

CHASSE AUX GROUPES FINIS

1) AVEC UN REVOLVER A BOUCHON *

Les groupes finis sont cette année à l'honneur. Une extraordinaire aventure mathématique se déroule depuis un siècle et plus spécialement depuis 1955. Elle vient d'aboutir à la connaissance et à la classification de tous les groupes finis.

L'aspect acrobatique de l'exploit apparaît lorsqu'on apprend qu'il a fallu, pour y parvenir, maîtriser quelques géants: le groupe simple de Janko (découvert en 1966) ne contient que 175.560 éléments, mais celui de Conway (1968) en comporte 4.157.776.806.543.360.000.

A partir d'une liste de groupes "simples", on peut reconstituer tous les groupes finis: on annonce en 1981 que l'on connaît désormais la liste exhaustive de tous les groupes finis simples.

Nous avons demandé à Paul BOREL, assistant à l'U.L.P. de nous raconter cette épopée. Notre collègue a fait un effort pédagogique très efficace, et bien des non-spécialistes tireront profit de son article. *

Mais il serait dommage que quelques détails techniques effarouchent trop de lecteurs: après tout, lorsque nous nous informons sur la greffe du coeur ou sur les satellites artificiels dans les revues de vulgarisation, nous acceptons d'avoir une vue d'ensemble sans saisir toutes les finesses.

Pour faciliter l'accès à l'article de Paul BOREL, nous avons décidé de raconter quelques faits, concernant les groupes finis, qui ont leur place dans l'enseignement primaire et secondaire.

* Dans le prochain numéro de l'Ouvert, paraîtra un article de Paul BOREL qui chasse le groupe fini avec des armes moins rudimentaires.

Sur les permutations

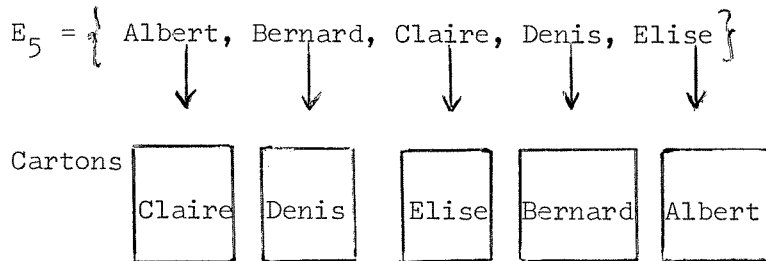
Soit E_n un ensemble de n objets.

L'ensemble de toutes les bijections de E_n sur E_n s'appelle le groupe des permutations de E_n , ou encore le groupe symétrique S_n . Il comporte $n!$ éléments.

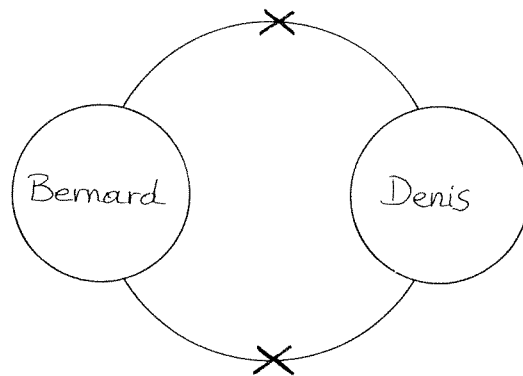
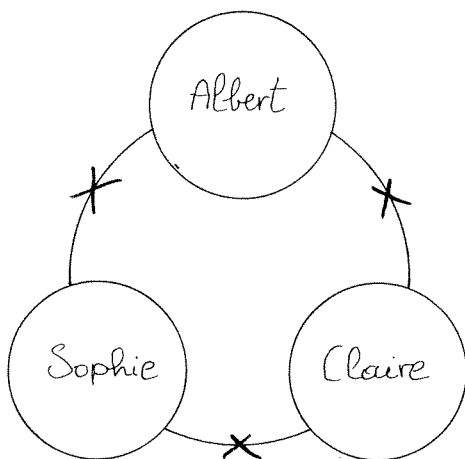
Georges PAPY a imaginé quelques manipulations qui ont été essayées dans des classes primaires [P] pour décrire des permutations.

