{Z}$;
- les sous-groupes issus de quotients avec $\frac{m}{n} = \frac{m'}{n'}$.

Les sous-groupes issus des ces quotients sont des **réseaux**, c'est-à-dire des ensembles de la forme $\mathbb{Z}u + \mathbb{Z}v$ où u et v sont des vecteurs à coordonnées entières. Ainsi, le lecteur pourra vérifier que, pour les rapports $\frac{4}{2} = \frac{6}{3}$, on trouve le réseau $\mathbb{Z}(4,0) + \mathbb{Z}(2,3)$, alors qu'avec $\frac{8}{2} = \frac{12}{3}$, on trouve deux réseaux, $\mathbb{Z}(8,0) + \mathbb{Z}(2,3)$ et $\mathbb{Z}(8,0) + \mathbb{Z}(6,3)$. Réciproquement, on pourra vérifier que tout réseau est issu de cette construction ; par exemple, $\mathbb{Z}(a,b) + \mathbb{Z}(c,d)$ conduit à $\mathbf{L}_1 = \frac{ad-bc}{b \wedge d}\mathbb{Z}$, $\mathcal{L}_1 = (a \wedge c)\mathbb{Z}$.

b) Les sous-groupes de $\mathbb{Z}/2$ sont $\overline{0}$ et $\mathbb{Z}/2$; ceux de $\mathbb{Z}/6$ sont $\{\overline{0}\}$, $\{\overline{0}, \overline{2}, \overline{4}\}$, $\{\overline{0}, \overline{3}\}$ et $\mathbb{Z}/6$. On en déduit qu'il y a huit sous-groupes rectangles, et deux non rectangles :

$$\{(\overline{0},\overline{0}), (\overline{0},\overline{2}), (\overline{0},\overline{4}), (\overline{1},\overline{1}), (\overline{1},\overline{3})(\overline{1},\overline{5})\}$$

$$\{(\overline{0},\overline{0}), (\overline{1},\overline{3})\}$$

obtenus avec les mêmes techniques.

c) $\mathcal{S}_3$ admet six sous-groupes, donc trente-six sous-groupes rectangles. Il y a six automorphismes de $\mathcal{S}_3$ donc six sous-groupes à six éléments non rectangles. Par exemple

$$\{(\tau_1,\tau_2), (\tau_2,\tau_1), (\tau_3,\tau_3), (\sigma,\sigma^2), (\sigma^2,\sigma), (e,e)\}$$

pour l'automorphisme intérieur défini par la transposition τ_3. Les seuls quotients sont $\mathcal{S}_3/\{e,\sigma,\sigma^2\}$ et $\langle\tau_i\rangle/\{e\}$, et cela permet de définir d'autres sous-groupes.

2.5.2 Les groupes de Prüfer

1) $\mathbb{U}_n$ est un groupe monogène, dont un générateur est $\zeta_n = e^{\frac{2i\pi}{n}}$. Il est isomorphe à $\mathbb{Z}/n$: c'est la version « multiplicative » du groupe cyclique à n éléments.

2) Soient z et z' deux éléments de $\mathbb{U}_{p^\infty}$. Alors $z^{p^n} = z'^{p^{n'}} = 1$ pour certains n et n' et donc $(zz')^{p^{\sup(n,n')}} = 1$. De plus, $z^{p^{n+1}} = 1$ prouve que $\mathbb{U}_{p^n} < \mathbb{U}_{p^{n+1}}$. Pour être plus concret, les premiers éléments de $\mathbb{U}_{2^\infty}$ sont :

$$\mathbb{U}_{2^\infty} = \{1, -1, i, -i, e^{i\pi/4}, e^{3i\pi/4}, e^{-i\pi/4}, e^{-3i\pi/4}, \ldots\}$$

où on s'est arrêté aux racines huitièmes. $\mathbb{U}_{p^\infty}$ est un sous-groupe multiplicatif du groupe des nombres complexes de module 1, noté $\mathbb{U}$.

3) On utilise le fait qu'un élément d'ordre p^k est une racine primitive p^k-ième de l'unité et donc engendre $\mathbb{U}_{p^k}$. Raisonnons par l'absurde, si la suite des ordres des éléments de $\mathbf{H}$ était infinie, pour tout élément z de $\mathbb{U}_{p^\infty}$ d'ordre p^k, il existerait un élément h de $\mathbf{H}$ d'ordre supérieur $p^{k'}$ et $\mathbf{H}$ contiendrait $\mathbb{U}_{p^{k'}}$ et donc z, $\mathbb{U}_{p^\infty}$ serait inclus dans $\mathbf{H}$ donc égal à $\mathbf{H}$. Si maintenant on choisit dans $\mathbf{H}$ un élément d'ordre maximum p^{k_0}, $\mathbf{H}$ est égal à $\mathbb{U}_{p^{k_0}}$ par le même argument. Les sous-groupes forment donc une chaîne ; c'est à cause de cette propriété qu'ils partagent avec les groupes cycliques $\mathbb{Z}/p^\alpha\mathbb{Z}$, que les groupes de Prüfer sont aussi appelés groupes **quasi-cycliques**.

4) Considérons l'application $z \mapsto z^{p^n}$, de $\mathbb{U}_{p^\infty}$ dans $\mathbb{U}_{p^\infty}$. C'est un morphisme de groupe, son noyau est $\mathbb{U}_{p^n}$ et elle est surjective ; tout élément de $\mathbb{U}_{p^\infty}$ est de la forme $e^{2\ell i\pi/p^k}$ et est l'image de $e^{2\ell i\pi/p^{k+n}}$. On en déduit l'isomorphisme demandé, tous les sous-groupes de $\mathbb{U}_{p^\infty}$ sont finis et d'indice infini.

5) Le groupe $\mathbb{U}$ des nombres complexes de module 1 est isomorphe au groupe additif $\mathbb{R}/2\pi\mathbb{Z}$ ou, ce qui revient au même, au groupe $\mathbb{R}/\mathbb{Z}$. Par cet isomorphisme, les éléments du p-groupe de Prüfer sont envoyés sur les classes de fractions de la forme $\frac{k}{p^n}$. Ces éléments forment donc un groupe isomorphe au p-groupe de Prüfer, parfois noté $(\mathbb{Q}/\mathbb{Z})_p$.

6) Prenons la notation additive. Pour définir un endomorphisme f de $\mathbb{U}_{p^\infty}$, il suffit de le définir pour les $\frac{1}{p^n}$. Posons donc :

$$f\left(\frac{1}{p^n}\right) = \frac{a_n}{p^n}$$

où a_n est dans $\{0, 1, \ldots, p^n - 1\}$. En effet, il est nécessaire que cette image g vérifie $p^n g = 0$ dans le groupe $(\mathbb{Q}/\mathbb{Z})_p$. Il faut néanmoins d'autres conditions pour que ce soit un morphisme ; on doit en effet avoir :

$$pf\left(\frac{1}{p^n}\right) = f\left(p\frac{1}{p^n}\right) = f\left(\frac{1}{p^{n-1}}\right)$$

ce qui donne :

$$p\frac{a_n}{p^n} - \frac{a_{n-1}}{p^{n-1}} \in \mathbb{Z} \iff a_n \equiv a_{n-1} \pmod{p^{n-1}}$$

À tout endomorphisme f, correspond donc une suite $(a_1, a_2, \ldots, a_n, \ldots)$, les entiers a_i pris dans $\{0, 1, \ldots, p^i - 1\}$ devant vérifier les congruences ci-dessus. Réciproquement, de telles suites donnent lieu à un endomorphisme de $\mathbf{G}$; ces suites sont en bijection avec l'anneau des **entiers p-adiques**.

7) Soient σ et σ' deux éléments de $\mathcal{S}_{(\mathbb{N})}$. Alors $\sigma \circ \sigma'$ est dans $\mathcal{S}_{(\mathbb{N})}$ puisque tous les entiers sont fixes à partir d'un certain rang.

8) Soit **H** l'ensemble des σ fixant tous les $i > n$. Alors, l'application restriction est un isomorphisme de **H** sur $\mathcal{S}_n$ et l'on fera l'identification. Par ailleurs, tout élément σ de $\mathcal{S}_{(\mathbb{N})}$ est dans un des $\mathcal{S}_n$, il suffit de prendre n tel que σ fixe tous les éléments supérieurs à n, et donc

$$\mathcal{S}_{(\mathbb{N})} = \bigcup_{n \geqslant 1} \mathcal{S}_n$$

9) Tout élément σ de $\mathcal{S}_{(\mathbb{N})}$ peut être considéré comme élément d'un des $\mathcal{S}_n$. On peut alors définir sa signature, mais il faut vérifier l'indépendance par rapport à n. Soit en effet $n' > n$, comme σ fixe tous les entiers entre n et n', le nombre k des orbites est augmenté de $n' - n$ et :

$$\varepsilon(\sigma) = (-1)^{n-k} = (-1)^{n'-k'}$$

La signature reste donc un morphisme, car deux permutations de $\mathcal{S}_{(\mathbb{N})}$ peuvent toujours être considérées comme un même élément d'un $\mathcal{S}_n$. On peut définir le groupe alterné $\mathcal{A}_{(\mathbb{N})}$, noyau de ce morphisme. Ce sera l'union de tous les groupes alternés $\mathcal{A}_n$.
Montrons que $\mathcal{A}_{(\mathbb{N})}$ est simple, ce sera un premier exemple de groupe simple infini. Soit **H** un sous-groupe normal de $\mathcal{A}_n$. Soit $i \geqslant 5$. Alors $\mathbf{H} \cap \mathcal{A}_i$ est soit réduit à e, soit égal à $\mathcal{A}_i$ puisque ce groupe est simple. Supposons que pour un indice i, cette intersection soit réduite à e. Alors si $x \in \mathbf{H}$ n'est pas dans $\mathcal{A}_i$, il est dans $\mathcal{A}_n$ pour $n > i$, mais alors $\mathbf{H} \cap \mathcal{A}_n$ n'est pas réduit à e, et $\mathcal{A}_n$ est inclus dans **H**, et donc $\mathcal{A}_i$ est inclus dans **H**, ce qui est absurde. Dans ce cas, **H** est réduit à e. L'alternative est que **H** contienne tous les $\mathcal{A}_n$ pour $n \geqslant 5$, et alors $\mathbf{H} = \mathcal{A}_{(\mathbb{N})}$. Remarquons que le raisonnement fonctionne pour un groupe qui est l'union d'une suite croissante de groupes dont une infinité est simple.

10) **K** est formé des $\prod_{i \in I} \tau_i$, où I est un sous-ensemble fini quelconque de $\mathbb{N}$. Ces éléments sont tous d'ordre deux, et **K** est commutatif puisque les générateurs τ_i sont des transpositions à supports disjoints.

3.5.1 Les groupes $\mathbf{GL}(n, \mathbb{K})$, $\mathbf{PGL}(n, \mathbb{K})$, $\mathbf{SL}(n, \mathbb{K})$, $\mathbf{PSL}(n, \mathbb{K})$

1) **Préliminaires**

a) Il suffit de dire que $\mathbf{SL}(n, \mathbb{K})$ est le noyau du morphisme déterminant :

$$\det : \mathbf{GL}(n, \mathbb{K}) \to \mathbb{K}^*$$

b) On a donc une suite exacte :

$$e \longrightarrow \mathbf{SL}(n, \mathbb{K}) \xrightarrow{i} \mathbf{GL}(n, \mathbb{K}) \xrightarrow{\det} \mathbb{K}^* \longrightarrow e$$

Pour montrer que c'est un produit semi-direct, il suffit de trouver un relèvement, l'ensemble des matrices de la forme

$$\begin{pmatrix} 1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 1 & \vdots \\ 0 & & & 0 & k \end{pmatrix}$$

avec k parcourant $\mathbb{K}^*$. Ces matrices forment bien un sous-groupe isomorphe à $\mathbb{K}^*$ et l'application s qui à k associe la matrice correspondante est bien une section, puisque le déterminant d'une de ces matrices est k.

> ***Remarque :*** Il arrive qu'on puisse choisir un relèvement tel que le produit soit direct ; il suffit pour cela de trouver une section à valeur dans le centre de $\mathbf{SL}(n, \mathbb{K})$. On associera à k la matrice scalaire dont tous les éléments diagonaux sont égaux à une des racines n-ièmes de k. Cela fonctionnera donc, en dimension impaire, pour le corps des réels, tout le temps pour le corps des complexes.

c) L'étude a été faite dans le premier problème. On trouve donc que le centre est formé des matrices scalaires qui sont dans $\mathbf{SL}(n, \mathbb{K})$, c'est-à-dire qui sont de la forme λI_n, où $\lambda^n = 1$.

d) Soit $A = (a_{ij})$ une matrice de $\mathbf{GL}(n, \mathbb{K})$ dont la classe $\overline{A}$ est dans le centre de $\mathbf{PGL}(n, \mathbb{K})$. Alors, pour toute matrice B inversible, $\overline{AB} = \overline{BA}$ soit $AB = \lambda BA$ pour un certain scalaire λ (qui dépend de B a priori). En prenant pour B une matrice de transvection, $T_{ij} = I + aE_{ij}$, où a est quelconque, on voit que A est diagonale. Le groupe $\mathbf{PGL}(n, \mathbb{K})$ est donc de centre trivial, et il en va de même pour $\mathbf{PSL}(n, \mathbb{K})$.

e) Une base étant choisie, il y a isomorphisme entre l'ensemble des matrices inversibles $\mathbf{GL}(n, \mathbb{K})$ et le groupe des automorphismes de l'espace vectoriel $\mathbb{K}^n$. On l'appelle également groupe linéaire, on le note $\mathbf{GL}(\mathbb{K}^n)$, et on le confond souvent avec le groupe des matrices inversibles.
$\mathbf{GL}(\mathbb{K}^n)$ agit sur l'ensemble des droites vectorielles par $g.D = g(D)$. Cette action n'est pas fidèle, son noyau est l'ensemble des endomorphismes g tels que $g(D) = D$ pour toute droite. On a alors $g(x) = \lambda_x x$ pour tout vecteur x, et en utilisant la linéarité, on peut montrer que λ_x est une constante ; le noyau de l'action ne contient donc que les homothéties, et c'est le centre de $\mathbf{GL}(n, \mathbb{K})$. On en déduit que l'action passe au quotient du groupe linéaire par son centre. Cette action est transitive, car deux droites étant données, il existe toujours une application linéaire transformant un vecteur non nul de l'une, en un vecteur non nul de l'autre ; il suffit de compléter chacun de ces vecteurs en une base. De plus, on peut imposer que le déterminant de cette application linéaire soit 1, en multipliant au besoin l'image d'un vecteur par un scalaire. Ainsi, le groupe $\mathbf{PSL}(n, \mathbb{K})$ agit aussi sur l'ensemble des droites, fidèlement et transitivement. Cette action est à la base d'une démonstration de la simplicité de (presque) tous les groupes $\mathbf{PSL}(n, \mathbb{K})$, voir les problèmes de la section 6.3 (chapitre 6).

2) **Calculs des cardinaux ; premiers cas particuliers**

a) Un automorphisme de $\mathbb{K}^n$ est déterminé par l'image de la base canonique, image qui doit être une base. Il y a donc $q^n - 1$ choix pour l'image du premier vecteur, car on n'exclut que le vecteur nul. Pour le suivant, il faut exclure les vecteurs colinéaires au premier vecteur qui sont sur une droite de cardinal q. Dans le cas suivant, il faudra exclure les vecteurs d'un plan, q^2 éléments. Ainsi :

$$|\mathbf{GL}(n, \mathbb{K})| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Le centre, formé des homothéties, est de cardinal $q - 1$ d'où :

$$|\mathbf{PGL}(n, \mathbb{K})| = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{q - 1}$$

Enfin, comme $\mathbf{SL}(n, \mathbb{K})$ est d'indice $q-1$, il a même cardinal.

b) $x \in \mathbb{K}^*$ vérifie $x^n = 1$ s'il est dans le groupe cyclique $\mathbb{K}^*$ d'ordre $q-1$, et si son ordre divise n. Si $d = n \wedge (q-1)$, on a $x^d = 1$ (puisque d est combinaison de n et de $q-1$), et tout x vérifiant $x^d = 1$ est aussi solution de $x^n = 1$. L'étude des sous-groupes des groupes cycliques nous a montré qu'il y a exactement d solutions. Le centre de $\mathbf{SL}(n, \mathbb{K})$ est formé des homothéties de rapport x vérifiant $x^n = 1$. On en déduit que :

$$|\mathbf{PSL}(n, \mathbb{K})| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-1})}{(q-1)d}$$

c) • Pour $n = 2$, on obtient la table suivante (en indexant les colonnes par le cardinal du corps) :

	2	3	4	5	7	8	9
$\lvert\mathbf{GL}\rvert$	6	48	180	480	2016	3528	5760
$\lvert\mathbf{PGL}\rvert = \lvert\mathbf{SL}\rvert$	6	24	60	120	336	504	720
$\lvert\mathbf{PSL}\rvert$	6	12	60	60	168	504	360

• Pour $n = 3$

*	2	3	4
$\lvert\mathbf{GL}\rvert$	168	11232	181440
$\lvert\mathbf{PGL}\rvert = \lvert\mathbf{SL}\rvert$	168	5616	60480
$\lvert\mathbf{PSL}\rvert$	168	5616	20160

• Pour $n = 4$, contentons-nous de :

$$|\mathbf{PSL}(4, \mathbb{F}_2)| = 20160$$

On constate quelques coïncidences,

$$|\mathbf{PSL}(2, \mathbb{F}_4)| = |\mathbf{PSL}(2, \mathbb{F}_5)|$$
$$|\mathbf{PSL}(3, \mathbb{F}_2)| = |\mathbf{PSL}(2, \mathbb{F}_7)|$$
$$|\mathbf{PSL}(3, \mathbb{F}_4)| = |\mathbf{PSL}(4, \mathbb{F}_2)|$$

À part dans le dernier cas, ces égalités correspondent à des groupes isomorphes.

d) On se place donc dans le cas du corps $\mathbb{F}_2 = \{0, 1\}$ à deux éléments, le seul élément non nul étant 1, une matrice est inversible ssi son déterminant est 1. De plus, la seule homothétie est l'identité, d'où :

$$\mathbf{GL}(n, \mathbb{F}_2) \cong \mathbf{SL}(n, \mathbb{F}_2) \cong \mathbf{PGL}(n, \mathbb{F}_2) \cong \mathbf{PSL}(n, \mathbb{F}_2)$$

e) Il y a $2^2 - 1 = 3$ vecteurs non nuls dans ce plan, et ils sont non colinéaires. On en déduit que $\mathbf{PSL}(2, \mathbb{F}_2)$ agit sur un ensemble de trois éléments. Mais cette action est fidèle, donc $\mathbf{PSL}(2, \mathbb{F}_2)$ s'identifie à un sous-groupe de $\mathcal{S}_3$. Comme il a même cardinal, il est isomorphe à $\mathcal{S}_3$; pour concrétiser cet isomorphisme, il faut choisir un ordre dans les trois droites, par exemple $\mathrm{Vect}(e_1)$, $\mathrm{Vect}(e_2)$, $\mathrm{Vect}(e_1 + e_2)$ et l'image de la transposition $(1, 2)$ sera la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, tandis que la permutation $(1, 2, 3)$ correspondra à la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. On a donc l'isomorphisme :

$$\mathbf{PGL}(2, \mathbb{F}_2) \cong \mathbb{S}_3$$

f) La première chose qu'on peut dire de ce groupe, est qu'il est d'ordre $168 = 2^3 \times 3 \times 7 \ldots$ Nous verrons plus tard que c'est un groupe simple, mais on peut commencer par dire :

- qu'agissant fidèlement sur $\mathbb{P}^2(\mathbb{F}_2)$ qui a 7 éléments, c'est un sous-groupe de $\mathcal{S}_7$.
- Un 2-Sylow a huit éléments. Donc un 2-Sylow particulier sera le groupe des matrices triangulaires supérieures $\mathbf{T}(3,2)$ (qui coïncide d'ailleurs avec $\mathbf{TU}(3,2)$).
- On peut déterminer le nombre des 2-Sylow en calculant le normalisateur de ce 2-Sylow particulier, on voit facilement qu'il vaut encore $\mathbf{T}(3,2)$ d'indice 21 ; il y a vingt-et-un 2-Sylow. Il est possible de le voir géométriquement, en observant que notre 2-Sylow est le stabilisateur d'une paire de points du plan projectif, qu'il y a 21 paires de points, et que le groupe agit transitivement sur les paires de points.

