NOUVELLES ANNALES DE MATHÉMATIQUES

ÉTIENNE POMEY

Sur le plus grand commun diviseur de deux polynômes entiers

Nouvelles annales de mathématiques 3^e série, tome 7 (1888), p. 407-427

<http://www.numdam.org/item?id=NAM_1888_3_7__407_1>

SUR LE PLUS GRAND COMMUN DIVISEUR DE DEUX POLYNOMES ENTIERS;

PAR M. ETIENNE POMEY

Je me propose, dans ce travail, de chercher les conditions nécessaires et suffisantes pour que les polynômes entiers

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

m étant supérieur ou égal à n, aient un plus grand commun diviseur de degré p, et de former ce plus grand commun diviseur.

LEMME I. — *L'expression générale des polynômes entiers u, v satisfaisant à l'identité*

$$uf + vg \equiv 0 \tag{1}$$

est donnée par les formules

$$u \equiv g_1 A, \tag{2}$$
$$v \equiv -f_1 A, \tag{3}$$

où A désigne un polynôme entier quelconque et f_1 et g_1 les quotients de f et g par leur plus grand commun diviseur θ.

En effet, l'identité (1) peut s'écrire

$$uf_1\theta + vg_1\theta \equiv 0. \tag{4}$$

Si f et g sont premiers entre eux, on peut supposer $\theta = 1, f_1 = f, g_1 = g$. S'ils ne sont pas premiers entre eux, θ n'est pas identiquement nul. Dans les deux cas, on peut donc diviser l'identité (4) par θ, ce qui donne

$$uf_1 + vg_1 \equiv 0. \tag{5}$$

On voit ainsi que g_1 divise uf_1; mais g_1 est premier avec f_1; donc il divise u, et l'on a

$$u \equiv g_1 A, \tag{2}$$

A étant un polynôme entier. Alors l'identité (5) peut s'écrire

$$g_1 A f_1 + v g_1 \equiv 0$$

ou, puisque g_1 n'est pas identiquement nul,

$$v = -f_1 A. \tag{3}$$

Ainsi, pour que u et v puissent satisfaire à la relation (1), il faut qu'ils rentrent dans les formules (2) et (3); d'ailleurs les polynômes donnés par ces formules satisfont à l'identité (1), quel que soit le polynome A. Le théorème est donc démontré.

LEMME II. — *Lorsque le plus grand commun diviseur θ de f et g est de degré p, il existe, quelle que soit la valeur de q, prise parmi les nombres* 1, 2, 3, .. , p, *deux polynômes u, v de degrés respectifs $n-q$, $m-q$, satisfaisant à l'identité $uf + vg \equiv 0$.*

En effet, θ étant, par hypothèse, de degré p, les polynômes f_1 et g_1, quotients de f et g divisés par θ, sont des degrés $n-p$ et $m-p$; alors, si dans les formules (2) et (3) du lemme I, qui définissent tous les couples de polynômes u, v satisfaisant à $uf + vg \equiv 0$, on prend pour A un polynôme arbitraire de degré $p-q$, en désignant par q l'un des nombres 1, 2, .. , p, les poly-

nômes u, v correspondants fournis par ces formules ont respectivement pour degrés $n-q$ et $m-q$.

LEMME III. — *Lorsque le plus grand commun diviseur* θ *de* f *et* g *est de degré* p, *il existe un couple de polynômes* u, v *respectivement de degré* $n-p$ *et* $m-p$, *satisfaisant à l'identité* $uf+vg\equiv 0$. *Il n'en existe qu'un seul, abstraction faite d'un facteur constant arbitraire.*

En effet, θ étant de degré p, f_1 et g_1 sont de degré $n-p$ et $m-p$. Alors, d'après les formules (2) et (3) du lemme I, tous les couples de polynômes u, v, de degré $n-p$ et $m-p$, satisfaisant à $uf+vg\equiv 0$, s'obtiendront en multipliant g_1 et $-f_1$ par une même constante A, arbitraire d'ailleurs.

LEMME IV. — *Lorsqu'il existe un couple de polynômes* u, v, *déterminés à un facteur constant arbitraire près, respectivement de degrés* $n-p$ *et* $m-p$, *tels que* $uf+vg$ *soit identiquement nul, le plus grand commun diviseur* θ *de* f *et* g *est de degré* p.

En effet, l'expression générale des polynômes u, v satisfaisant à l'identité $uf+vg\equiv 0$ est donnée par les formules (2) et (3) du lemme I. Pour que ces polynômes u, v soient déterminés, à un facteur arbitraire près, il faut que le polynôme A se réduise à une constante; alors, pour que u et v aient pour degrés $n-p$ et $m-p$, il faut que g_1 et f_1 soient eux-mêmes de degrés $n-p$ et $m-p$; or ces derniers polynômes sont les quotients de g et f par θ; il faut donc que θ soit de degré p.

Ces lemmes préliminaires établis, on peut rattacher les conditions d'existence d'un plus grand commun di-

viseur de degré p, soit au résultant d'Euler-Bézout-Sylvester, soit à celui de Bézout-Cauchy. C'est ce que je ferai successivement dans la première et dans la seconde Partie de ce travail.

PREMIÈRE PARTIE.

