Une incarnation peu connue du corps des nombres réels

Xavier Caruso

Septembre 2008

Résumé

Le but de cette note est de donner une présentation peu connue du corps des nombres réels à partir de la notion de quasi-endomorphismes de $\mathbb{Z}$. L'auteur n'a pas vraiment réussi à déterminer l'origine de cette construction, mais note que celle-ci apparaît dans plusieurs articles ([1] [2], [3]) ainsi que dans la version anglaise de Wikipedia ([4]), références dans lesquelles le point de vue adopté est légèrement différent et aboutit à ce que l'on peut légitimement appeler une construction de $\mathbb{R}$ (au prix toutefois d'une démonstration un peu plus pénible).

Mots-clés : construction des nombres réels, quasi-morphismes de groupes.

La notion centrale dans tout ce qui suit est celle de *quasi-endomorphisme* de $\mathbb{Z}$ dont on donne tout de suite la définition.

Définition 1. Une fonction $f : \mathbb{Z} \to \mathbb{Z}$ est appelé un *quasi-endomorphisme* s'il existe une constante C_f (dépendant de f) telle que $|f(n+m) - f(n) - f(m)| \leqslant C_f$ pour tous entiers relatifs n et m.

Notons $\mathcal{A}$ l'ensemble des quasi-endomorphismes de $\mathbb{Z}$. C'est clairement un groupe abélien pour l'addition usuelle des fonctions. En réalité, $\mathcal{A}$ est également stable par l'opération de composition des fonctions. Pour démontrer cela, on considère f et g deux éléments de $\mathcal{A}$, on note C_f et C_g des constantes données par la définition, et on estime

$$\begin{aligned}
&|g \circ f(n+m) - g \circ f(n) - g \circ f(m)| \\
&\qquad \leqslant |g \circ f(n+m) - g(f(n) + f(m))| + |g(f(n) + f(m)) - g(f(n)) - g(f(m))| \\
&\qquad \leqslant |g \circ f(n+m) - g(f(n) + f(m))| + C_g \\
&\qquad \leqslant |g(f(n+m) - f(n) - f(m))| + 2C_g.
\end{aligned}$$

La quantité $|f(n+m) - f(n) - f(m)|$ est par définition majorée par C_f ; ainsi si M désigne le plus grand des $|g(i)|$ pour $|i| \leqslant C_f$, on a bien trouvé un majorant universel à $|g \circ f(n+m) - g \circ f(n) - g \circ f(m)|$, à savoir $M + 2C_g$. On prendra garde cependant au fait que $(\mathcal{A}, +, \circ)$ *n'est pas* un anneau, la propriété de distributivité n'étant pas satisfaite. On énonce maintenant une proposition tout à fait cruciale pour faire le lien entre $\mathcal{A}$ et $\mathbb{R}$.

Proposition 2. *Soit f un quasi-endomorphisme de $\mathbb{Z}$. Alors la suite des quotients $(\frac{f(n)}{n})_{n \geqslant 1}$ est convergente (dans $\mathbb{R}$).*

Démonstration. Notons C_f un majorant universel de $|f(n+m)-f(n)-f(m)|$ et remarquons avant tout qu'une récurrence très simple (sur k) donne directement

$$|f(n_1 + \cdots + n_k) - f(n_1) - \cdots - f(n_k)| \leqslant (k-1)C_f \leqslant kC_f$$

pour tout k et tout k-uplet d'entiers $(n_1, \dots, n_k)$. Soient n et m deux entiers strictement positifs. L'inégalité précédente appliquée aux uplets $(n, \dots, n)$ et $(m, \dots, m)$ donne

$$|f(nm) - mf(n)| \leqslant mC_f \quad \text{et} \quad |f(nm) - nf(m)| \leqslant nC_f$$

soit encore, en divisant par nm :

$$\left|\frac{f(nm)}{nm} - \frac{f(n)}{n}\right| \leqslant \frac{C_f}{n} \quad \text{et} \quad \left|\frac{f(nm)}{nm} - \frac{f(m)}{m}\right| \leqslant \frac{C_f}{m}.$$

