Des **e**xponentielle**s** contin**U**es dans la théorie des ensembles de **Z**ermelo-**F**raenkel avec axiome du choix dépendant

Alain **W**azner

Préliminaires sur la théorie des groupes

Un théorème d'isomorphisme de la théorie des groupes

Lemme 1 : Si N et H sont deux sous-groupes et si H est un sous-groupe distingué de G alors $NH = \{nh/n \in N,\ h \in H\} = HN$ et c'est un sous-groupe de G dont H est un sous-groupe distingué.

Preuve : Si $n \in N$, $h \in H$ alors $nh = nhn^{-1}n$ est le produit de $nhn^{-1} \in H$ par $n \in N$ et donc $NH \subset HN$.

$hn = hnh^{-1}h$ est le produit de $hnh^{-1} \in N$ par $h \in H$ et donc $HN \subset NH$.

Le neutre e de G est aussi celui de H et de N et la relation $e = ee$ entraîne que $e \in NH$.

Soient à présent $n' \in N$, $h' \in H$ alors $hnh'n' = hnh'n^{-1}nn'$ est le produit de $h \in H$ par $nh'n^{-1} \in H$ et par $nn' \in N$: il appartient donc à HN.

L'inverse de hn est $n^{-1}h^{-1} = n^{-1}h^{-1}nn^{-1}$ c'est le produit de $n^{-1}h^{-1}n \in H$ par $n^{-1} \in N$: il appartient donc à HN.

HN est alors un sous-groupe de G car contenant son neutre et étant stable pour l'opération de groupe et par inversion de ses éléments. H est distingué dans G donc si $h \in H$, $g \in G$ alors $g^{-1}hg \in H$, cette inclusion est à fortiori vraie pour

$g \in NH \subset G$: H est donc distingué dans NH.

Théorème :Soit G un groupe et H, N deux sous-groupes distingués de G, alors

$$(N \simeq G/H) \Rightarrow N \supset H$$

Preuve : puisque G/H est isomorphe à N, il existe un morphisme $\Psi : G \to N$ de noyau H, le dit premier théorème d'isomorphisme de la théorie des groupes conclut à l'existence d'un isomorphisme $\overline{\Psi}$: $\begin{cases} G/H & \to & N \\ gH & \mapsto & \overline{\Psi}(gH) \end{cases}$ avec $\overline{\Psi}(gH) \overset{déf}{=} \Psi(g)$.

Si F est un sous-groupe distingué de G alors on a bien défini une action de groupe de G sur G/F par $h.gF \overset{déf}{=} hgF$ $(\forall h, g \in G)$ puisque si e est le neutre de G alors

$$e.gF = egF = gF$$

$$k.h.gF = k.hgF = khgF = (kh).gF$$

$\forall s \in G$, *$\omega(sF)$ l'orbite de sF est G/F* : Puisque $\omega(sF) = \{g.sF/g \in G\} = \{gsF/g \in G\}$ soit $\{g'F/g' \in G\} = G/F$ (Où on a posé $g' = gs$).

G_{sF} le fixateur de sF est F :

G_{sF} est l'ensemble $\{g \in G/g.sF = sF\}$, lequel

est $\{g \in G / gsF = sF\}$. Si $gsF = sF$ alors $gse = gs \in gsF = sF$ donc $\exists f \in F$, $gs = sf$ et $g = sfs^{-1} \in F$ puisque F est un sous-groupe distingué de G.
Réciproquement si $g \in F$ alors

$$g.sF = gsF = gFs = Fs = sF$$

puisque F est un sous-groupe distingué de G et $gF = F$, $\forall g \in F$.
La bijection $\left\{\begin{array}{lll} G/G_{sF} & \to & \omega(sF) \\ gG_{sF} & \mapsto & g.sF \end{array}\right.$ est le morphisme identité de G/F.

