NOUVELLES ANNALES DE MATHÉMATIQUES

L. MALEYX

Détermination des diviseurs à coefficients commensurables, d'un degré donné, d'un polynôme entier en x à coefficients commensurables

Nouvelles annales de mathématiques 2e série, tome 14 (1875), p. 97-120

<http://www.numdam.org/item?id=NAM_1875_2_14__97_0>

DÉTERMINATION DES DIVISEURS A COEFFICIENTS COMMENSURABLES, D'UN DEGRÉ DONNÉ, D'UN POLYNOME ENTIER EN x A COEFFICIENTS COMMENSURABLES;

PAR M. L. MALEYX.

I. Deux diviseurs d'un polynôme entier en x qui ne diffèrent que par un coefficient constant, ayant la même composition algébrique, ne sont pas considérés comme distincts.

II. En multipliant un polynôme entier en x, à coefficients commensurables, par un multiple commun des dénominateurs de ses coefficients, et en divisant les coefficients du produit par leur plus grand commun diviseur, on forme un nouveau polynôme à coefficients entiers premiers entre eux; le nouveau polynôme, qui ne diffère du premier que par un coefficient constant, admet les mêmes diviseurs que lui, et conserve la qualité de diviser exactement tous ceux que le premier divisait lui-même.

III. De là résulte que la recherche de tous les diviseurs à coefficients commensurables d'un polynôme entier en x à coefficients commensurables se ramène à celle de tous les diviseurs à coefficients entiers premiers entre eux d'un polynôme entier en x jouissant des mêmes propriétés.

IV. Le produit d'un polynôme entier en x à coefficients entiers premiers entre eux par un polynôme entier dont certains coefficients sont des nombres fractionnaires irréductibles ne peut être un polynôme à coefficients entiers.

Réduisons tous les coefficients du polynôme multiplicateur à leur plus petit dénominateur commun, et soit α l'un des facteurs premiers de ce dénominateur que nous représenterons par $\alpha \times m$; le polynôme multiplicateur est de la forme

$$\frac{\alpha \times P + Q}{\alpha \times m},$$

$\alpha \times P$ étant la somme des numérateurs des termes dont le coefficient est divisible par α, et Q la somme de ceux dont aucun coefficient n'est divisible par α. Mettons de même le multiplicande sous la forme

$$\alpha \times P_1 + Q_1;$$

Q contient au moins un terme différent de zéro, sans quoi $\alpha \times m$ ne serait pas le plus petit dénominateur commun des coefficients du multiplicateur, et Q_1 contient aussi au moins un terme, puisque les coefficients du multiplicande sont premiers entre eux.

Cela posé, effectuons le produit; on trouve

$$\frac{\alpha^2 PP_1 + \alpha P_1 Q + \alpha PQ_1 + QQ_1}{\alpha \times m},$$

et, pour démontrer que tous les coefficients du produit ne sont pas entiers, il suffit de montrer que l'un au moins des coefficients du numérateur n'est pas divisible par le facteur α qui entre au dénominateur.

Or, parmi les termes du produit $Q \times Q_1$, il en existe au moins un qui ne se réduit pas avec les autres et dont le coefficient n'est pas divisible par α, puisqu'il est le produit de deux nombres dont aucun n'est divisible par le nombre premier α. Ce terme ne peut admettre de semblables que parmi ceux des produits $\alpha^2 PP_1$, $\alpha P_1 Q$, αPQ_1, qui sont tous divisibles par α; le coefficient du terme résultant de leur réduction étant la somme de plusieurs nombres divisibles par α et d'un seul qui ne l'est pas ne saurait être divisible par α.

Il en résulte que la division d'un polynôme à coefficients entiers par un polynôme à coefficients entiers premiers entre eux ne peut se faire exactement que tout autant que le quotient est un polynôme à coefficients entiers.

V. Soient

$$F(x) = Ax^m + A_1 x^{m-1} + \ldots + A_m$$

un polynôme entier en x et à coefficients entiers;

$$\varphi(x) = ax^p + bx^{p-1} + \ldots + l$$

un second polynôme entier en x, à coefficients entiers premiers entre eux et diviseur du premier; $\psi(x)$ le quotient dont les coefficients doivent être des nombres entiers d'après le numéro précédent; on aura

$$F(x) = \varphi(x) \times \psi(x).$$

Remplaçons-y x par $\frac{\alpha}{\beta}$, et multiplions les deux membres par β^m; on aura

$$\beta^m F\left(\frac{\alpha}{\beta}\right) = \beta^p \varphi\left(\frac{\alpha}{\beta}\right) \times \beta^{m-p} \psi\left(\frac{\alpha}{\beta}\right)$$

ou

$$\begin{aligned} &A\alpha^m + A_1\alpha^{m-1}\beta + \ldots + A_m\beta^m \\ &\quad = (a\alpha^p + b\alpha^{p-1}\beta + \ldots + l\beta^p)K, \end{aligned}$$

K étant un nombre entier.

D'après cela, $a\alpha^p + b\alpha^{p-1}\beta + \ldots + l\beta^p$ doit être un diviseur arithmétique du nombre

$$A x^m + A\ \alpha^{m-1}\beta + \ldots + A_m\beta^m.$$

Désignons ce diviseur par M, on aura l'équation du premier degré

$$a\alpha^p + b\alpha^{p-1}\beta + \ldots + l\beta^p = M$$

entre les $p+1$ coefficients inconnus $a, b, \ldots, l$ du polynôme cherché.

