Calculabilité en analyse

David Waszek

27 janvier 2009

« computability as an illuminating
concept applicable to classical analysis »
O. Aberth [1]

La notion de calculabilité s'applique naturellement aux objets élémentaires de l'analyse : on peut distinguer, parmi les réels, les fonctions réelles, etc., ceux qui possèdent la propriété d'être en un certain sens — que nous expliciterons — calculables ; c'est en fait dans ce cadre que Turing, dans son article fondateur [10], introduisit sa fameuse machine.

Après avoir dégagé ces notions, nous examinerons certains résultats et certains méthodes de l'analyse classique à la lumière de ces nouvelles distinctions (nous nous demanderons par exemple si le zéro d'une fonction calculable est nécessairement un réel calculable) dans la perspective d'éclairer de manière différente leur signification et leur portée.

1 Préliminaires : calculabilité

§1.1. Fonctions calculables Nous manipulerons ici l'idée de calculabilité de manière informelle ; et même si les résultats que nous développerons sont fondés sur les définitions rigoureuses que fournit la théorie de la calculabilité, nous nous en tiendrons dans cet article introductif à l'intuition du lecteur (pour plus de détails, cf. p. ex. [12]). Nous partirons ainsi de la notion intuitive de « programme » — une suite d'instructions élémentaires que l'on peut suivre mécaniquement — et nous dirons qu'une *fonction partielle* $f : \mathrm{E} \subseteq \mathbf{N}^p \to \mathbf{N}$ est calculable s'il existe un programme qui, prenant $x \in \mathbf{N}^p$ en entrée, termine et produit $f(x)$ si $x \in \mathrm{E}$, et ne termine pas si $x \notin \mathrm{E}$.

L'ensemble des fonctions calculables *totales* à p variables sera noté $\mathcal{C}_p$.

§1.2. Ensembles récursivement énumérables. On dit qu'un ensemble $\mathrm{A} \subseteq \mathbf{N}$ est récursivement énumérable s'il existe un programme qui en énumère les éléments ; il existe alors une fonction calculable totale $f : \mathbf{N} \to \mathbf{N}$, injective, telle que $\mathrm{A} = \{f(0), f(1), ...\}$.

§1.3. Ensembles récursifs. On dit qu'un ensemble $\mathrm{A} \subseteq \mathbf{N}$ est récursif s'il existe un programme capable d'indiquer, pour $n \in \mathbf{N}$, si $n \in \mathrm{A}$ ou $n \notin \mathrm{A}$; autrement dit, si la fonction caractéristique de A est calculable.

§1.4. Deux résultats. Il existe un ensemble $\mathrm{A} \subseteq \mathbf{N}$ récursivement énumérable mais non récursif.

Il existe deux ensembles B et $\mathrm{C} \subseteq \mathbf{N}$, dits *récursivement inséparables*, tels qu'il n'existe pas d'ensemble récursif $\mathrm{D} \subseteq \mathbf{N}$ vérifiant $\mathrm{B} \subseteq \mathrm{D}$ et $\mathrm{C} \subseteq \mathbf{N} \setminus \mathrm{D}$. Cela signifie qu'il n'existe pas de programme capable d'affirmer, pour tout entier n, si, à supposer que $n \in \mathrm{B} \cup \mathrm{C}$, on a plutôt $n \in \mathrm{B}$ ou $n \in \mathrm{C}$.

Nous utiliserons de manière répétée, et sans rappeler leur définition, les ensembles A, B et C du paragraphe précédent, ainsi que des fonctions a, b et $c \in \mathcal{C}_1$ (totales) injectives les énumérant. La fin de cette section est consacrée à la démonstration de l'existence de A et peut être sautée.

§1.5. Indice d'un programme. Supposons maintenant que nous ayons choisi une formalisation précise de la notion de programme calculant une fonction partielle $f : \mathrm{E} \subseteq \mathbf{N}^p \to \mathbf{N}$, i.e. grossièrement parlant que nous ayons fixé un « langage de programmation » ; tous les programmes possibles sont alors représentables par des suites finies de caractères d'un certain alphabet fini, donc par des entiers. On appelle l'entier associé à un programme *indice* de ce programme.