N et H étant des sous-groupes normaux de G en faisant agir G à gauche sur G/N et G/H comme précédemment on a $\forall s \in G$, $G_{sN} = N$ et $G_{sH} = H$, $\omega(sH) = G/H$ et $\omega(sN) = sN$, les identités sur G/H et G/N sont les bijections $\left\{\begin{array}{lll} G/G_{sH} & \to & \omega(sH) \\ gG_{sH} & \mapsto & g.sH \end{array}\right.$ et $\left\{\begin{array}{lll} G/G_{sN} & \to & \omega(sN) \\ gG_{sN} & \mapsto & g.sN \end{array}\right.$

On définit une deuxième action de G sur G/H en posant

$$(\forall g, s \in G)\ g.sH = \Psi(g)\overline{\Psi}^{-1} \circ \Psi(s)\,(= \Psi(g)sH)$$

puisque si e est le neutre de G alors

$e.sH = \overline{\Psi}^{-1} \circ \Psi(s) = sH$ et puisque $(\forall u, t, s \in G)$

$$\begin{aligned} u.(t.sH) &= u.\left(\Psi(t)\overline{\Psi}^{-1} \circ \Psi(s)\right) = u.\left(\Psi(t)sH\right) \\ &= \Psi(u)\Psi \circ \overline{\Psi}^{-1}\left(\Psi(t)sH\right) \\ &= \Psi(u)\Psi(t)\left(\Psi \circ \overline{\Psi}^{-1}(sH)\right) \\ &= \Psi(ut)\left(\Psi \circ \overline{\Psi}^{-1}(sH)\right) = (ut).sH \end{aligned}$$

$\forall s \in G$, *$\omega(sH)$ l'orbite de sH est sNH* car $\omega(sH) = \{\Psi(g)sH/g \in G\}$ et comme g parcourant G, $\Psi(g)$ parcourt N... on obtient $\omega(sH) = NsH = sNH$ puisque $sN = Ns$ $(\forall s \in G)$.
Soit $g \in G$ tel que $g.sH = sH$ alors $\Psi(g)sH = sH$. L'élément $\Psi(g)s = \Psi\ g\ e$ appartient à $\Psi(g)sH$, donc à sH : il existe donc $h \in H$ tel que $\Psi(g)s = sh$. On a alors $\Psi(g) = shs^{-1} \in H$ puisque H est distingué dans G. Si $\Psi(g) \in H$ alors $\Psi(g)sH = \Psi(g)Hs = Hs = sH$. *$G_{sH}$ le fixateur de sH est donc $\{g \in G/\Psi(g) \in H\}$ soit le sous-groupe de G/H : $\overline{\Psi}^{-1}(H)$.*
L'image par l'isomorphisme $\overline{\Psi}$ du groupe $\overline{\Psi}^{-1}(H)$ -c'est à dire le groupe $\overline{\Psi}\left(\overline{\Psi}^{-1}(H)\right) = H$- est par définition de $\overline{\Psi}$ incluse dans N soit $\boxed{N \supset H}$.
On définit bien un morphisme de groupes par

$\Theta \ : \left\{ \begin{array}{ccc} G/H & \to & G/N \\ gH & \mapsto & gN \end{array} \right.$ puisque si $g_1H = g_2H$ alors $g_2^{-1}g_1 \in H \subset N$ et donc $g_1N = g_2N$ et par le troisième théorème d'isomorphisme de la théorie des groupes $G/N \simeq (G/H)/(N/H)$. On remarquera que *l'isomorphisme* $\overline{\Theta} : \left\{ \begin{array}{lcl} (G/H)/(N/H) & \to & G/N \\ gH.(N.H) & \mapsto & gN \end{array} \right.$ *n'est pas l'identité de* G/N et en dépit de l'égalité qui le définit $N/H = \{nH/n \in N\}$ *n'est pas le groupe* N *bien que* $gH.(N/H) = gN$. En effet l'opération de groupe sur N est $n" = n' + n$ et l'opération sur (N/H), *est l'opération de groupe de classes* $n"H = n'H + nH$. Il faut *distinguer* gN comme classe et élément du groupe G/N de gN comme classe et élément du groupe $(G/H)/(N/H)$.

Quelle axiomatique pour les exponentielles discontinues ?

