6.

SUR LES INVARIANTS FONDAMENTAUX DE LA FORME BINAIRE DU HUITIÈME DEGRÉ.

[*Comptes Rendus*, LXXXIV. (1877), pp. 240—244, 532—534.]

ON sait que le nombre des invariants linéairement indépendants de l'ordre j, appartenant à une forme binaire du degré i, est égal à la différence de deux nombres dont l'un, le plus grand, est le nombre de manières de représenter $\frac{ij}{2}$ comme la somme de j nombres (avec des répétitions à volonté) choisis entre les nombres $0, 1, 2, \ldots, i$, et l'autre est le nombre de manières de former $\frac{ij}{2} - 1$ selon la même loi.

Ainsi le nombre d'invariants de l'ordre n, appartenant à la forme binaire du degré 8, est la différence entre deux *dénumérants*, l'un du système

$$\begin{aligned} y + 2z + 3t + 4u + 5v + 6w + 7\rho + 8\sigma &= 4n, \\ x + y + z + t + u + v + w + \rho + \sigma &= n; \end{aligned}$$

l'autre du système

$$\begin{aligned} y + 2z + 3t + 4u + 5v + 6w + 7\rho + 8\sigma &= 4n - 1, \\ x + y + z + t + u + v + w + \rho + \sigma &= n. \end{aligned}$$

On comprendra que le dénumérant d'une équation ou d'un système d'équations simultanées en nombres entiers veut dire le nombre de solutions que cette équation ou ce système admet en nombres entiers.

Or j'ai démontré ailleurs que le dénumérant d'un système quelconque d'équations simultanées peut toujours s'exprimer au moyen de dénumérants simples, c'est-à-dire appartenant chacun à une seule équation, et l'on trouvera sans difficulté que la différence entre les deux dénumérants dont il est ici question sera le coefficient de t^n dans la fonction génératrice

$$G = \frac{1 + t^8 + t^9 + t^{10} + t^{18}}{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)(1 - t^6)(1 - t^7)}. \tag{1}$$

Ce résultat est parfaitement d'accord avec l'expression donnée par M. Cayley dans son *Second Memoir on Quantics*, c'est-à-dire

$$\frac{(1-x)(1+x-x^3-x^4+x^6+x^7+x^8+x^9+x^{10}-x^{12}-x^{13}+x^{15}+x^{16})}{(1-x^2)^2(1-x^3)^2(1-x^4)(1-x^5)(1-x^7)};$$

car on trouvera, par un calcul algébrique des plus simples, que ces deux fonctions génératrices sont identiques en valeur.

En vertu de la forme donnée à G dans l'équation (1), on peut immédiatement déduire les conséquences suivantes, que je nommerai désormais, si j'ai occasion de les citer, *principes:*

(1) Il existe des invariants, appartenant à la forme binaire octavique des ordres 2, 3, 4, 5, 6, 7, que je nomme les *invariants primaires.*

(2) Il existe* quatre invariants des ordres 8, 9, 10, 18, disons x, y, z, θ, tels, que chaque autre invariant peut s'exprimer comme une fonction linéaire de x, y, z, θ, les coefficients et le terme constant de telle fonction étant des fonctions rationnelles et entières des invariants primaires.

(3) Il sera impossible de former aucune équation linéaire de la nature exprimée plus haut entre x, y, z, θ.

(4) x, y, z seront indépendants entre eux. Quant à θ, il y aura deux hypothèses à faire: ou il est indépendant de x, y, z, ou l'on peut prendre pour sa valeur une fonction linéaire quelconque de xz et y^2.

Je démontrerai que la dernière hypothèse doit être rejetée, c'est-à-dire qu'il existe en effet un invariant fondamental de l'ordre 18, de sorte que le système complet des invariants se composera de six, que je nomme *primaires*, dont les ordres sont 2, 3, 4, 5, 6, 7, et cinq dont les ordres sont 0, 8, 9, 10, 18, que je nommerai *secondaires*, car on ne doit jamais oublier que la constante 1 est un invariant du degré zéro.

Traitons désormais les invariants primaires comme des constantes, cela facilitera beaucoup la parole dans cette dissertation.

Supposons que y^2, zx ne puissent pas s'exprimer séparément comme fonctions linéaires de x, y, z, 1; puisque, pour une valeur quelconque de x, y, z, on peut substituer $ax+b$, $cy+d$, $ez+fx+g$, on verra facilement qu'on peut instituer les équations suivantes entre x, y, z:

$$xz-y^2=T, \tag{2}$$

$$x^2=Ax+By+Cz+D, \tag{3}$$

$$xy=A'x+B'y+C'z+D', \tag{4}$$

$$yz=L'x+M'y+N'z+P', \tag{5}$$

$$z^2=Lx+My+Nz+P, \tag{6}$$

[* Cf. p. 62 below.]

où l'on remarquera que l'on a fait disparaître le terme xz ou y^2 dans l'équation pour z^2 par le moyen du multiplicateur arbitraire λ, qu'on peut ajouter à z. Multiplions

(2) par x et z,
(3) y,
(4) x et z,
(5) x et z,
(6) y.

