French Exam, Winter 2005

Text 1

(1)

[1934b] Une propriété caractéristique des groupes de substitutions linéaires finis

Si à tout élément S d'un groupe l'on a fait correspondre une matrice $\mathfrak{M}_s$ à r lignes et r colonnes, de déterminant non nul, de telle sorte que

$$\mathfrak{M}_{S.T} = \mathfrak{M}_S . \mathfrak{M}_T,$$

l'on dit, comme on sait, que l'on a défini une représentation $\mathcal{D}$ de degré r du groupe. Soient $\mathcal{D}$, $\mathcal{D}'$ deux représentations de degrés r, r' : si l'on fait subir à une série de variables $x_1, x_2, \ldots, x_r$ la substitution $\mathfrak{M}_S$ de $\mathcal{D}$, à une autre série $y_1, y_2, \ldots, y_{r'}$ la substitution $\mathfrak{M}'_S$ de $\mathcal{D}'$, les produits x_i, y_j subiront une transformation $\mathfrak{M}_S \times \mathfrak{M}'_S$ (produit kroneckérien de $\mathfrak{M}_S$ et $\mathfrak{M}'_S$), et les matrices $\mathfrak{M}_S \times \mathfrak{M}'_S$ constituent une représentation $\mathcal{D} \times \mathcal{D}'$ de degré $r.r'$ du groupe, qui est dite le *produit* de $\mathcal{D}$ et $\mathcal{D}'$. D'autre part, les matrices

$$\left\| \begin{matrix} \mathfrak{M}_S & 0 \\ 0 & \mathfrak{M}'_S \end{matrix} \right\|$$

constituent une représentation $\mathcal{D} + \mathcal{D}'$ de degré $r + r'$, la *somme* de $\mathcal{D}$ et $\mathcal{D}'$. Enfin, $\mathcal{D}$ et $\mathcal{D}'$ sont dites *équivalentes*, et l'on écrit $\mathcal{D} \sim \mathcal{D}'$, si $r = r'$ et s'il existe une matrice C telle que $\mathfrak{M}_S = C . \mathfrak{M}'_S . C^{-1}$ quel que soit S. Si, comme d'habitude, $\chi(S) = \mathrm{Sp}(\mathfrak{M}_S)$ désigne la trace de $\mathfrak{M}_S$ ou *caractère* de $\mathcal{D}$, le caractère de $\mathcal{D} \times \mathcal{D}'$ sera $\chi(S).\chi'(S)$, celui de $\mathcal{D} + \mathcal{D}'$ sera $\chi(S) + \chi'(S)$; enfin, si $\mathcal{D} \sim \mathcal{D}'$, $\chi(S) = \chi'(S)$.

Si alors on ne distingue pas entre représentations équivalentes, les représentations d'un groupe forment une algèbre sur l'anneau des entiers rationnels. En particulier, si le groupe est fini, on démontre que toutes les représentations sont des combinaisons linéaires, à coefficients entiers, d'un nombre fini d'entre elles : d'où il suit que toute représentation $\mathcal{D}$ satisfait à une équation $\mathcal{D}^m + a_1 \mathcal{D}^{m-1} + \ldots + a_m . 1 \sim 0$ à coefficients entiers rationnels. Cette équation signifie que, si l'on fait passer dans le second

(2)

membre tous les termes à coefficient negatif, les deux membres sont des représentations équivalentes : il faut entendre naturellement que chaque membre est alors *somme* (au sens défini plus haut) de termes $\mathcal{D}^k$, $\mathcal{D}^k$ désignant le *produit* de k facteurs $\mathcal{D} \times \mathcal{D} \times \ldots \times \mathcal{D}$; 1 est la représentation identique ($r = 1$, $\mathfrak{M}_S = 1$). D'ailleurs on peut supposer que les matrices $\mathfrak{M}_S$ sont *unitaires-orthogonales* (nous dirons simplement *orthogonales*), c'est-à-dire que les substitutions linéaires définies par ces matrices conservent la forme hermitienne $x_1\overline{x}_1 + x_2\overline{x}_2 + \ldots + x_r\overline{x}_r$: car on démontre que toute représentation d'un groupe fini est équivalente à une telle représentation.

