

## TRIANGULATIONS

M. Bauer et C. Itzykson  
Service de Physique Théorique †  
Centre d'Etudes de Saclay, 91191 Gif-sur-Yvette Cedex, France

1. GROUPE CARTOGRAPHIQUE
2. STRUCTURE COMPLEXE
3. STRUCTURE ARITHMETIQUE
4. DECOMPOSITION CELLULAIRE DE L'ESPACE DES MODULES
  - A. La caractéristique virtuelle
  - B. Formules d'intersection

Ces notes traitent de diverses questions liées à la triangulation des surfaces.

Ce sujet, à l'origine de la partie la plus élémentaire de la topologie, se révèle d'une richesse insoupçonnée. D'une part physiciens et mathématiciens en explorant la "gravité quantique" à deux dimensions en ont tiré des informations sur l'espace des modules des courbes algébriques. D'autre part un théorème de Belyi établit une équivalence entre courbes arithmétiques et recouvrements finis de la droite projective ramifiés aux images réciproques de trois points (0, 1 et  $\infty$ ) de sorte qu'une décomposition de la sphère de Riemann en deux triangles peut être relevée en une triangulation caractéristique de la courbe. Il s'ensuit que le groupe de Galois  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  agit sur les triangulations (des surfaces orientables compactes) dont les sommets adjacents portent deux valeurs distinctes parmi trois possibles.

La combinatoire, la théorie des groupes à divers titres, la topologie et l'arithmétique semblent inextricablement mêlées. On se bornera ici à décrire les aspects les plus élémentaires, accessibles aux auteurs, en mettant plutôt l'accent sur les points qui leur sont obscurs.

Que la théorie des groupes (finis ou plus généralement discrets) soit liée aux décompositions cellulaires trouve son origine dans l'interprétation graphique d'une présentation par générateurs et relations qui date au moins de Cayley (cf. le chapitre 8 du livre de Coxeter et Moser). Une décomposition cellulaire d'une surface compacte orientable est engendrée par un "groupe cartographique" (orienté) selon la terminologie de Grothendieck dans son "Esquisse d'un programme". Notre collègue J.-M. Drouffe en avait aussi donné la construction, qu'on pourrait généraliser en dimension supérieure. Ce groupe apparaît aussi dans des travaux d'analyse combinatoire consacrés aux hypergraphes. Nous allons voir qu'il permet de donner des preuves élémentaires de propriétés combinatoires simples.

Il est peut être plus intéressant de souligner combien de questions restent sans réponse, les plus fascinantes étant de nature arithmétique. Ce sont aussi celles devant lesquelles les physiciens se trouvent malheureusement les plus démunis. On pourra consulter à ce sujet les travaux de Voevodsky et Shabat, et pour les aspects les plus fondamentaux le livre " $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ " où sont rassemblées les contributions des théoriciens des nombres difficiles à déchiffrer pour les non-spécialistes.

Pour donner une idée de notre ignorance citons ici le problème relatif au théorème d'existence fondamental de Riemann dans son mémoire sur les fonctions Abéliennes: une variété analytique unidimensionnelle compacte est une variété algébrique.

† Laboratoire de la Direction des Sciences de la Matière du Commissariat à l'Energie Atomique

Si la donnée des ramifications d'une telle surface au dessus de trois points  $0, 1, \infty$ , de la droite projective sur  $\mathbb{C}$  détermine effectivement la structure complexe et si on dispose dès l'abord d'une fonction rationnelle sur la surface  $\Sigma$  donnée par l'application  $\beta : \Sigma \rightarrow \mathbb{C}P_1$ , il n'y a à notre connaissance aucune méthode constructive générale pour engendrer le corps des fonctions rationnelles sur  $\Sigma$ . Ceci rend la bijection (de Belyi),

$$(\Sigma, \beta) \begin{array}{c} \xrightarrow{(1)} \\ \xleftarrow{(2)} \end{array} \text{décomposition cellulaire finie}$$

hautement non triviale dans la direction (2) au sens algébrique voire arithmétique. Tout au plus comme le font Voevodsky et Shabat peut on chercher à accumuler des exemples. A fortiori les questions de corps de définition et d'action Galoisienne sont elles hors de portée en dehors de quelques généralités.

Comme on l'a indiqué, l'étude détaillée des décompositions cellulaires est par ailleurs intéressante, en ce qu'elle se transporte en une décomposition de l'espace des modules des classes d'isomorphisme des courbes algébriques à  $n$  points marqués, espace de dimension  $6g - 6 + 2n$  (sur  $\mathbb{R}$ ). On évoquera brièvement dans une dernière section, quelques résultats dus à Harer, Zagier, Penner, Witten et Kontsevich, en se bornant à la partie algébrique, la plus familière aux auteurs.

On s'est efforcé de trouver un compromis entre la terminologie des physiciens et celle des mathématiciens et entre le français et le franglais. En particulier on appellera *groupe cartographique* (groupe cartographique orienté selon Grothendieck) tout groupe discret qui admet une présentation en termes de deux générateurs dont l'un est une involution (complétée le cas échéant par des relations). Un tel groupe est un quotient naturel du groupe fondamental de la droite projective (sur  $\mathbb{C}$ ) privée de trois points. De même, on appellera *carte* (finie) la donnée d'un ensemble (fini) de brins (drapeaux orientés selon Grothendieck) muni d'une action transitive d'un groupe cartographique, équipé de sa présentation, tel que l'involution agisse sans point fixe. Ceci revient à dire que la classe d'équivalence de l'involution n'intersecte pas le stabilisateur  $B$  de l'un quelconque des brins. Il s'ensuit pour  $G$  fini que son ordre et le nombre de brins (qui en est un sous multiple) sont pairs. Si le stabilisateur  $B$  est réduit à l'identité on parlera de *carte régulière* (par référence aux solides réguliers). Sauf indication contraire nous nous limiterons aux groupes et cartes finis.

Ces notes sont en partie le fruit d'une collaboration avec P. Cohen et J. Wolfart d'une part, J.-B. Zuber et P. Di Francesco d'autre part. J.-M. Luck nous a prêté main forte pour la partie numérique. Nous les remercions tous vivement.

## 1. GROUPE CARTOGRAPHIQUE

On considère un ensemble fini de cellules bidimensionnelles polygonales (le nombre de côtés est aussi supposé fini) tel que les arêtes soient identifiées par paires (qui peuvent appartenir à la même cellule). La surface obtenue est compacte pour toute topologie raisonnable. Nous supposons toujours qu'elle est connexe. Comment s'assurer qu'elle est orientable ? Chaque cellule peut être orientée, ce qui conduit à un ordre cyclique des sommets. On demande alors que les arêtes identifiées portent une orientation opposée. Ces données, que nous appelons par abus de langage une carte, ont été diversement dénommées dans des travaux récents. Dans les modèles de matrices des physiciens, elle apparaît comme "graphes de Feynmann à doubles arêtes (ou propagateurs) orientés" dans un développement perturbatif ('t Hooft), ou encore "graphes épais" (Penner). Les sommets où ces arêtes dédoublées se rencontrent héritent d'un ordre cyclique, tandis que les faces correspondent aux cycles formés par les lignes orientées (Figure 1).

A chaque carte on associe une carte duale obtenue en échangeant les sommets et les faces. Soit  $S$  le nombre de sommets,  $A$  celui des arêtes (après identification) et  $F$  celui des faces.

Coupant chaque arête en deux demi arêtes chacune attachée à un sommet (ces sommets pouvant être distincts ou confondus), nous obtenons  $2A$  brins (par dualité on obtient ainsi les

doubles arêtes chacune attachée à une face). Si  $S_v$  et  $F_v$  désignent les nombres respectifs de sommets et de faces de valence  $v$ , on a les relations

$$\begin{aligned} 2A &= \sum v S_v = \sum v F_v \\ S &= \sum S_v \quad F = \sum F_v \end{aligned}$$

Ainsi le nombre de sommets ou de faces de valence impaire est-il pair.

Définissons deux éléments du groupe  $\Sigma_{2A}$  des permutations des  $2A$  brins, supposés indexés, en utilisant la représentation fléchée des physiciens. Chaque arête entrante en un sommet est suivie d'une arête sortante. La permutation  $\sigma_0$  résultante a pour décomposition cyclique une représentation des sommets avec leur valence. De même chaque brin est associé à un partenaire pour reconstituer une double arête définissant une involution  $\sigma_1$  possédant  $A$  cycles de longueur 2. Enfin la décomposition cyclique de la permutation  $\sigma_2$  telle que

$$\sigma_0 \sigma_1 \sigma_2 = \text{id.}$$

code les faces avec leur valences. Le groupe cartographique  $G$  ainsi engendré agit transitivement sur la carte connexe qui peut être identifiée avec l'espace quotient  $G/B$  où  $B$  est le stabilisateur d'un brin (changer de brin conjugué  $B$  dans  $G$ ),  $G$  étant muni de sa présentation  $\{\sigma_0, \sigma_1, \sigma_2\}$ . Un élément de  $G$  qui agit trivialement sur les brins est forcément l'identité, ce qui impose des restrictions sur  $B$ . En effet, si  $G$  est un groupe fini à trois générateurs  $\sigma_2, \sigma_1, \sigma_0$  vérifiant entre autres les relations  $\sigma_1^2 = \sigma_0 \sigma_1 \sigma_2 = 1$ ,  $\sigma_1 \neq 1$  et  $B$  est un sous groupe de  $G$ , on peut essayer d'associer une carte à  $G/B$ , dont les éléments sont identifiés aux demi-arêtes. Les arêtes sont les orbites de l'action de  $\sigma_1$ , les faces les orbites de l'action de  $\sigma_2$  et les sommets les orbites de l'action de  $\sigma_0$ . Ceci reconstruit bien une carte si et seulement si les orbites de  $\sigma_1$  ont toujours deux éléments, c'est-à-dire si et seulement si  $\sigma_1$  agit sans points fixes sur  $G/B$ . Ceci signifie que la classe de conjugaison de  $\sigma_1$  dans  $G$  ne rencontre pas  $B$ . Dans ce cas, il est facile de vérifier que le groupe cartographique de la carte associée à  $G/B$  est le quotient de  $G$  par le plus grand sous groupe invariant de  $G$  contenu dans  $B$  (ce sous groupe invariant est l'intersection des conjugués de  $B$  dans  $G$ ). Il y a donc une correspondance biunivoque entre les cartes de groupe cartographique  $G$  muni de sa présentation  $\{\sigma_0, \sigma_1, \sigma_2\}$  et les sous groupes de  $G$  disjoints de la classe de conjugaison de  $\sigma_1$  et ne contenant aucun sous groupe invariant non trivial de  $G$ .

La caractéristique d'Euler d'une carte

$$\chi = S - A + F$$

est paire. En effet comme sous groupe de  $\Sigma_{2A}$  le groupe cartographique  $G$  possède une représentation alternée unidimensionnelle:  $g \rightarrow \rho(g) = (-1)^{\#\text{cycles pairs}}$ . Si  $S_+$  ( $F_+$ ) désignent le nombre de sommets (faces) de valence paire, on a d'après ce qui précède

$$\begin{aligned} \rho(\sigma_0) &= (-1)^{S_+} = (-1)^S \\ \rho(\sigma_1) &= (-1)^{A_+} \\ \rho(\sigma_2) &= (-1)^{F_+} = (-1)^F \end{aligned}$$

et la relation  $\sigma_0 \sigma_1 \sigma_2 = \text{id.}$  entraîne  $(-1)^X = 1$ .

En fait  $\chi$  est non seulement pair mais inférieur ou égal à 2 comme l'argument suivant (datant au moins de Poincaré) l'indique. Notons  $n_i$ ,  $i = 0, 1, 2$ , l'ordre de  $\sigma_i$ . Alors  $n_1 = 2$  et  $n_0 (n_2)$  est le plus petit commun multiple des valences des sommets (des faces). Considérons l'espace vectoriel  $V$  des 1-formes harmoniques, c'est-à-dire des fonctions  $\varphi$  définies sur les brins (à valeurs réelles) telles que pour  $i = 0, 1, 2$ , et tout brin  $x$

$$\sum_{0 \leq k \leq n_i - 1} \varphi(\sigma_i^k x) = 0$$

Evidemment  $\dim V \leq A$ . Les  $S$  ( $F$ ) relations pour  $i = 0$  ( $i = 2$ ) satisfont une unique relation en raison de la connexité, de sorte que

$$\dim_{\mathbb{R}} V = A - (S - 1) - (F - 1) = 2 - \chi = 2g \geq 0$$

ce qui prouve l'assertion et définit le genre  $g \geq 0$ .

Les inégalités

$$2A \leq n_0 S \quad 2A \leq n_2 F$$

entraînent

$$\chi \geq 2A \left( \frac{1}{n_0} + \frac{1}{2} + \frac{1}{n_2} - 1 \right)$$

Ainsi

- (i) si  $\frac{1}{n_0} + \frac{1}{2} + \frac{1}{n_2} > 1$  le genre est nul  
(ii) si  $\frac{1}{n_0} + \frac{1}{2} + \frac{1}{n_2} = 1$  le genre est 0 ou 1

Lorsque les inégalités précédentes sont des égalités on dira que la carte est *semi-régulière* (tous les sommets et toutes les faces ont même valence). Il est clair qu'une carte régulière (cas où le stabilisateur d'un brin est réduit à l'identité) est semi-régulière mais la réciproque n'est pas toujours vraie.

Le groupe  $G$  défini ci-dessus s'identifie au groupe cartographique orienté de Grothendieck qui agit sur les drapeaux formés d'un sommet d'une arête incidente et d'une face bordant l'arête, muni d'une relation d'orientation. On définit trois involutions renversant l'orientation échangeant un élément (sommet, arête ou face) de chaque drapeau. Les produits par paires engendrent le groupe cartographique orienté. Cependant ces définitions doivent être modifiées si une arête est incidente sur le même sommet à ses deux extrémités, s'il existe des sommets de valence un, ou enfin si une arête n'est incidente que sur une seule face, inconvénient que ne possède pas la définition précédente.

Le groupe cartographique  $G$  ne doit pas être confondu avec le groupe de symétrie  $H$  de la carte. Ce dernier est défini comme le centralisateur de  $G$  dans  $\Sigma_{2A}$ , c'est-à-dire l'ensemble des permutations des  $2A$  brins qui commutent avec l'action de  $G$ .

*Proposition 1.* L'ordre du groupe de symétrie  $H$  divise  $2A$  et est isomorphe (mais non identique) au groupe cartographique si et seulement si la carte est régulière.

Soit  $x$  un brin générique et faisons agir  $G$  et  $H$  respectivement à gauche et à droite de telle sorte que la commutativité s'écrive

$$(gx)h = g(xh) \quad g \in G, \quad h \in H$$

La transitivité de  $G$  entraîne que les orbites de  $H$  ont toutes le même nombre d'éléments égal à l'ordre de  $H$  de sorte que

$$2A = |H| \times \#(\text{orbites})$$

Si la carte est régulière, l'ensemble des brins s'identifie au groupe cartographique (en tant qu'ensemble) par son action à gauche qui commute avec l'action de  $G$  à droite donc  $H$  contient un groupe isomorphe à  $G$ , et d'après ce qui précède,  $H$  est isomorphe à  $G$ . Finalement si  $H$  est isomorphe à  $G$  son ordre est à la fois un diviseur et un multiple de  $2A$ , donc  $|H| = |G| = 2A$  ce qui n'est possible pour une action transitive de  $G$  que si  $G$  agit sans point fixe et la carte est régulière.

En genre zéro les cartes régulières (ou même semi-régulières) correspondent aux solides platoniciens. L'inégalité  $\frac{1}{n_0} + \frac{1}{n_2} > \frac{1}{2}$  se réécrit  $(n_0 - 2)(n_2 - 2) < 4$  ce qui donne lieu à la table

$$G \sim H$$

$$(a) \left. \begin{array}{l} n_1 = 2 \quad n_2 = n \geq 2 \quad S = A = n \quad F = 2 \\ n_0 = n \quad n_2 = 2 \quad A = F = n \quad S = 2 \end{array} \right\} \text{groupe diédral d'ordre } 2n, D_n$$

$$(b) \quad n_0 = n_2 = 3 \quad S = F = 4 \quad A = 6 \quad \text{groupe tétraédral } A_4 \text{ d'ordre } 12$$

$$(c) \left. \begin{array}{l} n_0 = 4 \quad n_2 = 3 \quad S = 6 \quad A = 12 \quad F = 8 \\ n_0 = 3 \quad n_2 = 4 \quad S = 8 \quad A = 12 \quad F = 6 \end{array} \right\} \text{groupe octaédral } S_4 \text{ d'ordre } 24$$

$$(d) \left. \begin{array}{l} n_0 = 5 \quad n_2 = 3 \quad S = 12 \quad A = 30 \quad F = 20 \\ n_0 = 3 \quad n_2 = 5 \quad S = 20 \quad A = 30 \quad F = 12 \end{array} \right\} \text{groupe icosaédral } A_5 \text{ d'ordre } 60$$

Dans les cas (b), (c), (d) le groupe  $G$  admet un système de deux générateurs l'un d'ordre 2 l'autre d'ordre 3 =  $\inf(n_0, n_2)$ .

En genre 1 l'égalité  $(n_0 - 2)(n_2 - 2) = 4$  correspond aux quotients des réseaux réguliers

$$(a) \left. \begin{array}{l} n_0 = 3 \quad n_2 = 6 \quad \text{hexagonal} \\ n_0 = 6 \quad n_2 = 3 \quad \text{triangulaire} \end{array} \right\}$$

$$(b) \quad n_0 = n_2 = 4 \quad \text{carré}$$

Les cas les plus intéressants sont relatifs à un genre  $g$  supérieur à 1. Pour une carte régulière

$$g - 1 = A \left( \frac{1}{2} - \frac{1}{n_0} - \frac{1}{n_2} \right)$$

Nous retrouvons l'inégalité de Hurwitz en demandant que le groupe de symétrie  $H$  soit d'ordre  $2A$  aussi grand que possible, c'est-à-dire à  $g$  fixé en minimisant la quantité positive  $\frac{1}{2} - \frac{1}{n_0} - \frac{1}{n_2}$  ou encore  $n_0$  et  $n_2$ , chacun d'eux devant être supérieur ou égal à 3 (pour que  $g > 1$ ). Les valeurs (3,3), (3,4), (3,5) et (3,6) correspondant à  $g \leq 1$ , on trouve que (3,7) est l'extremum cherché (correspondant soit à  $n_0 = 3, n_2 = 7$  soit à la carte duale  $n_0 = 7, n_2 = 3$ ). Dans ces conditions  $|G| = 2A$  et l'on en tire

*Proposition 2.* Pour  $g$  supérieur à 1, l'ordre du groupe de symétrie d'une carte régulière est inférieur ou égal à  $84(g - 1)$ .

Quand cette borne est atteinte on parle de carte régulière de Hurwitz et de groupe (cartographique ou de symétrie) de Hurwitz engendré par trois générateurs de produit unité et d'ordre 2,3,7 respectivement.

Pour une carte de Hurwitz on a  $S$ (ou  $F$ ) =  $28(g - 1)$ ,  $A = 48(g - 1)$ ,  $F$ (ou  $S$ ) =  $12(g - 1)$ . On sait que cette borne n'est pas toujours atteinte. Par exemple en genre 2 l'ordre du plus grand groupe de symétrie est 48 (il s'agit du produit direct  $\mathbb{Z}/2\mathbb{Z} \times S_4^*$ ). En revanche en genre 3 on a le célèbre groupe de Hurwitz  $PSL_2(F_7) \sim L_3(F_2)$  d'ordre 168 (pour une revue des groupes de Hurwitz voir M. Conder).

En revenant au cas d'une carte arbitraire soit  $S_v$  ( $F_v$ ) le nombre de sommets (de faces) de valence  $v$ . Dans des modèles de matrices chaque carte est comptée avec un poids de la forme  $\frac{1}{|H|}$  où l'ordre du groupe symétrie apparaît sous la forme

$$|H| = \prod_v \frac{v^{S_v} S_v!}{\nu_S}$$

\* Correspondant à une carte formée de 16 triangles se rencontrant par 8 en 6 sommets (avec 24 arêtes) ou par dualité de 6 octogones se rencontrant par triplets en 16 sommets, double recouvrement de la sphère ramifié aux sommets d'un octaèdre.

expression dans laquelle l'entier positif  $\nu_S$  est défini de la manière suivante. Ayant indexé tous les brins par  $2A$  symboles, on compte le nombre  $\nu_S$  de façons distinctes de les joindre de manière à produire la carte donnée (sans indexation). En d'autres termes  $\nu_S$  est le nombre d'involutions  $\sigma_1 \in \Sigma_{2A}$  telles que,  $\sigma_0$  étant donné, ces deux permutations engendrent des groupes  $G$  isomorphes mais distincts. Deux tels choix  $\sigma_1$  et  $\sigma'_1$  ayant même décomposition cyclique ( $2^A$ ) sont conjugués dans  $\Sigma_{2A}$ . Il existe donc une permutation  $k$  commutant à  $\sigma_0$  telle que  $\sigma'_1 = k^{-1}\sigma_1 k$ . Si  $\text{Com}(\sigma_0)$  désigne le commutant de  $\sigma_0$  dans  $\Sigma_{2A}$  et  $\text{Com}(\sigma_0, \sigma_1)$  - isomorphe à  $H$  - le sous groupe de ces éléments qui commutent aussi avec  $\sigma_1$ , on a

$$\nu_S = \frac{|\text{Com}(\sigma_0)|}{|\text{Com}(\sigma_0, \sigma_1)|}$$

La classe de  $\sigma_0$  étant  $\prod_v (v)^{S_v}$  l'ordre de son commutant est

$$|\text{Com}(\sigma_0)| = \prod_v v^{S_v} S_v !$$

tandis que  $|\text{Com}(\sigma_0, \sigma_1)| = |H|$  ce qui justifie l'expression ci-dessus. Bien entendu on a pour une définition adéquate la formule duale

$$|H| = \prod_v \frac{v^{F_v} F_v}{\nu_F}$$

Le groupe de symétrie  $H$  agit linéairement sur l'espace vectoriel  $V$  des 1-formes harmoniques par

$$\varphi \longrightarrow \varphi^h : \quad \varphi^h(x) = \varphi(xh)$$

où l'on vérifie sans peine que  $\varphi^h$  est encore harmonique. Il s'ensuit que  $V$  est un  $H$ -module (en général réductible). Dans le cas, probablement très spécial, où en tensorisant par  $\mathbb{C}$ ,  $V$  se décomposerait en deux représentations irréductibles conjuguées de  $H$ , on en concluerait\* que  $g||H|$ . C'est ce qui se produit par exemple pour la carte de Hurwitz de  $PSL_2(F_7)$ , mais  $g$  étant premier avec  $g-1$ , ceci ne peut avoir lieu pour d'autres cartes de Hurwitz que si  $g$  est un diviseur de  $84$  ce qui majorerait l'ordre du groupe de symétrie correspondant par  $84 \times 83 = 6.972$ .

