Astérisque

JOSEPH OESTERLÉ

Dessins d'enfants

Astérisque, tome 290 (2003), Séminaire Bourbaki,
exp. n° 907, p. 285-305

<http://www.numdam.org/item?id=SB_2001-2002__44__285_0>

Séminaire BOURBAKI Juin 2002
54e année, 2001-2002, nº 907, p. 285 à 305

DESSINS D'ENFANTS

par **Joseph OESTERLÉ**

> Cette découverte, qui techniquement se réduit à si peu de choses, a fait sur moi une impression très forte, et elle représente un tournant décisif dans le cours de mes réflexions, un déplacement notamment de mon centre d'intérêt en mathématique, qui soudain s'est trouvé fortement localisé. Je ne crois pas qu'un fait mathématique m'ait jamais autant frappé que celui-là, et ait eu un impact psychologique comparable. Cela tient certainement à la nature tellement familière, non technique, des objets considérés, dont tout dessin d'enfant griffonné sur un bout de papier (pour peu que le graphisme soit d'un seul tenant) donne un exemple parfaitement explicite. À un tel dessin se trouvent associés des invariants arithmétiques subtils, qui seront chamboulés complètement dès qu'on y rajoute un trait de plus.
>
> Alexander GROTHENDIECK, *Esquisse d'un programme,* 1984.

En 1984, Alexander Grothendieck présente un programme de recherche, intitulé *Esquisse d'un programme* ([9]), pour demander son détachement au CNRS (qu'il obtiendra, et conservera jusqu'à son départ en retraite en 1988). Grothendieck y utilise le terme de dessin d'enfant (dans son sens courant) comme un analogue imagé de certaines cartes cellulaires ; il explique que « toute carte orientée finie se réalise canoniquement sur une courbe algébrique complexe », et que « le groupe de Galois de $\overline{\mathbf{Q}}$ sur $\mathbf{Q}$ opère sur la catégorie de ces cartes de façon naturelle » : cela se déduit de la comparaison de différents points de vue sur les revêtements de $\mathbf{P}_1 - \{0, 1, \infty\}$. Depuis, le terme de dessin d'enfant a été souvent repris, avec un sens mathématique variable suivant les auteurs, pour désigner les objets (ou classes d'isomorphisme d'objets) intervenant dans l'un ou l'autre de ces points de vue. Nous ne chercherons pas à le définir ici, et nous nous contenterons de l'utiliser pour désigner l'ensemble de la théorie.

Voici quelques raisons qui plaident pour porter une attention particulière aux revêtements finis de la courbe $\mathbf{P}_1 - \{0, 1, \infty\}$:

a) C'est la courbe algébrique la plus simple dont le groupe fondamental n'est pas commutatif.

b) Elle a beaucoup de revêtements sur $\overline{\mathbf{Q}}$: d'après un théorème de Belyĭ, toute courbe algébrique intègre sur $\overline{\mathbf{Q}}$ possède un ouvert de Zariski non vide qui se réalise comme un tel revêtement.

c) Elle s'identifie à l'espace des modules $M_{0,4}$ des courbes de genre 0 munies de 4 points marqués. L'étude de l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur son π_1 est le point de départ de l'étude de la tour de Grothendieck-Teichmüller (formée des groupoïdes fondamentaux de tous les espaces de modules $M_{g,n}$, sur lesquels opère $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$).

Notations

a) Si K est un corps, $\mathbf{P}_\mathrm{K}$ désigne la droite projective, considérée comme une courbe algébrique sur K, et $\mathbf{P}(\mathrm{K}) = \mathrm{K} \cup \{\infty\}$ l'ensemble de ses points rationnels ; on note $\mathbf{P}'_\mathrm{K}$ et $\mathbf{P}'(\mathrm{K})$ les complémentaires de $\{0, 1, \infty\}$ dans $\mathbf{P}_\mathrm{K}$ et $\mathbf{P}(\mathrm{K})$.

b) On note $\overline{\mathbf{Q}}$ l'ensemble des nombres complexes qui sont algébriques sur $\mathbf{Q}$. C'est une clôture algébrique de $\mathbf{Q}$. On note $\mathrm{G}_\mathbf{Q}$ son groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$; c'est un groupe profini.

1. REVÊTEMENTS FINIS DE $\mathbf{P}_1 - \{0, 1, \infty\}$

1.1. Le point de vue topologique et le point de vue algébrique complexe

Les revêtements finis de la droite projective complexe privée de 0, 1, ∞ peuvent être considérés de deux points de vue :

— *le point de vue topologique* : ce sont les revêtements finis de l'espace topologique $\mathbf{P}'(\mathbf{C}) = \mathbf{C} - \{0, 1\}$;

— *le point de vue algébrique* : ce sont les revêtements étales de la courbe algébrique complexe $\mathbf{P}'_\mathbf{C}$.

Ces deux points de vue sont équivalents. En effet, d'après un théorème de Grothendieck (*cf.* [13], XII, th. 5.1), pour tout schéma S de type fini sur $\mathbf{C}$, le foncteur « passage aux points complexes » est une équivalence de la catégorie des revêtements étales de S sur celle des revêtements (topologiques) finis de $\mathrm{S}(\mathbf{C})$. Dans le cas particulier qui nous intéresse, celui où $\mathrm{S} = \mathbf{P}'$, on peut bien sûr déduire directement ce résultat du théorème d'existence de Riemann.

> *Remarque.* — L'anneau des fonctions régulières de $\mathbf{P}'_\mathbf{C}$ est $\mathbf{C}[z, z^{-1}, (1-z)^{-1}]$ (où z est une indéterminée). Tout revêtement étale de $\mathbf{P}'_\mathbf{C}$ est affine. Le foncteur « algèbre des fonctions régulières » est une équivalence de la catégorie des revêtements étales de $\mathbf{P}'_\mathbf{C}$ sur la catégorie opposée à celle des algèbres étales et finies sur $\mathbf{C}[z, z^{-1}, (1-z)^{-1}]$.

1.2. Le point de vue des revêtements ramifiés

Un *revêtement ramifié fini* d'une surface topologique compacte S est par définition un couple (X, p), où X est une surface topologique compacte et $p : X \to S$ une application continue, dont le germe en chaque point $x \in X$ est isomorphe à celui de $z \mapsto z^{e(x)}$ au voisinage de 0 dans $\mathbf{C}$, pour un entier $e(x) \geqslant 1$. L'entier $e(x)$ s'appelle *l'indice de ramification* de p en x ; s'il est égal à 1, on dit que p est *non ramifié* en x. Tout revêtement fini du complémentaire d'une partie finie de S se prolonge de manière unique (à isomorphisme unique près) en un revêtement ramifié fini de S.

Le foncteur de restriction est donc une équivalence de la catégorie des revêtements ramifiés finis de $\mathbf{P}(\mathbf{C})$, non ramifiés au-dessus de $\mathbf{P}'(\mathbf{C})$, dans celle des revêtements finis de $\mathbf{P}'(\mathbf{C})$.

On a des résultats analogues dans la situation algébrique : les revêtements ramifiés considérés dans ce cas sont les couples (X, p), où X est une courbe algébrique projective et lisse sur $\mathbf{C}$ et $p : X \to \mathbf{P}_{\mathbf{C}}$ un morphisme fini, étale au-dessus de $\mathbf{P}'_{\mathbf{C}}$.

> *Remarque.* — Le corps des fonctions rationnelles de $\mathbf{P}_{\mathbf{C}}$ est $\mathbf{C}(z)$. Le foncteur « algèbre des fonctions rationnelles » est une équivalence de la catégorie des revêtements ramifiés de $\mathbf{P}_{\mathbf{C}}$, étales au-dessus de $\mathbf{P}'_{\mathbf{C}}$, sur la catégorie opposée à celle des algèbres réduites de dimension finie sur $\mathbf{C}(z)$, non ramifiées en dehors de $0, 1, \infty$.

Le foncteur « passage aux points complexes » permet de passer, pour les revêtements ramifiés, du cadre algébrique au cadre topologique. Les fibres en 0, 1 et ∞ des revêtements ramifiés considérés dans les deux cadres s'identifient canoniquement ; les notions d'indices de ramification définies dans les deux cadres coïncident.

1.3. Le point de vue des groupes fondamentaux (cas topologique)

Rappelons la définition du groupoïde fondamental $\varpi_1(S)$ d'un espace topologique S : ses points sont ceux de S ; les flèches reliant un point a à un point b sont les classes d'homotopie strictes de chemins reliant a à b ; l'ensemble de ces flèches est noté $\pi_1(S; a, b)$, ou $\pi_1(S, a)$ si $a = b$. La composée de deux flèches $\gamma \in \pi_1(S; a, b)$ et $\gamma' \in \pi_1(S; b, c)$ sera notée $\gamma'\gamma$ (contrairement à l'usage en topologie où on l'écrit plutôt $\gamma\gamma'$).

Soit (Y, q) un revêtement de S. La famille $(q^{-1}(a))_{a \in S}$ des fibres de q est un $\varpi_1(S)$-ensemble : chaque élément de $\pi_1(S; a, b)$ définit, par relèvement des chemins, une bijection de $q^{-1}(a)$ sur $q^{-1}(b)$. Supposons que S soit localement contractile (ou plus généralement que chaque point $a \in S$ possède un voisinage U connexe par arcs tel que l'homomorphisme $\pi_1(U, a) \to \pi_1(S, a)$ soit nul). Le foncteur $(Y, q) \mapsto (q^{-1}(a))_{a \in S}$ est alors une équivalence de la catégorie des revêtements de S dans celle des $\varpi_1(S)$-ensembles ; les revêtements finis correspondent aux $\varpi_1(S)$-ensembles $(E_a)_{a \in S}$ formés d'ensembles finis.

On peut remplacer dans ce qui précède le groupoïde fondamental par un sous-groupoïde plein, contenant au moins un point dans chaque composante connexe par arcs de S. En particulier, si S est connexe par arcs et $a \in S$, le foncteur « fibre en a »

est une équivalence de la catégorie des revêtements finis de S sur celle des $\pi_1(S;a)$-ensembles finis.

Ceci s'applique en particulier au cas où $S = \mathbf{P}'(\mathbf{C})$: pour tout $a \in \mathbf{P}'(\mathbf{C})$, le foncteur « fibre en a » est une équivalence de la catégorie des revêtements finis de $\mathbf{P}'(\mathbf{C})$ sur celle des $\pi_1(\mathbf{P}'(\mathbf{C}), a)$-ensembles finis.

Remarques. — 1) On peut faire jouer le rôle de point-base à un sous-ensemble contractile de $\mathbf{P}'(\mathbf{C})$. Prenons par exemple l'intervalle $]0,1[$ et notons π le groupe fondamental correspondant ; il possède deux générateurs canoniques c_0 et c_1 (correspondant à un tour effectué dans le sens trigonométrique autour de 0 et 1 respectivement) ; le π-ensemble associé à (Y,q) s'identifie dans ce cas à l'ensemble des composantes connexes de $q^{-1}(]0,1[)$.

