

ODILE SIMON

## **Algorithme de multiplicativité des sommes de carrés**

*Informatique théorique et applications*, tome 26, n° 6 (1992), p. 485-506.

[http://www.numdam.org/item?id=ITA\\_1992\\_\\_26\\_6\\_485\\_0](http://www.numdam.org/item?id=ITA_1992__26_6_485_0)

© AFCET, 1992, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## ALGORITHME DE MULTIPLICATIVITÉ DES SOMMES DE CARRÉS (\*)

par Odile SIMON (1)

Communiqué par P. FLAJOLET

Résumé. – Dans cet article, on présente des algorithmes pour effectuer l'opération suivante : Soit  $A$  un anneau de coordonnées d'une courbe plane affine sur un corps  $k$  et  $m$  un entier positif, étant donné une famille  $(f_i)$ ,  $i \in \{1, \dots, p\}$ , d'éléments de  $A$ , telle que chaque  $f_i$  divise  $1 + p_{i,1}^2 + \dots + p_{i,m}^2$ , (les  $p_{i,j}$  étant donnés), trouver en les calculant,  $m$  éléments  $q_1, \dots, q_m$  tels que  $f = \prod_{1 \leq i \leq p} f_i$  divise  $1 + q_1^2 + \dots + q_m^2$  dans  $A$ . Ce résultat se présente comme une certaine « stabilité multiplicative » des éléments « 1 + somme de  $m$  carrés », et c'est ainsi qu'on y fera référence.

Abstract. – Let  $A$  be the coordinate ring of an affine plane curve over a field  $k$  and  $m$  be a positive integer. Let  $(f_i)$ ,  $i \in \{1, \dots, p\}$ , be a family of elements of  $A$ . Suppose that for each  $i \in \{1, \dots, p\}$ , are given elements  $p_{i,1}, \dots, p_{i,m} \in A$  such that  $f_i$  divides  $1 + p_{i,1}^2 + \dots + p_{i,m}^2$  in  $A$ . Then algorithms are given to compute  $q_1, \dots, q_m \in A$  such that  $f = \prod_{1 \leq i \leq p} f_i$  divides  $1 + q_1^2 + \dots + q_m^2$ . This is a "multiplicative stability" result for the set of elements "1 + a sum of  $m$  squares" and it will be referred so.

### INTRODUCTION

On rappelle le 17<sup>e</sup> problème de Hilbert :  $\mathbb{R}$  étant le corps des nombres réels, tout polynôme de  $\mathbb{R}[X_1, \dots, X_n]$ , étant positif ou nul sur  $\mathbb{R}^n$ , est-il somme de carrés de fractions rationnelles ? Artin a donné une réponse positive à ce problème en étendant le résultat à tout corps réel clos ([1], [2], ch. 6).

Pfister [8] et Mahé [7], ont obtenu des résultats quantitatifs, dont se déduit le résultat suivant [10] :

PROPOSITION : Soient  $k$  un corps réel clos,  $A$  une  $k$ -algèbre de degré de transcendance, inférieur ou égal à  $d \in \mathbb{N}$ ,  $f$  un élément de  $A$  strictement positif

(\*) Reçu juillet 1990, accepté septembre 1991.

(1) I.R.M.A.R., Université de Rennes-I, Campus de Beaulieu, 35042 Rennes Cedex, France.

sur le spectre réel de  $A$ , non diviseur de zéro dans  $A$ , alors il existe  $q \in A$ , somme de  $d - 2 + 2^d$  carrés tel que  $f$  divise  $1 + q$ .

On en déduit les deux cas particuliers suivants. Si  $A = k[X]$  ou  $k[X, Y]/(C)$  où  $C$  est un élément non constant de  $k[X, Y]$ , tout élément de  $A$ , ne s'annulant pas sur le spectre réel de  $A$ , non diviseur de zéro dans  $A$ , divise  $1 + q$  où  $q$  est un carré dans  $A$ .

Cette proposition donne l'existence d'un nombre borné de carré mais n'est pas constructive.

Dans cet article, pour des données particulières, on obtient la construction effective d'un nombre de carrés, non forcément inférieur au nombre  $d$  donné par la proposition mais constant à partir des données. Plus précisément : étant données des familles  $(f_i)$  et  $\{p_{i,j}\}_{i \in \{1, \dots, p\}, j \in \{1, \dots, m\}}$  d'éléments d'un anneau  $A$  que l'on précisera, telles que, pour chaque  $i$ ,  $f_i$  divise  $1 + p_{i,1}^2 + \dots + p_{i,m}^2$ , on donne un algorithme calculant  $m$  éléments de  $A$ ,  $q_1, \dots, q_m$ , tels que  $f = \prod_{1 \leq i \leq p} f_i$  divise  $1 + q_1^2 + \dots + q_m^2$ .

Le paragraphe 1 est consacré à l'algorithme pour  $k[X]$ ,  $k$  étant un corps quelconque. Cette algèbre étant factorielle, l'algorithme pourra utiliser les techniques standards du théorème chinois et du lemme de Hensel.

Dans les paragraphes 2 et 3, on s'intéresse à  $A = k[X, Y]/c(X, Y)$ , où  $c(X, Y) = 0$  est une courbe plane définie sur  $k$ ; les techniques nécessaires utilisent intensivement la norme  $N: A \rightarrow k[X]$ . Par une première méthode, on obtient un résultat comparable au principe de la norme de Knebusch [6], ch. VII, th. 5.1, dans lequel « formes quadratiques » est remplacé par «  $1 +$  somme de  $m$  carrés » et on en déduit le résultat. Par une autre méthode, on obtient un algorithme calqué sur celui de  $k[X]$ , en définissant une division modulaire dans  $k[X, Y]$ , selon les méthodes de D. Duval et C. Dicrescenzo [3].

Les algorithmes développés dans cet article ont été implémentés sur Macsyma; en annexe de [9], on en trouve l'exécution sur quelques exemples.

## PRÉLIMINAIRES

NOTATION : Pour dire qu'un élément  $f$  d'un anneau est somme de  $n$  carrés,  $n \in \mathbb{N}^*$ , on notera  $f = n \diamond$ ; c'est la notation de Pfister adaptée aux nécessités typographiques.

*Remarque 0.1* : Réduction du problème.

Dans le reste de l'article, il suffira de travailler avec deux éléments  $f_1$ , et  $f_2$  et on obtiendra la stabilité du produit de  $p$  éléments par récurrence sur  $p$ .

La construction repose en partie sur celle d'idempotents dans un anneau quotient. Le lemme suivant où l'on reconnaît le théorème chinois, avec une conclusion plus spécialisée, sera utilisé plusieurs fois :

LEMME 0.2 : Soit  $A$  un anneau commutatif,

$$P(X_1, \dots, X_m) \in A[X_1, \dots, X_m].$$

Soient  $f_1, f_2, s_1, s_2, a_1, \dots, a_m, b_1, \dots, b_m, \lambda, \mu \in A$  tels que

$$1. s_1 f_1 = P(a_1, \dots, a_m)$$

$$2. s_2 f_2 = P(b_1, \dots, b_m)$$

$$3. \lambda f_1 + \mu f_2 = 1$$

alors il existe un algorithme donnant  $q_1, \dots, q_m$  tels que  $f_1 f_2$  divise  $P(q_1, \dots, q_m)$  dans  $A$ .

*Démonstration* : En multipliant 3 par  $\lambda f_1$  d'une part, et par  $\mu f_2$  d'autre part, on obtient que  $\lambda f_1$  et  $\mu f_2$  sont des idempotents modulo  $f_1 f_2$ .

Donc, pour tout  $n \in \mathbb{N}$ , tout  $n$ -uplet  $(i_1, \dots, i_n) \in \{1, \dots, m\}^n$ , l'expression suivante :

$$(a_{i_1} \mu f_2 + b_{i_1} \lambda f_1) \dots (a_{i_n} \mu f_2 + b_{i_n} \lambda f_1) - a_{i_1} \dots a_{i_n} \mu f_2 - b_{i_1} \dots b_{i_n} \lambda f_1$$

est un multiple de  $f_1 f_2$ , que l'on explicite aisément. On en déduit que :

$$\begin{aligned} P(a_1 \mu f_2 + b_1 \lambda f_1, \dots, a_m \mu f_2 + b_m \lambda f_1) \\ = P(a_1, \dots, a_m) \mu f_2 + P(b_1, \dots, b_m) \lambda f_1 + \text{multiple de } f_1 f_2. \end{aligned}$$

D'autre part, en utilisant les égalités 1 et 2, on a :

$$(\lambda s_1 + \mu s_2) f_1 f_2 = P(a_1, \dots, a_m) \mu f_2 + P(b_1, \dots, b_m) \lambda f_1$$

Le lemme est démontré en posant, pour  $j=1, \dots, m$ ,  $q_j = a_j \mu f_2 + b_j \lambda f_1$ .

