UNIVERSITE Joseph FOURIER
Institut FOURIER
URA188 du CNRS

IREM DE GRENOBLE

CONFERENCES DE MATHEMATIQUES
IREM Institut FOURIER 1993

THEORIE DES INVARIANTS

Cycle de trois conférences **de Michel BRION**

12, 19 et 26 mai 1993

INTRODUCTION

La théorie des invariants a eu son heure de gloire au cours du XIXème siècle pour être délaissée au début du XXème et resurgir depuis cinquante ans : d'abord dans les travaux de H.WEYL, en liaison avec la théorie des groupes classiques, puis dans le cadre de la géométrie algébrique, sous l'impulsion de D. MUMFORD.

On se propose dans cet exposé de reprendre la théorie à ses origines, telle qu'elle a été créée par G.BOOLE (1815-1864), et surtout A. CAYLEY(1821-1895) et J. J. SYLVESTER (1814-1897). On restera par conséquent assez dans le style de l'époque, en essayant de traduire la terminologie du moment, principalement marquée par une certaine répugnance à la manipulation des indices et des symboles de sommation.

A titre d'exemple, on appelait à l'époque **forme** un polynôme homogène dont les coefficients appartiennent à un domaine qui n'est pas précisé. On peut considérer qu'il s'agit du corps des nombres complexes, bien que la notion de corps ne fût pas employée à l'époque. En tout cas pour l'exposé, les coefficients seront considérés comme complexes. Une forme sera dite **binaire** (resp.**ternaire**), si c'est un polynôme à deux (resp. trois) indéterminées. Elle sera dite **linéaire, quadratique, cubique** selon quelle est de degré total 1, 2 ou 3, **biquadratique ou quartique** si son degré total est 4.

Une forme binaire de degré p s'écrit alors sous la forme suivante qui introduit des coefficients du binôme :

$$u(x,y) = ax^p + b\,px^{p-1}y + c\,\frac{p(p-1)}{2}x^{p-2}y^2 + \ldots + t\,v^p$$

ce qu'on écrirait aujourd'hui : $u(x,y) = \sum_{j=0}^{p} \binom{p}{j} a_j x^{p-j}y^j$.

PREMIERE PARTIE

NAISSANCE DE LA THEORIE

Dans son article initial de 1843[BOOLE], G. BOOLE remarque que si on effectue dans l'expression ci-dessus de la forme binaire la substitution linéaire

$x = lX + mY$ & $y = l'X + m'Y$,

on obtient une forme binaire de même degré U(X,Y). Il utilise alors la notation symbolique

$u(x,y) = (a_0,a_1,\ldots,a_p)(x,y) = (A_0,A_1,\ldots,A_p)(X,Y) = U(X,Y)$.

Il remarque que les A_i sont fonction des a_j et des paramètres de la substitution l, m, l',m'.

Dans le cas d'une forme linéaire, (p = 1) on a

$A_0 = a_0l + a_1l'$ & $A_1 = a_0m + a_1m'$.

Dans le cas quadratique (p = 2) avec $u(x,y) = a_0x^2 + 2a_1xy + a_2y^2$

$u(x,y) = a_0(lX + mY)^2 + 2a_1(lX + mY)(l'X + m'Y) + a_2(l'X + m'Y)^2$ il trouve :

$A_0 = a_0l^2 + 2a_1ll' + a_2l'^2$

$A_1 = a_0lm + a_1(lm' + l'm) + a_2l'm'$

$A_2 = a_0m^2 + 2a_1mm' + a_2m'^2$

puis plus généralement que les A_i sont des polynômes en les paramètres de la substitution et sont linéaires en les a_j.

Cela amène à poser la définition initiale d'un invariant de forme binaire (définition dûe à CAYLEY) :

DEFINITION.- On appelle **invariant des formes binaires de degré p** un polynôme à coefficients complexes $f(a_0, a_1, \ldots, a_p)$ qui se transforme par les substitutions linéaires sous la forme

$$f(a_0,a_1,\ldots,a_p) \rightarrow f(A_0,A_1,\ldots,A_p) = f(a_0,a_1,\ldots,a_p) \times \Phi(l, l', m, m')$$

où $\Phi(l, l', m, m')$ est un polynôme qui dépend de f et de p.

Cette définition peut paraître arbitraire. Elle est cependant naturelle, comme le montrent les premiers exemples :
Le plus célèbre d'entre eux, et le plus immédiat, est le **discriminant** d'une forme binaire.
Toute forme binaire telle que $a_0 \neq 0$ peut se mettre sous la forme

$$u(x, y) = a_0(x - \alpha_1 y)(x - \alpha_2 y) \ldots (x - \alpha_p y),$$

où les α_j sont les zéros complexes du polynôme

$$X^p + p\frac{a_1}{a_0} X^{p-1} + \frac{a_2}{a_0}\frac{p(p-1)}{2} X^{p-2} + \ldots + \frac{a_p}{a_0}.$$

Par extension, si j est le plus petit entier tel que a_{p-j} soit non nul, on dira que la forme admet j zéros à l'infini.
Dans le cas où il n'y a pas de zéro à l'infini, on définit le discriminant de la forme comme la quantité

$$D(u) = a_0^{2(p-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

La quantité dans le produit est invariante par permutation des racines du polynôme. C'est donc un polynôme en les fonction symétriques élémentaires des racines, donc en les $\frac{a_j}{a_0}$. Il en résulte que D est un polynôme à coefficients entiers en les a_j. Le degré de ce polynôme est 2(p - 1). A partir de là on obtient la définition générale du discriminant puisqu'il suffit d'y annuler les premiers coefficients dans le cas d'existence de zéros à l'infini.

Le théorème de BOOLE s'énonce alors :

$$D(A_0, A_1, \ldots, A_p) = (lm' - l'm)^{p(p-1)} D(a_0, a_1, \ldots, a_p).$$

Cette formule conduit à considérer un invariant comme une fonction des racines de la forme, la condition de nullité de l'invariant s'exprimant en termes de propriétés projectives des racines. En effet, si les racines de u sont les α_i, les racines de U sont les transformées des racines de u par la transformation homographique $z \to (m'z - m)/(-l'z - l')$.

Le discriminant est nul si et seulement si le polynôme de u admet une racine multiple, propriété qui est invariante par transformation homographique.
On désigne par $\mathbb{P}^1$ la droite projective complexe, quotient de $\mathbb{C}\times\mathbb{C} \setminus \{(0,0)\}$ par la relation de colinéarité complexe. Cet espace peut être considéré comme $\mathbb{C}$

auquel on ajoute un point à l'infini. Une transformation homographique est l'application induite par un automorphisme linéaire de $\mathbb{C}\times\mathbb{C}$. [Voir l'annexe] Un point de $\mathbb{P}^1$ peut être envoyé n'importe où dans $\mathbb{P}^1$ par une homographie. Deux points distincts peuvent être envoyés sur n'importe quel doublet de points, à condition que ceux-ci soient distincts Etant donnés trois points distincts, il existe une homographie et une seule qui les envoie sur trois points distincts donnés. Par contre on ne peut pas envoyer quatre points distincts sur quatre points distincts donnés, simplement parce que tout homographie conserve le birapport de quatre points listés dans un ordre donné.
[Voir annexe sur Droite projective complexe et birapport]

LES INVARIANTS DE CAYLEY

A partir de ces données, CAYLEY a identifié en 1849 un premier invariant pour une forme quartique $u(x,y) = ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$:

$$I(a,b,c,d,e) = ae - 4bd + 3c^2.$$

Dans une lettre à CAYLEY, BOOLE lui dit avoir trouvé un autre invariant, sans donner de justification, à savoir

$$J(a,b,c,d,e) = ace - ad^2 - b^2e - c^2 + 2bcd.$$

En terme géométriques, on peut interpréter ces invariants comme suit :

L'invariant I est nul si et seulement si les quatre racines du polynôme ont un birapport égal à -j ou $-j^2$, j désignant la racine cubique canonique de l'unité. On dit dans ce cas que les quatre racines sont en **division équiharmonique.**

L'invariant J est nul si et seulement les quatre racines sont en **division harmonique,** c'est-à-dire si leur birapport est égal à l'un des nombres -1, 2 ou 1/2.

De plus ces deux invariants sont en quelque sorte des "invariants de base", ce qui signifie que tout invariant d'une forme quartique est un polynôme en I et J. Par exemple le discriminant satisfait à $D = I^3 - 27J^2$.

CAYLEY a décrit les invariants et a donné une approche de leur étude, mais avec des erreurs. Celles-ci ont provoqué de nombreuses disputes entre mathématiciens.

Voici les principaux énoncés de CAYLEY :

THEOREME.- Soit $f(a_0,a_1,...,a_j,...,a_p)$ un invariant de degré d pour une forme binaire de degré p.
I Le polynôme $f(a_0,a_1,...,a_j,...,a_p)$ est homogène en les a_i.
II.Le polynôme $\Phi(l, l', m, m')$ associé à la transformation de $f(a_0,a_1,...,a_j,...,a_p)$ est la puissance (pd/2)-ième du déterminant de la transformation.
III.Le polynôme $f(a_0,a_1,...,a_j,...,a_p)$ est isobare en les a_i, avec la signification suivante : si à chacun des coefficients a_i on affecte le poids entier i, le poids d'un monôme $\prod_0^p a_j^{n(j)}$ est la somme $\sum_0^p jn(j)$. En ce sens les monômes intervenant dans $f(a_0,a_1,...,a_j,...,a_p)$ ont tous le même poids dp/2.

☞ I.On considère les substitutions linéaires induites par les homothéties. Si $f(a_0,a_1,...,a_j,...,a_p)$ est un invariant de degré d, il existe un polynôme en une variable Ψ tel que pour tout $\lambda\in\mathbb{C}$ on ait $\Phi(\lambda,0,0,\lambda) = \Psi(\lambda)$. De plus on a la relation $\Psi(\lambda)\Psi(\nu) = \Psi(\lambda\nu)$.
Par différentiation par rapport à λ on obtient $\nu\Psi'(\nu) = \Psi'(1)\Psi(\nu)$, ce qui implique que $\Psi(\nu)$ est de la forme $\gamma\nu^{\Psi'(1)}$ et $\gamma = 1$ d'après la valeur en 1.
II. En termes modernes [DIEUDONNE ET CARREL, chap.2, p.21], on a un homomorphisme de $GL(2,\mathbb{C})$ dans $\mathbb{C}^*$ qui s'exprime sous forme polynomiale en les coefficients des matrices. Un tel homomorphisme est une puissance du déterminant. Par ailleurs le degré total de f est dp, ce qui permet de conclure.
III. On considère les substitutions de la forme [x = X & y = λY] dont le déterminant est λ. Par définition et d'après II on a l'égalité

$$f(a_0,\lambda a_1, ...,\lambda^j a_j,...,\lambda^p a_p) = \lambda^{dp/2} f(a_0,a_1,...,a_j,...,a_p).$$

Par ailleurs, si a_j est de poids j, le poids de $\prod_0^p a_j^{n(j)}$ est la somme $\sum_0^p jn(j)$. ✍

COROLLAIRE.- La dimension de l'espace vectoriel des invariants de degré d d'une forme binaire de degré p est inférieure ou égale au nombre de solutions en entiers naturels du sytème $[\sum_0^p n(j) = d \;\&\; \sum_0^p jn(j) = dp/2]$.

NOTATION.- On désigne respectivement par Ω et O les deux opérateurs différentiels homogènes et isobares

$$\Omega = \sum_{1}^{p} j a_{j-1} \frac{\partial}{\partial a_j} \qquad O = \sum_{0}^{p-1} (p-j) a_{j+1} \frac{\partial}{\partial a_j}.$$

Le premier est de degré 0 et de poids -1, le second de degré 0 et de poids 1.
On note $\mathbf{U}(d,p)$ l'espace vectoriel complexe des polynômes homogènes de degré d en $a_0,a_1,\ldots,a_j,\ldots,a_p$. Pour tout $w \in 0. .dp$ on note $\mathbf{V}(w,d,p)$ le sous-espace vectoriel de $\mathbf{U}(d,p)$ engendré par les polynômes de degré d et de poids w.

REMARQUES.- Il est clair d'une part que $\mathbf{U}(d,p)$ est la somme directe des $\mathbf{V}(w,d,p)$, d'autre part que $\Phi: \mathbf{U}(d,p) \to \mathbf{U}(d,p)$ défini par $a_j \to a_{p-j}$ est un automorphisme involutif tel que $\forall w \in 0. .dp\ \Phi(\mathbf{V}(w,d,p)) = \mathbf{V}(dp - w,d,p)$.
En particulier la restriction de Φ à $\mathbf{V}(dp/2,d,p)$ est un automorphisme de ce sous-espace. Enfin un calcul simple montre que $\Omega = \Phi \circ O \circ \Phi$.

Avec ces notations, on a le théorème suivant, démontré par SYLVESTER, ARONHOLD, EISENSTEIN...

THEOREME A.-Les trois énoncés suivants sont équivalents :

I. Le polynôme I est un invariant de degré d des formes binaires de degré p;

II. Le polynôme I est de degré d, annulé par Ω et par $\mathbf{O}$;

III Le polynôme I est isobare de poids dp/2 et est annulé par Ω .

☞ On considère les substitutions linéaires de la forme $[x = X \ \&\ y = \lambda X + Y]$ dans un premier temps, de la forme $[x = X + \mu Y \ \&\ y = Y]$ dans un second temps. Le déterminant de chacune de ces substitutions est 1. Dans le premier cas une telle substitution transforme les a_j en les $A_s(\lambda)$. Un calcul direct montre qu'on a les formules :

$$A_s(\lambda) = \sum_{j=0}^{p-s} \binom{p-s}{j} \mu^j a_{j+s} \qquad (\bullet)$$

Soit alors I un polynôme homogène de degré d et isobare de poids dp/2.
On a simplement

$$\left(\frac{\partial}{\partial \lambda}\right)_{\lambda=0} I(A_0(\lambda),\ldots,A_p(\lambda)) = \sum_{j=0}^{p} (p-j) a_{j+1} \frac{\partial I}{\partial a_j}(a_0,a_1,\ \ldots,a_j,\ldots,a_p).$$

$$(\frac{\partial}{\partial\lambda})_{\lambda=0}\ I(A_0(\lambda),...,A_p(\lambda)) = O(I)(a_0,a_1,\ ...,a_j,...,a_p),$$

En faisant un peu mieux à partir de la relation (•), on établit l'égalité

$$\exp(m\Omega)I(a_0,a_1,\ ...,a_j,...,a_p) = I(A_0(m),...,A_p(m))$$

$$\exp(\lambda O)I(a_0,a_1,\ ...,a_j,...,a_p) = I(A_0(\lambda),...,A_p(\lambda)).$$

Procédant de même avec les substitutions du second type, celles-ci transforme les a_j en les $B_t(\mu)$ avec les propriétés :

$$B_t(\mu) = \sum_{j=0}^{s} \binom{s}{j} \mu^j a_{s-j} \qquad (\bullet\bullet)$$

Pour le même polynôme I on obtient

$$(\frac{\partial}{\partial\mu})_{\mu=0}\ I(B_0(\mu),...,B_p(\mu)) = \sum_{s=0}^{p} s a_{s-1} \frac{\partial I}{\partial a_s}(a_0,a_1,\ ...,a_s,...,a_p).$$

$$(\frac{\partial}{\partial\mu})_{\mu=0}\ I(B_0(\mu),...,B_p(\mu)) = \Omega(I)(a_0,a_1,\ ...,a_j,...,a_p),$$

En faisant un peu mieux à partir de la relation (••), on établit l'égalité

$$\exp(\mu\Omega)I(a_0,a_1,\ ...,a_j,...,a_p) = I(B_0(\mu),...,B_p(\mu)).$$

Encore une remarque: toute matrice carrée d'ordre 2 à coefficients complexes et de déterminant 1 s'écrit comme un produit d'au plus trois matrices :

$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix} \times \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}$, ce qui permet de décomposer toute substitution en un produit par une homothétie (tout élément de $\mathbb{C}$ est un carré) de au plus trois telles matrices.

Cela étant, si I est un invariant, on a pour tout λ et pour tout μ les identités

$$\exp(\lambda O)I(a_0,a_1,\ ...,a_j,...,a_p) = I(a_0,a_1,\ ...,a_j,...,a_p),$$

$$\exp(\mu\Omega)I(a_0,a_1,\ ...,a_j,...,a_p) = I(a_0,a_1,\ ...,a_j,...,a_p),$$

ce qui implique $O(I) = \Omega(I) = 0$.

Réciproquement si $\Omega(I) = O(I) = 0$, alors pour tout λ et pour tout μ on a

$$\exp(\lambda O)I(a_0,a_1,\ ...,a_j,...,a_p) = \exp(\mu\Omega)I(a_0,a_1,\ ...,a_j,...,a_p) = I(a_0,a_1,\ ...,a_j,...,a_p)$$

et on conclut via la dernière remarque que I est un invariant, ce qui prouve l'équivalence de I et II et l'implication I ⇒ III.

III⇒II. Cette propriété sera un corollaire de résultats ultérieurs. ✍

REMARQUE.- Il résulte de ce théorème que pour tout p et tout d il existe une base de **W**(d,p) formée de polynômes à coefficients entiers rationnels, car les

coefficients du sytème linéaire défini par l'annulation de Ω et de O sont entiers.

SECONDE PARTIE

DENOMBREMENT D'INVARIANTS

On se propose maintenant de déterminer la dimension de l'espace vectoriel complexe $\mathbf{W}(d,p)$ des invariants de degré d d'une forme binaire de degré p, selon la méthode découverte par CAYLEY[CAYLEY,4] et mise au point par SYLVESTER [SYLVESTER,1]. Dans le langage du siècle dernier, cette dimension est le nombre d'invariants asyzygétiques de degré d.

THEOREME B.- Pour tout triplet de nombre naturels (w,d,p) soit (w;d,p) le nombre de solutions en nombres entiers du système d'équations

$$[\sum_{0}^{p} n(j) = d \;\&\; \sum_{0}^{p} jn(j) = w].$$

La dimension de $\mathbf{W}(d,p)$ est le nombre (dp/2;d,p) - (-1 + dp/2;d,p).

☞ Soit $\mathbf{V}(w;d,p)$ l'espace vectoriel des polynômes homogènes en les p+1 indéterminées $a_0,a_1,...,a_j,...,a_p$ qui sont de degré d et isobares de poids w. L'idée de CAYLEY est de considérer l'application Ω: $\mathbf{V}(w;d,p) \rightarrow \mathbf{V}(w;d,p)$ dont le noyau est $\mathbf{W}(d,p)$. Le Théorème repose alors uniquement sur la surjectivité de cette application qui est utilisée implicitement par CAYLEY. La preuve de la surjectivité de Ω fut établie par SYLVESTER. Elle repose sur les deux lemmes et la proposition techniques suivants . ✍

LEMME.- Soit M un polynôme homogène en $a_0,a_1,...,a_j,...,a_p$, de degré d et isobare de poids w. Alors on a $[\Omega O - O\Omega](M) = (dp - 2w)M$.

☞ Il suffit de vérifier par un calcul direct l'identité :

$$\Omega O - O\Omega = pa_0\partial_0 + \sum_{j=1}^{p-1} (p - 2j)a_j\partial_j .- pa_p\partial_p$$

Appliquant cette identité à un monôme $U = a_0^{n(0)}a_1^{n(1)}a_0^{n(0)}...a_p^{n(p)}$ de degré d et de poids w on obtient

$$[\Omega O - O\Omega](U) = \{pn(0) + \sum_{j=1}^{p-1} (p - 2j)n(j) - pn(p)\}U = (dp - 2w)U$$ ✍

LEMME.- Soit M un polynôme homogène de degré d et isobare de poids w annulé par Ω. Soit e = dp - 2w. Alors

$$\forall m \in \mathbb{N}, \Omega^m O^m(M) = (m)!(e)(e-1)...(e-m+1)M .$$

☞ Il suffit de faire le calcul à partir du lemme précédent. ✍

PROPOSITION.- Pour tout w > dp/2 la restriction de l'application Ω: **V**(w,d,p) → **V**(w - 1,d,p) est injective. Pour tout w < dp/2 la restriction de l'application O: **V**(w,d,p) → **V**(w + 1,d,p) est injective.

