Ch. Biehler

Sur l’élimination par la méthode d’Euler

Nouvelles annales de mathématiques 3e série, tome 6 (1887), p. 67-75

<http://www.numdam.org/item?id=NAM_1887_3_6__67_1>

SUR L'ÉLIMINATION PAR LA MÉTHODE D'EULER;

PAR M. CH. BIEHLER.

1. On sait que, si $F(x, y)$ et $G(x, y)$ sont deux polynômes homogènes en x et y, de degrés respectifs m et p, si $\Delta(x, y)$ est le plus grand commun diviseur de ces deux polynômes, $\Delta(x, y)$ est de la forme

$$\Delta(x, y) = U\,G(x, y) + V\,F(x, y),$$

U et V étant des polynômes entiers et homogènes en x et y.

On le voit immédiatement en observant que les restes successifs obtenus dans les opérations qui conduisent au plus grand commun diviseur Δ sont tous de cette forme.

Cela posé, on démontre aisément que, si $F(x, y)$ divise un produit de deux polynômes $G(x, y) \times H(x, y)$ et s'il est premier avec $G(x, y)$, il divise $H(x, y)$; les polynômes F, G et H sont homogènes.

En effet, les deux polynômes $F(x, y)$ et $G(x, y)$ étant premiers entre eux, on pourra trouver deux polynômes U et V, tels que

$$U\,G(x, y) + V\,F(x, y) = 1;$$

par suite,

$$U\,G(x, y) \times H(x, y) + V\,F(x, y) \times H(x, y) = H(x, y).$$

$F(x, y)$ divise, par hypothèse, le produit

$$G(x, y) \times H(x, y);$$

il divise donc les deux parties du premier membre et par suite il divise $H(x, y)$.

Cette proposition va nous permettre de démontrer le théorème d'Euler, à savoir :

La condition nécessaire et suffisante pour que deux polynômes $F(x, y)$, $G(x, y)$ homogènes aient un diviseur commun en x et y, c'est qu'il existe deux polynômes U et V de degrés respectivement moindres que F et G, tels que l'on ait identiquement

$$U\, G(x, y) + V\, F(x, y) = 0.$$

La condition est nécessaire ; car, si $F(x, y)$ et $G(x, y)$ ont un diviseur commun Θ, on aura

$$F(x, y) = \Theta F_1(x, y),$$
$$G(x, y) = \Theta G_1(x, y)$$

et, par suite,

$$F_1(x, y)\, G(x, y) - G_1(x, y)\, F(x, y) = 0,$$

ce qui fait voir que la condition est nécessaire.

Elle est suffisante ; car, si elle est remplie, on aura

$$U\, G(x, y) = -V\, F(x, y)$$

Si $F(x, y)$ et $G(x, y)$ étaient premiers entre eux, $F(x, y)$ divisant le produit $U\, G(x, y)$ et étant premier avec $G(x, y)$ devrait diviser U qui est de degré inférieur à F ; les polynômes $F(x, y)$ et $G(x, y)$ ne pouvant être premiers entre eux admettent un plus grand commun diviseur de degré supérieur à zéro.

On peut montrer de plus que, si U et V sont respectivement de degrés $m - \lambda$ et $p - \lambda$, les fonctions $F(x, y)$, $G(x, y)$ admettent un plus grand commun diviseur qui est de degré λ au moins.

Supposons, en effet, que le facteur commun à $F(x, y)$ et à $G(x, y)$ soit de degré λ' plus petit que λ.

$$F(x, y) = \theta F_1(x, y),$$
$$G(x, y) = \theta G_1(x, y).$$

$F_1(x, y)$ sera de degré $m - \lambda'$; $G_1(x, y)$, de degré $p - \lambda'$, et l'on aura

$$U G_1(x, y) + V F_1(x, y) = 0;$$

U et V étant de degrés respectivement inférieurs à F_1 et à G_1, les polynômes F_1 et G_1 ne sauraient être premiers entre eux; il existe donc un facteur commun à $F(x, y)$ et à $G(x, y)$ de degré au moins égal à λ.

