
LA LONGUE MARCHÉ À TRAVERS LA
THÉORIE DE GALOIS
A. GROTHENDIECK

La “Longue Marche” à Travers la Théorie de Galois

avec Notes

<https://grothendieck.umontpellier.fr/archives-grothendieck/>

Ce texte a été déchiffré et transcrit par Mateo Carmona et Matthias Kunzer

SOMMAIRE

1. Topos multigaloisiens	6
2. Application aux revêtements des topos	10
3. Variantes pro-multigaloisiennes	12
4. Compléments, remords	13
5. Introduction du contexte arithmétique; “conjecture anabélienne fondamentale”	15
6. Analyse locale de (X, S) en un $s \in S$	19
7. Reformulation “bordélique” de la conjecture (le purgatoire nécessaire...)	21
8. Réflexions taxonomiques	25
9. Structure tangentielle en les $s \in S$	26
10. Ajustement des hypothèses (remords)	27
11. Conditions sur les systèmes de groupoïdes obtenus à partir de situations géométriques	29
12. L’analogie topologique	30
13. Retour au cas arithmétique; formulation “galoisienne”	31
13 bis. Retour sur la notion de groupe à lacets	33
14. Digression cohomologique (sur le “bouchage de trous”)	34
14 bis. Où on revient sur les morphismes mixtes	35
15. Retour sur le cas topologique: orbites critiques des scindages d’extensions; . . .	36
16. Bouchage et forage de trous: préliminaires topologiques généraux	37
17. Complément au §15; sous-groupes de groupes à lacets	38
18. Forage de trous; applications aux sous-groupes finis de $\text{Autext}_{\text{lac}}(\pi)$	39
19. Tour de Teichmüller	40
20. Digression: description 2-isotopique de la catégorie des isomorphismes topologiques	41
21. Les espaces de Teichmüller	42

A. GROTHENDIECK

23. Retour sur les surfaces à groupes (finis) d'opérateurs ("mise en équations" du problème)	43
24. Essai de détermination de \mathcal{A}^{or} ; lien avec les relations $\pi_{g,(\nu, \nu+n-1)}^\Gamma = \{1\}$, programme de travail	44
25. Groupes de Teichmüller "spéciaux"	45
25 bis. "Cas des deux groupes" d'opérateurs; retour sur les notations	46
26. Groupes de Teichmüller profinis (Discrétification et prédiscrétification)	47
27. Changement de type (g, ν)	58
28. Changement de type (g, ν) (suite)	65
29. Critique de l'approche précédente	73
30. Propriétés des $\mathcal{N}_{g,\nu}, \Pi_{g,\nu}$	80
a) Propriétés liées aux sous-groupes finis	80
31. Digression sur les relèvements d'une action extérieure d'un groupe fini	85
32. Retour sur les aspects arithmétiques du bouchage de trous: relations entre $\Pi_{g,\nu}$ et $\Pi_{g,\nu-1}$	87
33. Digression topologique	105
33bis. Etude des revêtements finis - relation entre les $\mathcal{N}_{g,\nu}, \Gamma_{g,\nu}$ pour g variable . . .	123
34. Description heuristique profinie de la catégorie des courbes algébriques définies sur des sous-extensions finies K de $\overline{\mathbb{Q}}/\mathbb{Q}$ (i.e. de \mathbb{C}/\mathbb{Q})	128
35. L'injectivité de $\Pi_{\mathbb{Q}} \rightarrow \text{Autext}_{\text{lac}}(\hat{\pi}_{0,3})$	132
36. L'isomorphisme $\Pi_{\mathbb{Q}} \xrightarrow{\sim} \Pi_{1,1}$ et l'injectivité de $\Pi_{\mathbb{Q}} \rightarrow \text{Autext}(\hat{\mathfrak{Z}}_{1,1}^+) \simeq \text{Autext}(SL(2, \mathbb{Z})^\wedge)$	138
37. Théorie des modules des courbes elliptiques via Legendre	152
38. Détermination de $\pi_{0,3}[\cdot]$	174
39. Propriétés de congruence de l'opération de $\Pi_{\mathbb{Q}}$ sur $\hat{\pi}_{0,3}$, liées à l'homomorphisme $\mathcal{N}_{1,1} \longrightarrow GL(2, \hat{\mathbb{Z}})$	175
40. Paraphrase topologico-isotopique de la théorie de Legendre	176
43. Digression sur les 1-cocycles des groupes cycliques	179
44. Retour sur les notations. Mise en équations dans $SL(2, \hat{\mathbb{Z}})$	180
46. Notations définitives (?) - récapitulation des calculs pour les automorphismes à lacets de $\hat{\pi}_{0,3}$ et de $\hat{\mathfrak{E}}_{0,3}^+$	182

47. Retour sur l'homomorphisme $\hat{\pi}_{0,3} \xrightarrow{\hat{\phi}} \hat{\mathfrak{S}}_{0,3}^+$, les groupes $\widetilde{\mathcal{M}}_{l,\varnothing}, \widetilde{\mathcal{N}}_{l,\varnothing}, \widetilde{\mathcal{M}}_{l,\varnothing}^!(l)$. . .	183
48. Construction d'un schéma en groupes	184
49. Les groupes $\mathcal{M}_{\rho,\sigma}$ généraux	185
50. Enveloppes schématiques de groupes discrets: cas métabélien	186
Exemple: la tour de Fermat	187
52. Approximations de Lie des systèmes de Galois-Teichmüller	188
Notes	189
I. Théorie de Kummer	190
II. Action de Galois sur Teichmüller	191
III. Paradigmes des courbes algébriques (version provisoire)	192
IV. Teichmülleries	193
V. Printemps 81 (vieille rédaction)	194
VI. Groupoïdes de Teichmüller et les $S_0 \text{ Tg}^!, S_0 \text{ TG}$	195
VII. Structure à l'infini des $M_{g,\nu}$	196
VIII. Teichmüller	202
IX. Notes Anabéliennes	203

§ 1. — TOPOS MULTIGALOISIENS

Proposition (1.1). — Soit E une catégorie. Conditions équivalentes :

a) E est un topos, et tout objet de E est localement constant.

b) E est équivalent à une catégorie \widehat{C} , où C est un groupoïde (on verra plus loin que l'on peut choisir C canoniquement).

b') Il existe une famille $(G_i)_{i \in I}$ de groupes et une équivalence de catégories

$$E \xrightarrow{\sim} \prod_{i \in I} \text{Ens}(G_i)$$

c) Conditions d'exactitudes ad-hoc, du type de celles données dans SGA1 ...

Démonstration. $b) \Rightarrow b') \Rightarrow a)$ immédiat. Pour $a) \Rightarrow b)$ je suis moins sûr, peut être faut-il supposer que E est localement connexe, et qu'il a suffisamment de foncteurs fibres i.e. suffisamment de points.