☞ Soit I∈V(w,d,p) tel que Ω(I) = 0. D'après le lemme, pour m assez grand on a $\Omega^m O^m(I) = (m)!(e)(e-1)...(e-m+1)I$, et le coefficient de I dans cette expression n'est pas nul. Mais pour m assez grand on a Ω∘Φ(I) = Φ∘O(I) = 0, donc I = 0. La seconde assertion résulte de la remarque qui suit le Théorème de CAYLEY. ✍

Munis de ce résultats intermédiaires on peut achever la démonstration des deux Théorèmes :

Preuve de III ⇒ II du Théorème A de SYLVESTER : Il suffit de démontrer la nullité de O(I) dès que I est annulé par Ω et appartient à **V**(dp/2,d,p). Or dans ce cas on a Ω∘O(I) = 0 et la proposition précédente implique l'injectivté de la restriction Ω: **V**(dp/2+1,d,p) → **V**(dp/2,d,p). ✍

Preuve du Théorème B de SYLVESTER : Pour tout w∈0. .dp la dimension de **V**(w,d,p) est (w;d,p). Soit λ(w) la dimension du noyau de la restriction de Ω à **V**(w,d,p). On sait d'après la proposition technique ci-dessus que pour tout w > dp/2 le nombre λ(w) est nul. De plus on a λ(0) = (0;d,p) et pour tout j≤ dp/2 on a évidemment λ(w) ≥ (w;d,p) - (w + 1;d,p). On a donc

$$(dp/2;d,p) \leq \sum_{w=0}^{dp/2} \lambda(w).$$

Pour tout w∈0. .dp/2 soit F(w) une base du noyau de la restriction de Ω à **V**(w,d,p) et soit G(w)= {x(w,1), . . . ,x(w,λ(w))} la famille image de F(w) par $O^{(dp/2) - w}$. D'après la proposition technique, la restriction de $O^{(dp/2) - w}$ à V(w,d,p) est injectiive, ce qui implique que cette famille est libre. En fait la

famille $\{x(w,j) \mid w\in 0. .dp/2, \forall w,j\in 1. .\lambda(w)\}$ est libre dans $\mathbf{V}(dp/2,d,p)$, comme on le voit en appliquant à une combinaison linéaire nulle de cette famille la séquence des puissances de Ω et en utilisant le second lemme technique.

On a donc $(dp/2;d,p) \geq \sum_{w=0}^{dp/2} \lambda(w)$ et par conséquent égalité.

Celle-ci implique pour tout $w\in 0. .dp/2$ l'égalité $\lambda(w) = (w;d,p) - (w + 1;d,p)$. Ceci assure pour tout $w\in 0. .(dp/2 -1)$ la surjectivité de la restriction de Ω à $\mathbf{V}(w,d,p)$ et la conclusion du Théorème. ✍

Du point de vue historique, on peut citer deux textes qui illustrent ce théorème

•CAYLEY[CAYLEY 4,p.256] : En particulier, une fonction I, de degré i et isobare de poids ip/2 telle que $\Omega(I) = 0$ est un invariant.
Je prends maintenant pour I la fonction la plus générale des coefficients,de degré i et de poids ip/2; alors $\Omega(I)$ est une fonction de degré i et de poids (ip/2)-1 et les coefficients arbitraires de la fonction I doivent être déterminés de sorte que $\Omega(I) = 0$. Le nombre de coefficients arbitraires est égal au nombre de termes dans I et le nombre d'équations à satisfaire est égal au nombre de termes de $\Omega(I)$; donc le nombre de coefficients arbitriares qui restent indéterminés est egal au nombre de termes dans I, moins le nombre de termes dans $\Omega(I)$; et M. la différence en question est égale au nombre d'invariants asyzygétiques, i-e le nombre d'invariants asyzygétiques de degré i et de poids ip/2, est égal au nombre de termes de degré i et de poids ip/2 moins le nombre de termes de degré i et de poids (ip/2)-1.

•SYLVESTER[SYLVESTER 2, p.72] . Il y a trois méthodes pour traiter la question de la liste des invariants et covariants fondamentaux : la réaliste, la symbolique et la fataliste ou peprotique. Dans la première de ces méthodes, (explicite ou réaliste) les formes dérivées, en notation complète ou abrégée, sont exhibées grâce à des formes canoniques. C'est ainsi que j'ai établi la liste pour les cubiques ternaires et pour les quartiques et quintiques binaires, dans mes premiers articles au Philosophical Magazine, au Cambridge et Dublin Mathematical Journal, et dans ma Trilogie, publiée dans les Philosophical Transactions. Dans la seconde Méthode, (symbolique, schématique ou embryonique), les formes dérivées ne sont pas exhibées, mais sont étudiées au moyen d'un processus symbolique qui fournit la clé de leur existence (c'est la méthode suivie , avec un aussi grand succès par le professeur GORDAN). LA troisième (déontologique ou peprotique), qui précède la seconde dans l'ordre chronologique, est la méthode indiquée par le professeur CAYLEY, dans son mémorable second article sur les formes, publié dans les Philosophical Transactions, qui, sans doute à cause d'une erreur commise par son illustre auteur, est tombée dans l'oubli, et dont la validité même a été mise en question. Dans cette méthode, les expressions des formes dérivées, et les procédés par lesquels elles ont été mises à jour, sont ignorés tous les deux: ces formes sont considérées comme des entités purement arithmétiques, et c'est par le moyen de l'instrument le plus subtil pour soumettre la nature et la raison à la question - une équation aux dérivées partielles - que les lois numériques auxquelles ces formes sont assujetties, se trouvent dépendre d'un problème de partition des nombres.

REMARQUE.- Le nombre (w;d,p) s'interprète en termes de partition d'entiers. En effet, si on effectue dans le système $[\sum_0^p n(j) = d \;\&\; \sum_0^p jn(j) = w]$ le changement de variable $m(j) = \sum_1^{p-j} n(i)$, le nombre (w;d,p) est le nombre de solutions en entiers naturels du système $\begin{cases} m(1) \leq d \;\&\; \sum_1^p m(j) = w \\ m(1) \geq m(2) \geq \ldots \geq m(p) \end{cases}$

C'est le nombre de partitions de w en p sommants inférieurs ou égaux à d.
La représentation d'une telle partition sous forme de diagramme montre immédiatement qu'on a l'égalité (w;d,p) = (w;p,d).
Ceci s'énonce sous la forme de la loi de réciprocité de HERMITE :

COROLLAIRE.- Le nombre d'invariants asyzygétiques (i-e linéairement indépendants) de degré d d'une forme binaire de degré p est égal au nombre d'invariants asyzygétiques de degré p d'une forme binaire de degré d.

☞ Ce nombre est (dp/2;d,p) - (-1 + dp/2,d,p). ✍

THEOREME- Pour tout entier p et tout entier d la fraction rationnelle

$$\phi(d,p,X) = \prod_1^d \frac{1-X^{p+j}}{1-X^j}$$

est un polynôme dit polynôme de GAUSS, et pour tout $w \in \mathbb{N}$, le nombre (w;d,p) est le coeficient de z^w dans le polynôme de GAUSS $\phi(d,p,z)$.

☞ On pose $u(i,p,z) = \sum_0^{ip} (w;i,p)z^w$.

La série entière formelle en x, à coefficients polynomiaux en z, $\sum_0^\infty u(i,p,z)x^i$ est la somme de la famille des $z^{n(1) + 2n(2) + \ldots + pn(p)}\, x^{n(0) + n(1) + n(2) + \ldots + n(p)}$
C'est donc la fraction rationnelle en x et z $\frac{1}{(1-x)(1-xz)(1-xz^2)\ldots(1-xz^p)}$.
Dans cette dernière fraction, le remplacement de x par xz donne l'identité :

$$\sum_0^\infty u(i,p,z)x^iz^i = \frac{1}{(1-xz)(1-xz^2)\ldots(1-xz^{p+1})}$$
$$= \frac{(1-x)}{(1-xz^{p+1})} \times \frac{1}{(1-x)(1-xz)(1-xz^2)\ldots(1-xz^p)}$$

$$\sum_0^\infty u(i,p,z)x^iz^i = \frac{(1 - x)}{(1 - xz^{p+1})} \times \sum_0^\infty u(i,p,z)x^i.$$

D'où $(1 - xz^{p+1})\sum_0^\infty u(i,p,z)x^iz^i = (1 - x)\sum_0^\infty u(i,p,z)x^i$.

Identifiant les coefficients des x^i on obtient $u(0,p,z) = 1$ et pour tout $i \geq 1$:

$u(i,p,z)\ z^i - z^{p+i}u(i-1,p,z) = u(i,p,z) - u(i-1,p,z)$,

$u(i,p,z)\ (1 - z) = u(i-1,p,z)\ (1 - z^{p+i})$.

On en déduit par récurrence sur i le résultat du Théorème. ✍

COROLLAIRE.- Le nombre d'invariants asyzygétiques de degré d associés à une forme binaire de degré p est le coefficient de $z^{dp/2}$ dans le développement de la fraction rationnelle $\frac{(1 - z^{p+1})...(1 - z^{p+d})}{(1- z^2)...(1- z^d)}$.

C'est aussi le coefficient de $z^{dp/2}$ dans le développement de la fraction rationnelle $\frac{(1 - z^{d+1})...(1 - z^{p+d})}{(1- z^2)...(1- z^p)}$.

☞ La première assertion résulte du Théorème de CAYLEY-SYLVESTER, la seconde de la formule de réciprocité de HERMITE. ✍

EXEMPLES POUR LES PREMIERES VALEURS DE P

1. Il n'y a pas d'invariant non constant pour les formes linéaires binaires.

2. Le coefficient de z^d dans $\backslash F((1 - z^{d+1})...(1 - z^{d+2});(1 - z^2))$ est le coefficient de z^d dans $\frac{1}{(1 - z^2)}$. C'est donc 1 si d est pair et 0 si d est impair. Une forme quadratique n'a donc pas d'invariant de degré impair et pour tout entier n, l'espace des invariants de degré 2n est engendré par la puissance n-ième du discriminant.

3. Le coefficient de $z^{3d/2}$ dans $\frac{(1 - z^{d+1})(1 - z^{d+2})(1 - z^{d+3})}{(1 - z^2)(1- z^3)}$ est le coefficient de $z^{3d/2}$ dans $\frac{(1 - z^{d+1} - z^{d+2} - z^{d+3})}{(1 - z^2)(1- z^3)} = \frac{1}{(1 - z^2)(1- z^3)} - \frac{z^{d+1}}{(1 - z^2)(1- z)}$. C'est donc le coefficient de $z^{3d/2}$ dans $\frac{1}{(1 - z^2)(1- z^3)}$ moins le coefficient de $z^{d/2}$ dans $\frac{z}{(1 - z^2)(1- z)}$.

C'est aussi le coefficient de $z^{3d/2}$ dans l'expression

$$\frac{1}{(1 - z^2)(1- z^3)} - \frac{z^3}{(1 - z^6)(1- z^3)} = \frac{1 + z^2 - z^3 - z^4}{(1 - z^6)(1- z^3)}.$$

En définitive ce nombre est le coefficient de $z^{3d/2}$ dans $\frac{1}{1 - z^6}$, c'est-à-dire le coefficient de z^d dans $\frac{1}{1 - z^4}$. On en conclut d'une part que si d n'est pas multiple de 4, il n'y a pas d'invariant de degré d et que si d = 4e, l'espace des invariants de degré d est engendré par la puissance e-ième du discriminant.

COROLLAIRE.- Soit p un entier. Il n'y a pas d'invariant de degré 1 pour les formes binaires de degré p. Il y a un invariant de degré 2 si et seulement si p est pair et un invariant de degré 3 si et seulement si p est multiple de 4.

☞ C'est une conséquence de la loi de réciprocité de HERMITE. ✍

4. On cherche le coefficient de z^{2d} dans $\frac{(1 - z^{d+1})(1 - z^{d+2})(1 - z^{d+3})(1 - z^{d+4})}{(1- z^2)(1- z^3)(1- z^4)}$.

C'est le coefficient de z^{2d} dans $\frac{(1 - z^{d+1} - z^{d+2} - z^{d+3} - z^{d+4})}{(1- z^2)(1- z^3)(1- z^4)}$,

ou dans $\frac{1}{(1- z^2)(1- z^3)(1- z^4)} - \frac{z^{d+1}}{(1 - z)(1- z^2)(1- z^3)(1- z^4)}$,

ou dans $\frac{1}{(1- z^2)(1- z^3)(1- z^4)} - \frac{z^2}{(1- z^2)(1- z^4)(1- z^6)}$,

ou dans $\frac{1 - z^2 + z^3}{(1- z^2)(1- z^4)(1- z^6)}$ ou, pour raison de parité, dans $\frac{1}{(1- z^4)(1- z^6)}$.

C'est le coefficient de z^d dans $\frac{1}{(1- z^2)(1- z^3)}$.

Connaissant déjà les invariants I et J qui sont algébriquement indépendants et de degrés respectifs 2 et 3, on conclut que les invariants d'une forme binaire quartique sont les polynômes en I et J, et d'après la formule de réciprocité que toute forme binaire de degré supérieur ou égal à 2 admet un invariant de degré 4.

FONCTION GENERATRICE DE L'ALGEBRE DES INVARIANTS

DEFINITION.- Pour tout entier p, la fonction génératrice de l'algèbre des invariants de la forme binaire de degré p est la fonction $z \to F(p,z)$ dont le développement en série entière formelle est $\sum_0^\infty \dim_{\mathbb{C}}(\mathbf{W}(d,p))z^d$.

Les exemples ci-dessus montrent que les premières fonctions génératrices sont $F(1,z) = 1$, $F(2,z) = \frac{1}{1 - z^2}$, $F(3,z) = \frac{1}{1 - z^4}$, $F(4,z) = \frac{1}{(1 - z^2)(1 - z^3)}$.

On montre par le même type de calcul que les fonctions génératrices suivantes sont respectivement :

$$F(5,z) = \frac{1+z^{18}}{(1 - z^4)(1 - z^8)(1 - z^{12})} = \frac{1- z^{36}}{(1 - z^4)(1 - z^8)(1 - z^{12})(1 - z^{18})}$$

$$= 1 + z^4 + 2z^8 + 3z^{12} + 4z^{16} + z^{18} + ..$$

$$F(6,z) = \frac{1 + z^{15}}{(1 - z^2)(1 - z^4)(1 - z^6)(1 - z^{10})} = \frac{1 - z^{30}}{(1 - z^2)(1 - z^4)(1 - z^6)(1 - z^{10})(1 - z^{15})}$$

$$= 1 + z^2 + 2z^4 + 3z^6 + 3z^8 + 4z^{10} + 6z^{12} + 6z^{14} + z^{15} + ...$$

Dans le cas p = 5, on a un invariant I_4 de degré 4 qui engendre $\mathbf{W}(8,5)$. L'intersection de $\mathbf{W}(8,5)$ avec $\mathbb{C}[I_4]$ est $\mathbb{C}I_4^2$. Il existe donc un invariant I_8, irréductible de degré 8. L'intersection de $\mathbf{W}(12,5)$ et de $\mathbb{C}[I_4, I_8]$ est l'espace vectoriel engendré par $\{I_4^3, I_4I_8\}$. Il existe donc un invariant I_{12} irréductible de degré 12. L'espace $\mathbf{W}(18,5)$ est engendré par un invariant irréductible I_{18} car les degré des précédents invariants sont tous multiples de 4. D'après la seconde forme de la fraction rationnelle, la dimension de $\mathbf{W}(36,5)$ est d'une unité inférieure à la dimension de l'espace vectoriel engendré par les puissances adhoc de I_4, I_8 et I_{12} . On en déduit qu'il existe une relation (syzygie) entre ces invariants, c'est-à-dire que I_{18}^2 est un polynôme en I_4, I_8 et I_{12}.

De même, dans le cas p = 6, on obtient cinq invariants irréductibles I_2, I_4, I_6, I_{10} et I_{15} et une syzygie de degré 30, c'est-à-dire que I_{15}^2 est un polynôme en I_2, I_4, I_6, I_{10}.

Les cas p = 7 et p = 8 sont un peu plus douloureux. Les fonctions génératrices sont respectivement :

$$F(7,z) = \frac{1 + 2z^8 + 4z^{12} + 4z^{14} + 5z^{16} + 9z^{18} + 6z^{20} + 9z^{22} + 8z^{24} + 9z^{26} + 6z^{28}}{(1 - z^4)(1 - z^8)(1 - z^{12})^2(1 - z^{20})}$$

$$+ \frac{9z^{30} + 5z^{32} + 4z^{34} + 4z^{36} + 2z^{40} + z^{48}}{(1 - z^4)(1 - z^8)(1 - z^{12})^2(1 - z^{20})}.$$

$$F(8,z) = \frac{1 + z^8 + z^9 + z^{10} + z^{18}}{(1 - z^2)(1 - z^3)(1 - z^4)(1 - z^5)(1 - z^6)(1 - z^7)}.$$

A ce niveau on peut se poser la question de savoir si tous les invariants sont des polynômes en un nombre fini d'entre eux, autrement dit, en termes modernes, si l'algèbre des invariants est de type fini.

A cette question CAYLEY répondait négativement. Nous verrons dans ce qui suit qu'il s'est trompé, comme le montrent les travaux de HILBERT qui ont pratiquement réglé le problème des invariants, ou du moins ses aspects théoriques. Le début de l'argument de CAYLEY est le suivant :

> •[CAYLEY,4 p. 252] On peut remarquer qu'étant donné une équation aux dérivées partielles, ou un système de telles équations, il y aura toujours un nombre fini ν tel que pour tout système de ν intégrales indépendantes, toute autre intégrale est fonction (en général irrationnelle, seulement exprimable comme racine d'une équation) des ν intégrales indépendantes ; et si à ces ν intégrales on adjoint une seule autre intégrale qui n'est pas fonction rationnelle des ν intégrales, il est facile de voir que toute autre intégrale est fonction rationnelle des ν+1 integrales ; mais une telle intégrale n'est pas en général une fonction rationnelle et entière des ν + 1 intégrales ; et il n'y a pas en général de nombre fini d'intégrales, telle que tout autre intégrale soit une fonction rationnelle et entière de ces intégrales, i-e le nombre d'intégrales irréductibles est en général infini ; **et il semblerait que ce soit le cas dans la théorie des invariants.**

C'est l'assertion en gras ci-dessus qui est incorrecte.

GENERATEURS ET RELATIONS POUR LES ALGEBRES D'INVARIANTS

On adopte dans cette dernière partie la terminologie d'aujourd'hui, quitte à revenir sur les énoncés des précurseurs.

DEFINITIONS ET NOTATIONS DIVERSES.- Soient k un corps commutatif et A une sous-algèbre graduée de $k[x_1,\ldots,x_n]$. Un ensemble E d'éléments

homogènes de A est un système de générateurs de A si tout élément de A s'écrit comme un polynôme en les éléments de E.
Si l'algèbre A admet un système générateur fini (on dit alors qu'elle est de type fini), on désignera par $(a_1,...,a_m)$ un système générateur de A tel que a_1 soit de degré minimal dans A et pour tout $i\in 2..m$, a_i soit de degré minimal dans $A\backslash k[a_1,...,a_{i-1}]$.
Soit A une algèbre graduée de type fini munie d'un système générateur $(a_1,...,a_m)$. On appelle **relation** (ou syzygie) de A (associée à ce système) tout polynôme $P\in k[y_1,...y_m]$ tel que $P(a_1,...,a_m) = 0$ où les y_i sont algébriquement indépendants et pour tout $i\in 1..m$, y_i a pour degré le degré α_i de a_i.

LEMME.- avec les notations ci-dessus, l'ensemble des relations de A est l'idéal homogène I de $k[y_1,...y_m]$, noyau de l'homomorphisme surjectif d'algèbres $k[y_1,...y_m] \to A \to 0$ défini par $[\forall j\in 1..m,\ y_j \to a_j]$.