Mais considérons un instant le groupe de toutes les substitutions linéaires orthogonales à r variables : les matrices $\mathfrak{M}$ qui en sont les éléments en constituent une représentation $\mathcal{D}_0$, la plus simple de toutes; si $f(x)$ est un polynome à coefficients positifs, $f(\mathcal{D}_0)$, au sens défini tout à l'heure, en est une autre, de degré $f(r)$. Soit $f\langle \mathfrak{M} \rangle$ la matrice, à $f(r)$ lignes et $f(r)$ colonnes, que $f(\mathcal{D}_0)$ fait correspondre à l'élément $\mathfrak{M}$ du groupe orthogonal (1). On aura

$$f\langle \mathfrak{M}\mathfrak{M}' \rangle = f\langle \mathfrak{M} \rangle . f\langle \mathfrak{M}' \rangle, \tag{1}$$

cette égalité exprimant que $f(\mathcal{D}_0)$ est une représentation. De plus, le caractère de $f(\mathcal{D}_0)$ sera $\mathrm{Sp} f\langle \mathfrak{M} \rangle = f(\mathrm{Sp}\mathfrak{M})$.

Cela posé, nous allons d'abord retrouver le résultat indiqué plus haut. Soit $\mathcal{D}$ une représentation d'un groupe fini, qui fasse correspondre à l'élément S la matrice (orthogonale) $\mathfrak{M}_S$; les traces $\mathrm{Sp}(\mathfrak{M}_S) = \chi(S)$ sont des nombres algébriques, à savoir des sommes de racines de l'unité. Soit $F(x) = 0$ l'équation à coefficients entiers de plus bas degré qui ait pour racines tous les $\chi(S)$; et soit $F(x) = f(x) - g(x)$, f et g étant des polynomes à coefficients entiers positifs. Alors, les représentations $f(\mathcal{D})$, $g(\mathcal{D})$ du groupe, constituées par les matrices $f\langle \mathrm{M}_S \rangle$, $g\langle \mathfrak{M}_S \rangle$, auront même caractère $f[\chi(S)] = g[\chi(S)]$, *et l'on sait que dans ce cas elles sont équivalentes :*

$$f\langle \mathfrak{M}_S \rangle = \mathrm{C} . g\langle \mathfrak{M}_S \rangle . \mathrm{C}^{-1}, \tag{2}$$

ce qui signifie précisément que $\mathcal{D}$ satisfait à l'équation $F(\mathcal{D}) \sim 0$.

Tout cela est bien connu. Mais je me propose de démontrer que récipro-

(1) Cette matrice n'a, bien entendu, rien de commun avec la matrice $f(\mathfrak{M})$ à r^2 éléments qui s'obtient à partir de $\mathfrak{M}$ en formant les sommes et les produits au sens de l'algèbre des matrices.

Text 2 ④

On peut aussi procéder comme dans 1) et remarquer que l'existence du p.p.c.m. de u et v équivaut à celle d'une *borne inférieure* de Au et Av dans l'ensemble ordonné des idéaux fractionnaires principaux; or celle-ci est $Au \cap Av$.

III. Deux éléments a, b de A sont dits *étrangers* (ou *premiers entre eux*) si 1 est un de leurs p.g.c.d. Rappelons l'important LEMME D'EUCLIDE. *Soient a, b, c des éléments d'un anneau principal* A; *si a divise bc et est étranger à b, alors a divise c.*

Démonstration succinte : par Bezout (2), on a a' et $b' \in A$ tels que $1 = a'a + b'b$; d'où $c = a'ac + b'bc$; comme a divise chaque terme du second membre, il divise c.

