BULLETIN DE LA S. M. F.

A. BLOCH

Mémoire d'analyse diophantienne linéaire

Bulletin de la S. M. F., tome 50 (1922), p. 100-110

<http://www.numdam.org/item?id=BSMF_1922__50__100_0>

MÉMOIRE D'ANALYSE DIOPHANTIENNE LINÉAIRE :

PAR M. A. BLOCH.

Cette étude a pour but, par l'exploitation systématique d'un certain procédé, de retrouver les propositions essentielles de la théorie et d'établir aussi quelques résultats nouveaux.

1. LEMME. — *Soient n nombres entiers,* $a_1, a_2, \ldots, a_n$, de *plus grand commun diviseur* d_n, *écrits sur une ligne* l_n : *il est possible de former un déterminant* D_n, *dont la première ligne soit* l_n, *et la valeur* d_n.

Le théorème est vrai pour $n = 2$. Supposons-le vrai pour $n - 1$, et soit D_{n-1} le déterminant formé avec $a_1, a_2, \ldots, a_{n-1}$; on peut alors trouver deux nombres A et B entiers tels que $Ad_{n-1} - Ba_n = d_n$. Considérons le déterminant suivant, d'ordre n : le premier mineur en haut à gauche est D_{n-1} ; la dernière colonne est a_n, 0, ..., 0, A; la dernière ligne $\frac{a_1}{d_{n-1}}$ B, ..., $\frac{a_{n-1}}{d_{n-1}}$ B, A ; sa valeur sera d_n.

THÉORÈME FONDAMENTAL. — *Soit un tableau à n colonnes et p lignes, de module* d_p : *on peut y ajouter* $n - p$ *lignes, de façon à avoir un déterminant égal à* d_p (1).

Le théorème est démontré pour $p = 1$: établissons que, s'il est vrai pour $p - 1$, il est vrai pour p.

Nous nous placerons, pour simplifier l'écriture, dans le cas de $n = 5$, $p = 3$.

Nous avons à considérer le tableau T_3 :

$$\begin{matrix} a_1^1 & a_1^2 & a_1^3 & a_1^4 & a_1^5 \\ a_2^1 & a_2^2 & a_2^3 & a_2^4 & a_2^5 \\ a_3^1 & a_3^2 & a_3^3 & a_3^4 & a_3^5 \end{matrix} \qquad \text{de module } d_3.$$

Nous supposons le problème résolu pour le tableau T_2 des deux premières lignes, de module égal à d_2.

---

(1) *Cf.* par exemple E. CAHEN, *Théories des nombres*, t. I, n° 391.

Considérons alors le produit

$$\begin{vmatrix} a_1^1 & a_1^2 & a_1^3 & a_1^4 & a_1^5 \\ a_2^1 & a_2^2 & a_2^3 & a_2^4 & a_2^5 \\ \alpha_3^1 & \alpha_3^2 & \alpha_3^3 & \alpha_3^4 & \alpha_3^5 \\ \alpha_4^1 & \alpha_4^2 & \alpha_4^3 & \alpha_4^4 & \alpha_4^5 \\ \alpha_5^1 & \alpha_5^2 & \alpha_5^3 & \alpha_5^4 & \alpha_5^5 \end{vmatrix} \times \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \beta_3^1 & \beta_3^2 & b_3^3 & b_3^4 & b_3^5 \\ \beta_4^1 & \beta_4^2 & b_4^3 & b_4^4 & b_4^5 \\ \beta_5^1 & \beta_5^2 & b_5^3 & b_5^4 & b_5^5 \end{vmatrix}$$

$$= \begin{vmatrix} a_1^1 & & & a_1^2 & & a_1^3 & a_1^4 & a_1^5 \\ a_2^1 & & & a_2^2 & & a_2^3 & a_2^4 & a_2^5 \\ a_1^1\beta_3^1+a_2^1\beta_3^2+\alpha_3^1 b_3^3+\alpha_4^1 b_3^4+\alpha_5^1 b_3^5 & & & a_1^2\beta_3^1+a_2^2\beta_3^2+\alpha_3^2 b_3^3+\alpha_4^2 b_3^4+\alpha_5^2 b_3^5 & & \cdots & \cdots & \cdots \\ a_1^1\beta_4^1+a_2^1\beta_4^2+\alpha_3^1 b_4^3+\alpha_4^1 b_4^4+\alpha_5^1 b_4^5 & & & \cdots\cdots\cdots & & \cdots & \cdots & \cdots \\ \cdots\cdots\cdots & & & \cdots\cdots\cdots & & \cdots & \cdots & \cdots \end{vmatrix}$$