$\mathbb{R}$ comme espace vectoriel sur $\mathbb{Q}$

Dans cette partie la théorie des ensembles est la théorie Zermelo-Fraenkel. L'axiome du choix général permet de conclure à l'existence de bases pour tout espace vectoriel sur un corps et en particulier pour l'espace vectoriel $\mathbb{R}$ *sur le corps* $\mathbb{Q}$.

$(\mathbb{R},+)$ est un groupe additif, on lui ajoute une opération externe notée . dont l'opérande est à valeur sur $\mathbb{Q}$, par $\lambda.x = \lambda \times x$ où $\lambda \in \mathbb{Q}$ et $x \in \mathbb{R}$. Les propriétés du produit sur $\mathbb{R}$ font que l'opération . a les propriétés suivantes :

- $(\forall x \in \mathbb{R})\ 0.x = 0$
- $(\forall \lambda, \mu \in \mathbb{Q})\ (\forall x \in \mathbb{R})\ (\lambda + \mu).x = \lambda.x + \mu.x$
- $(\forall \lambda \in \mathbb{Q})\ (\forall x, y \in \mathbb{R})\ \lambda.(x + y) = \lambda.x + \lambda.y$
- $(\forall \lambda, \mu \in \mathbb{Q})\ (\forall x \in \mathbb{R})\ \lambda.(\mu.x) = (\lambda \times \mu).x$

$\mathbb{R}$ est un espace vectoriel sur $\mathbb{Q}$, celui-ci admet une base en tant qu'espace vectoriel sur le corps $\mathbb{Q}$.

L'existence d'une base sur tout espace vectoriel démontrée comme conséquence du lemme de Zorn, lui-même équivalent à l'axiome de choix général dans l'axiomatique Zermelo-Fraenkel de la théorie des ensembles

Ce résultat est considéré à tord comme un classique acquis de la théorie des espaces vectoriels et nous en rappelons la démonstration utilisant l'axiomatique dite Z.F.CG (théorie Zermelo-Fraenkel avec généralité de l'axiome du choix).

Soit K un corps, E un K-espace vectoriel, non réduit à $\{0\}$, nous ordonnons l'ensemble $\mathcal{P}(E)$ des parties de E par l'inclusion, nous considérons $\mathcal{L} \subset \mathcal{P}(E)$ l'ensemble des parties libres de E.

$\mathcal{L}$ n'est pas vide car il contient au moins un singleton $\{x\}$ avec $x \neq 0$.
Si $\mathcal{C}$ est une partie totalement ordonnée de $\mathcal{L}$ alors $\mathcal{M} = \cup_{c \in \mathcal{C}} c$ est un majorant de $\mathcal{C}$, c'est aussi une partie libre de E :
En effet, si $\sum_{i=1}^{n} k_i e_i = 0$ avec $k_i \in K$ et $e_i \in \mathcal{M} = \cup_{c \in \mathcal{C}} c$ alors,
$(\forall i \in \{1, .., n\})(\exists c_i \in \mathcal{C}) e_i \in c_i$: les e_i sont des items d'au plus n parties libres c_i distinctes de $\mathcal{C}$, comme ces n parties sont totalement ordonnées par inclusion, la famille $(c_i)_{1 \leq i \leq n}$ admet un plus grand élément c^* dans $\mathcal{C}$: autrement dit $\sum_{i=1}^{n} k_i e_i$ est une combinaison linéaire nulle sur la partie libre c^*, ce qui entraîne que $k_i = 0 \ \forall i \in \{1, ..., n\}$.
Ceci étant vrai pour toute combinaison linéaire sur $\mathcal{M}$, il suit que $\mathcal{M}$ *est une partie libre de E.*
$\mathcal{L}$ est donc une partie non vide et inductive de E et, par application du lemme de Zorn, il existe un élément $\mathcal{B}$ de $\mathcal{L}$ qui est maximal pour l'ordre de l'inclusion.
$\mathcal{B}$ est une base de E : Soit $x \in E$, si x est un vecteur de $\mathcal{B}$ il est égal à $1.x$ et c'est une combinaison linéaire de vecteurs de $\mathcal{B}$.
Si $x \notin \mathcal{B}$ alors la partie $\mathcal{B}' = \mathcal{B} \cup \{x\}$ n'est pas libre car si elle l'était $\mathcal{B}$ ne serait pas une partie libre maximale. Il existe alors une combinaison linéaire nulle à coefficients non tous nuls de vecteurs de $\mathcal{B}'$,