Il est facile de voir qu'en faisant les éliminations dialytiques convenables, on obtiendra cinq équations linéaires entre x, y, z, xz, y^2, 1. De plus, dans chacune de ces équations, le coefficient de xz doit être égal à celui de y^2; car, si c'est combiné avec (2), on trouvera xz et y^2 comme fonctions linéaires contraires à l'hypothèse de x, y, z. Ainsi chacune de ces cinq équations doit être une identité et fournira ainsi cinq liaisons entre les coefficients, de sorte qu'on pourrait attendre de trouver vingt-cinq de ces liaisons ; mais, en faisant le calcul, on trouvera qu'il n'y a plus que onze indépendantes, que j'écris de la manière suivante :

(1) Le groupe $B' = A$, $C' = B$, $L' = M$, $M' = N$, $N' = A'$; de sorte que l'on peut substituer respectivement les lettres

$$\begin{matrix} A, & B, & C, \\ K, & A, & B, \\ M, & N, & K, \\ L, & M, & N, \end{matrix}$$

au lieu de

$$\begin{matrix} A, & B, & C, \\ A', & B', & C', \\ L', & M', & N', \\ L, & M, & N. \end{matrix}$$

Il y aura encore un groupe de cinq équations que voici :

$$D = BK - CN, \tag{12}$$

$$P = MK - AL, \tag{13}$$

$$D' = CM - AK, \tag{14}$$

$$P' = LB - NK, \tag{15}$$

$$T = CL - K^2, \tag{16}$$

et finalement

$$CL - AN = 0. \tag{17}$$

Mais on peut obtenir encore une nouvelle équation identique en multipliant (2) par xz, (3) par (6), et (4) par (5); car on a

$$xzT = x^2 . z^2 - xz . yz.$$

Les cinq liaisons qui en résultent seront indépendantes entre elles-mêmes, mais une d'elles ne sera qu'une répétition de (16). Les quatre qui restent sont toutes nouvelles et peuvent s'écrire

$$2(KBM - CMN - ALB + ANR) = 0, \tag{18}$$

$$LB^2 - 2KNB + CN^2 + AT = 0, \tag{19}$$

$$CM^2 - 2AKM + LA^2 + NT = 0, \tag{20}$$

$$2(BM - AN)T = 0. \tag{21}$$

Ainsi l'on a

$$\text{ou } T = 0, \quad \text{ou } BM = AN.$$

Si $BM = AN$, on obtient, en combinant avec (18) et (19), $AT = 0$, et, en combinant avec (18) et (20), $NT = 0$. Donc

$$\text{ou } T = 0, \quad \text{ou } A = 0, \quad N = 0, \quad \text{et} \quad BM = 0.$$

Mais si

$$N = 0 \quad \text{et} \quad B = 0, \quad D = 0,$$

et si

$$A = 0 \quad \text{et} \quad M = 0, \quad P = 0.$$

Donc

$$\text{ou } T = 0, \quad \text{ou } A = 0, \quad B = 0, \quad D = 0, \quad \text{ou } N = 0, \quad M = 0, \quad P = 0.$$

Donc on a

$$xz = y, \quad \text{ou } x^2 = Cz, \quad \text{ou } z^2 = Lx;$$

mais chacune de ces équations est inadmissible. Donc l'hypothèse que θ n'est pas indépendant est fausse, et nous avons établi que les invariants *secondaires* de la forme binaire octavique sont respectivement de l'ordre

$$0, \ 8, \ 9, \ 10, \ 18.$$

J'ajoute que, pour obtenir les *principes* qui ont conduit à ce résultat, on n'a besoin de s'appuyer sur aucune autre chose que la forme même de la fonction génératrice prise en conjonction avec la vérité intuitive que chaque combinaison d'invariants est elle-même un invariant.

A cause d'une erreur qui s'est glissée dans le *Second Memoir on Quantics* de M. Cayley, dans son explication des conséquences qui découlent de la fonction génératrice pour les covariants appartenant aux formes au-dessus du quatrième et les invariants au-dessus du sixième degré, on a pensé (voir *Théorie des formes binaires*, de M. Faà de Bruno, p. 150) que la théorie elle-même est en défaut et que les équations linéaires qui conduisent à cette fonction, après qu'un certain point est passé, cessent d'être indépendantes. J'ai examiné cette question de près et j'arrive à la *certitude* du contraire.

En effet, l'indépendance de ces équations est une conséquence d'un théorème très-curieux que j'ai découvert, un théorème plutôt de position que d'arithmétique que voici. Prenons trois nombres quelconques i, j, w avec la seule condition que w ne soit pas plus grand que $\frac{ij}{2}$. Formons toutes les combinaisons possibles avec les chiffres $0, 1, 2, \ldots, i$, qui donnent la somme w: que le nombre de ces partitions soit m et qu'elles soient nommées $P_1, P_2, \ldots, P_m$.

