Revue d'histoire des mathématiques,
7 (2001), p. 67–89.

LA PREMIÈRE MÉTHODE GÉNÉRALE DE FACTORISATION DES POLYNÔMES. AUTOUR D'UN MÉMOIRE DE F.T. SCHUBERT

Maurice Mignotte et Doru Ştefănescu (*)

Résumé. — Nous présentons deux ouvrages peu connus de N. Bernoulli (1708) et de F.T. Schubert (1794) sur la factorisation des polynômes à coefficients entiers ainsi que les recherches de L. Kronecker et B.A. Hausmann sur le même sujet. La méthode de factorisation de Bernoulli-Schubert utilise le calcul des différences finies et l'interpolation par différences finies. Elle a été redécouverte par Kronecker (1882), qui a utilisé l'interpolation de Lagrange. Les deux procédés permettent de factoriser des polynômes dont les degrés et les coefficients sont petits. Un algorithme qui combine les résultats de Bernoulli-Schubert et Kronecker a été obtenu par B.A. Hausmann. Sa méthode est plus efficace pour des polynômes stables. Ces trois méthodes sont brièvement comparées avec les algorithmes modernes de factorisation.

Abstract. — The first general method of factorization of polynomials. On a memoir of F.T. Schubert. — We analyse two little known papers of N. Bernoulli (1708) and F.T. Schubert (1794) on the factorization of integer polynomials as well as the work of L. Kronecker and B.A. Hausmann on the same topic. The factorization method of Bernoulli-Schubert uses the calculus and the interpolation of finite differences. It was rediscovered by Kronecker (1882), who used Lagrange interpolation. Both procedures allow the effective factorization of polynomials having small degrees and coefficients. An algorithm combining the results of Bernoulli-Schubert and Kronecker was obtained by B.A. Hausmann. His method is particularly useful for the factorization of stable polynomials. The three methods are briefly compared with modern factorization algorithms.

(*) Texte reçu le 1er juillet 1999, révisé le 5 avril 2001.
M. Mignotte, Université Louis Pasteur, UFR de Mathématique, 67084 Strasbourg Cedex (France). Courrier électronique : mignotte@math.u-strasbg.fr.
D. Ştefănescu, Université de Bucarest, B.P. 39-D5, Bucarest 39 (Roumanie).
Courrier électronique : stef@irma.u-strasbg.fr et stef@mat.fizica.unibuc.ro.

Mots clés : factorisation des polynômes, I. Newton, G.W. Leibniz, N. Bernoulli (I), F.T. Schubert, L. Kronecker.

Classification AMS : 01A50, 01A55, 01A45, 01A60, 12-03, 39-03.

INTRODUCTION

Die Definition der Irreductibilität entbehrt so lange einer sicheren Grundlage, als nicht eine Methode angegeben ist, mittels derer bei einer bestimmten, vorgelegten Function entschieden werden kann, ob dieselbe der aufgestellten Definition gemäss irreductibel ist oder nicht[1].

L. Kronecker (1882)

L'étude de la décomposition d'un polynôme à coefficients entiers en produit de polynômes irréductibles remonte au XVII^{e} siècle. Après les procédés inventés par Isaac Newton et Gottfried W. Leibniz pour trouver les diviseurs linéaires et quadratiques, un véritable algorithme général de factorisation n'a été construit que par Nicolas (I) Bernoulli et Friedrich T. Schubert.

La première publication, due à N. Bernoulli, date de 1708 ; sa diffusion a été très limitée et on peut penser qu'elle a été quasiment inconnue du milieu mathématique. La publication de F.T. Schubert paraît en 1798 dans le journal de l'Académie des Sciences de Saint-Pétersbourg[2]. Ce mémoire de Schubert a été lui aussi peu connu de la communauté mathématique. En revanche les recherches de Leopold Kronecker de 1882 sur le même sujet ont joui d'une notoriété rapide.

À notre connaissance, le travail de Nicolas Bernoulli n'a pas été cité depuis 1900. Un ouvrage aussi important que l'*Encyclopédie des sciences mathématiques* éditée par Jules Molk [1907] (réimpression [1992]) ignore les mémoires de N. Bernoulli et F.T. Schubert. Ce dernier cependant est cité au moins deux fois : par Moritz Cantor [1908, p. 137] et par Donald E. Knuth [1969, p. 390]. Notons que la bibliographie sur les racines des polynômes de John Michael McNamee [1993] ne mentionne pas les ouvrages de N. Bernoulli et de F.T. Schubert.

