LA NOTION DE GROUPE : TRÈS BREF HISTORIQUE

Les propriétés de la famille, changeons l'appellation, de la société, voire du groupe des permutations des racines d'une équation polynomiale – on voit apparaître la dénomination de groupe vers 1815 – fournissent des renseignements précieux sur les propriétés de ces racines. Galois les met en évidence vers 1830.

Lagrange, dans les années 1770-1771, est le premier à avoir énoncé et démontré une propriété qui concerne les groupes – à son époque certes on ignorait ce qu'était la structure de groupe. C'est Cayley en 1853 qui en propose une première définition abstraite. La version abstraite définitive a été donnée par Weber en 1895.

Le tableau suivant, retouché, a été emprunté au site de l'Université Libre de Bruxelles.

Voir également : http://www-history.mcs.st-andrews.ac.uk/HistTopics/Abstract_groups.html

1895	Weber	Axiomatique des groupes.
1902	Huntington	Axiomes « classiques » des groupes.
1906	Burnside	Conjecture que tout groupe simple (càd. n'ayant pas de sous-groupe invariant) non cyclique est de cardinal pair. Les groupes simples jouent pour les groupes le même rôle que les nombres premiers.
1938	Frucht	Tout groupe fini est isomorphe au groupe formé des automorphismes d'un certain graphe (isomorphismes du graphe avec lui-même), avec la loi usuelle de composition.
1947	Markov - Post	Il n'existe pas d'algorithme permettant de déterminer de manière systématique si deux produits des générateurs d'un groupe représentent le même élément du groupe.
1957	Chevalley - Steinberg Suzuki - Ri	Théorie des groupes simples ; construction utilisant les ressources de la topologie, de l'algèbre des champs finis, du calcul vectoriel, de la théorie des isomorphismes.
1959	Novikov	Construit un groupe infini dont tous les éléments sont d'ordre fini.
1963	Feit - Thompson	Démontrent la conjecture de Burnside (voir 1906).
1972	Gorenstein	Etablit un programme pour la classification des groupes simples. Ce programme sera achevé en 1980 (voir cette date) par Aschbacher, Gorenstein, Fischer etc.
1980	Griess - Fischer	Construisent un groupe simple de cardinal énorme, le « monstre », groupe de rotations d'un espace vectoriel de dimension 19683. Ceci achève la classification des groupes simples.

LEÇONS INTRODUCTIVES À LA THÉORIE DES GROUPES

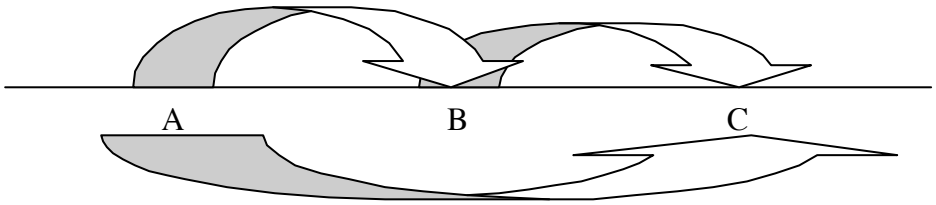
C.P.BRUTER

CHAPITRE I

LA STRUCTURE DE GROUPE

L'évolution du monde s'accomplit par des transformations de nature très diverse, parfois si lentes que nous n'en avons pas conscience. Un être vivant, par exemple, est le résultat de telles transformations t. Ces transformations sont réunies dans un ensemble **T**.

Un exemple simple de telles transformations et qu'il convient de garder constamment à l'esprit, est celui des transformations de même type appelées *translations*, qu'elles soient *rectilignes*, ou bien *angulaires* et appelées alors *rotations* : ce sont des opérations de transport, elles peuvent être de nature spatiale, ou bien, temporelle.



Si t_{ab} est la transformation qui transporte l'objet O du lieu A à l'endroit B, plus généralement si t_{ab} est la transformation qui transforme l'objet O de l'état A en l'état B, si t_{bc} est la transformation qui transforme ce même objet de l'état B à l'état C, la transformation globale qui le transforme de l'état A à l'état C est notée t_{ac}, et l'on dit que :

Définition 1.1 : t_{ac} est la *composition* de t_{ab} et de t_{bc}.

La manière physique dont s'accomplit cette composition ne nous est pas toujours accessible. On la codifie toutefois souvent par un symbole visible comme +, x, *, ou bien qui peut être sous-entendu. On écrit donc la transformation de l'état A à l'état C sous la forme symbolique

$$t_{ac} = t_{ab} * t_{bc} \text{ ou bien } t_{ac} = t_{ab}\, t_{bc}.$$

Un des points également importants de cette description de l'évolution du monde physique est la *stabilité* de notre système de transformations, en ce sens que la composition et dans cet ordre des deux transformations t_{ab} et t_{bc} donnera toujours le même résultat. De sorte que, de manière alors plus savante, on peut également décrire la composition des

transformations par la donnée d'une application, par exemple encore notée *, qui au couple de transformations (t_{ab}, t_{bc}) fait correspondre une transformation *unique* t_{ac} :

$$* : \mathbf{T} \times \mathbf{T} \rightarrow \mathbf{T}$$
$$(t_{ab}, t_{bc}) \longmapsto t_{ac}$$

Notons que tous les ensembles de transformations physiques ne peuvent pas être décrits par ce formalisme. Il signifie en effet que deux quelconques de ces transformations peuvent se composer. Or prenons la transformation de chauffe t_{ge} qui transforme la glace en eau, puis celle t_{ev} qui transforme l'eau en vapeur : la transformation $t_{ge}\ t_{ev}$ est bien réalisable, mais celle $t_{ev}\ t_{ge}$ n'a aucun sens.

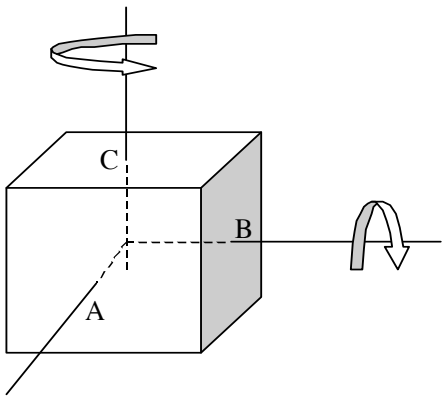
Autrement dit nous nous plaçons (désormais) dans le cadre restreint, mais quand même très large, des ensembles de transformations **T** pour lesquelles tt' et t't ont un sens, quelles que soient les transformations t et t' de **T**.

En général, pour ces transformations, accomplir tt' puis t", ou bien accomplir t puis t't", revient au même, ce que l'on code par :

$$(tt')\ t'' = t(t't'').$$

Définition 1.2 : Cette propriété est appelée l'*associativité*.

Il est par contre bien plus fréquent, notamment lorsque les transformations deviennent complexes, que tt' soit différent de t't. Supposons par exemple que t soit une rotation de 90° autour de l'axe vertical d'une bille de centre O, et que t' soit une rotation de même angle autour d'un axe horizontal de cette même bille : soit A un point de la bille située dans le plan horizontal.



La rotation t l'amène en B. Prenons OB pour définir l'axe horizontal de rotation : alors t' laisse fixe le point B, t'(t(A)) = t'(B) = B. Commençons maintenant par la rotation t': elle amène A en C situé sur l'axe vertical, et la rotation t autour de cet axe laisse évidemment C invariant: t(t'(A)) = t(C) = C qui est différent de B.

Définition 1.3 : Lorsque quelles que soient t et t', t' t = t t' la loi de composition est dite *commutative* (ou *abélienne*)[1]. C'est une limitation qu'il sera parfois nécessaire d'indiquer.

[1] F. Klein et ses successeurs utilisaient le terme « permutable ».

Les ensembles structurés par une loi de composition associative sont appelés des *monoïdes* par les uns, *demi-groupes* par les autres.

De manière conventionnelle, on fait en général apparaître la présence d'une transformation, souvent fictive, qui laisse invariant l'objet. Son effet est neutre. Cette transformation véritablement *neutre* t_n, c'est-à-dire par action à gauche et à droite, vérifie de ce fait :

$$t_n\, t = t\, t_n = t,$$

et en particulier :

$$t_n\, t_n = t^2_n = t_n.$$

Définition 1.4 : On dit d'un tel ensemble **T** de transformations t muni d'une loi de composition définie sur tous les couples d'éléments, associative, et possédant un élément neutre, qu'il possède la *structure de demi-groupe à élément neutre*. Du point de vue de l'auteur, on devrait réserver l'appellation de demi-groupe à un monoïde à élément neutre. On notera ce demi-groupe par (**T**, *), ou plus simplement par la lettre G :

$$G = (\mathbf{T}, *).$$

Du point de vue physique, la *stabilité* que présente un objet, liée à l'équilibre local des forces en présence, implique la présence de symétries dans sa constitution, et donc au sein de l'ensemble des transformations qui l'ont conduit à son état actuel.

Soit ainsi **T** un ensemble de transformations de même type, t une transformation de cet ensemble transformant l'objet O de l'état A à l'état B. La donnée nouvelle est l'existence d'une transformation réversible t^{-1} qui ramène l'objet de l'état B à l'état A.

L'exemple simple est celui de la translation : codant par t_3 le transport de l'objet O de la borne kilométrique 10 jusqu'à la borne kilométrique 13, il existe également un transport t_{-3} qui amène l'objet O de la borne kilométrique 13 jusqu'à la borne kilométrique 10. De ce fait, la composition des deux transports t_3 et t_{-3} revient à laisser l'objet fixe : on aboutit donc à la transformation neutre t_n.

Comme dans le cas des translations, on va supposer maintenant que toute transformation t admet un élément t^{-1} vérifiant $t\, t^{-1} = t^{-1}\, t = t_n$:

Définition 1.5 : t^{-1}est alors appelé un *symétrique* de t. En fait, de par la proposition suivante, t^{-1} sera appelé *le* symétrique de t.

Proposition 1.1 : *Soit* G = (**T**, *) *un demi-groupe à élément neutre*, *et* t *l'un de ses éléments admettant un symétrique* t^{-1} : *celui-ci est unique*.

<Preuve : Raisonnons par l'absurde. Supposons que t ait deux symétriques t^{-1} et t'^{-1} : par définition, $t\, t^{-1} = t_n$ et $t'^{-1}\, t = t_n$. Par conséquent $t'^{-1}(t\, t^{-1}) = t'^{-1}\, t_n = t'^{-1}$. Mais, par l'associativité de la loi de composition, on a également : $t'^{-1}(t\, t^{-1}) = (t'^{-1}t)\, t^{-1} = t_n\, t^{-1} = t^{-1}$. Par conséquent $t'^{-1} = t^{-1}$.>

Définition 1.6 : On dit qu'un ensemble **T** de transformations :

(*c*) muni d'une loi de composition
(*a*) associative,

(*n*) d'une transformation neutre t_n,
(*s*) tel que toute transformation t admet une symétrique t^{-1} vérifiant $t\,t^{-1} = t^{-1}t = t_n$

qu'il possède la *structure de groupe*.

Par abus de langage ou par extension, on appelle aussi *groupe* un ensemble de transformations, de mouvements, d'objets qui possède la structure de groupe, et donc vérifiant les propriétés "*cans*" (ou "*snac*" pour celui qui lirait de bas en haut).

A titre d'exercice, on vérifiera que tout demi-groupe fini est un groupe.
Lorsque le groupe est commutatif, on pourra appeler ses éléments des *vecteurs*. Mais, attention, il en faut bien davantage pour qu'un tel groupe puisse également être appelé un espace vectoriel !

Un groupe particulier est le groupe dit *trivial*, réduit au seul élément neutre, souvent noté **1**.

Dans quels exemples de situation verrons-nous apparaître la structure de groupe ? Chaque fois que l'on sera en présence de transformations, de déplacements présentant un caractère marqué de réversibilité, exprimée dans le langage mathématique sous le nom de symétrie. Un cas d'étude très classique est celui des polygones et plus généralement des polyèdres que l'on caractérise par l'ensemble de leurs symétries par rapport à des points, des droites, des plans, par les rotations qui les laissent invariants.

La réversibilité des transformations pourra être locale, et être traduite en termes de groupes locaux de transformations, de déplacements. Ces groupes locaux de mouvement pourront éventuellement donner naissance à des groupes globaux. Les groupes de translations et de rotations locales en sont les plus représentants à la fois fondateurs et les plus simples. Ils sont très présents en physique fondamentale.

On pourra suivre les effets des déplacements d'objets par la trace qu'ils laissent dans les espaces au sein desquels ils évoluent, à la manière des traînées de combustion que laissent derrière eux les avions dans le ciel. Ces traces sont des trajectoires, des courbes lorsqu'elles paraissent sans épaisseur, des sortes de tubes multidimensionnels lorsque les épaisseurs sont visibles.

La structure de l'ensemble de ces traces possibles au sein d'un espace est un révélateur de la structure de l'espace lui-même. Les traces partant d'un lieu de l'espace et y retournant possèdent la structure de groupe, car la combinaison de deux traces de cette nature constitue encore une trace du même type. Ces groupes de traces sont appelés les *groupes d'homotopie* de l'espace considéré, et caractérisent ce qu'on appelle sa topologie globale. Parmi eux, le groupe de trajectoires fermées, c'est-à-dire de traces unidimensionnelles qui quittent un point et y reviennent, est appelé le *groupe fondamental* de cet espace.

On peut remplacer chaque trajectoire par une succession de segments attachés les uns aux autres en leurs extrémités et qui forment comme des chaînes. Si les traces sont pluridimensionnelles, les maillons des chaînes, qui chacun ont un poids, deviennent des éléments polyédriques pondérés à plusieurs dimensions. Correspondant aux groupes d'homotopie, les groupes de chaînes pondérées sont appelés des groupes d'*homologie*.

Les translations pouvant être représentées par des symboles numériques, les structures de groupes apparaissent de manière naturelle au sein des ensembles de nombres. L'exploitation des propriétés structurelles des représentation des objets, tant par le numérique que par le géométrique, a permis et permet encore d'enrichir considérablement la connaissance des propriétés de ces objets.

Remarque terminologique:

La symétrie est une gage de stabilité. L'exploitation de la notion de symétrie a joué un rôle considérable dans le développement de la physique. Les physiciens du début du XXe siècle, Pierre Curie notamment (selon son principe, la symétrie présente dans les causes se retrouve dans les effets), ont mis en relief ce rôle. Cette notion a pris davantage d'importance en mathématiques après les travaux qu'Emmy Noether (1882-1935) a consacrés à la physique mathématique. Les succès des physiciens en physique des particules a contribué à faire encore davantage prendre conscience de l'intérêt de la symétrie. Félix Klein (1849-1925), dans sa conférence célèbre (en 1872) sur l'emploi de la théorie des groupes en géométrie et appelée le *programme d'Erlangen*, ignore encore cette importance : se référant à l'arithmétique, il utilise le terme d' « inverse » pour désigner le symétrique d'un élément. On évitera bien sûr cet emploi terminologique premier, loin d'avoir la richesse sémantique du terme « symétrie ».

CHAPITRE II

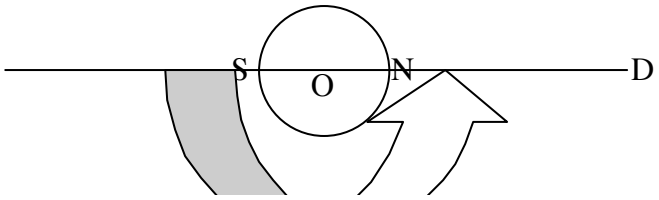
UN PREMIER EXEMPLE DE GROUPE CLASSIQUE : LE GROUPE SINGULIER PRIMORDIAL

2.1 Introduction

Les permutations d'objets furent les premiers sujets d'étude (par Montmort au XVII^{e} siècle) dont le développement, en liaison avec la recherche des solutions d'équations polynomiales et avec la mise en évidence de structures sous l'influence des philosophes et logiciens de l'école anglaise, conduisit au XIX^{e} siècle à fonder la théorie des groupes. Les noms de Lagrange, Galois, Cayley sont attachés à cette création.

Tout objet *se déploie* à partir d'une *singularité primordiale*, caractérisée par une forme d'*extrémalité*, en l'occurrence de minimalité. Dans notre étude, l'objet le plus petit pouvant être muni de la structure de groupe, en dehors bien sûr du groupe quasi fictif réduit à un élément neutre, possède deux éléments. Nous allons donner plusieurs expressions concrètes de ce groupe primordial, que l'on pourra déployer dans diverses directions selon la signification donnée à ses éléments.

Considérons donc Nord et Sud, deux pions dont on peut échanger les places, que l'on peut permuter entre eux (interprétation combinatoire), que l'on peut également représenter par deux points N et S, déterminant la droite D qui les supportent (interprétations géométriques).



2.2 Première interprétation géométrique : comme groupe de rotations

Commençons par l'examen de la situation géométrique, immédiatement visible et compréhensible. On suppose les points N et S placés à distance 1 du milieu O de NS.

Ces deux points forment alors, dans l'espace unidimensionnel D, le cercle $\mathbf{\Sigma}^0 = \{N, S\}$ de rayon unité, une représentation de la sphère topologique $\mathbf{S}^0$ de dimension 0. L'équation cartésienne de ce cercle est simplement :

$$x^2 = 1.$$

Le fait de ne pas échanger les places de N et de S se traduit par une rotation symbolique, la rotation neutre t_n, qui laisse fixes tous les points de la sphère : on la code maintenant par {+1}. Un sens de rotation étant fixé, l'échange des places des deux pions se traduit par une unique autre rotation r : on la code par {-1}. On peut composer ces rotations. L'observation physique de ces compositions conduit à écrire :

$$\{+1\}\{+1\} = \{+1\}$$
$$\{+1\}\{-1\} = \{-1\}$$
$$\{-1\}\{+1\} = \{-1\}$$
$$\{-1\}\{-1\} = \{+1\}$$

Les rotations *dans un sens donné* sur cette sphère forment ainsi un ensemble fini à deux éléments {{+1},{-1}, muni d'une loi de composition associative, pour laquelle {+1} est élément neutre, {-1} est son propre symétrique. On note ce groupe **SO**(1), appelé :

Définition 2.1 : le *groupe des rotations propres du cercle* $\mathbf{\Sigma}^0$.

2.3 Interprétation combinatoire : comme groupe de permutations

Plaçons-nous maintenant du point de vue combinatoire. Soit **E** = {N, S} l'ensemble des pions. Le fait de ne pas les bouger se traduit par une application bijective $t_n : \mathbf{E} \rightarrow \mathbf{E}$ qui est ici l'application identique $t_n(N) = N$, $t_n(S) = S$. Le fait de permuter N et S se traduit par une autre application bijective $\tau : \mathbf{E} \rightarrow \mathbf{E}$ pour laquelle $\tau(N) = S$, $\tau(S) = N$. On a bien sûr les mêmes règles que précédemment en remplaçant {+1} par t_n et {-1} par τ :

$$t_n \; t_n = t_n$$
$$t_n \; \tau = \tau$$
$$\tau \; t_n = \tau$$
$$\tau \; \tau = t_n$$

Ainsi toute permutation entre les éléments d'un ensemble se traduit par une bijection de cet ensemble sur lui-même. Ce groupe des permutations ou des bijections d'un ensemble à deux éléments sur lui-même sera noté ici $\mathbf{\Sigma}_2$ – on ne confondra pas cette notation avec celle $\mathbf{\Sigma}^2$ du « cercle » de rayon 1 dans l'espace tridimensionnel usuel, appelé dans le langage courant une sphère ; l'emploi du terme « sphère », quelle que soit la dimension de celle-ci, est réservé par nous à l'espace topologique qui sous-tend un « cercle », représentation de cette sphère dans un espace métrique par des points équidistants d'un centre.

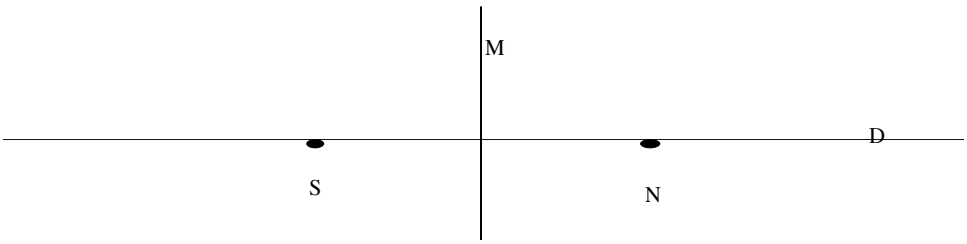
Définition 2.2 : $\mathbf{\Sigma}_2$ est appelé le *second groupe symétrique*, ou groupe symétrique *d'ordre* 2.

La transformation τ qui échange les places des seuls deux pions N et S porte un nom particulier :

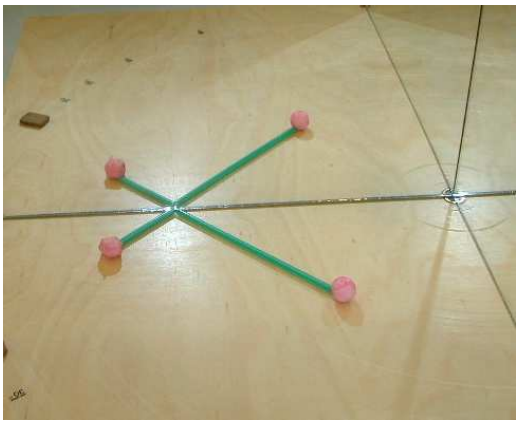
Définition 2.3 : On appelle *transposition* $\tau_{ij,n}$ toute permutation qui échange les places de deux éléments i et j d'un ensemble à n éléments, et laisse invariant les autres éléments.

2.4 Deuxième interprétation géométrique : comme groupe de réflexions

Imaginons que l'on place en O, perpendiculairement à la droite D, un miroir plan M à double face réfléchissante. L'observateur placé dans le demi-plan de droite voit N et son image en S, l'observateur placé dans le demi-plan de gauche voit S et son image N. N et S se correspondent par réflexion naturelle ρ_M sur le miroir M :



$$\rho_M(N) = S,\ \rho_M(S) = N.$$



Conception et Réalisation par Maria DEDÓ (Milano)

L'ensemble à deux éléments $\mathbf{W}_2 = \{t_n, \rho_M\}$ qui vérifie $(\rho_M)^2 = t_n$ est appelé un *groupe de réflexions* ou encore un *groupe de Weyl*.

2.5 Un codage commun pour les trois groupes $\mathbf{SO}(1), \mathbf{\Sigma}_2, \mathbf{W}_2$

Au lieu de la manière multiplicative employée jusqu'à présent, on peut coder ces trois groupes de la même façon additive : en notant par 0 leur élément neutre, par 1 le second élément du groupe, et par le signe + leur loi de composition, on a alors les règles :

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

Ce groupe $(\{0,1\}, +)$ est noté $\mathbf{Z}/2\mathbf{Z}$.

2.6 Importance des groupes de réflexion

2.6.1 La notion d'isométrie

Définition 2.4 : On qualifie de *métrique* (sans référence anthropocentrique), ou bien de *géométrique* (en maintenant cette référence), un espace (topologique) sur lequel est définie une distance entre tout couple de points de cet espace. On note ici par (V, β) un tel espace.

Les déplacements de certains objets dans notre espace usuel s'accomplissent sans déformation : c'est une des gages de leur stabilité locale, d'une certaine pérennité. Les distances entre les points de ces objets sont donc conservées. D'où la fort utile

Définition 2.5 : On appelle *isométrie* entre deux espaces géométriques une bijection qui conserve les distances.

Il en est ainsi en particulier des transformations *à l'intérieur* d'un même espace géométrique (V, β) qui conservent les distances.

Définition 2.6 : On notera par $I(V)$ l'ensemble de ces transformations. Il possède la structure de groupe, est appelé le *groupe d'isométries* de (V, β).

Ces groupes d'isométries sont parmi les plus utiles.

L'importance des groupes de réflexions tient maintenant au résultat suivant que l'on présente ici dans le cadre restreint des espaces euclidiens, avant de l'énoncer plus tard dans le cadre de situations plus générales. Ce résultat est relatif aux isométries euclidiennes. La définition de ces isométries et la démonstration, simple, du théorème seront données dans le prochain paragraphe.

Théorème 2.1 *Les isométries d'un espace vectoriel euclidien* $E = (V, \beta)$ *sont des compositions de translations et de rotations. Si cet espace est de dimension* n*, toute isométrie est le produit de* $n + 1$ *réflexions au plus*.

En voici l'illustration dans le plan usuel, celui de la géométrie euclidienne classique. Selon le théorème, toute isométrie plane est le produit d'au plus 3 réflexions :

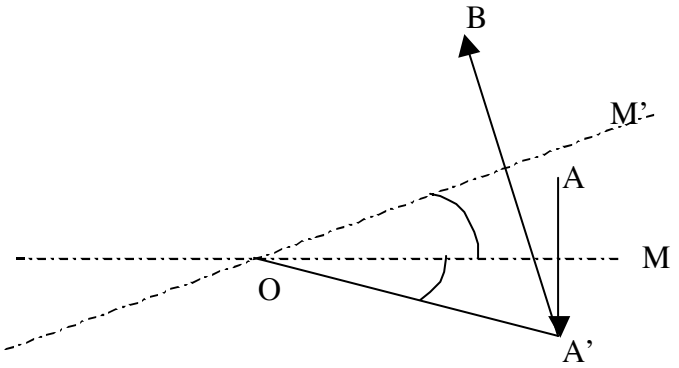
Symétrie simple : *une réflexion*, la symétrie ρ_M par rapport au miroir M :

cf le paragraphe 2.4

Selon l'apparence, le résultat de la composition de deux réflexions diffère selon que les deux miroirs sont concourants à distance finie ou non.

Rotation : *deux réflexions*, la rotation r d'angle 2θ en dimension 2 de centre O :

Soit θ l'angle entre deux miroirs non parallèles M et M', α l'angle entre le miroir M et OA. Soit une orientation du plan. Pour celle-ci, l'angle <(OA, OA') entre OA et OA', A' étant l'image de A par réflexion sur M, vaut - 2α. L'angle entre OA' et OB, B étant l'image par réflexion de A' sur M', vaut 2(α + θ). Par suite l'angle entre OA et OB, <(OA, OA') + <(OA', OB), vaut 2θ.