Si le noyau I est de type fini comme $k[y_1,...y_m]$-module, on s'en donne un système générateur fini d'éléments homogènes $(b_1,...b_{m_1})$ tel que b_1 soit de degré minimal et pour tout $j\in 2..m_1$, b_j soit de degré minimal dans $I\backslash < b_1,...,b_{j-1} >$, où on désigne par $< b_1,...,b_{j-1} >$ l'idéal de $k[y_1,...y_m]$ engendré par $b_1,...,b_{j-1}$.
On appelle alors secondes syzygies de A les éléments du noyau de l'homorphisme canonique de $k[y_1,...y_m]$-modules $\phi_2: \bigoplus_{j=0}^{m_1} (k[y_1,...y_m])z_j \to I$ défini par $z_j \to b_j$. Ce noyau est l'ensemble des solutions dans $(k[y_1,...y_m])^{m_1}$ de l'équation $\sum_1^{m_1} f_j b_j = 0$. C'est un $k[y_1,...y_m]$-module gradué. S'il admet un système générateur fini, on peut construire de la même façon les **troisièmes syzygies** de A et ainsi de suite tant que le noyau trouvé est de type fini.

CAYLEY avait repéré des secondes syzygies (resp. troisièmes syzygies) de la forme $\{c_{ij} = z_i b_j - z_j b_i \mid i < j\}$ (resp $d_{ijk} = c_{ij}z_k + c_{jk}kz_i - c_{ik}z_j \mid i< j < k\}$ les syzygies "automatiques". Son erreur fut de croire que les syzygies, a chaque niveau, étaient engendrées uniquement par celles-ci.

Du point de vue numérique, étant donnée une k-algèbre graduée B, la fonction génératrice F(B,Z) de B est par définition la fonction dont le

développement en série formelle est $\sum_{n=0}^{\infty} (\dim B_n) z^n$ où B_n est le k-espace vectoriel engendré par les termes homogènes de degré n de B.

La fonction génératrice de $k[y_1,...y_m]$ est la fraction rationnelle $\prod_{i=1}^{m1} (1- z^{\alpha_i})^{-1}$

A partir de la suite exacte $I \to k[y_1,...y_m] \to A \to 0$, on a la relation entre fonctions génratrices $F(A,z) + F(I,z) = F(k[y_1,...y_m],z)$. En ce qui concerne les secondes syzygies, on convient que le degré de chaque z_j est le degré e_j de b_j.

On a une suite exacte de modules gradués $J \to \bigoplus_{j=1}^{m_1} (k[y_1,...y_m])z_j \to I \to 0$. La fonction génératrice de $\bigoplus_{j=1}^{m_1} (k[y_1,...y_m])z_j$ est $\dfrac{\sum_{j=1}^{m_1} z^{e_j}}{\prod_{i=1}^{m} (1 - z^{\alpha_i})}$.

La fonction génératrice de A est donc la différence de fractions rationnelles

$\dfrac{\sum_{j=1}^{m_1} z^{e_j}}{\prod_{i=1}^{m} (1 - z^{\alpha_i})}$ - [fonction génératrice des secondes syzygies].

Si l'hypothèse de CAYLEY était correcte, les degré des syzygies "automatiques" de niveau t serait les sommes de t des e_j. Il en résulterait en bref que la fonction génératrice de l'algèbre des invariants serait de la forme $\prod_{i=1}^{m1} (1- z^{\varepsilon_i}) \bullet \prod_{i=1}^{m} (1- z^{\alpha_i})^{-1})$, ce qui n'est pas le cas, entre autres, pour les formes binaires de degrés p = 7 et p = 8.

Entre 1890 et 1893, HILBERT [D. HILBERT,1 & 2] a résolu le problème de finitutepour les algèbres d'invariants, au moins au plan théorique. On peut résumer ses résultats dans trois théorèmes suivants dont on ne donnera pas ici de démonsration.

THEOREME I.- Pour toute suite infinie de formes des n variables $x_1,x_2,...,x_n$, par exemple $F_1,F_2,F_3...$, il existe toujours un entier m tel que toute forme de la suite s'écrive

$$F = A_1F_1 + A_2F_2...+ A_mF_m,$$

où A_1, A_2, ..., A_m sont des formes appropriées de ces n variables.

THEOREME II.- Si on a un sytème d'équations

$$F_{t_1}X_1 + F_{t_2}X_2 + ... + F_{t_{m(1)}}X_{m(1)} = 0 \qquad (t= 1,2,...m),$$

où les coefficients sont des formes données en n variables, et où , sont m(1) formes à déterminer, il existe toujours un nombre fini m(2) de systèmes de solutions

$$X_1 =X_{1s},..., X_{m(1)} = X_{m(1)s} \qquad (s=1,2,...m(2)),$$

tel que toute autre solution homogène puisse s'écrire sous la forme

$$X_l = A_1X_{l\,1} + ... + A_{m(2)}X_{l\,m(2)},$$

où $A_1,A_2,...., A_{m(2)}$ sont des formes en n variables.

THEOREME III.- Si on a un sytème (comme dans le Théorème II), alors la construction des relations entre solutions conduit à un second système de même type; de ce second système dérivé, on tire de même un troisième système dérivé. Ce processus s'arrête toujours, et c'est au plus le n-ième système d'équations qui n'a pas de solution.

En ce qui concerne spécifiquement les invariants, HILBERT prouve que si $I_1,...,I_m$ sont des invariants qui engendrent l'idéal engendré par les invariants, alors $I_1,...,I_m$ engendrent l'algèbre des invariants.

☞ L'idée de la preuve de ce résultat est la suivante : on construit un opérateur différentiel ρ tel que pour tout invariant P et tout polynome homogène Q on ait $\rho(PQ) = P\rho(Q)$ et $\rho(1) = 1$ et tel que pour tout P on ait degré(ρ(P)) $\leq$ degré(P) (en particulier pour tout invariant P, $\rho(P) = P$).

Dans le cas spécifique des formes binaires, l'opérateur ρ est $\sum_{j=0}^{\infty} (-1)^j \frac{\Omega^j O^j}{j!(j+1)!}$.

Soit alors I un invariant de forme binaire. Il existe des formes $A_1,...,A_m$ telles que $I = A_1I_1 + ... + A_m I_m$ avec pour tout i degré(A_i) < degré(I)
On a alors $\rho(I) = I = \rho(A_1)I_1 + ... + \rho(A_m)I_m$ avec degré $\rho(A_i)$ < degré(I).
Les $\rho(A_1)$ sont des invariants de degré strictement inférieur à degré de I et on peut terminer en raisonnant par récurrence sur le degré de I. ✍

En définitive, l'algèbre des invariants est de type fini, les syzygies, secondes syzygies ,...., ont des systèmes de générateurs finis et la chaîne des syzygies s'arrête aprè un nombre fini d'étapes.

BIBLIOGRAPHIE

[G.BOOLE] Exposition of a general Theory of linear Transformations, Cambridge Math. Jour. III,1843, pp 1-20 & 106-118.

[A. CAYLEY ,1] On the Theory of linear Transformations, Cambridge Math. Jour. IV, 1845, pp.193-209.

[A. CAYLEY, 2] An introductory Memoir upon Quantics, Philosoph. Transac., 1854, pp.244-258. Œuvres complètes t.II,pp. 221-234. CAMBRIDGE University Press,1889.

[A. CAYLEY, 3] Research on the partition of Numbers, Philosoph. Transac., 1855, pp.127-140. Œuvres complètes t.II,pp. 235-249. CAMBRIDGE University Press,1889.

[A. CAYLEY, 4] A second Memoir upon Quantics, Philosoph. Transac., 1856, pp.101,126. Œuvres complètes t.II,pp. 250-275. CAMBRIDGE University Press,1889.

[E.B. ELLIOT] Algebra of Quantics, Chelsea, New York.

[D. HILBERT,1] Über die Theorie der algebraischen Formen, Math. Anal. 36,(1890), pp. 473-534.

[D. HILBERT,2] Über die vollen Invariantensysteme, Math. Anal. 42,(1893), pp. 313 & ss.

[J.J. SYLVESTER] Proof of the hitherto undemonstrated fundamental Theorem of invariants, Philos.Mag., 1878, pp. 117-126. Œuvres Tome III, pp 117-126, CHELSEA,N-Y, 1973.

Pour aller plus loin :

[J. DIEUDONNE & J.B. CARRELL]
Invariant Theory, old and new,
Academic Press, 1971.

[D. MUMFORD] Geometric Invariant Theory,
coll Ergebnisse des Math.34, SPRINGER,1965.

[H. WEYL] The Classical Groups, their invariants and representations
PRINCETON University Press, 1946-1973.

ANNEXE 1

DROITE PROJECTIVE COMPLEXE TRANSFORMATIONS HOMOGRAPHIQUES.

DEFINITION.- On appelle droite projective complexe l'espace $\mathbb{P}^1$ quotient de $\mathbb{C}\times\mathbb{C}\setminus\{0,0\}$ par la relation de colinéarité : $x\mathcal{R}y \Leftrightarrow \exists(\mu,\nu)\in\mathbb{C}\times\mathbb{C}\setminus\{0,0\}$, $\mu x + \nu y = 0$.

Un système de représentants de $\mathbb{P}^1$ est $\mathbb{C}^{\sim} = \mathbb{C} \cup\{\infty\}$ avec la convention que tout $z\in\mathbb{C}$ est le représentant de la direction de (z,1) tandis que ∞ est le représentant de la direction de (1,0). On prolonge les opérations de $\mathbb{C}$ à $\mathbb{C}^{\sim}$, donc à $\mathbb{P}^1$ par les,propriétés

$$\infty + \infty = \infty \; ; \; \forall a \neq 0 : a + \infty = \infty \; , \; a.\infty = \infty \; , \; a/\infty = 0 \; , a/0 = \infty.$$

DEFINITION. Soit $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$ une matrice carrée d'ordre 2 inversible à coefficients complexes . On appelle transformationn homographique de $\mathbb{P}^1$ associée à u la transformation T_u induite par l'application $\mathbb{C}$-linéaire admettant u comme matrice dans la base canonique de $\mathbb{C}\times\mathbb{C}$.

Avec les notations de la définition ci-dessus, la transformation T_u est donnée par :

$$\forall\, z\in\mathbb{C}\setminus\{-dc^{-1}\},\; T_u(z) = (az+b)/(cz+d) \; ; \; T_u(-dc^{-1}) = \infty \; ; \; T_u(\infty) = a/c.$$

De plus, les points fixes de T_u sont les images dans $\mathbb{P}_1$ des directions propres de u.
Une transformation homographique a donc deux points fixes distincts ou un point fixe "double".

On sait que le centre $Z(GL(2,\mathbb{C}))$ de $GL(2,\mathbb{C})$ est le groupe des homothéties isomorphe à $\mathbb{C}^*$. Le groupe des transformations homographiques de $\mathbb{P}^1$ est donc isomorphe au groupe quotient $PSL(2,\mathbb{C}) = GL(2,\mathbb{C})/\mathbb{C}^*$.

DEFINITION. - Soient z_1, z_2, z_3, z_4 quatre éléments distincts de $\mathbb{P}^1$. On appelle birapport de ces quatre nombres l'élément de $\mathbb{C}^{\sim}$ qu'on note (z_1, z_2, z_3, z_4) donné par : $(z_1, z_2, z_3, z_4) = \dfrac{z_1 - z_3}{z_1 - z_4} \div \dfrac{z_2 - z_3}{z_2 - z_4}$.

On prolonge la définition du birapport comme suit :
Si z_2, z_3, z_4 sont distincts et $z_1 = z_3$, alors $(z_1, z_2, z_3, z_4) = 0$;
Si z_1, z_2, z_4 sont distincts et $z_2 = z_3$, alors $(z_1, z_2, z_3, z_4) = \infty$;
Si z_1, z_2, z_3 sont distincts dans $\mathbb{C}$ et $z_4 = \infty$ alors $(z_1, z_2, z_3, z_4) = \dfrac{z_1 - z_3}{z_2 - z_3}$.

PROPOSITION.- Soit T: $\mathbb{P}^1 \to \mathbb{P}^1$ une bijection.
Les deux assertions suivantes sont équivalentes :

1) L'application T est une homographie ;
2) L'application T "conserve le birapport ".

☞ 1) $\Rightarrow$ 2) Soit T la transformation homographique associée à la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Si c est nul, il est est clair que T est le produit de la translation $\tau(b,)$ par la similitude $\sigma(c,)$, donc que T conserve le birapport.
Si c n'est pas nul, on peut décomposer T en le produit

$$T = \tau(ac^{-1},) \circ \sigma((ad-bc)c^{-1},) \circ I \circ \tau(dc^{-1},) \circ \sigma(c)$$

où I est la transformation $z \to 1/z$. La vérification de la conservation du birapport par cette homographie se fait par calcul direct, compte tenu des conventions faites relativement à ∞.
2) $\Rightarrow$ 1) Soient z_2, z_3, z_4 trois points distincts de $\mathbb{C}$ dont les images par T sont Z_2, Z_3, Z_4, toutes distinctes de ∞. Pour tout $z \in \mathbb{P}_1 \setminus \{z_2, z_3, z_4\}$ on a l'égalité

$$\frac{z - z_3}{z - z_4} \div \frac{z_2 - z_3}{z_2 - z_4} = \frac{T(z) - Z_3}{T(z) - Z_4} \div \frac{Z_2 - Z_3}{Z_2 - Z_4} .$$

Soient ϕ_1: $\mathbb{P}^1 \to \mathbb{P}^1$ l'homographie définie par $\phi_1(z) = \dfrac{z - z_3}{z - z_4} \div \dfrac{z_2 - z_3}{z_2 - z_4}$
et ϕ_2: $\mathbb{P}^1 \to \mathbb{P}^1$ l'homographie définie par $\phi_2(z) = \dfrac{z - Z_3}{z - Z_4} \div \dfrac{Z_2 - Z_3}{Z_2 - Z_4}$
D'après la formule ci-dessus T est la transformation homographique $\phi_2^{-1} \circ \phi_1$. ✍

On appelle birapport de quatre points du plan le birapport de leurs affixes.

PROPOSITION.- Soient z_1, z_2, z_3, z_4 quatre points de $\mathbb{P}^1$ dont le birapport est défini et qu'on note ρ. Si on fait agir le groupe symétrique $\mathbf{S}_4$ sur les indices de ces points, on obtient une action de sur l'ensemble des valeurs des birapports possibles. Ces birapports appartiennent à la famille

☞ L'ensemble E des valeurs des birapports obtenus est de cardinal au plus 24.
La transposition (2 1 3 4) et la transposition (1 2 4 3) changent ρ en ρ^{-1}.
La transposition (3 2 1 4) et la transposition (1 4 3 2) changent ρ en $1-\rho$. Pour tout $x \in E$, le sous-groupe de $\mathbf{S}_4$ qui laisse x fixe est donc au moins d'ordre 4, et les groupes qui fixent un point sont tous conjugués les uns des autres dans $\mathbf{S}_4$.
On en conclut que l'ensemble E est le support de la famille de l' énoncé. ✍
Pour que l'ensemble des valeurs obtenues par action de $\mathbf{S}_4$ sur les indices de quatre points distincts soit de cardinal différent de 6, il faut et il suffit qu'on ait

$\rho = \rho^{-1}$ ce qui donne $\rho = -1$ et $E = \{-1,2,1/2\}$, car on ne peut avoir $\rho = 1$.

ou $\rho = 1- \rho$ ce qui donne $\rho = 1/2$ et $E = \{-1,2,1/2\}$

ou $\rho = (1 - \rho)^{-1}$, ce qui donne $\rho = -j$ ou $-j^2$ et $E = \{-j,-j^2\}$.

ou $\rho = 1 - \rho^{-1}$, ce qui donne $\rho = -j$ ou $-j^2$ et $E = \{-j,-j^2\}$.

Ceci indique pourquoi on trouve ces valeurs particulières de birapport dans l'exposé de Michel BRION.

PROPOSITION.- Soient z_1, z_2, z_3, z_4 quatre points distincts de $\mathbb{C}$.
Les deux assertions suivantes sont équivalentes :

(i) Le birapport (z_1, z_2, z_3, z_4) est réel ;

(ii) Les quatre points du plans dont les affixes respectifs sont z_1, z_2, z_3 et z_4 appartiennent à une même droite ou a un même cercle.

☞ La démonstration repose essentiellement sur le fait que l'image par la transformation $z \to 1/z$ d'une droite munie du point ∞ et ne passant pas par O est un cercle et que par similitude toute droite peut être transformée en l'axe réel.
En effet, Soit Δ une droite du plan ne passant pas par O. Soit H la projection orthogonale de O sur la droite Δ. Soit $ae^{i\varphi}$ l'affixe de H. La droite Δ est caractérisée comme l'ensemble $\{M \in \mathbb{R}^2; < \mathbf{OM},\mathbf{OH} > = 0\}$.
L'équation cartésienne de la droite Δ est donc $[x \cos\varphi + y \sin\varphi - a = 0]$.
L'inverse M'(x',y') du point M(x,y) dans l'inversion de pôle O et de puissance 1 est caractérisé par :
$[(x,y) \neq (0,0)$ & $x' = x/(x^2 + y^2)$ & $y' = y/(x^2 + y^2)]$ qui est équivalente à
$[(x',y') \neq (0,0)$ & $x = x'/(x'^2 + y'^2)$ & $y' = y'/(x'^2 + y'^2)]$
On en déduit que l'inverse de la droite Δ est l'ensemble des points M(u,v) qui vérifient :

$$[(u,v) \neq (0,0) \text{ \& } u \cos\varphi + v \sin\varphi - a(u^2 + v^2) = 0].$$

Cet ensemble est le cercle privé de O centré au point $(1/2a)\cos\phi$, $(1/2a)\sin\phi$) et de rayon 1/2a. Par ailleurs l'image de ∞ par l'inversion $z \to 1/z$ est O.

i) $\Rightarrow$ (ii) On peut supposer que les trois points z_1, z_2 et z_3 sont "à distance finie". Si ces trois points sont alignés, il existe une similitude qui les transforme tous trois en trois nombres réels. On en conclut que l'image de z_4 est soit ∞ si $z_4 = \infty$, soit un nombre réel, ce qui prouve que z_4 appartient la droite engendrée par z_1, z_2 et z_3. Si les points z_1, z_2 et z_3 ne sont pas alignés, il existe une transformation homographique qui transforme leur cercle circonscrit en l'axe réel. L'image de z_4 est un nombre réel, donc appartient au cerle de z_1, z_2 et z_3.

(ii) $\Rightarrow$ (i) Soit E la droite ou le cercle support de z_1, z_2, z_3 et z_4. Il existe une transformation homographique qui transforme E en la droite réelle et la conservation du birapport implique que ce birapport est réel. ✍

ANNEXE 2

RESULTANT DE DEUX POLYNOMES ET DISCRIMINANT

POSITION DU PROBLEME

A l'origine le problème est de trouver un critère simple pour que deux polynômes sur le même corps K aient un facteur commun non constant, où, ce qui est équivalent, qu'ils aient un zéro commun dans une clôture algébrique de K.

DEFINITION DU RESULTANT

LEMME - Soient f(X) et g(X) deux polynômes à coefficients dans un corps commutatif K, de degrés non nuls respectifs m et n. Soit d un entier non nul inférieur ou égal au minimum de m et de n.
Les deux assertions suivantes sont équivalentes :

1) Les polynômes f(X) et g(X) ont un facteur commun de degré d dans K[X].

2) Il existe dans K[X] deux polynômes p(X) de degré $\leq$ n-d et q(X) de degré $\leq$ m-d tels que f(X)p(X) + g(X)q(X) = 0

☞ 1) $\Rightarrow$ 2) Soit r(X) un facteur commun à f(X) et g(X) de degré d. On a alors les deux décompositions $f(X) = r(X)f_1(X)$ et $g(X) = r(X)g_1(X)$ avec degré($f_1(X)$) = m-d et degré($g_1(X)$) = n-d.On peut alors choisir $p(X) = -g_1(X)$ et $q(X) = f_1(X)$.
2) $\Rightarrow$ 1) Soient deux polynômes p(X) de degré $\leq$ n-d et q(X) de degré $\leq$ m-d tels que f(X)p(X) + g(X)q(X) = 0. Si f(X) et g(X) étaient sans facteur commun de degré $\geq$ d, leur PGCD serait de degré < d et on aurait des relations du type :

$f(X) = r(X)f_1(X)$, $g(X) = r(X)g_1(X)$,$(f_1(X),g_1(X)) = 1$,
degré($f_1(X)$) >m-d ;
$f_1(X)p(X) + g_1(X)q(X) = 0$.