En regroupant ces deux inégalités, on obtient finalement

$$\left|\frac{f(n)}{n} - \frac{f(m)}{m}\right| \leqslant \frac{C_f}{n} + \frac{C_f}{m}$$

à partir de quoi on déduit immédiatement que la suite des $(\frac{f(n)}{n})_{n \geqslant 1}$ est de Cauchy et donc converge. □

La proposition permet de définir l'application $\ell : \mathcal{A} \to \mathbb{R}$, $f \mapsto \lim_{n\to\infty} \frac{f(n)}{n}$. On vérifie sans difficultés que c'est un morphisme de groupes (pour l'addition des deux côtés).

Théorème 3. *L'application ℓ est surjective et son noyau $\mathcal{K}$ s'identifie à l'ensemble des quasi-endomorphismes bornés.*

Démonstration. La surjectivité est simple : un antécédent de $x \in \mathbb{R}$ est donné par le quasi-morphisme $f : n \mapsto E(xn)$ où $E(\,\cdot)$ désigne la fonction « partie entière ».

Pour le calcul du noyau, on suppose donné $f : \mathbb{Z} \to \mathbb{Z}$ un quasi-endomorphisme tel que $\lim_{n\to\infty} \frac{f(n)}{n} = 0$. Notons comme d'habitude C_f un élément qui majore tous les $|f(n+m) - f(n) - f(m)|$ pour n et m variant dans $\mathbb{Z}$. En faisant « $n = m = 0$ », on obtient déjà $|f(0)| \leqslant C_f$. Nous allons montrer maintenant que $|f(n)| \leqslant C_f$ pour tout $n > 0$. Supposons que ce ne soit pas le cas et notons n_0 un entier strictement positif tel que $|f(n_0)| > C_f$. On a alors $|f(kn_0) - kf(n_0)| \leqslant (k-1)C_f$ d'où l'on tire

$$|f(kn_0)| \geqslant |f(n_0)| + (k-1)(|f(n_0)| - C_f).$$

On en déduit que la suite extraite des $(\frac{f(kn_0)}{kn_0})_{k\geqslant 1}$ ne converge pas vers 0, ce qui constitue notre contradiction. Pour les n négatifs finalement, on écrit $|f(0) - f(n) - f(-n)| \leqslant C_f$, d'où il suit $|f(n)| \leqslant |f(0)| + |f(-n)| + C_f$ et donc $|f(n)| \leqslant 3C_f$ si $n < 0$. □

Théorème 4. *Soient f et g deux éléments de $\mathcal{A}$. Alors $\ell(g \circ f) = \ell(g)\ell(f)$.*

Démonstration. On distingue trois cas selon le signe de $\ell(f)$. Tout d'abord, si $\ell(f) = 0$, f est bornée d'après le théorème 3. Ainsi $g \circ f$ l'est aussi, d'où on déduit que $\ell(g \circ f) = 0 = \ell(g)\ell(f)$. Si maintenant $\ell(f) > 0$, on remarque que $f(n)$ tend vers $+\infty$ (puisqu'il est équivalent à $\ell(f)n$). Ainsi, à partir d'un certain rang, $f(n)$ ne s'annule pas, et on peut écrire

$$\frac{g \circ f(n)}{n} = \frac{g \circ f(n)}{f(n)} \cdot \frac{f(n)}{n} \tag{1}$$

ce qui conclut en passant à la limite. Si finalement $\ell(f) < 0$, en reprenant l'égalité (1), on est amené à justifier que $\lim_{n\to-\infty} \frac{f(n)}{n} = \ell(f)$, ce qui est à peu près clair après avoir remarqué que $|f(n) + f(-n)| \leqslant |f(0)| + C_f$ pour tout n. □