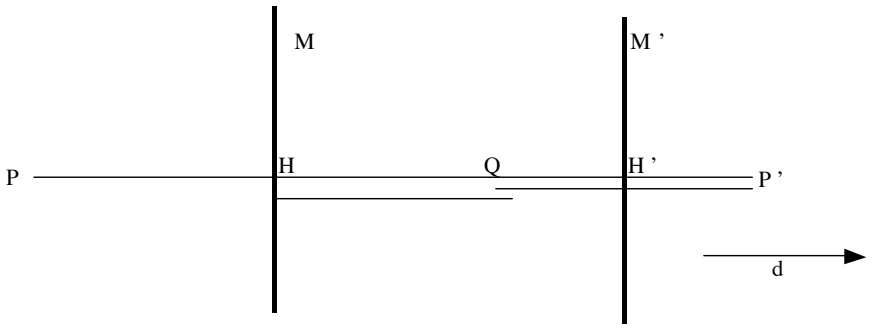


Ainsi :

Proposition 2.2 : *Toute rotation* r *plane de centre* O, *d'angle* 2θ, *est engendrée par la composition de deux réflexions* ρ_M *et* $\rho_{M'}$ *sur deux miroirs quelconques concourants en* O, *et séparés de la distance angulaire* θ.

Ttanslation : *deux réflexions*, la translation t de longueur 2θ en dimension 2 dans la direction d :

Soient, dans le plan usuel, P un point, M et M' deux miroirs parallèles, perpendiculaires à la direction d, et distants de la longueur HH' = θ.



L'image Q de P par réflexion sur le miroir M est telle que PQ = PH + HQ avec, en longueur, PH = HQ.

L'image P' de Q par la réflexion sur M' est telle que QP' = QH' + H'P' avec, en longueur, QH' = H'P'.

Par conséquent, PP' = PH + HQ + QH' + H'P'. Puisque HQ + QH' = HH' = PH + H'P' :

$$PP' = 2\ HH' = 2\theta.$$

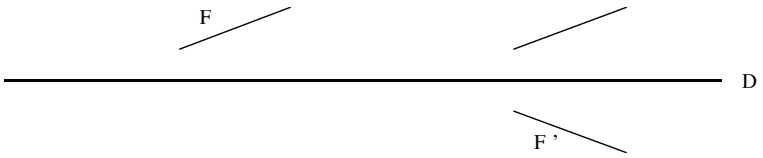
Ainsi :

Proposition 2.3 : *Toute translation plane* t *de longueur* 2θ, *dans la direction* d, *est engendrée par deux réflexions* ρ_M *et* $\rho_{M'}$ *sur deux miroirs parallèles quelconques perpendiculaires à la direction* d, *et séparés de la distance rectiligne* θ.

SG (symétrie glissante) : *trois réflexions*, la symétrie glissante g d'axe D :

La seule composition de trois réflexions qui soit une isométrie est la composition d'une translation $t = \rho_M \circ \rho_{M'}$ et d'une symétrie ρ_D par rapport à un miroir parallèle à la direction d de la translation :

Définition 2.7 : $g = \rho_D \circ t$ est appelée une *symétrie glissante d'axe* D.



2.6.2 Une propriété des groupes d'isométrie

Les groupes d'isométrie sont topologiques dans le sens suivant :

Définition 2.8 : On dit que G = (**T**, *) est un *groupe topologique* si, non seulement G possède la structure de groupe, mais si de plus **T** est un espace topologique (par conséquent entièrement défini par l'organisation du filtre des voisinages de chacun de ses points) pour lequel les applications de multiplication $(t, t') \mid\rightarrow t * t'$ et de symétrie $t \mid\rightarrow t^{-1}$ sont continues.

Définition 2.9 : Un groupe topologique dont tous les points sont ouverts est appelé un *groupe discret*.

C'est le cas, en particulier, des groupes d'isométrie dits *cristallographiques* qui comprennent les groupes de pavage des espaces.

2.7 Expression analytique des isométries euclidiennes et des réflexions naturelles

2.7.1 Le cadre géométrique général et euclidien

Le cadre géométrique dans lequel nous opérons est d'abord celui d'espaces topologiques munis d'une structure d'espace vectoriel. Par référence à la mécanique statique, un espace vectoriel V peut être compris comme un groupe commutatif G de vecteurs forces, sur lequel opère de manière extérieure un *deus ex machina* qui contracte ou dilate *linéairement* les vecteurs. Cette dernière opération est évaluée par l'intermédiaire d'un corps de nombres K, par exemple les réels $\mathbb{R}$ ou les nombres de Chuquet-Cardan $\mathbb{C}$. Si la précision s'avère nécessaire, on écrira V = (G, K).

La plus ancienne des métriques que l'on peut imposer sur un tel espace vectoriel, est celle induite par l'expérience quotidienne à travers le théorème de Pythagore et la mécanique

classique. Dans cette mécanique, le travail, noté u.w, d'une force w le long d'un trajet représenté par un vecteur u est le nombre $u.w = u_1w_1 + u_2w_2 + \ldots + u_nw_n$, où u_i et w_i sont respectivement les composantes du vecteur déplacement u et du vecteur force w présents dans l'espace V, relativement à une base de cet espace.

On voit immédiatement que :

i) $(ku).w = k(u.w) = u.(kw)$
ii) $(u + u').w = u.w + u'.w$, $u.(w + w') = u.w + u.w'$
iii) si quel que soit u, $u.w = 0$, alors w est le vecteur nul
iv) $u.w = w.u$.

On introduit de manière un peu plus générale l'application $\beta : V \times V \rightarrow K$ qui, au couple de vecteurs (u, w), associe $\beta(u, w) = \beta(w, u) = u.w$. Lorsque $\beta(u, w) = 0$, les vecteurs sont dits *orthogonaux*. L'application β, qui vérifient les deux propriétés précédentes i) et ii) est dite *linéaire* en u et en w : elle est appelée un *forme bilinéaire* sur V. La propriété iv) est dite de *non-dégénérescence*. Vérifiant la condition iv), β est dite de plus *symétrique*. Sous ces quatre conditions, β sera alors appelée un *produit scalaire*.

La donnée du produit scalaire β sur V en fait un espace que nous dirons *géométrique*. On le notera alors (V, β).

Le travail $\beta(x, x) = x.x$, également noté $|x|^2$, est le *carré de la longueur* de x. Cette longueur est notée $|x|$.

Lorsque $K = \mathbb{R}$, on montre qu'on peut trouver une base de (V, β) formée de vecteurs orthogonaux deux à deux de sorte que $|x|^2 = x_1^2 + x_2^2 + \ldots + x_r^2 - (x_{r+1}^2 + \ldots + x_n^2)$. Naturellement, on supposera *a priori* que V est rapporté à une telle base.

Si r = n, on dit que l'espace vectoriel (V, β) est *euclidien* ou *pythagoricien*. On notera alors E l'espace (V, β).

Remarquons qu'on peut dans ce cas identifier V à l'espace $\mathbb{R}^n$ rapporté à sa base dite *canonique* formée des n vecteurs $e_i = (0, 0, \ldots, 0, 1_{\text{(en position i)}}, 0, \ldots, 0)$.

Une situation plus générale serait par exemple celle où $|x|^2$ s'écrirait sous la forme :

$$|x|^2 = a_1(x)\, x_1^2 + a_2(x)\, x_2^2 + \ldots + a_n(x)\, x_n^2,$$

les coefficients variables $a_i(x)$ restant disons tous positifs, mais pouvant croître ou décroître de manière uniforme, ou bien varier de manière périodique. Une métrique aussi générale est dite *riemannienne*.

Dans le cas euclidien - doté par conséquent d'une structure métrique uniforme - où nous allons nous placer dans un premier temps, le carré de la distance entre les extrémités U et W des vecteurs u et w est égal à $\beta(w - u, w - u) = (w_1 - u_1)^2 + (w_2 - u_2)^2 + \ldots + (w_n - u_n)^2 = |w - u|^2$

$|w - u| = d(u, w)$ est une *distance* au sens classique du terme : elle est nulle si u et w désignent le même vecteur, indépendante de l'ordre dans lequel on choisit les vecteurs d(u, w)

= d(w, u), positive si w et u sont distincts, vérifie l'inégalité triangulaire d(u, w) ≤ d(u, v) + d(v, w).

2.7.2 L'isométrie dans le cadre euclidien

Puisqu'une isométrie conserve les distances entre tous les couples de points-images, elle transforme tout triangle non dégénéré OBC en un triangle O'B'C', dit *congruent*, qui aura les mêmes longueurs de côté, les mêmes angles, la même aire (2-volume) que le triangle OBC. Un tel triangle OBC est la plus petite figure qui caractérise une surface. Deux de ses côtés suffisent pour le définir.

Ces côtés peuvent être considérés comme deux vecteurs linéairement indépendants formant une base du plan qui contient le triangle. On peut supposer que O est le point représentatif du vecteur origine $\bar{O}$ du plan en tant qu'espace vectoriel.

Une isométrie entre un espace vectoriel de dimension 2 et un autre espace va donc respecter avant tout la structure d'espace vectoriel de la source : l'image sera donc également un espace vectoriel.

De ce fait, l'isométrie est alors entièrement déterminée par la donnée : de l'image O' de l'origine, d'une base de l'espace source et de son image s'appuyant sur O', et de la condition qui exprime l'égalité des longueurs entre les couples de sommets (0-simplexes) ainsi définis.

Ces propriétés de conservation métrique s'étendent aussitôt aux espaces vectoriels de dimension quelconque. Ainsi, une isométrie transformera un tétraèdre (plus généralement un n-simplexe, un polytope) en un autre tétraèdre (un autre n-simplexe, un autre polytope) de même dimension.

Si donc μ est une isométrie, le vecteur nul $\bar{O}$ de E aura *a priori* pour image dans E, le vecteur $\mu(\bar{O}) = \bar{O}'$. On posera $t = \bar{O}\,\bar{O}'$.

Lemme 2.3 : *Soit* $\mu : E \rightarrow E$ *l'application telle* $\mu(w) = t + w = w' : \mu$, *translation de vecteur* t, *est une isométrie*.

<Preuve : Cela résulte de ce que $\beta(w' - u', w' - u') = \beta((w + t) - (u + t), (w + t) - (u + t)) = \beta(w - u, w - u)$.>

Une transformation h de l'espace vectoriel V réel qui respecte sa structure d'espace vectoriel transformera toute droite vectorielle D_u, formée des vecteurs ru où r décrit l'ensemble des réels, en une autre droite vectorielle. h vérifie donc :

i) $h(ru) = r\,h(u)$
ii) $h(u + v) = h(u) + h(v)$

h est alors appelée une *application linéaire*.

Définition 2.10 : Une application linéaire qui conserve les distances sera appelée un *isométrie linéaire*.

Lemme 2.4 : *Une isométrie linéaire* h *est un isomorphisme de* E *sur son image*..

<Preuve : h est bijectif sur son image. Notons d'abord que si u est un vecteur de l'espace source différent du vecteur nul, il a une longueur, et son image u' = h(u) a la même longueur. Si par ailleurs les vecteurs u et v de la source sont distincts et de même longueur, le vecteur u – v n'est pas le vecteur nul, a une longueur non nulle, de même que son image h(u – v) = h(u) – h(v) = u' – v'. Et donc ces vecteurs images sont également distincts. >

Ce lemme montre qu'on peut se restreindre à ne considérer que des applications linéaires entre espaces de même dimension, de considérer en particulier isomorphismes de E isométriques de E sur E. C'est pourquoi, presque ès le début de ce paragraphe, nous nous sommes placés dans ce cadre.

Lemme 2.5 : *Si* h *est une isométrie linéaire de* E *dans* E*, elle vérifie* $\beta(u, w) = u.w = h(u).h(w) = \beta(h(u), h(w))$.

<Preuve : Si h est une isométrie, elle conserve les longueurs par hypothèse, de sorte que, quel que soit u, $\beta(u, u) = u.u = h(u).h(u) = \beta(h(u), h(u))$. Or, par la bilinéarité de β : $\beta(u + w, u + w) = \beta(u, u + w) + \beta(w, u + w) = \beta(u, u) + \beta(w, w) + 2\beta(u, w)$, d'où l'on déduit que :

$$2\beta(u, w) = \beta(u + w, u + w) - \beta(u, u) - \beta(w, w) =$$
$$\beta(h(u + w), h(u + w)) - \beta(h(u), h(u)) - \beta(h(w), h(w)) = 2\beta(h(u), h(w)) >$$

Définition 2.11 : h : E → E, isométrie linéaire, porte alors également le nom de *transformation orthogonale*, terminologie qu'on va justifier.

On suppose E et son image rapportés chacun à leur base canonique. Soit alors $A^{tj} = h(e_j)$ l'image du vecteur de base e_i par h. Le vecteur $u = u_1e_1 + \ldots + u_ne_n$ est alors transformé par h en :

$$h(u) = u' = u_1\, h(e_1) + \ldots + u_n\, h(e_n) = u_1\, A^{t1} + \ldots + u_j\, A^{tj} + \ldots + u_n\, A^{tn}$$

ce qu'on note de manière condensée $h(u) = u^t\, A^t$ où u^t désigne les composantes de u disposées en ligne.

Dans cette dernière notation :

$A^t = (A^{t1}, \ldots, A^{tn})$, $A^{tj} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{ij} \\ \vdots \\ a_{nj} \end{pmatrix}$ désigne l'ensemble des composantes a_{ij} de $h(e_j)$ disposées en colonne, A^t représente la *matrice* de h par rapport aux bases considérées de l'espace source et de son image, c'est-à-dire le tableau des coefficients a_{ij} où a_{ij}, situé au croisement de la i-ème ligne et de la j-ième colonne, désigne comme précédemment la i-ième composante du vecteur A_j.

$u = \begin{pmatrix} u_1 \\ \vdots \\ u_j \\ \vdots \\ u_n \end{pmatrix}$ désigne maintenant, disposées en colonne, les composantes u_i du vecteur u.

. Notons par

$$A_1 = (a_{11} \ldots a_{1j} \ldots a_{1n})$$

la liste des coefficients de la première ligne de A^t, plus généralement par A_i la liste des coefficients de la i-ième ligne de A. Alors la matrice A se présente maintenant sous la forme :

$$A = \begin{pmatrix} A_1 \\ \cdot \\ \cdot \\ A_i \\ \cdot \\ \cdot \\ A_n \end{pmatrix}$$

Avec cette présentation, $A\,u = u' = \begin{pmatrix} A^{1t}.u \\ \cdot \\ \cdot \\ A^{it}.u \\ \cdot \\ \cdot \\ A^{nt}.u \end{pmatrix}$ où, par exemple,

$$A^{1t}.u = (a_{11} \ldots a_{1j} \ldots a_{1n}) \begin{pmatrix} u_1 \\ \cdot \\ u_j \\ \cdot \\ u_n \end{pmatrix} = a_{11}\,u_1 + a_{12}\,u_2 + \ \ldots + a_{1n}\,u_n.$$

On reconnaît ici le produit scalaire des vecteurs u et A^{1t} où les composantes de A^{1t} sont disposés en ligne, au contraire de celles de u ou de A_1 disposées en colonne.

Désormais, w^t désignera la présentation en ligne des composantes de w. On dit que w^t est le *transposé* de w, dont la présentation des composantes est faite en colonne. Dans ces conditions, le produit scalaire $\beta(u, w)$ prend la valeur $u^t w = w^t u$.

Si w' = A w, on vérifie simplement que $w'^t = w^t A^t$, où A^t, la *transposée* de la matrice A, s'obtient en plaçant en ligne i la colonne de A de même indice i.

Si h est une isométrie linéaire, $h(u).h(w) = u.w = u^t w = h(u)^t h(w) = u^t A^t A\, w$, ce qui implique que $A^t A = I$, l'identité. Le coefficient α_{ij} de la matrice produit $A^t A$ s'obtient en faisant le produit scalaire de la ligne i par la colonne j. Ce produit scalaire est ici nul à moins que i = j. C'est pourquoi l'on dit que la matrice A de l'isométrie h, et l'application linéaire h elle-même, sont *orthogonales*.

On vérifie aisément que :

Proposition 2.6 : *Les ensembles* **T**(E) *des translations sur* E *et* **O**(E) *des transformations des transformations orthogonales sur* E *sont structurés en groupe*.

La représentation de chaque transformation orthogonale par une matrice A permet d'identifier le groupe **O**(E) au groupe **O**(n), formé par l'ensemble des matrices de type A avec la multiplication entre matrices comme loi de composition.

Définition 2.12 : **O**(n) est alors appelé le groupe des *rotations* de E.

Le *déterminant* de A, det A, évalue le n-volume algébrique de l'hyper-parallélépipède défini par les n vecteurs colonnes ou lignes de A : det A = det A^t. La relation A^t A = I implique alors que det (A^t A) = 1, et donc que (det A)^2 = 1, ou encore det A = ± 1.

Cette dernière condition conduit à diviser les rotations de E en deux sous-groupes :

Définition 2.13 : Celui des rotations A dites *positives* ou *propres* de déterminant 1, formant le groupe noté **SO**(n), dit *groupe spécial orthogonal*, et celui des rotations A dites *négatives* ou *impropres*, ayant bien sûr le même nombre d'éléments que son « opposé ».

Définition 2.14 : On appellera *isométrie (euclidienne) sur l'espace euclidien* E, l'application $\delta : E \rightarrow E$ définie localement par la relation :

$$\delta(u) = u' = \mu(h(u)) = t + h(u),$$

δ est donc <u>une</u> composée d'une translation μ de vecteur t, et d'une transformation orthogonale h sur E.

Il est bien vrai que $\delta(u)$ est une isométrie puisque $\beta(u' - w', u' - w') = \beta(t + h(u) - t - h(w), t + h(u) - t - h(w))$ = (par linéarité) $\beta(h(u - w), h(u - w)) = \beta(u - w, u - w)$ (puisque h est une isométrie).

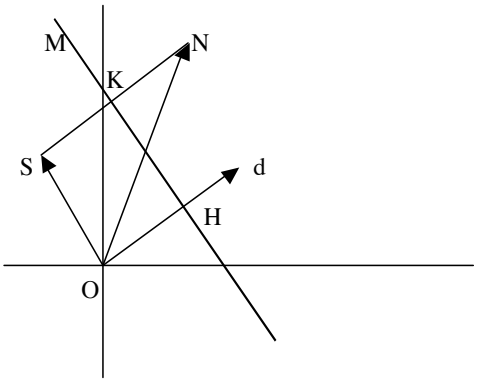
2.7.4 <u>Expression analytique d'une réflexion naturelle dans un espace vectoriel euclidien</u>

Définition 2.15 : Un *miroir naturel plan* M d'un espace euclidien E est un hyperplan affine (sous-espace vectoriel affine de dimension n-1).

v et d étant deux vecteurs faisant entre eux l'angle a, $\beta(v, d) = |\, v \,|\, |\, d \,|$ cos a. En particulier, si v = d, $\beta(d, d) = |\, d \,|\, |\, d \,| = |\, d \,|^2$. On suppose que d est un vecteur unitaire de sorte que $\beta(d, d) = 1$.

Du point de vue analytique, un miroir naturel M(d, h) est défini d'une part par le vecteur unitaire d qui lui est orthogonal, et d'autre part par le vecteur translation OH, où H est la projection orthogonale de O sur M.

On note par h la longueur algébrique de ce vecteur que l'on peut également définir par la projection $\beta(u, d) = u.d = h$ de tout vecteur u de M sur le vecteur unitaire normal au miroir d.



L'image de ON (un vecteur noté v) par la réflexion naturelle ρ_M sur M est le vecteur OS tel que :

$$OS = ON + NS = ON + 2\,NK = ON + 2\,k\,d$$

où k est un scalaire pour lequel le vecteur $ON + NK = v + k\,d$ appartient au miroir M, soit, en termes analytiques, $\beta(v + k\,d, d) = h$. On déduit de là que $k = h - \beta(v, d)$, et que :

$$\rho_M(v) = v + 2\,(h - \beta(v,d))\,d.$$

Si le miroir plan est un sous-espace vectoriel de dimension n-1, h est nul, et $\rho_M(v)$ s'écrit plus simplement :

$$\rho_M(v) = v - 2\,\beta(v,d)\,d\ .$$

Lemme 2.7 : $\rho_M(\rho_M(v)) = v$, *et* ρ_M *est une isométrie linéaire*.

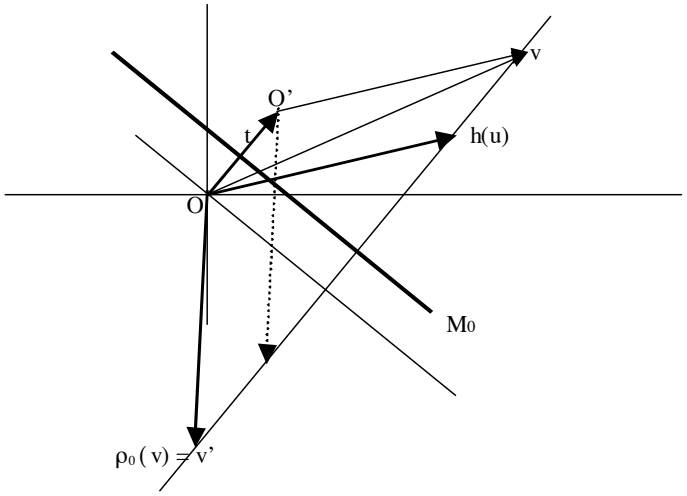
<Preuve : Les vérifications sont faciles. Par exemple, pour la seconde assertion, en supposant $h = 0$ pour alléger le calcul :

1) ρ_M est une isométrie puisque : $\beta(\rho_M(v), \rho_M(v)) = \beta(v - 2\,\beta(v,d)\,d,\ v - 2\,\beta(v,d)\,d) = \beta(v, v) - 2\,\beta(v,d)\,\beta(v, d) - 2\,\beta(v,d)\,\beta(d, v) + 4\beta(v,d) = \beta(v, v))$.
2) ρ_M est une application linéaire car β étant linéaire en v, $\rho_M(v + w) = v + w - 2\,\beta(v + w,d)\,d = (v - 2\,\beta(v,d)\,d) + (w - 2\,\beta(w,d)\,d)$.>

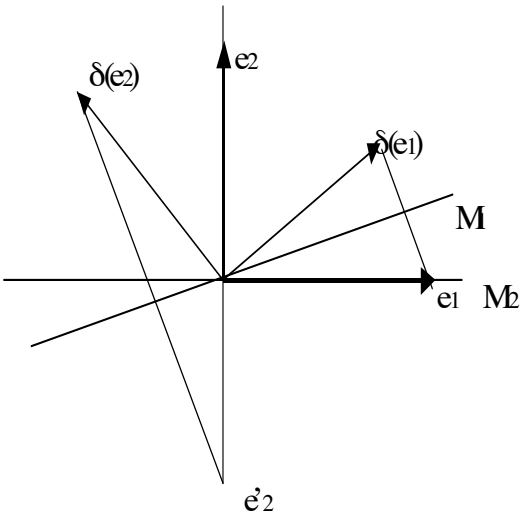
L'expression de $\rho_M(v)$ permet de donner une définition analytique de la réflexion naturelle sur le miroir plan M (d, h).

Définition 2.16 : M(d, h) étant un miroir plan naturel, l'application $\rho_M : E \rightarrow E$ définie par $\rho_M(v) = v + 2\,(h - \beta(v,d))\,d$ sera appelée la *réflexion naturelle* sur M.

<Preuve du théorème 2.1 : Soit $\delta : E \rightarrow E$ une isométrie euclidienne définie localement par $\delta(u) = \mu(h(u)) = t + h(u) = v$. On a $\delta(\bar{O}) = t = \bar{O}\,\bar{O}'$. Soit M_0 l'hyperplan médiateur de $\bar{O}\,\bar{O}'$. $\bar{O}$ s'obtient à partir de $\bar{O}'$ par une réflexion ρ_0 sur M_0 : $\rho_0\,\delta(\bar{O}) = \bar{O}$.



Posons $\rho_0 \delta = \delta_1$, et soit $\delta_1(u) = v'$ le réfléchi de $\delta(u) = v$ par rapport à M_0. Comme la réflexion est une opération linéaire, le réfléchi v' est la somme du réfléchi de t, qui est le vecteur nul, et du réfléchi de h(u) par rapport à M_0.



Par conséquent v' est aussi le réfléchi de h(u) par rapport à l'hyperplan vectoriel parallèle à M_0. Par le lemme précédent 2.5, l'application δ_1 est une isométrie linéaire.

Soit alors la base canonique de E, et $e'_1 = \delta_1(e_1)$. L'hyperplan médiateur de $e'_1 - e_1$, M_1, définit une réflexion ρ_1 de sorte que $\rho_1 \delta_1(e_1) = e_1$. Posons $\delta_2 = \rho_1 \delta_1$.

Considérons maintenant $\delta_2(e_2) = \rho_1 \delta_1(e_2) = e'_2$. Si $e'_2 - e_2$ n'est pas le vecteur nul, l'hyperplan plan médiateur de $e'_2 - e_2$, M_2, définit une réflexion ρ_2 de sorte que $\rho_2 \delta_2(e_2) = e_2 = \rho_2 \rho_1 \delta_1(e_2)$. Remarquons alors que M_2 contient e_1, de sorte que δ_2 laisse ce vecteur invariant : en effet $(e'_2 - e_2).e_1 = e'_2 .e_1 - 0 = \delta_2(e_2).e_1$, et, puisque $\delta_2(e_1) = e_1$, $(e'_2 - e_2).e_1 = \delta_2(e_2).\delta_2(e_1) = e_2 .e_1 = 0$.

Si $e'_2 - e_2$ est le vecteur nul, on prend pour ρ_2 l'identité.

