Astérisque

DANIEL LAZARD

Primitives des fonctions élémentaires

Astérisque, tome 121-122 (1985), Séminaire Bourbaki,
exp. n° 630, p. 295-308

<http://www.numdam.org/item?id=SB_1983-1984__26__295_0>

Séminaire BOURBAKI
36e année, 1983-84, n° 630 Juin 1984

PRIMITIVES DES FONCTIONS ÉLÉMENTAIRES
(d'après Risch et Davenport)

par Daniel LAZARD

INTRODUCTION

Le calcul intégral se divise en deux parties complémentaires : le calcul des intégrales "définies" ou calcul des aires et celui des intégrales "indéfinies" ou calcul des primitives. Que le premier soit susceptible de traitement par ordinateur est maintenant une évidence ; c'est beaucoup moins connu pour le second bien que de très importants progrès dans la théorie du calcul des primitives ont eu lieu depuis 1969, en liaison très intime avec la programmation effective.

La dérivation est une opération très simple qui peut se programmer ainsi :

dérive(f,x):= si "f indépendant de x" alors 0 ;
si f = x alors 1 ;
si "f = g+h" alors dérive(g,x) + dérive(h,x) ;
Si "f = g.h" alors g.dérive(h,x)+dérive(g,x).h ; ...

Les seuls problèmes, qui sortent du cadre de cet exposé, résident dans la représentation de f et la programmation des tests entre guillemets ainsi que dans la simplification du résultat.

Au contraire, l'opération inverse qu'est le calcul de la primitive pose de nombreux problèmes : s'il est vrai que toute fonction continue admet une primitive, cet ensemble non dénombrable de fonctions est trop grand pour que ses éléments puissent être représentés en machine. Il faut donc se limiter à un ensemble plus restreint : nous prendrons les fonctions *élémentaires*, c'est-à-dire les fonctions qui peuvent s'écrire à partir des éléments de $\mathbb{Z}$ et de x en itérant les 4 opérations rationnelles ainsi que la prise de logarithmes, d'exponentielles ou l'extraction de racines de polynômes. Ce corps n'est pas stable pour l'intégration, et le problème, encore ouvert, doit donc être reformulé ainsi ;

Etant donnée une fonction élémentaire, calculer sa primitive ou démontrer qu'elle n'est pas élémentaire.

Un deuxième problème réside dans la représentation multiple des logarithmes complexes et des racines. La solution employée consiste en une formulation purement algébrique qui ramène le choix des déterminations des logarithmes ou des racines au

choix d'isomorphismes vers les fonctions continues. Il est nécessaire de préciser cette formulation algébrique avant de pouvoir énoncer les principaux théorèmes.

1. FONCTIONS ÉLÉMENTAIRES. ÉTAT DE LA THÉORIE.

Un *corps différentiel* est un corps K muni d'une fonction D de K dans K, la *dérivation* telle que $D(f+g) = D(f)+D(g)$ et $D(fg) = fD(g)+gD(f)$. La dérivation de f sera noté f'. Le corps $Q(x)$ sera toujours considéré comme muni de l'unique dérivation telle que $x' = 1$. On appelle *constante* un élément de dérivée nulle.

Si $f'=fg'$ on dit que f est une *exponentielle* de g et g un *logarithme* de f. On note $f = e^g$ et $g = \log f$.

Une extension *élémentaire simple* $K(f)$ d'un corps différentiel K est une extension différentielle où f est soit une constante, soit algébrique sur K, soit le logarithme d'un élément de K, soit l'exponentielle d'un élément de K. Une *extension élémentaire* $K(f_1,\ldots,f_k)$ de K est une extention telle que $K(f_1,\ldots,f_i)$ soit une extension élémentaire simple de $K(f_1,\ldots,f_{i-1})$ pour tout i. Une extension élémentaire est *algébrique* (resp. *purement transcendante*) si chaque f_i non constant est algébrique (resp. transcendant sur $K(f_1,\ldots,f_{i-1})$) ; ainsi $Q(x,f,e^{f/2})$ avec $f=\log(x)$ n'est pas purement transcendante.

Enfin on appelle *fonction élémentaire, fonction élémentaire purement transcendante, fonction algébrique* un élément d'une extension correspondante de $Q(x)$.

L'état actuel des connaissances théoriques est résumé par les trois théorèmes suivants dans l'énoncé desquels "integrer" signifie "calculer une primitive dans une extension élémentaire ou démontrer qu'il n'y a pas de telle primitive".

THÉORÈME 1 (Risch, 1969). Il existe un algorithme pour intégrer les fonctions élémentaire purement transcendantes.