3) **Autres cas particuliers. $\mathbf{GL}(2,\mathbb{F}_3)$, $\mathbf{GL}(2,\mathbb{F}_4)$, $\mathbf{GL}(2,\mathbb{F}_5)$**

a) Dans le plan vectoriel $(\mathbb{F}_3)^2$, il y a quatre droites, puisque tout vecteur non nul (il y en a huit) engendre une droite et chaque droite contient deux vecteurs non nuls. En général, le même raisonnement montre que $(\mathbb{F}_q)^2$ contient $q+1$ droites, donc $\mathbb{P}^1(\mathbb{F}_q)$ a $q+1$ éléments. Le groupe $\mathbf{GL}(2,\mathbb{F}_3)$ agit sur l'ensemble des quatre droites, le noyau de l'action est formé des homothéties, $\mathbf{PGL}(2,\mathbb{F}_3)$ agit donc fidèlement et s'identifie à un sous-groupe de $\mathcal{S}_4$. Mais comme il a même cardinal, il est isomorphe à $\mathcal{S}_4$:

$$\mathbf{PGL}(2,\mathbb{F}_3) \cong \mathcal{S}_4$$

b) $\mathbf{SL}(2,\mathbb{F}_3)$ a même cardinal que $\mathbf{PGL}(2,\mathbb{F}_3)$ et pourtant ces deux groupes ne sont pas isomorphes. $\mathbf{SL}(2,\mathbb{F}_3)$ agit transitivement sur l'ensemble des quatre droites, et le noyau est formé des matrices I et $-I$, les deux homothéties qui sont de déterminant 1. L'image de l'action est le seul sous-groupe d'indice 2 de $\mathcal{S}_4$, donc $\mathcal{A}_4$. On a alors une suite exacte :

$$e \longrightarrow \mathbb{Z}/2 \xrightarrow{i} \mathbf{SL}(2,\mathbb{F}_3) \xrightarrow{\phi} \mathcal{A}_4 \longrightarrow e$$

et l'on en déduit l'isomorphisme :

$$\mathbf{PSL}(2,\mathbb{F}_3) \cong \mathcal{A}_4$$

Quant à $\mathbf{SL}(2,\mathbb{F}_3)$, il n'est pas isomorphe à $\mathcal{S}_4$, ne serait-ce que parce que son centre est non trivial (c'est $\pm I$), c'est le **groupe binaire tétraédral** que nous retrouverons dans un des problèmes du dernier chapitre, et que nous avons déjà rencontré dans l'exercice 2.2.14

c) $\mathbf{PGL}(2,\mathbb{F}_4)$ agit fidèlement et transitivement sur l'ensemble des 5 droites de $(\mathbb{F}_4)^2$; comme son cardinal est 60, il est isomorphe au seul groupe d'indice 2 de $\mathcal{S}_5$, c'est-à-dire $\mathcal{A}_5$:

$$\mathbf{PGL}(2,\mathbb{F}_4) \cong \mathcal{A}_5$$

Dans le corps $\mathbb{F}_4$, la seule solution de $x^2 = 1$ est 1, donc le centre de $\mathbf{SL}(2,\mathbb{F}_4)$ est trivial ; comme $\mathbf{PSL}(2,\mathbb{F}_4)$ agit fidèlement sur l'ensemble des 5 droites, on a les isomorphismes :

$$\mathbf{PSL}(2,\mathbb{F}_4) \cong \mathbf{SL}(2,\mathbb{F}_4) \cong \mathcal{A}_5$$

d) Cette fois, $\mathbf{PGL}(2,\mathbb{F}_5)$ agit fidèlement et transitivement sur un ensemble de 6 droites, donc est isomorphe à un sous-groupe de $\mathcal{S}_6$. Comme il est de cardinal 120, c'est un sous-groupe d'indice 6, dont on sait qu'il est isomorphe à $\mathcal{S}_5$. On a donc :

$$\mathbf{PGL}(2,\mathbb{F}_5) \cong \mathcal{S}_5$$

Enfin, $\mathbf{PSL}(2,\mathbb{F}_5)$ s'identifiant à un sous-groupe du précédent et étant de cardinal 60 est isomorphe à $\mathcal{A}_5$. Remarquons que ce sous-groupe n'est pas le stabilisateur d'un point puisqu'il agit transitivement sur l'ensemble des six droites.

e) Le cardinal de $\mathbf{GL}(n,\mathbb{F}_p)$ est :

$$(p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = p^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(p^i-1)$$

on en déduit qu'un p-Sylow a $p^{\frac{n(n-1)}{2}}$ éléments. Or, le groupe $\mathbf{TU}(n,\mathbb{F}_p)$ a exactement ce nombre d'éléments, il suffit de compter les cases libres dans une matrice, sachant qu'elle est triangulaire supérieure et que la diagonale est remplie de 1. En utilisant le fait que le normalisateur de ce groupe est $\mathbf{T}(n,\mathbb{F}_p)$, on peut compter les p-Sylow :

$$\frac{\prod_{i=1}^{n}(p^i-1)}{(p-1)^n}$$

Ainsi, dans le cas de $\mathbf{GL}(2,\mathbb{F}_3)$, il y a quatre 3-Sylow.

3.5.2 Produits semi-directs en géométrie

1) **Le groupe affine**

a) L'application **dir** qui, à toute application affine f, associe sa direction $\overrightarrow{f}$ a pour noyau l'ensemble des translations. Les translations forment donc un sous-groupe normal dans le groupe affine et l'on a la suite exacte :

$$id \longrightarrow \mathcal{T}(\mathcal{E}) \xrightarrow{i} \mathbf{GA}(\mathcal{E}) \xrightarrow{\mathbf{dir}} \mathbf{GL}(\mathbb{E}) \longrightarrow id$$

puisque l'application **dir** est surjective.

b) Il faut trouver un relèvement du groupe linéaire dans le groupe affine ; choisissant un point A, l'ensemble des applications affines fixant A convient, on le note $\mathbf{GA}_A(\mathcal{E})$. On a donc un produit semi-direct :

$$\mathbf{GA}(\mathcal{E}) = \mathcal{T}(\mathcal{E}) \rtimes \mathbf{GA}_A(\mathcal{E})$$

La décomposition d'une application affine f s'écrit alors :

$$f = t_{\vec{u}} \circ g$$

où $\vec{u}$ est le vecteur $\overrightarrow{Af(A)}$ et où g fixe A, en ayant la même direction que f. La composition des applications affines se fait suivant la règle :

$$f \circ f' = t_{\vec{u}} \circ g \circ t_{\vec{u}'} \circ g' = t_{\vec{u}} \circ \left(g \circ t_{\vec{u}'} \circ g^{-1}\right) \circ g \circ g' = t_{\vec{u}} \circ t_{\vec{g}(\vec{u}')} \circ g \circ g'$$

Enfin, comme le groupe des translations est isomorphe à l'espace vectoriel $\mathbb{E}$ (en tant que groupe additif), on peut donner une vision « externe » de ce produit semi-direct :

$$\mathbf{GA}(\mathcal{E}) = \mathbb{E} \rtimes \mathbf{GL}(\mathbb{E})$$

où l'action est l'action naturelle du groupe linéaire sur l'espace vectoriel, comme le montre le calcul ci-dessus.

c) Écrivons :

$$M = \begin{pmatrix} \mathcal{M} & U \\ 0 & 1 \end{pmatrix}$$

où U est la matrice colonne du vecteur $\overrightarrow{OO'}$, et 0 désigne une matrice ligne formée de 0. Alors, le produit matriciel $X' = MX$ se ramène au système :

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \mathcal{M} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

donnant les expressions analytiques d'une application affine. De plus, la matrice du composé de deux applications affines est le produit des matrices de chaque application affine, puisque :

$$MM' = \begin{pmatrix} \mathcal{M} & U \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathcal{M}' & U' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathcal{M}\mathcal{M}' & U + \mathcal{M}U' \\ 0 & 1 \end{pmatrix}$$

où on retrouve les formules du produit semi-direct vues ci-dessus. On constate ainsi que le groupe affine de dimension n se plonge dans le groupe linéaire de dimension $n+1$, ce qui se comprend très bien quand on fait un peu de géométrie projective.

d) Rappelant que le groupe des homothéties-translations est la réunion du groupe des translations et de l'ensemble des homothéties, on est conduit par les mêmes observations que ci-dessus, à la suite exacte :

$$id \longrightarrow \mathcal{T}(\mathcal{E}) \xrightarrow{i} \mathcal{HT}(\mathcal{E}) \xrightarrow{r} \mathbb{K}^* \longrightarrow id$$

où r est le morphisme qui, à une homothétie, associe son rapport (et à une translation associe 1). Cette suite exacte est scindée, un relèvement étant le groupe des homothéties de même centre. Le groupe des homothéties-translations peut donc s'écrire comme produit semi-direct :

$$\mathcal{HT}(\mathcal{E}) = \mathbb{E} \rtimes \mathbb{K}^*$$

e) Lorsque le corps de base $\mathbb{K}$ est un corps fini, les groupes affines sont finis. En dimension un, ils sont engendrés par la translation de 1, et l'homothétie de centre 0 et rapport r où r est un générateur de $\mathbb{K}^*$. On trouve donc la présentation :

$$\mathbf{GA}(1, \mathbb{F}_q) = \langle a, b \mid a^q = b^{q-1} = 1,\ bab^{-1} = a^r \rangle$$

Pour $q = 2, 3, 4, 5$, on retrouve les groupes $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{A}_4 = (\mathbb{Z}/2)^2 \rtimes \mathbb{Z}/3$. Dans le dernier cas, par exemple, il y a quatre translations qui forment un groupe de Klein et qui échangent les quatre points par doubles transpositions. Les homothéties sont, elles, d'ordre trois. Le groupe affine de $\mathbb{F}_5$ est un groupe métacyclique à 20 éléments. C'est un sous-groupe de $\mathcal{S}_5$.

En dimension deux, lorsque q est un nombre premier, les groupes affines $\mathbf{GA}(2, \mathbb{F}_q)$ ont $q^2(q^2-1)(q^2-q)$ éléments et ainsi de suite. Ainsi $\mathbf{GA}(2, \mathbb{F}_2)$ a 24 éléments. Comme c'est un sous-groupe de $\mathcal{S}_4$, il coïncide avec $\mathcal{S}_4$.

On a déjà observé que le groupe des automorphismes du groupe $(\mathbb{Z}/p)^n$ coïncide avec le groupe linéaire de ce groupe, considéré comme espace vectoriel ; le produit semi-direct qu'est le groupe affine coïncide donc avec l'holomorphe de $(\mathbb{Z}/p)^n$. Cela ne marche

plus dans le cas de $\mathbb{F}_q$, mais le même argument montre que :

$$\mathrm{Hol}(\mathbb{F}_{p^m}) \cong \mathbf{GA}(m, \mathbb{F}_p)$$

2) **Le groupe orthogonal**

a) Une matrice orthogonale est inversible (puisque d'inverse sa transposée). De plus,

$$(OO')^t(OO') = OO'^tO'^tO = I \text{ et } O^{-1t}O^{-1} = 1$$

montrent que l'ensemble des matrices orthogonales est bien un groupe.
En dimension 1, $\mathbf{O}(n, \mathbb{R}) = \{+1, -1\}$ et en dimension 2, le groupe orthogonal est constitué des matrices de la forme :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ ou } \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \text{ avec } a^2 + b^2 = 1$$

b) La formule ${}^tOO = I$ prouve que $\det(O)^2 = 1$, puisque $\det({}^tO) = \det(O)$. Il existe des matrices orthogonales de déterminant 1 et de déterminant -1 (penser à des matrices diagonales) ; on en déduit qu'il y a une suite exacte :

$$id \longrightarrow \mathbf{SO}(n, \mathbb{R}) \xrightarrow{i} \mathbf{O}(n, \mathbb{R}) \xrightarrow{\det} \{+1, -1\} \longrightarrow 1$$

Le groupe spécial orthogonal est un noyau, donc normal dans le groupe orthogonal ; c'est le groupe des matrices orthogonales de déterminant +1, qu'on appelle aussi matrices orthogonales directes. Pour voir si la suite exacte est scindée, il faut trouver un relèvement, donc un sous-groupe du groupe orthogonal d'ordre 2, contenant l'identité et une involution de déterminant -1, il suffit de prendre par exemple la matrice d'une réflexion. Le produit sera direct s'il existe un relèvement normal ; mais cela n'est possible que si l'involution est dans le centre du groupe orthogonal. Il en résulte que seule $-I$ convient, et elle ne sera de déterminant -1 qu'en dimension impaire, seul cas où le groupe orthogonal est produit direct du groupe spécial orthogonal et de $\mathbb{Z}/2$.

c) Un simple calcul de produit de matrices montre que $\mathbf{SO}(2, \mathbb{R})$ est commutatif. On a d'ailleurs les isomorphismes :

$$\mathbf{SO}(2, \mathbb{R}) \cong \mathbb{U} \cong \mathbb{R}/2\pi\mathbb{Z} \cong \mathcal{A}$$

où $\mathbb{U}$ est le groupe (multiplicatif) des nombres complexes de module 1, et $\mathcal{A}$ le groupe (additif) des angles orientés de vecteurs. Les éléments de $\mathbf{SO}(2, \mathbb{R})$ sont appelés **rotations**, on peut leur associer bijectivement un angle.

Une autre méthode maintenant, on vérifie que les matrices de la forme $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ avec $a^2 + b^2 = 1$ sont involutives. Soit r une rotation, et s une involution. Alors $r \circ s = s'$ d'où $r = s' \circ s$; toute rotation est produit de deux involutions dont l'une est arbitraire. On en déduit $s \circ r \circ s^{-1} = s \circ (r \circ s) = s \circ s' = r^{-1}$, puis

$$\rho \circ r \circ \rho^{-1} = \sigma \circ \sigma' \circ r \circ \sigma' \circ \sigma = r$$

qui montre à nouveau que deux rotations commutent. On « comprend » également pourquoi ce phénomène ne se poursuit pas, dès la dimension 3, il n'y a pas que des involutions dans $\mathbf{O}(n, \mathbb{R}) \setminus \mathbf{SO}(n, \mathbb{R})$.

d) Les sous-groupes finis de $\mathbf{SO}(2, \mathbb{R})$ peuvent être déterminés de la façon suivante. Un sous-groupe d'ordre n a des éléments x qui vérifient tous $x^n = 1$. Ils sont tous dans le groupe des racines n-ièmes de l'unité qui est cyclique d'ordre n.

Conclusion. Les sous-groupes finis de $\mathbf{SO}(2,\mathbb{R})$ sont les groupes cycliques $\mathbb{Z}/n$.
Les groupes finis de $\mathbf{O}(2,\mathbb{R})$ sont d'abord ceux qu'on vient de décrire, les groupes cycliques qui sont inclus dans le groupe spécial orthogonal. Soit $\mathbf{G}$ un sous-groupe fini quelconque du groupe orthogonal, mais qui n'est pas inclus dans le groupe spécial orthogonal. Alors $\mathbf{G}^+ = \mathbf{G} \cap \mathbf{SO}(2,\mathbb{R})$ est cyclique d'ordre n, et la restriction de la suite exacte ci-dessus s'écrit :

$$id \longrightarrow \mathbf{G}^+ \xrightarrow{i} \mathbf{G} \xrightarrow{\det} \{+1,-1\} \longrightarrow 1$$

Mais cette suite exacte est scindée puisque tous les éléments de $\mathbf{G} \setminus \mathbf{G}^+$ sont des involutions et permettent de faire un relèvement. De plus, le groupe des rotations est cyclique, l'action est donnée par $s \circ r \circ s^{-1} = r^{-1}$, on reconnaît le groupe diédral $\mathbb{D}_{2n}$.

e) L'ensemble des quaternions unitaires est un groupe puisque $|qq'| = |q||q'|$ et $|q^{-1}| = |q|^{-1}$, en notant $|q|$ la norme d'un quaternion définie par :

$$|q| = \sqrt{\alpha^2 + \beta^2 + \gamma^2 + \delta^2} = \sqrt{q\overline{q}}$$

Le groupe des quaternions unitaires contient bien sûr le groupe quaternionique $\mathbb{H}_8$. Nous le noterons S^3 car il est en bijection avec la sphère $S^3 \subset \mathbb{R}^4$ qui est donc munie ainsi d'une structure de groupe. Dans sa version matricielle, on le note $\mathbf{SU}(2)$[1]. Remarquons enfin que q est unitaire ssi $q^{-1} = \overline{q}$.

f) Un quaternion pur est caractérisé par $\overline{z} = -z$. On voit donc que si $z \in \mathbb{E}$, alors

$$\overline{qzq^{-1}} = \overline{q^{-1}}\,\overline{z}\,\overline{q} = -qzq^{-1}$$

et qzq^{-1} est dans $\mathbb{E}$. De plus, $z \mapsto qzq^{-1}$ est $\mathbb{R}$-linéaire.

$$|qzq^{-1}|^2 = \overline{q^{-1}}\,\overline{z}\,\overline{q}qzq^{-1} = q|z|^2q^{-1} = |z|^2$$

puisque $|z|^2$ réel commute avec q ; et $\phi(q)$ est une isométrie, car la norme d'un quaternion pur correspond bien à la norme dans l'espace euclidien $\mathbb{E}$ tel que nous l'avons défini. Reste à montrer que l'on arrive dans le groupe des rotations. Pour cela, on peut commencer par remarquer que le produit de deux quaternions purs s'écrit :

$$zz' = -\langle z|z'\rangle + z \wedge z'$$

et qu'un quaternion unitaire peut s'écrire $q = a + u$ où a est réel, u un quaternion pur. On a alors :

$$\begin{aligned} qzq^{-1} &= (a+u)z(a-u) \\ &= a^2z + a(uz - zu) - uzu \\ &= (a^2 - \langle u|u\rangle)z - 2a(u \wedge z) + 2\langle z|u\rangle u \end{aligned}$$

où on a utilisé la formule précédente ainsi que les propriétés du produit vectoriel. Détaillons quand même le calcul de uzu :

$$\begin{aligned} uzu &= (-\langle u|z\rangle + u \wedge z)u \\ &= -\langle u|z\rangle u + (u \wedge z) \wedge u \\ &= -\langle u|z\rangle u + \langle u|u\rangle z - \langle u|z\rangle u \\ &= -2\langle u|z\rangle u + \langle u|u\rangle z \end{aligned}$$

1. Groupe spécial unitaire formé des matrices unitaires de déterminant 1. Ces matrices s'écrivent $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ où $|a|^2 + |b|^2 = 1$, voir 2.3.3.

On a appliqué la formule du double produit vectoriel que l'on trouve dans tous les livres de géométrie. Comme q est un quaternion pur, on peut poser $a = \cos\theta$ et $u = \sin\theta v$ où v est un vecteur unitaire. On obtient :

$$qzq^{-1} = (\cos 2\theta)z + (1 - \cos 2\theta)\langle v|z\rangle v + (\sin 2\theta)v \wedge z$$

dont on vérifie qu'il correspond à l'image de z par la rotation d'axe orienté par v et d'angle 2θ. Voir, par exemple, [25]. Notre calcul prouve également la surjectivité. Chercher le noyau, revient à chercher le centralisateur des éléments de $\mathbb{E}$. Or, le calcul montre que le centralisateur de i est Vect$(1, i)$ et, de même, pour j et k. Le centralisateur de $\mathbb{E}$ tout entier est formé des réels, ce qui donne deux quaternions purs ± 1, toute rotation correspond à deux quaternions unitaires opposés, soit deux points antipodaux sur la sphère S^3. On a donc une suite exacte :

$$e \longrightarrow \mathbb{Z}/2 \xrightarrow{i} S^3 \xrightarrow{\phi} \mathbf{SO}(3,\mathbb{R}) \longrightarrow 1$$

g) Cette suite exacte n'est pas scindée ; en effet, si l'on considère $i \in S^3$, son image est un demi-tour, celui d'axe Vect(i), d'ordre 2. Il ne peut être « relevé » dans S^3 que par i ou $-i$ qui sont d'ordre quatre, il n'existe donc pas de section.

3) **Le groupe des isométries**

a) On a encore une suite exacte

$$id \longrightarrow I^+(\mathcal{E}) \xrightarrow{i} I(\mathcal{E}) \xrightarrow{\det} \{+1, -1\} \longrightarrow 1$$

et cette suite est scindée, un relèvement s'obtient avec une involution de déterminant négatif, par exemple une réflexion :

$$I(\mathcal{E}) = I^+(\mathcal{E}) \rtimes \mathbb{Z}/2$$

On peut vérifier qu'on ne peut obtenir un produit direct dès la dimension 2.

b) Cette fois la suite exacte s'écrit :

$$id \longrightarrow \mathcal{T}(\mathcal{E}) \xrightarrow{i} I^+(\mathcal{E}) \xrightarrow{\text{dir}} \mathbf{SO}(\mathbb{E}) \longrightarrow 1$$

C'est encore une suite exacte, comme dans le cas du groupe affine ; un relèvement est constitué de l'ensemble des isométries qui conservent un point donné. Le groupe des translations est également normal dans le groupe des isométries tout entier.

c) Soit $\mathbf{G}$ un groupe fini d'isométries. Si A est un point quelconque, l'orbite de A sous l'action de $\mathbf{G}$ est un ensemble fini de points, stable par tout élément g de $\mathbf{G}$. Mais alors, l'isobarycentre des points de cet ensemble est stable par g ; les éléments de $\mathbf{G}$ ont (au moins) un point invariant commun. L'étude des sous-groupes finis de $I(\mathcal{E})$ est ainsi ramenée à l'étude des sous-groupes finis de $\mathbf{O}(\mathbb{E})$. En dimension 2, on a donc les groupes diédraux qui sont les groupes d'isométries conservant un polygone régulier et les groupes cycliques, qu'on peut voir comme les groupes d'isométries conservant un polygone régulier avec des côtés orientés (dans le même sens).

