Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 2 (1900)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THÉORÈMES DE BEZOUT ET D'EULER

Autor: Poussart, A.

DOI: https://doi.org/10.5169/seals-3558

THÉORÈMES DE BEZOUT ET D'EULER

L'établissement de la formule $AU + BV = R_n$ et l'évaluation des degrés des polygones U et V se font généralement d'une façon lourde et pénible ; je me propose de donner une démonstration plus rapide et beaucoup plus facile à présenter.

A polynôme de degré m, B de degré p, $m > p$. La recherche du plus grand commun diviseur donne les identités

$$(1) \qquad \left\{ \begin{array}{l} A = BQ + R \\ B = RQ_1 + R_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ R_{n-2} = R_{n-1} Q_n + R_n \end{array} \right.$$

ou

$$(2) \qquad \left\{ \begin{array}{r} R = A - BQ \\ R_1 + RQ_1 = B \\ R_2 + R_1Q_2 - R = 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ R_n + R_{n-1} Q_n - R_{n-2} \ldots\ldots = 0 \end{array} \right.$$

1° $AU + BV = R_n$, U et V polynômes entiers.

Je résous le système (2) par rapport à R_n ; le déterminant des inconnues est $\pm$ I.

$$(3) \qquad \pm R_n = \left| \begin{array}{llll} A - BQ\ 0\ 0\ 0 & \ldots\ldots & & 1 \\ B & 0\ 0 \ldots\ldots & & 1\ Q_1 \\ 0 & \ldots\ldots\ldots\ldots & & 1\ Q_2 - 1 \\ 0 & \ldots\ldots\ldots\ldots & & 1\ Q_3 - 1\ 0 \\ \ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots \\ \ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots \\ 0\ Q_n - 1\ 0 & \ldots\ldots\ldots\ldots & \ldots & \ldots \end{array} \right|$$

d'où

$$R_n = AU + BV.$$

2° Si R_n est de degré q, U est de degré $p-q-1$ au plus et V de degré $m-q-1$ au plus.

Le terme de degré le plus élevé dans U est contenu dans $Q_1 Q_2 \ldots Q_n$, celui de V dans $QQ_1 \ldots Q_n$; je multiplie membre à membre les identités (1).

$$ABRR_1 \ldots R_{n-2} = BRR_1 \ldots R_{n-1} QQ_1 \ldots Q_n + \ldots$$

Si on tient compte des facteurs communs aux premiers termes des deux membres, on voit que $QQ_1 \ldots Q_n R_{n-1}$ est du degré de A. Or R_n est de degré q, R_{n-1} est donc au moins de degré $q+1$, par suite $QQ_1 \ldots Q_n$ est au plus de degré $m-q-1$ et comme Q est de degré $m-p$, $Q_1 Q_2 \ldots Q_n$ est au plus de degré $p-q-1$.

CONSÉQUENCES

I. Si R_n est le plus grand commun diviseur, U et V sont premiers entre eux,

R_n contient les facteurs communs à A et B et ne contient qu'eux, donc U et V ne peuvent avoir de facteur commun.

II. Les polynômes U et V sont les seuls polynômes de degré $p-q-1$, $m-q-1$ ou de degré inférieur vérifiant la relation $AU + BV = R_n$:

Si on avait

$$AU_1 + BV_1 \equiv Rn$$

on en conclurait :

$$A(u - U_1) \equiv B(V_1 - V).$$

Or A et B ont q facteurs communs, donc les $m-q$ autres facteurs de A devraient diviser $V_1 - V$ qui est de degré $m-q-1$ au plus.

III. *Théorème de Bezout.* — $AU + BV = 1$. — Si A et B sont premiers entre eux, q degré du plus grand commun diviseur est nul, divisant par R_n,

$$AU + BV = 1.$$

Les théorèmes I et II s'appliquent encore à U et V.

IV. *Théorème d'Euler.* — La condition nécessaire et suffisante pour que A et B aient un plus grand commun diviseur de degré q, est qu'on puisse trouver deux polynômes premiers entre eux, U de degré $p-q$, V de degré $m-q$ et tels que :

$$AU + BV = 0.$$

1° La condition est nécessaire. Supposons $R_n = 0$, l'identité fondamentale devient

$$AU + BV = 0.$$

Le plus grand commun diviseur est alors R_{n-1} qui est degré q, il en résulte d'après le n° 2 que U est de degré $p-q$ et V de degré $m-q$.

U et V sont premiers entre eux, car s'ils avaient un commun diviseur du premier degré, on aura après l'avoir supprimé :

$$AU_1 + BV_1 = 0$$
$$U_1 \text{ de degré } p-q-1 \qquad V_1 \text{ de degré } m-q-1.$$

En admettant que les $p-q-1$ facteurs de U_1 appartiennent à B, il y aurait encore $q+1$ facteurs de B qui devraient appartenir à A, ce qui est contre l'hypothèse.

2° La condition est suffisante. V de degré $m-q$ est premier avec U, donc ses $m-q$ facteurs appartiennent à A et il reste q facteurs de A qui appartiennent à B.

A. Poussart (Paris).