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. »

Newton considère comme premier exemple

$$x^4 - x^3 - 5x^2 + 12x - 6 = 0,$$

trouve, par cette méthode, $x^2 + 2x - 2$ et $x^2 - 3x + 3$ comme diviseurs possibles et conclut que « la réduction réussit pour chacun des deux ».

Les successeurs de Newton

Les contemporains de Newton ont été vivement intéressés par ces résultats, ils ont essayé de comprendre le procédé de factorisation de Newton et de donner des justifications de la règle indiquée par lui. Parmi eux on peut citer G.W. Leibniz, J. Hermann, N. Bernoulli (I), et plus tard D. Bernoulli puis F.T. Schubert.

Hermann

Jakob Hermann (1678–1733) donne une démonstration dans sa lettre du 12 juillet 1708 adressée à Leibniz, [*Math. Schriften*, IV, p. 328–332]. Il considère un polynôme de degré m,

$$Ax^m + px^{m-1} + qx^{m-2} + rx^{m-3} \quad etc.$$

et étudie les diviseurs possibles à coefficients entiers de la forme $ax \pm b$ et $axx \pm bx \pm c$, en utilisant des tableaux de différences finies des valeurs du polynôme à factoriser. Pour le cas d'un diviseur linéaire il utilise les valeurs 1, 0 et -1 et obtient que la progression arithmétique de la dernière colonne doit être $a \pm b$, $\pm b$, $-a \pm b$. Pour les diviseurs quadratiques Hermann considère les valeurs en $2, 1, 0, -1$, etc. et étudie un tableau dans lequel il pose les valeurs calculées en f, g, h, k :

$aff \pm bf \pm c$	$\pm bf \pm c$	$\pm 2b \pm c$
$agg \pm bg \pm c$	$\pm bg \pm c$	$\pm b \pm c$
$ahh \pm bh \pm c$	$\pm bh \pm c$	$\pm c$
$akk \pm bk \pm c$	$\pm bk \pm c$	$\mp b \pm c$

Leibniz

Leibniz a publié une recension d'*Arithmetica universalis* dans les *Acta eruditorum* de novembre 1708 (p. 519–526). Il reprend l'exemple du polynôme $x^3 - x^2 - 10x + 6$ et le tableau de Newton ainsi que la factorisation de ce polynôme.

Leibniz, qui n'était pas satisfait par la méthode de Newton, en donne une autre dans sa lettre adressée à Jakob Hermann du 6 septembre 1708 [Leibniz,*Math. Schriften*, IV, p. 335–339]. Cette lettre contient une note intitulée «*Methodus generalis investigandi divisores formularum rationalium integralium ex datis divisoribus numerorum rationalum integrorum*». Leibniz discute le cas des polynômes de degré 5 et considère comme exemple la factorisation du polynôme $2x^5 + 3x^4 + 8x^3 + 6xx + 5x + 6$ qu'il note $\odot$. Il cherche une factorisation en un produit d'un polynôme cubique $b + cx + dxx + ex^3$ par un polynôme quadratique $\beta + \gamma x + \delta xx$. Il choisit un entier h plus grand que les coefficients du polynôme à factoriser et remarque que la valeur du diviseur du polynôme $\odot$ en h est un diviseur de la valeur du polynôme à factoriser en ce point. Pour le polynôme $2x^5 + 3x^4 + 8x^3 + 6xx + 5x + 6$ il prend $h = 10$ et obtient la valeur 238656. Ensuite il forme un tableau des diviseurs de ce nombre, et étudie ses propriétés. Il trouve qu'il n'existe pas de facteur linéaire et finalement obtient les facteurs $2x^3 + x^2 + x + 2$ et $x^2 + x + 3$. Leibniz considère uniquement des polynômes dont les coefficients sont positifs et il calcule la valeur du polynôme à factoriser pour un entier plus grand que tous les coefficients. Ce qui distingue sa méthode de celle de Newton est que Leibniz utilise une seule valeur du polynôme.

On trouve une excellente présentation de la méthode de Leibniz dans l'article de E. Netto et R. Le Vavasseur intitulé « Réductibilité dans le domaine des nombres rationnels », [Molk 1907, 2$^{\text{e}}$ partie, p. 209–210].

D. Bernoulli

Daniel Bernoulli (1700–1782) donne des explications supplémentaires sur la méthode de Newton dans une note de bas de page insérée dans *Arithmetica universalis* [Newton 1761, p. 63–64]. Il étudie le cas particulier des diviseurs linéaires $mx + n$ des polynômes cubiques $2x^3 + xx + g$. Il considère les valeurs -2, 1, 0 et -1 et étudie ensuite les tableaux de différences finies de leurs diviseurs.

2. L'ALGORITHME DE BERNOULLI-SCHUBERT

Nicolas (I) Bernoulli (1687–1759)

Neveu de Jacques et Jean Bernoulli, Nicolas Bernoulli[3] a étudié les mathématiques avec ses oncles. Il a beaucoup voyagé et a été professeur à Padoue et à Bâle. La plus grande partie de ses recherches se trouve dans sa correspondance qui comprend presque 560 lettres, dont une grande partie avec Pierre Rémond de Montmort (1678–1719).