Le fait que $f_1(X)$ divise q(X) est contradictoire avec la définition des degrés ✍

La condition 2) du LEMME 1.1 permet de transformer la recherche de l'existence d'un facteur commun aux deux polynômes en un problème d'algèbre linéaire. En effet, si on décompose les polynômes sur la base canonique de K[X], on a des écritures du type suivant

$$f(X) = \sum_{i=0}^{m} f_i X^{m-i} \qquad g(X) = \sum_{i=0}^{n} g_i X^{n-i}$$

$$p(X) = \sum_{i=0}^{n-d-1} p_i X^{n-d-i} \qquad q(X) = \sum_{i=0}^{m-d-1} q_i X^{m-d-i}$$

La relation entre ces quatre polynômes, les inconnues étant les p_i et les q_i, s'écrit, en considérant comme nuls les coefficients à partir du degré de chaque polynôme

$$\sum_{i,j} f_i p_j X^{m+n-d-j-i} + g_i q_j X^{m+n-d-j-i} = 0 ;$$

$$\sum_{s=0}^{m+n-d} X^{m+n-d-s} \sum_{i=0}^{s} f_i p_{s-i} + g_i q_{s-i} = 0.$$

On obtient ainsi, à raison d'une équation linéaire par puissance de X, un système linéaire de m+n-d+1 équations à m+n-2d+2 inconnues.
Si d =1, le système linéaire ainsi obtenu est carré d'ordre m+n.
Pour qu'il admette une solution non triviale, il faut et il suffit que son déterminant soit nul.

$$\forall\, s \in 0..\ m+n,\ \sum_{i=0}^{s} f_i p_{s-i} + g_i q_{s-i} = 0 \qquad (1)$$

EXEMPLE.- La matrice de ce système, dans le cas m = 5 et n = 3,est :

s	p0	p1	p2	q0	q1	q2	q3	q4
0	f0	0	0	g0	0	0	0	0
1	f1	f0	0	g1	g0	0	0	0
2	f2	f1	f0	g2	g1	g0	0	0
3	f3	f2	f1	g3	g2	g1	g0	0
4	f4	f3	f2	0	g3	g2	g1	g0
5	f5	f4	f3	0	0	g3	g2	g1
6	0	f5	f4	0	0	0	g3	g2
7	0	0	f5	0	0	0	0	g3

DEFINITION - Avec les notations utilisées ci-dessus, le résultant des deux polynômes f(X) et g(X) est le déterminant du système linéaire (1).

AUTRES FORMULATIONS DU RESULTANT

Pour appréhender plus facilement les calculs qui vont suivre, on va se fixer les entiers m et n non nuls, et considérer d'une part les m indéterminées $\{Y_1,Y_2, \ldots ,Y_m\}$ que sont les zéros "formels" du polynôme f(X), le coefficient dominant F de f(X), et de même pour g(X) les zéros "formels" $\{Z_1,Z_2, \ldots ,Z_n\}$ et son coefficient dominant G. Avec ces notations les polynômes sont respectivement

$f(X) = F(X - Y_1)(X - Y_2) \ldots (X - Y_m)$

$g(X) = G(X - Z_1)(X - Z_2) \ldots (X - Z_n)$

LEMME - Le résultant des deux polynômes f(X) et g(X) est un polynôme homogène de degré n en les variables $f_0,f_1,\ldots ,f_m$, et de degré m en les variables $g_0,g_1,\ldots ,g_n$. De plus, l'un des ses termes est $f_0^n g_0^m$

☞ Il suffit de considérer le déterminant . ✍

Considérons maintenant l'expression

$$S(f,g) = F^n G^m \prod_{i,j} (Y_i - Z_j)$$

Le produit ci-dessus est une forme homogène de degré m en les Y_i et de degré m en les Z_j. Il en résulte que S(f,g) est une forme de degré n en les $f_0,f_1,\ldots ,f_m$ et de degré m en les $g_0,g_1,\ldots ,g_n$ Par ailleurs le résultant R s'écrit comme le produit par $F^n G^m$ d'un polynôme homogène de degré n en les Y_i et de degré m en les Z_j. Ceci résulte immédiatemenet du fait que d'une part les fonctions symétriques élémentaires sont de degré 1 par rapport à chacun des zéros, d'autre part du fait que la fonction symétrique élémentaire de degré k est $(-1)^k a_k/a_0$. Enfin ce dernier polynôme s'annule chaque fois qu'on y substitue un Y_i à un Z_j ou vice versa.Il est donc divisible par $(Y_i - Z_j)$ pour tout i et tout j, donc par leur produit. Ceci permet de conclure, en utilisant la dernière assertion du LEMME 2.1. que R et S sont égaux. On déduit de cette étude les deux résultats suivants :

PROPOSITION - Soient f(X) et g(X) deux polynômes à coefficients dans un corps commutatif K, de degrés non nuls respectifs m et n. Dans une clôture algébrique de K, soient respectivement $\{\sigma_1,\sigma_2, \ldots ,\sigma_m\}$ la famille des zéros de f(X) et $\{\chi_1,\chi_2, \ldots ,\chi_n\}$ celle des zéros de g(X). On a les égalités :

$$R(f,g) = f_0^n \prod_{j=1}^{m} g(\sigma_j) = (-1)^{mn} g_0^m \prod_{j=1}^{n} f(\chi_j)$$

☞ Il suffit de regrouper les termes dans l'expression S(f,g) ✍

PROPOSITION - En tant que polynôme homogène des m+n+2 variables, le résultant est asolument irréductible.

APPLICATION AUX DISCRIMINANTS

DEFINITION 3.1.- Soit α un entier algébrique de degré n dont les conjugués sur **Q** sont $\alpha_1,\alpha_2, \ldots ,\alpha_n$. On définit le discriminant de α comme le nombre algébrique

$$D(\alpha) = \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Ce nombre algébrique est un entier rationnel car c'est une fonction symétrique des zéros du polynôme irréductible de α. On peut donc dire que c'est le discriminant du polynôme irréductible de α. Si on désigne par f(X) le polynôme irréductible de α sur **Q**, on a immédiatement

$$D(\alpha) = \prod_{i=1}^{n} f'(\alpha_i)$$

D'où, en application des résultats du paragraphe précédent,

PROPOSITION - Soit α un entier algébrique de degré n dont le polynôme irréductible de α sur **Q** est f(X). Le discriminant de α est le résultant de f(X) et de son polynôme dérivé f'(X).

EXEMPLE.- Le polynôme standard de degré 3 est
$X^3 + a_1X^2 + a_2X + a_3$. Son polynôme dérivé est $3X^2 + 2a_1X + a_2$ dont les zéros sont formellement a + b et a - b avec $a = (-a_1/3)$ et $b = \sqrt{a_1^2 - 3a_2}/3$, ce qui donne $a^2 - b^2 = (a_2/3)$, $a^2 + b^2 = (2a_1^2 - 3a_2)/9$, et $a^2 + 3b^2 = (4a_1^2 - 9a_2)/9$.

D'après la formule de la PROPOSITION 2.3.,le discriminant du polynôme est donné par :

$D(f(X)) = 27[(a+b)^3 + a_1(a+b)^2 + a_2(a+b) + a_3][(a-b)^3 + a_1(a-b)^2 + a_2(a-b) + a_3]$

$=27[(a^2-b^2)^3 + 2aa_1(a^2-b^2)^2 + 2a_2(a^2-b^2)(a^2+b^2) + 2aa_3(a^2+3b^2) + a_1^2(a^2-b^2)^2$
$+ 2aa_1a_2(a^2-b^2) + 2a_1a_3(a^2+b^2) + a_2^2(a^2-b^2) + 2aa_2a_3 + a_3^2]$

$=[a_2^3 - 2a_1a_1a_2^2 + 2a_2^2(2a_1^2 - 3a_2) - 2a_1 a_3(4a_1^2 - 9a_2) + 3a_1^2a_2^2$
$-6a_1^2a_2^2 + 6a_1a_3((2a_1^2 - 3a_2) + 9a_2^3 - 18a_1a_2a_3 + 27a_3^2]$

$$D(fX) = 4a_2^3 - a_1^2a_2^2 - 4a_1^3a_3 - 18a_1a_2a_3 + 27a_3^2$$

UNIVERSITE GRENOBLE I (UJF)
Institut FOURIER
URA188 du CNRS

IREM DE GRENOBLE

CONFERENCES DE MATHEMATIQUES
IREM Institut FOURIER 1993

GROUPES ET GRAPHES

Cycle de trois conférences

de Vlad SERGIESCU

2 , 9 et 16 juin 1993

PREMIERE PARTIE
NOTIONS SUR LES GROUPES
ET LEURS GRAPHES DE CAYLEY

A la théorie des groupes sont principalement attachés les noms de GALOIS, ABEL, SCHMIDT qui a dégagé la notion de groupe abstrait,Felix KLEIN et le programme d'ERLANGEN, BURNSIDE et de nombreux autres mathématiciens de renom depuis cent cinquante ans.

0. GROUPES

Rappelons qu'un groupe est un ensemble non vide G muni d'une loi interne $*$, qu'on notera le plus souvent multiplicativement, ayant les propriété suivantes :

associativité $\forall a\in G,\ \forall b\in G,\ \forall c\in G,\ a*(b*c) = (a*b)*c$.

Il existe un élément distingué, dit **élément neutre**, et noté e tel que

$\forall a\in G,\ a*e = e*a = a$.

Tout élément admet un **inverse** pour la loi $*$, à savoir

$\forall a\in G,\ \exists b\in G,\ a*b = b*a = e$.

La propriété d'associativité implique l'unicité de l'élément neutre e et pour tout $a\in G$ l'unicité de son inverse.

Des exemples classiques de groupes sont les suivants :

•Le groupe $\mathbb{Z}$ des entiers rationnels avec la loi d'addition usuelle.

•Les groupes $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers modulo un entier donné n, munis de l'addition induite par l'addition usuelle de $\mathbb{Z}$.

•Pour tout ensemble non vide E, le groupe S_E des bijections de E dans lui-même muni de la composition des applications, en particulier le groupe S_n des bijections de 1. . n dans lui-même, groupe dont le cardinal est n!, produit des n premiers entiers non nuls.
•Etant donné un entier n et un corps commutatif $\mathbb{K}$, on désigne par GL(n,$\mathbb{K}$) le groupe des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ muni de la multiplication des matrices induite par la composition des applications linéaires de $\mathbb{K}^n$ dans lui-même lorsqu'on le munit de sa base canonique.

Sous-groupe d'un groupe.- Soit (G,*) un groupe. Une partie non vide H de G est un sous-groupe de G si elle est stable pour la la loi * et si munie de la loi induite,elle a une structure de groupe.
Si e est l'élément neutre de G, {e) est un sous-groupe de G.
L'intersection d'une famille quelconque de sous-groupes de G est un sous-groupe de G. En particulier on appelle sous-groupe de G engendré par une partie A de G l'intersection des sous-groupes de G contenant A.
L'ensemble $\{g\in G \mid \forall h\in G, gh = hg\}$ est un sous-groupe de G appelé le **centre** de G et noté en général Z(G).

Homomorphisme de groupes.- Soient G et H deux groupes. On appelle homomorphisme du groupe G dans le groupe H toute application ϕ: G → H qui respecte la structure des deux groupes, c'est-à-dire telle que

$$\forall g\in G, \forall h\in G,\ \phi(gh) = \phi(g)\phi(h).$$

Le **noyau** d'un homomorphisme de groupes est l'image réciproque de l'élément neutre du groupe but. Le noyau d'un homomorphisme de G dans un groupe quelconque est un sous-groupe de G.
On dira que la suite de groupes 1 → H → G → K → 1 est exacte si l'homomorphisme H → G est injectif et si l'image de H est le noyau de l'homorphisme surjectif de G sur K .

Opération d'un groupe sur un ensemble.- Soit G un groupe et X un ensemble non vide. On appelle **opération à gauche** (resp à droite) de G sur X une application F : G×X → X [notée (g,x) → gx] telle que

- $\forall g,h\in G,\ \forall x\in X, F(g,F(h,x)) = F(gh,x)$ [resp $F(hg,x)$]

i-e $\forall g,h\in G,\ \forall x\in X, (gh)x = g(hx)$ [resp. $(gh)x = h(gx)$].

- $\forall x\in X, F(e,x) = x$.

Une telle opération est dite **libre** si $\forall g\in G, \{\exists x\in X, F(g,x) = x\} \Rightarrow g = e$.

Exemple: Le groupe des translations entières opère librement sur l'espace affine $\mathbb{R}^2$.

1. QUELQUES CLASSES REMARQUABLES DE GROUPES

1.1. Le groupe libre sur un ensemble E.- Soit E un ensemble non vide. On considère l'ensemble des familles finies de couples de la forme $(a,p)\in E\times\mathbb{Z}^*$, c'est-à-dire l'ensemble des mots réduits dont l'alphabet est E. On munit cet ensemble de l'opération de concaténation avec simplification, celle-ci étant définie par

$(a,i)\hat{}(a,j)$ = si $i\neq -j$ alors $(a,i+j)$ sinon le mot vide.

L'élément neutre de la loi de concaténation est le mot vide et pour toute famille $\{(a_i,p_i) \mid i\in 1..k\}$ l'inverse de cette famille est la famille $\{(a_{k+1-i},-p_{k+1-i}) \mid i\in 1..k\}$. (On écrit habituellement (a,i) sous la forme a^i).On obtient ainsi un groupe appelé le **groupe libre non commutatif** sur E.

1.2. Les groupes abéliens.- Ce sont les groupes dont la loi est commutative. On verra dans un instant la raison de ce qualificatif dû à ABEL. En général on note additivement la loi d'un groupe abélien.

1.3. Groupes résolubles.- Soit $(G,*)$ un groupe. Un **commutateur** de G est un élément de la forme $a*b*a^{-1}*b^{-1}$ avec a et b éléments de G. On appelle sous-groupe des commutateurs de G et on note [G,G] le sous-groupe engendré par les commutateurs de G. En particulier un groupe est abélien si et seulement si son groupe des commutateurs est le sous-groupe {e}. On dit que le groupe G est résoluble s'il existe un entier $n\in\mathbb{N}$ tel que la séquence définie par
$G_0 = G$, $G_{i+1} = [G_i,G_i]$ se termine par $G_n = \{e\}$.

Exemples.- • Tout groupe abélien est résoluble.

• Considérons le groupe affine de $\mathbb{R}$, groupe des bijections de $\mathbb{R}$ dans lui-même $GA(\mathbb{R}) = \{x \to ax + b, \mathbb{R} \to \mathbb{R} \mid a\in\mathbb{R}^*, b\in\mathbb{R}\}$. Il est facile de voir que tout commutateur de ce groupe est une translation car le produit des quatre rapports d'homothétie est 1, donc que le groupe des commutateurs de $GA(\mathbb{R})$ est $\mathbb{R}$. C'est dire que le groupe $GA(\mathbb{R})$ est résoluble. Il nest pas abélien, évidemment. On dit que ce groupe est de profondeur 2.

La terminologie vient de ce que le critère de résolubilité d'une équation algébrique par radicaux donné par GALOIS s'exprime en terme de résolubilité d'un certain groupe fini lié à l'équation. Avant GALOIS, ABEL avait prouvé qu'une telle équation était résoluble par radicaux dès que ce

même groupe était commutatif. D'où la terminologie de abélien pour les groupes commutatifs.

• Tout groupe fini d'ordre impair est résoluble. C'est le théorème de FEIT & THOMSON, dont la première démonstration a demandé quelques cent cinquante pages et constitue le fondement de la classification des groupes finis.

• Le groupe des isométires du cube de l'espace euclidien $\mathbb{R}^3$ est résoluble de profondeur 3. [Voir développement en appendice I]

• Le groupe de HEISENBERG (appendice II) est résoluble et même nilpotent, c'est-à-dire que la suite des sousgroupes $G^i = [G,G^{i-1}]$ se termine par {e}.

1.4. Groupes simples.- Soit (G,*) un groupe. On dit qu'un sous groupe H de G est distingué, ou normal, ou **invariant**, si pour tout $s \in G$ on a $sHs^{-1} = H$.
En particulier [G,G] est un sous-groupe invariant de G ; en effet, pour tout commutateur [a,b] et pour tout $s \in G$ on a $s[a,b]s^{-1} = [sas^{-1}, sbs^{-1}]$ et cette propriété s'étend à un produit quelconque de commutateurs.
Dans le même ordre d'idée, on dit que deux éléments g et h de G sont conjugués s'il existe $s \in G$ tel que $g = shs^{-1}$.
Soit $\phi: G_0 \to G_1$ un homomorphisme de groupes. Le noyau de ϕ est un sous-groupe invariant de G_0. De façon générale, si H_1 est un sous groupe invariant de G_1 alors $\phi^{-1}(H_1)$ est un sous-groupe invariant de G_0.
A partir de là on voit que tout sous-groupe invariant d'un groupe G est le noyau d'un homomorphisme. En effet, soit H un sous-groupe invariant du groupe G. Considérons sur l'ensemble sous-jacent à G la relation binaire

$$\mathfrak{R}(g,h) = \{gh^{-1} \text{ appartient à } H\}.$$

C'est une relation d'équivalence sur G. De plus, si $\mathfrak{R}(g,h)$ et $\mathfrak{R}(g',h')$ sont vraies, alors $\mathfrak{R}(gg',hh')$ l'est, précisément parce que H est invariant ; en effet on a l'égalité $(gg')(hh')^{-1} = gh^{-1}\{h(g'h'^{-1})h^{-1}\}$. Cette propriété permet de définir une loi de groupe, dite loi quotient, sur l'ensemble quotient G/H de G par la relation $\mathfrak{R}$, de telle sorte que la surjection canonique $q: G \to G/H$ soit un homomorphisme de groupes dont le noyau est précisément H ; on a donc une suite exacte

$$1 \to H \to G \to G/H \to 1.$$

On dit qu'un groupe G est **simple** si les seuls sous-groupes distingués de G sont G et {e}. Si G est un groupe simple non abélien, on a [G,G] = G.
Un groupe simple abélien est un groupe cyclique d'ordre un nombre premier.

Exemples : • On démontre que pour tout n ≥ 5 le groupe A_n, sous-groupe des permutations paires de 1..n est simple. Cela permet de construire des équations algébriques de degré quelconque supérieur ou égal à 5 qui ne sont pas résolubles par radicaux.

• On démontre également que pour tout corps commutatif K et pour tout enyier m ≥ 3 le groupe PSL(m,K) obtenu à partir du groupe SL(m,K) des matrices de déterminant 1 modulo les homothéties, est simple.

1.5. Groupes de type fini.- Un groupe est dit de type fini s'il admet un nombre fini de générateurs. Un tel groupe est nécessairement dénombrable car l'ensemble des mots qu'on peut écrire sur un alphabet fini est dénombrable comme union dénombrable d'ensembles dénombrables.

Exemples.- •Le groupe abélien $\mathbb{Z}\times\mathbb{Z}$ est de type fini engendré par (1,0) et (0,1) ou par tout doublet de la forme {(a,b),(c,d)} tel que ad-bc ∈{-1,+1}.

•Soit $\mathbb{Q}_{(2)}$ le groupe additif des nombres dyadiques, ensemble des nombres rationnels dont le dénominateur en écriture réduite est une puissance de 2. Ce groupe n'est pas de type fini, tout simplement parce que l'ensemble des dénominateurs possibles, en écriture réduite, est infini.

I.6. Groupe de présentation finie

Définition.- On dit qu'un goupe G est de présentation finie s'il existe un entier n et un homorphisme surjectif du groupe libre sur un alphabet à n lettres F(n) à valeurs dans G dont le noyau est de type fini en tant que sous-groupe invariant du groupe libre, c'est-à-dire si le noyau de cet homomorphisme est engendré par une famille finie d'éléments de F(n) et l'ensemble de leurs conjugués.

Les groupes de présentation finie jouent un rôle important comme groupes fondamentaux des variétés compactes (le groupe fondamental est le groupe des lacets pointés modulo la déformation).

Exemples.- • Les groupes libres de type fini, abélien ou non, sont des groupes de présentation finie.