Il existe une description intrinsèque du groupe de symétrie  $H$  d'une carte. Marquons un brin  $x$ , soit  $B_x \subset G$  son groupe d'isotropie dans le groupe cartographique, et considérons le normalisateur  $\text{Norm}(B_x) \subset G$ , c'est-à-dire le sous groupe des  $g \in G$  tels que  $g B_x g^{-1} = B_x$ . Il est clair que  $B_x$  est un sous groupe invariant de  $\text{Norm}(B_x)$ .

**Proposition 3.** Le groupe de symétrie  $H$  est isomorphe à

$$\text{Norm}(B_x)/B_x$$

Si la carte est régulière  $B = \{\text{id}\}$ ,  $\text{Norm}(B) = G$  et nous retrouvons l'isomorphisme  $H \sim G$ .

La preuve se fait en trois étapes:

(i) Si  $x$  et  $y = xh$  sont des brins de la même orbite du groupe de symétrie, alors  $B_x = B_y$ . En effet  $g \in B_x$  implique que  $g(xh) = (gx)h = xh$ , donc  $B_x \subset B_y$  et de même  $B_y \subset B_x$ .

(ii)  $H$  privé de l'identité agit sans point fixe sur les brins comme conséquence de la transitivité de  $G$  (voir plus haut).

(iii) Soient deux brins  $x$  et  $y$  tels que  $B_x = B_y = B$ . Par l'hypothèse de transitivité, il existe  $\gamma \in G$  tel que  $y = \gamma x$  et  $\gamma B \gamma^{-1} = B$  donc  $\gamma \in \text{Norm}(B)$ . Fixant  $x$  et  $\gamma$ , pour un brin générique  $z$ , il existe  $g \in G$  tel que  $z = gx$ .

L'application  $h$  des brins dans les brins

$$h : \quad z \longrightarrow zh = g\gamma x$$

\* La dimension d'une représentation irréductible (sur  $\mathbb{C}$ ) divise l'ordre d'un groupe fini (cf. Serre).

est bien définie en vertu de la propriété de  $\gamma$ . Pour tout  $g' \in G$

$$(g'z)h = (g'g)\gamma x = g'(zh)$$

En identifiant l'ensemble des brins avec le quotient  $G/B$  il s'ensuit que  $(gB)h = gB\gamma = g\gamma B$  ce qui donne l'application  $h : gB \longrightarrow g\gamma B$  telle que

$$g' \circ h = h \circ g' : \quad gB \longrightarrow g'g\gamma B$$

Nous avons ainsi un homomorphisme  $\text{Norm}(B) \longrightarrow H$  de noyau  $B$ . Cet homomorphisme est surjectif puisque étant donné  $h \in H$  on peut trouver  $\gamma \in \text{Norm}(B)$  tel que  $y = xh = \gamma x$  ce qui complète la preuve.

On dira qu'une carte est un recouvrement d'une autre si les conditions suivantes sont satisfaites. Soit  $\hat{G}(\hat{\sigma}_0, \hat{\sigma}_1, \hat{\sigma}_2)$  le groupe cartographique de la première carte agissant sur un ensemble de  $2A$  brins  $\hat{B}$  et  $G(\sigma_0, \sigma_1, \sigma_2)$ ,  $B$  les quantités analogues pour la seconde. On demande qu'il existe une application surjective

$$f : \quad \hat{B} \longrightarrow B$$

telle que

$$f(\hat{\sigma}_i \hat{x}) = \sigma_i f(\hat{x})$$

Comme on l'a remarqué plus haut, un élément de  $G$  qui agit trivialement sur tous les brins est forcément l'identité. Comme  $f$  est surjective, la définition d'un recouvrement impose que toute relation entre  $\hat{\sigma}_0, \hat{\sigma}_1, \hat{\sigma}_2$  dans  $\hat{G}$  est vraie pour  $\sigma_0, \sigma_1, \sigma_2$  dans  $G$ , ce qui signifie que  $G$  est un quotient de  $\hat{G}$ . On peut représenter  $\hat{B}$  comme  $\hat{G}/\hat{B}$  et  $B$  comme  $G/B$ . On peut alors décrire plus explicitement les recouvrements. Partant de  $\hat{G}$  un groupe cartographique,  $G$  un groupe quotient de  $\hat{G}$  (où l'on note  $p$  la projection  $\hat{G} \xrightarrow{p} G \longrightarrow 1$ ) tel que  $p(\hat{\sigma}_1) \neq e$ , et  $B$  un sous groupe de  $G$  tel que  $B = G/B$  soit une carte de groupe cartographique  $G$ , les recouvrements de  $B$  de groupe cartographique  $\hat{G}$  sont indexés par les sous groupes de  $p^{-1}(B)$ . Notant  $\hat{B}$  un tel sous groupe,  $\hat{B} = \hat{G}/\hat{B}$  recouvre  $B$ . La preuve est élémentaire. On prouve d'abord que tous les sous groupes de  $p^{-1}(B)$  ont les propriétés voulues pour que  $\hat{G}/\hat{B}$  soit bien une carte de groupe cartographique  $\hat{G}$ . On montre ensuite que le diagramme

$$\begin{array}{ccc} \hat{G} & \xrightarrow{p} & G \\ \downarrow & & \downarrow \\ \hat{G}/\hat{B} & & G/B \end{array}$$

se complète naturellement en un diagramme commutatif

$$\begin{array}{ccc} \hat{G} & \xrightarrow{p} & G \\ \downarrow & & \downarrow \\ \hat{G}/\hat{B} & \xrightarrow{f} & G/B \end{array}$$

où  $f$  a les propriétés d'un recouvrement.

Un cas particulier est le suivant. On considère une carte et son groupe cartographique  $G(\sigma_0, \sigma_1, \sigma_2)$ , on prend pour  $\hat{B}$  le groupe  $G$  lui-même en tant qu'ensemble. Alors  $G$  agit sur  $\hat{B}$  par multiplication à gauche. On prend  $\hat{\sigma}_i = \sigma_i$  qui est une involution sans point fixe sur  $\hat{B}$ . On choisit un brin  $x$  de la carte initiale et on définit l'application  $\hat{B} \longrightarrow B$  par  $(g \in \hat{B}) \longrightarrow (gx \in B)$ . Toutes les fibres ont pour cardinal  $|B_x|$  et on vérifie que les propriétés de recouvrement sont satisfaites, ainsi

**Proposition 4.** Toute carte possède un recouvrement par une carte régulière admettant comme groupe de symétrie le groupe cartographique de la carte initiale.

En raison de la symétrie de la carte régulière, cette construction ne dépend pas essentiellement du choix du brin  $x$  dans la carte initiale. Si on conserve la notation  $n_0, n_2$  pour les plus petits communs multiples des valences des sommets et des faces de la carte initiale et si on pose  $n = |B_x|$  de sorte que  $|G| = 2An$ , la carte régulière qui la recouvre a pour caractéristique d'Euler

$$\chi' = 2An \left( \frac{1}{n_0} - \frac{1}{2} + \frac{1}{n_2} \right) \leq n \chi$$

donc un genre  $g'$  tel que

$$g' \geq 1 + n(g - 1)$$

inégalité intéressante si  $g > 1$ . Il va sans dire que  $n_0$  et  $n_2$ , les ordres de  $\sigma_0$  et  $\sigma_2$ , divisent  $|G| = 2An$ .

Les groupes cartographiques (finis), c'est-à-dire ceux qui admettent une présentation en termes de deux générateurs dont l'un est une involution, sont très nombreux. Nous n'avons pas fait une étude exhaustive de cette question (qui le mériterait). Mentionnons à titre d'exemples les quotients finis du groupe modulaire  $PSL_2(\mathbb{Z})$  et les groupes symétriques  $\Sigma_n$ . Les premiers parce que le groupe modulaire admet une présentation en termes de deux générateurs dont l'un est une involution, l'autre d'ordre trois, les seconds parce qu'ils sont engendrés par un cycle  $\sigma_0 = (1, 2, \dots, n)$  d'ordre  $n$  et une transposition  $\sigma_1 = (1, 2)$  tandis que  $\sigma_2 = (\sigma_0 \sigma_1)^{-1} = (2)(n, n-1, \dots, 3, \hat{2}, 1)$  est d'ordre  $(n-1)$ . La carte régulière correspondante est telle que  $S = \frac{n!}{n}$ ,  $A = \frac{n!}{2}$ ,  $F = \frac{n!}{n-1}$  (avec  $F$  échangé avec  $S$  pour la carte duale) et son genre est

$$g = 1 + \frac{(n-2)!}{4} [n^2 - 5n + 2]$$

qui vaut 0 pour  $n \leq 4^*$ , tandis que pour  $n > 4$  le genre croît très rapidement.

Un autre exemple intéressant est fourni pour  $p$  premier supérieur à 3 par le groupe affine modulo  $p$  agissant sur la droite affine  $L_p$  identifiée avec le corps  $F_p$ , correspondant aux transformations

$$u \longrightarrow au + b, \quad a \in F_p^*, \quad u, b \in F_p$$

où  $F_p^*$  est le groupe multiplicatif cyclique de  $F_p$  de générateur  $\eta$  (c'est-à-dire que  $p-1$  est la plus petite puissance telle que  $\eta^{p-1} = 1 \pmod{p}$ ). On peut prendre comme générateurs

$$\sigma_0 \quad u \longrightarrow \eta u \quad \sigma_0^{p-1} = 1$$

$$\sigma_1 \quad u \longrightarrow -u - 1 \quad \sigma_1^2 = 1$$

d'où

$$\sigma_2 = -\eta^{-1}u - 1 \quad \begin{array}{ll} p \equiv 1 \pmod{4} & \sigma_2^{p-1} = 1 \\ p \equiv -1 \pmod{4} & \sigma_2^{\frac{p-1}{2}} = 1 \end{array}$$

Une carte régulière associée aura  $S = p$ ,  $A = \frac{p(p-1)}{2}$  et suivant que  $p \equiv 1(4)$ ,  $F = p$  (il s'agit de  $p-1$ -gones) ou  $p \equiv -1(4)$ ,  $F = 2p$  (qui sont des  $\frac{p-1}{2}$ -gones).

Le genre est alors donné par

$$g - 1 = \begin{cases} \frac{p(p-5)}{4} & \text{si } p \equiv 1(4) \\ \frac{p(p-7)}{4} & \text{si } p \equiv -1(4) \end{cases}$$

Comme il y a  $p$  sommets et  $\frac{p(p-1)}{2}$  arêtes, la carte correspond au graphe complet sur  $p$  points complété par les faces (on vérifie que chaque arête est incidente sur deux sommets distincts sinon

\* Les cas  $n = 2$  et  $3$  correspondent respectivement au segment et au triangle, et sont identifiables aux cas diédraux  $D_2$  et  $D_6$ .

il existerait un entier  $k$  tel que  $\sigma_1 = \sigma_0^k$ , ce qui est impossible). On en déduit que le graphe complet à  $p$  sommets ( $p$  premier supérieur à 3) peut être tracé sans intersections sur une surface compacte orientable de genre  $g$  donné par la formule précédente. Ceci est à comparer avec le problème classique de coloriage des cartes (ou son dual) selon lequel (Ringel (1974)) en genre  $g > 0$  pour colorier toute carte de sorte que des faces adjacentes portent des couleurs distinctes, il suffit de  $n$  couleurs où l'entier  $n$ , nombre chromatique, est la partie entière de

$$\frac{7 + \sqrt{1 + 48g}}{2}$$

Cette partie entière est en tous cas une borne supérieure. De manière équivalente, le graphe complet à  $n$  sommets peut être tracé sur une surface (orientable) de genre  $g \geq \frac{(n-3)(n-4)}{12}$  (inégalité de Heawood). En effet, les faces étant au moins triangulaires  $2A = n(n-1) \geq 3F$  de sorte que la formule d'Euler entraîne  $2g - 2 = \frac{n(n-1)}{2} - n - F \geq \frac{n(n-1)}{6} - n$ , qui est l'inégalité précédente. Le théorème de coloriage en genre positif est alors que l'inégalité peut être saturée, en ce sens qu'on peut trouver  $g = \gamma(n) = \text{Inf} \left\{ r \in \mathbb{Z}, r \geq \frac{(n-3)(n-4)}{12} \right\}$ .

En genre 1 le nombre chromatique est 7, ce qui s'identifie au cas précédent quand  $p = 7$ . Montrons comment pour  $p = 5, 7$  la construction précédente se présente en termes d'une courbe elliptique arithmétique.

Soit d'abord  $p = 5 \equiv 1(4)$ . Pour tracer sur un tore le graphe complet (auto-dual) ayant 5 sommets, 10 arêtes et 5 faces carrées, nous considérons les sommets du réseau carré bi-dimensionnel comme l'ensemble des entiers de Gauss  $\mathbb{Z}(\sqrt{-1})$ . L'idéal premier engendré par

$$\tau = 2 + \sqrt{-1}$$

de norme 5 ( $\tau^2 - 4\tau + 5 = 0$ ) correspond à un sous réseau et le quotient  $\mathbb{Z}(\sqrt{-1})/\tau\mathbb{Z}(\sqrt{-1})$  (qui s'identifie au corps  $F_5$ ) contient 5 sommets et 5 carrés du pavage initial. Si nous identifions les arêtes avec celles du réseau initial, chaque sommet (chaque face) est joint au quatre autres comme l'indique la Figure 2a. Nous avons ainsi le graphe complet dessiné sur la courbe elliptique d'invariant modulaire  $j(\tau/5) = j(\sqrt{-1}) = 12^3$ . De plus le groupe de symétrie de  $\mathbb{Z}(\sqrt{-1})$  engendré par les translations et rotations multiples d'un quart de tour devient un groupe de symétrie de la configuration  $(\sqrt{-1} \tau = 2\tau - 5, \sqrt{-1} 5 = 5\tau - 10)$  et son action est celle du groupe affine sur la droite sur  $F_5$ . Si on représente les brins par une paire  $(x \in \mathbb{Z}(\sqrt{-1}) \pmod{\tau}, (\sqrt{-1})^a, a \pmod{4})$  deux générateurs possibles sont

$$\begin{aligned} \sigma_0(x, \sqrt{-1}^a) &= (x, \sqrt{-1}^{a+1}) \\ \sigma_1(x, \sqrt{-1}^a) &= (x + \sqrt{-1}^a, \sqrt{-1}^{a+2}) \end{aligned}$$

On vérifie les relations

$$\sigma_0^4 = \sigma_1^2 = (\sigma_0 \sigma_1)^4 = (\sigma_0^2 \sigma_1)^5 = \sigma_1 \sigma_0^2 \sigma_1 \sigma_0^3 \sigma_1 \sigma_0 = 1$$

impliquant que  $\sigma_2^4 = 1$  (comme il se doit) et que  $\sigma_0^2 \sigma_1$  engendre un sous groupe cyclique invariant d'ordre 5

$$\begin{aligned} \sigma_1^{-1}(\sigma_0^2 \sigma_1) \sigma_1 &= (\sigma_0^2 \sigma_1)^4 \\ \sigma_0^{-1}(\sigma_0^2 \sigma_1) \sigma_0 &= (\sigma_0^2 \sigma_1)^2 \end{aligned}$$

Tout élément du groupe s'écrit alors

$$g_{\alpha\beta} = (\sigma_0^2 \sigma_1)^\alpha \sigma_0^\beta \quad \alpha \pmod{5}, \quad \beta \pmod{4}$$

avec la loi de multiplication

$$g_{\alpha_1 \beta_1} g_{\alpha_2 \beta_2} = g_{\alpha_1 + 3\beta_1 \alpha_2, \beta_1 + \beta_2},$$

qui est bien celle du groupe affine puisque 3 est un générateur de  $F_5^*$ .

Dans le cas  $p = 7, g = 1$  on peut reprendre l'exercice utilisant l'identification des sommets du réseau triangulaire avec les entiers de Eisenstein  $Z(\omega), \omega = \exp 2\sqrt{-1}\frac{\pi}{6}$  de la forme  $m + n\omega$  de norme  $m^2 + n^2 + mn$ . L'idéal premier est engendré par

$$\tau = 2 + \omega$$

de norme 7 ( $\tau^2 - 5\tau + 7 = 0$ ).

Le réseau triangulaire modulo l'idéal engendré par  $\tau$  contient 7 sommets, 21 arêtes et 14 faces triangulaires correspondant au graphe complet sur 7 points (Figure 2b). Comme précédemment les brins sont des paires ( $x \in Z(\omega) \bmod \tau, \omega^a, a \bmod 6$ ) et l'action du groupe de symétrie du réseau est engendrée par

$$\begin{aligned}\sigma_0(x, \omega^a) &= (x, \omega^{a+1}) \\ \sigma_1(x, \omega^a) &= (x + \omega^a, \omega^{a+3})\end{aligned}$$

On vérifie que

$$\sigma_0^6 = \sigma_1^2 = (\sigma_0\sigma_1)^3 = (\sigma_0^3\sigma_1)^7 = 1$$

Comme

$$\begin{aligned}\sigma_1^{-1}(\sigma_0^3\sigma_1)\sigma_1 &= (\sigma_0^3\sigma_1)^6 \\ \sigma_0^{-1}(\sigma_0^3\sigma_1)\sigma_0 &= (\sigma_0^3\sigma_1)^5\end{aligned}$$

l'élément  $\sigma_0^3\sigma_1$  engendre un sous groupe cyclique invariant d'ordre 7. Un élément générique du groupe est représenté sous la forme

$$g_{\alpha, \beta} = (\sigma_0^3\sigma_1)^\alpha \sigma_0^\beta, \quad \alpha \bmod 7, \quad \beta \bmod 6$$

avec

$$g_{\alpha_1, \beta_1} g_{\alpha_2, \beta_2} = g_{\alpha_1 + 3\beta_1 \alpha_2, \beta_1 + \beta_2}$$

qui est le groupe affine sur  $F_7$ , 3 étant aussi dans ce cas un générateur de  $F_7^*$ . La courbe elliptique correspondante a pour invariant modulaire  $j(\frac{\tau}{7}) = j(\omega) = 0$ .

La décomposition barycentrique d'une carte conduit à une triangulation dont les sommets correspondent aux sommets, milieux d'arêtes et milieux des faces. Pour cette triangulation les nombres de sommets, d'arêtes et de faces triangulaires deviennent

$$\begin{aligned}S' &= S + A + F \\ A' &= 6A \\ F' &= \Sigma 2vF_v = 4A\end{aligned}$$

et le genre est invariant. Nous l'appellerons carte (ou triangulation) dérivée. Soit  $G'$  son groupe cartographique. Les sommets de la triangulation peuvent être classés en trois familles du type  $S, A$  ou  $F$ . En identifiant les sommets de chaque classe on obtient la carte régulière à 3 sommets, 3 arêtes et 2 faces (triangulation élémentaire d'une sphère) de groupe cartographique et de symétrie  $\Sigma_3$ . Ceci engendre un homomorphisme surjectif  $G' \rightarrow \Sigma_3 \rightarrow 1$  de noyau  $\Gamma$  (et correspond à la présentation de Belyi). On se convainc que  $\Gamma$  est engendré par les éléments  $\tilde{\sigma}_0 = \sigma_0'^2$  et  $\tilde{\sigma}_1 = \sigma_1'\sigma_0'^2\sigma_1'$ . Ces derniers engendrent bien un sous groupe invariant  $\Gamma$  dans  $G'$  puisque

$$\begin{aligned}\sigma_0'^{-1}\tilde{\sigma}_0\sigma_0' &= \tilde{\sigma}_0 \\ \sigma_1'^{-1}\tilde{\sigma}_0\sigma_1' &= \tilde{\sigma}_1 \\ \sigma_0'^{-1}\tilde{\sigma}_1\sigma_0' &= \tilde{\sigma}_0^{-1}\tilde{\sigma}_1^{-1} \\ \sigma_1'^{-1}\tilde{\sigma}_1\sigma_1' &= \tilde{\sigma}_0\end{aligned}$$

où on a utilisé la relation  $(\sigma_0'\sigma_1')^3 = 1$  de la triangulation, et les images  $t_0, t_1$  de  $\sigma_0', \sigma_1'$  dans l'application  $G' \rightarrow G'/\Gamma$  vérifient

$$t_0^2 = t_1^2 = (t_0t_1)^3 = 1$$

qui sont les relations génératrices de  $\Sigma_3$  (en tant que groupe de Weyl de l'algèbre de Lie  $\mathfrak{sl}_3$ ). Enfin, on s'assure que ni  $t_0$  ni  $t_1$  ne sont identiquement l'identité.

Les brins de la carte originale forment une sous-famille de ceux de la triangulation, stable pour l'action de  $\tilde{\sigma}_0$  et  $\tilde{\sigma}_1$ , action qui devient celle respectivement de  $\sigma_0$  et  $\sigma_1$ . On en déduit la suite exacte d'homomorphismes

$$\begin{array}{ccccccc} 1 & \longrightarrow & \Gamma & \longrightarrow & G' & \longrightarrow & \Sigma_3 \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \\ & & G & & \downarrow & & \\ & & & & 1 & & \end{array}$$

En général  $\Gamma$  n'est pas isomorphe à  $G$  comme le montre l'exemple de genre zéro à 2 sommets, 1 arête et 1 face pour lequel  $|G \sim Z/2Z| = 2$ , tandis que la carte dérivée, qui n'est pas régulière, possède 4 sommets, 6 arêtes et 4 faces et un groupe cartographique à 24 éléments, cependant que  $|\Gamma \sim Z/2Z \times Z/2Z| = 4$ . Cette carte dérivée s'obtient à partir de la carte tétraédrale de même nombre de sommets, arêtes et faces, en procédant à la transformation dite "flip" (correspondant à l'échange de diagonales dans un quadrilatère) affectant deux faces du tétraèdre. On passe ainsi d'un groupe cartographique d'ordre 12 ( $A_4$ ) à  $G'$  d'ordre 24 (qui à la différence de  $A_4$  possède un élément d'ordre 4).

Les triangulations dérivées d'une carte ne sont pas les plus générales parmi celles où il est possible de partager les sommets en trois classes, les sommets d'un triangle appartenant à chacune d'entre elles. C'est cette classe plus générale qui intervient dans le théorème de Belyi. Cependant une telle carte admettra une triangulation dérivée barycentrique.

## 2. STRUCTURE COMPLEXE

Aux données combinatoires d'une carte on associe une surface de Riemann compacte. Il s'agit d'un recouvrement fini de la sphère de Riemann qui n'est ramifié qu'aux images inverses de 0, 1,  $\infty$  (correspondant respectivement aux sommets, "milieux" d'arêtes et "milieux" de faces).

