NOUVELLES ANNALES DE MATHÉMATIQUES

E. POMEY

Sur le plus grand commun diviseur de deux polynômes entiers

Nouvelles annales de mathématiques 3^e série, tome 7 (1888), p. 66-90

<http://www.numdam.org/item?id=NAM_1888_3_7__66_0>

SUR LE PLUS GRAND COMMUN DIVISEUR DE DEUX POLYNOMES ENTIERS;

PAR M. E. POMEY.

Je me propose, dans cette Note, de chercher, à l'égard de deux polynômes entiers,

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m,$$
$$g = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n,$$

1° les conditions nécessaires et suffisantes pour que f et g aient comme plus grand commun diviseur un polynôme de degré p; 2° l'expression explicite de ce polynôme; 3° les quotients respectifs de f et g, divisés par ce polynôme.

L'étude de ces questions peut être rattachée, soit au résultant d'Euler, soit à celui de Bezout-Cauchy : nous diviserons cette Note en deux parties se rapportant respectivement à ces deux points de vue. Nous aurons d'ailleurs recours, dans l'une et dans l'autre partie, à un théorème fondamental bien connu, mais dont nous rappellerons la démonstration.

THÉORÈME FONDAMENTAL. — *Lorsqu'il existe deux polynômes entiers u et v, respectivement de degrés $n - p$ et $m - p$, satisfaisant à l'identité*

$$uf + vg = 0, \tag{1}$$

f et g ont un diviseur commun de degré au moins égal à p.

En effet, désignons par d le plus grand commun diviseur de u et v, ce polynôme d pouvant se réduire à

une constante, et par u_1 et v_1 les quotients de u et v divisés par d. L'identité (1) peut s'écrire alors

$$d(u_1 f + v_1 g) = 0,$$

ou, puisque d n'est pas identiquement nul,

$$u_1 f + v_1 g = 0. \tag{2}$$

D'après cette identité, u_1 divise $v_1 g$; mais u_1 est premier avec v_1, d'après un théorème connu ; donc il divise g, et l'on a

$$g = u_1 \mathrm{P}, \tag{3}$$

P désignant un polynôme entier. Il en résulte, par l'identité (2),

$$f = -v_1 \mathrm{P}. \tag{4}$$

Or, f et g sont respectivement de degrés m et n; u_1 et v_1 sont au plus des degrés $n-p$ et $m-p$. Donc, d'après (3) et (4), f et g ont un diviseur commun P de degré au moins égal à p.

Première Partie.

Définitions. — Désignons par R_0 le déterminant d'ordre $m+n$ formé par les coefficients de x^0, x^1, x^2, ..., x^{m+n-1} dans les polynômes suivants :

$$\begin{array}{llll} x^{n-1}f, & x^{n-2}f, & \ldots, & x^1 f, \quad x_0 f, \\ x^0 g, & x^1 g, & \ldots, & x^{m-2} g, \quad x^{m-1} g. \end{array}$$

On a ainsi, en supposant des zéros à toutes les places laissées vides en dehors des deux parallélogrammes re-

couverts par les coefficients a et b,

$$R_0 = \left|\begin{array}{ccccccccc}
 & & & a_0 & a_1 & a_2 & \cdots & \cdots & a_m \\
 & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
 & a_0 & a_1 & a_2 & \cdots & \cdots & a_m & & \\
a_0 & a_1 & a_2 & \cdots & \cdots & a_m & & & \\
b_0 & b_1 & b_2 & \cdots & b_n & & & & \\
 & b_0 & b_1 & b_2 & \cdots & b_n & & & \\
 & & \cdots & \cdots & \cdots & \cdots & \cdots & & \\
 & & & \cdots & \cdots & \cdots & \cdots & \cdots & \\
 & & & & b_0 & b_1 & b_2 & \cdots & b_n
\end{array}\right| \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} n \text{ lignes.} \\ \left.\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right\} m \text{ lignes.} \end{array}$$

R_0 est le déterminant d'Euler, dans lequel on a seulement renversé l'ordre des n premières lignes.

Nous supposons $m \geq n$.

Soit p un nombre entier inférieur ou au plus égal à n. Supprimons dans R_0 les p premières et les p dernières lignes : alors les p dernières colonnes ne contiennent plus que des zéros; en les supprimant également, il reste un tableau rectangulaire que je désigne par T_p.

Si l'on supprime les p premières colonnes de ce tableau T_p, il reste un tableau carré, dont j'appelle R_p le déterminant des éléments. On voit en somme que R_p se déduit de R_0 en y supprimant les p premières et les p dernières lignes, ainsi que les p premières et les p dernières colonnes.

Soit i l'un des nombres entiers $1, 2, \ldots, p$. J'appelle $R_{p,i}$ le déterminant déduit de R_p en y remplaçant la première colonne par la colonne qui, dans le tableau T_p, occupe le rang i.

Je désigne par D_p le déterminant obtenu au moyen de R_p, en ajoutant à sa première colonne multipliée par x^p les p premières colonnes du tableau T_p, respectivement multipliées par $x^0, x^1, x^2, \ldots, x^{p-1}$.

J'appelle enfin U_{n-p-1} et V_{m-p-1} les deux détermi-

nants obtenus en remplaçant successivement la première colonne de R_p par celles-ci

$$\begin{array}{ll} x^{n-p-1} & 0 \\ \cdot & \cdot \\ x^1 & 0 \\ x^0 & 0 \\ 0 & x^0 \\ 0 & x^1 \\ \cdot & \cdot \\ 0 & x^{m-p-1}. \end{array}$$

($n-p$ zéros ; $m-p$ zéros)

Ces définitions étant posées, nous allons établir plusieurs lemmes importants.

LEMME I. — *L'expression développée du polynôme* D_p *est*

$$D_p \equiv R_{p,1}x^0 + R_{p,2}x^1 + \ldots + R_{p,p}x^{p-1} + R_p x^p.$$

En effet, d'après sa définition, D_p est la somme de $p+1$ déterminants qui se déduisent de R_p en y remplaçant successivement la première colonne par les $p+1$ premières colonnes de T_p, respectivement multipliées par x^0, x^1, x^2, ..., x^p. Or ces déterminants sont précisément ceux qu'on a désignés plus haut par $R_{p,i}(i=1, 2, 3, \ldots, p)$ et R_p, et qu'on a multipliés respectivement par x^0, x^1, x^2, ..., x^p, ce qui démontre le lemme.