- Le groupe SL(2,Z) est de présentation finie [voir l'annexe].
- Considérons le groupe affine de $\mathbb{Q}_{(2)}$,

$$GA(\mathbb{Q}_{(2)})=\{x \to ax+b,\ \mathbb{Q}_{(2)} \to \mathbb{Q}_{(2)} \mid a\in 2^{\mathbb{Z}}, b\in\mathbb{Q}_{(2)}\}$$

Dans ce groupe, considérons d'une part l'homothétie de rapport 2, h: $x \to 2x$ et d'autre part la translation t: $x \to x+1$. On vérifie sans grande peine d'une part que h et t engendrent le groupe $GA(\mathbb{Q}_{(2)})$, d'autre part que $hth^{-1}t^{-2}$ est l'identité. Soient F(a,b) le groupe libre construit sur l'alphabet {a,b} et ϕ l'homomorphisme de F(a,b) dans $GA(\mathbb{Q}_{(2)})$ qui associe t à a et h à b. C'est un homomorphisme surjectif dont on peut montrer que le noyau est engendré par $bab^{-1}a^{-2}$ et ses conjugués.

On peut se poser la question de savoir si un groupe de type fini est de présentation finie. La réponse est négative comme on peut le montrer à l'aide de l'exemple que voici :

Exemple.- Soit $f : [0 , 1] \to [0 , 1]$ la bijection $(x \to x^2)$ et soit $x_0 = 1/4$

Soit ψ: $[0 , 1] \to [f(x_0) , x_0]$ l'application affine $x \to (x_0 - f(x_0))x + f(x_0)$, c'est-à-dire ψ: $[0 , 1] \to [1/4 , 1/2]$, $\psi(x) = (x+1)/4$.

Soit g la transformation définie par

$g(x)$ = si $x\in[f(x_0) , x_0]$ alors $\psi\circ f\circ\psi^{-1}(x)$ sinon x, c'est-à-dire

$g(x)$ = si $x\in[1/4 , 1/2]$ alors $4x^2-2x+1/2$ sinon x.

On désigne par G le sous-groupe des bijections de [0,1] sur [0,1] engendré par les applications f et g.

Soit h la transformation $f\circ g\circ f^{-1}$.

On montre que les applications h et g commutent.

Pour cela on examine deux éventualités :

a) si $x \geq f(x_0)$ on a $f^{-1}(x) \geq x_0$ et $h(x) = x$.

b) si $x \leq f(x_0)$ on a $f^{-1}(x)\in[0 , x_0]$.

Si $x \leq f\circ f(x_0)$ alors $h(x) = x$, sinon on a d'une part $g(x) = x$ et d'autre part $f^{-1}(x)\in[f(x_0) , x_0]$, ce qui implique

$g\circ f^{-1}(x)\in[f(x_0) , x_0]$ et donc $f\circ g\circ f^{-1}(x)\geq x_0$ et $g\circ f\circ g\circ f^{-1}(x)= f\circ g\circ f^{-1}(x)$. On a dans ce cas $h\circ g(x) = g\circ h(x)$ et on conclut à l'égalité $g\circ h = h\circ g$.

De même on montre que pour tout couple (m,n) d'entier les fonctions $f^m g f^{-m}$ et $f^n g f^{-n}$ commutent. La famille $\{f^m g f^{-m} \mid m\in\mathbb{Z}\}$ engendre un sous-groupe H de G qui est un sous-groupe abélien libre de rang infini ; L'homomorphisme surjectif de G dans Z qui a un mot en f et g associe la somme des exposants de f dans ce mot a pour noyau le groupe H. En utilisant cette propriété, on eut montrer que G n'est pas de présentation finie.

2. GRAPHE DE CAYLEY D'UN GROUPE

Rappelons qu'un **graphe** (non orienté) G = (V, A) est la donnée d'un ensemble non vide V dit ensemble des sommets du graphe, et d'un sous-ensemble A de l'ensemble des paires de points de V, appelé ensemble des arêtes du graphe. On dit qu'une arête du graphe est incidente à un sommet si ce sommet lui appartient et que le graphe est localement fini si pour tout sommet du graphe, le nombre des arêtes du graphe incidentes à ce sommet est fini. Une famille finie $\{v_0, v_1, v_2, \ldots v_n\}$ de sommets du graphe constitue un **chemin** (resp. un **cycle**) du graphe si pour tout $i \in 0..n-1$ (resp. pour tout $i \in \mathbb{Z}/n\mathbb{Z}$), $\{v_i, v_{i+1}\}$ est une arête du graphe.
Un graphe est dit **connexe** si deux sommets quelconques du graphe sont joints par un chemin.
Un graphe est un **arbre** si on en distingue un sommet appelé la **racine** et s'il est connexe et sans cycle.
Si G (resp. T) est un graphe, (resp. un arbre) on note Aut(G) (resp.Aut(T)) le groupe des automorphisme du graphe (non orienté) , c'est-à-dire l'ensemble des bijections de V dans lui-même qui laissent stable l'ensemble des arêtes du graphe (resp de l'arbre).

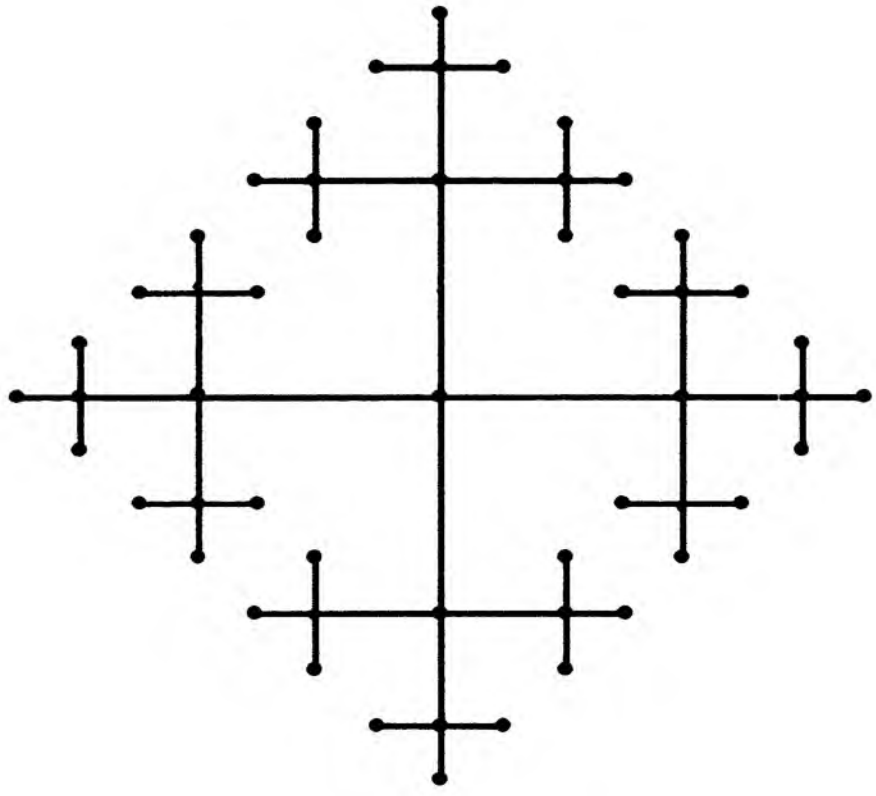
Soient G un groupe de type fini et S un système fini de générateurs de G qui soit symétrique (stable par passage à l'inverse) et tel que si s appartient à S alors s^2 est différent de e.[Cette clause est superflue tant qu'on ne cherche pas à doter le graphe d'une orientation ; il suffit en fait de supposer que e n'appartient pas à S]. On définit le graphe de CAYLEY associé au couple (G,S) comme celui qui a pour ensemble de sommets l'ensemble des éléments de G et pour ensemble d'arêtes l'ensemble des paires $\{\{g,h\} \mid \exists s \in S,\ h = gs\}$, ce qui est non ambigu car S est symétrique. La finitude de S implique que ce graphe est localement fini.

Exemples.- •Soit S le système de générateurs {-1,1} du groupe additif $\mathbb{Z}$. Le graphe de CAYLEY correspondant est la chaîne infinie des paires {a, a+1} pour a parcourant $\mathbb{Z}$.

• En généralisant le cas précédent, si on considère le système S formé des éléments de la base canonique de $\mathbb{R}^n$ et de leurs opposés, on obtient l'ensemble des mailles de $\mathbb{Z}^n$.

• Si G est le groupe libre F(a,b) àdeux générateurs et si S est le système symétrique fondamental $\{a,b,a^{-1},b^{-1}\}$ le graphe de CAYLEY

correspondant est un **arbre** dont on peut figurer [Cf. figure ci-dessous] les premières branches, la racine de l'arbre étant le mot vide. Dans la construction, on commence par e puis a,b,a^{-1},b^{-1}, dans le sens trigonométrique, et on itère en divisant à chaque étape par deux la longueur des représentants d'arête pour éviternles recoupement du dessin.



L'arbre de du groupe libre F(a,b)

Remarques.- Soit G le graphe de CAYLEY d'un groupe G correspondant à un système de générateurs S.

1) Ce graphe est connexe.

2) Le groupe G opère à gauche sur son graphe de CAYLEY, l'opération étant donnée simplement par $(g,h) \rightarrow gh$, cette action préservant les arêtes, présisément parce qu'on considère que l'arête {g,h} est définie par la multiplication à droite de g par un générateur appartenant à S..

Ce sera l'un des objectifs des deux exposés qui suivront de montrer comment les graphes de CAYLEY d'un groupe permettent de démontrer des propriétés de ce groupe.

3. QUELQUES PROPRIETES DES GROUPES LIBRES

Un question à laquelle on aimerait bien savoir répondre est "comment reconnaître si un groupe est un groupe libre ?". Enumérons quelques propriétés qui éclairent ce problème :

3.1. Le lemme du ping-pong de Félix KLEIN.- Dans le cas d'un groupe à deux générateurs, on a une réponse : Soit G un groupe engendré par les deux éléments a et b. Supposons que le groupe G opère sur un ensemble X de telle sorte qu'il existe deux parties disjointes de X, X_1 et X_2 telles que $\forall n\in\mathbb{N}^*, a^nX_1\subset X_2$ & $b^nX_2\subset X_1$ & $b^nX_2 \neq X_1$. Alors $<a,b>$ engendre librement le groupe G. En effet, pour tout mot non vide sur G, $\omega = a^{i_1}b^{j_1}a^{i_2}b^{j_2}\ldots a^{i_n}b^{j_n}$, on montre qu'on a soit $w.X_1 \neq X_1$ soit $wX_2 \neq X_2$.

Exemple.- Considérons le sous-groupe G du groupe $SL(2,\mathbb{Z})$ (le groupe des matrices carrées à coefficients entiers et d'ordre 2 dont le déterminant est +1), engendré par les deux matrices $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ et $B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$.
Soient X l'ensemble $\mathbb{Z}\times\mathbb{Z}$, X_1 l'ensemble $\{(x,y)\in\mathbb{Z}\times\mathbb{Z} \mid y^2 > x^2\}$ et X_2 l'ensemble $\{(x,y)\in\mathbb{Z}\times\mathbb{Z} \mid y^2 < x^2\}$. Alors pour tout entier n non nul positif, AX_1 est inclus strictement dans X_2 car (1,0) n'appartient pas à AX_1. De même AX_2 est inclus dans X_1. Donc G est engendré librement par ces deux matrices.

3.2. L'alternative de TITS.- Soient K un corps commutatif, n un entier supérieur ou égal à 2 et G un sous-groupe de GL(n,K). Alors ou bien G admet comme sous-groupe un groupe libre a au moins deux générateurs libres, ou bien G admet un sous-groupe résoluble H tel que l'ensemble quotient G/H soit fini.

Il s'agir là d'un théorème difficile dont la portée dépasse le cadre des groupes libres et des groupes linéaires. Pour une introduction à ce sujet voir [H].

3.3. Le théorème de NIELSEN & SCHREIER.- Tout sous-groupe d'un groupe libre est un groupe libre. Ce théorème est une conséquence d'un théorème sur l'action d'un groupe sur un arbre :

Un groupe G est libre si et seulement si il existe un arbre T sur lequel G opère librement.

Un groupe libre agit librement suer son graphe de CAYLEY. Réciproquement, on peut avoir une idée de la preuve selon le schéma suivant : Soit T un arbre sur lequel G agit librement ; soit $G\backslash T$ l'espace quotient, espace des orbites. Cet espace est un graphe. On choisit dans T un sous-arbre T' qui s'envoie homorphiquement sur un sous-arbre maximal de par la projection canonique T Æ . Soit alors S l'ensemble des éléments de G tels qu'il existe une arête de T dont l'une des extremités appartienne à T' et l'autre à gT'. On démontre que S engendre librement G. (Pour plus de détails voir le Chapitre I de [Se]).

Remarques • LA théorie des groupes agissant sur les arbres est dûe au départ à J.P. SERRE, [Se], qui a reformulé dans ce cadre de larges parties de la combinatoire des groupes. Un prolongement de celle-ci, la théorie des groupes agissant sur les R-arbres est actuellement l'objet de nombreux développements [Sh].

•Si G est un groupe libre de type fini, il est faux en général qu'un sous-groupe H de G soit de type fini, contrairement à se qui se passe dans le cas abélien. Par exemple, si on considère l'homomorphisme ϕ: F(a,b) $\rightarrow \mathbb{Z}$ défini par ϕ(m) = la somme des exposants de b dans le mot m, le noyau de cet homorphisme est le groupe engendré par les mots de la forme $b^n a b^{-n}$ avec $n \in \mathbb{Z}$, groupe qui n'est pas de type fini. de même le sous-groupe des commutateurs d'un groupe libre de type fini n'est pas de type fini

BIBLIOGRAPHIE POUR CETTE PARTIE

[H] La HARPE.- Free groups in lear groups,
L'Enseignement Mathématique,1983, pp. 129-145.

[R] D.J.ROBINSON.- A Course in the Theory of Groups,
Springer-Verlag, 1982.

[Se] J.P. SERRE;- Arbres et amalgames et SL2, Astérisque, n°46, 1983.

[Sh]. P.B. SHALEN, Dendrology of Groups, dans Geometrical Methods in Group Theory, E.GHYS,A. HAEFLIGER & A. VERJOVSKI editeurs, World Scientific, 1991.

SECONDE PARTIE
LE PROBLEME DE BURNSIDE

On distinguera deux versions de ce problème, d'une part le problème de BURNSIDE général

> **Soit G un groupe de type fini et de torsion, c'est-à-dire tel que pour tout $g \in G$ il existe $n(g) \in \mathbb{N}^*$ tel que $g^{n(g)} = e$.**
> **Le groupe G est-il fini ?**

d'autre part le problème spécial

> **Soit g un groupe de type fini et uniformément de torsion, c'est-à-dire tel qu'il existe un entier naturel non nul n avec $\forall g \in G$, $g^n = e$. Le groupe G est-il fini ?**

Comme son nom l'indique, c'est BURNSIDE qui a le premier traité ces problèmes [B, 1902].

On connaît la réponse à ce problème dans plusieurs cas particuliers :

A.- Si G est un groupe abélien, alors la réponse est positive pour les deux problèmes. En effet on démontre que tout groupe abélien est isomorphe à un produit de groupes de la forme $\mathbb{Z}^r \times (\mathbb{Z}/k_1\mathbb{Z}) \times (\mathbb{Z}/k_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/k_{m-1}\mathbb{Z}) \times (\mathbb{Z}/k_m\mathbb{Z})$ où r est un entier naturel et où les entiers k_j sont tels que k_j divise k_{j+1} pour tout $j \in 1..m-1$. Par suite, si G est de torsion alors r est nul, G est fini d'exposant k_m et de cardinal $k_1 \times k_2 \times \ldots \times k_{m-1} \times k_m$.

B.- Si G est un groupe d'exposant 2, c'est-à-dire tel que [$\forall g \in G$ gg = e], la réponse est encore positive car G est abélien.
En effet on a $\forall$ $(g,h) \in G \times G$, $ghg^{-1}h^{-1} = ghgh = (gh)(gh) = e$.

C.- Si G est d'exposant 3, alors G est fini. Ce cas du problème avait déjà été considéré par BURNSIDE. La démonstration repose sur le lemme suivant :

1. Lemme.- Soit G un groupe d'exposant 3.
Pour tout couple $(g,h) \in G \times G$, g commute avec hgh^{-1}.

☞ On a les égalités $[g, hgh^{-1}] = ghghhh(ggh)(gg)hh = ghgh(hgg)(hgg)hh$
$[g, hgh^{-1}] = ghghghhhh = ghghgh = e.$ ✍

Supposons d'abord que le groupe G est engendré par deux générateurs g et h et soit G_0 le groupe des commutateurs de G. Par définition de ce sous-groupe et de la notion de groupe quotient, on a une suite exacte de groupes :

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow G/G_0.$$

Soit $g^nh^mg^{-n}h^{-m}$ un commutateur construit à partir des générateurs. D'après le lemme, ce commutateur est $(ghg^{-1}h^{-1})^{mn}$. En effet, quitte à remplacer g et h par leurs inverses respectifs,on peut supposer que les exposants m et n sont des entiers naturels. On raisonne par récurrence sur m en fixant n quelconque. On a pour tout $n\in\mathbb{N}$: $g^nhg^{-n}h^{-1}g^nhg^{-n}h^{-1} = g^nhg^{-n}g^nhg^{-n}h^{-2} = g^nh^2g^{-n}h^{-2}$.
On intervertit les rôles de g et de h pour obtenir le résultat annoncé.
Un premier résultat est que le groupe G_0 est monogène et de 3-torsion, donc qu'il est fini et isomorphe à $\mathbb{Z}/3\mathbb{Z}$. L'exactitude de la suite ci-dessus montre que le groupe G/G_0 est un groupe de 3-torsion abélien ayant un système de deux générateurs (par définition du groupe des commutateurs), donc est fini, et on conclut que G est fini de cardinal inférieur à 27.

A partir de là on raisonne par récurrence sur le nombre minimum de générateurs du groupe G. La propriété de finitude est vraie si ce nombre est 2.
Soit l'hypothèse de récurrence H(n)

H(n) Tout groupe de 3-torsion admettant
un ensemble de n générateurs est fini.

Soit alors G un groupe de 3-torsion admettant n+1 générateurs, $g_0,g_1,\ldots,g_n$.
Soit H le sous-groupe distingué de G engendré par g_0. On a une suite exacte de groupes $1 \longrightarrow H \longrightarrow G \longrightarrow G/H$. D'après l'hypothèse H(n) le groupe G/H est fini.
Pour tout couple (s,t) d'éléments de G on a d'après le lemme l'égalité

$$sg_0s^{-1}tg_0t^{-1} = sg_0[s^{-1}tg_0t^{-1}s]s^{-1} = s[s^{-1}tg_0t^{-1}s]g_0s^{-1} = [tg_0t^{-1}]sg_0s^{-1}$$

ce qui prouve que le groupe H, groupe abélien, de type fini et de 3-torsion est fini et en définitive que G est fini.

Cela étant , la réponse au problème de BURNSIDE est en général négative. Le premier contre-exemple a été donné par GOLOD et SHAFAREVITCH [G, 1965], à l'occasion de recherches arithmétiques liées à la théorie du corps de classe. Leur résultat s'énonce comme suit :

Pour tout nombre premier p > 3 il existe un groupe de p-torsion de type fini et infini.

NOVIKOV et ADJAM [N & A,1968] ont donné une autre réponse négative au problème spécial de BURNSIDE, sous la forme suivante :

Soit F(a,b) le groupe libre à deux générateurs. Pour tout n, soit H(n) le sous-groupe invariant de F(a,b) engendré par les puissances n-èmes des éléments de F(a,b) et soit B(n) le groupe quotient F(a,b)/H(n). Pour tout n > 4281 le groupe B(n) est infini.