On peut alors concevoir un programme à deux entrées, dit *universel*, qui, pour un couple (i, n) :

– ne termine pas si i n'est pas l'indice d'un programme à une entrée ;

– simule le fonctionnement du programme d'indice i sur l'entrée n sinon.

Notons u la fonction partielle à deux variables associée.

§1.6. Deux caractérisations. Si $\mathrm{A} \subseteq \mathbf{N}$ est récursivement énumérable, alors il existe un programme à une entrée $n \in \mathbf{N}$ qui s'arrête ssi $n \in \mathrm{A}$ (le programme qui parcourt les éléments de A selon leur énumération et s'arrête lorsqu'il rencontre n). Réciproquement, si un tel programme existe, pour énumérer A on peut parcourir les couples $(n, t) \in \mathbf{N}^2$ dans l'ordre « zig-zag » ; pour chaque couple, simuler t opérations de l'exécution du programme sur l'entrée n ; et énumérer n comme élément de A si cette exécution s'achève précisément au bout des t opérations effectuées.

Si $\mathrm{A} \subseteq \mathbf{N}$ est récursif, alors A et $\mathbf{N} \setminus \mathrm{A}$ sont récursivement énumérables : il suffit de parcourir tous les entiers et d'énumérer ceux que la fonction caractéristique de A désigne comme membres de l'un ou de l'autre. Pour établir la réciproque, on suit les deux énumérations en parallèle, à tour de rôle, jusqu'à rencontrer l'entier que l'on cherche.

§1.7. Un ensemble récursivement énumérable non récursif. Considérons l'ensemble A des indices de programmes qui terminent sur leur propre indice, i.e. $\mathrm{A} = \{i \in \mathbf{N} : u(i, i) \text{ est défini}\}$.

Il est récursivement énumérable, car $n \in \mathrm{A}$ si et seulement si le programme universel s'arrête sur l'entrée (n, n) (cf **§1.6**).

Il n'est pas récursif car son complémentaire n'est pas récursivement énumérable : il s'agit en effet de l'ensemble des indices de programmes qui ne s'arrêtent pas sur leur propre indice. Supposons (cf **§1.6**) qu'il existe un programme à une entrée i s'arrêtant ssi $i \in \mathbf{N} \setminus \mathrm{A}$: il s'arrêterait ssi $i \notin \mathrm{A}$, donc ssi le programme d'indice i ne s'arrête pas sur l'entrée i. Considérons maintenant l'indice d de ce programme : sur l'entrée d, s'il s'arrête, il devrait ne pas s'arrêter ; et s'il ne s'arrête pas, il devrait s'arrêter : un tel programme ne peut donc exister et A n'est pas récursif.

2 Les réels calculables

Par souci de simplicité, nous nous limiterons au cas des réels positifs.

§2.1. Définitions. Il est naturel de considérer qu'un réel ξ est calculable s'il existe un algorithme capable d'en donner une approximation rationnelle à toute précision demandée ; autrement dit, il existe une suite de rationnels (r_n) convergeant vers ξ, *calculable*, c.-à-d. vérifiant :

(2.1a) $\exists p, q \in \mathcal{C}_1,\ \forall n \in \mathbf{N},\ q(n) \neq 0 \quad \text{et} \quad r_n = \dfrac{p(n)}{q(n)}$

et il est algorithmiquement possible de majorer l'indice du terme à partir duquel on atteint n'importe quelle précision :

(2.1b) $\exists e \in \mathcal{C}_1,\ \forall N \in \mathbf{N},\ \forall n \geq e(N), |\xi - r_n| < \dfrac{1}{2^N}$

On dira que e est un *module de convergence* pour la suite r_n, et que la convergence de (r_n) est *calculable*. On obtient facilement la définition équivalente :

(2.1c) $\exists p \in \mathcal{C}_1,\ \forall n \in \mathbf{N}^*,\ \left|\xi - \dfrac{p(n)}{n}\right| < \dfrac{1}{n}$

où ne figure plus qu'une seule fonction calculable, p, dont on peut dire qu'elle *représente* ξ. D'autres représentations sont envisageables, par exemple par une fonction $p \in \mathcal{C}_1$ telle que $p(n)$ soit le n^{e} chiffre du développement décimal de ξ.