Définition (1.2). — Si les conditions équivalentes b), b') ci-dessus sont satisfaites, on dit que C est un topos multigaloisien (ou une catégorie multigaloisienne).

Proposition (1.3). —

a) Si E est multigaloisien tout topos induit C/S aussi.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

b) Toute somme de topos multigaloisiens (i.e. tout produit de catégories multigaloisiennes) est un topos multigaloisien.

Proposition (1.4). — Soient E un topos, C la catégorie des points de E , (opposée à la catégorie des foncteurs fibres sur E). Le foncteur canonique $E \times C^\circ \longrightarrow \text{Ens}$ induit un foncteur canonique

$$E \longrightarrow \text{Hom}(E^\circ, \text{Ens}) = \widehat{C}$$

Ceci posé [E étant multigaloisien]

a) C est un groupoïde (appelé groupoïde fondamental du topos multigaloisien E et souvent noté $\Pi_1(E)$).

b) $E \longrightarrow \widehat{C}$ est une équivalence de catégories.

Un objet S d'un topos E est dit 0-connexe s'il est $\neq \emptyset_E$ (i.e. n'est pas objet initial) et s'il est connexe (i.e. $S \simeq S' \amalg S''$ implique $S' \simeq \emptyset_E$ ou $S'' \simeq \emptyset_E$) - cela signifie aussi que le topos induit E/S est 0-connexe i.e. n'est pas le topos initial ("topos vide", équivalent à la catégorie finale) et qu'il est connexe, i.e. ...

On dit que S est 1-connexe (ou simplement connexe) s'il est 0-connexe et si tout objet S' de E/S localement constant est constant - ce qui ne dépend encore que du topos induit E/S , qui sera dit alors 1-connexe.

Proposition (1.5). — Soit E un topos multigaloisien, et soit S un objet de E . Conditions équivalentes :

a) S est 1-connexe

b) S est 0-connexe et projectif

c) Le foncteur covariant représenté par S

$$T \mapsto \text{Hom}_E(S, T)$$

est un foncteur fibre, ou encore (comme il est déjà exact à gauche) il commute aux \varinjlim inductives quelconques (N.B. il suffit qu'il commute aux sommes et aux passages aux quotients ...)

A. GROTHENDIECK

d) E/S est équivalent au topos ponctuel

e) (Si $E = \widehat{C}$, C un groupoïde) le foncteur S sur C est représentable.

Définition (1.6). — On dit alors, parfois que S (ou mieux, le topos E/S) est un revêtement universel du topos multigaloisien E .

Proposition (1.7). — Soit E_\circ la sous-catégorie pleine de E formée des objets 1-connexes (de la catégorie multigaloisienne E), et $\Pi_1(E)$ le groupoïde fondamental de E . On a par (1.5). un foncteur canonique

$$E_\circ \longrightarrow \Pi_1(E)$$

(associant à tout $S \in \text{Ob}(E_\circ)$ le foncteur fibre qu'il représente, ou plutôt le "point" correspondant de C), qui est (non seulement pleinement fidèle mais même) une équivalence de catégorie : tout foncteur fibre sur E est représentable (par un objet (1-connexe) essentiellement unique comme de juste ...)

Corollaire (1.8). — Soit P un "point" de E (associé à un foncteur fibre F_P). Il existe un objet 1-connexe S de E et un relèvement

$$\begin{array}{ccc} P & \xrightarrow{\alpha} & E/S \\ & \searrow & \swarrow \\ & E & \end{array}$$

(i.e. $\alpha \in F(S)$) et cela détermine (S, α) à isomorphisme près.

En fait, S est l'unique objet de E qui représente F_P ...

Définition (1.9). — On dit que S (ou E/S) est le revêtement universel ponctué au dessus de P déterminé par le point P .

Scholie (1.10). Se donner un "point" du topos multigaloisien E , ou se donner un revêtement universel, revient essentiellement au même : chacun détermine l'autre ...

Proposition (1.11). — Soient E, E' deux topos multigaloisiens, $\Pi_1(E), \Pi_1(E')$ leur groupoïdes fondamentaux. Le foncteur évident

$$\text{Hom}_{\text{top}}(E, E') \longrightarrow \text{Hom}(\Pi_1(E), \Pi_1(E'))$$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

est une équivalence de catégories ; posant $C = \Pi_1(E)$, $C' = \Pi_1(E')$ on trouve une équivalence quasi-inverse en composant

$$\begin{array}{ccc} \mathrm{Hom}(C, C') & \longrightarrow & \mathrm{Hom}_{top}(\widehat{C}, \widehat{C'}) \xrightarrow{\sim} \mathrm{Hom}_{top}(C, C') \\ & & \cap \\ & & \mathrm{Hom}(\widehat{C}, \widehat{C'}) \end{array}$$

(1.12). Explicitation du cas où E, E' sont 0-connexes et ponctués, donc donnés comme $E \simeq \mathrm{Ens}(G), E' \simeq \mathrm{Ens}(G') \dots$

§ 2. — APPLICATIONS AUX REVÊTEMENTS DES TOPOS

Théorème (2.1). — *soit E un topos localement connexe (i.e. dont tout objet est somme d'objets connexes) et localement simplement connexe (i.e. admettant un système de générateurs qui sont 1-connexes) ⁽¹⁾. Alors la catégorie E_{lc} des objets localement constants de E est un topos multigaloisien, et l'inclusion*

$$(2.1.1.) \quad E_{lc} \hookrightarrow E$$

commute aux \varprojlim finies (N. B. en fait sans hypothèses sur le topos E , E_{lc} est stable par \varprojlim finies) et aux \varinjlim quelconques.

Définition (2.2). — *On dénote ce topos par $E_{[1]}$, on l'appelle l'enveloppe multigaloisienne de E et le morphisme de topos transposé de l'inclusion (2.1.1.) :*

$$E \longrightarrow E_{[1]}$$

prend le nom de morphisme canonique.

N. B. C'est l'équivalent en théorie des topos de l'opération de "tuage des π_i pour $i \leq 2$ ". On peut définir aussi $E_{[0]}$ et une suite

$$E \longrightarrow E_{[1]} \longrightarrow E_{[0]}$$

($E_{[0]}$ est le topos *discret* défini par $\pi_0(E)$, qui a un sens satisfaisant dès que E localement connexe ...).

¹N.B. peut-être faut-il supposé que E ait "assez de points" i.e. assez de foncteurs libres...

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Moyennant des hypothèses convenables sur E (du type “locale contractibilité”), on doit pouvoir définir les $E_{[i]}$ pour tout $i \in \mathbb{N}$, et des morphismes canoniques

$$E \longrightarrow \dots E_{[i]} \longrightarrow E_{[i-1]} \longrightarrow \dots E_{[1]} \longrightarrow E_{[0]}$$

(2.3). Le *groupeïde fondamental* de E se définit comme ayant pour objets les points de E (qui induisent des points de $E_{[1]}$ grâce à $E_{[1]} \longrightarrow E$), et comme morphismes les morphismes *de points* de $E_{[1]}$. On a donc des foncteurs canoniques

$$\underline{\text{Pt}}(E) \xrightarrow{\alpha} \Pi_1(E) = \Pi_1(E_{[1]})$$

où β est une équivalence (mais pas surjectif sur les objets), et où bien sur α n’est pas nécessairement une équivalence ni même pleinement fidèle, ou seulement fidèle.