4.4.1 Groupes commutatifs définis par générateurs et relations

1) Premiers exemples

a) Tout élément de $\mathbf{G}$ s'écrivant comme composé d'éléments de X ou de leurs inverses, il suffit de remarquer que si x et y commutent, leurs inverses commutent également. Réciproquement, on sait déjà que tout groupe admet une présentation par générateurs et relations, et il suffit d'ajouter les relations $x + y = y + x$ si le groupe est commutatif. Une façon alternative de voir les choses est de partir d'un groupe commutatif libre, engendré par les éléments de X, donc de la forme :

$$\bigoplus_{x \in X} \mathbb{Z}_x$$

où $\mathbb{Z}_x$ est une copie de $\mathbb{Z}$ indexée par x, et de quotienter ce groupe par le groupe des relations.

b) Le groupe $\langle a| \ \rangle$ est monogène infini, isomorphe à $\mathbb{Z}$, et bien sûr commutatif. De même, $\text{grab}\langle a|\ 5a = 0\rangle$ est monogène engendré par un élément d'ordre 5, il est isomorphe à $\mathbb{Z}/5$. Enfin, $\mathbf{K} = \text{grab}\langle a, b \mid 5a = 0,\ 7b = 0\rangle$ contient le sous-groupe engendré par a, d'ordre 5, le sous-groupe engendré par b, d'ordre 7. Ces deux groupes sont normaux, puisque $\mathbf{K}$ est abélien, ils commutent et leur intersection est nulle, $\mathbf{K}$ est isomorphe au produit direct $\mathbb{Z}/5 \times \mathbb{Z}/7 \cong \mathbb{Z}/35$. Remarquons le contraste avec le cas non commutatif, où le groupe de présentation

$$\mathbf{K}' = \langle a, b \mid a^5 = b^7 = 1\rangle$$

est infini.

c) i) On remarque que

$$\begin{aligned} p^n x_n - x_0 &= p^{n-1}(px_n - x_{n-1}) + p^{n-2}(px_{n-1} - x_{n-2}) \\ &\quad + \ldots + (px_1 - x_0) \\ &= \textstyle\sum_{i=0}^{n-1} p^i(px_{i+1} - x_i) \end{aligned}$$

et $S_2 < S_3$. L'inclusion est stricte car $px_2 - x_1 \notin S_3$, si

$$px_2 - x_1 = m_0 px_0 + m_1(px_1 - x_0) + \ldots$$

alors, par identification dans le groupe libre engendré par les x_i, $p = m_2 p^2$ et $-1 = m_1 p$, m_1 et m_2 sont nuls, de même que tous les autres coefficients.
De la même façon, $S_1 < S_2$ puisque :

$$p^{n+1} x_n = p(p^n x_n - x_0) + px_0$$

et l'inclusion est bien stricte car $px_1 - x_0$ n'est pas dans le groupe engendré par les $p^{k+1}x_k$, voir le coefficient de x_0.
Des inclusions $S_1 < S_2 < S_3$, on déduit, par le théorème de Von Dyck, qu'il existe des morphismes surjectifs de $\mathbf{G}_3$ sur $\mathbf{G}_2$ et de $\mathbf{G}_2$ sur $\mathbf{G}_1$, donc que $\mathbf{G}_3$ est isomorphe à un quotient de $\mathbf{G}_2$ et $\mathbf{G}_2$ est isomorphe à un quotient de $\mathbf{G}_1$.

ii) Dans le cas du groupe $\mathbf{G}_1$, chaque relation ne concerne qu'un générateur, et le groupe des relations peut donc s'écrire :

$$S_1 = \mathbb{Z}px_0 \oplus \mathbb{Z}p^2 x_1 \oplus \ldots \oplus \mathbb{Z}p^{n+1} x_n \oplus \ldots$$

et donc le quotient du groupe commutatif libre engendré par ces relations est

$$\mathbf{G}_1 = \mathbb{Z}/p \oplus \mathbb{Z}/p^2 \oplus \ldots \oplus \mathbb{Z}/p^{n+1} \oplus \ldots$$

iii) Nous allons montrer que $\mathbf{G}_3$ est isomorphe au p-groupe de Prüfer. Notons $\bar{x}_k$ la classe de x_k et définissons un morphisme f de $\mathbf{G}_3$ sur $(\mathbb{Q}/\mathbb{Z})_p$ par :

$$f(\bar{x}_k) = \frac{1}{p^k}$$

L'existence de ce morphisme est assurée par le théorème de Von Dyck (*cf.* 2.2.11) puisque, dans le groupe de Prüfer :

$$p\frac{1}{p} = 0 \quad \text{et} \quad p\frac{1}{p^{k+1}} = \frac{1}{p^k}$$

(on a noté une fraction comme sa classe d'équivalence). Le morphisme est surjectif, il faut montrer qu'il est injectif, si $x \in \mathbf{G}_3$ s'écrit

$$x = \sum_{i=0}^{n} a_k \bar{x}_k$$

où les a_k sont des entiers, les relations permettent de le simplifier en $x = a\bar{x}_n$ où a est entier. S'il est dans le noyau, a doit être multiple de p^n, d'où $x = 0$ puisque les relations de $\mathbf{G}_3$ impliquent $p^n\bar{x}_n = 0$.

2) Cas fini

a) Un groupe abélien de type fini est engendré par un nombre fini d'éléments, donc est quotient d'un groupe abélien libre de type fini, c'est-à-dire quotient de $\mathbb{Z}^n$ par un de ses sous-groupes. Remarquons que la restriction donnée par l'énoncé (nombre fini de relations) n'est pas utile, un sous-groupe d'un groupe abélien libre de type fini est toujours abélien libre de type fini (*cf.* 4.2.9), donc le groupe des relations a toujours un nombre fini de générateurs.

b) – Échanger ligne ou colonne revient à permuter les (e_i) ou les (f_j).

– L'opération décrite revient à remplacer e_j par $e_j - ae_i$, le système de vecteurs obtenu reste une base de $\mathbb{Z}^n$.

– Le même type d'opération sur les colonnes fait subir une transformation analogue sur les (f_j), le nouveau système restant une base de $\mathbf{H}$.

– Cette transformation équivaut à un changement de signe d'un des vecteurs de la base de $\mathbb{Z}_n$ ou de la base de $\mathbf{H}$.

c) On a donc au départ une matrice adaptée qui est une colonne. S'il y a au moins deux coefficients non nuls, une succession d'opérations sur les lignes peut faire apparaître le pgcd de ces deux entiers, puis avec les autres coefficients non nuls le pgcd d de tous les éléments de la colonne. Les mêmes opérations, plus des permutations et des changements de signes permettent alors de mettre à zéro tous les éléments de la colonne sauf celui contenant d. En notant (e'_i) la base de $\mathbb{Z}^n$ obtenue à la suite de ces opérations :

$$\bigoplus_{i=1}^{n} \mathbb{Z}e'_i/\mathbb{Z}de'_1 \cong \mathbb{Z}/d \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$$

Si $d = 1$, cela signifie que f_1 est vecteur d'une base de $\mathbb{Z}^n$, et que le quotient est isomorphe à $\mathbb{Z}^{n-1}$.

d) Dans le cas général, il faut procéder colonne après colonne de la façon suivante. Soit d_1 le pgcd de tous les coefficients de la matrice adaptée. On commence, en faisant des opérations sur les lignes, par mettre la première colonne sous la forme obtenue ci-dessus, avec en première position m_1 pgcd des éléments de la première colonne. Si m_1 est égal à d_1, des opérations sur les colonnes permettent de mettre la matrice sous la forme :

$$\begin{pmatrix} d_1 & 0 \\ 0 & M \end{pmatrix}$$

où 0 représente une ligne ou colonne nulle ; il suffit alors de continuer avec la matrice M, on obtient la forme désirée. Remarquons, en passant, qu'il ne peut y avoir de colonne nulle, le nombre de vecteurs dans une base de $\mathbf{H}$ est constant.
Si maintenant m_1 n'est pas égal à d_1, on s'y ramène ainsi ; il existe au moins une ligne dont m_1 ne divise pas tous les éléments ; si ce n'est pas la première, en faisant une combinaison de cette ligne avec la première, on obtient une première ligne avec m_1 et des éléments non tous divisibles par m_1. Par des manipulations de colonnes, on peut mettre en tête de cette ligne le pgcd de ses éléments, m_1' qui est strictement plus petit que m_1, et des zéros sur le reste de la ligne. Si m_1' n'est pas d_1, on recommence en revenant cette fois à la première colonne... Mais ce chassé-croisé doit se terminer car la suite m_1, m_1' est strictement décroissante.

e) En notant (e_i') la nouvelle base de $\mathbb{Z}^n$, la base de $\mathbf{H}$ est de la forme $(d_i e_i')$ pour i allant de 1 à k et :

$$\bigoplus_{i=1}^{n} \mathbb{Z}e_i'/\mathbb{Z}d_1e_1' \oplus \mathbb{Z}d_2e_2' \oplus \ldots \oplus \mathbb{Z}d_ke_k' \cong \mathbb{Z}/d_i \oplus \mathbb{Z}/d_{i+1} \oplus \ldots \oplus \mathbb{Z}/d_k \oplus \mathbb{Z}^{n-r}$$

où d_i est le premier des diviseurs différent de 1 ; on a obtenu la décomposition du groupe abélien de type fini $\mathbb{Z}^n/\mathbf{H}$.

f) i. Voici les matrices obtenues, le lecteur rétablira aisément les opérations utilisées :

$$\begin{pmatrix} 2 & 4 & 6 \\ -2 & 2 & 4 \\ 0 & 6 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ -2 & 6 & 10 \\ 0 & 6 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 10 \\ 0 & 6 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 10 \\ 0 & 0 & 2 \end{pmatrix} \to$$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & -2 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix} \to$$

Le lecteur remarquera que, par fantaisie, on a traité la première ligne avant la première colonne. Le groupe quotient $\mathbb{Z}^n/\mathbf{H}_1$ est donc isomorphe à $(\mathbb{Z}/2)^2 \times \mathbb{Z}/6$.

ii. Cet exemple est une variante du précédent, car on obtient une colonne nulle ; voici la succession des matrices obtenues :

$$\begin{pmatrix} 12 & 4 & 4 \\ 13 & 6 & 5 \\ 6 & 2 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & -2 & -1 \\ 13 & 6 & 5 \\ 6 & 2 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 \\ 0 & -20 & -8 \\ 0 & -10 & -4 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 20 & 8 \\ 0 & 10 & 4 \end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&10&4\\0&20&8\end{pmatrix}\to\begin{pmatrix}1&0&0\\0&2&4\\0&4&8\end{pmatrix}\to\begin{pmatrix}1&0&0\\0&2&0\\0&4&0\end{pmatrix}\to\begin{pmatrix}1&0&0\\0&2&0\\0&0&0\end{pmatrix}$$

La raison de l'apparition de cette colonne nulle est tout simplement que les vecteurs, dont nous sommes partis, ne sont pas indépendants. Le groupe quotient est isomorphe à $\mathbb{Z}/2\times\mathbb{Z}$.

g) Pour que le quotient soit fini, il est nécessaire et suffisant que $k=n$, et donc que $\mathbf{H}$ soit libre de rang n et ait une matrice adaptée carrée inversible.

h) Plaçons-nous donc dans l'hypothèse de la question précédente ; le nombre d'éléments de $\mathbb{Z}^n/\mathbf{H}$ est le produit des facteurs invariants (d_i). Or ce produit n'est autre que le déterminant de la matrice adaptée finale ; et l'on voit sans peine que les opérations faites sur une matrice adaptée, quand elle est carrée, ne changent pas la valeur absolue de son déterminant. Il suffit d'utiliser la multilinéarité de ce déterminant. Il en résulte que le cardinal du quotient est la valeur absolue du déterminant de n'importe quelle matrice adaptée.
On retrouve, en particulier, le fait bien connu qu'une matrice est adaptée à $\mathbb{Z}^n$ lui-même ssi elle est de déterminant ±1. C'est donc une caractérisation des matrices à coefficients entiers dont l'inverse est à coefficients entiers.

6.1 LES PRODUITS EN COURONNE

6.1.1 Un exemple

1) Si M et N sont des éléments de $\mathbf{B}_n$, leur produit est encore une matrice de $\mathbf{B}_n$. Posons $m_{ij}=a_i\delta_{i,\sigma(j)}$ et $n_{ij}=b_i\delta_{i,\tau(j)}$ où δ est le symbole de Kronecker[1], σ et τ des permutations et $(a_i),(b_i)$ des éléments de $\{-1,1\}^n$. Alors, la matrice produit MN a des coefficients p_{ij} donnés par :

$$p_{ij}=\sum_{k=1}^{n}a_ib_k\delta_{i,\sigma(k)}\delta_{k,\tau(j)}=a_ib_{\sigma^{-1}(i)}\delta_{i,\sigma\circ\tau(j)}$$

et c'est donc un élément de $\mathbf{B}_n$. La même formule permet d'obtenir la matrice inverse de M. Le cardinal de $\mathbf{B}_n$ est $2^n n!$.

2) Le groupe $\mathbf{G}_n$ est un sous-groupe de $\mathbf{B}_n$, formé des matrices pour lesquelles la suite (a_i) est constante égale à 1. On voit qu'il n'est pas normal. Prenons par exemple pour M la matrice pour laquelle $m_{11}=-1$, $m_{ii}=1$ si $i>1$, les autres coefficients étant nuls. Alors, si $P\neq I$ est dans $\mathbf{G}_n$, MPM^{-1} est une matrice qui contient deux éléments ayant la valeur -1 (ligne 1 et colonne 1).
En revanche, $\mathbf{D}_n$ est normal dans $\mathbf{B}_n$ puisque c'est le noyau de l'application qui à la matrice (m_{ij}) associe la matrice $(|m_{ij}|)$. On vérifie en effet immédiatement que cette application est un morphisme en utilisant le calcul ci-dessus.

3) On peut appliquer le critère de produit semi-direct, mais le calcul fait ci-dessus donne également le résultat ; l'action de $\mathbf{G}_n$ (identifié à $\mathcal{S}_n$) sur $\mathbf{D}_n$ (identifié à $\{+1,-1\}^n$) est

1. Par définition, $\delta_{i,j}$ est nul, sauf si $i=j$ et il vaut alors 1. La matrice carrée, dont les coefficients sont $\delta_{i,j}$ est la matrice identité.

donnée par $\sigma.(a_i) = (a_{\sigma^{-1}(i)})$ (*cf.* 3.1.8) et la loi dans le produit $\mathbf{D}_n \rtimes \mathbf{G}_n$ s'écrit :

$$(a, \sigma)(b, \tau) = (a\sigma.b, \sigma \circ \tau)$$

ce qui correspond exactement au produit de matrices fait ci-dessus.

4) $\mathbf{B}_1$ est le groupe $\{+1, -1\}$. $\mathbf{B}_2$ est un groupe de cardinal 8, ayant un sous-groupe normal isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$. On reconnaît le groupe diédral $\mathbb{D}_8$, voir l'exercice 2.3.1.

5) Le groupe $\mathbf{B}_3$ a 48 éléments. Son sous-groupe $\mathbf{B}_3^+$ est le noyau de l'application déterminant, donc est normal et d'indice 2 ; on en déduit une structure de produit direct, puisque l'image de cette application déterminant se relève en un groupe engendré par $-I$. Il en résulte l'isomorphisme :

$$\mathbf{B}_3 = \mathbf{B}_3^+ \times \mathbb{Z}/2$$

6) Plaçons-nous dans $\mathbb{R}^3$ de sorte que la base canonique soit orthonormée, les huit points de coordonnées $(\pm 1, \pm 1, \pm 1)$ sont les sommets d'un cube. Comme les éléments de $\mathbf{B}_3$ sont des matrices orthogonales qui conservent ce cube, et qu'il y en a 48, $\mathbf{B}_3$ est bien le groupe octaédral ; voir l'étude de ce groupe dans le problème 5.2.2. Cherchons à interpréter le sous-groupe $\mathbf{D}_3$. Il est constitué des réflexions par rapport aux trois plans de symétries parallèles aux faces, des demi-tours autour des perpendiculaires à ces plans, de $\pm$id. Par ailleurs, on vérifie que $\mathbf{G}_3$ est le stabilisateur du sommet $(1, 1, 1)$. Comme nous savons également que le groupe des isométries directes qui conservent le cube, $\mathbf{B}_3^+$, est isomorphe à $\mathcal{S}_4$, on aura les deux décompositions :

$$\mathbf{B}_3 \cong (\mathbb{Z}/2)^3 \rtimes \mathcal{S}_3 \cong \mathbb{Z}/2 \times \mathcal{S}_4$$

7) Il s'agit de montrer que $\mathbf{B}_n$ est le groupe des isométries qui conservent une figure géométrique. C'est le cas de $\mathbf{B}_2$ pour le carré, de $\mathbf{B}_3$ pour le cube ou l'octaèdre. Soit donc un espace vectoriel euclidien de dimension n, muni d'une base orthonormée directe (e_i). On appellera **hypercube** le polyèdre intersection des demi-hyperespaces contenant l'origine, et dont les équations sont $x_i = \pm 1$. Il y a 2^n sommets de coordonnées ± 1, on voit clairement que tout élément de $\mathbf{B}_n$ transforme les sommets en des sommets, et l'on peut démontrer que c'est le groupe des isométries conservant l'hypercube. Il conserve également l'hyperoctaèdre associé (obtenu en prenant pour sommets les points dont les coordonnées sont nulles sauf une valant ± 1), d'où son nom, groupe hyperoctaédral.

6.1.2 Un cas plus général

1) Il suffit de prendre pour $\mathbf{H}$ le groupe $\mathbb{Z}/2$ (dans sa version multiplicative), et pour $\mathbf{G}$ le groupe $\mathcal{S}_n$, $\mathbf{B}_n = \mathbb{Z}/2 \wr \mathcal{S}_n$. En effet, le produit de deux éléments du produit en couronne se fait de la façon suivante :

$$((a_i), \sigma)((b_i), \tau) = ((a_i b_{\sigma^{-1}(i)}), \sigma\tau)$$

et c'est exactement ce que donne le produit de deux éléments de $\mathbf{B}_n$.

2) Le groupe $\mathbf{G}$ admet un relèvement dans $\mathbf{W}$, l'ensemble des couples $((e)_{i=1..n}, g)$ où g parcourt $\mathbf{G}$. Ce n'est pas un sous-groupe normal de $\mathbf{W}$, car l'action de $\mathbf{G}$ n'est pas triviale (quand $\mathbf{H}$ bien sûr n'est pas réduit à un élément).
Le groupe $\mathbf{H}^n \times \{e\}$ est lui normal dans $\mathbf{W}$, et il contient des sous-groupes $\mathbf{H}_i$, projections, qui sont tous isomorphes à $\mathbf{H}$ mais ne sont pas normaux dans $\mathbf{W}$, le groupe $g\mathbf{H}_i g^{-1}$ est $\mathbf{H}_{g^{-1}(i)}$. Il existe un autre sous-groupe isomorphe à $\mathbf{H}$, c'est le sous-groupe diagonal formé des couples $(h)_{i=1..n}, e)$ où le premier terme est le n-uple constant et où h parcourt $\mathbf{H}$.

3) Les groupes $\mathbb{Z}/n \wr \mathbb{Z}/m$ peuvent être définis ainsi. Les éléments sont des couples $((a_i), b)$ où les m a_i sont dans $\mathbb{Z}/n$ et b dans $\mathbb{Z}/m$. La loi de groupe est alors :

$$((a_i), b)((a'_i), b') = (a_i + a_{i+b}, b + b')$$

l'indice étant pris modulo m. On peut reconnaître $\mathbb{Z}/2 \wr \mathbb{Z}/2$ comme étant le groupe diédral $\mathbb{D}_8$ (groupe non commutatif qui est un produit semi-direct). Parmi les autres, $\mathbb{Z}/3 \wr \mathbb{Z}/2$ est d'ordre dix-huit, $\mathbb{Z}/2 \wr \mathbb{Z}/3$ est d'ordre vingt-quatre. C'est un bon exercice de chercher à les identifier dans la liste fournie dans l'annexe...

4) Commençons par le premier arbre. Une bijection va conserver ou échanger les deux branches principales, puis on pourra échanger ou non les deux branches secondaires. Si l'on numérote les extrémités de ces branches de gauche à droite, il y a un premier sous-groupe de permutations :

$$id,\ (1,2),\ (3,4),\ (1,2)(3,4)$$

qui est isomorphe au groupe de Klein $(\mathbb{Z}/2)^2$. Si maintenant on utilise une permutation qui échange les branches principales, par exemple $(1,3)(2,4)$, on obtient un produit semi-direct $\mathbb{Z}/2^2 \rtimes \mathbb{Z}/2$ isomorphe au produit en couronne $\mathbb{Z}/2 \wr \mathbb{Z}/2$. On a déjà vu que ce produit semi-direct est isomorphe au groupe diédral $\mathbb{D}_8$ et d'ailleurs l'arbre a des points communs avec un carré... Ce groupe est un 2-Sylow de $\mathcal{S}_4$. Quant au groupe du second arbre, il est construit en prenant deux groupes isomorphes à $\mathbb{D}_8$, bijections des deux sous-arbres au-dessus des branches maîtresses, et l'on fait un produit semi-direct avec le groupe $\mathbb{Z}/2$. C'est un groupe qui peut s'écrire :

$$\mathbb{D}_8 \wr \mathbb{Z}/2 \cong (\mathbb{Z}/2 \wr \mathbb{Z}/2) \wr \mathbb{Z}/2$$

Il a $8^2 \times 2 = 128$ éléments et c'est un 2-Sylow de $\mathcal{S}_8$. En tant que groupe de permutations, il est engendré par le groupe diédral sur $(1,2,3,4)$, le groupe diédral sur $(5,6,7,8)$ et la permutation $(1,5)(2,6)(3,7)(4,8)$ qui échange les branches maîtresses. Notre construction est le point de départ de la construction des p-Sylow de $\mathcal{S}_{p^k}$ et, plus généralement, de $\mathcal{S}_n$. Voir, par exemple, [24].
Profitons-en pour vérifier que, dans la version présentée, le produit en couronne n'est pas associatif :

$$\mathbb{Z}/2 \wr (\mathbb{Z}/2 \wr \mathbb{Z}/2)$$

a pour cardinal $2^8 \times 8 = 2\,048$ éléments.

5) Quant au groupe d'isomorphismes de notre couronne, le même type de discussion montre qu'il est produit en couronne de $\mathcal{S}_3$ par $\mathbb{Z}/6$. Il a donc $6^6 \times 6$ éléments.