Nicolas Bernoulli a donné une autre démonstration de la méthode de Newton en 1708, publiée en 1745 seulement[4]. Cette preuve a été communiquée par son oncle Jean Bernoulli à Leibniz dans une lettre du 16 mai 1708 [Leibniz, *Math. Schriften*, III, p. 827–835]. Dans cette lettre, Jean Bernoulli insère une note de son neveu, intitulée «*Regula generalis inveniendi aequationes, per quas alia quaepiam data, modo reducibilis sit, dividi potest*». Il propose à Leibniz de publier la note de son neveu Nicolas, alors agé de 20 ans, dans les *Acta eruditorum*. Finalement, ce texte a paru en 1745 dans la correspondance entre Leibniz et Jean (I) Bernoulli, [Bernoulli, 1745, vol. 2, p. 180].

Le travail de N. Bernoulli

Dans sa note, N. Bernoulli développe la procédure de Newton et il donne des tableaux détaillés sur la méthode des différences finies. Il se rapporte, par exemple, à l'équation $3x^3 - 4xx - 6x + 15 = 0$ et considère la suite 1, 1, 3, 7, 13, formée avec des diviseurs des valeurs absolues de ce polynôme en 2, 1, 0, −1, −2. Ensuite il considère le tableau

	differ. 1	differ. 2 per 2 divisae
1		
	0	
1		1
	−2	
3		1
	−4	
7		1
	−6	
13		

et trouve le facteur $xx - 3x + 3 = 0$.

[3] Appelé aussi Nicolas (I) Bernoulli, pour le distinguer de son cousin Nicolas (II) Bernoulli (1695–1725).

[4] Voir, dans [Molk 1907, p. 210], la note de Gustaf Eneström au bas de la page 700 .

Dans un autre exemple N. Bernoulli obtient la factorisation du polynôme $2x^7+2x^6-16x^5-13x^4+41x^3+22xx-32x-9$. Par sa méthode il trouve les diviseurs $2x^3-4x-1$ et $x^4+x^3-6xx-4x+9$, donc des facteurs cubiques et biquadratiques, au-delà de ce qu'obtenait Newton dans *Arithmetica universalis*.

N. Bernoulli envisage de trouver tous les diviseurs possibles par cette méthode et donne une règle pour former les tableaux de différences. Il considère «*une équation*»

$$P+Qx+Rxx+Sx^3+Tx^4+Vx^5+Wx^6 \quad etc. = 0,$$

un diviseur possible de la forme

$$p+qx+rxx+sx^3+tx^4+vx^5 \quad etc. = 0$$

et les valeurs de ce diviseur possible en 3, 2, 1, 0, −1, −2, −3, puis construit le tableau des différences itérées

	differentiae primae	diff 2ae per 2 div
$p+3q+9r+27s+81t+243u$		
	$q+5r+19s+65t+211u$	
$p+2q+4r+8s+16t+32u$		$r+6s+25t+90u$
	$q+3r+7s+15t+31u$	
$p+q+r+t+u$		$r+3s+7t+15u$
	$q+r+s+t+u$	
p		$r+0s+t+0u$
	$q-r+s-t+u$	
$p-q+r-s+t-u$		$r-3s+7t-15u$
	$q-3r+7s-15t-31u$	
$p-2q+4r-8s+16t-32u$		$r-6s+25t-90u$
	$q-5r+19s-65t-211u$	
$p-3q+9r-27s+81t-243u$		

diff 3ae per 3 divisae	diff 4ae per 4 divisae	diff 5ae per 5 divisae
$s+6t+25u$		
	$t+5u$	
$s+2t+5u$		u
	$t+0u$	
$s-2t+5u$		u
	$t-5u$	
$s-6t+25u$		

et donne des conditions pour obtenir des progressions arithmétiques dans les colonnes de ce tableau, ce qui permet de reconnaître un diviseur[5].

Friedrich Theodor Schubert (1758–1825)

Né le 30 octobre 1758 à Helmstedt (Braunschweig), décédé le 21 octobre 1825 à Saint-Pétersbourg (Russie), Schubert a étudié à Greifswald et Göttingen, ensuite a été précepteur entre 1780 et 1783. Il s'établit alors en Russie où il est successivement inspecteur scolaire du département d' Hapsal en Estonie (1783–1785), géographe (1785), membre correspondant de l'Académie de Saint-Pétersbourg (1786), membre de cette Académie (1789), surveillant de la bibliothèque et du cabinet des monnaies de l'Académie (1800–1819), etc. [Cantor 1908, p. 429][6].