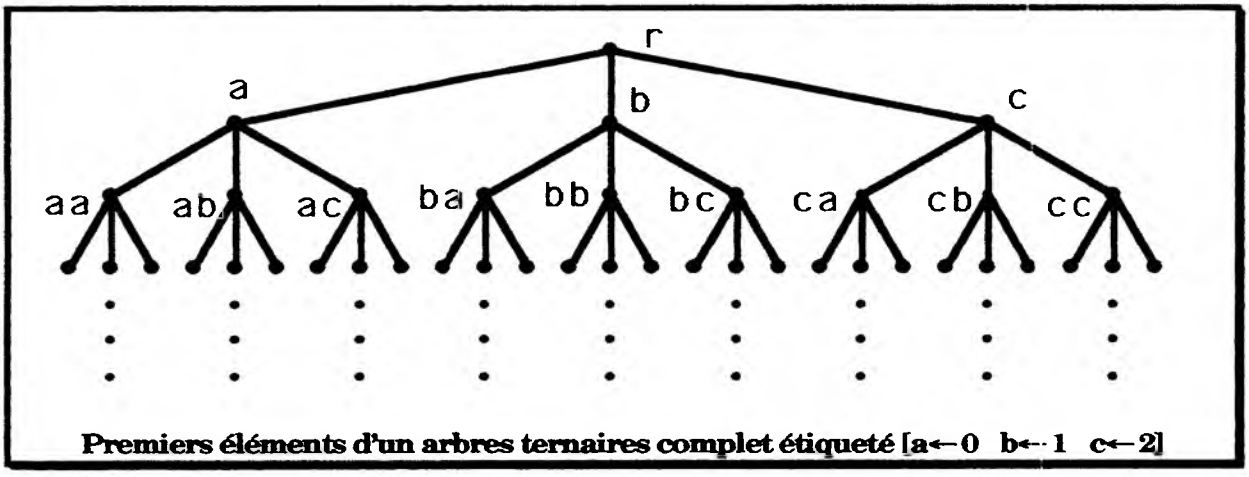
Depuis, ce résultat a été amélioré, en ce sens qu'on estime qu'il est vrai pour les valeurs de n supérieures à 33. Par ailleurs, on sait que B(2), B(3), B(4) et B(6) sont finis, mais on ne connaît pas le résultat pour B(5).

La suite de cet exposé est consacrée à la recherche d'une réponse négative simple et élégante au problème de BURNSIDE, dûe dans cette présentation à GUPTA & SIDKI [G&S, 1983], qui ont prouvé le résultat général :

Pour tout nombre premier p ≥3 il existe un groupe infini de p-torsion qui admet deux générateurs d'ordre p.

Il se trouve qu'à lorigine de cette preuve se trouve une idée de la théorie des automates.

La suite de cet exposé est consacrée à la preuve de ce résultat pour le cas p = 3, qui est la plus simple à présenter. Elle repose sur l'utilisation d'un arbre ternaire.
Soit T l'arbre ternaire complet admettant une racine r [Cf. figure].



Premiers éléments d'un arbres ternaires complet étiqueté [a←0 b←1 c←2]

Les sommets de niveau n de cet arbre sont repérés par leur écriture à n chiffres en base 3. Pour tout sommet u de T, on désigne par T_u le sous-arbre ternaire complet dont la racine est le sommet u. Il est clair que cet arbre est isomorphe à T. Soit G un groupe opérant sur T. Par transport, G opère sur T_u. Par commodité on notera G_u une copie de G opérant sur T_u. comme G opère sur T et pour tout u on notera g_u l'élément $g \in G$ opérant sur T_u.

Le groupe G dont on va se servir est un groupe d'automorphismes de T a deux générateurs, G = <t,a> où t et a sont définis comme suit :

- La transformation t permute circulairement les sommets 0,1 et 2 de T dans cet ordre et décalque chaque T_i sur $T_{(i+1) \bmod 3}$.
- La transformation a laisse fixe les sommets 0,1 et 2;

  La restriction de a à T_0 est t_0.

  La restriction de a à T_1 est l'inverse de t_1.

  La restriction de a à T_2 laisse fixe les sommets 2, 20, 21 et 22.

  Sa restriction à T_{20} et à T_{21} est la restriction de t_{20} et de t_{21}.

  Sa restriction à T_{22} s'obtient récursivement à partir de la construction précédente en transportant T sur T_{22}.

La transformation a se traduit sur la notation des sommets comme suit :
Soit u un sommet du k-ème niveau de T, dont l'écriture en base 3 est $i_1,i_2,...,i_k$. Si ce nombre ne contient que le chiffre 2, alors a(u) = u. Sinon soit n le plus petit entier tel que $i_n \neq 2$. Alors on a $a(u) = i_1,i_2,...,\pi(i_n),...,i_k$ où $\pi(i) = (1- i)$ modulo 3.
On vérifie sans peine que t et a sont d'ordre 3.

Proposition.- Le groupe G = < t,a > est un groupe infini de torsion dont l'ordre de chaque élément est une puissance de 3.

A.- Non finitude de G. Pour cela on va prouver l'existence d'un sous-groupe H de G, d'indice 3, et d'un homomorphisme surjectif de H sur G.
Tout élément de G agit sur l'ensemble {0,1,2} par permutation circulaire sur le premier niveau de T. On a donc un homomorphisme surjectif de G sur $\mathbb{Z}/3\mathbb{Z}$ fourni par $g \to \phi(g)$ = [la classe modulo 3 de la somme des exposants de t dans une écriture quelconque de g comme produit de puissances de t et de a].
On a alors :

Lemme.- Le noyau H de $\phi: G \to \mathbb{Z}/3\mathbb{Z}$ est engendré par a, $b = tat^{-1}$ et $c = t^{-2}at^{-2}$.

☞ Soit $g \in G \setminus \{1\}$ qui se décompose comme produit de puissances de a et de t sous la forme $g = a^{i(1)}t^{j(1)}\ldots a^{i(k)}t^{j(k)}$. On peut écrire cette décomposition sous la forme $a^{i(1)}\,[t^{j(1)}a^{i(2)}t^{-j(1)}][t^{j(1)+j(2)}a^{i(3)}t^{-j(1)-j(2)}]\ldots[]\ldots t^{j(1)+j(2)+\ldots+j(k)}$ où le m-ième terme entre crochets est $t^{s(m)}a^{i(m)}t^{-s(m)}$ avec $s(m) = j(1) + \ldots + j(m)$. Puisque seules interviennent les classes des exposants de t modulo 3, on peut écrire g sous la forme $\theta(a,b,c)t^{s(k)}$ où $\theta(a,b,c)$ est un mot écrit sur l'alphabet $\{a,b,c,a^{-1},b^{-1},c^{-1}\}$. L'élément g appartient à H si et seulement si s(k) est congru à 0 modulo 3, c'est-à-dire si et seulement si g appartient au sous-groupe de G engendré par a, b et c. ✍

Montrons qu'il existe un homomorphisme surjectif de H sur G.
D'une part tout élément de G laisse fixes les sommets du premier niveau de l'arbre T.
D'autre part la transformation a est caractérisée par ses restrictions respectives à T_0, T_1 et T_2, c'est-à-dire qu'elle s'identifie à (t_0,t_1^{-1},a_2).
On a les représentations par les restrictions :

$$a \sim (t_0,t_1^{-1},a_2) \qquad b \sim tat^{-1} = (a_0,t_1,t_2^{-1}) \qquad c \sim (t_0^{-1},a_1,t_2),$$

à partir desquelles on constate, puisque H laisse globalement fixe T_0, que l'application restriction de H sur G_0 est un homorphisme surjectif de groupes. Ceci prouve que H s'envoie surjectivement sur G et donc que G est infini.

B.- G est un 3-groupe.- Dans le paragraphe A, l'écriture d'un élément $g \in G$ sous la forme $\theta(a,b,c)\ t^{\varepsilon}$ avec $\varepsilon \in \{0,1,-1\}$ et $\theta(a,b,c)$ mot de longueur minimum écrit avec $\{a,b,c,a^{-1},b^{-1},c^{-1}\}$ permet de définir la longueur de g, l(g), comme $\text{long}(\theta(a,b,c))$ si $\varepsilon = 0$ et $1 + \text{long}(\theta(a,b,c))$ si $\varepsilon \in \{1,-1\}$. On définit de façon analogue la notion de longueur pour les éléments des groupes G_u.
On va prouver par récurrence sur l'entier n la propriété

$$\forall n \in N, \forall g \in G,\ l(g) \leq n \Rightarrow g^{3^n} = e.$$

Au rang n = 1, ou bien g appartient à H et g appartient à $\{a,b,c,a^{-1},b^{-1},c^{-1}\}$ ou bien g n'appartient pas à H et g appartient à $\{t,t^{-1}\}$; dans tous les cas on a $g^3 = e$.

Supposons la propriété vraie au rang n. et soit g un élément de longueur $l(g) = n + 1 \geq 2$. On distingue deux cas :

(i) L'élément g appartient à H, c'est-à-dire $g = \theta(a,b,c)$.

(ii) L'élément g n'appartient à H, c'est-à-dire $g = \theta(a,b,c)t^{\varepsilon}, \varepsilon \in \{-1,1\}$.

(i) On décompose g sous la forme $({}_0g,{}_1g,{}_2g)$ et on montre que chacune des "coordonnées" de g est d'ordre au plus 3^{n+1}. Il suffit pour cela de faire la démonstration pour la première.

On écrit ${}_0g = \theta(t_0,a_0,t_0^{-1}) = \theta\hat{}(a_0,b_0,c_0)t_0^{\eta}$.Par définition, les syllabes figurant dans le mot $\theta\hat{}(a_0,b_0,c_0)$ proviennent uniquement des syllabes écrites avec b dans le mot $\theta(a,b,c)$. La longueur de $\theta(a,b,c)$ étant supérieure ou égale à 2, l'une des lettres a ou c (ou leurs inverses) figurent dans $\theta(a,b,c)$ et on en déduit que la longueur de $\theta\hat{}(a_0,b_0,c_0)$ est strictement inférieure à celle de $\theta(a,b,c)$.

- Si on a $\eta = 0$, alors d'après l'hypothèse de récurrence l'ordre de ${}_0g$ divise 3^n, donc divise 3^{n+1} .
- si on a $h \neq 0$, alors on est dans le cas (ii).

(ii) On écrit g sous la forme $\theta(a,b,c)t^{\eta}$ avec $\eta \in \{1,-1\}$. La démonstration est du même type pour $\eta = 1$ et pour $\eta = -1$. On a supposera donc $\eta = 1$.

On a par définition de a,b et c : $g^3 = \theta t\theta t\theta t = \theta t\theta t^{-1}t^2\theta t^{-2} = \theta(a,b,c)\theta(b,c,a)\theta(c,a,b)$

En particulier, raisonnant à nouveau composante par composante, on a

$${}_0(g^3) = \theta(t_0,a_0,t_0^{-1})\theta(a_0,t_0^{-1},t_0)\theta(t_0^{-1},t_0,a_0)$$

Si maintenant on écrit ${}_0(g^3)$ sous la forme $\omega(a_0,b_0,c_0)t_0^{-\mu}$, d'une part μ est nul, car t_0 et t_0^{-1} apparaissent autant de fois chacun pour chaque syllabe de θ ; d'autre part la longueur de ω est inférieure à celle de θ, car à chaque syllabe de θ correspond une occurrence de a_0 dans ω. On en déduit que la longueur de ω est inférieure ou égale à celle de θ et on conclut de l'hypothèse de récurrence que (g^3) a pour ordre un diviseur de 3^n. D'où le résultat complet.

Enfin on peut montrer que pour tout entier n il existe dans G un élément d'ordre 3^n, c'est-à-dire que cet exemple ne peut pas servir pour résoudre le second problème de BURNSIDE.

Remarque.- On peut démontrer que G n'est pas un groupe de présentation finie. D'ailleurs le probllème de BURNSIDE pour cette classe de groupes est toujours ouvert.

BIBLIOGRAPHIE

[B, 1902] BURNSIDE W.- *On an unsettled question in the Theory of discontinuous groups,* Quart.Jour. Pure & Applied Math., **33**, 1902, 230-238.

[G, 1964] GOLOD A.S.- *On nil-algebras and finitely approximable p-groups,*, Izv. Akad.Nauk. SSSR,Ser. MAth. **28**, 1964, 273-276.

[G&S, 1983] GUPTA N. & SIDKI S.- *On the BURNSIDE problem for periodic groups,*, Math. Zeit., **182**, 1983, 385-388.

[N&A, 1968] NOVIKOV P.S. & ADJAN S.I. - *Infinite periodic groups,I, II, III,* Dokl. Akad. Nauk. SSSR, 245, Ser. Math. 32, 1968, 212-244, 251-254, 709-734.

APPENDICE AUX CONFERENCES DE V. SERGIESCU
TROIS EXEMPLES

ANNEXE I : LES ISOMETRIES DU CUBE

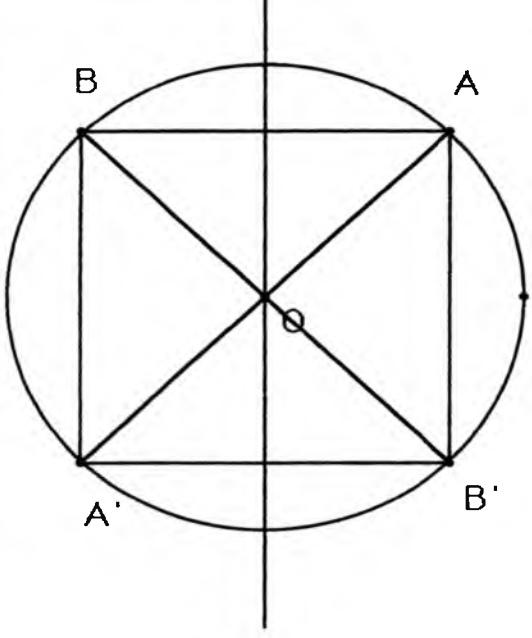
Désignons par C_n le pavé de l'espace euclidien orienté $\mathbb{R}^n$ dont les sommets ont pour coordonnées les entiers 1 et -1.

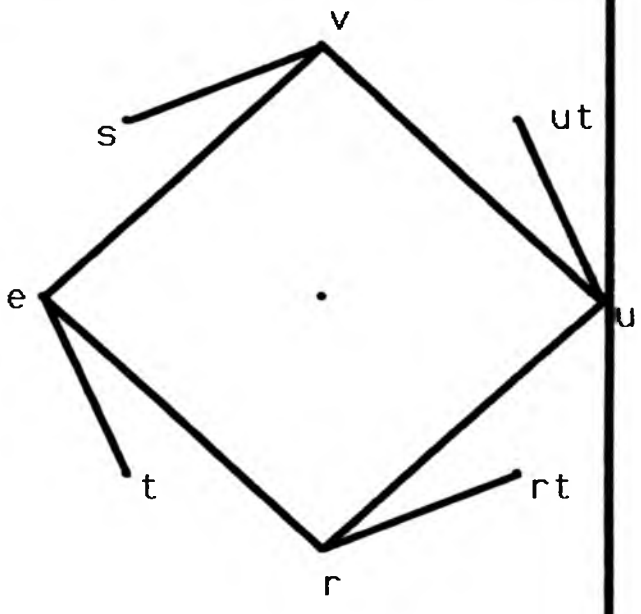
Le groupe des isométries de C_1 est le groupe d'ordre 2 engendré par la symétrie centrale S. Le graphe de CAYLEY de ce groupe d'isométries est réduit à ceci :

$$e \rightarrow S$$

Le groupe des isométries de C_2 est le groupe diédral D_8, d'ordre 8, engendré par la symétrie τ induite par la symétrie centrale de C_1 et par la symétrie σ par rapport à la diagonale principale du carré. En effet (Cf. figure 1), la transformation $\tau\circ\sigma$ est la rotation ρ d'angle $\pi/2$, qui est d'ordre 4 et qui vérifie la relation $\sigma\circ\rho\circ\sigma = \rho^{-1}$.
Soit I une isométrie du cube. Quitte à faire un produit $r^{-k}I$, avec $k\in\{0,1,2,3\}$, on se ramène au cas où A = (1,1) est fixe, puis par multiplication par σ^m, avec $m\in\{0,1\}$,au cas où B= (-1,1) est fixe. C'est dire qu'on a $I = r^k\sigma^m$.
Le groupe des commutateurs de ce groupe est un groupe de rotations (déterminant 1).Le calcul direct des commutateurs montre que ce groupe est engendré par le commutateur $\sigma\tau\sigma\tau$ qui est la symétrie centrale , laquelle est d'ordre 2. Ce sous-groupe est aussi le centre du groupe. On peut donc dresser la table du groupe sous la forme ci-après.

	ε	ρ^2	ρ	ρ^{-1}	σ	$\rho^2\sigma$	τ	$\rho^{-1}\sigma$
ε	ε	ρ^2	ρ	ρ^{-1}	σ	$\rho^2\sigma$	τ	$\rho^{-1}\sigma$
ρ^2	ρ^2	ε	ρ^{-1}	ρ	$\rho^2\sigma$	σ	$\rho^{-1}\sigma$	τ
ρ	ρ	ρ^{-1}	ρ^2	ε	τ	$\rho^{-1}\sigma$	$\rho^2\sigma$	σ
ρ^{-1}	ρ^{-1}	ρ	ε	ρ^2	$\rho^{-1}\sigma$	τ	σ	$\rho^2\sigma$
σ	σ	$\rho^2\sigma$	$\rho^{-1}\sigma$	τ	ε	ρ^2	ρ^{-1}	ρ
$\rho^2\sigma$	$\rho^2\sigma$	σ	τ	$\rho^{-1}\sigma$	ρ^2	ε	ρ	ρ^{-1}
τ	τ	$\rho^{-1}\sigma$	σ	$\rho^2\sigma$	ρ	ρ^{-1}	ε	ρ^2
$\rho^{-1}\sigma$	$\rho^{-1}\sigma$	τ	$\rho^2\sigma$	σ	ρ^{-1}	ρ	ρ^2	ε





Dans la figure de gauche, la symétrie τ est la symétrie par rapport à l'axe "vertical", la symétrie σ celle par rapport à la droite AA' où A' = -A.
La figure de droite représente un graphe de CAYLEY des isométries du carré, avec u = $\rho\tau$, v = $\rho^2\tau$. et s représente σ. (r pour ρ et t pout τ sur la figure dessinée avec Cabri-géomètre)

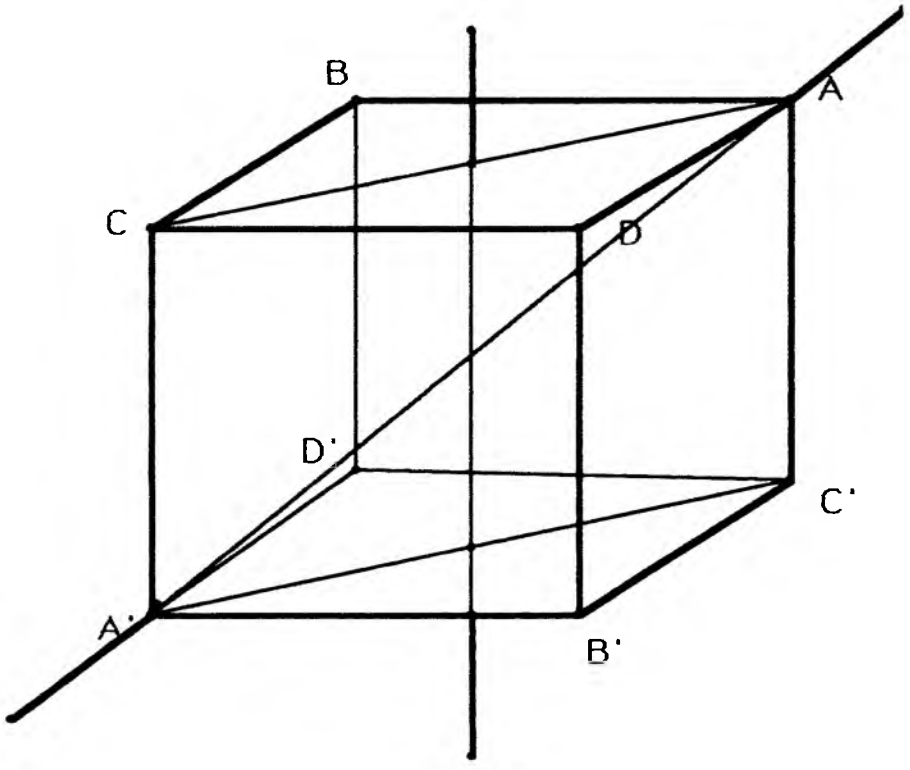
Le groupe quotient $D_8/[D_8,D_8]$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$, engendré par les classes de σ et de τ. On en conclut que le groupe des isométries du carré est résoluble de profondeur 2.

Prenons comme système de générateurs de D_8 l'ensemble $\{\rho, \rho^{-1}, \sigma, \tau\}$ (On ne peut faire autrement que de considérer des éléments d'ordre 2). On obtient le graphe de la figure de droite ci-dessus, en dessinant de façon particulière le groupe des commutateurs.

Groupe des isométries de C_3.