THÉORÈME 2 (Davenport, 1979). Il existe un algorithme pour intégrer les fonctions algébriques.

THÉORÈME 3 (Davenport, 1983). Il existe un algorithme pour intégrer les fonctions élémentaires purement transcendantes sur une extension algébrique de $Q(x)$.

L'état d'avancement de la programmation est le suivant : l'algorithme de Risch a été programmé par Moses et est disponible dans MACSYMA. L'algorithme de Davenport -1979 a été programmé par lui-même et est disponible sous REDUCE (MULTICS de Grenoble). Il est toutefois limité aux fonctions où les seules racines qui apparaissent sont des racines carrées, éventuellement imbriquées. La raison de cette restriction est que le maniement des nombres algébriques est actuellement très mal maitrisé : on ne sait pas contourner les problèmes posés par la taille exponentielle du groupe de Galois ni contrôler la taille des entiers qui interviennent. Il s'agit d'un domaine de recherche presqu'inexploré. Enfin, la programmation de l'algorithme

de Davenport-1983 n'a pas encore été entreprise.

Tous ces algorithmes sont basés sur le théorème suivant qui prédit la forme de la primitive ; ce théorème remonte à Liouville (1833), mais la forme précise ci-dessous est due à Risch (1969).

THÉORÈME 4. Soit K un corps differentiel de corps des constantes K_0. Si un élément f de K admet une primitive dans une extension élémentaire de K, elle peut être mise sous la forme

$$F = v_0 + \sum_{i=1}^{k} c_i \log v_i$$

avec $v_0 \in K$, $c_1,\ldots,c_k$ algébriques sur K_0, linéairement indépendants sur $\mathbb{Q}$ et $v_i \in K(c_1,\ldots,c_k)$ pour $i > 1$.

Démonstration : On écrit

$$f = v_0' + \Sigma\, c_i \frac{v_i'}{v_i}$$

où les v_i sont dans une extension élémentaire $L = \bar{K}(t_1,\ldots,t_n)$ d'une clôture algébrique $\bar{K}$ de K (au départ, les c_i sont nuls) ; on veut montrer que les v_i peuvent être pris dans $\bar{K}$; une récurrence sur n permet de se ramener au cas où $n = 1$; on décompose v_0 en éléments simples relativement à la variable t_1 et les v_i ples permet alors de montrer que les v_i peuvent être pris dans $\bar{K}$. La complétude de la théorie des corps algébriquement clos permet de choisir les c_i algébriques sur K et un argument de théorie de Galois permet de conclure. ∎

A partir de là, la théorie va consister à préciser la forme des v_i en fonction de celle de v. Ainsi, si f est une fraction rationnelle, il en est de même des v_i, et on peut préciser leur forme de manière à ramener l'intégration à la résolution d'un système d'équation linéaires (méthode de Horowitz). C'est essentiellement ce qui va être fait pour l'intégration des fonctions algébriques.

2. LE THÉORÈME DE RISCH.

Supposant démontré le théorème 2, nous allons esquisser la démonstration des théorème 1 et 3.

Etant donné un corps différentiel K, rappelons qu'*intégrer* un élément de K signifie calculer une primitive dans une extension élémentaire de K ou démontrer qu'il n'en existe pas. De même, nous allons considérer le problème suivant que nous appellerons *problème de Risch* pour K.

Etant donnés des éléments $f, g_1,\ldots,g_n$ de K, trouver une base sur K_0 (corps des constantes de K) de l'espace vectoriel W des solutions dans K de

$$y' + fy \in V$$

où V est le K_0-espace vectoriel engendré par les g_i.

Il faut remarquer qu'en substituant les éléments de la base de V dans l'équation, on trouve facilement la matrice de l'application naturelle de W dans V. Résoudre $y + fy = g_1$ revient alors à calculer l'image réciproque de g_1.

Les théorèmes 1 et 3 résultent immédiatement des résultats suivant dans les énoncés desquels K est un corps différentiel et la locution "on sait" est une abréviation pour "il existe un algorithme pour".

LEMME 1. Soient $u \in K$ et t transcendant sur K vérifiant $ut' = u'$ (i.e. $t = \log u$). Si l'on sait intégrer dans K, on sait intégrer dans $K(t)$.

LEMME 2. Soient $u \in K$ et t transcendant sur K vérifiant $t' = tu'$(i.e. $t = \exp u$). Si l'on sait intégrer et résoudre le problème de Risch dans K, on sait intégrer dans $K(t)$.