6) Pour reprendre les exemples vus ci-dessus, prenons un arbre qui a n branches principales qui portent m sous-branches. Alors son groupe d'automorphismes est le produit en couronne $\mathcal{S}_m \wr \mathcal{S}_n$ de cardinal $(m!)^n \times n!$, qui divise donc $(mn)!$, car tout automorphisme de l'arbre est un sous-groupe du groupe de bijections des extrémités.

6.1.3 Le cas général

1) Prenons pour X l'ensemble $\{1,2,\ldots,n\}$. Alors $\mathbf{H}^X$ est en bijection avec $\mathbf{H}^n$, à f on associe la liste $(f(1), f(2), \ldots, f(n))$. Si maintenant $\mathbf{G}$ est un sous-groupe du groupe symétrique $\mathcal{S}_n$, il agit sur X et sur $\mathbf{H}^X$, $\sigma.f(x) = f(\sigma^{-1}(x))$ et la liste devient $(f(\sigma^{-1}(1)), f(\sigma^{-1}(2)), \ldots, f(\sigma^{-1}(n)))$. C'est exactement la situation de la partie précédente.

2) $\mathbf{G}$ s'identifie à l'ensemble $\mathbf{G}^*$ des (f_e, g) où g parcourt $\mathbf{G}$ et où f_e est l'application constante égale à e, neutre de $\mathbf{H}$. Si maintenant on fixe $x \in X$ et l'on considère les applications f_h, valant h pour x et valant e pour les autres éléments de X, on obtient un groupe isomorphe à $\mathbf{H}$.

3) $\mathbf{H}^*$ est bien sûr isomorphe à $\mathbf{H}$, et si, par un abus de notation, on l'identifie à son image dans le produit semi-direct $\mathbf{W}$, c'est un sous-groupe de $\mathbf{W}$. Si maintenant on considère $\mathbf{H}^*\mathbf{G}^*$, c'est un aussi un sous-groupe du groupe $\mathbf{W}$ qui est isomorphe à $\mathbf{H} \times \mathbf{G}$.

4) Il faut vérifier que c'est une action. C'est immédiat pour le neutre et :

$$\begin{aligned}(f', g').((f, g).\psi(x)) &= (f', g').\widetilde{\psi}(x)\\ &= f'(x).\widetilde{\psi}(g'^{-1}.x)\\ &= f'(x).(f(g'^{-1}.x).\psi(g^{-1}.g'^{-1}.x)\\ (f'g'.f, g'g).\psi(x) &= f'(x)f(g'^{-1}.x).\psi((g'g)^{-1}.x)\end{aligned}$$

avec des notations faciles à comprendre. Si l'on se restreint à $\mathbf{G}^*$, et à $\mathbf{H}^*$ les actions s'écrivent :

$$g.\psi(x) = \psi(g^{-1}.x) \quad \text{et} \quad (h.\psi)(x) = h.\psi(x)$$

avec les identifications, on retrouve les deux actions habituelles, sur l'ensemble de départ et sur l'ensemble d'arrivée.

5) Si $\mathbf{H}$ n'est pas commutatif, il n'y a pas de raison que le produit restreint soit normal dans le produit complet ; on peut essayer avec par exemple un conjugué de (e, g) où e est l'application constante égale à e, par un élément de la forme (f, e) où f est quelconque.

6) Soit (f, g) un élément du centre. Cherchons le conjugué de (k, e) où $k(x) = h \neq e$, tous les autres éléments valant e. Si g ne fixe pas x, le conjugué est différent de k. On en déduit que g est forcément l'identité, lorsque l'action de $\mathbf{G}$ sur X est fidèle. Maintenant, l'examen du conjugué d'un élément de la forme (e, τ) où e désigne l'application constante égale à e et τ un élément de $\mathbf{G}$ qui transforme x en y, montre que $f(x) = f(y)$, la transitivité impose donc que f soit constante. Dans le cas du produit complet, le centre est donc un groupe diagonal construit sur le centre de $\mathbf{H}$. Dans le cas du produit restreint, il est réduit au neutre.
Le résultat précédent s'applique au produit restreint (produit semi-direct de p-groupes, c'est un p-groupe). On a ainsi un contre-exemple au résultat bien connu sur les p-groupes finis, leur centre est trivial.

7) Les éléments de $\mathbf{K}$ s'écrivant $(u_n, 0)$, on a bien sûr :

$$(u_n, 0)(v_n, 0) = (u_n + v_n, 0)$$

et $\mathbf{K}$ est un sous-groupe. En revanche, si t est le couple $(0, 1)$ où 0 est pour la suite nulle, $t(u_n, 0)t^{-1} = (u_{n-1}, 0)$, et donc le conjugué des $\mathbf{K}$ correspond aux suites nulles à partir de 1 ; on a bien $t\mathbf{K}t^{-1} < \mathbf{K}$. On peut d'ailleurs construire une chaîne de conjugués inclus les uns dans les autres. Signalons pour terminer qu'il est peu fréquent d'avoir de tels exemples.

6.2 GROUPES POLYÉDRAUX ET BINAIRES POLYÉDRAUX

6.2.1 Groupe d'isométries conservant un ensemble

1) Il suffit de considérer l'action du groupe des isométries sur les sous-ensembles du plan. Le groupe des isométries conservant S est alors son stabilisateur pour cette action.

2) Faisons un catalogue, sans détailler tous les arguments.

   – Le groupe des isométries d'une droite contient toutes les translations de vecteurs appartenant à la direction de la droite, toutes les symétries centrales de centre sur la droite, cela forme le groupe des isométries directes conservant la droite (il ne peut y avoir d'autre translation, ni d'autre rotation). Le groupe formé est isomorphe au produit semi-direct $\mathbb{R} \rtimes \{+1, -1\}$ (qui est un groupe diédral généralisé). En composant avec la réflexion d'axe la droite, on obtient les pseudo-symétries ayant pour axe cette droite et les réflexions d'axe orthogonal à la droite. Comme la réflexion d'axe la droite commute avec les translations et les symétries centrales, le groupe obtenu est le produit direct du groupe précédent avec le groupe à deux éléments.

   – Toutes les rotations de centre le centre du cercle, toutes les réflexions d'axe un diamètre du cercle conviennent, et il n'y en a pas d'autre car le centre du cercle doit être un point invariant. Le groupe obtenu est le produit semi-direct de $\mathbb{U}$ par le groupe à deux éléments, puisqu'aucune de ces réflexions ne commute avec les rotations.

   – Le groupe des isométries d'un carré est le groupe diédral $\mathbb{D}_8$, il suffit de rechercher les rotations conservant le carré ; leur centre est le centre du carré et elles forment un groupe cyclique d'ordre 4. On compose alors avec une des réflexions qui conservent le carré.

   – Si le rectangle n'est pas carré, le groupe des isométries du rectangle est le groupe de Klein $\mathcal{V}$, contenant une symétrie centrale, deux réflexions d'axes les médiatrices des côtés et l'identité. Ce groupe, isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$ est aussi connu sous le nom de groupe... du rectangle.

   – Si le triangle est équilatéral, son groupe d'isométries est $\mathbb{D}_6$ ou $\mathcal{S}_3$. S'il est isocèle sans être équilatéral, il n'y a que l'identité et la réflexion d'axe la médiatrice qui est axe de symétrie, et si le triangle est vraiment quelconque, il n'y a que l'identité.

3) Commençons par observer que le modèle des sommets d'un polygone convexe régulier à n côtés est l'ensemble des racines n-ièmes de l'unité, sur le cercle trigonométrique. Une rotation conservera ce polygone si son centre est l'origine et si son angle est un multiple de $\frac{2\pi}{n}$. Le groupe des rotations est donc cyclique d'ordre n, en composant avec la réflexion d'axe Ox, on obtient le groupe diédral $\mathbb{D}_{2n}$.

4) Si S est fini, alors les éléments de I_S ont un point fixe commun. Soit en effet G l'isobarycentre des points de S. Comme une isométrie conserve les barycentres, tout élément f de I_S transforme G en l'isobarycentre des éléments de $f(S) = S$ dont en G ; le point G est un point invariant de S, nous avons d'ailleurs utilisé ce résultat dans certains des exercices précédents. Par ailleurs, si S contient $n+1$ points affinement indépendants en dimension n, l'action de I_S sur S est fidèle (une isométrie qui fixe ces points est l'identité) et I_S est isomorphe à un sous-groupe du groupe symétrique de S donc est fini. On peut même réduire à n points, car une isométrie fixant un hyperplan est l'identité ou une réflexion. Ainsi, il y a

un nombre fini d'isométries planes fixant deux points, mais un nombre infini en dimension trois.

5) Si $\mathbf{G}$ est un groupe fini, soit A un point quelconque ; son orbite est finie, appelons M l'isobarycentre des points $g(A)$, où g parcourt $\mathbf{G}$. Alors M est fixe par tout élément g_0 de $\mathbf{G}$, puisque c'est l'isobarycentre des $g_0(g(A))$ et que la translation à gauche est une bijection de $\mathbf{G}$.

6) En vectorialisant en un point fixe commun des isométries de $\mathbf{G}$, il y a isomorphisme entre un groupe fini d'isométries ponctuelles et un groupe fini d'isométries vectorielles (ou transformations orthogonales). Les sous-groupes finis de $\mathbf{SO}(2,\mathbb{R})$ sont faciles à déterminer, un tel sous-groupe est un sous-groupe fini de $\mathbb{U}$, groupe des racines n-ièmes de l'unité, qui est en bijection avec $\mathbf{SO}(2,\mathbb{R})$. D'après le théorème de Lagrange, un tel groupe est formé d'éléments qui vérifient $x^n = 1$, c'est donc un sous-groupe du groupe cyclique des racines n-ièmes de l'unité, donc un groupe cyclique. Soit alors un sous-groupe fini $\mathbf{G}$ de $\mathbf{O}(2,\mathbb{R})$. Le morphisme déterminant a pour noyau un sous-groupe fini de $\mathbf{SO}(2,\mathbb{R})$. S'il est surjectif, $\mathbf{G}^+ = \mathbf{G} \cap \mathbf{SO}(2,\mathbb{R})$ est un sous-groupe normal d'indice 2 de $\mathbf{G}$; c'est un sous-groupe cyclique d'ordre n, et $\mathbf{G}$ est un groupe diédral $\mathbb{D}_{2n}$. En effet, il existe un relèvement de la forme $\{id, \sigma\}$, où σ est n'importe quelle isométrie négative de $\mathbf{G}$ (ce sont toutes des réflexions), et aucun de ces relèvements n'est normal, car aucune isométrie ne commute avec toutes les rotations de $\mathbf{G}$[1]. On obtient donc une structure semi-directe, dont on sait qu'elle est unique. Voir pour cette question le problème 3.5.2.

6.2.2 Sous-groupes finis de SO(3)

1) Soit x un point de P. C'est un pôle de la rotation g_0 ; prenons $g \in \mathbf{G}$, alors $g \circ g_0 \circ g^{-1}(g(P)) = g(P)$ prouve que $g(P)$ est aussi un pôle d'un élément de $\mathbf{G}$. Il y donc bien une action, par restriction, de $\mathbf{G}$ sur P.

2) $\mathbf{G}_x$ est un groupe formé de rotations ayant toutes le même axe. Les restrictions de ces rotations à l'orthogonal de l'axe forment un sous-groupe de rotation planes, isomorphes à $\mathbf{G}_x$. Ce groupe est donc cyclique ; on note n_x son cardinal, qui est bien sûr inférieur à n. Il n'est pas égal à un, seule l'identité est d'ordre 1.

3) La formule de Burnside s'écrit :

$$k = \frac{1}{n}\sum_{g\in G} \chi_g$$

où χ_g est le nombre des points fixes de la rotation g. Si $g \neq id$, cette rotation a deux points fixes, les deux intersections de l'axe de g avec la sphère ; et l'identité a pour points fixes tous les éléments de P. On en déduit :

$$nk = 2(n-1) + |P| = 2(n-1) + \sum_{i=1}^{k} |Gx_i| = 2(n-1) + \sum_{i=1}^{k} \frac{n}{n_i}$$

ce qui donne, en remuant un peu, la relation :

$$n\sum_{i=1}^{k}\left(1 - \frac{1}{n_i}\right) = 2(n-1)$$

1. À l'exception du cas du groupe de Klein.

4) Si $k = 1$, le premier membre de la relation précédente est strictement inférieur à n, ce qui donne $2(n-1) < n$ soit $n < 2$, exclu à part le cas où **G** est réduit à l'identité. Par ailleurs, chaque facteur $1 - \frac{1}{n_i}$ est supérieur à $\frac{1}{2}$, donc la relation précédente prouve que $2(n-1) \geqslant \frac{kn}{2}$, d'où $(4-k)n \geqslant 4$, et k ne peut être supérieur à 4.
Si maintenant $k = 2$, on a :

$$n\left(2 - \frac{1}{n_1} - \frac{1}{n_2}\right) = 2n - 2$$

ce qui s'écrit :

$$2 = \frac{n}{n_1} + \frac{n}{n_2}$$

mais ces deux rapports sont des entiers puisque $n_i | n$ par le théorème de Lagrange. La seule solution est donc $2 = 1 + 1$ et $n_1 = n_2 = n$.
Pour $k = 3$, on a trois orbites et l'on peut supposer $n_1 \leqslant n_2 \leqslant n_3$; la relation s'écrit :

$$1 < 1 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

ce qui empêche que tous les n_i soient supérieurs ou égaux à 3. Nécessairement $n_1 = 2$. On a alors :

$$\frac{1}{2} < \frac{1}{2} + \frac{2}{n} = \frac{1}{n_2} + \frac{1}{n_3}$$

ce qui empêche n_2 et n_3 d'être tous deux supérieurs ou égaux à 4. Il reste $n_2 = 2$, et alors n est pair et $n_3 = \frac{n}{2}$, ou bien $n_2 = 3$, et l'on a alors :

$$\frac{2}{n} = \frac{1}{6} - \frac{1}{n_3}$$

comme $n_3 \geqslant 3$, cela laisse trois possibilités, $n_3 = 3$, et $n = 12$ ou $n_3 = 4$ et $n = 24$ ou enfin $n_3 = 5$ et $n = 60$.

5) Si $n_1 = n_2 = n$, chaque orbite a un seul élément, son stabilisateur est le groupe tout entier. C'est donc qu'il y a deux pôles, opposés, un seul axe pour les n rotations, et le groupe est cyclique d'ordre n. Un objet susceptible d'avoir ce groupe comme stabilisateur sera par exemple une pyramide à base polygone régulier à n côtés, voir figure 6.3.

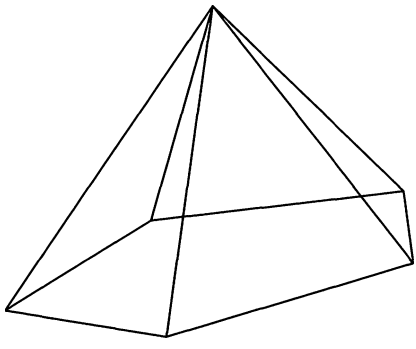


Figure 6.3 Pyramide

6) On suppose maintenant qu'il y a trois orbites, avec $n = 2m$ pair, $n_1 = n_2 = 2$ et $n_3 = m$. Si, pour commencer, $m = 2$, alors les stabilisateurs sont trois groupes engendrés par des rotations d'angles π ou demi-tours, et donc les trois orbites sont formées de pôles opposés. Mais si x est un pôle, pour que son orbite ne contienne que le point opposé, il faut que les axes des autres demi-tours soient dans le plan orthogonal. Les trois demi-tours ont donc des axes deux à deux perpendiculaires, et le groupe $\mathbf{G}$ est le groupe $(\mathbb{Z}/2)^3$.
Si $m > 2$, la troisième orbite contient deux pôles opposés, axe d'une rotation ρ d'ordre $m > 2$. Les autres orbites ont des stabilisateurs d'ordre 2, donc correspondant à des demi-tours, d'axe orthogonal à celui de ρ. Comme leur cardinal est m, les sommets de chaque orbite forment un polygone régulier à n côtés, la figure formée dans le plan est donc celle de deux polygones réguliers imbriqués, et le groupe $\mathbf{G}$ est engendré par un ρ et un des demi-tour r : on vérifie que $r \circ \rho \circ r = \rho^{-1}$ et l'on reconnaît le groupe diédral $\mathbb{D}_{2m}$. La figure la plus simple dont le stabilisateur est un polygone régulier plan à n côtés.

7) Soit $\mathbf{G}$ le groupe des rotations conservant un tétraèdre régulier ; il contient les rotations joignant un sommet au centre de la face opposée, au nombre de huit (deux par sommet), les demi-tours d'axes joignant les milieux des arêtes opposées, soit trois éléments, ce qui fait douze avec l'identité. Une façon rapide de voir qu'il n'y a rien d'autre est de considérer le groupe de toutes les isométries conservant le tétraèdre, c'est un sous-groupe du groupe des permutations des quatre sommets, et le groupe des rotations en est un sous-groupe d'indice 2 (application déterminant) : il a donc un maximum de 12 éléments. Nous avons en prime le fait que ce groupe est isomorphe à $\mathcal{A}_4$. Les pôles d'un demi-tour sont dans une même orbite qui contient six éléments, et qui dessine un octaèdre régulier, homothétique de celui qui joint les milieux des arêtes. Les pôles des autres rotations sont dans deux orbites de quatre éléments qui forment deux tétraèdres réguliers. Voir la figure 6.4 où l'on a représenté un seul des tétraèdres et l'octaèdre inscrit.

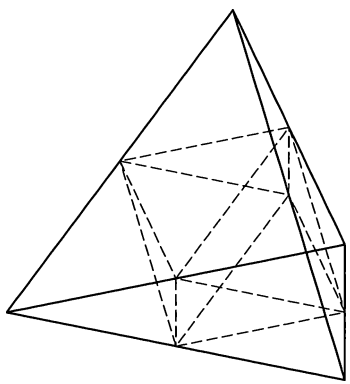


Figure 6.4 Tétraèdre

Reste à montrer qu'il n'y a pas d'autre groupe correspondant à cette structure d'orbites sur P. L'idée de départ est que nous connaissons les ordres des éléments de $\mathbf{G}$, il y a deux orbites de quatre éléments, correspondant à huit rotations d'ordre trois, une orbite de six éléments pour trois rotations d'ordre deux. Appelons A, B, C et D les éléments d'une des orbites d'ordre quatre. Ces quatre points ne sont pas coplanaires, sinon les axes des

demi-tours qui les permutent et des rotations d'ordre trois seraient aussi dans le même plan, et donc également tous les pôles. C'est impossible, les rotations d'ordre trois doivent faire sortir les points de ce plan. On en déduit que **G** agit sur cet ensemble de quatre points, de façon fidèle (une isométrie fixant quatre points non coplanaires est l'identité), et donc que **G** est un sous-groupe d'indice deux du groupe $\mathcal{S}_4$, isomorphe donc à $\mathcal{A}_4$; il ressort également de cela que les quatre points A, B, C et D sont équidistants et forment un tétraèdre régulier.

8) Dans le cas c), il y a une orbite ayant douze points, pôles de rotations d'ordre deux, une orbite ayant huit points, pôles de rotations d'ordre trois, et une orbite de six points, pôles de rotations d'ordre quatre. On s'intéresse à l'orbite de huit points ; ces points sont opposés deux à deux (car une rotation d'ordre trois a deux pôles). On peut faire agir **G** sur les quatre segments joignant ces points opposés ; on montre que cette action est fidèle. Si en effet une rotation induit l'identité sur ces quatre segments, elle ne peut en fixer point par point qu'un seul au plus (son axe) ; les deux autres sont donc transformés en leur opposé, soit les quatre segments sont coplanaires, soit deux coplanaires, l'autre perpendiculaire à ce plan. Mais alors les axes des demi-tours de **G** vont être dans ces deux directions, ce qui est incompatible avec le fait qu'ils sont permutés par les éléments d'ordre trois. On en déduit que **G** qui a 24 éléments est isomorphe à $\mathcal{S}_4$. On peut alors montrer que ces trois segments sont les diagonales d'un cube. Si l'on comptabilise les rotations qui conservent le cube : huit d'ordre trois d'axes ces trois diagonales, six d'ordre quatre d'axes joignant les milieux des faces opposées, les trois demi-tours de mêmes axes, et enfin les six demi-tours d'axes joignant les milieux des arêtes opposées, on obtient, avec l'identité, nos 24 éléments. Ce groupe de rotation s'appelle le **groupe octaédral**. Il a déjà été rencontré dans l'étude des produits en couronne du problème précédent. Il est (comme son nom l'indique...) également le groupe des rotations qui conservent un octaèdre régulier. Les sommets de cet octaèdre peuvent être vus comme les éléments de l'orbite de six points, homothétique de l'octaèdre inscrit dans un cube que montre la figure 6.5.

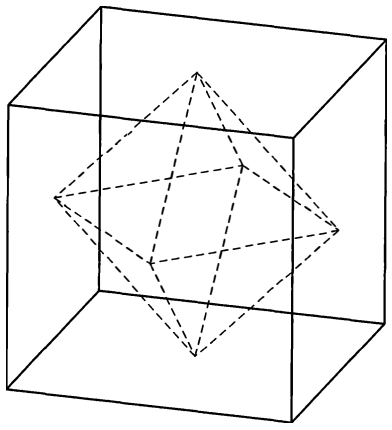


Figure 6.5 Cube

Dans le dernier cas, contentons-nous d'un examen rapide[1]. Il y a une orbite ayant trente points, pôles de quinze rotations d'ordre deux, une orbite ayant vingt points, pôles de vingt rotations d'ordre trois, enfin une orbite ayant douze points, pôles de vingt-quatre rotations d'ordre cinq. Intéressons-nous à cette orbite. Une rotation d'ordre cinq ayant pour axe le segment joignant deux points laisse stables les dix autres. On peut éliminer le cas où ces dix points sont coplanaires ; ils forment donc deux pentagones réguliers dans des plans parallèles à l'axe de notre rotation. En utilisant le fait que ces points sont opposés deux à deux, on vérifie que la figure obtenue est un icosaèdre régulier. L'orbite à vingt points est constituée par les sommets d'un dodécaèdre régulier, homothétique de celui qui joint les centres des faces de l'icosaèdre (fig. 6.6).