Le groupe des isométries du cube C_3 admet comme sous-groupe un groupe D, isomorphe à D_8, qui laisse globalement fixe la "face supérieure" du cube et laisse fixe le troisième vecteur de la base canonique. Ce groupe est engendré par une rotation d'ordre 4 que nous noterons ρ et par une symétrie plan que nous noterons σ. Il admet aussi un sous-groupe d'ordre 3 engendré par une rotation R qui permute circulairement les faces contenant A = (1,1,1). Il

contient enfin la symétrie centrale S, laquelle commute avec toutes les isométries du cube puisque c'est une homothétie.



Montrons que le groupe du cube est engendré par tous ces éléments : Soit U une isométrie du cube. Quitte à multiplier à gauche U par S^m avec $m\in\{0,1\}$ puis par un élément $\xi^{-1}\in D$, on peut supposer que le point A est fixe par I.
Soit B le point (-1,1,1) ; le point U(B) est à la distance 2 de A ; c'est donc B, -C ou D, avec C = (-1,-1,1) et D = (1,-1,1) (Cf. figure).
Quitte à multiplier à gauche U par une puissance de R, R^{-k} avec $k\in\{0,1,2\}$, on peut supposer que B est fixe par U. Le point U(C) est alors à la distance $2\sqrt{2}$ de A et à la distance 2 de B. C'est donc soit le point C, soit le point -D.
Soit Σ la symétrie plane par rapport au plan engendré par {A,B,-A,-B}. Quitte à multiplier à gauche U par Σ^n avec $n\in\{0,1\}$ on peut supposer que U laisse fixe A, B et C, donc est l'identité. Or la symétrie Σ n'est autre que la transformation $R\sigma R^{-1}$.
Ceci prouve que le groupe des isométries de C_3 est engendré par D,R et S.

A.1.1. Proposition.- Le groupe ROT(3) des rotations du cube euclidien C_3 est isomorphe au groupe S_4.

☞ Désignons respesctivement par a,b,c,d les quatre diagonales du cube passant respectivement par les quatre points A, B, C et D. Toute rotation du cube définit une permutation de {a,b,c,d}. On a donc un homomorphisme naturel ψ: ROT(3) $\rightarrow S_4$

avec en particulier $\psi(R) = \begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}$ et $\psi(\rho) = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$.

a) Soit U une isométrie du cube qui laisse globalement fixe chacune des diagonales du cube. Si cette isométrie laisse globalement fixe la face supérieure du cube, elle fixe chacun des points A,B, C et D et elle est l'identité. Si au contraire elle transforme la face supérieure en la face inférieure, elle transforme les points A,B,C et D en leurs opposés respectifs et elle est la symétrie centrale S.
Ceci prouve que l'homomorphisme ψ est injectif.
b) Soient T_1 = (-B,-A,-D,-C), T_2 = (-D,-C,-B,-A) et T_3 = (C,D,A,B) = ρ^2, les trois retournements par rapport aux axes de coordonnées. On a les égalités :

$\psi(T_1) = \tau_{ab}\tau_{cd}$ $\psi(T_2) = \tau_{ad}\tau_{bc}$ $\psi(T_3) = \tau_{ac}\tau_{bd}$

On a ainsi trois éléments d'ordre 2 de A_4. Les images par ψ des rotations R, T_1RT_1, T_2RT_2, et T_3RT_3 sont des permutations circulaires d'ordre 3 laissant respectivement fixes les points a, b, d et c. Elle fournissent huit éléments d'ordre 3 de A_4. On en déduit que l'image par ψ du groupe engendré par $\{R,T_1,T_2,T_3\}$ est le groupe alterné A_4.
De plus $\psi(\rho)$ a une signature -1, ce qui prouve que ψ est surjectif, donc est un isomorphisme. ✍

Remarque.- Le groupe $\psi^{-1}(A_4)$ est engendré par R et par T_3, donc par R et P = RT_3 car on a $T_1 = RT_3R^{-1}$ et $T_2 = R^{-1}T_3R$.

Corollaire.- Le groupe ISO(3) des isométries du cube est d'ordre 48.

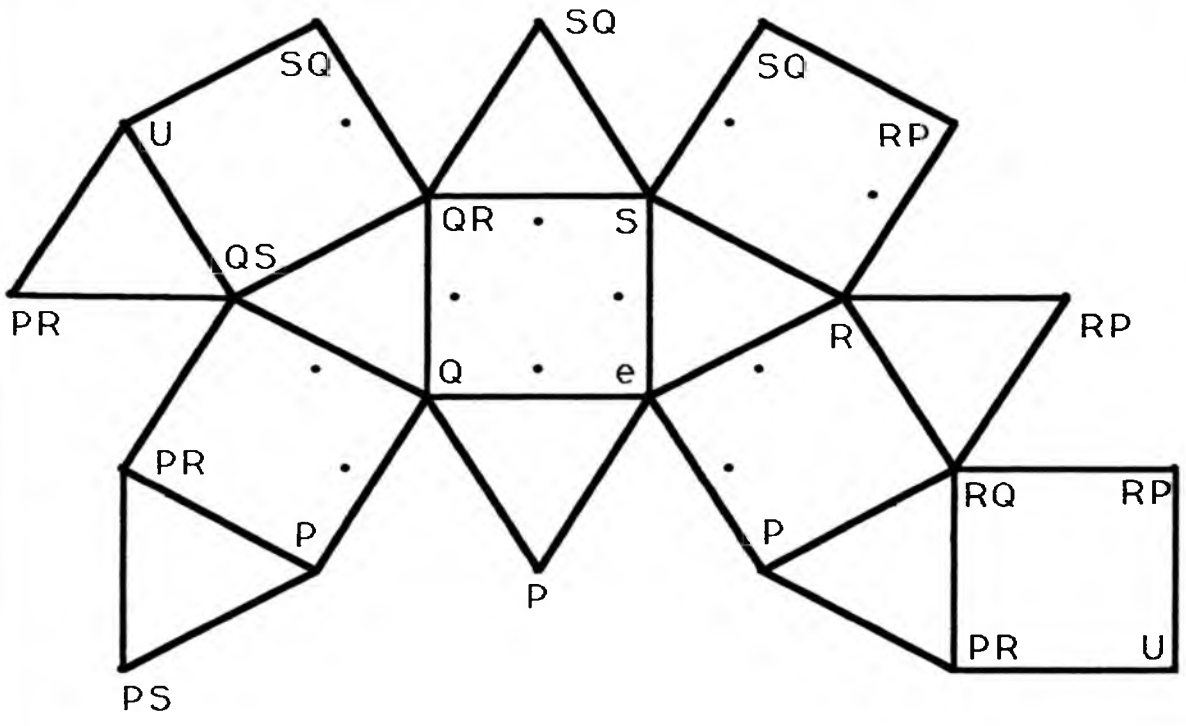
A.1.2. Proposition.- A. Le groupe G_1 des commutateurs de ISO(3) est le groupe d'ordre 12 engendrépar R et T_3, isomorphe au groupe aterné A_4.

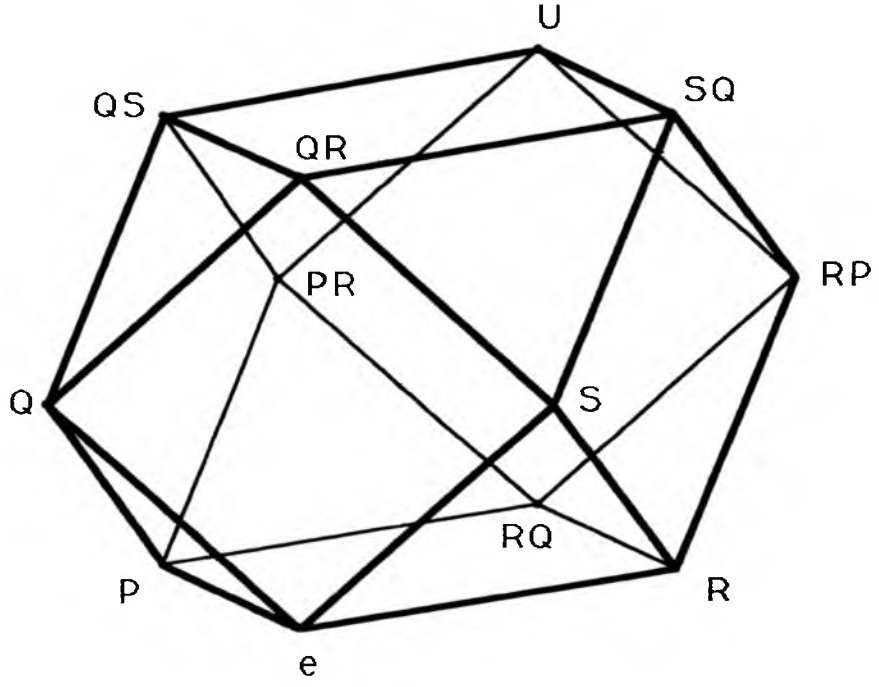
B. Le groupe G_2 des commutateurs de G_1 est le sous-groupe engendré par R.

☞ A. On utilise le fait que ISO(3) admet un sous-groupe isomorphe à ISO(2), sous-groupe des isométries qui laisse globalement invariante la face supérieure du cube.

En particulier le groupe des commutateurs de ce sous-groupe est un sous-groupe du groupe des commutateurs de ISO(3). En particulier $\rho^2 = T_3$ est un commutateur de ISO(3), de même que ses conjugués T_1 et T_2. Par ailleurs, soit σ est symétrie par rapport au plan d'équation $x_1 = x_2$. On a $\sigma = (A,D,C,B)$ et $\sigma R = (A,B-C,-D)$. Cette transformation est une symétrie plane, donc est d'ordre 2. On a $R = \sigma R \sigma R^2 = \sigma R \sigma R^{-1}$, ce qui prouve que R est un commutateur de ISO(3). Tout commutateur a pour image par ψ une permutation paire, ce qui prouve que ρ n'est pas un commutateur. On a donc bien $G_1 = < R, T_3 >$.
B. A partir du fait que $T_2 = R^{-1}T_3R$ on obtient que $T_1 = T_2T_3 = R^{-1}T_3RT_3$ est un commutateur de G_1, de même que ses conjugués T_2 et T_3 dans G_1. On vérifie sans peine que pour tout $i \in \{1,2,3\}$ $RTiR^{-1}$ est un T_j, donc que le groupe $H = \{e,T_1,T_2,T_3\}$ est invariant dans G_1. Le quotient est un groupe d'ordre 3, donc est cyclique, ce qui prouve que H contient G_2. On a donc $H = G_2$ qui est isomorphe au groupe de KLEIN $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le groupe ISO(3) est donc de profondeur 3.

Pour en terminer avec cet exemple, on va construire un graphe de CAYLEY pour chacun des groupes $G_1 \simeq A4$ et $ROT(3) \simeq S_4$.
Pour le premier, on utilise la remarque faite plus haut et on considère le système de générateurs symétrique $\mathcal{S}_1 = \{R, S = R^{-1}, P = T_3R, Q = P^{-1}\}$ dont tous les éléments sont d'ordre 3, ce qui permet d'éviter les générateurs d'ordre 2. Tout sommet du graphe de CAYLEY est de degré 4, ce qui implique que le graphe a 24 arêtes. Ce graphe présente des cycles de longueur 3 dûs aux ordres des générateurs et des cycles de longueur 4 dûs à la relation $P = RQR$.
Traçant ce graphe de proche en proche, on est amené à en dessiner un patron qui fournit un polyèdre de $\mathbb{R}^3$, très précisément un **cuboctaèdre** obtenu à partir d'un cube en tronquant chaque sommet par le plan passant par les milieux des trois arêtes adjacentes.

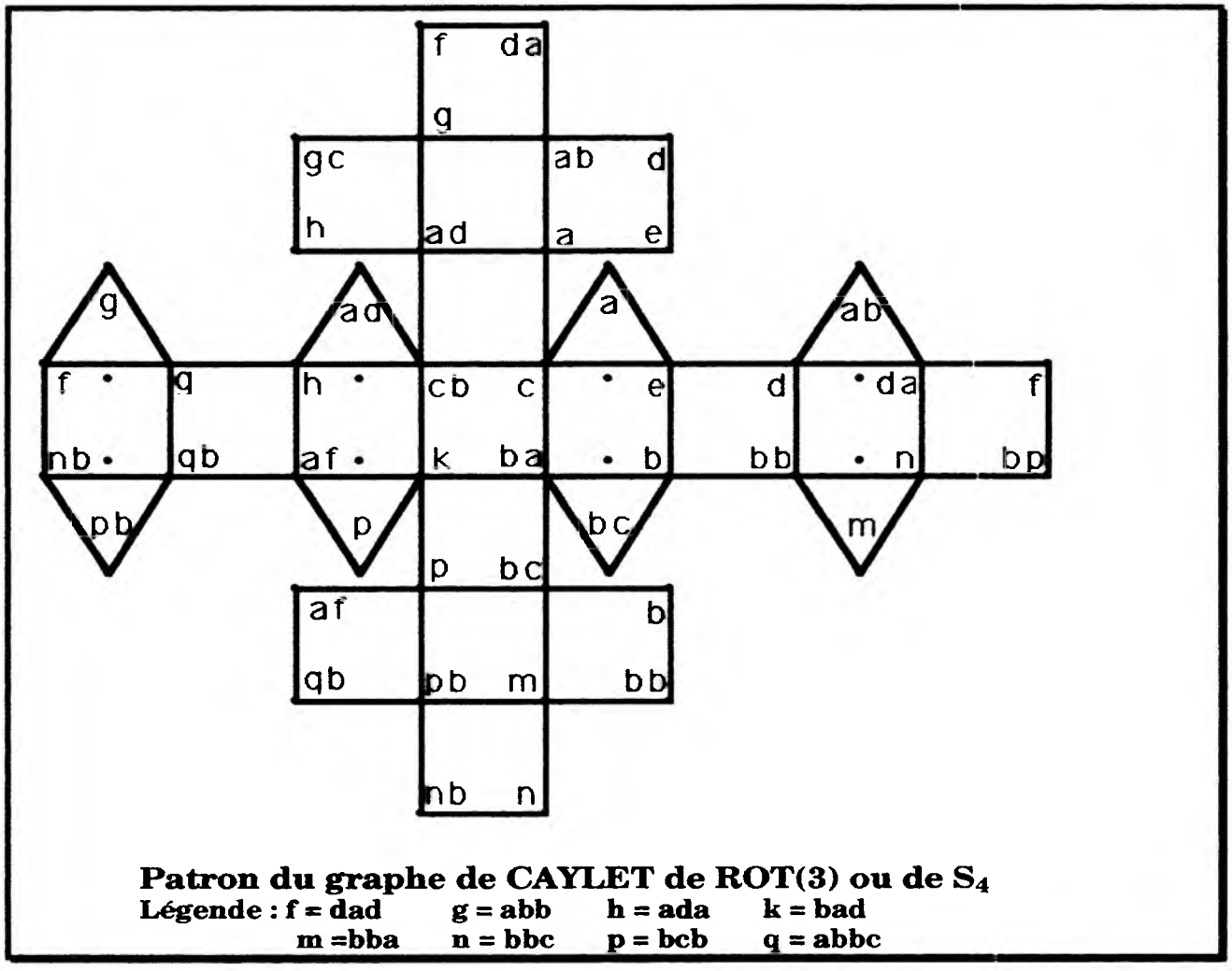




Le cuboctaedre,
graphe de CAYLEY du groupe des commutateurs de ROT(3)
La transformation U est PRP et PS = RP

En ce qui concerne le groupe ISO(3) ou S_4, on remarque qu'il est engendré par R qui est d'ordre 3 et fournit des cycles d'ordre 3, et par ρ qui est d'ordre 4 et fournit des cycles d'ordre 4. Par ailleurs on a la relation rRrR = e qui

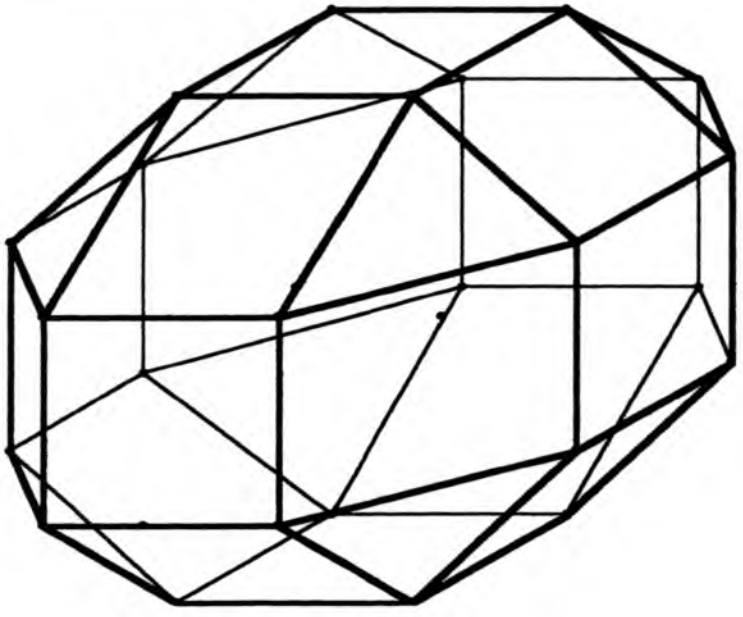
fournit aussi des cycles d'ordre 4. On construit le graphe de proche en proche avec le système symétrique de générateurs S = {a =R, b = ρ, c = R^{-1}, d = ρ^{-1}}. On obtient également un patron qui s'avère être un patron de polyèdre de $\mathbb{R}^3$. Ce polyèdre convexe admet une rotation d'ordre 8.
Voir les diverses figures correspondantes.



Patron du graphe de CAYLET de ROT(3) ou de S_4
Légende : f = dad g = abb h = ada k = bad
m =bba n = bbc p = bcb q = abbc

Remarque.- Bien entendu les patrons ne sont pas uniques. On sait qu'un patron s'obtient à partir du polyèdre en traçant un sous-arbre maximal du graphe et en découpant le long de toutes les arêtes ne figurant pas dans l'arbre.

Vu dans l'espace, ce polyhèdre a l'allure suivante :



Le polyhèdre du graphe de CAYLEY de S_4

On laisse le soin au lecteur de voir si on peut construire un graphe de CAYLEY du groupe ISO(3) comme graphe des arêtes d'un polyèdre convexe de $\mathbb{R}^3$.

APPENDICE 2 : LE GROUPE DE HEISENBERG CLASSIQUE

On définit le groupe de HEISENBERG classique, et on note ici $\mathbb{H}(3)$, le groupe des matrices triangulaires supérieures d'ordre 3 à coefficients entiers rationnels de la forme : $M(u,v,w) = \begin{bmatrix} 1 & u & w \\ 0 & 1 & v \\ 0 & 0 & 1 \end{bmatrix}$.

2.1. Proposition.- Soient respectivement $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ et $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

a. Le groupe $\mathbb{H}(3)$ est engendré par A et B.

b. Le groupe des commutateurs de $\mathbb{H}(3)$ coïncide avec le centre de $\mathbb{H}(3)$. C'est le sous-groupe isomorphe à $\mathbb{Z}$ engendré par $C = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

En particulier pour tout couple d'entiers rationnels (m,n) on a
$A^mB^nA^{-m}B^n = C^{mn}$

c. Tout élément de $\mathbb{H}(3)$ s'écrit d'une manière unique sous la forme $C^tA^mB^n$ où m, n et t sont des entiers rationnels.

☞ On calcule le produit général de deux éléméents de $\mathbb{H}(3)$:

$$M(m, n, p)\times M(\mu, \nu, \pi) = M(m + \mu, n + \nu, p + m\nu + \pi).$$

a. Le calcul direct d'un produit de la forme $A^mB^nA^pB^q$ donne le résultat suivant :

$$A^mB^nA^pB^q = M(m + p, n + q, qm + pq + mn).$$

En particulier pour tout triplet $(\mu, \nu, \pi)\in\mathbb{Z}^3$, on aura $A^mB^nA^pB^q = M(\mu, \nu, \pi)$ si le sytème suivant a une solution en nombres entiers :

$$[m + p = \mu, n + q = \nu, qm + pq + mn = \pi]$$

ou $[n(m - \mu) = \pi - \mu\nu, p = \mu - m, q = \nu - n]$.