En procédant par récurrence, on construit ainsi n réflexions $\rho_1, \rho_2, \ldots, \rho_n$ et l'isométrie $\rho_n \rho_{n-1} \ldots \rho_1\delta_1$ qui laisse invariants les vecteurs de la base canonique, et par conséquent est l'identité. Par suite $\delta_1 = \rho_1\rho_2 \ldots\rho_n$, et comme $\rho_0 \delta = \delta_1$, $\delta = \rho_0 \rho_1\rho_2 \ldots\rho_n$.>

2.8 Quelques extensions de la notion de réflexion naturelle

La réflexion naturelle fait appel à trois ingrédients principaux :

i) en premier lieu un miroir M,
ii) en second lieu une application ρ, dite *involutive*, telle que $\rho \circ \rho = \rho^2 =$ l'identité,
iii) en troisième lieu, liée à ρ, une relation métrique entre un vecteur et son image.

La généralisation de la réflexion naturelle va passer d'abord par celle de M. Une droite n'est qu'un cercle de rayon infini, de sorte que la première généralisation de M consiste à remplacer l'hyperplan par une (hyper-)sphère, puis par un (super-)hyperboloïde. L'équation dans E d'un tel (super-)hyperboloïde est par exemple :

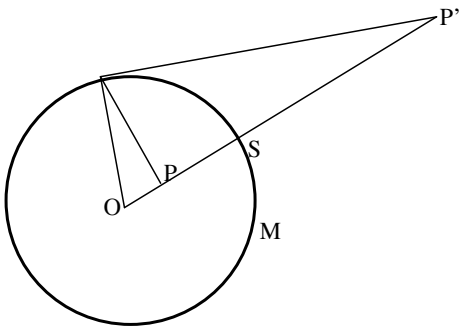
$$x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_n^2 = k > 0.$$

Un tel objet contient comme cas particulier des sphères : il en est ainsi de sa section par le sous-espace des x_j nuls, pour les indices $j \geq r+1$. On passera ensuite à une étape suivante de généralisation en considérant des hyper-surfaces d'abord convexes, puis plus quelconques quoique régulières, etc.

La difficulté est plus grande pour donner des généralisations précises et calculables de la réflexion naturelle ρ adaptées aux choix des miroirs. En considérant, par exemple, la réfraction comme une généralisation de la réflexion naturelle, l'image d'un point P peut ne pas être situé sur la normale au miroir et passant par ce point P.

La difficulté s'accroît encore pour imposer des relations métriques précises et pertinentes entre le vecteur u et son image par ρ.

Du point opérationnel, effectif, bien qu'il ait pris déjà de l'âge, le stade le plus avancé auquel on soit parvenu est celui de la prise en considération de la transformation dite conforme. Reconstruisons rapidement un cheminement qui conduit à établir cette transformation.



On part du cercle, ou plus généralement de la sphère, lieu social des points équidistants d'un centre O ayant un pouvoir singulier. Si S est un point de cette sphère, on considère ici le produit OS.OS de la longueur OS par elle-même, et dont la valeur positive k est indépendante du point S. Ce n'est là qu'un cas particulier d'une situation plus générale où l'on considère deux points P et P' alignés avec O, de sorte que le produit des longueurs OP.OP' reste constant, égal à k. Comme OP' = k/OP, on dit que P et P' sont *inverses* l'un de l'autre dans *une inversion de centre* O et *de puissance* k.

Si S est situé sur la droite support des points O, P et P', OP = OS + SP, OP' = OS + SP' de sorte que $OP.OP' = OS^2 + SP.SP' + OS.(SP + SP')$, d'où l'on déduit, puisque $OS^2 = OP.OP'$, que $SP.SP' + OS.(SP + SP') = 0$. Lorsqu'on éloigne O de sorte que le rayon de la sphère devient infinie, SP et SP' restant finis, il vient, après division par la longueur de OS, SP + SP' = 0 : la sphère est devenue localement un miroir plan, P et P' sont en réflexion naturelle par rapport à ce miroir. La réflexion n'est donc qu'un cas particulier de l'inversion.

v désignant le vecteur OP, son image w = OP' vérifie la relation $w = \frac{k}{\beta(v, v)} v$ de sorte que $\beta(v, w) = k$.

Plus généralement, on pourra considérer un produit scalaire β sur E, O'dans E défini par le vecteur de translation t = OO', et des vecteurs v = t + v', w = t + w'.

Définitions 2.17 :
Première extension : On dira que les vecteurs v = t + v' et w = t + w', ainsi que leurs extrémités respectives P et P', sont *inverses* l'un de l'autre par rapport à O' si $w' = \frac{k}{\beta(v', v')} v'$, où k est la *puissance* de l'inversion. On dira également que P' est le *réfléchi* (ou l'*inverse*) de P par rapport à l'hyper-surface $M_{\beta,k}$ d'équation $\beta(v - t, v - t) = k$, et qu'un point S, situé à l'intersection de $M_{\beta,k}$ la droite vectorielle engendrée par v - t, est un point *associé* à v.

La réflexion ou inversion ρ dans le cas présent s'écrit :

$$w = \rho_M(v) = t + \frac{k}{\beta(v', v')} v' = t + \frac{k}{\beta(v - t, v - t)} (v - t).$$

Deuxième extension : Soit $r_{\theta,S}$ une rotation d'angle θ dépendant d'un point S de $M_{\beta,k}$ associé à v.

Si w est de la forme :

$$w = r_{\theta,S}(t + \frac{k}{\beta(v - t, v - t)} (v - t)) = \rho_{M,\theta}(v)$$

on dira que, par la *réfraction* $\rho_{M,\theta}$, w (respectivement P)'est le *réfracté* de v (respectivement P) d'angle θ par rapport à l'hypersurface $M_{\beta,k}$. D'autres définitions de la réfraction peuvent être adoptées pour se rapprocher davantage de la réalité physique, où SP' est le rayon réfracté.

2.9 Les groupes de la géométrie à deux dimensions

Les espaces standard à deux dimensions sont par définition des surfaces, le plan, la sphère et ses déformations en ellipsoïdes, les paraboloïdes, les hyperboloïdes. Toutes ces surfaces peuvent analytiquement définies par des équations du second degré.

L'espace à deux dimensions le plus simple est le plan euclidien usuel, celui muni de la métrique de Pythagore. Plongé dans l'espace usuel à trois dimensions, il a pour équation analytique générale :

$$(ax + by + cz - d)^2 = 0.$$

Ellipsoïdes et hyperboloïdes ont pour équation analytique des expressions de la forme :

$$ax^2 + by^2 + cz^2 - d = 0$$

On peut étudier la géométrie de tous ces espaces soit directement, soit par l'intermédiaire de l'une de leur *représentations* bien choisie sur des espaces plans, munis alors d'une métrique adaptée.

Cette représentation est l'*ombre* que fait cet espace éclairé par une source extérieure sur un écran. C'est à nouveau dire ici le rôle de la lumière et de la théorie géométrico-physique de cette lumière dans la conception et la mise sur pied de toute la théorie mathématique, qui « n'est qu' » une physique abstraite. La lumière n'était-elle pas présente au moment où l'on a envisagé et utilisé le phénomène de la réflexion ?

La source lumineuse peut être ou non située à l'infini. On la placera souvent en un *point singulier* de la surface, en un pôle dit nord ou en un pôle dit sud. On dira alors que *l'ombre est une projection stéréographique de la surface*.

Les symétries internes présentes au sein des surfaces font que par des réflexions conduisant à des rotations, certaines propriétés restent invariantes, comme en particulier la conservation des angles. Reproduites sur le plan de représentation, ces transformations forment un groupe, appelé

Définition 2.18 : le *groupe des homographies ou encore des transformations linéaires fractionnaires*.

Vérifions immédiatement que leur ensemble a bien la structure de groupe.

Si z est un élément de **R** ou de **C**, l'expression analytique d'une telle transformation est de la forme :

$$z' = h(z) = \frac{az + b}{cz + d}.$$

Comme les transformations des points sur la surface aboutit à des points en général distincts, il est nécessaire que a/ b soit différent de c/d (sinon h(z) = b/d quel que soit z).

Sous cette condition supposée vérifiée pour toute homographie, leur ensemble contient la transformation identique qui joue le rôle d'élément neutre (a = 1, b =c = d = 0). La composée de h (a, b, c ,d) et de $\eta(\alpha, \beta, \gamma, \delta)$ est encore une homographie puisque :

$$\eta h\,(z) = \frac{\alpha\dfrac{az + b}{cz + d} + \beta}{\gamma\dfrac{az + b}{cz + d} + \delta} = \frac{(\alpha a + \beta c)z + \alpha b + \beta d}{(\gamma a + \delta c)z + \gamma b + \delta d}.$$

On vérifie également sans peine l'associativité.

Si z' est donné par l'expression précédente, alors cz'z + z'd = az + b, soit z(cz' – a) = b – z'd, et

$$z = \frac{dz'-b}{a-cz'} = h^{-1}(z).$$

Ces expressions sont valides pour le couple z = -d/c, z' = ∞.

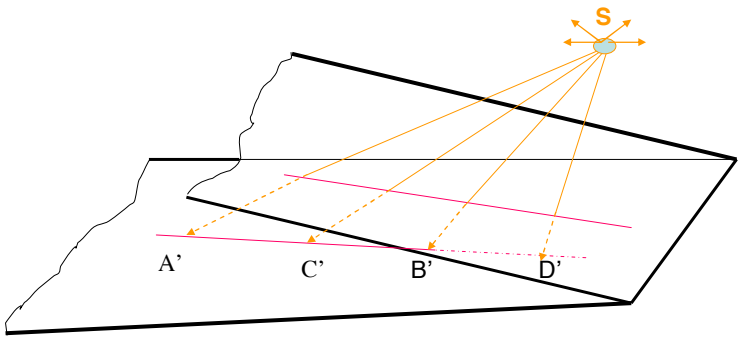
Selon les propriétés des coefficients de ces transformation, et donc selon leur signification géométrique, le groupe qu'elles forment porte des noms différents. Nous allons les découvrir maintenant.

Les groupes de la géométrie projective

Le cas d'une variable réelle

Soit S une source lumineuse dans l'espace usuel, P une plan dans cet espace et E_2 un plan euclidien de représentation.

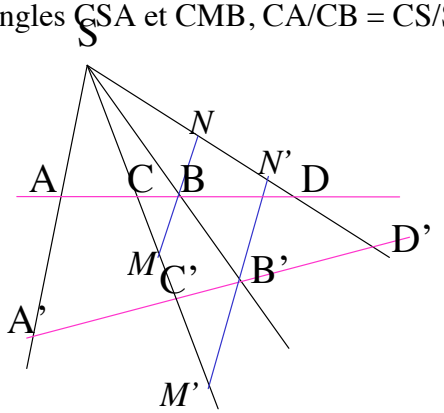
L'Invariant caractéristique de la Géométrie projective



Le double rapport ou birapport (cross ratio) est conservé par la projection lumineuse

[CA/CB]/[DA/DB] = [C'A'/C'B']/[D'A'/D'B']

Par le faisceau lumineux issu de la source S, la droite D_P, représentée par l'ensemble des nombres réels auxquels on a ajouté un point (d'Alexandrov) noté ∞, est projetée en la droite D_P' dans E_2. Dans le plan formé par S et D_P, on a la configuration suivante :



les droites MN et M'N' étant parallèles à la droite SAA', il vient, de par la similitude des triangles CSA et CMB, CA/CB = CS/SM = SA/MB. De par la similitude des triangles DBN et DAS, il vient : DA/DB = SA/NB. Par conséquent [CA/CB]/[DA/DB] = [SA/MB]/[SA/NB] = NB/MB. On établit de la même façon l'égalité analogue :
[C'A'/C'B']/[D'A'/D'B'] = [SA'/M'B']/[SA'/N'B'] = N'B'/M'B'.

Mais de par la similitude des triangles SMB et SM'B', SNB et SN'B', les rapports NB/MB et

N'B'/M'B' sont égaux. On obtient alors l'égalité des *birapports* :

$$[CA/CB]/[DA/DB] = [C'A'/C'B']/[D'A'/D'B'].$$

Ce birapport est indépendant par construction de la droite D' qu'on peut se donner a priori. Ainsi la géométrie projective euclidienne sur un espace à une dimension conserve les birapports. Il s'agit là de la propriété caractéristique de cette géométrie. L'euclidienne standard est simplement caractérisée par le fait que la source S se trouve à l'infini : ce sont alors les égalités du théorème de Thalès standard qui entrent en jeu.

Notons que la valeur du birapport peut s'obtenir à partir du calcul des aires des triangles (évaluées par des expressions de la forme ½ AB . AC sin BAC).

L'expression analytique du birapport est simple. Il s'écrit, x désignant la position de C, a, celle de A, b celle de B, d celle de D :

$$\frac{(x-a)/(x-b)}{(d-a)/(d-c)} = k\frac{x-a}{x-b}$$

Or de manière générale, la relation z' = h(z) = $\frac{az+b}{cz+d}$ s'écrit aussi :

$$z' = \frac{\frac{a}{c}(cz+d-d+\frac{bc}{a})}{cz+d} = \frac{a}{c} + \frac{bc-ad}{c(cz+d)}.$$

de sorte que $$k\frac{x-a}{x-b} = k(1+\frac{b-a}{x-b}).$$

On a une expression analogue dans laquelle toutes les lettres précédentes sont modifiées par l'ajout du symbole « ' ». L'égalité des deux expressions fait que :

$$\frac{1}{x'-b'} = p + \frac{q}{x-b},$$

d'où l'on déduit que :

$$x' = h(x) = \frac{\alpha x+\beta}{\gamma z+\delta}.$$

Définition 2.18 : Une transformation de type h est appelée une *homographie* ou encore, notamment par les anglo-saxons, une *transformation linéaire fractionnaire*.

Vérifions immédiatement que l'ensemble de ces transformations a bien la structure de groupe.

Si z est un élément de $D_P = \mathbf{R}\cup\infty$, l'expression analytique d'une telle transformation est de la forme :

$$z' = h(z) = \frac{az + b}{cz + d}.$$

Comme les transformations des points sur la droite aboutissent à des points en général distincts, il est nécessaire que a/ b soit différent de c/d (sinon h(z) = b/d quel que soit z) : on peut également traduire ce fait par la relation $ad - bc \neq 0$. Sous cette condition supposée vérifiée pour toute homographie :

.

n) leur ensemble contient la transformation identique qui joue le rôle d'élément neutre (a = 1, b =c = d = 0).

c) la composée de h (a, b, c ,d) et de $\eta(\alpha, \beta, \gamma, \delta)$ est encore une homographie puisque :

$$\eta h\,(z) = \frac{\alpha\dfrac{az + b}{cz + d} + \beta}{\gamma\dfrac{az + b}{cz + d} + \delta} = \frac{(\alpha a + \beta c)z + \alpha b + \beta d}{(\gamma a + \delta c)z + \gamma b + \delta d}.$$

a) On vérifie également sans peine l'associativité.

s) Si z' est donné par l'expression précédente, alors cz'z + z'd = az + b, soit z(cz' – a) = b – z'd, et

$$z = \frac{dz' - b}{a - cz'} = h^{-1}(z).$$

Ces expressions sont valides pour le couple z = -d/c, z' = ∞.

Cet ensemble des homographies est donc bien muni de la structure de groupe.

Définition 2.19 : Ce groupe des homographies sur la droite projective réelle D_P est appelé le *groupe des transformations projectives de la droite réelle*, PGL(1, **R**).

On donne souvent à la « droite » $D_P = \mathbf{R}\cup\infty$ et à ses éléments une autre signification : le nombre z représente dans cette interprétation la pente d'une droite vectorielle du plan E_2, de sorte que la droite projective est une représentation de l'ensemble des droites vectorielles de E_2. Etablissons que E_2 la relation d'équivalence suivante : deux vecteurs v et v' sont équivalents ssi ils appartiennent à la même droite vectorielle. Cette droite vectorielle est donc la classe d'équivalence d'un vecteur quelconque qui lui appartient, et qui peut être choisi comme représentant de cette classe, de cette droite. La droite projective quant à elle est l'ensemble de ces classes d'équivalence.

Si on choisit comme représentant le vecteur de longueur 1 qui fait un angle positif avec une droite vectorielle de référence, on obtient pour *autre représentation* de la droite projective le cercle de E_2 de rayon unité.

Exercice : On se donne le cercle, une tangente à ce cercle, le point S du cercle diamétralement opposé au point de contact de la tangente avec le cercle. On joint S à quatre points A, B, C, D de cette droite, ce qui permet d'établir un birapport. En utilisant l'inversion de centre S et de puissance le carré du rayon du cercle, montrer qu'on peut établir un birapport équivalent pour les quatre points situés aux intersections A', B', C', D' du cercle et des quatre droites issues de S. (Ces quatre derniers points sont appelés les projections stéréographiques des quatre premiers).

Généralisation

Les nombres réels forment un ensemble qui a la structure de groupe commutatif pour l'addition, de groupe pour la multiplication à condition de ne pas tenir compte du zéro, élément neutre de l'addition, cette multiplication étant distributive par rapport à l'addition. On dit **R** forme un corps.

Prenons un espace vectoriel réel et géométrique à deux dimensions engendré par les vecteurs unitaires supposés orthogonaux e_1 et e_2. On note i la rotation qui transforme e_1 en e_2, et on écrit $e_2 = i\, e_1$. Alors tout vecteur v de cet espace s'écrit :

$$v = x\, e_1 + y\, e_2 = x\, e_1 + y\, i\, e_1 = (x + i\, y)\, e_1.$$

On remarque que $i\, e_2 = i^2\, e_1 = -\, e_1$, ce qui conduit à poser $i^2 = -1$.

Définition 2.20 : $z = x + iy$ est appelé un *nombre de Chuquet-Cardan de dimension 2* ou encore un *nombre complexe*. (Trouvez-vous que vraiment il s'agit là de quelque chose de complexe ?)

On vérifie aisément que cet ensemble **C** de nombres possède également la structure de corps. On peut également introduire sur l'ensemble des vecteurs d'un espace vectoriel une multiplication de sorte que l'ensemble de ces vecteurs est également muni d'une structure de corps. On peut aussi généraliser à la Elie Cartan la définition précédente des nombres de Chuquet-Cardan et obtenir des corps.

Soit donc **K** un corps d'éléments z. On introduit sur ce corps les transformations homographiques h pour lesquelles ad – bc est différent de 0 :

$$z' = h(z) = \frac{az + b}{cz + d}.$$

On notera PG(1, **K**) le groupe de ces transformations. Lorsque **K** = **C**, ce groupe contient toutes les transformations importantes de la géométrie du plan standard.

Letters to the Editor

Review Journal for Older Books

I propose establishing a mathematical book review journal that only reviews books written more than fifty years ago.

Let me illustrate why by means of an example. Weinstock (*Am. J. Phys.* **50**(7), July 1982) claimed that an "examination of Newton's *Principia* reveals a fallacy in its purported proof of the ... fact that an inverse-square central force acting on a particle requires that the particle move in a conic-section orbit," and that "the body of Newton scholars ... missed the fallacy for nearly three centuries." In fact, Weinstock says that he "detected not even a timid tweet from any whistle blown to call attention to the actual *fallacy* embodied in the *Principia ... not since Johann* Bernoulli's in 1710." Apparently, Weinstock did not read the classical German literature, where the "mistake" was clearly recognised and understood again and again (e.g., Suter, *Geschichte der mathematischen Wissenschaften*, vol. 2, p. 164; Fleckenstein, "Johann I Bernoulli als Kritiker der 'Principia' Newtons," *Elemente der Mathematik* **1**, 1946, p. 101).

In my view, this episode is symptomatic of two modern evils. First, we as a community encourage disrespect for classical knowledge. I once overheard a graduate student express dissatisfaction that a Galois theory course worked over the complex number since "one never uses $\mathbb{C}$ anyway." We made these people. We could show our students how complex numbers were the heart and soul of virtually all algebra, geometry, and analysis throughout the 19th century. But we don't. We hurry them into research and this is what we get. Second, "everybody writes and nobody reads" (Erdős attributes this saying to Fejér; *Coll. Math. J.* **12**(4), 1981).

My proposed book review journal would strive to cure both these ills by reverting Weinstock's analysis that a modern scholar "has more interesting, more urgent, more rewarding ways to spend time and energy than to hack away painfully through the turgid exposition of a classic treatise" and that "that sort of effort is accordingly consigned to a future that never arrives" to say that there is nothing more interesting, more urgent, more rewarding than to study a classic treatise and that that sort of effort was carried out in a past that is now long gone.

—*Vicktor Blåsjö*
Marlboro College
blasjo@marlboro.edu

(Received May 13, 2007)

Complex History

Complex numbers and linear fractional mappings are of frequent use. Most students are familiar with these notions; they are usually taught with a few historical references. From that last point of view, the following facts may be of some interest.

1) Linear fractional maps are sometimes called Möbius maps and "homographies" by the French mathematicians. In fact, Euler introduced this mapping in his paper "De projectione geographica superficiei sphaericae"; it appeared in the *Acta academiae scientiarum Petropolitanae*, 1777 : I, 1778, pp. 133–142 (vol. 28, Series prima, p. 286). He wrote:

> For that reason, to the function $\Delta(z)$, let us give such a general form
>
> $$\frac{a+bz}{c+dz};$$
>
> (Hanc ob causam functioni $\Delta : z$ talem formam generalem tribuamus)
>
> $$\frac{a+bz}{c+dz};$$

It is a trivial but pleasant remark that since Euler the notation has not been changed. Euler adds all at once:

> [b]ut for z let us take the last form given above, which was $z = \text{tang } \frac{1}{2}v(\cos t \pm \sqrt{-1}\sin t)$
>
> (at vero pro z sumamus formam postremam supra expositam, qua erat $z = \text{tang } \frac{1}{2}v(\cos t \pm \sqrt{-1}\sin t)$).

Almost in the beginning of his article, Euler uses the following terms:

> This point in the plane must be so determined by two orthogonal coordinates x and y, so that... $x = \Delta(\text{tang } \frac{1}{2}v(\cos t + \sqrt{-1}\sin t)) + \Delta(\text{tang } \frac{1}{2}v(\cos t - \sqrt{-1}\sin t))$, $y\sqrt{-1} = \Delta(\text{tang } \frac{1}{2}v(\cos t + \sqrt{-1}\sin t)) - \Delta(\text{tang } \frac{1}{2}v(\cos t - \sqrt{-1}\sin t))$, where it is manifest that if the undefined letter of the function Δ were omitted, [these formulae] would give the construction of the hemisphere either boreal or austral.
>
> (id punctum in plano per binas coordinates orthogobales x et y ita determinari debeat, ut sit...)

2) At the end of the seventeenth century, a polynomial was said to be a "complex quantity" ("une quantité complexe" in Bossut's treatise of Algebra). So has been understood the polynomial $ax + by$ where $a = 1, b = \sqrt{-1}$. (Recall that the term imaginary, introduced by Descartes in his *Geometry* (1637) (from the fact that for instance the intersection of a line with a circle might not be visible at all), is not at all convenient for naming $\sqrt{-1}$.) In fact the first person who introduced an example of such a number was the physician Nicolas Chuquet in 1484. I bet that his paper fell into the hands of another physician, Gerolimo Cardano: he uses exactly the same words as Chuquet to describe these "impossible numbers". That is why I use the terminology "Chuquet-Cardan numbers" instead of "complex numbers":

I don't [want to] put in the mind that these numbers are awfully complex and dangerous entities.

—Claude P. Bruter
University of Paris
bruter@univ-paris12.fr

(Received May 18, 2007)

Reed Ends Arms Fair Business

A recent article by Allyn Jackson ["Jumping Ship: 'Topology' Board Resigns", May 2007] made reference to a campaign that I've been helping to coordinate. The aim of the campaign was to force Reed Elsevier to stop organising arms fairs. The method of the campaign was to galvanise scientific, academic, and medical opinion against Reed's involvement in this business.

On 1 June, Reed announced that they would withdraw from the "defence industry" during the second half of 2007. The reason that they gave was as follows:

"[I]t has become increasingly clear that growing numbers of important customers and authors have very real concerns about our involvement in the defence exhibitions business. We have listened closely to these concerns and this has led us to conclude that the defence shows are no longer compatible with Reed Elsevier's position as a leading publisher of scientific, medical, legal, and business content."

A substantial number of prominent mathematicians, including Sir Michael Atiyah, participated in the campaign, which included a publishing boycott, an on-line petition, and a number of high-profile open letters from different groups.

Reed's arms fair business turned over more than 20 million pounds last year. Despite this, the pressure that has been brought to bear by the scientific, academic, and medical communities has proved more than Reed could bear.

—Nick Gill
Institute for Mathematical Sciences, Chennai, India
nickgill@cantab.net

(Received June 7, 2007)

Establish a Photo Archive

It seems that the AMS has been passing up an opportunity to build a valuable historical archive of photographs. I discovered this during the past few months when looking for official sources of photographs of distinguished women in mathematics—the AMS did not own a single photograph of any of the 25 women of interest to me. I was stunned, as I thought surely the AMS would at least have been taking photographs at the meetings it sponsors—if you take the photograph, you have the copyright to it. What could be simpler? Surely mathematics departments would be happy to donate hi-res scans of the photographs of their distinguished members, etc. The physicists, on the other hand, have a magnificient collection at the Segre Visual Archives of the Niels Bohr Library and Archives, which is a part of the American Institute of Physics. They say the library and archives also acquire materials that can best be preserved at the American Institute of Physics, including photographs, oral histories, books, AIP and member society archives, etc. Perhaps there is a good reason that the AMS does not maintain an archive, but I do not see it.

—Stanley Burris
University of Waterloo
snburris@rogers.com

(Received June 8, 2007)

Correction

Jonathan Sondow (Letters to the Editor, May 2007, page 590) was misidentified. He is an alumnus, not an employee, of Princeton University.

—Andy Magid

CHAPITRE III

PREMIERES GENERALISATIONS : GROUPES CYCLIQUES ET SOUS-GROUPES

3.1 Première extension géométrique : les groupes cycliques

3.1.1 Notions de groupe monogène, de groupe cyclique

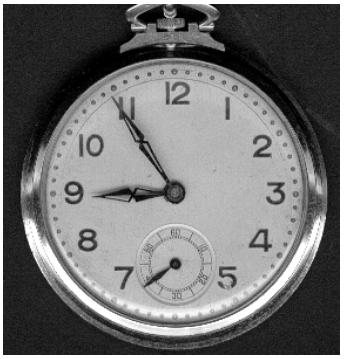
Nous allons maintenant entreprendre de déployer l'exemple primordial, en considérant un ensemble de **E** de m pions, appelés respectivement 1, 2, …, m. Ce déploiement se fera sous les deux angles, géométrique et combinatoire. Ce paragraphe est consacré à une première extension géométrique.