2. Nous allons étudier maintenant quelques propriétés des polynômes U et V qui nous seront utiles dans la suite.

I. *Si les polynômes* $F(x, y)$, $G(x, y)$ *n'admettent pour plus grand commun diviseur qu'une fonction du premier degré* $\beta x - \alpha y$, *les polynômes* U *et* V, *qui fournissent l'identité d'Euler, sont premiers entre eux,* U *et* V *étant de degrés* $m - 1$, $p - 1$.

En effet, si U et V admettaient un facteur commun Θ, on aurait

$$U = \theta U_1,$$
$$V = \theta V_1,$$

et, par suite, l'identité

$$U G(x, y) + V F(x, y) = 0,$$

devenant

$$U_1 G(x, y) + V_1 F(x, y) = 0,$$

nous montre que $F(x, y)$ et $G(x, y)$ admettent un plus grand commun diviseur de degré supérieur au premier, ce qui est contraire à l'hypothèse faite sur F et G.

II. *Si les deux polynômes* $F(x, y)$, $G(x, y)$ *n'admettent pour plus grand commun diviseur qu'une fonction du premier degré de la forme* $\beta x - \alpha y$, *il n'existe qu'un seul système de polynômes* U *et* V *satisfaisant à l'identité d'Euler*, U *et* V *étant, comme précédemment, de degrés* $m - 1$ *et* $p - 1$.

Supposons, en effet, qu'il existe deux systèmes U et V, U_1 et V_1 donnant les identités

$$U\,G(x, y) + V\,F(x, y) = 0,$$
$$U_1 G(x, y) + V_1 F(x, y) = 0;$$

on en tirera

$$(UV_1 - VU_1)\,G(x, y) = 0$$

ou

$$UV_1 - VU_1 = 0.$$

Les polynômes U et V, d'après le théorème précédent, sont premiers entre eux; par suite, U doit diviser U_1 et l'on a

$$U = \lambda U_1:$$

d'où

$$V = \lambda V_1,$$

λ étant une constante : le système (U_1, V_1) est donc identique au système (U, V).

III. *S'il existe plus d'un système de polynômes* U *et* V *de degrés* $m - 1$ *et* $p - 1$ *satisfaisant à l'identité d'Euler, les polynômes* $F(x, y)$, $G(x, y)$ *admettent un plus grand commun diviseur de degré supérieur à un.*

Cela résulte immédiatement du théorème précédent, car U et V ne sauraient dans ce cas être premiers entre eux, à cause de l'égalité

$$UV_1 - VU_1 = 0,$$

qui nous ferait voir que les deux systèmes (U, V), (U_1, V_1) rentrent dans un seul. U et V admettant un plus grand commun diviseur Θ, qui est au moins du premier degré, on a

$$U = \Theta U_2,$$
$$V = \Theta V_2,$$

et l'identité

$$U_2 G(x, y) + V_2 F(x, y) = 0$$

nous montre que $F(x, y)$ et $G(x, y)$ admettent un plus grand commun diviseur de degré supérieur à un.

IV. *S'il n'existe qu'un seul système de polynômes* U *et* V *de degrés respectifs* $m - 1$ *et* $p - 1$, *qui donnent l'identité d'Euler, les polynômes* $F(x, y)$, $G(x, y)$ *n'admettent qu'un facteur linéaire commun.*

Cette proposition est une conséquence immédiate des précédentes ; car, si les polynômes $F(x, y)$, $G(x, y)$ admettaient un plus grand commun diviseur de degré λ, λ étant plus grand que un, on aurait

$$F(x, y) = \Theta F_1(x, y),$$
$$G(x, y) = \Theta G_1(x, y),$$

et, par suite,

$$F_1(x, y)\, G(x, y) - G_1(x, y)\, F(x, y) = 0.$$

En multipliant les deux membres par un polynôme arbitraire Φ de degré $\lambda - 1$, on obtiendrait une infinité de fonctions de degrés $m - 1$ et $p - 1$, à savoir

$$\Phi F_1(x, y) \quad \text{et} \quad \Phi G_1(x, y),$$

qui satisferaient à l'identité d'Euler, ce qui est contraire à l'hypothèse.

