Primitive, où te caches-tu ?
Une introduction à l'algèbre différentielle

Certains calculs de primitive ne relèvent pas de la virtuosité calculatoire... ils ne peuvent tout simplement pas être menés à bout avec des fonctions dites *élémentaires*. Pour exemple de telles fâcheuses primitives, il n'y a qu'à penser à la *vulgaire et sylvestre* $\int \mathrm{e}^{-x^2}\mathrm{d}x$ ou à la terrible $\int \frac{\sin(x)}{x}\mathrm{d}x$. (N'oublions pas que calculer une primitive est différent de l'évaluation d'une intégrale.)

Mais alors, où se cachent ces primitives ? Comment les trouver tant est que cela soit possible ? Pourquoi ne peut-on pas toujours exprimer la primitive d'une fonction donnée sous la forme d'une fonction dite élémentaire ?

Pour répondre à ces questions, nous nous baladerons dans les contrées de l'algèbre différentielle. Nous allons transposer des idées très intuitives et évidentes sur $\mathbb{R}$ ou $\mathbb{C}$ à un anneau ou un corps. Nous verrons par exemple en quoi l'arithmétique des polynômes ou des fractions rationnelles sur un corps k est déterminante dans la solution du problème (bien que cela semble surprenant !). On conclut en présentant sommairement une méthode effective et constructive : une procédure pour déterminer si oui ou non une fonction donnée admet une primitive élémentaire, et si oui la déterminer. On ne rentre pas dans les détails de l'implémentation (la description complète court sur une centaine de pages [Bro13]). L'auteur a pu en implémenter quelques bouts.

On profite enfin de quelques notes de bas de page pour présenter diverses ressources facilement accessibles, d'un intérêt premier et répondant à certaines questions que peut se poser le lecteur. Le lecteur bénéficiera sans doute de réserver ces ouvertures à une lecture ultérieure. De plus, quinze défis ont été parsemés le long du document.

Table des matières

Par l'habitude et l'intuition, on saisit bien en quoi consistent l'intégration et la différentiation. On pensera notamment aux représentations géométriques : aire sous la courbe, pente et taux de variation. On développe ensuite et perfectionne une capacité à manier ces objets lorsqu'on les formalise : limite, intégrale de Riemann, preuves ε-esques... Notre propos nous amène à découvrir une toute autre facette de ces objets : les considérations analytiques vont disparaître pour laisser place à un problème d'algèbre et d'arithmétique. Fort heureusement, nous allons nous retrouver en terrain connu puisque certains des énoncés que nous connaissions en analyse réelle se redémontrent dans ce nouveau cadre. Toutefois, l'algèbre différentielle ne se limite pas en une reformulation de ce que l'on sait déjà sur le corps des réels, c'en est aussi une généralisation.

1. Dérivation sur un corps k et propriétés élémentaires

1.1. **Anneaux et corps différentiels ([Kap57], [Bar07], [HB21]).** Supposons que l'on dispose d'un anneau commutatif et unitaire A. Un anneau différentiel (A, ∂) est un anneau muni d'une dérivation $\partial : A \to A$ vérifiant, pour tous f et g éléments de A :

$$\partial(f+g) = \partial(f) + \partial(g), \qquad \partial(fg) = \partial(f)g + f\partial(g). \tag{1}$$

On appelle alors corps différentiel un anneau différentiel (k, ∂) où k est un corps. Pour la suite (à moins d'une mention expresse du contraire), on se donne un corps différentiel commutatif (k, ∂).

L'étude de deux sous-corps vient naturellement à l'esprit : le noyau de ∂, noté $\ker(\partial)$, et son image, noté $\mathrm{Im}(\partial)$. Le noyau de la dérivation ∂ nous est déjà connu sous une autre forme. En effet, si l'on revient à la définition $\ker(\partial) = \{f \in k \mid \partial(f) = 0\}$ et que l'on pense à l'interprétation habituelle de $\frac{\mathrm{d}f}{\mathrm{d}x} = 0$, on constate alors que les éléments de $\ker(\partial)$ sont ce que l'on va appeler les constantes associées à la dérivation ∂. Le sous-corps formé par ces éléments est noté $\mathrm{Const}_\partial(k)$.

L'étude de $\mathrm{Im}(\partial)$ va s'avérer bien plus intrigante ! On dit d'un élément $g \in k$ qu'il appartient à l'image de la dérivation ∂ s'il existe $f \in k$ tel que $\partial(f) = g$. Réfléchissons à l'envers désormais : ne pourrait-on pas dire que f est une[1] "primitive" de g sur k ? Accepter une telle nomenclature revient à concevoir l'intégration comme l'opération inverse de la dérivation (ce à quoi nous sommes familiarisés). C'est exactement ce que nous allons faire. On peut dès lors formuler le problème : où se cache f ? Plus précisément, pour tout $g \in k$, quand existe-t-il $f \in k$ tel que $\partial(f) = g$. En d'autres termes, on cherche à mesurer le défaut de surjectivité[2] de la dérivation ∂. Et si jamais un tel f n'existe pas, peut-on aller chercher "au-dessus" de k (dans des extensions "plus grosses" que k) ?[3] Notre but va être de formaliser petit à petit tout cela.

