Théorie des groupes

François Capaces[1], Christophe Antonini[2], Olivier Teytaud[3], Pierre Borgnat[4], Annie Chateau[5], and Edouard Lebeau[6]

[1], ,
[2]Enseignant en CPGE, Institut Stanislas, Cannes
[3]Chargé de rechercher INRIA, Université d'Orsay, Orsay
[4]Chargé de recherche CNRS, ENS Lyon, Lyon
[5]Maitre de conférence, Université Montpellier-2, Montpellier
[6]Enseignant en CPGE, Lycée Henri Poincaré, Nancy

25 novembre 2021

Introduction à la théorie des groupes et étude de quelques groupes classiques.

1 Théorie des groupes

La théorie des groupes apparaît au premier abord un sujet bizarre, abstrait, déconnecté du réel. En fait, via les travaux de J.-L. Lagrange, les groupes émergent pour l'étude des équations algébriques ; E. Galois utilise les groupes pour l'étude du corps de décomposition d'un polynôme séparable. La géométrie a aussi été un fournisseur, avec notamment les groupes de permutations et d'isométries. Ainsi, l'histoire n'a pas suivi la désormais classique introduction à l'algèbre par (i) groupes (ii) anneaux (iii) corps : les groupes ont émergé peu à peu comme dénominateur commun

à beaucoup de choses ([1]). Il est à noter que l'on peut faire des choses intéressantes aussi avec des structures algébriques plus simples que les groupes, comme les monoïdes (qui ont une loi de composition interne associative et un élément neutre), qui sont eux-mêmes un peu plus qu'un semi-groupe (dans un semi-groupe, on n'impose pas l'existence d'un élément neutre). Les groupoïdes, qu'on ne discutera pas non plus, sont au contraire une « complication » des groupes (un groupe s'identitifie à un groupoïde, mais les groupoïdes ne s'identifient pas en général à des groupes). On définira plus loin des algèbres (qui serviront dans des cadres très variés, dont l'analyse), des espaces vectoriels (qui nous serviront en géométrie bien sûr, mais aussi en analyse fonctionnelle), etc. La transition (artificielle) de l'algèbre vers l'analyse est en général datée à peu près à l'instant où de l'infinitésimal (topologie ou différentiation) arrive, de même que la transition de la théorie des ensembles (la base) vers le reste est à peu près à l'instant où on ne voit plus les axiomes dans la vie quotidienne ; cela dit, l'axiome du choix n'en finit pas de revenir un peu partout, et la théorie de la mesure, bien analytique et bien concrète, impacte directement les choix axiomatiques (axiome de Solovay, axiome du choix).

Après les bases (1.1), on verra la notion centrale de groupe quotient (1.2), les opérations de groupe (1.3), les produits (en tout genre) de groupes (1.4), les théorèmes de Sylow (1.5) et leurs applications (1.6), les groupes abéliens (1.7), puis quelques exercices (1.8) et un peu de zoologie (1.9 pour les actions de groupes et 1.10 pour le reste), suivie pour finir d'applications à la géométrie (1.10.12). Des références pour aller plus loin sont [**?**, 3, **?**, **?**, 1].

1.1 Les bases

1.1.1 Définition d'un groupe

Un **groupe** est un ensemble G, muni d'une **loi de composition interne** (lci), c'est-à-dire une application de $G \times G \to G$, généralement notée par la concaténation ($(x, y) \mapsto xy$), vérifiant :
•$\forall x, y, z\ (xy)z = x(yz)$
•$\exists 1 : \forall x\ x.1 = 1.x = x$; 1 est dit l'élément neutre
•$\forall x \exists x^{-1}; xx^{-1} = x^{-1}x = 1$

Pour vérifier qu'un ensemble muni d'une lci est bien un groupe, il suffit de vérifier que les deux premiers •sont vérifiés, et que pour tout x il existe x^{-1} tel que $xx^{-1} = 1$.

G est dit **commutatif ou abélien** si $\forall x, y\ xy = yx$. Dans ce cas on note souvent la loi additivement ; l'élément neutre est alors noté 0, et x^{-1} est noté $-x$.

G est un **p-groupe**, avec p premier, si G est de cardinal une puissance de p.

1.1.2 Homomorphismes

On appelle **homomorphisme** du groupe G dans le groupe G' une fonction ϕ telle que $\forall x, y\ \phi(xy) = \phi(x)\phi(y)$.

On montre que pour tout tel ϕ :
•$\phi(1) = 1$
•$\forall x\ \phi(x^{-1}) = \phi(x)^{-1}$
On note $Hom(G, G')$ l'ensemble des homomorphismes de G dans G'.

La fonction constante égale à 1 est un homomorphisme de G dans G' ; éventuellement ce peut être le seul.

L'inverse d'un homomorphisme bijectif est un homomorphisme bijectif.

L'ensemble des **automorphismes**, i.e. des **endomorphismes** bijectifs, i.e. homomorphismes de G dans G bijectifs, noté $Aut(G)$, est un groupe pour la composition.

Exemple 0.1 Exemples

— G groupe, $x \in G$

$\phi_x \in Hom(\mathbb{Z}, G)$, avec $\phi_x(n) = x^n$; le plus petit n tel que $\phi_x(n) = 1$, s'il existe est appelé ordre de x.

— G groupe, $g \in G$

La fonction $\alpha_g : x \mapsto gxg^{-1}$ est un automorphisme de G, dit automorphisme **intérieur** associé à g, appelée aussi **conjugaison** par g. En outre la fonction $g \mapsto \alpha_g$ est un homomorphisme de G dans $Aut(G)$. Son noyau est le centre de G.

L'ensemble des automorphismes intérieurs d'un groupe est un sous-groupe (la notion de sous-groupe est définie ci-dessous) de l'ensemble des automorphismes du groupe.

(G, G') groupes, $\phi \in Hom(G, G')$

$\bullet Ker\ \phi := \{g \in G / \phi(g) = 1\}$ est un sous-groupe distingué de G.

$\bullet Im\ \phi = \{\phi(g)\ ;\ g \in G\}$ est un sous-groupe de G'.

$\bullet \phi$ injectif $\iff Ker\ \phi = \{1\}$

1.1.3 Sous-groupe

DÉFINITION 0.1 **Sous-groupe**
$H \subset G$ est un **sous groupe de** G si et seulement si :
- $\bullet 1 \in H$
- $\bullet (x, y) \in H^2 \to xy \in H$
- $\bullet \forall x \in H,\ x^{-1} \in H$

Un sous-groupe est un groupe, et tout groupe contenu dans un groupe (pour les mêmes lois) est un sous-groupe de ce groupe. Cela ne sera pas le cas pour les anneaux.

On peut noter les conditions dessus plus simplement : $1 \in H \wedge HH \subset H \wedge H^{-1} \subset H$

DÉFINITION 0.2 **distingué**
Deux sous-groupes A et B de G sont dits **conjugués** s'il existe $g \in G$ tel que $A = g.B.g^{-1}$.

Étant donné H sous-groupe de G, le **normalisateur** de H est $N_G(H) = \{g \in G; gHg^{-1} = H\}$.

Un sous-groupe N est dit **distingué** (ou **normal**) si pour tout $g \in G$ $gNg^{-1} = N$; on note $N \lhd G$. Cela signifie qu'il est stable par tout automorphisme intérieur (définition d'un automorphisme en partie 1.1.2).

Un sous-groupe N est dit **caractéristique** si il est stable par tout automorphisme.

Un groupe est dit **simple** si ses seuls sous-groupes distingués sont $\{1\}$ et G.

L'ensemble des x tels que x commute avec tout élément est appelé le **centre** d'un groupe. Le centre est un sous-groupe. On note $Z(G)$ le centre de G.

Intuition Il faut bien voir ce que dit la définition du normalisateur – le normalisateur de H « fait » de H un sous-groupe normal, au sens où H est normal dans son normalisateur. En fait le normalisateur est le plus grand sous-groupe contenant H dans lequel H est distingué.

Propriétés •Un sous-groupe est distingué si et seulement si son normalisateur est le groupe tout entier.

•Un sous-groupe est distingué si et seulement si il n'est conjugué à aucun autre sous-groupe.

•Un sous-groupe caractéristique est distingué (évident).

•Tout sous-groupe d'un groupe abélien est distingué ; par contre, en considérant H_8 le groupe des quaternions, on peut constater qu'il n'y a pas de réciproque (voir 1.10.10).

•$\{1\}$ et G sont toujours à la fois des sous-groupes distingués et caractéristiques.

•Le centre d'un groupe est caractéristique et distingué.

Exemple – $\mathbb{Z}/p\mathbb{Z}$ est simple (en effet ses seuls sous-groupes sont ses sous-groupes triviaux, donc ses seuls sous-groupes distingués sont ses sous-groupes triviaux).
– U_n est simple (voir §1.10.11, page 35)

DÉFINITION 0.3 **commutateur**
On appelle **commutateur** de x et y l'élément $x.y.x^{-1}.y^{-1}$.

On appelle **groupe dérivé** d'un groupe le sous-groupe engendré (Voir paragraphe 1.1.5 pour la définition de sous-groupe engendré par une partie) par les commutateurs. On note $D(G)$ le groupe dérivé de G.

Il faut bien noter que l'ensemble des commutateurs n'est pas nécessairement un groupe ; le groupe dérivé est le **sous-groupe engendré** par l'ensemble des commutateurs.

$D(G)$ est distingué et même caractéristique dans G.

1.1.4 Extensions

DÉFINITION 0.4 **suite exacte**
On appelle **suite exacte** un schéma comme suit :

$$1 \xrightarrow{} A \xrightarrow{i} B \xrightarrow{s} C \xrightarrow{} 1$$

où A, B et C sont des groupes, et
•i est un homomorphisme injectif de A dans B
•s est un homomorphisme surjectif de B dans C
•$Ker\ s = Im\ i$
(on note 0 au lieu de 1 lorsque les groupes sont notés additivement)
Lorsque i et s ne sont pas précisés, cela signifie simplement que l'on peut trouver de tels i et s.
On dit alors que B est une **extension** de A par C. Si en outre il existe $\overline{C}$ sous-groupe de B tel que la restriction de s à $\overline{C}$ est un isomorphisme, alors on dit que $\overline{C}$ est un **relèvement**. Cela est équivalent à dire qu'il existe un homomorphisme t de C dans B tel que $s \circ t = Id_C$. S'il y a un relèvement, l'extension est dite **scindée**, et t est appelée **section** de s.

1.1.5 Sous-groupe engendré

PROPOSITION 0.1
Soit G un groupe, X inclus dans G.
Il existe un plus petit sous-groupe H de G contenant X. On peut le définir de deux façons :
(i) H est l'intersection de tous les sous-groupes contenant X
(ii) H est l'ensemble des produits finis d'éléments de $X \cup X^{-1}$.

Démonstration *(i) est évident car l'intersection de sous-groupes est un sous-groupe.*
(ii) on procède en trois points :
•*K ainsi défini est un sous-groupe*
•*$X \subset K$ donc par (i) $H \subset K$*
•*$K \subset H$ est clair.*

DÉFINITION 0.5 **partie génératrice**
On note $H =< X >$, H est appelé groupe **engendré** par X, et X est appelée **partie génératrice** de H. Si X est réduit à un seul élément x on note souvent $H =< x >$ au lieu de $H =< \{x\} >$.
Un groupe est dit **monogène** s'il est engendré par un seul élément. On appelle groupe **cyclique** un groupe monogène fini.
On appelle **ordre d'un élément** le cardinal du groupe engendré par cet élément.

Intuition Si deux homomorphismes coïncident sur une partie génératrice d'un groupe, alors ils coïncident sur l'ensemble du groupe.

Application 0.2 Cela sera utile pour la proposition 0.23. Pour aller loin des sentiers battus, les groupes cycliques sont utilisés en analyse de discrépance ([2]), elle-même utilisable en intégration par quasi-Monte-Carlo.

DÉFINITION 0.6 **de type fini**
On dit que G est **de type fini** si $\exists X$ fini qui engendre G.

Ainsi $\mathbb{Z}$, $\mathbb{Z}^n$ sont de type fini, et tout groupe fini est de type fini.

Intuition Tout groupe de type fini est dénombrable.
Il n'y a pas de réciproque, car par exemple $(\mathbb{Q}^*, \times)$ n'est pas de type fini bien que dénombrable (preuve en considérant des hypothétiques générateurs et leurs décompositions en facteurs premiers)

$(\mathbb{Q}, +)$ non plus (considérer l'inf de l'intersection avec R^+ d'un ensemble fini de générateurs, en réduisant au même dénominateur)

PROPOSITION 0.2
Le groupe engendré par un ensemble réduit à un élément x est commutatif, et est l'ensemble des x^n avec $n \in \mathbb{Z}$. Il est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/k\mathbb{Z}$ pour un certain $k \in \mathbb{N}$.

Démonstration *$\{x^n\}$ est un groupe et contient x, donc il est inclus dans $< x >$; s'il est fini alors il existe un plus petit n tel que $x^p = x^{p+n}$, et donc $x^n = 1$, et donc $< x >= \{x^0, ..., x^{n-1}\}$.*

PROPOSITION 0.3
Tout sous-groupe d'un groupe cyclique est cyclique.

Démonstration *Un tel sous-groupe H de G est évidemment fini. Notons ensuite a un générateur du groupe G ; le groupe est donc de la forme $a^0, ..., a^{n-1}$. Soit $p > 0$ minimal tel que $a^p \in H$; montrons que les $(a^p)^q$ pour $q \in \mathbb{N}$ recouvrent H. Soit $h \in H$. Pour un certain k, $h = a^k$. Par définition de p, $p \leq k$. Soit i maximal tel que $k = ip + q$ avec $0 \leq q < p$; alors $h = a^k = a^{ip}a^q = (a^p)^i a^q$. On a alors $a^q = h/(a^p)^i$; or*

- *$h \in H$,*
- *$a^p \in H$ par définition de p et donc aussi $(a^p)^i \in H$;*
- *$a^q = ((a^p)^i)^{-1}h$, produit d'éléments de H, est donc aussi élément de H.*

a^q est donc élément de H bien que $q < p$; par définition de p (minimal tel que $a^p \in H$ parmi les $p > 0$), q est donc nul. Ceci implique que $(a^p)^i = h$. Ceci vaut pour tout h ; on a donc bien montré que H était engendré par a^p.