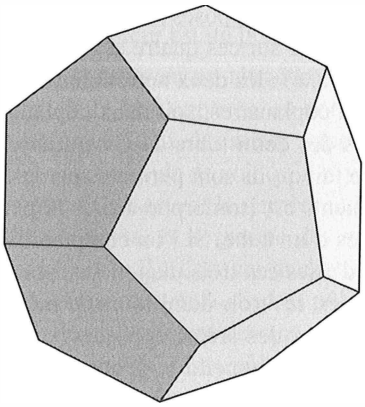


Figure 6.6 Dodécaèdre

Le groupe **G** est nommé **groupe icosaédral**. On peut montrer qu'il est isomorphe à $\mathcal{A}_5$, voici une indication sur une méthode « géométrique » ; dans un dodécaèdre, il y a cinq cubes inscrits, dont les arêtes sont des diagonales des faces (qui sont des pentagones), et chaque sommet du dodécaèdre est sommet de deux des cubes, ces deux cubes ayant alors une diagonale en commun. On peut alors voir (si l'on voit bien...) que :

- les rotations d'ordre deux conservent un cube et permutent les autres par paires, formant quinze doubles transpositions des cinq cubes ;
- les rotations d'ordre trois laissent fixes deux cubes (ceux qui ont pour diagonale commune l'axe de la rotation) et permutent les trois autres cycliquement, formant vingt 3-cycles ;
- les rotations d'ordre cinq permutent les cinq cubes circulairement, formant vingt-quatre 5-cycles.

6.2.3 Sous-groupes finis de O(3)

1) $\mathbf{G}^+$ est le noyau du morphisme déterminant, c'est un sous-groupe normal de **G**. Si le morphisme est surjectif, c'est-à-dire s'il existe au moins une isométrie négative (réflexion ou

1. On pourra consulter avec profit un bon livre de géométrie, comme [15], [8], [27].

réflexion rotatoire), c'est un sous-groupe d'indice 2 de $\mathbf{G}$. Sinon, $\mathbf{G}$ ne contient que des rotations et c'est un des groupes étudiés ci-dessus.

2) Pour un groupe cyclique, on peut prendre un polygone régulier et placer des flèches sur les côtés, ce qui empêchera les réflexions. Pour le groupe diédral, on peut utiliser des antiprismes. Voir le cas d'un antiprisme hexagonal, dont le groupe des isométries est le groupe diédral $\mathbb{D}_{12}$, figure 6.7, à condition d'ajouter des flèches qui orientent les côtés des deux hexagones en sens contraire. On peut traiter de la même façon les autres groupes.

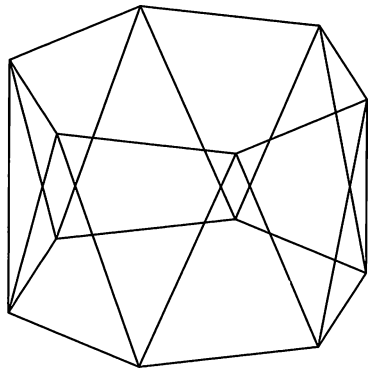


Figure 6.7 Antiprisme

3) Dire que $\mathbf{G}$ contient $-id$, c'est dire que la suite exacte

$$id \longrightarrow \mathbf{G}^+ \xrightarrow{i} \mathbf{G} \xrightarrow{\det} \{+1, -1\} \longrightarrow 1$$

est scindée, avec de plus un relèvement $\{id, -id\}$ normal, puisque $-id$ commute avec tout. On a donc un produit direct $\mathbf{G} \cong \mathbf{G}^+ \times \mathbb{Z}/2$. Dans le cas où $\mathbf{G}^+$ est cyclique, on obtient un groupe dont les éléments sont de la forme $\pm r^k$, où r est une rotation génératrice, $-r^k$ est alors une réflexion rotatoire. Il y a une réflexion si n est pair. Si $\mathbf{G}$ est diédral, on trouve les mêmes $\pm r^k$, des demi tours, mais aussi les opposés des demi-tours, qui sont des réflexions hyperplanes de plans contenant l'axe de r. On pourra de même étudier les autres groupes.

4) Le groupe $\Gamma = \langle \mathbf{G}, -id \rangle$ contient $-id$, il est donc du type précédent, et de la forme $\mathbf{H} \times \{+id, -id\}$ où $\mathbf{H}$ est un sous-groupe fini de $\mathbf{SO}(3)$. Mais alors Γ est la réunion de quatre ensembles de même cardinal :

$$\mathbf{G}^+, \ -\mathbf{G}^-, \ \mathbf{G}^-, \ -\mathbf{G}^+$$

où $\mathbf{G}^- = \mathbf{G} \setminus \mathbf{G}^+$. Les deux premiers de ces ensembles sont formés d'isométries directes, c'est donc $\mathbf{H}$. On en déduit que $\mathbf{G}^+$ est un sous-groupe d'indice deux de $\mathbf{H}$. Notons $\mathbf{H}_0$ ce sous-groupe et $\mathbf{H}_1$ son complémentaire ; alors Γ est la réunion des quatre ensembles :

$$\mathbf{H}_0, \ \mathbf{H}_1, -\mathbf{H}_0, \ -\mathbf{H}_1$$

puisque $\mathbf{G}$ ne contient pas $-id$, c'est que $\mathbf{G} = \mathbf{H}_0 \cup -\mathbf{H}_1$. Réciproquement, si $\mathbf{H}$ est un sous-groupe d'isométries directes et $\mathbf{H}_0$ un sous-groupe d'indice deux, de complémentaire $\mathbf{H}_1$, alors $\mathbf{G} = \mathbf{H}_0 \cup -\mathbf{H}_1$ est un groupe ; il est d'ailleurs isomorphe à $\mathbf{H}$, l'application $\phi(r) = r$ si $r \in \mathbf{H}_0$ et $\phi(r') = -id \circ r' = -r'$ si $r \in \mathbf{H}_1$ est un isomorphisme de groupe.

Pour aller plus loin dans la description, il faut chercher ceux, parmi les groupes finis de rotations, qui ont un sous-groupe d'indice deux. Ce sont :

- le groupe cyclique d'ordre pair $2n$, engendré par la rotation r d'angle $\frac{2\pi}{n}$. On obtient alors un groupe mixte $\mathbf{G}$ contenant le groupe des rotations engendré par r^2, et les réflexions rotatoires $-id \circ r^{2k+1}$ de même axe. Ce groupe est effectivement cyclique d'ordre n, engendré par la réflexion rotatoire $-r$;
- le groupe diédral d'ordre $2n$, et son sous-groupe cyclique d'ordre n. On obtient un groupe $\mathbf{G}$ contenant les rotations et les opposés des demi-tours qui sont des réflexions. C'est le groupe diédral du plan, « prolongé » par l'identité dans la direction orthogonale au plan. C'est le groupe des isométries qui conservent une pyramide régulière à base polygonale ;
- le groupe diédral d'ordre $2n$ où n est pair. Il a pour sous-groupe le groupe diédral d'ordre n ; on ajoute à ce sous-groupe les opposés des demi-tours qui sont des réflexions, et les opposés des rotations qui sont des réflexions rotatoires ;
- le groupe octaédral qui, isomorphe à $\mathcal{S}_4$, a un seul sous-groupe d'indice deux ; ce sous-groupe est formé des rotations qui correspondent aux permutations paires des diagonales. Il y a les trois demi-tours d'axes joignant les centres des faces opposées, les huit rotations d'ordre trois autour des diagonales, et l'identité. Le groupe mixte $\mathbf{G}$ contient alors ces rotations et les opposés des autres, c'est-à-dire les opposés des six rotations d'ordre quatre qui sont des réflexions rotatoires, les six opposés des demi-tours joignant les centres d'arêtes parallèles opposées qui sont des réflexions de plans contenant également des arêtes parallèles opposées.

Le groupe tétraédral $\mathbf{T}$ (isomorphe à $\mathcal{A}_4$) ne contient pas de sous-groupe d'indice 2, c'est le cas également du groupe icosaédral qui n'a pas de sous-groupe d'ordre 30[1]. Notre description achève donc la description des sous-groupes finis d'isométries de l'espace.

5) Les groupes d'isométrie complets du cube et de l'icosaèdre sont les produits $\mathbf{O} \times \{\pm id\}$ et $\mathbf{I} \times \{\pm id\}$ car $-id$ fait partie de ces groupes. En revanche, un tétraèdre régulier n'a pas de centre de symétrie, et son groupe complet d'isométrie est donc mixte ; c'est le dernier groupe décrit dans la question précédente, comme on le voit quand on inscrit un tétraèdre dans un cube. Il est isomorphe à $\mathcal{S}_4$ comme le groupe octaédral.
Une remarque pour conclure. Les groupes que nous avons décrits ne sont pas uniques... Il suffit de changer la position et la taille du tétraèdre pour avoir un autre groupe tétraédral, mais tous les groupes tétraédraux sont conjugués par une isométrie.

6.2.4 Groupes polyédraux

1)

$$(p, q, r) = \langle a, b \mid a^p = b^q = (ab)^r = 1 \rangle$$

en utilisant que $c^{-1} = ab$ est d'ordre r.

2)

$$(p, p, 1) = \langle a, b \mid a^p = b^p = ab = 1 \rangle = \langle a \mid a^p = 1 \rangle = \mathbb{Z}/p$$

1. Car il est simple, puisqu'il est isomorphe à $\mathcal{A}_5$, et n'a donc pas de sous-groupe d'indice deux qui serait normal.

3)
$$(2,2,r) = \langle a,b \mid a^2 = b^2 = (ab)^r = 1\rangle = \langle a,c \mid a^2 = c^r = 1,\ aca^{-1} = c^{-1}\rangle$$
Sous cette dernière forme, on reconnaît le groupe diédral $\mathbb{D}_{2r}$. On a utilisé que si $c = ab$, alors $b = ac$ puisque a est d'ordre deux, et $(ac)^2 = 1$ s'écrit $aca^{-1} = c^{-1}$.

4) Soit $\mathbf{G}$ le groupe $(2,3,3)$. Une façon de montrer qu'il est fini est de montrer que la liste :
$$e,\ b,\ b^2,\ a,\ ab,\ (ab)^2,\ ab^2,\ (ab^2)^2,\ aba,\ ab^2a,\ abab^2,\ ab^2ab$$
forme une liste d'éléments auxquels tous les autres se ramènent. On obtient douze éléments au maximum. Et il suffit de trouver un modèle où ces éléments sont distincts ; c'est le groupe tétraédral $\mathbf{T}$ qui donne le modèle le plus direct, en interprétant a comme un demi-tour, b comme une rotation d'ordre trois, $c = b^{-1}a$ est alors une autre rotation d'ordre trois. De façon équivalente, on peut prendre pour a une double-transposition de $\mathcal{A}_4$, et pour b un 3-cycle.

5) Ici encore, la grande difficulté est de montrer que $(2,3,4)$ est fini. Posons
$$\mathbf{G} = \langle a,b \mid a^2 = b^3 = (ab)^4 = 1\rangle$$
On va montrer que $\mathbf{N} = \langle b,(ab)^2\rangle$ est normal dans $\mathbf{G}$; comme $\mathbf{G}$ est engendré par b et ab, il suffit de regarder le conjugué $ab(b)(ab)^{-1} = aba = (ab)^2b^{-1}$. Maintenant, il est immédiat que l'indice de $\mathbf{N}$ est inférieur à 2 puisque $b\mathbf{N} = \mathbf{N}$, on peut avoir $a\mathbf{N} \neq \mathbf{N}$, et toutes les autres classes sont l'une de ces deux classes, car $ba\mathbf{N} = a\mathbf{N}$ puisque $a^-ba \in \mathbf{N}$. Enfin, le groupe $\mathbf{N}$ est d'ordre inférieur à 12. En effet, les éléments b et $(ab)^2$ vérifient les relations :
$$b^3 = (ab)^4 = (b(ab)^2)^3 = 1$$
Seule est à vérifier la dernière relation. On a :
$$b(ab)^2 = (ab)b^{-1}(ab)^{-1}$$
car cette égalité équivaut à $b(ab)^{-1} = a$. On en déduit que $b(ab)^2$ est un conjugué de b^{-1} donc que son cube vaut 1. Il en résulte qu'il existe un morphisme surjectif du groupe $\mathcal{A}_4$ sur $\mathbf{N} = (2,3,3)$. On en déduit que le cardinal de $\mathbf{N}$ est inférieur à 12, celui de $\mathbf{G}$ est inférieur à 24 ; c'est terminé, si l'on vérifie que le groupe octaédral satisfait les relations de $\mathbf{G}$ en prenant pour a un demi-tour d'axe joignant les centres d'arêtes parallèles opposées, b étant une rotation d'ordre trois d'axe une grande diagonale.

6) Admettant que le cardinal est soixante, il suffit de montrer que deux éléments engendrant le groupe icosaédral satisfont ces relations. En numérotant les cubes inscrits dans le dodécaèdre, on peut choisir pour a le demi-tour qui laisse le cube 1 fixe et échange 2, 3 et 4, 5. Pour b, on prend la rotation d'ordre 3 qui laisse 2 et 4 fixes et qui permute circulairement 1, 3 et 5. On vérifie alors que ab est la permutation circulaire $(1,2,3,4,5)$, et donc les relations sont satisfaites. Il reste à voir que ces permutations engendrent le groupe icosaédral $\mathbf{I}$, il suffit pour cela de vérifier que tous les trois cycles sont bien dans le groupe... Ce n'est pas long en calculant les conjugués de $(1,3,5)$ par a et les puissances de ab.
Regardons le modèle suivant du groupe $(3,3,3)$. a, b et c sont trois rotations d'angle $\frac{2\pi}{3}$ et de centre sur les sommets d'un triangle équilatéral direct ; alors abc est l'identité, comme on peut le voir en utilisant des composés de réflexions ou directement. Mais ce groupe est infini puisqu'il contient des translations comme $a^{-1}b$. Signalons pour terminer que cette approche géométrique permet d'interpréter tous les groupes polyédraux, mais il faut se placer en géométrie euclidienne (comme nous venons de le faire), ou en géométrie sphérique

(cela concerne les groupes des questions précédentes) ou enfin en géométrie hyperbolique. Seul le cas sphérique produit des groupes finis.

6.2.5 Groupes binaires polyédraux

1) D'après le théorème de Lagrange, si q est dans un groupe fini d'ordre n, $q^n = 1$, ce qui prouve que la norme de q est 1, donc que q est unitaire. Le groupe $\mathbf{G}$ est donc un sous-groupe du groupe $\mathbf{H}$ des quaternions unitaires. Or, on sait qu'il existe un morphisme surjectif ϕ de $\mathbf{H}$ sur le groupe $\mathbf{SO}(3,\mathbb{R})$. Par ce morphime, l'image de ce groupe $\mathbf{G}$ est donc un sous-groupe fini de $\mathbf{SO}(3,\mathbb{R})$. Comme le noyau du morphisme est ± 1, il y a deux cas. Si $\mathbf{G}$ ne contient pas -1 il est isomorphe à $\phi(\mathbf{G})$, sinon $\mathbf{G}/\pm 1$ est isomorphe à $\phi(\mathbf{G})$.

2) Dans le cas où $\mathbf{G}$ ne contient pas -1, il ne contient pas de quaternion unitaire pur (dont le carré est -1), et donc $\phi(\mathbf{G})$ ne contient pas de demi-tour : cela élimine presque tous les sous-groupes de $\mathbf{SO}(3,\mathbb{R})$, sauf les groupes cycliques d'ordre impair. $\mathbf{G}$ est alors cyclique, par exemple engendré par le quaternion $\cos\left(\frac{2\pi}{k}\right) + i\sin\left(\frac{2\pi}{k}\right)$ (qui est un complexe...).

3) Supposons que $\phi(\mathbf{G}) = (p,q,r)$. Alors, si $\mathbf{G}$ contient -1, il sera formé de deux fois plus d'éléments que $\phi(\mathbf{G})$. Si $\phi(\mathbf{G})$ est engendré par les rotations a, b et c, $\mathbf{G}$ contiendra les quaternions A, B et C, où $A = \cos\frac{\pi}{p} + u\sin\frac{\pi}{p}$, avec u quaternion unitaire pur dirigeant l'axe de la rotation a, de même pour B et C. Puisque :

$$A^p = B^q = C^r = -1$$

ces quaternions suffisent à engendrer $\mathbf{G}$. On vérifie que $ABC = -1$ et $\mathbf{G}$ admet la présentation :

$$\mathbf{G} = \langle A, B, C \mid A^p = B^q = C^r = ABC = Z,\ Z^2 = -1\rangle$$

Il n'y a pas d'autre relation (indépendante), sinon on aurait aussi une autre relation pour $\phi(\mathbf{G})$.

4) Le groupe $\langle p,p,1\rangle$ s'écrit donc :

$$\begin{aligned}\langle p,p,1\rangle &= \langle A,B,C \mid A^p = B^p = C = ABC,\ C^2 = 1\rangle\\ &= \langle A,C \mid A^p = C,\ C^2 = 1\rangle\\ &= \langle A \mid A^{2p} = 1\rangle\end{aligned}$$

la première simplification provenant de ce que B et A sont alors inverses l'un de l'autre. On trouve donc un groupe cyclique d'ordre pair (dont un modèle est tout simplement $\langle e^{\frac{i\pi}{p}}\rangle$. Au vu de la question 2, il y a donc tous les groupes cycliques.
Le groupe $\langle 2,2,r\rangle$ s'écrit :

$$\begin{aligned}\langle 2,2,r\rangle &= \langle A,B,C \mid A^2 = B^2 = C^r = ABC,\ C^2 = 1\rangle\\ &= \langle B,C \mid B^2 = C^r = (BC)^2,\ C^2 = 1\rangle\\ &= \langle B,C \mid B^2 = C^r,\ B^{2r} = 1,\ BCB^{-1} = B^{-1}\rangle\end{aligned}$$

on reconnaît bien la présentation du groupe dicyclique d'ordre $4r$.

5) Il s'agit donc de montrer que si $a^p = b^3 = c^2 = abc = z$, alors $(abc)^2 = 1$. Cela a déjà été fait dans l'exercice 2.2.14, et résulte d'un calcul un peu... sordide. En utilisant les relations

$a = b^{-1}a^{-1}b^2$ et $b = a^{p-1}b^{-1}a^{-1}$, on trouve :

$$\begin{array}{rcll} z = a^p & = & ba^pb^{-1} & \text{car } z \text{ commute à } b \\ & = & b(b^{-1}a^{-1}b^2)^pb^{-1} & \\ & = & (a^{-1}b)^p & \text{en développant} \\ & = & a^{p-2}b^{-1}a^{-1} & \text{seconde relation} \\ & = & (a^{p-3}b^{-1})^p & \text{on développe} \end{array}$$

On utilise aussi dans ce calcul que z commute à a. Si $p = 3$, on a fini $z = b^{-3} = b^3$ donc $z^2 = 1$. Si $p = 4$, on continue :

$$z = (ab^{-1})^4 = a(b^{-1}a)^4a^{-1} = (b^{-1}a)^4 = (a^{-1}b)^{-4} = z^{-1}$$

Pour $p = 5$, c'est du même style mais un peu plus long :

$$\begin{array}{rcl} z = (a^2b^{-1})^5 & = & ((b^{-1}a^{-1}b^2)^2b^{-1})^5 \\ = (b^{-1}a^{-1}ba^{-1}b)^5 & = & (a^{-1}ba^{-1})^5 \\ = (ba^{-2})^5 & = & (a^2b^{-1})^{-5} \\ = z^{-1} & & \end{array}$$

6.3 TRANSITIVITÉ, BLOCS, GROUPES PRIMITIFS

6.3.1 Groupes transitifs

1) Il n'y a comme autres sous-groupes que les conjugués de $\langle 1, 2\rangle$, qui n'est pas transitif, car il fixe 3.

2) Dire que $\mathbf{G}$ est transitif, c'est dire que l'ensemble des entiers $\{1, 2, \ldots, n\}$ sur lequel il agit ne contient qu'une seule orbite. Si $\mathbf{G}_1$ est le stabilisateur de 1, on a donc :

$$[\mathbf{G} : \mathbf{G}_1] = n$$

et $\mathbf{G}$ est de cardinal multiple de n.

3) Il est immédiat que les groupes indiqués sont transitifs, et il reste à montrer qu'il n'y en a pas d'autre ; comme le cardinal d'un groupe transitif doit être un multiple de 4, les seules possibilités sont 4, 8 et 12. Le seul sous-groupe d'ordre 12 est le groupe alterné, un sous-groupe d'ordre 8 est un 2-Sylow, ils sont tous conjugués à celui que nous avons donné, et il est clair (en utilisant l'automorphisme intérieur) qu'un conjugué d'un groupe transitif est transitif. Reste le cas des groupes d'ordre 4 qui ne peuvent contenir que des éléments d'ordre 2 ou 4. On a tous les groupes du type $\langle (1, 2, 3, 4)\rangle$ et le groupe $\mathcal{V}$, les seul autres groupes possibles du type $\langle (1, 2), (3, 4)\rangle$ ne sont pas transitifs (1 a pour image 1 ou 2).