RÉSULTANT D'EULER-BÉZOUT-SYLVESTER.

Notations. — Dans ce qui suit, nous désignerons par R_0 le déterminant suivant, d'ordre $m+n$

$$\begin{vmatrix}
 & & & & b_0 & a_0 & & & & \\
 & & & . & b_1 & a_1 & a_0 & & & \\
 & & . & & . & . & a_1 & . & & \\
 & . & & & . & . & . & & . & \\
 & b_0 & & & . & . & . & & & a_0 \\
b_0 & b_1 & & & b_n & . & . & & & a_1 \\
b_1 & . & & . & & a_m & . & & & . \\
. & . & & . & & & a_m & & & . \\
. & . & . & & & & & . & & . \\
. & b_n & & & & & & & . & . \\
b_n & & & & & & & & & a_m
\end{vmatrix},$$

dans lequel les m premières colonnes contiennent uniquement les coefficients de g, les n dernières uniquement les coefficients de f, et où l'on considère comme nuls tous les éléments non écrits situés en dehors des deux parallélogrammes recouverts par les a et par les b. Sauf une légère modification d'arrangement, ce déterminant est le résultant d'Euler-Bézout-Sylvester relatif aux polynômes f et g.

Nous désignerons par R_i le déterminant qui se déduit de R_0 par la suppression des i rangées quadrangulaires extrêmes, c'est-à-dire par la suppression des i premières

et des i dernières lignes, ainsi que des i premières et des i dernières colonnes.

Nous appellerons R_{ij} le déterminant obtenu au moyen de R_i en substituant à sa première ligne les éléments correspondants de la $j^{\text{ième}}$ ligne de R_0.

En désignant par q l'un quelconque des nombres 1, 2, ..., $p+1$ et posant

$$u \equiv \alpha_0 + \alpha_1 x - \alpha_2 x^2 + \ldots + \alpha_{n-q} x^{n-q},$$
$$v \equiv \beta_0 + \beta_1 x + \beta_2 x^2 - \ldots - \beta_{m-q} x^{m-q},$$

nous appellerons S_q le système d'équations obtenu en égalant à zéro les coefficients du polynôme $uf + vg$, ce système étant écrit sous la forme spéciale suivante :

$$\begin{aligned}
b_0\beta_0 + a_0\alpha_0 &= 0,\\
b_0\beta_1 + b_1\beta_0 + a_1\alpha_0 - a_0\alpha_1 &= 0,\\
&\cdots\cdots\cdots\cdots\\
\ldots + b_{n-1}\beta_1 - b_n\beta_0 + a_n\alpha_0 + a_{n-1}\alpha_1 + \ldots &= 0,\\
&\cdots\cdots\cdots\cdots\\
\ldots + b_n\beta_{m-n} + a_m\alpha_0 - a_{m-1}\alpha_1 - \ldots &= 0,\\
\ldots - b_n\beta_{m-n-1} - a_m\alpha_1 + \ldots &= 0,\\
&\cdots\cdots\cdots\cdots\\
b_n\beta_{m-q} + a_m\alpha_{n-q} &= 0.
\end{aligned}$$

Nous appellerons enfin $S_{q,k}$ le système qu'on déduit de S_q en y supprimant les k premières équations, et $S^h_{q,k}$ le système obtenu en remplaçant la première équation $S_{q,k}$ par la $h^{\text{ième}}$ équation de S_q.

De ces définitions résultent les remarques suivantes :

Première remarque préliminaire. — Si l'on considère le système $S_{q,q-1}$, composé de $m+n-2q+2$ équations linéaires et homogènes par rapport aux $m+n-2q+2$ quantités β_{m-q}, β_{m-q-1}, ..., β_0, α_0, α_1, ..., α_{n-q}, les coefficients de ces quantités dans ce système forment un tableau carré, dont le déterminant est R_{q-1}, d'après la définition de R_i.

Deuxième remarque préliminaire. — D'après ce qu'on vient de voir, le déterminant des coefficients des β et des α dans $S_{p,p-1}$ est R_{p-1}. Alors, si l'on supprime la première équation du système $S_{p,p-1}$, ce qui donne le système $S_{p,p}$, et que dans ce dernier on supprime les termes en β_{m-p}, on voit que les coefficients des β et des α restants forment un tableau carré, dont le déterminant se déduit de R_{p-1} en supprimant sa première ligne et sa première colonne. Comme le nombre p désigne, dans ce travail, le degré du plus grand commun diviseur, il est au plus égal à n, et par suite le déterminant considéré est

$$\Delta = \begin{vmatrix} . & b_{p-1} & b_p & a_p & a_{p-1} & . & \\ & & . & . & & & \\ & & . & . & & & \\ & & . & . & & & \\ & & b_n & . & & & \\ & . & & a_m & . & & \\ b_n & & & & & . & \\ 0 & & & & & & a_m \end{vmatrix}.$$

Il présente $m-p$ colonnes formées avec les coefficients b, et $n-p+1$ colonnes formées avec les coefficients a.