LEMME 3. Soient $u \in K$ et t transcendant sur K vérifiant $t' = tu'$ ou $ut'=u'$. Si l'on sait intégrer dans $K(t)$ et résoudre le problème de Risch dans K, on sait résoudre le problème de Risch dans $K(t)$. (Si t est un logarithme, les seules intégrations sont des intégrations d'éléments de K).

LEMME 4. On sait intégrer et résoudre le problème de Risch dans $\mathbb{Q}(x)$ ou dans une extension algébrique de $\mathbb{Q}(x)$.

Les lemmes 1 et 2 se démontrent de la manière suivante : on applique le théorème de Liouville $f = v_0' + \Sigma\, c_i \frac{v_i'}{v_i}$; on décompose en éléments simples dans $K(t)$ les deux membres de cette égalité et on les identifie. Quand t est un logarithme, cette identification conduit à tester si les primitives de certaines fonctions de K sont élémentaires et d'une forme particulière ; dans le cas où t est une exponentielle, on est ramené à des équations différentielles de la forme $y' + fy = g$ qu'il faut résoudre dans K, la différence provenant de ce que la dérivation n'abaisse pas le degré d'un polynôme en $\exp(u)$. Remarquons que la méthode s'applique également au cas de $\mathbb{Q}(x)$.

Démonstration du lemme 3 : Si $g \in V$, il s'agit de résoudre $y' + fy = g$, les éléments f,y et g étant des fractions rationnelles en t ; on ne connait pas g, mais on connait son dénominateur : le ppcm des dénominateurs des g_i. Si p est un polynôme irréductible, on écrit le début des développements p-adiques de y,f et g :

$$y = Yp^a + \ldots,\quad f = Fp^b + \ldots,\quad g = Gp^c + \ldots$$

$$y' = Yap'p^{a-1} + Y'p^a + \ldots$$

Il en résulte que $a \geqslant \max(c+1, c-b)$ ou que $b = -1$ et $a = -F/p' \bmod p$. Ceci permet

de déterminer un multiple du dénominateur de y. (Si t est une exponentielle et $p = t$, alors $p|p'$ et on trouve $a \geqslant \max(c,c-b)$ ou $b = 0$ et $Y'/Y + au' + F = 0$; la dernière expression signifie que la primitive de F est élémentaire d'une forme bien particulière et permet de calculer a). On peut maintenant chasser les dénominateurs, ce qui conduit à une équation

$$R z' + Sz = T$$

polynomiale en t. L'identification des coefficients des puissances de t permet de se ramener à un problème de Risch sur K, dès que l'on a borné le degré de z, ce qui nécessite une intégration dans K.

Démonstration du lemme 4 : Pour $\mathbb{Q}(x)$, la démontration est identique, mais plus simple que dans le cas logarithmique, et bien connue pour l'intégration. L'intégration dans le cas algébrique sera traitée au paragraphe suivant. Enfin, soient K un corps de fonctions algébriques, v une valuation de K ne prolongeant pas la valuation à l'infini de $\mathbb{Q}(x)$ et p une uniformisante locale ; l'équation $dy/dx + fy = g$ se réécrit

$$\frac{dy}{dp} + f\frac{dx}{dp}y = g\frac{dx}{dp}$$

et l'argument de la démonstration du lemme 3 permet de minorer la valuation de y en v. Ceci détermine donc un diviseur D tel que $(y) \geqslant D$. L'algorithme de Coates (voir plus bas) permet de déterminer une base de l'espace des fonctions satisfaisant cette inégalité et la solution du problème de Risch n'est plus que de l'algèbre linéaire.

3. FONCTIONS ALGÉBRIQUES

Dès l'abord, les fonctions algébriques posent des problèmes de représentation ; suivant Davenport nous représenterons une fonction algébrique f sous la forme $g(x,y_1,\ldots,y_n)/h(x)$ où g et h sont des polynômes et où les variables sont reliées par des équations polynomiales $F_1(x,y_1) = 0$, $F_2(x,y_1,y_2) = 0, \ldots$ Ainsi $(x+\sqrt{x^2-1})/\sqrt[3]{x}$ est représenté par $y_2^2\,(x+y_1)/x$ avec $y_1^2 - x^2 + 1 = 0$ et $y_2^3 - x = 0$. Autrement dit une fonction algébrique f est une fonction rationnelle g/h sur la courbe C définie par les équations $F_i = 0$, ce qui n'est qu'une formulation géométrique pour dire que f appartient au corps $L = K(x,y_1\ldots,y_n)\ (F_1,\ldots F_n)$.