Le théorème 3 donne un isomorphisme de groupes entre $\mathcal{R} = \mathcal{A}/\mathcal{K}$ et $\mathbb{R}$. Étant donné que $\mathbb{R}$ est un anneau, ceci permet de munir $\mathcal{R}$ d'une structure d'anneau. Le théorème 4 montre que la loi de multiplication obtenue n'est rien d'autre que celle déduite de la composition usuelle des fonctions par passage au quotient. D'aucuns préféreront peut-être aller « dans l'autre sens » selon le schéma suivant :

– démontrer en premier lieu que la loi $\circ$ définie sur $\mathcal{A}$ passe au quotient pour définir une multiplication sur $\mathcal{R}$: il s'agit donc de vérifier que si $f \equiv f' \pmod{\mathcal{K}}$ et $g \equiv g' \pmod{\mathcal{K}}$, alors $f \circ f' \equiv g \circ g' \pmod{\mathcal{K}}$;
– dans un second temps, montrer que $(\mathcal{R}, +, \circ)$ est un anneau : il s'agit essentiellement de vérifier la distributivité ;
– montrer finalement que l'application $\mathcal{R} \to \mathbb{R}$ induite par ℓ est un isomorphisme d'anneaux : c'est l'argument du théorème 4.

Bien que peut-être moins naturel, le raisonnement par transport de structures a l'avantage d'être plus succint. C'est la raison pour laquelle nous avons choisi de présenter celui-ci, et de donner simplement quelques indications sur l'autre approche en laissant au lecteur le soin de compléter les détails.

Dans tous les cas, comme annoncé dans le titre, on a obtenu une présentation assez inattendue des nombres réels : ceux-ci peuvent être vus comme des quasi-endomorphismes de $\mathbb{Z}$ si l'on prend soin d'identifier deux quasi-endormorphismes lorsque leur différence est bornée. En outre, l'addition et la multiplication des réels correspondent respectivement à la somme et la composition des quasi-endomorphismes. L'ordre usuel sur $\mathbb{R}$ se lit aussi de façon assez simple sur les quasi-endormophismes : si f et g représentent respectivement les réels x et y, alors $x \leqslant y$ si, et seulement si la fonction différence $f - g$ est majorée sur $\mathbb{N}$ (exercice facile laissé au lecteur).

On peut alors se demander si cette description ne permet pas d'obtenir une construction proprement dite de $\mathbb{R}$, c'est-à-dire si l'on peut montrer directement (*i.e.* sans supposer connue la notion de nombre réel) le théorème suivant :

Théorème 5. *Le quotient $\mathcal{R} = \mathcal{A}/\mathcal{K}$ muni de sa structure d'anneau discutée précédemment et de l'ordre défini par*

$$f \leqslant g \quad \text{si, et seulement si} \quad f - g \text{ est majorée sur } \mathbb{N}$$

est un corps totalement ordonné qui satisfait la propriété de la borne supérieure.

Ceci est en fait possible, et c'est l'approche qu'on trouve dans [1], [2] et [3]. En fait, la difficulté principale pour démontrer le théorème 5 est de montrer que chaque élément de $\mathcal{A}/\mathcal{K}$ admet un représentant $f \in \mathcal{A}$ dont le C_f est majoré une constante absolue. Pour une preuve complète du théorème, on pourra se reporter à [3].

Références

[1] N. A'Campo, *A natural construction for the real numbers* (2003), disponible à `http://arxiv.org/pdf/math/0312016`

[2] B. Odgers, N. H. Vo, *Analysis of an efficient construction of the reals* (2002), disponible à `http://www.math.mq.edu.au/~street/efficient.pdf`

[3] R. Street, *An efficient construction of the real numbers* (2004), disponible à `http://www.math.mq.edu.au/~street/EffR.pdf`

[4] `http://en.wikipedia.org/wiki/Construction_of_real_numbers`