F.T. Schubert a publié plusieurs livres sur l'astronomie, y inclus un traité d'astronomie théorique en trois volumes (trois éditions, dont une en français, 1791) et une histoire de l'astronomie (1804). Il est l'auteur de plusieurs articles publiés dans *Nova Acta Academiæ Scientiarum Petropolitanæ*, *Berliner Astronomisches Jahrbuch* (fondée par Johann Bode) et *Monatliche Korrespondenz zur Beförderung der Erd- und Himmels-kunde* (éditée par Franz Xaver von Zach) entre 1788 et 1830 [Poggendorff 1863, t. 2, p. 850–852]. Ses recherches ne portent pas seulement sur l'astronomie mais aussi sur la géométrie, l'analyse et l'algèbre. En plus de son mémoire sur la factorisation des polynômes de 1798, il a publié en 1810 un autre article sur l'algèbre, «*Demonstratio theoremati algebraici*», dans les *Mémoires de l'Académie des sciences* de Saint-Pétersbourg. En analyse, par exemple, il s'est penché sur les séries de Taylor, les extrema, le développement des séries en fractions continues et les fonctions implicites en deux variables. Cela prouve qu'il avait des préoccupations encyclopédiques, comme la plupart des mathématiciens du siècle des Lumières. Formé en Allemagne, en particulier comme étudiant à Göttingen, Schubert a eu l'occasion de consulter les œuvres de Leibniz et de Newton, d'où son intérêt pour le calcul des diviseurs linéaires et quadratiques des polynômes à coefficients entiers.

N. Bernoulli et F.T. Schubert sont des pionniers. Avant eux il y avait,

[5] Voir la motivation plus loin.

[6] Notons que F.T. Schubert est l'arrière–grand–père maternel de la célèbre mathématicienne Sophie Kovalevskaya (1850–1891) [Brockhaus-Efron, vol. 30, p. 499–500].

à notre connaissance, seulement des études particulières — pas de traitement du cas général. Même si leurs techniques de rédaction (usage des tableaux, présentation des méthodes par des exemples) remontent au moins à Newton, leurs techniques pour la factorisation étaient en avance de plus de cent ans.

F.T. Schubert et Arithmetica universalis

Dès le début de son mémoire Schubert précise que sa méthode repose sur des résultats de I. Newton pour trouver des facteurs de degré un ou deux des polynômes à coefficients entiers [Newton 1707].

F.T. Schubert cite, au début de son mémoire (p. 172), l'ouvrage *Universal Arithmetick. Of the Invention of Divisors.* Il ne donne ni l'année, ni l'éditeur. Puisqu'il s'agit d'une version anglaise, il est probable qu'il a utilisé la traduction de Raphson de 1710 ou de 1728, [Newton 1710]. Rien n'indique que Schubert connaissait le travail de N. Bernoulli [1708].

Même si son ouvrage est contemporain des œuvres de Lagrange, le style de Schubert est très proche de celui de Newton, Leibniz et Bernoulli. Il énonce une règle générale, ensuite il donne la justification sur des exemples.

On ignore la raison pour laquelle il s'est occupé de la méthode de Newton. Tandis que pour Bernoulli l'ouvrage de Newton était récent et avait attiré l'intérêt des contemporains, le mémoire de Schubert [1798] sur la factorisation semble être passé quasiment inaperçu.

Le travail de Schubert

Décrivons ce que F.T. Schubert a exposé dans son mémoire. Nous conservons pour le moment ses notations, ensuite nous adopterons des conventions plus modernes.

Schubert considère un polynôme à coefficients entiers[7], qu'il note X,

$$X = Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots$$

et il se propose de trouver un facteur, noté y, de degré $n \geq 1$ à coefficients entiers,

$$y = ax^n + bx^{n-1} + cx^{n-2} + \cdots + fxx + gx + h.$$

[7] Comme Jakob Hermann, voir [Leibniz, *Math. Schriften*, IV, p. 329].

Il écrit (p. 177) qu'on a $X = yY$, avec

$$Y = (kx^{\mu} + \ell x^{\mu-1} + \cdots)(px^{\tau} + qx^{\tau-1} + \cdots)$$

et il en déduit

$$m = n + \mu + \tau \quad \text{et} \quad A = akp,$$

même s'il n'utilise pas cette décomposition. Puis il considère le polynôme

$$ax^n - y = -bx^{n-1} - cx^{n-2} - \cdots - fxx - gx - h,$$

calcule les valeurs des polynômes X et $ax^n - y$ aux points 0, ± 1, ± 2, ... et construit le tableau suivant (page 178) :

x	Factor y	ax^n	Residua
$+2$	$2^n a + 2^{n-1}b + \cdots + 4f + 2g + h$	$+2^n a$	$-2^{n-1}b - 2^{n-2}c - \cdots - 4f - 2g - h = \mathcal{M}$
$+1$	$a + b + c + \cdots + f + g + h$	$+a$	$-b - c - \cdots - f - g - h = \mathcal{N}$
0	$+h$	0	$-h = \mathcal{O}$
-1	$\pm a \pm b \pm c \pm \cdots + f - g + h$	$\pm a$	$\mp b \pm c \mp \ldots - f + h - h = \mathcal{P}$
-2	$\pm 2^n a \pm 2^{n-1}b \cdots + 4f - 2g + h$	$\pm 2^n a$	$\mp 2^{n-1}b \pm 2^{n-1}c \mp \cdots - 4f + 2g - h = \mathcal{Q}$

Ensuite Schubert calcule les différences $\Delta^j(ax^n - y)$ et s'aperçoit que la suite des valeurs de $\Delta^{n-2}(ax^n - y)$ est une progression arithmétique de nombres entiers.