1.2 Groupe quotient

Après avoir rappelé la notion d'ensemble quotient, on présentera la notion de groupe quotient, avant de passer au fameux théorème de Lagrange quant aux cardinaux des groupes.

1.2.1 Rappel : ensemble quotient

Soit X un ensemble, et $\mathcal{R}$ une relation d'équivalence sur X ; l'ensemble des classes pour $\mathcal{R}$ est une partition de X. Cet ensemble de classes, noté $X/\mathcal{R}$, est appelé **ensemble quotient** de X par $\mathcal{R}$. La classe d'un élément est notée $\Pi(x)$, x est dit un représentant de $\Pi(x)$. Π est appelée **surjection canonique**.

Il y a en fait ainsi bijection entre l'ensemble des relations d'équivalence et l'ensemble des partitions en parties non vides. À toute relation d'équivalence $\equiv$ on peut associer une fonction f telle que $x \equiv y \iff f(x) = f(y)$ (il suffit pour le montrer de considérer la fonction Π).

Étant donnée une fonction définie sur X, on peut définir $\overline{f}$ **fonction quotient** si f est constante sur les classes d'équivalences, $\overline{f}$ étant alors définie par $\overline{f}(\Pi(x)) = f(x)$.

1.2.2 Le cas des groupes

DÉFINITION 0.7 **classes à gauche de G suivant H**
Étant donné H un sous-groupe de G, on définit les **classes à gauche de G suivant H** comme les xH, $x \in G$, et les **classes à droite suivant** H comme les Hx.
On note G/H l'ensemble des classes à gauche, $H \setminus G$ l'ensemble des classes à droite.
On note $(G : H)$ le cardinal de G/H quand celui-ci est fini.

On travaille généralement sur G/H plutôt que sur $H \setminus G$.

PROPOSITION 0.4
Les classes à gauche déterminent une partition de G en parties non vides. Pareil pour les classes à droite.

PROPOSITION 0.5
Étant donné N sous-groupe de G, il y a équivalence entre les trois assertions suivantes :
- N est distingué
- $gN = Ng$ pour tout g
- il existe une structure de groupe sur le quotient G/N telle que Π soit un homomorphisme.

On voit donc que dans ce cas $G/H = H \setminus G$. Cette propriété d'un sous-groupe distingué est fondamentale : la partition en classes à droite est égale à la partition en classes à gauche. Ce fait est caractéristique des sous groupes distingués.

PROPOSITION 0.6
G et G' deux groupes, N sous-groupe distingué de G, $\phi \in Hom(G, G')$; alors les deux assertions suivantes sont équivalentes :
- Il existe $\overline{\phi}$ de G/N dans G' tel que $\phi = \overline{\phi} \circ \Pi$
- $N \subset Ker\ \phi$

Dans ce cas $\overline{\phi}$ est unique, et est un homomorphisme de groupes de G/N dans G'.

THÉORÈME 0.7
En particulier, $\overline{\phi}$ est une injection si $N = Ker\ \phi$, et induit un isomorphisme de $G/(Ker\ \phi)$ dans $Im\ \phi$.

Les preuves de ces faits sont faciles, et ces résultats sont logiques intuitivement ; si on quotiente par quelque chose de 'trop gros' par rapport au noyau, alors on n'a plus la précision requise pour reconstruire la fonction.

$G/D(G)$ est un groupe abélien ($D(G)$ est le groupe dérivé, cf plus haut), c'est d'ailleurs le plus grand quotient abélien de G.

THÉORÈME 0.8 **Factorisation d'homomorphismes**
Soit G un groupe, H un sous-groupe distingué de G, ϕ un homomorphisme de G vers un groupe G'.

Si $H \subset Ker\ \phi$, alors il existe une application $\tilde{\phi}$ de G/H dans G' telle que

$$\phi = \tilde{\phi} \circ p$$

avec p la projection canonique de G sur G/H.

Application 0.3 Cela servira par exemple pour le théorème 0.26.

Démonstration *On ne donnera ici que quelques éléments, en laissant le reste des vérifications au lecteur. La fonction $\tilde{\phi}$ est bien définie, car si deux éléments ont même image par p alors ils ont même image par ϕ, et l'application $\tilde{\phi}$ est bien un homomorphisme car ϕ en est un.*

1.2.3 Le théorème de Lagrange

DÉFINITION 0.8 **indice de H dans G**
On appelle **indice de H dans G**, avec H un sous-groupe de G, le cardinal de G/H.

Un théorème fondamental :

THÉORÈME 0.9 **Théorème de Lagrange**
Soit G un groupe fini, et H un sous-groupe de G, alors

$$|G| = |H|.|G/H|$$

Démonstration *Il suffit de montrer que chaque classe d'équivalence est de même cardinal, et que ce cardinal est $|H|$ (chose facile à prouver !).*
On remarque qu'il n'est absolument pas nécessaire que H soit distingué.

1.3 Opération d'un groupe sur un ensemble

DÉFINITION 0.9 **action à gauche**
Avec G un groupe et X un ensemble, on appelle **action à gauche** de G sur X une application α de $G \times X$ dans X telle que :
•$\forall x \ \ \alpha(1, x) = x$
•$\forall g, h, x \ \ \alpha(g, \alpha(h, x)) = \alpha(g.h, x)$
On dit aussi que G **opère à gauche** sur X où que G est une **opération à gauche** sur X. Usuellement on note plus simplement $g.x$ au lieu de $\alpha(g, x)$. Les deux conditions deviennent alors :
•$1.x = x$
•$g.(h.x) = (g.h).x$
On définit de manière symétrique une **action à droite**. Une **action** sans plus de précision désigne une action à gauche. On dit que X est un **G-ensemble**.

Propriétés •$g.x = y \iff g^{-1}.y = x$
•Étant donné x et y dans X il n'est pas du tout nécessaire qu'il existe un g tel que $g.x = y$.
•Si G opère sur X alors tout sous-groupe H de G opère sur X pour la loi restreinte.

L'équivalence suivante est fondamentale : se donner une action de G sur X revient à se donner un homomorphisme ϕ de G dans le groupe $\sigma(X)$ des permutations de X ($g.x = \phi(g).x$).

Un exemple fondamental est l'action d'un groupe sur lui-même ; l'action est en fait simplement la loi du groupe. Il est clair que les conditions sont vérifiées.

Pour le cas des actions à droite, il faut noter que si on a une action à droite $a_1(x, g)$, alors $a_2(g, x) = a_1(x, g^{-1})$ est une action à gauche du groupe opposé (le groupe opposé à G étant G (en

tant qu'ensemble) muni de la loi $(x, y) \to yx$). On travaillera à peu près toujours avec des classes à gauche, les résultats étant les mêmes, et puisqu'on peut reformuler un problème d'actions à droite en terme d'actions à gauche.

DÉFINITION 0.10 **isomorphisme**
Étant donnés X et X' deux G-ensembles, on appelle **G-homomophisme** de X vers X' une application ϕ de X dans X' telle que $\phi(g.x) = g.\phi(x)$ pour tous $x \in X$ et $g \in G$. On note $Hom(X, X')$ l'ensemble des homomorphismes de X sur X'. Comme d'habitude, un **isomorphisme** est un homomorphisme bijectif.

Un exemple facile et classique : soit G un groupe et X un G-ensemble. L'application ϕ_x pour $x \in X$ qui à g dans G associe $g.x$ est un homomorphisme de G (en tant que G-ensemble) sur X (en tant que G-ensemble).

Démonstration *Soit g dans G et y dans G (y est pris dans G en tant que G-ensemble) alors $\phi_x(g.y) = g.y.x$ et $g.\phi_x(y) = g.y.x$.*

DÉFINITION 0.11 **G-orbite**
On note G_x et on appelle **stabilisateur** ou **fixateur** de $x \in X$ l'ensemble des $g \in G$ tels que $g.x = x$. C'est un sous-groupe de G, qui n'est pas nécessairement distingué.

On appelle **G-orbite** de x appartenant à X (ou plus simplement **orbite** s'il n'y a pas de risque de confusion) et on note $\omega(x)$ ou $G.x$ la classe d'équivalence de x pour la relation $\mathcal{R}$ définie par $a\mathcal{R}b \iff \exists g \in G / g.a = b$ (il est facile de vérifier qu'il s'agit bien d'une relation d'équivalence).

Un G-ensemble est dit **homogène** s'il ne contient qu'une seule orbite.

On dit que $x \in X$ est un **point fixe**, si l'orbite de x est réduite à $\{x\}$.

On dit que G opère **transitivement** si $\forall x \forall y \exists g\ y = g.x$.

On dit que G opère k **fois transitivement** si $\forall (x_i)_{i\in\{1,\dots,k\}} \forall (y_i)_{i\in\{1,\dots,k\}} (i \neq j \to x_i \neq x_j \wedge y_i \neq y_j) \to \exists g \forall i \in \{1, ..., k\} / y_i = g.x_i$.

On dit que G opère **fidèlement** si $(\forall x\ g.x = x) \to g = 1$.

De manière équivalente, G opère fidèlement si l'action α est injective (i.e. $Ker\ \alpha = \{1\}$), où l'on voit α comme un morphisme de G dans l'ensemble des permutations (i.e. des bijections) de X.

Application 0.4 On verra une jolie application des orbites avec la définition formelle **??** de polygone régulier (ou polyèdre régulier, etc).

PROPOSITION 0.10
Lorsque G est fini, on a pour tout x dans X, $|\omega(x)|.|G_x| = |G|$.

Démonstration *On constatera simplement que l'application qui à $\overline{g}$ associe $g.x$ de G/G_x dans $\omega(x)$ est une bijection.*

La figure 1 tâche de montrer l'allure générale d'un G-ensemble.

Propriétés Chaque orbite est un ensemble homogène.

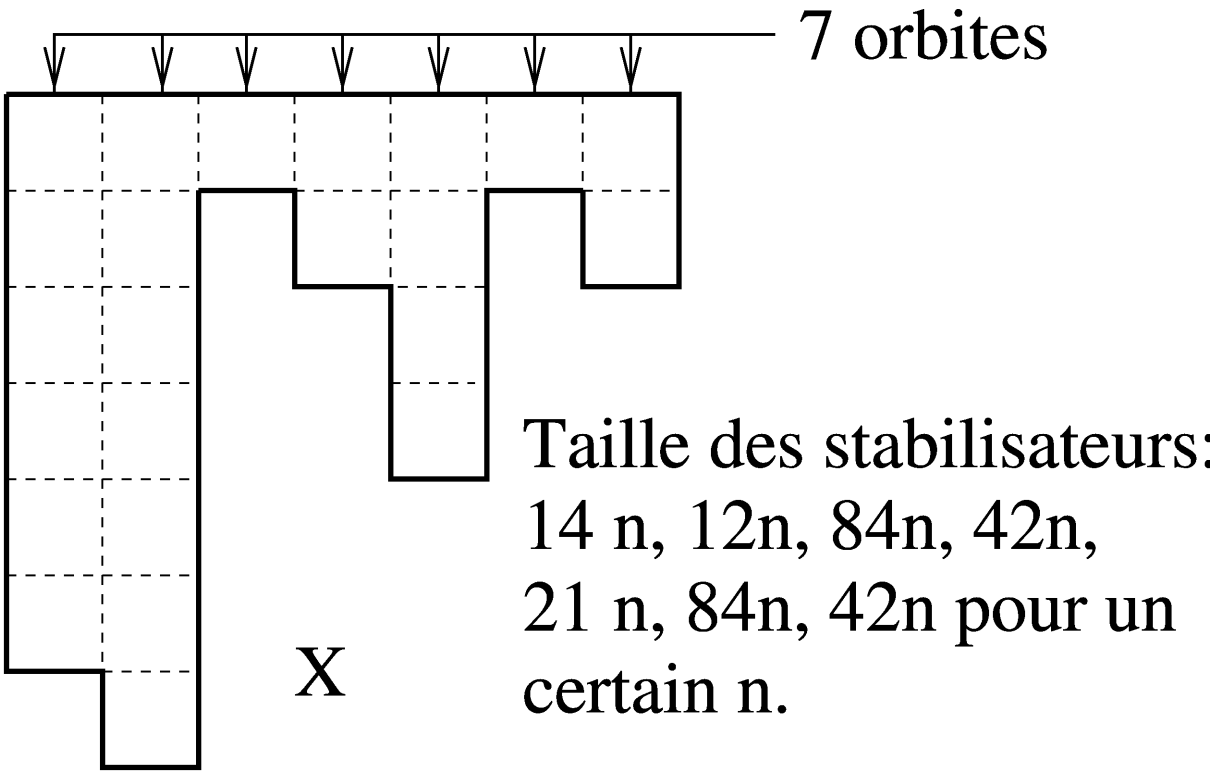

FIGURE 1 – Exemple de G-ensemble X.
Commentaire : Les séparations verticales sont les séparations entre les orbites, qui réalisent une partition de X. L'action n'étant pas nécessairement injective, les orbites ne sont pas nécessairement de même cardinal que G. A l'intérieur d'une même orbite, le stabilisateur est toujours le même à conjugaison près, et en particulier, les stabilisateurs dans une même orbite sont équipotents. Si le groupe et l'ensemble sont finis, le cardinal du groupe est le produit du cardinal de l'orbite par le cardinal d'un stabilisateur de cette orbite. On notera que le cardinal du groupe agissant sur cet ensemble est au moins 84 (ppcm des cardinaux des orbites).