Si l'on donne à $\frac{\alpha}{\beta}$ $p+1$ valeurs distinctes $\frac{\alpha}{\beta}, \frac{\alpha_1}{\beta_1}, \frac{\alpha_2}{\beta_2}, \ldots, \frac{\alpha_p}{\beta_p}$; si l'on désigne généralement par M_t un diviseur convenablement choisi de $\beta_t^m F\left(\frac{\alpha_t}{\beta_t}\right)$, la résolution du système des $p+1$ équations

$$\begin{array}{l}
a\alpha^p + b\alpha^{p-1}\beta + \ldots + l\beta^p = M,\\
a\alpha_1^p + b\alpha_1^{p-1}\beta_1 + \ldots + l\beta_1^p = M_1,\\
a\alpha_2^p + b\alpha_2^{p-1}\beta_2 + \ldots + l\beta_2^p = M_2,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
a\alpha_p^p + b\alpha_p^{p-1}\beta_p + \ldots + l\beta_p^p = M_p
\end{array}$$

fera connaître les $p+1$ coefficients du diviseur $\varphi(x)$.

VI. Désignons maintenant par m_t le nombre des diviseurs de $\beta_t^m F\left(\frac{\alpha_t}{\beta_t}\right)$. Si l'on donne à M_t successivement les valeurs de tous ces diviseurs dans le système des $p+1$ équations du numéro précédent, on formera un nombre de systèmes analogues égal à

$$m \times m_1 \times m_2 \times \ldots \times m_p.$$

En résolvant chacun de ces systèmes, on déterminera les coefficients d'un nombre égal de polynômes de degré p, parmi lesquels figureront tous les diviseurs de degré p à coefficients entiers premiers entre eux du polynôme $F(x)$.

Mais en même temps qu'on obtiendrait ainsi les coefficients de tous les polynômes cherchés, on obtiendrait aussi ceux d'un nombre considérable de polynômes qui ne conviendraient pas à la question, et qu'il faut chercher à exclure.

VII. On peut exclure tout système de valeurs de M, $M_1, \ldots, M_p$, pour lequel :

1° L'un de ces coefficients désignés d'avance, M par exemple, aurait une valeur négative; en effet, en changeant simultanément les signes de $M, M_1, \ldots, M_p$, on pourrait rendre M positif, et l'on ne ferait ainsi que changer les signes de $a, b, \ldots, l$, ce qui n'altérerait pas le diviseur correspondant;

2° On trouverait des valeurs fractionnaires de a, $b, \ldots, l$;

3° On trouverait des valeurs entières de $a, b, \ldots, l$, admettant un facteur commun;

4° On trouverait des valeurs de $a, b, \ldots, l$, ne rendant pas $\beta^p_{p+1}\varphi\left(\frac{\alpha_{p+1}}{\beta_{p+1}}\right)$ diviseur de $\beta^m_{p+1}F\left(\frac{\alpha_{p+1}}{\beta_{p+1}}\right)$, $\frac{\alpha_{p+1}}{\beta_{p+1}}$ étant distincte des $p+1$ valeurs déjà données à $\frac{\alpha}{\beta}$.

5° On trouverait des valeurs de $a, b, \ldots, l$ ne rendant pas $\varphi(x)$ diviseur de $F(x)$, ce qui arriverait nécessairement si l'on était conduit à mettre un coefficient fractionnaire au quotient.

VIII. Ces différents moyens d'exclusion peuvent se combiner et s'appliquer diversement suivant les valeurs de p, α, β; nous nous bornerons dans ce qui suit à exposer quelques procédés réguliers conduisant au résultat quand p a l'une des valeurs 1, 2, 3, puis à indiquer d'une façon générale comment on pourrait opérer pour les degrés supérieurs.

Diviseurs du premier degré.

IX. Tout diviseur du premier degré d'un polynôme entier en x est de la forme $ax + b$, a étant un diviseur du coefficient A du premier terme du polynôme considéré, b un diviseur de son dernier terme A_m.

Nous supposerons que nous ayons préalablement supprimé dans $F(x)$ les diviseurs $x - 1$ ou $x + 1$ s'ils y étaient contenus.

On peut, d'après ce qu'on a vu n° VII, exclure comme valeurs de a les diviseurs négatifs de A, l'association dans un même binôme d'un diviseur de A et d'un diviseur de A_m admettant un facteur commun.

Un système de valeurs de a et de b ne peut être accepté que tout autant que leur somme, résultat de la substitution de 1 dans le binôme $ax + b$, et que leur différence, résultat de la substitution de -1 dans le même binôme, seront des diviseurs respectifs de $F(1)$ et de $F(-1)$ qui ne sont pas nuls.

On formera tous les binômes ne satisfaisant pas à ces conditions d'exclusion et on les essayera par la division, en prenant soin de l'ordonner de manière que le premier terme du diviseur ait le plus grand coefficient.

Pour faciliter ces opérations, on forme d'abord le tableau des valeurs possibles de $a + b$ qu'on compare à celui des diviseurs de $F(1)$, puis le tableau des valeurs possibles de $a - b$ qu'on compare à celui des diviseurs de $F(-1)$.

Soit, pour exemple, le polynôme

$$F(x) = 15x^4 + 16x^3 - 46x^2 - 5x + 6.$$

I		II		III	IV		V
a	b	$a+b$		$F(1)=-14$	$a-b$		$F(-1)=-36$
15	6	15+2	17	14	15+1	16	36
5	3	15+1	16	7	5−2	3	18
3	2	15−1	14	2	5+3	8	12
1	1	15−2	13	1	5+6	11	9
	−1	5+6	11		3+1	4	6
	−2	5+3	8		3+2	5	4
	−3	5+2	7		1−6	−5	3
	−6	5+1	6		1+2	3	2
		5−1	4		1+3	4	1
		5−2	3				
		5−3	2				
		5−6	−1				
		3+2	5				
		3+1	4				
		3−1	2				
		3−2	1				
		1+6	7				
		1+3	4				
		1+2	3				
		1−2	−1				
		1−3	−2				
		1−6	−5				

On inscrit d'abord dans un premier tableau I les diviseurs positifs de 15 qui sont les valeurs possibles de a, et à côté tous les diviseurs de six valeurs possibles de b.