Il est facile de montrer que l'ensemble $\mathcal{R}$ des réels calculables est un sous-corps dénombrable de $\mathbf{R}$.

§2.2. Le lemme de l'ordre (Rice [8]). Soient deux réels calculables α et β. Si $\alpha \neq \beta$, il est algorithmiquement possible de déterminer si $\alpha < \beta$ ou $\beta < \alpha$. Il suffit en effet de calculer les approximations rationnelles $p(n)/n$ et $q(n)/n$ de α et β telles qu'en (2.1c) jusqu'à ce que $|p(n)/n - q(n)/n| \geq 2/n$, ce qui finit nécessairement par arriver si $\alpha \neq \beta$.

Ce lemme permet de passer algorithmiquement, pour un *irrationnel* calculable ξ, d'une représentation de type (2.1c) à une représentation par développement décimal, puisqu'on peut comparer ξ aux rationnels de la forme $k/10^n$; quant aux rationnels, ils sont trivialement calculables selon les deux définitions, dont on montre alors facilement l'équivalence. Il faut porter attention à cette distinction de cas entre rationnels et irrationnels, que nous retrouverons : il n'existe en fait pas de procédure générale pour passer de la représentation (2.1) au développement décimal (voir **§3.4**).

§2.3. Un réel non calculable (Specker [9]). Considérons la suite :

$$u_n = \sum_{k=0}^{n} \frac{1}{2^{a(k)}}$$

Elle converge, mais n'admet pas de module de convergence, sans quoi on obtiendrait une procédure de décision pour A. De plus, sa limite ξ ne peut être calculable : u étant monotone, on pourrait déduire un module de convergence pour u du module de convergence d'une autre suite de type (2.1a) convergeant de manière calculable vers ξ.

3 Suites calculables

§3.1. Définition. On dira qu'une suite $(\xi_n)_{n\in\mathbf{N}}$ de réels est calculable s'il existe un algorithme capable d'approximer n'importe quel terme de la suite à une précision arbitraire ; en adaptant la définition (2.1) :

$$(3.1)\quad \exists p,q,e\in\mathcal{C}_2,\ \forall n,K\in\mathbf{N},\ \forall k\geq e(n,K),\ \begin{cases} q(n,k)\neq 0 \\ \left|\xi_n-\dfrac{p(n,k)}{q(n,k)}\right|<\dfrac{1}{2^K}\end{cases}$$

(*a fortiori*, tous les ξ_n sont calculables). On approxime en fait notre suite par une suite double explicitement calculable de rationnels qui converge de manière calculable selon les deux variables. Une modification similaire à (2.1c) permet de représenter la suite par une fonction calculable de deux variables.

Cette définition se généralise aisément au cas des suites doubles.

Notons tout de suite que l'exemple de **§2.3** nous montre que l'équivalent calculable du théorème de Bolzano-Weierstrass est faux : il existe des suites calculables bornées qui n'admettent pas de valeur d'adhérence calculable.

§3.2. Intérêt. Les résultats de calculabilité portant sur un nombre fini d'objets (ici, de réels calculables) sont toujours immédiats : par exemple, si on se donne $\alpha,\beta\in\mathcal{R}$, il *existe* un « algorithme » trivial qui indique si $\alpha=\beta$. Cela ne signifie pas que nous connaissions effectivement la réponse dans ce cas précis, ni qu'il existe une procédure générale pour tester l'égalité de deux réels calculables.