LEMME II. — *On a identiquement*

$$D_p \equiv U_{n-p-1}f + V_{m-p-1}g.$$

En effet, D_p ne change pas si l'on ajoute à sa première colonne les suivantes respectivement multipliées par x^{p+1}, x^{p+2}, ..., x^{m+n-1}. Les éléments de sa pre-

mière colonne deviennent ainsi

$$x^{n-p-1}f, \quad \ldots, \quad x^1 f, \quad x^0 f, \quad x^0 g, \quad x^1 g, \quad \ldots, \quad x^{m-p-1} g.$$

Cette colonne peut s'écrire sous la forme suivante :

$$\begin{aligned}
&x^{n-p-1}f + 0.g,\\
&\ldots\ldots\ldots,\\
&x^1 f + 0.g,\\
&x^0 f + 0.g,\\
&0.f + x^0 g,\\
&0.f + x^1 g,\\
&\ldots\ldots\ldots,\\
&0.f + x^{m-p-1} g.
\end{aligned}$$

On voit alors que D_p est la somme des deux déterminants obtenus en remplaçant la première colonne de R_p successivement par les premiers, puis par les seconds termes des éléments binômes qu'on vient d'écrire. Ces déterminants contiennent en facteur, l'un f, l'autre g, et l'on voit que les multiplicateurs de f et g sont les déterminants désignés par la notation U_{n-p-1}, V_{m-p-1}, ce qui démontre l'identité annoncée.

Lemme III. — *Lorsque p est inférieur à n, les polynômes U_{n-p-1}, V_{m-p-1}, ordonnés par rapport aux puissances décroissantes de x, ont respectivement pour premiers termes $b_n R_{p+1} x^{n-p-1}$, $-a_m R_{p+1} x^{m-p-1}$. Lorsque p est égal à n, le premier de ces polynômes est identiquement nul, le second se réduit à $(b_n)^{m-n-1}$, en sorte qu'on a $U_{-1} \equiv 0$ et $V_{m-n-1} = (b_n)^{m-n-1}$.*

En effet, supposons d'abord $p < n$. En développant U_{n-p-1} par rapport aux éléments de sa première colonne, on obtient un polynôme entier en x, ordonné par rapport aux puissances décroissantes, dont le premier terme est de degré $n - p - 1$. Le coefficient de

ce terme est le déterminant qu'on déduit de R_p par la suppression de sa première ligne et de sa première colonne. Or la dernière colonne de R_p a évidemment pour premier élément a_m ; les éléments suivants sont des zéros, sauf le dernier qui est b_n. Par conséquent, en supprimant la première ligne de R_p, l'élément a_m, qui figurait en tête de la dernière colonne, se trouve supprimé, et la dernière colonne du déterminant obtenu par la suppression de la première ligne et de la première colonne de R_p, se compose d'eléments nuls, sauf le dernier qui est b_n; d'ailleurs, si l'on supprimait encore cette colonne, ainsi que la dernière ligne, le déterminant restant serait R_{p+1}. Le coefficient de x^{n-p-1} est donc un déterminant qui, développé par rapport aux éléments de la dernière colonne, se réduit à $b_n R_{p+1}$.

De même, en développant V_{m-p-1} par rapport aux éléments de sa première colonne, on obtient un polynôme entier en x, de degré $m-p-1$; dans ce développement, c'est le terme relatif au dernier élément de la première colonne qui a le plus haut degré. Or cet élément, x^{m-n-1}, occupe le $(m+n-2p)^{\text{ième}}$ rang dans la première colonne. Le terme qu'il fournit est donc $(-1)^{m+n-2p+1} x^{m-n-1} \delta$, en désignant par δ le déterminant déduit de R_p par suppression de sa première colonne et de sa dernière ligne. Mais la dernière colonne de R_p ayant pour premier élément a_m et pour dernier élément b_n, tandis que tous les autres sont nuls, on voit que la dernière colonne de δ a pour premier élément a_m et que tous les autres éléments de cette colonne sont nuls; d'ailleurs cet élément a_m occupe dans la première ligne le $(m+n-2p-1)^{\text{ième}}$ rang; enfin le déterminant obtenu en supprimant dans δ la première ligne et la dernière colonne est R_{p+1}; par suite, on a $\delta = (-1)^{m+n-2p} a_m R_{p+1}$, en sorte que, fina-

lement, le terme du plus haut degré dans V_{m-p-1} est

$$(-1)^{2(m+n-2p)+1} a_m R_{p+1} x^{m-p-1}. \quad \text{ou} \quad -a_m R_{p+1} x^{m-p-1}.$$

Supposons maintenant $p = n$. D'après la définition de U_{n-p-1}, la première colonne de ce déterminant, pour $p = n$, n'a que des éléments nuls, au nombre de $m - n$. Par suite, le polynôme U_{-1} est identiquement nul.

Quant à V_{m-p-1}, sa première colonne, dans l'hypothèse $p = n$, a pour éléments $x^0, x^1, x^2, \ldots, x^{m-n-1}$. Or R_n est le déterminant d'ordre $m - n$ suivant

$$R_n = \begin{vmatrix} b_n & & \\ b_{n+1} & b_n & \\ \cdots & \cdots & \\ \cdots\cdots & & b_n \end{vmatrix} \quad (m - n \text{ lignes}),$$

tous les éléments placés au-dessus de la diagonale principale étant nuls. V_{m-n-1}, par définition, se déduit de R_n en remplaçant sa première colonne par les éléments qu'on vient de citer; c'est donc le déterminant d'ordre $m - n$ suivant :

$$V_{m-n-1} = \begin{vmatrix} x^0 & & \\ x^1 & b_n & \\ \cdots & \cdots & \cdots \\ x^{m-n-1} & \cdots & b_n \end{vmatrix} = x^0 (b_n)^{m-n-1} = (b_n)^{m-n-1}.$$

Lemme IV. — *Lorsque f et g ont pour plus grand commun diviseur un polynôme de degré p, le déterminant R_p est différent de zéro.*

Dans le cas où p est égal à n, on a immédiatement $R_p \equiv R_n = (b_n)^{m-n}$: ce déterminant est donc différent de zéro.