1.2. **Exemples de dérivation.**

1.2.1. *Dérivation triviale.* La moins intéressante bien évidemment[4]. Elle est définie sur tout anneau A et vaut 0 en toutes circonstances.

Défi 1. *Montrer que la seule dérivation possible sur $\mathbb{Z}$ ou $\mathbb{Q}$ est la dérivation triviale.*

1.2.2. *Dérivation naturelle.* Sans elle, que faire ?[5] Pour la construire, formons $A[X]$ l'anneau des polynômes sur A en une indéterminée X. Prenons un polynôme $P = \sum_{i=0}^{n} a_i X^i$. Dans ce cas, la dérivation naturelle est définie comme suit : $D(P) = \sum_{i=1}^{n} i a_i X^{i-1}$. On remarque alors que $D(X) = 1$.

En introduisant une dérivation spécifique, on remarque que l'on peut ramener toute dérivation d'un polynôme à un calcul de dérivation sur les éléments du corps de base.

Proposition 2. *Soient ∂ une dérivation et D la dérivation naturelle, puis on définit la dérivation $P^\partial = \sum \partial(a_i) X^i$ d'un polynôme $P = \sum a_i X^i$ (avec cette dérivation on relève les coefficients). Alors, pour un élément u du corps de base considéré, on a :*

$$\partial(P(u)) = P^\partial(u) + D(P(u))\partial(u). \tag{2}$$

Démonstration. On développe, par linéarité, le membre de gauche :

$$\partial(P(u)) = \sum \partial(a_i u^i) = \sum \partial(a_i) u^i + \sum a_i \partial(u^i) = \sum \partial(a_i) u^i + \sum i a_i u^{i-1} \partial(u). \tag{3}$$

Ce qui conclut à la forme désirée. □

Plus généralement, on peut *mélanger* des dérivations entre elles pour en obtenir de nouvelles.

1.2.3. *Mélanges et combinaisons de dérivations.* Soient $(\partial_i)_{i\in[\![1,n]\!]}$ des dérivations définies sur un corps k. On remarque que, pour des scalaires λ_i, $\sum \lambda_i\partial_i$ est encore une dérivation (la preuve ne pose aucun soucis). On remarque, avec le défi suivant, qu'une dérivation peut se représenter comme combinaison d'autres dérivations.

Défi 3 ([Bar08])**.** *On se donne deux dérivations ∂ et δ de $k(X)$ définies comme suit : $\partial(X^n) = nX^{n-1}$ et $\delta(P) = X\partial(P)$ avec P un élément de $k(X)$. Prouver que :*

$$\delta^n = X^n\partial^n + \sum_{i=1}^{n-1}\Big(\sum_{j=1}^{i}\frac{(-1)^{i-j}}{i!}\binom{i}{j}j^n\Big)X^i\partial^i \tag{4}$$

où ∂^n (resp. δ^n) correspond à n compositions de ∂ (resp. δ).

1.3. **Premières propriétés ([Tre09], [ÉNS95]).** Sans beaucoup de surprise, on s'attend à ce que l'élément neutre 0 et unité 1 appartiennent à $\mathrm{Const}_\partial(k)$. C'est bien évidemment le cas : $\partial(0+0) = \partial(0)+\partial(0)$ et $\partial(1) = \partial(1\cdot 1) = \partial(1)\cdot 1 + 1\cdot\partial(1) = 2\cdot\partial(1)$ implique que $\partial(0) = 0$ et $\partial(1) = 0$. Nous allons voir que l'on peut espérer bien plus : soient n un entier et f un élément non nul de k, il vient par récurrence (exercice !) que $\partial(f^n) = nf^{n-1}\partial(f)$. De même, pour f et g deux éléments de k avec g inversible :

$$\partial(f) = \partial\big(f/g\cdot g\big) = \partial(f/g)g + f/g\partial(g), \tag{5}$$

on en déduit que :

$$\partial(f/g) = \frac{\partial(f)g - f\partial(g)}{g^2}. \tag{6}$$

Défi 4. *Prouver la formule de dérivation logarithmique (évidemment semblable à l'habituelle). Soient des coefficients e_i entiers et des éléments inversibles f :*

$$\partial\Big(\prod_{i=1}^{n} f_i^{e_i}\Big)\Big/\prod_{i=1}^{n} f_i^{e_i} = \sum_{i=1}^{n} e_i\frac{\partial(f_i)}{f_i}. \tag{7}$$

1.4. **Règle de Leibniz.** On peut aisément généraliser la règle du produit $\partial(fg) = \partial(f)g + f\partial(g)$.

Proposition 5. *Soient f et g deux éléments de k et n un entier naturel. Alors :*

$$\partial^n(fg) = \sum_{i=0}^{n}\binom{n}{i}\partial^i(f)\partial^{n-i}(g). \tag{8}$$

La preuve ne soulève pas de difficulté, c'est une simple récurrence très similaire à celle faite pour démontrer la formule du binôme de Newton. Il existe en réalité une explication à pareille ressemblance entre ces deux formules[6].