obtenu en multipliant les colonnes du premier déterminant par les lignes du second. Le premier est, par hypothèse, égal à d_2; nous allons choisir les termes du second de façon que le produit satisfasse aux conditions de l'énoncé.

Égalant aux a_3^i les termes de la troisième ligne du produit, on obtient un système dont le déterminant est d_2. Résolvons-le : on voit, sur les formules de résolution, que les b_3^i sont entiers et divisibles par $\frac{d_3}{d_2}$. Mais, de plus, $\frac{d_3}{d_2}$ est leur plus grand commun diviseur; en effet, on a, par exemple,

$$\begin{vmatrix} a_1^i & a_2^i & a_3^i-\alpha_3^i b_3^3-\alpha_4^i b_3^4-\alpha_5^i b_3^5 \\ a_1^j & a_2^j & a_3^j-\alpha_3^j b_3^3-\alpha_4^j b_3^4-\alpha_5^j b_3^5 \\ a_1^k & a_2^k & a_3^k-\alpha_3^k b_3^3-\alpha_4^k b_3^4-\alpha_5^k b_3^5 \end{vmatrix} = 0.$$

Donc, si les b_3^i étaient tous divisibles par $k\frac{d_3}{d_2}$, les déterminants de T_3 seraient tous divisibles par $k d_3$.

Les nombres β_3^1 et β_3^2, au contraire, ne sont pas entiers, en général; mais cela n'a pas d'importance, comme on va voir.

Les b_3^i et β_3^i étant ainsi déterminés, on peut choisir, d'après le théorème précédent, les b_4^i et b_5^i de façon que

$$\begin{vmatrix} b_3^3 & b_3^4 & b_3^5 \\ b_4^3 & b_4^4 & b_4^5 \\ b_5^3 & b_5^4 & b_5^5 \end{vmatrix} = \frac{d_3}{d_2};$$

prenant pour les β_4^i et β_5^i des entiers quelconques, on aura au

second membre un déterminant satisfaisant à toutes les conditions requises.

2. On sait ce que l'on entend par module d'un tableau, module d'un système de formes; de même on a des sous-modules (1) : le premier, le deuxième, etc., qui sont les plus grands communs diviseurs des premiers mineurs, des deuxièmes, etc.

Lorsque le module est nul, le premier sous-module non nul est le plus grand sous-module; si g est la différence, que nous appelons *genre*, entre la hauteur et le rang, c'est le $g^{\text{ième}}$ sous-module; quand le module n'est pas nul, il se confond avec lui.

Ceci posé, on a le théorème suivant :

Théorème. — *Soit un système de formes; considérons le tableau de ses coefficients; considérons d'autre part le tableau indéfini de même hauteur, formé en écrivant les uns à la suite des autres tous les systèmes de valeurs que peuvent prendre les formes : ces deux tableaux ont mêmes module et sous-modules (et par suite même rang)* (2).

En effet, les déterminants d'ordre k du deuxième tableau s'expriment en fonction linéaire et homogène des déterminants d'ordre k du premier : donc le sous-module correspondant du deuxième est un multiple du même sous-module du premier; d'ailleurs le deuxième tableau comprend le premier, comme on le voit en annulant toutes les variables, sauf une, que l'on égale à 1; donc le sous-module du deuxième divise celui du premier; ces deux sous-modules sont donc égaux (3).

Corollaire. — *Lorsque deux systèmes de formes représentent les mêmes entiers, ils ont même rang, mêmes module et sous-modules* (4).