Supposons maintenant p inférieur à n.

Je vais démontrer que, dans ce cas, si R_p est nul, le

plus grand commun diviseur θ de f et g n'est pas de degré p, ou, ce qui revient évidemment au même, que dans l'hypothèse $R_p = 0$, si θ n'est pas de degré inférieur à p, il est nécessairement de degré supérieur à ce nombre.

Supposons, en effet, R_p nul. D'après la définition de ce déterminant, on a

$$R_p = \begin{vmatrix} a_{2p-n+1} & a_{2p-n+2} & \dots & \dots & \dots & \dots & \dots & a_m \\ \dots\dots & \dots\dots & \dots & \dots & \dots & \dots & \dots & \\ a_{p-1} & a_p & \dots & \dots & \dots & a_m & & \\ a_p & a_{p+1} & \dots & \dots & a_m & & & \\ b_p & b_{p+1} & \dots & b_n & & & & \\ b_{p-1} & b_p & \dots & \dots & b_n & & & \\ \dots\dots & \dots & \dots & \dots & \dots & \dots & & \\ \dots\dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ b_{2p-m+1} & b_{2p-m+2} & \dots & \dots & \dots & \dots & \dots & b_n \end{vmatrix},$$

formule valable pour toute valeur de p, en faisant la convention que tous les éléments a ou b affectés d'un indice négatif ne sont pas autre chose que des zéros.

Multiplions la première colonne de R_p par x^p, et ajoutons à cette colonne les suivantes multipliées respectivement par x^{p+1}, x^{p+2}, ..., $x^{m+n-p-1}$. On obtient de la sorte un nouveau déterminant R qui est égal à $R_p x^p$; par conséquent R est nul, et il y a entre les éléments de chaque colonne de R une même relation linéaire et homogène, dans laquelle les coefficients ne sont pas tous nuls : nous allons écrire cette relation, en particulier, à l'égard des éléments de la première colonne.

D'après la façon dont on déduit R de R_p, on voit qu'un élément quelconque $a_{p-\lambda}$ pris parmi les $n-p$ premiers éléments de la première colonne de R_p et un élément quelconque $b_{p\,\mu}$ pris parmi les $m-p$ der-

niers de cette colonne sont respectivement remplacés dans R par les éléments polynômes suivants :

$$A_\lambda = a_{p-\lambda}x^p + a_{p-\lambda+1}x^{p+1} + \ldots + a_m x^{m+\lambda},$$
$$B_\mu = b_{p-\mu}x^p + b_{p-\mu+1}x^{p+1} + \ldots + b_n y^{m+\mu}.$$

Cela posé, si l'on désigne par i un entier inférieur à p, on a

$$A_i = x^i(a_{p-i}x^{p-i} + \ldots + a_m x^m)$$
$$= x^i f - x^i(a_0 + a_1 x + \ldots + a_{p-i-1}x^{p-i-1}),$$

ou, en désignant par $A_{p-1,i}$ un polynôme de degré $p-1$ au plus,

$$A_i = x^i f - A_{p-1,i}. \qquad (1)$$

D'autre part, si j désigne un entier égal ou supérieur à p, on a

$$A_j = x^j(a_{p-j}x^{p-j} + \ldots + a_m x^m)$$
$$= x^j(a_0 + a_1 x + \ldots + a_m x^m),$$

puisque les a affectés d'indices négatifs sont nuls, et, par suite,

$$A_j = x^j f. \qquad (2)$$

D'après les formules (1) et (2), on peut donc poser, d'une façon générale, que λ soit inférieur, égal ou supérieur à p,

$$A_\lambda = x^\lambda f - A_{p-1,\lambda}, \qquad (3)$$

en appelant $A_{p-1,\lambda}$ un polynôme de degré $p-1$ au plus, qui peut être identiquement nul.

On démontre exactement de même qu'on a

$$B_\mu = x^\mu g - B_{p-1,\mu}, \qquad (4)$$

où $B_{p-1,\mu}$ désigne un polynôme qui, s'il n'est pas identiquement nul, est au plus de degré $p-1$.

Il résulte alors des formules (3) et (4) que la rela-

tion identique qui existe entre les éléments de la première colonne de R peut s'écrire

$$\sum_{\lambda=0}^{\lambda=n-p-1} \alpha_\lambda (x^\lambda f - A_{p-1,\lambda}) + \sum_{\mu=0}^{\mu=m-p-1} \beta_\mu (x^\mu g - B_{p-1,\mu}) = 0,$$

ou bien

$$(5) \quad \left\{ \begin{array}{l} f \sum_{\lambda=0}^{\lambda=n-p-1} \alpha_\lambda x^\lambda + g \sum_{\mu=0}^{\mu=m-p-1} \beta_\mu x^\mu \\ \qquad = - \sum_{\lambda=0}^{\lambda=n-p-1} \alpha_\lambda A_{p-1,\lambda} + \sum_{\mu=0}^{\mu=m-p-1} \beta_\mu B_{p-1,\mu}, \end{array} \right.$$

les diverses valeurs des coefficients α_λ et β_μ n'étant pas toutes nulles.