Dans un deuxième tableau II, on inscrit les sommes de chaque valeur de a avec chaque valeur de b première avec celle de a, et les résultats effectués de ces additions.

En comparant ces résultats avec les diviseurs de F(1) disposés dans un troisième tableau III, on reconnaît qu'on ne peut accepter que neuf associations possibles d'une valeur de a et d'une valeur correspondante de b.

Dans un quatrième tableau IV, on inscrit les neuf valeurs correspondantes de la différence $a - b$, et les résultats effectués de ces soustractions.

La comparaison de ces résultats avec les diviseurs de $F(-1)$ contenus dans un cinquième tableau V permet de réduire à quatre le nombre des associations possibles d'une valeur de a et d'une valeur de b.

Il ne peut donc exister que quatre diviseurs du premier degré du polynôme proposé : ces diviseurs sont

$$5x+2, \quad 3x-1, \quad x-2, \quad x-3;$$

vérifiés par la division, il n'en reste que deux d'acceptables, à savoir : $5x+2$, $3x-1$.

Tel est le procédé à peu près suivi dans toutes les Algèbres pour la détermination des racines commensurables, et qui résout la question proposée.

Diviseurs du second degré.

X. Tout diviseur du second degré d'un polynôme entier $F(x)$ a la forme ax^2+bx+c. D'après le n° V et en désignant par M, M_1, M_2, M_3 des diviseurs convenablement choisis et respectifs de $\beta^m F\left(\frac{\alpha}{\beta}\right)$, $\beta^m F\left(-\frac{\alpha}{\beta}\right)$, $\alpha^m F\left(\frac{\beta}{\alpha}\right)$, $\alpha^m F\left(-\frac{\beta}{\alpha}\right)$, on doit avoir

$$\begin{aligned}
a\alpha^2+b\alpha\beta+c\beta^2&=M,\\
a\alpha^2-b\alpha\beta+c\beta^2&=M_1,\\
a\beta^2+b\alpha\beta+c\alpha^2&=M_2,\\
a\beta^2-b\alpha\beta+c\alpha^2&=M_3.
\end{aligned}$$

Trois de ces équations suffisent pour déterminer a, b, c; la quatrième sera une équation de condition servant de moyen d'exclusion d'après le n° VII. Or, pour qu'un système de valeurs de M, M_1, M_2, M_3 puisse fournir pour a, b, c des valeurs entières satisfaisant aux quatre équations précédentes, il faut que $M+M_3$ soit un multiple de $\alpha^2+\beta^2$; qu'il en soit de même de M_1+M_2; que $M+M_3=M_1+M_2$; que $M-M_1$ soit un multiple de $2\alpha\beta$; qu'enfin $M-M_2$ le soit de $\alpha^2-\beta^2$. Les systèmes de valeurs de M, M_1, M_2, M_3, qui satisferont à ces conditions, seront généralement assez peu nombreux pour qu'on puisse tenter la résolution des systèmes d'équations correspondants.

Pour déterminer les valeurs de M, M_1, M_2 qui satisfont à ces conditions, on formera un tableau composé de neuf colonnes verticales; dans la deuxième, on inscrira l'une au-dessous de l'autre toutes les valeurs possibles de M, c'est-à-dire des diviseurs de $\beta^m F\left(\frac{\alpha}{\beta}\right)$; dans la première et la troisième, on inscrira respectivement, à gauche et à droite de chaque valeur de M, les restes positifs de ses divisions par $\alpha^2-\beta^2$ et par $2\alpha\beta$. De même, on placera dans la cinquième, et les unes au-dessous des autres, les valeurs de M_1, diviseurs de $\beta^m F\left(-\frac{\alpha}{\beta}\right)$, et dans les quatrième et sixième colonnes, à gauche et à droite de chaque valeur de M_1, les restes positifs de ses divisions par $2\alpha\beta$ et par $\alpha^2+\beta^2$. Enfin, dans la huitième colonne, on placera l'une au-dessous de l'autre toutes les valeurs de M_2, diviseurs de $\alpha^m F\left(\frac{\beta}{\alpha}\right)$, et dans les septième et neuvième, à gauche et à droite de chaque valeur de M_2, les restes positifs de ses divisions par $\alpha^2+\beta^2$ et par $\alpha^2-\beta^2$.

Pour qu'un système de valeurs de M, M_1, M_2 soit acceptable, il faut que $M-M_1$ soit multiple de $2\alpha\beta$, c'est-à-dire que les restes des divisions de M et M_1 par $2\alpha\beta$ soient égaux, ce qu'on constate à l'aide des nombres des troisième et quatrième colonnes; que M_1+M_2 soit un multiple de $\alpha^2+\beta^2$, c'est-à-dire que les restes des divisions de M_1 et M_2 par $\alpha^2+\beta^2$ forment une somme égale à $\alpha^2 + \beta^2$, ce que l'on constate à l'aide des nombres contenus dans les sixième et septième colonnes; enfin que $M - M_2$ soit un multiple de $\alpha^2 - \beta^2$, ce qui se voit à l'aide des restes des première et neuvième colonnes.