3. Cherchons maintenant en fonction des coefficients de $F(x, y)$ et de $G(x, y)$ la condition nécessaire et suffisante pour que les polynômes $F(x, y)$ et $G(x, y)$ aient un facteur commun.

Il faudra, d'après ce qui précède, qu'en posant

$$U = \alpha_0 x^{m-1} + \alpha_1 x^{m-2} y + \ldots + \alpha_{m-1} y^{m-1},$$
$$V = \beta_0 x^{p-1} + \beta_1 x^{p-2} y + \ldots + \beta_{p-1} y^{p-1},$$

on ait identiquement, pour des valeurs convenables des coefficients α et β,

$$U\,G(x. y) + V\,F(x, y) = 0.$$

Si

$$F(x, y) = A_0 x^m + A_1 x^{m-1} y + \ldots + A_m y^m,$$
$$G(x, y) = B_0 x^p + B_1 x^{p-1} y + \ldots + B_p y^p;$$

en égalant à zéro les coefficients de $x^{m+p-1}, x^{m+p-2}y, \ldots, y^{m+p-1}$, on aura les équations

$$\begin{array}{lll} B_0\alpha_0 & + A_0\beta_0 & = 0, \\ B_1\alpha_0 + B_0\alpha_1 + \ldots & + A_1\beta_0 + A_0\beta_1 & = 0, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots, \\ \qquad B_p\alpha_{m-1} & + A_m\beta_{p-1} & = 0. \end{array}$$

Ces équations, au nombre de $m+p$, sont linéaires et homogènes par rapport aux $m+p$ inconnues $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}, \beta_0, \beta_1, \ldots, \beta_{p-1}$.

Elles doivent admettre pour ces quantités des valeurs qui ne sont pas toutes nulles; il faut par suite que le déterminant d'ordre $m+p$ de leurs coefficients soit égal à zéro. Soit Δ ce déterminant,

$$\Delta = \begin{vmatrix} B_0 & 0 & 0 & \ldots & 0 & A_0 & 0 & \ldots & 0 \\ B_1 & B_0 & 0 & \ldots & . & A_1 & A_0 & \ldots & 0 \\ \ldots & \ldots & . & \ldots & . & \ldots & \ldots & \ldots & . \\ 0 & \ldots & . & \ldots & B_p & 0 & \ldots & \ldots & A_m \end{vmatrix}.$$

$\Delta = 0$ est la condition nécessaire pour que les deux fonctions $F(x, y)$, $G(x, y)$ aient un facteur commun au moins du premier degré.

Je vais démontrer que cette condition est dans tous les cas suffisante.

Supposons que $\Delta = 0$ et que l'un des déterminants d'ordre $m+p-1$, mineur de Δ, ne soit pas nul. On pourra donner à l'une des inconnues $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$, $\beta_0, \beta_1, \ldots, \beta_{p-1}$ une valeur arbitraire et choisir $m+p-1$ des équations, de telle sorte que le déterminant des inconnues qui y figurent ne soit pas nul ; ce sera le mineur que nous avons supposé différent de zéro ; les équations déterminent pour les $m+p-1$ inconnues qui y figurent des valeurs de la forme

$$\begin{array}{ll} \alpha_0 = \lambda_0 \alpha, & \beta_0 = \mu_0 \alpha, \\ \alpha_1 = \lambda_1 \alpha, & \beta_1 = \mu_1 \alpha, \\ \ldots\ldots\ldots, & \ldots\ldots\ldots, \\ \alpha_{m-1} = \lambda_{m-1} \alpha, & \beta_{p-1} = \mu_{p-1} \alpha, \end{array}$$

où α désigne la valeur de l'inconnue choisie arbitrairement et $\lambda_0, \lambda_1, \ldots, \lambda_{m-1}, \mu_0, \mu_1, \ldots, \mu_{p-1}$ des quantités parfaitement déterminées qui ne sont pas toutes nulles, l'une d'elles étant égale à l'unité.