Observons d'abord que, dans le paragraphe précédent, nous avons donné trois noms différents à un même groupe intrinsèque, selon la sémantique que nous lui avons accordée, le codage que nous avons établi. Ce groupe possède deux éléments, ce qui conduit à cette première définition :

Définition 3.1 : On appelle *ordre d'un groupe* le nombre d'éléments qu'il contient : o(G) = card G. Le groupe est évidemment *fini* lorsque son cardinal est fini.

Par composition de {-1} (ou de σ) avec lui-même, on obtient tous les autres (dans le cas singulier présent l'autre) éléments du groupe. D'où la définition :

Définition 3.2 : Un groupe G = (**T**, *) est dit *monogène* s'il contient un élément g, appelé un *générateur*, à partir duquel, par composition répétée de cet élément avec lui-même, on obtient tous les autres éléments du groupe.



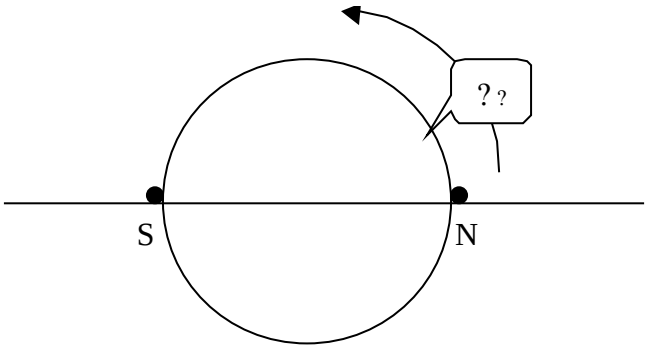
Voici une particularité des groupes monogènes :

Proposition 3.1. *Tout groupe monogène* G = (**T**, *) *est commutatif.*

<**Preuve** : Notons multiplicativement la loi de composition du groupe. Soient t_p et t_q deux éléments de **T**. Puisqu'ils sont engendrés par g, il existe deux entiers naturels p et q tels que t_m

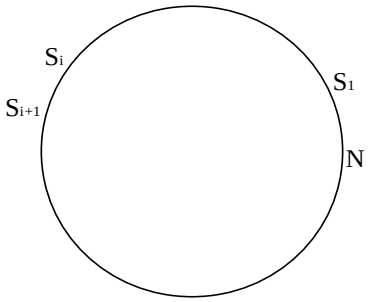
$= g^p$, $t_q = g^q$. Le composé $t_p\ t_q = g^p\ g^q = g^{p+q}$ est aussi un élément du groupe. Comme p + q = q + p, il s'écrit aussi $t_q\ t_p$, la loi de composition est commutative.>

Nous pouvons plonger le cercle de dimension 0, $\mathbf{\Sigma}^0$, dans le cercle de dimension 1, $\mathbf{\Sigma}^1$ (le cercle habituel dans le plan). Le passage de N à S s'accomplit alors par une rotation de 180° dans le plan.



On considérera ce passage de N à S comme une *translation* (*angulaire*) dans l'espace *fermé* formé par le *cercle* $\mathbf{\Sigma}^1$. C'est la raison pour laquelle le groupe symétrique d'ordre 2, $\mathbf{\Sigma}_2$, porte également le nom de *groupe cyclique* d'ordre 2, noté alors $\mathbf{C}_2$.

Dans cette représentation, le cercle a été divisé en deux parts égales. Nous pouvons plus généralement le diviser en n parts égales, et, un sens de parcours ayant été fixé, marquer les points successifs N, S_1, S_2, … , S_{m-1} de cette division sur le cercle.



Le passage de N à S_1, de S_i à S_{i+1}, s'accomplit par une rotation r d'angle $2\pi/m$. Si l'on imagine que N est un cavalier, r(N) est son transport en S_1, $r(r(N)) = r^2(N)$ est son transport en S_2, etc, $r^m(N) = N = t_n(N)$.

Autrement dit, les m-1 rotations : $r_1 = r$, $r_2 = r^2$, …, $r_{m-1} = r^{m-1}$, qui se composent entre elles, sont telles que :

$$r^m = t_n$$

de sorte que, si p + q = m :

$$r^p r^q = t_n$$

ce qui signifie que l'on peut considérer r^p comme le symétrique de r^q.

Ainsi, l'ensemble $\mathbf{T}_m = \{t_n, r, r_2, \ldots, r_k, \ldots, r_{m-1}\}$ des rotations d'angle constant, muni de la loi de composition des rotations, possède la structure de groupe monogène. Il est d'ordre fini m.

Définition 3.3 : Un groupe monogène d'ordre fini m est appelé un *groupe cyclique.* Il est noté $\mathbf{C}_{m.}$ Entièrement défini par la donnée d'un générateur tel que r, et la valeur de m, l'écriture :

$$\mathbf{C}_m = <r, r^m = t_n>$$

s'appelle une *présentation* de $\mathbf{C}_m$. m est également appelé la *période* du groupe cyclique.

3.1.2 Codages d'un groupe cyclique

Les groupes cycliques admettent deux codages principaux que nous qualifierons ainsi : *rotationel* ou *multiplicatif* pour le premier, *horaire* ou *additif* pour le second.

Le codage rotationel ou multiplicatif est celui que nous avons utilisé dans le paragraphe précédent : dans ce codage, $r_k = r^k$.

Dans le codage horaire ou additif, l'élément neutre est représenté par 0, r_k par k, de sorte $\mathbf{T}_m$ est codé par {0, 1, 2 , …, m – 1}. La multiplication précédent devient une addition (à $r(r) = r^2$ correspond 1 + 1 = 2), avec la règle m – 1 + 1 = 0. On note souvent par **Z**/m**Z** un groupe cyclique ainsi codé additivement.

Remarque : Les éléments des groupes étant vus comme des transformations, on pensera souvent à les visualiser en en pensant à la position de l'objet qu'elles transforment. Ainsi, si r est une rotation, on pensera à r(N) par exemple. On comprendra mieux alors la signification d'une égalité telle que

$$r^k = r^p .$$

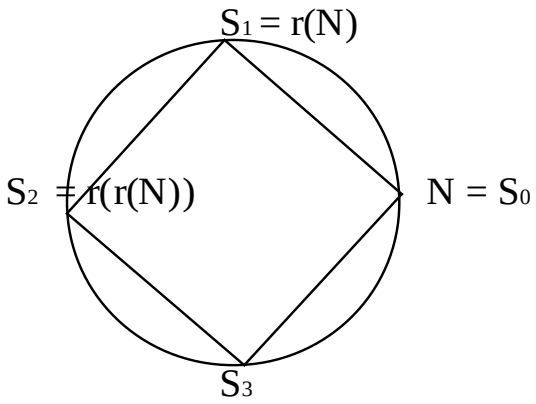
Elle signifie en fait que $r^k(N) = r^p(N)$: les deux rotations transportent dans la même position finale un objet situé en position initiale N.

3.1.3 Structure interne d'un groupe : la notion de sous-groupe

L'examen d'un exemple va nous permettre d'aborder l'étude de la structure interne de ces groupes, parmi les plus élémentaires.

Exemple : L'examen du cas où m = 3 ne révèle rien de nouveau. Supposons par contre m = 4, et posons $r = r_{90}$. Alors :

$$r_2 = r^2 = r_{180}, \quad r_3 = r^3 = r_{270} \quad r^4 = (r_2)^2 = r_{360} = t_n.$$



Voici une première remarque. Ce groupe $\mathbf{C}_4$ contient le sous-ensemble $H = \{t_n, r_2\}$ contenant r_2 qui échange la place de N et de son symétrique sur le cercle. On peut donc munir H de la structure de groupe pour la même loi de composition que $\mathbf{C}_4$, et l'identifier au groupe primordial. Ainsi, pour la même loi de composition, un groupe peut contenir des parties elles-mêmes structurées en groupe. D'où la

Définition 3.4 : Soit G un groupe. Une partie H de G est un *sous-groupe* de G si H a une structure de groupe pour la loi de composition définie sur G. Cela implique que G et H ont même élément neutre. G et $\mathbf{1} = \{t_n\}$ sont appelés les *sous-groupes triviaux* de G.

Connaître un groupe est alors connaître en particulier la manière dont il se structure en sous-groupes, et les propriétés de ces sous-groupes.

Nous emploierons divers procédés pour atteindre ce but. Ils proviennent de l'observation des groupes élémentaires, de la mise en valeur de leurs propriétés que l'on généralise sous forme d'énoncés, énoncés que l'on démontre ensuite.

Ainsi, l'examen du groupe $\mathbf{C}_4$ précédent et d'autres groupes de la même nature conduit tout naturellement à ce premier énoncé.

Proposition 3.2. *Soit* G *un groupe quelconque contenant un élément* g *tel que* $g^m = t_n$. *On suppose qu'il n'existe pas* $p < m$ *tel que* $g^p = t_n$ *Alors le groupe cyclique d'ordre* m, $\mathbf{C}_{g,m}$ *engendré par* g, *est un sous-groupe de* G. *Il contient toutes les puissances de* g.

<**Preuve** : G contient g et donc l'ensemble H de tous les composés de g avec lui-même, de la forme g^s. En particulier H contient ceux d'entre eux pour lesquels $s \leq m$: ils forment un ensemble $\mathbf{C}_{g,m}$. $\mathbf{C}_{g,m}$ contient l'élément neutre par hypothèse. Si $s + r = m$:

$$g^{s+r} = g^s g^r = t_n,$$

de sorte que tout élément de la forme g^s ($s \leq m$) admet un symétrique unique. $\mathbf{C}_{g,m}$ a la structure de groupe cyclique.

Supposons maintenant s quelconque. Posons $s = km + r$ où $r < m$ est le reste de la division euclidienne de s par m. Alors $g^s = g^{km + r} = g^{km} g^r = t_n g^r = g^r$ appartient à $\mathbf{C}_{g,m}$, et par conséquent $H = \mathbf{C}_{g,m}$.>

Théorème 3.3. *Tout sous-groupe* H *d'un groupe cyclique engendré par un élément* g *est cyclique.* H *est engendré par* g^k*, où* k *est le plus petit entier tel que* g^k *appartienne à* H.

<**Preuve** : Soit H un sous-groupe d'un groupe cyclique **C**, engendré par g. Si H est un sous-groupe trivial, le théorème est évident. Sinon il contient des éléments de **C**. Soit k le plus petit entier tels que g^k appartienne à H. H contient notamment toutes les puissances de g^k, elles sont de la forme g^{qk}. Si k = 1, H = **C**. k étant différent de 1, soit s un entier tel que g^s appartienne à H. On peut poser s = qk + r où r < k, de sorte que $g^s = g^{qk}\, g^r$: la composition de deux éléments de H étant encore un élément de H, il en résulte que g^r, égal au produit à gauche du symétrique de g^{qk} par g^s, est également un élément de H. Mais cette donnée est incompatible avec le fait que k est le plus petit entier tel que g^k appartienne à H. Donc r est nul, et H ne contient que des puissances de g^k, qui est le générateur de H.>

Considérons maintenant le cas de $\mathbf{C}_3$: engendré par la rotation r d'angle 2π/3, il a pour éléments r, r^2, t_n. Mais on peut aussi engendrer ce groupe par un autre élément, r^2 : on a en effet les égalités : $r = (r^2)^2$, r^2, $t_n = (r^2)^3 = r^6$. Dans ce cas donc, $\mathbf{C}_3$ a deux générateurs, r et r^2, et l'on remarque ce nombre 2 est celui du nombre d'entiers inférieurs à 3, l'ordre du groupe, et premiers avec 3.

Considérons maintenant le cas de $\mathbf{C}_6$ pour lequel nous allons utiliser le codage additif. Ses éléments forment l'ensemble {0, 1, 2, 3, 4, 5} : 1 est un générateur puisque par additions successives de 1 on reconstitue la totalité de l'ensemble. Par contre ni 2, ni 3 ne sont pas des générateurs du groupe, car, par additions successives de 2, on obtient seulement 0, 2 et 4, et par additions successives de 3, on obtient seulement 0 et 3. Les sous-ensembles {0, 2, 4} et {0, 3} sont munis de la structure de groupe induite par celle de $\mathbf{C}_6$. Par contre 5 est un générateur de $\mathbf{C}_6$: aux nombres 5, 5 + 5 = 10 = 4 + 6, 15, 20, 25, 30 correspondent en effet ces éléments respectifs du groupe : 5, 4, 3, 2, 1, 0.

Reprenons au contraire le cas de $\mathbf{C}_4$. Il possède un seul sous-groupe d'ordre 2, nous l'avons noté H_2, et 2 est un entier qui divise 4.

Ces exemples illustrent et conduisent au résultat suivant :

Théorème 3.4. *Soit* φ(m) *le nombre d'entiers naturels inférieurs à* m *et premiers avec lui, et* $\mathbf{C}_m$ *un groupe cyclique d'ordre* m *engendré par* g :

1) $\mathbf{C}_m$ *possède* φ(m) *générateurs de la forme* g^p *où* p *est premier avec* m.
2) *Si par contre* q *divise* m, $\mathbf{C}_m$ *ne contient qu'un seul sous-groupe d'ordre* q.

<**Preuve** : 1) Supposons que le groupe $\mathbf{C}_m$, engendré par g, soit également engendré par g^p. Il existe alors un plus petit entier k, différent de 1, tel que $(g^p)^k = g = g\, t_n$, soit encore $g[g^{pk-1} - t_n] = 0$. Par ailleurs, puisque $\mathbf{C}_m$ est un groupe cyclique d'ordre m, $g^m = t_n$, et plus généralement $t_n = g^{qm}$.

La relation $g[g^{pk-1} - t_n] = 0$ implique donc que $g^{pk-1} = t_n = g^{qm}$, soit pk –1 = qm, ou encore pk – qm = 1. Cette relation qui implique que p soit premier avec m : si p en effet divisait m, on aurait m = rp, soit p(k – rq) = 1, une relation impossible les nombres étant entiers. Donc si p est premier avec m avec $(g^p)^k = g$, on est certain que g^p engendre le groupe cyclique $\mathbf{C}_m$. La résolution de l'équation pk = qm + 1 permet par ailleurs d'obtenir k et $\mathbf{C}_m$.

2) Supposons au contraire que q divise m : m = aq, de sorte que $g^{aq} = (g^a)^q = t_n$. De par la proposition 3.2, cette dernière relation indique que $\mathbf{C}_m$ contient un sous-groupe

cyclique d'ordre q engendré par g^a, et un sous-groupe cyclique d'ordre a engendré par g^q. Ces deux groupes cycliques sont confondus si a = q.

Soit par ailleurs H un tel sous-groupe cyclique d'ordre q. Comme on l'a vu au cours de la démonstration du théorème 3.3, il est engendré par g^k où k est le plus petit entier naturel inférieur à m tel que g^k appartienne à H, de sorte que $(g^k)^q = t_n$. On en déduit que k = a.>

De ces énoncés, résulte le :

Corollaire 3.5. *Tout groupe monogène dont l'ordre est un nombre premier ne contient pas de sous-groupes non triviaux.*

Une dernière remarque. Rappelons que, dans le plan, toute rotation peut être présentée comme la composition de deux réflexions par rapport à deux miroirs. Un groupe cyclique étant un groupe de rotations discrètes, il en résulte qu'un groupe cyclique est également un groupe de Weyl.

Les groupes cycliques étant des groupes finis de structure maintenant connue et qui paraît assez simple, on peut se demander dans quelle mesure tout groupe fini ne serait pas la « composition », un terme ici à préciser, de groupes cycliques. Nous ne tarderons pas à apporter la réponse à cette question.

3.2 Action d'un sous-groupe. Relation d'équivalence définie par un sous-groupe : groupe-quotient

3.2.1 L'exemple des entiers

Voici maintenant une autre remarque. Prenons un élément de $\mathbf{C}_4$ n'appartenant pas à H, comme par exemple r_1, et composons cet élément avec ceux de H. On obtient :

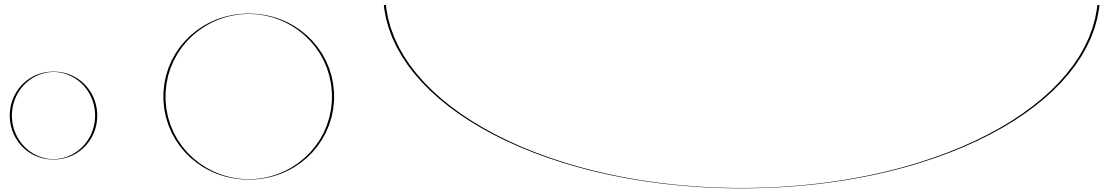
$$t_n\, r_1 = r_1, \quad r_2\, r_1 = r_3.$$

On peut interpréter cette composition soit comme une *action* à gauche des éléments du sous-ensemble H sur r_1, soit comme une *action de transport* à droite des éléments de H par r_1. On obtient le sous-ensemble $H^*(r_1) = \{r_1, r_3\}$ qui a même nombre d'éléments que H, mais aucun élément commun avec H. Si on fait agir H sur r_3 qui est dans $H^*(r_1)$, on obtiendra à nouveau $H^*(r_1)$ car $t_n\, r_3 = r_3$, $r_2\, r_3 = r_1$. $H^*(r_1)$ peut être considéré comme la *trajectoire* de r_1 sous l'action de H.

Si le groupe était plus important, et possédait un autre élément t n'appartenant ni à H ni à $H^*(r_1)$, il déplacerait H en $H^*(t)$, n'ayant aucun élément commun avec les précédents sous-ensembles. De la sorte, plus généralement, un groupe G peut être découpé par un sous-groupe H en tranches de même largeur, égale au nombre d'éléments de H.

Nous allons pouvoir examiner mieux ce phénomène sur un autre exemple.

Considérons à nouveau, dans le plan, un cercle divisé de manière régulière. La translation angulaire élémentaire est caractérisée par l'angle $2\pi/m$. On fait tendre n vers l'infini, et, par convention, on notera par $2\pi/\mathbf{N}$ la translation infinitésimale obtenue. On fait



croître simultanément le rayon du cercle vers l'infini, de sorte qu'il éclate en une droite infinie, également divisée de manière régulière : la translation angulaire élémentaire devient une translation rectiligne élémentaire, et l'ensemble des points S_m de la division du cercle devient maintenant un ensemble de points sur la droite, codés respectivement par m :

…	-m	…	-3	-2	-1	0	1	2	3	…	m …
…	S_{-m}	…	S_{-3}	S_{-2}	S_{-1}	S_0	S_1	S_2	S_3	…	S_m …

De la sorte, on obtient une représentation linéaire du groupe **Z** des *entiers*, identifié au *groupe des translations discrètes* de l'espace euclidien à une dimension.

En tant que provenant d'un groupe cyclique, **Z** est lui-même un groupe monogène, engendré par la translation rectiligne {1}.

Un changement de l'unité de mesure n'affectera pas la structure de l'ensemble des translations. Considérons ainsi l'ensemble des translations rectilignes de longueur k, formant l'ensemble noté k**Z** :

$$k\mathbf{Z} = \{-\infty, \ldots, -mk, \ldots, -2k, -k, 0, k, 2k, \ldots, mk, \ldots, \infty\}.$$

Structuré en groupe, ce sous-ensemble de **Z** en est un sous-groupe. **Z** étant monogène, les propositions précédentes indiquent que tout sous-groupe de **Z** est de la forme k**Z**. (On peut reprendre la démonstration du théorème 3.3 : soit k le plus petit entier positif d'un sous-groupe H de **Z**. La composition de cet élément avec lui-même est un élément de H, de sorte que pk appartient à H. Soit par ailleurs n un élément de H : il s'écrit n = pk + r où r est inférieur à k. La composition de deux éléments de H appartenant à H, n – pk = r appartient à H : si r n'est pas nul, ce fait contredit l'hypothèse selon laquelle k est le plus petit élément positif de H. Par conséquent r doit être nul, et H = k**Z**).

Voici une application important de ce fait, le

Théorème 3.6 (de Bachet-Bezout). *Pour que les entiers* $p_1, p_2, \ldots, p_n$ *soient premiers entre eux, il faut et il suffit qu'existent des entiers* $\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_n$ *tels que*

$$\hat{u}_1 p_1 + \hat{u}_2 p_2 + \ldots + \hat{u}_n p_n = 1.$$

<**Preuve** : Soit d'abord $p_1, p_2 \ldots, p_n$ un système de n nombres entiers. On vérifie aisément que, lorsque les u_i parcourent l'ensemble des entiers, l'ensemble I des nombres $p = u_1 p_1 + u_2 p_2 + \ldots + u_n p_n$ possède la structure de groupe. I étant un sous-groupe du groupe monogène **Z**, le théorème 3.3 nous dit qu'existe un plus petit entier positif d qui engendre I, de sorte qu'on peut écrire globalement : I = d**Z**. Ou encore localement, les u_i étant donnés, l'élément p de I est un multiple de d :

$$p = u_1 p_1 + u_2 p_2 + \ldots + u_n p_n = q\, d.$$

Cette relation étant indépendante du choix des u_i, elle signifie que les p_i sont divisibles par d. En effet, par exemple pour $u_1 = 1$, $u_{i\neq1} = 0$, $p_1 = q_1$ d. Comme tout autre diviseur commun aux p_i divise p, quels que soient les u_i, ce diviseur divise également d, qui est donc le plus grand commun diviseur des p_i. d étant un nombre de I, ensemble des nombres de la forme $u_1 p_1 + u_2 p_{2+} \ldots + u_n p_n$, il existe un système particulier de u_i alors notés $\hat{u}_i$ pour lequel q = 1, et par conséquent tel que :

$$\hat{u}_1 p_1 + \hat{u}_2 p_{2+} \ldots + \hat{u}_n p_n = d.$$

Si maintenant on suppose que les p_i sont premiers entre eux, leur plus grand commun diviseur d est égal à 1, d'où l'énoncé du théorème direct.

Réciproquement, cette condition étant vérifiée, le plus grand commun diviseur des p_i divise 1 : il ne peut qu'être 1 ; les p_i sont donc premiers entre eux.>

Reprenons maintenant l'examen de k**Z**. Pour mieux fixer les idées, supposons que k = 3. Considérons un cavalier N placé en 0. L'élément 3m du sous-groupe de translations H = 3**Z** va le transporter en un lieu situé en position 3 m + 0, de sorte que l'ensemble des positions du cavalier par l'action de tous les élément de H, sa trajectoire, est l'ensemble que, par convention, on notera H + 0 ou bien H^*_0 :

$$H^*_0 = \{-\infty, \ldots, (-3m) + 0 \ \ldots, \ (-6) + 0, (-3) + 0, \ 0, \ 3 , 6, \ldots, 3m, \ldots, \ \infty\},$$

soit

$$H^*_0 = \{-\infty, \ldots, -3m\ldots, \ -6 , \ -3 \ , \ 0, \ 3 , 6, \ldots, 3m, \ldots, \ \infty\} = H.$$

Si le cavalier est placé en position 1, les éléments de H vont le transporter en des positions formant l'ensemble :

$$H + 1 = H^*_1 = \{-\infty, \ldots, (-3m) + 1 \ \ldots, \ (-6) + 1, (-3) + 1, \ 1, \ 4 , 7, \ldots, 3m + 1, \ldots, \ \infty \}.$$

Si le cavalier est placé en position 2, les éléments de H vont le transporter en des positions formant l'ensemble :

$$H + 2 = H^*_2 = \{-\infty, \ldots, (-3m) + 2 \ \ldots, \ -4, -1, \ 2, \ 5 , 8, \ldots, 3m + 2, \ldots, \ \infty \}.$$

Si le cavalier est placé en position 3, on retrouve l'ensemble des éléments de H : plus généralement $H^*_{3m} = H$.

Les sous-ensembles H^*_i, qui ont évidemment même nombre d'éléments (on dit qu'ils sont équipotents), forment une partition de **Z** : $H^*_0 \cup H^*_1 \cup H^*_2 = \mathbf{Z}$. Par suite, le nombre d'éléments de **Z**, son cardinal, vaut 3 fois le nombre d'éléments de H :

$$\text{card } (\mathbf{Z}) = 3 \text{ card}(3\mathbf{Z})$$

Pour mesurer les longueurs de draps dans les temps anciens, on utilisait une règle qui servait d'unité de mesure. Cette règle était appelée un *module.* Dans le cas présent, le module est 3.

Considérons comme *équivalentes deux positions* x, y *séparées par un même multiple du module*, ce qui s'écrit, pour une valeur convenable de m :

$$y - x = 3m$$

ou encore :

$$y - x \in 3\mathbf{Z}.$$

Alors tous les éléments d'un sous-ensemble H^*_i donné sont équivalents entre eux. Le sous-ensemble forme une *classe d'équivalence*, et n'importe quel élément de ce sous-ensemble en est un *représentant* : 0, 1, 2 peuvent donc être choisis pour représenter respectivement les classe $H^*_0 = H$, H^*_1, H^*_2.

Pour être plus clair dans ce qu'il va advenir, changeons encore les notations : notons par $\underline{0}$ la classe H^*_0 représentée par 0, par $\underline{1}$ la classe H^*_1 représentée par 1, par $\underline{2}$ la classe H^*_2 représentée par 2 , et par $H^* = \{\underline{0}, \underline{1}, \underline{2}\}$ enfin cet ensemble de classes à trois éléments.

Notons qu'on peut munir H* d'une loi de groupe pour l'addition, avec $\underline{0}$ pour élément neutre. En effet, l'addition $\underline{0} + \underline{0}$ signifiant l'ensemble des sommes d'un élément quelconque de $\underline{0}$ avec un élément quelconque de $\underline{0}$, cette somme admet $\underline{0}$ pour résultat. De même, prenons un élément quelconque de $\underline{1}$, soit 3m + 1, et effectuons sa somme avec un autre élément quelconque de $\underline{1}$, soit 3p + 1 : nous obtenons l'élément 3(m + p) + 2, qui est un élément de $\underline{2}$: par conséquent $\underline{1} + \underline{1} = \underline{2}$. On vérifie de la même façon que $\underline{1} + \underline{2} = \underline{0}$: $\underline{1}$ est le symétrique de $\underline{2}$.