Par exemple si E est 1-connexe (i.e. $\Pi_1(E)$ équivalent à la catégorie ponctuelle, il ne s’ensuit pas nécessairement que les Hom dans $\underline{\text{Pt}}(E)$ soient tous de cardinal ≥ 1 !)

Comme un point P de E définit un point (noté encore P par abus) de $E_{[1]}$, on peut donc définir le *revêtement universel* de E basé en ce point, comme un objet S 1-connexe de $E_{[1]}$ - il est caractérisé dans E par le fait d’être localement constant, 1-connexe, et muni d’un relèvement

$$P \longrightarrow E/S$$

Mais comme α n’est pas une équivalence de catégorie (bien qu’il soit essentiellement surjectif si on suppose que E a suffisamment de points ...) on *ne peut pas* dire que tout revêtement universel de E soit défini à isomorphisme unique près

§ 3. — VARIANTES “PRO-MULTIGALOISIENNES”, RESPECTIVEMENT PROFINIES



(en se bornant, pour simplifier, au cas des topos localement connexes ...)

§ 4. — COMPLÉMENT-REMORD SUR LES CATÉGORIES MULTIGALOISIENNES

qui précise l'intention que pour un topos E , la donnée d'un objet $S \in E$ définit un topos induit $E/S \longrightarrow E$, et que S se reconstitue à isomorphisme près par la connaissance du topos induit en tant que topos *au dessus* de E . Ici, E étant multigaloisien, E/S aussi - et il se pose la question quand un morphisme de topos multigaloisien $E' \longrightarrow E$ peut être considéré comme un morphisme d'induction. Si $C = \Pi_1(E)$, $C' = \Pi_1(E')$, la donnée de $E' \longrightarrow E$ équivaut à la donnée d'un foncteur $C' \longrightarrow C$.

On trouve que $E' \longrightarrow E$ est un morphisme d'induction si et seulement si $C' \longrightarrow C$ est *fidèle*. Ainsi, on trouve une équivalence entre la catégorie E (des objets S de la catégorie multigaloisienne $E \simeq \widehat{C}$, où C est un groupoïde quelconque si on y tient ⁽²⁾) et la catégorie dont les objets sont les "groupoïdes C' au dessus de C ", avec un foncteur structural $C' \longrightarrow C$ *fidèle*, les morphismes de C'_1 dans C'_2 étant les *classes d'isomorphie* ⁽³⁾ de couples (f, α) d'un foncteur $f : C'_1 \longrightarrow C'_2$ et d'un isomorphisme de foncteurs $\alpha : p_1 \xrightarrow{\sim} p_2 \circ f$

$$\begin{array}{ccc} C'_1 & \xrightarrow{f} & C'_2 \\ & \searrow p_1 \quad \swarrow p_2 & \\ & C & \end{array}$$

Dans le cas où par exemple C est la catégorie réduite à un seul objet, avec groupe d'automorphisme G , cette description de la catégorie $E = \text{Ens}(G)$ est évidemment un peu

²un peu vif !

³préciser les isomorphismes entre couples (f, α) et (g, β) ...

A. GROTHENDIECK

lourde, mais elle s'insère bien dans certains contextes plus bas.

Ainsi, si k est un corps de base, la catégorie E des schémas étales sur k se décrit, en terme d'une clôture séparable k_s de k et du groupe profini $\Gamma = \text{Gal}(k_s/k)$, comme les groupoïdes profinis au dessus du groupoïde profini $(pt, \Gamma) \dots$ Nous voulons insérer cette description dans une “description” “galoisienne” de [certains] schémas [lisses quasi-projectifs de dimension ≤ 1] sur k , du moins si k corps de type fini sur Q .

§ 5. — INTRODUCTION DU CONTEXTE ARITHMÉTIQUE; “CONJECTURE ANABÉLIENNE FONDAMENTALE”

Soit K une extension de type fini de \mathbb{Q} , et choisissons une clôture algébrique \bar{K} de K . On pose $\Gamma = \text{Gal}(\bar{K}/K)$.

5.1. Nous considérons des couples (X, S) , où :

- a) X est un schéma projectif et lisse sur K , de dimension ≤ 1 ;
- b) S est sous schéma fini réduit de X (donc fini étale sur K) contenu dans la réunion des composantes irréductibles de dimension 1 de X .

Les morphismes $(X', S') \longrightarrow (X, S)$ seront par définition les morphismes de schémas

$$f : X' \longrightarrow X$$

tels que

$$S' = f^{-1}(S)_{red}$$

i.e. tels que $\text{supp } S' = f^{-1}(\text{supp } S)$.

Nous cherchons une “description galoisienne” de cette catégorie, ou tout au moins d’une sous-catégorie pleine V_K que nous allons définir maintenant.

Lemme (5.2). — *Soit Γ un corps algébriquement clos, X une courbe projective lisse connexe sur Ω , S une partie finie de $X(\Omega)$, $U = X \setminus S$, g le genre de X et $n = \text{card } S$. Conditions équivalentes :*

A. GROTHENDIECK

- a) $\pi_1(U)$ non abélien,
- b) $\text{Aut}(U)$ fini,
- c) pour tout schéma connexe réduit X de type fini sur Ω , l'ensemble des morphismes non constants de X dans U est fini,
- d) on est dans l'un des trois cas suivant : 1°) $g \leq 2$ 2°) $g = 1, n \leq 1$ 3°) $g = 0, n \leq 3$
- e) (si $\Omega \subset \mathbb{C}$) le revêtement universel de $X(\mathbb{C}) \setminus S(\mathbb{C})$ est isomorphe au demi plan de Poincaré,
- f) (??) (si $\Omega = \overline{\mathbb{Q}}, S \neq \emptyset$) Le revêtement universel de $X \setminus S = U$ est isomorphe à celui de $P_\Omega^1 \setminus \{0, 1, \infty\}$.

Définition (5.3). — On dit alors que (X, S) est anabélien.

Comme cette condition est (par d) par exemple) invariante par extension du corps de base algébriquement clos, on étend cette définition au cas d'un couple (X, S) , avec (X, S) comme dans (5.1) (**N.B.** On regarde séparément les composantes connexes de $X_{\overline{K}} \dots$). dorénavant, dans (5.1) nous allons nous borner au cas de couples (X, S) anabéliens.