2) On peut également faire jouer le rôle de point-base à un germe d'ensemble contractile (par exemple le germe en 0 de l'intervalle $]0,1[$) ; le rôle de la fibre est alors tenu par l'ensemble des relèvements continus de ce germe.

3) Le groupe des permutations de $\{0,1,\infty\}$ opère sur $\mathbf{P}'(\mathbf{C})$. Plutôt que de choisir un seul point-base, il est parfois plus commode d'en prendre un nombre fini, stable par ce groupe de symétrie. Dans *Esquisse d'un programme*, Grothendieck propose le choix suivant : on interprète $\mathbf{P}'(\mathbf{C})$ comme l'espace de modules $M_{0,4}(\mathbf{C})$ paramétrant les classes d'isomorphisme de courbes de genre 0 (projectives, lisses, irréductibles sur $\mathbf{C}$) munies (d'une suite ordonnée) de 4 points marqués (deux à deux distincts) : un point $a \in \mathbf{P}'(\mathbf{C})$ correspond à la classe d'isomorphisme de la droite projective, munie de $(0,1,\infty,a)$.

Considérons une courbe de genre 0 munie de 4 points marqués ; en général, le groupe des automorphismes de la courbe qui stabilisent l'ensemble des points marqués est d'ordre 4 (et isomorphe au groupe de Klein). Il n'est plus grand que lorsque la classe d'isomorphisme de la courbe, munie de ses points marqués, correspond à l'un des points -1, $\frac{1}{2}$, 2, ρ, $\overline{\rho}$ de $\mathbf{P}'(\mathbf{C})$ (avec $\rho = \frac{1+i\sqrt{3}}{2}$). Grothendieck propose de prendre ces 5 points de $\mathbf{P}'(\mathbf{C})$ comme points-base.

Les classes d'isomorphisme des courbes de genre 0 munies de 4 points marqués, et qui possèdent une structure réelle pour laquelle l'ensemble des points marqués est stable par conjugaison complexe, correspondent dans $\mathbf{P}'(\mathbf{C})$ à la réunion des deux droites et des deux cercles représentés sur la figure 1 ci-dessous. En ne conservant que les portions de ces courbes reliant les points-base choisis, on obtient 6 chemins reliant respectivement chacun des trois points -1, $\frac{1}{2}$, 2 à chacun des deux points ρ, $\overline{\rho}$. Le sous-groupoïde plein du groupoïde fondamental $\mathbf{P}'(\mathbf{C})$ bâti sur ces 5 points-base est le groupoïde libre engendré par les classes de ces six chemins.

Cette construction qui peut sembler pédante dans le cas de $\mathbf{P}'(\mathbf{C})$ prend par contre tout son sel lorsqu'on essaie de la généraliser aux espaces de modules $M_{g,n}$.

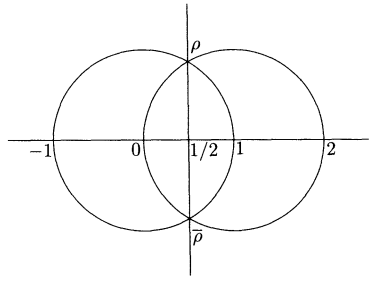

FIGURE 1

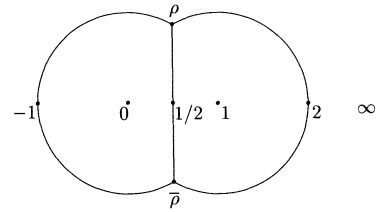

FIGURE 2

1.4. Le point de vue des groupes fondamentaux (cas algébrique)

Le groupoïde fondamental a un analogue en géométrie algébrique. Rappelons-en brièvement la définition, due à Grothendieck. Soit S un schéma. Un *point géométrique* de S est un point a de S à valeurs dans un corps séparablement clos ; sa donnée équivaut à celle d'un point s de S et d'une extension séparablement close k du corps résiduel de s. On définit la fibre en a d'un revêtement étale (Y, q) de S comme l'image réciproque de a par l'application $Y(k) \to S(k)$ déduite de q. On obtient ainsi un foncteur « fibre en a » de la catégorie des revêtements étales de S dans celle des ensembles finis.

Le groupoïde fondamental de S, noté $\varpi_1^{ét}(S)$, ou simplement $\varpi_1(S)$ lorsque cela ne prête pas à confusion, a pour points les points géométriques de S (en limitant les corps où ils prennent leurs valeurs à un univers, si on veut que ces points forment un ensemble) ; les flèches reliant un point a à un point b sont par définition les isomorphismes du foncteur « fibre en a » sur le foncteur « fibre en b » de la catégorie des revêtements étales de S dans celle des ensembles finis ; l'ensemble de ces flèches est noté $\pi_1^{ét}(S; a, b)$, ou $\pi_1^{ét}(S, a)$ si $a = b$ (la mention « *ét* » pouvant être omise lorsque cela ne prête pas à confusion). On munit $\pi_1^{ét}(S; a, b)$ de la topologie de la convergence simple dans les fibres en a des revêtements étales de S ; c'est un ensemble profini. La composition et l'inversion des flèches sont continues.

Supposons que le schéma S n'ait qu'un nombre fini de composantes connexes (ce qui est le cas par exemple s'il est nœthérien). Le foncteur qui à un revêtement étale de S associe la famille de ses fibres géométriques, munie de l'opération du groupoïde $\varpi_1^{ét}(S)$, est une équivalence de la catégorie des revêtements étales de S dans celle des familles (indexées par l'ensemble des points géométriques de S) d'ensembles finis, munies d'une opération continue de $\varpi_1^{ét}(S)$. On peut remplacer dans ce qui précède le groupoïde fondamental par tout sous-groupoïde plein contenant au moins un point dans chaque composante connexe de S. En particulier, si S est connexe et que a est un point géométrique de S, le foncteur « fibre en a » est une équivalence de la catégorie des revêtements étales de S sur celle des ensembles finis, munis d'une opération continue du groupe profini $\pi_1^{ét}(S, a)$.

Lorsque S est un schéma de type fini sur $\mathbf{C}$, tout point a de $S(\mathbf{C})$ est un point géométrique de S et l'équivalence de catégorie rappelée au n° 1.1 permet d'associer à toute classe de chemins reliant a à un point b de $S(\mathbf{C})$ un élément de $\pi_1^{ét}(S; a, b)$. Cela définit un morphisme canonique du groupoïde topologique $\varpi_1(S(\mathbf{C}))$ dans le groupoïde algébrique $\varpi_1^{ét}(S)$. Pour $a, b \in S(\mathbf{C})$, $\pi_1^{ét}(S; a, b)$ s'identifie au séparé complété de $\pi_1(S(\mathbf{C}); a, b)$ pour la structure uniforme suivante : un système fondamental d'entourages est formé des ensembles $\{(\gamma, \delta) \mid \delta \in \gamma U\}$, où U parcourt l'ensemble des sous-groupes d'indice fini de $\pi_1(S(\mathbf{C}), a)$.

Ceci s'applique en particulier au cas où $S = \mathbf{P}'_{\mathbf{C}}$: pour tout point géométrique a de $\mathbf{P}'_{\mathbf{C}}$, le foncteur « fibre en a » est une équivalence de la catégorie des revêtements

étales de $\mathbf{P}'_{\mathbf{C}}$ sur celle des ensembles finis, munis d'une opération à gauche continue de $\pi_1^{\text{ét}}(\mathbf{P}'_{\mathbf{C}}, a)$. Lorsque $a \in \mathbf{P}'(\mathbf{C})$, le groupe topologique $\pi_1^{\text{ét}}(\mathbf{P}'_{\mathbf{C}}, a)$ s'identifie au complété profini de $\pi_1(\mathbf{P}'(\mathbf{C}), a)$. Comme $\pi_1(\mathbf{P}'(\mathbf{C}), a)$ est isomorphe au groupe libre à deux générateurs, l'homomorphisme $\pi_1(\mathbf{P}'(\mathbf{C}), a) \to \pi_1^{\text{ét}}(\mathbf{P}'_{\mathbf{C}}, a)$ est injectif.

Remarques. — 1) Soient S une courbe algébrique lisse sur un corps de caractéristique 0, $\overline{\mathrm{S}}$ sa compactifiée lisse, et ξ un vecteur tangent non nul à $\overline{\mathrm{S}}$ en un point géométrique a de $\overline{\mathrm{S}} - \mathrm{S}$. On peut faire jouer à ξ le rôle d'un point-base géométrique de S (*cf.* [6]). La fibre en ξ d'un revêtement étale (Y, q) de S peut être décrite dans ce cas comme suit : on prolonge le revêtement étale en un morphisme fini $(\mathrm{X}, p) \to \overline{\mathrm{S}}$, où X est la compactifiée lisse de Y ; si b est un point géométrique de X au-dessus de a, et e l'indice de ramification de p en b, la partie principale de p en b est une application homogène t_b de degré e de l'espace tangent à X en b dans l'espace tangent à $\overline{\mathrm{S}}$ en a ; on prend alors pour fibre de ξ la réunion disjointe des ensembles $t_b^{-1}(\xi)$, pour b au-dessus de a. Le groupe fondamental de S en ξ peut encore être défini comme le groupe des automorphismes du foncteur « fibre en ξ ». Nous en donnerons une description galoisienne ultérieurement (*cf.* 2.5, remarque).

2) Pour $i \neq j$ dans $\{0, 1, \infty\}$, définissons un vecteur tangent à $\mathbf{P}_{\mathbf{C}}$ en i comme suit : $\overrightarrow{01}$ est le vecteur tangent $\frac{d}{dz}$ en 0 ; $\overrightarrow{ij}$ est son image par l'automorphisme de $\mathbf{P}_{\mathbf{C}}$ qui permute $\{0, 1, \infty\}$ en appliquant 0 sur i et 1 sur j. La remarque 1 s'applique par exemple en prenant pour S la courbe $\mathbf{P}'_{\mathbf{C}}$ et pour ξ l'un des six vecteurs tangents $\overrightarrow{ij}$. Le groupe fondamental de $\mathbf{P}'_{\mathbf{C}}$ en $\overrightarrow{01}$ est canoniquement isomorphe au complété profini du groupe fondamental (topologique) de $\mathbf{P}'(\mathbf{C})$ obtenu en faisant jouer le rôle de point-base soit à $]0, 1[$, soit au germe de $]0, 1[$ en 0 (*cf.* n° 1.3, remarques 1 et 2).

1.5. Le point de vue des cartes triangulaires orientées tricoloriées

La surface topologique $\mathbf{P}(\mathbf{C})$ possède une décomposition cellulaire canonique, dont le 1-squelette est $\mathbf{P}(\mathbf{R})$ et l'ensemble des sommets $\{0, 1, \infty\}$.