La méthode de Bernoulli-Schubert repose sur la propriété suivante :

Soit F un polynôme à coefficients rationnels de degré d plus petit que n. On considère $y_i = F(x_i)$, où $x_1 = x_0 + a, \ldots, x_n = x_0 + na$, avec x_0 et a des entiers. Alors la suite $\Delta^{d-1}(y_0, \ldots, y_n)$ est en progression arithmétique.

Dans leurs mémoires Bernoulli et Schubert supposent implicitement cette propriété. Mais ils connaissaient parfaitement les résultats de Newton. Schubert rappelle au début de son ouvrage les recherches de Newton sur les différences finies ainsi que sur les facteurs de degré un ou deux des polynômes [Newton 1707]. Schubert ne donne aucune référence aux travaux antérieurs de Nicolas Bernoulli. Il ne cherche pas à déterminer le polynôme y mais $x^n - y$, réduisant ainsi le degré d'une unité. Grâce aux tableaux des différences, il évite de considérer les opérations avec des

rationnels qui ne soient pas des entiers, ce qui pourrait arriver si on cherchait les facteurs par interpolation. Ces artifices permettent de minimiser les calculs et élargissent un peu la famille des polynômes pour lesquels sa méthode aboutit à la factorisation.

Poursuivons la lecture du mémoire de Schubert. Dans les §§7–12 (p. 180–185), il considère les valeurs que prend X aux points 0, ± 1, ± 2, $\pm 3, \ldots$ et il regarde les diviseurs de ces valeurs. Il donne des formules pour les possibles diviseurs linéaires, quadratiques, cubiques et biquadratiques. Ensuite il affirme que «*regulam nostram uno exemplo illustrasse sufficiet*» («il suffira d'un exemple pour illustrer notre règle»). Cette façon d'argumenter un résultat était largement utilisée avant le XIX$^{\text{e}}$ siècle. On va voir plus loin que sa méthode est correcte.

Comme exemple il choisit

$$X = x^6 - 2x^5 + 3x^4 - 3x^3 + 3x^2 - 2x + 1$$

et il cherche un facteur de degré quatre, soit

$$y = ax^4 + bx^3 + cx^2 + dx + e.$$

Il considère d'abord les valeurs de X aux points 3, 2, 1, 0, -1, -2 et construit un tableau contenant ces valeurs ainsi que les entiers positifs qui sont des diviseurs de ces valeurs. La colonne de ces diviseurs est appelée *factores speciales* (facteurs spéciaux).

x	X	Factores speciales y
+3	+427	1. 7. (61). 427.
+2	+33	1. 3. (11). 33.
+1	+1	(1).
0	+1	(1).
−1	+15	1. 3. (5). 15.
−2	+217	1. 7. (31). 217.

La signification des diviseurs entre parenthèses va être expliquée un peu plus tard. Schubert choisit $a = 1$ et construit le tableau de différences :

x^4	Residua x^4-y	$\Delta(x^4-y)$	$\Delta^2(x^4-y)$
+81	+80. 74. (+20). etc.		
		+65. +61. (+15).	
+16	+15. +13. (+5). −17		+50. +48. (+10).
		+15. +13. (+5).	
+1	( ).		+14. +12. (+4).
		+1. +1. (+1).	
0	(−1).		+2. 0. (−2).
		−1. +1. (+3).	
+1	0. −2. (−4). −14.		+14. +12. (−8).
		−15. −11. (+11).	
+16	+15. +9. (−15). −201.		

Le tableau précédent est construit selon la règle suivante : chacune des colonnes $\Delta(x^4-y)$ et $\Delta^2(x^4-y)$ est la suite formée par les différences des termes des deux suites successives de la colonne précédente. Choisissant dans la colonne des valeurs de x^4-y les nombres entre parenthèses, on obtient dans les colonnes $\Delta(x^4-y)$ et $\Delta^2(x^4-y)$ les nombres entre parenthèses. La dernière suite, celle de la colonne $\Delta^2(x^4-y)$, est une progression arithmétique de raison 6. Il cherche alors le polynôme x^4-y qui prend les valeurs entre parenthèses dans la colonne des valeurs de x^4-y. Il résout le système d'équations linéaires correspondant et trouve

$$x^4-y=x^3-x^2+x-1$$

donc

$$y=x^4-x^3+x^2-x+1.$$

Ensuite il observe que y est un vrai facteur du polynôme X et obtient l'autre facteur

$$X/y=x^2-x+1,$$

d'où la factorisation de X :

$$x^6-2x^5+3x^4-3x^3+3x^2-2x+1=(x^4-x^3+x^2-x+1)\cdot(x^2-x+1).$$

Analyse de la méthode de Bernoulli-Schubert

Le procédé de Bernoulli-Schubert repose sur l'interpolation des facteurs possibles du polynôme de départ, en utilisant la méthode des différences

finies comme déjà chez Newton et Leibniz. Bernoulli et Schubert ont le mérite de détailler la méthode de Newton, de fournir des explications nouvelles et de rendre ainsi cette méthode plus accessible.