On appliquera ce lemme au polynôme

$$P(X_1, \dots, X_m) = 1 + X_1^2 + \dots + X_m^2.$$

Dans cette application, on voit qu'il n'y a pas une solution unique  $q_1, \dots, q_m$ , pour chaque  $j \in \{1, \dots, m\}$ , on peut choisir, en particulier, entre :

$$q_j = a_j \mu f_2 + b_j \lambda f_1 \quad \text{et} \quad q'_j = a_j \mu f_2 - b_j \lambda f_1.$$

LEMME 0.3 : Soient  $f, s$  et  $a_1, \dots, a_m$  tels que  $fs = 1 + a_1^2 + \dots + a_m^2$  dans un anneau  $A$  commutatif unitaire, dans lequel 2 est inversible. Alors pour tout

entier  $r \geq 2$ , on sait calculer  $t$  et  $q_1, \dots, q_m$  dans  $A$  tels que

$$tf^r = 1 + q_1^2 + \dots + q_m^2.$$

Ce qui peut aussi s'exprimer de la manière suivante : si  $-1$  est une somme de  $m$  carrés modulo  $f$ , alors, pour tout  $r \geq 2$ ,  $-1$  est une somme de  $m$  carrés modulo  $f^r$ , que l'on peut calculer effectivement.

*Démonstration* : Par hypothèse, on a

$$-1 + sf = -1(1 - sf) = a_1^2 + \dots + a_m^2. \quad (1)$$

Pour  $r = 2$ , il suffit donc de montrer que  $(1 - sf)^{-1}$  est un carré dans  $A/(f^2)$ . Dans  $A[T]$ , on a l'égalité polynomiale :

$$(1 + T/2)^2(1 - T) = 1 - T^2(3 + T)/4$$

ainsi,  $(1 - T)^{-1}$  existe et est un carré dans  $A[T]/(T^2)$ . En substituant  $sf$  à  $T$  et en multipliant (1) par  $(1 + sf/2)^2$ , on obtient :

$$(a_1^2 + \dots + a_m^2)(1 + sf/2)^2 = -1(1 - s^2 f^2(3 + sf)/4)$$

$$(a_1^2 + \dots + a_m^2)((3 + a_1^2 + \dots + a_m^2)/2)^2 = -1 + s^2 f^2(1 + (a_1^2 + \dots + a_m^2)/4). \quad (2)$$

Ainsi, on a calculé  $q_j$ ,  $j \in \{1, \dots, m\}$ , tels que  $-1 = q_1^2 + \dots + q_m^2$  modulo  $f^2$ .

Pour tout entier  $r > 2$ , on sait calculer  $k \in \mathbb{N}$  tel que

$$2^{k-1} < r \leq 2^k$$

En appliquant  $k$  fois, la formule (2), on calcule  $u$  et  $q_1, \dots, q_m$  vérifiant

$$uf^{2^k} = 1 + q_1^2 + \dots + q_m^2.$$

Si on pose  $t = u(f^{2^k - r})$ , on a le résultat, pour  $r$ .

## 1. ALGORITHME POUR LA STABILITÉ DE L'ÉCRITURE DU PRODUIT DANS $k[X]$

Soit  $k$  un corps.

**THÉORÈME 1.1** : Soit  $f_1$  et  $f_2$  deux éléments de  $k[X]$  tels que  $f_1$  divise  $1 + x_1^2 + \dots + x_m^2$ ,  $f_2$  divise  $1 + y_1^2 + \dots + y_m^2$ , dans  $k[X]$ , alors il existe un algorithme calculant effectivement  $s$  et  $q_1, \dots, q_m$  dans  $k[X]$  tels que

$$sf_1 f_2 = 1 + q_1^2 + \dots + q_m^2.$$

*Démonstration* : Soit  $p_1 = \text{pgcd}(f_1, f_2)$ . Si  $\text{deg } p_1 = 0$ , alors  $f_1$  et  $f_2$  sont premiers entre eux, par l'algorithme d'Euclide, on sait calculer  $\lambda$  et  $\mu$  dans  $k[X]$  tels que  $1 = \lambda f_1 + \mu f_2$ . En appliquant le lemme 0.2, on calcule alors  $q_1, \dots, q_m$  et on obtient  $s$  par division euclidienne. Sinon, soit  $\text{deg } p_1 > 0$ . Le but est de trouver un facteur de  $f_2$ , premier avec  $f_1$ . On a  $f_1 = p_1 g_1$  et  $f_2 = p_1 h_1$ ,  $\text{deg } h_1 < \text{deg } f_2$ . Si  $f_1$  et  $h_1$  ne sont pas premiers entre eux, on considère  $p_2 = \text{pgcd}(f_1, h_1)$  donc  $\text{deg } p_2 > 0$  et  $h_1$  se factorise :  $h_1 = p_2 h_2$  avec  $\text{deg}(h_2) < \text{deg}(h_1)$ ; de plus, comme  $p_2$  est un diviseur commun à  $f_1$  et  $f_2$ , il divise  $p_1$ .

On construit ainsi une famille  $(p_i, h_i)$ , où  $p_i = \text{pgcd}(f_1, h_{i-1})$  et  $h_{i-1} = p_i h_i$  tant que  $\text{deg } p_{i-1} > 0$ . La suite  $(\text{deg } h_i)_i$  est une suite strictement décroissante et on a  $\text{deg}(p_i) \leq \text{deg}(h_{i-1})$ . Donc, on trouve  $r + 1$ , fini, tel que  $p_{r+1}$  est de degré 0, ainsi  $f_1$  et  $h_r$  sont premiers entre eux. On a

$$f_1 f_2 = f_1 p_1 p_2 \dots p_r h_r,$$

où chaque  $p_i$  divise  $p_1$ , ainsi  $f_1^{r+1} h_r$  est multiple de  $f_1 f_2$ . L'élément  $h_r$  et d'après le lemme 0.3, l'élément  $f_1^{r+1}$  divisent  $1 + m \diamond$  que l'on sait calculer; or  $f_1^{r+1}$  et  $h_r$  sont premiers entre eux et donc en appliquant le lemme 0.2, on calcule  $s$  et  $q_1, \dots, q_m$  dans  $k[X]$  tels que

$$s f_1^{r+1} h_r = 1 + q_1^2 + \dots + q_m^2$$

d'où le résultat.

*Remarque* : Étant donné, dans  $k[X]$ , l'écriture  $sf = 1 + a_1^2 + \dots + a_m^2$ , on peut calculer  $q_1, \dots, q_m$  et  $t$  dans  $k[X]$  tels que  $tf = 1 + q_1^2 + \dots + q_m^2$  avec, pour tout  $j \in \{1, \dots, m\}$ ,  $\text{deg } q_j < \text{deg } f$  et  $\text{deg } t < \text{deg } f - 1$ . En effet, il suffit de prendre pour  $q_j$  le reste de la division euclidienne de  $a_j$  par  $f$ , et on obtient le résultat.

Le coût de l'algorithme s'élève avec le degré des polynômes manipulés. La remarque précédente permet une réduction du degré pour les données, en particulier, dans le théorème 1.1, si  $f_2$  divise  $1 + y_1^2 + \dots + y_m^2$ , on peut remplacer les  $y_j$  par des polynômes de degré inférieur à celui de  $h_r$ .

**1.2. Mise en forme de l'algorithme**

Étant données, dans  $k[X]$ , deux familles  $(f_i)$ ,  $(A_i)_{i=1, \dots, p}$ , avec  $A_i = (a_{ij})_{j=1, \dots, m}$ , telles que, pour chaque  $i$ ,  $f_i$  divise  $1 + a_{i,1}^2 + \dots + a_{i,m}^2$  dans  $k[X]$ , l'algorithme décrit ci-dessous calcule par itération sur  $i$ , des éléments de  $k[X]$  :  $q_1, \dots, q_m$  tels  $\prod_{i=1, \dots, p} f_i$  divise  $1 + q_1^2 + \dots + q_m^2$ .

Initialisation :  $C := A_1, F := f_1, i := 1$ .

Dans la boucle suivante, pour  $i=2$  à  $p$ , on fait le passage de l'écriture d'un multiple de  $F$  comme  $1 + m \diamond$  à l'écriture d'un multiple de  $F \star f_i$  comme  $1 + m \diamond$ .