Cas $n = 5$:

1) Cherchons une permutation ϕ qui normalise le groupe engendré par $c = (1, 2, 3, 4, 5)$. Cela signifie $\phi \circ c \circ \phi^{-1} = c^k$ où k est un entier entre 1 et 5. Autrement dit, $\phi(1) = p$ et $\phi(i+1) = \phi(i)+k$ soit $\phi(i) = p+(i-1)k$ en travaillant modulo 5. Cette formule montre que le normalisateur cherché est le groupe affine de l'anneau $\mathbb{Z}/5$. Plus simplement, il est engendré par c et les permutations $u_k : i \mapsto ki \pmod 5$; ces permutations sont dans notre cas :

$$id, (1, 2, 4, 3) \text{ (multiplication par 2)}, (1, 3, 4, 2) \text{ (par 3)}, (1, 4)(2, 3) \text{ (par 4)}$$

et forment un groupe isomorphe à $\mathbb{Z}/4$, et au groupe des inversibles du corps $\mathbb{Z}/5$. Le normalisateur est donc isomorphe au produit semi-direct de $\mathbb{Z}/5$ par $\mathbb{Z}/4$, il a vingt éléments et a été rencontré dans le problème sur les produits semi-directs en géométrie.

2) Soit $\mathbf{H}$ un sous-groupe de $\mathcal{S}_5$, d'indice ℓ. Alors $\mathcal{S}_5$ agit sur le quotient $\mathcal{S}_5/\mathbf{H}$ par translation. Le noyau de cette action est un sous-groupe normal. Si c'est le groupe alterné, $\mathbf{H}$ est d'indice 2 et c'est le groupe alterné ; si c'est l'identité, $\mathcal{S}_5$ s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_\ell$, et donc $\ell \geqslant 5$, ce qui limite le cardinal à 24. Mais un sous-groupe transitif a un cardinal divisible par 5, s'il est non trivial restent possibles les cardinaux 5, 10 ou 20.

3) On connaît les sous-groupes de 5 éléments ; ce sont les conjugués du groupe cyclique $\langle(1,2,3,4,5)\rangle$, et ils sont bien sûr transitifs. Un groupe ayant 10 ou 20 éléments admettra donc un 5-Sylow de ce type, et il sera transitif. Comme le 5-Sylow est unique d'après les théorèmes de Sylow, ces groupes seront des sous-groupes du normalisateur. L'étude de ce normalisateur montre que l'on aura donc un groupe a 20 éléments, $\langle(1,2,3,4,5),(1,3,4,2)\rangle$, et un groupe a 10 éléments, $\langle(1,2,3,4,5),(1,4)(2,3)\rangle$, à conjugaison près.
L'étude des groupes transitifs devient plus difficile pour $n = 6$, il y a alors quatorze types de groupes primitifs.

6.3.2 Blocs

1) Si B est un bloc, il est non vide et contient un élément x. Comme le groupe est transitif, tout élément de X est de la forme $g.x$ et est donc dans $g.B$. On en déduit que les $g.B$ recouvrent $\mathbf{G}$. De plus, ils sont disjoints, car si $g.B$ et $g'.B$ ont un élément commun $g.x = g'.y$, on a $x = (g^{-1}g').y$ ce qui prouve, par définition de B, que $B = (g^{-1}g').B$ et donc $g.B = g'.B$. Ce même argument montre que les $g.B$ sont des blocs, on a un système de blocs, ensemble sur lequel agit $\mathbf{G}$. Dans le cas fini, le cardinal de B est un diviseur du cardinal de X.

2) Il y a bien sûr les singletons, ainsi que le groupe tout entier. Nous les appellerons « blocs triviaux ». Mais dans le cas du carré, il y a également les blocs formés de deux points diagonalement opposés ; cela traduit le fait géométrique que les isométries conservent les diagonales. Les ensembles formés de deux sommets consécutifs ne sont pas des blocs. On retrouve des blocs diagonaux dans le cas du groupe octaédral.

3) Soit en effet un tel groupe $\mathbf{H}$, et $B = \mathbf{H}.x$. Alors, si $g.B$ et B ont un élément commun, on a une égalité de la forme $gh.x = h'.x$ où h et h' sont dans $\mathbf{H}$. Mais alors $h'^{-1}gh \in \mathbf{G}_x \subset \mathbf{H}$, donc g est dans $\mathbf{H}$ et $g.B = B$, B est un bloc. Réciproquement, si B est un bloc sous l'action de $\mathbf{G}$, et x dans B, on définit $\mathbf{H}$ par :

$$g \in \mathbf{H} \iff g.x \in B$$

C'est visiblement un sous-groupe de $\mathbf{G}$, contenant le stabilisateur de x, et B peut s'écrire $B = \mathbf{H}.x$ (on utilise la transitivité).

4) Soit $\sigma = (1,2,\ldots,n)$. Cherchons les blocs contenant 1. D'après la question précédente, ils sont de la forme $\mathbf{H}.1$, où $\mathbf{H}$ contient le stabilisateur de 1 qui est ici l'identité. Si d est un diviseur de n, il lui correspond un seul sous-groupe de $\langle\sigma\rangle$, et le bloc $1, 1+d, 1+2d$ qui a $\frac{n}{d}$ éléments. Ainsi, pour $n = 6$, on a les blocs :

$$\{1\},\ \{1,2,3,4,5,6\},\ \{1,3,6\},\ \{1,4\}$$

et par exemple, les deux blocs à trois éléments se dessinent comme les deux triangles équilatéraux inscrits dans un hexagone régulier.

5) Rappelons pour commencer que tous les stabilisateurs sont conjugués, puisque l'action est transitive. Si $\mathbf{G}_x$ est maximal, la construction des blocs faite ci-dessus prouve que les blocs

contenant x sont $\mathbf{G}_x x = \{x\}$ et $\mathbf{G}x = X$, et de même, s'il n'y a que des blocs triviaux, tous les stabilisateurs sont des sous-groupes maximaux.

6) On se place dans le cas où $\mathbf{G}$ agit sur un ensemble ayant au moins deux éléments... et même un peu plus car toute action sur un ensemble à deux éléments est primitive. Soient a et b deux éléments distincts d'un bloc B et $g.B$ un bloc disjoint, contenant deux éléments distincts a' et b'. Alors, par 2-transitivité, il existe h transformant a en a et b en b', et $h.B \cap B$ n'est pas vide sans que $h.B$ soit égal à B.

6.3.3 Simplicité des groupes spéciaux projectifs linéaires

1) – Montrons d'abord que $\mathbf{N}.x$ est un bloc. Si $g\mathbf{N}.x \cap \mathbf{N}.x$ est non vide, il contient un élément tel que $gn.x = n'.x$, où n et n' sont dans $\mathbf{N}$. Mais comme $\mathbf{N}$ est normal dans $\mathbf{G}$, gn peut s'écrire $n''g$ et l'on en déduit $g.x \in \mathbf{N}.x$. Mais alors, puisque $\mathbf{G}$ est primitif, on a $\mathbf{N}.x = \{x\}$ auquel cas $\mathbf{N}$ est inclus dans le stabilisateur de x, ou bien $\mathbf{N}.x = X$, qui signifie que $\mathbf{G}$ agit transitivement sur X. Mais il est exclu que $\mathbf{N} \subset \mathbf{G}_x$, car, par normalité, on en déduirait $\mathbf{N} \subset g\mathbf{G}_x g^{-1} = \mathbf{G}_{g.x}$. $\mathbf{N}$ serait inclus dans l'intersection de tous les stabilisateurs (l'action est transitive) et serait donc réduit au neutre (l'action est fidèle). Reste donc ce qui était notre objectif, $\mathbf{N}$ agit transitivement.

– $\mathbf{N}$ n'est pas inclus dans un stabilisateur, comme nous venons de le voir, donc, par maximalité de $\mathbf{G}_x$, on a bien $\mathbf{NG}_x = \mathbf{G}$ (en observant au passage que $\mathbf{N}$ étant normal dans $\mathbf{G}$, $\mathbf{NG}_x$ est bien un sous-groupe de $\mathbf{G}$).

– Pour $g \in \mathbf{G}$, le groupe $g\mathbf{A}g^{-1}$ peut s'écrire $nh\mathbf{A}h^{-1}n^{-1} = n\mathbf{A}n^{-1}$ où $n \in \mathbf{N}$ et $h \in \mathbf{G}_x$. On a utilisé la question précédente et l'hypothèse sur $\mathbf{A}$. On en déduit que $g\mathbf{A}g^{-1} \subset \mathbf{NA}$, en utilisant encore la normalité de $\mathbf{N}$ dans $\mathbf{G}$. Au vu de l'hypothèse, on a bien $\mathbf{G} = \mathbf{NA}$.

– Le second théorème d'isomorphisme permet d'annoncer que $\mathbf{G}/\mathbf{N} = \mathbf{NA}/\mathbf{N}$ est isomorphe à $\mathbf{A}/\mathbf{A} \cup \mathbf{N}$, donc est abélien. On en déduit que $\mathbf{N}$ contient le groupe dérivé $\mathbf{G}'$. Comme $\mathbf{G}$ est parfait, il vient $\mathbf{N} = \mathbf{G}$. On a donc démontré que $\mathbf{G}$ est un groupe simple.

2) a) Étant donnés deux vecteurs non colinéaires, on peut toujours les considérer comme les deux premiers vecteurs d'une base. Il existe toujours une application linéaire transformant ces deux vecteurs en deux vecteurs non colinéaires, il suffit de les compléter en une base. Il est donc possible de transformer un couple de droites distinctes en un couple de droites distinctes. Par ailleurs, on peut multiplier l'image d'un de ces vecteurs par une constante non nulle sans changer ce fait, et donc obtenir une application linéaire dans le groupe spécial linéaire. Enfin, en passant au quotient on obtient le résultat que le groupe $\mathbf{PSL}(n, \mathbb{K})$ est 2-transitif sur l'espace projectif $\mathbb{P}(\mathbb{K}^n)$[1]. De plus, comme le noyau de l'action du groupe linéaire sur l'ensemble des droites est formé des homothéties, donc du centre, cette action est fidèle.

b) Le fait que le groupe spécial linéaire soit engendré par les matrices de transvections est bien connu. C'est la traduction en terme de produit matriciel de l'algorithme du pivot de Gauss, appliqué à une matrice de déterminant égal à 1, voir par exemple [14]. De plus, l'exercice 5.3.5 montre que toute transvection est un commutateur, à condition de disposer de trois indices distincts, donc pour $n \geqslant 3$. On en déduit que le groupe dérivé de $\mathbf{SL}(n, \mathbb{K})$ est lui-même. On obtient le même résultat quand on divise par le

1. C'est l'ensemble des droites vectorielles.

centre (car, pour l'écrire de façon abrégée, $[a,b]\mathcal{Z} = [a\mathcal{Z}, b\mathcal{Z}]$).
Dans le cas où $n = 2$, on peut calculer un commutateur :

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}$$

et si le corps a plus de trois éléments, on peut choisir a non nul de sorte que $a^2 - 1$ soit non nul ; on obtient ainsi qu'une transvection est un commutateur (un même calcul règle le cas des matrices triangulaires inférieures).
Il reste $\mathbf{PSL}(2,\mathbb{F}_2)$ et $\mathbf{PSL}(2,\mathbb{F}_3)$, mais ces groupes sont respectivement égaux à $\mathcal{S}_3$ et $\mathcal{A}_4$ qui ne sont pas simples, le problème est donc réglé. On peut remarquer que dans ces deux cas le groupe dérivé n'est pas égal au groupe tout entier, voir 5.1.8.

c) Commençons par identifier le stabilisateur **S** de la droite engendrée par le premier vecteur de base. C'est l'ensemble des (classes de) matrices dont la première colonne est ${}^t(a, 0, 0, \ldots 0)$ où a est non nul conviendra (si son déterminant est 1). On peut trouver un représentant de la forme $\begin{pmatrix} 1 & \ell \\ 0 & M \end{pmatrix}$ où M est de déterminant 1 en multipliant par une homothétie. Il contient notre ensemble de matrices A. De plus :

$$\begin{pmatrix} 1 & \ell \\ 0 & I_{n-1} \end{pmatrix}\begin{pmatrix} 1 & \ell' \\ 0 & I_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \ell+\ell' \\ 0 & I_{n-1} \end{pmatrix}$$

Ce groupe est normal dans **S**, on peut faire un calcul direct ou dire que c'est le noyau du morphisme qui à $\begin{pmatrix} 1 & \ell \\ 0 & M \end{pmatrix}$ associe M dans le groupe spécial linéaire.
Pour montrer que $\mathbf{PSL}(n,\mathbb{K})$ est engendré par les conjugués des éléments de **A**, il est préférable de prendre une vision géométrique ; les transvections, qui engendrent le groupe $\mathbf{SL}(n,\mathbb{K})$ peuvent être géométriquement définies ainsi :

$$t_{v,\phi}(x) = x + \phi(x)v$$

où v est un vecteur non nul, ϕ une forme linéaire, dont le noyau est un hyperplan **H** contenant le vecteur v. On constate aisément que cette application linéaire admet 1 comme seule valeur propre et **H** comme sous-espace propre. Les matrices de transvection $T_{ij} = I + E_{ij}$ que nous avons souvent utilisées sont caractérisées par le vecteur $v = e_i$ et la forme linéaire $x \mapsto x_j$. Les applications linéaires, dont la matrice est dans **A**, sont définies par :

$$x \mapsto x + \left(\sum_{i=2}^{n} a_i x_i\right) e_1$$

elles représentent toutes les transvections dont le vecteur est e_1. Si l'on considère un élément g quelconque de $\mathbf{SL}(n,\mathbb{K})$, et a un élément de **A**, alors $g \circ a \circ g^{-1}$ est aussi une transvection :

$$g \circ a \circ g^{-1}(x) = x + \phi(g^{-1}(x))g(e_1)$$

Si l'on veut obtenir une transvection quelconque, il suffit donc de choisir g transformant e_1 en un vecteur de la transvection et, comme ϕ parcourt toutes les formes linéaires annulant e_1, $\phi \circ g^{-1}$ parcourt toutes les formes linéaires annulant $g(e_1)$. On termine en disant que le groupe spécial linéaire est engendré par les transvections, et en passant au quotient. Toutes les hypothèses du critère d'Iwasawa sont satisfaites, le groupe projectif spécial linéaire est simple, sauf dans les deux cas signalés.

6.4 SUR LES SOUS-GROUPES

1) On sait que $\mathbf{H} \leqslant \mathbf{K}$, il faut montrer que $\mathbf{K} \leqslant \mathbf{H}$. Soit x quelconque dans $\mathbf{K}$. Comme $\mathbf{K} \subset \mathbf{KL} = \mathbf{HL}$, on a :

$$\exists h \in \mathbf{H},\ \exists \ell \in \mathbf{L},\ x = h\ell$$

Mais alors $\ell = h^{-1}x \in \mathbf{K}$, et donc $\ell \in \mathbf{L} \cap \mathbf{K} = \mathbf{L} \cap \mathbf{H}$ et $\ell \in \mathbf{H}$. On en conclut que x produit de deux éléments de $\mathbf{H}$ est dans $\mathbf{H}$.

Dans le cadre des espaces vectoriels, cette propriété s'écrit :

$$\left.\begin{array}{rcl} \mathbf{H} \cap \mathbf{L} & = & \mathbf{K} \cap \mathbf{L} \\ \mathbf{H} + \mathbf{L} & = & \mathbf{K} + \mathbf{L} \\ \mathbf{H} & \subset & \mathbf{K} \end{array}\right\} \quad \Rightarrow \quad \mathbf{H} = \mathbf{K}$$

Elle peut se démontrer comme nous l'avons fait ou, dans le cas de la dimension finie, en utilisant la formule de Grassmann :

$$\dim(\mathbf{H} + \mathbf{L}) = \dim \mathbf{H} + \dim \mathbf{L} - \dim(\mathbf{H} \cap \mathbf{L})$$

Remarquons que, dans cette question, les ensembles $\mathbf{HL}$ et $\mathbf{KL}$ ne sont pas forcément des sous-groupes.

2) Il est immédiat que $\mathbf{H}(\mathbf{L} \cap \mathbf{K}) \subset (\mathbf{HL}) \cap \mathbf{K}$ puisque :

$$\mathbf{L} \cap \mathbf{K} \subset \mathbf{L} \quad \Rightarrow \quad \mathbf{H}(\mathbf{L} \cap \mathbf{K}) \subset \mathbf{HL}$$

et

$$\mathbf{H} \subset \mathbf{K} \quad \text{et} \quad \mathbf{L} \cap \mathbf{K} \subset \mathbf{K} \quad \Rightarrow \quad \mathbf{H}(\mathbf{L} \cap \mathbf{K}) \subset \mathbf{K}$$

Pour la réciproque, on va revenir aux éléments : soit $k \in (\mathbf{HL}) \cap \mathbf{K}$. Alors il existe $h \in \mathbf{H}$ et $\ell \in \mathbf{L}$ tels que $k = h\ell$, mais alors $\ell = h^{-1}k \in \mathbf{K}$ puisque $\mathbf{H} \subset \mathbf{K}$. Donc $\ell \in \mathbf{L} \cap \mathbf{K}$, c'est-à-dire que $\mathbf{HL} \cap \mathbf{K} \subset \mathbf{H}(\mathbf{L} \cap \mathbf{K})$.

En notation additive, on a donc :

$$\mathbf{H} \leqslant \mathbf{K} \quad \Rightarrow \quad (\mathbf{H} + \mathbf{L}) \cap \mathbf{K} = \mathbf{H} + (\mathbf{L} \cap \mathbf{K})$$

Sans hypothèse, cette égalité n'a pas lieu, il suffit de prendre par exemple trois droites distinctes d'un plan vectoriel.

3) Si $\mathbf{H}$ et $\mathbf{K}$ sont deux sous-groupes de $\mathbf{G}$, alors $\mathbf{H} \cap \mathbf{K}$ est un sous-groupe de $\mathbf{G}$, et il contient tous les sous-groupes de $\mathbf{G}$ qui sont inclus dans $\mathbf{H}$ et dans $\mathbf{K}$: c'est donc la borne inférieure. Par ailleurs, le groupe $\langle \mathbf{H}, \mathbf{K} \rangle$, engendré par $\mathbf{H}$ et $\mathbf{K}$ est, par définition, le plus petit sous-groupe de $\mathbf{G}$ qui contienne $\mathbf{H}$ et $\mathbf{K}$: c'est la borne supérieure. On a donc :

$$\mathbf{H} \vee \mathbf{K} = \mathbf{H} \cap \mathbf{K} \qquad \text{et} \qquad \mathbf{H} \wedge \mathbf{K} = \langle \mathbf{H}, \mathbf{K} \rangle$$

4) Les démonstrations sont immédiates, ce sont des traductions directes : par exemple, si $\mathbf{H} \leqslant \mathbf{K}$ alors $\mathbf{H}$ est minorant commun de $\mathbf{H}$ et de $\mathbf{K}$, et c'est le plus grand, car tout minorant commun est inférieur à $\mathbf{H}$, et donc $\mathbf{H} = \mathbf{H} \wedge \mathbf{K}$. De même, $\mathbf{H} = \mathbf{H} \wedge \mathbf{K}$ implique que $\mathbf{H}$ minore $\mathbf{H}$ et $\mathbf{K}$. On traite de même l'autre équivalence, et la rédaction montre que l'on n'utilise que les propriétés d'un treillis.

5) L'étude faite des sous-groupes d'un groupe cyclique prouve que le treillis des sous-groupes est en bijection avec l'ensemble des diviseurs de n. Si l'on munit cet ensemble de la relation « divise », ces deux treillis sont isomorphes.

6) Il faut démontrer que $\mathcal{N}(\mathbf{G})$ est stable pour les deux opérations : c'est bien connu pour $\wedge$, car l'intersection de deux sous-groupes normaux dans $\mathbf{G}$ est un sous-groupe normal dans $\mathbf{G}$: cf. l'exercice . En ce qui concerne l'opération $\vee$, commençons par rappeler que :

$$\langle \mathbf{H}, \mathbf{K} \rangle = \mathbf{HK}$$

dès que l'un des deux groupes est normal dans $\mathbf{G}$. Si les deux sous-groupes sont normaux dans $\mathbf{G}$ et si l'on considère un élément g de $\mathbf{G}$, on a alors :

$$g\mathbf{H}\mathbf{K}g^{-1} = \mathbf{H}gg^{-1}\mathbf{K} = \mathbf{HK}$$

et donc $\mathbf{H} \vee \mathbf{K} = \mathbf{HK}$ est normal dans $\mathbf{G}$.

Terminons en signalant que l'examen du treillis des sous-groupes, même complété par celui des sous-groupes normaux ne permet pas de distinguer des groupes : deux groupes peuvent avoir leur treillis de sous-groupes isomorphes sans être isomorphes.

6.5 DES GROUPES D'ORDRE 12

1) Pour chercher les sous-groupes d'un groupe fini, on peut procéder de façon systématique, en considérant les sous-groupes engendrés par 1 élément, puis 2 éléments.... On peut également utiliser un logiciel de calcul formel spécifique comme GAP.

a) Commençons par le cas bien connu du **groupe alterné** $\mathcal{A}_4$. Il y a trois éléments d'ordre 2, les trois double-transpositions $u = (1,2)(3,4)$, $v = (1,3)(2,4)$ et $w = (1,4)(2,3)$ qui engendrent chacune un sous-groupe à deux éléments ; deux d'entre elles engendrent un groupe à quatre éléments, isomorphe au groupe de Klein, qui est le seul 2-Sylow de $\mathcal{A}_4$, et est donc un sous-groupe normal d'ordre 4. Les autres éléments (différents du neutre), sont les huit 3-cycles, qui engendrent au total quatre sous-groupes d'ordre 3. On a déjà constaté qu'il n'y a pas de sous-groupe à six éléments. Au total : 10 sous-groupes (y compris les deux triviaux).

b) Passons au **groupe diédral** $\mathbb{D}_{12}$, engendré par une rotation r d'ordre 6, et par une symétrie σ. C'est le groupe des isométries qui conservent un hexagone, par exemple celui qui joint les points d'affixes les racines sixième de l'unité. Il contient des sous-groupes à deux éléments :

- $\langle r^3 \rangle$; géométriquement, r^3 est $-\mathrm{id}$, la symétrie par rapport au centre de l'hexagone. Ce groupe est le centre, il est donc normal dans le groupe diédral.
- $\langle \sigma \rangle$, $\langle r \circ \sigma \rangle$, $\langle r^2 \circ \sigma \rangle$, $\langle r^3 \circ \sigma \rangle$, $\langle r^4 \circ \sigma \rangle$, $\langle r^5 \circ \sigma \rangle$ sont les groupes engendrés par les réflexions. Ils sont tous conjugués les uns des autres.