5	M	12	12	M_1	13	13	M_2	5
4	399	3	9	1089	10	10	816	1
3	133	1	3	363	12	5	408	3
2	57	9	1	121	4	12	272	2
1	21	9	3	99	8	9	204	4
4	19	7	9	33	7	6	136	1
2	7	7	11	11	11	11	102	2
3	3	3	9	9	9	3	68	3
1	1	1	3	3	3	12	51	1
4	— 1	11	1	1	1	9	48	3
2	— 3	9	11	— 1	12	8	34	4
3	— 7	5	9	— 3	10	11	24	4
1	— 19	5	3	— 9	4	4	17	2
4	— 21	3	1	— 11	2	3	16	1
3	— 57	3	3	— 33	6	12	12	2
2	—133	11	9	— 99	5	8	8	3
1	—399	9	11	— 121	9	6	6	1
			9	— 363	1	4	4	4
			3	—1089	3	3	3	3
						2	2	2
						1	1	1

M	M_1	M_2
399	— 9	204
133	121	48
57	9	17
57	— 363	272
57	— 363	12
21	1089	16
21	33	136
21	33	6
21	— 3	16
21	— 363	51
3	99	408
1	— 9	48
1	1	51
— 1	— 121	4
— 3	9	17
— 3	— 363	272
— 3	— 363	12
— 21	— 9	204
— 57	99	408
— 57	— 9	48
—133	11	2
—133	— 121	17
—399	1089	16
—399	33	136
—399	33	6
—399	— 3	16
—399	— 363	51

M	M_1	M_2
133	121	48
21	33	6
3	— 9	48
— 1	—121	4
— 3	9	17
— 3	—363	12
—133	—121	17
—399	—363	51

Pour éclaircir ce qui précède, prenons pour exemple le polynôme considéré dans le n° IX

$$F(x) = 15x^4 + 16x^3 - 46x^2 - 5x + 6.$$

Posons $\alpha = 3$, $\beta = 2$; on a

$$\begin{aligned} 2^4 F(\tfrac{3}{2}) &= 399 = 3 \times 7 \times 19, \\ -\,2^4 F(-\tfrac{3}{2}) &= 1089 = 3^2 \times 11^2, \\ -\,3^4 F(\tfrac{2}{3}) &= 816 = 2^4 \times 3 \times 17, \\ -\,3^4 F(-\tfrac{2}{3}) &= 1044 = 2^2 \times 3^2 \times 29, \end{aligned}$$

$$\alpha^2 - \beta^2 = 5, \quad 2\alpha\beta = 12, \quad \alpha^2 + \beta^2 = 13.$$

Formons le tableau à neuf colonnes dont nous venons de nous occuper, et dans un second tableau à trois colonnes, et placé à droite du premier, nous disposerons par lignes horizontales les systèmes de valeurs de M, M_1, M_2 qui peuvent se correspondre d'après nos vérifications.

Pour un motif donné, il suffit d'inscrire dans le premier tableau les valeurs positives possibles de l'une des trois quantités M, M_1, M_2, soit de M_2.

Le tableau étant constitué, nous prenons l'une des valeurs de M, 399 par exemple. Le reste de sa division par 12 étant 3, les seules valeurs de M_1 qui puissent correspondre sont 363, 99, 3, -9, -33, -1089; le reste de la division de 363 par 13 étant 12, les seules valeurs de M_2 qui puissent lui correspondre sont celles qui, divisées par 13, fournissent pour reste 1, soit 1; mais comme cette valeur de M_2 divisée par 5 donne pour reste 1, tandis que 399 donne le reste différent 4, elle est à rejeter. On reconnaît de même que 399 ne peut s'associer à 99 ni à 3. -9 divisé par 13 donne pour reste 4 et peut s'associer aux valeurs de M_2, qui, divisées par 13, donnent pour reste 9; ces valeurs sont 204, 48; la première seule divisée par 5 donne le même reste que 399, et par conséquent est la seule acceptable. Nous inscrirons donc dans le second tableau comme pouvant se correspondre les valeurs de M, M_1, M_2 respectivement égales à 399, -9, 204. On voit par ce moyen que 399 ne peut s'associer ni à -33 ni à -1089.

En répétant successivement les mêmes opérations pour chacune des valeurs de M, on constitue le tableau complet des valeurs de M, M_1, M_2 qui peuvent être associées en groupes, au nombre de 27, et consignées dans le second tableau.

Le nombre de ces associations peut être diminué en observant que $M_1 + M_2 = M + M_3$; on ne devra donc retenir que les systèmes pour lesquels $M_1 + M_2 - M$ sera un diviseur de $3^4 F\left(-\frac{2}{3}\right)$; il est facile de juger s'il en est ainsi en formant les différentes valeurs de M_1+M_2-M prises dans le second tableau et en les comparant au tableau des diviseurs de $3^4 F\left(-\frac{2}{3}\right)$.

On reconnaît ainsi qu'il n'y en a que huit qui sont acceptables, et on les a placés dans un troisième tableau voisin des deux premiers.

De la résolution des huit systèmes d'équations correspondants on déduit les huit trinômes diviseurs possibles

$$\begin{array}{ll} 15x^2 + x - 2, & x^2 + x - 3, \\ 3x^2 - x, & 15x - 30x + 12, \\ 3x^2 - x - 6, & 19x^2 + x - 11, \\ 5x^2 - 10x + 4, & 57x^2 + 3x - 33. \end{array}$$

On reconnaît qu'on peut rejeter *a priori* le sixième et le huitième comme n'ayant pas leurs coefficients premiers entre eux; le septième, dont le coefficient du premier terme, 19, ne divise pas le coefficient 15 du premier terme de $F(x)$; le deuxième et le quatrième, dont les termes indépendants 0, 4 ne divisent pas le terme indépendant 6 du polynôme $F(x)$. Il ne reste donc à essayer par la division que le premier, le troisième et le cinquième; le premier et le cinquième sont les seuls pour lesquels elle se fasse. Le polynôme proposé n'admet donc que deux diviseurs du second degré à coefficients commensurables premiers entre eux

$$15x^2 + x - 3,$$
$$x^2 + x - 3.$$

XI. On sait qu'une équation algébrique de degré m, à coefficients commensurables, qui admet une racine incommensurable d'une équation du second degré à coefficients commensurables, admet aussi la seconde racine de cette équation; la détermination des diviseurs du second degré à coefficients commensurables d'un polynôme de degré m ayant la même propriété permet de déterminer les racines incommensurables de la forme $a + \sqrt{b}$ d'une équation algébrique à coefficients commensurables.