Répéter

- $i := i + 1$
- Recherche de  $r \in \mathbb{N}$  et  $h_r$  facteur de  $f_i$  tels que
  - $\text{pgcd}(F, h_r) = 1$
  - $F \star f_i$  divise  $F^{r+1} \star h_r$
- Recherche de  $k \in \mathbb{N}$  tel que  $2^{k-1} < r + 1 \leq 2^k$
- Calcul des coefficients  $l, m$  pour l'identité de Bezout entre  $h_r$  et  $F^{r+1}$ , tels que

$$l \star h_r + m \star F^{r+1} = 1$$

- Calcul, à partir de la solution obtenue pour  $F$ , d'un  $m$ -uplet  $D = (d_1, \dots, d_m)$  tel que  $F^{2^k}$  divise  $1 + d_1^2 + \dots + d_m^2$
- $F := F \star f_i$
- Calcul de  $C = (q_1, \dots, q_m)$ , tel que  $F$  divise  $1 + q_1^2 + \dots + q_m^2$
- Réduction du degré de la solution obtenue.

Jusqu'à  $i = p$

Dans [9] annexe 1, on trouvera un programme écrit pour  $m=1$ . Il est exécuté sur Macsyma pour l'exemple suivant, où  $p=4$  :

$$f_1 = 1 + x^2, \quad f_2 = f_3 = 1 + x^6, \quad f_4 = 1 + (x^3 + x + 1)^2.$$

Le polynôme  $f = \prod_{1 \leq i \leq 4} f_i$  est de degré 20, la solution  $C$ , de plus bas degré, obtenue est de degré  $19 = \deg f - 1$  avec  $s$  de degré  $18 = \deg f - 2$ .

## 2. THÉORÈME EFFECTIF DE LA NORME ET SON APPLICATION À LA STABILITÉ DE L'ÉCRITURE DU PRODUIT POUR CERTAINES COURBES

NOTATION : Soit  $k$  un sous-corps de  $\mathbb{R}$ . Soit  $c$  un élément de  $k[X, Y]$  unitaire en  $Y$  et de degré  $n$  en  $Y$ . On note  $A$  l'anneau  $k[X, Y]/c$  et  $B$  la clôture intégrale de  $k[X]$  dans la clôture algébrique de  $k(X)$ . On sait que  $A$  est un  $k[X]$ -module libre de rang  $n$  et  $B[Y]/c$  un  $B$ -module libre de rang  $n$ .

Pour  $u \in k[X, Y]$ , on note  $V(u)$  l'ensemble des points de la courbe représentative de  $u=0$  dans  $\mathbb{C}^2$ , et  $p_1$  la première projection de  $\mathbb{C}^2$  sur  $\mathbb{C}$ .

DÉFINITION 2.1 : Soit  $v \in k[X, Y]$ , on appelle *lieu étale de  $v$  sur  $\mathbb{C}[X]$* , l'ensemble des points  $(x, y)$  de  $V(v)$  pour lesquels  $\partial v / \partial Y(x, y)$  est non nul.

Le lieu étale de  $v$  est l'ensemble des points de  $V(v)$  où  $p_1$  est un homéomorphisme local pour la topologie usuelle de  $\mathbb{C}^2$ .

DÉFINITION 2.2 : Soit  $u \in k[X, Y]$ , on appelle *norme de  $u$  relative à l'extension* :  $k[X] \rightarrow A$  et on note  $N(u)$  l'élément de  $k[X]$  défini par

$$N(u) = \text{Résultant}(c, u, Y).$$

THÉORÈME DE LA NORME 2.3 : soit  $u \in k[X, Y]$  tel que

- (a)  $V(u) \cap V(c)$  soit contenu dans le lieu étale de  $c$ .  
 (b)  $p_1|_{V(u) \cap V(c)}$  soit injective.

Si  $u$  divise  $1 + m \diamond$  que l'on sait écrire dans  $A$  alors il existe un algorithme effectif donnant  $s, d_1, \dots, d_m$  dans  $k[X]$  tels que

$$sN(u) = 1 + d_1^2 + \dots + d_m^2.$$

La démonstration de ce théorème nécessite d'abord de montrer que  $u$  divise  $N(u)$  dans  $A$  et que le quotient est calculable, en utilisant le polynôme caractéristique  $P_u$  de l'application linéaire de  $A$  dans  $A$ , définie par la multiplication par  $u$ .

La traduction des hypothèses (a) et (b) du théorème, en fonction des coefficients de  $P_u$ , donnera une famille d'idempotents à partir de l'identité de Bezout.

Des algorithmes sur les fonctions symétriques des racines et les sommes de Newton permettra la construction effective du résultat.

Quelques préliminaires sont nécessaires avant la démonstration.

DÉFINITION 2.4 : Étant donné un module libre  $E$  de rang  $n$  sur un anneau commutatif  $R$  et une application linéaire  $\phi$  de  $E$  dans  $E$ , de matrice  $M$  dans une base donnée, on appelle *polynôme caractéristique de  $M$*  l'élément  $P_M$  de  $R[Z]$  défini par

$$P_M(Z) = \det(ZI - M)$$

où  $I$  est la matrice identité d'ordre  $n$ .

Ce polynôme est indépendant de la base choisie pour une application linéaire  $\phi$  donnée, [5], ch. XV, § 4, ce qui permet de dire que  $P_M(Z)$  est le *polynôme caractéristique de l'application linéaire  $\phi$* .

Si  $E$  est une  $R$ -algèbre finie et libre, pour  $u \in E$ , on note  $P_u$  le polynôme caractéristique de l'application  $R$ -linéaire de  $E$  dans  $E$  qui, à tout élément  $f$  de  $E$ , associe  $u \cdot f \in E$ .

Le polynôme  $c$  considéré comme polynôme en  $Y$  à coefficients dans  $k[X]$  admet  $n$  racines distinctes ou confondues dans  $B$ , que l'on note  $y_1, \dots, y_n$ .

PROPOSITION 2.5 : Soit  $u \in A$ , alors, on a

1. dans  $B[Z]$ , la factorisation

$$P_u(Z) = \prod_{1 \leq i \leq n} (Z - u(X, y_i))$$

2. dans  $k[X][Z]$ ,  $P_u(Z) = \text{Résultant}(c, Z - u, Y)$ .

*Démonstration* : On note  $y$  l'image de  $Y$  dans  $A$  et dans  $B[Y]/c$ . La multiplication par  $y$  de  $A$  dans  $A$  admet la même matrice  $M$  que la multiplication par  $y$  de  $B[Y]/c$  dans  $B[Y]/c$ .

D'après le théorème d'Hamilton-Cayley ([5], ch. XV, Th. 8), on a  $P_y(M) = 0$ . La matrice  $P_y(M)$  est la matrice de la multiplication par  $P_y(y)$  de  $B[Y]/c$  dans lui-même. Comme  $B[Y]/c$  est un  $B$ -module libre,  $P_y(y) = 0$ . Si on considère le polynôme  $P_y$  en la variable  $Y$  à coefficients dans  $B$ , son image dans  $B[Y]/c$  étant nulle, il est multiple de  $c$ ; de plus, il est unitaire et de degré  $n$ , donc, on a  $P_y = c$ . Ainsi, on obtient la factorisation dans  $B[Z]$  :

$$P_y(Z) = \prod_{1 \leq i \leq n} (Z - y_i).$$

D'après le théorème 14 de [5], ch. XV, § 4, on a

$$P_u(Z) = \prod_{1 \leq i \leq n} (Z - u(X, y_i)).$$

On connaît ainsi les racines de  $P_u(Z)$  dans  $B$ . Et, comme  $c$  est unitaire, d'après [11], ch. IV, § 28, on a  $P_u(Z) = \text{Résultant}(c, Z - u, Y)$  dans  $k[X, Z]$ .

PROPOSITION 2.6 : Soit  $u \in k[X, Y]$ , alors  $u$  divise  $N(u)$  dans  $A$  et il existe un algorithme effectif pour calculer  $Su \in A$  tel que  $N(u) = u(X, Y) Su(X, Y)$ .

*Démonstration* : Soit

$$P_u(Z) = Z^n + a_{n-1} Z^{n-1} + \dots + a_1 Z + a_0.$$

D'après [11], ch. IV, § 28 et la proposition 2.5, on a

$$N(u) = \prod_{1 \leq i \leq n} u(X, y_i) = (-1)^n P_u(0) = (-1)^n a_0 \quad \text{dans } k[X].$$

Dans  $A$ ,  $Y$  vérifie  $c(X, Y) = 0$ , donc  $u(X, Y)$  est une racine de  $P_u$ , ainsi

$$\begin{aligned} N(u) &= (-1)^{n-1} [u(X, Y)^n + a_{n-1} u(X, Y)^{n-1} + \dots + a_1 u(X, Y)] \\ &= (-1)^{n-1} u(X, Y) (u(X, Y)^{n-1} + \dots + a_1). \end{aligned}$$

Ainsi on obtient une factorisation de  $N(u)$  dans  $A$ , avec

$$Su(X, Y) = (-1)^{n-1} (u(X, Y)^{n-1} + \dots + a_1).$$

Si  $T$  désigne le polynôme  $(-1)^{n-1} (P_u(Z) - a_0)/Z$  alors on peut toujours écrire  $Su(X, Y) = T(u(X, Y))$ .