Le théorème qui précède nous permettra de résoudre la question suivante : on a un système de formes; elles peuvent prendre

---

(1) J'emploie dans tout ceci, dans un but d'abréviation, une terminologie qui n'a nullement la prétention d'être définitive.

(2) *Cf.* Chatelet, *Leçons sur la théorie des nombres*, p. 50-52.

(3) Si l'un des sous-modules est nul, l'autre l'est évidemment.

(4) *Cf.* E. Cahen, *loc. cit.*, n° 278.

certains systèmes de valeurs; supposons qu'on leur impose les valeurs d'un de ces systèmes : quels sont alors les formes et systèmes de formes dont les valeurs demeurent absolument arbitraires?

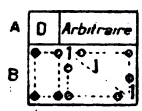
Soient A le système donné, B un des systèmes nouveaux qu'il s'agit de déterminer. Remarquons d'abord que la propriété de B, supposée vraie pour un système particulier de valeurs de A, est vraie pour tout pareil système (possible bien entendu). En effet : lorsqu'on suppose données aux formes de A les valeurs qu'elles prennent pour les valeurs x_{i0} des variables x_i, les formes de B demeurent par hypothèse absolument indéterminées. Supposons maintenant données aux formes de A les valeurs qu'elles ont en faisant $x_i = x_{i1}$; je dis que l'on peut alors donner aux formes de B des valeurs quelconques. En effet, dans le système total d'équations que l'on obtient par cette double supposition, faisons le changement d'inconnues $x_i = X_i + x_{i1} - x_{i0}$: on obtient un système qui est possible d'après l'hypothèse.

Nous appellerons les systèmes B immutants de A, les systèmes (A, B) immués de A. Il est clair que si un système B est immutant de A, il est immutant de tout système se déduisant linéairement de A, et en particulier d'un système quelconque extrait de A; en particulier, si A est de rang r, ses immutants sont identiques à ceux d'un système indépendant de r formes prises dans A.

3. Théorème. — *Pour qu'un système* A *à module non nul admette pour immutant un système* B, *il faut et il suffit que les tableaux* A *et* (A, B) *aient même module.*

La condition est nécessaire. Le module de (A, B) est en effet un multiple du module de A; je dis qu'il lui est égal. Soit, en effet, D un déterminant du tableau A; dans le tableau indéfini formé avec les valeurs de (A, B), on peut trouver les éléments ci-dessous.

Fig. 1.



Or, le déterminant qu'ils forment est égal à D.

La condition est suffisante. Supposons que (A, B) ait même module que A; ajoutons, s'il est nécessaire, des formes au système total (A, B) de façon à obtenir un système carré de même module (théorème fondamental); je dis que le système obtenu en égalant les formes de A à des valeurs accessibles, et les autres à des nombres arbitraires λ est possible; en effet, en résolvant par les formules de Cramer, on obtient des expressions qui, par hypothèse, doivent être entières pour certaines valeurs des λ : elles sont donc toujours entières, car les coefficients des λ sont entiers.

Ce théorème prouve qu'un système à module non nul admet des immutants (théorème fondamental); on voit, de plus, que si n est le nombre des variables, p le nombre des formes, un système immutant a au plus $n - p$ formes et qu'il peut en avoir $n - p$. Alors, de ce qui a été dit précédemment résulte qu'un système de rang r admet des immutants; le nombre des formes est au plus $n - r$ et peut lui être égal.

Ici peut s'intercaler le théorème suivant, dont la démonstration pourrait prendre place immédiatement après le théorème fondamental. Nous le plaçons ici pour profiter de ce que l'appareil de la démonstration est le même que pour le théorème précédent :

Théorème (*Heger*). — *Pour qu'un système d'équations à module non nul soit possible, il faut et il suffit que le module du tableau des coefficients soit égal à celui de ce même tableau complété par les termes tout connus* (1).

La condition est nécessaire. Cela se voit immédiatement sur les équations elles-mêmes.

La condition est suffisante.

Formons un système carré de même module (théorème fondamental) en adjoignant des équations de seconds membres quelconques. Résolvons par les formules de Cramer : on obtient des nombres entiers, comme on le voit par la formule de Laplace.