Supposons alors que le plus grand commun diviseur θ de f et g ne soit pas de degré inférieur à p; θ est donc de degré supérieur à $p-1$. Or il divise le premier membre de l'identité (5), comme diviseur commun à f et g; par suite, il divise le second membre; mais celui-ci est de degré $p-1$ au plus, puisque les divers polynômes $A_{p-1,\lambda}$, $B_{p-1,\mu}$ sont au plus de degré $p-1$, quand ils ne sont pas identiquement nuls; donc, θ étant de degré supérieur à $p-1$, le second membre de (5) est identiquement nul. Alors cette identité se réduit à

$$(6) \qquad f \sum_{\lambda=0}^{\lambda=n-p-1} \alpha_\lambda x^\lambda + g \sum_{\mu=0}^{\mu=m-p-1} \beta_\mu x^\mu \equiv 0.$$

Observons que, l'entier p étant, dans l'hypothèse actuelle, au plus égal à l'entier non négatif $n-1$, aucune des diverses valeurs que prennent λ et μ dans (6) n'est négative, et que, par conséquent, les coefficients de f et g dans cette identité sont des polynômes entiers en x. D'ailleurs ces polynômes ne sont ni l'un ni l'autre

identiquement nuls : en effet, l'évanouissement de l'un d'eux entraînerait, en vertu de l'identité (6) elle-même, l'évanouissement de l'autre, puisque ni f ni g n'est identiquement nul; mais alors toutes les valeurs des coefficients α_λ, β_μ seraient nulles, contrairement à ce qu'on a établi plus haut.

En résumé, l'existence de l'identité (6), dans les conditions que nous venons de préciser, prouve qu'il y a deux polynômes entiers u, v non évanouissants, dont les degrés respectifs sont au plus égaux à $n-p-1$ et $m-p-1$, qui satisfont à l'identité $uf+vg\equiv 0$. Par conséquent, d'après le théorème fondamental démontré au début de cette Note, θ est au moins de degré $p+1$, c'est-à-dire de degré supérieur à p.

Il est donc prouvé par ce qui précède que, lorsque R_p est nul, si θ n'est pas de degré inférieur à p, il est de degré supérieur. L'existence d'un plus grand commun diviseur de degré p est donc incompatible avec la condition $R_p=0$: elle exige qu'on ait $R_p\gtrless 0$.

Ces lemmes préliminaires vont nous permettre de démontrer très simplement quatre théorèmes, dont les deux premiers fournissent chacun individuellement, sous des formes différentes, les conditions nécessaires et suffisantes pour que le plus grand commun diviseur θ de f et g soit de degré p, le troisième donne explicitement l'expression de ce polynôme θ, enfin le dernier donne les quotients de f et g divisés par θ.

Théorème I. — *Pour que le plus grand commun diviseur θ de f et g soit de degré p, il faut et il suffit que l'on ait*

$$R_{p-1,1}=R_{p-1,2}=\ldots=R_{p-1,p-1}=R_{p-1}=0 \qquad \text{et} \qquad R_p\gtrless 0.$$

En effet, supposons que θ soit de degré p. Le

lemme IV montre déjà qu'on a $R_p \gtrless 0$. D'autre part, changeons p en $p-1$ dans les identités du lemme I et du lemme II, celles-ci deviennent

$$(1) \qquad \begin{cases} D_{p-1} & R_{p-1,1}x^0 + R_{p-1,2}x^1 + \dots \\ & + R_{p-1,p-1}x^{p-2} + R_{p-1}x^{p-1}, \end{cases}$$

$$(2) \qquad D_{p-1} = U_{n-p}f + V_{m-p}g.$$

En vertu de l'identité (2), θ qui divise f et g divise aussi D_{p-1}, ce qui exige que ce dernier polynôme soit identiquement nul, puisqu'il est de degré $p-1$ au plus, tandis que θ est de degré p. Mais alors, d'après (1), on a

$$R_{p-1} = R_{p-1,2} = \dots = R_{p-1,p-1} = R_{p-1} = 0.$$

Les conditions énoncées sont donc nécessaires.

Réciproquement, supposons ces conditions remplies. D'après (1), D_{p-1} est identiquement nul, et, par suite, d'après (2), on a

$$(3) \qquad U_{n-p}f + V_{m-p}g = 0.$$

Or, d'après le lemme III, les termes de degrés $n-p$ et $m-p$ dans U_{n-p} et V_{m-p} ont pour coefficients respectifs $b_n R_p$, $-a_m R_p$. Mais a_m et b_n sont essentiellement différents de zéro, d'autre part R_p est aussi différent de zéro, puisqu'on suppose remplies les conditions indiquées par l'énoncé; donc U_{n-p} et V_{m-p} sont exactement des degrés marqués par leurs indices. Alors, en vertu du théorème fondamental établi au début et de l'identité (3), le degré de θ est au moins p. D'ailleurs, à cause de l'identité du lemme II, θ divise D_p, qui n'est que de degré p au plus; le degré de θ ne peut donc être supérieur à p, à moins que D_p soit identiquement nul, ce qui exige, d'après le lemme I, qu'on ait en particulier $R_p = 0$, résultat contraire à l'une des conditions qu'on suppose remplies. Par conséquent, θ est exacte-

ment de degré p, et les conditions énoncées sont suffisantes.

THÉORÈME II. — *Pour que f et g aient un plus grand commun diviseur θ de degré p, il faut et il suffit que l'on ait*

$$R_0 = R_1 = R_2 = \ldots = R_{p-1} = 0 \qquad \text{et} \qquad R_p \lesseqgtr 0.$$

En effet, soit p le degré de θ. Chacun des polynômes $D_0, D_1, D_2, \ldots, D_{p-1}$ est divisible par θ, d'après les identités qu'on déduit de celle du lemme II en remplaçant p successivement par $0, 1, 2, \ldots, p-1$; tous ces polynômes sont de degré inférieur à p : donc chacun d'eux est identiquement nul. En particulier, les coefficients de la plus haute puissance de x dans ces polynômes sont nuls; or ces coefficients sont $R_0, R_1, R_2, \ldots, R_{p-1}$. Enfin, le lemme IV a eu pour objet de démontrer la condition $R_p \lesseqgtr 0$. Les conditions énoncées sont donc nécessaires.

Réciproquement, supposons qu'on ait

$$(\alpha) \qquad R_i = 0 \quad \text{pour} \quad i < p \qquad \text{et} \qquad R_p \lesseqgtr 0.$$

Soit q le degré de θ; d'après la partie directe qui vient d'être démontrée, on a

$$(\beta) \qquad R_i = 0 \quad \text{pour} \quad i < q, \qquad \text{et} \qquad R_q \lesseqgtr 0.$$

La coexistence des conditions (α) et des conditions (β) entraîne évidemment la condition $q = p$; le degré de θ est donc p et les conditions énoncées sont suffisantes.