Notons que Schubert [1798, p. 182] affirme que par cette méthode il ne peut pas découvrir des facteurs multiples[8]. Son argumentation repose sur la remarque que d'une égalité $X(d) = 0 \cdot y(d)$, avec d une racine entière de X, on ne peut rien déduire sur la valeur de $y(d)$. Cependant on peut éviter les racines entières du polynôme en choisissant les valeurs pour lesquelles le polynôme ne s'annule pas. Par exemple, si on considère le polynôme

$$X = x^4 - 2x^3 + 2x^2 - 2x + 1$$

on va voir qu'il a des facteurs multiples. Ce polynôme s'annule en 1, mais si on choisit pour nœuds du tableau des différences les points 2, 3, 4, 5 et 6 on trouve par son algorithme les diviseurs $x^2 + 1$ et $x^2 - 2x + 1$, ensuite la factorisation

$$x^4 - 2x^3 + 2x^2 - 2x + 1 = (x - 1)^2(x^2 + 1).$$

Par ailleurs, puisqu'on cherche une factorisation du polynôme, dès qu'on trouve un entier d tel que $X(d) = 0$ on peut diviser le polynôme par le facteur linéaire $x - d$ avant d'appliquer la méthode de Bernoulli-Schubert.

3. L'ALGORITHME DE KRONECKER ET CELUI DE HAUSMANN-KRONECKER

C'est le mathématicien allemand Leopold Kronecker qui est considéré comme le premier inventeur d'un algorithme général de factorisation des polynômes à coefficients entiers. Dans son ouvrage [Kronecker 1882], il étudie la factorisation des polynômes d'une variable à coefficients entiers sur une seule page (p. 10), (voir aussi [Kronecker 1897, p. 256–258]). Kronecker s'était occupé de ce problème auparavant. Par exemple, dans ses leçons non publiées sur les équations algébriques du semestre d'hiver 1880/1881 [Kronecker ms 1880], il présente déjà — et en détail — ce procédé. Il reviendra sur ce sujet dans son cours sur la théorie des nombres [Kronecker 1901, p. 178–181].

[8] « *Facile denique perspicitur, methodo hac factores multiplices reperiri non posse.* »

Il est partisan d'une approche constructive des mathématiques (voir sa remarque sur l'irréductibilité au début de cet article). Kronecker considère la factorisation des polynômes à coefficients entiers dans un contexte général. Son algorithme s'insère dans un grand projet : la présentation dans une même théorie de la théorie algébrique des nombres et de celle des fonctions algébriques d'une variable.

Dans son ouvrage, les polynômes à coefficients entiers jouent un rôle fondamental. La plus grande partie de son travail est dédiée à l'étude des "Gattungen", des quantités algébriques sur des "Rationalitätsbereiche", c'est-à-dire des éléments algébriques sur le corps des fractions d'un anneau de polynômes de plusieurs variables sur les entiers.

Selon Kronecker, pour vérifier qu'un anneau de polynômes est factoriel, il faut donner une méthode de décomposition. Dans son cours, avant de quitter la section sur la factorisation des polynômes, il tient à indiquer un algorithme pour la factorisation des polynômes à plusieurs variables. La transformation qu'il utilise est, du point du vue de la complexité des calculs, assez mauvaise, mais donne quand même une solution effective du problème.

Brièvement le procédé de factorisation de Kronecker est le suivant :

Soit $F(x)$ un polynôme à coefficients entiers de degré $2n$ ou $2n+1$. Pour trouver un diviseur à coefficients entiers il suffit de trouver un diviseur de degré n ou plus petit. Soient des entiers distincts r_0, r_1, r_2, $\ldots$, r_n et soient

$$g_0(x) = \frac{(x-r_1)(x-r_2)\cdots(x-r_n)}{(r_0-r_1)(r_0-r_2)\cdots(r_0-r_n)},$$
$$g_1(x) = \frac{(x-r_0)(x-r_2)\cdots(x-r_n)}{(r_1-r_0)(r_1-r_2)\cdots(r_1-r_n)},$$
$$\cdots\cdots$$

Alors, chaque polynôme à coefficients entiers $f(x)$, dont le degré ne dépasse pas n, est representé par une combinaison linéaire des polynômes $g(x)$, à savoir

$$f(x) = f(r_0)g_0(x) + f(r_1)g_1(x) + \cdots + f(r_n)g_n(x),$$

(ce n'est autre que la formule d'interpolation de Lagrange).

Si $f(x)$ est un diviseur du polynôme donné $F(x)$, alors le coefficient de $g_h(x)$ dans cette représentation doit être un diviseur de l'entier $F(r_h)$,

et donc on doit discuter seulement un nombre fini de systèmes de coefficients afin d'obtenir tous les diviseurs de $F(x)$ ou de démontrer l'irréductibilité de $F(x)$.

On peut noter que L. Kronecker étudie encore plus brièvement[9] l'utilité de sa méthode pour la factorisation des polynômes à plusieurs variables à coefficients entiers. Pour factoriser un polynôme en n variables, notées par x, x', …, $x^{(n)}$, il propose le changement de variables :

$$x' = c_1 x^g, \quad x'' = c_2 x^{g^2}, \ldots, \quad x^{(n)} = c_n x^{g^n}$$

avec c_i des entiers et g un entier positif, ce qui conduit à un polynôme d'une variable à coefficients entiers.