Nous allons présenter ces mémoires peu connus de N. Bernoulli et F. T. Schubert ainsi que le développement ultérieur de ces idées dans des travaux des XIX^{e} et XX^{e} siècles.

La note de Nicolas Bernoulli est, à notre connaissance, le premier travail où on donne une méthode générale pour la décomposition d'un polynôme

[1] La définition de l'irréductibilité manque d'une base solide, tant qu'on n'a pas inventé une méthode par laquelle il serait possible de décider si une fonction donnée est irréductible ou non selon cette définition.

[2] C'est un rapport présenté le 19 juin 1794 à l'Académie de Saint-Pétersbourg, dont Schubert était membre.

à coefficients entiers en produit de polynômes irréductibles. Sa méthode a été retrouvée et présentée avec plus de détails par F.T. Schubert.

Le problème de la factorisation effective des polynômes constitue une des questions fondamentales dans le domaine du calcul formel qui a connu un essor formidable depuis le début des années 1970. Il faut dire que des algorithmes beaucoup plus efficaces, et de principes radicalement différents, ont été inventés dans les dernières décennies.

1. DE NEWTON À LEIBNIZ

Les travaux sur la factorisation des polynômes à coefficients entiers avant Bernoulli-Schubert se concentrent généralement sur la recherche des facteurs linéaires et quadratiques. Évidemment, pour les diviseurs linéaires, ce problème est résolu dès qu'on a trouvé toutes les racines rationnelles du polynôme à factoriser. Des procédés pour trouver ces racines étaient déjà connus au milieu du XVII^{e} siècle [Molk 1907, p. 209–210].

Newton, Arithmetica universalis

Newton a exposé une méthode systématique pour trouver les diviseurs linéaires et quadratiques dans son traité *Arithmetica universalis* [Newton 1707]. Cet ouvrage correspond à la rédaction d'un cours professé par Newton entre 1673 et 1683 où il propose une présentation unifiée de l'arithmétique et de l'algèbre. Le manuscrit de ce cours a été déposé par Newton pendant l'hiver 1683–1684 sous le titre *Arithmeticæ universalis Liber primus.* Il se trouve dans [*Math. Papers*, vol. 5], édités par D.T. Whiteside. Dans une section d'*Arithmetica universalis* intitulée *De inventione Divisorum*, Newton énonce des règles pour trouver les facteurs d'un polynôme et discute plusieurs exemples. La méthode de Newton repose sur l'étude des tableaux de différences finies et l'interpolation des polynômes par différences finies. C'est un des outils fréquemment utilisé jusqu'au début du XX^{e} siècle.

Si $y_0, \ldots, y_n$ est une suite de nombres réels, le *tableau des différences* de cette suite est formé par les différences finies $\Delta^i(y_0, \ldots, y_n)$, où

$$\Delta^1(y_0, \ldots, y_n) = \{y_1 - y_0, y_2 - y_1, \ldots, y_n - y_{n-1}\} = \{y_0^{(1)}, y_1^{(1)}, \ldots, y_{n-1}^{(1)}\},$$

$$\Delta^i(y_0, \ldots, y_n) = \Delta^1(y_0^{(i-1)}, \ldots, y_{n-i}^{(i-1)}).$$

La méthode de Newton

Newton présente sa méthode en énonçant deux règles [Newton, 1802, p. 46–47]. La première décrit la manière de trouver les diviseurs d'un nombre entier positif. La seconde s'énonce ainsi :