1.5. **Pour aller plus loin – compilation de défis.** Accessible en première ou deuxième année, on peut se référer à l'exercice X1.11 de [Kou18] sur le crochet de Lie et ses principales propriétés. Pour découvrir des dérivations exotiques on pourra faire l'exercice 19 page 342 de [Hel01] sur la dérivation galoisienne de $\mathbb{F}_q[t]$ ou étudier une dérivation en deux variables [Now08]. Dans certains cas, on peut classifier les dérivations (dérivations intérieures de $\mathcal{M}_n(k)$, de certaines algèbres de Jordan [Jac49 ; Sch49] ou bien considérer les dérivations extérieures et le problème de Johnson [AM19]). On peut également s'amuser à faire de l'arithmétique ou de l'algèbre (en caractéristique p avec la formule de Hochschild [MR89, § 25], la formule de Barsotti-Cartier [Zin, part. II, chap. IV-B] ou en définissant un opérateur exponentiel [Mat16] voire en *tordant* des opérations usuelles en considérant les polynômes de Ore [Car18], ou en cherchant des dérivations vérifiant des relations polynomiales [Now89]). Enfin, pour une exposition à la rigueur bourbakiste, on consultera [Bou98, III, § 10, n°2].

Pour la belle histoire, un chercheur de l'Institut de Mathématiques de Toulouse viendrait de résoudre une conjecture d'algèbre différentielle [Ete23].

2. Arithmétique dans $k[X]$, $k(X)$ et au-delà

2.1. **Avec $\mathbb{Q}[X]$ on est loin du compte !** Néanmoins, tout n'est pas à plaindre... Donnons nous un polynôme $P = \sum a_i X^i$, existe-t-il un polynôme $Q \in \mathbb{Q}[X]$ tel que $\partial(Q) = P$, avec ∂ la dérivation naturelle ? Autrement dit, la primitive d'un polynôme à coefficient rationnel est-elle un polynôme à coefficient rationnel ? Oui, évidemment, il suffit de prendre $Q = \sum \frac{a_i}{i+1} X^{i+1}$.

Posons nous la même question pour $P = \sqrt{1-X^2}$: existe-t-il un polynôme $Q = \sum a_i X^i$ tel que $\partial(Q) = P$? Montrons, par l'absurde, que cela est impossible. Si un tel Q existait, on aurait alors nécessairement $\left(\sum i a_i X^{i-1}\right)^2 = 1 - X^2$. Une considération sur le degré oblige le côté gauche de l'équation à être de degré 2. On obtient alors : $(a_1 + 2a_2 X)^2 = 1 - X^2$. Donc :

$$a_1^2 + 4a_1 a_2 X + 4a_2^2 X^2 = 1 - X^2. \tag{9}$$

Par identification, on voit que c'est impossible : il n'existe pas de rationnel a_2 tel que $4a_2^2 = -1$.

Peut-être pouvons nous chercher au-delà des polynômes : chez les fractions rationnelles ? Cela ne va pas toujours suffire, comme on va de suite le constater avec un autre exemple.

2.2. **À la recherche de la primitive de $1/X$ dans $\mathbb{Q}(X)$.** Classiquement, une primitive de $1/X$ est $\log|X|$. Tout du moins, on obtient ce résultat lorsque l'on regarde dans une classe de fonctions suffisamment grande. Que peut-on espérer si l'on traite ce problème sur $\mathbb{Q}(X)$ par exemple ? La fonction admet-elle nécessairement une primitive (dans ce corps différentiel) ? Si la réponse est négative, où doit-on la chercher ?

Proposition 6 ([Tre09])**.** *La fonction $1/X$ n'admet pas de primitive dans $(\mathbb{Q}(X), \partial)$: il n'existe pas deux polynômes premiers entre eux p et $q \neq 0$ à coefficients dans $\mathbb{Q}$ tels que $1/X = \partial(p/q)$.*

Démonstration. Nous allons chercher à aboutir à une absurdité. Supposons alors qu'il existe p et $q \neq 0$ premiers entre eux tels que $1/X = \partial(p/q)$. Ainsi :

$$\frac{1}{X} = \partial(p/q) = \frac{\partial(p)q - p\partial(q)}{q^2}. \tag{10}$$

En multipliant par X et q^2, on remarque que X doit diviser q ce qui permet alors d'écrire $q = X^n q_0$ pour n et q_0 convenables (X ne divisant pas q_0). On injecte alors la nouvelle expression de q :

(11)
$$q^2 = X(\partial(p)q - p\partial(q)) \iff X^{2n} q_0^2 = Xq\partial(p) - Xp\partial(q) = X^{n+1} q_0 \partial(p) - npX^n q_0 - pX^{n+1}\partial(q_0).$$

On simplifie :

$$X^n q_0^2 = Xq_0\partial(p) - npq_0 - pX\partial(q_0). \tag{12}$$

On voit que l'on peut factoriser par X en manipulant l'équation :

$$npq_0 = X(q_0\partial(p) - p\partial(q_0) - X^{n-1} q_0^2). \tag{13}$$

Or, X ne divisant pas q_0, la précédente égalité nous assurerait que X divise p. Ceci est impossible (autrement X serait un facteur commun à p et q, or ils sont premiers entre eux). En conclusion, la fonction $1/X$ n'admet pas de primitive dans le corps différentiel considéré. □

Défi 7. *Même question pour* $f(X) = \dfrac{1}{1+X^2}$.