Afin d'éviter les problèmes d'indécidabilité, le corps K des constantes doit être explicitement défini à partir de $\mathbb{Q}$ par une succession d'extensions simples transcendantes ou algébriques de polynôme minimal connu (Si c est une constante dont l'égalité à 0 est indécidable, et f une fonction dont l'intégrale n'est pas élémentaire, l'intégration de $cf(x)$ est un problème indécidable). Avec ces notations, on peut préciser le théorème de Liouville.

THÉORÈME 5. Soient f une fonction algébrique et $r_1, \ldots, r_k$, une base du $\mathbb{Z}$-module engendré par les résidus de la forme différentielle fdx. A chaque place P, la forme fdx a le résidu $\sum_P a_{iP} r_i$; soit d_i le diviseur $\sum_P a_{iP}.P$. Si f a une primitive élémentaire, alors

$$f = v_0' + \sum_{i=1}^{k} \frac{r_i}{j_i} \frac{v_i'}{v_i}$$

avec $v_0 \in K$, $v_i \in K(r_1, \ldots, r_k)$ et $(v_i) = j_i d_i$

(On désigne par (v_i) le diviseur de v_i).

Démonstration : On écrit le théorème de Liouville, et en jouant sur les propriétés de la dérivée logarithmique, on se ramène au cas où les (v_i) sont $\mathbb{Q}$-linéairement indépendants, ainsi que les c_i. Un peu d'algèbre linéaire permet alors de regrouper les termes pour aboutir au résultat. ∎

La stratégie d'intégration est alors la suivante :

1) Déterminer les pôles de fdx et leurs résidus, sans oublier les places à l'infini.

2) En déterminer une base et calculer les d_i.

3) Déterminer j_i tel que $j_i d_i$ soit le diviseur d'une fonction v_i. Calculer v_i ou montrer que c'est impossible.

4) Dériver pour calculer v_0'.

5) Calculer le diviseur des pôles de v_0' ; en déduire celui des pôles de v_0 et calculer v_0 ou montrer une impossibilité.

Les problèmes posés par les différentes étapes sont fort différents : les étapes 2 et 4 sont sans problèmes.

Aux étapes 3 et 5 il faut déterminer une fonction dont le diviseur possède certaines propriétés. Cela se fait en deux temps : on calcule d'abord l'espace vectoriel des fonction v tel que $(v) \geqslant -D$ où D est un diviseur positif (celui des pôles) ; à ce moment, les autres contraintes que doivent satisfaire D sont linéaires et il est facile de calculer, s'il en existe, une fonction les satisfaisant.

Les problèmes sont donc :

A) Donner une définition explicite des notions de pôle et de résidu et des algorithmes permettant de les calculer.

B) Déterminer un ensemble fini J aussi petit que possible tel que si j_i existe

il appartienne à J ; il suffit toutefois de majorer j_i

C) Etant donné un diviseur positif D, calculer une base de l'espace des fonctions v telles que $(v) \geqslant -D$.

4. PLACES - DÉVELOPPEMENT DE PUISEUX

Pour résoudre le problème A, il faut une vue plus algorithmique de la situation : jusqu'à présent, les données étaient des fractions rationnelles dont la représentation est simple et les algorithmes pouvaient être copiés sur les démonstrations, à condition d'avoir des programmes efficaces pour la décomposition en élément simple, le calcul du pgcd, la factorisation de polynômes,...Ici, la situation est différente : les notions de places, résidus,... ne sont pas habituellement présentées d'une manière constructive. Voici la représentation de Davenport des places d'une courbe $F(x\ y) = 0$:

C'est une liste de paires indiquant des substitutions ; la première(x,x-a) ou (x,1/x) est la substitution nécéssaire pour ramener la place au dessus de 0. Après avoir substitué la nouvelle valeur de x dans F, on calcule les débuts des développements de Puiseux des solutions de $F(x,y) = 0$, ce qui donne les places et leur ramification. Pour une place de ramification e, on ajoute la paire (x, x^e) qui transforme la série de Puiseux en série de Laurent, puis l'indication de la racine de $F(x,y) = 0$ considérée ; on continue d'une manière analogue s'il y a d'autres équations $F_2(x,y,y_2) = 0,...$ (Dans le programme de Davenport, les polynômes F_i sont de la forme $y_i^2 + f_i\ (x,y_1,...,\ y_{i-1})$, ce qui évite de nombreuses complications).

A partir de là, le calcul des pôles et des résidus des fonctions ou des formes différentielles devient théoriquement assez simple: on calcule les places au dessus des zéros du dénominateurs et de l'infini ; on effectue les substitutions indiquées et on calcule le terme de degre -1 du développemnt en série de Puiseux (en fait de Laurent) de la fonction ou de la forme. De même, le genre de la courbe s'obtient en calculant le degré du diviseur de dx, qui est concentré aux places ramifiées et à l'infini.