Cela permet d'associer à tout revêtement ramifié (X, p) de $\mathbf{P}(\mathbf{C})$, non ramifié au-dessus de $\mathbf{P}'(\mathbf{C})$, une carte triangulaire orientée tricoloriée $\mathrm{G} = (\mathrm{X}, \mathrm{K}, \mathrm{S}, t)$ (*cf.* Appendice, n° 2, pour la définition de ces cartes) : on munit la surface topologique X de l'orientation déduite par p de celle de $\mathbf{P}(\mathbf{C})$, on prend pour K l'ensemble fermé $p^{-1}(\mathbf{P}(\mathbf{R}))$, pour S l'ensemble fini $p^{-1}(\{0, 1, \infty\})$, et pour $t : \mathrm{S} \to \{0, 1, \infty\}$ l'application déduite de p.

Le foncteur ainsi défini est une équivalence de la catégorie des revêtements ramifiés de $\mathbf{P}(\mathbf{C})$, non ramifiés au-dessus de $\mathbf{P}'(\mathbf{C})$, sur la catégorie isotopique des cartes triangulaires orientées tricoloriées. (La définition des morphismes de cette catégorie, un peu technique, est précisée dans *loc. cit.*).

Exercice. — Considérons les ensembles d'arêtes de G de type $\{\infty, 0\}$, $\{0, 1\}$ et $\{1, \infty\}$ respectivement, et les ensembles de faces de G, positives et négatives respectivement. La relation d'incidence définit une bijection de chacun des trois premiers ensembles sur chacun des deux derniers. Vérifier que ces cinq ensembles et six bijections définissent un ϖ-ensemble, où ϖ est le groupoïde considéré dans la remarque 3 de 1.3, et que ce ϖ-ensemble est canoniquement isomorphe à celui associé au revêtement de $\mathbf{P}'(\mathbf{C})$ déduit de (X, p).

1.6. Le point de vue des cartes cellulaires orientées bicoloriées

À tout revêtement ramifié fini (X, p) de $\mathbf{P}(\mathbf{C})$, non ramifié au-dessus de $\mathbf{P}'(\mathbf{C})$, on associe une carte cellulaire orientée bicoloriée (X, K, S, b) (*cf.* Appendice, n° 3) en munissant la surface topologique X de la même orientation qu'au n° 1.5, en prenant pour K l'ensemble fermé $p^{-1}([0,1])$, pour S l'ensemble fini $p^{-1}(\{0,1\})$, et pour b : $S \to \{0,1\}$ l'application déduite de p.

Le foncteur ainsi défini est une équivalence de la catégorie des revêtements ramifiés fini de $\mathbf{P}(\mathbf{C})$, non ramifiés au-dessus de $\mathbf{P}'(\mathbf{C})$, sur la catégorie isotopique des cartes cellulaires orientées bicoloriées (*cf. loc. cit.*).

1.7. Le point de vue combinatoire

À tout revêtement fini (Y, q) de $\mathbf{P}'(\mathbf{C})$, associons l'ensemble E des composantes connexes de $q^{-1}(]0,1[)$, muni des permutations σ_0 et σ_1 suivant lesquelles les générateurs canoniques du groupe fondamental $\pi = \pi_1(\mathbf{P}'(\mathbf{C}),]0,1[)$ opèrent sur E (*cf.* remarque 1 du n° 1.3).

On définit ainsi une équivalence de la catégorie des revêtements finis de $\mathbf{P}'(\mathbf{C})$ dans celle des ensembles finis munis de deux permutations.

> *Remarque.* — Soit (X, p) l'unique (à isomorphisme unique près) revêtement ramifié de $\mathbf{P}(\mathbf{C})$ prolongeant (Y, q) et soit G la carte triangulaire orientée tricoloriée qui lui a été associée au n° 1.5. Le triplet (E, σ_0, σ_1) peut se décrire à partir de G comme suit : E est l'ensemble des arêtes de G de type $\{0,1\}$; si s est un sommet de type 0 (resp. de type 1) de G, les arêtes de G de type $\{0,1\}$ dont s est une extrémité sont munies d'un ordre cyclique[(1)] déduit de l'orientation de X en s, et σ_0 (resp. σ_1) applique chacune de ces arêtes sur la suivante pour cet ordre cyclique.

Notons $\langle\sigma_0\rangle$ et $\langle\sigma_1\rangle$ les sous-groupes de $\mathfrak{S}_E$ engendrés par σ_0 et σ_1 respectivement. Leurs orbites dans E paramètrent les points des fibres $p^{-1}(0)$ et $p^{-1}(1)$, *i.e.* les sommets de type 0 et 1 de G. On peut paramétrer les points de $p^{-1}(\infty)$, *i.e.* les sommets de type ∞ de G, par les orbites de $\langle\sigma_\infty\rangle$, où $\sigma_\infty = \sigma_0^{-1}\sigma_1^{-1}$, en associant à chaque sommet s de type ∞ l'ensemble des arêtes de type $\{0,1\}$ bordant une face positive dont s est un sommet. Les indices de ramification de p en les points au-dessus de 0, 1 et ∞ sont les cardinaux des orbites correspondantes de $\langle\sigma_0\rangle$, $\langle\sigma_1\rangle$ et $\langle\sigma_\infty\rangle$.

Pour que Y (ou ce qui revient au même X) soit connexe, il faut et il suffit que le groupe engendré par σ_0 et σ_1 opère transitivement sur E. La formule de Riemann-Hurwitz permet alors de « lire » le genre g de X sur (E, σ_0, σ_1) : on a $2g - 2 = n - n_0 - n_1 - n_\infty$, où n est le cardinal de E (égal au degré du revêtement), et n_0, n_1, n_∞ les nombres d'orbites respectifs de σ_0, σ_1, σ_∞ dans E.

---

(1) Un *ordre cyclique sur* un ensemble fini A est une permutation σ de A qui engendre un sous-groupe transitif de $\mathfrak{S}_A$; si a est un élément de A, on dit que $\sigma(a)$ est l'élément suivant pour cet ordre cyclique.

1.8. Le point de vue des sous-groupes d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$

Notons $\mathfrak{H}$ le demi-plan de Poincaré, *i.e.* l'ensemble des nombres complexes de partie imaginaire > 0. Le groupe $\mathbf{SL}_2(\mathbf{Z})$ opère sur $\mathfrak{H}$ par $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \tau\right) \mapsto \frac{a\tau+b}{c\tau+d}$.

Notons $\Gamma(2)$ le sous-groupe d'indice 6 de $\mathbf{SL}_2(\mathbf{Z})$ formé des matrices congrues à la matrice unité modulo 2. La surface de Riemann $\mathrm{Y}(2) = \Gamma(2)\backslash\mathfrak{H}$ paramètre les classes d'isomorphisme de courbes elliptiques sur $\mathbf{C}$, munies de deux points d'ordre 2 distincts : à l'élément $\Gamma(2)\tau$ de $\mathrm{Y}(2)$ correspond la classe d'isomorphisme de la courbe elliptique $\mathbf{C}/(\mathbf{Z}+\mathbf{Z}\tau)$, munie des points d'ordre 2 images de $\frac{\tau}{2}$ et $\frac{1}{2}$. Il existe un unique nombre complexe $\lambda(\tau)$ tel que la courbe elliptique d'équation $y^2 = x(x-1)(x-\lambda(\tau))$, munie de ses points $(0,0)$ et $(1,0)$, soit isomorphe à la précédente.

La fonction λ ainsi définie est holomorphe sur $\mathfrak{H}$, et invariante par $\Gamma(2)$: c'est une fonction modulaire de poids 0 pour $\Gamma(2)$. Elle définit par passage au quotient un isomorphisme de $\mathrm{Y}(2)$ sur $\mathbf{P}'(\mathbf{C})$, qui se prolonge en un isomorphisme de la surface de Riemann $\mathrm{X}(2)$ (compactifiée de $\mathrm{Y}(2)$ par adjonction des pointes) sur $\mathbf{P}(\mathbf{C})$; celui-ci applique les trois pointes $\Gamma(2)\infty$, $\Gamma(2)0$ et $\Gamma(2)1$ de $\mathrm{X}(2)$ sur 0, 1 et ∞ respectivement. L'image par λ de la demi-droite $i]0,+\infty[$ est l'intervalle $]0,1[$.

La surjection canonique $\mathfrak{H} \to \mathrm{Y}(2)$ est un revêtement universel de $\mathrm{Y}(2)$. On en déduit que tout triplet $(\mathrm{Y}, q, \mathrm{A})$, où (Y, q) est un revêtement *connexe non vide* de $\mathbf{P}'(\mathbf{C})$ et A une composante connexe de $q^{-1}(]0,1[)$, est isomorphe à un unique triplet de la forme $(\mathrm{Y}_\Gamma, q_\Gamma, \mathrm{A}_\Gamma)$, où Γ est un sous-groupe d'indice fini de $\Gamma(2)$ contenant $\{\pm 1\}$, Y_Γ la surface de Riemann $\Gamma\backslash\mathfrak{H}$, q_Γ le composé de la surjection canonique $\mathrm{Y}_\Gamma \to \mathrm{Y}(2)$ et de l'isomorphisme $\mathrm{Y}(2) \to \mathbf{P}'(\mathbf{C})$ ci-dessus, et A_Γ l'image de la demi-droite $i]0,+\infty[$ dans Y_Γ. De plus l'isomorphisme entre ces deux triplets est unique.

Variante. — Soient (X, p) un revêtement ramifié *connexe non vide* de $\mathbf{P}(\mathbf{C})$, non ramifié au-dessus de $\mathbf{P}'(\mathbf{C})$ et A une composante connexe de $p^{-1}(]0,1[)$. Supposons que les indices de ramification des points de $p^{-1}(1)$ divisent 2 et que ceux des points de $p^{-1}(\infty)$ divisent 3. Le triplet $(\mathrm{X}, p, \mathrm{A})$ est alors isomorphe à un unique triplet de la forme $(\mathrm{X}_\Gamma, p_\Gamma, \mathrm{A}_\Gamma)$, où Γ est un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$ contenant $\{\pm 1\}$, X_Γ est la surface de Riemann compactifiée de $\Gamma\backslash\mathfrak{H}$, p_Γ se déduit par passage au quotient de $\frac{1728}{j}$, où j est l'invariant modulaire, et A_Γ est l'image de la demi-droite $i]1,+\infty[$ dans X_Γ. De plus l'isomorphisme entre ces deux triplets est unique.

Exercice. — Tout sous-groupe d'indice fini de $\Gamma(2)$ est aussi un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbf{Z})$. Interpréter cela, via les dictionnaires ci-dessus, en termes de subdivisions barycentriques de cartes cellulaires triangulaires tricoloriées, et en déduire sans calculs la relation $j = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. Faire le lien avec la fig. 1.