Par exemple, il choisit un ensemble E_n d'élèves, auxquels il distribue des cartons vierges. Chacun inscrit son nom sur le carton. On ramasse, on bat le jeu et l'on redistribue les cartes:

Voici un exemple pour $n=5$.



Papy demande alors à chacun de ces élèves de saisir avec sa main droite la main gauche du camarade dont le nom figure sur le carton. Mais avant de le faire, on interroge la classe pour prévoir ce qui va arriver. Certains comprennent tout de suite qu'on obtiendra d'abord des farandoles, mais bientôt quelqu'un affirme: "Ca va faire des rondes".



En termes savants, on arrive au

Théorème : Toute permutation d'un ensemble fini se décompose en cycles (I_3)

Remarque : Il peut arriver qu'un enfant reçoive le carton qui porte son propre nom. (C'est alors un point fixe de la permutation). Parfois, un cycle ne comprend que deux éléments (comme ici $\{ \text{Bernard, Denis} \}$). C'est alors une transposition .

Une autre façon concrète de se représenter une permutation est d'envisager un dérangement. Par exemple, dans une bibliothèque, il y a exactement n livres avec des emplacements choisis pour chacun d'eux. Malheureusement, ils sont actuellement disposés en pagafe.

Une méthode assez longue, mais curieuse, de les remettre en place est la suivante: on choisit un livre mal rangé et on le transpose avec le livre qui occupe indûment sa place. On répète l'opération autant de fois qu'il le faut.

Mais comme après chaque transposition, le nombre des livres bien rangés a augmenté d'une unité, on parviendra finalement à un rangement complet.

Théorème : Toute permutation de n objets est composée d'un nombre fini de transpositions (cf. (I_3)).

Ce mode de rangement peut s'effectuer de nombreuses façons, mais on peut prouver que le nombre de transpositions nécessaires est toujours de même parité: cela permet de distinguer les permutations paires des impaires.

Définition : le sous-groupe alterné A_n de S_n est constitué par les $\frac{1}{2} \times n!$ permutations paires .

Les groupes finis considérés comme groupes de transformation

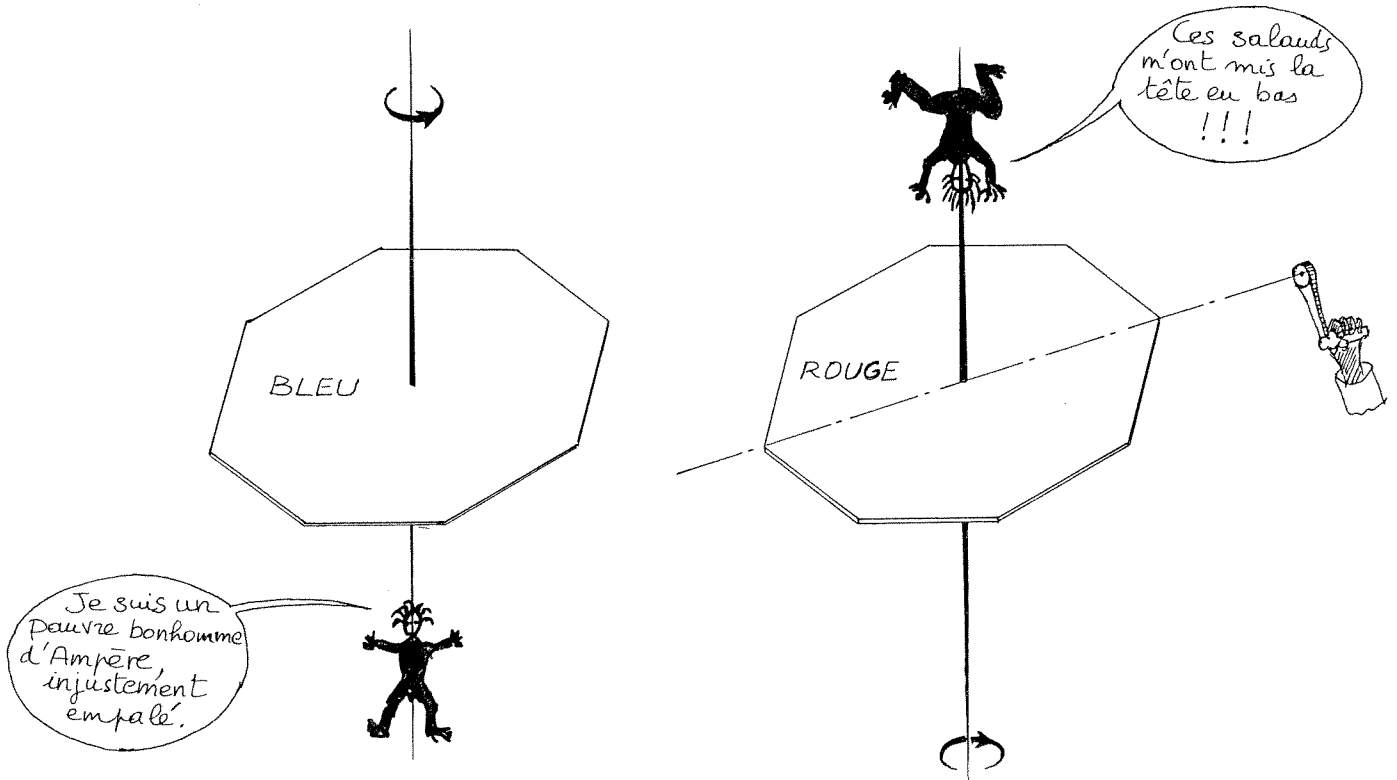
On peut munir E_n de structures supplémentaires et étudier le sous-groupe de \mathcal{J}_n formé par les bijections d'un ensemble de n éléments qui respecte cette structure.