IV. Enfin on a l'important « décomposition en facteurs premiers » :

THÉORÈME. *Étant donné un anneau principal* A *et son corps des fractions* K, *il existe une partie* P *de* A *telle que tout $x \in K$ s'écrive de façon unique*

6. $x = u \prod_{p \in P} p^{v_p(x)}$

où u est un élément inversible de A, *et où les exposants $v_p(x)$ sont des éléments de* Z *presque tous nuls sauf un nombre fini d'entre eux.*

Pour un exposé plus systématique de ces questions, nous renvoyons le lecteur à [1], *Algèbre*, chap. VI, § 1 à chap. VII, § 1. Une partie de la théorie (plus précisément tout ce qui ne tourne pas autour de l'identité de Bezout) s'étend à des anneaux plus généraux que les anneaux principaux, à savoir les anneaux *factoriels*; voir [7], ou [2] Algèbre commutative, chap. VII, § 3.

1.2. Un exemple : les équations $x^3 + y^3 = z^3$ et $x^4 + y^4 = z^4$

Une des parties les plus attirantes de la Théorie des Nombres est l'étude des *équations diophantiennes*. Il s'agit d'équations polynômes $P(x_1, \ldots, x_n) = 0$ à coefficients dans Z (resp. dans Q), dont on cherche les solutions (x_i) en nombres entiers (resp. en nombres rationnels). On peut remplacer Z (resp. Q) par des anneaux A (resp. des corps K) plus généraux; nous en verrons un exemple plus tard (§ 6).

Nous allons étudier ici deux cas particuliers de la fameuse *équation de Fermat:*

1. $x^n + y^n = z^n$.

Fermat a affirmé avoir demandé que, pour $n \geqslant 3$, cette équation n'a pas de solution (x, y, z) en nombres entiers tous non-nuls; sa démonstration n'a pas été retrouvée. De très nombreux mathématiciens ont, depuis, intensément travaillé sur ce problème, et montré que l'affirmation de Fermat est vraie pour un grand nombre de valeurs de l'exposant n; cependant aucune démonstration générale (i. e. valable pour tout n) n'a été trouvée.

L'opinion aujourd'hui la plus courante est que, dans sa « démonstration », Fermat avait commis une erreur, mais une erreur digne de ce mathématicien de premier ordre. Par exemple il aurait pu avoir l'idée (géniale pour son époque) d'opérer dans l'anneau des entiers du corps des racines n-ièmes de l'unité, et avoir cru que cet anneau est toujours principal. En effet, on sait démontrer l'assertion de Fermat pour tout exposant n tel que cet anneau soit principal; mais il ne l'est pas pour tout n; bien plus, pour n premier, cet anneau n'est principal que pour un nombre fini de valeurs de n [1].

Pour $n = 2$, l'équation (1) a des solutions entières, par exemple (3,4,5). On peut en donner une description complète :

THÉORÈME 1. *Si x, y, z sont des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$, il existe un entier d et des entiers étrangers u, v tels que (à une permutation près de x et y) on ait:*

2. $x = d(u^2 - v^2) \qquad y = 2duv \qquad z = d(u^2 + v^2)$

Un calcul facile montre que les formules (2) donnent des solutions de $x^2 + y^2 = z^2$. Réciproquement soient x, y, z des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$. Quitte à diviser x, y, z par leur p.g.c.d., on peut les supposer étrangers dans leur ensemble; ils sont alors étrangers deux à deux, car, si, par exemple, x et z ont un facteur premier commun p, alors p divise $y^2 = z^2 - x^2$ et donc y. En particulier deux des nombres x, y, z sont impairs, et le troisième est nécessairement pair. Les nombres x et y ne peuvent être tous deux impairs, car sinon, on aurait $x^2 \equiv 1 \pmod 4$, $y^2 \equiv 1 \pmod 4$ d'où $z^2 \equiv 2 \pmod 4$ contrairement au fait que z^2 est un carré. On a donc, après échange éventuel de x et y.