De même formons toutes les partitions semblables avec la somme $w-1$, que leur nombre soit μ et nommons-les $\Pi_1, \Pi_2, \ldots, \Pi_\mu$.

On doit observer que le nombre m ne peut jamais devenir plus petit que μ, à cause de la condition que w n'est pas plus grand que $\frac{ij}{2}$.

Quand un Π quelconque, disons Π_λ, peut être déduit d'un P quelconque, disons P_l, par moyen de diminuer un des chiffres qui y entrent par l'unité, je nomme Π_λ une dérivée de P_l et dans le cas contraire une non-dérivée.

Formons un rectangle de m sur μ et à la tête des colonnes écrivons les sommes P et à côté de chaque ligne les sommes Π. De cette manière on peut dire que chaque place dans le rectangle aura une certaine longitude désignée par un P et une latitude désignée par un Π. Dans chaque place dont la latitude est une *dérivée* de la longitude, écrivons un signe quelconque, par exemple une croix, et dans toutes les autres places insérons des zéros. Par une diagonale d'une *matrice* carrée, comprenons une combinaison quelconque des positions occupées par ces éléments qui entrent dans la valeur du déterminant qui y appartient. Ces diagonales se diviseront, selon la règle élémentaire pour le calcul des déterminants, en deux espèces positives et négatives. De plus on peut sous-entendre par une diagonale *effective* une diagonale dans laquelle il n'entre nul *zéro*.

Or, avec le rectangle dont j'ai parlé, formons toutes les matrices carrées *complètes* possibles, c'est-à-dire des carrés de μ^2 plans. Il peut arriver que, pour un certain nombre d'entre elles, il n'y aura nulle diagonale effective, mais on peut démontrer qu'il en existe toujours une au moins qui possède une ou plusieurs diagonales. S'il n'y a qu'une seule diagonale effective, évidemment le déterminant ne peut pas s'évanouir; mais s'il y en a plusieurs, alors je dis que toutes ces diagonales effectives pour un déterminant donné porteront le même signe, de sorte que, si l'on donne des valeurs positives quelconques aux éléments désignés par des croix, la somme des produits qui correspondent à ces diagonales ne peut pas devenir égale à zéro. Cette proposition, fort remarquable, suffit pour démontrer la suffisance de la règle mise en doute par M. de Bruno. Pour trouver le nombre total de covariants appartenant à une forme donnée du degré i, d'un ordre donné j dans les coefficients, et d'un degré donné k dans les variables, on n'aura qu'à prendre la différence de deux dénumérants de deux systèmes de deux équations simultanées dans l'une desquelles les termes constants seront $\frac{ij-k}{2}$ et dans l'autre $\frac{ij-k}{2}-i$. Comme conséquence de ce théorème, il est facile de démontrer que le nombre total des covariants de l'ordre j n'est autre chose que le nombre de manières de former la somme $\frac{ij}{2}$ ou $\frac{ij-1}{2}$ avec j des chiffres $0, 1, 2, 3, \ldots, i$.

Toutes ces conclusions se trouvent peut-être étendues à des *systèmes* de formes binaires.

Par exemple, si l'on considère le cas de deux formes binaires seulement, disons des degrés i et i', et si, pour plus de simplicité, on traite le problème du nombre *total* de covariants de l'ordre j dans ces coefficients par rapport à une des deux formes, et j' par rapport à l'autre, ce nombre sera le dénumérant d'un système ternaire d'équations simultanées en nombres entiers, que voici :

$$y+2z+3t+\ldots+it+\eta+2\zeta+\ldots+i'\tau=\frac{ij+i'j'+\epsilon}{2}, \tag{1}$$

$$x+y+z+\ldots+t=j, \tag{2}$$

$$\zeta+\eta+\quad\ldots+\tau=j', \tag{3}$$

ϵ étant égal à zéro si $ij+i'j'$ est pair, et à -1 dans le cas contraire, et ainsi, en général, pour un système contenant un nombre de formes quelconques.

Le théorème qui porte à la démonstration de l'indépendance des équations linéaires dont il a été fait mention plus haut peut être mis sous une forme plus générale, que voici:

Soit Q une quantité quelconque d'un ou plusieurs systèmes de variables $x, y, z, \ldots, x', y', \ldots, x'', y'', \ldots$.

Prenons l'émanant de cette quantité par rapport à $\xi, \eta, \ldots, \xi', \eta', \ldots, \xi'', \eta'', \ldots$.

Substituons, pour $\xi, \eta, \ldots$, des fonctions linéaires *omnipositives* quelconques de $x, y, z \ldots$, pour $\xi', \eta', \ldots$ des fonctions linéaires *omnipositives* de $x', y', \ldots$, de sorte qu'on obtiendra une nouvelle quantité tout à fait semblable, dans sa constitution, à Q, mais dont les coefficients seront fonctions linéaires des coefficients de Q. Alors je dis que ces fonctions linéaires seront nécessairement indépendantes entre elles. Par une fonction linéaire omnipositive on comprendra facilement que je désigne une fonction linéaire dont tous les coefficients sont des quantités qui ne sont ni négatives ni nulles.