et le coefficient de x, item de $\mathcal{B}'$ n'est pas 0 car alors il existerait une combinaison linéaire nulle à coefficients non tous nuls de vecteurs de la partie libre $\mathcal{B}$. Si $\lambda x + \sum_{i=1}^{n} \lambda_i e_i = 0$ avec $\lambda \neq 0,\ e_i \in \mathcal{B}$ était cette combinaison linéaire alors $x = -\sum_{i=1}^{n} \frac{\lambda_i}{\lambda} e_i$ serait combinaison linéaire de vecteurs de $\mathcal{B}$.
On a écrit que $\mathcal{B}$ est une partie génératrice de E et, comme c'est déjà une partie libre, que c'est une base de E.

L'exemple de la collection de morphismes $\Phi_{.,.}$

Cette collection se spécialise en une base β du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$ et en un entier l différent de 1 de cette manière : Nous posons $\Phi_{\beta,l}(0) = 1$ et si $x \in \mathbb{R}^*$ alors $\exists n \in \mathbb{N},\ x = \sum_{i=1}^{n} q_i b_i$ avec $q_i \in \mathbb{Q}$ et b_i un vecteur de β alors nous posons

$$\Phi_{\beta,l}(x) = l^{\sum_{i=1}^{n} q_i}$$

La collection $\Phi_{\beta,l}$ est une collection de solutions non continues de $f(x+y) = f(x) \times f(y)$.
Si $x = \sum_{i=1}^{n} q_i e_i$ et $y = \sum_{i=1}^{m} r_i e'_i$ avec $q_i, r_i \in \mathbb{Q}$ e_i, e'_i vecteurs de β alors

$$\begin{aligned}\Phi_{\beta,l}(x+y) &= l^{\sum_{i=1}^{n} q_i + \sum_{i=1}^{m} r_i} \\ &= l^{\sum_{i=1}^{n}} \times l^{\sum_{i=1}^{m} r_i} = \Phi_{\beta,l}(x) \times \Phi_{\beta,l}(y)\end{aligned}$$

$\Phi_{\beta,l}$ n'est pas constante, elle prend la valeur 1 et la valeur l sur les vecteurs de bases. $\Phi_{\beta,l}$ est une puissance rationnelle d'un nombre entier : c'est un nombre algébrique. Comme l'ensemble des nombres algébriques est dénombrable, comme $\Phi_{\beta,l}(x)$ admet au moins deux valeurs et est toujours algébrique, l'image de $\mathbb{R}$ contient au moins deux valeurs et est au plus dénombrable. Si $\Phi_{\beta,l}$ était continue alors l'image de la partie connexe $\mathbb{R}$ serait connexe : ce serait un singleton ou un intervalle de $\mathbb{R}$ de mesure non nulle. Comme un intervalle de mesure non nulle n'est pas dénombrable et que $\Phi_{\beta,l}$ admet au moins deux valeurs : $\Phi_{\beta,l}$ n'est pas continue et d'après ce qui précède $\Phi_{\beta,l}$ n'est pas continue en tout $x \in \mathbb{R}$.

Sur la collection des morphismes $\Phi_{\beta,l}$ et de leurs noyaux G_β

Dans ce qui suit on fixe une base β du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$ et nous définissons la collection $G_\beta = Ker(\Phi_{\beta,l})$ indexée par les réels l.

$$G_\beta = \{x \in \mathbb{R}, x = \sum_{i \in I fini} r_i b_i \ et \ \sum_{i \in I fini} r_i = 0\}$$

G_β est un sous-groupe de $\mathbb{R}$ comme noyau d'un morphisme de groupe.