L'existence d'une telle procédure générale n'est pas facile à manipuler directement ; il est plus simple d'utiliser la propriété affaiblie que pour chaque couple de *suites* calculables (ξ_n), (ψ_n), il existe une procédure de décision valable pour tous leurs termes, c.-à-d. un algorithme qui, sur l'entrée d'un indice n, indique si $\xi_n=\psi_n$. Nous montrerons plus loin que cette dernière propriété est en défaut, et donc que l'égalité entre réels calculables n'est pas décidable.

Nous justifierons similairement qu'il n'existe pas de procédure générale pour passer de la représentation par approximations rationnelles à la représentation décimale.

Cependant, il n'existe pas de suite calculable parcourant tous les éléments de $\mathcal{R}$ (cf. p. ex. Weihrauch [11] pp. 104–105) ; et l'existence, pour chaque suite calculable particulière, d'une procédure valable pour tous les termes de la suite, n'est pas suffisante pour qu'il existe une procédure générale, valable pour tous les réels calculables, fait que nous rencontrerons en **§4.1**.

§3.3. Indécidabilité de $\alpha=\beta$. Posons :

$$u_{n,k}=\begin{cases}0 & \text{s'il n'existe pas d'entier } m\leq k \text{ tel que } n=a(m)\,; \\ 2^{-m} & \text{où } m=\min\{p\leq k;\ n=a(p)\} \text{ sinon.}\end{cases}$$

Cette suite double est du type (3.1) car $e(n,k) = 2^{-k}$ en est un module de convergence ; sa limite :

$$u_n = \begin{cases} 0 & \text{s'il n'existe pas d'entier } m \in \mathbf{N} \text{ tel que } n = a(m)\,; \\ 2^{-m} & \text{où } m = \min\{p \in \mathbf{N};\ n = a(p)\} \text{ sinon.} \end{cases}$$

est donc une suite calculable. Une procédure capable de déterminer si $u_n = 0$ donnerait immédiatement une procédure de décision pour A.

§3.4. Un contre-exemple (Mostowski [6]). Considérons similairement la suite double :

$$v_{n,k} = \begin{cases} \frac{1}{10} - \frac{1}{10^{k+2}} & \text{si } \forall m \leq k,\ n \neq b(m) \text{ et } n \neq c(m)\,; \\ \frac{1}{10} - \frac{1}{10^{m+2}} & \text{si } m = \min\{p \leq k;\ n = b(p)\}\,; \\ \frac{1}{10} + \frac{1}{10^{m+2}} & \text{si } m = \min\{p \leq k;\ n = c(p)\}. \end{cases}$$

La convergence est ici encore calculable ; la suite limite (v_n) est donc calculable, et le premier chiffre du développement décimal de v_n est nul si $n \in$ B, non nul si $n \in$ C : il n'est pas calculable.

4 Fonctions calculables

§4.1. Définition. Nous ne pouvons développer ici la théorie des fonctions partielles calculables d'ordre supérieur $\Phi :\subseteq \mathcal{C}_1 \to \mathcal{C}_1$ (voir Kleene [5]). Informellement, Φ correspond à un algorithme capable, à partir de la description d'un algorithme calculant $f \in \mathcal{C}_1$, de calculer $\Phi(f)(n)$ pour tout n.

En représentant les réels calculables par des éléments de $\mathcal{C}_1$, comme suggéré en **§2.1**, on peut déduire de cette notion celle de fonction réelle calculable. Nous admettrons (Grzegorczyk [3, 4]) que cette définition est équivalente à la suivante.