Réduction des calculs par Runge

Par interpolation le polynôme $f(x)$ intervenant dans l'algorithme de Kronecker peut être à coefficients rationnels non entiers. Si on prend, par exemple,

$$F(x) = 7x^4 - 6x^3 + 8x^2 - x + 2,$$

on trouve $F(-1) = 24$, $F(0) = 2$, $F(1) = 10$. Si on suppose $f(-1) = 4$, $f(0) = 1$ et $f(1) = 5$, on obtient

$$f(x) = \tfrac{7}{2}x^2 + \tfrac{1}{2}x + 1$$

qui n'est pas à coefficients entiers.

La méthode de Kronecker suppose le calcul de tous les polynômes d'interpolation $f(x)$, mêmes ceux qui ne sont pas à coefficients entiers. C. Runge [1886] a proposé une méthode qui évite de calculer ces polynômes, ce qui permet de réduire la taille des calculs. Il utilise les mêmes notations que Kronecker. Il remarque que si $f(x)$ est à coefficients entiers, alors $(f(x) - f(r_\alpha))/(x - r_\alpha)$ prend des valeurs entières, donc $f(r_\beta) - f(r_\alpha)$ doit être divisible par $r_\beta - r_\alpha$. Alors, parmi les diviseurs entiers Θ_α de $f(r_\alpha)$, il faut examiner seulement ceux assujettis aux conditions de type

$$\Theta_\alpha \equiv \Theta_\beta \quad \big(\text{mod. } \overline{r_\alpha - r_\beta}\,\big).$$

[9] Une demi-page de Kronecker [1882, p. 11].

Les remarques de Van der Waerden

Dans son célèbre traité d'algèbre, Bartel Van der Waerden [1937] fait, en particulier, deux remarques sur le mémoire de Kronecker. Il affirme qu'il est préférable d'utiliser les différences finies pour l'interpolation plutôt que l'interpolation de Lagrange. C'est le choix de Newton, Leibniz, N. Bernoulli et Schubert, mais pas celui de Kronecker. Par ailleurs, il suggère d'utiliser la décomposition des polynômes modulo un nombre premier pour obtenir des informations sur la factorisation des polynômes sur les entiers ordinaires. On peut considérer que cette remarque anticipe la méthode moderne de Berlekamp-Zassenhaus.

L'approche de Hausmann

Bernard A. Hausmann [1937] a donné une autre amélioration de l'algorithme de Kronecker. Sa méthode permet d'établir, grâce à l'étude d'une liste d'entiers, si le polynôme interpolé correspondant est vraiment un diviseur d'un polynôme f à coefficients entiers. Par ailleurs, il suggère d'utiliser des propriétés des polynômes de Hurwitz[10] ainsi que l'étude des tableaux de différences. Il faut bien observer que Hausmann, de même que Kronecker, semble avoir complètement ignoré les travaux de N. Bernoulli et F.T. Schubert.

Hausmann revient aux différences finies. Il considère un polynôme $f(x)$ de degré n à coefficients entiers qui est *de Hurwitz*. On notera que l'hypothèse de stabilité des polynômes conduit à une méthode plus efficace que celle de Kronecker, mais on se reportera aussi à nos remarques comparatives. Il note qu'un tel polynôme $f(x)$ possède seulement des coefficients strictement positifs et il le suppose factorisé en $f(x) = g_1(x) \cdot g_2(x)$, avec $g_1(x)$ de degré r et $g_2(x)$ de degré s. Il substitue à x les valeurs 1, 2, ..., $n+1$ et obtient les ensembles de valeurs

$$[a_0, \ldots, a_n] = [b_0, \ldots, b_n] \cdot [c_0, \ldots, c_n],$$

où $a_i = f(i+1)$, $b_i = g_1(i+1)$ et $c_i = g_2(i+1)$.

B.A. Hausmann considère alors les tableaux des différences des suites $(a_i)_i$, $(b_i)_i$ et (c_i) et obtient ensuite le résultat suivant :

[10] On dit aussi polynômes stables. Ce sont les polynômes dont toutes les racines sont de partie réelle négative.

THÉORÈME. — *Si* $[a_0, \ldots, a_n] = [b_0, \ldots, b_n] \cdot [c_0, \ldots, c_n]$, *où les* a_i *ont été obtenus à partir d'un certain polynôme* $f(x)$, *du type considéré, par substitution à* x *des* $n+1$ *entiers* $1, 2, \ldots, n+1$, *et où les* b_i *et les* c_i *satisfont les relations*

1) $a_i = b_i c_i$;

2) $b_0 \geq 2$ *et* $b_0 < b_1 < \cdots < b_n$;

3) $c_0 \geq 2$ *et* $c_0 < c_1 < \cdots < c_n$;

alors les b_i *définissent un polynôme* $g_1(x)$ *et les* c_i *définissent un polynôme* $g_2(x)$ *tels que* $f(x) = g_1(x) \cdot g_2(x)$ *si et seulement si les différences d'ordre* r *des* b_i *sont constantes, les différences d'ordre* s *des* c_i *sont constantes et* $r + s = n$.