PROPOSITION 0.11
G groupe, X et X' des G-ensembles homogènes, alors les assertions suivantes sont équivalentes :
- $X \simeq X'$
- $\exists (x, x') \in X \times X'; G_x = G_{x'}$
- $\exists (x, x') \in X \times X'; G_x$ est conjugué à $G_{x'}$
- $\forall (x, x') \in X \times X', G_x$ est conjugué à $G_{x'}$

Démonstration *laissée en exercice.*

Intuition Cas classiques :

•Le groupe orthogonal $O(3, \mathbb{R})$ opère sur $\mathbb{R}^3$; les orbites sont les sphères de centre l'origine, le stabilisateur de 0 est $O(3, \mathbb{R})$ tout entier, et le stabilisateur d'un point quelconque autre que 0 est l'ensemble des rotations d'axe la droite vectorielle engendrée par ce point et des symétries par rapport à un sous-espace vectoriel passant par ce point. 0 est un point fixe.

•On peut faire opérer G sur ses sous-groupes par conjugaison, avec $g.H = gHg^{-1}$. Le stabilisateur d'un point (c'est-à-dire d'un sous-groupe) est alors le normalisateur de ce point (*i.e.* de ce sous-groupe).

•Si X est un espace topologique et est un G-ensemble tel que pour tout $g \in G$ l'application $y \mapsto g.y$ est un homéomorphisme, alors on dit que G **agit sur** X **par homéomorphismes**. La topologie quotient pour la relation d'équivalence « être dans la même orbite » vérifie des propriétés intéressantes (voir proposition **??** et théorème **??**).

PROPOSITION 0.12
Un G-ensemble homogène est isomorphe à un quotient G/H de G pour l'action de G sur G/H par translation à gauche.

Pour bien voir l'intérêt de cette remarque, il faut se rappeler que tout G-ensemble est partitionné naturellement en orbites, qui sont des G-ensembles homogènes, et que donc on peut identifier à des actions par translation d'un groupe sur un groupe quotient.

PROPOSITION 0.13 **Sur l'ensemble des points fixes**
Étant donnés G un p-groupe et X un ensemble sur lequel agit G, le cardinal de l'ensemble des points fixes de X pour G est congru au cardinal de X modulo p.

Démonstration *Le cardinal des orbites divise le cardinal de G, donc le cardinal de l'union des orbites est congru au nombre d'orbites de cardinal 1 modulo p. Le cardinal de l'union des orbites est le cardinal de X.*

1.4 Produits

Il faut bien noter que même si de nombreuses applications des résultats ci-dessous se font avec des groupes finis, ils sont valables pour des groupes quelconques.

1.4.1 Produit direct

Définition 0.12 **Produit direct de deux groupes**
On appelle **produit direct** de deux groupes N et H et on note $N \times H$ le produit cartésien des groupes N et H muni du produit terme à terme

$$(n, h).(n', h') = (nn', hh')$$

La fonction p_2 qui à (n, h) associe h est appelée **projection** de $N \times H$ sur H.

La fonction p_1 qui à (n, h) associe n est appelée **projection** de $N \times H$ sur N.

On définit alors la généralisation à un produit d'un nombre quelconque de groupes $\Pi_{i\in I}G_i$. La loi

$$((g_i)_{i\in I}, (h_i)_{i\in I}) = (g_i h_i)_{i\in I}$$

munit le produit d'une structure de groupe ; on appelle ce groupe le **groupe produit**.

On définit aussi le **produit restreint** des G_i comme étant le sous-groupe du produit des G_i des éléments $(g_i)_{i\in I}$ ne comportant qu'un nombre fini de g_i différents de l'élément neutre. S'il s'agit d'un produit d'un nombre fini de groupes il est clair que le produit restreint est égal au produit.

•p est surjective, c'est un morphisme surjectif, son noyau est distingué et isomorphe à N. On a une suite exacte

$$1 \to N \xrightarrow{i} N \times H \xrightarrow{p} H \to 1$$

avec $i(n) = (n, 1)$.

•$N \times \{1\}$ est le noyau de p, il est distingué ; et $\{1\} \times H$ est distingué aussi.

1.4.2 Produit semi-direct

Définition 0.13 **Produit semi-direct**
Étant donnés deux groupes N et H, et un morphisme de groupe ϕ de H dans l'ensemble des automorphismes de N (autrement dit, ϕ est une action de H sur N) ; alors on appelle produit semi-direct de N et H relativement à ϕ et on note $N \rtimes H$ le produit cartésien $N \times H$ muni de la loi $(n, h).(n', h') = (n(h.n'), hh')$.

On note que formellement il faudrait préciser $N \rtimes_\phi H$ pour souligner la dépendance en ϕ.

Application 0.5 On verra une jolie application du produit semi-direct avec l'étude de $O_2(\mathbb{R})$ (proposition **??**).

Proposition 0.14
Quelques propriétés des produits semi-directs :•$N \rtimes H$ est un groupe

•On a une suite exacte

$$1 \to N \xrightarrow{i} N \rtimes H \xrightarrow{s} H \to 1$$

avec $i(n) = (n, 1)$ et $s(n, h) = h$.

•$i(N)$, c'est-à-dire $N \times \{1\}$ est distingué, mais pas $\{1_N\} \times H$ (contrairement au cas du produit direct).

Démonstration *Vérification facile.*

Intuition En identifiant N et $N \times \{1\}$ d'une part, H et $\{1\} \times H$ d'autre part, on constate qu'un produit semi-direct peut toujours s'écrire comme produit semi-direct de deux sous-groupes lié au morphisme ϕ de G dans $Aut(N)$ défini par $(\phi(h))(n) = hnh^{-1}$.

1.4.3 Identifier un produit direct ou semi-direct

Cette partie est fondamentale pour ramener l'étude d'un groupe à l'étude de groupes plus petits (tâche fondamentale en théorie des groupes !).

PROPOSITION 0.15 **Décomposition en produit semi-direct**
Si on a une suite exacte

$$1 \to N \xrightarrow{i} G \xrightarrow{s} H \to 1$$

(c'est-à-dire si i est injective, si s est surjective, et si $Ker\ s = Im\ i$) et si on a un sous-groupe $\overline{H}$ de G sur lequel la restriction de s est un isomorphisme vers H (c'est-à-dire un relèvement, une section, voir la partie 1.4.2), alors G est isomorphe à $i(N) \rtimes \overline{H}$ relativement à la loi de l'automorphisme intérieur (voir la remarque de 1.4.2).

On peut donc aussi dire que G est isomorphe à $N \rtimes H$, i étant un isomorphisme de N sur $\overline{N} = i(N)$, et s étant un isomorphisme de $\overline{H}$ sur H.

⊡ **Identification d'un produit semi-direct** **Intuition** La condition de la proposition 0.15 est suffisante mais non nécessaire ; on peut avoir une extension sans relèvement, c'est-à-dire non scindée, c'est-à-dire sans qu'il y ait de section, sans pour autant que le groupe ne soit pas le produit semi-direct de N par H.

Démonstration *On considère $\overline{N}$ l'image de i, et $\underline{H}$ le sous-groupe de G sur lequel la restriction de s est un isomorphisme vers H.*

Puisque $\overline{N} = Ker\ s$, $\overline{N} \lhd G$ (un noyau de morphisme de groupe est toujours distingué). Il est clair que :

- $\overline{N} \cap \overline{H} = \{1\}$
- $G = \overline{N}.\overline{H}$

Le premier point est évident, du fait que s est un isomorphisme depuis $\overline{H}$, et a donc un noyau nul.

Pour le deuxième point, soit $g \in G$, alors $s(g) = s(h)$ avec $h \in H$, et $s(g.h^{-1}) = s(g).s(h)^{-1} = 1$, donc $g.h^{-1} \in N$. L'écriture d'un élément de G comme produit d'un élément de N par un élément de H est unique (facile, au vu de $\overline{N} \cap \overline{H} = \{1\}$) ; G est donc ainsi en bijection avec $\overline{N} \times \overline{H}$, par $\phi(nh) = (n, h)$. On cherche maintenant à établir une loi sur $\overline{N} \times \overline{H}$ telle que cette bijection soit un isomorphisme.

Le produit de $n.h$ par $n'h'$ est $n.h.n'h'$, que l'on doit donc exprimer comme un produit d'un élément de $\overline{N}$ par un élément de $\overline{H}$; on peut réécrire $n.h.n'.h'$ sous la forme $n.(h.n'.h^{-1}).h.h'$; puisque N est distingué, il s'agit bien du produit de $n.h.n'.h^{-1}$ (élément de $\overline{N}$) par $h.h'$ (élément de $\overline{H}$).

On vérifie facilement que la loi $(n, h).(n', h') = (n.(h.n'.h^{-1}), h.h')$ fait de cette bijection un morphisme.

Intuition Remarque importante : L'hypothèse revient exactement à avoir une extension scindée, c'est-à-dire une extension munie d'un relèvement (voir 1.1.4).

PROPOSITION 0.16
Si G est un groupe, si N et H sont des sous-groupes de G, si $N \lhd_{\text{I}} G$, si $N \cap H = \{1\}$ et si $G = N.H$, alors $G \simeq N \rtimes H$.

Démonstration *Il suffit de reprendre la preuve ci-dessus.*

⊡ **Identification d'un produit direct** En fait un produit direct est un cas particulier de produit semi-direct.

En reprenant les notations de la définition du produit semi-direct et des démonstrations ci-dessus, on a équivalence entre les assertions suivantes :

•$\phi(h) = Id_N$ pour tout h

•$\overline{H}$ est distingué

•la loi de groupe sur $N \rtimes H$ est celle du produit direct

On peut aussi raisonner sur les suites exactes. Lorsque l'on a une suite exacte avec relèvement, i.e. avec une section, i.e. si l'extension est scindée, ET si $\forall (n,h) \in N \times H \ nh = hn$, alors $G \simeq \overline{N} \times \overline{H} \simeq N \times H$.

Intuition On peut très bien avoir $A \times B$ (produit direct) $\simeq A \rtimes_\phi B$, avec ϕ autre que $\phi(h) = Id_N$ pour tout h ; donc il ne suffit pas de décomposer un groupe comme produit semi-direct non trivial pour conclure qu'il n'est pas un produit direct. [3] cite ainsi $\sigma_3 \times \mathbb{Z}/2\mathbb{Z}$.

1.5 Théorèmes de Sylow. Groupes de Sylow

Les deux théorèmes de Sylow sont extraits du classique [3].

DÉFINITION 0.14 **p-sous-groupe de Sylow**
On appelle **p-sous-groupe de Sylow** ou plus simplement **p-Sylow** d'un groupe G de cardinal n, un sous-groupe de G d'ordre p^r avec p premier divisant n et $n = p^r.m$ et $p \not| \, m$ (p ne divisant pas m).

PROPOSITION 0.17
Un sous-groupe P de G est un p-sous-groupe de Sylow de G si :
•P est un p-groupe
•$(G : P)$ est premier à p.

La démonstration de la proposition précédente, immédiate, est laissée en exercice ; nous passons au plus difficile

THÉORÈME 0.18 **Théorème de Sylow**
G étant un groupe fini, et p un nombre premier divisant l'ordre de G, alors G admet au moins un p-sous-groupe de Sylow.

Démonstration *On va procéder par étapes.* •*Tout d'abord un cas particulier :* $\mathbb{Z}/p\mathbb{Z}$ *est un corps fini puisque* p *est premier, et* $GL(n,\mathbb{Z}/p\mathbb{Z})$ *est d'ordre* $\Pi_{i=0}^{n-1}(p^n-p^i)$*, comme on peut s'en convaincre en comptant les bases de* $(\mathbb{Z}/p\mathbb{Z})^n$*. Le cardinal de ce groupe est donc* $m.p^{n.(n-1)/2}$*, avec* $p \not| m$*. Un* p*-Sylow de ce groupe est alors l'ensemble des matrices de la forme*

$$\underbrace{\left\{\begin{pmatrix} 1 & * & * & \dots & * & * \\ 0 & 1 & * & \dots & * & * \\ 0 & 0 & 1 & \dots & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ 0 & 0 & \dots & 0 & 1 & *0 \\ 0 & \dots & 0 & 0 & 1 & \end{pmatrix}\right.}_{n \text{ colonnes}} \left.\vphantom{\begin{pmatrix} 1 & * & * & \dots & * & * \\ 0 & 1 & * & \dots & * & * \\ 0 & 0 & 1 & \dots & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ 0 & 0 & \dots & 0 & 1 & *0 \\ 0 & \dots & 0 & 0 & 1 & \end{pmatrix}}\right\} n \text{ lignes}$$

•*On a maintenant besoin d'un lemme :*

LEMME 0.19
Soit G *un groupe d'ordre* $p^\alpha.m$*, avec* $p \not| m$ *et* p *premier,* H *un sous-groupe de* G *et* S *un* p*-Sylow de* G*. Alors il existe* $a \in G$ *tel que* $a.S.a^{-1} \cap H$ *soit un* p*-Sylow de* H*.*

begindivdemonstrationbegintext endtext G *opère sur* G/S *par translation à gauche (voir 1.9.1) ; le stabilisateur d'un élément* $g.S$ *est* $g.S.g^{-1}$*.*

D'autre part H *opère sur* G/S *par translation à gauche aussi ; le stabilisateur d'un élément* $g.S$ *est* $g.S.g^{-1} \cap H$*.*

Il est clair que tout $a.S.a^{-1} \cap H$ *est bien un* p*-groupe, il reste à en trouver un qui soit bien un* p*-Sylow. Il suffit pour cela que le quotient du cardinal de* H *par le cardinal de* $H \cap a.S.a^{-1}$ *soit premier avec* p *; donc il suffit que le cardinal de* $H/(H \cap a.S.a^{-1})$ *soit premier avec* p*.*

Or ce cardinal est en fait le cardinal de l'orbite de $a.S$ *dans* G/S *sous l'action de* H *; or toutes ces orbites ne peuvent être de cardinal un multiple de* p*, sinon le cardinal de* G/S *serait un multiple de* p*, ce qui contredirait le fait que* S *est un* p*-Sylow.*

Ce lemme est donc prouvé.