G_β est dense dans $\mathbb{R}$ et n'est pas connexe. En tant que $\mathbb{Q}$-espace vectoriel $\mathbb{R}$ n'est pas de dimen-

sion finie - En effet si $dim_{\mathbb{Q}}(\mathbb{R}) = n < +\infty$ alors $\mathbb{R}$ est isomorphe et donc équipotent à $\mathbb{Q}^n$, il est alors dénombrable, or $\mathbb{R}$ n'est pas dénombrable - il suit que pour nombre entier p on peut trouver au moins p éléments distincts dans la base β. En particulier on peut en trouver quatre et nous appelons a, b, c, d quatre de ces nombres réels tous non nuls. Comme β est une $\mathbb{Q}$-base de $\mathbb{R}$, les réels $a - b$ et $c - d$ ne sont pas nuls et par définition $\Phi_{\beta,l}(a - b) = \Phi_{\beta,l}(c - d) = l^0 = 1$. On en déduit donc que $a - b \in G_\beta$ et $c - d \in G_\beta$.
Il n'existe pas de réel $x > 0$ tel que $G_\beta = x\mathbb{Z}$: si c'est le cas alors il existe des entiers relatifs m et n tels que $a-b = m\times x$ et $c-d = n\times x$, il vient alors $x = \dfrac{1}{m}\times a - \dfrac{1}{m}\times b = \dfrac{1}{n}\times c - \dfrac{1}{n}\times d$. Cette double égalité signifie que x admet deux décompositions distinctes comme combinaison linéaire d'éléments de β et contredit le fait que β est une $\mathbb{Q}$-base de $\mathbb{R}$.
D'après ce qui précède des sous-groupes de $\mathbb{R}$:
G_β est un sous-groupe de $\mathbb{R}$ dense dans $\mathbb{R}$.
G_β n'est pas fermé : s'il l'était alors il serait égal à sa fermeture $\mathbb{R}$ et, pour tout $l \in \mathbb{N}$, $\Phi_{\beta,l}$ serait l'application identique à 1, or en un élément de base b_i on a $\Phi_{\beta,l}(b_i) = l$.
G_β n'est pas ouvert : s'il l'était alors en fixant un élément b_i de base, son translaté $b_i + G_\beta$ serait

encore un ouvert dense dans $\mathbb{R}$.
L'intersection $G_\beta \cap (b_i + G_\beta)$ est vide puisque $\Phi_{\beta,l}$ est constante égale à 1 sur G_β et constante égale à l sur $b_i + G_\beta$ (c'est une application élémentaire du premier théorème d'isomorphisme de la théorie des groupes). Deux ouverts denses de $\mathbb{R}$ seraient d'intersection vide, ceci contredit l'application suivanfete du théorème de Baire : toute intersection finie ou dénombrable d'ouverts denses de $\mathbb{R}$ complet est dense dans $\mathbb{R}$.
La collection G_β est une collection de groupes isomorphes à $\mathbb{R}/\mathbb{Q}$: d'après le dit premier théorème d'isomorphisme de la théorie des groupes, il existe pour tout l un isomorphisme $\overline{\Phi}_{\beta,l}$ tel que $\mathbb{R}/G_\beta \overset{\overline{\Phi}_{\beta,l}}{\to} \{l^q/q \in \mathbb{Q}\}$. ln_l : le logarithme à base l est un isomorphisme tel que $ln_l\left(\{l^q/q \in \mathbb{Q}\}\right) = \mathbb{Q}$, de sorte que sur la figure suivante la flèche représente un isomorphisme.

$$(\mathbb{R}/G_\beta, +) \overset{ln_l \circ \overline{\Phi_{\beta,l}}}{\to} (\mathbb{Q}, +)$$

Il suit pour tout β un *isomorphisme*

$$\mathbb{R}/\mathbb{Q} \to G_\beta$$

Tout groupe G_β est invariant par toute homothétie de rapport rationnel, c'est un $\mathbb{Q}$-module :
Soit $x \in G_\beta$ et $r \in \mathbb{Q}$ alors $x = \sum_{i \in I fini} r_i b_i$ et $r \times x = \sum_{i \in I fini} (r.r_i) b_i \in r.G_\beta$.

Réciproquement si $y \in r.G_\beta$ alors $\exists r_i \in \mathbb{Q}$ tels que $y = r \times \sum_{i \in I fini} r_i b_i$, on a donc $y = \sum_{i \in I fini} (r.r_i) b_i \in G_\beta$ puisque $\forall i,\ r.r_i \in \mathbb{Q}$.