En le développant par rapport aux éléments de la dernière ligne, on a

$$\Delta = a_m \cdot \begin{vmatrix} . & b_{p-1} & b_p & a_p & a_{p-1} & . & \\ & & . & . & & & \\ & & . & . & & & \\ & & . & . & & & \\ & & b_n & . & & & \\ & . & & a_m & . & & \\ . & & & & & . & \\ b_n & & & & & & a_m \end{vmatrix},$$

le déterminant qui multiplie a_m présentant $m - p$ colonnes formées avec les b et $n - p$ formées avec les a. Ce déterminant est donc R_p, et l'on a

$$\Delta = a_m R_p.$$

Troisième remarque préliminaire. — Lorsque dans $S_{q,q-1}$ on remplace la première équation par la $h^{\text{ième}}$ équation de S_q, h étant l'un quelconque des nombres 1, 2, ..., $q-1$, les coefficients des β et des α dans le système obtenu $S^h_{q,q-1}$ forment un tableau carré, dont le déterminant est $R_{q-1,h}$, d'après la définition de $R_{i,j}$ donnée précédemment. Ainsi le déterminant de $S^j_{p\,p-1}$ ($j = 1, 2, \ldots, p-1$) est $R_{p-1,j}$, et le déterminant de $S^{j+1}_{p+1,p}$ ($j = 0, 1, 2, \ldots, p-1$) est $R_{p,j+1}$.

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*

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

En effet, si θ est de degré p, il existe (lemme II), quelle que soit la valeur de q choisie parmi les nombres 1, 2, ..., p, deux polynômes

$$u \equiv \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-q} x^{n-q},$$
$$v \equiv \beta_0 + \beta_1 x + \ldots + \beta_{m-q} x^{m-q},$$

où α_{n-q} et β_{m-q} sont différents de zéro, qui rendent identiquement nul le polynôme $uf + vg$, c'est-à-dire dont les coefficients vérifient le système S_q et, par suite, aussi le système $S_{q,q-1}$. Il en résulte que ce dernier système admet pour les β et les α une solution où ces quantités ne sont pas toutes nulles, puisque β_{m-q} et α_{n-q} en particulier, qui figurent dans la dernière équation avec les coefficients b_n, a_m essentiellement différents de zéro, ont, dans cette solution, des valeurs non

nulles. Par conséquent, enfin, le déterminant de ce système, qui est R_{q-1}, d'après la première remarque préliminaire, est nul; et, comme q désigne l'un quelconque des nombres 1, 2, ..., p choisi arbitrairement, on a

$$R_0 = R_1 = R_2 = \ldots = R_{p-1} = 0.$$

En outre, d'après le lemme III, le système S_p fournit pour les β et les α une solution déterminée, à un facteur constant arbitraire près, dans laquelle α_{n-p} et β_{m-p} ont des valeurs différentes de zéro. Or, si l'on attribue à l'une quelconque des inconnues α_{n-p}, β_{m-p} une valeur arbitraire non nulle, la dernière équation fournit pour l'autre inconnue une valeur finie non nulle. Le système $S_{p,p}$, composé de $m+n-2p+1$ équations linéaires et non homogènes par rapport aux $m+n-2p+1$ inconnues $\beta_{m-p-1}, \ldots, \beta_0, \alpha_0, \alpha_1, \ldots, \alpha_{n-p}$, admet alors pour celles-ci une solution finie unique en fonction de β_{m-p}. Il en résulte que le déterminant formé par les coefficients des β et des α autres que β_{m-p} dans ce système est différent de zéro. Or on a vu (deuxième remarque préliminaire) que ce déterminant Δ a pour valeur $a_m R_p$; mais a_m est essentiellement différent de zéro; par conséquent, R_p est lui-même différent de zéro.

Les conditions énoncées sont donc nécessaires.

Réciproquement, ces conditions sont suffisantes; car, en les supposant remplies, θ ne peut être de degré inférieur à p, puisque cela exigerait que l'un des déterminants $R_0, R_1, \ldots, R_{p-1}$ fût différent de zéro; il ne peut pas non plus être de degré supérieur à p, attendu que cela exigerait la condition $R_p = 0$. Dans les deux cas, le résultat serait en contradiction avec les hypothèses. Donc θ est de degré p.

On peut démontrer un second théorème équivalent au précédent, mais qui donne les conditions nécessaires et suffisantes au moyen de $p+1$ déterminants de même ordre que R_p.

THÉORÈME II. — *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, si θ est de degré p, il résulte du lemme III que le système S_p admet pour les β et les α une solution unique (abstraction faite d'un facteur constant arbitraire), dans laquelle les valeurs de α_{n-p} et β_{m-p} ne sont pas nulles. Il en est ainsi, en particulier, du système $S_{p,p-1}$ et de chacun des $p-1$ systèmes $S^j_{p,p-1}$ ($j = 1, 2, \ldots, p-1$). Donc les déterminants de ces systèmes homogènes, qui sont R_{p-1}, $R_{p-1,1}$, $R_{p-1,2}$, ..., $R_{p-1,p-1}$, d'après la troisième remarque préliminaire, sont nuls.