(5.4). A un couple (X, S) (pas nécessairement anabélien) - plus généralement à tout schéma X localement de type fini sur S - on associe un objet “de nature galoisienne” [à] savoir le groupoïde fondamental profini $\Pi(X)$ de X (fermé (?) si on veut des revêtements universel de X), muni d'un foncteur canonique

$$\begin{array}{ccc} \Pi_1(X) & \longrightarrow & \Pi_1(K) \\ & \parallel & \\ & [\text{Tors}(\Gamma)] & \end{array}$$

Un morphisme de K -schémas

$$X' \xrightarrow{f} X$$

définit un foncteur

$$\Pi_1(X') \xrightarrow{\Pi_1(f)} \Pi_1(X)$$

et un isomorphisme de commutation α :

[]

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

On trouve ainsi un foncteur, de la catégorie des schémas localement de type fini X sur K , dans la “catégorie des groupoïdes profinis sur $\Pi_1(K)$ ”, définie comme au $n^\circ 4$.

Quand on passe à la catégorie des schémas localement de type fini connexes, *munis d'un point géométrique au dessus de \bar{K}/K* ⁴ (i.e. d'un $x \in X$, d'une clôture séparable $\bar{k}(x)$ de $k(x)$ et d'un K -morphisme $\bar{K} \hookrightarrow \bar{k}(x)$), cela correspond à un foncteur des K -schémas localement de type fini et connexes, ponctués sur \bar{K}/K (au sens précédent) vers la catégorie des groupes profinis Π munis d'un homomorphisme (de groupes profinis)

$$\Pi \longrightarrow \Gamma$$

(dont l'image sera d'ailleurs nécessairement ouverte donc d'indice fini, pour des objets provenant de X comme [ci-]dessus).

Conjecture (5.5)⁵ — *La restriction du foncteur précédent $X \mapsto (\Pi_1(X) \text{ sur } \Pi_1(K))$ aux schémas projectifs lisses de dimension ≤ 1 et anabéliens (i.e. tels que (X, S) soit anabélien, où S est la réunion des composantes de dimension 0) est pleinement fidèle.*

Il revient au même de dire ceci:

Définition (5.5 bis). — *Le foncteur qui, à tout X comme dans 5.5. et de plus connexe, (de dimension 0 ou 1), muni d'un point géométrique ξ au dessus de \bar{K} , associe le groupe profini $\pi_1(X, \xi)$ sur $\Gamma = \pi_1(K, \xi)$, est un foncteur pleinement fidèle.*

Il faut quand même expliciter les morphismes $(X, \xi) \longrightarrow (X', \xi')$ dans la catégorie de départ : morphismes de K -schémas $X \xrightarrow{f} X'$, munis d'un morphisme (ou classe de chemins) $f(\xi) \simeq \xi'$.

Ces conjectures se réduisent à la théorie de Galois, pour des X de dimension 0. Pour des X de dimension 1, elles ne concernent que des X tels que les composantes connexes de $X_{\bar{K}}$ soient de genre ≤ 2 (ou, ce qui revient au même, introduisant l'extension finie $K' = H^0(X, \underline{O}_X)$ de K , de sorte que X soit géométriquement connexe sur K' , tel que X comme courbe algébrique sur K' soit de genre ≤ 2 . On voit aisément (prenant $X' = (K)$, $X = P_K^1$ courbe elliptique sur K) qu'elles deviennent fausses sinon - c'est pourquoi il a fallu introduire S , plus l'hypothèse

⁴il vaut mieux dire : munis d'un revêtement universel...

⁵c'est un peu faux cf $n^\circ 9$

A. GROTHENDIECK

anabélienne sur (X, S) , pour associer à (X, S) une structure plus riche que $\Pi_1(X)$ sur $\Pi_1(K)$. On trouvera des conjectures (par exemple) pour X courbe géométriquement connexe sur K de genre 1 (resp. 0), *pourvu* que S soit de degré ≤ 1 (resp. ≤ 3).

§ 6. — ANALYSE LOCALE DE (X, S) EN UN $s \in S$

On s'intéresse au cas où $\dim_s(X) = 1$, i.e. où s n'est pas point isolé dans X .

Soit \underline{O}_s le hensélisé (ou le complété, si on y tient) de $\underline{O}_{X,s}$, K_s son corps de fractions, $D_s^* = \text{Spec}(K_s)$, on identifie s à $k(s)$ ($k(s)$ est le corps résiduel de l'anneau-jauge \underline{O}_s)... Considérons $D_s = \text{Spec}(\underline{O}_s)$ ("disque arithmétique relatif à $k(s)$ "), donc $D_s^* = D_s \setminus s =$ ("disque épointé") $\longrightarrow D_s$, on a

[]

Pour le choix d'un point géométrique ξ_s de D_s^* sur \bar{K}/K (i.e. d'une clôture algébrique \bar{K}_s de K_s et d'une K -injection $\bar{K} \hookrightarrow \bar{K}_s$), ce diagramme de groupoïdes se reflète en un homomorphisme de groupes ⁶ de

[]

dont le noyau, on le sait par Kummer, est canoniquement isomorphe à $T(\bar{k}_s) \simeq T(\bar{K}_s) [\simeq T(\bar{K})]$.

On veut exprimer la donnée de cet isomorphisme privilégié comme une structure supplémentaire sur (6.1) - i.e. sur le groupoïde $\Pi_1(D_s^*)$ sur $\Pi_1(s)$ (ou sur $\Pi_1(K)$) - On peut le dire ainsi: si à tout $\xi \in \Pi - 1(D_s^*)$, on associe le noyau de

$$\text{Aut}(\xi) \longrightarrow \text{Aut}(i(\xi))$$

(qui est aussi le noyau des composés

$$\text{Aut}(\xi) \longrightarrow \text{Aut}(i(\xi)) \longrightarrow \text{Aut}(p_s(\xi) = q_s(i_s(\xi)))$$

⁶**N.B.** Le choix de \bar{K}_s implique un choix de \bar{k}_s - c'est la flèche pointillée (6.1).

A. GROTHENDIECK

on trouve un groupe *abélien*, qui ne dépend (à isomorphisme près) que de $i(\xi) = \xi'$ [ceci, et la suite de la phrase, marche chaque fois qu'on a un foncteur de groupoïdes connexes à noyau abélien et surjectif sur les Hom], et pour ξ' variable forme un système local sur $\Pi_1(D_s)$, qu'on peut appeler le π_1 *relatif* du groupoïde $\Pi_1(D_s^*)$ sur le groupoïde $\Pi_1(D_s)$.

Ceci dit, on a un isomorphisme de systèmes locaux de groupes

$$\pi_1(\Pi_1(D_s^*) \text{ sur } \Pi_1(D_s)) \simeq q_s^*(T_K)$$

où T_K est le système local de Tate sur K .