Les fonctions U et V sont donc

$$\begin{aligned} U &= \alpha(\lambda_0 x^{m-1} + \lambda_1 x^{m-1} y + \ldots + \lambda_{m-1} y^{m-1}), \\ V &= \alpha(\mu_0 x^{p-1} + \mu_1 x^{p-1} y + \ldots + \mu_{p-1} y^{p-1}); \end{aligned}$$

abstraction faite du facteur α, elles donnent le système unique de fonctions de degrés $m-1$ et $p-1$ satisfaisant à l'identité

$$U\,G(x, y) + V\,F(x, y) = 0.$$

La solution précédente étant la plus générale pour les quantités $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}, \beta_0, \beta_1, \ldots, \beta_{m-1}$, il s'ensuit que, si un mineur d'ordre $m+p-1$ de Δ est différent de zéro, il n'existe qu'un seul système de polynômes d'ordre $m-1$ et $p-1$ donnant l'identité d'Euler, et, par suite, d'après les théorèmes précédents, les deux fonctions $F(x, y)$ et $G(x, y)$ admettent pour plus grand commun diviseur une fonction du premier degré seulement.

Ce qui précède montre évidemment que les fonctions U et V sont effectivement de degrés $m - 1$ et $p - 1$; car λ_0 et μ_0 ne sauraient être nuls, les polynômes U et V s'abaisseraient aux degrés $m - 2$ et $p - 2$ au moins, et, en les multipliant par un polynôme arbitraire du premier degré, on obtiendrait une infinité de fonctions U et V de degrés $m - 1$ et $p - 1$ qui satisferaient à l'identité d'Euler, ce qui n'est pas possible d'après ce qui précède.

On voit donc que, si $\Delta = 0$ *et si un mineur d'ordre* $m + p - 1$ *de* Δ *est différent de zéro, les deux fonctions* $F(x, y)$ *et* $G(x, y)$ *admettent pour plus grand commun diviseur une fonction qui n'est que du premier degré.*

Si tous les déterminants d'ordre $m + p - 1$, mineurs de Δ, sont nuls, et si un déterminant d'ordre $m + p - 2$, mineur de Δ, n'est pas nul, la solution la plus générale du système des équations en $\alpha_0, \alpha_1, \ldots, \beta_0, \beta_1 \ldots$ est de la forme

$$\begin{array}{ll} \alpha_0 = \lambda_0 \alpha + \lambda'_0 \alpha', & \beta_0 = \mu_0 \alpha + \mu'_0 \alpha', \\ \alpha_1 = \lambda_1 \alpha + \lambda'_1 \alpha', & \beta_1 = \mu_1 \alpha + \mu'_1 \alpha', \\ \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots, \\ \alpha_{m-1} = \lambda_{m-1} \alpha + \lambda'_{m-1} \alpha' ; & \beta_{p-1} = \mu_{p-1} \alpha + \mu'_{p-1} \alpha', \end{array}$$

où α et α' sont des arbitraires, $\lambda_0, \ldots, \lambda'_0, \ldots, \mu_0, \ldots, \mu'_0, \ldots$ des quantités parfaitement déterminées, qui ne sont pas toutes nulles.

Dans ce cas, les fonctions U et V prennent la forme

$$\begin{aligned} U &= \alpha U_1 + \alpha' U'_1, \\ V &= \alpha V_1 + \alpha' V'_1, \end{aligned}$$

U_1, U'_1, V_1, V'_1 étant des polynômes bien déterminés.

Il existe, dans ce cas, une infinité de fonctions U et V qui donnent l'identité d'Euler; par suite, d'après ce qui précède, $F(x,y)$ et $G(x,y)$ ont un plus grand commun diviseur, qui est au moins du deuxième degré.

On voit que U et V sont en nombre infini; car U_1 et V_1 ne peuvent pas être identiquement nuls à la fois, pas plus que U'_1 et V'_1, puisque, dans l'expression de $\alpha_0, \alpha_1, \ldots, \beta_0, \beta_1, \ldots$, un coefficient de α est égal à l'unité, ainsi qu'un coefficient de α'.

On voit donc que, si $\Delta = 0$ et si tous les mineurs d'ordre $m+p-1$ de Δ sont nuls, les fonctions $F(x,y)$, $G(x,y)$ admettent un facteur commun qui est au moins du second degré.

Il en serait de même si l'ordre du premier des mineurs qui ne s'annule pas s'abaissait au-dessous de l'ordre $m+p-2$.