4. Nous allons généraliser ces propriétés pour les systèmes de genre quelconque.

---

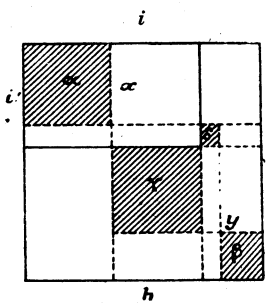
(1) *Cf.* J. Heger, *Denkschriften d. K. Akad. d Wissensch. Mathem. Naturwissensch. Klasse*, t. XIV, 1858, II, p. 1 — Chatelet, *loc. cit.*, p. 57.— E. Cahen, *loc. cit.*, n° 195.

Pour cela, nous ouvrirons une parenthèse.

Considérons un déterminant D d'ordre h, et, à l'intérieur, un tableau T de dimensions i et i'. Développons le déterminant (*voir* figure ci-dessous) par la formule de Laplace appliquée dans le sens de la largeur, puis chacun des déterminants du dessus par la formule de Laplace appliquée dans le sens de la hauteur : nous obtenons un développement de D par rapport aux déterminants extraits de T *d'ordre supérieur ou égal à* $i+i'-h$, il y aura donc un terme indépendant de T si $i+i' \leqq h$, et aucun si $i+i' > h$. D'ailleurs, en intervertissant l'ordre de la hauteur et de la largeur, on obtient un développement analogue, et il est

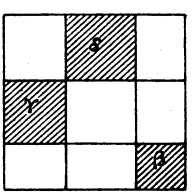
Fig. 2.

$y = x - (i + i' - h)$



certain *a priori* que les deux développements sont identiques, comme on le voit immédiatement en supposant variables les éléments de T. On pourrait le retrouver en calculant les coefficients :

Fig. 3.

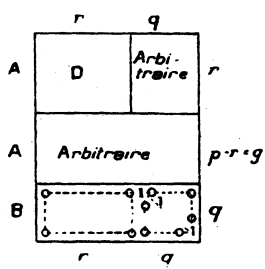


on trouve pour le coefficient de α (*fig.* 2) $\Sigma\beta\gamma\delta$ (avec des signes + ou — que nous nous abstenons de préciser); de même, dans le cas de $i+i' \leqq h$, le terme constant est $\Sigma\beta\gamma\delta$ (*fig.* 3). Dans ce qui va suivre, on aura toujours $i+i' > h$.

5. Théorème. — *Pour qu'un système* A *admette pour immutant un système* B, *il faut et il suffit que les tableaux* A *et* (A, B) *aient même genre et même plus grand sous-module.*

La condition est nécessaire. Soient r et g le rang et le genre de A, p et q les nombres de formes respectifs de A et B. D'abord il est clair que le genre de (A, B) est au moins g; considérons le $g^{\text{ième}}$ sous-module de (A, B) : c'est un multiple du $g^{\text{ième}}$ sous-module de A, qui est le plus grand sous-module; je dis qu'il lui est égal. Pour le voir, considérons le tableau indéfini des valeurs de (A, B); le plus grand sous-module cherché est le plus grand commun diviseur des déterminants d'ordre $q+r$ de ce tableau; or, si D est un déterminant d'ordre r de A, dans le tableau indéfini on peut trouver les éléments ci-dessous (1), où figure un déterminant

Fig. 4.



d'ordre $q+r$ égal à D. Donc les plus grands sous-modules sont bien égaux, et par suite les genres sont les mêmes.

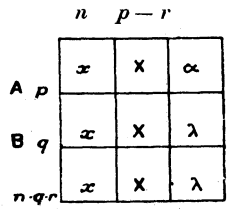
Nous retrouvons $q \leqq n-r$, sinon dans le tableau (A, B) les déterminants d'ordre $q+r$ seraient nuls, puisque alors on aurait $q+r > n$.