Posons maintenant

$$D_S = \prod_{s \in S} D_s \quad (\text{"multidisque arithmétique en } S\text{"})$$

$$D_S^* = \prod_{s \in S} D_s^* \quad (\text{"multicouronne arithmétique en } S\text{"})$$

On a un homomorphisme de groupoïdes

$$\Pi_1(D_s^*) \xrightarrow{\sigma_s} \Pi_1(S) \quad (\xrightarrow{j_s} \Pi_1(K))$$

et un isomorphisme canonique

$$([\]_S)/\Pi_1(S) \simeq j_S^*(T(K))$$

Ceci posé, on a aussi un morphisme

$$D_s^* \xrightarrow{\rho_s} X \setminus S$$

induisant

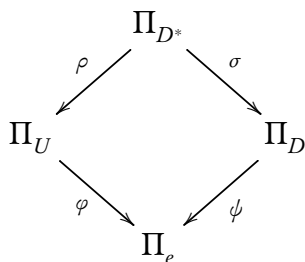
$$\Pi_1(D_s^*) \xrightarrow{\Pi_1(\rho_s)} \Pi(X \setminus S).$$

§ 7. — REFORMULATION “BORDÉLIQUE” DE LA CONJECTURE (LE PURGATOIRE NÉCESSAIRE ...)

Ainsi, à (X, S) comme dans 5.1., on associe:

1°) Trois groupoïdes (profinis) Π_U, Π_D, Π_{D^*} (en plus de $\Pi_e = \Pi_1(\text{Spec}(K))(\simeq \text{Tors}(\Gamma))$);

2°) Quatre foncteurs (de groupoïdes profinis) :



3°) Un isomorphisme de commutation

$$\alpha : \varphi \rho \simeq \psi \sigma$$

(qui est même l’identité dans le cas de système provenant de (X, S) , mais il vaut mieux oublier qu’il en soit ainsi). Ces données satisfaisant aux conditions préliminaires

- a) σ induit un isomorphisme sur les π_0 , et des épimorphismes sur les Hom, et il est à noyau abélien ;
- b) ψ est fidèle.

A. GROTHENDIECK

[c) ρ est fidèle...

d) φ est épimorphique modulo groupes finis sur les Aut...]

La condition a) permet déjà de définir le π_1 relatif $\pi_1(\sigma) = \pi_1(\Pi_{D^*}/\Pi_D)$, qui est un système local de groupes abéliens sur Π_D i.e. un foncteur $(\Pi_D)^\circ \longrightarrow \text{Ens}$, et la dernière donnée

4°) Un isomorphisme kummérien

$$\chi : \pi_1(\sigma) \simeq \psi^*(T)$$

Si on a deux systèmes de cette nature $\Pi = (\Pi_U, \Pi_D, \Pi_{D^*}, \varphi, \psi, \rho, \sigma, \alpha, \chi)$ et $\Pi' = (\Pi'_U, \dots)$, un *morphisme* de Π' dans Π est un système de trois foncteurs

$$f_U : \Pi'_U \longrightarrow \Pi_U$$

$$f_D : \Pi'_D \longrightarrow \Pi_D$$

$$f_{D^*} : \Pi'_{D^*} \longrightarrow \Pi_{D^*}$$

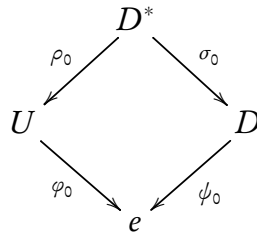
et de quatre isomorphismes de commutation $\alpha_{D^*,D}$, $\alpha_{D^*,U}$, $\alpha_{U,e}$, $\alpha_{D,e}$, pour les quatre faces du prisme

[]

satisfaisant une équation de compatibilité avec α , α' que je n'écris pas - signifiant que les *deux* isomorphismes u , v de foncteurs

[]

obtenus respectivement, u en utilisant successivement α , $\alpha_{D^*,D}$, $\alpha_{D,e}$, v en utilisant successivement $\alpha_{D^*,U}$, $\alpha_{U,e}$, α' , sont égaux. [Cette compatibilité pourrait s'exprimer en interprétant la donnée de Π comme celle d'une catégorie fibrée Π sur la "catégorie carrée" Q :



LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

(où $\varphi_0 \rho_0 = \psi_0 \sigma_0$) à restriction à e imposée, et en prenant des foncteurs cartésiens entre catégories fibrées...]

De plus, on exige autre une compatibilité, savoir que l'homomorphisme de systèmes locaux en groupes abéliens sur Π'_D

$$\pi_1(\sigma') \longrightarrow (f_D)^*(\pi_1(\sigma))$$

défini à l'aide de $f_{D^*}, f_D, \alpha_{D^*,D}$ rende commutatif le diagramme suivant d'isomorphismes de systèmes locaux sur Π'_D ⁷ :

[]

(où x est déduit de $\alpha_{D,e} : \psi' \simeq \psi \circ f_D$)

Pour Π, Π^* fixés, les systèmes $(f_\alpha = (f_U, f_D, f_{D^*}, \alpha_{D^*,D}, \alpha_{D^*,U}, \alpha_{U,e}, \alpha_{D,e}))$ précédents forment une catégorie de façon naturelle - en fait un groupoïde - en prenant comme morphismes μ de (f', α') dans (f, α) les triplets de morphismes (foncteurs profinis)

$$f'_U \xrightarrow{\mu_U} f_U, \quad f'_D \xrightarrow{\mu_D} f_D, \quad f'_{D^*} \xrightarrow{\mu_{D^*}} f_{D^*}$$

satisfaisant quatre conditions de compatibilité avec $\alpha_{D^*,D}$ et $\alpha'_{D^*,D}$, avec $\alpha_{D^*,U}$ et $\alpha'_{D^*,U}$ avec $\alpha_{U,e}$ et $\alpha'_{U,e}$, avec $\alpha_{D,e}$ et $\alpha'_{D,e}$ respectivement (i.e. on travaille avec une sous-catégorie pleine de la catégorie des Hom entre catégories fibrées sur Q , à fibre en e fixée...).

J'ai l'impression que le groupoïde $\text{Hom}((f', \alpha'), (f, \alpha))$ est toujours *rigide*, i.e. $\text{Aut}(f, \alpha)$ est toujours réduit au groupe unité - j'ai la flemme de vérifier - donc que si (f', α') et (f, α) son isomorphes, l'isomorphisme en question est unique. Quoi qu'il en soit, on posera

$$\text{Hom}((f', \alpha'), (f, \alpha)) = \pi_0 \text{Hom}((f', \alpha'), (f, \alpha))$$

D'où une *catégorie* des systèmes $\Pi = (\Pi_U, \Pi_D, \Pi_{D^*}, \varphi, \psi, \rho, \sigma, \alpha, \kappa)$.

On a un foncteur des couples (X, S) ⁸ (où X schéma localement de type fini sur K , S sous schéma fermé de X étale sur K , tels que pour tout $s \in S$, X soit lisse de dimension relative 1 en s) vers cette catégorie bordélique B)

Conjecture bordélique (7.1). — *Quand on se borne aux (X, S) tels que X projectif lisse de dimension ≤ 1 , et qui de plus sont anabéliens, alors le foncteur précédent est pleinement fidèle⁹.*

⁷non cela ne marche que pour le cas de morphismes étales, sinon il faut faire intervenir la multiplication par les "degrés de ramifications" $d_{i'}$ ($i' \in \pi_0(\Pi'_{D^*})$).