THÉORÈME III. — *Lorsque f et g ont pour plus grand commun diviseur θ un polynôme de degré p, θ est, à un facteur constant près, le polynôme D_p dont l'expression développée est fournie par le lemme I.*

En effet, le terme du plus haut degré de D_p est $R_p x^p$, d'après le lemme I. En vertu du lemme IV, R_p est différent de zéro. Donc D_p est exactement de degré p; mais, d'après l'identité du lemme II, il est divisible par θ, qui, par hypothèse, est lui-même de degré p. Par conséquent, θ ne diffère de D_p que par un facteur indépendant de x.

Remarque. — Lorsque p est égal à n, le lemme II donne

$$D_n \equiv U_{-1} f + V_{m-n-1} g.$$

Or, le lemme III apprend que U_{-1} est identiquement nul et que V_{m-n-1} se réduit à $(b_n)^{m-n-1}$. On a donc

$$D_n \equiv (b_n)^{m-n-1} g.$$

θ n'est donc autre chose que g, ainsi que cela était évident *a priori*.

Théorème IV. — *Lorsque le plus grand commun diviseur θ de f et g est de degré p, les quotients de f et g divisés par θ sont respectivement* HV_{m-p}, $-HU_{n-p}$, *en désignant par* H *une constante qui, si l'on prend* $\theta \equiv D_p$, *a pour valeur*

$$-\left(\frac{1}{R_p}\right)^2.$$

En effet, on a, par application des lemmes I et II,

$$\begin{aligned} D_{p-1} \equiv{}& R_{p-1,1} x^0 + R_{p-1,2} x^1 + \ldots + R_{p-1,p-1} x^{p-2} \\ &+ R_{p-1} x^{p-1} \equiv U_{n-p} f + V_{m-p} g. \end{aligned}$$

Le polynôme θ de degré p, divisant f et g, divise donc D_{p-1} : or celui-ci n'est que de degré $p-1$ au plus; il est donc identiquement nul et l'on a, par suite,

$$U_{n-p} f + V_{m-p} g \equiv 0. \tag{1}$$

D'ailleurs, d'après le lemme III, les polynômes U_{n-p},

V_{m-p} ont respectivement pour termes de degrés les plus élevés $b_n R_p x^{n-p}$, $-a_m R_p x^{m-p}$ et, par conséquent, en vertu de la condition essentielle $a_m b_n \gtrless 0$ et de la condition $R_p \gtrless 0$ qui résulte du lemme IV, ils sont exactement des degrés $n-p$ et $m-p$.

Soient alors φ et γ les quotients obtenus en divisant f et g par θ. L'identité (1) peut s'écrire

$$U_{n\ p}\varphi\theta + V_{m\ p}\gamma\theta = 0,$$

ou, puisque θ n'est pas identiquement nul,

$$U_{n\ p}\varphi + V_{m\ p}\gamma \equiv 0 \tag{2}$$

D'après (2), φ divise $V_{m\ p}\gamma$, mais il est premier avec γ, dont il divise V_{m-p} et, par conséquent, φ et $V_{m\ p}$ étant tous deux de degré $m-p$, on a

$$\varphi = HV_{m\ p}, \tag{3}$$

en désignant par H un facteur indépendant de x. En tenant compte de (3), la relation (2) donne alors

$$\gamma = -HU_{n\ p} \tag{4}$$

Si l'on prend $\theta \equiv D_p$, le polynôme f, identique à $\varphi\theta$, est identique à $HD_p V_{m-p}$ et a, par suite, même terme de degré m que lui, ce qui donne

$$a_m = HR_p(-a_m R_p),$$

d'où

$$H = -\left(\frac{1}{R_p}\right)^2. \tag{5}$$

Les formules (3), (4) et (5) démontrent le théorème.

Seconde Partie.

Définitions. — Soient encore les deux polynômes entiers

$$f \equiv a_0 + a_1 x + \ldots + a_m x^m,$$
$$g \equiv b_0 + b_1 x + \ldots + b_n x^n,$$

m étant supérieur ou égal à n.

Posons

$$f_p = a_{p+1} + a_{p+2} x + \ldots + a_m x^{m-(p+1)},$$
$$g_p \equiv b_{p+1} + b_{p+2} x + \ldots + b_n x^{n-(p+1)},$$

p désignant un nombre entier au plus égal à n, avec la convention $g_n \equiv 0$.

Appelons c_{ij} le coefficient de x^j dans le polynôme entier

$$g_i f - f_i g,$$

et r_0 le déterminant d'ordre m suivant

$$\left|\begin{array}{cccccccccc}
c_{00} & c_{01} & c_{02} & \ldots & \ldots & \ldots & \ldots & \ldots & c_{0,m-1} & \\
c_{10} & c_{11} & c_{12} & \ldots & \ldots & \ldots & \ldots & \ldots & c_{1,m-1} & \left.\vphantom{x}\right\} n \text{ lignes} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots & \\
c_{n-1,0} & c_{n-1,1} & c_{n-1,2} & \ldots & \ldots & \ldots & \ldots & \ldots & c_{n-1,m-1} & \\
b_0 & b_1 & b_2 & \ldots & \ldots & b_n & & & & \\
 & b_0 & b_1 & b_2 & \ldots & \ldots & b_n & & & \left.\vphantom{x}\right\} m-n \text{ lignes}; \\
 & & \ldots & \ldots & \ldots & \ldots & \ldots & & & \\
 & & & b_0 & b_1 & b_2 & \ldots & \ldots & b_n &
\end{array}\right|$$

r_0 est le résultant de Bezout. Les coefficients c_{ij} y occupent un rectangle, et les coefficients b un parallélogramme en dehors desquels nous supposons des zéros à toutes les places laissées vides.

Supprimons dans r_0 les p premières lignes; il reste alors un Tableau rectangulaire que nous désignerons par t_p.