**PROPOSITION 2.7 :** *Soit  $u \in k[X, Y]$ , les hypothèses (a) et (b) du théorème de la norme sont satisfaites si et seulement si  $P_u(0)$  et  $P'_u(0)$  sont premiers entre eux dans  $k[X]$ .*

*Démonstration :* Si  $P_u(Z) = Z^n + a_{n-1}Z^{n-1} + \dots + a_1Z + a_0$ , d'après les propriétés des fonctions symétriques élémentaires des racines d'un polynôme et de la dérivation, on a dans  $B$  :

$$P_u(0) = a_0 = (-1)^n \prod_{1 \leq i \leq n} u(X, y_i)$$

$$P'_u(0) = a_1 = (-1)^{n-1} \sum_{1 \leq i \leq n} \prod_{j \neq i} u(X, y_j).$$

Or,  $P_u(0)$  et  $P'_u(0)$  ne sont pas premiers entre eux si et seulement s'ils admettent un zéro commun dans  $\mathbb{C}$ , soit  $x_0$ . Alors si  $y_{0,1}, \dots, y_{0,n}$  sont les racines de  $c(x_0, Y)$  dans  $\mathbb{C}$ , on a

$$\prod_{1 \leq i \leq n} u(x_0, y_{0,i}) = 0$$

donc, il existe  $h \in \{1, \dots, n\}$  tel que  $u(x_0, y_{0,h}) = 0$ ; d'autre part, on a alors

$$P'_u(0)(x_0) = 0 = \prod_{j \neq h} u(x_0, y_{0,j})$$

donc il existe  $j \neq h$  tel que  $u(x_0, y_{0,j}) = 0$ .

Si  $y_{0,j}$  est différent de  $y_{0,h}$ ,  $p_1|_{V(u) \cap V(c)}$  n'est pas injective et l'hypothèse (b) n'est pas vérifiée. Sinon,  $c(x_0, Y)$  admet une racine double :  $y_{0,j} = y_{0,h}$ , donc  $\partial c / \partial Y(x_0, y_{0,h}) = 0$  et alors  $V(u) \cap V(c)$  n'est pas contenu dans le lieu étale de  $c$  et l'hypothèse (a) n'est pas vérifiée.

Réciproquement, si  $p_1|_{V(u) \cap V(c)}$  n'est pas injective, il existe  $x_0 \in \mathbb{C}$  et deux racines distinctes de  $c(x_0, Y)$ ,  $y_{0,1}, y_{0,2}$ , telles que

$$u(x_0, y_{0,1}) = u(x_0, y_{0,2}) = 0.$$

Donc  $P_u(0)$  et  $P'_u(0)$  ont un zéro commun dans  $\mathbb{C}$ .

Si  $(x_0, y_0) \in V(u) \cap V(c)$  et  $\partial c / \partial Y(x_0, y_0) = 0$  alors  $y_0$  est une racine double de  $c(x_0, Y)$  et  $P_u(0)$  et  $P'_u(0)$  ont un zéro commun dans  $\mathbb{C}$ .

*Démonstration du théorème de la norme* : D'après la proposition 2.7,  $P_u(0)$  et  $P'_u(0)$  sont premiers entre eux dans  $k[X]$ , par l'algorithme d'Euclide, on sait calculer  $\lambda$  et  $\mu$  dans  $k[X]$  tels que

$$\lambda P'_u(0) + \mu P_u(0) = 1$$

ce qui peut s'écrire, dans  $B$ , en remplaçant  $\mu$  par  $(-1)^n \mu$  et  $\lambda$  par  $(-1)^{n-1} \lambda$  :

$$\lambda \sum_{1 \leq i \leq n} Su(X, y_i) + \mu N(u) = 1.$$

Par définition de  $N(u)$  et de  $Su$ , on obtient une famille d'idempotents de  $B$  modulo  $N(u)$  :

$$e_i = \lambda Su(X, y_i) = \lambda \prod_{j \neq i} u(X, y_j) \quad \text{pour } i = 1, \dots, n.$$

Par hypothèse, il existe  $r, P_1, \dots, P_m$  dans  $A$  tels que

$$r * u = 1 + P_1^2 + \dots + P_m^2.$$

Pour simplifier l'écriture, on note  $P_{h,i}$  pour  $P_h(X, y_i)$ . Pour tout  $i = 1, \dots, n$ , on a, dans  $B$

$$1 = P_{1,i}^2 + \dots + P_{m,i}^2 - r(X, y_i) u(X, y_i)$$

en multipliant par  $e_i$ , l'égalité devient :

$$e_i = P_{1,i}^2 e_i + \dots + P_{m,i}^2 e_i - r(X, y_i) e_i u(X, y_i).$$

Comme  $e_i u(X, y_i) = \lambda N(u)$  et que  $e_i = e_i^2$  modulo  $N(u)$ , on obtient :

$$e_i = P_{1,i}^2 e_i^2 + \dots + P_{m,i}^2 e_i^2 \quad \text{dans } B \quad \text{modulo } N(u).$$

En faisant la somme sur  $i = 1, \dots, n$ , on obtient :

$$1 = \sum_{1 \leq h \leq m} \left( \sum_{1 \leq i \leq n} P_{h,i}^2 e_i^2 \right) \quad \text{dans } B \quad \text{modulo } N(u).$$

Ainsi, modulo  $N(u)$ , on a

$$1 = \sum_{1 \leq h \leq m} \left( \sum_{1 \leq i \leq n} P_{h,i} e_i \right)^2.$$

Si on pose, pour tout  $h = 1, \dots, m$ ,

$$d_h = \sum_{1 \leq i \leq n} P_{h,i} e_i = \lambda \sum_{1 \leq i \leq n} P_h(X, y_i) Su(X, y_i),$$

$d_h$  est une fonction symétrique des racines  $y_1, \dots, y_n$  de  $c$ , donc  $d_h$  appartient à  $k[X]$ , et on obtient que  $N(u)$  divise  $1 + d_1^2 + \dots + d_m^2$  dans  $k[X]$ .

Pour calculer effectivement  $d_1, \dots, d_m$ , on constate que si

$$\lambda(X) P_h(X, y) S u(X, y) = d_{h,0}(X) + d_{h,1}(X)y + \dots + d_{h,n-1}(X)y^{n-1}$$

dans  $A$ , alors

$$d_h = \sum_{1 \leq i \leq n} (d_{h,0} + d_{h,1}y_i + \dots + d_{h,n-1}y_i^{n-1})$$

Si on note  $W_j = y_1^j + \dots + y_n^j$ , la somme de Newton d'ordre  $j$  des racines de  $c$ , on a

$$d_h = d_{h,0} W_0 + d_{h,1} W_1 + \dots + d_{h,n-1} W_{n-1}.$$

Dans [12], ch. IV, § 46, on trouve une formule de récurrence permettant de calculer les  $W_j$  en fonction des coefficients de  $c$  dans  $k[X]$ . Ce qui donne le calcul effectif de  $d_h$  pour  $h=1, \dots, m$ . La division euclidienne dans  $k[X]$  permet de calculer  $s$ . Ainsi, on a obtenu le théorème de la norme.

## 2.8. Mise en forme de l'algorithme de la norme

1. Donnée de  $c$  unitaire et de degré  $n$  en  $Y$ .
2. Donnée des  $P_1, \dots, P_m$  et de  $u$  tels que  $u$  divise  $1 + P_1^2 + \dots + P_m^2$  dans  $k[X, Y]/c$  et vérifie les hypothèses du théorème de la norme.
3. Calcul du polynôme caractéristique  $Pu = \text{Résultant}(c, Z - u, Y)$ .
4. Calcul des coefficients de degré 0,  $a_0(X)$ , et de degré 1,  $a_1(X)$  en  $Z$  dans  $Pu$ .
5. Calcul de  $\lambda$  et  $\mu$  par l'algorithme Euclide dans  $k[X]$  tels que  $\lambda a_1 + \mu a_0 = 1$ .
6. Calcul de  $Su$  tels que  $N(u) = u * Su$ .
7. Calcul des sommes de Newton pour le polynôme  $c$ .
8. Pour  $j=1$  à  $m$ 
  - calcul de  $Q_j = P_j * Su * \lambda$
  - réduction de  $Q_j$  modulo  $c$ , en un polynôme de degré  $\leq n-1$  en  $Y$
  - calcul de  $d_j$  en utilisant  $Q_j$  et les sommes de Newton pour  $c$ .
9. Calcul de  $s$  par la division euclidienne dans  $k[X]$ .