⁸[les] morphismes $(X', S') \longrightarrow (X, S)$ sont les morphismes $f : X' \longrightarrow X$ tels que $f^{-1}(S)_{red} = S'$

⁹**N.B.** La fidélité est facile...

A. GROTHENDIECK

Description de la catégorie bordélique en termes de théorie de groupes.

Soit $I = \pi_0(\Pi_{D^*}) \simeq \pi_0(\pi_D)$. Choisissons un élément D_i^* dans chaque composante de Π_{D^*} , et soit $D_i = \sigma(D_i^*)$. Pour tout i , choisissons un isomorphisme

[]

Quitte à remplacer l'objet par un "sous-objet" isomorphe on peut supposer que Π_{D^*} est la catégorie somme de catégories $[E_i]$ définies par les $E_i = \text{Aut}(D_i^*)$, Π_D la catégorie somme des catégories $[\Gamma_i]$ définies par les $\Gamma_i = \text{Aut}(D_i)$, le foncteur σ s'exprimant par un système d'homomorphismes

$$\sigma_i : E_i \longrightarrow \Sigma_i \quad (i \in I)$$

qui sont surjectifs de noyaux abéliens, le foncteur ϕ par un système d'inclusions $\phi_i : \Gamma_i \hookrightarrow \Gamma$ et la donnée de κ équivaut en fait à des isomorphismes

$$\kappa_i : \ker \sigma_i \simeq T(\overline{K})$$

compatibles avec les opérations de Γ_i et de Γ sur les deux $[?]$ respectivement, et les inclusions ϕ_i . On peut dire que la donnée de (σ, ϕ, κ) est exprimée par la donnée du système $(E_i)_{i \in I}$, d'un système de suites exactes

[]

§ 8. — RÉFLEXIONS TAXONOMIQUES

Le cas $\dim X = 0$ se traduit sur le paradigme du système $(T(\overline{K}) \xrightarrow{x_i} E_i \hookrightarrow \rho_i E \xrightarrow{p} \Gamma)$ par la condition p injectif et donc $I = \emptyset$ - donc ce cas décrit simplement par la donnée d'un *sous-groupe* ouvert de $E \hookrightarrow \Gamma$, i.e. une sous-extension finie L de \overline{K}/K (N.B. on aura bien sûr $X' = \text{Spec } L$, et le choix faits sur X - i.e. sur $\Pi_{D^*}(=\emptyset) \longrightarrow \Pi_U \longrightarrow \Pi_e$ - aboutissant à cette description, reviennent ici au choix d'une telle K -immersion de $L = H^0(X, O_X)$ dans \overline{K}/K).

Le cas $\dim X = 1$ se traduit par le fait que $E \longrightarrow \Gamma$ n'est pas injectif - quand à I , il peut être vide ou non dans ce cas. S'il est vide, la description se fait donc simplement en termes d'un homomorphisme de groupes profinis $E \xrightarrow{p} \Gamma$ (ou Γ donnée d'avance = $\text{Gal}(\overline{K}/K)$) = $\text{Aut}_{\Pi_e}(\Omega)$.

Supposons données maintenant à la fois

[]

§ 9. — STRUCTURE TANGENTIELLE EN LES $s \in S$ ¹⁰

Revenant à la description des (X, S) par $\Pi_{D^*} \longrightarrow \Pi_U \longrightarrow \Pi_e$, un $s_i \in S$ correspond donc à une composante connexe de $\Pi_{D_i^*}$ dans Π_{D^*} , ou un Π_{D_i} de son quotient Π_D .

Considérons $\Pi_{D_i^*} \xrightarrow{\sigma_i = \sigma_{D_i^* D_i}} \pi D_i$. On va décrire certaines sections (à isomorphisme près) de ce morphisme de groupoïdes, i.e. des couples (γ, λ) où γ est un foncteur $\Pi_{D_i} \xrightarrow{\gamma} \Pi_{D_i^*}$ et λ un isomorphisme $\sigma_i \circ \gamma \simeq Id$.

¹⁰[Les sections d'extensions "de deuxième type"]

§ 10. — AJUSTEMENT DES HYPOTHÈSES (REMORDS)

Je me rends compte que dans la définition des morphismes $(X', S') \xrightarrow{f} (X, S)$, l'hypothèse $f^{-1}(S)_{red} = S'$ est étriquée - il faut prendre des morphismes *quelconques* $X' \setminus S' \xrightarrow{x} X \setminus S$ (se prolongeant bien sûr en $\hat{f} : X' \rightarrow X$). On aura donc $\hat{f}^{-1}(S)_{red} \subset S'$, mais S' peut être strictement plus grand que $\hat{f}^{-1}(S)_{red}$.

Il faut ajuster en conséquence la description de la “catégorie bordélique” - les objets restent les diagrammes de groupoïdes $D : \Pi_{D^*} \rightarrow \Pi_U \rightarrow \Pi_e$ (plus donnée de Kummer), mais un morphisme d'un D' dans un D ne définit plus nécessairement un $\Pi'_{D^*} \rightarrow \Pi_{D^*}$ (en plus de $\Pi'_U \rightarrow \Pi_U$) il faut se donner une partie I'_f de $I' = \text{pi}_0(\Pi'_{D^*})$ et se donner seulement $\Pi'_{D^*, I'_f} \xrightarrow{f_{D^*}} \Pi_{D^*}$ (avec donnée de commutation $\alpha_{D^*, U}$ relative au carré avec f_U). Bien sûr, dans la description en termes de E', E etc, on exige que pour $i' \in I' \setminus I'_f$, $f_E : E' \rightarrow E$ est trivial sur $E'_{i'} \subset E'$ - et τ est défini comme $I'_{f'} \rightarrow I$; les données relatives aux $i' \in I'_{f'}$ ($f_{i'} : E_{i'} \rightarrow E_{i=\tau(i')}$, les $\alpha_{i'} \in E$) sont pareilles que dans le cas envisagé précédemment.

N.B. Cela signifie en fait qu'on commence à “boucher les trous” (de X') correspondants aux $i' \in I' \setminus I'_{f'}$, en remplaçant E' par le groupe quotient de E' par le sous-groupe invariant engendré par les $L_{i'} = \chi_{i'}(T(\bar{K}))(i' \in I' \setminus I'_{f'})$, et les $E_{i'}(i' \in I'_{f'})$ par leurs images dans le dit groupe quotient, et en oubliant $I' \setminus I'_{f'}$ i.e. remplaçant I' par $I'_{f'}$.

[Pour bien faire, il faudrait exprimer ces opérations aussi au niveau des diagrammes de groupoïdes $\Pi'_{D^*} \rightarrow \Pi'_U \rightarrow \Pi_e \dots$].