La méthode de Hausmann traite de la factorisation des polynômes à coefficients entiers qui sont stables, c'est-à-dire dont les parties réelles des racines sont négatives. Bien sûr, comme le signale Hausmann, cette méthode peut aussi être utilisée dans le cas de polynômes qui ne sont pas stables grâce à une translation convenable. En effet, pour un polynôme $f(x)$ quelconque, si M est un nombre positif tel que

$$\big|f(z)\big| \neq 0 \quad \text{pour} \quad |z| \geq M,$$

alors le polynôme $S(x) = f(x - \lfloor M \rfloor - 1)$ est stable.

B.A. Hausmann choisit pour M la borne des racines obtenue par Cauchy [1829] : pour le polynôme $P(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$, la borne supérieure de Cauchy pour les modules des racines est $M = 1 + \max |a_k|/|a_0|$, $(k = 1, 2, \ldots, n)$. On obtient la factorisation de $S(x)$, et ensuite, par translation, celle de $f(x)$. Mais en général les coefficients du polynôme $S(x)$ sont très grands, ce qui rend la méthode inutilisable en pratique pour des polynômes quelconques. En passant, on peut aussi noter que tester si le polynôme $f(x)$ est stable est une tâche lourde dès que le degré n de $f(x)$ atteint cinq.

L'avantage de l'approche de Hausmann est qu'au lieu de calculer les polynômes d'interpolation et vérifier par division si un tel polynôme est un diviseur de $f(x)$, on construit des tableaux de différences des suites b_i et c_i. Si leurs ordres sont r, respectivement s, et si on trouve $r+s = n$, alors on a trouvé une factorisation de $f(x)$. Sinon, on essaie d'autres valeurs. Il n'y a qu'un nombre fini d'essais nécessaires.

4. COMPARAISONS DES DIVERSES MÉTHODES

Au terme de cette analyse on peut noter que le facteur commun entre les méthodes de Bernoulli-Schubert, Kronecker et Hausmann est la recherche des facteurs possibles par l'intermédiaire de la factorisation des valeurs prises par ces polynômes.

• *Premier pas.* — Il est commun à toutes ces méthodes. Il consiste à calculer les valeurs du polynôme à factoriser $F(x)$ pour un certain nombre $e+1$ d'entiers distincts : a_0, a_1, ..., a_e. Ce nombre d'entiers distincts est au plus $n+1$, où n désigne le degré du polynôme.

• *Deuxième pas.* — Partie commune aux trois méthodes : On choisit $b_0, \ldots, b_e$ diviseurs de $a_0, \ldots, a_e$.

a) Bernoulli et Schubert choisissent e égal au degré du polynôme, étudient la tabulation de $(b_0, \ldots, b_n)$ et testent si elle correspond à l'ensemble des valeurs d'un polynôme $f(x)$. Si ce n'est pas le cas l'essai a échoué, sinon on calcule le polynôme g_1 grâce au théorème d'interpolation par différences finies de Newton.

b) Kronecker se contente de prendre pour e le plus grand entier ne dépassant pas la moitié du degré de $F(x)$ et il construit directement $f(x)$ par la méthode d'interpolation de Lagrange.

c) Hausmann, comme Schubert, prend e égal au degré du polynôme et considère simultanément g_1 défini par $g_1(i+1) = b_i$ et g_2 défini par $g_2(i+1) = a_i/b_i$. Il vérifie ensuite si les tabulations de g_1 et g_2 correspondent à celles d'un couple de polynômes et utilise son théorème.

• *Troisième pas.* — Les deux premiers auteurs doivent enfin tester si le polynôme $f(x)$ est effectivement un diviseur de $F(x)$, si ce n'est pas le cas ils essaient une autre décomposition, à condition qu'il en reste encore.

Cela n'a pas beaucoup de sens de comparer les efficacités respectives des trois méthodes, en pratique, aucune n'étant utilisable dès que le degré de F dépasse six. La raison est la suivante : pour chaque valeur a_i de $F(x)$ le nombre de choix des b_i est égal à deux fois le nombre des diviseurs positifs des a_i (sauf pour la méthode de Hausmann), il y a donc un nombre considérable d'essais à effectuer pour n au moins égal à six.

Les méthodes contemporaines diffèrent totalement de celles des pionniers. Elles permettent de factoriser des polynômes dont le degré est de l'ordre de la centaine, alors que, même avec les ordinateurs d'aujourd'hui,

les méthodes de Bernoulli-Schubert, Kronecker et Hausmann ne permettraient pas de factoriser des polynômes de degré vingt.

Dans les méthodes modernes de factorisation on utilise deux étapes :

• On choisit d'abord un nombre premier convenable p et on factorise le polynôme modulo p. Cette factorisation est très rapide et on dispose de plusieurs algorithmes efficaces qui reposent essentiellement sur des remarques d'algèbre linéaire sur les corps finis.

• On raffine la factorisation modulo une puissance d'un nombre premier. Cette technique utilise un lemme célèbre de Kurt Hensel [1918] en analyse p-adique et des majorations sur les coefficients d'un diviseur possible d'un polynôme. Ces dernières majorations peuvent être démontrées grâce à l'algèbre élémentaire sur les nombres complexes [Mignotte, 1974].

Il existe deux méthodes pour achever cette factorisation : la première est due à Zassenhaus [1969] et Berlekamp [1967], l'autre a été inventée par A.K. Lenstra, H.W. Lenstra et L. Lovász [1982].