1.9. Le point de vue algébrique sur $\overline{\mathbf{Q}}$

Soient k un corps algébriquement clos de caractéristique 0, k' une extension algébriquement close de k et S un schéma de type fini sur k. Soit S' le schéma sur k' déduit de S par extension des scalaires. Le foncteur « extension des scalaires de k à k' » est une équivalence de la catégorie des revêtements étales de S sur celle des revêtements étales de S'. De façon équivalente, si s' est un point géométrique de S' et s le point

géométrique correspondant de S, l'homomorphisme canonique $\pi_1^{ét}(S', s') \to \pi_1^{ét}(S, s)$ est un isomorphisme (*cf.* [13], XIII, cor. 3.5 et remarque 3.1.3).

En particulier, le foncteur « extension des scalaires de $\overline{\mathbf{Q}}$ à $\mathbf{C}$ » est une équivalence de la catégorie des revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ sur celle des revêtements étales de $\mathbf{P}'_{\mathbf{C}}$. Comme précédemment, ces catégories sont aussi équivalentes aux suivantes :

— la catégorie des revêtements ramifiés de $\mathbf{P}_{\overline{\mathbf{Q}}}$, étales au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$;

— la catégorie opposée à celle des algèbres étales et finies sur $\overline{\mathbf{Q}}[z, z^{-1}, (1-z)^{-1}]$;

— la catégorie opposée à celle des algèbres réduites de dimension finie sur $\overline{\mathbf{Q}}(z)$, non ramifiées en dehors de $0, 1, \infty$;

— la catégorie des ensembles finis munis d'une opération à gauche continue de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$, pour a un point géométrique de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ (ou un vecteur tangent non nul à $\mathbf{P}_{\overline{\mathbf{Q}}}$ en 0, 1 ou ∞).

1.10. Le théorème de Belyĭ

Soient X une courbe algébrique projective et lisse sur $\overline{\mathbf{Q}}$ et p une fonction rationnelle sur X qui n'est constante sur aucune composante connexe de X. On peut considérer p comme un morphisme fini de X dans la droite projective $\mathbf{P}_{\overline{\mathbf{Q}}}$. On dit que p est une *fonction de Belyĭ* si ce morphisme est étale au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$. Cette terminologie est justifiée par le très surprenant théorème suivant de Belyĭ ([1]) :

THÉORÈME 1. — *Soit* X *une courbe algébrique projective et lisse sur* $\overline{\mathbf{Q}}$. *Pour tout ensemble fini* $S \subset X(\overline{\mathbf{Q}})$, *il existe une fonction de Belyĭ* p *sur* X *telle que* $p(S) \subset \{0, 1, \infty\}$.

Soit f une fonction rationnelle sur X, qui n'est constante sur aucune composante connexe de X, *i.e.* un morphisme fini de X dans $\mathbf{P}_{\overline{\mathbf{Q}}}$. L'ensemble R_f des points de $X(\overline{\mathbf{Q}})$ en lesquels ce morphisme est ramifié est fini. Si q est une fonction de Belyĭ sur $\mathbf{P}_{\overline{\mathbf{Q}}}$ qui applique $f(S) \cup f(R_f)$ dans $\{0, 1, \infty\}$, on peut prendre $p = q \circ f$. Il nous suffit donc de traiter le cas où $X = \mathbf{P}_{\overline{\mathbf{Q}}}$.

Notons dans ce cas d le degré maximum des points de S sur $\mathbf{Q}$ et e le nombre de points de S de degré d ; nous démontrerons le théorème par récurrence sur le couple (d, e) (pour l'ordre lexicographique). Traitons d'abord le cas où $d \geqslant 2$. Choisissons un point $a \in S$ de degré d. Notons f son polynôme minimal ; il est de degré d, à coefficients rationnels. L'ensemble R_f se compose de ∞ et des racines du polynôme dérivé de f. Ses points sont donc de degré $\leqslant d-1$ sur $\mathbf{Q}$ et il en est de même des points de $f(R_f)$. Quant aux points de $f(S)$, ils sont de degré $\leqslant d$ et il y en a au plus $e-1$ de degré d, puisque $f(a) = 0$. Le premier alinéa et l'hypothèse de récurrence permettent de conclure.

Traitons maintenant le cas où $d = 1$, c'est-à-dire où $S \subset \mathbf{P}(\mathbf{Q})$. Si $e \leqslant 3$, on peut prendre pour p une homographie. Supposons $e \geqslant 4$. Par une homographie, on se ramène au cas où S contient $\{0, 1, \infty\}$ et au moins un point a dans l'intervalle $]0, 1[$.

Écrivons $a = \frac{m}{m+n}$ avec m, n entiers $\geqslant 1$ premiers entre eux et notons f le polynôme $t^m(t-1)^n$. On a $\mathrm{R}_f \subset \{0, 1, \infty, a\} \subset \mathrm{S}$ et $f(\mathrm{S})$ a au plus $e-1$ éléments, puisque $f(0) = f(1) = 0$. Le premier alinéa et l'hypothèse de récurrence permettent encore de conclure.

2. OPÉRATIONS DE $\mathrm{G}_{\mathbf{Q}}$ SUR LES DESSINS D'ENFANTS

2.1. Opération de $\mathrm{G}_{\mathbf{Q}}$ sur la catégorie des revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$

Posons $\mathrm{R} = \overline{\mathbf{Q}}[z, z^{-1}, (z-1)^{-1}]$. Pour $\sigma \in \mathrm{G}_{\mathbf{Q}}$, notons σ_{R} l'automorphisme de l'anneau R qui prolonge σ et fixe z. Soit A une algèbre sur R, *i.e.* un anneau muni d'un homomorphisme $\rho : \mathrm{R} \to \mathrm{A}$. Le même anneau, muni de l'homomorphisme $\rho \circ \sigma_{\mathrm{R}}^{-1}$ est une nouvelle R-algèbre que nous noterons ${}^{\sigma}\mathrm{A}$ (et qui est canoniquement isomorphe à celle déduite de A par l'extension des scalaires σ_{R}). Tout homomorphisme de R-algèbres $u : \mathrm{A} \to \mathrm{B}$ est aussi un homomorphisme de R-algèbres de ${}^{\sigma}\mathrm{A}$ dans ${}^{\sigma}\mathrm{B}$, que nous noterons ${}^{\sigma}u$. Si τ est un second élément de $\mathrm{G}_{\mathbf{Q}}$, on a ${}^{\sigma}({}^{\tau}\mathrm{A}) = {}^{\sigma\tau}\mathrm{A}$ et ${}^{\sigma}({}^{\tau}u) = {}^{\sigma\tau}u$. Nous avons ainsi défini une opération de $\mathrm{G}_{\mathbf{Q}}$ sur la catégorie des R-algèbres. Elle stabilise la sous-catégorie pleine formée des algèbres étales et finies sur R.

Explicitons l'opération correspondante de $\mathrm{G}_{\mathbf{Q}}$ sur la catégorie des revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$: si (Y, q) est un tel revêtement, le revêtement ${}^{\sigma}(\mathrm{Y}, q) = ({}^{\sigma}\mathrm{Y}, {}^{\sigma}q)$ (dit *conjugué de* (Y, q) *par* σ) est défini comme suit : ${}^{\sigma}\mathrm{Y}$ a même schéma sous-jacent que Y, mais son morphisme structural vers $\mathrm{Spec}(\overline{\mathbf{Q}})$ est celui de Y composé avec $\mathrm{Spec}(\sigma^{-1})$; le morphisme ${}^{\sigma}q : {}^{\sigma}\mathrm{Y} \to \mathbf{P}'_{\overline{\mathbf{Q}}} = \mathrm{Spec}(\mathrm{R})$ est le composé de q avec $\mathrm{Spec}(\sigma_{\mathrm{R}}^{-1})$.

> *Remarque.* — Le groupe $\mathrm{G}_{\mathbf{Q}}$ opère de manière analogue sur la catégorie des $\overline{\mathbf{Q}}(z)$ algèbres réduites de dimension finie, non ramifiées en dehors de $\{0, 1, \infty\}$ et sur celle des revêtements ramifiés de $\mathbf{P}_{\overline{\mathbf{Q}}}$, étales au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$.
>
> Il opère aussi sur l'une quelconque des autres catégories $\mathscr{C}$ équivalentes à cette dernière (par exemple celle des ensembles finis munis de deux permutations), avec cependant dans ce cas les complications mineures venant du fait que, pour un objet D de $\mathscr{C}$ et $\sigma \in \overline{\mathbf{Q}}$, l'objet ${}^{\sigma}\mathrm{D}$ n'est que défini de manière unique à isomorphisme unique près, et que ${}^{\sigma}({}^{\tau}\mathrm{D})$ n'est pas égal, mais seulement canoniquement isomorphe à ${}^{\sigma\tau}\mathrm{D}$, etc.

2.2. Corps de définition, corps des modules d'un revêtement

Soient (Y, q) un revêtement étale de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ et L un sous-corps de $\overline{\mathbf{Q}}$. Un *modèle* de (Y, q) sur L est un triplet $(\mathrm{Y}_{\mathrm{L}}, q_{\mathrm{L}}, \varphi)$, où $(\mathrm{Y}_{\mathrm{L}}, q_{\mathrm{L}})$ est un revêtement étale de $\mathbf{P}'_{\mathrm{L}}$ et φ un isomorphisme du revêtement $(\mathrm{Y}_{\overline{\mathbf{Q}}}, q_{\overline{\mathbf{Q}}})$ déduit de $(\mathrm{Y}_{\mathrm{L}}, q_{\mathrm{L}})$ par extension des scalaires de L à $\overline{\mathbf{Q}}$ sur le revêtement (Y, q).

On dit que L est un *corps de définition* de (Y, q) s'il existe un *modèle* de (Y, q) sur L. Il existe des corps de définition de (Y, q) qui sont de degré fini sur $\mathbf{Q}$.

Soit (Y_L, q_L, φ) un modèle de (Y, q) sur L. Le revêtement $(Y_{\overline{\mathbf{Q}}}, q_{\overline{\mathbf{Q}}})$ est canoniquement isomorphe à chacun de ses conjugués par $G_L = \mathrm{Gal}(\overline{\mathbf{Q}}/L)$, d'où par transport de structure un isomorphisme $u_\sigma : (Y, q) \to {}^\sigma(Y, q)$ pour tout $\sigma \in G_L$. Ces isomorphismes satisfont la relation de cocycle $u_{\sigma\tau} = {}^\sigma u_\tau \circ u_\sigma$ pour $\sigma, \tau \in G_L$.

Inversement, si des isomorphismes $u_\sigma : (Y, q) \to {}^\sigma(Y, q)$, pour $\sigma \in G_L$, satisfont cette relation de cocycle, ils proviennent par la construction précédente d'un modèle de (Y, q) sur L, unique à isomorphisme unique près.

Remarque. — Soit (Y_L, q_L, φ) un modèle de (Y, q) sur L. Alors $(\sigma, g) \mapsto u_\sigma^{-1}\, {}^\sigma g u_\sigma$ définit une opération continue de G_L sur le groupe des automorphismes de (Y, q). L'ensemble des classes d'isomorphisme de modèles de (Y, q) sur L est paramétré par $H^1(G_L, \mathrm{Aut}(Y, q))$. Il est en particulier réduit à un seul élément si le groupe des automorphismes de (Y, q) est réduit à l'élément neutre.