3. x impair, y pair, z impair.

Écrivons l'équation

4. $y^2 = z^2 - x^2 = (z - x)(z + x)$.

Comme le p.g.c.d. de $2x$ et de $2z$ est 2, et que $2x = (z + x) - (z - x)$ et $2z = (z + x) + (z - x)$, le p.g.c.d. de $z - x$ et $z + x$ ne peut être que 2. Posons $y = 2y'$, $z + x = 2x'$, $z - x = 2z'$, où y', x', z' sont des entiers, car y, $z + x$ et $z - x$ sont pairs par (3). On a alors $y'^2 = x'z'$. Comme x' et z' sont étrangers, la décomposition en facteurs premiers de y'^2 montre que x' et z' sont des *carrés* u^2 et v^2 : en effet tout facteur premier de y'^2 va, avec son exposant pair, soit tout entier dans x', soit tout entier dans z'. On a donc $z + x = 2u^2$, $z - x = 2v^2$, $y^2 = 2u^2 \cdot 2v^2$, d'où $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$. Ici u et v sont étrangers, sinon x, y, z auraient un facteur premier commun. On en déduit (2) en remultipliant par le p.g.c.d.d. CQFD.

1. Voir C. L. Siegel — « Gesammelte Werke », t. III, p. 436-442.

THÉORÈME 2. *L'équation* $x^4 + y^4 = z^2$ *n'a pas de solution en nombres entiers* $x_1 y_1 z \geqslant 1$.

Raisonnons par l'absurde. On a alors une solution (x, y, z) où z est *minimal*. Pour celle-ci, x, y et z sont étrangers deux à deux : en effet, si par exemple, x et y avaient un facteur premier commun p, alors p^4 diviserait z^2, donc p^2 diviserait z, et $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}\right)$ serait une solution contredisant la minimalité de z; les deux autres cas sont analogues et plus faciles. Comme notre équation s'écrit $(x^2)^2 + (y^2)^2 = z^2$, on peut lui appliquer le th. 1 : après permutation éventuelle de x et y, on voit qu'on a des entiers $u, v \geqslant 1$ et étrangers tels que

$$5. \quad x^2 = u^2 - v^2, \qquad y^2 = 2uv, \qquad z = u^2 + v^2.$$

Comme $4 \mid y^2$, la relation $y^2 = 2uv$, montre que l'un des deux nombres u et v est pair; l'autre est nécessairement impair; la répartition « u pair, v impair » donne $u^2 \equiv 0 \pmod 4$, $v^2 \equiv 1 \pmod 4$, d'où $x^2 = u^2 - v^2 \equiv -1 \pmod 4$ ce qui est absurde; donc u est impair et $v = 2v'$. La relation $y^2 = 4uv'$ et le fait que u et v' sont étrangers montrent que u et v' sont des carrés a^2 et b^2. Appliquons encore le th. 1, cette fois à l'équation $x^2 + v^2 = u^2$ (cf. (5)); comme x et u sont impairs, v pair, et x, v, u étrangers deux à deux, on a des entiers étrangers $c, d \geqslant 1$ tels que :

$$6. \quad x = c^2 + d^2, \qquad v = 2cd, \qquad u = c^2 + d^2.$$

Or, de $v = 2v' = 2b^2$, on déduit $cd = b^2$, de sorte que c et d sont encore des carrés x'^2 et y'^2, car ils sont étrangers. Comme $u = a^2$, la dernière équation (6) s'écrit

$$7. \quad a^2 = x'^4 + y'^4$$

et a la *même forme* que l'équation donnée. Mais, on a, par (5), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, d'où $z > a$, ce qui contredit le caractère minimal de z. Notre assertion est donc démontrée

Une légère variante de notre démonstration montre que, étant donnée une solution (x, y, z) en entiers $\geqslant 1$ de $x^4 + y^4 = z^2$, on construit une suite (x_n, y_n, z_n) de telles solutions, où la suite (z_n) est strictement décroissante, ce qui est absurde. Ceci est la méthode de *descente infinie*, due à Fermat.