Tout groupe G_β n'est pas mesurable par la mesure de Lebesgue.

Supposons qu'un le soit et posons $\alpha = \mu(G_\beta)$ où μ est la mesure de Lebesgue. Comme $\forall r \in \mathbb{Q}$ $G_\beta = r.G_\beta$ alors $\mu(G_\beta) = \mu(r.G_\beta) = |r|.\mu(G_\beta)$ et donc $\mu(G_\beta) = 0$ mais l'existence d'un isomorphisme de groupe de $(\mathbb{R}/G_\beta, +)$ vers $(\mathbb{Q}, +)$ entraîne que $\mathbb{R}$ admet une partition comme union dénombrable de translatés de G_β, qui sont tous de mesure nulle, $\mu(\mathbb{R})$ est alors la somme d'une série, absolument convergente et dont les termes sont les mesures -égales à zéro- de translatés de G_β. La somme d'une telle série est 0 ce qui contredit que $\mu(\mathbb{R}) = \infty$.

$\forall(\beta, \beta'),\ G_\beta = G'_\beta$ on pose alors $G = G_\beta$. En effet G_β et G'_β sont des groupes isomorphes au groupe $\mathbb{R}/\mathbb{Q}$ et puisqu'ils contiennent $\mathbb{Q}$ ils sont égaux.

Il existe, par l'axiome du choix général, un groupe de nombres réels isomorphe à $\mathbb{R}/\mathbb{Q}$: ce groupe est dense dans $\mathbb{R}$, et pour la topologie de la distance il n'est ni ouvert ni fermé, il n'est pas mesurable pour la mesure de Lebesgue, il n'est pas dénombrable, il est le noyau d'une ex-

ponentielle discontinue en tout point, le terme exponentielle signifiant morphisme de groupe de $(\mathbb{R}, +)$ *vers* $(\mathbb{R}_*^+, \times)$.

Dans l'axiomatique Z.F.CG le groupe unique G isomorphe à $\mathbb{R}/\mathbb{Q}$ n'existe pas

Tout sous-groupe propre $(G, +)$ de $(\mathbb{R}, +)$ isomorphe à $\mathbb{R}/\mathbb{Q}$ par $i \ : G \to \mathbb{R}/\mathbb{Q}$ qui existe par l'axiome du choix général n'est pas fini (sa caractéristique est nulle), *n'est pas infini et dénombrable* sinon $\mathbb{R}$ serait *la partition dénombrable*

$$\sqcup_{k \in I \subset \mathbb{N}} i(g_k)$$

où $i(g_k)$ est une classe de $\mathbb{R}/\mathbb{Q}$ si on a posé $G = \{g_0, \ g_1, \ \dots\}$. Or, pour tous les k entiers $i(g_k)$ étant un ensemble dénombrable parce que classe $x + \mathbb{Q}$ de $\mathbb{R}/\mathbb{Q}$, ceci signifie que $\mathbb{R}$ serait alors dénombrable comme union finie ou dénombrable de ces ensembles dénombrables. G qui est :

- soit le groupe dénombrable $a\mathbb{Z}$ avec $a \in \mathbb{R}^+$,
- soit dense dans $\mathbb{R}$,

ne peut être que dense dans $\mathbb{R}$.
On en déduit que :

- $\forall g \in G$, $i(g)$ est une classe $x + \mathbb{Q}$ de $\mathbb{R}/\mathbb{Q}$,
- $\mathbb{R} = \sqcup_{g \in G} i(g)$ où G est dense.

$\mathbb{Q}G = G$ *c.a.d.* G *est un* $\mathbb{Q}$*-module* et comme G est unique il ne peut être que $\mathbb{Q}$ qui est Lebesgue-mesurable ce qui contredit son existence.
Dans l'axiomatique Zermelo-Fraenkel de la théorie des ensembles avec axiome du choix dépendant, le groupe de Lie des solutions de l'équation aux différences

$$\boxed{f(x+y) = f(x) \times f(y)}$$

est celui des exponentielles à coefficient réel.