•Maintenant on peut s'attaquer au cas général ; soit G un groupe vérifiant les hypothèses ; G est isomorphe à un sous-groupe de σ_n par le théorème de Cayley (voir 1.9.1). À son tour, σ_n est isomorphe à un sous-groupe de $GL(n,\mathbb{Z}/p\mathbb{Z})$ (on considère la base canonique $(e_i)_{i\in[1,n]}$ de $(\mathbb{Z}/p\mathbb{Z})^n$, et l'application qui à σ dans σ_n associe l'application linéaire qui à e_i associe $\sigma(e_i)$).

Par le premier point, ce groupe admet un p-Sylow ; et par le deuxième point, un sous-groupe d'un groupe admettant un p-Sylow admet un p-Sylow.enddivdemonstration

COROLLAIRE 0.20
Si G un est groupe de cardinal $p^r.m$ avec $p \not| m$ et p premier, alors G possède des sous-groupes d'ordre p^q pour tout $q \leq r$.

Démonstration *G contient un p-Sylow, donc un sous-groupe de cardinal p^r. On peut donc se ramener au cas des p-groupes. Le centre d'un p-groupe est non trivial, comme on le montre en 1.10.1. On considère donc G un p-groupe, et $Z(G)$ son centre, de cardinal p^r. En appliquant l'hypothèse de récurrence à $Z(G)$, on a bien des groupes d'ordre p^q, pour $q \leq r$. On considère maintenant le groupe-quotient de G par $Z(G)$, il est de cardinal p^{r-q}, on peut donc lui appliquer l'hypothèse de récurrence et y trouver un groupe de cardinal p^t pour $t \leq r-q$. En considérant l'image inverse par la projection canonique sur le groupe quotient, on obtient alors un groupe de cardinal p^{t+q}, pour $t \leq r-q$, donc pour tout cardinal p^u avec $q \leq u \leq r$.*

THÉORÈME 0.21 **Deuxième théorème de Sylow**
Étant donné G un groupe, de cardinal $|G| = p^r.m$, avec $p \not| m$.
- Tout p-groupe inclus dans G est inclus dans un p-Sylow de G.
- Les p-Sylow sont tous conjugués.
- Les p-Sylow forment une orbite de G sous l'action de G par automorphisme intérieur.
- Un p-Sylow est distingué si et seulement si il est l'unique p-Sylow.
- Le nombre de p-Sylow est congru à 1 modulo p et divise $|G|$.
- Le nombre de p-Sylow divise m.

Démonstration *•Démonstration de l'affirmation « Tout p-groupe inclus dans G est inclus dans un p-Sylow de G » :*

Supposons H un p-groupe de G. Soit S un p-Sylow de G, dont l'existence est donnée par le premier théorème de Sylow. D'après le lemme 0.19 inclus dans la démonstration du premier théorème de Sylow, il existe a dans G tel que $a.S.a^{-1} \cap H$ soit un p-Sylow de H.

H étant un p-groupe, H est nécessairement égal à $a.S.a^{-1} \cap H$. Donc H est bien inclus dans un Sylow.

•Pour montrer l'affirmation « Les p-Sylow sont tous conjugués », il suffit de faire le même raisonnement avec H un p-Sylow.

•Démonstration de l'affirmation « Les p-Sylow forment une orbite de G sous l'action de G par automorphisme intérieur » :

On a vu que les p-Sylow étaient tous conjugués ; si un autre élément leur est conjugué, c'est aussi un p-Sylow ; le résultat est donc en fait complètement évident.

•Démonstration de l'affirmation « Un p-Sylow est distingué si et seulement si il est l'unique p-Sylow » :

Si un p-Sylow est distingué et s'il n'est pas unique alors il est conjugué à l'autre - donc il n'est pas distingué. Ceci clôt la démonstration dans le sens « distingué $\rightarrow$ unique ».

Réciproquement s'il est unique, alors s'il n'est pas distingué, alors il est conjugué à un autre p-Sylow - donc il n'est pas unique.

•Démonstration de l'affirmation « Le nombre de p-Sylow est congru à 1 modulo p et divise $|G|$ » :

On rappelle que la proposition 0.13 affirme que le nombre de points fixes d'un ensemble X sous l'action d'un p-groupe G est congru au cardinal de X modulo p.

Il suffit alors de considérer l'ensemble des p-Sylow ; on peut faire agir dessus un p-Sylow S quelconque par conjugaison. Le nombre de p-Sylow est donc congru au nombre de points fixes de l'ensemble des p-Sylow sous l'action de S modulo p. Il reste donc à montrer qu'il y a un unique point fixe. L'existence d'un point fixe est évidente, il s'agit de S lui-même. Supposons que T soit un autre point fixe, T est donc un p-Sylow tel que pour tout s dans S, $sTs^{-1} = T$. On considère le groupe engendré par T et S, S et T sont des p-Sylow de ce groupe. Dans ce groupe toujours, T est distingué ; donc il est l'unique p-Sylow, donc il est égal à S. D'où le résultat.

•Démonstration de l'affirmation « Le nombre de p-Sylow divise m » :

Le nombre de p-Sylow est le cardinal d'une orbite, donc il divise le cardinal de G, or il est congru à 1 modulo p, donc il divise m.

1.6 Applications des groupes de Sylow

Cet exemple, consistant à montrer qu'un groupe de cardinal 63 ne peut être simple, est tiré de l'excellent [3].

PROPOSITION 0.22
Un groupe d'ordre 63 ne peut être simple.

Démonstration *on considère les 7-Sylow de G d'ordre 63 ; ce nombre de 7-Sylow divise $\frac{63}{7}$ donc 9, et est congru à 1 modulo 7 ; donc il y a un unique 7-Sylow, donc il est distingué, donc G n'est pas simple.*

1.7 Groupes abéliens

On rappelle qu'un groupe abélien est un groupe commutatif.

PROPOSITION 0.23
Un groupe abélien G est de type fini si et seulement si il existe un homomorphisme surjectif de $\mathbb{Z}^n$ sur G pour un certain n, c'est-à-dire s'il est isomorphe à un quotient de $\mathbb{Z}^n$ par un de ses sous-groupes [1].
Plus précisément, G est alors engendré par n éléments, si n est minimal.

Application 0.6 Cela nous servira pour la proposition 0.26.

Démonstration *En effet, supposons que G est finiment engendré, par $g_1, ..., g_n$. Considérons alors l'application de $\mathbb{Z}^n$ dans G définie par $(p_1, ..., p_n) \mapsto p_1.g_1 + ... + p_n.g_n$. Puisque G est engendré par les g_i ET G est commutatif, cette application est surjective. Il est clair que c'est un morphisme puisque G est commutatif. Donc G est isomorphe au quotient de $\mathbb{Z}^n$ par le noyau de ce morphisme, d'où le résultat.*

Réciproquement, supposons que l'on ait un morphisme surjectif de $\mathbb{Z}^n$ sur G ; alors il est égal à l'homomorphisme $(p_1, ..., p_n) \mapsto p_1.g_1 + ... + p_n.g_n$, avec g_i l'image de $(\underbrace{0, ..., 0}_{i-1 fois}, 1, 0, ..., 0)$ (voir la remarque de la partie 1.1.5). Il est donc clair que G est engendré par les g_i.

DÉFINITION 0.15 **Somme**
Soit $(A_i)_{i\in I}$ une famille de groupes abéliens. On note $\bigoplus_{i\in I} A_i$ l'ensemble des familles $(x_i)_{i\in I}$ avec $x_i \in A_i$ et les x_i presque tous nuls ; c'est un groupe abélien pour l'addition terme à terme ; on l'appelle **somme** des groupes A_i.
On identifie A_i à l'ensemble des $(x_i)_{i\in I}$ tels que $j \neq i \rightarrow x_j = 0$.
Si $\forall i\ A_i = A$ alors on note $A^{(I)} = \bigoplus_{i\in I} A_i$.

Notons que la somme est exactement le produit restreint, dans le cas des groupes abéliens.

PROPOSITION 0.24 **Propriété universelle des groupes abéliens**
Étant donnée une famille $(A_i)_{i\in I}$ de groupes abéliens, A' un groupe abélien, ϕ_i un homomorphisme de A_i sur A', alors il existe un unique homomorphisme de $\bigoplus A_i$ vers A' tel que la restriction de cet homomorphisme à A_i soit ϕ_i.

Démonstration *Considérer $\phi(x) = \sum_{i\in I} \phi_i(x_i)$.*

Définition 0.16 **Somme directe**
A étant un groupe abélien, les A_i étant des sous-groupes de A, alors :

•les A_i sont dits en **somme directe** si l'application canonique de $\bigoplus A_i$ dans A qui à $(x_i)_{i\in I}$ associe $\sum_i x_i$ est injective. On identifie alors son image avec $\bigoplus_{i\in I} A_i$.

•On dit que A est **somme directe** des A_i si l'application est bijective. On note alors (abusivement) $A = \bigoplus_{i\in I} A_i$.

Proposition 0.25
A abélien, $(A_i)_{i\in I}$ famille de sous-groupes, alors les A_i sont en somme directe si $\sum_{i\in I} x_i = 0$ avec $x_i \in A_i$ (support fini) implique $\forall i\ x_i = 0$.

Définition 0.17 **Groupe de torsion**
Un élément d'un groupe est dit **élément de torsion** s'il est d'ordre fini.

Un groupe abélien est dit **sans torsion** si aucun de ses éléments (autres que le neutre) n'est d'ordre fini.

Un groupe abélien est dit **de torsion** si tous ses éléments sont d'ordre fini.

Étant donné p un nombre premier, un groupe abélien est dit **de p-torsion** si tous ses éléments sont d'ordre une puissance de p.

Un groupe abélien est dit **libre** s'il est isomorphe à $\mathbb{Z}^n$ pour un certain $n \in \mathbb{N}$.

On appelle **sous-groupe de torsion** d'un groupe abélien G le sous-groupe constitué par les éléments de torsion [2].

Proposition 0.26
Un groupe de torsion [3] et de type fini est fini.

Démonstration *En effet, si G est de type fini et abélien, alors c'est un quotient de $\mathbb{Z}^n$, par la proposition 0.23.*

On considère alors ppcm le ppcm des ordres des n générateurs donnés par la proposition 0.23. L'ordre de tout élément est alors un diviseur de ppcm. L'homomorphisme surjectif de $\mathbb{Z}^n$ dans son quotient a pour noyau un ensemble contenant $(k\mathbb{Z})^n$. Donc il se factorise à travers $(\mathbb{Z}/k\mathbb{Z})^n$ (voir le théorème 0.8). Donc le groupe G est de cardinal plus petit que k^n.

Les deux théorèmes ci-dessous sont donnés sans démonstration (laissées aux lecteurs pour exercice !).

Théorème 0.27
•Tout groupe abélien sans torsion de type fini est libre.

•Tout sous-groupe d'un groupe libre est libre.

•Deux groupes libres $\mathbb{Z}^n$ et $\mathbb{Z}^p$ sont isomorphes si et seulement si $n = p$.

•Tout groupe abélien de type fini est produit d'un groupe libre et d'un groupe de torsion. Cette décomposition est unique à isomorphisme près.

THÉORÈME 0.28
Tout groupe abélien fini G s'exprime de manière unique sous la forme

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

avec $\forall i \in [1, n-1]\ a_i | a_{i+1}$, et $a_1 > 1$.

DÉFINITION 0.18 **facteurs invariants**
Les a_i sont appelés **facteurs invariants** du groupe.
La décomposition ainsi obtenue est appelée **décomposition cyclique** du groupe G.

Cette décomposition a de nombreuses conséquences :

COROLLAIRE 0.29
Soit G un groupe abélien fini ; il existe un élément d'ordre le ppcm des ordres des éléments du groupe.

Démonstration •*Soit G un groupe abélien fini.*
•*La décomposition cyclique nous permet d'écrire G sous la forme*

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

•*On considère un élément $x = (x_1, \ldots, x_n)$ de ce produit.*
•*L'ordre de x est le ppcm des ordres des x_i ; or l'ordre de x_i divise a_i, qui lui-même divise a_n.*
•*Le ppcm des ordres est donc en fait un diviseur de a_n, donc c'est a_n lui-même.*
•*L'élément $(0, \ldots, 0, 1)$ convient donc (on peut remplacer 1 par n'importe quel générateur de $\mathbb{Z}/a_n\mathbb{Z}$).*
Autre conséquence :

COROLLAIRE 0.30
Soit G un groupe abélien fini. Pour tout diviseur d de $Card(G)$, il existe un sous-groupe H de G d'ordre d.

Démonstration •*On écrit G sous forme :*

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

•*Décomposons d en facteurs premiers :*

$$d = \Pi_{i=1}^{m} p_i$$

•*Définissons :*

$$d_1 = pgcd(d, a_1)$$
$$d_2 = pgcd(\frac{d}{d_1}, a_2)$$
$$d_3 = pgcd(\frac{d}{d_1 d_2}, a_3)$$
$$\ldots$$

$$d_n = pgcd(\frac{d}{d_1 \dots d_{n-1}}, a_n)$$

•*Puisque* $d|card(G)$ *et* $card(G) = \Pi_{i=1}^{n} a_i$*, on arrive à se « débarrasser » de chaque facteur premier de* d *dans l'un des* d_i*, et donc* $\Pi_{i=1}^{n} d_i = d$*.*

•*Pour tout* i*,* d_i *divise* a_i*.*

•*Dans un groupe cyclique, il existe un sous-groupe du cardinal de n'importe quel diviseur de l'ordre du groupe, donc dans* $\mathbb{Z}/(a_i\mathbb{Z})$ *il existe un sous-groupe* H_i *de cardinal* d_i*.*

•*Le produit des* H_i *est un sous-groupe de* G *de cardinal* d*.*

Un corollaire, sans preuve :

COROLLAIRE 0.31
Soit G un groupe abélien fini. Soit $c = p_1^{n_1} p_2^{n_2} \dots p_l^{n_l}$ la décomposition de $c = card(G)$ en facteurs premiers. Alors pour tout $i \in [1, l]$ il existe un et un seul sous-groupe H_i de G de cardinal $p_i^{n_i}$. En outre, G est isomorphe au produit des H_i.