2.3. **Extension de corps.** Au regard de la proposition précédente, on est un petit peu embêté de ne pas trouver notre fameux logarithme comme primitive. Où se cache-t-il ? Il va falloir aller voir *au-dessus* du corps des rationnels : dans une extension (plus ou moins "grosse") ! L'idée va consister à ajouter des "quantités" à un corps de base pour l'*étendre* et espérer qu'une primitive existe dans l'extension ainsi formée. En particulier, on ne va considérer que trois types de quantités : les quantités dites algébriques, exponentielles et logarithmiques. Remarquons

qu'indirectement d'autres quantités sont alors contenues : par exemple, grâce aux quantités exponentielles, on peut former des quantités trigonométriques.

Soit K une extension du corps k ($k = \mathbb{Q}(X)$ pour nous), cad. $k \subset K$ et K est un corps.

Définition 8 ([Tre09]). *Soit $t \in K$.*
- *On dit que t est **algébrique** sur k s'il est racine d'un polynôme non nul à coefficients dans k. Autrement, il est dit **transcendant** sur k.*
- *On dit que t est une **exponentielle** sur k s'il existe un élément $f \in k$ tel que $\partial(t) = t\partial(f)$.*
- *On dit que t est un **logarithme** sur k s'il existe un élément $f \in k^\times$ tel que $\partial(t) = \partial(f)/f$.*

*Enfin, t est **élémentaire** sur k s'il est algébrique, exponentielle ou logarithmique sur k.*

Notre but est de construire une extension convenable, dite élémentaire, dans laquelle on peut être sûr de trouver la primitive, si elle existe, d'une fonction donnée. On va donc partir de notre corps de base $k = \mathbb{Q}(X)$ et lui adjoindre[7] des quantités algébriques, exponentielles ou logarithmiques jusqu'à être sûr qu'une primitive vive dans l'extension formée. Le théorème 12 nous donnera alors la forme que doit revêtir notre fonction pour qu'elle admette une primitive dans l'extension élémentaire.

L'adjonction d'un élément t_1 au corps k se note $k(t_1)$. On peut alors adjoindre un nouvel élément t_2 pour obtenir une nouvelle extension $k(t_1, t_2)$. Ainsi, on construit une *tour de corps* $k \subset k(t_1) \subset k(t_1, t_2) \subset k(t_1, t_2, t_3) \subset ...$

Définition 9 ([Tre09]). *On dit que K est une **extension élémentaire** de k s'il existe des éléments $t_1, t_2, \dots, t_n$ de K tels que $K = k(t_1, t_2, \dots, t_n)$ et t_i est élémentaire sur $k(t_1, t_2, \dots, t_{i-1})$ pour tout $i \in [\![1, n]\!]$.*

Ce peut être un exercice amusant de déterminer l'extension élémentaire dans laquelle vit une fonction. Prenons l'exemple de $f(x) = \exp(x/2) + \exp(x) + \exp(2x)$. On se dit que $\mathbb{Q}(x, t_1, t_2, t_3)$ doit convenir, avec $t_1 = \exp(x/2)$, $t_2 = \exp(x)$, $t_3 = \exp(2x)$. On remarque alors que $f = t_1 + t_2 + t_3$ et t_1 est une exponentielle sur $\mathbb{Q}(x)$, t_2 est une exponentielle sur $\mathbb{Q}(x, t_1)$, et t_3 est une exponentielle sur $\mathbb{Q}(x, t_1, t_2)$. Or, ce n'est pas la seule extension élémentaire contenant f, on en a par exemple une autre bien plus agréable : posons $\theta = \exp(x/2)$. On remarque alors que $f = \theta + \theta^2 + \theta^4 \in \mathbb{Q}(x, \theta)$.

Défi 10. *Même travail : $f(x) = \sqrt{\ln(x^2 + 3x + 2)(\ln(x + 1) + \ln(x + 2))}$, $g(x) = x^\alpha$ ($\alpha \in \mathbb{Q}$).*

Maintenant que l'on sait où chercher, il ne reste plus qu'à le faire !

3. De la décomposition en éléments simples au théorème de Liouville

C'est bien l'une des seules fois que l'on va être content de se servir de la décomposition en éléments simples (sur un corps k) !

3.1. Décomposition en éléments simples.

Théorème 11 ([God63]). *Soit k un corps commutatif et $f(X) = p(X)/q(X)$ une fraction rationnelle à une indéterminée à coefficients dans k avec $q(X) = q_1(X)^{r_1} \dots q_n(X)^{r_n}$ où les polynômes irréductibles q_i sont deux à deux non proportionnels. On a l'unique décomposition :*

$$f(X) = g(X) + \sum_{i=1}^{n} \sum_{0 \le r \le r_i} \frac{h_{i,r}(X)}{q_i(X)^r} \tag{14}$$

avec g et $h_{i,r}$ des polynômes tels que $\deg(h_{i,r}) < \deg(q_i)$ quels que soient i et r.

Remarquons que lorsque $k = \mathbb{C}$ les polynômes $h_{i,r}$ sont nécessairement des constantes et dans le cas où $k = \mathbb{R}$ ce sont des polynômes de degré 1 au plus.