Avant de démontrer la « stabilité multiplicative » sous certaines hypothèses dans  $k[X, Y]/c$ , on va interpréter géométriquement les hypothèses (a) et (b) du théorème de la norme. On ne suppose plus  $c$  unitaire en  $Y$ ; soit  $n$  le degré total de  $c$  en  $X$  et  $Y$ .

D'après [4], ch. 3, § 1, on rappelle que, pour  $u \in k[X, Y]$  un point  $(x_0, y_0)$  de  $V(u)$  est dit *point singulier* de  $V(u)$  si  $\partial u / \partial X(x_0, y_0) = \partial u / \partial Y(x_0, y_0) = 0$ . La *tangente* en un point  $(x_0, y_0)$  non singulier de  $V(u)$  est donnée par l'équation :

$$\partial u / \partial X(x_0, y_0)(X - x_0) + \partial u / \partial Y(x_0, y_0)(Y - y_0) = 0.$$

On appelle *droite verticale* toute droite d'équation  $X = x_0$  dans le plan  $\mathbb{C}^2$ .

Ainsi, un point  $(x_0, y_0)$  de  $V(c)$  appartient au lieu étale de  $c$  sur  $\mathbb{C}[X]$  si et seulement si  $(x_0, y_0)$  est un point non singulier et  $V(c)$  n'admet pas de tangente verticale en  $(x_0, y_0)$ .

Géométriquement les hypothèses (a) et (b) éliminent les trois situations suivantes :

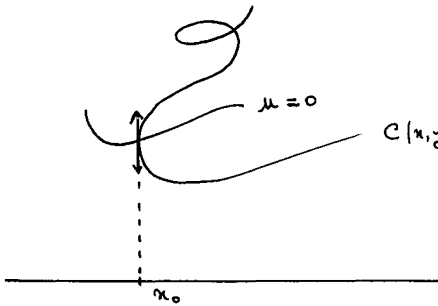


Figure 1

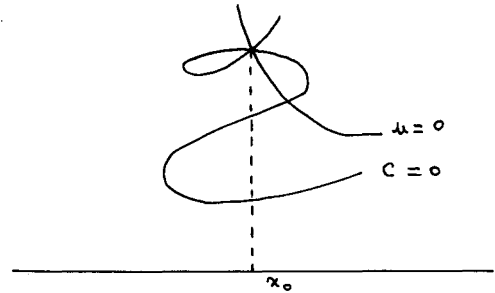


Figure 2

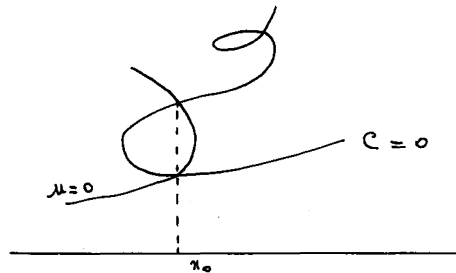


Figure 3

**THÉORÈME 2.9 :** Soit  $f$  un élément de  $k[X, Y]$  tel qu'aucun point singulier de  $c$  n'appartienne à  $V(f)$  et que  $V(f)$  et  $V(c)$  n'aient pas de composantes irréductibles communes. Si  $f$  est le produit d'une famille finie  $(f_j)_{j \in \{1, \dots, p\}}$  telle que chaque  $f_j$  divise  $1 + m \diamond$  que l'on sait écrire dans  $k[X, Y]/c$ , alors il existe un algorithme pour calculer  $q_1, \dots, q_m$  tels que, dans  $k[X, Y]/c$ ,  $f$  divise  $1 + q_1^2 + \dots + q_m^2$ .

*Démonstration :* On a  $V(f) = \bigcup_{1 \leq j \leq p} V(f_j)$  et  $\text{degré } f = \sum_{1 \leq j \leq p} \text{degré } f_j$ .

D'après le théorème de Bézout ([4], ch. V, § 3), le cardinal de  $V(f) \cap V(c)$  est majoré par  $n \cdot \text{degré } f$ . Soit  $q$  ce cardinal. Comme les points singuliers de  $c$  n'appartiennent pas à  $V(f)$ , le cas de la figure 2 n'existe pas. Il suffit de

trouver un système de coordonnées dans lequel aucun couple d'éléments de  $V(f) \cap V(c)$  ne se trouve sur une même droite verticale et dans lequel  $V(c)$  n'admet pas de tangente verticale en un point de  $V(f) \cap V(c)$ . On a au plus  $q(q-1)/2$  droites joignant deux à deux des éléments de  $V(f) \cap V(c)$  et au plus  $q$  tangentes à  $V(c)$  en ces points.

La notion de points d'intersection, de droite joignant deux points donnés et de droite tangente à une courbe est une notion intrinsèque, ne dépendant pas du système de coordonnées choisi. Par contre, on change la notion de droite verticale en faisant le changement de variables  $x=X+tY, y=Y$ . Il y a au plus

$$q + q(q-1)/2 = q(q+1)/2$$

valeurs à ne pas prendre pour  $t$ , pour éviter les cas de figures 1 et 3. Pour obtenir, de plus, l'équation de  $V(c)$  unitaire dans le nouveau système de coordonnées et de degré  $n$  en  $y$ , il n'y a qu'un nombre fini,  $d$ , de valeurs de  $t$  à éliminer. Comme tout sous-corps de  $\mathbb{R}$  est infini, il existe un système de coordonnées,  $x=X+tY, y=Y$ , dans lequel, pour tout  $j \in \{1, \dots, p\}$ ,  $F_j(x, y) = f_j(x-ty, y)$  vérifie les hypothèses du théorème 2.3 et dans lequel  $C(x, y)$  est unitaire. On détermine  $t$  algorithmiquement en essayant au plus  $(q(q+1)/2) + d$  valeurs. Dans  $k[x, y]/(C)$ , on peut appliquer l'algorithme déduit du théorème de la norme pour calculer, pour chaque

$$j \in \{1, \dots, p\} \quad D_{j,1}, \dots, D_{j,m}$$

tels que  $N(F_j)$  divise  $1 + D_{j,1}^2 + \dots + D_{j,m}^2$  dans  $k[x]$ ; cet algorithme donne aussi  $SF_j$ , pour  $j=1, \dots, p$ .

En appliquant l'algorithme du paragraphe 1, à la famille  $(N(F_j))$  dans  $k[x]$ , on obtient  $Q_1, \dots, Q_m$  et  $S$  tels que

$$S \prod_{1 \leq j \leq p} N(F_j) = 1 + Q_1^2 + \dots + Q_m^2.$$

D'après la proposition 2.6,  $\prod_{1 \leq j \leq p} f_j(x-ty, y)$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $k[x, y]/C(x, y)$ .

Comme l'opération « changement de variables » conserve les produits, en remplaçant  $x$  et  $y$  par leur valeur respective, on obtient

$$q_h(X, Y) = Q_h(X+tY) \quad \text{pour } h=1, \dots, m$$

$$s(X, Y) = S(X+tY) \sum_{1 \leq j \leq p} SF_j(X+tY, Y)$$

tels que dans  $k[X, Y]/c$ , on a :

$$s \prod_{1 \leq j \leq p} f_j = 1 + q_1^2 + \dots + q_m^2$$

C.Q.F.D.

## 2.10. Mise en forme de l'algorithme pour la stabilité de l'écriture du produit par la méthode de la norme

Cet algorithme va permettre pour une famille  $(f_j)_{j=1, \dots, p}$  soit de trouver un système convenable de coordonnées dans lequel on puisse appliquer l'algorithme de la norme à chaque  $f_j$ , soit de dire si l'un des  $V(f_j)$  possède un point singulier de  $c$  ou une composante irréductible commune avec  $V(c)$  :

1. Donnée de  $c$  de degré total  $n$ ,  $e_n =$  coefficient de  $Y^n$ , calcul de  $d$ , degré du polynôme  $e_n(X)$ .
2. Donnée des  $(f_i)_{i=1, \dots, p}$  et des  $m$ -uplets  $(P_i)_{i=1, \dots, p}$  pour tout  $i$ , on a  $P_i = (P_{i,j})_{j=1, \dots, m}$  tels que  $f_i$  divise  $1 + P_{i,1}^2 + \dots + P_{i,m}^2$ .