Cela signifie donc qu'en fait, on s'est ramené à la situation envisagée au début, où $S' = \hat{f}^{-1}(S)_{red}$... Donc finalement la différence des deux points de vue n'est pas énorme, et celui

A. GROTHENDIECK

adopté au début a l'avantage de l simplicité plus grande (tout est relatif !)

§ 11. — CONDITIONS SUR LES SYSTÈMES DE GROUPOÏDES OBTENUS À PARTIR DE SITUATIONS GÉOMÉTRIQUES

On en a déjà cité au passage, par exemple que les groupes noyaux de $\Pi_{D^*} \longrightarrow \Pi_e$ sont abéliens (avec l'isomorphisme de Kummer \varkappa) et que les images sont des sous-groupes ouverts, et de même pour l'image des π_1 dans le cadre de l'interprétation en termes de

$$T(\overline{K}) \xrightarrow{x_i} E_i \xrightarrow{\rho_i} E \xrightarrow{p} \Gamma$$

(cas de la “dim 1” - on n'exclut pas le cas $I = \emptyset$ le cas “dim 0” étant trivial)

- a) L'image Σ de p est ouverte, plus précisément il existe un sous-groupe ouvert $\Gamma' \subset \Gamma$ au dessus duquel E ait une section [et même une “section admissible” en un sens qui sera défini par la suite - de sorte à exclure les sections “triviales” provenant des $E_i \dots$].
- b) L'image
- c)
- d)

§ 12. — L'ANALOGIE TOPOLOGIQUE

§ 13. — RETOUR AU CAS ARITHMÉTIQUE

Retour au cas arithmétique, où on veut décrire en termes “galoisiens” les couples (X, S) anabéliens connexes sur un corps K de type fini sur Q . [**N. B.** Si on prend un K de type fini sur F_p , il faudrait se borner aux groupes fondamentaux “premiers à p ”, à cela près nos développements pourraient se faire quand même...]

Il est devenu clair qu’en termes d’une clôture algébrique \overline{K} de K , d’où un groupe de Galois profini $\Gamma = \text{Gal}(\overline{K}/K)$, la description la plus simple est en termes de groupes extérieures à lacets et d’actions extérieures de sous-groupes ouverts Σ de Γ dessus.

De façon précise, on choisit une composante connexe \overline{X}_0 de \overline{X} (ou ce qui revient au même, \overline{U}_0 de $\overline{U} = (X \setminus S)_{\overline{K}}$), soit Σ son stabilisateur dans Γ (il est remplacé par un conjugué, quand on change \overline{U}_0). Alors Σ opère sur le schéma \overline{U}_0 , donc opère extérieurement sur π_1 (considéré comme groupe extérieure). Or sur celui-ci il y a une $T(\overline{K})$ -structure à lacets, avec comme ensemble d’indices $I = S_0(\overline{K}) \subset S(\overline{K}) \simeq S_0(K) \wedge_{\Sigma} \Gamma$ [vide si et seulement si $S \neq \emptyset$] et l’opération de Σ sur π est compatible avec cette structure à lacet, et le caractère cyclotomique $\chi : \Gamma \hat{Z}^*$ (plutôt, $\chi|_{\Sigma}$). Ainsi l’opération de Σ sur π implique son action sur Σ , d’où $S(\overline{K}) \simeq S_0(\overline{K}) \wedge_{\Sigma} \Gamma$ en tant que σ -ensemble - on récupère donc le K -schéma étale S . Mais mieux, on récupère tout le diagramme

$$\Pi_{\overline{D}_0^*} \longrightarrow [\Pi_{\overline{U}_0} \longrightarrow] \Pi_{\overline{U}} \longrightarrow \Pi_e$$

et l’opération de Σ dessus d’où le diagramme des topos classifiant - où si on préfère, le diagramme

$$\Pi_{D^*} \longrightarrow \Pi_U \longrightarrow \Pi_e$$

A. GROTHENDIECK

(avec les notations du début de ces notes, qui deviendraient ici

$$\Pi_{D^*, \Gamma} \longrightarrow \Pi_{U, \Gamma} \longrightarrow \Pi_{e, \Gamma}$$

plus bien sur K [?]....

Les homomorphismes $(X', S') \xrightarrow{f} (X, S)$ [$f^{-1}(S) \subset S'$, f dominant] se décrivent simplement (via le choix d'un \overline{X}'_0 au dessus d'un \overline{X}_0 par des homomorphismes extérieures $\pi(= \pi_1(\overline{X}_0)) \longrightarrow \pi(= \pi_1(\overline{X}'_0))$, compatibles avec les actions de Σ ($\subset \Sigma$) et de Σ , et avec les structures à lacets anabéliennes (ce qui s'exprime à l'aide d'une application $\tau : (I' \subset \overline{S}'_0) \longrightarrow I = \overline{S}_0$ ¹¹ compatible avec σ' , et un système d'entiers naturels $(d_{i'})_{i' \in I'}$).

Il faut cependant compléter, pour $I = \emptyset$, la définition de la structure à lacets, par la donnée d'un isomorphisme

$$\chi : T^{\otimes -1} \xrightarrow{\sim} H^2(\pi, \widehat{Z})$$

[**N.B.** en caractéristique $p \geq 0$, on doit se borner aux composantes ℓ -adiques avec $\ell \neq p$] i.e.

$$\widehat{Z} \xrightarrow{\sim} H^2(\pi, \Gamma)$$

compatible avec l'action de Σ - et il faut exiger, dans l'interprétation "galoisienne" de $f : (X', S') \longrightarrow (X, S)$, quand $S = S' = \emptyset$ que l'homomorphisme $\pi \longrightarrow \pi'$ induit un diagramme commutatif

[]

¹¹**N.B.** $I' = \overline{S}'_0 \cup f^{-1}(\overline{S}_0)$

§ 13 bis. — RETOUR SUR LA NOTION DE GROUPE À LACETS

§ 14. — DIGRESSION COHOMOLOGIQUE (SUR LE “BOUCHAGE
DE TROUS”)

§ 14 bis. — OÙ ON REVIENT SUR LES MORPHISMES MIXTES

§ 15. — RETOUR SUR LE CAS TOPOLOGIQUE

§ 16. — BOUCHAGE ET FORAGE DE TROUS : PRÉLIMINAIRES
TOPOLOGIQUES GÉNÉRAUX



§ 17. — COMPLÉMENTS SUR LES OPÉRATIONS DE GROUPES
FINIS SUR LES SURFACES (COMPLÉMENT AU PARAGRAPHE 15)