Bien que la solution théorique soit claire la programmation n'est ni réalisée ni facile quand on ne se limite pas aux racines carrées : outre le maniement des polygônes de Newton qui n'est guère compliqué, il faut distinguer les différents nombres algébriques conjugués qui apparaissent et effectuer de nombreuses manipulations (factorisation de polynômes notamment) pour lesquelles on ne connait pas d'algorithmes suffisamment rapides.

5. TORSION D'UN DIVISEUR

La résolution du problème B revient à majorer la torsion du diviseur d_i dans le groupe des classes de diviseur ou jacobienne. Ayant ainsi obtenu une majoration de j_i il n'y a plus qu'un nombre fini de valeurs possibles pour ce nombre ; on est donc ramené à résoudre un nombre fini de fois le problème C. Cette majoration de la torsion dépend de la nature du corps des constantes.

5.1. *Corps des constantes algébrique, genre 1.*

Ce cas est essentiel, car les exemples en genre $\geqslant 2$ sont très rares. Si le corps de définition de la fonction et du diviseur est $\mathbb{Q}$, on connait une majoration absolue de la torsion :

PROPOSITION 1. - (Mazur) L'ordre d'un diviseur de torsion d'une courbe de genre 1 définie sur $\mathbb{Q}$ est au plus 12.

Malheureusement on ne connait pas de borne analogue pour les corps de nombres; de toute façon une telle borne générale rend les calculs très coûteux, surtout si le diviseur n'est pas de torsion. Aussi Davenport a proposé l'algorithme suivant :

ALGORITHME 1. Entrées: une courbe elliptique et un diviseur.
Sortie : l'ordre du diviseur.

a - Changer de coordonnées pour mettre la courbe sous forme canonique de Weierstrass

$$Y^2 = X^3 + aX + b$$

avec a et b entiers algébriques.

b - A l'aide de la loi de groupe sur la courbe, identifier le diviseur à un point $P_0 = (X_0, Y_0)$ de la courbe.

c - Si P_0 est entier (i.e. a des coordonnées entiers algébriques), calculer $P_1, P_2, \ldots$ avec $P_i = 2P_{i-1}$ jusqu'à ce que

- *ou bien le dénominateur de la première coordonnée de P_i ne soit pas entier ; alors P_0 n'est pas de torsion.*
- *ou bien, il existe $j \leqslant i$ avec $P_i = \pm P_j$; dans ce cas P_0 est d'ordre $m2^j$ avec m diviseur de $2^{i-j} \pm 1$.*
- *ou bien P_i est le point à l'infini ; alors l'ordre de P_0 est 2^i.*

d - Si P_0 n'est pas entier, soit p le dénominateur de X_0 ; si p n'est pas premier, P_0 n'est pas de torsion ; si p est premier, calculer

$P_1 = pP_0$, $P_2 = pP_1$,... jusqu'à trouver le point à l'infini ou un dénominateur ne divisant pas p ; l'ordre est alors p^i ou l'infini, respectivement.

Cet algorithme est basé sur les deux résultats classiques suivants :

PROPOSITION 2. La courbe $y^2 = X^3 + X + b$ n'a qu'un nombre fini de points entiers ou de points dont le dénominateur divise un entier donné.

PROPOSITION 3. Si (X,Y) est un point d'ordre n sur la courbe précédente (avec a,b entiers algébriques), alors, ou bien X est un entier algébrique, ou bien n est puissance du nombre premier p et pX est un entier algébrique.

Ayant ces résultats, le seul point difficile est l'étape a. Pour celà, on choisit un point P et deux fonction X et Y ayant des pôles d'ordre 2 et 3 en P et pas d'autres pôles ; ceci se fait à l'aide de l'algorithme de Coates, ci-dessous ; il existe une relation linéaire entre x^3, y^2, xy,x^2,x, y et 1 qui donne la forme cherchée après un changement de variables faciles.

5.2. Corps des constantes algébriques, genre quelconque.

Dans ce cas, la méthode utilisée utilise une stratégie fréquente en calcul algébrique : réduire le problème modulo un nombre premier p. La notion de bonne réduction que nous décrivons est essentiellement celle de Serre et Tate mise sous forme directement utilisable pour notre objectif.

DÉFINITION 1. Une courbe C d'équation $F(x,y) = 0$ a bonne réduction modul un nombre premier p si F est absolument irréductible modulo p et si le genre ne décroît pas par réduction modulo p.