Si l'on supprime les p premières colonnes de t_p, il reste un Tableau carré, dont nous appelons r_p le déterminant des éléments. On voit, en somme, que r_p se déduit de r_0 en y supprimant les p premières lignes et les p premières colonnes.

Soit i l'un des nombres 1, 2, 3, ..., p. J'appelle $r_{p,i}$ le déterminant déduit de r_p en y remplaçant la première colonne par la colonne qui, dans le Tableau t_p, occupe le rang i.

Je désigne par d_p le déterminant obtenu au moyen de r_p en ajoutant à sa première colonne multipliée par x_p les p premières colonnes du Tableau t_p respectivement multipliées par x^0, x^1, x^2, ..., x^{p-1}.

J'appelle enfin u_{n-p-1} et v_{m-p-1} les deux déterminants obtenus en remplaçant successivement la première colonne de r_p par celles-ci :

$$\begin{array}{ll} \varphi_p & -f_p \\ \varphi_{p+1} & -f_{p+1} \\ \cdot & \cdot \\ \varphi_{n-1} & -f_{n-1} \\ 0 & x^0 \\ \cdot & x^1 \\ \cdot & \cdot \\ 0 & x^{m-n-1}. \end{array}$$

Ces définitions posées, nous allons établir plusieurs lemmes importants :

LEMME 1. — *L'expression développée du polynôme* d_p *est*

$$d_p = r_{p,1}x^0 + r_{p,2}x^1 + \ldots + r_{p,p}x^{p-1} + r_p x^p.$$

En effet, d'après sa définition, d_p est la somme de $p+1$ déterminants qui se déduisent de r_p en y remplaçant successivement la première colonne par les $p+1$ premières colonnes de t_p, respectivement multipliées

par $x^0, x^1, x^2, \ldots, x^p$. Or, ces déterminants sont précisément les déterminants $r_{p,i}(i = 1, 2, \ldots, p)$ et r_p, définis plus haut, qu'on a multipliés respectivement par $x^0, x^1, x^2, \ldots, x^p$; ce qui démontre le lemme.

LEMME 2. — *On a identiquement*

$$d_p \equiv n_{n-p-1} f + v_{m-p-1} g.$$

En effet, d_p ne change pas si l'on ajoute aux éléments de sa première colonne les éléments correspondants des colonnes suivantes respectivement multipliés par x^{p+1}, x^{p+2}, ..., x^{m-1}. Cette première colonne devient ainsi

$$\left.\begin{array}{l} c_{p,0} + c_{p,1}x + \ldots + c_{p,m-1}x^{m-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n-1,0} + c_{n-1,1}x + \ldots + c_{n-1,m-1}x^{m-1} \\ b_0 + b_1 x + \ldots + b_n x^n \\ b_0 x + b_1 x^2 + \ldots + b_n x^{n+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_0 x^{m-n-1} + \ldots + b_n x^{m-1} \end{array}\right\} \text{ ou bien } \left\{\begin{array}{l} g_p f - f_p g \\ \ldots\ldots\ldots \\ g_{n-1} f - f_{n-1} g \\ 0.f + x_0 g \\ 0.f + x^1 g \\ \ldots\ldots\ldots \\ 0.f + x^{m-n-1} g. \end{array}\right.$$

On voit alors que d_p est la somme des deux déterminants obtenus en remplaçant la première colonne de r_p, d'abord par les premiers termes, ensuite par les seconds termes des éléments binômes qu'on vient d'écrire. Ces déterminants contiennent en facteur, l'un f, l'autre g, et l'on voit que les multiplicateurs de f et g sont les déterminants désignés par la notation u_{n-p-1}, v_{m-p-1}; ce qui démontre l'identité annoncée.

LEMME 3. — *Les termes du plus haut degré dans* u_{n-p-1} *et* v_{m-p-1} *sont*

$$b_n r_{p+1} x^{n-p-1} \qquad \text{et} \qquad -a_m r_{p+1} x^{m-p-1},$$

à moins que p soit égal à n, auquel cas le premier polynôme u_{-1} *est identiquement nul, et le second* v_{m-n-1} *se réduit à* $(b_n)^{m-n-1}$.

En effet, supposons d'abord $p < n$: les éléments de la

première colonne de u_{n-p-1} sont des polynômes entiers en x dont les indices vont en croissant et, par conséquent, dont les degrés vont en déeroissant, d'après la définition de ces polynômes. Alors, en développant u_{n-p-1} par rapport aux éléments de sa première colonne, comme les mineurs correspondants sont indépendants de x, on obtient un polynôme entier, dont le degré est celui de g_p, c'est-à-dire $n-p-1$, et le terme du plus haut degré a pour coefficient le produit de b_n, coefficient de x^{n-p-1} dans g_p, par le mineur de u_{n-p-1} relatif à l'élément g_p. Ce mineur est le déterminant qu'on déduit de r_p par la suppression de sa première ligne et de sa première colonne, c'est-à-dire r_{p+1}.

Dans v_{m-p-1}, les éléments de la première colonne sont : d'abord une suite de polynômes, dont le premier $-f_p$ est celui de degré le plus élevé, puis une suite d'éléments monômes, dont le dernier x^{m-n-1} a le degré le plus élevé. Le degré de f_p est $m-p-1$, nombre supérieur à $m-n-1$, puisque par hypothèse on a $p<n$. Le degré de v_{m-p-1} est donc $m-p-1$, et le coefficient de x^{m-p-1} dans ce polynôme est, comme on le voit immédiatement, $-a_m r_{p+1}$.