Diviseurs du troisième degré.

XII. Les diviseurs du troisième degré d'une fonction entière $F(x)$ ont la forme

$$ax^3 + bx^2 + cx + d;$$

et, toujours d'après le n° V, en désignant par M, M_1, M_2, M_3 des diviseurs convenablement choisis et respectifs de

$$\beta^m F\left(\frac{\alpha}{\beta}\right), \quad \beta^m F\left(-\frac{\alpha}{\beta}\right), \quad \alpha^m F\left(\frac{\beta}{\alpha}\right), \quad \alpha^m F\left(-\frac{\beta}{\alpha}\right),$$

on a

$$a\alpha^3 + b\alpha^2\beta + c\alpha\beta^2 + d\beta^3 = M,$$
$$a\alpha^3 - b\alpha^2\beta + c\alpha\beta^2 - d\beta^3 = M_1,$$
$$a\beta^3 + b\alpha\beta^2 + c\alpha^2\beta + d\alpha^3 = M_2,$$
$$a\beta^3 - b\alpha\beta^2 + c\alpha^2\beta - d\alpha^3 = M_3.$$

La résolution de ces quatre équations fera connaître les valeurs inconnues et cherchées de a, b, c, d. Recherchons d'abord, comme dans le n° X, des conditions simples auxquelles soient assujettis M, M_1, M_2, M_3, pour pouvoir se correspondre. Ces conditions se déduisent en général de la propriété que doit avoir un système de valeurs de M, M_1, M_2, M_3, de fournir pour a, b, c, d des valeurs entières.

Multiplions la première de ces quatre équations par $\alpha+\beta$, la deuxième par $\alpha-\beta$, la troisième par $\alpha+\beta$, la quatrième par $\beta-\alpha$; elles deviennent

$$\begin{aligned}
&a\alpha^4+(a+b)\alpha^3\beta+(b+c)\alpha^2\beta^2\\
&\qquad+(c+d)\alpha\beta^3+d\beta^4=M\,(\alpha+\beta),\\
&a\alpha^4-(a+b)\alpha^3\beta+(b+c)\alpha^2\beta^2\\
&\qquad-(c+d)\alpha\beta^3+d\beta^4=M_1(\alpha-\beta),\\
&a\beta^4+(a+b)\alpha\beta^3+(b+c)\alpha^2\beta^2\\
&\qquad+(c+d)\alpha^3\beta+d\alpha^4=M_2(\alpha+\beta),\\
&a\beta^4-(a+b)\alpha\beta^3+(b+c)\alpha^2\beta^2\\
&\qquad-(c+d)\alpha^3\beta+d\alpha^4=M_3(\beta-\alpha).
\end{aligned}$$

Retranchons maintenant la seconde de la première, la troisième de la seconde, la quatrième de la troisième, la première de la quatrième, on a

$$\begin{aligned}
&M\,(\alpha+\beta)-M_1(\alpha-\beta)=2\alpha\beta[\alpha^2(a+b)+\beta^2(c+d)],\\
&M_1(\alpha-\beta)-M_2(\alpha+\beta)\\
&\quad=(\alpha^2+\beta^2)[(a-b)(\alpha^2-\beta^2)-\alpha\beta(a+b+c+d)],\\
&M_2(\alpha+\beta)-M_3(\beta-\alpha)=2\alpha\beta[\beta^2(a+b)+\alpha^2(c+d)],\\
&M_3(\beta-\alpha)-M\,(\alpha+\beta)\\
&\quad=(\alpha^2+\beta^2)[(a-d)(\beta^2-\alpha^2)-\alpha\beta(a+b+c+d)].
\end{aligned}$$

On voit, d'après cela, que, pour qu'un système de valeurs de M, M_1, M_2, M_3 puisse être acceptable, il faut que $M(\alpha + \beta)$ et $M_1(\alpha - \beta)$ divisés par $2\alpha\beta$ donnent le même reste; qu'il en soit de même de $M_1(\alpha - \beta)$ et $M_2(\alpha + \beta)$, divisés par $\alpha^2 + \beta^2$; $M_2(\alpha + \beta)$ et $M_3(\beta - \alpha)$, divisés par $2\alpha\beta$; $M_3(\beta - \alpha)$ et $M(\alpha + \beta)$, divisés par $\alpha^2 + \beta^2$.

On vérifie aussi facilement sur les quatre équations initiales que $M + M_2$ et que $M_1 + M_3$ sont des multiples de $\alpha + \beta$; donc M et $-M_2$, divisés par $\alpha + \beta$, doivent fournir le même reste; il en est de même de M_1 et $-M_3$. Pour faciliter la vérification de ces conditions, on formera un tableau composé de seize colonnes verticales. Dans la seconde, on écrira tous les diviseurs de $\beta^m F\left(\frac{\alpha}{\beta}\right)$ l'un au-dessous de l'autre; cette colonne renferme ainsi les valeurs possibles de M, à gauche de chaque valeur de M, et dans la première colonne on placera le reste de la division de $M(\alpha + \beta)$ par $\alpha^2 + \beta^2$; à droite de chaque valeur de M on placera dans la troisième colonne le reste de sa division par $\alpha + \beta$, et dans la quatrième colonne le reste de la division de $M(\alpha + \beta)$ par $2\alpha\beta$.

La sixième colonne renfermera les valeurs de M_1, chacune précédée dans la cinquième colonne du reste de la division de $M_1(\alpha - \beta)$ par $2\alpha\beta$, et suivie dans la septième du reste de la division de M_1 par $\alpha + \beta$, et dans la huitième du reste de la division de $M_1(\alpha - \beta)$ par $(\alpha^2 + \beta^2)$.