PROPOSITION 4. Il n'y a qu'un nombre fini de nombres premiers de mauvaise réduction.

PROPOSITION 5. L'ordre du groupe des classes de diviseurs (jacobienne) d'une courbe de genre g définie sur F_q est majoré par $(\sqrt{q} + 1)^{2g}$.

PROPOSITION 6. S'il y a bonne réduction modulo p, l'ensemble des classes de diviseurs d'ordre premier à p s'injecte dans la jacobinne modulo p.

COROLLAIRE. La connaissance de l'ordre de la jacobienne modulo p pour deux nombres premiers de bonne réduction donne un multiple de l'ordre de tout diviseur de torsion.

Si on connait des algorithmes efficaces pour calculer le corps résiduel d'un

corps de nombres, tester l'irréductibilité absolue modulo p d'un polynôme et calculer l'ordre de la jacobienne et le genre d'une courbe définie sur F_q, on en déduit aisément un multiple de l'ordre de tout diviseur d'une courbe définie sur un corps de nombres : il suffit d'utiliser au moins deux nombres premiers de bonne réduction. Si on ne sait pas calculer exactement l'ordre de la jacobienne modulo p, on obtient cependant un majorant de l'ordre du diviseur.

Actuellement, la plupart des algorithmes nécéssaires n'ont pas encore été implantés : il faut d'abord programmer, en tenant compte des particularités de la caractéristique p, les algorithmes de calcul des places et des développements en série de "Puiseux", ainsi que l'analogue de l'algorithme de Coates. Le genre est facile à calculer : il suffit de réduire modulo p les différentielles de première espèce et de vérifier qu'elles restent de première espèce et linéairement indépendantes. Pour l'irréductibilité absolue, Dicreszenzo et Duval viennent de décrire un algorithme polynomial qui n'est encore ni programmé ni généralisé à la caractéristique p. Enfin, pour l'ordre de la jacobienne, rien d'autre ne semble connu que la stratégie évidente qui est très inefficace.

5.3. Corps des constantes transcendant

Dans ce cas, le calcul de la torsion d'un diviseur se fait à l'aide des opérateur de Gauss-Manin qui utilise la différentiation par rapport à une constante transcendante, ce qui peut surprendre si cette constante est e ou π. Il faut aussi noter que,si e et π apparaissent simultanément un résultat de non intégrabilité ne pourra être que de la forme "Si e et π sont algébriquement indépendant,...".

Dans ce paragraphe, les équations de la courbe considérée sont supposées polynomiales en un paramètre transcendant u ; la dérivation par rapport à u est notée D, alors que la dérivation par rapport à x est notée '.
L'algorithme est le suivant :

Algorithme 2. - Entrées : Une courbe algébrique et un diviseur $n_1P_1+\ldots n_kP_k$.

Sortie : infini ou un entier divisant l'ordre du diviseur.

a.- Calculer une base B de l'espace des différentielles de première espèce (algorithme de Coates) ; $g := card(B)$ *est le genre de la courbe.*

b.- Pour chaque ωdx *dans B faire*

b1.- Calculer les constantes $A_0,\ldots,A_{2g}$ *et la fraction rationnelle* $R = R(x,y_1,\ldots)$ *telles que*

$$A_0\omega + A_1D\omega +\ldots+A_{2g}\,D^{2g}\omega = R'$$

(une fois chassés les dénominateurs, c'est de l'algèbre linéaire)

b2.- Pour chaque P_j *de première coordonnée* X_j

Calculer $B_0 := 0$ *et* $B_i = DB_{i-1} + DX_j D^{i-1}\omega$ *pour* $i = 1,\ldots,2g$

($D^{i-1}\omega$ *est évalué au point* P_j*, c'est une dérivation partielle ; on a donc* $D^i\int_0^{X_j}\omega = \int_0^{X_j} D^i\omega + B_i$*).*

Calculer $S_j := A_0B_0 + \ldots + A_{2g}B_{2g} + R(P_j)$

b3.- Si $n_1S_1 + \ldots + n_kS_k \neq 0$ *sortir "infini"*

c.- Choisir un entier u_0 *tel qu'il y ait bonne réduction modulo* $u-u_0$ *(cf. 5.2) ; substituer partout* u_0 *à* u*.*

Si après cette substitution l'ordre du diviseur obtenu est infini, sortir infini ; sinon sortir l'ordre du diviseur obtenu.