L'ensemble des $\sigma \in G_{\mathbf{Q}}$ tels que le revêtement ${}^\sigma(Y, q)$ soit isomorphe à (Y, q) est un sous-groupe ouvert d'indice fini de $G_{\mathbf{Q}}$. Il est donc égal à G_K pour un corps de nombres K. Le corps K est appelé le *corps des modules* du revêtement (Y, q). Il est contenu dans tout corps de définition de (Y, q), mais n'en est pas forcément un lui-même, sauf si le groupe des automorphismes de (Y, q) est réduit à l'élément neutre : en effet dans ce cas, il existe pour tout $\sigma \in G_K$ un unique isomorphisme u_σ de (Y, q) sur ${}^\sigma(Y, q)$, et la condition de cocycle est automatiquement vérifiée.

Remarques. — 1) Le corps des modules est l'intersection des corps de définition (*cf.* [3], ou [5], 3.4).

2) On trouvera dans [5] une description cohomologique des obstructions à ce que le corps des modules soit un corps de définition et diverses conditions suffisantes pour que ces obstructions soient triviales.

3) La notion de corps de définition, de corps des modules d'un revêtement étale de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ ne dépend que de la classe d'isomorphisme de ce revêtement ; elle conserve donc un sens pour les objets (ou classes d'isomorphismes d'objets) de chacune des catégories équivalentes à celle des revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ (par exemple celle des ensembles finis munis de deux permutations).

4) Soient (Y, q) un revêtement étale de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ et (E, σ_0, σ_1) le triplet formé d'un ensemble fini muni de deux permutations qui lui est associé (*cf.* 1.7). Pour que le corps des modules de (Y, q) soit *réel*, il faut et il suffit qu'il existe une permutation u de E telle que $u \circ \sigma_0 = {\sigma_0}^{-1} \circ u$ et $u \circ \sigma_1 = {\sigma_1}^{-1} \circ u$. Pour que $\mathbf{R}$ soit un corps de définition de (Y, q), il faut et il suffit qu'il existe une *involution* de E satisfaisant la condition précédente ; les classes d'isomorphisme de modèles de (Y, q) sur $\mathbf{R}$ sont alors paramétrées par les classes de conjugaison de telles involutions dans le groupe des permutations de E.

5) Soit K un corps de nombres. Pour tout revêtement ramifié (X, p) de $\mathbf{P}_{\overline{\mathbf{Q}}}$, étale au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ et sans automorphismes non triviaux, de corps des modules K, considérons l'unique (à isomorphisme unique près) modèle (X_K, p_K) de (X, p) sur K. Une variante du théorème de Belyĭ, due à Couveignes ([4]), affirme que toute courbe projective et lisse sur K est isomorphe à une courbe X_K obtenue de cette manière. Il en résulte en particulier que lorsque X est connexe de genre 0 (donc isomorphe à $\mathbf{P}_{\overline{\mathbf{Q}}}$), X_K n'est pas forcément isomorphe à $\mathbf{P}_K$ (mais peut être une conique sur K sans points rationnels).

6) Soient (X, p) un revêtement ramifié de $\mathbf{P}_{\overline{\mathbf{Q}}}$, étale au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$, a un point de $p^{-1}(0)$, ξ un point de la fibre du vecteur tangent $\overrightarrow{01}$ (*cf.* 1.4, remarques 1 et 2). Une variante des définitions de ce numéro permet d'introduire la notion de corps de définition et de corps des modules du triplet (X, p, a), et du triplet (X, p, ξ). Dans chacun de ces deux cas, le corps des modules est un corps de définition : dans le second cas, cela résulte du fait que (X, p, ξ) n'a pas d'automorphismes non triviaux ; pour le premier cas, *cf.* [2], th. 2.

2.3. Groupoïde fondamental d'un schéma de type fini sur un corps

Nous verrons dans la suite de cet exposé que l'ensemble des informations concernant l'opération de $G_{\mathbf{Q}}$ sur la catégorie des revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ est codé dans le groupoïde fondamental de $\mathbf{P}'_{\mathbf{Q}}$ (et même dans son groupe fondamental en un point rationnel).

Nous allons rappeler dans ce numéro les liens entre le groupoïde fondamental d'un schéma S *géométriquement connexe* de type fini sur un corps k et celui du schéma $\overline{S}$ qui se déduit de S par extension des scalaires à une clôture algébrique $\overline{k}$ de k. Des morphismes de schémas $\overline{S} \to S$ et $S \to \mathrm{Spec}(k)$, on déduit des morphismes de groupoïdes $\varpi_1^{ét}(\overline{S}) \to \varpi_1(S)$ et $\varpi_1^{ét}(S) \to \varpi_1^{ét}(\mathrm{Spec}(k))$. En particulier, si $\overline{a}$ est un point géométrique de $\overline{S}$ (à valeurs dans un corps séparablement clos Ω, qui *ipso facto* est une extension de $\overline{k}$), et si a et c sont les points géométriques de S et de $\mathrm{Spec}(k)$ images de $\overline{a}$, on a une suite de groupes profinis et d'homomorphismes continus

$$1 \longrightarrow \pi_1^{ét}(\overline{S}, \overline{a}) \longrightarrow \pi_1^{ét}(S, a) \longrightarrow \pi_1^{ét}(\mathrm{Spec}(k), c) \longrightarrow 1\,. \tag{1}$$

Cette suite est exacte ([13], IX, th. 6.1) et $\pi_1^{ét}(\mathrm{Spec}(k), c)$ est canoniquement isomorphe au groupe de Galois $\mathrm{Gal}(k_s/k)$, où k_s est la fermeture séparable de k dans $\overline{k}$. Chaque élément de $\mathrm{Gal}(k_s/k)$ définit donc (en faisant opérer un de ses relèvements par conjugaison sur $\pi_1^{ét}(\overline{S}, \overline{a})$) un élément du groupe $\mathrm{Out}(\pi_1^{ét}(\overline{S}, \overline{a}))$ (où, par définition, le groupe $\mathrm{Out}(G)$ des automorphismes extérieurs d'un groupe profini G est le quotient du groupe des automorphismes continus de G par le sous-groupe formé des automorphismes intérieurs).

Si $\overline{b}$ est un second point géométrique de $\overline{S}$ (pas forcément à valeurs dans le même corps séparablement clos), l'ensemble $\pi_1^{ét}(\overline{S}; \overline{a}, \overline{b})$ est non vide et tout élément u de cet ensemble définit un isomorphisme $x \mapsto uxu^{-1}$ de $\pi_1^{ét}(\overline{S}, \overline{a})$ dans $\pi_1^{ét}(\overline{S}, \overline{b})$; celui-ci ne dépend pas de u à automorphisme intérieur près. On en déduit donc un isomorphisme canonique de $\mathrm{Out}(\pi_1^{ét}(\overline{S}, \overline{a}))$ sur $\mathrm{Out}(\pi_1^{ét}(\overline{S}, \overline{b}))$, ce qui permet légitimement de définir $\mathrm{Out}(\pi_1^{ét}(\overline{S}))$ sans référence au point-base.

L'homomorphisme de $\mathrm{Gal}(k_s/k)$ dans $\mathrm{Out}(\pi_1^{ét}(\overline{S}))$ déduit de (1) ne dépend pas non plus du point-base. En effet, soient σ' et σ'' des relèvements d'un élément $\sigma \in \mathrm{Gal}(k_s/k)$ dans $\pi_1^{ét}(S, a)$ et $\pi_1^{ét}(S, b)$. Pour $x \in \pi_1(\overline{S}, \overline{a})$, on a, en identifiant $\pi_1^{ét}(\overline{S}; \overline{a}, \overline{b})$ à une partie de $\pi_1^{ét}(S; a, b)$, $\sigma''(uxu^{-1})\sigma''^{-1} = v(\sigma' x \sigma'^{-1})v^{-1}$, où $v = \sigma'' u \sigma'^{-1}$; il suffit donc de démontrer que $u^{-1}v$ appartient à $\pi_1^{ét}(\overline{S}, \overline{a})$, *i.e.* opère trivialement sur la fibre en c de tout revêtement étale de $\mathrm{Spec}(k)$ de la forme $\mathrm{Spec}(k')$, où k' est une

extension séparable de degré fini de k, ce qui est immédiat. En conclusion, on dispose d'un homomorphisme canonique

$$\mathrm{Gal}(k_s/k) \longrightarrow \mathrm{Out}(\pi_1^{ét}(\overline{\mathrm{S}}))\,.$$

Lorsque le point géométrique $a : \mathrm{Spec}(\Omega) \to \mathrm{S}$ est rationnel sur k, *i.e.* se factorise par un morphisme $\mathrm{Spec}(k) \to \mathrm{S}$, ce morphisme définit une section continue $\pi_1^{ét}(\mathrm{Spec}(k), c) \to \pi_1^{ét}(\mathrm{S}, a)$ de l'extension (1), qui est donc canoniquement scindée. L'image par cette section d'un élément σ de $\mathrm{Gal}(k_s/k) \approx \pi_1(\mathrm{Spec}(k), c)$ sera notée σ_a.

Chaque point $a \in \mathrm{S}(k)$ définit un point géométrique de S et un point géométrique de $\overline{\mathrm{S}}$ à valeurs dans $\overline{k}$, que nous noterons encore a par abus. Pour $a, b \in \mathrm{S}(k)$, on définit une opération de $\mathrm{Gal}(k_s/k)$ sur l'ensemble $\pi_1^{ét}(\overline{\mathrm{S}}; a, b)$ en posant, pour $u \in \pi_1^{ét}(\overline{\mathrm{S}}; a, b)$,

$$^{\sigma}u = \sigma_b u \sigma_a^{-1}\,,$$

le calcul étant effectué dans $\pi_1^{ét}(\mathrm{S}; a, b)$. (On notera que la flèche figurant au second membre appartient bien à $\pi_1^{ét}(\overline{\mathrm{S}}; a, b)$, car $u^{-1}\sigma_b u \sigma_a^{-1}$ appartient à $\pi_1^{ét}(\overline{\mathrm{S}}, a)$ d'après ce que nous avons vu plus haut.) L'opération de $\mathrm{Gal}(k_s/k)$ ainsi définie est compatible avec la composition des flèches.