Si, de plus, on attribue à β_{m-p} une valeur arbitraire non nulle, dans le système $S_{p,p}$, qui est linéaire et non homogène par rapport aux quantités β_{m-p-1}, ..., β_0, α_0, ..., α_{n-p}, ce système admettant une solution unique pour ces quantités, le déterminant de leurs coefficients dans $S_{p,p}$ est différent de zéro. Or, d'après la deuxième remarque préliminaire, ce déterminant Δ a pour valeur $a_m R_p$, et comme a_m est essentiellement différent de zéro, on a $R_p \gtrless 0$. Les conditions énoncées sont donc nécessaires.

Elles sont suffisantes. En effet, en les supposant remplies, le système S_p fournit, pour les β et les α, un seul système de valeurs, déterminées à un facteur constant près, où α_{n-p} et β_{m-p} sont différents de zéro. Il y a donc

un couple de polynômes u, v, de degrés $n-p$ et $m-p$, tels que le polynôme $uf+vg$ soit identiquement nul, et il n'en existe qu'un, abstraction faite d'un facteur constant arbitraire. Par conséquent (lemme IV), le plus grand commun diviseur θ est de degré p.

Expression du plus grand commun diviseur de f et g. — En supposant que f et g aient un plus grand commun diviseur θ de degré p, proposons-nous de former ce polynôme.

Si l'on peut trouver deux polynômes u, v déterminés, et un polynôme déterminé θ de degré p, tels qu'on ait $uf+vg\equiv\theta$, ce polynôme θ est le plus grand commun diviseur de f et g; car, si cette relation existe, tout diviseur commun à f et g divise θ; il en est ainsi, en particulier, du plus grand commun diviseur de f et g, et, comme il est de même degré p que θ, il lui est égal, à un facteur constant près.

De cette simple observation résulte immédiatement la marche à suivre pour rechercher θ.

Posons

$$u\equiv\alpha_0+\alpha_1x+\ldots+\alpha_{n-q}x^{n-q},$$
$$v\equiv\beta_0+\beta_1x+\ldots+\beta_{m-q}x^{m-q},$$
$$\theta\equiv\gamma_0+\gamma_1x+\ldots+\gamma_{p-1}x^{p-1}+x^p,$$

et cherchons à déterminer q de façon que l'identité $uf+vg\equiv\theta$ ait lieu pour des valeurs déterminées des α, des β et des γ.

L'identité $uf+vg\equiv\theta$ est équivalente à un système d'équations linéaires par rapport aux α, aux β et aux γ; ce système n'est pas homogène, puisque le coefficient de x^p dans θ est l'unité. Pour qu'il fournisse une solution unique pour les α, les β et les γ, il faut que le nombre d'équations soit égal à celui des inconnues. Or celles-ci sont en nombre $(n-q+1)+(m-q+1)+p$,

nombre qui surpasse le nombre $p+2$ des termes de θ de la quantité $(n-q)+(m-q)$, positive ou nulle. Il faut donc que le nombre des termes de $uf+vg$ surpasse d'autant d'unités le nombre $p+2$. Or ce nombre de termes est supérieur d'une unité au degré $m+n-q$ de ce polynôme. On doit donc avoir

$$m+n-q+1=(m+n-2q)+p+2,$$

c'est-à-dire

$$q=p+1.$$

Pour que cette valeur de q soit admissible, il faut et il suffit qu'elle ne rende pas négatif le nombre $n-q$, puisque celui-ci représente le degré de u. Il faut donc et il suffit qu'on ait $n-(p+1)\geq 0$, c'est-à-dire $p\leq n-1$, ou enfin que p ne soit pas égal à n, puisque, d'après sa définition, p ne peut surpasser n. Or on peut exclure le cas où p serait égal à n, sans restreindre la généralité du raisonnement, puisque, dans ce cas, θ est immédiatement connu et n'est autre chose que le polynôme g lui-même.

Adoptant donc pour q la valeur $p+1$, le système qui détermine les α, les β et les γ est

$$\left.\begin{array}{l}
\qquad b_0\ \beta_0+a_0\ \alpha_0 \qquad\qquad -\gamma_0 = 0,\\
\qquad\qquad \cdots\cdots\cdots\cdots \qquad\quad \cdots\cdots\ \cdot\\
+b_{j-1}\beta_1+b_j\ \beta_0+a_j\ \alpha_0+a_{j-1}\alpha_1+\ldots-\gamma_j = 0,\\
\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\qquad +b_{p-1}\beta_0+a_{p-1}\alpha_0+ \qquad -\gamma_{p-1} = 0,
\end{array}\right\}\ \text{A}$$

$$\left.\begin{array}{l}
\qquad +b_p\ \beta_0+a_p\ \alpha_0+ \qquad -1 = 0,\\
+b_{p+1}\beta_0+a_{p+1}\alpha_0+\ldots \qquad = 0,\\
\qquad\qquad \cdots\cdots\cdots\cdots\cdots\\
b_n\beta_{m-p-1} \qquad\qquad +a_m\alpha_{n-p-1} = 0
\end{array}\right\}\ \text{B}$$

Le groupe A des p premières équations se déduit du groupe des p premières équations du système S_{p+1} en

retranchant à leurs premiers membres respectivement $\gamma_0, \gamma_1, \ldots, \gamma_{p-1}$. Le second groupe B est le groupe $S_{p+1,p}$, où l'on a simplement retranché l'unité au premier membre de la première équation.