Habituellement, on se sert de la décomposition en éléments simples d'une fraction rationnelle afin de pouvoir l'intégrer : on *casse* la fraction rationnelle en petits bouts que l'on sait intégrer terme à terme. Il n'y a pas à en demander plus : nous avons un algorithme simple à mettre en œuvre pour déterminer la primitive d'une première classe de fonctions. En revanche, cet algorithme semble loin d'être le bon... on doit factoriser le numérateur et le dénominateur de la fraction rationnelle afin de pouvoir opérer la décomposition. Le problème étant, qu'en toute généralité, on ne sait pas le faire (autrement, on pourrait déterminer les racines d'un polynôme quelconque).

Fort heureusement, on peut se sortir de ce pétrin. Le développement étant surtout technique, on renvoie au chapitre 2 de [Bro13]. La bonne nouvelle étant, *qu'en théorie*, on dispose d'un algorithme pour traiter avec les fractions rationnelles. Qu'attendre alors d'autres classes de fonctions ? L'une des devises de la théorie fondée par Liouville, dont on s'apprête à découvrir le principal résultat dans la partie suivante, peut se résumer ainsi : *si une fonction s'exprime "relativement simplement" alors, si elle possède une primitive, cette dernière doit être "relativement simple"*. Le théorème 12 nous donne la forme exacte de la primitive, lorsqu'elle existe. On peut également tirer profit de ce théorème en montrant qu'une fonction n'admet pas de primitive élémentaire (c'est-à-dire qu'il n'existe pas de primitive dans une extension élémentaire).

3.2. **Théorème de Liouville-Rosenlicht.**

Théorème 12 ([Bro13])**.** *Soit (k, ∂) un corps différentiel et f un élément de k. S'il existe une extension élémentaire E de k vérifiant*[8] $\mathrm{Const}_\partial(k) = \mathrm{Const}_\partial(E)$ *et qu'il existe un élément g de E tel que $\partial(g) = f$, alors il existe $v \in k$, $u_1, \dots, u_n \in k^*$ et $c_1, \dots, c_n \in \mathrm{Const}_\partial(k)$ tels que :*

$$f = \partial(v) + \sum_{i=1}^{n} c_i \frac{\partial(u_i)}{u_i}.^{9} \tag{15}$$

Formellement, on voit une certaine ressemblance entre la décomposition en éléments simples (équation 14) et l'expression de f (équation 9). Ce n'est pas que pur apparence ! À titre d'exemple, la plupart des algorithmes d'intégration symbolique reposent sur et généralisent des techniques utilisées pour l'intégration des fonctions rationnelles.

3.3. **À la recherche de la primitive de** $\exp(-x^2)$**.**

Nous pouvons enfin toucher au but ! Nous allons montrer qu'il n'existe pas d'extension raisonnable (c'est-à-dire plus grosse que $\mathbb{C}(X)$) dans laquelle on peut trouver une primitive élémentaire de $\exp(-x^2)$. Pour ce faire, nous avons besoin d'un résultat découlant du théorème de Liouville-Rosenlicht[10].

Corollaire 13. *Soient f et g deux éléments inversibles de $\mathbb{C}(X)$, avec g non constant. Alors la primitive $\int f(X)\exp(g(X))\mathrm{d}X$ est élémentaire si et seulement si $f(X) = a'(X) + a(X)g'(X)$ pour un élément a de $\mathbb{C}(X)$.*

Idée de démonstration ([Con, § 5]). On laisse le sens évident en exercice. Supposons que la primitive de $f(X)\exp(g(X))$ soit élémentaire. Par le théorème 12, on peut alors écrire :

$$f\exp(g) = \partial(v) + \sum_{i=1}^{n} c_i \frac{\partial(u_i)}{u_i} \tag{16}$$

avec $v \in \mathbb{C}(X)$, $u_1, \dots, u_n \in \mathbb{C}(X)^*$ et $c_1, \dots, c_n \in \mathrm{Const}_\partial(\mathbb{C}(X)) = \mathbb{C}$. L'objectif va être de ramener un problème transcendantal (incluant une exponentielle) à de pures considérations algébriques. Qu'à cela ne tienne, raisonnons sur $\mathbb{C}(X, Y)$. On sent que v et les u_i doivent dépendre de f **et** de $\exp(g)$. Faisons apparaître explicitement ces dépendances en ayant posé $\exp(g) = Y$:

$$f(X)Y = \partial(v(X,Y)) + \sum_{i=1}^{n} c_i \frac{\partial(u_i(X,Y))}{u_i(X,Y)}. \tag{17}$$

On montre par des considérations similaires à celles de la section 1.3 une formule de dérivation dans $\mathbb{C}(X,Y)$ (après avoir décomposé de v sous la forme p/q) :

$$\partial(v(X,Y)) = \frac{\partial(p(X,Y))q(X,Y) - p(X,Y)\partial(q(X,Y))}{q(X,Y)^2}. \tag{18}$$