« Si la quantité, après avoir été divisée par tous les diviseurs simples, demeure encore composée, et qu'on soupçonne qu'elle contienne quelque diviseur composé ; disposez-la selon les dimensions de quelqu'une de ses lettres, et substituez successivement à la place de cette lettre, trois ou un plus grand nombre de termes de la progression arithmétique $3, 2, 1, 0, -1, -2$. Et il en résultera autant de valeurs différentes, que vous écrirez avec les diviseurs à côté des termes de la progression qui les auront produites ; ayant soin d'écrire aussi chaque diviseur avec un signe positif et un signe négatif. Comparez les diviseurs qui se trouvent dans une ligne avec ceux des autres lignes, pour voir s'ils ne formeraient pas une progression arithmétique. Et pour cela, commencez par les plus forts, pour descendre aux plus faibles, en suivant la même marche que la progression arithmétique $3, 2, 1, 0, -1, -2$. Si cette recherche vous fournit quelque progression dont les termes ne diffèrent que d'une unité, ou quelque nombre qui divise la plus haute puissance de la quantité proposée, écrivez cette progression dans le même ordre que la première, plaçant chacun de ses termes à côté de la ligne des diviseurs qui l'a produit ; et le terme qui, dans cette progression, répondra au terme 0 de la progression primitive, étant divisé par la différence des termes, et joint à la lettre à laquelle il avait été substitué, formera une quantité avec laquelle il faudra tenter la division. »

Dans le reste de la section sur «*la manière de trouver les diviseurs*» Newton considère plusieurs polynômes particuliers et analyse leurs factorisations possibles. Pour le polynôme $x^3 - x^2 - 10x + 6$, par exemple, il choisit les valeurs $x = 1,\ 0,\ -1$ et obtient les entiers $-4,\ 6,\ +14$. Ensuite il construit le tableau suivant avec les diviseurs positifs des valeurs absolues de ces nombres. Il présente ainsi le tableau suivant :

1	4	$1,\ 2,\ 4$	$+4$
0	6	$1,\ 2,\ 3,\ 6$	$+3$
-1	14	$1,\ 2,\ 7,\ 14$	$+2$

Mettant en évidence dans la dernière colonne une progression arithmétique,

il en déduit que le polynôme $x+3$ est un diviseur [Newton 1761, p. 62] et que l'autre facteur est $xx-4x+2$:

« Ensuite comme le terme le plus élevé x^3 n'a de diviseur que l'unité, je cherche parmi les diviseurs quelque progression dont les termes ne diffèrent que d'une unité, et qui, en descendant des plus forts aux plus faibles, décroissent comme ceux de la progression 1, 0, -1. Je ne trouve qu'une progression de cette espèce, c'est 4, 3, 2. Je prends donc le terme $+3$ qui se trouve dans la même ligne que 0 de la première progression 1, 0, -1, je le joins à x, et je tente la division par $x+3$; elle réussit, et j'obtiens pour quotient $xx-4x+2$ » [Newton 1802, p. 47].

Newton sait que l'interpolation pourrait conduire à des diviseurs linéaires à coefficients rationnels qui ne soient pas des entiers. Ainsi le polynôme $6y^4-y^3-21yy+3y+20$ admet le facteur $y+\frac{4}{3}$. Newton remarque qu'en le multipliant par le diviseur 3 du coefficient dominant on obtient $3y+4$, qui est un diviseur à coefficients entiers.

Dans son cours [Newton, *Math. Papers*, vol. 5, p. 46] ainsi que dans *Arithmetica universalis*, Newton [1802, p. 49–50] donne également une méthode pour trouver les diviseurs quadratiques :

« Substituez dans la proposée, à la place de la lettre, quatre ou un plus grand nombre de termes de la progression 3, 2, 1, 0, -1, -2, -3. Placez tous les diviseurs des nombres qui en résulteront dans les mêmes lignes que les termes de la progression ; élevez les termes de la progression au quarré ; multipliez ces quarrés par quelque diviseur numérique du terme le plus élevé de la quantité proposée ; ajoutez successivement à ces produits les diviseurs des nombres qui ont résulté de vos suppositions ; retranchez-les ensuite, et écrivez ces sommes et ces différences dans le même ordre que les termes de la première progression ; cherchez toutes les progressions qui peuvent se rencontrer dans ces sommes et ces différences, en allant des termes d'une ligne à ceux de la ligne suivante. Soit, par exemple, $\mp C$ le terme d'une progression de cette espèce qui se trouve dans la même ligne que le terme 0 de la première progression ; soit $\mp B$ la différence qu'on obtient en retranchant $\mp C$ du terme immédiatement supérieur qui se trouve dans la même ligne que le terme 1 de la première progression ; soit enfin A un diviseur numérique du terme le plus élevé, et ℓ la lettre de la quantité proposée ; alors $A\ell\ell \pm B\ell \pm C$ sera un diviseur qu'il faudra essayer. »