Ayant fait choix d'un point base arbitraire (hors de ces trois points), les générateurs  $c_0, c_1, c_\infty$  du groupe fondamental  $\pi_1(CP_1 - \{0, 1, \infty\})$  correspondant à des circuits élémentaires autour de 0, 1,  $\infty$  et satisfaisant à la relation

$$c_0c_1c_\infty = \text{id.}$$

agissent sur les fibres de recouvrement comme  $\sigma_0, \sigma_1, \sigma_2$  respectivement sur les brins de la carte. Notons  $\pi_1$  pour faire bref, le groupe fondamental ci-dessus. On a donc un homomorphisme surjectif

$$\pi_1 \longrightarrow G \longrightarrow 1$$

dont le noyau est engendré par  $c_0^{n_0}, c_1^{n_1}, c_\infty^{n_2}$  et les autres relations satisfaites par les  $\sigma_i$ .

La droite projective réelle coupe la sphère marquée en 0, 1,  $\infty$  en deux triangles. Notons  $\Sigma$  le recouvrement ramifié défini ci-dessus et  $\beta$  la projection sur la sphère de Riemann. L'image inverse par  $\beta$  de la triangulation de la sphère devient la triangulation dérivée de la carte. En particulier, les arêtes initiales s'identifient à  $\beta^{-1}[0, 1]$  tandis que  $\beta^{-1}[1, \infty]$  dessine sur  $\Sigma$  la carte duale. De même  $\beta^{-1}$  permet de relever la structure complexe qui transforme  $\Sigma$  en une surface de Riemann compacte, revêtement à  $2A$  feuillettes de la sphère de Riemann ramifiée en  $\beta^{-1}(0, 1, \infty)$ . La projection  $\beta$  définit, au moyen de la coordonnée  $x$  sur la sphère, un élément du corps rationnel sur  $\Sigma$  qui prend aux sommets, milieux d'arêtes et milieux de faces de la carte qu'on imagine tracée sur  $\Sigma$ , les valeurs 0, 1,  $\infty$  respectivement qui sont des valeurs critiques. En un sommet (milieu de face) de valence  $v$ , la fonction  $x$  s'exprime comme  $(t - t_s)^v \left( \frac{1}{(t-t_f)^v} \right)$  en fonction d'un paramètre uniformisant local, à une racine  $v$ -ième de l'unité près (si  $v = 1$ , il n'y a pas ramification). Dans cette construction il est clair que toute symétrie de la carte provient d'un automorphisme de la surface de Riemann laissant la fonction  $\beta$  invariante.

La surface  $\Sigma$  peut elle même être considérée comme la "surface de Riemann" d'une seconde fonction rationnelle  $y$  prenant une valeur donnée (par exemple  $\infty$ ) en  $2A$  points de  $\Sigma$  qui se

projettent en  $2A$  points distincts de  $CP_1 - \{0, 1, \infty\}$  (qu'on aura tout intérêt à prendre ou rationnels ou algébriques). Dans ces conditions  $y$ , bien que n'étant pas entièrement spécifié, satisfait une équation polynomiale de degré  $2A$  à coefficients polynomiaux en  $x$  définissant une carte algébrique. On note que au dessus du point 1 la fonction  $x$  possède  $A$  points de ramification d'ordre 2.

Donnons une description équivalente de la structure complexe de  $\Sigma$ . Choisissons par exemple un recouvrement simplement connexe de  $\Sigma$  moins  $\beta^{-1}\{0, 1, \infty\}$  par un plan hyperbolique  $\mathcal{H}$  en identifiant  $CP_1 - \{0, 1, \infty\}$  à  $\mathcal{H}/\Gamma(2)$  où  $\Gamma(2)$  est le sous groupe de niveau 2 du groupe modulaire (le groupe modulaire étant le quotient  $PSL_2(\mathbb{Z})$  et le sous groupe  $\Gamma(2) \subset PSL_2(\mathbb{Z})$ , étant formé des matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv I$  modulo 2, quotienté par son centre  $\pm I$ ). On représentera alors  $\Sigma - \beta^{-1}\{0, 1, \infty\}$  par le quotient  $\mathcal{H}/\Gamma$  où  $\Gamma$  est d'indice fini dans  $\Gamma(2)$  (précisément d'indice  $2A$ ). Soit  $x$  la fonction qui applique  $\mathcal{H}/\Gamma(2)$  sur  $CP_1 - \{0, 1, \infty\}$  normalisée en demandant qu'elle prenne les valeurs 0, 1,  $\infty$  aux trois points paraboliques. La projection  $\beta$  est alors donnée par  $M \in \mathcal{H}/\Gamma \rightarrow x(M)$ . Enfin l'action du groupe cartographique sur les  $2A$  brins s'identifiera à celle de  $\Gamma(2)$  sur  $\Gamma(2)/\Gamma$ . En d'autres termes, il existera des homomorphismes surjectifs  $\Gamma(2) \rightarrow G \rightarrow 1^*$ , tels que  $\Gamma(2)/\Gamma \sim G/B$ . En un sens, on peut alors considérer  $\Sigma$  comme une courbe modulaire.

On peut remplacer dans cette construction  $\Gamma(2)$  par un groupe triangulaire  $\Delta$  de signature  $n_0, n_1 = 2, n_2$  et un sous groupe  $\Gamma \subset \Delta$  d'indice fini ( $2A$ ) dans  $\Delta$ . Le quotient  $\mathcal{H}/\Gamma$  apparaît alors comme un modèle, en général singulier de  $\Sigma$ ,  $\Gamma$  n'étant pas nécessairement fuchsien (c'est-à-dire agissant avec des points fixes).

En se référant à la remarque qui clôt la section précédente, si on dispose en général d'une application  $\beta : \Sigma \rightarrow CP_1$ , ramifiée en 0, 1,  $\infty$ , on pourra toujours lui associer l'application composée  $\beta' = f \circ \beta$  en passant à la triangulation dérivée appliquant respectivement les sommets  $x = 0, 1, \infty$  sur  $f(x) = 0$ , les "milieux" d'arêtes  $x = -1, \frac{1}{2}, 2$  sur  $f(x) = 1$  et les "milieux" de faces  $x = \frac{1 \pm i\sqrt{3}}{2}$  sur  $f(x) = \infty$  soit en respectant les notations classiques de Klein

$$f(x) : 1 - f(x) : 1 = 27x^2(1-x)^2 : (2x^3 - 3x^2 - 3x + 2)^2 : 4(x^2 - x + 1)^3$$

En d'autres termes, on considère la variable  $x$  comme le birapport de 4 valeurs distinctes et  $f$  comme l'invariant sous l'action du groupe de Klein à 6 éléments, image des permutations:

$$SL_2(F_2) \sim PSL_2(\mathbb{Z})/\Gamma(2)$$

Bien entendu les ordres de ramification de  $\beta'$  au dessus de  $f(x) = 1$  sont tous égaux à deux.

### 3. STRUCTURE ARITHMETIQUE

C'est à ce point qu'un physicien commence à perdre pied. Le résultat le plus important - à la vérité pour l'instant le seul de ce domaine - est dû à Belyi comme indiqué dans l'introduction. Nous allons esquisser (une partie de) la démonstration pour son intérêt constructif dans un sens, en regrettant de ne pouvoir en dire autant dans l'autre sens. Reprenant les termes de l'auteur

**Théorème 1 (Belyi).** Une courbe algébrique régulière et complète sur un corps de caractéristique nulle est définie sur  $\bar{\mathbb{Q}}$  si et seulement si on peut la présenter comme revêtement de  $\mathbb{P}_1$  ramifié aux images inverses de 0, 1,  $\infty$ .

La restriction à 0, 1,  $\infty$  n'est pas essentielle puisque le groupe des automorphismes (algébriques) de  $\mathbb{P}_1$  est transitif sur les triplets de points. Soit donc une courbe  $X$  sur  $\bar{\mathbb{Q}}$  (dite alors arithmétique) et  $t$  un élément du corps rationnel sur la courbe dont  $U$  désigne l'ensemble fini des valeurs critiques (qui peuvent contenir le point à l'infini) de sorte que  $U$  (ou  $U \setminus \{\infty\}$ ) soit dans

\* Le noyau de cet homomorphisme est  $\Gamma'$ , le plus grand sous groupe invariant de  $\Gamma(2)$  d'indice fini contenu dans  $\Gamma$ . D'où  $G \sim \Gamma(2)/\Gamma'$ ,  $B \sim \Gamma/\Gamma'$ . Enfin le groupe d'automorphisme est le quotient du normalisateur de  $\Gamma$  dans  $\Gamma(2)$  par  $\Gamma$ . On notera au passage une conséquence du théorème de Nielsen-Schreier : tout sous groupe d'indice fini  $j$  du groupe  $\Gamma(2)$  (groupe libre à deux générateurs) est un groupe libre à  $j + 1$  générateurs.

$\bar{\mathbb{Q}}$ . Cette donnée permet de considérer  $X$  comme recouvrement de  $\mathbb{P}_1$  ramifié aux images inverses de  $U$ . Il s'agit maintenant de passer de cet ensemble à  $(0, 1, \infty)$ . Belyi procède en deux temps. Par une application polynomiale on passe de  $U$  à  $V$  tel que  $V$  (ou  $V \setminus \{\infty\}$ ) soit dans  $\bar{\mathbb{Q}}$  puis par une seconde application polynomiale de  $V$  à  $\{0, 1, \infty\}$ .

Soit  $h_1$  le polynôme minimal à coefficients rationnels qui s'annule sur  $U$  (ou  $U \setminus \{\infty\}$ ). L'application  $X \rightarrow h_1 \circ t$  est ramifiée aux images inverses de l'origine, des valeurs critiques du polynôme  $\{h_1(\xi) \mid h_1'(\xi) = 0\}$  et peut être de l'infini. Soit  $h_2$  un second polynôme minimal à coefficients rationnels qui s'annule aux valeurs critiques  $h_1(\xi) \in \bar{\mathbb{Q}}$ . On a  $\deg h_2 \leq \text{deg } h_1 - 1$  par un raisonnement classique. Les valeurs critiques de l'application  $h_2 \circ h_1 \circ t$  sont en  $\infty, 0$ , l'image de 0 par  $h_2$  (qui est rationnelle) et les valeurs critiques de  $h_2$  en nombre strictement inférieur à celles de  $h_1$ . Poursuivant de la sorte, en un nombre d'itérations inférieur ou égal à  $\text{deg}(h_1)$  on obtient un élément  $f \in \bar{\mathbb{Q}}(X)$ ,  $f = h_\ell \circ h_{\ell-1} \circ \dots \circ h_1 \circ t$  n'ayant que des valeurs critiques rationnelles et (peut être) l' $\infty$ . Soit  $V \subset Q$  cet ensemble fini de points. Dans un second temps, il s'agit de trouver un polynôme  $g$  (à coefficients rationnels) de valeurs critiques 0, 1,  $\infty$  et tel que  $g(V) \subset \{0, 1, \infty\}$ . Si l'on parvient à construire un tel polynôme  $g$ , l'application  $g \circ f$  donnera la présentation cherchée de  $X$  comme recouvrement de  $\mathbb{P}$ , non ramifié en dehors des images inverses de  $\{0, 1, \infty\}$ . Supposons qu'on dispose d'un polynôme  $g_1$ , ayant des propriétés analogues à  $g$  mais relativement à un sous ensemble  $V_1 \subset Q$  tel que  $V = V_1 \cup \{\xi\}$ . L'élément  $g_1 \circ f \in \bar{\mathbb{Q}}(X)$  aura comme valeurs de ramification finies  $(0, 1, g_1(\xi))$ . Si l'on peut trouver un polynôme à coefficients rationnels  $g_2$  admettant  $\{0, 1, \infty\}$  comme seules valeurs critiques et tel que l'image de 0, 1,  $s = g_1(\xi)$  appartienne à l'ensemble  $\{0, 1\}$ , le polynôme  $g$  cherché sera alors  $g = g_2 \circ g_1$ . Répétant autant de fois qu'il le faut cette construction on voit qu'on se ramène au cas où l'ensemble  $V$  est réduit à trois points que par un automorphisme de  $\mathbb{P}_1$ , on peut supposer de la forme 0, 1,  $s = \frac{m}{m+n}$ ,  $m, n$  entiers positifs et à la construction d'un polynôme à coefficients rationnels, dont la dérivée s'annule en 0 et 1 et qui envoie 0, 1 et  $s$  sur l'ensemble 0, 1. Un tel polynôme  $p$  est

$$p(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$$

En 0 ou 1 ce polynôme s'annule tandis qu'en  $s = \frac{m}{m+n}$  l'unique point distinct de 0, 1 ou sa dérivée s'annule, sa valeur est 1.

La réciproque, à savoir que si  $X$  est un recouvrement (fini)  $\mathbb{P}$ , non ramifié en dehors des images inverses de  $\{0, 1, \infty\}$ , alors  $X$  peut être défini sur  $\bar{\mathbb{Q}}$  est une propriété de rigidité qui repose sur un critère de Weil. On a vu ci-dessus que le théorème d'existence de Riemann définit  $X$  comme surface de Riemann compacte en fait comme une courbe algébrique (complète). Si  $\sigma$  est un automorphisme de  $\mathbb{C}$  laissant  $\bar{\mathbb{Q}}$  fixe, son action sur  $X$  définit un autre recouvrement de  $\mathbb{P}_1$  ramifié aux images inverses de 0, 1,  $\infty$  de même degré (de même nombre de feuillettes). Pour que  $X^\sigma$  soit une surface de Riemann compacte (connexe) il ne peut y avoir qu'un choix fini de  $\sigma$  tel que  $X^\sigma$  soit non isomorphe à  $X$  (il vient au même de dire que chaque tel recouvrement de degré  $n$  correspond à un sous groupe d'indice  $n$  dans  $\pi_1(CP_1 \setminus \{0, 1, \infty\})$  et qu'il n'y a qu'un nombre fini de tels sous groupes). En d'autres termes pour presque tous les  $\sigma$ ,  $X^\sigma \equiv X$ . Le critère de Weil revient alors à dire que dans cette situation  $X$  peut être défini sur une extension finie de  $\bar{\mathbb{Q}}$ .

Nous ne sommes pas sûrs de bien comprendre cette preuve. Mais en examinant des cas concrets (ou la donnée est l'action finie de  $\pi_1(CP_1 \setminus \{0, 1, \infty\})$  sur les feuillettes de recouvrements) et "solubles" (ce qui est rare) on se convainc qu'on est amené à résoudre des cascades d'équations à coefficients rationnels.

Donnons d'abord quelques exemples. Peut être le plus frappant est-il celui présenté par Oesterlé décrivant les conjugués d'un dessin d'enfant (au sens propre).

Sur une surface de genre zéro supposons qu'on dispose d'une application

$$\begin{aligned} \beta : y &\rightarrow x \\ \Sigma \sim \mathbb{P}_1 &\rightarrow \mathbb{P}_1 \end{aligned}$$

dont les points de ramification appartiennent à l'ensemble  $\beta^{-1}(0, 1, \infty)$ . Il s'agit de construire l'application rationnelle

$$x = \frac{P(y)}{Q(y)}$$

où  $P$  et  $Q$  sont premiers entre eux (sur  $\bar{\mathbb{Q}}$ ),  $y$  apparaissant comme un générateur du corps des fonctions rationnelles sur  $\Sigma$ . Quitte à substituer à  $y$  une transformée homographique, on peut supposer  $\deg P = \deg Q = n$ , degré du recouvrement, normaliser  $Q$  à la forme  $y^n + \dots$  et s'assurer que la valeur  $y = \infty$  correspond à un point régulier d'image rationnelle - par exemple  $-1$  - (et l'on pourra choisir  $\left(\frac{dx}{dy}\right)_{y^{-1}=0} = 1$ ) ce qui revient à écrire

$$\frac{P}{Q} = \frac{-y^n + ay^{n-1} + \dots}{y^n + by^{n-1} + \dots}, \quad a + b = 1.$$

De la sorte il reste  $2n - 1$  coefficients à déterminer. Puisque seules les préimages de  $0, 1, \infty$  sont des points de ramification, il s'ensuit que  $P'Q - Q'P = 0$  entraîne  $QP(Q - P) = 0$ , c'est-à-dire, comme  $Q, P$  et  $P - Q$  sont premiers entre eux, que l'on peut trouver trois entiers positifs  $\alpha_0, \alpha_1, \alpha_\infty$ , et un polynôme  $S$  tels que

$$P^{\alpha_0}(Q - P)^{\alpha_1}Q^{\alpha_\infty} = (P'Q - Q'P)S$$

D'ailleurs on pourra se limiter à  $\alpha_0 + \alpha_1 + \alpha_\infty \leq 2n - 1$ . En effet factorisons (sur  $\mathbb{C}$ )  $P'Q - Q'P$ , de degré inférieur ou égal à  $2n - 1$ , en produit de trois polynômes  $\rho_0\rho_1\rho_\infty$  tels que les racines de  $\rho_0$  (respectivement  $\rho_1, \rho_\infty$ ) annulent  $P$  (respectivement  $Q - P, Q$ ). La multiplicité d'une racine de  $\rho_i$  est majorée par  $\deg \rho_i$  de sorte qu'on peut choisir  $\alpha_i \leq \deg \rho_i$  et  $\alpha_0 + \alpha_1 + \alpha_\infty \leq 2n - 1$  impliquant un nombre fini de triplets  $\{\alpha_i\}$  possibles.

Effectuant la division euclidienne de  $P^{\alpha_0}(Q - P)^{\alpha_1}Q^{\alpha_\infty}$  par  $P'Q - Q'P$ , opération rationnelle dans le corps engendré sur  $\mathbb{Q}$  par les coefficients, on obtient un polynôme en  $y$  de degré inférieur ou égal à  $2n - 2$ . L'annulation de ses  $2n - 1$  coefficients fournit ainsi pour tout triplet  $\{\alpha_i\}$ ,  $2n - 1$  conditions algébriques qui ont au plus un nombre fini de solutions correspondant aux applications de Belyi de genre zéro et de degré  $n$ . Celles ayant un ordre de ramification 2 en  $\beta^{-1}(1)$  correspondant aux triangulations dérivées décrites ci-dessus.

Donnons l'exemple classique (Klein) de la décomposition tétraédrale de la sphère, carte régulière et de la carte dérivée en douze paires de triangles. Dans la normalisation choisie  $y = \infty$  est l'un des points de ramification - on pourrait y remédier par une transformation homographique - et correspond à un "milieu de face", envoyé sur  $x = 1$ , tandis qu'on envoie les sommets en  $x = 0$  et les milieux d'arêtes à l'infini.

Posant

$$s = y(y^3 + 8), \quad a = -y^6 + 20y^3 + 8, \quad f = (y^3 - 1)$$

tels que  $-s^3 + a^2 + 64f^3 = 0$ , on définit

$$\beta : y \rightarrow x = \frac{P(y)}{Q(y)} = \frac{s^3}{a^2}$$

et on vérifie que

$$P(Q - P)Q = -\frac{1}{3}(P'Q - Q'P)saf$$

Le groupe cartographique identique au groupe de symétrie est le groupe alterné à 12 éléments  $A_4$  et la courbe est définie sur  $\mathbb{Q}$ .

Avec les mêmes conventions, les cartes régulières de groupe  $S_2, S_3, S_4$  correspondent respectivement aux applications, définies sur  $\mathbb{Q}$  (pour la dernière voir Figure 3)

$$y \rightarrow x = y^2$$

$$y \rightarrow x = \left(\frac{y^3 - 1}{y^3 + 1}\right)^2$$

$$y \rightarrow x = \frac{1}{64} \frac{[(48y^4 - 8y^2 + 3)(16y^4 + 40y^2 + 1)]^3}{[y(4y^2 - 1)(16y^4 + 8y^2 + 9)(144y^4 + 8y^2 + 1)]^2}$$

Il existe aussi une construction "transcendante" du générateur du corps des fonctions rationnelles dans le cas des cartes régulières de la sphère (correspondant aux solides réguliers).

Reprenons d'abord l'exemple du tétraèdre régulier ci-dessus et l'application de Belyi

$$x = \frac{y^3(y^3 + 8)^3}{(y^6 - 20y^3 - 8)^2}$$

Une image inverse du demi plan  $\text{Im } x > 0$  est un triangle dans le plan  $y$  dont les côtés peuvent être des arcs de cercles (correspondant à la subdivision barycentrique du tétraèdre). Une application de Schwarz

$$t = \int_0^x \frac{dz}{z^{1-\frac{1}{3}}(1-z)^{1-\frac{1}{6}}}$$

transforme le demi plan  $\text{Im } x > 0$  dans le sixième d'un triangle équilatéral d'angles au sommets  $\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{6}$ . La fonction inverse  $y(t)$  satisfait à

$$\left(6 \frac{dy}{dt}\right)^2 = 1 - y^3$$

qui est l'équation affine de la courbe elliptique  $F^3$  (la courbe de Fermat de degré 3 et de genre 1) double recouvrement de la sphère ramifiée aux sommets du tétraèdre et le corps cherché  $\mathbb{Q}(y(t))$  où  $y$  est à normalisation près, la fonction de Weierstrass sur cette courbe. La construction s'interprète en "mettant à plat" le tétraèdre régulier comme un ensemble de triangles équilatéraux avec identification des côtés. La fonction de Belyi cherchée est alors une fonction doublement périodique dont la dérivée s'annule aux sommets, prenant 2 fois chaque valeur dans une cellule élémentaire du groupe de translation (rapport modulaire  $e^{2i\pi/6}$ ) : à translation près, c'est la fonction de Weierstrass.

On peut répéter une construction analogue pour l'octaèdre où l'on trouve que le corps rationnel cherché est un sous corps de celui des fonctions méromorphes sur une courbe de genre 4, triple recouvrement de la sphère ramifié aux images inverses des 6 sommets d'un octaèdre régulier, d'équation affine

$$4 \left(12 \frac{dy}{dt}\right)^3 = y^6 - 20y^3 - 8$$

(on posera  $v = 12 \frac{dy}{dt}$ ).

Enfin le cas de l'icosaèdre donne comme générateur une fonction méromorphe sur une surface de genre 25, sextuple recouvrement de la sphère ramifié aux images inverses des sommets de l'icosaèdre.