3. Calcul du degré total de chaque  $f_i$ .

4. Si il existe  $i \in \{1, \dots, p\}$  tel que Résultant  $(c, f_i, Y) = 0$

alors  $c$  et  $f_i$  possède une composante commune

sinon

– pour  $i=1$  à  $p$

calcul du nombre maximum,  $d_i$ , de directions ne convenant pas pour  $f_i$  (on note  $n_i$  le nombre de directions essayées pour  $f_i$ )

–  $i := 0$ ;  $n_0 := 0$ ;  $d_0 := 0$ ;

– Tant que ( $i < p$  et  $n_i \leq d_i + d$ )

–  $i := i + 1$ ;  $n_i := 1$ ;

– calcul du polynôme caractéristique  $Pf_i = \text{Résultant}(c, Z - f_i, Y)$

– calcul de ses coefficients  $a_0(X)$  de degré 0 et  $a_1(X)$  de degré 1 en  $Z$

– calcul de test = degré du pgcd de  $a_0$  et  $a_1$ ,

– tant que ( $e_n = 0$  ou test  $> 0$ ) et ( $n_i \leq d_i + d$ )

● faire le changement de variable  $X := X + Y$ ,  $Y := Y$  dans les  $m$ -uplets  $(P_i)_{i=1, \dots, p}$  et dans  $c$ ;  $n_i := n_i + 1$

● calcul du coefficient  $e_n$  de  $Y^n$  dans  $c$

● calcul du polynôme caractéristique  $Pf_i$ , de  $a_0$  et  $a_1$

● calcul de test = degré du pgcd de  $a_0$  et  $a_1$

Si  $n_i > d_i + d$

alors  $f_i$  passe par un point singulier de  $c$

sinon dans le nouveau système de coordonnées

– algorithme de la norme pour chaque  $f_i$ , calcul de  $Sf_i$

– algorithme de la stabilité de l'écriture du produit dans  $k[X]$  pour

$$N(f) = \prod_{1 \leq i \leq p} N(f_i)$$

– retour aux coordonnées initiales.

Cet algorithme a 3 sorties :

1.  $c$  et  $f$  ont une composante commune
2.  $f$  passe par un point singulier de  $c$
3. résultat :  $Q_1, \dots, Q_m$  tels que  $f$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $k[X, Y]/c$ .

Dans [9], annexe 2, on trouvera un programme écrit pour  $m=1$ . Il a été exécuté sur les exemples suivants :

exemple 1 :

$$c = 1 + (X + Y)^2, \quad f_1 = 1 + (X + Y)^6$$

sortie :  $f$  et  $c$  ont une composante commune.

exemple 2 :

$$c = ((X-2)^2 + Y^2 - 3)((X+2)^2 + Y^2 - 3), \quad f_1 = 1 + (X + Y)^2$$

$c$  admet  $(0, i)$  comme point singulier, et  $f_1$  passe par ce point singulier

exemple 3 :

$$c = 1 + X^2 + Y^2, \quad f_1 = 1 + (X + Y)^2, \quad f_2 = 1 + (2Y + X)^2$$

on a besoin d'effectuer 2 changements de variables ( $t=2$ ). Donc, l'algorithme de la norme est exécuté dans  $k[x, y]/c$ ,  $x = X + 2Y$ ,  $y = Y$ .

### 3. ALGORITHME POUR LA STABILITÉ DE L'ÉCRITURE DU PRODUIT POUR LES COURBES, OBTENU PAR CALCUL MODULAIRE

Soit  $k$  un corps, on considère  $c$  et  $f$  dans  $k[X, Y]$ , avec la seule condition géométrique suivante : leurs courbes représentatives dans  $\mathbb{C}^2$  n'ont pas de composantes irréductibles communes. Pour le corps  $k$ , l'hypothèse requise est que  $c$  puisse être rendu unitaire par changement de variables. On ne se limite pas aux sous-corps de  $\mathbb{R}$ . Soit  $A = k[X, Y]/c$ .

**THÉORÈME 3.1 :** *Si  $f$  est le produit d'une famille finie  $(f_i)_{i=1, \dots, p}$ , telle que chaque  $f_i$  divise  $1 + m \diamond$  que l'on sait écrire dans  $A$ , alors il existe un algorithme pour calculer  $Q_1, \dots, Q_m$  dans  $A$  tels que  $f$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $A$ .*

Comme dans le paragraphe 2, après un éventuel changement de variables dans  $c$  et  $f$ , on se ramène au cas où  $c$  est unitaire en  $Y$ .

Soit  $N(f)$  la norme de  $f$  relative à l'extension  $k[X] \rightarrow A$ . D'après la proposition 2.6,  $f$  divise  $N(f)$  dans  $A$ , donc pour obtenir le théorème 3.1, il

suffit d'obtenir la « stabilité multiplicative » dans

$$A/N(f) = k[X, Y]/(N(f), c).$$

Si les courbes, représentant  $f$  et  $c$ , avaient une composante irréductible commune, alors  $N(f)$  serait nul et le travail qui suit ne pourrait être fait.

**DÉFINITION 3.2 :** On appelle *norme sans facteur carré de  $f$  relative à l'extension  $k[X] \rightarrow A$* , notée  $nr(f)$ , l'élément de  $k[X]$  suivant :

$$N(f)/\text{pgcd}(N(f), N(f)')$$

Par définition,  $nr(f)$  est un polynôme de  $k[X]$  sans facteur carré.

**PROPOSITION 3.3 :** *Soit une décomposition en facteurs de  $nr(f) = \prod_{1 \leq i \leq h} v_i$ . Si pour chaque  $i \in \{1, \dots, h\}$ , l'image de  $f$  dans  $A/v_i$  divise  $1 + m \diamond$  que l'on sait écrire, alors il existe un algorithme pour calculer  $Q_1, \dots, Q_m$  tels que l'image de  $f$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $A/N(f)$ .*

*Démonstration :* Pour tout  $v \in k[X]$ , dire que  $f$  divise  $1 + m \diamond$  dans  $A/v$  est équivalent à dire que  $v$  divise  $1 + m \diamond$  dans  $A/f$ .

En utilisant la remarque 0.1 et le lemme 0.2 pour l'anneau  $A/f$  et le produit  $nr(f) = \prod_{1 \leq i \leq h} v_i$ , on obtient que  $nr(f)$  divise  $1 + m \diamond$  que l'on sait calculer dans  $A/f$ . On sait qu'il existe  $k \in \mathbb{N}$  tel que  $N(f)$  divise  $nr(f)^k$ . Cet entier peut se déterminer algorithmiquement sans faire la décomposition de  $N(f)$  en facteurs premiers. Le lemme 0.3 appliqué à l'anneau  $A/f$  et à l'image de  $nr(f)$  dans  $A/f$ , pour l'entier  $k$ , donne une méthode de calcul pour les éléments  $Q_1, \dots, Q_m$  tels que  $(nr(f))^k$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $A/f$ . Donc  $f$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $A/f$ .

Pour obtenir une décomposition de  $nr(f)$  vérifiant les hypothèses de la proposition 3.3, on pourrait imaginer de factoriser  $nr(f)$  indépendamment du problème, ce serait une opération coûteuse (voire impossible selon le corps). La technique, que l'on va décrire ici, évite toute factorisation systématique et ne fait que des calculs de PGCD, peu coûteux et facilement réalisables. Pour cela, on va introduire la notion de division dans  $k[X, Y]$  modulo un élément de  $k[X]$ , qui va induire une notion de PGCD de deux éléments de  $k[X, Y]$  modulo un élément de  $k[X]$  et va permettre d'établir des identités de Bezout comme au paragraphe 1.

**NOTATION :** Par convention, sauf précision différente, pour tout  $v \in k[X]$ , sans facteur carré, on désignera les éléments de  $k[X, Y]$  ou de  $(k[X]/v)[Y]$ ,

par des lettres majuscules :  $D, D_1, E \dots$  la même lettre en minuscule désignera le degré en  $Y$  :  $d, d_1, e \dots$  et celle en écriture grecque :  $\delta, \delta_1, \varepsilon \dots$  leur coefficient dominant en  $Y$ , appartenant à  $k[X]$  ou à  $k[X]/v$ .

LEMME 3.4 : Soient  $v \in k[X]$ , sans facteur carré,  $D$  et  $E$  des éléments non nuls de  $(k[X]/v)[Y]$ . On peut construire une factorisation de  $v = v_1 \dots v_h$  telle que, pour tout  $i = 1, \dots, h$ , on ait, dans  $(k[X]/v_i)[Y]$  :

soit  $E = 0$  ou  $D = 0$ ,

soit  $d \geq e$  et  $\text{pgcd}(\varepsilon, v_i) = 1$  ou respectivement  $d < e$  et  $\text{pgcd}(\delta, v_i) = 1$ .

On peut alors écrire dans  $(k[X]/v_i)[Y]$

$$D = QE + R \quad \text{ou respectivement} \quad E = QD + R$$

avec  $r < \inf(e, d)$ .

On dit que la division de  $D$  par  $E$  ou resp. de  $E$  par  $D$  modulo  $v_i$  est possible,  $Q$  est appelé le quotient de  $D$  par  $E$  ou resp. de  $E$  par  $D$  modulo  $v_i$  et  $R$  le reste de la division modulo  $v_i$ . Ils sont définis de façon unique.