Dans la dixième, on placera les valeurs de M_2; à gauche de chaque valeur de M_2, dans la neuvième colonne, on mettra le reste de la division de $M_2(\alpha + \beta)$ par $\alpha^2 + \beta^2$; à droite dans la onzième, le reste de la division de $-M_2$

par $\alpha + \beta$, et dans la douzième le reste de la division de $M_2(\alpha + \beta)$ par $2\alpha\beta$.

Enfin la quatorzième colonne renfermera les valeurs de M_3 ; à gauche de chacune d'elles, on placera dans la treizième colonne le reste de la division de $M_3(\beta - \alpha)$ par $2\alpha\beta$; à droite dans la quinzième le reste de la division de $-M_3$ par $\alpha + \beta$, et dans la seizième le reste de la division de $M_3(\beta - \alpha)$ par $\alpha^2 + \beta^2$.

Il est toujours entendu, pour un motif donné, qu'on peut n'inscrire dans ce tableau que les valeurs positives de l'une des quatre quantités M, M_1, M_2, M_3.

Par le moyen de ce tableau, on détermine les systèmes de valeurs de M, M_1, M_2, M_3, qui peuvent se correspondre d'après les conditions qu'on vient d'établir, et on les consignera dans un second tableau. Si le nombre de ces systèmes est considérable, on pourra éliminer ceux qui fournissent une valeur de a, qui ne divise pas A, ou une valeur de d qui ne divise pas A_m. Les valeurs de a et de d sont assez simples; on trouve, en ajoutant et retranchant la première et la deuxième des équations considérées, ainsi que la troisième et la quatrième,

$$2a\alpha^3 + 2c\alpha\beta^2 = M + M_1, \quad 2b\alpha^2\beta - 2d\beta^3 = M - M_1,$$

$$2a\beta^3 + 2c\alpha^2\beta = M_2 + M_3, \quad 2b\alpha\beta^2 + 2d\alpha^3 = M_2 - M_3,$$

d'où l'on déduit facilement

$$a = \frac{\alpha(M + M_1) - \beta(M_2 + M_3)}{2(\alpha^4 - \beta^4)},$$

$$d = \frac{\alpha(M_2 - M_3) - \beta(M - M_1)}{2(\alpha^4 - \beta^4)}.$$

Si l'on accepte comme convenable un système de valeurs de M, M_1, M_2, M_3, et qu'on veuille faire le calcul des valeurs correspondantes de a, b, c, d, au lieu de les calculer directement, il peut être plus commode de faire le calcul initial des quantités $a+c$, $a-c$, $b+d$, $b-d$, définies par les formules suivantes, se déduisant facilement de celles qui précèdent :

$$a+c = \frac{1}{2(\alpha^2+\beta^2)}\left(\frac{M+M_1}{\alpha}+\frac{M_2+M_3}{\beta}\right),$$

$$a-c = \frac{1}{2(\alpha^2-\beta^2)}\left(\frac{M-M_1}{\alpha}-\frac{M_2-M_3}{\beta}\right),$$

$$b+d = \frac{1}{2(\alpha^2+\beta^2)}\left(\frac{M-M_1}{\beta}+\frac{M_2-M_3}{\alpha}\right),$$

$$b-d = \frac{1}{2(\alpha^2-\beta^2)}\left(\frac{M-M_1}{\beta}-\frac{M_2-M_3}{\alpha}\right).$$

XIII. Nous allons appliquer ce qui précède à un exemple. Prenons

$$\begin{aligned} F(x) = {} & 18x^7+79x^6-55x^5-310x^4 \\ & +20x^3+307x^2+29x-40. \end{aligned}$$

Posons

$$\alpha = 3, \quad \beta = 2,$$

on a

$$2\alpha\beta = 12, \quad \alpha^2+\beta^2 = 13, \quad \alpha+\beta = 5,$$
$$\alpha-\beta = 1, \quad \beta-\alpha = -1;$$

de plus, on trouve

$$-2^7 F\left(\frac{3}{2}\right) = 2288, \quad -2^7 F\left(-\frac{3}{2}\right) = 2516,$$

$$3^7 F\left(\frac{2}{3}\right) = 133878, \quad 3^7 F\left(-\frac{2}{3}\right) = 50466.$$

Formons sur ces nombres les deux tableaux dont on a donné l'explication générale dans le numéro précédent.

5/13	M	5	5/12	12	M_1	5	13	5/13	M_2	—1/5	5/12	—1/12	M_3	—1/5	—1/13
0	2288	3	4	8	2516	1	7	7	133878	2	6	6	50466	4	0
0	1144	4	8	10	1258	3	10	10	66939	1	3	3	25233	2	0
0	572	2	4	5	629	4	5	11	44626	4	2	2	16822	3	0
0	286	1	2	4	148	3	5	12	22313	2	1	1	8411	4	0
0	208	3	8	2	74	4	9	7	2526	4	6	6	3882	3	5
9	176	1	4	8	68	3	3	10	1263	2	3	3	1941	4	9
0	143	3	7	1	37	2	11	11	842	3	10	2	1294	1	6
0	104	4	4	10	34	4	8	12	421	4	5	1	647	3	3
11	88	3	8	5	17	2	4	4	318	2	6	6	78	2	0
0	52	2	8	4	4	4	4	2	159	1	3	9	39	1	0
12	44	4	4	2	2	2	2	10	106	4	2	10	26	4	0
0	26	1	10	1	1	1	1	5	53	2	1	11	13	2	0
6	22	2	2	11	— 1	4	12	4	6	4	6	6	6	4	7
2	16	1	8	10	— 2	3	11	2	3	2	3	9	3	2	10
0	13	3	5	8	— 4	1	9	10	2	3	10	10	2	3	11
3	11	1	7	7	— 17	3	9	5	1	4	5	11	1	4	12
1	8	3	4	2	— 34	1	5	8	— 1	1	7	1	— 1	1	1
7	4	4	8	11	— 37	3	2	3	— 2	2	2	2	— 2	2	2
10	2	2	10	4	— 68	2	10	11	— 3	3	9	3	— 3	3	3
5	1	1	5	10	— 74	1	4	9	— 6	1	6	6	— 6	1	6
				8	— 148	2	8	8	— 53	3	11	1	— 13	3	0
				7	— 629	1	8	3	— 106	1	10	2	— 26	1	0
				2	—1258	2	3	11	— 159	4	9	3	— 39	4	0
				4	—2516	4	6	9	— 318	3	6	6	— 78	3	0
								1	— 421	1	7	11	— 647	2	10
								2	— 842	2	2	10	— 1294	4	7
								3	— 1263	3	9	9	— 1941	1	4
								6	— 2526	1	6	6	— 3882	2	8
								1	— 22313	3	11	11	— 8411	1	0
								2	— 44626	1	10	10	—16822	2	0
								3	— 66939	4	9	9	—25233	3	0
								6	—133878	3	6	6	—50466	1	0