DÉFINITION 0.19 **centralisateur**
Les H_i, uniques, sont appelés les composantes primaires du groupe commutatif G.

1.8 Exercices sur les groupes

On présente ici une liste d'exercices et de zoologies reliés aux groupes, par ordre à peu près croissant d'originalité ou de difficulté.

1.8.1 Zoologie préliminaire des groupes

Les objets suivants sont-ils des groupes ?
$(\mathbb{C}^*, .), (\mathbb{R}^*, .), (\mathbb{C}, +), (\mathbb{R}, +), (\mathbb{R}, .), (\mathbb{Q}, +), (\mathbb{Q}, .), (\mathbb{N}, .), (\mathbb{Z}, +)$, l'ensemble des translations du plan, l'ensemble à la fois des translations et des homothéties affines (pour la composition) ? Ces groupes sont-ils commutatifs ?

Oui il s'agit de groupes, sauf $(\mathbb{R}, .)$, $(\mathbb{Q}, .)$, $(\mathbb{N}, .)$. Tous ces groupes sont commutatifs sauf le groupe à la fois des translations et des homothéties.

1.8.2 Conditions suffisantes allégées

On va voir ici une définition équivalente et moins contraignante des groupes, et un cas particulier suffisant pour assurer la commutativité d'un groupe.

Conditions réduites pour un groupe Si G a une loi de composition interne associative, un élément 1 tel que $\forall g \; g1 = g$, et un élément g' pour tout g tel que $gg' = 1$, alors G est un groupe.

Démonstration *On multiplie* gg' *par* g' *à gauche, et on montre que* $g'g = 1$ *en utilisant le* g'' *tel que* $g'g'' = 1$*. Il est ensuite facile de voir que* $1g = g$*.*

Condition suffisante de commutativité Si tout élément est son propre inverse, alors G est commutatif.

1.8.3 $\mathbb{Z}/n\mathbb{Z}$

Pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ comporte un seul sous-groupe d'ordre d.
Démonstration *L'existence est immédiate. On obtient l'unicité en considérant l'ensemble des éléments x tels que $dx = 0$.*
Étant donnés deux entiers n et k, on a équivalence entre les trois assertions suivantes :
– $\overline{k}$ (dans $\mathbb{Z}/n\mathbb{Z}$) engendre $\mathbb{Z}/n\mathbb{Z}$.
– n et k sont premiers entre eux.
– $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

On consultera la section **??** pour plus d'informations sur $\mathbb{Z}/n\mathbb{Z}$ (en tant qu'anneau).

1.8.4 Zoologie des sous-groupes

•Tout sous-groupe d'un groupe cyclique est cyclique.
•Si G est un sous-groupe de $(\mathbb{R}, +)$, alors G est monogène ou dense.
Démonstration *Considérer l'inf de $\mathbb{R}^+ \cap G$.*
•Il existe des sous-groupes denses de $\mathbb{R}$ de type fini.
Démonstration *$\mathbb{Z} + \sqrt{2}\mathbb{Z}$ en est un exemple.*
•L'union de deux sous-groupes est un groupe si et seulement si l'un est inclus dans l'autre.
•Le produit élément par élément de deux sous-groupes A et B est un sous-groupe si et seulement si $AB = BA$.
Démonstration *upposons que AB soit un sous-groupe. Alors soit $a \in A$ et $b \in B$. $a^{-1}b^{-1} \in AB \to ba \in AB$ donc $BA \subset AB$.*
ab admet un inverse dans AB donc $a'b'ab = 1$, donc $b'ab = a'^{-1}$, donc $ab = b'^{-1}a'^{-1}$, donc $ab \in BA$, donc $AB \subset BA$.
Réciproquement, supposons $AB = BA$, alors l'inverse de ab, $b^{-1}a^{-1}$, appartient bien à AB ; en outre il est immédiat que AB est stable par produit.
•L'image d'un sous-groupe distingué par un homomorphisme est un sous-groupe distingué de l'image de l'homomorphisme. L'image réciproque d'un sous-groupe distingué par un homomorphisme est un sous-groupe distingué.

•L'intersection de deux sous-groupes distingués est un sous-groupe distingué.

•Tout sous-groupe d'un groupe abélien est distingué ; mais on peut avoir cette propriété sans que le groupe soit abélien ; considérer par exemple $\{1,i,j,k,-1,-i,-j,-k\}$, muni des opérations $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$ (notons que ce groupe possède aussi la propriété de n'avoir que des sous-groupes propres abéliens).

1.8.5 Divers

•Dans un groupe, on suppose que $(ab)^n = 1$; montrer que $(ba)^n = 1$. Ceci implique que l'ordre de ab est égal à l'ordre de ba.

•Montrer que $\mathbb{Q}$ n'est pas de type fini.
Démonstration *Considérer un nombre fini d'éléments de $\mathbb{Q}$, et un dénominateur commun de ces éléments.*
•L'ensemble des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ muni de la composition est isomorphe à $((\mathbb{Z}/n\mathbb{Z})^*, \times)$.

•Un sous-groupe additif de $\mathbb{R}$ est soit dense, soit de la forme $a.\mathbb{Z}$. De même, $\mathbb{R}^{+*}$ muni de la multiplication n'admet que des sous-groupes denses ou de la forme $a^{\mathbb{Z}}$.
Démonstration *Considérer la borne* inf *de l'intersection du sous-groupe et de $\mathbb{R}^{+*}$. Le cas multiplicatif s'obtient en considérant le* log*, qui est un isomorphisme de groupe, et qui préserve la densité.*
•$\mathbb{Z} + b\mathbb{Z}$ dans $(\mathbb{R}, +)$ est de la forme $a.\mathbb{Z}$ si b est rationnel, et dense si b est irrationnel.

1.9 Zoologie des opérations d'un groupe sur un ensemble

1.9.1 Opération d'un groupe G sur lui-même par translation à gauche

On associe à tout élément g de G la fonction qui à $x \in G$ associe $g.x$.
Cette opération est transitive (il y a une seule orbite) et fidèle.

THÉORÈME 0.32 **Théorème de Cayley**
Si G est fini, alors G est isomorphe à un sous-groupe du groupe des permutations de G.

Démonstration *L'application qui à g associe l'application $x \mapsto g.x$ est un homomorphisme injectif ; donc G est isomorphe à son image par cette application, qui est donc un sous-groupe du groupe des permutations de G.*
Pour « fixer les idées », on peut se représenter $\mathbb{Z}/n\mathbb{Z}$ isomorphe à l'ensemble des applications qui à $\overline{x}$ associe $\overline{x}+\overline{p}$.

1.9.2 Opération d'un groupe G sur le quotient G/H par translation à gauche

À un élément g et une classe $g'.H$ on associe la classe $g.g'.H$. On vérifie facilement que cette opération est bien définie et définit bien une opération d'un groupe sur un ensemble. En effet, l'opération est clairement transitive, par contre elle n'est pas fidèle en général. Le noyau de l'application ϕ associée (voir définition d'une opération d'un groupe sur un ensemble) est égal à

$$\bigcap_{g\in G} g.H.g^{-1}$$

1.9.3 Opération d'un groupe sur lui-même par automorphismes intérieurs

À $g \in G$ on associe l'automorphisme intérieur $x \mapsto g.x.g^{-1}$.
Propriétés •Les orbites sont exactement les classes d'équivalence pour la relation de conjugaison.
•Le stabilisateur d'un élément x est l'ensemble des g tels que $x = g.x.g^{-1}$, c'est-à-dire $x.g = g.x$; c'est donc l'ensemble des éléments qui commutent avec x, on l'appelle **centralisateur** de x. On généralise cette définition en l'élargissant aux parties de G ; le **centralisateur** d'une partie est l'ensemble des éléments qui commutent avec tous les éléments de cette partie.
•Le centralisateur de G tout entier est donc le centre de G, c'est-à-dire l'ensemble des éléments qui commutent avec tous les autres.
•Les éléments d'une classe de conjugaison ont même ordre et même nombre de points fixes.
On peut par exemple considérer le groupe $GL(n,\mathbb{K})$; les classes de conjugaison, c'est-à-dire les orbites, sont alors les classes d'équivalence pour la relation « être semblable à ».

1.10 Zoologie des groupes

On trouvera une étude des groupes $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$ dans la partie **??**.

1.10.1 Les p-groupes

Rappelons qu'un p-groupe est un groupe de cardinal (donc d'ordre) p^r avec p un nombre premier.

PROPOSITION 0.33 **Le centre d'un p-groupe non trivial est non trivial**
Si G est un p-groupe de cardinal > 1 alors son centre est de cardinal > 1.

Démonstration *On partitionne G selon les orbites de ses éléments par action des automorphismes intérieurs.*

On commence par remarquer que Z est l'ensemble des points fixes de cette action. On note ensuite $g_1,\ldots,g_k$ des représentants des orbites non-triviales (de sorte que $i \neq j \Rightarrow \omega(g_i) \cap \omega(g_j) = \emptyset$). Ainsi, Z et les $(\omega(g_i))_{1\leq i\leq k}$ forment une partition de G, et donc

$$|G| = |Z| + \sum_{i=1}^{k} |\omega(g_i)|$$

Par la proposition 0.10, on a $\forall i, |\omega(g_i)| = \frac{|G|}{|H_{g_i}|} = p^{r_i}$ pour un certain $r_i \in [0, r]$, car $G = p^r$ (H_{g_i} représente le stabilisateur de g_i). Comme l'orbite $\omega(g_i)$ est non triviale, on a $|\omega(g_i)| > 1$ et donc $r_i \geq 1$. Autrement dit, on a, pour tout i, p divise $|\omega(g_i)|$. On déduit alors de la formule 30 que p divise $|Z|$, et comme $|Z| \neq 0$ (car $1 \in Z$), on obtient bien que le centre de G est non trivial.

1.10.2 Groupe linéaire et groupe spécial linéaire

DÉFINITION 0.20
Étant donné $\mathbb{K}$ un corps commutatif quelconque et E un $\mathbb{K}$-espace vectoriel de dimension finie, on appelle **groupe linéaire** $GL(E)$ le groupe des automorphismes de E.

$GL(E)$ est isomorphe à $GL(n, \mathbb{K})$, groupe des matrices inversibles de taille $n \times n$, à coefficients dans $\mathbb{K}$, avec n la dimension de E.

On notera que deux matrices semblables A et B vérifient qu'il existe P tel que $A = P^{-1}.B.P$; cela revient donc à dire que A et B sont conjuguées.

DÉFINITION 0.21 **groupe spécial linéaire**
Le noyau de l'homomorphisme qui à f associe son déterminant est par définition l'ensemble des automorphismes de déterminant 1 ; on l'appelle **groupe spécial linéaire** et on le note $SL(E)$.

$SL(E)$ est isomorphe à $SL(n, \mathbb{K})$, groupe des matrices de $GL(n, \mathbb{K})$ de déterminant 1. Ne surtout pas dire que le groupe spécial linéaire est égal ou isomorphe au groupe spécial orthogonal !

Attention aussi au fait qu'alors que le groupe spécial orthogonal est la restriction du groupe orthogonal aux matrices de déterminant positif, qui est exactement égal à la restriction du groupe orthogonal aux matrices de déterminant 1 puisque les matrices orthogonales ont un déterminant dans $\{-1, 1\}$, le groupe spécial linéaire n'est pas la restriction du groupe linéaire aux matrices de déterminant positif mais bien aux matrices de déterminant 1 ! En effet, les matrices inversibles peuvent avoir un déterminant autre que 1 ou -1.

PROPOSITION 0.34
On a une suite exacte :

$$1 \to SL(E) \to GL(E) \xrightarrow{\text{dét}} \mathbb{K}^* \to 1$$

En outre, $GL(E)$ est isomorphe au produit semi-direct de $SL(E)$ par $\mathbb{K}^*$.

$\mathbb{K}^*$ désignant $\mathbb{K} - \{0\}$.

Démonstration *Il suffit de prendre pour injection de $SL(E)$ dans $GL(E)$ la simple identité, et de considérer le sous-groupe H de $GL(E)$ des matrices de la forme*

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

avec λ non nul.

Le déterminant induit bien une bijection de H sur $\mathbb{K}^*$, on a bien $H \cap SL(E)$ réduit à l'élément neutre, on a bien

$$SL(E).H = GL(E),$$

et $SL(E)$ est clairement distingué.

PROPOSITION 0.35 **Générateurs de $GL(E)$ et $SL(E)$**
On a les générateurs suivants :
•$GL(E)$ est engendré par l'ensemble des transvections et des dilatations de E.
•$SL(E)$ est engendré par l'ensemble des transvections de E.

Démonstration *On ne détaillera pas intégralement la preuve, laborieuse, mais peu difficile. Il suffit de montrer les points suivants, dans cet ordre :*

•*Toute matrice de la forme $I+\lambda E_{i,j}$ pour $i \neq j$, avec $\lambda \in \mathbb{K}$ et $E_{i,j}$ la matrice définie par $(E_{i,j})_{k,l} = 1$ si $i = k$ et $j = l$ et 0 sinon, est la matrice d'une transvection. L'inverse d'une matrice de transvection, est une matrice de transvection.*

•*Une matrice de déterminant 1 est égale à un produit de matrices de transvections. Pour le prouver, on considère M une telle matrice, on la multiplie par des matrices de transvection pour se ramener à une matrice n'ayant qu'un seul élément non nul sur la première ligne, pour que cet élément soit l'élément en haut à gauche, et pour qu'il soit égal à 1. Il suffit alors de procéder par récurrence en considérant un produit de matrices par bloc.*

(ce point est exactement le deuxième point annoncé)

•*Une matrice appartenant à $GL(E)$ est le produit d'une matrice appartenant à $SL(E)$ et d'une matrice de dilatation (voir proposition 0.34).*

1.10.3 Groupe orthogonal et groupe spécial orthogonal

DÉFINITION 0.22 **groupe orthogonal d'un espace euclidien E**
On appelle **groupe orthogonal d'un espace euclidien** E l'ensemble des automorphismes orthogonaux de E muni de la composition $\circ$; on le note $O(E)$.