Ce système admet au moins la solution

$$\{n = 1, m = \pi + \mu - \mu\nu, p = \mu\nu - \pi, q = \nu - 1].$$

b. Soit $L = M(\mu, \nu, \pi)$ un élément du centre de $\mathbb{H}(3)$.
Il vérifie la relation $\forall(m,n)\in\mathbb{Z}^2$, $m\nu - n\mu = 0$.
Inversement on vérifie sans peine que toute matrice $M(0,0,p) = C^p$ appartient au centre de $\mathbb{H}(3)$.
Pour tout triplet (m, n p) d'entiers rationnels tel que $n \neq 0$ et $p \neq 0$ on a :
$A^mB^nA^p = A^mB^{n-1}BA^p = A^mB^{n-1}BAA^{p-1} = A^mB^{n-1}C^{-1}ABA^{p-1} = C^{-1}A^mB^{n-1}ABA^{p-1}$
Par descente on obtient l'égalité : $A^mB^nA^p = C^{-np}A^{m+p}B^n$.
Cela fournit immédiatement $A^mB^nA^{-m}B^{-n} = C^{mn}$
De plus un générateur "ordinaire" du groupe des commutateurs de $\mathbb{H}(3)$ est par définition de la forme :
$\{C^pA^mB^n\}\{C^\pi A^\mu B^\nu\}\{C^{-p}B^{-n}A^{-m}\}\{C^{-\pi}B^{-\nu}A^{-\mu}\} = A^mB^nA^\mu B^{\nu-n}A^{-m}B^{-\nu}A^{-\mu}$
et d'après le calcul qu'on vient d'effectuer :
$\{C^pA^mB^n\}\{C^\pi A^\mu B^\nu\}\{C^{-p}B^{-n}A^{-m}\}\{C^{-\pi}B^{-\nu}A^{-\mu}\} = C^{-m\mu}A^{m+\mu}B^\nu A^{-m}B^{-\nu}A^{-\mu}$
$= C^{-m(\mu-\nu)}$.

Ceci prouve que le groupe des commutateurs de $\mathbb{H}(3)$ est engendré par C et est égal au centre de $\mathbb{H}(3)$.

c. L'existence de la décomposition annoncée est établie plus haut. Par ailleurs, une écriture de la forme $C^tA^mB^n = C^uA^vB^w$ est équivalente à $C^{t-u}A^mB^{n-w}A^{-v} = e$, elle-même équivalente à $C^{t-u+nv-vw}A^{m-v}B^{n-w} = e = M(m-v, n-w,(m-v)(n-w)+t-u+v(n-w))$,
ce qui implique $n = w$, $m = v$ et $t = u$ puis l'unicité de la décomposition. ✍

2.2 Proposition.- Si un élément de $\mathbb{H}(3)$ est décomposé comme mot en A et en B avec exposants positifs ou négatifs, la somme des exposants de A et la somme des exposants de B ne dépendent pas de la décomposition choisie. En particulier on a une suite exacte de groupes :

$$1 \to [\mathbb{H}(3), \mathbb{H}(3)] \to \mathbb{H}(3) \to \mathbb{Z}\times\mathbb{Z} \to 0,$$

où l'homorphisme $\mathbb{H}(3) \to \mathbb{Z}\times\mathbb{Z}$ fait correspondre à tout élément de $\mathbb{H}(3)$ le couple formé de la somme des exposants de A et de la somme des exposants de B dans n'importe quelle écriture.

☞ Il suffit de remarquer que pour tout $x\in\mathbb{H}(3)$ dela forme $x = \prod_{i=1}^{N} A^{\alpha(i)}B^{\beta(i)}$
on a une écriture standard : $x = C^{\theta(x)}A^uB^v$, avec $u = \sum_{i=1}^{N} \alpha(i)$ et $v = \sum_{i=1}^{N} \beta(i)$.
Le reste de la preuve est immédiat. ✍

La proposition précédente donne une idée d'un graphe de CAYLEY pour ce groupe : on choisit le système de générateurs $\{A, A^{-1}, B, B^{-1}, C, C^{-1}\}$. Les arêtes de ce graphe sont de l'une des formes $A^mB^nA^p = C^{-np}A^{m+p}B^n$.
$\{C^\mu A^\alpha B^\beta, C^{\mu+1}A^\alpha B^\beta\}$, $\{C^\mu A^\alpha B^\beta, C^{\mu+}A^\alpha B^{\beta+1}\}$, $\{C^\mu A^\alpha B^\beta, C^{\mu-\beta}A^{\alpha+1}B^\beta\}$
On laisse au lecteur le soin de le tracer.

APPENDICE 3 : LE GROUPE SL(2,ℤ)

Ce groupe est le groupe multiplicatif des matrices carrées à coefficients entiers rationnels, d'ordre 2 et de déterminant 1. Ce groupe joue un rôle très important en arithmétique et en géométrie. On le retient également dans cette appendice comme exemple de groupe opérant sur un ensemble, avec applications à des phénomènes artistiques.

3.1. Définition et proposition.- On appelle demi-plan de POINCARE l'ensemble $\mathfrak{H}$ des nombres complexes dont la partie imaginaire est strictement positive.
On définit une opération de SL(2,ℤ) sur $\mathfrak{H}$ en posant :

$$\forall z\in\mathfrak{H},\forall g\in SL(2,\mathbb{Z}),\ g=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow g.z=\frac{az+b}{cz+d}.$$

☞ On vérifie sans peine les propriétés

$$\forall z\in\mathfrak{H},\forall g\in SL(2,\mathbb{Z}),\forall g'\in SL(2,\mathbb{Z})\ g(g'z)=(gg')z.$$

$$\forall z\in\mathfrak{H},\forall g\in SL(2,\mathbb{Z}),\ g=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow im(g.z)=\frac{im(z)}{|cz+d|^2}.$$ ✍

Soient respectivement $S=\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ et $T=\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Avec cette notation on a :

3.2. Proposition. - a. L'élément S est d'ordre 4 et la transformation de $\mathfrak{H}$ qui lui correspond est le produit de l'inversion géométrique de pôle 0 et puissance 1 par la symétrie par rapport au second axe de coordonnées. Cette dernière est d'ordre 2, de même que la classe de S dans PSL(2,ℤ)=SL(2,ℤ)/{-1,1}.

b. L'élément T engendre un groupe isomorphe à ℤ et la transformation de $\mathfrak{H}$ qui lui correspond par l'action de SL(2,ℤ) est la translation de vecteur 1.
Le produit ST est d'ordre 6. Son image dans PSL(2,ℤ) est d'ordre 3.

c. Le centre de SL(2,ℤ) est {I, -I}.

d. Un domaine fondamental de $\mathfrak{H}$ pour l'action de SL(2,ℤ) est l'ensemble $\mathfrak{D}$ = {z | -1/2 ≤ re(z) ≤ 0 & | z | ≥ 1} ∪ {z | 0 < re(z) < 1/2 & | z | > 1}. Le groupe SL(2,ℤ) est engendré par S et T.

☞ Les assertions a, b et c se prouvent directement. En ce qui concerne l'assertion **d.**, soit $z \in \mathcal{H}$. L'ensemble des points $\{cz + d \mid (c,d) \in \mathbb{Z}\times\mathbb{Z}\}$ est un réseau de $\mathbb{C}$ engendré par 1 et zet le sous-ensemble $L(z) = \{cz + d \mid (c,d) \in \mathbb{Z}\times\mathbb{Z}$, c et d premiers entre eux$\}$ ne contient pas 0. En particulier la fonction $u \in \mid u \mid$ de L(z) dans $\mathbb{R}_+^*$ admet un minimum et on en déduit que la fonction $g \rightarrow$ Im(g.z) de $SL(2,\mathbb{Z})$ dans $\mathbb{R}_+^*$ admet un maximum. Soit $g \in SL(2,\mathbb{Z})$ réalisant ce maximum. Il existe alors $j \in \mathbb{Z}$ tel que $re(T^j g.z) \in [-1/2,1/2[$ avec $im(T^j g.z) = im(g.z)$. Si on avait $\mid T^j g.z \mid < 1$, on a aurait $im(ST^j g.z) = im(T^j g.z)/ \mid T^j g.z \mid >$ Im(g.z) et une contradiction. Enfin si $T^j g.z$ n'appartient pas à $\mathcal{D}$ mais est de module 1, $ST^j g.z$ appartient à $\mathcal{D}$. Soient z_1 et z_2 dans $\mathcal{D}$ tels qu'existe $g \in SL(2,\mathbb{Z})$ avec $z_2 = g.z_1$. On peut supposer que $im(z_2) \geq im(z_1)$. On en déduit que $\mid cz_1 + d \mid \leq 1$, équivalent à $1 \geq c^2 \mid z_1 \mid^2 + d^2 + 2cdre(z_1) \geq 0$, et implique $1 \geq c^2 + d^2 - \mid cd \mid$. Cette dernière inégalité implique l'une des trois conséquences :

- c = 0 et $d \in \{-1,1\}$, la transformation associée à g est une translation entière, donc l'identité car $re(z_1 - z_2) < 1$, c'est-à-dire $g \in \{-I,I\}$

- $c \in \{-1,1\}$ et d = 0, et g est soit ±I soit ±S. Dans le second cas, cela impliquerait $\mid z_1 \mid = 1$ et une contradiction car les affixes de z_1 et de z_2 seraient symétriques par rapport au second axe de coordonnées.

- c et d sont de module 1. On a $re(z_1) = -1/2$, $\mid z_1 \mid = 1$ et cd =1.

On en déduit que $im(z_2) = im(z_1) = \sqrt{3}/2$ et donc $z_1 = z_2$ avec $g \in \{-I,I\}$.

Obtenant dans tous les cas $z_1 = z_2$, on conclut que $\mathcal{D}$ est un domaine fondamental pour l'action de $SL(2,\mathbb{Z})/\{-I,I\}$.

Soit $g \in SL(2,\mathbb{Z})$ et soit $z_0 \in \mathcal{D}$. Soit $\alpha \in \mathbb{Z}$ tel que $re(T^\alpha g(z_0)) \in [-1/2, 1/2[$. Si on a $\backslash\mathbf{B}\backslash bc\backslash \mid T^\alpha g(z_0)) < 1$ on fait agir S pour obtenir $\backslash\mathbf{B}\backslash bc\backslash \mid ST^\alpha g(z_0)) > 1$, puis éventuellement une nouvelle translation T^β pour obtenir $T^\beta ST^\alpha g(z_0) \in \mathcal{D}$. On en déduit alors que la transformation associée à g est celle qui est associée à $T^{-\alpha}S^3T^{-\beta}$, c'est à dire que modulo -I, g est égale à $T^{-\alpha}S^3T^{-\beta}$,car on vient de voir que $\mathcal{D}$ est domaine fondamental de $\mathcal{H}$ pour l'action de $SL(2,\mathbb{Z})/\{-I,I\}$. Si on a $\backslash\mathbf{B}\backslash bc\backslash \mid T^\alpha g(z_0)) = 1$, ou bien $T^\alpha g(z_0) = z_0$ ou bien $ST^\alpha g(z_0) = z_0$ et on conclut de la même façon. ✍

3.4. Lemme. Soit p un nombre premier. La réduction modulo p induit un homorphisme surjectif ϕ_p: $SL(2,\mathbb{Z}) \rightarrow SL(2,\mathbb{Z}/p\mathbb{Z})$. En particulier le noyau de ϕ_p est un sous-groupe invariant de $SL(2,\mathbb{Z})$ d'indice $(p + 1)p(p -1)$.

☞ La première assertion résulte simplement du fait que la réduction modulo p est un homorphisme d'anneaux surjectif et de ce que pour les deux groupes les éléments S et T engendrent le groupe. En ce qui concerne la second assertion, d'une part le cardinal de $GL(2,\mathbb{Z}/p\mathbb{Z})$ est $(p^2 - 1)(p - 1)$, le nombre de bases de $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ comme espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$ [Une telle base est donnée par le choix d'un premier élément non nul puis d'un second élément n'appartenant pas à la droite engendrée par le premier]. L'application déterminant est un homorphisme surjectif de $GL(2,\mathbb{Z}/p\mathbb{Z})$ sur $(\mathbb{Z}/p\mathbb{Z})\setminus\{0\}$ qui est d'ordre p - 1. On conclut. ✍

On remarquera que la première assertion du lemme reste vraie si on remplace p par un entier quelconque.

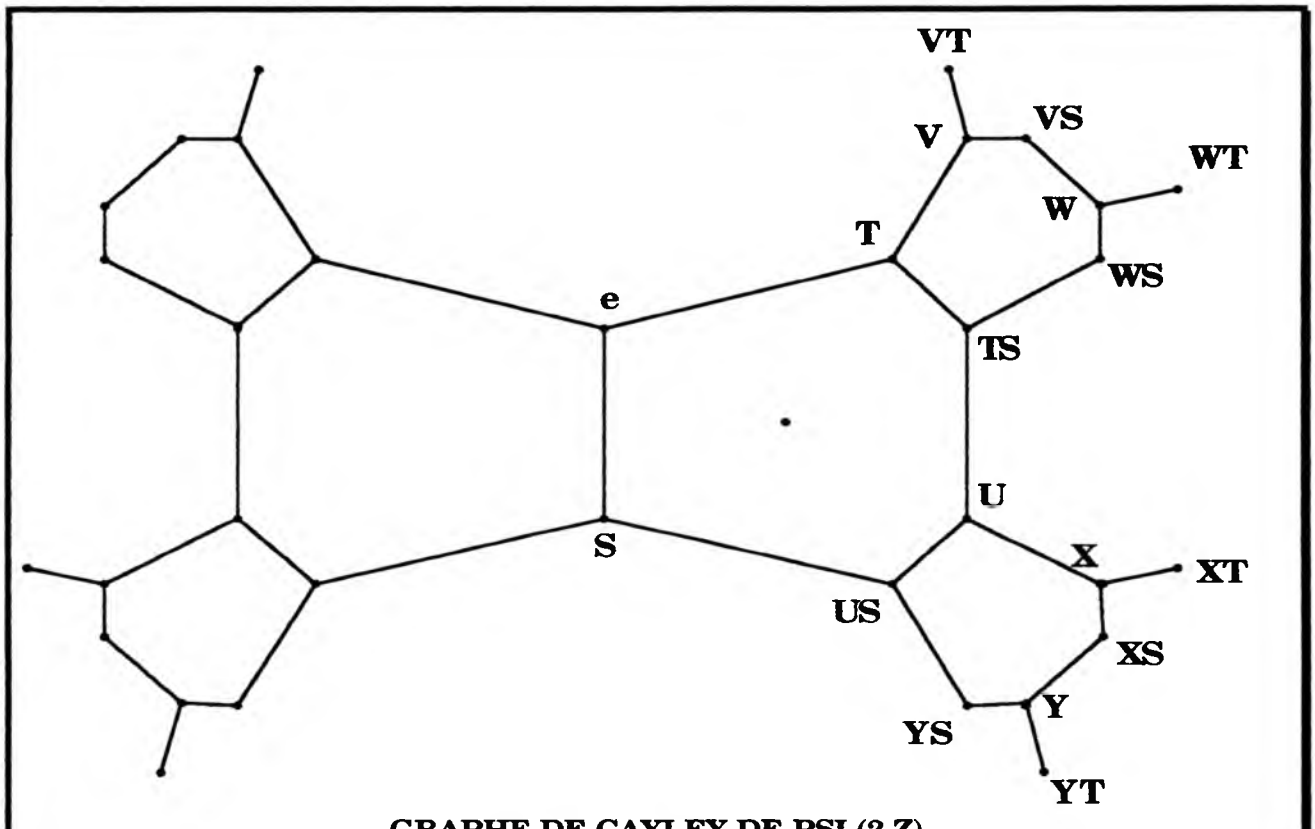
On va utiliser ce lemme pour se livrer à un exercice consistant à identifier les deux premiers groupes de commutateurs du groupe $PSL(2,\mathbb{Z}) = SL(2, \mathbb{Z})/\{-I,I\}$. Dans ce groupe, l'élément S est d'ordre 2 tandis que l'élément ST est d'ordre 3.

3.5. Proposition.- Le groupe des commutateurs de $PSL(2, \mathbb{Z})$ est le sous-groupe G d'indice 6 engendré par les éléments ST^3 et T^2ST.
Le groupe K des commutateurs de G est le sous-groupe distingué de $PSL(2,\mathbb{Z})$ engendré par T^6. Le groupe G/K est un groupe abelien libre de rang 2.

☞ Désignons par G le sous-groupe de engendré par ST^3, T^3S, TST^2 et T^2ST.
On a $ST^3 = T^{-1}ST^{-1}ST^2 = T^{-1}[ST^{-1}ST]T$ qui est un commutateur. Les quatre autres candidats générateurs sont des conjugués de celui-ci, donc sont des commutateurs. Précisément on a
$S[ST^3]S = T^3S$ $\quad T[ST^3]T^{-1} = TST^2$ $\quad T^2[ST^3]T^{-2} = T^2ST = (TST^2)(T^{-3}S)$
$T^{-1}[ST^3]T = (TST^2)^{-1}ST^3$ $\quad T^{-2}[ST^3]T^2 = (ST^3)^{-1}(T^2ST)^{-1}(T^3S)(ST^3)$
Ceci prouve entre autres que le groupe G est un sous-groupe invariant de $PSL(2, \mathbb{Z})$ puisque ce groupe est engendré par (les classes modulo $\{-I,I\}$) de S et T. Le groupe G est engendré par les trois éléments $u = ST^3$, $v = T^6$ et $w = T^2ST$.
Dans le groupe quotient $PSL(2, \mathbb{Z})/G$ la classe de S est d'ordre 2 et la classe de T est d'ordre 6 avec T^3 congru à S. Ce groupe est donc d'ordre 6 engendré par la classe de T. Puisque ce groupe quotient est abélien, le groupe G contient le groupe des commutateurs de $PSL(2, \mathbb{Z})$. Le groupe G est donc le groupe des commutateurs de $PSL(2, \mathbb{Z})$.

On a par calcul direct l'identité : $wu^{-1}w^{-1}u = T^2ST\ T^{-3}S\ (T^2ST)^{-1}ST^3 = T^6$;
Il en résulte que le groupe des commutateurs de G contient tous les conjugués de T^6 dans PSL(2,$\mathbb{Z}$), donc contient K, le sous-groupe distingué de PSL(2,Z) engendré par T^6.
On peut montrer facilement que le groupe G est engendré librement par u et w. Le groupe G/K est engendré par les classes de u et de w. Il est abélien d'après l'identité ci-dessus. Donc le groupe des commutateurs de G est le groupe K. De plus, le groupe G/K est l'"abelianisé" du groupe libre à deux générateurs, donc est isomorphe au groupe abelien libre de rang 2.
En particulier la classe de u dans G/K est d'ordre infini. ✍

Pour terminer, essayons de donner un graphe de CAYLEY de PSL(2,$\mathbb{Z}$). On prend comme générateurs les classes de S et de T. Les cycles de base de ce graphe sont d'ordre 6 et on a une reproduction récursive de ces cycles.
On obtient par exemple la disposition de la figure ci-dessous.



GRAPHE DE CAYLEY DE PSL(2,Z)
U = TST V =TT W = VST = TTST X = UT Y = XST
L'inverse d'un point est son symétrique par rapport à la droide de S et de e

Remarques finales.- • La remarque de caractère artistique est la suivante : la fonction homographique $z \to \frac{iz+1}{iz-1}$ réalise une bijection du demi-plan de POINCARE sur le disque unité ouvert. On peut donc par tranfert faire agir $PSL(2,\mathbb{Z})$ sur le disque. En particulier le pavage de $\mathcal{H}$ par les images de D fournit un pavage isométrique (dans le cadre de la géométrie hyperbolique) du disque, pavage par des triangles isocèles don l'angle au sommet est nul. On se rapproche ainsi de certains dessins de ESCHER, sauf qu'ESCHER utilisait des pavages par des polygones réguliers hyperboliques de plus de trois cotés.

• Enfin le groupe $PSL(2,\mathbb{Z})$ agit, (non librement puisque ce n'est pas un groupe libre), sur un arbre géodésique (c'est-à-dire dont les arêtes sont des arcs de géodésique du plan hyperbolyque) joignant les barycentres des cellules d'un tel pavage. Voir à ce sujet [Se] de la bibliographie de la première partie.