Pour avoir l'inconnue γ_j, j désignant l'un quelconque des nombres 0, 1, 2, ..., $p-1$, nous calculerons les α et les β au moyen du système B, et nous porterons leurs valeurs dans la $(j+1)^{\text{ième}}$ équation du système A. Or on sait que le résultat final de cette substitution s'obtient en égalant à zéro le déterminant complet D du système formé par la réunion de la $(j+1)^{\text{ième}}$ équation de A avec le système B. On a ainsi

$$D = \begin{vmatrix} \cdot & \cdot & \cdot & \cdot & b_j & a_j & \cdot & \cdot & \cdot & -\gamma_j \\ & & & & b_p & a_p & & & & -1 \\ & & & b_p & b_{p+1} & a_{p+1} & a_p & & & 0 \\ & & & & \cdot & \cdot & & & & 0 \\ & & & & \cdot & \cdot & & & & \\ & & & & \cdot & \cdot & & & & \\ & & & & b_n & \cdot & & & & \\ & & & b_n & & a_m & & & & \\ & & \cdot & & & & a_m & & & \\ & \cdot & & & & & & \cdot & & \\ \cdot & & & & & & & & \cdot & 0 \\ b_n & & & & & & & & a_m & \end{vmatrix} = 0,$$

les deux premiers éléments de la dernière colonne de D étant $-\gamma_j$ et -1, et tous les autres étant nuls.

Or, le déterminant obtenu en supprimant dans D la dernière colonne et la première ligne est celui du système $S_{p+1,p}$, c'est-à-dire R_p, d'après la première remarque préliminaire. Le déterminant obtenu en supprimant la dernière colonne et la seconde ligne de D est celui du système $S^{j+1}_{p+1,p}$: c'est donc $R_{p,j+1}$ en vertu de la troisième remarque préliminaire. Il résulte de là que,

en développant D par rapport aux éléments de la dernière colonne, l'équation précédente peut s'écrire

$$\gamma_j R_p - R_{p,j+1} = 0,$$

d'où

$$\gamma_j = \frac{R_{p,j+1}}{R_p}.$$

On peut donc facilement énoncer le théorème suivant :

THÉORÈME III. — *Lorsque le plus grand commun diviseur* θ *de* f *et* g *est de degré* p, *l'expression de ce polynôme est donnée par l'identité*

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

SECONDE PARTIE.

RÉSULTANT DE BÉZOUT-CAUCHY.

Notations. — Dans ce qui suit, nous poserons

$$\left.\begin{aligned} f_i &\equiv a_{i+1} + a_{i+2} x + \ldots + a_m x^{m-i-1}, \\ g_i &\equiv b_{i+1} + b_{i+2} x + \ldots + b_n x^{n-i-1}, \\ g_i f - f_i g &\equiv c_{i0} + c_{i1} x + \ldots + c_{i,m+n-i-1} x^{m+n-i-1}, \end{aligned}\right\} (i \leq n)$$

$$r_0 = \begin{vmatrix} c_{00} & c_{10} & \ldots & c_{n-1,0} & b_0 & & & & & \\ c_{01} & c_{11} & \ldots & c_{n-1,1} & b_1 & b_0 & & & & \\ \cdot & \cdot & \ldots & \cdot & \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & \ldots & \cdot & \cdot & \cdot & & \cdot & & \\ \cdot & \cdot & \ldots & \cdot & \cdot & \cdot & & & \cdot & \\ \cdot & \cdot & \ldots & \cdot & \cdot & \cdot & & & & b_0 \\ \cdot & \cdot & \ldots & \cdot & b_n & \cdot & & & & \cdot \\ \cdot & \cdot & \ldots & \cdot & & b_n & & & & \cdot \\ \cdot & \cdot & \ldots & \cdot & & & \cdot & & & \cdot \\ \cdot & \cdot & \ldots & \cdot & & & & \cdot & & \cdot \\ \cdot & \cdot & \ldots & \cdot & & & & & & \cdot \\ c_{0,m-1} & c_{1,m-1} & \ldots & c_{n-1,m-1} & & & & & & b_n \end{vmatrix}.$$

Ce déterminant r_0 est le résultant d'ordre m de Bézout-Cauchy. Les coefficients c_{ij} y occupent la surface d'un rectangle, dans lequel c_{ij} est à l'intersection de la $(i+1)^{\text{ième}}$ ligne et de la $(j+1)^{\text{ième}}$ colonne. Les coefficients b y occupent la surface d'un parallélogramme. En dehors de ces deux surfaces, tous les éléments sont nuls.

Nous appellerons r_i le déterminant formé au moyen de r_0, en y supprimant les i premières lignes et les i premières colonnes, et r_{ij} le déterminant qu'on déduit de r_i en substituant à sa première ligne les éléments correspondants de la $j^{\text{ième}}$ ligne de r_0.

