JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

W. RIVIER

Sur un théorème fondamental de l'Algèbre

Journal de mathématiques pures et appliquées 9e série, tome 10 (1931), p. 213-218.

<http://www.numdam.org/item?id=JMPA_1931_9_10__213_0>

Sur un théorème fondamental de l'Algèbre;

PAR W. RIVIER.

Nous nous proposons de démontrer à nouveau le théorème suivant :

L'équation

$$(1) \qquad \sum_{\mu=1}^{\mu=m} \sum_{\nu=1}^{\nu=n} a_{\mu\nu} x_\mu y_\nu = (a_{11}, a_{12}, \ldots, a_{mn}),$$

où $a_{11}, a_{12}, \ldots, a_{mn}$ représentent des coefficients entiers, est résoluble en nombres entiers ([1]).

Voici d'abord quelques observations destinées à rappeler l'importance de ce théorème.

En satisfaisant de la manière envisagée à l'équation (1), on satisfait du même coup à l'équation

$$(2) \qquad \left(\sum_{\mu=1}^{\mu=m} a_{\mu 1} x_\mu, \sum_{\mu=1}^{\mu=m} a_{\mu 2} x_\mu, \ldots, \sum_{\mu=1}^{\mu=m} a_{\mu n} x_\mu\right) = (a_{11}, \ldots, a_{mn}).$$

Il s'ensuit que, si l'on réussit à établir que toute équation de la forme (1) possède la propriété d'être résoluble en nombres entiers, cette propriété s'étendra d'elle-même aux équations de la forme

$$(3) \qquad \sum_{\mu=1}^{\mu=m} \sum_{\nu=1}^{\nu=n} \sum_{\rho=1}^{\rho=r} a_{\mu\nu\rho} x_\mu y_\nu z_\rho = (a_{111}, \ldots, a_{mnr}),$$

([1]) La notation $(a, b, c, \ldots)$, où $a, b, c, \ldots$ désignent des nombres entiers, représente le plus grand commun diviseur des nombres $a, b, c \ldots$.

puis, de ces équations, à celles de la forme

$$(4)\qquad \sum_{\mu=1}^{\mu=m}\sum_{\nu=1}^{\nu=n}\sum_{\rho=1}^{\rho=r}\sum_{\sigma=1}^{\sigma=s} a_{\mu\nu\rho\sigma}x_\mu y_\nu z_\rho u_\sigma = (a_{1111}, \ldots, a_{mnrs}),$$

et ainsi de suite. La résolution de l'équation (3) peut en effet se ramener à la résolution d'une équation de la forme (2), suivie de celle d'une équation de la forme (1), la résolution de l'équation (4) à celle d'une équation de la forme (2), suivie de celle d'une équation de la forme (3), etc. En particulier, si l'on se donne n entiers premiers entre eux, il sera toujours possible de leur adjoindre $n(n-1)$ autres entiers tels que l'on puisse, avec tous ces entiers, former un déterminant d'ordre n, de valeur égale à 1, qui admette les n entiers donnés comme éléments d'une même colonne. C'est en partie sur ce dernier résultat, en partie directement sur le théorème proposé, que repose le théorème d'existence de la forme réduite

$$e_1 x_1 y_1 + e_2 x_2 y_2 + \ldots$$

d'une forme bilinéaire à coefficients entiers (1).

Pour démontrer le théorème proposé (2), nous nous appuierons sur deux lemmes.

Lemme I. — *L'équation*

$$(5)\qquad u(ax+by)+v(\alpha x+\beta y)=(a, b, \alpha, \beta),$$

où a, b, α et β représentent des coefficients entiers, est résoluble en nombres entiers. (En d'autres termes : le théorème proposé est vrai pour $m=2$, $n=2$.)

Démonstration du lemme I. — Posons

$$(a, b)=d, \qquad (\alpha, \beta)=\delta.$$

(1) *Voir* Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten* (*Journ. de Crelle*, t. 86, p. 157 et suiv.).

(2) Pour d'autres démonstrations de ce théorème, *voir* notamment : Frobenius, *ibid.*, p. 151 et suiv.

Soient r et s deux entiers tels que l'on ait

$$ar + bs = d. \tag{6}$$

La solution générale de l'équation

$$ax + by = d$$

est alors donnée par les relations

$$x = r + \frac{b}{d}k, \qquad y = s - \frac{a}{d}k, \tag{7}$$

où k représente un entier arbitraire.

Portons ces valeurs de x et de y dans la forme $\frac{\alpha}{\delta}x + \frac{\beta}{\delta}y$. Nous obtenons identiquement :

$$\frac{\alpha}{\delta}x + \frac{\beta}{\delta}y = \mathrm{M}k + \mathrm{N},$$

en posant

$$\frac{b}{d}\frac{\alpha}{\delta} - \frac{a}{d}\frac{\beta}{\delta} = \mathrm{M}, \qquad r\frac{\alpha}{\delta} + s\frac{\beta}{\delta} = \mathrm{N}. \tag{8}$$

Résolvons par rapport à $\frac{\alpha}{\delta}$ et à $\frac{\beta}{\delta}$ le système des relations (8). En tenant compte de (6), nous trouvons :

$$\frac{\alpha}{\delta} = s\mathrm{M} + \frac{a}{d}\mathrm{N}, \qquad \frac{\beta}{\delta} = -r\mathrm{M} + \frac{b}{d}\mathrm{N}.$$