On a vu par ailleurs que card ($\mathbf{Z}$) = 3 card($3\mathbf{Z}$) = card(H*) card($3\mathbf{Z}$), de sorte qu'il est justifié, par convention, de noter H* par $\mathbf{Z}/3\mathbf{Z}$, ou par $\mathbf{Z}/3$, ou encore par $\mathbf{Z}_3$ et de l'appeler le *groupe-quotient* de $\mathbf{Z}$ par $3\mathbf{Z}$**.**

Nous allons maintenant donner une expression générale au contenu assez riche de cet exemple.

3.2.2 Action d'un groupe sur un ensemble. Relations d'équivalence associées

Nous avons rencontré au second chapitre les groupes de mouvements $\mathbf{SO}(1)$, $\mathbf{\Sigma}_2$ et $\mathbf{W}_2$ qui modifient la position des éléments N et S de l'ensemble $\mathbf{E} = \{N, S\}$, et au paragraphe précédent, le sous-groupe de mouvements $3\mathbf{Z}$ qui déplacent la position des éléments de l'ensemble $\mathbf{E} = \mathbf{Z}$. On dit que ces groupes *opèrent* sur $\mathbf{E}$. Plus généralement :

Définition 3.5 : On dit que le groupe $G = (\mathbf{T},*)$ *opère à gauche* sur l'ensemble $\mathbf{E}$ s'il existe une application $\gamma : G \times \mathbf{E} \rightarrow \mathbf{E}$ qui vérifie les règles :

1) l'action de l'élément neutre laisse invariant tout élément de $\mathbf{E}$:

$$\gamma(t_n, x) = x$$

2) l'action de t' sur l'élément $y = \gamma(t, x)$ est aussi celle de t' * t sur x :

$$\gamma(t', \gamma(t,x)) = \gamma(t' * t, x)$$

Si on convient de noter par t.x l'image $\gamma(t,x)$, la deuxième relation peut encore s'écrire :

$$t'.(t.x) = (t' * t).x$$

Définition 3.6 : Soient l'élément x de **E**, et $\mathcal{T}$ un ensemble de transformations qui, par ses éléments t, transforme x en d'autres éléments t .x de **E** : l'ensemble $\mathcal{T}$ x = {t.x, t ∈ $\mathcal{T}$} des éléments transformés s'appelle la *trajectoire* (ou *orbite*) de x *sous l'action à gauche de* $\mathcal{T}$, ou plus simplement la *trajectoire à gauche* de x définie par $\mathcal{T}$.

On définit bien sûr les même notions « à droite ».

La donnée du couple ($\mathcal{T}$, **E**) s'appelle un *système dynamique.* Lorsque $\mathcal{T}$ est un groupe discret, en particulier fini, le système dynamique est lui-même appelé un *système dynamique discret.*

Naturellement, un système en évolution est caractérisé par le comportement de ses trajectoires, leur stabilité, les trajectoires singulières autour desquelles s'organisent les autres trajectoires.

Nous allons rester ici dans le cadre où les transformations de $\mathcal{T}$ opèrent sur l'ensemble **E** = **T** des éléments d'un groupe G = (**T**,*), et en forment un sous-groupe H. Pour faciliter l'écriture, nous supposons que H est d'ordre fini m :

$$H = \{t_n, t_1, t_2, \ldots, t_{m-1}\}.$$

La trajectoire à gauche de x est alors l'ensemble :

$$\underline{x}_H = H*x = \{x, t_1*x, t_2*x, \ldots, t_{m-1}*x\}.$$

Un premier fait remarquable est que, si l'on considère comme équivalents x et y deux éléments de **T** situés sur la même trajectoire à gauche, la relation $\mathcal{E}_g$ établie entre x et y est bien une relation d'équivalence au sens mathématique du terme.

Dire en effet que x et y = t_k.x sont sur la même trajectoire s'exprime par le fait que :

> y x^{-1} (= t_k) ∈ H lorsque la loi de composition * est la multiplication,
> ou bien y – x ∈ H lorsque la loi de composition * est l'addition.

Proposition 3.7. *La relation* $\mathcal{E}_g$ *entre* x *et* y *définie par* x $\mathcal{E}_g$ y ⇔ y – x ∈ H *est une relation d'équivalence.*

<**Preuve** : On utilise ici la notation additive. Vérifions que la relation $\mathcal{E}_g$ vérifie les propriétés *rst* (*r*éflexivité, *s*ymétrie, *t*ransitivité) : x est équivalent à lui-même puisque x – x = t_n ∈ H. Si x est équivalent à y, alors y est équivalent à x : en effet si y – x = t ∈ H , x – y = - t ∈ H. Si x est équivalent à y qui est équivalent à z, alors x – y = t , y – z = t' et x – y + y – z = t + t' ∈ H .>

Du fait de cette proposition, la relation d'équivalence $\mathcal{E}_g$ entraîne que l'ensemble **T** est découpé en classes d'équivalence qui sont les différentes trajectoires que définit l'action de H sur les éléments de G. D'où d'une part, ici, cette dénomination des trajectoires :

Définition 3.7 : On appelle également une telle trajectoire H*x de x la *classe à gauche de* x *par l'action de* H, et *index* de H dans G, noté quelquefois [G : H], le nombre de trajectoires à

gauche (classes à droite) définies par H dans **T**. On notera par K ou, de manière plus traditionnelle, par G/H l'ensemble des classes d'équivalence ainsi définies.

Lorsque x est un élément d'un groupe G dont H est un sous-groupe, on peut interpréter différemment H*x en considérant que x est l'élément qui opère sur H. Par exemple, si H est le sous-groupe H = k**Z** de **Z**, et si x = 5, alors, en H+5 = {kp + 5 où p parcourt **Z**} : l'effet de 5 sur H est de translater ses éléments de 5. C'est pourquoi on donne le nom générique de *translation* à cette action, considérant qu'on translate H à droite : H*x est alors appelé la *classe à droite de* H *par l'action de* x.

Un second fait remarquable déjà remarqué est que toutes les trajectoires (classes) ont alors même nombre d'éléments – on fait la démonstration pour les classes à gauche :

Théorème 3.8. *Soit* H *un sous-groupe d'un groupe de transformations* G = (**T**, *). *Alors toutes les trajectoires définies par l'action de* H *sur les éléments de* **T** *ont même nombre d'éléments que* H :

$$\text{card}(H) = \text{card}(H*x).$$

<**Preuve** : Notons par H*x = {y = t*x, t ∈ H} la trajectoire de x sous l'action à gauche de H. Par construction, l'application $h_x : H \rightarrow H*x$ telle que $h_x(t) = y = t * x$ est surjective. Elle est aussi injective, car si $h_x(t) = h_x(t') = y$, égalité qui s'écrit aussi $t * x = t' * x = y$, puisque x admet un symétrique dans G, $t * x * x^{-1} = t' * x * x^{-1}$, soit encore t = t'. h_x est donc une bijection.>

Comme on a le même résultat en considérant les classes à droite, on évitera l'emploi de l'indice signifiant gauche ou droite lorsque cela n'est pas nécessaire.

On en déduit cet énoncé, déjà établi au XVIII^{e} siècle par Lagrange dans le cadre de la théorie des permutations :

Théorème 3.9. card (G) = [G : H] card(H), *ou encore* : *l'ordre d'un sous-groupe d'un groupe fini divise l'ordre du groupe.*

Voici deux applications simples de ce résultat. D'abord le :

Théorème 3.10. *Soit* G = (**T**,*) *un groupe fini d'ordre* m. *Quel que soit l'élément* t *de* **T**,

$$t^m = t_n.$$

<**Preuve** : Soit t un élément de **T**. G étant fini, si l'on fait parcourir à m l'ensemble des nombres naturels, t^m va parcourir les éléments d'un sous-groupe cyclique $\mathbf{C}_{o(t)}$ de G, d'ordre o(t) au plus égal à m. On a donc d'une part $t^{o(t)} = t_n$ (cf la proposition 3.2), et d'autre part, par le théorème précédent, $m = o(t)\,[G : H_{o(t)}]$, et par suite $t^m = (t^{o(t)})^{[G : H]} = (t_n)^{[G : H]} = t_n$.>

puis celui-ci, qui étend le corollaire 3.5 :

Théorème 3.11 *Tout groupe fini G dont l'ordre est un nombre premier est cyclique.*

<**Preuve :** Soit t un élément de **T** : G étant fini, t engendre un sous-groupe cyclique d'ordre k de G : par le théorème précédent, k divise l'ordre de G ; il est donc réduit à l'élément neutre ou est G lui-même.>

3.2.3 Notions liées à la stabilité : stabilisateur, sous-groupes invariants, groupes-quotient

Les parties F fixes, invariantes donc stables d'un système dynamique sont d'un intérêt particulier. Elles servent de repères dans un monde en changement.

Définition 3.8 : On appelle *stabilisateur* de F, St(F), le sous-ensemble de $\mathfrak{I}$ qui laisse invariant F. Parmi ces parties F, deux retiennent l'attention : d'une part la plus grande de ces parties, et d'autre part les plus petites d'entre elles, celles réduites à un seul élément x : leur trajectoire se résume alors à eux-mêmes. Ainsi par exemple les rotations autour d'un point x laissent invariant ce point.

Proposition 3.12 *Supposons que l'ensemble de transformations ait une structure de groupe* G = (**T**, *). *Soit* x *un élément de* **T**. *Le stabilisateur de* x *est un sous-groupe commutatif de* G.

<**Preuve** : Le stabilisateur contient évidemment l'élément neutre de **T**. La relation t'.(t.x) = (t' * t).x entraîne l'associativité des compositions de transformations puisque la loi de groupe est associative. Si t et t'appartiennent à St(x), t.x = x = t'.x : par conséquent (t' * t).x = t'.(t .x) = t'.x = x, de même que (t * t').x = t.(t'.x) = t.x = x. Ainsi, la loi de composition est commutative. Puisque $t^{-1}.(t * x) = t^{-1}.x = (t^{-1} * t).x = t_n.x = x$, le symétrique de t appartient à St(x). St(x) a bien la structure de groupe.>

Définition 3.9 : Lorsque l'ensemble de transformations **T** possède la structure de groupe, St(x) est alors appelé le *sous-groupe d'isotropie* de x.

Il résulte de la proposition précédente que *si un groupe G n'a pas de sous-groupe commutatif, aucun élément de G ne peut être invariant par l'action de l'un de ses sous-groupes.*

Considérons maintenant la situation d'un changement de repère défini par une transformation g. Le groupe des rotations autour d'un point O laisse ce point invariant : comment s'établit le groupe des rotations autour de g(O) = O' ? L'essentiel de la réponse est contenu dans cet énoncé, que le lecteur a sans doute déjà rencontré sous une forme plus cachée en Algèbre Linéaire :

Théorème 3.13 *Soient* x *et* y de*ux éléments de* G *appartenant à une même trajectoire définie par un sous-groupe* H. *Soit* t *un élément de* G *tel que* t.x = y. *Alors* $St(y) = t\ St(x)\ t^{-1}$.

<**Preuve** : Soit g un élément du stabilisateur de y : g.y = y. Par conséquent t.x = y = g.y = g.(t.x) = (g *t).x, et par suite, par multiplication à gauche par t^{-1} des deux membres les plus éloignés de cette égalité, $x = (t^{-1} * g * t).x$. Ainsi $(t^{-1} * g * t) = s$ est un élément du stabilisateur de x. La relation $g \mid\!\rightarrow s$ définit la relation entre St(y) et St(x) qu'on peut écrire sous l'une des deux formes : $St(x) = t^{-1}\ St(y)\ t$, $St(y) = t\ St(x)\ t^{-1}$. Cette relation est une bijection car s = s' s'écrit aussi : $t^{-1} * g * t = t^{-1} * g' * t$, soit g = g'. >

Définition 3.10 : On qualifie de *conjugués* ou de *semblables* deux sous-groupes H et H' de G pour lesquels existe un élément t du groupe tel que :

$$H = t^{-1}\ H'\ t.$$

Le cas particulier significatif est naturellement celui où le sous-groupe reste invariant par le transport g.

Définition 3.11 : On dit qu'un sous-groupe N de G = (**T**, *) est *invariant* (ou *normal* ou *distingué*) s'il reste invariant pour tout transport t de G, par conséquent, pour tout t ∈ **T** :

$$N = t^{-1} * N * t.$$

De cette définition résulte que *tous les sous-groupes d'un groupe commutatif sont invariants*. (La notion d'invariance ayant un caractère physique fondamental, il convient d'employer le terme invariant et non point ceux de distingué ou de normal).

La relation $N = t^{-1} * N * t$ s'écrit également $t * N = N * t$. Autrement dit, dans le cas où est invariant, les trajectoires N*t définies par l'action à gauche de N, coïncident avec les trajectoires t N définies par l'action à droite de N.

Théorème 3.14 *Si* N *est un sous-groupe invariant de* G, *alors l'ensemble* G/N = K *des trajectoires (ou classes) peut être muni de la structure de groupe pour la loi de composition de* G.

<**Preuve** : Soit $\underline{x}$ = N*x et $\underline{y}$ = N*y deux classes distinctes. On pose $\underline{x} * \underline{y}$ = {(t * x) * (t' * y) lorsque t et t' parcourent N}. Or $t * x * t' * y = t * x * t' * x^{-1} * x * y = t * (x * t' * x^{-1}) * x * y$. Comme $N = x * N * x^{-1}$, $x * t' * x^{-1}$ est un élément t'' de N, de sorte que $t * t'' = h$ appartient à N. Par suite $\underline{x} * \underline{y}$ = {h * x * y lorsque h parcourt N} = N * (x * y). On vérifie alors immédiatement que G/N est muni d'une structure de groupe d'élément neutre $\underline{t_n} = N *_{tn} = t_n *_H$.>

Définition 3.12 : Si N est sous-groupe invariant du groupe G, G/N = K est alors appelé le *groupe-quotient* de G par N.

Bien sûr éventuellement triviaux, tout groupe G admet deux sous-groupes invariants, respectivement appelés son sous-groupe *centralisateur* et son sous-groupe *dérivé*.

Définition 3.13 : Le *centralisateur* c(G) de G est l'ensemble des éléments c de G qui sont les stabilisateurs à droite et à gauche de tous les éléments de G : $c * g * c^{-1} = g$ pour tout élément g de G.

Il est clair que si c et c' appartiennent au centralisateur $c * c' = c''$ appartient aussi à c(G), puisque $(c * c')^{-1} * g * (c * c') = (c * c') * g * (c'^{-1} * c^{-1}) = c * (c' * g * c'^{-1}) * c^{-1} = c * g * c^{-1} = g$. c(G) est un sous-groupe de G.

c(G) est invariant : soit en effet $t * c * t^{-1} = h$ un élément de $t * c(G) * t^{-1}$. Vérifions qu'il appartient également à c(G). En effet, $h * g * h^{-1} = (t * c * t^{-1}) * g * (t * c * t^{-1})^{-1} = (t * c * t^{-1}) * g * (t * c^{-1} * t^{-1}) = t * [c * (t^{-1} * g * t) * c^{-1}] * t^{-1} = = t * (t^{-1} * g * t) * t^{-1} = g$.

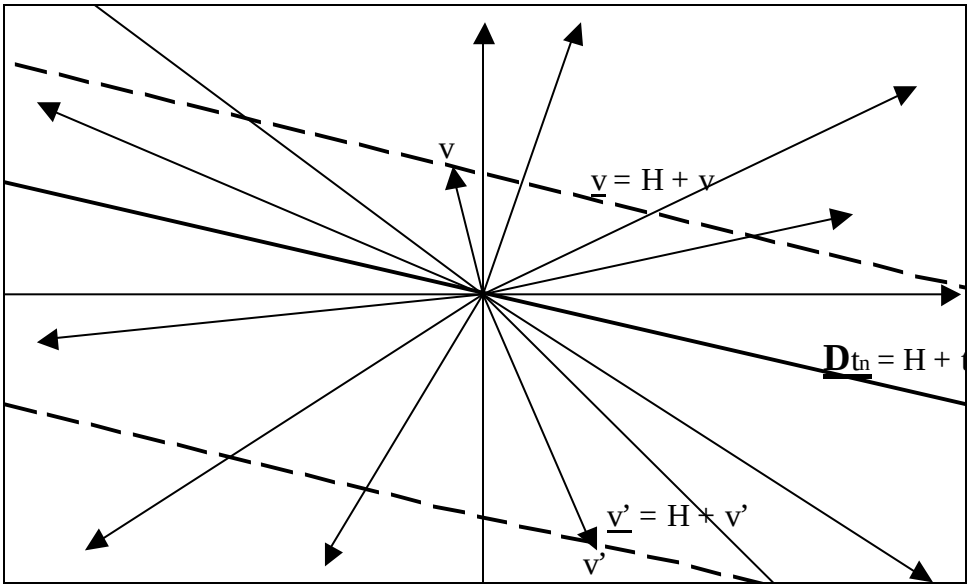
Définition 3.14 : Si g et h sont deux éléments de G, on évalue le défaut de commutation entre ces deux éléments par l'évaluation de Lie $[g, h] = (g * h) * (h * g)^{-1} = g * h * g^{-1} * h^{-1} = k$, appelée le *commutateur* de g et h.

Définition 3.15 : Le *sous-groupe dérivé* de G, D(G), est le sous-groupe engendré par les commutateurs de G. Il contient donc ces commutateurs et leurs produits qui, eux-mêmes, ne sont pas forcément des commutateurs.

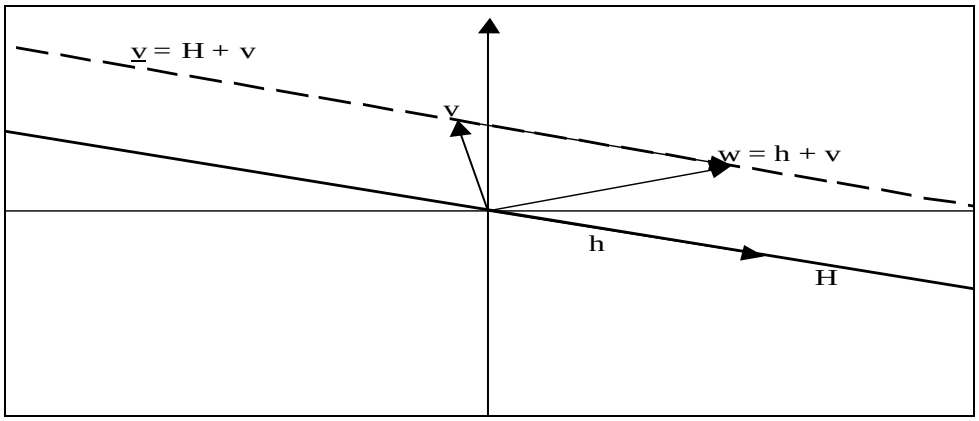
Vérifions que D(G) est un sous-groupe invariant. Il suffit de vérifier que $t * k * t^{-1}$ est encore un commutateur. Or $t * k * t^{-1} = t * g * h * g^{-1} * h^{-1} * t^{-1} = (t * g) * h * g^{-1} * h^{-1} * t^{-1} = (t * g * t^{-1}) * (t* h * t^{-1}) * (t * g^{-1} * t^{-1}) (t * h^{-1} * t^{-1})$.

Un autre exemple de groupe-quotient

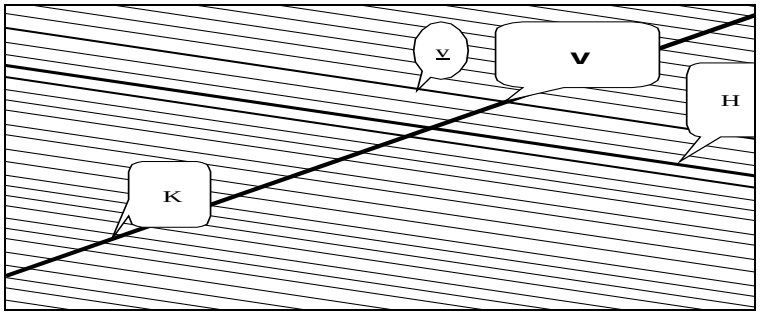
G est ici le groupe des vecteurs de l'espace vectoriel standard à deux dimensions sur l'ensemble des réels. La loi de composition est ici l'addition notée +. Sur le dessin sont représentés quelques-uns de ces vecteurs. H est un sous-groupe de ces vecteurs formant une droite vectorielle $\mathbf{D}\underline{t_n}$ qui apparaît en trait plein plus épais : elle porte les vecteurs $t_n + h$ où h parcourt H.



v est un vecteur de G. La classe $\underline{v} = H + v$ de v est formée de l'ensemble des vecteurs $w = h + v$ où h parcourt H. $\underline{v}$ est également la droite affine représentée en traits espacés plus épais. Les vecteurs v et w définissent la même classe, $\underline{v} = \underline{w}$, et en sont, chacun, un représentant. Lorsque v varie les différentes droites forment un système de fils (on dit de feuilles) parallèles qui couvrent tout l'espace.



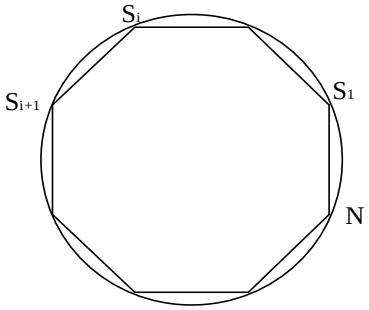
On choisit un représentant dans chaque classe de telle sorte qu'ils appartiennent à un même sous-espace vectoriel K. Il y a bien sûr une infinité de manières de choisir K : l'essentiel est que tous ces choix sont des répliques du même sous-espace abstrait. Dans le cas présent, du point de vue pratique, on prend n'importe quelle droite vectorielle K distincte de H. L'intersection v = v ∩ K est un représentant de v situé dans le sous-espace vectoriel K. On identifie la structure de G/H à celle de K.



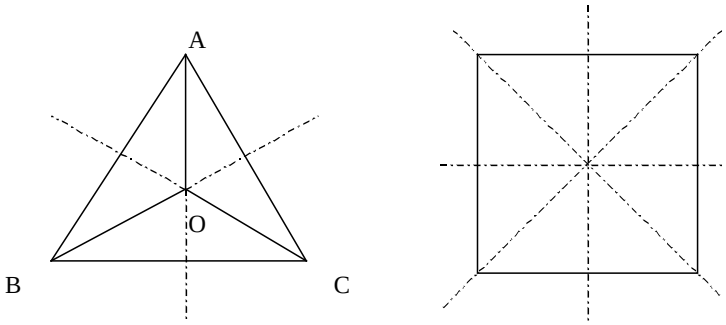
En dimension supérieure, si H est un sous-espace vectoriel de dimension k de l'esapce vectoriel G de dimension n, G/H a pour dimension n - k.

Exemple : Un nouveau déploiement du groupe primordial, le groupe diédral D_m

Le déploiement du groupe primordial en un groupe cyclique a été accompagné, du point de vue géométrique, par le découpage du périmètre d'un cercle en parts égales. Si l'on joint les points successifs de cette division par un segment, on obtient un polygone régulier dont on peut étudier les symétries. On y voit apparaître deux des transformations principales qui définissent le groupe primordial : les rotations, étudiées précédemment dans cadre plus général, et les réflexions, ici par rapport aux « diagonales » du polygone. Ces diagonales joignent et sommets opposés et les milieux des côtés opposés si le nombre m des côtés est pair, les milieux de ces côtés aux sommets opposés si m est impair.



Conception et Réalisation par Maria DEDÓ



Définition 3.13 : On appelle *groupe diédral* d'ordre 2m, $\mathbf{D}_m$, le groupe des transformations orthogonales du plan euclidien laissant invariant le polygone régulier à m côtés non orientés.

Ces transformations sont donc d'une part les m rotations autour du centre O du polygone, d'angle $2\pi/m$, formant le groupe cyclique $\mathbf{C}_m = \langle r, r^m = t_n \rangle$, et d'autre part les m réflexions (ou symétries) ρ_i par rapport aux m « diagonales » du polygone.

Puisque les rotations peuvent être elles-mêmes définies par des réflexions, un groupe diédral peut alors être compris comme un groupe **W** de réflexions. Nous allons donner ici une autre manière de présenter $\mathbf{D}_m$, en étudiant d'abord l'exemple de $\mathbf{D}_3$.

Dans ce cas, on a évidemment $r^3 = \rho_i^{\,2} = t_n$.

On voit, par exemple, que la rotation r qui amène CA sur AB, et donc A en B, suivie de la réflexion sur le miroir OA qui amène alors A au point appelé initialement C, est aussi la réflexion de miroir OB, ce qui s'écrit :

$$\rho_a \, r = \rho_b .$$

Par permutation circulaire, on obtient deux autres relations analogues : $\rho_b \, r = \rho_c$, $\rho_c \, r = \rho_a$, et par suite $(\rho_a \, r = \rho_b) r = \rho_b \, r = \rho_c = \rho_a \, r^2$.

Avec ces propriétés, la relation $\rho_b{}^2 = t_n$ s'écrit également $(\rho_a \, r)^2 = \rho_a \, r \, \rho_a \, r = t_n$:

on traduit ainsi que la composition de la rotation r qui amène A en B, suivie de la symétrie ρ qui amène maintenant A en C, puis d'une rotation r qui conduit A en sa position initiale, suivie de la symétrie ρ_a qui le laisse invariant, laisse A invariant.

De là vient également qu'avec une seule réflexion, $\rho_a = \rho$, et la rotation r, on code toutes les autres réflexions. Pour connaître tous les éléments du groupe, on sait maintenant qu'ils sont de la forme $r^p \, \rho^{\,q}$ ou $\rho^{\,q} \, r^p$, il faut encore examiner la commutation des produits de ρ et de r.

Or on voit également, par exemple, que, pour aller de B en A, on peut, par une rotation aller en C, puis par une réflexion aller en A, ou bien par une réflexion aller en C, puis par une rotation aller en A, ce qui s'écrit :

$$\rho_b \, r = r \, \rho_a \text{ ou encore } \rho_b = r \, \rho_a \, r^{-1}$$

et par permutation circulaire : $\rho_c = r \, \rho_b \, r^{-1}$, $\rho_a = r \, \rho_c \, r^{-1}$.