Exemple : \mathcal{J}_8 possède $8! = 40.320$ éléments. Mais on peut identifier E_8 à l'ensemble des sommets d'un cube et chercher le groupe des 48 isométries de l'espace qui conservent le cube. Parmi celles-ci, il y a 24 isométries directes **[B]**.

On peut aussi identifier E_8 à l'ensemble des sommets d'un octogone régulier, découpé dans du carton, dont les faces sont colorées différemment.

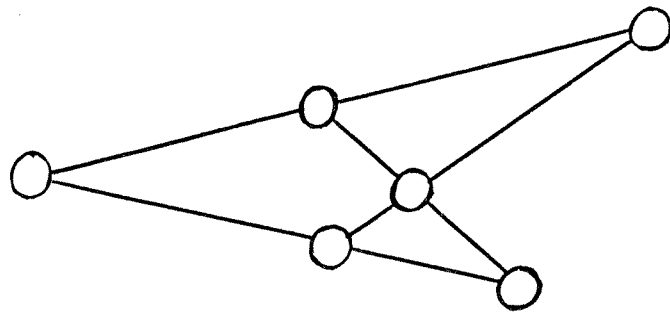
Le groupe diédral D_8 est le groupe des isométries directes qui conservent ce carton.

Il y a 8 permutations "circulaires" obtenues sans retourner le carton, mais le groupe diédral D_8 comporte aussi des isométries qui échangent la couleur des faces.



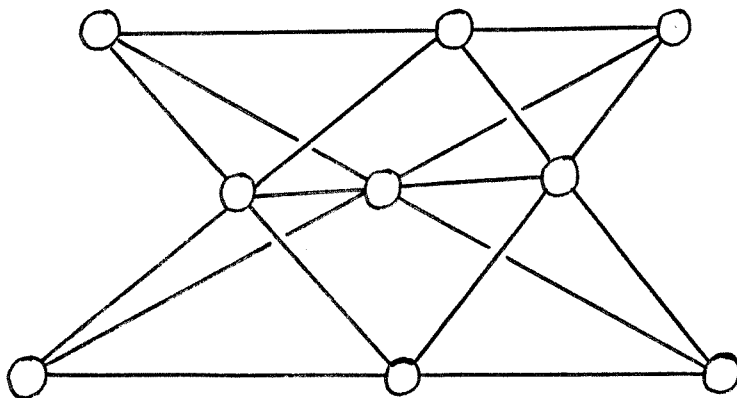
Ce sont les 8 demi-tours effectués autour d'un des 8 axes de symétrie situés dans le plan de l'octogone.

On lira dans $[I_6]$, le récit d'une manipulation effectuée en CE_2 , sur les 24 bijections du quadrilatère complet, qui conservent les alignements.