2.4. L'homomorphisme canonique $\mathrm{G}_{\mathbf{Q}} \to \mathrm{Out}(\widehat{\pi})$

Appliquons les résultats de 2.3 au cas particulier où $k = \mathbf{Q}$, $\overline{k} = \overline{\mathbf{Q}}$ et $\mathrm{S} = \mathbf{P}'_{\mathbf{Q}}$. On obtient un homomorphisme canonique $\mathrm{G}_{\mathbf{Q}} \to \mathrm{Out}(\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}))$, où pour définir $\mathrm{Out}(\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}))$ on peut prendre pour point-base un point géométrique arbitraire. En prenant un point de l'intervalle $]0, 1[$, par exemple $\frac{1}{2}$, on obtient donc un homomorphisme canonique

$$\rho : \mathrm{G}_{\mathbf{Q}} \longrightarrow \mathrm{Out}(\widehat{\pi})$$

où $\widehat{\pi}$ est le complété profini du groupe π considéré dans la remarque 1 du n° 1.3. Notons que $\widehat{\pi}$ est un groupe profini libre à deux générateurs (ceux-ci étant les images des éléments c_0 et c_1 de π).

THÉORÈME 2. — *L'homomorphisme canonique $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{Out}(\widehat{\pi})$ est injectif.*

Cela résulte des deux lemmes suivants :

Lemme 1. — Si σ appartient au noyau de ρ, tout revêtement étale (Y, q) de $\mathbf{P}'_{\overline{\mathbf{Q}}}$ est isomorphe à son conjugué $^{\sigma}(\mathrm{Y}, q)$.

Nous pouvons supposer Y connexe. Soient a un point de $\mathbf{P}'(\mathbf{Q})$ et σ_a le relèvement canonique de σ dans $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}}, a)$ (*cf.* 2.3). Si σ appartient au noyau de ρ, σ_a opère par conjugaison dans $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$ suivant un automorphisme intérieur. Le groupe $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$ opère transitivement dans les fibres géométriques $q^{-1}(a)$ et $^{\sigma}q^{-1}(a)$ et $x \mapsto \sigma(x)$ est une bijection de $q^{-1}(a)$ dans $^{\sigma}q^{-1}(a)$, équivariante pour l'automorphisme $g \mapsto \sigma_a g \sigma_a^{-1}$ de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$. Si donc H est le stabilisateur d'un point $x \in q^{-1}(a)$ dans $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$, celui de $\sigma(x)$ est $\sigma_a \mathrm{H} \sigma_a^{-1}$, qui est conjugué à H dans $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$; cela

implique que les $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, a)$-ensembles $q^{-1}(a)$ et ${}^{\sigma}q^{-1}(a)$ sont isomorphes, et donc que les revêtements (Y, q) et ${}^{\sigma}(\mathrm{Y}, q)$ le sont.

Lemme 2. — Le groupe $\mathrm{G}_{\mathbf{Q}}$ opère fidèlement dans l'ensemble des classes d'isomorphismes de revêtements étales de $\mathbf{P}'_{\overline{\mathbf{Q}}}$.

Pour tout $j \in \overline{\mathbf{Q}}$, il existe en effet d'après le théorème de Belyĭ (th. 1) un revêtement étale (Y, q) de $\mathbf{P}'_{\overline{\mathbf{Q}}}$, où Y est un ouvert de Zariski non vide d'une courbe elliptique sur $\overline{\mathbf{Q}}$ d'invariant modulaire j. Le corps des modules de ce revêtement contient $\mathbf{Q}(j)$.

Remarque. — H. W. Lenstra a démontré que $\mathrm{G}_{\mathbf{Q}}$ opère déjà fidèlement dans l'ensemble des classes d'isomorphismes de revêtements (X, p) de $\mathbf{P}_{\overline{\mathbf{Q}}}$, étales au-dessus de $\mathbf{P}'_{\overline{\mathbf{Q}}}$, possédant les propriétés suivantes : X est connexe, de genre 0 et a un seul point au-dessus de ∞ (ce qui équivaut à dire que (X, p) est isomorphe à un couple $(\mathbf{P}_{\overline{\mathbf{Q}}}, f)$, où la fonction de Belyĭ f est un polynôme, ou encore que le 1-squelette de la carte bicoloriée associée est un arbre). Pour la démonstration, *cf.* [12], th. II.4.

2.5. Le groupe fondamental de $\mathbf{P}'_{\mathbf{Q}}$ en $\overrightarrow{01}$

Nous allons maintenant préciser la structure du groupe fondamental de $\mathbf{P}'_{\mathbf{Q}}$, lorsqu'on fait jouer le rôle de point-base au vecteur tangent $\overrightarrow{01} = (0, \frac{d}{dz})$, ou plus généralement aux vecteurs tangents $\overrightarrow{ij}$ qui se déduisent de $\overrightarrow{01}$ par les automorphismes de $\mathbf{P}_{\mathbf{Q}}$ qui stabilisent $\{0, 1, \infty\}$ (*cf.* n° 1.4, remarque 2). La théorie est semblable à celle décrite en 2.3 pour les points-base rationnels sur le corps de base : on a en particulier une suite exacte de groupes profinis, canoniquement scindée,

$$1 \longrightarrow \pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01}) \longrightarrow \pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}}, \overrightarrow{01}) \longrightarrow \mathrm{G}_{\mathbf{Q}} \longrightarrow 1. \tag{2}$$

Le groupe $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ est canoniquement isomorphe à $\pi_1^{ét}(\mathbf{P}'_{\mathbf{C}}, \overrightarrow{01})$, c'est-à-dire au complété profini $\widehat{\pi}$ du groupe fondamental de $\mathbf{P}'(\mathbf{C})$ où le rôle de point-base est tenu par le germe en 0 de $]0, 1[$, ou encore par $]0, 1[$ (1.3, remarques 1 et 2). C'est donc un groupe profini libre à deux générateurs (ceux-ci, que nous noterons x et y, correspondant par les isomorphismes précédents aux générateurs c_0 et c_1 de π).

Comme la suite exacte (2) est canoniquement scindée, le groupe $\mathrm{G}_{\mathbf{Q}}$ opère sur $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$, et $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}}, \overrightarrow{01})$ est canoniquement isomorphe au produit semi-direct de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ par $\mathrm{G}_{\mathbf{Q}}$. Toute la richesse de la structure du groupe $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}}, \overrightarrow{01})$ est donc codée dans la manière dont le groupe $\mathrm{G}_{\mathbf{Q}}$ opère sur $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$. Cette opération est définie par un homomorphisme

$$\mathrm{G}_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})) \tag{3}$$

qui relève l'homomorphisme $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{Out}(\widehat{\pi})$ considéré en 2.4 (lorsqu'on identifie $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ à $\widehat{\pi}$), et qui par suite est injectif.

Remarque. — Avant d'étudier cet homomorphisme, nous allons donner une description alternative de cette suite exacte (2) en termes galoisiens. Choisissons une uniformisante locale t de $\mathbf{P}_{\mathbf{Q}}$ en 0 telle que $dt(\overrightarrow{01}) = 1$, par exemple $t = z$. Soit $\overline{\mathbf{Q}}\{\{t\}\}$

le corps des séries de Puiseux en t à coefficients dans $\overline{\mathbf{Q}}$. C'est une extension algébriquement close de $\overline{\mathbf{Q}}(z)$ (on plonge $\overline{\mathbf{Q}}(z)$ dans $\overline{\mathbf{Q}}\{\{t\}\}$ en associant à chaque fraction rationnelle son développement de Laurent en t au point 0). Notons M la plus grande extension algébrique de $\overline{\mathbf{Q}}(z)$ contenue dans $\overline{\mathbf{Q}}\{\{t\}\}$ et non ramifiée en dehors de $\{0,1,\infty\}$. C'est une extension galoisienne de $\mathbf{Q}(z)$. Les groupes profinis $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01})$ et $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{01})$ sont canoniquement isomorphes à $\mathrm{Gal}(\mathrm{M}/\overline{\mathbf{Q}}(z))$ et $\mathrm{Gal}(\mathrm{M}/\mathbf{Q}(z))$, et la suite exacte (2) s'identifie à la suite exacte

$$1 \longrightarrow \mathrm{Gal}(\mathrm{M}/\overline{\mathbf{Q}}(z)) \longrightarrow \mathrm{Gal}(\mathrm{M}/\mathbf{Q}(z)) \longrightarrow \mathrm{Gal}(\overline{\mathbf{Q}}(z)/\mathbf{Q}(z)) \approx \mathrm{G}_{\mathbf{Q}} \longrightarrow 1\,.$$

Le relèvement canonique de $\sigma \in \mathrm{G}_{\mathbf{Q}}$ dans $\mathrm{Gal}(\mathrm{M}/\mathbf{Q}(z))$ opère dans M par $\Sigma a_\lambda t^\lambda \mapsto \Sigma\sigma(a_\lambda)t^\lambda$.

Si (E,p) est un revêtement étale connexe de $\mathbf{P}'_{\mathbf{Q}}$ et K son corps de fonctions rationnelles, il existe une bijection canonique de la fibre en $\overrightarrow{01}$ de ce revêtement (*cf.* 1.4, remarque 1) sur l'ensemble des plongements $\mathbf{Q}(z)$-linéaires de K dans M, par laquelle l'opération de $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{01})$ sur la fibre s'identifie à l'opération $(g,u) \mapsto g\circ u$ de $\mathrm{Gal}(\mathrm{M}/\mathbf{Q}(z))$ sur l'ensemble de ces plongements.

Soit σ un élément de $\mathrm{G}_{\mathbf{Q}}$. L'élément σ opère sur les racines n-ièmes de l'unité par élévation à la puissance $\chi_n(\sigma)$-ième, où $\chi_n(\sigma)$ est un entier premier à n bien défini modulo n, *i.e.* un élément de $(\mathbf{Z}/n\mathbf{Z})^\times$. Les $\chi_n(\sigma)$, pour $n \geqslant 1$, définissent un élément $\chi(\sigma)$ de la limite projective des $(\mathbf{Z}/n\mathbf{Z})^\times$, c'est-à-dire du groupe multiplicatif $\widehat{\mathbf{Z}}^\times$ du complété profini $\widehat{\mathbf{Z}}$ de $\mathbf{Z}$. L'application $\chi : \mathrm{G}_{\mathbf{Q}} \to \widehat{\mathbf{Z}}^\times$ est un homomorphisme continu, appelé le *caractère de Teichmüller*.

Le groupe $\mathrm{G}_{\mathbf{Q}}$ opère sur l'ensemble $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01},\overrightarrow{10})$. La définition de cette opération est analogue à celle donnée en 2.3 dans le cas de points-base rationnels : pour $\sigma \in \mathrm{G}_{\mathbf{Q}}$ et $u \in \pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01},\overrightarrow{10})$, on a

$$^\sigma u = \sigma_{\overrightarrow{10}} u \sigma_{\overrightarrow{01}}^{-1}\,,$$

où $\sigma_{\overrightarrow{01}}$ et $\sigma_{\overrightarrow{10}}$ sont les relèvements canoniques de σ dans $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{01})$ et $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{10})$ respectivement.