On veut alors montrer l'existence d'un élément a de $\mathbb{C}(X)$ tel que $f(X) = a'(X) + a(X)g'(X)$. On va chercher à faire apparaître une quantité $h(X)$ telle que $f(X)Y = h(X)Y$. Pour ce faire, l'idée est de constater que le dénominateur de $f(X)Y$ ne peut pas dépendre de Y (puisque Y apparaît seulement au numérateur). Il doit en être alors de même du côté droit de l'équation (17) une fois (18) injecté dedans. Cela revient à dire qu'un certain nombre de termes doivent s'annuler pour avoir un dénominateur ne dépendant pas de Y. Tout n'est désormais plus qu'un problème de divisibilité ! On se demande quand est-ce que tel polynôme divise tel polynôme (afin de savoir quand un Y est susceptible d'apparaître au dénominateur). Enfin, moyennant, des divisions à la chaîne et en déterminant la seule forme possible pour le dénominateur du côté droit de l'équation (17), on en déduit la forme convenue de $h(X)$. □

Défi 14. *Prouver que* $\int \exp(-x^2)$ *n'admet pas de primitive élémentaire. Indice : suivre les idées de la preuve de la proposition 6 pour aboutir à une contradiction basée sur le corollaire 13.*

4. Primitive de fonctions : l'algorithme de Risch

Il est relativement simple de concevoir un algorithme pour dériver une expression symbolique (on sait que dans le pire des cas une méthode de type brute force fonctionnera). Il y a un aspect très combinatoire au problème (ce qui donne sans doute une raison de plus à la ressemblance entre la formule du binôme de Newton et celle de dérivation de Leibniz). En revanche, lorsqu'il s'agit d'intégrer symboliquement une expression, on se trouve (en toute généralité) démuni.

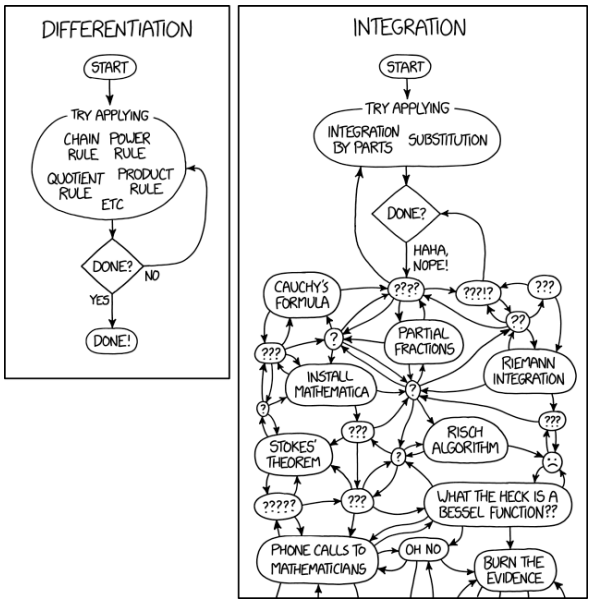

Figure 1 – xkcd

Décomposons le problème. On connaît un algorithme (très intuitif) pour intégrer des fractions rationnelles. On a déjà évoqué les limites pratiques d'une telle méthode. Existe-t-il une approche algorithmiquement moins couteuse ? Au lieu de chercher à factoriser complètement le dénominateur d'une fraction (comme on peut le faire dans le théorème 11), on peut ajouter une contrainte (par exemple une décomposition sans facteur carré). Le problème n'est pas définitivement réglé, mais on avance. Bronstein [Bro13, p. 58] propose par exemple un algorithme utilisant la factorisation sans facteur carré de Yun (et les séries de Laurent).

À ce stade là, on a l'impression d'avoir fait un petit peu le tour de nos fractions rationnelles. Peut-on adjoindre de nouvelles fonctions (l'exponentielle, le logarithme, le sinus cardinal...) ? Oui, on l'a par ailleurs fait implicitement dans la partie 3.3. Tout le savoir accumulé sur les fractions rationnelles va enfin pouvoir être utilisé à bon escient dans un cadre plus général !

Précisons tout d'abord que l'algorithme de Risch n'est pas monolithique. C'est un complexe qui se décline dans diverses situations [Par23]. L'une des idées maîtresses est de procéder parallèlement à ce que l'on a fait dans la preuve du corollaire 13 : on transforme un problème faisant

intervenir des quantités non algébriques en un problème purement algébrique (en considérant des extensions et en introduisant de nouvelles variables algébriques encodant **formellement** des quantités transcendantales par exemple). Comme on sait résoudre le problème de primitivation pour les fractions rationnelles, il n'y a plus qu'à procéder par récurrence sur la longueur de l'extension élémentaire. La tâche est néanmoins extrêmement ardue à tel point qu'il ne semble exister aucune implémentation complète de l'algorithme [Cho].

La contribution informatique de l'auteur se ramène à une découverte de divers algorithmes tendant vers l'algorithme de Risch (ainsi qu'une implémentation d'un artificiel et très simple langage symbolique). On en trouvera le contenu sur le dépôt ci-joint. L'auteur s'excuse d'avoir programmé en Python. Une version Haskell est prévue pour un futur encore quelque peu lointain.