Démonstration : Si on a  $d \geq e$ ,  $\text{pgcd}(\varepsilon, v) = 1$ , alors  $\varepsilon$  est inversible dans  $k[X]/v$ , on calcule son inverse  $\lambda$  par l'algorithme d'Euclide. Pour le polynôme :

$$R_1 = D - \delta \lambda Y^{d-e} E$$

on a  $r_1 < d$ . Si  $r_1$  est supérieur ou égal à  $e$ , on recommence en remplaçant  $(D, d, \delta)$  par  $(R_1, r_1, \rho_1)$ , pour obtenir  $R_2$ . Comme la suite d'entiers  $(r_k)$  est strictement décroissante, au bout d'un nombre fini d'opérations, on obtient un  $k$  tel que  $r_k < e$ , et en additionnant la suite d'égalités, on a

$$R = R_k = D - QE.$$

Si on a  $d < e$  et  $\text{pgcd}(\delta, v) = 1$ , on a le même résultat en inversant les rôles de  $D$  et  $E$ . On a obtenu la division modulo  $v$  et la factorisation de  $v$  est alors triviale.

Si on a  $d \geq e$  et  $\text{pgcd}(\varepsilon, v) = \mu_1 \neq 1$ , ou  $e > d$  et  $\text{pgcd}(\delta, v) = \mu_1 \neq 1$ , soit  $\mu_2 = v/\mu_1$ . On a une factorisation de  $v = \mu_1 \mu_2$ . Il reste à étudier séparément la division modulo  $\mu_1$  et modulo  $\mu_2$ .

Lorsque, modulo un facteur donné,  $D$  et  $E$  sont non nuls, et que la division n'est pas possible, il se factorise en deux polynômes de degré strictement inférieur, en effet, le pgcd ne peut pas être le facteur lui-même, le coefficient dominant étant non nul modulo ce facteur. Ainsi la factorisation s'arrête.

Si un polynôme est non nul modulo  $v_i$ , facteur irréductible, le pgcd de son coefficient dominant et de  $v_i$  est forcément 1, et alors la division est possible modulo ce polynôme. On obtient donc, par ce procédé, le résultat.

On appelle *scindage de  $v$  en  $(\mu_1, \mu_2)$*  dans l'essai de division de  $D$  par  $E$  la factorisation nécessaire, ci-dessus.

**DÉFINITION 3.5 :** Soient  $v \in k[X]$ ,  $D$  et  $E$  deux éléments non nuls de  $k[X, Y]$ , si modulo  $v$ , toutes les divisions successives de l'algorithme d'Euclide sont possibles jusqu'à obtenir un reste nul, on dit que *l'algorithme d'Euclide aboutit pour  $D$  et  $E$  dans  $k[X, Y]/v$* . Le dernier reste non nul est appelé *le pgcd de  $D$  et  $E$  modulo  $v$* ; il est défini à un élément inversible de  $k[X, Y]/v$  près.

**PROPOSITION 3.6 :** Soient  $v \in k[X]$ ,  $D$  et  $E$  appartenant à  $k[X, Y]/v$ , alors on peut trouver effectivement une factorisation de  $v$ ,  $v = v_1 \dots v_n$  telle que pour chaque  $i$ , dans  $k[X, Y]/v_i$ , soit l'algorithme d'Euclide aboutit pour  $D$  et  $E$ , soit  $D = 0$  ou  $E = 0$ .

Pour chaque  $i$ , tel que  $D$  et  $E$  soient non nuls dans  $k[X, Y]/v_i$ , si  $P_i$  est le dernier reste non nul obtenu, il existe  $L$  et  $M$ ,  $D_1$  et  $E_1$  tels que dans  $k[X, Y]/v$  :

$$\begin{aligned} LD + ME &= P_i \\ D &= P_i D_1, \quad E = P_i E_1 \end{aligned}$$

avec  $\deg_Y D = \deg_Y P_i + \deg_Y D_1$ ,  $\deg_Y E = \deg_Y P_i + \deg_Y E_1$ .

*Démonstration :* Ayant une factorisation de  $v$  satisfaisant au lemme 3.4 pour  $D$  et  $E$ , on factorise éventuellement les facteurs obtenus pour un essai de division de  $D$  ou  $E$  par les restes obtenus, et ainsi de suite pour les divisions successives de l'algorithme d'Euclide.

Les éléments  $L$ ,  $M$ ,  $D_1$  et  $E_1$  se calculent dans la suite d'égalités obtenues par les divisions successives dans  $k[X, Y]/v_i$ .

Comme le nombre de scindages possibles est inférieur au degré de  $v$ , comme les degrés des restes des divisions successives forment une suite strictement décroissante de  $\mathbb{N}$ , au bout d'un nombre fini d'opérations, scindage ou division, on obtient une factorisation de  $v$ , telle que modulo chacun de ses facteurs, le reste de la dernière division soit nul.

Revenant au problème posé, avec cette notion de pgcd et d'identité de Bezout, semblable à celle de  $k[X]$ , on va obtenir une proposition calquée sur le théorème 1.1.

**PROPOSITION 3.7 :** Soient  $f_1$  et  $f_2$  deux éléments de  $A$  divisant  $1 + m \diamond$  que l'on sait écrire. Alors, il existe un algorithme pour trouver une factorisation de

$nr(f)$  dans  $k[X, Y]$  telle que, pour chacun des facteurs  $v$ , il puisse calculer  $Q_1, \dots, Q_m$  tels que  $f_1 f_2$  divise  $1 + Q_1^2 + \dots + Q_m^2$  dans  $k[X, Y]/v$ .

*Démonstration* : D'après la proposition 3.6, on sait trouver une factorisation de  $nr(f)$  telle que, pour chaque facteur  $v$  :

(a) soit  $f_1 = 0$  ou  $f_2 = 0$  modulo  $v$ ,

(b) soit l'algorithme d'Euclide aboutit pour  $f_1$  et  $f_2$  dans  $k[X, Y]/v$ .

(a) Dans  $k[X, Y]/v$ , soit  $f_j = 0$ , pour  $j = 1$  ou  $2$ . On a  $f_1 f_2 = 0 = f_j$  et donc  $f_1 f_2$  divise  $1 + m \diamond$  que l'on connaît dans  $k[X, Y]/v$ , on a le résultat pour ce facteur.

(b) soit  $P_1$  le pgcd de  $f_1$  et  $f_2$  modulo  $v$ .

Si  $P_1$  est de degré 0 en  $Y$ , d'après la proposition 3.6, on sait calculer  $L$  et  $M$  tels que  $P_1 = L f_1 + M f_2$ . On a  $P_1 = \pi \in k[X]$  et par construction,  $\text{pgcd}(\pi, v) = 1$ , donc, on sait calculer  $\lambda$  et  $\mu$  dans  $k[X]$  tels que  $\lambda \pi + \mu v = 1$ . Ainsi,

$$\lambda \pi = (\lambda L) f_1 + (\lambda M) f_2 = 1 - \mu v.$$

Alors, le lemme 0.2 appliqué pour l'anneau  $k[X, Y]/v$  et les éléments  $f_1$  et  $f_2$  donne le résultat.

*Si on* sait calculer  $H_1$  tel que  $f_2 = P_1 H_1$ ; d'après la proposition 3.6, on a  $\deg_Y H_1 < \deg_Y f_2$ , modulo  $v$ . On peut trouver une factorisation de  $v$  satisfaisant à la proposition 3.6 pour  $f_1$  et  $H_1$  et on recommence jusqu'à trouver un facteur de  $f_2$  tel que son pgcd avec  $f_1$  soit de degré 0 en  $Y$ .

Comme le nombre de facteurs possibles de  $nr(f)$  est fini, à partir d'un certain rang, il n'y a plus de scindage possible. Dans la décomposition maximale obtenue, il y a deux sortes de facteurs :

- ceux tels que  $f_1 = 0$  ou  $f_2 = 0$  modulo ce facteur;
- ceux tels que, si  $v_i$  est l'un d'eux, on obtient, un entier  $r = r(v_i)$ , un facteur  $H_r$  de  $f_2$  tel que le pgcd modulo  $v_i$  de  $f_1$  et  $H_r$  soit de degré 0 en  $Y$  et  $f_r = P_1 P_2 \dots P_r H_r$ , chaque  $P_k$  divisant  $P_1$ . Par le même procédé que celui du théorème 1.1, on obtient le résultat dans  $k[X, Y]/v_i$ .

La proposition 3.7 construit une factorisation de  $nr(f)$  satisfaisant aux hypothèses de la proposition 3.3, laquelle donne le résultat du théorème.