M	M_1	M_2	M_3
2288	— 68	2	—16822
2288	—2516	—133878	50466
1144	2516	2526	—50466
1144	68	— 66939	—25233
572	148	53	— 13
572	4	318	50466
572	— 68	1263	25233
286	74	— 6	50466
286	2	159	25233
286	2	— 44626	—16822
286	—1258	— 106	—16822
208	68	— 1263	—25233
208	— 4	— 318	—50466
208	— 148	— 53	13
143	— 17	— 318	— 78
143	— 629	— 53	— 8411
104	4	6	50466
52	2516	133878	—50466
52	68	— 2	16822

M	M_1	M_2	M_3
208	— 148	— 53	13
143	— 17	— 318	— 78

a	*b*	*c*	*d*
2	13	— 2	— 7
9	8	—15	— 8

Après avoir formé nos tableaux, prenons dans le premier une des valeurs de M, 2288 par exemple; le reste de la division de son quintuple par 12 étant 4, il ne peut y avoir de valeurs correspondantes de M_1 que celles qui, divisées par 12, donnent pour reste 4, à savoir 148, 4, — 68, — 2516, que nous allons examiner séparément.

148 divisé par 13 donnant pour reste 5, et 2288 divisé par 5 donnant pour reste 3, on ne peut accepter de valeurs correspondantes de M_2 que celles dont le quintuple divisé par 13 donne pour reste 5, et dont le produit par —1 donne le reste 3. Or il n'en existe pas : donc 148 ne peut s'associer à 2288. Passons à 4 qui, divisé par 13, donne le reste 4; les valeurs de M_2 qui peuvent correspondre ont un quintuple qui, divisé par 13, donne pour reste 4, et un produit par —1 qui, divisé par 5, donne

pour reste 3 : on reconnaît, comme pour 148, qu'il n'en existe pas.

— 68 divisé par 13 donne pour reste 10; on ne peut prendre de valeurs correspondantes de M_2 que celles dont le quintuple divisé par 13 donne le reste 10, et dont le produit par — 1, divisé par 5, donne le reste 3. Il n'y a que 2 qui jouisse de cette propriété; le quintuple de 2 divisé par 12 donne le reste 10, — 68 divisé par 5 donne pour reste 2, le quintuple de 2288 divisé par 13 donne pour reste zéro; une valeur de M_3 ne peut s'associer à

$$M = 2288, \quad M_1 = -68, \quad M_2 = 2,$$

que tout autant que son produit par — 1, divisé par 12 donne le reste 10, divisé par 5 donne pour reste 2, divisé par 13 donne pour reste zéro; il n'y a parmi les valeurs de M_3 que — 16822 qui jouisse de cette propriété. On peut donc accepter le système

$$M = 2288, \quad M_1 = -68, \quad M_2 = 2, \quad M_3 = -16822,$$

consigné dans la première ligne horizontale du second tableau. On reconnaît de même que $M_1 = 2288$ peut s'associer à

$$M_1 = -2516, \quad M_2 = -133878, \quad M_3 = 50466,$$

et qu'il ne peut être réuni à aucun autre système de valeurs de M_1, M_2, M_3.

En répétant les mêmes vérifications sur chacune des valeurs de M, on reconnaît qu'on ne peut accepter que dix-neuf systèmes de valeurs de M, M_1, M_2, M_3, systèmes inscrits dans le second tableau. Le nombre de ces systèmes étant encore assez considérable, nous allons calculer la valeur de a, relative à chacun d'eux, d'après une formule connue, et nous ne retiendrons que ceux pour lesquels a sera un diviseur de 18, coefficient du premier terme de $F(x)$.

On trouve ainsi qu'il n'existe que deux systèmes acceptables inscrits dans un troisième tableau, placé au-dessous du second; et dans un quatrième tableau, on a inscrit les valeurs correspondantes de a, b, c, d.