De ces relations, et du fait que les entiers $\frac{\alpha}{\delta}$ et $\frac{\beta}{\delta}$ sont premiers entre eux, découle que M et N sont des entiers premiers entre eux. Il en résulte qu'on pourra choisir k de manière que $\mathrm{M}k + \mathrm{N}$ soit premier avec d; il suffira, en effet, de prendre $k = 0$, si tout diviseur premier de d entre dans M, sinon, k égal à l'une des solutions de la congruence

$$\mathrm{M}k + \mathrm{N} \equiv 1 \pmod{\mathrm{P}},$$

où P désigne le produit des diviseurs premiers de d qui n'entrent pas dans M. L'entier k étant ainsi choisi, soient x_0 et y_0 les valeurs correspondantes de x et de y, fournies par les relations (7); il viendra :

$$(ax_0 + by_0, \alpha x_0 + \beta y_0) = (d, (\mathrm{M}k + \mathrm{N})\delta) = (d, \delta) = (a, b, \alpha, \beta). \tag{9}$$

Soient alors u_0 et v_0 deux entiers satisfaisant à la condition

$$(10) \qquad u_0(ax_0+by_0)+v_0(\alpha x_0+\beta y_0)=(ax_0+by_0,\ \alpha x_0+\beta y_0).$$

En vertu de (9) et de (10), les quatre entiers x_0, y_0, u_0 et v_0 formeront un système de solutions de l'équation (5).

Le lemme I est ainsi démontré.

Nous désignerons dorénavant par $F(x_1, \ldots, x_m; y_1, \ldots, y_n)$, ou, plus simplement, par F, l'expression $\sum\limits_{\mu=1}^{\mu=m}\sum\limits_{\nu=1}^{\nu=n} a_{\mu\nu}x_\mu y_\nu$.

Lemme II. — *Si l'on peut résoudre séparément en nombres entiers chacune des deux équations*

$$(11) \qquad F=d',$$

$$(12) \qquad F=d'',$$

où d' et d'' représentent deux entiers donnés, on peut aussi résoudre en nombres entiers la suivante :

$$(13) \qquad F=(d', d'').$$

Démonstration du lemme II. — Supposons, en effet, deux systèmes de valeurs entières de $x_1, \ldots, y_n$:

$$\begin{cases} x_\mu = x'_\mu, \\ y_\nu = y'_\nu, \end{cases} \qquad \begin{cases} x_\mu = x''_\mu, \\ y_\nu = y''_\nu. \end{cases}$$
$$(\mu = 1, 2, \ldots, m;\ \nu = 1, 2, \ldots, n).$$

satisfaisant, le premier, à l'équation (11), le second, à l'équation (12). Posons

$$\Phi(u_1, u_2; v_1, v_2)=\sum_{\mu=1}^{\mu=m}\sum_{\nu=1}^{\nu=n} a_{\mu\nu}(u_1x'_\mu+u_2x''_\mu)(v_1y'_\nu+v_2y''_\nu).$$

On pourra écrire identiquement

$$\Phi=\sum_{\mu=1}^{\mu=2}\sum_{\nu=1}^{\nu=2} A_{\mu\nu}u_\mu v_\nu,$$

les A désignant des entiers déterminés. On pourra donc, en vertu du lemme I, résoudre en nombres entiers l'équation

$$\Phi = (A_{11}, A_{12}, A_{21}, A_{22}),$$

et aussi, par conséquent, la suivante:

$$(14) \qquad \Phi = (d', d''),$$

puisque, en vertu des relations

$$\Phi(1, 0; 1, 0) = d', \qquad \Phi(0, 1; 0, 1) = d'',$$

vérifiées par hypothèse, (d', d'') est divisible par $(A_{11}, A_{12}, A_{21}, A_{22})$.

Soit donc

$$u_1 = p, \qquad u_2 = q, \qquad v_1 = r, \qquad v_2 = s$$

un système de valeurs entières de u_1, u_2, v_1 et v_2 satisfaisant à l'équation (14). Les valeurs entières de $x_1, \ldots, y_n$:

$$x_\mu = p x'_\mu + q x''_\mu, \qquad y_\nu = r y'_\nu + s y''_\nu \qquad (\mu = 1, 2, \ldots, m; \nu = 1, 2, \ldots, n),$$

constitueront un système de solutions de l'équation (13).

Le lemme II est ainsi démontré.

Démonstration du théorème proposé. — Posons

$$\Delta_\mu = (a_{\mu 1}, a_{\mu 2}, \ldots, a_{\mu n}) \qquad (\mu = 1, 2, \ldots, m).$$

On peut évidemment résoudre séparément en nombres entiers chacune des m équations

$$F = \Delta_\mu \qquad (\mu = 1, 2, \ldots, m).$$

En vertu du lemme II, on pourra donc résoudre en nombres entiers l'équation

$$(15) \qquad F = (\Delta_1, \Delta_2).$$

Pouvant résoudre en nombres entiers l'équation (15) et l'équation

$$F = \Delta_3,$$

on pourra résoudre, en nombres entiers, la suivante :

$$F = (\Delta_1, \Delta_2, \Delta_3).$$

En continuant de la sorte, on voit finalement que l'on pourra résoudre en nombres entiers l'équation

$$F = (\Delta_1, \Delta_2, \ldots, \Delta_m).$$

c'est-à-dire la proposée.

C. Q. F. D.

Nous avons pensé que cette démonstration pourrait offrir quelque intérêt à cause de la méthode qu'elle fournit pour la résolution des équations de la forme proposée.