#### *Majoration du degré des polynômes sur lesquels on travaille*

En pratique, les différents calculs de division, pgcd et autres se font dans  $k[X, Y]$  modulo des éléments de  $k[X]$ ,  $N(f)$ ,  $nr(f)$  ou l'un de ses facteurs. La donnée de  $c$  n'a été utilisée que pour déterminer  $N(f)$ . Comme on

travaille dans un système de variables où  $c$  est unitaire en  $Y$ , si  $n$  est son degré en  $Y$ , en restant dans  $A$ , on peut substituer à  $Y^n$  sa valeur modulo  $c$ ,  $Y^n - c$ , dans chaque polynôme  $Q_1, \dots, Q_m$  du résultat. Ce qui donne des polynômes  $Q_1, \dots, Q_m$  de degré  $\leq n-1$  en  $Y$ , mais la substitution a élevé le degré en  $X$ . Comme  $f$  divise  $N(f)$  en prenant le reste de la division euclidienne des coefficients de  $Y^i$ ,  $i=0, \dots, n-1$ , dans chaque  $Q_j$ ,  $j=1, \dots, m$ , par  $N(f)$ , on obtient des polynômes  $Q_1, \dots, Q_m$  de degré  $\leq n-1$  en  $Y$  et strictement inférieur à  $\deg(N(f))$  en  $X$ .

### 3.8. Mise en forme de l'algorithme

Pour ne pas alourdir la description de l'algorithme, on prend  $m=1$  ce qui n'enlève aucune généralité.

Soit  $f = \prod_{1 \leq i \leq p} f_i$  tel que  $f_i$  divise  $1 + P_i^2$  dans  $k[X, Y]/c$ , les données sont  $c, f$  et la liste de la famille  $(P_i)$ ,  $i=1, \dots, p$ .

La construction de la factorisation de  $nr(f)$  peut se schématiser par un arbre; chaque nœud correspond à un scindage d'un facteur  $v$  en  $(v_1, v_2)$ , lorsque le coefficient dominant d'un diviseur n'est pas premier avec  $v$ . On obtient que  $nr(f)$  est le produit des feuilles de l'arbre.

La construction et le parcours de l'arbre vont se faire par un procédé de « back-tracking », en travaillant sur trois listes de couples, le premier terme étant un facteur,  $v$ , de  $nr(f)$ , le second étant un élément de  $k[X, Y]$ : list, list 0, list 1, que l'on va expliciter.

La liste list 1 est initialisée à  $[[nr(f), P_1]]$ , si  $f_1$  divise  $1 + P_1^2$  dans  $k[X, Y]/c$  et les deux autres à la liste vide : [ ].

Ayant trouvé une factorisation de  $nr(f)$  telle que  $D = \prod_{1 \leq k \leq i} f_k$  divise  $1 + 1 \diamond$  modulo chacun des facteurs, soit :

$$nr(f) = \prod_{1 \leq j \leq l} v_j \cdot \prod_{1 \leq h \leq e} \mu_h.$$

On a construit pour  $j=1, \dots, l$ , un polynôme  $Q_j$  tel que  $D$  divise  $1 + Q_j^2$  modulo  $v_j$  et pour chaque  $h=1, \dots, e$ , on a trouvé  $D$  nul modulo  $\mu_h$ , qui divise  $1 + P_{k_h}^2$ . On a

$$\text{list } 0 = [[\mu_1, P_{k_1}], \dots, [\mu_e, P_{k_e}]]$$

$$\text{list } 1 = [[v_1, Q_1], \dots, [v_l, Q_l]].$$

les  $\mu_1, \dots, \mu_e$  sont des feuilles définitives de l'arbre en construction.

Description de l'algorithme pour le passage de  $D$  à  $D * f_{i+1}$  : l'initialisation est :

$$E := f_{i+1}, \quad \text{list} := \text{list } 1, \quad \text{list } 1 := [ \quad ],$$

tant que list non vide.

Si  $\text{list} = [[v_j, Q_j], \dots \dots \dots]$ , on travaille dans  $k[X, Y]/v_j$ ;

Si  $D$  (resp.  $E$ ) est nul modulo  $v_j$ , le problème est résolu pour  $D * E$  modulo ce facteur, si  $D$  (resp.  $E$ ) divise  $1 + P^2$ , on ajoute  $[v, P]$  à list 0 et list devient  $[[v_{j+1}, Q_{j+1}], \dots \dots \dots]$ .

Sinon, si on trouve  $P$  tel que  $D * E$  divise  $1 + P^2$  modulo  $v_j$ , on ajoute  $[v_j, P]$  dans list 1 et list devient  $[[v_{j+1}, Q_{j+1}], \dots \dots \dots]$ .

Sinon, il y a scindage de  $v_j$  en  $(v_{j,1}, v_{j,2})$  dans un essai de division en effectuant l'algorithme d'Euclide, list devient

$$[[v_{j,1}, Q_j], [v_{j,2}, Q_j], [v_{j+1}, Q_{j+1}], \dots \dots \dots],$$

et on recommence avec le terme  $[v_{j,1}, Q_j]$ .

Il a été démontré que list devient  $[ \quad ]$  au bout d'un nombre fini d'étapes.

Dans [9], en annexe 3, on trouvera un programme écrit pour  $m=1$  et exécuté sur Macsyma pour les exemples suivants :

exemple 1 :

$$c = 1 + x^2 + y^2, \quad f_1 = 1 + (x + y)^2, \quad f_2 = 1 + (2y + x)^2$$

d'où  $nr(f) = 25x^5 + 34x^3 + 9x$ .

On obtient  $v_1 = x, v_2 = x^2 + 1/2, v_3 = 50x^2 + 18$ ; on obtient list 0 =  $[ \quad ]$ .

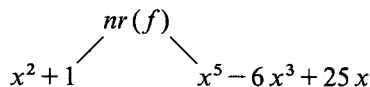
exemple 2 :

$$c = ((x + 2)^2 + y^2 - 3)((x - 2)^2 + y^2 - 3), \quad f_1 = 1 + (x + y)^2, \quad f_2 = 1 + x^2$$

dans ce cas  $f$  passe par un point singulier de  $c$  on a

$$nr(f) = x^7 - 5x^5 + 19x^3 + 25x$$

on obtient l'arbre suivant :



On obtient list 0 =  $[x^2 + 1, x]$ , car  $f_2 = 0$  modulo  $x^2 + 1$ .

exemple 3 :

$$c = y - x, \quad f_1 = 1 + x^2, \quad f_2 = 1 + y^2, \quad f_3 = 1 + (x + y)^2$$

on a  $nr(f) = (1 + x^2)(4x^2 + 1)$ .

Le facteur  $x^2 + 1$  est mis dans list 0 et le reste du calcul se fait modulo  $4x^2 + 1$ , sans autre scindage.

#### REMERCIEMENTS

L'auteur remercie vivement Louis Mahé pour ses nombreuses idées et ses conseils qui ont contribué à améliorer le contenu et la rédaction de cet article.

#### BIBLIOGRAPHIE

1. E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, Hamb. Abh.5, 1927, p. 100-115. Dans : The collected papers of Emil Artin, Reading, *Addison-Wesley*, 1965, p. 273-288.
2. J. BOCHNAK, M. COSTE et M.-F. ROY, Géométrie algébrique réelle, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, 3.Folge.Band 12, *Springer Verlag*, 1987.
3. C. DICRESCENZO et D. DUVAL, Utilisation des nombres algébriques avec le système algébrique « D5 ». Groupe de calcul formel de Grenoble, mai 1985.
4. W. FULTON, Algebraic Curves, Reading, *Benjamin*, 1969.
5. S. LANG, Algebra, Reading, *Addison-Wesley*, 1971.
6. T. Y. LAM, The algebraic theory of quadratic forms, Reading, *Benjamin*, 1973.
7. L. MAHE, Théorème de Pfister pour les variétés et anneaux de Witt réduits, *Invent. Math.*, 1986, 85, p. 53-72.
8. A. PFISTER, Zur Darstellung definiter Funktionen als Summe von Quadraten, *Invent. Math.*, 1967, 4, p. 229-237.
9. O. SIMON, Aspects quantitatifs de Stellensätze et algorithmes de multiplicativité des sommes de carrés, *Thèse 3<sup>e</sup> cycle*, Université de Rennes-I, 1987.
10. O. SIMON, Aspects quantitatifs de Nullstellensätze et de Positivstellensätze. Nombres de Pythagore, *Communications in Algebra*, 1989, 17, (3), p. 637-667.
11. B. L. VAN DER WAERDEN, Modern algebra, New York, *F. Ungar Publishing Company*, sixth printing, 1966.
12. H. WEBER, Traité d'Algèbre Supérieure traduit de l'allemand par J. Griess, Paris, *Gauthier-Villars*, 1898.