A notre connaissance l'exemple le plus simple de carte ayant des conjugués galoisiens est une troncation du "dessin d'enfant" d'Oesterlé. Il correspond au symbole féminin et possède deux conjugués (Figure 4). Ce sont des cartes à deux faces, l'une a un côté et l'autre neuf. On cherche donc une fraction rationnelle de la forme  $\frac{s(z)}{z+u}$  où  $s(z)$  est de degré 10, et  $-u$  le centre de la face à un côté, le centre de l'autre face étant à l'infini. Fixer le sommet d'ordre 4 à être à l'origine rigidifie le dessin aux dilatations près. Alors  $s(z)$  est de la forme  $\ell z^4(z+t)^3 p(z)$  où  $-t$  est la position du



sommet d'ordre 3 et où  $p$  est un polynôme unitaire de degré 3 dont les racines sont les positions des trois sommets d'ordre 1. Demander que  $\frac{s(z)}{z+u} - 1$  soit de la forme  $\frac{\ell q(z)^2}{z+u}$  où les zéros du polynôme unitaire  $q$  sont les milieux d'arêtes amène à un problème d'élimination. Il faut choisir  $\ell, t, u$ , les trois coefficients de  $p$  et les cinq de  $q$  de telle sorte que le polynôme

$$\ell z^4(z+t)^3 p(z) - (z+u) - \ell q(z)^2$$

soit identiquement nul. Les coefficients dominants se compensent, donc il reste dix équations homogènes en onze variables. On montre alors que les coefficients inconnus sont polynomiaux en  $t$  et  $u$ , et que  $t$  et  $u$  sont liés par la relation de degré 3

$$t^3 + 9t^2u + 99tu^2 + 105u^3 = 0$$

dont les trois solutions sont

$$\frac{t}{u} = -3 - \frac{6}{\alpha} + 4\alpha, -3 - \frac{6j}{\alpha} + 4j^2\alpha, -3 - \frac{6j^2}{\alpha} + 4j\alpha$$

où  $j = \exp \frac{2i\pi}{3}$  et  $\alpha$  est la racine cubique réelle de 6.

La première solution est réelle, et pour des raisons de symétrie, elle est donc associée au symbole féminin original. En général, il est difficile sauf en traçant numériquement l'image réciproque du segment  $[0, 1]$  pour chaque solution, de voir quel dessin conjugué est associé à une solution donnée des équations algébriques satisfaites par la fonction de Belyi. Les deux conjugués du symbole féminin illustrent déjà ce dilemme (voir Figure 5).

En plus de ceux qui figurent dans la contribution d'Oesterlé on trouvera d'autres exemples dans les articles de Shabat et Voevodsky (voir ci-dessous) et Wolfart.

Les considérations qui précèdent sont de nature trop élémentaires pour éclairer l'action de  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  sur les cartes et la liste des problèmes ouverts est énorme. Citons parmi ceux-ci:

1. Caractériser les courbes correspondant aux cartes régulières pour des familles aussi larges que possibles. Nous ne connaissons même pas la solution pour les groupes de permutations.
2. Quelles sont les cartes dont la courbe est définie sur  $\mathbb{Q}$ ? Examiner les réductions modulo un nombre premier.
3. Pour un genre positif, dans un modèle affine  $P(x, y) = 0$  où  $x$  est la fonction de Belyi d'une carte  $y$  étant une seconde fonction rationnelle sur la courbe (et donc  $P(x, y)$  de degré  $n = 2A$  en  $y$ ) chercher, par un choix approprié de  $y$ , à minorer le degré en  $x$ .
4. Caractériser la représentation du groupe d'automorphisme sur les formes harmoniques discrètes.

Cette énumération pourrait se poursuivre longtemps ou se résumer en une seule question: Quelles sont les propriétés arithmétiques susceptibles d'être lues sur une carte et quelles sont les cartes associées par  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ?

Pour répondre partiellement à la question 3, donnons une construction, celle du diviseur canonique - ou plutôt d'un représentant de la classe d'équivalence correspondante - susceptible de fournir des renseignements utiles.

Soit  $x$  la fonction rationnelle correspondant à l'application de Belyi  $\Sigma \rightarrow \mathbb{P}_1$  et  $S, A$  et  $\mathcal{F}$  les images réciproques par  $\beta$  des valeurs critiques 0, 1,  $\infty$ . S'il s'agit d'une triangulation dérivant d'une carte, ce sont les points correspondants respectivement aux sommets, arêtes et faces de la carte initiale.

La différentielle  $dx$  est alors méromorphe et son diviseur est un représentant de la classe canonique  $K$

$$\text{div}(dx) = \sum_{s \in S} (v(s) - 1)s + \sum_{a \in A} (v(a) - 1)a - \sum_{f \in \mathcal{F}} (v(f) + 1)f$$

Soit  $L(K)$  l'espace vectoriel (a priori sur  $\mathbb{C}$  ou plutôt sur  $\bar{\mathbb{Q}}$ ) des fonctions rationnelles sur  $\Sigma$  telles que

$$y \in L(K) \iff \text{div}(y) + \text{div}(dx) \geq 0$$

Ce sont des fonctions dont les zéros appartiennent à  $\mathcal{F}$ , les pôles à  $A \cup S$  et telles en outre qu'en tout point  $f \in \mathcal{F}$   $y$  a un zéro d'ordre au moins  $v(f) + 1$ , en tout  $a \in A$  un pôle d'ordre au plus  $v(a) - 1$ , enfin en tout  $s \in S$  un pôle d'ordre au plus  $v(s) - 1$ .

Le théorème de Riemann Roch implique qu'en genre positif

$$\ell(K) = \dim L(K) = g$$

et que pour tout  $y \in L(K)$ ,  $y dx$  différentielle holomorphe possède  $2g - 2$  zéros.

Considérons d'abord le cas particulier de genre 1. Il s'ensuit que  $L(K)$  est unidimensionnel. En d'autres termes une telle fonction  $y$  est unique à un facteur constant près et de plus  $y dx = dt$  est une différentielle holomorphe sans zéro. Dans ces conditions les inégalités précédentes deviennent des égalités, c'est dire que

$$\text{div}(y) = \sum_{f \in \mathcal{F}} (v(f) + 1)f - \sum_{a \in A} (v(a) - 1)a - \sum_{s \in S} (v(s) - 1)s$$

Dans le cas d'une triangulation dérivée  $v(a) = 2$  pour tout  $a$ , par conséquent

$$\text{nombre de zéros de } y = \sum_{f \in \mathcal{F}} (v(f) + 1) = F + 2A$$

$$\text{nombre de pôles de } y = A + \sum_{s \in S} (v(s) - 1) = 3A - S$$

Ces quantités sont bien égales puisqu'en genre 1 on a  $S + F = A$ . Il s'ensuit - toujours d'après Riemann - que les paires  $x, y$ , éléments de  $\bar{\mathbb{Q}}(\Sigma)$ , satisfont à une relation polynomiale

$$P(x, y) = 0$$

telle que

$$\begin{aligned} \deg_x P &= 2A + F \\ \deg_y P &= 2A \end{aligned}$$

donnant un plongement  $\Sigma \rightarrow \mathbb{P}_1 \times \mathbb{P}_1$ .

On adaptera ces raisonnements sur les degrés si la triangulation de Belyi est arbitraire auquel cas on aura

$$\begin{aligned} \deg_y P &= \deg(\beta) = \sum_{f \in \mathcal{F}} v(f) = \sum_{s \in S} v(s) \\ \deg_x P &= |\mathcal{F}| + \deg(\beta) \end{aligned}$$

Dans le cas général ( $g \geq 1$ ) on aura défini par le procédé précédent un espace vectoriel  $L(K)$  de  $g$  fonctions rationnelles sur  $\Sigma$  linéairement indépendantes. L'une quelconque prend chaque valeur un nombre égal à celui de ses pôles (comptés avec leur multiplicité), c'est-à-dire

$$\deg(y) \leq \sum_{a \in A} (v(a) - 1) + \sum_{s \in S} (v(s) - 1)$$

Pour une triangulation dérivée on a donc

$$\deg(y) \leq 3A - S$$

Comme  $A - S - F = 2(g - 1)$  ceci est équivalent à

$$\deg(y) \leq F + 2A + 2(g - 1)$$

l'inégalité étant remplacée par une inégalité en genre 1.

Comme précédemment on en conclut une relation polynomiale

$$P(x, y) = 0$$

quel que soit  $y \in L(K)$  avec

$$\begin{aligned} \deg_x P &\leq F + 2A + 2(g - 1) \\ \deg_y P &= 2A \end{aligned}$$

Ajoutons quelques remarques:

(i) Il y a dissymétrie de ces expressions entre sommets et faces, qu'on pourra compenser en considérant les relations entre  $y$  et  $x^{-1}$ .

(ii) Les raisonnements précédents ne permettent pas d'affirmer qu'une paire  $x, y$  engendre effectivement le corps  $\bar{\mathbb{Q}}(x, y)$ . C'est cependant génériquement très vraisemblable.

(iii) Le groupe d'automorphisme de la carte agit sur  $L(K)$ . Resterait à examiner de plus près cette action.

(iv) On pourrait examiner plus généralement  $L(nK)$ .

Quoi qu'il en soit la construction qu'on vient de décrire fournit un moyen effectif de relier les données combinatoires et analytiques en permettant d'aborder dans certains cas l'analyse du corps  $\bar{\mathbb{Q}}(\Sigma)$  et son éventuelle restriction, un corps de nombres, extension finie de  $\mathbb{Q}$ .

A titre d'illustration on va analyser un exemple dû à Shabat et Voevodsky en genre 1 qui conduit au corps de définition  $\mathbb{Q}(\sqrt{7})$  et donc à un unique conjugué. Soit la carte tracée sur un tore formée de 8 faces (triangulaires) de 12 arêtes et de quatre sommets groupés en deux paires  $(s_1^+, s_1^-)$  chacun de valence 7 et  $(s_2^+, s_2^-)$  chacun de valence 5. Le degré de l'application de Belyi est donc 24. Soit  $x$  la fonction correspondante qui prend la valeur zéro en  $s_1^\pm$  points critiques d'ordre 7 et  $s_2^\pm$  points critiques d'ordre 5, la valeur 1 aux douze milieux d'arêtes (indiqués par des cercles sur la Figure 6a) points critiques d'ordre 2, enfin la valeur  $\infty$  aux huit milieux de faces points critiques d'ordre 3 (puisque les faces sont des triangles). Superficiellement la figure admet une symétrie  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  indiquée schématiquement par des axes de symétrie, l'un d'eux échangeant les sommets  $s_1^+$  et  $s_1^-$ , l'autre les sommets  $s_2^+$  et  $s_2^-$ . Plus précisément, il s'agit de deux anti-automorphismes de la surface de Riemann dont le produit est une involution qui échange les faces  $f_i^+ \longleftrightarrow f_i^-$ , remarque qui va se révéler essentielle dans la suite. D'ailleurs on vérifie sans peine que le groupe d'automorphisme de la carte définie comme ci-dessus se réduit à cette involution. Montrons que ces données permettent de construire une fonction méromorphe sur la surface de Riemann correspondante de degré deux comme on s'y attend pour une courbe elliptique. En effet soit  $y$  la unique différentielle holomorphe à facteur près.

La fonction  $y$  (de degré 32) a des pôles d'ordre 6 en  $s_1^\pm$ , d'ordre 4 en  $s_2^\pm$  et des pôles simples aux douze milieux d'arêtes  $a_i$  tandis qu'elle a des zéros quadruples aux huit milieux de faces  $f_i$ . Il s'ensuit que la combinaison

$$z = x^5(x-1)^3y^6$$

est à un facteur près la fonction cherchée ayant deux pôles simples en  $s_1^\pm$  et deux zéros simples en  $s_2^\pm$ . Le théorème de Riemann-Hurwitz implique alors que  $z$  a quatre points critiques (où  $dz$ , ou si l'on préfère  $\frac{dz}{y dx}$ , s'annule simplement). Pour le voir il suffit de décomposer la sphère où  $z$  prend ses valeurs en deux polygones à  $n$  côtés dont les sommets sont ces points critiques, de relever cette décomposition sur le tore en quatre polygones à  $n$  côtés possédant  $2n$  arêtes et  $n$  sommets. Comme la caractéristique d'Euler s'annule  $n - 2n + 4 = 0$  et  $n = 4$ . Une autre façon de le voir consiste à remarquer que sur le tore les formes différentielles ont autant de zéros que de pôles. Or  $dz$  a deux pôles doubles donc quatre zéros. Ces quatre points sont insensibles à la normalisation (multiplicative) de  $z$ . Comme nous l'avons remarqué, les automorphismes d'une carte proviennent d'automorphismes de la courbe arithmétique associée. Nous notons  $\tilde{\mu}$  l'automorphisme du tore associé à l'automorphisme  $\mu$  de la carte. Il est facile de vérifier que  $\mu$  laisse 4 arêtes fixes (en

échangeant les deux demi-arêtes de ces quatre arêtes). Donc  $\tilde{\mu}$  a la même propriété, et possède un point fixe sur le milieu de ces quatre arêtes. Mais les automorphismes d'un tore ont soit zéro soit quatre points fixes. En effet si  $t$  est un paramètre uniformisant, un automorphisme est soit une translation (sans point fixe) soit la composée d'une translation et de l'inversion  $t \rightarrow -t$  (quatre points fixes car  $2t = 0$  a quatre solutions). Choisisant l'origine en un point fixe de  $\tilde{\mu}$  on a donc  $\tilde{\mu}(t) = -t$ , et  $dt \rightarrow -dt$ . Par définition d'un automorphisme  $x$  (donc  $dx$ ) est invariant. En conséquence  $y \rightarrow -y$  donc  $z$  est invariant. On a alors le résultat général suivant: sur une surface de Riemann les points fixes d'un automorphisme non trivial sont points critiques de toutes les fonctions méromorphes invariantes par cet automorphisme. Dans notre cas particulier la démonstration est triviale. Les fonctions invariantes dans  $\tilde{\mu}$  sont les fonctions de  $t^2$ , donc leur différentielle à un zéro au point fixe. On en déduit que les quatre points critiques de la fonction invariante  $z$  sont les points critiques de la fonction invariante  $x$  situées sur les quatre arêtes globalement invariantes. Donc les points critiques de  $z$  sont les quatre milieux d'arêtes  $a_1, a_2, a_3, a_4$ .

En suivant Shabat et Voevodsky cherchons maintenant à reconstruire  $x$  comme fonction rationnelle de  $z$ . Définissons  $\phi = \prod_{1 \leq i \leq 4} (z - z(f_i^\pm))$  polynôme unitaire de degré 4. La fonction  $\phi^3/z^5$  se comporte comme  $z^7$  pour  $z$  grand et comme  $z^{-5}$  pour  $z$  tendant vers zéro. Le produit  $x\phi^3/z^5$  est donc une constante puisque sans pôle, et l'on vérifie alors que  $x$  a bien des pôles d'ordre trois aux milieux des faces. Posons

$$\frac{\rho}{x} = \frac{\phi^3}{z^5} \quad (*)$$

où  $\rho$  est une constante. On constate qu'il s'agit bien d'une fonction de degré 24. Il faut alors s'assurer que  $x - 1$  a des zéros doubles aux douze milieux d'arêtes parmi lesquels  $a_1, a_2, a_3, a_4$  où  $z$  a des points critiques simples. On posera

$$\alpha = \prod_{1 \leq i \leq 4} (z - z(a_i))$$

et l'équation de la courbe cherchée pourra s'écrire

$$u^2 = \alpha(z)$$

tandis que

$$\rho \left( \frac{1}{x} - 1 \right) = \frac{\alpha\beta^2}{z^5} \quad (**)$$

où  $\beta$  est à son tour un polynôme du quatrième degré dont les zéros sont les images par paires sur la sphère  $z$  des huit milieux d'arêtes restants. Reste à exprimer l'égalité des expressions de  $x$  tirée de (\*) et (\*\*). Il est plus simple d'égaliser les dérivées par rapport à  $z$  de ces deux équations ce qui fait disparaître l'inconnue  $\rho$ . Il vient ainsi

$$\phi^2 [3z\phi' - 5\phi] = \beta [z(\alpha'\beta + 2\alpha\beta') - 5\alpha\beta]$$

où  $\phi, \alpha, \beta$  sont trois polynômes unitaires de degré 4 en  $z$ . Chaque membre est factorisé en produit d'un polynôme de degré 4 et un de degré 8. On constate que les termes de plus haut degré sont compatibles avec les égalités

$$\begin{aligned} 3z\phi' - 5\phi &= 7\beta \\ 7\phi^2 &= z(\alpha'\beta + 2\alpha\beta') - 5\alpha\beta \end{aligned}$$

Ou encore en éliminant  $\beta$

$$49\phi^2 = (z\alpha' - 5\alpha)(3z\phi' - 5\phi) + 2\alpha(3z^2\phi'' - 2z\phi')$$

Les inconnues sont les huit coefficients des deux polynômes unitaires  $\alpha$  et  $\phi$  tandis que nous obtenons en apparence huit équations en identifiant les deux membres de l'équation précédente où les coefficients de  $z^8$  sont égaux. Cependant l'une des équations est conséquence des sept autres

ce qui reflète le fait que l'échelle de  $z$  est arbitraire. Ceci n'affecte pas la valeur de l'invariant modulaire. On trouve pour équation de la courbe avec  $k = \pm\sqrt{7}$

$$u^2 = z^4 + 156z^3 + (17150 + 4256k)z^2 + (4452140 + 1690304k)z - (279416375 + 10544000k)$$

soit pour l'invariant modulaire deux valeurs positives qui encadrent  $12^3$

$$j = 4(114302 + 43141k) = 4(8 - 3k)^2(2 + k)^6(10 + 3k)^3$$

On confirme bien que le corps de définition de la carte initiale est  $\mathbb{Q}(\sqrt{7})$  et qu'elle n'admet qu'une conjuguée (Figure 6b). Resterait à associer la valeur positive,  $\sqrt{7}$  disons, à l'une des deux cartes, ce que nous n'avons pu faire que numériquement. Nous avons commencé par tracer l'image réciproque du segment  $[0, 1]$  par l'application de Belyi sur la sphère de la fonction  $z$  (Figure 7a-b) avant de remonter sur le tore. Le dessin original est associé à  $k = -\sqrt{7}$ , et son conjugué à  $k = +\sqrt{7}$  (voir Figure 8a-b).

Parmi les faibles informations dont on dispose sur les cartes qui se déduisent par action du groupe de Galois figure le fait que les nombres  $S_v$  et  $F_v$  de sommets et de faces de valence  $v$  sont les mêmes pour tout  $v$  (et bien sûr le nombre d'arêtes est conservé). Ceci suggère la définition suivante. On dira que deux cartes sont associées si elles ont les mêmes valeurs de  $S_v$  et  $F_v$  pour tout  $v$  - sans qu'elles soient nécessairement connexes. Or on a le résultat suivant de théorie des groupes - facile à vérifier -. Soit  $G$  un groupe fini d'ordre  $|G|$ ,  $\tilde{G}$  son dual, ensemble des représentations linéaires irréductibles (sur  $\mathbb{C}$ )  $C_1, C_2, C_3$  trois classes de  $G$

Lemme. Le nombre  $N_{C_1, C_2, C_3}$  de triplets  $g_1, g_2, g_3$  avec  $g_i \in C_i$  tels que  $g_1 g_2 g_3 = 1$  est donné par

$$N_{C_1, C_2, C_3} = \frac{|C_1||C_2||C_3|}{|G|} \sum_{r \in \tilde{G}} \frac{\chi^r(C_1) \chi^r(C_2) \chi^r(C_3)}{\dim_r}$$

où  $\dim_r$  est la dimension de la représentation  $r$  et  $\chi^r(C)$  la valeur du caractère correspondant sur la classe  $C$  de cardinal  $|C|$ .

La donnée des  $S_v, F_v$  tels que  $2A = \sum_v v S_v = \sum_v v F_v$  nous fournit trois classes de  $\Sigma_{2A}$  et un ensemble de cartes associées. Le nombre de triplets  $\sigma_0, \sigma_1, \sigma_2$  avec  $\sigma_0 \in \prod_v (v)^{S_v}, \sigma_1 \in (2)^A$  et  $\sigma_2 \in \prod_v (v)^{F_v}$  (avec la notation standard des classes du groupe des permutations) tels que  $\sigma_2 \sigma_1 \sigma_0 = 1^*$  est égal à la somme sur ces cartes associées (c'est-à-dire de tels triplets à équivalence près dans  $\Sigma_{2A}$ ) des entiers  $\frac{|\Sigma_{2A}|}{|H|}$  où  $H$  est le groupe d'automorphismes.

On en déduit l'égalité  $F(\{S_v, F_v\}) \equiv$

$$\frac{(2A-1)!!}{\prod_v v^{S_v+F_v} S_v! F_v!} \sum_{r \in \tilde{\Sigma}_{2A}} \frac{\chi^r(\prod_v (v)^{S_v}) \chi^r((2)^A) \chi^r(\prod_v (v)^{F_v})}{\dim_r} = \sum_{\text{cartes associées}} \frac{1}{|H_{\text{carte}}|}$$

qui conduit au critère de rationalité suivant

Proposition. Etant donnée une carte (connexe) telle que

$$|H|F(\{S_v, F_v\}) = 1$$

alors le corps de définition est  $\mathbb{Q}$ .

Ce critère est évidemment à rapprocher (mais est moins intrinsèque) du critère de rigidité énoncé dans l'exposé de Serre cité en référence (qui ne s'intéresse en outre qu'au cas régulier où  $|H|$  est l'ordre du groupe cartographique).

Exemple: Le tore.

\* Dans certains exemples nous avons inversé l'ordre  $\sigma_2 \sigma_1 \sigma_0 = 1$  (au lieu de  $\sigma_0 \sigma_1 \sigma_2 = 1$ ), ceci n'affecte évidemment pas la nature des résultats.

On a:  $S = 1, A = 3, F = 2$  et le genre vaut 1. On peut choisir:

$$\sigma_0 = (1, 4, 2, 5, 3, 6), \sigma_1 = (1, 5)(2, 6)(3, 4) = \sigma_0^3, \sigma_2 = (1, 2, 3)(4, 5, 6) = \sigma_0^2$$

Le groupe cartographique est abélien d'ordre 6, de générateur  $\sigma_0$ , isomorphe à  $\mathbb{Z}/6\mathbb{Z}$ .

Les permutations qui commutent avec  $\sigma_0, \sigma_1, \sigma_2$ , forment un groupe isomorphe (la carte est régulière):  $|H| = 6$ . En se servant de la table des caractères de  $\Sigma_6$  (F.D. Murnaghan, "The Theory of Group Representations" Dover, New York (1963), page 146) on trouve que la quantité à évaluer est

$$\frac{6 \times 5!!}{6^3 1! 3^2 2!} \cdot \left(1 + 1 - \frac{1}{5} - \frac{1}{5} - \frac{2}{10} - \frac{2}{10}\right) = 1$$

ce qui est bien ce qu'on attend pour la courbe elliptique d'invariant modulaire  $j = 0$  "définie" sur  $\mathbb{Q}$ .

De même on vérifie que la carte de genre zéro représentée sur la Figure 9 est définie sur  $\mathbb{Q}$ . On a tracé sur cette figure l'image inverse par la fonction de Belyi du segment  $[0, 1]$ .

Un cas très particulier où l'on saurait sans trop de peine évaluer  $F(\{S_v\}, \{F_v\})$  est celui où la carte n'a qu'un sommet ou qu'une face (c'est-à-dire tous les  $S_v = 0$  sauf  $S_{2A} = 1$ , ou tous les  $F_v = 0$  sauf  $F_{2A} = 1$ ).