Et on épuise ainsi les 7 éléments d'ordre 2.
Il reste des éléments d'ordre 3, comme r^2 et r^4, qui engendrent le même groupe d'ordre 3, et deux éléments d'ordre 6, r et r^5 qui engendrent le même groupe cyclique d'ordre 6, groupe des rotations de l'hexagone.
Passons aux sous-groupes non monogènes :

- Il y a les groupes à quatre éléments, engendrés par les couples (σ, r^3), $(r \circ \sigma, r^3)$, et $(r^2 \circ \sigma, r^3)$. Ces groupes sont les 2-Sylow du groupe diédral, ils sont isomorphes au groupe de Klein et sont conjugués.

– Il y a deux nouveaux groupes à 6 éléments, $\langle \sigma, r^2 \rangle$ et $\langle r \circ \sigma, r^2 \rangle$. Ces groupes sont isomorphes au groupe symétrique $\mathcal{S}_3$. Ils ne sont pas conjugués : leur intersection est le groupe à trois éléments engendré par r^2, et ils contiennent chacun trois des six groupes à deux éléments différents du centre.

Au total, seize sous-groupes.

c) Enfin examinons le cas du groupe $\mathcal{T}$, produit semi-direct de $\mathbb{Z}/3$ par $\mathbb{Z}/4$ (voir les exercices 2.3.5 et 3.3.6.) Il admet, entre autres, la présentation :

$$\mathcal{T} = \langle a, b \mid a^6 = e,\ b^2 = a^3,\ bab^{-1} = a^{-1} \rangle = \{e, a, a^2, a^3, a^4, a^5, b, b^3, ab, ab^3, a^2b, a^2b^3\}$$

Le seul élément d'ordre 2 est a^3, il engendre un groupe à deux éléments qui est le centre. Il y a deux éléments d'ordre 3, a^2 et a^5, qui engendrent un groupe cyclique à 3 éléments inclus aussi dans le groupe cyclique à 6 éléments engendré par a et a^5. Les six autres éléments sont d'ordre quatre et engendrent trois sous-groupes cycliques à quatre éléments contenant le centre.

Il n'y a pas d'autre sous-groupes, à part les sous-groupes triviaux : il faudrait plus d'un élément d'ordre 2 pour que $\mathcal{T}$ contienne un sous-groupe isomorphe à $\mathcal{S}_3$ ou à $\mathbb{Z}/2 \times \mathbb{Z}/2$. Au total donc, huit sous-groupes.

2) Un élément A de $\mathbf{H}$ s'écrit :

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

où a et c doivent être inversibles (puisque $\det(A) = ac$) et où b est quelconque. Il y a donc deux choix pour a et c, trois pour b. Au total : $2 \times 2 \times 3 = 12$ éléments. Par calcul direct, on vérifie rapidement que le groupe n'est pas commutatif et que le centre est réduit aux matrices I et $-I$ (on note 0, 1 et -1 les éléments du corps $\mathbb{F}_3$. Pour distinguer notre groupe $\mathbf{H}$ parmi les trois candidats possibles, on peut par exemple compter les éléments d'ordre 2 :

$$A^2 = \begin{pmatrix} a^2 & b(a+c) \\ 0 & c^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff \begin{cases} a^2 = c^2 = 1 \\ b(a+c) = 0 \end{cases}$$

On peut prendre $a = \pm 1$, $c = \pm 1$ et $b = 0$,ce qui donne trois éléments d'ordre 2 (quand on enlève I). Mais si $a = 1$ et $c = -1$, b est quelconque et cela donne deux nouvelles solutions, de même que $a = -1$ et $c = 1$. Il y a donc sept éléments d'ordre 2, notre groupe est isomorphe au groupe diédral $\mathbb{D}_{12}$.

3) On sait que $\mathrm{Int}(\mathbf{G}) \cong \mathbf{G}/\mathcal{Z}(\mathbf{G})$, et donc le nombre des automorphismes intérieurs est six. De plus, si on note i_A l'automorphisme intérieur déterminé par A, il existe des matrices telles que $i_A \circ i_{A'} \neq i_{A'} \circ i_A$ (puisqu'on n'a pas toujours $AA' = \pm A'A$), le groupe $\mathrm{Int}(\mathbf{G})$ est donc isomorphe au groupe non commutatif à six éléments, $\mathcal{S}_3$. Soyons plus précis ; commençons par remarquer qu'un automorphisme intérieur transforme une matrice en une matrice de même diagonale : c'est parce que l'on travaille dans un ensemble de matrices triangulaires supérieures. Ainsi, pour se déterminer un automorphisme, il suffit de déterminer l'image de deux générateurs. Si on choisit un élément s d'ordre 2 (différent de $-I$), et un élément r d'ordre 6, par exemple les matrices :

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad r = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

Il y aura trois choix possibles pour l'image de s parmi les matrices d'ordre 2 qui ont même diagonale que s et deux choix pour l'image de r, elle-même et $r^5 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ cela fait bien six éléments.

4) Il faut trouver un automorphisme qui ne soit pas intérieur. Une bonne idée est d'utiliser le déterminant... Il suffit de définir ϕ par : $\phi : M \mapsto \det(M) \times M$. Et ce n'est pas un automorphisme intérieur, car la diagonale n'est pas conservée si les deux éléments diagonaux sont distincts. Une autre façon d'écrire ϕ est :

$$\phi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} c & abc \\ 0 & a \end{pmatrix}$$

On a utilisé $a^2 = c^2 = 1$, puisque $a = \pm 1$ et $c = \pm 1$. Remarquons enfin que $\phi^2 = \mathbf{id}$ et que si ψ est un automorphisme extérieur, alors les éléments diagonaux sont échangés s'ils sont distincts (voir les choix possibles pour l'image d'un élément d'ordre 2). On en déduit que $\psi \circ \phi$ est un automorphisme qui conserve la diagonale, c'est un automorphisme intérieur, et l'ensemble des automorphismes de notre groupe est en bijection avec le produit ensembliste $\mathcal{S}_3 \times \mathbb{Z}/2$. Comme il n'y a pas de relèvement de $\mathbb{Z}/2$ dans le centre, il s'agit d'un produit semi-direct.

En définitive, le groupe des automorphismes de $\mathbb{D}_{12}$ est un groupe isomorphe à $\mathcal{S}_3 \rtimes \mathbb{Z}/2$, lequel est isomorphe à ... $\mathbb{D}_{12}$. Et pourtant, les automorphismes ne sont pas tous intérieurs. Une remarque, nous avons déjà vu (3.3.12) que le groupe des automorphismes du groupe diédral $\mathbb{D}_{2n}$ est l'holomorphe du groupe cyclique $\mathbb{Z}/n$. Or cet holomorphe est produit semi-direct du groupe cyclique $\mathbb{Z}/n$ par le groupe de ses automorphismes. Et ce dernier est isomorphe au groupe des inversibles de l'anneau $\mathbb{Z}/n$ (cf.3.3.7). Pour $n = 3$, cet holomorphe est donc de la forme $\mathbb{Z}/n \rtimes \mathbb{Z}/2$. C'est donc bien le groupe diédral lui-même.

5) Le calcul a déjà été explicité : on cherche une matrice inversible, le choix de la première colonne se fait parmi les vecteurs non nuls, il y a $3^2 - 1 = 8$ possibilités. Le choix de la seconde colonne se limite aux $3^2 - 3 = 6$ vecteurs indépendants restant. Le groupe a donc 48 éléments.

6) $\mathbf{G}$ agit sur $\mathbf{G}/\mathbf{H}$ par translation. Le noyau de l'action Φ est l'ensemble des éléments x de $\mathbf{G}$ tels que $xg\mathbf{H} = g\mathbf{H}$ pour tout g, c'est donc $\operatorname{Ker}\Phi = \bigcap_{g\in\mathbf{H}} g\mathbf{H}g^{-1}$. Comme $\mathbf{H}$ est l'ensemble des matrices triangulaires supérieures, cette intersection est facile à calculer. En effet, un conjugué de $\mathbf{H}$ est l'ensemble des matrices triangulaires inférieures (prendre pour g la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$), donc le noyau de Φ ne contient que des matrices diagonales. En prenant une autre matrice, par exemple $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, on voit que l'intersection ne contient que des matrices scalaires : en définitive, le noyau de Φ, contient $\pm I$, qui constitue $\mathcal{Z}(\mathbf{G})$.

Le groupe $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est isomorphe à un sous-groupe du groupe symétrique de $\mathbf{G}/\mathbf{H}$. Mais comme $\mathbf{H}$ est de cardinal 12 il est d'indice 4 et ce groupe symétrique est $\mathcal{S}_4$. Comme le cardinal de $\mathbf{G}/\mathcal{Z}(\mathbf{G})$ est 24, on en déduit :

$$\mathbf{G}/\mathcal{Z}(\mathbf{G}) = \mathbf{PGL}(2, \mathbb{F}_3) \cong \mathcal{S}_4$$

résultat déjà obtenu (plus facilement...) dans l'exercice 3.5.1.

7) $\mathbf{K}$ est bien sûr un groupe, comme intersection de groupes. Tout élément de $\mathbf{K}$ s'écrit

$$A = \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix}$$

où a est inversible, b quelconque dans $\mathbb{F}_4$. Il y a donc 3×4 éléments. Le plus rapide est sans doute de rechercher les éléments d'ordre 2. On constate que $A^2 = I$ équivaut à

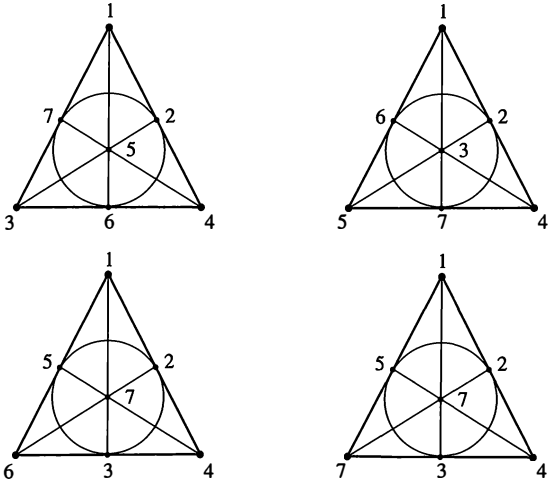
$$\begin{cases} a^2 = 1 \\ b\left(a + \frac{1}{a}\right) = 0 \end{cases}$$

Comme la première condition donne seulement $a = 1$, on voit que b est quelconque : il y a trois éléments d'ordre 2 qui, avec la matrice I, forment un sous-groupe d'ordre 4, isomorphe au groupe de Klein. D'après la première question, notre groupe est isomorphe au groupe alterné $\mathcal{A}_4$. C'est bien sûr un sous-groupe de $\mathbf{SL}(2, \mathbb{F}_4)$ dont nous savons (3.5.1) qu'il est isomorphe au groupe $\mathcal{A}_5$.

6.6 UN GROUPE D'ORDRE 168

1) Procédons par étapes :

- L'action de $\mathbf{G}$ sur les sommets est transitive : l'orbite de 1, par exemple, est constituée des sept points, on peut le vérifier par exemple en constatant que le cycle $\sigma = (1, 2, 3, 4, 5, 6, 7)$ stabilise l'ensemble $\mathbf{D}$ (il conserve l'alignement). Si $\mathbf{G}_1$ est le stabilisateur de 1, le cardinal de $\mathbf{G}/\mathbf{G}_1$ est donc 7.
- Examinons maintenant l'action de $\mathbf{G}_1$: l'orbite de 2 est constituée des six points différents de 1 : il existe en effet toujours une droite reliant 1 aux six autres points, et les sept droites sont interchangeables. Le cardinal de $\mathbf{G}_1/\mathbf{G}_{1,2}$ est donc 6.
- Si on considère maintenant l'action restreinte à $\mathbf{G}_{1,2}$: le point 4 est nécessairement fixe puisque 1, 2 et 4 sont alignés ; il s'agit de permuter les quatre autres sommets de sorte que la structure de graphe soit conservée : il est facile de voir qu'il n'y a que quatre solutions, une fois l'image de 3 choisie parmi les quatre possibles :



Et le groupe correspondant a quatre éléments, il est isomorphe au groupe du rectangle (ce qu'on vérifie bien en regardant la figure formée par les points 3, 5, 6 et 7).

En conclusion le cardinal de **G** est $7 \times 6 \times 4 = 168$.

2) On a déjà constaté que σ est un automorphisme du graphe. C'est aussi le cas de τ, d'après la fin de la question précédente. De plus, ces deux permutations sont paires, le groupe engendré est donc inclus dans $\mathcal{A}_7$, qui a 2520 éléments. Le groupe engendré par σ est de cardinal 7. Par ailleurs :

$$\sigma \circ \tau = (1,2,3)(4,5,7)$$

est un élément d'ordre 3. De plus, si on pose :

$$\alpha = \sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} = (1,4)(3,6,5,7)$$

et

$$\beta = \sigma \circ \tau \circ \sigma^{-1} = (1,4)(6,7)$$

on peut envisager le groupe $\langle \alpha, \beta \rangle$. Comme α est d'ordre 4, β et d'ordre 2 et comme

$$\beta \circ \alpha \circ \beta^{-1} = (1,4)(3,7,5,6) = \alpha^{-1}$$

ce groupe est le groupe diédral d'ordre huit. Le groupe **H** contient des sous-groupes d'ordre 7, 3 et 8, il est donc de cardinal supérieur à 168. Comme il est inclus dans **G**, de cardinal 168, il coïncide avec **G**.

3) Notre plan de Fano est en effet le graphe de $\mathbf{P}^2(\mathbb{F}_2)$. Une bijection est par exemple obtenue en prenant les trois points 3, 4, 1 comme projeté des vecteurs (1, 0, 0), (0, 1, 0) et (0, 0, 1). Le point 5 est alors le point de coordonnées projectives (1, 1, 1), c'est le point unité. Les trois autres points sont les projetés de la somme de deux vecteurs de base : 6, par exemple, est l'image du vecteur de coordonnées $(1,1,0) = (1,0,0) + (0,1,1)$, il est aligné avec 3 et 4. Comme $(1,1,0) = (1,1,1) + (0,0,1)$, il est également aligné avec 1 et 5, etc. Les homographies sont alors les bijections qui conservent l'alignement, ce sont des isomorphismes du graphe. Par exemple, les deux permutations σ et τ sont les images des homographies de matrices respectives :

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

On conclut en rappelant que dans le problème 6.3., nous avons démontré la simplicité de la quasi-totalité des groupes spéciaux projectifs linéaires. Notre groupe **G** est donc un groupe simple à 168 éléments.

Il est possible de montrer que c'est le **seul** groupe simple de cardinal 168. L'idée de la démonstration est, prenant un groupe simple à 168 éléments, est de trouver « à l'intérieur » de ce groupe, une image du plan de Fano.

6.7 SOUS-GROUPES MAXIMAUX

1) Les sous-groupes maximaux de $\mathbb{Z}$ sont les groupes $p\mathbb{Z}$ où p est premier : il n'y a pas de diviseur d'un nombre premier autre que 1 et lui-même, équivaut à : il n'existe pas de groupe strictement compris entre $\mathbb{Z}$ et $p\mathbb{Z}$. De la même façon, les sous-groupes maximaux de $\mathbb{Z}/n$ sont ceux engendrés par les diviseurs premiers de n.

2) Une démarche possible, naïve. Partant d'un sous-groupe strict $\mathbf{H}$ d'un groupe fini $\mathbf{G}$, on considère les sous-groupes $\langle \mathbf{H}, x\rangle$ où x est dans $\mathbf{G} \setminus \mathbf{H}$. Si tous ces sous-groupes coïncident avec $\mathbf{G}$, $\mathbf{H}$ est maximal. Sinon, on continue, et ce processus est effectif puisque $\mathbf{G}$ est fini. On a en fait montré que tout sous-groupe strict est inclus dans un sous-groupe maximal.

3) Soit $\mathbf{H}$ un sous-groupe maximal de $\mathbb{Q}$, s'il en existe. Le quotient $\mathbb{Q}/\mathbf{H}$ qui est commutatif, ne peut être qu'un groupe sans sous-groupe, donc cyclique de cardinal p premier (voir le théorème de correspondance). Or $\mathbb{Q}$ n'admet aucun sous-groupe d'indice fini. Si en effet $\mathbb{Q}/\mathbf{H}$ était de cardinal n, tout élément de ce quotient serait d'ordre n, ce qui se traduit par :

$$\forall r \in \mathbb{Q}, nr \in \mathbf{H}$$

Or tout rationnel peut se mettre sous la forme nr ($\frac{p}{q} = n\frac{p}{nq}$), donc $\mathbf{H} = \mathbb{Q}$. Rappelons que la propriété que nous venons d'utiliser traduit que $(\mathbb{Q}, +)$ est un groupe divisible (4.3.)

4) Si $\mathbf{M}$ est d'indice p premier, alors il ne peut exister de sous-groupe strictement inclus entre $\mathbf{M}$ et le groupe entier $\mathbf{G}$: cela est du à l'égalité

$$[\mathbf{G} : \mathbf{M}] = [\mathbf{G} : \mathbf{N}][\mathbf{N} : \mathbf{M}]$$

valable pour une chaîne de sous-groupes (voir 1.1.6). A contrario, un sous-groupe d'indice non premier peut être maximal : dans $\mathcal{S}_4$, il existe des sous-groupes d'indice 4, comme le stabilisateur de 4, isomorphe à $\mathcal{S}_3$ (en fait, tout sous-groupe d'indice 4 est isomorphe à $\mathcal{S}_3$, voir 3.2.11). Ce sous-groupe est maximal : il ne pourrait en effet être inclus que dans un sous-groupe d'ordre 12 ; or, comme tout groupe symétrique, $\mathcal{S}_4$ n'admet qu'un sous-groupe d'indice 2, c'est le groupe alterné $\mathcal{A}_4$. Comme notre sous-groupe d'ordre 6 contient des transpositions, il n'est pas inclus dans le groupe alterné et est donc maximal. Un commentaire : il est rare qu'un sous-groupe d'indice 4 soit maximal...

5) Si $\mathbf{M}$ est normal d'indice non premier, le théorème de correspondance montre qu'il y a bijection entre les sous-groupes de $\mathbf{G}$ contenant $\mathbf{M}$ et les sous-groupes de $\mathbf{G}/\mathbf{M}$; comme ce dernier est de cardinal non premier, il a des sous-groupes non triviaux (par exemple des Sylow), et $\mathbf{M}$ est n'est pas maximal. Dans l'autre sens, cela est dit dans la question précédente.

6) Supposons que le groupe fini $\mathbf{G}$ n'ait qu'un sous-groupe maximal, noté $\mathbf{M}$. Alors soit x un élément de $\mathbf{G} \setminus \mathbf{M}$. Le groupe $\langle x\rangle$ est inclus dans un sous-groupe maximal ou coïncide avec $\mathbf{G}$: comme x n'est pas dans $\mathbf{M}$, $\langle x\rangle = \mathbf{G}$ qui est donc cyclique fini. L'étude des sous-groupes maximaux de $\mathbb{Z}/n$ nous a convaincu qu'il n'y a qu'un sous-groupe maximal ssi $\mathbf{G}$ est cyclique primaire, d'ordre p^n où p est premier, et $\mathbf{M}$ est le (seul) sous-groupe d'ordre p^{n-1}.

7) On rappelle qu'un sous-groupe de $\mathbf{G}$ est caractéristique s'il est stable par tout isomorphisme de $\mathbf{G}$. Si on note $\mathcal{M}$ l'ensemble des sous-groupes maximaux de $\mathbf{G}$, alors l'image par un isomorphisme α d'un élément de $\mathcal{M}$ est aussi un élément de $\mathcal{M}$ (α induit une bijection entre les sous-groupes compris entre $\mathbf{H}$ et $\mathbf{G}$ et ceux compris entre $\alpha(\mathbf{H})$ et $\mathbf{G}$). Ainsi, un automorphisme permute les éléments de $\mathcal{M}$, donc conserve leur intersection $\Phi(\mathbf{G})$. Le sous-groupe de Frattini est caractéristique dans $\mathbf{G}$ donc normal dans $\mathbf{G}$.

Notre étude des sous-groupes maximaux du groupe cyclique $\mathbb{Z}/n$ montre que leur intersection est le groupe engendré par $p_1 p_2 \cdots p_k$ où les p_i sont les facteurs premiers de n. Le sous-groupe de Frattini de $\mathcal{S}_n$ est réduit au neutre : en effet, les stabilisateurs de 1, 2, ..., n sont des sous-groupes maximaux : on peut le démontrer « à la main », mais il est plus direct de se servir des arguments donnés dans le problème 6.2 (partie 6.3.2), et de dire que,

$\mathcal{S}_n$ étant primitif, le stabilisateur d'un élément est un sous-groupe maximal. L'intersection de ces stabilisateurs fixe 1, 2, ..., n, c'est l'identité.