Soient $\alpha, \beta \in \mathcal{R}$, $\alpha < \beta$. On dira que $f : I = [\alpha, \beta] \to \mathbf{R}$ est calculable si :

(i) L'image par f de toute suite calculable de I est une suite calculable (en particulier, l'image de tout réel calculable est calculable) ;

(ii) f est *calculablement uniformément continue* :

$$\exists d \in \mathcal{C}_1,\ \forall x, y \in I,\ \forall n \in \mathbf{N}, \left[|x - y| \leq \frac{1}{d(n)} \Rightarrow |f(x) - f(y)| \leq \frac{1}{2^n}\right]$$

La propriété (i) seule est moins forte (cf. remarque du **§3.2**) : il existe une fonction continue vérifiant (i) et pas (ii) (Pour-El / Richards [7], pp. 67–68).

§4.2. Le théorème des valeurs intermédiaires. On suppose, sans nuire à la généralité, que $I = [0,1]$, que $f(0) < 0$, $f(1) > 0$ et qu'on cherche un zéro de f. On va montrer qu'il existe un réel calculable $\xi \in I$ tel que $f(\xi) = 0$. Distinguons deux cas :

- Il existe un rationnel $r \in I$ tel que $f(r) = 0$: on a terminé ;
- Pour tout rationnel $r \in I$, $f(r) \neq 0$. On peut dans ce cas reprendre la démonstration dichotomique usuelle : on construit deux suites de rationnels (u_n) et (v_n) telles que $\forall n \in \mathbf{N}$, $f(u_n) < 0$, $f(v_n) > 0$ et $v_n - u_n = 2^{-n}$, ce qui nous garantit que leur convergence est calculable. On part de $u_0 = 0$, $v_0 = 1$; à chaque étape, on a, en posant $m = (u_n + v_n)/2$, $f(m) \neq 0$

puisque $m \in \mathbf{Q}$; on peut alors comparer $f(m)$ à 0 (cf. **§2.2**) et choisir u_{n+1} et v_{n+1} en fonction : ces suites sont donc calculables, convergent calculablement et leur limite commune est un zéro de f.

On voit ressurgir ici la distinction de cas rencontrée en **§2.2**, avec les mêmes conséquences : il n'existe pas de procédure générale permettant, à partir de la description d'une fonction f vérifiant les hypothèses ci-dessus, de calculer un zéro de f. Pour démontrer ce résultat, nous passerons par des suites de fonctions, selon un principe similaire à celui exposé en **§3.2**.

§4.3. Suites de fonctions, convergence uniforme calculable. On peut définir, selon le même principe qu'en **§3.1**, la notion de suite (puis, sans difficulté, de suite double) calculable $f_m : I \to \mathcal{R}$ de fonctions :

(i) pour toute suite calculable (u_k) de I, on impose à $(f_m(u_k))$ d'être calculable (en tant que suite double) ;

(ii) on impose à d d'être calculable (en tant que fonction de deux variables n et m).

On dit que $(f_{m,k})$ converge *calculablement uniformément* vers f_m si :

$$\exists e \in \mathcal{C}_2,\ \forall m, K \in \mathbf{N},\ \forall k \geq e(m,K),\ \|f_{m,k} - f_m\|_\infty < \frac{1}{2^K}$$

On montre aisément que la limite calculablement uniforme d'une suite double calculable de fonctions est encore une suite calculable de fonctions.

§4.4. La détermination des zéros n'est pas calculable (Pour-El / Richards [7], pp. 42–43). Pour justifier l'affirmation du **§4.2**, nous allons construire une suite $f_n : I \to \mathbf{R}$ de fonctions calculables vérifiant $\forall n \in \mathbf{N}$, $f_n(0) = -1$ et $f_n(1) = 1$, et telle qu'il n'existe pas de suite calculable (c_n) vérifiant $\forall n \in \mathbf{N}$, $f_n(c_n) = 0$.