Remarques

1. Prenons garde de ne pas considérer f comme *la* primitive de g. En effet, si f_1 et f_2 sont deux primitives différentes de g alors $\partial(f_1 - f_2) = \partial(f_1) - \partial(f_2) = 0$, autrement dit $f_1 - f_2 \in \mathrm{Const}_\partial(k)$. Comme d'habitude, deux primitives de g diffèrent d'une constante.
2. On rappelle qu'un morphisme $\chi : X \to Y$ est surjectif si $\forall y \in Y, \exists x \in X, \chi(x) = y$. On voit l'évident lien entre notre problème et la "recherche de la surjectivité" de ∂. En suivant le rude mais passionnant [Bar07] et en adoptant un point de vue catégorique, on pourrait être amené à penser en terme de conoyau.
3. Pour une approche analytique de la question, cf. l'article de la RMS [Ant99].
4. Mais sans elle, l'ensemble de toutes les dérivations sur un corps commutatif k ne formerait pas un k-espace vectoriel. On trouve un raffinement de ce résultat dans [Tre09, p. 12 et 13]. Cela montre un peu de structure chez nos dérivations !
5. Sans la dérivation naturelle que faire effectivement... tout du moins en caractéristique zéro ! En caractéristique p, certains énoncés perdent leur sens. Par exemple, il n'est pas toujours vrai pour un polynôme P que $\partial(P) = 0$ si et seulement si P est constant. Le rôle de la dérivation de Hasse-Schmidt est de généraliser la dérivation usuelle tout en s'assurant notamment que ce qui se passe bien en caractéristique 0 se passe bien en caractéristique p.
6. Prouver que l'on peut déduire la formule de Leibniz de la formule de Newton et inversement se fait plus simplement dans un sens que dans l'autre. Dans un cas, il suffit de considérer l'application exponentielle, dans l'autre on doit construire convenablement une nouvelle opération (le produit tensoriel) et certains endomorphismes. Pour plus de précisions sur ce beau lien, on fera le DM 23 donné à Louis Le Grand.
7. Adjoindre des éléments à k revient ici à considérer, intuitivement, le corps engendré par ces quantités.
8. On passe le détail de l'importance des constantes, se référer à [Bro13, p. 83 et s.]. On cherche uniquement à avoir une vue d'ensemble et une compréhension globale du résultat. De même, on laisse totalement de côté le cas hyperexponentiel.
9. Prouvons le théorème 12. On pourra par exemple consulter [Tre09, p. 30] ou [Bro13, p. 138 et s.] pour des précisions.

Défi 15. [11] *Soit $E = k(t_1, t_2, \ldots, t_m)$ une extension élémentaire de k. On rappelle que l'on dispose de la tour de corps suivante :*

$$k \subset k(t_1) \subset k(t_1, t_2) \subset \ldots \subset k(t_1, t_2, \ldots, t_m) = E. \tag{19}$$

Procédons par récurrence sur la "longueur" de la tour de corps, c'est-à-dire sur m.

Dans un premier temps, prouver que l'initialisation ($m = 0$) est vérifiée. Une fois fait, supposer qu'il existe un entier naturel $N = m$ tel que le théorème soit vérifié pour une tour de corps de longueur N. C'est en particulier le cas de la tour de corps à laquelle on enlève k. Comme le résultat est vérifié pour les N extensions $k(t_1) \subset k(t_1, t_2) \subset \ldots \subset k(t_1, t_2, \ldots, t_N)$, il l'est en particulier pour $k(t_1)$. On sait alors, par l'hypothèse de récurrence, qu'il existe $v \in k(t_1)$, $u_1, \ldots, u_n \in k(t_1)^*$ et $c_1, \ldots, c_n \in \mathrm{Const}_\partial(k(t_1))$ tels que $f = \partial(v) + \sum_{i=1}^n c_i \frac{\partial(u_i)}{u_i}$, avec $f \in k$. Sous couvert de l'hypothèse de récurrence, montrer que le résultat est vrai pour une tour de corps de longueur $N + 1$ revient à prouver que l'implication suivante est vraie : si f peut s'écrire sous la forme (9) dans $k(t_1)$ alors f peut s'écrire sous une forme similaire dans k (quitte à avoir d'autres coefficients). Ce qui conclura.

Une disjonction de cas nous invite à considérer les trois différents cas possibles.

Cas 1. *(t_1 **algébrique sur** k) Comme supposé précédemment, on travaille sur le corps commutatif $k = \mathbb{Q}(X)$. Modulo une petite perte de généralité (qui n'est pas problématique si l'on ne s'intéresse qu'aux grandes lignes de la preuve), on peut alors voir E comme un k-espace vectoriel sur lequel on définit naturellement la trace et la norme d'un élément de $x \in E$. La trace $\mathrm{Tr}(\cdot)$ de x est la trace de son application linéaire associée $m_x = xy$ (la multiplication par x dans E). De même, on définit la norme $N(\cdot)$ de $x \in E$*

comme le déterminant de son application linéaire associée m_x. Remarquer que $\mathrm{Tr}(f) = f\dim_k(E)$, *pour* $f \in k$. *Prouver que, pour tout* $a \in E^*$, *on a :*

$$\mathrm{Tr}(\partial(a)) = \partial(\mathrm{Tr}(a)) \text{ et } \mathrm{Tr}\Big(\frac{\partial(a)}{a}\Big) = \frac{\partial(N(a))}{N(a)}. \tag{20}$$