Nous appellerons s_q le système d'équations suivant :

$$\begin{array}{l}
c_{q-1,0}\,\lambda_0 + c_{q,0}\,\lambda_1 + \ldots + c_{n-1,0}\,\lambda_{n-q} + \lambda_{n-q+1} b_0 = 0,\\
c_{q-1,1}\,\lambda_0 + c_{q,1}\,\lambda_1 + \ldots + c_{n-1,1}\,\lambda_{n-q} + \lambda_{n-q+1} b_1 + \lambda_{n-q+2} b_0 = 0,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
c_{q-1,n}\,\lambda_0 + c_{q,n}\,\lambda_1 + \ldots + c_{n-1,n}\,\lambda_{n-q} + \lambda_{n-q+1} b_n + \lambda_{n-q+2} b_1 + \ldots = 0\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
c_{q-1,m-1}\,\lambda_0 + c_{q,m-1}\,\lambda_1 + \ldots + c_{n-1,m-1}\,\lambda_{n-q} \qquad + \lambda_{m-q} b_n = 0
\end{array}$$

Nous désignerons par $s_{q,k}$ le système qu'on déduit de s_q en y supprimant les k premières équations, et par $s^h_{q,q-1}$ le système obtenu en remplaçant la première équation de $s_{q,q-1}$ par la $h^{\text{ième}}$ équation de s_q.

Cela posé, nous ferons quatre remarques préliminaires importantes.

Première remarque préliminaire. — Si l'on considère le système $s_{q,q-1}$, composé de $m-q+1$ équations linéaires et homogènes par rapport aux $m-q+1$ quantités $\lambda_0, \lambda_1, \ldots, \lambda_{m-q}$, le déterminant des coefficients de ce système est r_{q-1}, d'après la définition de r_i.

Deuxième remarque préliminaire. — D'après ce qu'on vient de voir, le déterminant de $s_{p,p-1}$ est r_{p-1}.

Alors, si l'on supprime la première équation de $s_{p,p-1}$, ce qui donne $s_{p,p}$, et que dans ce dernier système on supprime les termes en λ_0, le déterminant des coefficients restants se déduit de r_{p-1} en supprimant sa première ligne et sa première colonne : ce déterminant est donc r_p.

Troisième remarque préliminaire. — Lorsque dans $s_{q,q-1}$ on remplace la première équation par la $h^{\text{ième}}$ équation de s_q, h étant l'un quelconque des nombres 1, 2, ..., $q-1$, le déterminant du système obtenu $s^h_{q,q-1}$ est $r_{q-1,h}$, d'après la définition de r_{ij}.

Ainsi, le déterminant $s^j_{p,p-1}$ $(j = 1, 2, \ldots, p-1)$ est $r_{p-1,j}$, et le déterminant de $s^{j+1}_{p+1,p}$ $(j = 0, 1, 2, \ldots, p-1)$ est $r_{p,j+1}$.

Quatrième remarque préliminaire. — On peut mettre les polynômes u et v

$$\left.\begin{aligned} u &\equiv \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-q} x^{n-q} \\ v &\equiv \beta_0 + \beta_1 x + \ldots + \beta_{m-q} x^{m-q} \end{aligned}\right\} \qquad (q = 1, 2, \ldots, p+1)$$

sous la forme

$$\begin{aligned} u &\equiv \lambda_0 g_{q-1} + \lambda_1 g_q + \ldots + \lambda_{n-q} g_{n-1}, \\ v &\equiv \mu_0 f_{q-1} + \mu_1 f_q + \ldots + \mu_{n-q} f_{n-1} \\ &\quad + \lambda_{n-q+1} + \lambda_{n-q+2} x + \ldots + \lambda_{m-q} x^{m-q-1}, \end{aligned}$$

λ_0 et μ_0 étant différents de zéro, si ces polynômes sont exactement de degrés $n-q$ et $m-q$.

En effet, pour cela, il faut et il suffit que les systèmes obtenus par identification donnent pour les λ et les μ des valeurs finies et déterminées, quels que soient les α

et les β. Or ces deux systèmes sont :

$$
\left.\begin{array}{ll}
b_n\lambda_0 & = \alpha_{n-q},\\
b_{n-1}\lambda_0 + b_n\lambda_1 & = \alpha_{n-q-1},\\
\cdots\cdots\cdots & \\
b_{n+q-h}\lambda_0 + \ldots + b_n\lambda_{h-q} & = \alpha_{n-h},\\
\cdots\cdots\cdots\cdots\cdots & \\
b_q\lambda_0 + \ldots\ldots\ldots\ldots + b_n\lambda_{n-q} & = \alpha_0,
\end{array}\right\} \mathrm{U}
$$

$$
\left.\begin{array}{ll}
a_m\mu_0 & = \beta_{m-q},\\
a_{m-1}\mu_0 + a_m\mu_1 & = \beta_{m-q-1},\\
\cdots\cdots\cdots & \\
a_{m+q-h}\mu_0 + \ldots + a_m\mu_{h-q} & = \beta_{m-h},\\
\cdots\cdots\cdots\cdots\cdots & \\
a_{q+m-n}\mu_0 + \ldots\ldots\ldots\ldots + a_m\mu_{n-q} & = \beta_{m-n},\\
a_{q+m-n-1}\mu_0 + \ldots\ldots\ldots\ldots + a_{m-1}\mu_{n-q} + \lambda_{m-q} & = \beta_{m-n-1},\\
\cdots\cdots\cdots\cdots\cdots & \\
a_q\mu_0 + \ldots\ldots\ldots\ldots + a_n\mu_{n-q} + \lambda_{n-q+1} & = \beta_0.
\end{array}\right\} \mathrm{V}
$$

Le déterminant des coefficients des inconnues λ du système U est $(b_n)^{n-q+1}$, qui est différent de zéro : ces inconnues ont donc des valeurs finies déterminées.