Il s'agissait de transporter de toutes les façons possibles six jetons disposés sur les cases de la marelle ci-dessus, sur une marelle analogue, en respectant les alignements.

J'ai moi-même expérimenté, avec des étudiants du DEUG, au cours de 4 séances de deux heures chacune, l'étude des 108 bijections conservant les alignements dans la figure de Pappus ci-dessous:



Signalons enfin, le célèbre groupe de Klein. C'est celui que Dagobert manipula jadis, lorsqu'à côté de la façon triviale I de mettre sa culotte à l'endroit, il étudia les trois façons a, b, c de la retourner. Ce groupe, dont voici la table de Pythagore:

	I	a	b	c
I	I	a	b	c
a	a	I	c	b
b	b	c	I	a
c	c	b	a	I

est aussi le groupe des isométries directes qui conservent la figure de l'espace formée de trois droites concourantes deux à deux perpendiculaires.

Usage des sous-groupes pour "dévisser" un groupe

Tant que le cardinal d'un groupe n'est pas trop élevé, il est possible de l'étudier directement, (par exemple sur sa table de Pythagore). Mais pour les groupes plus "gros", on a besoin de relais.

Ainsi on cherchera à classer les éléments du groupe en classes d'équivalence. Celles-ci, pour être utiles, devraient avoir des liens étroits avec la structure du groupe étudié.

Soit Γ un sous-groupe de G.

Définition : On dira que deux éléments a et b de G, sont équivalents (modulo Γ) si le produit $a \times b^{-1}$ appartient à Γ .

C'est précisément parce que Γ est un groupe, que l'on obtient ainsi une relation d'équivalence. Et Γ lui-même est la classe des éléments de G équivalents à l'élément neutre (la transformation identique).

L'étude de l'ensemble-quotient G/Γ rend parfois de grands services pour l'étude de G , mais malheureusement, il n'est pas toujours possible de le munir naturellement d'une structure de groupe. En général, si $a \equiv a' \pmod{\Gamma}$ et $b \equiv b' \pmod{\Gamma}$, il n'est pas toujours vrai que $a \times b \equiv a' \times b' \pmod{\Gamma}$.

S'il n'en est pas ainsi, on ne peut pas composer des classes d'équivalence. Evariste GALOIS a attiré l'attention sur les sous-groupes distingués Γ qui définissent des groupes-quotient. Ils sont caractérisés par la propriété suivante:

$$\left\{ \forall a \in G \quad \forall b \in \Gamma \quad aba^{-1} \in \Gamma \right\}$$

Dès que l'on connaît un sous-groupe distingué Γ de G , on peut ramener l'étude de G à celle de deux groupes moins "gros".

Γ et G/Γ .

Exemple. Soit \mathbb{Z}_6 le groupe additif des entiers modulo 6. C'est un groupe commutatif. Par conséquent, tous ses sous-groupes sont distingués (car $aba^{-1} = b$).

$\mathbb{Z}_6 = \{ \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5} \}$ (la classe $\underline{6}$ est identique à la classe $\underline{0}$).

Considérons les deux sous-groupes suivants : $\{ \underline{0}, \underline{3} \}$ et $\{ \underline{0}, \underline{2}, \underline{4} \}$

On vérifie qu'ils sont respectivement isomorphes à \mathbb{Z}_2 et \mathbb{Z}_3 .

Inversement, considérons le groupe produit $\mathbb{Z}_2 \times \mathbb{Z}_3$ dont les éléments sont des couples (a, b) où a est une classe d'entiers modulo 2 et b une classe d'entiers modulo 3.

La composition de (a, b) et de (a', b') s'obtient, dans $\mathbb{Z}_2 \times \mathbb{Z}_3$ en ajoutant indépendamment les coordonnées : (les premiers modulo 2 et les derniers modulo 3).