Appliquer la trace de chaque côté de l'équation (9) puis conclure. Question subsidiaire : où a été (implicitement) utilisé le caractère algébrique sur k *de* t_1 *?*

Cas 2. *(*t_1 ***transcendant sur*** k, *[MS08]) Supposons* t_1 *transcendant sur* k. *On peut factoriser les* $u_i(t)$ *sous la forme* $\lambda q_1(t)^{r_1} \dots q_s(t)^{r_s}$ *avec les* q_i *des polynômes irréductibles et unitaires. Appliquer la formule de dérivation logarithmique (4) pour montrer que :*

$$\frac{\partial(u_i)}{u_i} = \frac{\partial(\lambda)}{\lambda} + \sum_{k=1}^{s} r_k \frac{\partial(P_k)}{P_k}. \tag{21}$$

En injectant (21) dans (9), on voit que l'on peut raisonner uniquement avec des polynômes irréductibles. Le même raisonnement s'applique pour v. *On obtient alors une bien grande expression de* f. *Montrer que dans cette expression il n'existe pas de polynômes* P *dits normaux, c'est à dire que l'on n'a jamais* $\mathrm{pgcd}(P, \partial(P)) = 1$.

Comme l'extension considérée est élémentaire, il ne reste plus qu'à considérer les cas logarithmiques et exponentiels.

Cas 2.A. *(*t_1 ***logarithmique sur*** k*) Comme* t_1 *est logarithmique, il existe* $a \in k^*$ *tel que* $\partial(t_1) = \partial(a)/a$. *Prouver que tout polynôme* $p \in k[t_1]$ *est normal. Ainsi une partie de l'expression de* f *est nulle. Montrer alors que* $\partial(v)$ *est un élément de* k. *En déduire que* $v = \mu t_1 + \nu$ *avec* μ *et* ν *deux éléments de* k. *En déduire alors une expression de* f *sous la forme voulue (qui dépend donc de* a*).*

Cas 2.B. *(*t_1 ***exponentiel sur*** k*) Comme* t_1 *est exponentiel, il existe* $a \in k^*$ *tel que* $\partial(t_1)/t_1 = a$. *Procéder similairement au cas logarithmique à la différence cette fois ci que l'expression de* f *possède un (seul) élément normal.*

10. Pour d'autres applications, par exemple les intégrales elliptiques, on pourra considérer avec intérêt [Con, p. 8].
11. Pour les plus intéressés, il existe une démonstration plus sophistiquée (utilisant des résultats de théorie de Galois) mais, apparemment, plus naturelle.

Références

[Jac49] N. Jacobson. ***Derivation Algebras and Multiplication Algebras of Semi-Simple Jordan Algebras***. 1949.

[Sch49] R. D. Schafer. ***Inner derivations of non-associative algebras***. 1949.

[Kap57] I. Kaplansky. ***An Introduction to Differential Algebra***. 1957.

[God63] R. Godement. ***Cours d'algèbre***. 1963.

[MR89] H. Matsumura et M. Reid. ***Commutative Ring Theory***. 1989.

[Now89] Nowicki. ***Derivations satisfying polynomial identities***. 1989.

[ÉNS95] ÉNS. ***Épreuve de mathématiques commune à Lyon et Cachan***. 1995.

[Bou98] N. Bourbaki. ***Algebra I : Chapters 1-3***. 1998.

[Ant99] R. Antetomaso. « **Sous-espaces stables par primitivation** ». In : *RMS* (1999).

[Hel01] Y. Hellegouarch. ***Invitation aux mathématiques de Fermat-Wiles***. 2001.

[Bar07] C. Bardavid. ***Notions de base en théorie de Galois différentielle***. 2007.

[Bar08] C. Bardavid. ***Lien entre les dérivations ∂ et δ***. 2008.

[MS08] A. Moussaoui et R. Santharoubane. ***Primitives élémentaires de fonctions élémentaires***. 2008.

[Now08] Nowicki. ***An example of a simple derivation in two variables***. 2008.

[Tre09] P. Tremblay. ***Intégration à l'usage du mathématicien, extensions transcendantes***. 2009.

[Bro13] M. Bronstein. ***Symbolic Integration I : Transcendental Functions***. 2013.

[Mat16] S. Mattarei. ***Exponentials of derivations in prime characteristic***. 2016.

[Car18] X. Caruso. ***Polynômes de Ore en une variable***. 2018.

[Kou18] É. Kouris. ***Une année de colles en math sup MPSI***. 2018.

[AM19] A. A. Arutyunov et A. S. Mishchenko. ***A smooth version of Johnson's problem on derivations of group algebras***. 2019.

[HB21] E. Hecky et G. Bartlett. ***Algèbre différentielle***. 2021.
[Ete23] A. Etesse. ***On the Schmidt–Kolchin conjecture on differentially homogeneous polynomials. Applications to (twisted) jet differentials on projective spaces***. 2023.
[Par23] B. Parisse. ***Intégration (l'algorithme de Risch)***. 2023.
[Cho] T. Chow. ***Does there exist a complete implementation of the Risch algorithm ? (Mathoverflow)***.
[Con] B. Conrad. ***Impossibility theorems for elementary integration***.
[Zin] Zinn-Justin. ***Dérivations dans les corps et anneaux de caractéristique*** p.