8) Soit x un non générateur et $\mathbf{M}$ un sous-groupe maximal. Si x n'est pas dans $\mathbf{M}$, alors $\langle \mathbf{M}, x\rangle$ est un sous-groupe de $\mathbf{G}$ contenant strictement $\mathbf{M}$, c'est $\mathbf{G}$. l'ensemble $S = \mathbf{M} \cup \{x\}$ est donc générateur, tandis que $S \setminus \{x\}$ ne l'est pas : on en déduit que les non-générateurs sont inclus dans tout sous-groupe maximal, donc dans $\Phi(\mathbf{G})$. Réciproquement, cela fonctionne un peu pareil : si x est dans $\Phi(\mathbf{G})$, supposons que $\mathbf{G} = \langle S, x\rangle$. Alors, si S ne suffit pas à engendrer $\mathbf{G}$, il est inclus dans un sous-groupe maximal $\mathbf{M}$. Mais x est aussi dans tout sous-groupe maximal, donc $\langle S, w\rangle \leqslant \mathbf{M}$, absurde.

Un exemple, dans le cas de $\mathbb{Z}/12$, le sous-groupe de Frattini contient $\overline{0}$ et $\overline{6}$, ce qui signifie que ces deux éléments peuvent être enlevé d'une partie génératrice quelconque sans que cette partie cesse d'être génératrice. Ce n'est pas le cas de, par exemple $\overline{4}$, qui ne peut être ôté de la partie $\{\overline{3}, \overline{4}\}$. Par contre, $\overline{4}$ n'est pas un « générateur » du groupe cyclique, au sens où $\overline{4}$ n'engendre pas à lui seul $\mathbb{Z}/12$.

9) On sait que $\Phi(\mathbf{G})$ est caractéristique dans $\mathbf{G}$, en particulier il est normal dans $\mathbf{G}$. On peut lui appliquer le lemme de Frattini : si on se donne un p-Sylow $\mathbf{S}$ de $\Phi(\mathbf{G})$, on a :

$$\mathbf{G} = \Phi(\mathbf{G})\mathcal{N}_{\mathbf{G}}(\mathbf{S})$$

Mais comme $\Phi(\mathbf{G})$ est entièrement constitué de « non-générateurs », on peut se passer de ses éléments, et $\mathbf{G} = \mathcal{N}_{\mathbf{G}}(\mathbf{S})$. Cela signifie que $\mathbf{S} \lhd \mathbf{G}$ et, a fortiori, $\mathbf{S} \lhd \Phi(\mathbf{G})$. On en déduit (5.3.7) que le groupe de Frattini est toujours nilpotent.

Annexes

I TABLE DES NOTATIONS

$\mathbf{G}$, $\mathbf{H}$, $\mathbf{K}\ldots$	groupes ou sous-groupes
$\mathbf{G}'$	groupe dérivé
$\mathbf{G}_{ab}$	abélianisé, quotient de $\mathbf{G}$ par $\mathbf{G}'$
$\mathbf{L}(X)$	groupe libre engendré par X
$\mathbf{L}_{ab}(X)$	groupe abélien libre engendré par X
$\mathbf{I}$	groupe icosaédral
$\mathbf{O}$	groupe octaédral
$\mathbf{T}$	groupe tétraédral
A, B, $X\ldots$	ensembles
S^n	sphère de rayon 1 dans l'espace de dimension $n+1$
$\mathrm{Aut}(\mathbf{G})$	groupe des automorphismes de $\mathbf{G}$
$\mathrm{Int}(\mathbf{G})$	groupe des automorphismes intérieurs de $\mathbf{G}$
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	corps des rationnels, des réels, des complexes
$\mathbb{H}$	corps des quaternions
$\mathbb{H}_8$	groupe quaternionique
$\mathbb{H}_{2^n}$	groupe quaternionique généralisé
$\mathbb{F}_p$, $\mathbb{F}_q$	corps fini d'ordre p, $q = p^n$
$\mathbb{Z}$, $\mathbb{Z}/n$	groupe additif des entiers relatifs, des entiers modulo n
$\mathbb{Z}$, $\mathbb{Z}/n$	groupe monogène infini, groupe cyclique d'ordre n
$\mathbb{N}$	ensemble des entiers naturels
$(\mathbb{Q}/\mathbb{Z})_p$	p-groupe de Prüfer (notation additive)
$\mathbb{U}$	groupe des nombres complexes de module 1
$\mathbb{U}_n$	groupe des racines n-ièmes de l'unité
$\mathbb{U}_{p^\infty}$	p-groupe de Prüfer (notation multiplicative)
$\mathbb{D}_{2n}$	groupe diédral d'ordre $2n$

$\mathbf{GL}(n,\mathbb{K})$	groupe linéaire, matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$
$\mathbf{SL}(n,\mathbb{K})$	groupe spécial linéaire, matrices carrées $n \times n$ inversibles de déterminant 1
$\mathbf{PGL}(n,\mathbb{K})$	groupe projectif linéaire, quotient du groupe linéaire par son centre
$\mathbf{PSL}(n,\mathbb{K})$	groupe projectif spécial linéaire, quotient du groupe spécial linéaire par son centre
$\mathbf{T}(n,\mathbb{K})$	groupe des matrices triangulaires supérieures inversibles
$\mathbf{TU}(n,\mathbb{K})$	groupe des matrices triangulaires supérieures unipotentes
$\mathcal{A}_n$	groupe alterné, formé par les permutations paires
$\mathcal{C}_{\mathbf{G}}(x)$	centralisateur de x, ensemble des éléments qui commutent à x
$\mathcal{S}_n$	groupe symétrique des permutations de l'ensemble $\{1,2,\ldots,n\}$
$\mathcal{M}(n,\mathbb{A})$	anneau des matrices carrées $n \times n$ à coefficients dans $\mathbb{A}$
$\mathcal{N}_{\mathbf{G}}(\mathbf{H})$	normalisateur de $\mathbf{H}$ dans le groupe $\mathbf{G}$
$\mathcal{Z}(\mathbf{G})$	centre du groupe $\mathbf{G}$
$\langle X \rangle$	groupe engendré par l'ensemble X
$\langle X \mid S \rangle$	groupe engendré par X satisfaisant les relations S
$\langle u \mid v \rangle$	produit scalaire de deux vecteurs
$u \wedge v$	produit vectoriel de deux vecteurs
$n \wedge m$	pgcd de deux entiers
$[x,y]$	$xyx^{-1}y^{-1}$ commutateur de deux éléments
$[\mathbf{G} : \mathbf{H}]$	indice de $\mathbf{H}$ dans $\mathbf{G}$

II DESCRIPTION DES GROUPES AYANT MOINS DE 30 ÉLÉMENTS

Voici des tableaux présentant les premiers groupes finis.

Nombre d'éléments	Nombre de groupes	Cas commutatif	Cas non commutatif	Commentaires
1	1	$\{e\}$		
2	1	$\mathbb{Z}/2$		
3	1	$\mathbb{Z}/3$		
4	2	$\mathbb{Z}/4$		
		$\mathbb{Z}/2 \times \mathbb{Z}/2$		Groupe de Klein, noté $\mathcal{V}$
5	1	$\mathbb{Z}/5$		
6	2	$\mathbb{Z}/6$		
			$\mathcal{S}_3$	ou $\mathbb{D}_6$
7	1	$\mathbb{Z}/7$		
8	5	$\mathbb{Z}/8$		
		$\mathbb{Z}/4 \times \mathbb{Z}/2$		
		$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$		
			$\mathbb{D}_8$	Groupe diédral
			$\mathbb{H}_8$	Groupe quaternionique

La suite :

Nombre d'éléments	Nombre de groupes	Cas commutatif	Cas non commutatif	Commentaires
9	2	$\mathbb{Z}/9$ $\mathbb{Z}/3 \times \mathbb{Z}/3$		
10	2	$\mathbb{Z}/10$	$\mathbb{D}_{10}$	Groupe diédral
11	1	$\mathbb{Z}/11$		
12	5	$\mathbb{Z}/12$ $\mathbb{Z}/6 \times \mathbb{Z}/2$	$\mathcal{A}_4$ $\mathbb{D}_{12}$ $\langle 2,2,3\rangle = \mathcal{T}$	Groupe alterné, tétraédral Groupe diédral Groupe dicyclique
13	1	$\mathbb{Z}/13$		
14	2	$\mathbb{Z}/14$	$\mathbb{D}_{14}$	Groupe diédral
15	1	$\mathbb{Z}/15$		
16	14	$\mathbb{Z}/16$ $\mathbb{Z}/8 \times \mathbb{Z}/2$ $\mathbb{Z}/4 \times \mathbb{Z}/4$ $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	$\mathbb{H}_{16}$ $\mathbb{D}_{16}$ $\mathbb{Q}_8 \times \mathbb{Z}/2$ $\mathbb{D}_8 \times \mathbb{Z}/2$ G_1 G_2 G_3 G_4 G_5	Groupe quaternionique Groupe diédral
17	1	$\mathbb{Z}/17$		
18	5	$\mathbb{Z}/18$ $\mathbb{Z}/3 \times \mathbb{Z}/6$	$\mathcal{S}_3 \times \mathbb{Z}/3$ $\mathbb{D}_{18}$ $(3,3,3;2)$	Groupe diédral
19	1	$\mathbb{Z}/19$		
20	5	$\mathbb{Z}/20$ $\mathbb{Z}/2 \times \mathbb{Z}/10$	$\mathbb{D}_{20} = \mathbb{D}_{10} \times \mathbb{Z}/2$ $\langle 2,2,5\rangle$ $\mathbb{Z}/5 \rtimes \mathbb{Z}/4$	Groupe diédral Groupe dicyclique

Les groupes $\mathbf{G}_i$ ont la présentation :

$$\mathbf{G}_1 = \langle a,b \mid a^8 = b^2 = 1,\ ab = ba^3\rangle, \text{ groupe quasidiédral}$$
$$\mathbf{G}_2 = \langle a,b \mid a^8 = b^2 = 1,\ ab = ba^5\rangle$$
$$\mathbf{G}_3 = \langle a,b \mid a^4 = b^4 = 1,\ ab = ba^3\rangle$$
$$\mathbf{G}_4 = \langle a,b \mid a^4 = b^4 = 1,\ abab = 1,\ ab^3 = ba^3\rangle$$
$$\mathbf{G}_5 = \langle a,b,c \mid a^4 = b^2 = c^2 = 1,\ cbca^2b = 1,\ bab = a,\ cac = a\rangle$$

– Rappels sur les notations

• $\langle 2, 2, m\rangle$ représente le groupe dicyclique d'ordre $4m$, défini ainsi :

$$\langle 2, 2, m\rangle = \langle a, b \mid a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1}\rangle$$

Il fait partie de la famille des groupes définis par :

$$\langle l, m, n\rangle = \langle a, b, c \mid a^l = b^m = c^n = abc\rangle$$

(groupes binaires polyédraux).

• De même, la notation $\langle l, m \mid n\rangle$ représente le groupe défini par :

$$\langle l, m \mid n\rangle = \langle a, b \mid a^l = b^m, (ab)^n = 1\rangle$$

et $\langle l, m \mid n, q\rangle$:

$$\langle l, m \mid n, q\rangle = \langle a, b, c \mid a^l = b^m = c, (ab)^n = c^q = 1\rangle$$

• Enfin, la notation $(3, 3, 3; 2)$ se réfère à :

$$(3, 3, 3 ; 2) = \langle a, b, c \mid a^2 = b^2 = c^2 = (abc)^2 = (ab)^3 = (ac)^3 = 1\rangle$$

À partir de maintenant, nous n'indiquons plus les groupes commutatifs.

Nombre d'éléments	Nombre de groupes	Cas non commutatif	Commentaires
21	2	$\mathbb{Z}/7 \rtimes \mathbb{Z}/3$	
22	2	$\mathbb{D}_{22}$	Groupe diédral
23	1		
24	15	$\mathcal{A}_4 \times \mathbb{Z}/2$	
		$\mathbb{Z}/2 \times \mathbb{D}_{12}$	
		$\mathbb{Z}/3 \times \mathbb{D}_8$	
		$\mathbb{Z}/3 \times \mathbb{Q}_8$	
		$\mathbb{Z}/4 \times \mathcal{S}_3$	
		$\mathbb{Z}/2 \times \langle 2, 2, 3\rangle$	
		$\mathbb{D}_{24}$	Groupe diédral
		$\mathcal{S}_4$	Groupe symétrique, du tétraèdre
		$\langle 2, 3, 3\rangle = \mathbf{SL}(2, \mathbb{F}_3)$	Groupe binaire tétraédral
		$\langle 4, 6 \mid 2, 2\rangle$	
		$\langle -2, 2, 3\rangle$	
		$\langle 2, 2, 6\rangle$	Groupe dicyclique
25	2		
26	2	$\mathbb{D}_{26}$	Groupe diédral
27	5	$(3, 3 \mid 3, 3)$	
		$(\mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes \mathbb{Z}/3$	
28	4	$\mathbb{D}_{28}$	Groupe diédral
		$\langle 2, 2, 7\rangle$	Groupe dicyclique
30		$\mathbb{Z}/3 \times \mathbb{D}_{10}$	
		$\mathbb{Z}/5 \times \mathbb{D}_6$	
		$\mathbb{D}_{30}$	Groupe diédral

III LEXIQUE

Nom de groupes	Définition succincte
abélien	synonyme de groupe commutatif, $ab = ba$ pour tout a et b
alterné	sous-groupe du groupe symétrique formé des permutations paires
commutatif	synonyme de groupe abélien, $ab = ba$ pour tout a et b
complet	groupe de centre trivial et sans automorphisme extérieur
cyclique	groupe fini engendré par un seul élément.Ils sont tous isomorphes à $\mathbb{Z}/n$
dérivé	groupe engendré par les commutateurs
diédral	noté $\mathbb{D}_{2n}$, produit semi-direct de $\mathbb{Z}/n$ par $\mathbb{Z}/2$
dicyclique	groupe engendré par a et b tels que : $a^{2n} = 1$, $b^2 = a^n$, $bab^{-1} = a^{-1}$
de Klein	noté $\mathcal{V}$, appelé aussi groupe du rectangle, c'est $\mathbb{Z}/2 \times \mathbb{Z}/2$
hyperoctaédral	groupe de matrices ayant un seul élément non nul sur chaque ligne et sur chaque colonne, valant ± 1
monogène	groupe engendré par un seul élément. Il est isomorphe à $\mathbb{Z}$ ou est cyclique
nilpotent	groupe ayant une suite de composition centrale
parfait	groupe égal à son sous-groupe dérivé
polycyclique	groupe ayant une suite de composition dont tous les facteurs sont cycliques
polyédral	groupes engendrés par a, b et c tels que : $a^p = b^q = c^r = abc = 1$ Ceux qui sont finis sont liés aux polyèdres réguliers
primitif	sous-groupe d'un groupe de permutation n'ayant que des blocs triviaux
pronormal	sous-groupe $\mathbf{H}$ tel tout conjugué $x\mathbf{H}x^{-1}$ est conjugué dans le groupe $\langle \mathbf{H}, x\mathbf{H}x^{-1} \rangle$
quaternionique	un des deux sous-groupes non commutatifs à huit éléments
quaternionique généralisé	groupe engendré par a et b tels que : $a^{2^n} = 1$, $b^2 = a^{2^{n-1}}$, $bab^{-1} = a^{-1}$
résoluble	groupe ayant une suite de composition dont tous les facteurs sont commutatifs
simple	groupe n'ayant aucun sous-groupe normal autre que trivial
sous-normal	groupe faisant partie d'une chaîne de sous-groupes, chacun étant normal dans le suivant
symétrique	noté $\mathcal{S}_n$, groupe des bijections de $\{1, 2, \ldots, n\}$ dans lui-même

Bibliographie

[1] ALESSANDRI M. — *Thèmes de géométrie*. Dunod, 1999.

[2] ALPERIN J. et BELL R. B. — *Groups and Représentations*. Springer, 1995.

[3] ARNAUDIÈS J. et BERTIN J. — *Groupes et géométrie*. Ellipses, 1996.

[4] BOURBAKI N. —*Algèbre*. Hermann, 1970.

[5] BOUVIER A. et RICHARD D. — *Groupes*. Hermann, 1968.

[6] CALAIS J. — *Éléments de théorie des groupes*. PUF, 1991.

[7] COLLINS D. et ZIESCHANG H. — *Combinatorial Group Theory in Encyclopœdia of Mathematical Sciences*. Springer, 1993.

[8] COXETER H. —*Regular Polytopes*. Dover, 1973.

[9] COXETER H. — *Regular Complex Polytopes*. Cambridge University Press, 1974.

[10] COXETER H. et MOSER W. — *Generators and Relations for Discrète Groups*. Springer, 1965.

[11] DIXON J. D. — *Problems in Group Theory*. Dover, 1973.

[12] DIXON J. D. et MORTIMER B. —*Permutation Groups*. Springer, 1987.

[13] FRANCINOU S. et GIANELLA H. — *Exercices de mathématiques pour l'Agrégation*. Masson, 1993.

[14] GOBLOT R. —*Algèbre linéaire*. Masson, 1995.

[15] GOBLOT R. — *Thèmes de géométrie*. Masson, 1998.

[16] GORENSTEIN D. — *Finite Groups*. Harper & Row, 1968.

[17] HUMPHREYS J. F. —*A Course in Group Theory*. Oxford Science Publications, 1996.

[18] JOHNSON D. — *Presentations of Groups*. Cambridge University Press, 1990.

[19] KARGAPOLOV M. et MERZLIAKOV I. — *Éléments de la théorie des groupes*. Mir, 1985.

[20] MNEIMNE R. —*Éléments de géométrie*. Cassini, 1997.

[21] PERRIN D. — *Cours d'algèbre.* Ellipses, 1996.

[22] ROBINSON D. J. —*A Course in the Theory ofGroups.* Springer, 1991.

[23] ROSE J. S. —*A Course on Group Theory.* Cambridge University Press, 1978.

[24] ROTMAN J. J. —*An Introduction to the theory of Groups.* Springer, 1991.

[25] RUAUD J. et WARUSFEL A. — *Exercices de mathématiques pour l'agrégation.* Masson, 1995.

[26] SCOTT W. — *Group Theory.* Dover, 1964.

[27] DU VAL P. — *Homographies, Quaternions and Rotations.* Oxford University Press, 1964.

Adresses Internet

`http ://www.bath.ac.uk`
Site du « group pub forum » où les chercheurs en théorie des groupes se retrouvent pour se poser des questions, chercher des références. On y découvre une liste de discussions et des liens.

`http ://www.mat.bham.ac.uk`
Site de l'atlas des groupes finis. Il donne, en particulier, la table des caractères ainsi qu'une présentation des groupes classiques.

`http ://www-history.mcs.st-and.ac.uk/gap`
Site du logiciel GAP (Groups, Algorithms & Programming). Ce logiciel, gratuit et très riche, est un logiciel de calcul formel mathématique. Il permet de faire de l'arithmétique, de l'algèbre linéaire, mais surtout de la théorie des groupes, notamment des groupes finis.

`http ://www.mupad.de`
Encore un logiciel, développé par des universitaires, et adapté au calcul formel.

`http ://www.maplesoft.on.ca`
Le célèbre logiciel de calcul formel. Très puissant, il contient des fonctions utilisables pour l'étude des groupes.

`http ://www.math.niu.edu`
Parmi de nombreux exemples, un site où l'on trouve un cours d'algèbre.

`http ://www.clarku.edu`
Groupes et géométrie : les groupes de pavages, avec beaucoup d'illustrations.

Index

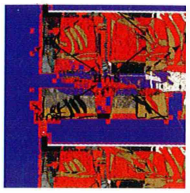
050667 - (I) - (1) - OSB 80° - PUB - API

Achevé d'imprimer sur les presses de SNEL Grafics sa – Z. I. des Hauts Sarts - Zone 3 – Rue Fond des Fourches 21
B-4041 Vottem (Herstal) – Tél +32 (0)4 344 65 60 - Fax +32 (0)4 286 9 9 61 – février 2007 – 41065

Dépôt légal : mars 2007 – Dépôt légal de la 1re édition : avril 2001

Imprimé en Belgique

SCIENCES SUP



2e édition

Jean Delcourt

THÉORIE DES GROUPES

Rappels de cours, exercices et problèmes corrigés

Depuis leur introduction au XIXe siècle par Évariste Galois, les groupes sont devenus incontournables en mathématiques, tant en algèbre qu'en analyse. La théorie des groupes est maintenant un domaine extrêmement vaste, avec de nombreuses spécialités faisant l'objet d'autant de recherches.

Cette deuxième édition révisée constitue un recueil d'exercices et de problèmes corrigés puis commentés, qui permet d'étudier, en plus des théorèmes de base, de nombreux et variés exemples de groupes, en insistant plus particulièrement sur les groupes finis. Mais c'est aussi un livre de « cours par les exercices », inspiré des méthodes anglo-saxonnes et russes, qui permet au lecteur, aidé par des rappels de cours, de démontrer lui-même de nombreux théorèmes à travers différents exemples.

Destiné aux étudiants en mathématiques de Licence 3 / Master 1, cet ouvrage sera également utile aux candidats à l'Agrégation et au Capes de mathématiques.

JEAN DELCOURT
est professeur agrégé (ENS Saint-Cloud) à l'université de Cergy-Pontoise.

MATHÉMATIQUES
PHYSIQUE
CHIMIE
SCIENCES DE L'INGÉNIEUR
INFORMATIQUE
SCIENCES DE LA VIE
SCIENCES DE LA TERRE

LICENCE | MASTER | DOCTORAT
1 2 3 4 5 6 7 8

9 782100 506675

6494371
ISBN 978-2-10-050667-5