Un analogue de 1.4 montre que le chemin continu $c : t \mapsto t$ de $[0,1]$ dans $\mathbf{P}_1(\mathbf{C})$ définit un élément de $\pi_1^{ét}(\mathbf{P}'_{\mathbf{C}},\overrightarrow{01},\overrightarrow{10})$, donc de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01},\overrightarrow{10})$. On notera encore c cet élément. Nous noterons f_σ l'élément $c^{-1}\,{}^\sigma c$ de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01})$.

PROPOSITION 1. — *L'élément f_σ appartient à l'adhérence $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01})'$ du sous-groupe dérivé de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}},\overrightarrow{01})$.*

Il s'agit de démontrer que f_σ opère trivialement sur la fibre en $\overrightarrow{01}$ des revêtements étales abéliens de $\mathbf{P}'_{\overline{\mathbf{Q}}}$, et il suffit pour cela de traiter le cas des revêtements induits par les revêtements ramifiés $\mathbf{P}_{\overline{\mathbf{Q}}} \to \mathbf{P}_{\overline{\mathbf{Q}}}$ de la forme $z \mapsto z^n$ et de la forme $z \mapsto 1-(1-z)^n$, où n est un entier $\geqslant 1$. Traitons par exemple le premier cas, le second étant similaire. Les fibres $\mathrm{F}_{\overrightarrow{01}}$ et $\mathrm{F}_{\overrightarrow{10}}$ en $\overrightarrow{01}$ et $\overrightarrow{10}$ du revêtement considéré se composent respectivement des vecteurs tangents $(0,\zeta\frac{d}{dz})$ et $(\zeta,-\zeta\frac{d}{dz})$, où ζ parcourt l'ensemble des racines n-ièmes de l'unité. L'élément $\sigma_{\overrightarrow{01}}$ de $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{01})$ opère dans $\mathrm{F}_{\overrightarrow{01}}$ par $(0,\zeta\frac{d}{dz}) \mapsto (0,\zeta^{\chi_n(\sigma)}\frac{d}{dz})$ et l'élément $\sigma_{\overrightarrow{10}}$ de $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}},\overrightarrow{10})$ opère dans

$\mathrm{F}_{\overrightarrow{10}}$ par $(\zeta, -\zeta\frac{d}{dz}) \mapsto (\zeta^{\chi_n(\sigma)}, -\zeta^{\chi_n(\sigma)}\frac{d}{dz})$; la bijection de $\mathrm{F}_{\overrightarrow{01}}$ sur $\mathrm{F}_{\overrightarrow{10}}$ définie par c est $(0, \zeta\frac{d}{dz}) \mapsto (\zeta, -\zeta\frac{d}{dz})$. Il en résulte aussitôt que $f_\sigma = c^{-1}\,{}^\sigma c = c^{-1}\sigma_{\overrightarrow{10}} c \sigma_{\overrightarrow{01}}^{-1}$ opère trivialement dans $\mathrm{F}_{\overrightarrow{01}}$.

Les deux éléments $\chi(\sigma) \in \widehat{\mathbf{Z}}^\times$ et $f_\sigma \in \pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})'$ que nous venons d'associer à σ contiennent toute l'information nécessaire à décrire la manière dont σ opère dans $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$. En effet :

PROPOSITION 2. — *L'élément σ opère dans $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ en appliquant les générateurs canoniques x et y sur $x^{\chi(\sigma)}$ et $f_\sigma^{-1} y^{\chi(\sigma)} f_\sigma$ respectivement.*

Identifions $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ et $\pi_1^{ét}(\mathbf{P}'_{\mathbf{Q}}, \overrightarrow{01})$ aux groupes de Galois $\mathrm{Gal}(\mathrm{M}/\overline{\mathbf{Q}}(z))$ et $\mathrm{Gal}(\mathrm{M}/\mathbf{Q}(z))$, comme dans la remarque ci-dessus. Alors x et $\sigma_{\overrightarrow{01}}$ s'identifient respectivement aux automorphismes $\sum a_\lambda z^\lambda \mapsto \sum a_\lambda e^{2\pi i\lambda} z^\lambda$ et $\sum a_\lambda z^\lambda \mapsto \sum \sigma(a_\lambda) z^\lambda$ de M. On en déduit aussitôt que l'on a $\sigma_{\overrightarrow{01}} x \sigma_{\overrightarrow{01}}^{-1} = x^{\chi(\sigma)}$.

Lorsqu'on identifie $\widehat{\pi}$ à $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{10})$, les générateurs c_0 et c_1 de π s'identifient à des générateurs topologiques x' et y' de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{10})$, et l'on a $x = c^{-1}x'c$, $y = c^{-1}y'c$. Du premier alinéa, on déduit par transport de structure par l'automorphisme $z \mapsto 1 - z$ de $\mathbf{P}_{\mathbf{Q}}$ que l'on a ${}^\sigma y' = y'^{\chi(\sigma)}$. Il en résulte que l'on a

$$ {}^\sigma y = ({}^\sigma c)^{-1} y'^{\chi(\sigma)} ({}^\sigma c) = f_\sigma^{-1} c^{-1} y'^{\chi(\sigma)} c f_\sigma = f_\sigma^{-1} y^{\chi(\sigma)} f_\sigma \,, $$

d'où la proposition.

2.6. Le groupe de Grothendieck-Teichmüller

Soit $\widehat{\mathrm{F}}$ un groupe profini libre à deux générateurs x et y. Il sera commode, si u est un homomorphisme continu de $\widehat{\mathrm{F}}$ dans un autre groupe profini et si a, b sont les images de x et y par u, de noter $f(a,b)$ l'image par u d'un élément f de $\widehat{\mathrm{F}}$. Avec ces notations, on a en particulier $f = f(x,y)$.

Posons $\mathrm{M} = \widehat{\mathbf{Z}}^\times \times \widehat{\mathrm{F}}$. Pour $(\lambda, f) \in \mathrm{M}$ et $g \in \widehat{\mathrm{F}}$, posons

$$ {}^{(\lambda,f)}g = g(x^\lambda, f^{-1}y^\lambda f). \tag{4} $$

L'application $g \mapsto {}^{(\lambda,f)}g$ est un endomorphisme continu du groupe profini $\widehat{\mathrm{F}}$. Définissons une loi de composition $\star$ sur M en posant

$$ (\lambda, f) \star (\mu, g) = (\lambda\mu, f.{}^{(\lambda,f)}g)\,. \tag{5} $$

On vérifie tout d'abord que l'on a

$$ {}^{(\lambda,f)\star(\mu,g)}h = {}^{(\lambda,f)}({}^{(\mu,g)}h) \tag{6} $$

pour $(\lambda, f) \in \mathrm{M}$, $(\mu, g) \in \mathrm{M}$ et $h \in \widehat{\mathrm{F}}$, puis que la loi de composition de M est associative. Elle admet pour élément neutre le couple $(1,1)$. En d'autres termes, M, muni de la loi de composition $\star$, est un monoïde, et (4) définit une opération de ce monoïde dans le groupe $\widehat{\mathrm{F}}$.

Nous avons au numéro précédent associé à chaque élément $\sigma \in \mathbf{G}_{\mathbf{Q}}$ un élément $\chi(\sigma)$ de $\widehat{\mathbf{Z}}^\times$ et un élément f_σ de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$. Identifions désormais $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ au

groupe $\widehat{\mathrm{F}}$ (en identifiant les éléments de $\pi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ notés x et y au numéro précédent aux éléments x, y de F).

PROPOSITION 3. — *L'application $\sigma \mapsto (\chi(\sigma), f_\sigma)$ de $\mathrm{G}_{\mathbf{Q}}$ dans* M *est un homomorphisme. Son image est contenue dans le groupe des éléments inversibles de* M. *De plus, pour tout $\sigma \in \mathrm{G}_{\mathbf{Q}}$ et tout $g \in \widehat{\mathrm{F}}$, on a ${}^{\sigma}g = {}^{(\chi(\sigma), f_\sigma)}g$.*

Il suffit de démontrer la dernière assertion lorsque g est un des deux générateurs topologiques x, y de $\widehat{\mathrm{F}}$, et elle résulte dans ce cas de la prop. 2. Si σ et τ sont deux éléments de $\mathrm{G}_{\mathbf{Q}}$, on a $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ et

$$f_{\sigma\tau} = c^{-1}.{}^{\sigma\tau}c = c^{-1}.{}^{\sigma}c.{}^{\sigma}({c^{-1}}^{\tau}c) = f_\sigma .{}^{\sigma}f_\tau = f_\sigma .{}^{(\chi(\sigma), f_\sigma)}f_\tau$$

d'où la première assertion. La seconde en résulte aussitôt.

Il résulte du th. 2 et de la prop. 2 que l'homomorphisme $\sigma \mapsto (\chi(\sigma), f_\sigma)$ de $\mathrm{G}_{\mathbf{Q}}$ dans M est injectif. Un problème fondamental consiste à essayer d'en déterminer l'image, car cela fournirait une sorte d'écriture des éléments de $\mathbf{G}_{\mathbf{Q}}$ (un peu analogue à l'écriture décimale des nombres réels ou l'écriture des nombres p-adiques comme vecteurs de Witt).

Remarque. — On peut donner de M une interprétation un peu plus intrinsèque : notons B l'ensemble à deux éléments $\{\overrightarrow{01}, \overrightarrow{10}\}$ et $\varpi_1^{\mathrm{B}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ le sous-groupoïde plein de $\varpi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ ayant B pour ensemble de points. Alors M s'identifie à l'ensemble des endomorphismes u du groupoïde $\varpi_1^{\mathrm{B}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ qui fixent les deux points, et possèdent la propriété suivante : il existe un élément $\lambda \in \widehat{\mathbf{Z}}^{\times}$ tel que u applique l'élément x de $\pi_1(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ sur x^λ et l'élément y' de $\pi_1(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{10})$ sur ${y'}^{\lambda}$. (Un tel endomorphisme est déterminé dès que l'on se donne λ et l'image de c, que l'on écrit cf ; il applique alors y sur $f^{-1}y^\lambda f$, c^{-1} sur $f^{-1}c^{-1}$ et x' sur $cfc^{-1}{x'}^{\lambda}cf^{-1}c$.)

Nous allons maintenant passer en revue trois conditions, découvertes par Drinfeld, qui permettent de restreindre le monoïde dans lequel l'homomorphisme $\mathrm{G}_{\mathbf{Q}} \to \mathrm{M}$ prend ses valeurs.

CONDITION I. — *Si $(\lambda, f) \in \mathrm{M}$ appartient à l'image de $\mathbf{G}_{\mathbf{Q}}$, on a $f(x,y)f(y,x) = 1$.*

Dans l'interprétation de M donnée dans la remarque, pour qu'un élément (λ, f) de M soit tel que $f(x,y)f(y,x) = 1$, il faut et il suffit que l'automorphisme du groupoïde $\varpi_1^{\mathrm{B}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ correspondant soit invariant par l'automorphisme de $\varpi_1^{\mathrm{B}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ déduit de $z \mapsto 1 - z$. Il est dès lors clair que l'ensemble de ces éléments est un sous-monoïde de M qui contient l'image de $\mathrm{G}_{\mathbf{Q}}$.