De la même façon, la transformation $\rho_b \, r$ peut s'obtenir en pratiquant d'abord une réflexion qui échange C et A mais laisse invariant B, puis deux rotations qui amènent B sur la position du nouveau C : $\rho_b \, r = r^2 \, \rho_b$. On peut obtenir également cette relation en remarquant qu'elle exprime que $\rho \, r$ est le symétrique de $r^2 \, \rho$, propriété qu'on peut aussi obtenir par le calcul $(\rho \, r \, r^2 \, \rho = \rho \, t_n \, \rho = t_n)$.

Compte tenu du fait que $r^3 = \rho^{\,2} = (\rho \, r)^2 = t_n$, on a obtenu tous les éléments du groupe, à savoir :

$$\mathbf{D}_3 = \{ t_n, r, r^2, \rho, r\,\rho, r^2\,\rho \}.$$

D_3 contient le sous-groupe $\mathbf{W}_2 = \{t_n, \rho\}$, et le sous-groupe cyclique $\mathbf{C}_3 = \{t_n, r, r^2\}$ qui est invariant. En effet, il reste invariant par l'action de tout élément de lui-même. Il suffit alors de vérifier qu'il reste invariant par l'action de ρ. Evaluons donc $\rho \, \mathbf{C}_3 \, \rho^{\,-1}$:

$\rho \, t_n \, \rho^{\,-1} = t_n$, $\rho \, r \, \rho^{\,-1} = \rho \, r \, \rho$ (puisque $\rho = \rho^{\,-1}$) $= (\rho \, r \, \rho)(r \, r^{-1}) = (\rho \, r \, \rho \, r) \, r^{-1} = t_n \, r^1 = r^2$
et $\rho \, r^2 \, \rho^{\,-1} = \rho \, r^2 \, \rho = (\rho \, r) \, \rho \, \sigma^{-1} (r \, \rho) = (\rho \, r \, \rho)(\rho \, r \, \rho) = r^4$ (d'après le calcul de $\rho \, r \, \rho^{\,-1} = \rho \, r \, \rho$ qui précède) $= r$.

Puisque $\mathbf{C}_3$, d'indice $6 : 3 = 2$, est un sous-groupe invariant, $\mathbf{D}_3/\mathbf{C}_3$ formé des deux classes $\underline{t_n}$, et $\underline{\rho}$, possède également la structure de groupe, la même que celle de $\mathbf{W}_2$.

A partir de cet exemple, on peut d'abord expliciter la structure générale du groupe diédral $\mathbf{D}_m$. Il est engendré par la rotation r d'angle $2\pi/m$ et la réflexion ρ par rapport à un axe de symétrie du polygone régulier à m côtés. r et ρ obéissent aux relations, qui constituent une présentation du groupe :

$$\mathbf{D}_m = \langle r , \rho : r^m = \rho^2 = (\rho r)^2 = t_n \rangle.$$

Voici des variantes de cette présentation :

1.Comme $(\rho r)^2 = t_n = (\rho r)\,(\rho r) = \rho\,(r\,\rho\,r)$, on a, puisque $\rho^2 = t_n$,

$$r\,\rho\,r = \rho,$$

soit :

$$\mathbf{D}_m = \langle r , \rho : r^m = \rho^2 = t_n,\ r\,\rho\,r = \rho \rangle.$$

2. Ou encore, la même relation $t_n = (\rho r)\,(\rho r) = (\rho\ r\ \rho)\ r$ entraîne que :

$$\rho\ r\ \rho = r^{-1},$$

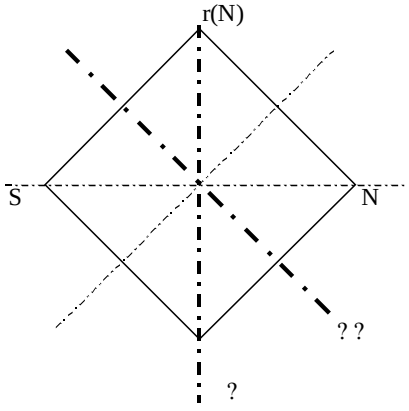
et par suite :

$$\mathbf{D}_m = \langle r , \rho : r^m = \rho^2 = t_n,\ \rho\ r\ \rho = r^{-1} \rangle.$$

3. Enfin, posant, $\rho = \rho_1$, puis $\rho\ r = \rho_2 = \rho_1\ r$, et donc $r = \rho_1\rho_2$, on obtient la présentation :

$$\mathbf{D}_m = \langle \rho_1, \rho_2 : \rho_1{}^2 = \rho_2{}^2 = (\rho_1\rho_2)^m = t_n \rangle.$$

Elle met en évidence que $\mathbf{D}_m$ est bien un groupe de Weyl puisque il est engendré par les deux réflexions ρ_1 et ρ_2, ρ_1 qui envoie N sur S, et ρ_2 qui envoie r(N) sur S. Dans la littérature courante, les miroirs correspondants à ces réflexions sont souvent notés α et β.



Dans le dessin ci-dessus associé à $\mathbf{D}_4$, les miroirs sur lesquels se font les réflexions font entre eux l'angle $\pi/4$, de sorte que le produit $\rho_1\rho_2$ des deux réflexions est la rotation r d'angle $\pi/2$.

$\mathbf{D}_m$ possède 2m éléments, par exemple :

$$t_n,\ r,\ r^2,\ \ldots\ ,\ r^{m-1},\ \rho,\ \rho\ r,\ \rho\ r^2,\ \ldots,\ \rho\ r^{m-1}.$$

Les m premiers forment un groupe cyclique $\mathbf{C}_m$, invariant car d'indice 2 dans $\mathbf{D}_m$.

Dans l'exemple, nous avons rencontré la relation $\rho_b\, r = r\, \rho_a$ ou encore $\rho_b = r\, \rho_a\, r^{-1}$. Par analogie avec le contenu de la définition 3.10, on introduit la :

Définition 3.16 : Deux éléments t et t' d'un groupe G sont *conjugués* ou encore *semblables* s'il existe un élément g du groupe tel que $t = g * t' * g^{-1}$. g est l'*élément de conjugaison* entre t et t'.

Proposition 3.15 *La relation de conjugaison définie par* g *est une relation d'équivalence sur* G.

<**Preuve** : La relation est réflexive car t est conjugué avec lui-même par l'intermédiaire de l'élément neutre. Elle est symétrique puisque que $t = g * t' * g^{-1}$ s'écrit également $t' = g^{-1} * t * g$. Elle est transitive puisque si que $t = g * t' * g^{-1}$ et si que $t' = h * t'' * h^{-1}$ alors $t = (g * h) * t'' * (h^{-1} * g^{-1})$.>

CHAPITRE IV

TRANSPORT ET PHOTOGRAPHIE D'UN GROUPE DANS UN AUTRE

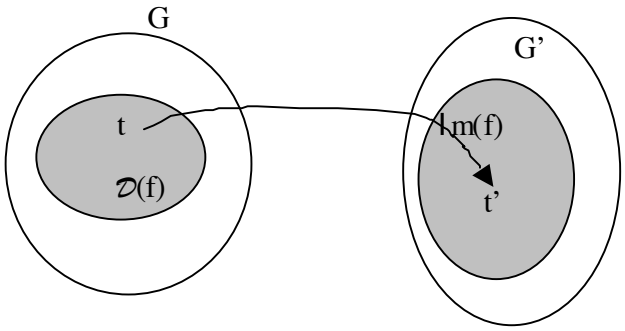
4.1 Motivation. Notion de morphisme, les propriétés principales qui lui sont associées

Etant donné un objet G, il arrive qu'on le transporte pour en faire usage dans un lieu différent, ou bien, notamment s'il est lointain et mal connu, qu'on en prenne des photographies d'assez bonne qualité pour être révélatrices de ses propriétés, et qu'on étudiera en détail.

Naturellement, au cours du transport, les principales qualités de l'objet ne doivent pas être perdues. Ou bien si une photographie est prise, l'image doit-elle être assez fidèle à la source pour être utilisable.

Si l'objet est un groupe G = (**T**,*), il sera donc nécessaire qu'après transport ou photographie, l'objet transporté G' conserve la structure de groupe, ou que la photographie G' la révèle : par suite G' sera également de la forme G' = (**T**', *').

Définitions 4.1 : Un transport ou une photographie f sont appelés des *applications*. Ce qui caractérise avant tout une application, au sens mathématique du terme, est que les trajectoires que suivent au cours de leur transport les éléments t de l'*espace-source* G sont filiformes : la trajectoire issue de t n'arrive qu'en un seul point t' de l'*espace d'arrivée* G' (si on raisonne en termes de transport), encore appelé l'*espace-image* (si on raisonne en termes photographiques). t'= f(t) est l'*image* unique de t, la *photographie*, le *transport*, la *représentation* de t. L'ensemble de ces points t' forme *l'image* de f, Im(f).



Il arrive que f ne transporte qu'une partie F de G : F = D(f) est appelé le *domaine de définition* de f.

Il arrive aussi que la portion de la plaque photographique impressionnée par les rayons issus de G, et formant l'image f(F) = Im(f) de F, soit plus petite que G'.

Il peut advenir également que deux trajectoires distinctes, donc issues de points sources différents, convergent vers le même point de l'espace d'arrivée : f est toujours

surjective sur son image. Si tout point de l'image est le point d'arrivée d'une seule trajectoire provenant de la source, l'application est dite *injective*.

On note également cette application par f : G → G'. Lorsqu'on ne précise pas le domaine de définition de f, on sous-entend que celui-ci est G dans son intégralité.

Les applications les plus utiles sont celles qui respectent autant que faire se peut la structure de l'espace source. Si donc deux éléments de l'espace source peuvent être composés, cette propriété essentielle devra être également celle de leurs images. On dit alors que f est un *morphisme*.

Plus précisément, on dit que l'application f est un *morphisme* de groupes ou encore un *homomorphisme* si, G et G' étant deux groupes d'élément neutre respectif t_n et t'_n, elle respecte la structure de G, en étant compatible avec celle de G', donnée précisée par cette condition : l'image de la composée de deux éléments de G est la composée des images,

$$f(x * y) = f(x) *' f(y).$$

Ceux qui sont familiers avec les espaces vectoriels vont retrouver ici des propriétés connues, dues au fait qu'un espace vectoriel V = (G, **K**) est avant tout un ensemble d'éléments appelés vecteurs qui est structuré en groupe commutatif G. Sur les éléments de ce groupe agit par l'extérieur un ensemble de dilatations algébriques représentées par des nombres, l'ensemble **K** de ces nombres étant structuré en corps.

Un sous-espace vectoriel U = (N, **K**) est avant un sous-groupe N de vecteurs du groupe G, invariant puisque G est commutatif. Le quotient G/N est alors le groupe des vecteurs d'un supplémentaire W de U : p, désignant la *projection* de l'espace V sur le sous-espace W, est un premier exemple de morphisme.

Plus généralement :

Proposition 4.1. *Soit N un sous-groupe invariant du groupe* G, *et* p : G → G/N = K *l'application de projection qui à* x *fait correspondre* N*x. *Alors* p *est un homomorphisme*.

<Preuve : Par construction de G/N, p(x*y) = N*x*y = N*x*N*y = p(x)*p(y) : p est donc un homomorphisme.>

Théorème 4.2. *L'image de l'élément neutre de* G *par un homomorphisme* f *est l'élément neutre de* G'.

<Preuve : Soit $f(t_n) = t'$ l'image de l'élément neutre de G. Par hypothèse $t_n * t_n = t_n$. Par suite $f(t_n * t_n) = f(t_n) = t'$, ou encore $t' *' t' = t'$. Multipliant les deux termes de cette égalité par t'^{-1}, il vient $t' = t_n'$: ainsi $f(t_n) = t'_n$.>

Théorème 4.3. *Le symétrique dans* G'*de* f(t) *est* $f(t^{-1}) = (f(t))^{-1}$.

<Preuve : Cela résulte de ce que $f(t*t^{-1}) = f(t_n) = t'_n = f(t) *' f(t^{-1})$.>

Corollaire 4.4. *Soit* f : G → G' *un homomorphisme entre groupes. L'image* f(G) *de* G *dans* G' *est un sous-groupe de* G'.

<Preuve : On a vu que l'élément neutre t'_n appartient à f(G), ainsi que le symétrique de f(t) quel que soit l'élément t de G. f(G) est contenu dans G' muni de la loi *' qui est associative ; par suite, cette même loi définie sur f(G) est également associative.>

Définition 4.2 : On appelle *noyau* de f l'ensemble N(f) des éléments n de G « perdus » au cours du transport, en ce sens que leurs images f(n) n'ont plus d'effet sur les éléments de G'. Elles ne peuvent qu'être localisées en l'élément neutre de G'. Autrement dit :

$$N(f) = N = \{n \in G \text{ tels que } f(n) = t'_n\}.$$

On emploie souvent la notation allemande Ker(f) pour désigner le noyau : la traduction de noyau en allemand étant « kernel »

Théorème 4.5. *Le noyau de* f , N(f), *est un sous-groupe invariant de* G.

<Preuve : Considérons N(f) = N : t_n lui appartient de par la définition d'un morphisme. Si n et n' appartiennent à N, $f(n) = f(n') = t'_n$, il en est de même pour n*n' puisque, de par la définition d'un morphisme, $f(n*n') = f(n) *' f(n') = t'_n *' t'_n = t'_n$. Le symétrique n^{-1} de n appartient aussi à N pour la même raison. Enfin, la loi de groupe sur G étant associative, elle reste associative sur N. N est donc bien un sous-groupe de G.

Il est invariant car si t est un élément quelconque donné de G, quel que soit l'élément n de N, $t*n*t^{-1}$ a pour image l'élément neutre de G' : calculons en effet $f(t)*'f(n)*'f(t^{-1}) = f(t)*'f(t^{-1})$; or $f(t)*'f(t^{-1}) = f(t*t^{-1}) = f(t_n) = t'_n$. Ainsi $t\,N\,t^{-1} = N$. >

Définition 4.3 : Un morphisme *surjectif*, tout point de l'espace d'arrivée est l'image d'un point au moins de l'espace-source, est quelquefois appelé un *épi-morphisme*, alors qu'un morphisme bijectif est appelé un *isomorphisme* : les groupes sont alors dits *isomorphes*.

Exemples : Un groupe abstrait auquel on donne autant de noms différents que de codages différents, que de sémantiques différentes conduit à obtenir des groupes isomorphes : c'est le cas par exemple des groupes rencontrés au second chapitre.

Un autre exemple d'ensemble de groupes isomorphes est celui formé par le groupe cyclique $\mathbf{C}_m$, le groupe $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}/m$, et le groupe U_m formé par les racines de l'équation $z^m - 1 = 0$.

Il est clair que si f est injective, d'après la définition même de l'injectivité, le noyau se réduit à l'élément neutre de G. Inversement, si ce noyau n'est pas réduit au sous-groupe trivial de G formé de son seul élément neutre, cela veut dire qu'il existe au moins deux trajectoires de transport en provenance d'un élément n de N et d'un élément n' de N qui arrivent en t'_n. Donc si le noyau n'est pas réduit à l'élément neutre de G – familièrement, si le noyau n'est pas nul – alors f ne saurait être injective. Montrons davantage, que si ce noyau est « nul », alors l'application est bien injective.

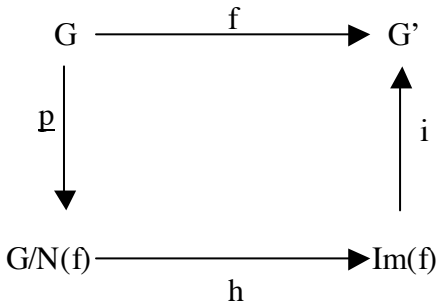
Théorème 4.6. *Le morphisme* $f : G \to G'$ *est injectif si et seulement si son noyau est réduit à l'élément neutre de* G.

<Preuve : On vient de voir que si f est injectif, alors son noyau est réduit à l'élément neutre de G. Réciproquement, raisonnant par l'absurde, supposons qu'on soit dans cette situation, et que f ne soit pas injectif : il existerait alors deux éléments distincts n et n' de G tels que f(n) = f(n') = t. On déduit de cette égalité, notant par $(f(n))^{-1} = t^{-1}$ le symétrique de f(n), que f(n')

*'$(f(n))^{-1}$ = t t^{-1} = t'$_n$. Or par le théorème 4.2, $(f(n))^{-1}$ = $f(n^{-1})$. De la sorte, on a l'égalité f(n') *'$(f(n))^{-1}$ = f(n')*'$f(n^{-1})$ = f(n'* n) = t'$_n$. Elle signifie que n'*n appartient au noyau, lequel est réduit à l'élément neutre de G. Comme ces élément sont distincts, l'un est le symétrique de l'autre. L'hypothèse s'écrit alors f(n) = t = $f(n^{-1})$: mais on a vu que $f(n^{-1})$ est le symétrique de f(n). Or le seul élément f(n) = t égal à son symétrique est l'élément neutre t'$_n$. Par conséquent n et son symétrique appartiennent au noyau, lequel est réduit par hypothèse à l'élément neutre de G ; par conséquent n est égal à son symétrique qui est cet élément neutre, ce qui contredit le fait que n et n' sont distincts.>

Définition 4.4 : Soit A une partie d'un ensemble B. On appelle *insertion* de A dans B l'application i : A → B telle que i(a) = a pour tout élément a de A.

Théorème 4.7. *Le morphisme* f : G → G' *peut être factorisé en* :
- *l'épimorphisme* p : G → G/N(f) *de* G *sur son groupe-quotient* G/N(f)
- *l'isomorphisme* h : G/N(f) → Im (f) *du groupe-quotient sur l'image de* G *par* f
- *l'insertion* i : Im(f) → G'.



<**Preuve :** L'application p : G → G/N(f) est un morphisme de groupe évidemment surjectif, donc un épimorphisme.

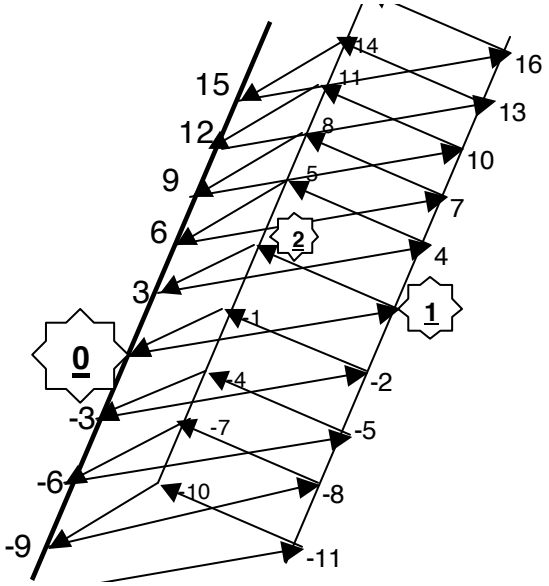
Soit t' l'image d'éléments x et y de G : f(x) = f(y) = t', par conséquent f(x)*'$f(y)^{-1}$ = t'$_n$ = $f(x*y^{-1})$, ce qui signifie que $x*y^{-1}$ appartient au noyau de f, et donc que x et y appartiennent à la même classe N*x = f(x). Il y a donc autant d'éléments images que de classes dans G/N(f). L'application bijective entre groupes h : G/N(f) → Im (f) est donc un isomorphisme. >

Voici un corollaire simple, qui est une reformulation du théorème de Lagrange 3.9 :

Corollaire 4.8. *Soit G est un groupe d'ordre fini et* f : G → G' *un morphisme. L'ordre de G est égal au produit de l'ordre du noyau de* f *par celui de son image.*

4.2 Extension et suite exacte. Produit direct de groupes

Plaçons-nous dans la situation où K = G/N(f). Sauf si le noyau se réduit à l'élément neutre, G est un groupe d'ordre plus élevé que celui de K, dont la structure est par ailleurs induite par celle de G. On dira que G est une *extension* de K *par* N(f), ou encore, nous plaçant d'un point de vue géométrique, que G est un *revêtement* de *base* K et de *fibre* N(f). Si x désigne un élément de K, l'ensemble des éléments n*x où n décrit N(f) forme la *fibre au dessus de* x.



Représentation géométrique des fibres au-dessus des éléments **0**, **1**, **2** de $\mathbf{Z_3}$: chaque fibre est isomorphe à $3\mathbf{Z}$. **Z** est le revêtement universel de $\mathbf{Z_3}$.

Définition 4.5 : Plus généralement, en nous plaçant du point de vue algébrique élaboré à partir de la méthode consistant à créer de nouveaux nombres par le processus d'extension [ ], on dira que le groupe G est une *extension du groupe* K *par le groupe* H, s'il existe un morphisme injectif (monomorphisme) $\underline{i} : H \rightarrow G$ et un morphisme surjectif (épimorphisme) $\underline{p} : G \rightarrow K$ dont le noyau $N(\underline{p})$ est $\underline{i}(H)$. On représente cette extension par le diagramme :

$$H \xrightarrow{\ \underline{i}\ } G \xrightarrow{\ \underline{p}\ } K$$

On dit que la suite de morphismes $(\underline{i}, \underline{p})$ est *exacte*. A partir de cette suite, on peut fabriquer la suite de morphismes appelée *suite exacte courte* :

$$\mathbf{1} \longrightarrow H \xrightarrow{\ \underline{i}\ } G \xrightarrow{\ \underline{p}\ } K \longrightarrow \mathbf{1}$$

Plus généralement, on peut fabriquer des *suites exactes longues* :

$$\mathbf{1} \longrightarrow \ldots H_n \longrightarrow \ldots H_{n-1} \longrightarrow H_{n-2} \ldots \longrightarrow \mathbf{1}$$

où l'image de l'injection précédente est le noyau de l'application suivante.

Le corollaire 4.8 montre qu'un sous-groupe invariant N d'un groupe G permet de décomposer celui-ci en deux parties, N d'une part et G/N d'autre part. Du point de vue ensembliste, l'ensemble **T** des éléments de G est égal au produit cartésien des ensembles d'éléments composant respectivement N et G/N.

Inversement, de manière plus générale, étant donnés deux groupes $G_1 = (\mathbf{T}_1, *_1)$ et $G_2 = (\mathbf{T}_2, *_2)$, d'élément neutre respectif t_{n1}, t_{n2}, est-il possible de construire un groupe $G = (\mathbf{T}, *)$ tel que $\mathbf{T} = \mathbf{T}_1 \times \mathbf{T}_2$? Pour cela, introduisons sur le produit cartésien **T** formé des éléments $t = (t_1, t_2)$, la loi de composition $* = (*_1, *_2)$ définie par :

$$t*t' = (t_1 *_1 t'_1,\ t_2 *_2 t'_2).$$

On note par $G_1 \otimes G_2$ l'ensemble **T** muni de cette loi de composition.

Il est presque immédiat que :

Proposition 4.9. $G = G_1 \otimes G_2$ *est un groupe*.

On peut évidemment entreprendre une telle construction avec un nombre quelconque de groupes $G_i = (\mathbf{T}_i, *_i)$.

Définition 4.6 : On dit alors que G, également noté $G_1 \otimes G_2 \otimes \ldots \otimes G_i \otimes \ldots$, est le *produit direct* des G_i, lesquels sont les *facteurs* de ce produit.

Par cette construction, il est aisé de vérifier que l'injection $\underline{i} : G_1 \rightarrow G$ définie par $\underline{i}(g_1) = (g_1, t_n)$ est un monomorphisme, que la projection $\underline{p} : G \rightarrow G_2$, définie par $\underline{p}(g_1, g_2) = g_2$ est un épimorphisme de noyau $N = \{(g_1, t_n)$ où g_1 parcourt $G_1\}$, et donc que la suite ainsi créée est exacte.

$$G_1 \xrightarrow{\ \underline{i}\ } G = G_1 \otimes G_2 \xrightarrow{\ \underline{p}\ } G_2$$

On peut généraliser quelque peu cette construction en remplaçant G_2 par un groupe qui lui est isomorphe.

Théorème 4.10 *Soit* G *un groupe admettant deux sous-groupes* N *et* H *tels que* N *soit invariant et n'ait en commun avec* H *que l'élément neutre. On suppose également* que G *est l'ensemble des éléments de la forme* n * h, *où* n *appartient à* N, h *à* H. *Alors* G/N *est isomorphe à* H.

<Preuve : Considérons l'ensemble de tous les produits n * h. Il est muni de la loi de composition * du groupe G. Il s'identifie alors au produit direct $N \otimes H$, puisque, de par l'invariance de N, $n * h * n' * h' = n *(h * n' * h^{-1}) * h * h' = n * n'' * h * h'$. Considérons la suite

$$H \xrightarrow{\ \underline{i}\ } G \xrightarrow{\ \underline{p}\ } G/N$$

et l'application $\underline{p} \circ \underline{i} : H \rightarrow G/N$. Comme N est le noyau de $\underline{p}$, et que H et N n'ont en commun que l'élément neutre, le noyau de $\underline{p} \circ \underline{i}$ se réduit à cet élément neutre : cette application est donc injective, et comme G, en tant que produit direct, a autant d'éléments que le produit de ceux de N et de H d'une part N, de ceux de G/N et de N d'autre part par le théorème de Lagrange, H est isomorphe à G/N.>

Exemple élémentaire : Prenons pour G_1 le groupe cyclique $\mathbf{C}_2 = <a, a^2 = t_n>$ et pour G_2 le groupe cyclique $\mathbf{C}_3 = <b, b^3 = t_n>$. Le produit se compose des 6 éléments : (t_n, t_n), (a, t_n), (t_n, b), (t_n, b^2), (a,b), (a, b^2). On pose $(a, b) = r$: alors $r^2 = (t_n, b^2)$, $r^3 = (a, t_n)$, $r^4 = (t_n, b)$, $r^5 = (a, b^2)$, $r^6 = (t_n, t_n) = t_n$: $\mathbf{C}_2 \otimes \mathbf{C}_3$ est isomorphe à $\mathbf{C}_6$.

Plus généralement,

Proposition 4.11 *Si m et n sont premiers entre eux*, $\mathbf{C}_n \otimes \mathbf{C}_m$ *est isomorphe à* $\mathbf{C}_{mn}$.