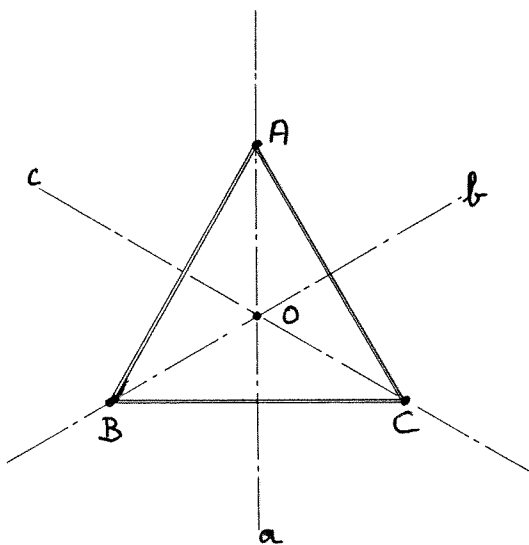
On vérifie alors que \mathbb{Z}_6 et $\mathbb{Z}_2 \times \mathbb{Z}_3$ sont isomorphes comme le montre la bijection suivante:

\mathbb{Z}_6	<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>
	↕	↕	↓			
$\mathbb{Z}_2 \times \mathbb{Z}_3$	(<u>0</u> , <u>0</u>)	(<u>1</u> , <u>2</u>)	(<u>0</u> , <u>1</u>)	(<u>1</u> , <u>0</u>)	(<u>0</u> , <u>2</u>)	(<u>1</u> , <u>1</u>)

Autre exemple

Considérons le groupe diédral D_3 , qui compte 6 éléments. Il s'identifie à \mathcal{F}_3 (mais ceci ne vaut plus aux ordres plus élevés).

On peut l'incarner dans le groupe G des isométries qui laissent invariant un triangle équilatéral ABC.



Si r est la rotation de $2\pi/3$ autour de O, si S_a, S_b, S_c sont les retournements par rapport aux médianes a, b, c, on a:

$$* G = \{ 1, r, r^2, S_a, S_b, S_c \},$$

1 désignant l'identité

* $\Gamma = \{ 1, r, r^2 \}$ est le sous-groupe des rotations de G, isomorphes à \mathbb{Z}_3 selon :

$$\underline{k} \longmapsto r^k$$

o	1	r	r ²	S _a	S _b	S _c
1	1	r	r ²	S _a	S _b	S _c
r	r	r ²	1	S _c	S _a	S _b
r ²	r ²	1	r	S _b	S _c	S _a
S _a	S _a	S _b	S _c	1	r	r ²
S _b	S _b	S _c	S _a	r ²	1	r
S _c	S _c	S _a	S _b	r	r ²	1

$\Gamma \simeq \mathbb{Z}_3$

Il est facile de voir que Γ est distingué dans G .
 Il faut prouver que, quel que soit $g \in G$, quel que soit
 $j \in \Gamma$, on a :

$$g \gamma g^{-1} \in \Gamma$$

C'est évident si g est aussi une rotation, un produit de rotations en étant une. Si g est un retournement, $g\gamma g^{-1}$ est le produit de 3 isométries dont deux impaires et une paire. $g\gamma g^{-1}$ est par conséquent paire. C'est donc une rotation, élément de Γ .

En conséquence, Γ est distingué dans G , et du même coup, \mathbb{Z}_3 l'est dans S_3 (*)

Par contre, $\{1, Sa\}$, $\{1, Sb\}$, $\{1, Sc\}$, tous isomorphes à \mathbb{Z}_2 sont des sous-groupes de G non distingués. Par exemple, $r \circ Sa \circ r^{-1} = Sb$. Plus généralement, les transformations de G permutent entre eux ces sous-groupes (ils sont dits conjugués), mais ne les conservent pas.

Le groupe quotient G/Γ (le seul qu'on puisse construire) est isomorphe à \mathbb{Z}_2 , et on peut le considérer comme le groupe des permutations des deux côtés du plan où est dessiné le triangle.

"Dévissage" et "revissage" d'un groupe fini

Supposons que G possède au moins un sous-groupe distingué Γ (distinct de G et du groupe trivial réduit à l'identité). Alors l'étude de G peut se ramener à celle des deux groupes plus "petits", Γ et G/Γ . On peut essayer de continuer le même processus sur ces deux derniers groupes, et poursuivre. On est arrêté lorsqu'on aboutit à un groupe simple, c'est-à-dire à un groupe qui n'a pas de sous - groupes distingués, non triviaux.

Par exemple, il en est ainsi pour \mathbb{Z}_p où p est un nombre premier. Parmi les autres groupes simples (dont l'énumération se trouvera dans l'article de Borel), citons les groupes alternés \mathcal{A}_n avec

(*) \mathbb{Z}_n est sous-groupe distingué de D_n , (et non de S_n) sauf pour $n=2$ et 3 .