La condition est suffisante, r, g, n, p, q ayant les mêmes significations que ci-dessus le système (A, B) a même genre que le système A, et par suite pour rang $q+r$. Si $q+r < n$, ajoutons $n-q-r$ formes immutantes du système (A, B). Alors (puisque la condition est nécessaire) le système total formé a même genre et même plus grand sous-module que le système (A, B) et par suite que le système A; cela signifie que le plus grand commun diviseur

(1) Dans la figure, afin de la rendre plus simple, nous supposons que D est formé avec les premières lignes; ceci ne sera pas répété plus loin dans un cas analogue (§ 6).

des déterminants d'ordre n du système total est égal au plus grand sous-module de A. Bordons alors (théorème fondamental) le sys-

Fig. 5.



tème total de $n+p-r$ formes, de $p-r$ colonnes de nouveaux coefficients, de façon à former un déterminant égal à ce plus grand sous-module, et introduisons, à côté des anciennes variables x, d'autres variables X. Égalons les formes de A à des nombres α, les autres à des nombres λ, et résolvons : dans les expressions des x, on ne sait rien sur les coefficients des α et ceux des λ sont entiers; dans les expressions des X, les coefficients des α sont entiers et ceux des λ sont nuls. Ces propriétés des coefficients s'obtiennent en les développant comme il a été dit plus haut (¹); on a ainsi, dans le cas des x, $i+i'-h=r-1$ et r, dans le cas des X, $i+i'-h=r$ et $r+1$ (d'ailleurs, l'intégrité des coefficients des α dans les X est évidente en appliquant une seule fois la formule de Laplace; mais, précisément, cette propriété ne nous servira pas). Supposons alors le système total non carré possible en nombres entiers pour certaines valeurs des α et des λ : je dis qu'il sera possible pour les mêmes valeurs des α et des valeurs quelconques des λ; en effet, dans le premier cas, en résolvant le système total carré, on doit trouver des valeurs des X nulles et des valeurs des x entières; il résulte de ce qui a été dit sur les coefficients des λ que ces propriétés subsistent dans le deuxième cas.

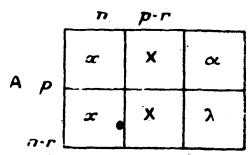
Théorème (*Frobenius*). — *Pour qu'un système d'équations linéaires soit possible, il faut et il suffit que son tableau et son tableau complété aient même rang et même plus grand sous-module* (²).

(¹) Par rapport au tableau des coefficients de A.

(²) *Cf.* Frobenius, *J. r. a. M.*, t. LXXXVI, 1879, p. 171. — E. Cahen, *loc. cit.*, n° 196.

L'appareil de la démonstration est le même que pour le théorème précédent.

Fig. 6.



La condition est nécessaire. Cela se voit immédiatement sur les équations elles-mêmes.

La condition est suffisante. Ajoutons $n - r$ formes immutantes, bordons comme précédemment de nouveaux coefficients et de nouvelles inconnues X, de façon à former un système carré de module égal au plus grand sous-module de l'énoncé; les deuxièmes membres des $n - r$ dernières équations sont quelconques. Résolvons et développons les expressions obtenues (1); on a pour les X, $i + i' - h = r + 1$; pour les x, $i + i' - h = r$; donc : 1° les X sont nuls; 2° les x sont entiers.

6. Nous dirons que des systèmes A, B, ... sont primitifs entre eux (dans leur ensemble) (2) lorsque les différents systèmes de valeurs qui peuvent être pris séparément par les systèmes peuvent l'être aussi simultanément.

Il suffit pour cela que l'un d'eux, A, ayant un certain système de valeurs fixes, les autres puissent prendre simultanément des systèmes de valeurs quelconques qui leur soient accessibles. Désignons en effet symboliquement par $f(x)$, $g(x)$, ... les systèmes A, B, ...; par hypothèse, l'équation symbolique $f(x) = f(x_0)$ est compatible avec les équations symboliques $g(x) = g(\xi')$, $h(x) = h(\xi'')$, ..., quels que soient ξ', ξ''. ...; je dis que les équations $f(x) = f(\xi)$, $g(x) = g(\xi')$, $h(x) = h(\xi'')$, ... sont compatibles quels que soient ξ, ξ', ξ'', ...; en effet, faisons dans ces équations le changement de variables $x = X + \xi - x_0$; il

(1) Cette fois par rapport au tableau complété des coefficients du système A.