<Preuve : Identifions d'abord tout groupe cyclique $\mathbf{C}_k$ à $\mathbf{Z}/k$. Son revêtement universel $\mathbf{Z}$ se projette sur lui par une application $\underline{p}_k$ de noyau $k\mathbf{Z}$. Considérons le morphisme $\underline{p} : \mathbf{Z} \rightarrow \mathbf{Z}/n \times \mathbf{Z}/m$, qui associe à l'entier x le couple $(\underline{x}_n, \underline{x}_m)$ où $\underline{x}_n = \underline{p}_n(x)$ (resp. $\underline{x}_m, p_m$) est l'image de x dans $\mathbf{Z}/n$ (resp. $\mathbf{Z}/m$) vérifiant l'égalité : $x = q_n\, n + x_n$ (resp. $x = q_m\, m + x_m$) avec $x_n < n$ (resp. $x_m < m$).

Le noyau de ce morphisme est formé des éléments x à la fois multiples de n et de m. Comme ces nombres sont premiers entre eux, mn est leur plus petit commun multiple. Le noyau est donc $mn\mathbf{Z}$. Or c'est aussi celui de l'application $\underline{p}_{nm}$ de $\mathbf{Z}$ sur $\mathbf{C}_{nm}$. On peut alors introduire l'application $\underline{i} : \mathbf{Z}/nm \rightarrow \mathbf{Z}/n \times \mathbf{Z}/m$ qui à $\underline{x}_{nm}$ fait correspondre $(\underline{x}_n, \underline{x}_m)$: on vérifie immédiatement que $\underline{i}$ est un morphisme, de noyau nul car les applications $\underline{p}_{nm}$, $\underline{p}$ et $\underline{i} \circ \underline{p}_{nm}$ ont même noyau. Par suite $\underline{i}$ est injectif, et comme les deux images de $\mathbf{Z}$ ont même nombre nm d'éléments, elles sont isomorphes.**>**

a et b désignant respectivement des générateurs de $\mathbf{C}_n$ et de $\mathbf{C}_m$, posant r = (a,b), on peut obtenir une preuve constructive de l'énoncé précédent en montrant que les nm puissances successives r^k pour $k \leq nm$ sont les éléments tous distincts de $\mathbf{C}_n \otimes \mathbf{C}_m$ et de $\mathbf{C}_{nm}$. Identifiant a à (a, t_n) et b à (t_n, b), le cas présent résulte alors de la proposition un peu plus générale suivante :

Proposition 4.12 : *Si les éléments* a *et* b *du groupe* G *commutent et sont respectivement d'ordre* n *et* m *premiers entre eux, alors* ab *est d'ordre* nm.

<Preuve : Puisque a et b commutent, $(ab)^{nm} = t_n$. Il s'agit de montrer que nm est le plus petit entier pour lequel cette situation se produit. Supposons donc qu'il existe un entier s tel que $(ab)^s = t_n$. Alors $(ab)^{ns} = a^{ns}\, b^{ns} = t_n$, et donc $b^{ns} = t_n$. L'ordre m de b divise ns, et comme m est premier avec n, il divise s. De même, l'ordre n de a divise s. Par conséquent nm est bien le plus petit entier tel que $(ab)^{nm} = t_n$.**>**

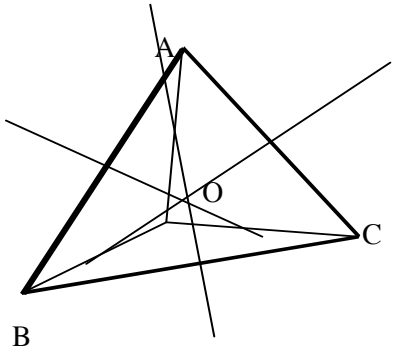
Voici l'exemple simple du cas où m et n ne sont pas premiers entre eux.

Exemple : le groupe diédral $\mathbf{D}_2$ ou *Vierergruppe de Klein* V4 : Ce groupe a été introduit par Cayley en 1834, mais on lui a donné, plus tard, le nom de Klein qui en a montré l'interprétation géométrique. Seul groupe diédral commutatif, $\mathbf{D}_2$ est aussi le produit $\mathbf{C}_2 \otimes \mathbf{C}_2$, formé des quatre éléments : $t_n = (t_n, t_n)$ $\tau = (\tau, t_n)$ $\sigma = (t_n, \sigma)$ et $\kappa = (\tau, \sigma)$. Voici la table de multiplication de ce groupe produit, encore appelé le *Vierergrupe* de Klein :

	t_n	τ	σ	κ
t_n	t_n	τ	σ	κ
τ	τ	t_n	κ	σ
σ	σ	κ	t_n	τ
κ	κ	σ	τ	t_n

Les trois éléments significatifs en sont τ, σ, et κ qui vérifient $\tau^2 = \sigma^2 = \kappa^2 = t_n$. Cette dernière relation constitue donc une présentation du groupe, constitué par trois réflexions.

On peut les représenter simultanément par trois couples de points symétriques autour d'un point central O, et situés sur trois axes se coupant deux à deux à angle droit. Si l'on considère un tétraèdre régulier ABCD, les segments joignant les milieux des couples d'arêtes opposés déterminent par exemple ces trois axes.



Dans l'étude des espaces vectoriels, un certain nombre de propriétés ne font appel qu'à la structure de groupe commutatif des vecteurs. C'est le cas par exemple de la décomposition d'un tel espace en somme et en produit directs. Nous allons donc rester ici dans le cadre simple des groupes commutatifs.

Définition 4.7 : Soient $H_1 = (\mathbf{T}_1, *)$ et $H_2 = (\mathbf{T}_2, *)$ deux sous-groupes d'un groupe commutatif n'ayant en commun que l'élément neutre : $\mathbf{T}_1 \cap \mathbf{T}_2 = t_n$. On appelle *somme directe* de ces deux sous-groupes, le sous-groupe H noté $H_1 \oplus H_2$ engendré par la réunion $\mathbf{T}_1 \cup \mathbf{T}_2$ des éléments de chacun des sous-groupes.

Proposition 4.13. *Soient* $H_1 = (\mathbf{T}_1, *)$ *et* $H_2 = (\mathbf{T}_2, *)$ *deux sous-groupes d'un groupe commutatif n'ayant en commun que leur élément neutre. Leur somme directe est isomorphe à leur produit direct.*

<Preuve : Montrons d'abord qu'existe une bijection $\underline{i}$ entre $H_1 \oplus H_2$ et $H_1 \times H_2$. Soit t un élément de $H_1 \oplus H_2$. Puisque t est engendré par des éléments de H_1 et de H_2, on peut toujours le mettre sous la forme $t = t_1 * t_2$, l'un de ces éléments pouvant être éventuellement l'élément neutre. t définit de la sorte un élément unique $\mathfrak{h} = (t_1, t_2)$ du produit $H_1 \times H_2$. Inversement, supposons que t soit défini par deux éléments $\mathfrak{h} = (t_1, t_2)$ et $\mathfrak{h}' = (t'_1, t'_2)$: on a donc l'égalité $t = t_1 * t_2 = t'_1 * t'_2$, et par conséquent celle-ci : $(t'_1)^{-1} * t_1 = (t_2)^{-1} * t'_2$. Mais $(t'_1)^{-1} * t_1$ est un élément de H_1, alors que $(t_2)^{-1} * t'_2$ appartient à H_2. Le seul élément commun à ces deux sous-groupes étant leur élément neutre, $t_1 = t'_1$, $t_2 = t'_2$. Ainsi t est associé à un seul élément du produit $H_1 \times H_2$.

Vérifions que la bijection $\underline{i} : H_1 \times H_2 \rightarrow H_1 \oplus H_2$ est un morphisme de groupe. Considérons le produit des éléments $\mathfrak{h} * \mathfrak{h}' = (t_1, t_2) * (t'_1, t'_2) = (t_1 * t'_1, t_2 * t'_2)$. Il a pour image l'élément $\underline{i}(\mathfrak{h} * \mathfrak{h}') = (t_1 * t'_1) * (t_2 * t'_2) =$ (de par l'associativité de la loi *) $t_1 * t'_1 * t_2 * t'_2 =$ (de par la commutativité de cette loi) $t_1 * t_2 * t'_1 * t'_2 = (t_1 * t_2) * (t'_1 * t'_2) = \underline{i}(\mathfrak{h}) * \underline{i}(\mathfrak{h}')$. $\underline{i}$ est donc bien un morphisme.>

Voici une autre propriété classique des espaces vectoriels qui ne fait appel qu'à leur structure de groupe commutatif.

Définition 4.8 : Soit $\underline{\pi} : \mathbf{E} \rightarrow \mathbf{E}$ une application d'un ensemble dans lui-même. On dit que $\underline{\pi}$ est une *projection* si $\underline{\pi}\,(\underline{\pi}\,(\mathbf{E})) = \underline{\pi}\,(E)$ - ce qu'on écrit $\underline{\pi} \circ \underline{\pi} = \underline{\pi}$. Soit $\underline{I} : \mathbf{E} \rightarrow \mathbf{E}$ l'application identique : employant la notation additive ici plus simple, notons par $\underline{I} - \underline{\pi}$ l'application définie par $(\underline{I} - \underline{\pi})(t) = \underline{I}(t) + (\underline{\pi}(t))^{-1}$ ($= \underline{\pi}(t)^{-1} * \underline{I}\,(t)$ en notation multiplicative).

Proposition 4.14. *Soit un homomorphisme* $\underline{\pi} : G \rightarrow G$ *où* G *est un groupe commutatif. Les trois propriétés suivantes sont équivalentes* :

1) $\underline{\pi}$ *est une projection*
2) $\underline{I} - \underline{\pi}$ *est une projection*
3) $G = Im(\underline{\pi}) \oplus N(\underline{\pi})$

<Preuve : Montrons que la propriété 1) entraîne la propriété 2) : vérifions que $\underline{I} - \underline{\pi}$ est une projection. Calculons en effet $(\underline{I} - \underline{\pi}) \circ (\underline{I} - \underline{\pi})$: $(\underline{I} - \underline{\pi}) \circ (\underline{I} - \underline{\pi}) = I - \underline{\pi} - \underline{\pi} + \underline{\pi} \circ \underline{\pi} = \underline{I} - \underline{\pi}$.

Inversement, si $(\underline{I} - \underline{\pi}) \circ (\underline{I} - \underline{\pi}) = (\underline{I} - \underline{\pi})$, on a aussi $I - \underline{\pi} - \underline{\pi} + \underline{\pi} \circ \underline{\pi} = \underline{I} - \underline{\pi}$, ce qui entraîne que $\underline{\pi} \circ \underline{\pi} = \underline{\pi}$.

Montrons que la propriété 1) entraîne la propriété 3) : Vérifions d'abord que l'image et le noyau de $\underline{\pi}$ ont l'élément neutre pour seul élément commun. Soit t un autre élément qui leur serait commun. Il appartient à l'image de $\underline{\pi}$, est donc de la forme $t = \underline{\pi}(t')$: $\underline{\pi}$ étant une projection, $\underline{\pi}\,(\underline{\pi}(t')) = \underline{\pi}(t') = t$. Par ailleurs t appartient au noyau, donc $\underline{\pi}(t) = t_n$. La comparaison des deux dernières égalités montre que $t = t_n$.

Par ailleurs, puisque $\underline{I} = \underline{\pi} + (\underline{I} - \underline{\pi})$, $G = Im\,(\underline{\pi}) + Im\,(\underline{I} - \underline{\pi})$. Mais tout élément de l'image de $\underline{I} - \underline{\pi}$ est de la forme $(\underline{I} - \underline{\pi})(t) = \underline{I}(t) - \underline{\pi}(t) = t - \underline{\pi}(t) = t'$, de sorte que $\underline{\pi}(t') = \underline{\pi}(t) - \underline{\pi}(\underline{\pi}(t)) = t_n$. Ainsi l'image de $\underline{I} - \underline{\pi}$ est contenue dans le noyau de $\underline{\pi}$, de sorte que $G = Im\,(\underline{\pi}) + N\,(\underline{\pi})$: G est somme directe de ces deux sous-groupes, et d'après le théorème précédent, en est aussi le produit direct.

Supposons pour terminer la dernière condition vérifiée. D'après ce que nous venons de voir, elle s'écrit aussi : $t = (\underline{I} - \underline{\pi})(t) + \underline{\pi}(t)$. On en déduit que $\underline{\pi}(t) = \underline{\pi}(\underline{I}(t) - \underline{\pi}(t)) + \underline{\pi}\,(\underline{\pi}(t))$. Or on a vu que $\underline{\pi}(\underline{I}(t) - \underline{\pi}(t)) = t_n$, et par conséquent $\underline{\pi}(t) = \underline{\pi}(\underline{\pi}(t))$.>

4.3 Produit semi-direct

4.3.1 Les automorphismes d'un groupe

Un groupe G étant donné, on peut coder ses éléments de différentes façons sans pour cela changer la structure du groupe. C'est ce qu'accomplit toute bijection de G sur lui-même qui est également un morphisme.

Définition 4.9 : Un isomorphisme d'un groupe avec lui-même est appelé un *automorphisme*.

Un cas très simple d'isomorphisme déjà rencontré est celui d'un sous-groupe N sur lui-même $\underline{t} : N \mid\rightarrow N$ qui le laisse invariant : pour un tel sous-groupe, l'application $\underline{t}\,(N) = N$ est définie à partir d'un élément t du groupe de sorte que $N = t^{-1} * N * t$.

De manière plus générale, l'application $\underline{t} : g \mid\rightarrow t^{-1} * g * t$ définit un automorphisme particulier de G, appelé un *automorphisme intérieur*. Vérifions en effet que $\underline{t}(g * g') = \underline{t}(g) * \underline{t}(g')$ c'est-à-dire que :

$$(t^{-1} * g * t) * (t^{-1} * g' * t) = t^{-1} * (g * g') * t\ .$$

C'est une conséquence immédiate du fait que la loi de composition est associative.

Les automorphismes d'un groupe G forment eux-mêmes un groupe Aut(G). Les automorphismes intérieurs en forment un sous-groupe. Bien sûr, si G est commutatif comme l'est un groupe cyclique, ce sous-groupe est le groupe trivial.

Proposition 4.15 : *Soit* $\mathbf{C}_m$ *un groupe cyclique et* $\underline{a}$ *un automorphisme de ce groupe engendré par* r. *Alors* $\underline{a}$(r) *est un autre générateur du groupe*.

<**Preuve** : Soit $t_n, r, r^2 \ldots, r^{m-1}$ les éléments du groupe, et r' = $\underline{a}$(r). Puisque $\underline{a}$ est une bijection, les éléments $\underline{a}(r^k)$ sont tous distincts et sont les éléments du groupe cyclique. Comme $\underline{a}$ est un morphisme, $\underline{a}(r^2) = \underline{a}(r)\ \underline{a}(r) = r'^2$ et donc plus généralement $\underline{a}(r^p) = r'^p$. Les éléments du groupe sont donc de la forme $t_n, r', r'^2 \ldots, r'^{m-1}$: ainsi r' engendre le groupe.>

De là vient que si $\underline{a}$ et $\underline{a}$' sont deux automorphismes distincts, les images $\underline{a}$(r) et $\underline{a}'$(r) devant être distinctes, il y a autant d'automorphismes que d'élément générateurs de $\mathbf{C}_m$. Il résulte alors du théorème 3.4 le

Corollaire 4.16 : Aut($\mathbf{C}_m$) *est un groupe d'ordre* φ(m).

Exemple : Le groupe cyclique $\mathbf{C}_3$ est engendré par r et par r^2. On convient que r définit l'automorphisme identique t_n :

$$t_n : \mathbf{C}_3 (t_n, r , r^2) \rightarrow \mathbf{C}_3 \ (t_n, r , r^2).$$

La substitution de r par r^2 définit l'automorphisme :

$$\underline{r} : \mathbf{C}_3 (t_n, r , r^2) \rightarrow \mathbf{C}_3 \ (t_n, r^2 , r = r^{4(\mathrm{mod}3)}).$$

Voyons ce que devient $\underline{r}(\mathbf{C}_3)$ quand on lui applique encore $\underline{r}$:

$$\underline{r} : \underline{r}(\mathbf{C}_3) (t_n, r^2 , r) \rightarrow \mathbf{C}_3 \ (t_n, r , r^2).$$

Ainsi :

$$\underline{r} \circ \underline{r} = t_n : \mathbf{C}_3 (t_n, r , r^2) \rightarrow \mathbf{C}_3 \ (t_n, r , r^2),$$

et par conséquent Aut($\mathbf{C}_3$) a même structure que le groupe primordial.

3 est un nombre premier, et lorsque p est premier, tout nombre qui lui est inférieur est premier avec lui, de sorte que φ(p) = p – 1. Dans ce cas,

Proposition 4.17 : *Si* p *est premier*, Aut($\mathbf{C}_p$) *est un groupe cyclique d'ordre* p - 1.

<**Preuve** : Puisque p est premier, $\mathbf{C}_p$ est engendré par r, r^2, …, r^{p-1}, et donc Aut($\mathbf{C}_p$) est formé des éléments $\underline{a}_i$ tels que $\underline{a}_1(r) = r$, $\underline{a}_2(r) = r^2$, …, $\underline{a}_k(r) = r^k$, …, $\underline{a}_{p-1}(r) = r^{p-1}$. Par suite l'automorphisme $\underline{a}_k$ tel que $\underline{a}_k(r) = r^k$, et par conséquent tel que $\underline{a}_k(r^n) = r^{kn\ (\mathrm{mod}(p-1))}$, vérifie également $\underline{a}_k(\underline{a}_q(r)) = \underline{a}_k(r^q) = r^{kq(\mathrm{mod}(p-1))} = \underline{a}_{kq(\mathrm{mod}(p-1))}(r)$. En posant $\underline{a}_1 = t_n$, $\underline{a}_2 = \underline{r}$, on a donc $\underline{a}_3 = \underline{r}^2$, etc, $\underline{r}^{p-1} = t_n$.>

Soit alors $\mathbf{C}_n$ un autre groupe cyclique d'ordre n. On peut considérer un morphisme α: $\mathbf{C}_n \rightarrow$ Aut($\mathbf{C}_m$). Autrement dit, si t est une rotation du groupe cyclique $\mathbf{C}_n$, α(t) est un

automorphisme de $\mathbf{C}_m$, donc ce même groupe mais dans un ordre particulier de présentation de ses éléments, spécifié par $\alpha(t)$.

Prenons par exemple $\mathbf{C}_2$, ses éléments sont l'élément neutre t_n et la réflexion ρ. Le groupe des automorphismes de $\mathbf{C}_4$ est isomorphe à $\mathbf{C}_3$ par la proposition précédente. Un morphisme α envoie $\mathbf{C}_2$ sur un sous-groupe de $\mathbf{C}_3$ ayant au plus deux éléments.

Si r'est un élément de $\mathbf{C}_m$, notons $\theta(t)(r') = t *_\theta r' = r'^\circ$ son image par $\theta(t)$. On remarquera que si $t = t_n$, son image par θ est l'automorphisme neutre, et donc $\theta(t_n)(r') = r'$.

Associé à θ et par son intermédiaire, on peut alors définir un produit entre $\mathbf{C}_n$ et $\mathbf{C}_m$. Soit d'abord (t, r) et (t', r') deux éléments de $\mathbf{C}_n \times \mathbf{C}_m$. On définit ainsi leur produit *« tordu »* par θ :

$$(t, r) \times_\theta (t', r') = (tt', r\, r'^\circ) = (tt', r\,(t *_\theta r')).$$

En prenant t et r comme générateurs respectivement de $\mathbf{C}_n$ et de $\mathbf{C}_m$, le produit « tordu » ou *semi-direct* de ces deux groupes, $\mathbf{C}_n \times_\theta \mathbf{C}_m$, est donc défini à partir de tous les couples (t^i, r^j) où $i = 1, 2, \ldots, n$, et $j = 1, 2, \ldots, m$.

On remarquera que $(t_n, r) \times_\theta (t, t_n) = (t, r)$. Par suite, en posant $(t, t_n) = \mathfrak{t}$ puis $(t_n, r) = \mathfrak{r}$, $(t^i, r^j) = \mathfrak{t}^i \times_\theta \mathfrak{r}^j$ peut être identifié au produit standard $t^i r^j$.

Par ailleurs, prenons pour $t\, r = r^p t$.

Remarquons que G s'identifie presque au produit direct N x H, puisque, de par l'invariance de N, $n * h * n' * h' = n *(h * n' * h^{-1}) * h * h' = n * n'' * h * h'$. Le presque vient de ce que on a dû écrire n'' au lieu de n.

Puisque $n'' = h * n' * h^{-1}$, la transformation $\underline{h} : n' \mapsto n'' = \underline{h}(n')$ est un automorphisme intérieur de N qui dépend de h. Soit alors $\alpha : H \to \mathrm{Aut}(N)$ l'application qui à h fait correspondre l'automorphisme $\underline{h}$. On peut alors écrire :

$$n'' = \underline{h}(n') = \alpha(h)(n').$$

Soit g est un autre élément de H. A l'élément g * h, est associé le produit :

$$n * (g * h) * n' * h' = n * (g * h) * n' * (h^{-1} * g^{-1}) * (g * h) * h' =$$

$$n * (g * (h * n' * h^{-1}) * g^{-1}) * g) * h * h' = n * (g * n'' * g^{*\,-1}) * h * h'$$

d'où l'on déduit que $\alpha(g * h)(n') = \alpha(g)(n'') = \alpha(g)(\alpha(h)(n')) = [\alpha(g) \circ (\alpha(h)](n')$: ainsi, l'application α est un morphisme de H, muni de la loi *, dans Aut (N) muni de la loi de composition des automorphismes.

Cette construction permet d'étendre ainsi la notion de produit direct de deux groupes :

Définition 4.15 : Soient $N = (\mathbf{T}_N, *_N)$ et $H = (\mathbf{T}_H, *_H)$ deux groupes, et un morphisme $\alpha : H \to \mathrm{Aut}(N)$. On appelle *produit semi-direct* de H par N relativement à α, $N \times_\alpha H$, l'ensemble $\mathbf{T}_N \times \mathbf{T}_H$ muni de la loi de composition * définie par :

$$(n, h) * (n', h') = (n *_N \alpha(h)(n'), h *_H h').$$

CHAPITRE V

LE GROUPE DES PERMUTATIONS

LES GROUPES RÉSOLUBLES

5.1 Une nouvelle généralisation du groupe primordial : le groupe des permutations

Le groupe primordial se rapporte à l'échange de places entre deux pions, opération qui porte le nom de permutation. Le jeu de cache-cache suggère d'entreprendre l'étude des échanges de place entre plusieurs acteurs.

On remarquera qu'un tel échange de place n'est autre qu'un bijection entre les éléments de l'ensemble **E** de ces acteurs. Par conséquent, l'ensemble $\mathbf{\Sigma}_n$ des échanges de places est également celui de l'ensemble des bijections de **E** sur **E**. Il possède la structure de groupe, avec pour loi de composition la composition entre bijections : il est nécessaire mais facile de vérifier la présence des propriétés structurales de cet ensemble.

Définition 5.1 : $\mathbf{\Sigma}_n$ est appelé le *groupe symétrique d'indice* n.

Proposition 5.1 $\mathbf{\Sigma}_n$ e*st un groupe d'ordre* n !.

<Preuve : La démonstration se fait facilement par récurrence. Il n'y a qu'une manière de placer un pion, deux manières de placer les deux pions N et S : soit on place N en premier, soit on place N en second. Les deux pions N e t S étant placés, on en ajoute un troisième P : on peut le placer en trois positions possibles, représentée chacune sur le dessin suivant par un ovale grisé :

Supposons alors qu'on ait montré qu'il a (n-1)! manières de placer n-1 pions. Considérons un ensemble de n pions : il est (n-1) ! manières de placer les n-1 premiers pions, et pour chacune de ces manières, le dernier pion peut être placé n façons. Le nombre de manières de placer les n pions est donc n(n-1) ! = n ! .>

Le groupe symétrique est le groupe le plus riche qu'on puisse établir sur un nombre fini d'éléments. Aussi comprend-on que Cayley, au dix-neuvième siècle, ait pu montrer que :

Théorème 5.2 (Cayley) *Tout groupe fini est un sous-groupe d'un groupe symétrique*.

Une bijection σ de $\mathbf{\Sigma}_n$ est précisée par ses valeurs en chaque élément de **E**. On présente le tableau de ces valeurs sous cette forme :

$$\sigma = \begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}$$

Les symboles de la ligne du haut peuvent être considérés comme des objets placés dans un ordre naturel donné. Les symboles de la ligne du bas peuvent être alors considérés comme les positions occupés par ces objets après leur permutation sous l'effet de σ.

Exemples 1 : On peut ainsi décrire $\mathbf{\Sigma}_2$ par :

$$\sigma_n = \begin{bmatrix} 12 \\ 12 \end{bmatrix} \quad \tau_{12,2} = \begin{bmatrix} 12 \\ 21 \end{bmatrix}$$

Prenons l'exemple du cas où n = 3. $\mathbf{\Sigma}_3$ a pour éléments :

$$\sigma_n = \begin{bmatrix} 123 \\ 123 \end{bmatrix} \quad \tau_{12,3} = \begin{bmatrix} 123 \\ 213 \end{bmatrix} \quad \tau_{23,3} = \begin{bmatrix} 123 \\ 132 \end{bmatrix} \quad \tau_{31,3} = \begin{bmatrix} 123 \\ 321 \end{bmatrix} \quad \gamma = \begin{bmatrix} 123 \\ 231 \end{bmatrix} \quad \sigma = \begin{bmatrix} 123 \\ 312 \end{bmatrix}$$

Que peut-on déduire de l'observation de l'objet $\mathbf{\Sigma}_3$?

1) Le couple de bijections $(\sigma_n, \tau_{12,3})$ laisse invariant 3, et possède la même structure que le couple de bijections $(\sigma_n, \tau_{12,2})$.

Ainsi, le couple de bijections $(\sigma_n, \tau_{12,3})$ forme un sous-groupe de $\mathbf{\Sigma}_3$, en correspondance bijective avec les éléments du groupe $\mathbf{\Sigma}_2$ dont il partage la même structure : les deux groupes sont isomorphes.