COROLLAIRE. *L'équation* $x^4 + y^4 = z^4$ *n'a pas de solution en nombres entiers* $x, y, z \geqslant 1$.

En effet cette équation s'écrit $x^4 + y^4 = (z^2)^2$, et on applique le th. 2.

1.3. Quelques lemmes sur les idéaux; l'indicateur d'Euler

Soit $n \geqslant 1$ un entier naturel. On appelle *indicateur d'Euler* de n, et on note $\varphi(n)$ le nombre des entiers q premiers à n et tels que $0 \leqslant q < n$ (il

Tom 3

(7)

[1949a] Sur l'étude algébrique de certains types de lois de mariage

En ces quèlques pages, écrites à la prière de C. Lévi-Strauss, je me propose d'indiquer comment des lois de mariage d'un certain type peuvent être soumises au calcul algébrique, et comment l'algèbre et la théorie des groupes de substitutions peuvent en faciliter l'étude et la classification.

Dans les sociétés dont il s'agit ici, les individus, hommes et femmes, sont répartis en classes, la classe de chacun étant déterminée, d'après certaines règles, par celles de ses parents; et les règles du mariage indiquent, suivant les classes auxquelles appartiennent respectivement un homme et une femme, si le mariage entre eux est possible ou non.

Dans une telle société, la totalité des mariages possibles peut donc se répartir en un certain nombre de types distincts; ce nombre est égal au nombre de classes entre lesquelles se répartit la population, s'il y a une formule unique qui, pour un homme d'une classe donnée, indique dans quelle classe il a le droit de choisir sa femme (ou, en d'autres termes, la sœur d'un homme de quelle classe il peut épouser); si au contraire il y a plusieurs de ces formules, alternant entre elles d'une manière déterminée, le nombre des types de mariage possibles pourra être double, triple, etc., du nombre des classes.

Soit donc, en tout cas, n le nombre de types de mariage;

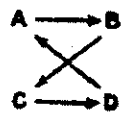
nous les désignons arbitrairement par n symboles, par exemple $M_1, M_2, \ldots, M_n$. Nous ne considérons que des lois de mariage satisfaisant aux deux conditions suivantes :

(A) Pour tout individu, homme ou femme, il y a un type de mariage et un seul qu'il (ou elle) a le droit de contracter.

(B) Pour tout individu, le type de mariage qu'il (ou elle) est susceptible de contracter dépend uniquement de son sexe et du type de mariage dont il (ou elle) est issu.

Par conséquent, le type de mariage que peut contracter un fils issu d'un mariage de type M_i (i étant l'un des nombres $1, 2, \ldots, n$) est une *fonction* de M_i, que nous pouvons, suivant la notation mathématique en usage en pareil cas, désigner par $f(M_i)$; il en sera de même pour une fille, la fonction correspondante, que nous désignerons par $g(M_i)$, étant ordinairement distincte de la précédente. La connaissance des deux fonctions f et g détermine complètement, du point de vue abstrait, les règles de mariage dans la société étudiée. Ces règles pourront donc se représenter par un tableau à trois lignes, dont la première énumère les types de mariage $M_1, \ldots, M_n$, tandis que la seconde et la troisième donnent respectivement les valeurs correspondantes des deux fonctions f et g.

Prenons un exemple simple. Soit une société à quatre classes, à échange généralisé, suivant le type suivant.