On appelle **groupe spécial orthogonal d'un espace euclidien** E l'ensemble des automorphismes orthogonaux de E de déterminant 1 muni de la composition $\circ$; on le note $SO(E)$ ou $O^+(E)$.

On note $O^-(E)$ le complémentaire de $SO(E)$ dans $O(E)$.

On note en outre $O_n(\mathbb{R})$ l'ensemble $O(\mathbb{R}^n)$ et $SO_n(\mathbb{R})$ ou $O_n^+(\mathbb{R})$ l'ensemble $SO(\mathbb{R}^n)$.

⊡ **Cas général** Ces espaces sont isomorphes aux espaces décrits en 1.10.4, on se contentera donc de détailler les cas spéciaux des dimensions 1, 2 et 3.

⊡ **Dimension** 1 Ce cas est de peu d'intérêt ; les seules transformations orthogonales sont $x \mapsto x$ et $x \mapsto -x$.

⊡ **Dimension** 2 Un rapide calcul montre que les matrices des transformations orthogonales en dimension 2 sont de l'une des deux formes suivantes :

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \begin{pmatrix} \cos(\theta) & \sin(\theta)\sin(\theta) \\ -\cos(\theta) & \end{pmatrix}.$$

La matrice de gauche représente une transformation du groupe spécial orthogonal (c'est-à-dire de déterminant 1, et donc dans $SO(E) = O^+(E)$), celle de droite une transformation qui n'est pas de ce groupe (c'est-à-dire que celle-ci est de déterminant -1, et donc dans $O^-(E)$).

(le calcul est facile, il suffit de se souvenir que $x^2 + y^2 = 1 \to \exists\theta / x = \cos(\theta)$ et $y = \sin(\theta)$)

DÉFINITION 0.23 **rotation d'angle θ**
On appelle **rotation d'angle θ** un endomorphisme associé à la matrice de gauche.

Toujours par des calculs sans grande difficulté on montrerait que $SO_2(\mathbb{R})$ commute, et est en fait isomorphe à $\mathbb{R}/(2\pi\mathbb{Z})$; les seules transformations orthogonales de déterminant 1 sont en fait les rotations. On note r_θ la rotation d'angle θ.

En étudiant la matrice de droite, on constate qu'elle est symétrique, donc diagonalisable (voir la partie **??**) ; son polynôme caractéristique est $X^2 - 1$; elle est semblable à $\begin{pmatrix} 1 & 00 \\ -1 & \end{pmatrix}$. Il s'agit donc en fait d'une symétrie par rapport à un hyperplan (ici hyperplan = droite car on est en dimension 2). Ainsi les transformations orthogonales de déterminant -1 sont en fait des symétries par rapport à des droites. On note que les symétries ne commutent pas, elles. On note s_θ la symétrie correspondant à θ (θ est en fait le double de l'angle de l'axe invariant avec le premier axe, i.e. l'axe des abscisses).

On notera que $s_\theta \circ s_{\theta'} = r_{\theta-\theta'}$.

⚠ *Attention 0.7* L'angle n'est défini qu'à 2π près pour les rotations et les symétries.

PROPOSITION 0.36
En dimension 3, $O^+(E)$ comporte :
- les rotations axiales
- l'identité, qui est un cas particulier de rotation axiale
- la symétrie par rapport à une droite, qui est un cas particulier de rotation axiale

En dimension 3, $O^-(E)$ comporte :
- les symétries orthogonales par rapport à un plan
- les composées d'une rotation autour d'un axe et d'une symétrie par rapport au plan orthogonal à cet axe

⊡ **Dimension** 3 On se donne f un endomorphisme orthogonal de E euclidien de dimension 3, et on considère I l'ensemble $\{x; f(x) = x\}$ (ensemble des invariants par f). On va classer les f possibles suivant la dimension de I.

◇ *dim* $I = 3$ Pas drôle : f est l'identité, et donc $f \in SO(E) = O^+(E)$.

◇ *dim* $I = 2$ Alors l'orthogonal de I est de dimension 1 ; la restriction de f à cet espace est un endomorphisme orthogonal (rappelons que si un espace est stable pour un endomorphisme orthogonal, alors son orthogonal aussi). Ce n'est pas l'identité puisque f n'est pas l'identité, donc il s'agit de $x \mapsto -x$ (si un endormorphisme est orthogonal, ses seules valeurs propres possibles sont 1 et -1). f est donc une symétrie par rapport à un plan. $f \in O^-(E)$.

◇ *dim* $I = 1$ La restriction de f à l'orthogonal de I (rappelons que si un espace est stable pour un endomorphisme orthogonal, alors son orthogonal aussi) est un endomorphisme orthogonal et n'a pas de vecteur invariant ; donc c'est une rotation. Donc f est une rotation autour d'un axe. Sa matrice est semblable à la matrice

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 00 \\ 0 & 1 & \end{pmatrix}$$

f est de déterminant 1, et donc appartient à $SO(E) = O^+(E)$.

◇ *dim* $I = 0$ En dimension 3, tout endomorphisme admet au moins une valeur propre (tout polynôme de degré impair admettant au moins une racine sur $\mathbb{R}$).

f admet donc nécessairement une valeur propre. Or un endomorphisme orthogonal ne peut avoir pour valeur propre que 1 ou -1 ; donc -1 est valeur propre.

On va maintenant considérer O, l'ensemble des x tels que $f(x) = -x$, et on va raisonner sur la dimension de O.

dim $O = 3$ On a alors f la symétrie par rapport à 0 ; f est dans $O(E)$ et pas dans $SO(E)$; f est dans $O^-(E)$. f est la composée d'une symétrie (= un demi-tour, donc une rotation) par rapport à une droite et de la symétrie par rapport au plan orthogonal à cette droite.

dim $O = 2$ **: cas impossible** Supposons *dim* $O = 2$.

Alors l'orthogonal de O est stable par f ; donc soit la restriction de f à cet orthogonal est l'identité, soit c'est moins l'identité ; puisque *dim* $I = 0$ il s'agit de moins l'identité. Donc en fait *dim* $O = 3$, d'où contradiction. Donc ce cas ne peut se produire.

dim $O = 1$ On considère alors la restriction de f à l'orthogonal de O. Il s'agit d'un endomorphisme orthogonal en dimension 2, sans valeur propre ; donc une rotation qui n'est pas une symétrie par rapport à un point, ni l'identité. f est de déterminant -1, et donc est dans $O(E)$ mais pas dans $SO(E)$; $f \in O^-(E)$.

1.10.4 Groupe orthogonal réel et groupe spécial orthogonal réel

DÉFINITION 0.24 **groupe orthogonal réel d'ordre n**
On appelle **groupe orthogonal réel d'ordre** n l'ensemble des matrices M réelles de type (n, n) telles que ${}^tM.M = I$, on le note $O_n(\mathbb{R})$; il s'agit d'un sous-groupe du groupe linéaire réel d'ordre n.

On appelle **groupe spécial orthogonal réel d'ordre** n l'ensemble des matrices M réelles de type (n, n) telles que ${}^tM.M = I$ et $det\ M = 1$, on le note $SO_n(\mathbb{R})$ ou $O_n^+(\mathbb{R})$; il s'agit d'un sous-groupe du groupe orthogonal réel d'ordre n et d'un sous-groupe du groupe spécial linéaire d'ordre n. C'est d'ailleurs leur intersection.

On appelle **matrice orthogonale** une matrice appartenant à $O_n(\mathbb{R})$ pour un certain n.

On ne parlera pas ici d'algèbre de Lie ; les puristes noteront que l'algèbre de Lie associée aux groupes de Lie $O(n)$ et $SO(n)$ est l'ensemble des matrices antisymétriques $n \times n$ à coefficients complexes.

PROPOSITION 0.37 **Propriété des matrices orthogonales réelles**
Une matrice est orthogonale si et seulement si sa transposée l'est.

Une matrice est orthogonale si et seulement si ses vecteurs colonnes forment une famille orthonormale de $\mathbb{R}^n$.

Une matrice est orthogonale si et seulement si ses vecteurs lignes forment une famille orthonormale de $\mathbb{R}^n$.

Une matrice est orthogonale si et seulement si il s'agit d'une matrice de changement de bases orthonormales.

Une matrice orthogonale est de déterminant 1 ou -1.

Une valeur propre de matrice orthogonale est soit 1 soit -1.

Une matrice orthogonale M vérifie $com(M) = det(M).M$.

1.10.5 Groupe affine d'un espace affine

DÉFINITION 0.25 **groupe affine d'un espace affine X**
On appelle **groupe affine d'un espace affine** X l'ensemble des applications affines bijectives de X dans lui-même muni de la composition ; c'est un groupe. On le note $GA(X)$.

On appelle **groupe spécial affine d'un espace affine** X l'ensemble des applications affines bijectives f de X dans lui-même telles que $det\ \overrightarrow{f} = 1$, muni de la composition ; c'est un groupe. On le note $SA(X)$.

Le fait qu'il s'agisse d'un groupe est facile à voir. La proposition suivante est évidente :

PROPOSITION 0.38
L'application $f \mapsto \overrightarrow{f}$ est un morphisme de $GA(X)$ dans $GL(\overrightarrow{X})$.

Notons que :

— Son noyau est le sous-groupe des translations.

— Ce morphisme est surjectif.

Étudions maintenant la structure du groupe $GA(X)$.

PROPOSITION 0.39
•$GA(X)$ est engendré par l'ensemble des dilatations affines de X.
•$SA(X)$ est engendré par l'ensemble des transvections affines de X.

⊡ **Générateurs de $GA(X)$ et $SA(X)$**
Démonstration *Simple conséquence de la proposition 0.35.*

⊡ **Sous-groupes remarquables de $GA(X)$**

◇ **Le sous-groupe des symétries** L'ensemble des symétries est un sous-groupe distingué de $GA(X)$. En effet, avec $s_{A,\overrightarrow{B}}$ la symétrie par rapport à A parallèlement à $\overrightarrow{B}$, on a

$$g \circ s_{Y,\overrightarrow{Z}} \circ g^{-1} = s_{g(Y),\overrightarrow{g}(\overrightarrow{Z})}$$

◇ **Le sous-groupe des translations** L'ensemble $T(X)$ des translations de l'espace affine X est un groupe pour la composition ; ce groupe est distingué. On le voit en constatant que c'est le noyau du morphisme qui à f dans $GA(X)$ associe $\overrightarrow{f}$ dans $GL(\overrightarrow{X})$.

◇ **Le sous-groupe des homothéties-translations** L'ensemble des homothéties et des translations d'un espace affine X est stable par composition et contient l'identité ; or il est inclus dans $GA(X)$. Donc c'est un sous-groupe de $GA(X)$. Il est généré par les homothéties (toute translation s'exprime comme composée de deux homothéties de rapport inverse).

Ce sous-groupe est exactement l'ensemble des bijections de X transformant toute droite en une droite parallèle.

◇ **Le sous-groupe des applications affines bijectives de X laissant une partie donnée invariante** On fixe une partie P de X, et on considère G l'ensemble des f appartenant à $GA(X)$ telles que $f(P) \subset P$; G est stable par composition et contient l'identité, c'est donc un sous-groupe de $GA(X)$.

◇ **En dimension finie, le sous-groupe des applications affines laissant fixe un repère** On suppose que X est de dimension finie n. On se donne alors un repère affine $A_0, A_1, ..., A_n$.

Nécessairement, une bijection affine f laissant invariant un repère a pour restriction à la partie $\{A_0, ..., A_n\}$ une permutation σ. Une application affine étant entièrement déterminée par l'image d'un repère affine, on en déduit que l'ensemble des applications affines bijectives laissant invariant le repère $A_0, A_1, ..., A_n$ est un groupe isomorphe à σ_{n+1}.

⊡ **Le groupe affine comme produit semi-direct** On a vu que $T(X)$, ensemble des translations de X, est distingué dans $GA(X)$, puisque noyau du morphisme $f \mapsto \overrightarrow{f}$. On a une suite exacte

$$\begin{array}{ccccccc} & & & & f \mapsto \overrightarrow{f} & & \\ 1 & \to & T(X) & \to & GA(X) & \to & GL(\overrightarrow{X}) \to 1 \end{array}$$

On se donne O appartenant à X donné ; l'application $f \mapsto \overrightarrow{f}$ induit une bijection de l'ensemble des bijections affines de X laissant O invariant sur $\overrightarrow{X}$; on a donc un relèvement de $GL(\overrightarrow{X})$.

Donc $GA(X) = T(X) \rtimes GL(\overrightarrow{X})$, avec pour action de $GL(X)$ dans $T(X)$ $\overrightarrow{f}.t = f_0^{-1} \circ t \circ f_0$ avec f_0 l'application affine laissant O invariant et associée à $\overrightarrow{f}$ (ce qui revient à $\overrightarrow{f}.t_{\overrightarrow{a}} = t_{\overrightarrow{f}(\overrightarrow{a})}$, en notant $t_{\overrightarrow{u}}$ la translation de vecteur $\overrightarrow{u}$).