CONDITION II. — *Si $(\lambda, f) \in \mathrm{M}$ appartient à l'image de $\mathbf{G}_{\mathbf{Q}}$, on a, en posant $z = (xy)^{-1}$ et $m = \frac{1}{2}(\lambda - 1)$, $f(z,x)z^m f(y,z)y^m f(x,y)x^m = 1$.*

Notons C l'ensemble des six éléments $\overrightarrow{ij}$, pour $i \neq j$ dans $\{0, 1, \infty\}$ et $\varpi_1^{\mathrm{C}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ le sous-groupoïde plein de $\varpi_1^{ét}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ ayant C pour ensemble de points. Dans l'interprétation de M donnée dans la remarque, pour qu'un élément (λ, f) de M satisfasse la condition I et la condition II, il faut et il suffit que l'automorphisme du groupoïde

$\varpi_1^{\mathrm{B}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$ correspondant se prolonge en un automorphisme u de $\varpi_1^{\mathrm{C}}(\mathbf{P}'_{\overline{\mathbf{Q}}})$, invariant par l'action du groupe des permutations de $\{0,1,\infty\}$ et tel que, si $d \in \varpi_1^{\acute{e}t}(\mathbf{P}'_{\overline{\mathbf{Q}}}; \overrightarrow{01}, \overrightarrow{0\infty})$ est la classe d'une « boucle reliant $\overrightarrow{01}$ à $\overrightarrow{0\infty}$ dans le demi-plan supérieur », $d^{-1}u(d)$ appartienne au sous-groupe fermé de $\pi_1(\mathbf{P}'_{\overline{\mathbf{Q}}}, \overrightarrow{01})$ engendré par x (auquel cas on a automatiquement $d^{-1}u(d) = x^m$ avec $m = \frac{1}{2}(\lambda - 1)$). Il est dès lors clair que l'ensemble des éléments de M satisfaisant les conditions I et II est un sous-monoïde de M qui contient l'image de $\mathrm{G}_{\mathbf{Q}}$.

CONDITION III. — Cette condition, plus technique, fait intervenir les relations entre les espaces de modules $M_{0,4}$ et $M_{0,5}$. Je n'ai pas réussi à en donner une interprétation aussi simple que pour les conditions I et II. Je renvoie donc pour la discussion de cette condition à l'article original de Drinfeld ([7]) et à ceux d'Ihara ([10], [11]).

L'ensemble des éléments inversibles de M qui satisfont les conditions I, II, III, est un groupe appelé le groupe de Grothendieck-Teichmüller et noté $\widehat{\mathrm{GT}}$. Une question naturelle est de savoir si l'image de $\mathrm{G}_{\mathbf{Q}}$ dans M est égale à $\widehat{\mathrm{GT}}$. Récemment, Yves André a développé un analogue local de ce formalisme pour $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ et démontré que ce groupe se réalise comme le groupe des automorphismes d'un foncteur π_1 approprié en géométrie p-adique.

APPENDICE : CARTES

1. Cartes cellulaires

En suivant [14], déf 1.1.1, nous appellerons *carte cellulaire* (de dimension 2) un triplet $\mathrm{G} = (\mathrm{X}, \mathrm{K}, \mathrm{S})$, où X est une surface topologique compacte (sans bord), K une partie fermée de X et S une partie finie de K, telles que : $\mathrm{X} - \mathrm{K}$ a un nombre fini de composantes connexes, chacune homéomorphe à un 2-disque ouvert ; $\mathrm{K} - \mathrm{S}$ a un nombre fini de composantes connexes, chacune homéomorphe à un 1-disque ouvert ; tout point de S est adhérent à $\mathrm{K} - \mathrm{S}$. Lorsque la surface topologique X est munie d'une orientation, on dit que la carte G est *orientée*.

Les points de S, les composantes connexes de $\mathrm{K} - \mathrm{S}$ et les composantes connexes de $\mathrm{X} - \mathrm{K}$ s'appellent respectivement les *sommets*, les *arêtes* et les *faces* de G. Ils définissent une décomposition cellulaire de X. Le bord de chaque face est réunion d'une famille d'arêtes et de sommets. Le bord de chaque arête se compose d'un ou deux sommets. Chaque arête est contenue dans le bord d'une ou de deux faces.

Si A est une arête et x un point de A, la limite projective des ensembles $\pi_0(\mathrm{U} - \mathrm{A})$, où U parcourt l'ensemble des voisinages de x dans X, a deux éléments ; chacun d'eux s'appelle une *rive* (ou une *orientation transverse*) de A en x. Lorsque l'arête A et la surface X sont orientées en x, on peut parler des rives gauche et droite de A en x.

2. Cartes triangulaires tricoloriées

Une *carte triangulaire* est une carte cellulaire (X, K, S) dans laquelle l'adhérence de chaque face, munie de la décomposition cellulaire induite par celle de X, est isomorphe à un simplexe euclidien de dimension 2 muni de la décomposition cellulaire standard. Le bord de chaque arête se compose alors de deux sommets (appelés ses extrémités), et le bord de chaque face comprend trois arêtes et trois sommets.

On appelle *carte triangulaire tricoloriée* un quadruplet (X, K, S, t), où (X, K, S) est une carte triangulaire et t une application qui assigne à chaque sommet un type dans $\{0, 1, \infty\}$, les trois sommets adhérents à une même face étant de types distincts. Si A est une arête d'une telle carte, les extrémités de A sont de types i et j distincts, et l'on dit que A est de type $\{i, j\}$.

Si une carte triangulaire tricoloriée est *orientée*, ses faces se divisent en faces positives et négatives : une face est positive si l'ordre cyclique dans lequel se succèdent les types de ses sommets sur son bord orienté est $0, 1, \infty$.

Soient $G = (X, K, S, t)$ et $G' = (X', K', S', t')$ deux cartes triangulaires orientées tricoloriées. Notons $\mathscr{T}(G, G')$ l'ensemble des applications continues $f : X \to X'$ qui induisent un homéomorphisme de l'adhérence de chaque face de X sur l'adhérence d'une face de X', cet homéomorphisme respectant la décomposition cellulaire, le type des sommets et l'orientation.

La *catégorie isotopique des cartes triangulaires orientées tricoloriées* est la catégorie dont les objets sont les cartes triangulaires orientées tricoloriées, un morphisme de G dans G' étant une classe d'isotopie, c'est-à-dire une composante connexe par arcs, de l'ensemble $\mathscr{T}(G, G')$ muni de la topologie de la convergence compacte.

3. Cartes cellulaires bicoloriées

On appelle *carte cellulaire bicoloriée* un quadruplet (X, K, S, t), où (X, K, S) est une carte cellulaire et b une application qui assigne à chaque sommet un type dans $\{0, 1\}$, chaque arête possédant une extrémité de type 0 et une extrémité de type 1.

Lorsqu'une carte cellulaire bicoloriée est orientée, chaque arête est munie en chacun de ses points d'une rive gauche et d'une rive droite (déterminées par l'orientation de l'arête du sommet de type 0 vers le sommet de type 1 et par l'orientation donnée de X).

Soient $G = (X, K, S, b)$ et $G' = (X', K', S', b')$ deux cartes cellulaires bicoloriées orientées. Notons $\mathscr{B}(G, G')$ l'ensemble des applications continues $f : X \to X'$ telles que $f^{-1}(S') = S$ et $f^{-1}(K') = K$, qui respectent les types des sommets et le caractère gauche ou droit des rives des arêtes.

La *catégorie isotopique des cartes cellulaires bicoloriées orientées* est la catégorie dont les objets sont les cartes cellulaires bicoloriées orientées, un morphisme de G dans G' étant une classe d'isotopie, c'est-à-dire une composante connexe par arcs, de l'ensemble $\mathscr{B}(G, G')$ muni de la topologie de la convergence compacte.

Remarque. — On définit une équivalence de la catégorie isotopique des cartes triangulaires orientées tricoloriées sur la catégorie isotopique des cartes cellulaires bicoloriées orientées par $G = (X, K, S, t) \mapsto (X, K', S', b)$, où S' est l'ensemble des sommets de G de type 0 ou 1, b coïncide avec t dans S' et K' est la réunion de S' et des arêtes de type $\{0, 1\}$ de G.

RÉFÉRENCES

[1] G. BELYĬ – « Galois extensions of a maximal cyclotomic field », *Izv. Akad. Nauk SSSR, Ser. Mat.* **43** (1979), no. 2, p. 267–276, en russe ; traduction anglaise dans : *Math. USSR Izv.* **14** (1979), p. 247-256.

[2] B. BIRCH – « Noncongruence subgroups, covers and drawings », in *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, p. 25–46.

[3] K. COMBES & D. HARBATER – « Hurwitz families and arithmetic Galois groups », *Duke Math. J.* **52** (1985), p. 821–839.

[4] J.-M. COUVEIGNES – « À propos du théorème de Belyĭ », *J. Théor. Nombres Bordeaux* **8** (1996), no. 1, p. 93–99.

[5] P. DÈBES & J.-C. DOUAI – « Algebraic covers : field of moduli versus field of definition », *Ann. scient. Éc. Norm. Sup.* 4^e *série* **30** (1997), p. 303–338.

[6] P. DELIGNE – « Le groupe fondamental de la droite projective moins trois points », in *Galois groups over* **Q**, Publ. MSRI, vol. 16, Springer, 1989, p. 79–298.

[7] V. G. DRINFELD – « On quasi-triangular quasi-Hopf algebras and some group closely associated with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ », *Leningrad Math. J.* **2** (1991), p. 829–860.

[8] A. GROTHENDIECK – « Technique de descente et théorèmes d'existence en géométrie algébrique, I. Généralités. Descente par morphismes fidèlement plats », in *Séminaire Bourbaki 1959/1960*, Benjamin, 1966, exp. n° 190 (réédité par la S.M.F en 1995).

[9] ———, « Esquisse d'un programme », in *Geometric Galois Actions*, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, p. 5–48.

[10] Y. IHARA – « Braids, Galois groups, and some arithmetic functions », in *Proceedings of the ICM (Kyoto, 1990)*, p. 99–120.

[11] ———, « On the embedding of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into $\widehat{\mathrm{GT}}$ », in *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, p. 289–305.

[12] L. SCHNEPS – « Dessins d'enfants », in *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, p. 47–77.

[13] *Revêtements étales et groupe fondamental, Séminaire de Géométrie Algébrique du Bois-Marie 1960/1961 (SGA 1)* – Lect. Notes in Math., vol. 224, Springer, 1970, dirigé par A. Grothendieck.

[14] C. VOISIN & J. MALGOIRE – *Cartes cellulaires*, Cahiers mathématiques, vol. 12, Université de Montpellier, 1977.

Joseph OESTERLÉ

Institut de mathématiques de Jussieu
175, rue du Chevaleret
F-75013 Paris
E-mail : oesterle@math.jussieu.fr