Il y a quatre types de mariage : (M_1) homme A, femme B; (M_2) homme B, femme C; (M_3) homme C, femme D; (M_4) homme D, femme A. Admettons de plus que les enfants d'une mère de classe A, B, C, D soient respectivement de classe B, C, D, A. Alors notre tableau est le suivant :

(Type de mariage des parents). .		M_1	M_2	M_3	M_4
(Type de mariage du fils). . . .	$f(M_i) =$	M_3	M_4	M_1	M_2
(Type de mariage de la fille). . .	$g(M_i) =$	M_2	M_3	M_4	M_1

De plus, comme il apparaît sur l'exemple ci-dessus, f et g sont des substitutions, ou, comme on dit aussi en pareil cas, des *permutations* entre $M_1, \ldots, M_n$; cela veut dire que, dans notre tableau, la seconde ligne (celle qui donne les valeurs de f) et la troisième (qui donne les valeurs de g) sont, comme la première, formées des symboles $M_1, \ldots, M_n$, rangés simplement dans un ordre différent de celui où ils figurent dans la première ligne. En effet, s'il n'en était pas ainsi, certains types de mariage disparaîtraient dès la seconde génération. Ceci montre déjà

réductible, et se compose de deux sous-populations, formées, l'une des classes A et B, l'autre des classes C et D. Le tableau des fonctions f et g pour cette société est le suivant :

$$\begin{array}{rcccc} & M_1 & M_2 & M_3 & M_4 \\ f(M_i) = & M_2 & M_1 & M_4 & M_3 \\ g(M_i) = & M_1 & M_2 & M_3 & M_4 \end{array}$$

Supposer qu'on a affaire à une société irréductible, c'est supposer, dans le langage de la théorie des groupes, que le groupe défini ci-dessus (groupe abélien de permutations engendré par f et g) est *transitif*. Un tel groupe, s'il est cyclique, est de structure extrêmement simple; si c'est un produit direct de deux groupes cycliques, les possibilités sont plus variées, et les principes de classification à employer sont plus compliqués; mais, en tout cas, ces questions peuvent être traitées suivant des méthodes connues. Nous nous bornerons ici à énoncer les résultats qu'on obtient dans le cas d'un groupe cyclique. Il est nécessaire pour cela d'indiquer le principe bien connu de la numération modulo n.

Soit n un entier quelconque. Calculer modulo n, c'est calculer en remplaçant toujours tout nombre par le reste qu'il laisse dans la division par n. Par exemple, la « preuve par 9 » bien connue en arithmétique élémentaire consiste à calculer modulo 9. De même, si l'on convient de calculer modulo 10, et qu'on ait à ajouter 8 et 7, on écrit 5; si l'on a à multiplier 3 par 4, on écrit 2; si l'on a à multiplier 2 par 5, on écrit 0; etc. Cela s'écrit ainsi : $8+7\equiv 5 \pmod{10}$; $3\times 4 \equiv 2 \pmod{10}$; $2\times 5 \equiv 0 \pmod{10}$; etc.; il est convenu, dans tout calcul de ce genre, de remplacer le signe $=$ par le signe $\equiv$ (qui se lit « congru à »). Dans le calcul modulo 10, on n'écrit jamais 10 ni un nombre plus grand que 10, de sorte qu'il n'y a, dans ce calcul, que 10 nombres, à savoir 0, 1, 2, ..., 9.

Reprenons donc le cas d'une société irréductible à groupe cyclique. Alors il est possible de distinguer dans cette société un certain nombre n de classes, et de les numéroter de 0 à $n-1$ de telle sorte qu'un homme de classe x épouse toujours une femme de classe $x+a \pmod{n}$, et que les enfants d'une femme de classe x soient toujours de classe $x+b \pmod{n}$, a et b étant deux nombres fixes, et tous les calculs étant faits modulo n. Par exemple, dans le système à échange généralisé décrit plus haut, on a $n=4$, $a=1$, $b=1$, comme on le voit en numérotant les classes A, B, C, D par 0, 1, 2, 3, respectivement.

Nous allons maintenant montrer comment on peut formuler