Le déterminant des coefficients des inconnues μ dans les $n-q+1$ premières équations du système V étant $(a_m)^{n-q+1}$ est aussi différent de zéro, et ces inconnues μ ont des valeurs finies déterminées. Enfin chacune des $m-n$ dernières équations du système V ne contient qu'une inconnue λ, qui est d'ailleurs affectée d'un coefficient égal à l'unité, en sorte que ces inconnues λ, à leur tour, ont des valeurs finies déterminées.

D'ailleurs la première équation de chacun des systèmes U, V montre que si u et v sont exactement de degrés $n-q$ et $m-q$, ce qui suppose $\alpha_{n-q}\beta_{m-q} \gtrless 0$, on a

$$\lambda_0\mu_0 \gtrless 0.$$

Théorème I. — *Pour que le plus grand commun divi-*

seur θ *de* f *et* g *soit de degré* p, *il faut et il suffit que l'on ait*

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

En effet, si θ est de degré p, il existe (lemme II), quelle que soit la valeur de q prise par les nombres 1, 2, ..., p, deux polynômes u, v de degrés $n-q$, $m-q$ tels que le polynôme $uf+vg$ soit identiquement nul. Égalons d'abord à zéro les coefficients des termes des degrés m, $m+1$, ..., $m+n-q$. Or le coefficient de x^{m+n-h}, h désignant l'un quelconque des entiers q, $q+1$, ..., n, est

$$\begin{aligned} &a_{m+q-h}\alpha_{n-q} + \ldots + a_{m-1}\alpha_{n-h+1} + a_m\alpha_{n-h} \\ &+ b_{n+q-h}\beta_{m-q} + \ldots + b_{n-1}\beta_{m-h+1} + b_n\beta_{m-h}, \end{aligned}$$

ou, d'après les équations U, V de la quatrième remarque préliminaire,

$$\begin{aligned} &(\lambda_0+\mu_0)(a_{m+q-h}\,b_n + \ldots + a_m b_{n+q-h}) \\ &+(\lambda_1+\mu_1)(a_{m+q-h+1}b_n + \ldots + a_m b_{n+q-h+1}) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &+(\lambda_{h-q}+\mu_{h-q})a_m b_n. \end{aligned}$$

En égalant à zéro les valeurs que prend cette expression, quand on y donne successivement à h les valeurs q, $q+1$, ..., n, on aura des équations de la forme

$$\begin{aligned} &(\lambda_0+\mu_0)a_m b_n &&= 0, \\ &(\lambda_0+\mu_0)\mathrm{H}_1 + (\lambda_1+\mu_1)a_m b_n &&= 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &(\lambda_0+\mu_0)\mathrm{H}_{n-q} + \ldots\ldots\ldots\ldots + (\lambda_{n-q}+\mu_{n-q})a_m b_n &&= 0, \end{aligned}$$

H_1, H_2, ..., H_{n-q}, ... étant des coefficients déterminés. Mais on a

$$a_m b_n \gtrless 0;$$

ce système exige donc

$$\mu_0 = -\lambda_0, \qquad \mu_1 = -\lambda_1, \qquad \ldots \qquad \mu_{n-q} = -\lambda_{n-q}.$$

En tenant compte de ce premier résultat, le polynôme $uf + vg$ devient

$$\begin{aligned} &\lambda_0(g_{q-1}f - f_{q-1}g) + \lambda_1(g_q f - f_q g) + \dots \\ &+ \lambda_{n-q}(g_{n-1}f - f_{n-1}g) + \lambda_{n-q+1}g \\ &+ \lambda_{n-q+2}xg + \dots + \lambda_{m-q}x^{m-n-1}g, \end{aligned}$$

ou bien

$$\begin{aligned} &\lambda_0(c_{q-1,0} + c_{q-1,1}x + \dots) \\ &+ \lambda_1(c_{q,0} + c_{q,1}x + \dots) \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ &+ \lambda_{n-q}(c_{n-1,0} + c_{n-1,1}x + \dots) \\ &- \lambda_{n-q+1}(b_0 + b_1 x + \dots + b_n x^n) \\ &+ \lambda_{n-q+2}(\quad b_0 x + \dots + b_{n-1}x^n + b_n x^{n+1}) \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &+ \lambda_{m-q}\ (\quad b_0 x^{m-n-1} + \dots\dots\dots\dots\dots + b_n x^{m-1}). \end{aligned}$$

Il reste actuellement à égaler à zéro les coefficients de $x^0, x, x^2, \dots, x^{m-1}$, ce qui donne le système désigné précédemment par s_q. Ce système doit avoir par rapport aux λ une solution où λ_0 ait une valeur non nulle. Il en est de même du système $s_{q,q-1}$; par suite, le déterminant de ce système, qui est r_{q-1} d'après la première remarque préliminaire, est nul. Et comme ceci a lieu en donnant à q successivement les valeurs $1, 2, \dots, p$, on a les conditions

$$r_0 = r_1 = r_2 = \dots = r_{p-1} = 0.$$

En outre, d'après le lemme III et en vertu de la quatrième remarque préliminaire, le système $s_{p,p}$ admet pour les λ une solution où λ_0 n'est pas nul; et, par suite, si l'on donne à λ_0 une valeur arbitraire non nulle, il admet pour les autres λ une solution finie unique, en sorte que le déterminant des coefficients de ces inconnues est différent de zéro. Mais, d'après la deuxième remarque

préliminaire, ce déterminant est r_p. On a donc

$$r_p \gtrless 0.$$

Les conditions énoncées sont, par conséquent, nécessaires.