2) Par simplicité, nous allons maintenant souvent écrire τ_{ij} au lieu de $\tau_{ij,3}$, et plus généralement de $\tau_{ij,n}$. Considérons la composée de τ_{12} avec τ_{23}, $\tau_{12}\ \tau_{23}$ en adoptant ici la convention que l'on effectue les compositions en partant de la droite vers la gauche.

(**N.B.** : de manière générale, la composition (ou produit) des permutations

$\begin{bmatrix} a_1 a_2 \ldots a_n \\ b_1 b_2 \ldots b_n \end{bmatrix}$ et $\begin{bmatrix} b_1 b_2 \ldots b_n \\ c_1 c_2 \ldots b_n \end{bmatrix}$ est la permutation $\begin{bmatrix} a_1 a_2 \ldots a_n \\ c_1 c_2 \ldots c_n \end{bmatrix}$).

L'objet I étant en position 1, l'objet II étant en position 2, l'objet III étant en position 3, la permutation

$\tau_{23} = \begin{bmatrix} 123 \\ 132 \end{bmatrix}$ laisse I invariant, place en position 2 l'objet III, et en position 3 l'objet II:

$$\tau_{23}(1) = 1$$
$$\tau_{23}(2) = 3$$
$$\tau_{23}(3) = 2$$

Le nouvel ordre des objets est I, III, II. On fait agir sur cette nouvelle disposition la permutation $\tau_{12} = \begin{bmatrix} 123 \\ 213 \end{bmatrix}$. Son effet est de placer en première position l'objet qui occupe la seconde position après la première permutation de place, c'est-à-dire l'objet III ; au total : (3 → 1). Cette seconde permutation laisse invariante l'objet en position 3 après la première permutation, et qui est l'objet II ; au total : (2 → 3) . Enfin l'objet I qui était en première position est astreint à occuper la seconde position (1 → 2). En résumé, $\tau_{12}\,\tau_{23} = \begin{bmatrix} 123 \\ 231 \end{bmatrix} = \gamma$.

On trouve aussi par exemple que $\tau_{23}\,\tau_{12} = \sigma$, que $\tau_{23}\,\tau_{12}\,\tau_{23} = \tau_{23}$, $\gamma = \tau_{12}\,\tau_{23}\,\tau_{12}$, et naturellement que $(\tau_{23})^2 = (\tau_{12})^2 = (\tau_{31})^2 = \sigma_n$.

Ainsi la composition entre elles des transpositions permet-elle d'obtenir tous les éléments du groupe.

Plus généralement et plus précisément :

Théorème 5.3 *Le groupe* $\mathbf{\Sigma}_n$ *est engendré par les* n-1 *transpositions* $\tau_{ii+1,n}$ $1 \leq i \leq n\text{-}1$.

<Preuve : Montrons tout d'abord, par récurrence, que les transpositions $\tau_{ij,n}$ engendrent le groupe. C'est le cas du groupe $\mathbf{\Sigma}_2$ qui se réduit à l'élément neutre et à la transposition $\tau_{12,2}$. Supposons maintenant que cette proposition soit vraie pour tout ensemble de cardinal inférieur ou égal à n-1. Considérons une bijection σ telle que $\sigma(n) = n$. Par l'hypothèse de récurrence, la restriction de σ au sous-ensemble {1, 2, …, n-1} est un produit de transpositions $\tau'_{ij,n-1}$. Posons $\tau_{ij,n} = \tau'_{ij,n-1}$ où i et j sont inférieurs ou égaux à n-1, et $\tau_{nn,n}(n) = n$. Alors σ est le produit de ces transpositions. Si $\sigma(n) = n' < n$, la permutation $\tau_{nn',n} \circ \sigma = \sigma'$ laisse n invariant : elle s'écrit donc comme un produit de transpositions, de même par conséquent que la permutation $\sigma = \tau_{nn',n} \circ \sigma'$.

Montrons maintenant qu'il suffit de prendre en compte les seules transpositions $\tau_{ii+1,n}$ $1 \leq i \leq n\text{-}1$ pour engendrer le groupe. Il suffit également pour cela de montrer que toute transposition peut être obtenue de cette manière. Soit τ_{pq} une telle transposition. Le résultat est

une tautologie si q = p+1. Supposons le résultat prouvé pour $\tau_{p(p+k)}$ avec k ≤ q-1. Alors la propriété est vraie pour τ_{pq} puisque $\tau_{pq} = \tau_{(q-1)\,q} \circ \tau_{p(q-1)} \circ \tau_{(q-1)\,q}$.>

5.2 Une généralisation intermédiaire de la notion de transposition : la notion de cycle

Reprenons le groupe primordial qui se rapporte aux échanges de place entre deux pions nommés ici P_1 et P_2 : la transposition τ envoie le pion P_1 en position 2, le pion P_2 en position 1. Nous allons généraliser ce mécanisme.

Exemple 2 : Soit trois pions, nommés P_1, P_2 et P_3. Le transport de P_1 en position 2, de P_2 en position 3, de P_3 en position 1 est une permutation particulière γ appelée une *permutation circulaire* ou un *cycle d'ordre* 3. Elle s'interprète comme la permutation :

$$\gamma = \begin{bmatrix} 1\,2\,3 \\ 2\,3\,1 \end{bmatrix}.$$

Définition 5.2 : On appelle *permutation circulaire* ou *cycle de longueur* ou *d'ordre* k sur un ensemble ordonné de positions **E** = {1, 2, …, k} une permutation γ : **E** → {1, 2, …, k} telle que $\gamma(i) = i + 1_{(\mathrm{mod}\ k)}$. Elle est donc la permutation :

$$\begin{bmatrix} 1 & 2 & .... & k-1 & k \\ 2 & 3 & ... & k & 1 \end{bmatrix}$$

On la note :

$$\gamma = [1, 2, \ldots, k].$$

Composons-la p fois avec elle-même :

$$\gamma^p = \begin{bmatrix} 1 & 2 & ... & k-p & k-p+1 & ... & k-1 & k \\ p+1 & p+2 & ... & k & 1 & ... & k-p-1 & k-p \end{bmatrix}$$

On a également, $\gamma^{k-1}(1) = k$, $\gamma^k(1) = 1 = t_n(1)$: γ engendre un groupe cyclique d'ordre k. On peut remarquer qu'on aboutit en position k à la suite de k-1 transpositions successives $\tau_{i(i+1)}$.

Plus généralement, soit **E** un ensemble ordonné de n positions p_i. Un *cycle d'ordre* k est une permutation qui laisse invariant n-k positions, et permute circulairement les k autres $p_1, p_2, \ldots, p_k$. L'ensemble de ces éléments transformés par le cycle en forme le *support*.

On note le cycle par la liste des éléments soumis à la permutation circulaire : on part du premier objet p_1 selon l'ordre naturel qui sera soumis à la permutation. On le fait suivre sur la liste par le symbole p_2 de sa position après la permutation : $p_2 = \gamma(p_1)$. Plus généralement, p_i sera suivi de $p_{i+1} = \gamma(p_i)$. L'écriture de la liste prend fin avec le terme p_k pour lequel $p_1 = \gamma(p_k)$: de la sorte, le cycle $\gamma = \begin{bmatrix} p_1, p_2, \ldots, p_k \\ p_2, p_3, \ldots, p_1 \end{bmatrix}$ est noté $[p_1, p_2, \ldots, p_k]$.

$$\text{Si } \gamma = [1, 2, \ldots, k], \text{ alors } \gamma^{-1} = [1, k, k\text{-}1, \ldots, 3, 2].$$

En effet, si $\gamma = \begin{bmatrix} 1 & 2 & .. & k-1 & k \\ 2 & 3 & ... & k & 1 \end{bmatrix}$ et si $\gamma^{-1} = \begin{bmatrix} 1 & 2 & ... & k-1 & k \\ k & 1 & .. & k-2 & k-1 \end{bmatrix}$, alors :

$$\gamma^{-1}(\gamma(1)) = \gamma^{-1}(2) = 1, \ldots, \gamma^{-1}(\gamma(k)) = \gamma^{-1}(1) = k.$$

Exemples : 1) Si $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{bmatrix}$

le cycle γ noté [1 5 3], permute circulairement ces éléments mais laisse invariant tous les autres.

Soit alors, plus généralement, $\mathbf{C}_\gamma$ le groupe cyclique engendré par γ. Si la position i appartient au cycle, alors son orbite par l'action du groupe est le cycle tout entier. Si i n'appartient pas au cycle, il est invariant par γ par définition du cycle.

2) La transposition τ_{12} appliquée à l'ensemble {1, 2, 3} n'est autre que le cycle [1 2], de même que la transposition τ_{23} n'est autre que le cycle [2 3] : alors le produit $\tau_{12}\,\tau_{23}$ n'est autre que le cycle σ de l'exemple 1 :

$$[1\ 2]\ [2\ 3] = [1\ 2\ 3].$$

On écrira plus généralement : **[i j] [j k] = [i j k].**

3) De la même façon, on vérifiera que [1 2] [3 4] = [1 2 3] [2 3 4] = $\begin{bmatrix} 1234 \\ 2143 \end{bmatrix}$.

Plus généralement, puisque **[j k] [j k]** est l'identité :

$$\textbf{[i j] [k l] = [i j] [j k] [j k] [k l] = [i j k] [j k l]}.$$

4) Considérons maintenant la permutation :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}$$

L'examen de cet exemple fait apparaître la présence de deux cycles : d'une part le cycle précédent γ = [1 3 2], d'autre part le cycle d'ordre 2, τ = [4 5]. On remarque que : ces deux cycles sont disjoints, ils commutent, σ = [1 3 2] [4 5], en est le produit.

Lemme 5.4 *Deux cycles à supports disjoints commutent.*

<Preuve : Soient γ et γ' deux cycles disjoints. Si k n'appartient ni au support de γ ni à celui de γ', il reste invariant tant par γ que par γ', et par conséquent $\gamma(\gamma'(k)) = \gamma'(\gamma(k)) = k$. Si k n'appartient pas au support de γ' mais à celui de γ, alors $\gamma'(k) = k$ et $\gamma(\gamma'(k)) = \gamma(k)$ lequel

appartient au support de γ, disjoint de celui de γ' : par conséquent $\gamma'(\gamma(k)) = \gamma(k)$. L'interversion des rôles de γ et de γ' n'altère pas le résultat.>

Théorème 5.5 *Une permutation* σ *se décompose d'une manière unique à l'ordre près en cycles disjoints commutant deux à deux.*

<Preuve : Soit σ une permutation agissant sur l'ensemble **E**. Considérons les trajectoires des divers éléments de cet ensemble sous l'action de σ. On trouve celles qui sont réduites à un seul élément : ce sont les éléments de **E** invariants par σ. Considérons une trajectoire Γ_t dans **E** non réduite à un élément : elle est définie par le groupe monogène engendré par σ, et un élément t de cette trajectoire. k désignant un élément quelconque de **E**, on pose $\gamma_\Gamma(k) = \sigma(k)$ si k appartient à la trajectoire, $\gamma_\Gamma(k) = k$ sinon. On a défini ainsi un cycle. Les trajectoires étant disjointes et formant une partition de **E**, on définit ainsi de manière unique autant de cycles disjoints que de trajectoires. Leur composition reconstitue σ.>

Proposition 5.6 *Le groupe* $\mathbf{\Sigma}_n$ *est engendré par les cycles* $\tau = [1\ 2]$ et $\gamma = [1\ 2\ \ldots\ n]$.

<Preuve : Par le théorème 5.3, il suffit de montrer que toute transposition τ_{ij} est engendrée par τ et γ. On remarque en effet que :

$\gamma\ \tau\ \gamma^{-1} = [2\ 3], \gamma\ [2\ 3]\ \gamma^{-1} = [3\ 4], \ldots,$
$[1\ 2]\ [2\ 3]\ [1\ 2] = [1\ 3], \ldots, [1\ k]\ [k\ \ k+1][1\ k] = [1\ \ k+1], \ldots$
$[1\ p]\ [1\ q][1\ p] = [p\ q].$>

5.3 Signature d'une permutation

Plaçons nos pions sur les bornes kilométriques d'une route. Ces bornes forment un ensemble qu'on peut identifier à celui **Z** des entiers. Soient x_i et x_j deux telles bornes. Soit deux cavaliers Porthos et d'Artagnan, encore nommés i et j. x_j (respectivement x_i) est la borne atteinte par j (respectivement par i). Si x_j marque 15 et x_i 10, $x_j - x_i = 5$ indique l'avance de d'Artagnan sur Porthos. Si les positions sont inversées, on aura alors $x_i - x_j = -5$. Ainsi, la transposition τ_{ij} se traduit par un changement de signe du monôme $x_j - x_i$.

Considérons maintenant une permutation σ de $\mathbf{\Sigma}_n$. Par le théorème 5.1, elle est le produit de transpositions $\tau_{i(i+1)}$. On va donc d'abord adjoindre à l'ensemble $\mathbf{E} = \{1, 2, \ldots, n\}$ des cavaliers, le polynôme $S(x_1, x_2, \ldots, x_n)$ associé aux transpositions possibles entre couples ordonnés de cavaliers. Plus précisément :

$$S(x_1, x_2, \ldots, x_n) = \prod_{i<j} (x_j - x_i).$$

Ce produit est calculé pour tous les couples (i, j) tels que $1 \leq i < j \leq n$.

Lemme 5.7 *Soit* τ *une transposition et le polynôme* $S^\tau(x_1, x_2, \ldots, x_n) = \prod_{i<j} (x_{\tau(j)} - x_{\tau(i)})$. *Son signe est opposé à celui de* $S(x_1, x_2, \ldots, x_n)$.

<Preuve : Examinons l'effet d'une transposition τ_{pq} $(p < q)$ sur l'ensemble des indices des variables du polynôme :

- les monômes de la forme $x_j - x_i$, où i comme j sont différents de p et q, sont inchangés

- les binômes de la forme $(x_k - x_p)\ (x_k - x_q)$ où $k > q$ deviennent $(x_k - x_q)\ (x_k - x_p)$: il sont invariants
- il en est de même pour les binômes de la forme $(x_p - x_k)\ (x_q - x_k)$ où $k < p$.
- les binômes de la forme $(x_k - x_p)\ (x_k - x_q)$ où $p < k < q$ restent également invariants
- par contre seul le monôme $x_q - x_p$ devient $x_p - x_q = -\ (x_q - x_p)$.>

Théorème 5.8 *Il existe un épimorphisme* ε *et un seul de* $\mathbf{\Sigma}_n$ *sur* $\mathbf{SO}(1)$ *tel que* $\varepsilon(\tau) = -\ 1$ *pour toute transposition* τ.

<Preuve : Soit $\varepsilon : \mathbf{\Sigma}_n \rightarrow \mathbf{SO}(1)$ une application du groupe symétrique dans le groupe des rotations du cercle $\mathbf{C}^0$, qui, à toute permutation σ, fait correspondre le signe $\varepsilon(S^\sigma) = \varepsilon(\sigma)$ du polynôme :

$$S^\sigma(x_1, x_2, \ldots, x_n) = \prod_{i<j} (x_{\sigma(j)} - x_{\sigma(i)}).$$

Par le lemme précédent, $\varepsilon(\tau) = -\ 1$ pour toute transposition τ.

Supposons que σ est une permutation quelconque. Par le théorème 5.1, elle est un produit de m transpositions : $\sigma = \tau_m\ \tau_{m-1} \ldots \tau_1$, de sorte que $S^\sigma = S^{\tau_m\ \tau_{m-1} \cdots\ \tau_1} = (S^{\tau_1})^{\tau_m\ \tau_{m-1} \cdots\ \tau_2}$. Par suite $\varepsilon(\sigma) = (-1)^m$.

Si maintenant on considère deux permutations $\sigma = \tau_m\ \tau_{m-1} \ldots \tau_1$ et $\sigma' = \tau'_{m'}\ \tau'_{m'-1} \ldots \tau'_1$, la permutation produit s'écrit :

$$\sigma'' = \sigma\ \sigma' = \tau_m\ \tau_{m-1} \ldots \tau_1\ \tau'_{m'}\ \tau'_{m'-1} \ldots \tau'_1,$$

de sorte que :

$$\varepsilon(\sigma\ \sigma') = \varepsilon(\sigma'') = (-1)^{m+m'} = (-1)^m\ (-1)^{m'} = \varepsilon(\sigma)\ \varepsilon(\sigma').$$

L'application ε est donc bien un épimorphisme.>

On remarquera que le signe de S^σ ne dépendant que de σ, il est alors indépendant du nombre de transpositions nécessaire pour obtenir σ, et par suite ce nombre de transpositions est toujours soit pair, soit impair.

Définition 5.3 : $\varepsilon(\sigma)$ est appelé la *signature* de σ. Elle est dite *paire* lorsque $\varepsilon(\sigma) = 1$, *impaire* lorsque $\varepsilon(\sigma) = -1$.

Une remarque :

Proposition 5.9 σ *et* σ^{-1} *ont même signature*.

<Preuve : En effet, σ et σ^{-1} sont engendrées par le même nombre de transpositions.>

Proposition 5.10 *Soit* σ *une permutation de* $\mathbf{\Sigma}_n$ *produit de* r *cycles disjoints* : $\varepsilon(\sigma) = (-1)^{(n-r)}$.

<Preuve : Soit $\gamma = [a_1\ a_2 \ldots a_k]$ un cycle de longueur k : γ est le produit de $k - 1$ transpositions :

$$\gamma = [a_1\ a_2]\ [a_2\ a_3]\ \ldots [a_{k-1}\ a_k].$$

Il est donc de signature $(-1)^{(k-1)}$. Par suite $\varepsilon(\sigma) = (-1)^{\Sigma\,(k-1)} = (-1)^{(n-r)}$.>

5.4 Le (sous-)groupe alterné $\mathbf{A}_n$

La somme de deux nombres pairs étant un nombre pair, le sous-ensemble des permutations « paires » de signature 1 forme un sous-groupe $\mathbf{A}_n$ du groupe symétrique $\mathbf{\Sigma}_n$.

Définition 5.4 : $\mathbf{A}_n$ est appelé le *n-ième groupe alterné*, ou *groupe alterné de degré* n.

En voici trois propriétés importantes.

Proposition 5.11 $\mathbf{A}_n$ *possède* n !/2 *éléments*.

<Preuve : Soit $\mathbf{I}_n$ l'ensemble des permutations impaires. On sait que toute permutation σ s'écrit comme un produit de transpositions : $\sigma = \tau_m \tau_{m-1} \dots \tau_1$.

Si elle est impaire, alors $\sigma' = \tau_{m-1} \dots \tau_1$ est paire. Si elle est paire, alors $\sigma' = \tau_{m-1} \dots \tau_1$ est impaire : par suite, la correspondance entre $\mathbf{A}_n$ et I_n est bijective.>

Proposition 5.12 $\mathbf{A}_n$ *est engendré par les cycles d'ordre* 3.

<Preuve : Les permutations d'ordre pair sont engendrées par des transpositions en nombre pair. Pour montrer notre assertion, il suffit alors de vérifier que le produit d'un couple quelconque de transpositions s'écrit comme un produit de 3-cycles. En effet, comme on l'a vu dans le second exemple, ce produit de deux transpositions quelconques est de la forme : soit [i j] [k l], équivalent au produit [i j k] [j k l], soit [i j] [j k], équivalent au produit [i j k]. >

Proposition 5.13 $\mathbf{A}_n$ *est un sous-groupe invariant de* $\mathbf{\Sigma}_n$.

<Preuve : Utilisons la définition de l'invariance d'un sous-groupe : $\mathbf{A}_n$ sera invariant si quelle que soit la permutation σ et l'élément a de $\mathbf{A}_n$: σ a σ^{-1} est aussi un élément de $\mathbf{A}_n$. σ et σ^{-1} ayant même signature, la signature de σ a σ^{-1} est paire : cet élément appartient donc à $\mathbf{A}_n$.>

Comme le nombre d'éléments de $\mathbf{A}_n$ est moitié moindre que celui de $\mathbf{\Sigma}_n$, le groupe quotient $\mathbf{\Sigma}_n/\mathbf{A}_n$ n'a que deux éléments, il est donc isomorphes au groupe singulier primordial $\mathbf{\Sigma}_2$. On a donc la suite exacte :

$$\mathbf{1} \longrightarrow \mathbf{A}_n \xrightarrow{i} \mathbf{\Sigma}_n \xrightarrow{p} \mathbf{\Sigma}_n/\mathbf{A}_n \longrightarrow \mathbf{1}$$

Exemple géométrique : les symétries du tétraèdre régulier

5.4 Les groupes résolubles

Avec les groupes finis dont l'ordre est un nombre premier, nous avons rencontré des groupes sans sous-groupes invariants autres que les sous-groupes triviaux. Ils sont donc de structure interne particulièrement simple. De manière générale,

Définition 5.4 : On appelle *groupe simple* un groupe dont les seuls sous-groupes invariants sont ses sous-groupes triviaux.

A l'inverse, l'exemple du groupe dihédral $\mathbf{D}_4$ nous montre l'existence de deux sous-groupes invariants commutatifs, $\mathbf{\Sigma}_4$ et $\mathbf{\Sigma}_2$, lequel est un sous-groupe de $\mathbf{\Sigma}_4$. La généralisation

immédiate de cet exemple conduit à considérer des groupes possédant une suite $N_1, N_2, \ldots, N_k$ de sous-groupes invariants et commutatifs tels que :

$$\mathbf{1} \subset N_k \subset N_{k-1} \subset \ldots \subset N_1 \subset G.$$

Plus généralement, on écarte la contrainte de commutativité pour aboutir à la :

Définition 5.5 : On appelle *résolution* d'un groupe G une suite N_i de sous-groupes invariants emboîtés de sorte que :

$$\mathbf{1} \subset N_k \subset N_{k-1} \subset \ldots \subset N_1 \subset G.$$

Les groupes-quotients N_i/N_{i+1} sont appelés les *groupes-quotients* de la résolution. Si ces quotients sont commutatifs, le groupe G est dit *résoluble*.

Le théorème suivant joue un rôle essentiel dans la théorie de la résolution des équations polynomiales, élaborée par Evariste Galois autour des années 1830. Il permet de montrer que les équations polynomiales de degré supérieur à 4 ne sont pas en général résolubles par radicaux. La condition pour qu'un tel polynôme admette des racines exprimables sous la forme de radicaux est que le groupe de permutations qui conserve les valeurs des fonctions symétriques des racines égales aux coefficients du polynôme soit résoluble. Bien que Galois n'en ait établi qu'une version encore restrictive, il a montré que $\mathbf{A}_5$ était le plus petit groupe simple non commutatif, lui attribuer la paternité de ce théorème est amplement mérité.

Théorème 5.14 (Galois) *Si* $n \geq 5$, $\mathbf{\Sigma}_n$ *n'est pas résoluble*.

<<Preuve : Elle se fait par l'absurde, en supposant que $\mathbf{\Sigma}_n$ est résoluble. On va montrer sous cette condition les lemmes suivants :

Lemme 5.15 : *Soit* N (=N_{i+1}) *un sous-groupe invariant d'un groupe quelconque* G (= N_i). *Le quotient* G/N *est commutatif si et seulement si* N *contient le dérivé* D(G) *de* G, *l'ensemble de tous les commutateurs* $x * y * x^{-1} * y^{-1}$ *de* G.

<Preuve : Soit x et y deux éléments de G. Par hypothèse, leur commutateur $x * y * x^{-1} * y^{-1}$ est dans N. Soit p la projection de N sur son groupe-quotient G/N. Son noyau étant N,

$$p(x * y * x^{-1} * y^{-1}) = \underline{t}_n = p(x) * p(y) * p(x^{-1}) * p(y^{-1}) = \underline{x} * \underline{y} * \underline{x}^{-1} * \underline{y}^{-1},$$

d'où l'on déduit que $\underline{x} * \underline{y} = \underline{y} * \underline{x}$, en d'autres termes G/N est commutatif.

Réciproquement, si G/N est commutatif, en écrivant à l'envers la suite des égalités précédentes, on en déduit que $x * y * x^{-1} * y^{-1}$ appartient à N.>

Lemme 5.16 *Supposons que, avec* $n \geq 5$, $\mathbf{\Sigma}_n$ *contienne un sous-groupe invariant* N_{i+1} *du sous-groupe invariant* N_i, *de sorte que* N_i *contienne tous les* 3*-cycles et que* N_i/N_{i+1} *soit commutatif, alors* N_{i+1} *contient également tous les* 3*-cycles*.

< Preuve : Rappelons le contenu du lemme 5.15 : N_{i+1} étant un sous-groupe invariant d'un groupe quelconque N_i , le quotient N_i/N_{i+1} est commutatif si et seulement si N_{i+1} contient le sous-groupe dérivé $D(N_i)$ formé par les commutateurs de N_i.

Soit alors, tel que $\mathbf{A}_n$, N_i un sous-groupe invariant contenant les 3-cycles de $\mathbf{\Sigma}_n$. Puisque $n \geq 5$, on peut prendre cinq éléments distincts quelconques de $\mathbf{\Sigma}_n$: i, j k, r, s, auxquels on associe les 3-cycles :

$$x = [ijk] \text{ et } y = [krs].$$

Alors

$$x\ y\ x^{-1}\ y^{-1} = [ijk]\ [krs]\ [ikj]\ [ksr] = [irk] \quad (G).$$

Tous les éléments de la forme $x\ y\ x^{-1}\ y^{-1}$ sont donc des 3-cycles, ils appartiennent à N_i par hypothèse, et les éléments i, j, k etc étant quelconques distincts, on obtient bien également par ce procédé tous les 3-cycles. Ils appartiennent également à N_{i+1} car N_i/N_{i+1} étant commutatif, N_{i+1} contient tous les commutateurs de N_i. Ainsi N_{i+1} est également constitué de tous les 3-cycles.>

Ainsi, le fait que N_i contienne tous les 3-cycles entraîne que N_{i+1} les contient également. Alors, il en sera de même pour N_{i+2}, etc, et donc pour le dernier maillon de la chaîne, à savoir le sous-groupe trivial **1**, ce qui est bien évidemment impossible : l'hypothèse de résolubilité de $\mathbf{\Sigma}_n$ ne tient pas .>>