Supposons maintenant $p=n$. Puisque g_n est identiquement nul, la première colonne de u_{n-p-1} (pour $p=n$) a tous ses éléments nuls, et par suite le polynôme u_{-1} est identiquement nul. Quant au déterminant v_{m-p-1}, dans l'hypothèse $p=n$, sa première colonne a pour éléments x^0, x^1, x^2, ..., x^{m-n-1} dont les coefficients, dans le déterminant développé, sont les mineurs relatifs à la première colonne de r_n. Or on a évidemment

$$r_n = \begin{vmatrix} b_n & & \\ b_{n-1} & b_n & \\ \cdots & \cdots & \\ \cdots & \cdots & b_n \end{vmatrix} \quad (m-n \text{ lignes}),$$

tous les éléments au-dessus de la diagonale principale étant nuls, et, par suite,

$$v_{m-n-1} = \begin{vmatrix} x_0 & & & \\ x^1 & b_n & & \\ \cdot\cdot & \cdots & & \\ x^{m-n-1} & \cdots & b_n \end{vmatrix} = x_0 (b_n)^{m-n-1} = (b_n)^{m-n-1}.$$

LEMME 4. — *Lorsque f et g ont un plus grand commun diviseur de degré p, le déterminant r_p est différent de zéro.*

La proposition est évidente pour $p = n$, attendu que l'on a

$$r_n = (b_n)^{m-n}.$$

Supposons maintenant p inférieur à n. D'après la définition de r_p, on a

$$r_p = \begin{vmatrix} c_{p,p} & c_{p,p+1} & \cdots & \cdot\cdot & \cdot\cdot & \cdots & c_{p,m-1} \\ c_{p+1,p} & c_{p+1,p+1} & \cdots & \cdot\cdot & \cdot\cdot & \cdots & c_{p+1,m-1} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdot\cdot & \cdot\cdot & \cdots & \cdots\cdots \\ c_{n-1,p} & c_{n-1,p+1} & \cdots & \cdot\cdot & \cdot\cdot & \cdots & c_{n-1,m-1} \\ b_p & b_{p+1} & \cdots & b_n & & & \\ b_{p-1} & b_p & \cdots & \cdot\cdot & b_n & & \\ \cdots\cdots & \cdots\cdots & \cdots & \cdot\cdot & \cdot\cdot & \cdots & \\ b_{p-m+n+1} & \cdots\cdots & \cdots & \cdot\cdot & \cdot\cdot & \cdots & b_n \end{vmatrix} \begin{matrix} \\ \\ \\ \} n-p \text{ lignes,} \\ \\ \\ \} m-n \text{ lignes,} \\ \\ \end{matrix}$$

formule valable pour toute valeur de p, en faisant la convention que tous les éléments b affectés d'un indice négatif ne sont pas autre chose que des zéros.

Ajoutons à la première colonne multipliée par x^p les suivantes multipliées respectivement par x^{p+1}, x^{p+2}, ..., x^{m-1}. On obtient de la sorte un nouveau déterminant r qui est égal à $r_p x^p$; par conséquent, si l'on suppose r_p nul, r est nul aussi, et il y a entre les éléments de chaque colonne de r une même relation linéaire et homogène dans laquelle les coefficients ne sont pas tous nuls :

nous allons écrire cette relation, en particulier, à l'égard des éléments de la première colonne.

D'après la façon dont on déduit r de r_p, on voit qu'un élément quelconque c_{ip}, qui figure en tête de l'une des $n - p$ premières lignes de r_p, se trouve remplacé dans r par l'élément polynôme

$$C_i \equiv c_{i,p}x^p + c_{i,p+1}x^{p+1} + \ldots + c_{i,m-1}x^{m-1}.$$

On peut écrire C_i sous la forme

$$C_i \equiv c_{i,0}x^0 + c_{i,1}x^1 + \ldots + c_{i,m-1}x^{m-1} - (c_{i,0}x^0 + c_{i,1}x^1 + \ldots + c_{i,p-1}x^{p-1})$$

ou, d'après la définition de $c_{i,j}$ et en appelant $C_{i,p-1}$ le polynôme de degré $p - 1$ au plus qui est placé entre parenthèses,

$$C_i \equiv g_i f - f_i g - C_{i,p-1}. \tag{1}$$

D'autre part, tout élément b_{p-k} situé en tête de l'une des $m - n$ dernières lignes est remplacé dans r par

$$B_k \equiv b_{p-k}x^p + b_{p-k+1}x^{p+1} + \ldots + b_n x^{n+k}.$$

Or, si h désigne un entier inférieur à p, on a

$$\begin{aligned} B_h &\equiv x^h(b_{p-h}x^{p-h} + \ldots + b_n x^n) \\ &\equiv x^h[b_0 + b_1 x + \ldots + b_n x_n \\ &\qquad - (b_0 + b_1 x + \ldots + b_{p-h-1}x^{p-h-1})] \\ &\equiv x_h g - (b_0 x^h + b_1 x^{h+1} + \ldots + b_{p-h-1}x^{p-1}), \end{aligned}$$

ou, en désignant par $B_{h,p-1}$ le polynôme de degré $p - 1$ au plus qui est placé entre parenthèses,

$$B_h \equiv x^h g - B_{h,p-1}. \tag{2}$$

Si l désigne un entier égal ou supérieur à p, on a

$$B_l \equiv x^l(b_{p-l}x^{p-l} + \ldots + b_n x^n) \equiv x^l(b_0 + b_1 x + \ldots + b_n x_n),$$

puisque les coefficients b affectés d'indices négatifs sont nuls, et, par suite,

$$B_l \equiv x^l g. \tag{3}$$

D'après les formules (2) et (3), on peut donc poser, d'une façon générale, que k soit inférieur, égal ou supérieur à p,

$$B_k \equiv x^k g - B_{k,p-1}, \tag{4}$$

en appelant $B_{k,p-1}$ un polynôme de degré $p-1$ au plus, qui peut être identiquement nul.

Il résulte alors des formules (1) et (4) que la relation identique qui existe entre les éléments de la première colonne de r peut s'écrire

$$\sum_{i=p}^{i=n-1} \alpha_i (g_i f - f_i g - C_{i,p-1}) + \sum_{k=0}^{k=m-n-1} \beta_k (x^k g - B_{k,p-1}) \equiv 0,$$

ou bien

$$\left\{ f \sum_{i=p}^{i=n-1} \alpha_i g_i + g \left[- \sum_{i=p}^{i=n-1} \alpha_i f_i + \sum_{k=0}^{k=m-n-1} \beta_k x^k \right] \right. \equiv \sum_{i=p}^{i=n-1} \alpha_i C_{i,p-1} + \sum_{k=0}^{k=m-n-1} \beta_k B_{k,p-1}, \tag{5}$$

les diverses valeurs des coefficients α_i, β_k n'étant pas toutes nulles.