(2) Par analogie avec la notion de forme primitive ou primaire; on pourrait dire aussi « arithmétiquement indépendants ».

vient

$$f(X) = f(x_0); \qquad g(X) = g(x_0 - \xi + \xi'); \qquad h(X) = h(x_0 - \xi + \xi'')\ldots,$$

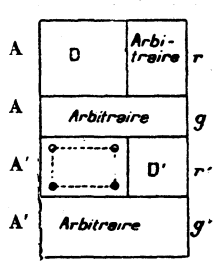
qui sont compatibles.

THÉORÈME. — *Pour que plusieurs systèmes soient primitifs dans leur ensemble, il faut et il suffit que le genre du système total qu'ils forment soit égal à la somme des genres* (1), *et son plus grand sous-module au produit des plus grands sous-modules.*

Nous supposons, pour fixer les idées, qu'il s'agit de deux systèmes; la démonstration est absolument la même dans le cas général. Soient A et A′ les deux systèmes, de rangs r et r', de genres g et g'.

La condition est nécessaire. D'abord, il est clair que le genre du système (A, A′) est au moins égal à la somme des genres g et g', et des $g^{\text{ième}}$ que le $(g+g')^{\text{ième}}$ sous-module est un multiple du produit et $g'^{\text{ième}}$ sous-modules (2); je dis qu'il lui est égal; en effet, soient D et D′ des déterminants d'ordre r et r' extraits des tableaux A et A′; on peut trouver dans le tableau indéfini des valeurs de (A, A′) les

Fig. 7.



éléments ci-dessus (3), où existe un déterminant d'ordre $r+r'$ égal à DD′; le $(g+g')^{\text{ième}}$ sous-module considéré, étant le plus grand commun diviseur des déterminants d'ordre $r+r'$ de ce

(1) Ou le rang à la somme des rangs.

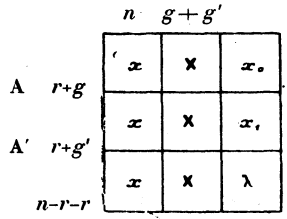
(2) En général, le $(h+h')^{\text{ième}}$ sous-module n'est pas multiple du produit des $h^{\text{ième}}$ et $h'^{\text{ième}}$ sous-module, à moins que l'on n'ait $h+h' < g+g'$, puisque alors il est nul.

(3) *Voir* note § 5.

tableau, divise tous les produits DD′, et par suite leur plus grand commun diviseur, lequel est égal à p. g. c. d. D × p. g. c. d. D′, c'est-à-dire au produit des plus grands sous-modules; donc, en définitive, il y a bien égalité.

La condition est suffisante. Fidèles à la méthode plusieurs fois employée, nous adjoignons au système total $n-(r+r')$ formes immutantes, nous bordons de $g+g'$ colonnes de coefficients nou-

Fig. 8.



veaux, multiplicateurs de $g+g'$ variables nouvelles X, de façon à former un déterminant carré égal en valeur absolue au plus grand sous-module du système total (A, A′). Égalons le système A ainsi complété à la valeur que prend A pour des valeurs x_0 des variables, le système A′ complété à la valeur prise par A′ pour des valeurs x_1; enfin le système provenant du système immutant à des entiers λ quelconques. Résolvons et développons les expressions obtenues par rapport au tableau formé par les coefficients de (A, A′) et la colonne des expressions en x_0 et x_1. On a ici pour les X, $i+i'-h=r+r'+1$; pour les x, $i+i'-h=r+r'$; chacun des déterminants ainsi introduits se développe à son tour par la formule de Laplace, et l'on voit bien aisément que les X sont nuls et les x entiers.

Désignons par module relatif d'un système composé par rapport aux systèmes composants, lesquels sont de genres g, g', ..., le quotient de son $(g+g'\ldots)^{\text{ième}}$ sous-module par le produit des plus grands sous-modules des composants. Alors le théorème précédent peut s'énoncer ainsi :

La condition nécessaire et suffisante pour que des systèmes soient primitifs dans leur ensemble est que le module relatif du système total qu'ils forment soit égal à l'unité.