On part de la suite double $(f_{n,k})$ de fonctions affines par morceaux définie par $f_{n,k}(0) = -1$, $f_{n,k}(1) = 1$ et :

$$f_{n,k}(1/3) = \begin{cases} 0 & \text{s'il n'existe pas d'entier } m \leq k \text{ tel que } n = b(m)\,; \\ -2^{-m} & \text{où } m = \min\{p \leq k;\ n = b(p)\} \text{ sinon.} \end{cases}$$

$$f_{n,k}(2/3) = \begin{cases} 0 & \text{s'il n'existe pas d'entier } m \leq k \text{ tel que } n = c(m)\,; \\ 2^{-m} & \text{où } m = \min\{p \leq k;\ n = c(p)\} \text{ sinon.} \end{cases}$$

La suite limite (f_n) est également affine par morceaux et vérifie :

$$f_n(1/3) = \begin{cases} 0 & \text{s'il n'existe pas d'entier } m \in \mathbf{N} \text{ tel que } n = b(m)\,; \\ -2^{-m} & \text{où } m = \min\{p \in \mathbf{N};\ n = b(p)\} \text{ sinon.} \end{cases}$$

$$f_n(2/3) = \begin{cases} 0 & \text{s'il n'existe pas d'entier } m \in \mathbf{N} \text{ tel que } n = c(m)\,; \\ 2^{-m} & \text{où } m = \min\{p \in \mathbf{N};\ n = c(p)\} \text{ sinon.} \end{cases}$$

De manière similaire à **§3.3**, la convergence est calculable aux points $1/3$ et $2/3$, donc calculablement uniforme puisque les fonctions sont affines par morceaux : la suite (f_n) est calculable.

Si $n \in$ B (resp. $n \in$ C), f_n admet un unique zéro en 2/3 (resp. 1/3) ; si $n \notin$ B $\cup$ C, f_n est nulle sur [1/3; 2/3]. Supposons qu'il existe (c_n) calculable. Pour n fixé, on peut calculer une approximation rationnelle r_n de c_n à 1/12 près ; alors $r_n > 1/2$ si $n \in$ B, $r_n < 1/2$ si $n \in$ C, ce qui permttrait de séparer calculablement B et C.

Conclusion

Les réels calculables forment un sous-corps *dénombrable* de **R** ; pourtant, c'est un corps réel clos (ce qu'on déduit facilement du théorème des valeurs intermédiaires du **§4.2**), qui semble contenir *tous* les réels particuliers que nous rencontrons usuellement.

L'analyse calculable s'avère ainsi une théorie séduisante pour mieux comprendre les réels que nous manipulons, et comment nous les manipulons ; nous n'avons donné ici qu'un aperçu très restreint des considérations qui peuvent la fonder, et du genre de résultats qu'un peut obtenir.

Références

[1] Oliver Aberth : Review : Marian B. Pour-El, J. Ian Richards, Computability in Analysis and Physics [7]. *The Journal of Symbolic Logic*, 56(2):749–750, 1991.

[2] René Cori et Daniel Lascar : *Logique mathématique*, volume 2. Dunod, 2003.

[3] Andrzej Grzegorczyk : Computable functionals. *Fundamenta Mathematicae*, 42:168–202, 1955.

[4] Andrzej Grzegorczyk : On the definitions of computable real continuous functions. *Fundamenta Mathematicae*, 44:61–71, 1957.

[5] Stephen C. Kleene : *Introduction to metamathematics*. North-Holland, 1952.

[6] Andrzej Mostowski : On computable sequences. *Fundamenta Mathematicae*, 44:37–51, 1957.

[7] Marian B. Pour-El et J. Ian Richards : *Computability in Analysis and Physics*. Springer-Verlag, 1989.

[8] H. G. Rice : Recursive real numbers. *Proceedings of the American Mathematical Society*, 5:784–791, 1954.

[9] Ernst Specker : Nicht konstruktiv beweisbare Sätze der Analysis. *The Journal of Symbolic Logic*, 14(3), 1949.

[10] Alan M. Turing : On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2 42:230–265, 1936–1937.

[11] Klaus Weihrauch : *Computable analysis*. Springer-Verlag, 2000.

[12] Pierre Wolper : *Introduction à la calculabilité*. Dunod, troisième édition, 2006.