Elles sont suffisantes; car, si θ était de degré inférieur à p, le premier déterminant r_i non nul aurait un indice inférieur à p, et si θ était de degré supérieur à p, le premier déterminant r_i non nul aurait un indice supérieur à p, résultats contraires l'un et l'autre aux hypothèses. Donc θ est de degré p.

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

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

Dans la démonstration du théorème précédent, on a déjà prouvé la nécessité des conditions $r_{p-1} = 0$ et $r_p \gtrless 0$, au cas où θ est de degré p. Il faut en outre, d'après le lemme III, que chacun des systèmes

$$s^j_{p,p-1} \; (j = 1, 2, \ldots, p-1)$$

ait une solution où les inconnues ne soient pas toutes nulles (puisque λ_0 est différent de zéro) : or cela exige que les déterminants de ces systèmes, qui, d'après la troisième remarque préliminaire, sont $r_{p-1,1}, r_{p-1,2}, \ldots, r_{p-1,p-1}$ soient nuls. Les conditions énoncées sont donc nécessaires.

Elles sont suffisantes. En effet, en les supposant remplies, il existe un couple et un seul de polynômes u, v de degrés $n-p$ et $m-p$, tels que $uf + vg$ soit identiquement nul (en faisant abstraction d'un facteur constant arbitraire pour u et v), et, par suite (lemme IV), θ est de degré p.

Expression du plus grand commun diviseur θ *de* f *et* g. — On suppose remplies les conditions énoncées soit dans le théorème I, soit dans le théorème II. Cela étant, on va chercher deux polynômes déterminés u et v, tels que $uf + vg$ soit un polynôme de degré p : ce polynôme sera le plus grand commun diviseur cherché θ.

Dans les polynômes u et v, pris sous la forme spéciale qu'autorise la quatrième remarque préliminaire, adoptons pour q la valeur $p+1$, puis posons

$$\theta \equiv \gamma_0 + \gamma_1 x + \ldots + \gamma_{p-1} x^{p-1} + x^p,$$

et identifions les polynômes $uf + vg$ et θ. On obtient ainsi un système d'équations qu'on peut décomposer en deux groupes : le premier groupe A se déduit du groupe des $p+1$ premières équations du système s_{p+1}, en retranchant respectivement à leurs premiers membres γ_0, γ_1, ..., γ_{p-1} ; le second groupe B est le groupe $s_{p+1,p}$, où l'on a simplement retranché l'unité au premier membre de la première équation.

L'équation donnant γ_j, où j a pour valeur l'un quelconque des nombres 0, 1, 2, ..., $p-1$, s'obtiendra en éliminant les λ entre la $(j+1)^{\text{ième}}$ équation du groupe A et les équations du système B. Le résultat de l'élimination s'obtient en égalant à zéro le déterminant complet d de ce système, ce qui donne

$$d = \begin{vmatrix} c_{p,j} & c_{p+1,j} & \ldots & c_{n-1,j} & b_j & b_{j-1} & \ldots & -\gamma_j \\ c_{p,p} & c_{p+1,p} & \ldots & c_{n-1,p} & b_p & b_{p-1} & \ldots & -1 \\ c_{p,p+1} & c_{p+1,p+1} & \ldots & c_{n-1,p+1} & b_{p+1} & b_p & \ldots & 0 \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot \\ c_{p,m-1} & c_{p+1,m-1} & \ldots & c_{n-1,m-1} & \ldots\ldots\ldots\ldots & & & b_n 0 \end{vmatrix} = 0.$$

Or le déterminant obtenu en supprimant dans d la der-

nière colonne et la première ligne est celui du groupe $s_{p+1,p}$, c'est-à-dire r_p d'après la première remarque préliminaire. Le déterminant obtenu en supprimant la dernière colonne et la seconde ligne de d est celui du système $s^{j+1}_{p+1,p}$ ($j = 0, 1, 2, \ldots, p-1$), c'est-à-dire $r_{p,j+1}$ en vertu de la troisième remarque préliminaire. En développant d par rapport aux éléments de la dernière colonne, l'équation $d = 0$ peut donc s'écrire

$$\gamma_j r_p - r_{p,j+1} = 0,$$

d'où

$$\gamma_j = \frac{r_{p,j+1}}{r_p}.$$

On peut donc enfin énoncer le théorème suivant :

Théorème III. — *Quand f et g ont un plus grand commun diviseur θ de degré p, ce polynôme est donné par l'identité*

$$r_p \theta \equiv r_{p,1} + r_{p,2} x + r_{p,3} x^2 + \ldots + r_{p,p} x^{p-1} + r_p x^p.$$