Dans ce cas, comme parmi les représentations de  $\Sigma_n$  seules celles associées aux partitions  $(q+1, 1^p)$  ont un caractère qui ne s'annule pas identiquement sur le cycle  $(n)$  on peut utiliser le résultat que

$$\sum_{p+q=n-1} (-1)^p y^p z^q \chi^{p,q} \left( \prod_v (v)^{k_v} \right) = \frac{\prod_v (z^v - y^v)^{k_v}}{z - y}$$

qui donne

$$\dim_{p,q} = \binom{n-1}{p} = \binom{n-1}{q}$$

$$\chi^{p,q}((n)) = (-1)^p$$

et si  $n = 2A$

$$\chi^{p,q}((2)^A) = (-1)^{\lfloor \frac{p+1}{2} \rfloor} \binom{A-1}{\lfloor \frac{p}{2} \rfloor}$$

où le crochet désigne la partie entière, résultats qu'on aura l'occasion d'utiliser plus loin.

Plus généralement

$$\sum_{\Sigma v S_v = \Sigma v F_v = 2A} \prod_v (t_v)^{S_v} (t'_v)^{F_v} F(\{S_v\}, \{F_v\}) = \sum_{\substack{\ell_1 > \ell_2 > \dots > \ell_{2A} \geq 0 \\ \Sigma \ell_k = A(2A+1)}} (-1)^{\frac{A(A-1)}{2}} \text{ch}_{\ell}(\theta) \text{ch}_{\ell}(\theta') \frac{\prod_{\ell \text{ impair}} \ell!! \prod_{\ell \text{ pair}} (\ell-1)!!}{\prod (\ell_{\text{impair}} - \ell_{\text{pair}})}$$

Les indices  $\ell_1 > \ell_2 > \dots > \ell_{2A} \geq 0$  indexent les tableaux d'Young ayant dans la ligne  $i$ ,  $f_i = \ell_i + i - 2A$  boîtes, la somme est restreinte aux termes tels que le nombre des  $\ell$  pairs est égal à celui des  $\ell$  impairs (c'est-à-dire  $A$ ); enfin les fonctions de Schur généralisées (caractères du groupe linéaire) sont exprimées en fonction des variables  $\theta_v = \frac{t_v}{v}$  (ou  $\theta'_v = \frac{t'_v}{v}$ ) par

$$\text{ch}_{\ell}(\theta) = \det p_{f_i+i-j}(\theta) |_{1 \leq i, j \leq 2A}$$

$$\sum_0^{\infty} z^f p_f(\theta) = \exp \sum_1^{\infty} z^n \theta_n$$

Il est en fait possible de trouver une fonction génératrice des quantités  $F_C(\{S_v\}, \{F_v\})$  où la somme des  $\frac{1}{|H|}$  ne porte que sur les cartes associées connexes à l'aide d'une intégrale matricielle.

Soit  $dM$  la mesure de Lebesgue sur l'ensemble des matrices hermitiennes  $N \times N$  et  $\Lambda$  une matrice définie positive. Dans le régime  $\Lambda \rightarrow \infty$  on a (grâce à une remarque d'I. Kostov) le développement asymptotique

$$\ln \left( \frac{\int dM \exp \left( -\frac{1}{2} \text{tr} M \Lambda M \Lambda + \sum_1^\infty g_k \text{tr} \frac{M^k}{k} \right)}{\int dM \exp \left( -\frac{1}{2} \text{tr} M \Lambda M \Lambda \right)} \right) = \sum F_C(\{S_v\}, \{F_v\}) g_1^{S_1} g_2^{S_2} \dots (\text{tr} \Lambda^{-1})^{F_1} (\text{tr} \Lambda^{-2})^{F_2} \dots$$

Hélas à la différence des problèmes traités dans la section suivante, on ne dispose pour l'instant d'aucune méthode efficace pour étudier cette fonction génératrice en dehors de l'expression donnée ci-dessus.

#### 4. DECOMPOSITIONS CELLULAIRES DE L'ESPACE DES MODULES

##### A. La caractéristique virtuelle

Jusqu'ici nous avons considéré chaque carte séparément. Il est possible d'utiliser des familles de cartes pour donner une décomposition cellulaire de l'espace des modules des courbes. La technique des intégrales matricielles permet alors d'obtenir des résultats concernant la topologie de cet espace de modules. Nous donnons brièvement dans cette section et la suivante deux exemples frappants.

Soit  $\Gamma_{g,n}$  le groupe modulaire correspondant à des surfaces de Riemann à  $n$  points marqués, quotient discret du groupe des difféomorphismes par ceux qui sont homotopes à l'identité. Il est possible de trouver un espace contractible  $\mathcal{T}$  sur lequel agit ce groupe et on appelle caractéristique d'Euler virtuelle  $\chi(\Gamma_{g,n})$  le quotient de la caractéristique d'Euler de  $\mathcal{T}/\Gamma'$ , où  $\Gamma' \subset \Gamma_{g,n}$  est un sous groupe d'indice fini  $[\Gamma_{g,n} : \Gamma']$  agissant sans point fixe sur  $\mathcal{T}$ , par l'indice en question. On se limitera au cas  $n > 0$ ,  $2g - 2 + n > 0$  et on posera d'abord  $n = 1$ .

Selon Harer et Zagier pour  $g > 0$

$$\chi(\Gamma_{g,1}) = \sum_{r=2g}^{6g-3} (-1)^{r-1} \frac{\lambda_g(r)}{2r}$$

où l'entier  $\lambda_g(r)$  est obtenu de la manière suivante. On considère un polygone à  $2r$  côtés et on compte le nombre  $\lambda_g(r)$  d'appariements distincts des côtés conduisant à une surface de genre  $g$  orientable (l'unique face correspond au point marqué) tels que la carte obtenue ne contiennent que des sommets de valence supérieure à deux. Ces cartes sont donc telles que

$$2A = 2r = \sum_{v \geq 3} v S_v \geq 3S$$

d'où l'on tire  $r \leq 6g - 3$  comme indiqué ci-dessus, l'autre borne  $r \geq 2g$  étant évidente. Pour obtenir la quantité voulue passons par l'intermédiaire des intégrales matricielles. Soit  $\mathcal{M}$  l'espace vectoriel des matrices hermitiennes à  $N$  lignes et colonnes,  $\dim_{\mathbb{R}} \mathcal{M} = N^2$  et si  $M$  désigne un élément générique soit

$$dM = \prod_{1 \leq i \leq N} dM_{ii} \prod_{i < j} d \text{Re} M_{ij} d \text{Im} M_{ij}$$

la mesure de Lebesgue sur  $\mathcal{M}$  invariante par l'action adjointe du groupe unitaire  $U(N)$ . Considérons alors une partition  $\underline{\nu}$  de l'entier  $2r$ , c'est-à-dire  $\underline{\nu} \equiv \{\nu_1, \dots, \nu_{2r} \mid \sum_j \nu_j = 2r\}$  et posons

$$t_{\underline{\nu}}(M) = \prod_j (\text{tr} M^j)^{\nu_j}$$

D'après les règles perturbatives de Feynman la valeur moyenne

$$\langle t_{\underline{\nu}} \rangle = \frac{\int dM e^{-\frac{1}{2} \text{Tr} M^2} t_{\underline{\nu}}(M)}{\int dM e^{-\frac{1}{2} \text{Tr} M^2}}$$

s'obtient comme somme sur des produits de cartes connexes ayant au total  $\nu_j$  sommets de valence  $j$  chacune affectée d'un poids égal à  $N^F$  ( $F$  nombre de faces).

Chaque carte (connexe ou pas) est décrite par un groupe cartographique engendré par deux permutations (de  $2r$  objets)  $\sigma_0$  et  $\sigma_1$ , avec  $\sigma_1^2 = 1$  et  $\sigma_0 \in \underline{\nu}$ , en identifiant les partitions avec les classes de conjugaison du groupe de permutations correspondant,  $\Sigma_{2r}$ , dont on notera  $\underline{\Sigma}_{2r}$  l'ensemble des classes. Rappelons que le nombre d'éléments de la classe  $\underline{\nu}$  est

$$|\underline{\nu}| = \frac{(2r)!}{\prod_j j^{\nu_j} \nu_j!}$$

Pour un élément  $\sigma \in \Sigma_{2r}$  on écrira parfois  $[\sigma]$  pour désigner sa classe au lieu  $\underline{\nu}(\sigma)$ . Cela étant, ayant choisi un représentant  $\sigma_0 \in \underline{\nu}$ , ce qui revient à indexer les  $2r$  matrices  $M$  figurant dans  $t_{\underline{\nu}}(M)$ , les règles perturbatives s'expriment sous la forme

$$\langle t_{\underline{\nu}} \rangle = \sum_{\underline{\mu} \in \underline{\Sigma}_{2r}} \sum_{\substack{\sigma_1 \in [2^r] \\ [\sigma_0 \sigma_1] \in \underline{\mu}}} N^{\sum \mu_i}$$

où l'on somme sur les permutations  $\sigma_1 \in [2^r]$  pondérées par  $N^{\sum \mu_i}$ ,  $\mu_i$  étant le nombre de cycles de longueur  $i$  de  $\sigma_0 \sigma_1$ , c'est-à-dire le nombre de faces de valence  $i$ .

Introduisons les caractères  $\chi^Y$  ( $Y$  un tableau d'Young à  $2r$  boîtes) du groupe  $\Sigma_{2r}$  qui satisfont aux relations d'orthogonalité et de complétude

$$\begin{aligned} \sum_Y \chi^Y(\sigma) \chi^Y(\tau) &= \frac{(2r)!}{|[ \sigma ]|} \delta_{[\sigma], [\tau]} \\ \sum_{\tau \in \Sigma_{2r}} \chi^Y(\tau) \chi^Y(\sigma \tau) &= (2r)! \delta_{Y, Y'} \frac{\chi^Y(\sigma)}{\chi^Y([1^{2r}])} \end{aligned}$$

où  $\chi^Y([1^{2r}])$  est bien évidemment la dimension de la représentation indexée par  $Y$ . Un calcul immédiat donne

$$\langle t_{\underline{\nu}} \rangle = \sum_{\underline{\mu} \in \underline{\Sigma}_{2r}} \langle t_{\underline{\nu}} \rangle_{\underline{\mu}}$$

où

$$\frac{\langle t_{\underline{\nu}} \rangle_{\underline{\mu}}}{|\underline{\mu}| N^{\sum \mu_i}} \equiv \frac{\langle t_{\underline{\mu}} \rangle_{\underline{\nu}}}{|\underline{\nu}| N^{\sum \nu_i}} = \frac{|[2^r]|}{(2r)!} \sum_Y \frac{\chi^Y([2^r]) \chi^Y(\underline{\mu}) \chi^Y(\underline{\nu})}{\chi^Y([1^{2r}])}$$

La symétrie de cette expression reflète l'échange des cartes avec leurs duales (c'est-à-dire l'échange des sommets avec les faces).

Revenons à  $\chi(\Gamma_{g,1})$ . Par dualité on voit que le calcul de  $\lambda_g(r)$  revient à l'évaluation de  $\langle t_{[2r]} \rangle \equiv \langle \text{tr} M^{2r} \rangle$  qui n'introduit que des cartes connexes. Plus précisément

$$\lambda_g(r) = \sum_{\substack{\underline{\mu}, \mu_1 = \mu_2 = 0 \\ \sum \mu_i = r+1-2g}} \frac{\langle t_{[2r]} \rangle_{\underline{\mu}}}{N^{\sum \mu_i}}$$

La condition  $\sum \mu_i = \{\text{nombre de faces de la carte duale connexe à un seul sommet et } r \text{ arêtes}\} = r + 1 - 2g$ , exprime qu'on obtient une surface de genre  $g$ , tandis que  $\mu_1 = \mu_2 = 0$  reflète la restriction introduite dans la définition de  $\lambda_g(r)$ . Cette restriction rend malaisé le calcul de  $\lambda_g(r)$

sous cette forme et justifie des développements combinatoires fort élaborés dans l'article de Harer et Zagier.

Si on introduit une quantité intermédiaire  $\epsilon_r(g)$  obtenue en levant cette restriction, il est facile en revanche de voir à l'aide des expressions données ci-dessus en termes de caractères que

$$\sum_{g \leq \lfloor \frac{r}{2} \rfloor} N^{1+r-2g} \epsilon_g(r) = \langle t_{[2r]} \rangle = \frac{(2r-1)!!}{2} \text{coeff. de } y^{r+1} \text{ dans } \left( \frac{1+y}{1-y} \right)^N$$

Il est cependant possible en jouant de nouveau sur la dualité de trouver une façon élégante d'évaluer  $\chi(\Gamma_{g,1})$ . Observons qu'on peut encore écrire

$$\lambda_g(r) = \sum_{\substack{\mu_1, \mu_2 = 0 \\ \sum \mu_i = r+1-2g}} \frac{\langle t_{\mu} \rangle_{[2r]}}{N} \frac{2r}{\prod_j j^{\mu_j} \mu_j!}$$

Soit en clair

$$\frac{\lambda_g(r)}{2r} = \frac{1}{N} \sum_{\substack{\mu_3, \mu_4, \dots \\ \sum 3\mu_3 + 4\mu_4 + \dots = 2r \\ \sum \mu_i = r+1-2g}} \left\langle \frac{1}{\mu_3!} \left( \frac{\text{tr } M^3}{3} \right)^{\mu_3} \frac{1}{\mu_4!} \left( \frac{\text{tr } M^4}{4} \right)^{\mu_4} \dots \right\rangle$$

Les conditions de sommation impliquent que

$$\mu_3 + 2\mu_4 + 3\mu_5 + \dots = 4g - 2$$

et justifient la remarque suivante due à Penner. Soit

$$Z(N, x) = \left\langle \exp \left( - \sum_{k \geq 3} x^{k-2} \frac{M^k}{k} \right) \right\rangle$$

alors

$$\phi(N, x) = \log Z(N, x)$$

admet un développement perturbatif formel en contributions de cartes connexes qui peut se réorganiser en une série de puissances de  $N$

$$\phi(N, x) = \sum_{s \geq 1} \phi_s(x) N^s$$

avec

$$\begin{aligned} \phi_1(x) &= \sum_{g \geq 1} x^{4g-2} \left( \sum_{r=2g}^{6g-3} (-1)^{r+1} \frac{\lambda_g(r)}{2r} \right) \\ &= \sum_g x^{4g-2} \chi(\Gamma_{g,1}) \end{aligned}$$

Bien entendu l'intégrale intervenant dans  $Z(N, x)$  est formelle. Pour lui donner un sens remarquons que la représentation intégrale de la fonction  $\Gamma$  d'Euler est équivalente pour  $x$  réel positif tendant vers zéro à

$$\frac{(ex^2)^{\frac{1}{x^2}}}{(2\pi x^2)^{1/2}} \Gamma \left( \frac{1}{x^2} \right) = \frac{\int_{-\infty}^{1/x} dm \exp \left( - \sum_{k \geq 2} \frac{m^k x^{k-2}}{k} \right)}{\int_{-\infty}^{\infty} dm \exp \left( - \frac{m^2}{2} \right)}$$

A des termes exponentiellement petits près, le développement asymptotique pour  $x \rightarrow \infty$  (formule de Stirling) n'est rien d'autre que le développement perturbatif de cette intégrale où pour chaque terme, on pourra étendre l'intervalle d'intégration à  $(-\infty, +\infty)$ . C'est le sens qu'on va donner à l'expression matricielle ci-dessus après avoir effectué l'intégrale "angulaire" compacte réduisant  $Z(N, x)$  à une intégrale sur les valeurs propres  $\lambda_i$  chacune limitée à une intervalle semi infini  $(-\infty, \frac{1}{x})$  sans modifier la série asymptotique perturbative. De la sorte nous obtenons avec la notation  $\Delta(\lambda) \equiv \prod_{1 \leq i < j \leq N} (\lambda_i - \lambda_j)$

$$Z(N, x) = \frac{1}{(2\pi)^{N/2} \prod_1^N p!} \int \prod_1^N (d\lambda_i \theta(1 - \lambda_i x) (1 - \lambda_i x)^{\frac{1}{x^2}} e^{\frac{\lambda_i}{x}}) \Delta(\lambda)^2$$

où  $\theta(u)$  est la fonction saut d'Heaviside,  $\theta(u) = 1$  pour  $u > 0$ ,  $\theta(u) = 0$  pour  $u < 0$ . La représentation intégrale de la fonction  $\Gamma$  donnée ci-dessus nous fournit

$$\begin{aligned} Z(N, x) &= \left[ \frac{(ex^2)^{\frac{1}{x^2}}}{\sqrt{2\pi}} \Gamma \left( \frac{1}{x^2} \right) \right]^N \frac{x^{-N^2}}{\prod_1^{N-1} p!} \det \prod_0^{r+s} (1 + px^2) |_{0 \leq r, s \leq N-1} \\ &= \left[ \frac{(ex^2)^{\frac{1}{x^2}}}{\sqrt{2\pi x^2}} \Gamma \left( \frac{1}{x^2} \right) \right]^N \prod_1^{N-1} (1 + px^2)^{N-p} \end{aligned}$$

Pour compléter le calcul, il suffit d'utiliser la formule asymptotique de Stirling

$$\ln \frac{(ex^2)^{\frac{1}{x^2}}}{\sqrt{2\pi x^2}} \Gamma \left( \frac{1}{x^2} \right) \sim \sum_{n \geq 1} \frac{B_{2n}}{2n(2n-1)} x^{4n-2}$$

où les nombres de Bernouilli  $B_n$  sont reliés aux polynômes de Bernouilli  $B_n(u)$  par les expressions

$$\begin{aligned} B_n(u) &= \sum_{0 \leq r \leq n} \binom{n}{r} B_r x^{n-r} \\ \frac{te^{tu}}{e^t - 1} &= \sum_{n \geq 0} B_n(u) \frac{t^n}{n!} \end{aligned}$$

de sorte que

$$\sum_{1 \leq p \leq N-1} p^k = \frac{B_{k+1}(N) - B_{k+1}}{k+1}$$

et

$$\begin{aligned} \phi(N, x) &\sim N \sum_1^{\infty} \frac{B_{2n}}{2n(2n-1)} x^{4n-2} \\ &+ \sum_{k \geq 1} (-1)^{k+1} \frac{x^{2k}}{k} \left[ \frac{N}{k+1} \sum_{r=1}^{k+1} N^r \binom{k+1}{r} B_{k+1-r} - \frac{1}{k+2} \sum_{r=1}^{k+1} N^r \binom{k+1}{r} B_{k+2-r} \right] \end{aligned}$$

Tenant compte de ce que pour  $k \geq 1$ ,  $B_{k+1}$  s'annule si  $k$  est pair, on trouve

$$\phi_1(x) = \sum_{g \geq 1} \chi(\Gamma_{g,1}) x^{4g-2} \sim - \sum_{g \geq 1} x^{4g-2} \frac{B_{2g}}{2g}$$

D'où le très remarquable

*Théorème (Harer-Zagier, Penner)*

$$\chi(\Gamma_{g,1}) = - \frac{B_{2g}}{2g} = \zeta(1-2g)$$

où  $\zeta(s)$  est la fonction  $\zeta$  de Riemann.

En poussant l'analyse, on montre que la caractéristique virtuelle de l'espace des modules de surfaces de genre  $g$  à  $n$  points marqués (non distingués) n'est autre que le coefficient de  $N^n$  dans le développement de  $\phi(N, x)$  et le calcul précédent montre que pour  $n > 0$ ,  $2g - 2 + n > 0$

$$\chi(\Gamma_{g,n}) = (-1)^{n-1} \frac{\zeta(1-2g)}{2g+n-2} \binom{2g+n-2}{n}$$

Cette formule est à prendre en un sens limite le cas échéant. Par exemple

$$g=0 \quad n=3 \quad \chi = \frac{1}{3!}$$

$$g=0 \quad n=4 \quad \chi = -\frac{1}{4!}$$

$$g=1 \quad n=1 \quad \chi = -\frac{1}{12}$$

Enfin lorsque l'expression a un sens, elle s'applique à  $\Gamma_g \equiv \Gamma_{g,0}$  sans point marqué sous la forme

$$\chi(\Gamma_g) = \frac{\chi(\Gamma_{g,1})}{2-2g} = \frac{\zeta(1-2g)}{2-2g} \quad g > 1$$

### B. Formules d'intersection

A ce jour l'application la plus remarquable des méthodes d'intégration matricielle est due à Witten et Kontsevich. Soit  $\mathcal{M}_{g,n}$  l'espace des modules des courbes de genre  $g$  à  $n$  points marqués et  $\overline{\mathcal{M}}_{g,n}$  une compactification adéquate (correspondant semble-t-il aux dégénérescences possibles des courbes projectives planes n'ayant au plus comme singularités que des points doubles à tangentes distinctes et tels que les points marqués ne viennent pas se confondre avec ces singularités). En chaque point marqué, on considère la première classe de Chern du fibre cotangent  $\mathcal{L}$  et pour une suite  $\{d_f \geq 0\}$  où  $f$  indexe les points distingués telle que

$$\sum_f d_f = 3g - 3 + n = \sum_i k_i$$

$k_i = \{\text{nombre de } d_f = i\}$

on pose

$$\langle \tau_0^{k_0} \dots \tau_i^{k_i} \dots \rangle = \int_{\mathcal{M}_{g,n}} c_1(\mathcal{L}_1)^{d_1} \dots c_1(\mathcal{L}_n)^{d_n}$$

$\mathcal{M}_{g,n}$  ayant la structure d'un quotient de l'espace de Teichmüller correspondant par le groupe modulaire, ces "nombres d'intersection" sont des rationnels, d'ailleurs positifs. Comme le montre Witten, il sont reliés par des relations triangulaires à coefficients entiers positifs (et même égaux à l'unité le long de la diagonale) aux nombres d'intersection des classes de cohomologie stables sur

$\overline{\mathcal{M}}_{g,0}$  introduites par Mumford, Morita et Miller qui s'expriment par des intégrales analogues sur  $\overline{\mathcal{M}}_{g,0}$ .