Puisque g_i est un polynôme entier de degré $n-(i+1)$, le coefficient de f dans (5) est un polynôme entier dont le degré est au plus $n-p-1$.

Le coefficient de g, dans (5), est la somme de deux termes dont le premier est un polynôme entier de degré $m-p-1$ au plus, puisque f_i est un polynôme entier de degré $m-(i+1)$, et le second est un polynôme entier de degré $m-n-1$ au plus; par conséquent, $m-n-1$ étant inférieur à $m-p-1$, puisqu'on a,

par hypothèse, $p < n$, le coefficient de g est un polynôme entier de degré $m - p - 1$ au plus.

Enfin, les polynômes $C_{i,p-1}$, $B_{k,p-1}$ étant chacun de degré $p - 1$ au plus, le second membre de (5) est un polynôme entier de degré $p - 1$ au plus.

Cela posé, si le plus grand commun diviseur θ de f et g n'est pas de degré inférieur à p, il est de degré supérieur à $p - 1$. Or il divise le premier membre de (5) et, par conséquent, aussi le second; mais celui-ci est de degré $p - 1$ au plus : il est donc identiquement nul. Alors l'identité (5) se réduit à

$$(6)\quad f\sum_{i=p}^{i=n-1}\alpha_i g_i + g\left[-\sum_{i=p}^{i=n-1}\alpha_i f_i + \sum_{k=0}^{k=m-n-1}\beta_k x^k\right] \equiv 0,$$

les coefficients α et β n'étant pas tous nuls.

Aucun des deux polynômes entiers, coefficients respectifs de f et de g dans (6), ne peut être identiquement nul sans que l'autre le soit aussi, en vertu de l'identité (6) elle-même, puisque ni f ni g n'est évanouissant. Or on a

$$\begin{aligned}\sum_{i=p}^{i=n-1}\alpha_i g_i \equiv{}& \alpha_p(b_{p+1} + b_{p+2}x + \ldots + b_n x^{n-p-1})\\ &+ \alpha_{p+1}(b_{p+2} + \ldots + b_n x^{n-p-2})\\ &+ \ldots\ldots\ldots\ldots\ldots\ldots\\ &+ \alpha_{n-2}(b_{n-1} + b_n x)\\ &+ \alpha_{n-1} b_n.\end{aligned}$$

Pour que ce polynôme soit identiquement nul, il faut et il suffit que l'on ait

$$\begin{aligned}&\alpha_p b_{p+1} + \alpha_{p+1} b_{p+2} + \ldots + \alpha_{n-2} b_{n-1} + \alpha_{n-1} b_n = 0,\\ &\alpha_p b_{p+2} + \alpha_{p+1} b_{p+3} + \ldots + \alpha_{n-2} b_n = 0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ &\alpha_p b_{n-1} + \alpha_{p+1} b_n = 0,\\ &\alpha_p b_n = 0.\end{aligned}$$

Comme b_n est différent de zéro, la dernière de ces équations exige que α_p soit nul; l'avant-dernière donne alors $\alpha_{p+1} = 0$, et ainsi de suite, de proche en proche, on voit que tous les α doivent être nuls. Mais alors le coefficient de g se réduit à $\Sigma \beta_k x^k$; or, on a vu qu'il s'évanouit en même temps que le coefficient de f; donc tous les coefficients β sont nuls.

En résumé, si les deux polynômes, coefficients de f et g dans (6), sont identiquement nuls, tous les coefficients α et tous les coefficients β sont nuls, résultat en contradiction avec l'existence, démontrée plus haut, de l'identité (6) pour des valeurs des α et des β non toutes nulles. Il en résulte, par conséquent, que les polynômes, coefficients de f et g dans (6), ne sont ni l'un ni l'autre identiquement nuls.

Alors, l'existence de l'identité (6), dans les conditions que l'on vient de préciser, montre qu'il y a deux polynômes entiers u, v, non évanouissants, dont les degrés respectifs sont au plus $n - p - 1$ et $m - p - 1$, qui satisfont à l'identité $uf + vg \equiv 0$. Par conséquent, d'après le théorème fondamental rappelé au début de ce travail, θ est au moins de degré $p + 1$.

En somme, lorsque r_p est nul, si θ n'est pas de degré inférieur à p, il est de degré supérieur et, par suite, enfin, lorsque θ est de degré p, on a

$$r_p \gtrless 0. \qquad \text{C. Q. F. D.}$$

Il suffit maintenant de remarquer que les théorèmes I, II, III, IV de la première Partie résultent uniquement du théorème fondamental et des lemmes I, II, III, IV, puis d'observer la parfaite analogie des lemmes 1, 2, 3, 4 de la seconde Partie avec ceux de la première, pour que l'on puisse énoncer et admettre, sans nouvelle démon-

stration, les théorèmes suivants, correspondant aux quatre théorèmes de la première Partie.

THÉORÈME 1. — *Pour que f et g aient un plus grand commun diviseur de degré p, il faut et il suffit que l'on ait*

$$r_{p-1,1} = r_{p-1,2} = \ldots = r_{p-1,p-1} = r_{p-1} = 0 \qquad et \qquad r_p \gtrless 0.$$

THÉORÈME 2. — *Pour que f et g aient un plus grand commun diviseur de degré p, il faut et il suffit que l'on ait*

$$r_0 = r_1 = r_2 = \ldots = r_{p-1} = 0 \qquad et \qquad r_p \gtrless 0.$$

THÉORÈME 3. — *Lorsque f et g ont un plus grand commun diviseur de degré p, ce polynôme est, à un facteur constant près, d_p, dont l'expression développée est fournie par le lemme 1. Lorsque p est égal à n, le plus grand commun diviseur est*

$$d_n \equiv (b_n)^{m-n-1} g.$$

THÉORÈME 4. — *Les quotients respectifs de f et g divisés par leur plus grand commun diviseur d_p sont*

$$-\left(\frac{1}{r_p}\right)^2 v_{m-p}, \quad \left(\frac{1}{r_p}\right)^2 u_{n-p}.$$