Le premier des systèmes de valeurs de a, b, c, d ne convient pas, parce que la valeur de $d = -7$ ne divise pas -40, terme indépendant de $F(x)$. Le seul diviseur du troisième degré à coefficients entiers premiers entre eux que puisse admettre $F(x)$ est donc

$$9x^3 + 8x^2 - 15x - 8.$$

Effectuant la division, elle réussit, et l'on trouve pour quotient

$$2x^4 + 7x^3 - 9x^2 - 13x + 5.$$

XIV. On peut, par des moyens analogues, déterminer les diviseurs à coefficients commensurables premiers entre eux de tous les degrés d'un polynôme donné; seulement la longueur des opérations croît avec le degré, c'est-à-dire avec le nombre des coefficients à déterminer dans le diviseur. On a vu, dans les trois cas examinés, que généralement la question se résume à déterminer les associations possibles des diviseurs désignés par M, $M_1, \ldots, M_p$ dans le n° V, et à rejeter les autres; et qu'on y est parvenu par un moyen qui permet de voir facilement si deux quelconques de ces diviseurs peuvent faire partie d'un même groupe. Or on peut toujours trouver un tel moyen de la manière suivante; considérons les deux égalités

$$\begin{aligned} a\alpha_g^p + b\alpha_g^{p-1}\beta_g + \ldots + l\beta_g^p &= M_g, \\ a\alpha_k^p + b\alpha_k^{p-1}\beta_k + \ldots + l\beta_k^p &= M_k; \end{aligned}$$

multiplions la première par β_k^p, la seconde par β_g^p, et retranchons-les, on a

$$a\left(\alpha_g^p \beta_k^p - \alpha_k^p \beta_g^p\right) + b\beta_k\beta_g\left(\alpha_g^{p-1}\beta_k^{p-1} - \alpha_k^{p-1}\beta_g^{p-1}\right)$$
$$+ c\beta_k^2\beta_g^2\left(\alpha_g^{p-2}\beta_k^{p-2} - \alpha_g^{p-2}\beta_g^{p-2}\right) + \ldots = \mathrm{M}_g\beta_k^p - \mathrm{M}_k\beta_g^p.$$

On en conclut que $\mathrm{M}_g\beta_k^p - \mathrm{M}_k\beta_g^p$ est divisible par $\alpha_g\beta_k - \alpha_k\beta_g$; en conséquence, les restes des divisions de $\mathrm{M}_g\beta_k^p$ et de $\mathrm{M}_k\beta_g^p$ par $\alpha_g\beta_k - \alpha_k\beta_g$ doivent être égaux; de là une vérification permettant de reconnaître, au moyen d'un tableau analogue à ceux dont nous nous sommes déjà servis, si les diviseurs M_g, M_k peuvent être associés.

XV. On établit en Algèbre qu'une équation à coefficients commensurables, dont le degré ne surpasse pas cinq et qui n'a pas de racines commensurables, ne peut avoir de racines multiples, à moins qu'elle ne soit du quatrième degré et que son premier membre ne soit un carré parfait. En d'autres termes, si un polynôme à coefficients commensurables, dont le degré ne surpasse pas cinq, n'admet aucun facteur du premier degré à coefficients commensurables, il n'est divisible par aucun facteur à coefficients commensurables élevé à une puissance supérieure à la première, à moins qu'il ne soit du quatrième degré et carré parfait.

De même, si un polynôme à coefficients commensurables, dont le degré ne surpasse pas huit, n'admet pas de facteurs du premier ou du second degré à coefficients commensurables, il n'est divisible par aucun facteur à coefficients commensurables élevé à une puissance supérieure à la première, à moins qu'il ne soit du sixième ou du huitième degré, et dans ces deux cas carré parfait, c'est-à-dire que l'équation formée en égalant ce polynôme à zéro ne peut avoir de racines égales à moins que son premier membre ne soit un carré.

En effet, dans les hypothèses faites, le facteur multiple qui pourrait entrer dans le polynôme considéré serait au moins du troisième degré et devrait entrer dans le polynôme au moins deux fois, ce qui exigerait que ce polynôme fût au moins du sixième degré; dans ce cas, le polynôme serait un carré. Si le polynôme était du septième ou du huitième degré, et divisible par le carré d'un facteur du troisième à coefficients commensurables, le quotient serait aussi un diviseur du premier ou du second degré à coefficients commensurables, ce qui est contraire à l'hypothèse; si le facteur multiple était du quatrième degré, le polynôme proposé, dont le degré ne surpasse pas huit, serait le carré de ce facteur multiple. On voit, par un raisonnement analogue, qu'un polynôme à coefficients commensurables dont le degré ne surpasse pas onze, n'admettant pas de diviseur à coefficients commensurables des degrés un, deux, trois, ne peut admettre de facteur multiple, à moins qu'il ne soit des degrés huit ou dix et dans les deux cas carré parfait.

XVI. Il est facile d'appliquer ce qui a été dit dans les numéros de I à XIV à la recherche des communs diviseurs d'un degré donné, de deux ou plusieurs polynômes à coefficients commensurables. Cette recherche serait même simplifiée, car, si l'on désigne par $F(x)$, $F_1(x)$,... ces différents polynômes, on ne devrait accepter pour M que les valeurs des diviseurs communs de

$$\beta^m F\left(\frac{\alpha}{\beta}\right), \quad \beta^{m'} F_1\left(\frac{\alpha}{\beta}\right), \ldots.$$

XVII. La recherche des facteurs multiples, d'un degré donné, d'un polynôme à coefficients commensurables, peut encore se déduire de ce qui précède par une modification encore plus restrictive; en effet, si l'on suppose que le polynôme cherché doive entrer à la puissance p dans le polynôme $F(x)$, on ne devra accepter pour M qu'un diviseur commun des nombres

$$\beta^m F\left(\frac{\alpha}{\beta}\right), \quad \beta^{m-1} F'\left(\frac{\alpha}{\beta}\right), \ldots, \quad \beta^{m-p+1} F^{p-1}\left(\frac{\alpha}{\beta}\right);$$

le diviseur devant entrer p fois dans le premier, $(p-1)$ fois dans le second,..., une fois dans le dernier.

En usant convenablement de ces principes, on peut arriver plus facilement à la détermination des facteurs multiples, des degrés différents, qui peuvent entrer dans un polynôme à coefficients commensurables, que par le procédé du plus grand commun diviseur algébrique.