La série formelle

$$F(t.) = \ln Z(t.) = \sum_{k_0, \dots, k_i, \dots} \left\langle \exp \sum_0^\infty \tau_i t_i \right\rangle$$

est uniquement déterminée par le

**Théorème (Witten, Kontsevich)**

(i)  $Z(t.) = \exp F(t.)$  est une fonction  $\tau$  au sens de Sato pour la hiérarchie des équations du système intégrable KdV (Kortweg et de Vries), ce qui revient à dire que  $u = \frac{\partial^2 F(t.)}{\partial t_0^2}$  satisfait aux conditions

$$\frac{\partial}{\partial t_n} u = \frac{\partial}{\partial t_0} R_{n+1} \left( u, \frac{\partial u}{\partial t_0}, \dots \right)$$

où les polynômes (différentiels) de Gelfand-Dikii

$$\begin{aligned} R_1 &= u \\ R_2 &= \frac{u^2}{2} + \frac{\partial^2 u}{12 \partial t_0^2} \\ &\dots \\ R_n &= \frac{u^n}{n!} + \dots \end{aligned}$$

satisfont à la relation de récurrence

$$(2n+1) \frac{\partial}{\partial t_0} R_{n+1} = \left( \frac{1}{4} \frac{\partial^3}{\partial t_0^3} + 2u \frac{\partial}{\partial t_0} + \frac{\partial u}{\partial t_0} \right) R_n$$

(ii)  $Z(t.)$  est un vecteur de plus haut poids pour une algèbre de Virasoro. Précisément, si pour  $m$  entier supérieur ou égal à  $-1$  on définit  $((-1)!! \equiv 1)$

$$\begin{aligned} 2L_m &= \sum_{k \geq m} \frac{(2k+1)!!}{(2(k-m)-1)!!} t_{k-m} \frac{\partial}{\partial t_k} + \frac{1}{2} \sum_{k+\ell=m-1} (2k+1)!! (2\ell+1)!! \frac{\partial^2}{\partial t_k \partial t_\ell} \\ &\quad - (2m+3)!! \frac{\partial}{\partial t_{m+1}} + \frac{t_0^2}{2} \delta_{m+1,0} + \frac{1}{8} \delta_{m,0} \end{aligned}$$

où  $\delta_{m,n}$  est le symbole de Kronecker, tels que

$$[L_m, L_n] = (m-n)L_{m+n}, \quad m, n \geq -1$$

alors

$$L_m Z(t.) = 0, \quad m \geq -1$$

Les assertions assez surprenantes du théorème sont à prendre au sens des séries formelles. L'algèbre de Lie infinie dont il est question dans la seconde partie est en fait une sous algèbre de l'algèbre de Virasoro qui ne pas fait apparaître la "charge centrale" c'est-à-dire la valeur du coefficient du cocycle de l'extension centrale de l'algèbre de Lie de Diff( $S_1$ ). Enfin les conditions (i) et (ii) sont surabondantes mais bien entendu compatibles.

Ce paragraphe va être consacré à la démonstration de ce théorème.

Donnons d'abord quelques indications, hélas un peu imprécises, sur le modèle combinatoire de  $\mathcal{M}_{g,n}$  qui conduit à représenter  $Z(t.)$  à l'aide d'intégrales sur des matrices hermitiennes. Il s'agit d'une décomposition cellulaire où chaque cellule est représentée par une carte (connexe) dont les sommets sont au moins trivalents, de genre  $g$ , ayant  $n$  faces, munie d'une "métrique" qui affecte une longueur positive à chaque arête:  $a \rightarrow \ell_a$  et à chaque face  $f$  un périmètre  $p_f = \sum_{a \subset f} \ell_a$ , le symbole  $a \subset f$  désignant la relation d'incidence. On attribue à chaque cellule une dimension égale au nombre de variables  $\ell_a$  indépendantes lorsque les  $p_f$  sont fixés, c'est-à-dire  $A - F$  (où le nombre de faces  $F$  est fixé à la valeur  $n$ ). Des relations

$$A = 2g - 2 + S + F, \quad 2A \geq 3S$$

on tire

$$A - n \leq 2(3g - 3 + n)$$

où l'égalité n'a lieu que si tous les sommets sont trivalents, correspondant aux cellules de dimension maximale (=  $\dim_{\mathbb{R}} \mathcal{M}_{g,n}$ ) celles auxquelles on se borne dans la suite.

A une face orientée de valence  $k$  bordée par les arêtes  $a_1, a_2, \dots, a_k$  dans cet ordre, à permutation cyclique près, on fait alors correspondre la 2-forme

$$\omega_f = \sum_{1 \leq i < j \leq k-1} d \left( \frac{\ell_i}{p_f} \right) \wedge d \left( \frac{\ell_j}{p_f} \right)$$

invariante dans un changement d'échelle et une permutation circulaire. Kontsevich montre alors que les nombres d'intersection cherchés s'expriment dans ce modèle sous la forme

$$\langle \tau_{d_1} \dots \tau_{d_n} \rangle = \int \prod_f \omega_f^{d_f}$$

où le signe somme est à interpréter comme une intégrale sur les cellules de dimension  $6g - 6 + 2n$  et une somme sur ces cellules, c'est-à-dire des cartes connexes à sommets trivalents affectées d'un poids égal à l'inverse de l'ordre de leur groupe d'automorphisme. A vrai dire, il est difficile de dire si dans l'article original on trouve une preuve ou une assertion de ce fait (il s'agit là d'une remarque qui n'engage que les auteurs, peu versés dans la topologie). On notera en particulier qu'une orientation cohérente est requise, compatible avec celle induite par la structure complexe de  $\mathcal{M}_{g,n}$ .

Ce point, capital, étant admis, le reste n'est affaire que de calcul. On obtiendra de deux façons la quantité

$$\int_0^\infty \prod_f dp_f e^{-\lambda_f p_f} \int \frac{(\sum_f p_f^2 \omega_f)^{3g-3+n}}{(3g-3+n)!}$$

qui assigne à chaque point marqué une variable  $\lambda_f$  conjuguée du périmètre  $p_f$ . D'après l'identification précédente, ceci s'écrit

$$\sum_{d_1+\dots+d_n=3g-3+n} \langle \tau_{d_1} \dots \tau_{d_n} \rangle 2^{3g-3+n} \prod_1^n (2d_f - 1)!! \lambda_f^{-(2d_f+1)}$$

Par ailleurs au prix d'un Jacobien donné par

$$\frac{1}{(3g-3+n)!} \prod_f dp_f \left( \sum_f p_f^2 \omega_f \right)^{3g-3+n} = 2^{5g-5+2n} d\ell_1 \dots d\ell_A$$

quelle que soit la carte de genre  $g$  à  $n$  faces (à un signe près qu'il faut soigneusement déterminer), on peut intégrer directement sur les longueurs  $\ell_a$  des arêtes communes aux faces de variables  $\lambda_f$ ,  $\lambda_{f'}$  ( $a \subset f$ ,  $a \subset f'$ ) distinctes ou confondues, chacune produisant un facteur  $\frac{1}{\lambda_f + \lambda_{f'}}$ . Combinant les facteurs 2 on trouve en désignant par  $\mathcal{C}_{g,n}$  l'ensemble des cartes connexes de sommets trivalents de genre  $g$  à  $n$  faces

$$\sum_{d_1+\dots+d_n=3g-3+n} \langle \tau_{d_1} \dots \tau_{d_n} \rangle \prod_1^n \frac{(2d_f - 1)!!}{\lambda_f^{2d_f+1}} = \sum_{C \in \mathcal{C}_{g,n}} \frac{2^{-S}}{|\text{Aut } C|} \prod_a \frac{2}{\lambda_{f(a)} + \lambda_{f'(a)}}$$

où  $|\text{Aut } C|$  est l'ordre du groupe d'automorphisme de la carte  $C$  et le dernier produit est sur les arêtes de la carte.

Le membre de droite suggère une interprétation en terme du développement perturbatif d'une intégrale matricielle normalisée si l'on effectue une sommation sur tous les choix possibles des  $\lambda_f$  parmi des valeurs  $\lambda_{(0)}, \dots, \lambda_{(N-1)}$  considérées comme les valeurs propres d'une matrice hermitienne définie positive de taille  $N \times N$ . Plus précisément posons

$$t_r(\Lambda) = -(2r-1)!! \text{tr } \Lambda^{-2r-1}, \quad r \geq 0$$

avec la convention  $(-1)!! = 1$ . On a alors

$$\begin{aligned} F(t(\Lambda)) &= \sum_{n \geq 1} \frac{1}{n!} \langle \tau_{d_1} \dots \tau_{d_n} \rangle t_{d_1}(\Lambda) \dots t_{d_n}(\Lambda) \\ &= \sum_{g,n} \sum_{C \in \mathcal{C}_{g,n}} \sum_{\lambda_1 \dots \lambda_n \in \{\lambda_{(0)}, \dots, \lambda_{(N-1)}\}} \left(\frac{i}{2}\right)^S \prod_a \frac{2}{\lambda_{f(a)} + \lambda_{f'(a)}} \end{aligned}$$

où l'on a noté que  $(-)^n = i^S$ . En effet la relation  $2A = 3S$  implique  $S = 2p$  et de  $S - A + F = S - A + n = 2p - 3p + n \equiv 0 \pmod{2}$ , il s'ensuit que  $p \equiv n \pmod{2}$ .

On a alors

Proposition 1

$$\begin{aligned} F(t(\Lambda)) &= \ell_n Z_N(\Lambda) \\ Z_N(\Lambda) &= \frac{\int dM \exp - \text{tr} \left( \frac{\Lambda M^2}{2} - i \frac{M^3}{6} \right)}{\int dM \exp - \text{tr} \frac{\Lambda M^2}{2}} \end{aligned}$$

Dans cette intégrale matricielle normalisée  $dM$  est la mesure de Lebesgue sur les matrices hermitiennes  $N \times N$  invariante par l'action adjointe du groupe unitaire et l'égalité est à entendre au sens du développement perturbatif (asymptotique) qui revient à remplacer  $\exp i \text{tr} \frac{M^3}{6}$  par son développement en série de puissances.

Il est naturel d'attribuer à  $\Lambda^{-1}$  le degré 1 de sorte que si l'on introduit la mesure normalisée

$$\begin{aligned} d\mu_\Lambda(M) &= \frac{\exp - \text{tr} \frac{\Lambda M^2}{2}}{\int dM \exp - \text{tr} \frac{\Lambda M^2}{2}} \\ Z_N(\Lambda) &= \sum_{k \geq 0} Z_{N,k}(\Lambda) \\ Z_{N,k}(\Lambda) &= \frac{(-)^k}{(2k)!} \int d\mu_\Lambda(M) \left( \text{tr} \frac{M^3}{6} \right)^{2k} \end{aligned}$$

où  $Z_{N,k}(\Lambda)$  est de degré  $3k$ . Bien entendu à  $N$  fixé seules  $N$  des variables  $t_r(\Lambda)$  sont algébriquement indépendantes, cependant l'expression que nous allons trouver pour  $Z_N(\Lambda)$  montre que

Proposition 2

Exprimé en fonction des quantités  $t_r(\Lambda)$ ,  $Z_{N,k}(\Lambda)$  est indépendant de  $N$  pour  $N \geq 3k$  (et n'est fonction que de  $t_r(\Lambda)$ ,  $r \leq 3k$ ). Si on note cette quantité  $Z_{.,k}(t(\Lambda))$  on obtiendra ainsi  $Z(t.)$  sous la forme

$$Z(t.) = \sum_{k \geq 0} Z_{.,k}(t.)$$

qui ne fait plus référence à la taille des matrices.

Nous en arrivons à l'évaluation des intégrales matricielles. Pour ce faire introduisons la fonction  $z(\lambda)$  correspondant au cas  $N = 1$

$$z(\lambda) = \frac{\int_{-\infty}^{+\infty} dm e^{-\frac{\lambda m^2}{2} + i \frac{m^3}{6}}}{\int_{-\infty}^{+\infty} dm e^{-\lambda \frac{m^2}{2}}}$$

qui à  $\lambda$  grand admet le développement asymptotique

$$z(\lambda) = \sum_{k \geq 0} c_k \lambda^{-3k} \quad c_k = \left(-\frac{2}{9}\right)^k \frac{\Gamma(3k + \frac{1}{2})}{\sqrt{\pi}}$$

et satisfait à une équation différentielle équivalente à l'équation d'Airy

$$\begin{aligned} (D^2 - \lambda^2) z(\lambda) &= 0 & D &= -e^{\frac{1}{3}\lambda^3} \lambda^{1/2} \left( \frac{\partial}{\lambda \partial \lambda} \right) \lambda^{-1/2} e^{-\frac{1}{3}\lambda^3} \\ & & &= \lambda + \frac{1}{2\lambda^2} - \frac{\partial}{\lambda \partial \lambda} \end{aligned}$$

Revenant au cas général, nous pouvons exprimer  $Z_N(\Lambda)$ , au prix d'un prolongement analytique et

d'une translation de la variable au numérateur, sous la forme

$$Z_N(\Lambda) = 2^{-\frac{N(N-1)}{2}} \prod_r \lambda_r^{1/2} \prod_{r < s} (\lambda_r + \lambda_s) \exp \frac{\Lambda^3}{3} \times \tilde{Z}_N(\Lambda)$$

$$\tilde{Z}_N(\Lambda) = \int d \left( \frac{M}{(2\pi)^{1/2}} \right) \exp i \operatorname{tr} \left( \frac{M^3}{6} + \frac{M\Lambda^2}{2} \right)$$

où nous avons explicitement écrit  $dM = \prod_i dM_{ii} \prod_{i < j} d \operatorname{Re} M_{ij} d \operatorname{Im} M_{ij}$ . La dernière intégrale est invariante si on remplace  $M$  par un conjugué  $M \rightarrow U M U^{-1}$  et simultanément  $\Lambda \rightarrow U \Lambda U^{-1}$  ( $U$  unitaire) aussi pouvons nous supposer  $\Lambda$  diagonal. Cependant il reste à effectuer l'intégrale sur les "angles relatifs". Cette intégrale était obtenue dans un travail avec J.-B. Zuber, par un argument de noyau de la chaleur. Nous avons appris depuis que la même intégrale avait été considérée bien plus tôt par Harish-Chandra. Quoiqu'il en soit on trouve

$$\tilde{Z}_N(\Lambda) = \int \prod_r \frac{dm_r}{(2\pi)^{1/2}} e^{i \left( \frac{m_r^2}{6} + \frac{m_r \lambda_r^2}{2} \right)} \prod_{r < s} \left( \frac{m_r - m_s}{2} - \frac{i \lambda_r^2}{2} \right)$$

où les indices  $r$  et  $s$  varient de 0 à  $N-1$  et les  $m_r$  sont les valeurs propres de la matrice  $M$ . On emploiera dans la suite la notation de Weyl pour le déterminant

$$|f_0(\lambda), \dots, f_{N-1}(\lambda)| = \det \begin{vmatrix} f_0(\lambda_0) & \dots & f_{N-1}(\lambda_0) \\ \vdots & & \vdots \\ f_0(\lambda_{N-1}) & \dots & f_{N-1}(\lambda_{N-1}) \end{vmatrix}$$

de sorte que le déterminant de Vandermonde s'écrit

$$|m^0, m^1, \dots, m^{N-1}| = \prod_{r < s} (m_r - m_s)$$

On effectue sans peine les intégrales dans  $\tilde{Z}_N(\Lambda)$  et reportant

$$Z_N(\Lambda) = \frac{|D^0 z(\lambda), \dots, D^{N-1} z(\lambda)|}{|\lambda^0, \dots, \lambda^{N-1}|}$$

C'est de cette expression légèrement réorganisée qu'on va partir pour obtenir les propriétés cherchées. Pour cela on introduit une seconde fonction (l'équation d'Airy est du second ordre)

$$\bar{z}(\lambda) = \frac{1}{\lambda} D z = \sum_{k \geq 0} d_k \lambda^{-3k}, \quad d_k = \frac{1+6k}{1-6k} c_k$$

et on note que

$$\begin{aligned} D^{2k} z &= \lambda^{2k} z \bmod \{D^{2k-1} z, \dots, D^0 z\} \\ D^{2k+1} z &= \lambda^{2k+1} \bar{z} \bmod \{D^{2k} z, \dots, D^0 z\} \end{aligned}$$

Ainsi on peut écrire

$$Z_N(\Lambda) = \frac{|\lambda^0 z, \lambda^1 \bar{z}, \lambda^2 z, \dots|}{|\lambda^0, \lambda^1, \lambda^2, \dots, \lambda^{N-1}|}$$

où au numérateur, le dernier terme est  $\lambda^{N-1} z$  si  $N$  est impair, ou  $\lambda^{N-1} \bar{z}$  si  $N$  est pair. Factorisons au numérateur et au dénominateur le produit  $(\lambda_0, \dots, \lambda_{N-1})^{N-1}$  et développons les fonctions  $z$  et  $\bar{z}$  en puissances de

$$x \equiv \lambda^{-1}$$

Nous trouvons en définitive la série

$$Z_N(\Lambda) = \sum_{n_0, n_1, \dots, n_{N-1} \geq 0} c_{n_0}^{(0)} c_{n_1}^{(1)} \dots c_{n_{N-1}}^{(N-1)} \frac{|x^{3n_0+N-1}, x^{3n_1+N-2}, \dots, x^{3n_{N-1}}|}{|x^{N-1}, x^{N-2}, \dots, x^{N-1}|}$$

où nous adoptons la convention

$$c_n^{(2p)} = c_n, \quad c_n^{(2p+1)} = d_n$$

Nous reconnaissons dans le rapport des deux déterminants un caractère polynomial du groupe linéaire (exprimé en terme des valeurs propres d'un élément de  $GL_N$  et étendu à toute matrice en vertu de sa nature polynomiale). En général pour une matrice  $X$  (ici  $\Lambda^{-1}$ ) diagonalisable de valeurs propres  $x_0, \dots, x_{N-1}$ , nous posons

$$\operatorname{ch}_{\ell_{N-1}, \dots, \ell_0}(X) = \frac{|x^{\ell_{N-1}}, \dots, x^{\ell_0}|}{|x^{N-1}, \dots, x^0|}$$

dont l'expression polynomiale en fonction des traces des puissances de  $X$

$$\theta_k(X) = \frac{1}{k} \operatorname{tr} X^k$$

s'appelle une fonction de Schur généralisée. Notons que

$$t_r(\Lambda) = -(2r+1)!! \theta_{2r+1}(\Lambda^{-1})$$

Définissons en outre les traces des puissances symétriques de  $X$  sous la forme

$$p_k(X) = \operatorname{tr} \bigotimes_{\operatorname{sym}}^k X$$

telles que

$$\sum_{k \geq 0} u^k p_k(X) = \det(1 - uX)^{-1} = \exp \sum_{n \geq 1} u^n \theta_n(X)$$

L'égalité entre les termes extrêmes définit les polynômes de Schur que nous notons encore  $p_k(\theta)$ , polynômes dans des variables  $\{\theta_1, \theta_2, \dots\}$

$$p_k(\theta) = \sum_{r \geq 1} \sum_{\nu_r = k} \frac{\theta_1^{\nu_1} \theta_2^{\nu_2} \dots}{\nu_1! \nu_2! \dots}, \quad p_0(\theta) = 1$$

Ces polynômes, comme le remarque Sato, jouissent de la propriété fondamentale

$$\frac{\partial p_k(\theta)}{\partial \theta_r} = \frac{\partial^r}{\partial \theta_1^r} p_k(\theta) = p_{k-r}(\theta)$$

où nous convenons que  $p_k(\theta)$  s'annule si son indice est négatif. Un calcul classique fondé sur la formule déterminantale de Cauchy permet alors d'exprimer les  $\operatorname{ch}$  en fonction des  $p$  sous la forme

$$\operatorname{ch}_{N-1+f_0, N-2+f_1, \dots, f_{N-1}} = \begin{vmatrix} p_{f_0} & & & \\ & p_{f_1} & & * \\ & & \ddots & \\ * & & & p_{f_{N-1}} \end{vmatrix}$$

où la notation symbolique implique que les indices croissent (décroissent) d'une unité à chaque déplacement vers la droite (gauche).

On en conclut que  $Z_N(\Lambda)$  admet un développement en termes de traces des puissances de  $\Lambda^{-1}$  de la forme

$$Z_N(\Lambda) = \sum_{n_0, \dots, n_{N-1} \geq 0} c_{n_0}^{(0)} c_{n_1}^{(1)} \dots c_{n_{N-1}}^{(N-1)} \begin{vmatrix} p_{3n_0} & & & \\ & \ddots & & * \\ * & & & p_{3n_{N-1}} \end{vmatrix} (\theta, (\Lambda^{-1}))$$



où les termes de degré  $k$ ,  $Z_{N,k}$ , sont obtenus en restreignant la somme par la condition  $n_0 + n_1 + \dots + n_{N-1} = k$ . La proposition 2 triviale pour  $k = 0$  ( $Z_{N,0} = 1$ ) en résulte si on suppose  $0 < 3k \leq N$ . Considérons dans  $Z_{N,k}$  un terme tel que  $\delta$  soit le plus petit entier satisfaisant  $r \geq \delta \rightarrow n_r = 0$ . On peut alors restreindre le déterminant correspondant à la taille  $\delta \times \delta$ , les indices des  $p$ . de la dernière colonne étant donnés par la suite  $3n_0 + \delta - 1, 3n_1 + \delta - 2, \dots, 3n_{\delta}$  dont la somme est  $3k + \sum_0^{\delta-1} r$ . Si  $\delta > 3k$  cette somme de  $\delta$  entiers positifs est inférieure à celle des  $\delta$  premiers entiers positifs: deux d'entre eux doivent donc être égaux, le déterminant s'annule et le premier correspondant est donc nul. On en conclut que pour tout terme qui contribue à  $Z$  a une "profondeur"  $\delta \leq 3k$  ce qui prouve que  $N \geq 3k \Rightarrow Z_{N,k} = Z_{3k,k} = Z_{.k}$  où à l'évidence lorsqu'on a pris les  $\theta$ . comme variables, ce terme est indépendant de  $N$  ce qu'affirme la proposition.

En outre en posant  $Z(\theta.) = \sum_{k \geq 0} Z_{.k}(\theta.)$  on peut présenter cette série comme

$$Z(\theta.) = \sum_{i \geq 0} \prod_{n_i < \infty} c_{n_i}^{(i)} \begin{vmatrix} p_{3n_0} & & * \\ & p_{3n_1} & \\ * & & \ddots \end{vmatrix} (\theta.)$$

Les déterminants, d'apparence infinie, se réduisent à des déterminants finis puisque pour presque tout  $i$ ,  $n_i = 0$  et que dans ces conditions la profondeur  $\delta$  d'un terme donné est finie ce qui implique que le déterminant peut être restreint à la taille finie  $\delta \times \delta$ .

L'expression de la série asymptotique ainsi obtenue permet de comprendre qu'elle est indépendante des variables d'indice pair comme il se doit d'après la construction initiale. En effet dérivons  $Z$  par rapport à  $\theta_{2p}$  ce qui revient à dériver successivement chaque ligne des déterminants. Or en dérivant la ligne d'indice  $r$ , en vertu de la propriété fondamentale des polynômes de Schur on substitue à

$$p_{3n_r-r}, p_{3n_r-r+1}, \dots, p_{3n_r}, p_{3n_r+1}, \dots$$

la suite

$$p_{3n_r-r-2p}, p_{3n_r-r+1-2p}, \dots, p_{3n_r-2p}, p_{3n_r+1-2p}, \dots$$

qui s'identifie à la ligne  $r + 2p$  à l'échange près de  $n_r$  avec  $n_{r-2p}$ . Dans cet échange le déterminant où l'on a dérivé la ligne  $r$  est impair tandis que son coefficient est pair en vertu de  $c_n^{(i)} = c_n^{(i+2p)}$  par définition. En conclusion

$$\frac{\partial}{\partial \theta_{2p}} Z(\theta.) = 0$$

On peut donc bien prendre comme variables les quantités  $t_r = -(2r+1)!! \theta_{2r+1}$ . Cependant pour la simplicité des expressions qui vont suivre, nous conservons la notation  $\theta$ .