$n \geq 5$, et aussi les groupes de Janko et Conway cités au début de cet article. \mathcal{A}_5 est aussi isomorphe au groupe des isométries directes d'un icosaèdre régulier.

On peut toujours poursuivre le "dévissage" d'un groupe fini en sous-groupes simples. Inversement, on connaît la solution du problème suivant, appelé problème d'extension des groupes :

Problème Etant donné deux groupes Γ et H , trouver un groupe G tel que :

- 1° Γ soit isomorphe à un sous-groupe distingué de G
- 2° H soit isomorphe au quotient G/Γ

Il existe une solution facile de ce problème, qui consiste à choisir pour G le groupe produit $\Gamma \times H$.

Mais il existe, en général d'autres solutions, et l'on sait les obtenir toutes.

Exemple A partir de $\Gamma = \mathbb{Z}_8$ et $H = \mathbb{Z}_2$, nous avons déjà obtenu le groupe non commutatif D_8 . On peut aussi obtenir les groupes commutatifs: $\mathbb{Z}_{16}, \mathbb{Z}_8 * \mathbb{Z}_2$ qui ne sont pas isomorphes, car le premier contient un élément d'ordre 16 (par exemple, $\underline{1}$), alors que tous les éléments du second sont d'ordre 8 au plus.

Autre exemple

A partir de \mathbb{Z}_3 et \mathbb{Z}_2 , nous avons déjà obtenu $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ qui est commutatif.

Le groupe du triangle, isomorphe à S_3 , est aussi fabriqué, comme on l'a vu, avec $\Gamma \cong \mathbb{Z}_3$ et des groupes isomorphes à \mathbb{Z}_2 . Mais il n'est pas commutatif !

Il est pourtant possible de reconstituer G à partir de $\Gamma \cong \mathbb{Z}_3$ et, par exemple, de $H = \{1, Sa\} \cong \mathbb{Z}_2$. La construction ne pourra pas se faire par produit direct, puisque ce procédé fournirait \mathbb{Z}_6 commutatif.

La construction à mettre en oeuvre est celle de produit semi-direct, qui fournit une autre solution au problème d'extension.

Cette méthode s'applique lorsque le groupe H opère sur Γ .

Cela signifie qu'à tout élément h de H , correspond un automorphisme φ_h de Γ , tel qu'au produit $h.h'$ de deux éléments de H correspond le composé des automorphismes φ_h et $\varphi_{h'}$.

On peut alors définir sur l'ensemble $\Gamma \times H$ la loi de composition suivante, notée $*$, alors que le point. est réservé aux groupes H et Γ

$$(\gamma, h) * (\gamma', h') = (\gamma \cdot \varphi_h(\gamma'), h \cdot h').$$

C'est la loi du produit semi-direct "tordue" grâce à φ .

Si φ_h n'est pas constamment réduit à l'automorphisme identique de Γ , le produit semi-direct diffère du groupe produit.

Cette construction s'applique en particulier si H et Γ sont tous les deux des sous-groupes d'un groupe Ω plus grand où Γ est en outre distingué. On peut alors choisir pour tout $h \in H$ φ_h égal à l'automorphisme intérieur de Γ défini ainsi :

$$\varphi_h: \gamma \longmapsto h \cdot \gamma \cdot h^{-1}.$$

C'est ce qui arrive, dans l'exemple précédent, avec $\Omega = \mathbb{Z}_3$, $\Gamma = \mathbb{Z}_3$ et $H = \{1, Sa\} \simeq \mathbb{Z}_2$.

On notera l'analogie (et les différences) entre le dévissage des groupes finis et les problèmes classiques suivants:

- décomposition d'un entier naturel en produit de facteurs premiers
- décomposition d'une fraction rationnelle en éléments simples
- analyse et synthèse d'un corps chimique pur en éléments simples.

Dans ce dernier cas, comme avec les groupes simples, l'analyse de deux corps purs isomères peut conduire à la même analyse brute, sans que la synthèse aboutisse au même produit final.

Evoquons encore deux thèmes auquel l'article de Borel fera allusion.

Les corps finis .