Remerciements

Nous sommes extrêmement reconnaissants à Norbert Schappacher qui a fait plusieurs remarques très pertinentes sur une première ébauche de rédaction et qui nous a communiqué les références de Kronecker [1880] et [1901].

BIBLIOGRAPHIE

Berlekamp (Elwyn)

[1967] Factoring polynomials over finite fields, *Bell Systems Technology Journal*, 46 (1967), p. 1853–1859.

Bernoulli (Jean I)

[1745] *Virorum Celeberr. Got. Gul. Leibnitii et Johan. Bernoulli Commercium philosophicum et mathematicum*, 2 vol., Lausanne & Genève : Bousquet, 1745.

Bernoulli (Nicolas I)

[1708] Regula generalis inveniendi aequationes, per quas alia quaepiam data, modo reducibilis sit, dividi potest, dans [Leibniz, *Math. Schriften*, III, p. 827–835].

Cantor (Moritz)

[1908] *Vorlesungen über die Geschichte der Mathematik*, Bd. IV, Leipzig : Teubner, 1908.

Cauchy (Augustin-Louis)

[1829] *Exercices de mathématiques*, 4^{e} année, Paris : De Bure Frères, 1829.

Encyclopédie Brockhaus-Efron

Entziklopedicheskii Slovar Brockhaus i Efron, 86 vols, Saint-Pétersbourg, 1890–1907.

Hausmann (Bernard A.)

[1937] A new simplification of Kronecker's method of factorization of polynomials, *American Mathematical Monthly*, 44 (1937), p. 574–576.

Hensel (Kurt)

[1918] Eine neue Theorie der algebraischen Zahlen, *Mathematische Zeitschrift*, 2 (1918), p. 433-452.

Knuth (Donald)

[1969] *The Art of Computer Programming*, vol. 2 : Seminumerical Algorithms, Reading Ma. : Addison-Wesley, 1969.

Kronecker (Leopold)

[ms 1880] Theorie der algebraischen Gleichungen, Wintersemester 1880/1881 (manuscrit L 2262, Bibliothèque UFR Mathématiques & Informatique, Strasbourg).

[1882] Grundzüge einer arithmetischen Theorie der algebraischen Grössen, *Journal für reine und angewandte Mathematik*, 92 (1882), p. 1–122.

[1897] *Leopold Kronecker's Werke*, Bd. II, p. 237–387, Leipzig : B.G. Teubner, 1897.

[1901] *Vorlesungen über allgemeine Arithmetik*, Leipzig : B.G. Teubner, 1901.

Leibniz (Gottfried Wilhelm)

[*Math. Schriften*] *Leibnizens mathematische Schriften*, hrsg. von C.I. Gerhardt, Halle 1850–1863.

Lenstra (Arjen), Lenstra (Hendrik), Lovasz (Làszlò)

[1982] Factoring polynomials with rational coefficients, *Mathematische Annalen*, 261 (1982), p. 515–534.

McNamee (John Michael)

[1993] A bibliography on roots of polynomials, *Journal of Computational and Applied Mathematics*, 47 (1993), p. 391–392 (+ disquette), voir également http ://www.elsevier.com/homepage/sac/cam/mcnamee/index.html.

Mignotte (Maurice)

[1974] An inequality about factors of polynomials, *Mathematics of Computation*, 28 (1974), p. 1153–1157.

Molk (Jules), éd.

[1907] *Encyclopédie des sciences mathématiques pures et appliquées*, t. 1, Paris : Gauthier-Villars, 1907. Réimpression Paris : J. Gabay, 1992.

Newton (Isaac)

[1707] *Arithmetica universalis*, Cambridge, 1707.

[1710] *Universal Arithmetick*, London, 1710. Reprinted in *Mathematical Works*, vol. 2, Johnson Reprint Corp., 1967.

[1761] *Arithmetica universalis*, Amsterdam, 1761.

[1802] *Arithmétique universelle de Newton*, trad. Noël Beaudeux, Paris : Bernard, An X, 1802.

[*Math. Papers*] *The Mathematical Papers of Isaac Newton*, éd. D.T. Whiteside, vol. 5, Cambridge : Cambridge University Press, 1972.

Poggendorff (Johann Christian), éd.

[1863] *Biographisch-literarisches Handwörterbuch zur Geschichte der exacten Wissenschaften*, Leipzig, 1863.

Runge (Carl)

[1886] Ueber die Zerlegung ganzer ganzzahliger Functionen in irreductible Factoren, *J. reine angew. Math.*, 99 (1886), p. 89–97.

SCHUBERT (Friedrich Theodor)
[1798] De Inventione Divisorum, *Nova Acta Academiae Scientiarum Petropolitanae*, 11 (1793), p. 172-182, Saint-Pétersbourg, 1798.
[1810] Demonstratio theorematis algebraici, *Mémoires de l'Académie impériale des sciences de Saint Pétersbourg* , s. 5, 2 (1810), p. 124–129.
VAN DER WAERDEN (Bartel)
[1937] *Moderne Algebra I*, Berlin : Springer Verlag, 1937.
ZASSENHAUS (Hans)
[1969] On Hensel factorization, *Journal of Number Theory*, 1 (1969), p. 291–311 .