Nous sommes maintenant en mesure de passer à la preuve du théorème. Puisque le passage à la limite  $N \rightarrow \infty$  ne présente aucune difficulté dans la série asymptotique quand on a fait choix des variables  $\theta. (\Lambda^{-1})$ , il est plus commode de revenir au cas  $N$  fini, quitte à faire tendre  $N \rightarrow \infty$  dans la suite. Observons qu'on peut récrire  $Z_N$  sous la forme d'un Wronskien. Posant

$$f_s(\theta.) = \sum_{n \geq 0} c_n^{(N-s-1)} p_{3n+s}(\theta.), \quad 0 \leq s \leq N-1$$

on a en effet

$$Z_N(\theta.) = \begin{vmatrix} \frac{\partial^{N-1}}{\partial \theta_1^{N-1}} f_{N-1} & \dots & \frac{\partial}{\partial \theta_1} f_{N-1} & f_{N-1} \\ \vdots & & \vdots & \vdots \\ \frac{\partial^{N-1}}{\partial \theta_1^{N-1}} f_0 & \dots & \frac{\partial}{\partial \theta_1} f_0 & f_0 \end{vmatrix} (\theta.)$$

où nous considérons les  $\theta$ . comme indépendants (à la vérité  $Z_N(\Lambda) \equiv Z_N(\theta. (\Lambda^{-1}))$ ). Cette expression suggère la considération d'un opérateur différentiel linéaire associé dont les solutions linéairement indépendantes sont les  $f_s(\theta.)$  en particulierisant la variable  $\theta_1$ . On pose  $d \equiv \frac{\partial}{\partial \theta_1}$  et on définit cet opérateur  $\Delta_N$  par

$$\Delta_N F = \sum_{0 \leq r \leq N} w_r(\theta.) d^{N-r} F = Z_N^{-1} \begin{vmatrix} d^N F & \dots & F \\ d^N f_{N-1} & \dots & f_{N-1} \\ \vdots & & \vdots \\ d^N f_0 & \dots & f_0 \end{vmatrix}$$

En toute rigueur les coefficients  $w_r(\theta.)$  devraient aussi porter l'indice  $N$  ( $w_0(\theta.) \equiv 1$ ) mais comme on s'en convaincra sans peine à  $r$  fixé et  $N$  assez grand  $w_r(\theta.)$  est indépendant de  $N$ . Il est commode en suivant Sato de remplacer l'opérateur différentiel  $\Delta_N$  par un opérateur pseudo-différentiel équivalent

$$\begin{aligned} \Delta_N &= W_N d^N \\ W_N &= \sum_{0 \leq r \leq N} w_r(\theta.) d^{-r} \end{aligned}$$

Nous n'utiliserons ici que les propriétés algébriques des opérateurs pseudo-différentiels. Ces derniers ont une longue histoire qui remonte au moins à la fin du siècle dernier. Pour un exposé on pourra consulter Gelfand-Dikii. Il nous suffit de mentionner l'extension de la règle de Leibniz. Notant  $a^{(k)}$  la  $k$ -ième dérivée d'une fonction  $a^{(0)} = a$ ,  $a^{(k)} = [d, a^{(k-1)}]$  on a

$$\begin{aligned} d^{-r} a &= \sum_{k \geq 0} (-)^k \binom{r+k-1}{k} a^{(k)} d^{-r-k} \\ a d^{-r} &= \sum_{k \geq 0} \binom{r+k-1}{k} d^{-r-k} a^{(k)} \end{aligned}$$

Désormais nous nous permettons d'être cavalier avec la limite  $N \rightarrow \infty$  et nous omettrons l'indice  $N$ . L'expression de  $\Delta$  nous fournit les coefficients  $w_r(\theta.)$  et on constate sans peine que

$$\begin{aligned} w_0(\theta.) &= 1 \\ w_1(\theta.) &= Z^{-1} \left( -\frac{\partial Z}{\partial \theta_1} \right) \end{aligned}$$

résultat bien connu. Plus généralement on peut écrire

$$w_r(\theta.) = \frac{1}{Z} \left( p_r \left( -\frac{\partial}{\partial \theta} \right) Z \right)$$

où pour faire bref on a noté

$$\frac{\partial}{\partial \theta} \equiv \frac{\partial}{\partial \theta_1}, \frac{1}{2} \frac{\partial}{\partial \theta_2}, \dots, \frac{1}{k} \frac{\partial}{\partial \theta_k}, \dots$$

L'opérateur inverse  $W^{-1}$  (au sens formel) est donné par des formules analogues que l'on trouve en manipulant les identités de Plücker

$$\begin{aligned} W^{-1} &= \sum_{r \geq 0} d^{-r} w_r^*(\theta.) \\ w_r^*(\theta.) &= Z^{-1} \left( p_r \left( \frac{\partial}{\partial \theta} \right) Z \right) \end{aligned}$$

Revenons à l'opérateur différentiel  $\Delta_N$  d'ordre  $N$  et différencions le par rapport à  $\theta_n$  pour  $n \ll N$ . Il existe alors un opérateur différentiel d'ordre  $n$  soit  $Q_n$  uniquement déterminé par la relation

$$\frac{\partial \Delta_N}{\partial \theta_n} = Q_n \Delta_N - \Delta_N d^n$$

En effet puisque le membre de gauche est d'ordre au plus  $N - 1$  tandis que celui de droite semble a priori d'ordre  $N + n$ , on en déduit que

$$Q_n = (\Delta_N d^n \Delta_N^{-1})_+ = (W_N d^n W_N^{-1})_+$$

où pour un opérateur pseudo différentiel  $P$  le symbole  $(P)_+$  désigne sa partie différentielle, et dans cette relation on peut passer à la limite  $N \rightarrow \infty$ .

L'opérateur  $Q_n$  étant ainsi choisi, ce qui assure que la combinaison  $Q_n \Delta_N - \Delta_N d^n$  est d'ordre inférieur à  $N$  montrons qu'elle s'identifie à  $\frac{\partial \Delta_N}{\partial \theta_n}$ . Pour ce faire il suffit donc d'établir que ces deux opérateurs ont la même action sur  $N$  fonctions linéairement indépendantes par exemple  $f_0, \dots, f_{N-1}$  qui engendrent le noyau de  $\Delta_N$ , ou encore sur  $f$ , une combinaison linéaire à coefficients constants de ces fonctions, telle donc que  $\Delta_N f = 0$ . L'égalité annoncée sera établie si l'on montre que

$$\frac{\partial \Delta_N}{\partial \theta_n} \cdot f + \Delta_N \frac{\partial f}{\partial \theta_n} = 0$$

Or  $f$ , qui admet un développement en polynômes de Schur, satisfait comme ces derniers à  $\frac{\partial f}{\partial \theta_n} = \frac{\partial f}{\partial \theta_n}$ , et le membre de gauche n'est autre que  $\frac{\partial}{\partial \theta_n} (\Delta_N f) = 0$ .

En récrivant

$$\begin{aligned} Q_n &= (W d^n W^{-1})_+ = (L^n)_+ \\ L &= W d W^{-1} = d + O(d^{-1}) \end{aligned}$$

les relations précédentes peuvent encore se récrire

$$\frac{\partial L}{\partial \theta_n} = [Q_n, L]$$

dont la compatibilité implique les conditions d'intégrabilité

$$\frac{\partial Q_m}{\partial \theta_n} - \frac{\partial Q_n}{\partial \theta_m} + [Q_m, Q_n] = 0$$

C'est là qu'on peut faire intervenir le fait que toutes les quantités introduites jusqu'ici sont indépendantes des  $\theta$ , d'indice pair. Par exemple si

$$u = \frac{\partial^2}{\partial \theta_1^2} \ln Z = \frac{\partial^2}{\partial t_0} \ln Z$$

on trouve

$$\begin{aligned} Q_2 &= d^2 + 2u \\ Q_3 &= d^3 + \frac{3}{2}(ud + du) = (Q_2^{3/2})_+ \end{aligned}$$

tandis que l'indépendance de  $u$  par rapport à  $\theta_2$  entraîne

$$\frac{\partial Q_2}{\partial \theta_3} = [Q_3, Q_2]$$

soit traduit dans les variables  $t_0, t_1$  la première des équations de la hiérarchie KdV

$$\frac{\partial u}{\partial t_1} = \frac{\partial}{\partial t_0} \left( \frac{1}{12} \frac{\partial^2 u}{\partial t_0^2} + \frac{1}{2} u^2 \right)$$

Plus généralement on montre que  $Q_n = (Q_2^{n/2})_+$  et donc

$$\frac{\partial}{\partial \theta_{2p+1}} Q_2 = \left[ (Q_2^{p+\frac{1}{2}})_+, Q_2 \right], \quad p \geq 1$$

qui est une forme concise de résumer la première partie du théorème.

On a déjà fait allusion à la fonction d'Airy et  $Z_N$  en est une version à argument matriciel. L'analogie de l'équation différentielle d'Airy va fournir la preuve de la seconde partie du théorème. En effet rappelons qu'on a écrit pour  $\Lambda$  diagonal

$$Z_N(\Lambda) = A(\Lambda) \tilde{Z}_N(\Lambda)$$

où

$$\tilde{Z}_N(\Lambda) = \int d \left( \frac{M}{(2\pi)^{1/2}} \right) \exp i \operatorname{tr} \left( \frac{M^3}{6} + \Lambda^2 \frac{M}{2} \right)$$

et  $A(\Lambda)$  est donné explicitement ci-dessus. En écrivant que l'intégrale de la dérivée du poids exponentiel par rapport à élément diagonal de  $M$  s'annule, on obtient les relations

$$0 = \left\langle \lambda_k^2 + M_{kk}^2 + \sum_{\ell, \ell \neq k} M_{k\ell} M_{\ell k} \right\rangle$$

où les crochets désignent l'intégration avec le poids

$$d \left( \frac{M}{2\pi} \right) \exp i \operatorname{tr} \left( \frac{M^3}{6} + \frac{\Lambda^2 M}{2} \right)$$

Le terme  $\langle \lambda_k^2 + M_{kk}^2 \rangle$  peut s'interpréter comme  $\left\langle \lambda_k^2 + \left( \frac{1}{i\lambda_k} \frac{\partial}{\partial \lambda_k} \right)^2 \right\rangle \tilde{Z}_N(\Lambda)$ . Pour les termes restant on exprime l'invariance de l'intégrale sous l'effet d'un changement infinitésimal de variable

$$M \rightarrow M + i\epsilon [X(M), M]$$

où

$$X(M)_{ab} = \delta_{ak} \delta_{bl} M_{kl}$$

de Jacobien  $1 + i\epsilon (M_{\ell\ell} - M_{kk})$  au premier ordre en  $\epsilon$ . Ceci fournit la relation

$$0 = \left\langle M_{\ell\ell} - M_{kk} - \frac{i}{2} (\lambda_k^2 - \lambda_\ell^2) M_{k\ell} M_{\ell k} \right\rangle$$

et conduit à récrire les équations précédentes

$$0 = \left\langle \lambda_k^2 + M_{kk}^2 - 2i \sum_{\ell, \ell \neq k} \frac{M_{kk} - M_{\ell\ell}}{\lambda_k^2 - \lambda_\ell^2} \right\rangle$$

soit un ensemble d'équations du second ordre couplées

$$\left\{ \lambda_k^2 - \left( \frac{1}{\lambda_k} \frac{\partial}{\partial \lambda_k} \right)^2 - 2 \sum_{\ell, \ell \neq k} \frac{1}{\lambda_k^2 - \lambda_\ell^2} \left( \frac{1}{\lambda_k} \frac{\partial}{\partial \lambda_k} - \frac{1}{\lambda_\ell} \frac{\partial}{\partial \lambda_\ell} \right) \right\} \tilde{Z}_N(\Lambda) = 0$$

Transformant ces équations en équations pour  $Z_N(\Lambda)$  à l'aide du facteur  $A$  explicite, développant en  $\lambda_k^{-1}$  à  $\lambda_k \rightarrow \infty$ , faisant tendre  $N \rightarrow \infty$ , on trouve la série

$$\sum_{m \geq -1} \frac{1}{(\lambda_k^2)^{2m+1}} L_m Z(t.) = 0$$

où les opérateurs  $L_m$  ont la forme indiquée dans l'énoncé du théorème. Bien entendu la relation précédente conduit à annuler séparément chaque coefficient  $L_m Z(t.)$  achevant la démonstration (on vérifie sans peine les règles de commutation des  $L_m$ ).

Il nous reste à conclure par quelques calculs effectifs de nombres d'intersection. Pour cela il est commode de développer  $\log Z = F = \sum_{g \geq 0} F_g$ , en contributions de genre donné. De même

$$u = \frac{\partial^2 F}{\partial t_0^2} = \sum_{g \geq 0} u_g$$

Posons

$$I_k(x, t.) = \sum_{p \geq 0} t_{k+p} \frac{x^p}{p!}$$

Appliquant la définition de  $F_g$  et le théorème de Witten et Kontsevich on trouve que  $u_0(t)$  est déterminée par l'équation de point fixe

$$u_0(t) = I_0(u_0, t)$$

Par inversion de Lagrange on obtient  $u_0$  puis par une double intégration  $F_0$ , ce qui fournit en genre zéro les nombres d'intersection

$$\langle \tau_{d_1} \dots \tau_{d_n} \rangle = \frac{(\sum d_i)!}{d_1! \dots d_n!}, \quad \sum_{1 \leq i \leq n} d_i = n - 3$$

qui sont dans ce cas des entiers positifs. Posant désormais

$$J_k(t) = I_k(u_0(t), t)$$

on obtient en genre 1

$$F_1(t) = \frac{1}{24} \ell_n \frac{1}{1 - J_1(t)} = \frac{1}{24} \ell_n \left( \frac{\partial u_0}{\partial t_0} \right)$$

Plus généralement si  $g > 1$  on trouve que  $F_g$  est donnée par une somme finie

$$F_g = \sum_{\sum_{2 \leq k \leq 2g-2} (k-1)\ell_k = 3g-3} \left\langle \tau_2^{\ell_2} \dots \tau_{3g-2}^{\ell_{3g-2}} \right\rangle \times \frac{1}{(1 - J_1)^{2(g-1) + \sum \ell_p}} \frac{J_2^{\ell_2} J_3^{\ell_3} \dots J_{3g-2}^{\ell_{3g-2}}}{\ell_2! \ell_3! \dots \ell_{3g-2}!}$$

où les coefficients sont eux mêmes des nombres d'intersection de genre  $g$ , déterminés par le théorème. Par exemple

$$F_2 = \frac{1}{5760} \left[ \frac{5J_4}{(1 - J_1)^3} + 29 \frac{J_2 J_3}{(1 - J_1)^4} + 28 \frac{J_2^3}{(1 - J_1)^5} \right]$$

d'où

$$\langle \tau_4 \rangle = \frac{1}{1152}, \quad \langle \tau_2 \tau_3 \rangle = \frac{29}{5760}, \quad \langle \tau_2^3 \rangle = \frac{7}{240}$$

et ainsi de suite. De même on peut resommer les termes ayant au dénominateur la plus grande puissance de  $1 - J_1$  à l'aide d'une équation de Painlevé, puis successivement ceux impliquant une puissance inférieure par une méthode perturbative.

Citons encore la propriété suivante des intégrales de Kontsevich, conjecturée initialement par Witten

**Théorème (Witten, DF-I-Z).** Il existe une application biunivoque  $\varphi$  des polynômes dans une infinité de variables

$$P \longleftrightarrow \varphi P$$

telle que

$$\frac{\int dM \exp \operatorname{tr} \left\{ i \frac{M^3}{6} - \frac{\Lambda M^2}{2} \right\} P(\operatorname{tr} M, \operatorname{tr} M^3, \operatorname{tr} M^5, \dots)}{\int dM \exp - \operatorname{tr} \frac{\Lambda M^2}{2}} = \varphi P \left( \frac{\partial}{\partial t_0}, \frac{\partial}{\partial t_1}, \dots \right) Z(t)$$

où  $t \equiv t. (\Lambda^{-1})$  et le membre de gauche doit être entendu au sens des séries formelles dans la limite  $N \rightarrow \infty$ .

Mentionnons enfin qu'il existe une généralisation du problème d'intersection impliquant des recouvrements finis des espaces de module où l'algèbre de Virasoro apparaît comme sous-algèbre de structures plus complexes appelées (par les physiciens) algèbres- $W$ .

## REFERENCES

Pour la première partie:

Yu.I. Manin, "Reflections on arithmetical Physics" in "Conformal Invariance and String Theory" Academic Press, N.Y. (1989), pages 293-303.

A. Grothendieck, "Esquisse d'un Programme"

G.V. Belyi, "On Galois Extensions of a Maximal Cyclotomic Field" *Math. USSR Izvestija* Vol.14 (1980) 247-256.

V.A. Voevodsky and G. Shabat, "Equilateral Triangulations of Riemann Surfaces and Curves over Algebraic Number Fields" *Soviet Math. Dokl.* **39** (1989) 38-41.

G.B. Shabat and V.A. Voevodsky, "Drawing Curves over Number Fields" in "A Grothendieck Festschrift" Birkhäuser.

Dirk-Jan Smit, "Summations over Equilaterally Triangulated Surfaces and the Critical String Measure" *Comm. Math. Phys.* **143** (1992) 253-285.

Marston Conder, "Hurwitz Groups: A Brief Survey", *Bulletin Am. Math. Soc.* (New series) **23** (1990) 359-370.

H.S.M. Coxeter, W.O.J. Moser, "Generators and Relations for Discrete Groups" (second edition) Springer (1965) Chap.8.

J.P. Serre,

"Groupes de Galois sur  $\mathbb{Q}$ ", Séminaire Bourbaki, Astérisque **161-162** (1988) 73-85;

"Représentations Linéaires des Groupes Finis", Hermann, Paris (1967).

T.L. Saaty, P.C. Kainen, "The Four Colour Problem" Mc Graw Hill, New York (1977).

G. Ringel, "Map Color Theorem" Springer New York (1974).

J. Wolfart, "Mirror Invariant Triangulations of Riemann Surfaces, Triangle Groups and Grothendieck Dessins: Variations on a Thema of Belyi" *Mathematisches Seminar der Universität, Frankfurt* (1992).

D. Mumford,

"Towards an Enumerative Geometry of the Moduli Space of Curves" in *Arithmetics and Geometry Vol.II*, Birkhäuser, Boston (1983).

"Galois Groups over  $\mathbb{Q}$ ", édité par J.P. Serre et Y. Ihara, *Publ. MSRI* n°16 (1989) Springer.

Y. Ihara, "Braids, Galois Groups, and Some Arithmetic Functions", *Proceedings of the International Congress of Mathematicians, Kyoto* (1990) 99, 120.

J. Oesterlé, contribution au Colloque en hommage à P. Cartier, 54<sup>ème</sup> Rencontre de Strasbourg (1992).

Pour la seconde partie:

J. Harer, D. Zagier, "The Euler Characteristic of the Moduli Space of Curves", *Inv. Math.* **85** (1986) 457-485.

D. Bessis, C. Itzykson, J.-B. Zuber, "Quantum Field Theory Techniques in Graphical Enumeration", *Adv. Appl. Math.* **1** (1980) 109-157.

C. Itzykson, J.-B. Zuber, "The Planar Approximation II", *J. Math. Phys.* **21** (1980) 411-421.

Harish-Chandra, "Differential Operators on a Semi-Simple Lie Algebra", *Am. J. Math.* **79** (1957) 87-120.

R.C. Penner, "The Decorated Teichmüller Space of Punctured Surfaces" *Comm. Math. Phys.* **113** (1987) 299-339.  
 "Perturbative Series and the Moduli Space of Punctured Surfaces", *J. Diff. Geom.* **27** (1988) 35-53.

E. Witten, "Two Dimensional Gravity and Intersection Theory on Moduli Space" *Surveys in Diff. Geom.* **1** (1991) 243-310.  
 "The N-Matrix Model and Gauged WZW Models" prétirage IAS, HEP-91/26

M. Kontsevich, "Intersection Theory on the Moduli Space of Curves" *Funct. Anal. and Appl.* **25** (1991) 123-128.  
 "Intersection Theory on the Moduli Space of Curves and the Matrix Airy Function", *Comm. Math. Phys.* **147** (1992) 1-23.

M. Sato, "Soliton Equations as Dynamical Systems on an Infinite Dimensional Grassmann Manifold" *RIMS Kokyuroku* **439** (1981) 30-46.  
 "The KP Hierarchy and Infinite Dimensional Grassmann Manifolds" *Proc. Symp. Pure Math.* **49** (1989) 51-66.

M. Sato, Y. Sato, "Soliton Equations as Dynamical Systems on an Infinite Dimensional Grassmann Manifold" *Lecture Notes in Num. Appl. Anal.* **5** (1982) 259-271.

I.M. Gelfand, L.A. Dikii, "Asymptotic Behaviour of the Resolvent of Sturm-Liouville Equations and the Algebra of the Korteweg-De Vries Equations", *Russian Math. Surveys* **30** (1975) 77-113.

C. Itzykson, J.-B. Zuber, "Matrix Integration and Combinatorics of Modular Groups" *Comm. Math. Phys.* **134** (1990) 197-207.  
 "Combinatorics of the Modular Group II, the Kontsevich Integrals", *Int. Journ. Mod. Phys.* **A7** (1992) 5661-5705.

P. Di Francesco, C. Itzykson, J.-B. Zuber, "Polynomial Averages in the Kontsevich Model" *Comm. Math. Phys.* **151** (1993) 193-219.

LEGENDES DES FIGURES

- Figure 1: Conventions graphiques.  
 Figure 2: Cartes correspondant au groupe affine sur  $\mathbb{F}_5$  (a) ou  $\mathbb{F}_7$  (b).  
 Figure 3: Carte régulière de groupe cartographique  $S_4$  (cube ou octaèdre).  
 Figure 4: Le symbole féminin et ses deux conjugués.  
 Figure 5: a - Le symbole féminin comme image inverse de l'application de Belyi; b-c - les conjugués du précédent.  
 Figure 6: a - La triangulation d'un tore considérée par Shabat et Voevodsky; b - la triangulation conjuguée.  
 Figure 7: a et b - L'image réciproque du segment [01] par l'application de Belyi dans l'exemple de Shabat et Voevodsky dans la variable  $z$ .  
 Figure 8: La triangulation de Shabat et Voevodsky relevée sur le recouvrement universel (a:  $k = -\sqrt{7}$ , b:  $k = +\sqrt{7}$ ).  
 Figure 9: Le dessin d'enfant "guillotiné".