En considérant l'isomorphisme évident entre $T(X)$ et $\overrightarrow{X}$ (c'est-à-dire en remplaçant une translation par le vecteur de cette translation) on peut aussi écrire

$$GA(X) = \overrightarrow{X} \rtimes GL(\overrightarrow{X})$$

Et quel que soit O dans X on peut écrire toute application bijective affine f de X dans X sous la forme $f = t \circ u_0$ avec u_0 application affine bijective laissant O invariant.

1.10.6 Groupe projectif d'un espace vectoriel de dimension finie

DÉFINITION - PROPOSITION 0.26 **1**
On se donne E un $\mathbb{K}$-espace vectoriel de dimension finie. L'ensemble des homographies de $P(E)$ dans $P(E)$ forme un groupe pour $\circ$, appelé **groupe projectif de** E, noté $PGL(E)$. Ce groupe est isomorphe à $GL(E)/(\mathbb{K}^*.I)$, avec I l'identité de E dans E.
On note usuellement $PGL_n(\mathbb{K})$ pour $PGL(\mathbb{K}^n)$.

Démonstration *Seul l'isomorphisme mérite d'être détaillé.*
Considérons l'application H, qui à un endomorphisme de E associe l'homographie associée à cet endomorphisme (on se donne bien entendu pour cela un repère projectif de E).
Son noyau est l'ensemble des applications linéaires de E dans E qui laissent toute droite invariante. Il faut donc montrer qu'un endomorphisme laissant toute droite invariante est une homothétie.

LEMME 0.40
Un endomorphisme d'un espace vectoriel laissant invariante toute droite est une homothétie.

begindivdemonstrationbegintext endtext On considère f un endomorphisme de E, tel que pour tout $x \in E$ il existe un scalaire λ_x tel que

$$f(x) = \lambda_x.x.$$

Soient $x, y \in E \setminus \{0\}$.
Il est clair que si x et y sont liés, alors $\lambda_x = \lambda_y$.
Considérons maintenant x et y linéairement indépendants.
Alors $f(x+y) = \lambda_{x+y}.x + \lambda_{x+y}.y = f(x) + f(y) = \lambda_{\ddot{x}}.x + \lambda_{\ddot{y}}.y$, donc $_x = _{x+y} = _y$.
On a donc montré le résultat souhaité.
Du coup, grâce à ce lemme, la preuve de la proposition est achevée.enddivdemonstration

1.10.7 Groupe unitaire et groupe spécial unitaire d'un espace hermitien

DÉFINITION 0.27 **groupe unitaire de E**
On appelle **groupe unitaire de** E et on note $U(E)$ avec E un espace hermitien (voir partie **??**) l'ensemble des automorphismes unitaires de E, c'est-à-dire des automorphismes f de E tels que $f^{-1} = f^*$, muni de la composition.

On appelle **groupe spécial unitaire de** E, et on note $SU(E)$, avec E un espace hermitien, le sous-groupe de $U(E)$ constitué des automorphismes unitaires de E de déterminant 1.

Ces groupes sont isomorphes aux groupes dont il est question ci-dessous.

On note bien que le déterminant d'un élément de $U(E)$ peut être n'importe quelle valeur du cercle unité, et pas seulement 1 et -1 comme dans le cas des endomorphismes orthogonaux d'un espace euclidien.

1.10.8 Groupe unitaire complexe d'ordre n et groupe spécial unitaire complexe d'ordre n

DÉFINITION 0.28 **groupe unitaire complexe d'ordre n**
L'ensemble des matrices M de type (n, n) à coefficients dans $\mathbb{C}$ telles que ${}^t\overline{M}.M = I$ est un groupe pour $\circ$; on l'appelle **groupe unitaire complexe d'ordre** n, et on le note $U_n(\mathbb{C})$.

L'ensemble des matrices M de type (n, n) à coefficients dans $\mathbb{C}$ telles que ${}^t\overline{M}.M = I$ et $det\ M = 1$ est un groupe pour $\circ$; on l'appelle **groupe spécial unitaire complexe d'ordre** n ; on le note $SU_n(\mathbb{C})$, c'est un sous-groupe de $U_n(\mathbb{C})$.

1.10.9 Groupe des similitudes d'un espace euclidien

DÉFINITION 0.29 **groupe des similitudes d'un espace euclidien E**
On appelle **groupe des similitudes d'un espace euclidien** E et on note $GO(E)$ l'ensemble des similitudes d'un espace euclidien E, muni de la composition $\circ$.

Il s'agit d'un groupe, sous-groupe de $GL(E)$ (groupe linéaire de E, ensemble des automorphismes de E).

Il est isomorphe à $\mathbb{R}_+^* \times O(E)$, avec $O(E)$ l'ensemble des automorphismes orthogonaux de E.

1.10.10 Groupe des quaternions

On le note H_8. Ses éléments sont $1, -1, i, j, k, -i, -j, -k$, et la multiplication est définie par la table suivante :

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

On peut aussi résumer la loi de multiplication par

$$ij = k, jk = i, ki = j$$

$$ji = -k, kj = -i, ik = -j$$

$$i^2 = j^2 = k^2 = -1.$$

On note que

$$D(H_8) = \{1, -1\}$$

$$Z(H_8) = \{1, -1\}$$

Le groupe des quaternions n'est pas commutatif. Ses sous-groupes sont $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$, et H_8 lui-même ; ils sont tous distingués. Cela montre d'ailleurs que la propriété des groupes abéliens d'avoir tous leurs sous-groupes distingués n'est pas une condition suffisante pour que le groupe soit abélien.

Application 0.8 Le groupe des quaternions sert par exemple à placer des points sur la sphère ; voir e.g. [2].

1.10.11 Groupe symétrique

DÉFINITION 0.30 **permutation**
On appelle **permutation** d'un ensemble une bijection de cet ensemble sur lui-même.

On appelle **support** d'une permutation σ sur un ensemble E l'ensemble des éléments $x \in E$ qui vérifient $\sigma(x) \neq x$.

On appelle **cycle** d'un ensemble une bijection f telle qu'il existe $a_1, ..., a_n$ (en nombre fini et distincts) tels que $f(a_i) = a_{i+1}$ pour $i < n$, $f(a_n) = a_1$ et $f(b) = b$ si b n'est aucun des a_i. On note alors $f = (a_1, a_2, \ldots, a_n)$. n est l'ordre du cycle ; il ne s'agit pas d'une définition, car cet ordre colle à la notion d'ordre sur les éléments d'un groupe. n est aussi appelé **longueur** du cycle.

On appelle **n-cycle** un cycle d'ordre n.

On appelle **transposition** une permutation qui « échange» deux éléments. On note (a, b) la transposition qui échange a et b. Une transposition est un cycle de longueur 2.

On appelle **groupe symétrique** d'un ensemble E l'ensemble des permutations de cet ensemble.

On note σ_n et on appelle **n-ième groupe symétrique standard** le groupe symétrique de $\{1, 2, ..., n\}$. Tous les groupes symétriques sur des ensembles de cardinal n sont isomorphes à σ_n.

Pour un n donné on appelle **signature** l'unique homomorphisme ϵ de σ_n dans $\{1, -1\}$ tel que $\epsilon(\tau) = -1$ lorsque τ est une transposition.

On appelle **n-ième groupe alterné** le noyau de ϵ (dans σ_n). On le note U_n.

On appelle **matrice associée à la permutation σ de σ_n** la matrice M telle que $M_{i,j} = \delta_{i,\sigma(j)}$.

Application 0.9 On utilisera la signature pour l'algèbre multilinéaire (section **??**), et en particulier le déterminant (section **??**).

Remarques et propriétés : •On parle aussi, au lieu de n-ième groupe symétrique standard, de **groupe symétrique d'ordre** n ; il faut bien voir que ce groupe n'est *PAS* d'ordre n mais d'ordre $n!$.

•Pour bien faire il faudrait démontrer que l'on caractérise bien ici la signature. Cela sera fait dans la proposition 0.46.

•$|\sigma_n| = n!$

•$Z(\sigma_n) = 1$ si $n \geq 3$.

•σ_n est engendré par les transpositions.

•σ_n est engendré par les transpositions de la forme $(a, a+1)$, avec $a \in [1, n-1]$.

•σ_n est engendré par les transpositions de la forme $(1, a)$, avec $a \in [2, n]$.

•σ_n est engendré par la transposition $(1, 2)$ et le cycle $(1, 2, ..., n)$.

•U_n est engendré par les cycles d'ordre 3.

•Des cycles de supports disjoints commutent.

PROPOSITION 0.41
Soit p une permutation de E fini. L'orbite d'un point x pour p est l'ensemble des $p^n(x)$ avec $n \in \mathbb{N}$. p est un cycle s'il existe une orbite et une seule qui soit de cardinal > 1.

Démonstration *Si on a un cycle, il est clair qu'il existe une seule orbite de cardinal > 1 ; si on a une seule orbite dans ce cas, alors on considère les éléments de l'orbite, la suite est évidente.*

THÉORÈME 0.42
Toute permutation peut s'écrire comme produit de cycles de supports deux à deux disjoints. La décomposition est unique à l'ordre près des facteurs.

Démonstration *Considérons une permutation σ de $\{1, 2, \ldots, n\}$. L'unicité de sa décomposition sous la forme annoncée découle immédiatement de l'étude des orbites de l'action de $< \sigma >$ sur $[1, n]$ (on considère ce qu'il se passe sur chaque orbite).*

Pour l'existence, on se restreint aussi à une telle orbite. Il est clair que σ se comporte sur cette orbite comme un cycle. D'où le résultat.

PROPOSITION 0.43
Le centre de σ_n est trivial dès que $n \geq 3$.

Démonstration *Soit σ élément non neutre de σ_n. Il existe alors i tel que $\sigma(i) = j \neq i$. On prend alors k différent à la fois de i et de j, et on constate que $\sigma \circ (j\ k)(i) \neq (j\ k) \circ \sigma(i)$*

PROPOSITION 0.44
L'opération de σ_n sur σ_n par automorphisme intérieur, comme étudié en 1.9.3, est fidèle pour $n \geq 3$.

⊡ **La conjugaison dans σ_n**

Démonstration *Il suffit de noter que le centre est trivial.*

PROPOSITION 0.45
•Pour tout m, l'ensemble des cycles d'ordre m est une orbite (c'est-à-dire une classe de conjugaison).

•Si $n \geq 5$ les cycles d'ordre 3 sont conjugués dans U_n.

Démonstration *Remarquons tout d'abord que si* $f = (x_1, ..., x_k) \in \sigma_n$ *et* $g \in \sigma_n$, *alors* $g.f.g^{-1} = (g(x_1), ..., g(x_k))$. *Pour montrer le premier point, il suffit alors, étant donnés deux cycles de même longueur* $(x_0, ..., x_k)$ *et* $(y_0, ..., y_k)$ *de considérer une permutation* p *qui à* x_i *associe* y_i *; on a bien* $p.x.p^{-1} = y$.

Le deuxième point est plus délicat, et utilise la proposition 0.44. Étant donnés deux 3-cycles (x_0, x_1, x_2) *et* (y_0, y_1, y_2), *on considère la permutation* p *de* U_n *qui à* x_i *associe* y_i *; on a bien* $x = p.y.p^{-1}$.

⊡ **Les matrices de permutations** L'application ϕ qui à une permutation associe la matrice associée à cette permutation est un morphisme injectif dans $GL_n(\mathbb{K})$ (ensemble des matrices inversibles de type (n, n)).

On a la propriété $\phi(s)^{-1} = \phi(s^{-1}) = {}^t\phi(s)$.

Le déterminant de $\phi(s)$ est égal à la signature de s.

PROPOSITION 0.46 **Différentes caractérisations de la signature**

On peut définir la signature ϵ sur σ_n de l'une des façons suivantes :

1) On appelle **inversion** d'une permutation p, une paire (i, j) d'éléments tels que $(j-i).(p(j)-p(i)) < 0$. On définit $\epsilon(p) = (-1)^{Inv(p)}$, avec $Inv(p)$ le nombre d'inversions.

2) Il existe un unique morphisme ϵ de σ_n sur $\{-1, 1\}$ tel que $\epsilon(t) = -1$ si t est une transposition.

3) $\epsilon(p)$ est égal à $(-1)^s$ avec s le nombre de transpositions dans une décomposition de p en produit de transpositions. Il est aussi égal au produit $\Pi_{i<j} \frac{p(j)-p(i)}{j-i}$.

⊡ **La signature**

Démonstration *Pour voir que* 1 *entraine* 2 *il faut voir que* $\epsilon(p)$ *est le produit* $\Pi_{i<j} \frac{p(j)-p(i)}{j-i}$, *le reste est facile.*

Il y a en outre une caractérisation de la signature par les matrices de permutation, donnée dans la section ci-dessus.

⊡ **Simplicité de U_n pour $n > 4$; conséquences** La preuve du théorème qui suit est tirée de l'excellent [[]p. 28]PER qui contient beaucoup d'autres choses pour approfondir les éléments contenus dans ce chapitre.

THÉORÈME 0.47
U_n est simple (i.e. sans sous-groupe distingué non trivial) si $n \geq 5$.

Démonstration *On procède en deux étapes :*

•*Le cas* $n = 5$

– *Le groupe* U_5 *se décompose en 60 éléments ; l'identité, 15 éléments d'ordre 2, qui sont des produits de deux transpositions disjointes, 20 éléments d'ordre 3, qui sont des 3-cycles, et 24 d'ordre 5, qui sont des 5-cycles. On va se préoccuper des classes de conjugaison de* U_5.

– *les éléments d'ordre* 2 *sont conjugués (facile).*

– *les* 3*-cycles sont conjugués.*

Supposons H *sous-groupe de* U_5, *et* $H \lhd U_5$, *et* $H \neq \{1\}$.