L'algorithme procède donc récursivement en réduisant le degré de transcendance du corps des constantes. L'opération b1 est possible car les $D^i(\omega dx)$ sont $2g + 1$ différentielles de deuxième espèce (sans résidu) et sont donc linéairement dépendantes. Le reste de l'algorithme est justifié par le résultat suivant de Manin ; si ω est une différentielle de première espèce, on lui associé l'opérateur différentiel $L = \Sigma A_i D^i$ où les A_i sont définis en b1, et on pose

$$J(P) = L\int_0^P \omega$$

où 0 est un point fixe arbitraire (opérateur de Picard-Fuchs)

PROPOSITION 7.- Un point P *de la jacobienne* A *est annulé par tous les opérateurs* J *si et seulement s'il existe un entier* n *tel que* nP *soit au dessus d'un point de la trace de* A *sur* k *(le corps des constantes étant* $k(u)$*).*

Un diviseur est donc de torsion si et seulement s'il est annulé par tous les opérateurs J et est de torsion après réduction modulo $u-u_0$, la réduction ne pouvant que diviser l'ordre du diviseur.

REMARQUE.- La programmation de cet algorithme présente une difficulté technique qui peut surprendre un mathématicien : il faut distinguer dans une même expression la dérivation totale et la dérivation partielle par rapport à U. Les systèmes actuels de calcul formel ne le peuvent pas facilement (sauf New SCRATCHPAD qui n'est pas encore disponible).

6.- ALGORITHME DE COATES.

La plupart des algorithmes présentés jusqu'ici nécessitent de savoir calculer une base de l'espace $L(D)$ des fonctions dont le diviseur est supérieur à $-D$. On peut supposer $D \geqslant 0$, car les conditions introduites par la partie négative de D sont des contraintes linéaires qui peuvent être résolues après coup.
Soit $L = K(x,y_1,\ldots,y_k)$ un corps de fonctions algébriques défini par les polynomes $F_i(x,y_1,\ldots,y_i)$; on appelle n le degré de L sur $K(x)$; l'algorithme va travailler localement sur les valuations de $K[x]$.

ALGORITHME 3.- Entrée : la courbe algébrique définie par les équations $F_i = 0$ et un diviseur D positif

Sortie : Une base sur K de l'espace $L(D)$ des fonctions de L de diviseur $\geqslant -D$

a.- Choisir n fonctions linéairement indépendantes sur $K[x]$ n'ayant pas de pôles à distance finie ; on peut prendre les monômes en z_i où z_i est le produit de y_i par le coefficient de plus haut degré de y_i dans F_i ; soit $V = (f_1,\ldots,f_n)$ le vecteur de L^n dont les composantes sont ces fonctions. On va modifier V de manière qu'à la fin de l'algorithme ses composantes soient une base du $K[x]$-module des fonctions telles que $(f) \geqslant -D$ au dessus des places à distance finies de $K[X]$.

b.- Calculer les racines du discriminant de la base sur $K(x)$ des n fonctions choisies.

c.- Pour chaque racine a trouvée et pour chaque valuation $x-a$ à distance finie de $K[X]$ au dessous d'une composante de D remplacer V par ΔMV où M est une matrice inversible sur $K[X]$ et Δ une matrice diagonale dont les coefficients sont des puissances négatives de $x-a$ (le calcul de M et Δ sera exposé plus bas ; ceci modifie le localisé au dessus de $x-a$ du module engendré par les composantes de V mais ne modifie pas les autres localisés).

d.- Remplacer V par MV où M est une matrice inversible sur $K[X]$ de manière que $L(D)$ ait pour base ceux des $x^j f_i$ dont le diviseur est $\geqslant -D$ au dessus de la place à l'infini de $K[X]$.

Le calcul des matrices M et Δ nécessite d'adapter au cas des anneaux de valuation discrète la forme explicite du théorème de structure des modules sur les anneaux principaux :

LEMME 5.- Etant donnée une matrice A sur un anneau de valuation discrète R d'uniformisante t, il existe une matrice de permutation S et une succession d'opérations élémentaires sur les colonnes, de matrice E, telles que SAE soit une matrice triangulaire inférieure dont les coefficients vérifient

$$i \leq j \Rightarrow a_{ii} \text{ divise } a_{kj} .$$

En tronquant les séries qui interviennent, on obtient :

COROLLAIRE.- Si K est un sous corps de représentants de A, on peut supposer E définie et inversible sur K[t], mais SAE n'est plus nécessairement triangulaire.