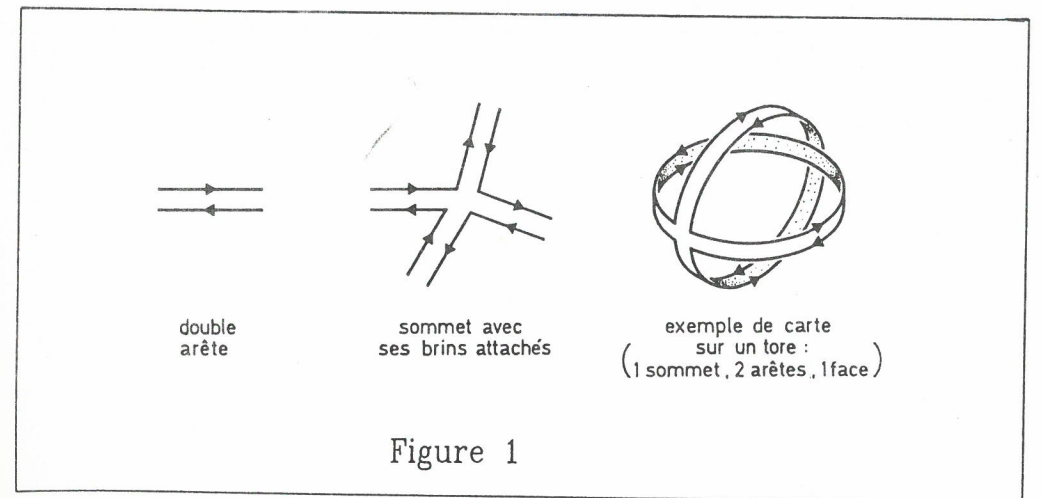


Figure 1

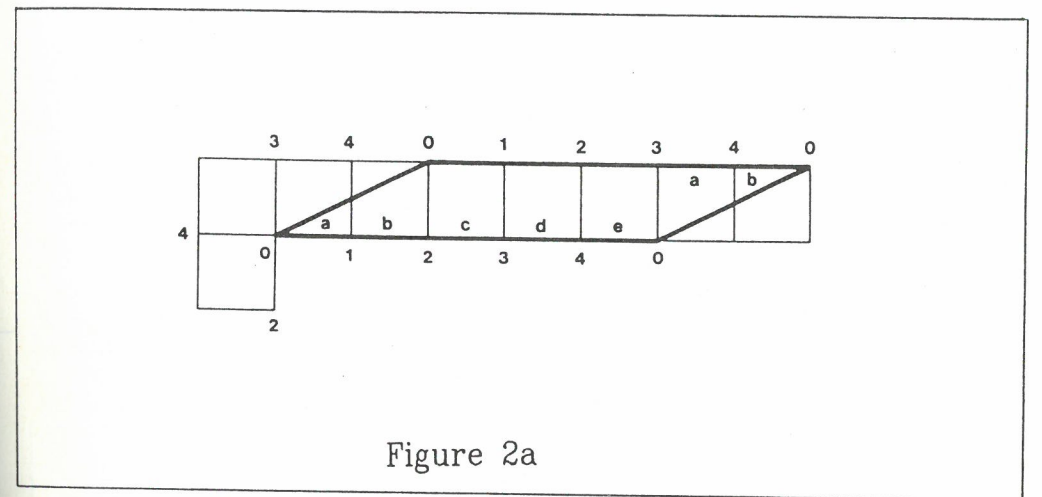


Figure 2a

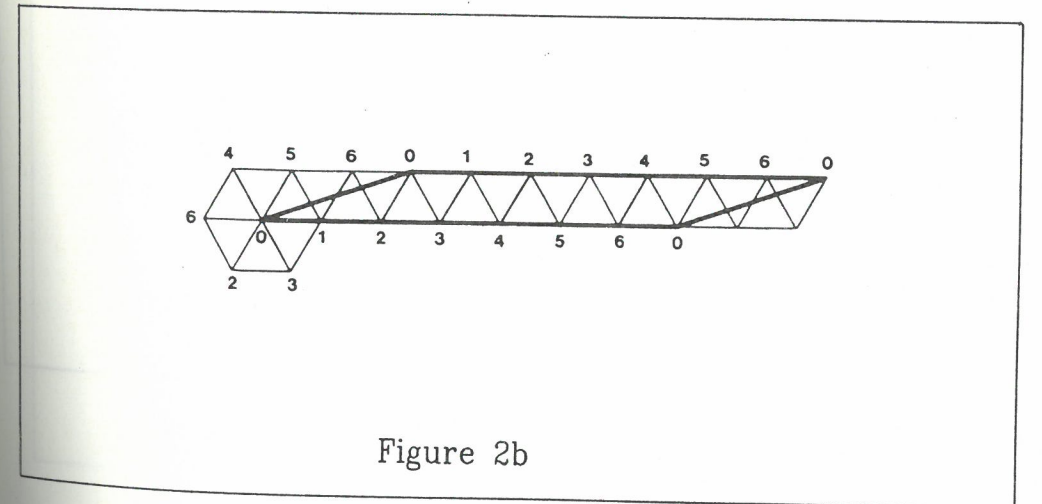


Figure 2b

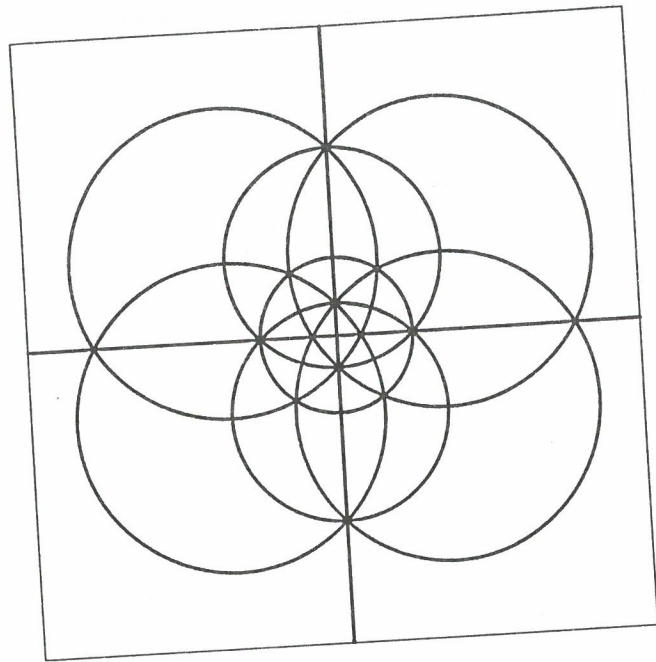


Figure 3

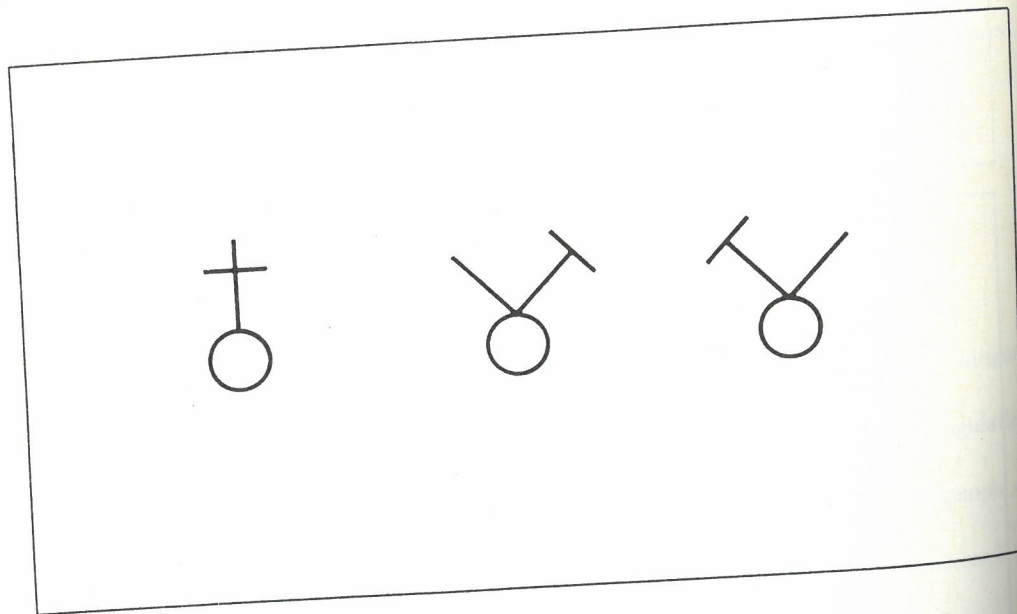


Figure 4

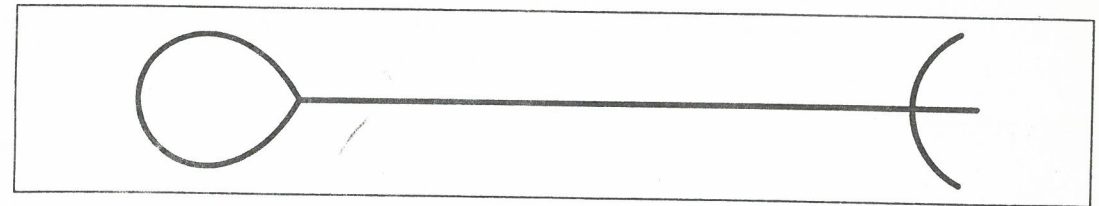


Figure 5a

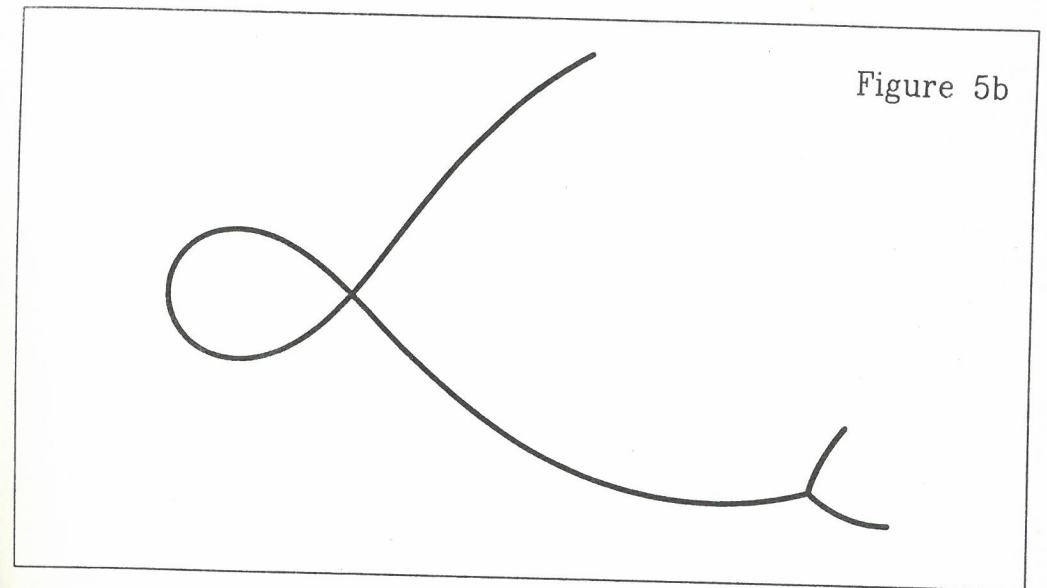


Figure 5b

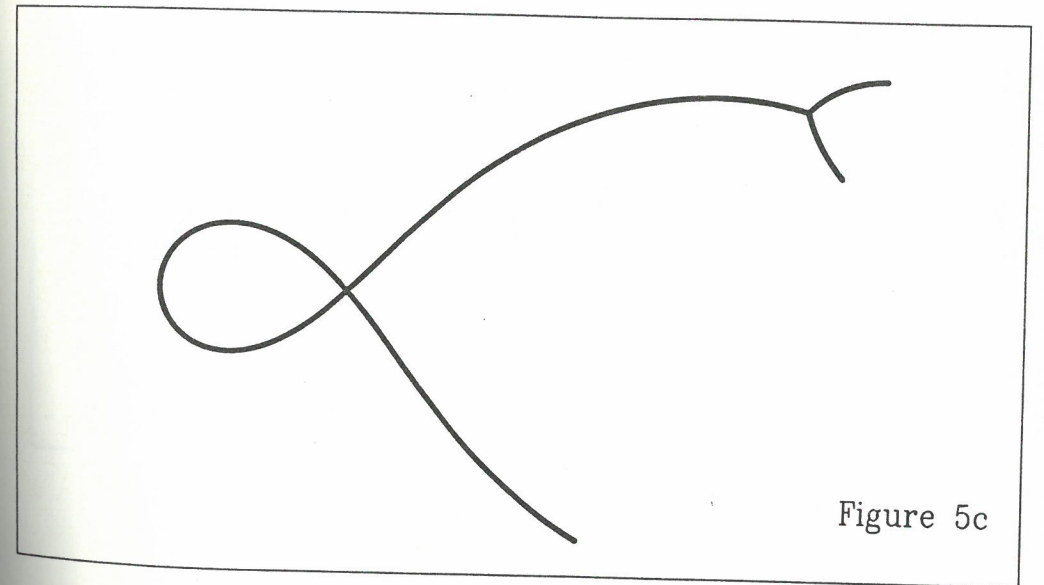


Figure 5c

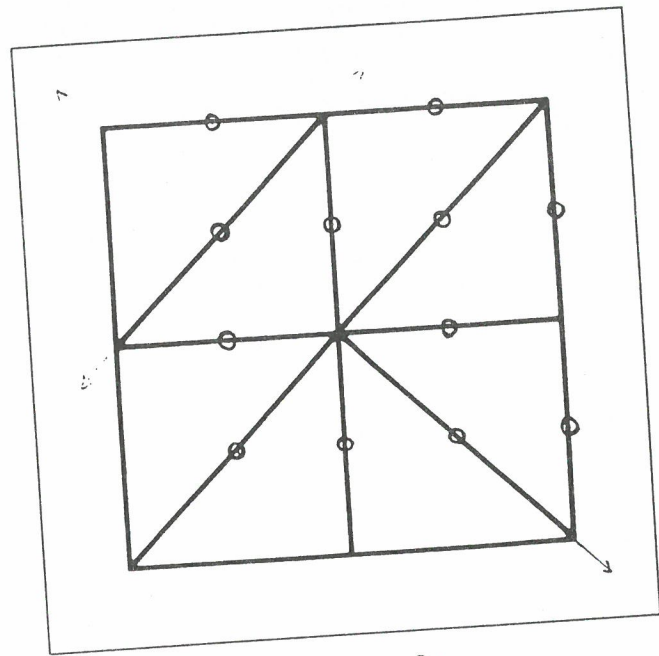


Figure 6a

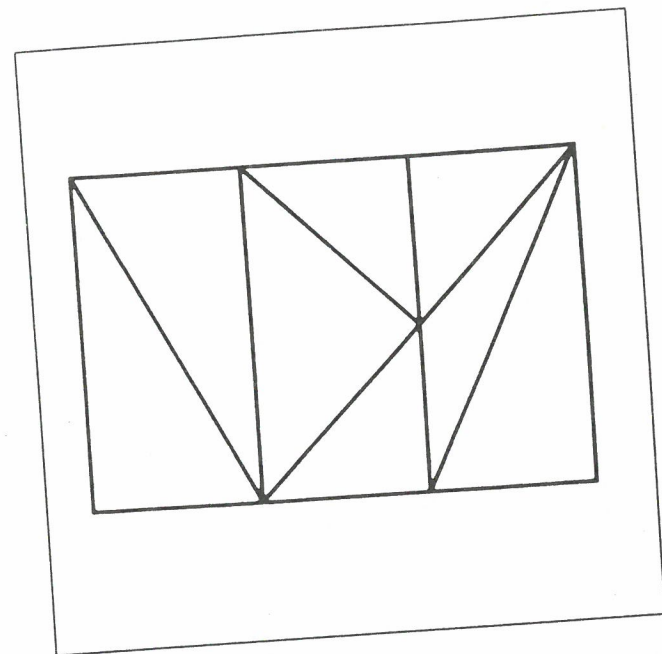


Figure 6b

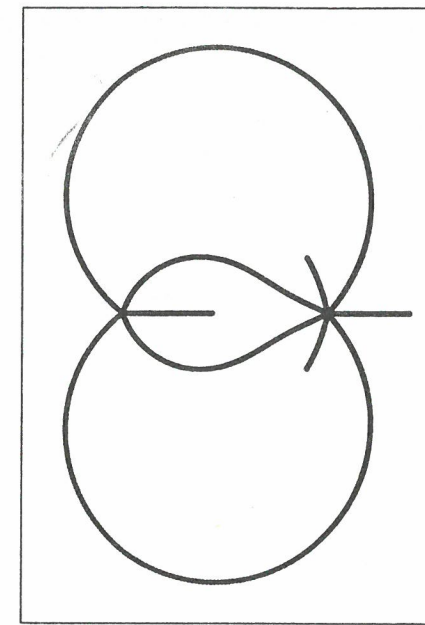


Figure 7a

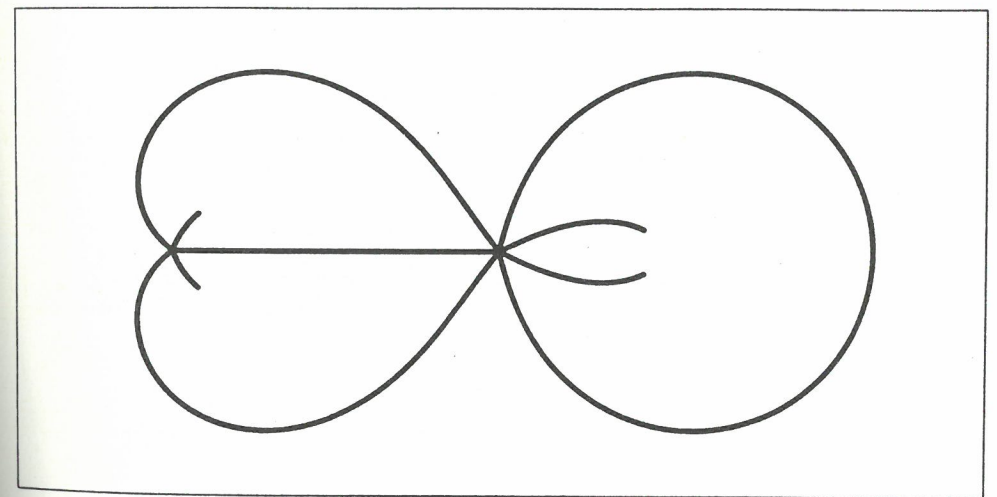


Figure 7b

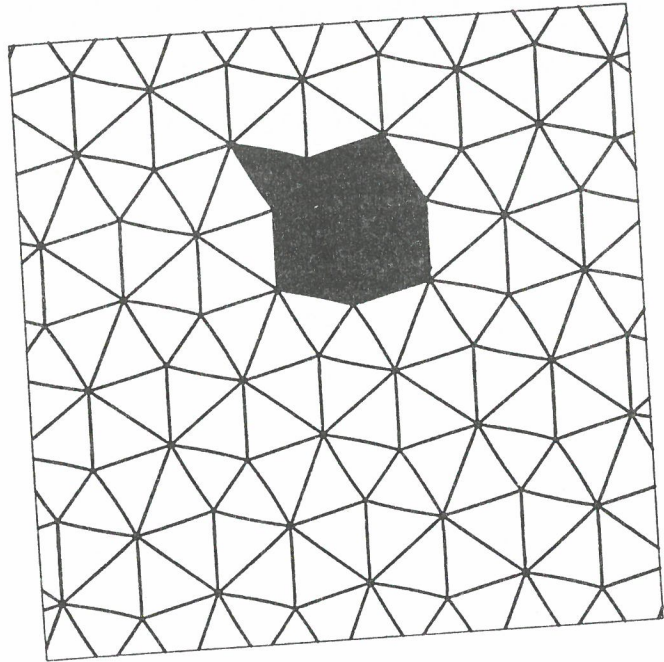


Figure 8a

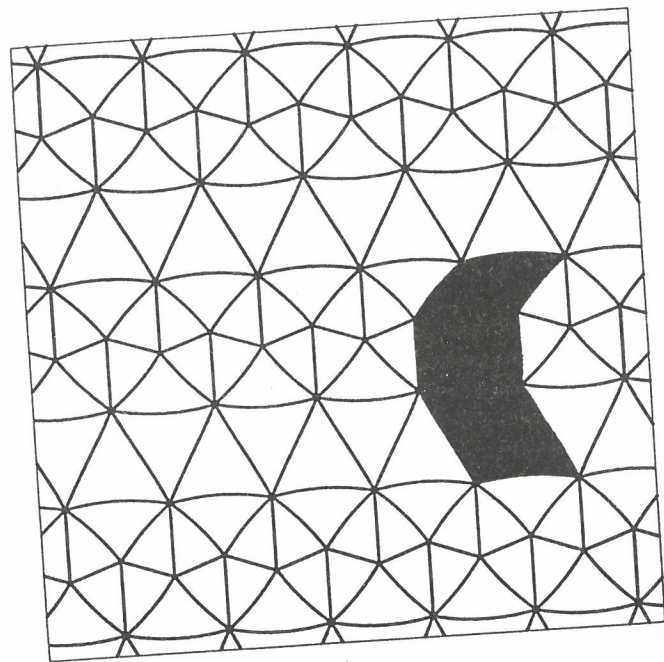


Figure 8b

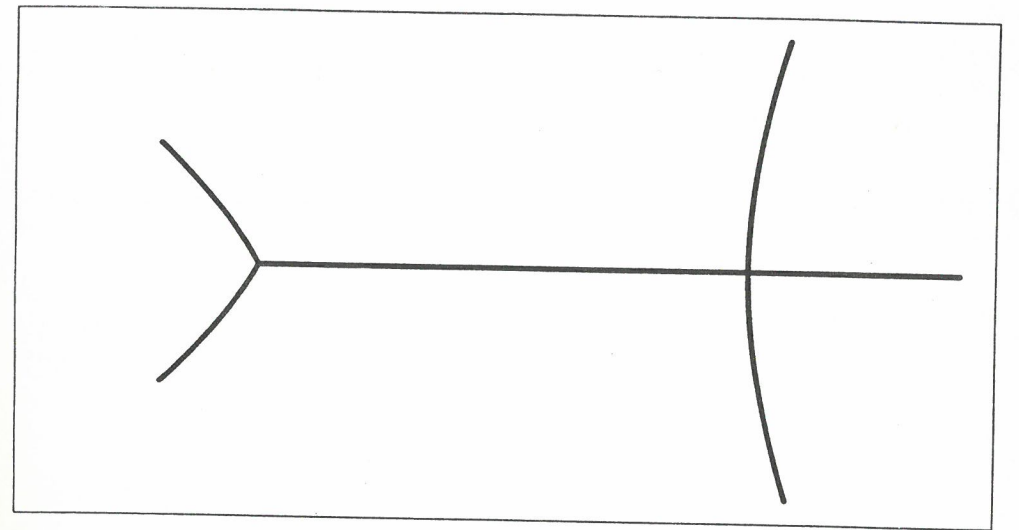


Figure 9