– *S'il contient un élément d'ordre* 3 *il les contient tous, puisqu'il est distingué et que les éléments d'ordre* 3 *sont conjugués.*

– *S'il contient un élément d'ordre 2 il les contient tous, puisqu'il est distingué et que les éléments d'ordre 2 sont conjugués.*

– *S'il contient un élément x d'ordre 5, alors il contient aussi le 5-Sylow engendré par x (voir les théorèmes de Sylow, 1.5). Les 5-Sylow étant tous conjugués, il les contient donc tous ; tout élément d'ordre 5 étant inclus dans un 5-sylow, tout élément d'ordre 5 est alors inclus dans H.*

– *S'il contient donc un seul type d'éléments parmi les éléments ci-dessus en plus de l'unité, alors son cardinal serait soit $1+20$, soit $1+24$, soit $1+15$; or ces nombres ne divisent pas 60. Donc il contient au moins deux types de ces éléments. Donc son cardinal est au moins $1+15+20$, et comme il divise 60, H est en fait égal à U_5. Le résultat est donc prouvé dans le cas de U_5.*

•*Le cas $n > 5$*

– *On considère $H \lhd\!\lhd U_n$, $H \neq \{1\}$; on considère σ dans H, $\sigma \neq 1$.*

– *Par hypothèse on a un certain a tel que $b = \sigma(a) \neq a$.*

– *on peut choisir c différent à la fois de a, de b et de $\sigma(b)$.*

– *on considère τ le 3-cycle (acb) ; $\tau^{-1} = (abc)$.*

– *On note ρ la permutation $(\tau.\sigma.\tau^{-1}).\sigma^{-1} = (acb)(\sigma.a, \sigma.b, \sigma.c)$.*

– *L'ensemble $\{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ ayant au plus 5 éléments (car $\sigma(a) = b$), on le complète par des éléments quelconques pour avoir un ensemble F de 5 éléments contenant $\{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$.*

– *ρ est l'identité en dehors de F, et $\rho(F) = F$.*

– *On constate que ρ est différent de l'identité car $\rho(b) \neq b$.*

– *U_F, ensemble des permutations paires de F est isomorphe à U_5 ; on a un morphisme injectif ϕ de U_F dans U_n en considérant pour une permutation t de U_F la permutation dont la restriction à F est t et la restriction à F^c est l'identité.*

– *On considère H' l'intersection de H et de U_F.*

– *H' est distingué dans U_F, clairement.*

– *il est clair que ρ_F appartient à U_F, et que ρ_F n'est pas l'élément neutre (toujours car $\rho_F(b) \neq b$).*

– *Par simplicité de U_F, on sait alors que H' est égal à U_F.*

– *On considère alors un 3-cycle c de F, il est dans H', donc $\phi(c)$ est dans H.*

– *H contient donc un 3-cycle, or puisqu'il est distingué il contient aussi sa classe de conjugaison, donc il contient tous les 3-cycles (les 3-cycles étant tous conjugués). Donc il contient le groupe engendré par les 3-cycles, c'est-à-dire U_n.*

Ceci termine la preuve.

COROLLAIRE 0.48
$D(U_n) = U_n$ pour $n \geq 5$ et $D(\sigma_n) = U_n$ pour $n \geq 2$.

Démonstration •*Première preuve (en utilisant le théorème) :*

$D(U_n)$ est distingué, donc il ne saurait être plus petit que U_n, puisque U_n est simple, donc $D(U_n) = U_n$.

$D(\sigma_n)$ est le sous-groupe engendré par les commutateurs de σ_n, or il est clair que ces commutateurs appartiennent à U_n (considérer leurs signatures). Donc $D(\sigma_n)$ est inclus dans U_n, or puisqu'il est distingué, il ne saurait être inclus strictement.

•*Deuxième preuve (élémentaire) :*

– *on montre facilement que tout commutateur de σ_n est dans U_n.*

– *on en déduit que $D(U_n) \subset D(\sigma_n) \subset U_n$*

– *on montre alors que tout 3-cycle de U_n s'écrit comme commutateur d'éléments de U_n ; en effet avec f un tel 3-cycle, f et f^2 sont conjugués dans U_n (vrai pour toute paire de 3-cycles), donc $f^2 = t.f.t^{-1}$, et donc $f = t.f.t^{-1}.f^{-1}$.*

COROLLAIRE 0.49
Les sous-groupes distingués de σ_n sont $\{1\}, U_n, \sigma_n$.

Démonstration *Supposons H sous-groupe distingué de σ_n.*

•$H \cap U_n$ est égal à 1 ou U_n.

•Si $H \cap U_n = U_n$, alors si $H \neq U_n$, alors H contient un produit impair de transpositions ; en multipliant par l'inverse du produit des transpositions sauf une on constate que H contient une transposition. Étant données deux transpositions, on constate qu'elles sont conjuguées par les éléments de U_n ; donc H contient en fait tout σ_n.

•Si $H \cap U_n = \{1\}$, alors ϵ est un isomorphisme de H sur $\epsilon(H)$. Donc H contient en fait un seul autre élément au plus. S'il en contient deux alors soit τ l'autre élément ; il doit commuter avec n'importe quel élément puisque H est distingué et puisque τ n'est pas conjugué à l'unité ; or le centre de σ_n est trivial.

COROLLAIRE 0.50
Soit G un sous-groupe de σ_n d'indice n. Alors G est isomorphe à σ_{n-1}.

Démonstration *On rappelle que l'on appelle indice d'un sous-groupe le cardinal de l'ensemble quotient. Un sous-groupe d'indice n de σ_n est donc en fait un sous-groupe de cardinal $(n-1)!$.*

Le cas $n \leq 4$ s'obtient facilement. Pour $n \geq 5$, on constate que σ_n ou G opère à gauche sur l'ensemble quotient (par translation à gauche, voir 1.9.2). On a donc un homomorphisme ϕ de σ_n dans l'ensemble des permutations de σ_n/G, qui est isomorphe à σ_n, car $\sigma_{\sigma_n/G} \simeq \sigma_{card(\sigma_n/G)} \simeq \sigma_n$. Il reste maintenant à voir que cet homomorphisme est injectif (le caractère surjectif se déduisant alors des cardinaux). Son noyau est l'intersection des $a.G.a^{-1}$ pour a dans σ_n, et donc il est de cardinal au plus le cardinal de G, donc $(n-1)!$; or il est distingué, et on a montré que les seuls sous-groupes distingués de σ_n étaient $\{1\}$, U_n et σ_n ; donc il s'agit de 1, d'où le résultat.

Admettons enfin sans preuve la proposition ci-dessous :

PROPOSITION 0.51
Si $n \neq 4$ et $n \neq 6$ tous les G vérifiant ces hypothèses sont conjugués. En fait, avec les mêmes hypothèses que ci-dessus, il existe i tel que G soit l'ensemble des permutations laissant i invariant.

⊡ **Décomposition de σ_n** On a une suite exacte

$$1 \to U_n \to \sigma_n \xrightarrow{\epsilon} \{-1, 1\} \to 1$$

avec ϵ la signature. Avec τ une transposition (c'est-à-dire une permutation de deux éléments) alors $\{Id, \tau\}$ est un groupe qui est une section pour ϵ, donc on a

$$\sigma_n \simeq U_n \rtimes \{\tau, Id\} \simeq U_n \rtimes \{-1, 1\} \simeq U_n \rtimes \mathbb{Z}/2\mathbb{Z}$$

En outre, σ_n est isomorphe à l'ensemble des automorphismes intérieurs lorsque $n \geq 3$; en effet le centre est alors trivial. On verra plus bas que l'ensemble des automorphismes intérieurs est lui-même égal à l'ensemble des automorphismes lorsque $n \neq 6$.

⊡ **Automorphismes de σ_n**

PROPOSITION 0.52
Un automorphisme de σ_n transformant toute transposition en transposition est un automorphisme intérieur.

◇ **Les automorphismes sont des automorphismes intérieurs lorsque** $n \neq 6$

Démonstration *On considère les transpositions* $t_i = (1, i)$ *pour* $i > 1$. *Ces transpositions engendrent toutes les transpositions. Il suffit donc de montrer que* ϕ, *qui transforme toutes ces transpositions en transpositions, coïncide avec un automorphisme intérieur.*

Pour cela on constate que :

•*les* $\phi(t_i)$ *ne sont pas disjointes deux à deux.*

•$\phi(t_i)$ *et* $\phi(t_j)$ *ont même élément commun que* $\phi(t_i)$ *et* $\phi(t_k)$.

•*on peut donc noter* $\phi(t_i)$ *sous la forme* (z_1, z_i).

•z *est la permutation recherchée, tel que l'automorphisme intérieur correspondant corresponde à* ϕ.

PROPOSITION 0.53
On suppose $n = 1.k_1 + 2.k_2 + ... + m.k_m$ et que σ est une permutation produit de $\sum_i k_i$ cycles disjoints, k_1 d'ordre 1, k_2 d'ordre 2, k_3 d'ordre 3, ... ,k_m d'ordre m. Alors le cardinal du centralisateur de σ est égal à

$$|c(\sigma)| = \Pi_{i=1}^{m} k_i!.i^{k_i}$$

Démonstration •*Tout d'abord on montre le résultat pour un seul cycle, d'ordre* n.

Le centralisateur est alors tout simplement de cardinal n *; il s'agit du sous-groupe engendré par ce cycle. Pour le voir on se ramène à un cycle* $(1, 2, ..., n)$ *; pour que* τ *commute avec ce cycle, il faut que* $\tau(n+1) = \tau(n) + 1$, *c'est-à-dire que* $\tau(n+1) - \tau(n) = 1$, *donc que* $\tau(n) = \tau(0) + n$ *(on compte modulo* n*) ; on a donc un élément dans le centralisateur pour tout élément de* $[1, n]$.

•*On le généralise ensuite à* k *cycles de même ordre* i.

Alors en se restreignant aux permutations laissant invariants chacun des supports, on a i *possibilités, on obtient donc* i^k. *Mais il reste la possibilité d'intervertir les supports, il faut donc multiplier par* $k!$. *Il est clair que toutes les permutations ainsi construites sont bien dans le centralisateur ; pour la réciproque, il suffit de supposer que* a *et* $a + 1$ *appartenant au support du même cycle (supposés de la forme* $(j, j + 1, .., j + i - 1)$, *et qu'ils ne sont pas envoyés dans un même support ; on constate alors que notre permutation ne saurait commuter avec notre produit de cycles.*

•*On le généralise enfin au cas le plus général.*

Il suffit de faire comme ci-dessus et de constater que quand deux supports n'ont pas la même taille il est impossible de mettre tous les éléments de l'un dans l'autre...

THÉORÈME 0.54
Si $n \neq 6$ alors tout automorphisme de σ_n est un automorphisme intérieur.

Démonstration *L'image d'une transposition par un automorphisme* ϕ *est d'ordre* 2, *et donc est un produit de* k *transpositions disjointes. Par la proposition 0.53 le cardinal de son centralisateur est alors* $2^k.k!.(n - 2.k)!$ *; ce cardinal est aussi le cardinal du centralisateur de notre transposition initiale, donc* $2.(n-2)!$. *Si* $n = 6$, *on a une solution avec* $n = 6$ *et* $k = 3$, *si* $n \neq 6$, *on a une seule solution pour* $k = 1$. *Donc l'image d'une transposition par* ϕ *est une transposition ; donc par la proposition 0.52,* ϕ *est un automorphisme intérieur.*

1.10.12 Groupes et géométrie

DÉFINITION 0.31 **Groupe diédral**
On appelle **groupe diédral d'ordre** n et on note D_n le groupe des isométries du plan conservant un polygone régulier à n côtés. Il contient $2.n$ éléments, comme on pourra s'en convaincre en distinguant le cas n pair et le cas n impair ; n rotations et n symétries.

On note R_n l'ensemble des n rotations de D_n.

PROPOSITION 0.55
On a $R_n \lhd\!\!\lhd D_n$, et donc

$$1 \to R_n \to D_n \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \to 1$$

en effet D_n étant d'ordre $2.n$, le quotient de D_n par R_n est d'ordre 2, et ne peut donc être qu'isomorphe à $\mathbb{Z}/2.\mathbb{Z}$.

Étant donnée $r \in D_n \setminus R_n$, $\{r, Id\}$ fournit une section ; donc on a $D_n = R_n \rtimes \{r, Id\}$, donc $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

⊡ **Groupe diédral** D_n On pourra consulter la partie « Sous-groupes finis de $O_2(\mathbb{R})$ » page **??** pour plus d'informations sur le groupe diédral. Ci-dessous une liste non exhaustive d'autres applications des groupes en géométrie :

- **cercle unité complexe** $(\mathbb{U}, \times)$, groupe des nombres complexes de module 1, permettant de définir les angles. Isomorphe à $O_2^+(\mathbb{R})$ et à $\mathbb{R}/2\pi\mathbb{Z}$.
- **groupe linéaire** $GL(E)$ des applications linéaire d'un espace vectoriel dans lui-même. Voir 1.10.2.
- **groupe affine** $GA(\xi)$ des bijections affines d'un espace affine ξ dans lui-même. Le centre de $GA(\xi)$ est réduit à l'identité. On remarquera notamment que si le groupe additif d'un espace vectoriel agit librement et transitivement sur un ensemble ξ, celui-ci est muni par cette opération d'une structure d'espace affine. Voir 1.10.5.
- **groupe des isométries** d'un ensemble (voir partie **??**)
- **groupe des similitudes** d'un espace euclidien (voir partie 1.10.9)
- **groupe orthogonal** d'un espace euclidien, $O(E)$; voir sections 1.10.3 et **??**.
- **groupe projectif** d'un espace vectoriel de dimension finie. Voir 1.10.6.

L'étude des sous-groupes finis de $O(3)$ est un préambule capital pour montrer que les seuls polyèdres réguliers convexes sont les 5 volumes platoniciens.

Références

[1] Wikipédia, *L'encyclopédie Libre, Wikipédia*, Wikipédia Fondation.

[2] B. Chazelle, *The Discrepancy Method*, Cambridge University Press, 2000.

[3] D. Perrin, *Cours d'algèbre*, Ellipses 1996.