Ces résultats, parfaitement explicites, s'appliquent de la manière suivante :

Soient $P = x-a$ ou $\frac{1}{x}$ une place de $K(x)$, R l'anneau de sa valuation, $P_1,\ldots,P_k$ les places de la courbe au dessus de P et S le R-module libre des éléments $(z_1,\ldots,z_n)$ de L^k tels que $v_{Pi}(z_i) \geqslant v_{Pi}(-D)$. On prend pour A la matrice des f_i sur la base canonique de S. Les matrices M de l'algorithme sont les transposées de la matrice E du corollaire ; la matrice Δ correspond à la division des éléments de la nouvelle base par la plus grande puissance de x-a qui les laissent dans S. En pratique, les coefficients de A sont représentés par les premiers termes de leur developpement de Puiseux.

REMARQUE.- Bien que cette présentation de l'algorithme de Coates diffère de celle qui est donnée habituellement, elle correspond essentiellement aux mêmes calculs, mais assure que la modification faite en une place ne modifie pas les localisés aux autres places. Par ailleurs un des problèmes dans l'utilisation de l'algorithme de Coates est la croissance de la taille des expressions intermédiaire ; l'adaptation de l'algorithme de Kannan et Bachem, de complexité polynomiale, devrait permettre de contrôler cette croissance et de donner une version polynomiale de l'algorithme de Coates.

CONCLUSION.

Nous n'avons pu donner ici que les grandes lignes de la méthode. Il y a bien entendu de nombreuses variantes. Nous n'avons pu signaler que les principaux problèmes posés par la programmation ; au delà de l'implantation et de l'optimisation des algorithmes il vont jusqu'à la conception même des systèmes de calcul formel.

BIBLIOGRAPHIE

J. COATES - Construction of Rational Functions on a Curve. Proc. Cam. Phil. Soc. 68 (1970) pp. 105-123.

J.H. DAVENPORT - On the integration of algebraic functions. Lecture Notes in Computer Science n° 102, Springer Verlag, 1981.

J.H. DAVENPORT - Intégration algorithmique des fonctions élémentairement transcendantes sur une courbe algébrique. Annales de l'Institut Fourier 34(1984).

J.H. DAVENPORT - The Risch differential equation problem. Soumis à Siam J. of Computation.

J.H. DAVENPORT - y'+fy=g. Congrès EUROSAM (Cambridge, 1984). A paraître aux Lect. Notes in Computer Science.

J.H. DAVENPORT et al. - New Scratchpad (IBM Research Center, Yorktown Heights, 1984)

C. DICRESCENZO, D. DUVAL - Computations on Curves - Congrès EUROSAM (cf. supra).

D. DUVAL - Une méthode géométrique de factorisation des polynômes en deux indéterminées. Journées de Calcul Formel (Luming 1983) CALSYF 3 (Mignotte, Université de Strasbourg).

R.D. JENKS - A Scratchpad primer : 11 heys to Scratchpad Congrès EUROSAM (Cambridge 1984) - A paraître aux Lect. Notes in Computer Science.

R. KANNAN, A. BACHEN - Polynomial algorithms for computing the Smith and Hermite normal form of an integer matrix. Siam J. Computation 8(1979) p. 499.507.

J. LIOUVILLE - Premier et second mémoire sur la détermination des intégrales dont la valeur est algébrique. Journal de l'Ecole Polytechnique 14(1833) cahier 22 p. 124-143.

Ju. I. MANIN - Algebraic curves over Fields with Differentiation. Izv. Akad. Nauk. SSSR Ser. Mat 22(1958) pp. 737-756. (translated in AMS Trans. Ser. 2 37(1964) pp. 59-78).

Ju. I. MANIN - Rational Points of Algebraic Curves over Function Fields. Izv. Akad. Nauk. SSSR Ser. Mat. 27(1963) pp. 1395-1440 (translated in AMS Trans. Ser. 2 50(1966) pp. 189-234).

B. MAZUR - Rational Isogenies of Prime Degree. Inventiones Math. 44(1978) pp. 129-162.

R.H. RISCH - The Problem of Integration in Finite Terms. Trans. A.M.S. 139(1969) pp. 167-189.

R.H. RISCH - The solution of the Problem of Integration in Finite Terms. Bulletin AMS 76(1970) pp. 605-608.

J.P. SERRE, J.T. TATE - Good Reduction of Abelian Varieties. Annals of Mathematics 88(1968) pp. 492-517.

Note.- Cette bibliographie est volontairement limitée aux résultats fondamentaux et aux articles récents. Pour une bibliographie détaillée, se reporter au livre de Davenport.

Daniel LAZARD

Institut de Programmation
Université Pierre et Marie Curie
F-75230 PARIS CEDEX 05

LITP et GRECO de Calcul Formel, CNRS.