Les corps infinis les plus communs sont \mathbb{Q} , \mathbb{R} et \mathbb{C} . On en fabrique d'autres à partir des corps de fractions rationnelles à une ou plusieurs variables. (Il existe aussi des corps infinis non commutatifs, dont le plus célèbre est le corps des quaternions, découverts par le mathématicien irlandais Hamilton en 1843).

Par contre, un célèbre théorème de Wedderburn affirme que "tout corps fini est commutatif".

Evariste Galois a trouvé tous les corps finis.

Théorème : pour chaque exposant entier $n \geq 1$ et chaque nombre premier p , il existe un corps fini (et un seul à un isomorphisme près) à p^n éléments.

Si $n = 1$, on trouve les corps des entiers modulo p (où p est premier) On trouvera, dans **[I₆]** (p. 92 et 93) des énoncés d'exercices qui fournissent une construction des corps de Galois à 4 et à 9 éléments.

Les groupes de Lie

En contraste avec les groupes finis, la mathématique contemporaine étudie beaucoup les groupes dont les éléments dépendent continuellement de plusieurs paramètres, réels ou complexes.

Ce sont les groupes introduits par le mathématicien norvégien Sophus Lie (1842-1899).

Les exemples les plus faciles à imaginer sont des groupes dont les éléments sont des matrices carrées.

Le groupe linéaire $GL(n)$ s'identifie au groupe multiplicatif des matrices carrées $n \times n$, dont le déterminant n'est pas nul.

(Pour qu'une matrice admette un inverse, il faut et il suffit que son déterminant diffère de 0). Chaque matrice dépend de n^2 paramètres.

Tous les groupes de transformation de la géométrie, (groupe affine, groupe orthogonal, groupe projectif, etc... etc...) dérivent de celui-ci, et s'introduisent implicitement dans l'enseignement secondaire.

Ainsi le groupe des déplacements du plan euclidien est un groupe de Lie dont le sous-groupe des translations est un sous-groupe distingué.

Autre exemple

Il est possible de présenter, dans l'enseignement secondaire (à partir de la 3ème ou la 2ème), le groupe des transformations affines de la droite, à titre d'exercice de calcul.

A tout couple de nombres réels (a, b) où $a \neq 0$, on associe l'application affine de \mathbb{R} sur \mathbb{R} , définie par

$$x \longmapsto ax + b$$

Calculons le composé des applications correspondant à (a, b) et (a', b') . On obtient :

$$x \longmapsto a'(ax+b) + b' = aa'x + (a'b + b').$$

Donc $(a', b') \circ (a, b) = (aa', a'b + b')$.

Muni de cette loi de composition, l'ensemble des transformations affines de la droite \mathbb{R} est un groupe de Lie non commutatif. Ces transformations dépendent de deux paramètres réels a et b .

Ce groupe est isomorphe au groupe des matrices $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$, muni de la

multiplication usuelle.

On remarquera qu'on obtient des groupes finis, lorsqu'on choisit les coefficients (a, b) (avec $a \neq 0$) dans un corps fini. Il est instructif de le faire, en utilisant le corps des entiers modulo 3.

Cette analogie des groupes de Lie avec les groupes finis, conduit à envisager des groupes de matrices, qui sont des groupes de Lie lorsque les coefficients sont pris dans \mathbb{R} ou \mathbb{C} et qui deviennent des groupes finis lorsque les coefficients sont pris dans un corps de Galois.

Après ce petit tour d'horizon élémentaire, nous interrompons traditionnellement le feuilleton par :
La suite au prochain numéro .

G. GLAESER.

Bibliographie

- [B] BUDDEN (F.J.), La fascination des groupes, Paris O.C.D.L., 1970.
- [I₃] IREM DE STRASBOURG, Livre du Problème, fascicule 3, La Parité, CEDIC
- [I₆] IREM DE STRASBOURG, Livre du Problème, fascicule 6, La Géométrie d'incidence, CEDIC
- [P] PAPY (G.), Groupes, Paris, Dunod, 1961

. Responsable de la publication

J. LEFORT

24 rue A. Schweitzer

WINTZENHEIM 68000 COLMAR.

. Impression

IREM de Strasbourg

10 rue du général Zimmer

67034 STRASBOURG Cedex