§ 18. — FORAGE DE TROUS ; APPLICATION AUX ACTIONS
EXTÉRIEURES DE GROUPES FINIS

Soit π' un groupe à lacets de type $(g, \nu + 1)$ non abélien

§ 19. — TOUR DE TEICHMÜLLER

§ 20. — DIGRESSION : DESCRIPTION 2-ISOTOPIQUE DE LA
CATÉGORIE DES SPHÈRES TOPOLOGIQUES

§ 21. — LIEN AVEC LES ESPACES DE TEICHMÜLLER

§ 23. — RETOUR SUR LES SURFACES À GROUPES D'OPÉRATEURS

§ 24. — ESSAI DE DÉTERMINATION DE $\mathcal{A}^{0\Gamma}$; LIEN AVEC LES
RELATIONS $\pi_{g,(\nu,\nu+n-1)}^\Gamma = \{1\}$, ET PROGRAMME DE TRAVAIL

§ 25. — GROUPES DE TEICHMÜLLER SPÉCIAUX

§ 25 bis. — CAS DES DEUX GROUPES. RETOUR SUR LES NOTATIONS

On se place d'abord pour fixer les idées dans le cas topologique et discret, mais la motivation

§ 26. — GROUPES DE TEICHMÜLLER PROFINIS (DISCRÉTIFICATION ET PRÉDISCRÉTIFICATION)

Soit π un groupe profini à lacets de type g, ν , T le \hat{Z} -module inversible de ses orientations. On suppose qu'on est dans le cas anabélien, et on admettra qu'alors

$$(1) \quad \text{Centre}(\pi) = \{1\},$$

plus généralement que le centralisateur dans π de tout sous-groupe ouvert de π est réduit à $\{1\}$. On aura donc encore une suite exacte canonique de groupes profinis

$$(2) \quad 1 \rightarrow \pi \rightarrow \text{Aut}_{\text{lac}}(\pi) \rightarrow \text{Autext}_{\text{lac}}(\pi) \rightarrow 1.$$

On posera aussi

$$(3) \quad \text{Autext}_{\text{lac}}(\pi) = \hat{\mathfrak{Z}}(\pi),$$

et on l'appellera le *groupe de Teichmüller étendu* de π . On posera aussi $\hat{\mathfrak{S}}(\pi) = \text{Aut}_{\text{lac}}(\pi)$, de sorte qu'on peut écrire (2) comme

$$(2') \quad 1 \rightarrow \pi \rightarrow \hat{\mathfrak{S}}(\pi) \rightarrow \hat{\mathfrak{Z}}(\pi) \rightarrow 1.$$

Appelons “base” de π un ensemble d'éléments de π : $(x_i, y_i)_{1 \leq i \leq g}$, $(l_j)_{1 \leq j \leq \nu}$, les l_j engendrant les différents groupes à lacets, satisfaisant

$$(4) \quad l_\nu l_{\nu-1} \cdots l_1 [x_g, y_g] \cdots [x_1, y_1] = 1,$$

A. GROTHENDIECK

et tels que ceci soit une relation génératrice. Si on choisit dans $\pi_{g,\nu}$ une base (discrète) (définition correspondante)¹², d'où une base de $\hat{\pi}_{g,\nu}$: on aura une bijection évidente

$$(5) \quad \text{Bases}(\pi) \xleftarrow{\sim} \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi).$$

L'ensemble des bases de π est un ensemble homogène sous $\hat{\mathfrak{S}}(\pi) = \text{Aut}_{\text{lac}}(\pi)$. Si la base correspond à un isomorphisme $u : \hat{\pi}_{g,\nu} \rightarrow \pi$, le groupe π_0 engendré par les x_i, y_i, l_j n'est autre que $u(\pi_{g,\nu})$. Les sous-groupes de π qui peuvent s'obtenir ainsi sont appelés les *discrétifications* de π . Celles-ci forment un ensemble homogène sous $\hat{\mathfrak{S}}(\pi) = \text{Aut}_{\text{lac}}(\pi)$, canoniquement isomorphe au quotient du $\hat{\mathfrak{S}}_{g,\nu}$ -ensemble à droite $\text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi)$ par $\mathfrak{S}_{g,\nu}$ ¹:

$$(6) \quad \text{Discrét}(\pi) \xleftarrow{\sim} \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \mathfrak{S}_{g,\nu}.$$

Les automorphismes (profinis à lacets) de π fixant une discrétification π_0 s'identifient aux automorphismes du groupe discret à lacets π_0 :

$$(7) \quad \text{Aut}_{\text{lac}}(\pi, \pi_0) \simeq \text{Aut}_{\text{lac}}(\pi_0).$$

La bijection (5) met sur l'ensemble des bases de π une structure de bitorseur sous $\hat{\mathfrak{S}}(\pi)$, $\hat{\mathfrak{S}}_{g,\nu}$, et la topologie correspondante en fait un ensemble profini. L'ensemble des discrétifications de π , qui est un quotient de l'ensemble précédent, hérite d'une topologie quotient, qui n'est autre que la topologie quotient du deuxième membre de (6). Cet espace n'est pas séparé ($\mathfrak{S}_{g,\nu}$ est toujours infini), car le groupe $\mathfrak{S}_{g,\nu} \subset \hat{\mathfrak{S}}_{g,\nu}$ n'est pas fermé. On désigne par $\text{Discrét}'(\pi)$ l'espace topologique séparé associé, s'identifiant à $\text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \overline{\mathfrak{S}}_{g,\nu}$, où $\overline{\mathfrak{S}}_{g,\nu}$ désigne l'adhérence de $\mathfrak{S}_{g,\nu}$ dans $\hat{\mathfrak{S}}_{g,\nu}$. On a d'ailleurs un homomorphisme évident $\hat{\mathfrak{S}}_{g,\nu} \rightarrow \hat{\mathfrak{S}}_{g,\nu}$ dont l'image est $\overline{\mathfrak{S}}_{g,\nu}$, nous admettrons qu'il est injectif et identifierons $\overline{\mathfrak{S}}_{g,\nu}$ à $\hat{\mathfrak{S}}_{g,\nu}$. Ainsi

$$(8) \quad \text{Discrét}'(\pi) \simeq \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \hat{\mathfrak{S}}_{g,\nu}.$$

¹²ou encore on définit $\pi_{g,\nu}$ comme le groupe discret de générateurs les x_i, y_i, l_j et de relation de définition (4)

Un élément de $\text{Discrét}'(\pi)$ s'appelle une classe de discrétifications de π (ou prédiscrétification de π). Si π_0 est une discrétification, on désigne sa classe par π_0^{\natural} . L'ensemble des classes de discrétifications de π est un espace homogène sous $\hat{\mathfrak{S}}(\pi)$, le stabilisateur de π_0^{\natural} s'identifiant à l'adhérence de $\mathfrak{S}(\pi_0) = \text{Aut}_{\text{lac}}(\pi_0)$ dans $\hat{\mathfrak{S}}(\pi)$, ou encore à $\hat{\mathfrak{S}}(\pi_0)$. Celle-ci contient toujours π .

$$(9) \quad \text{Aut}_{\text{lac}}(\pi, \pi_0^{\natural}) \simeq \hat{\mathfrak{S}}(\pi_0).^2$$

Pour toute [pré?]discrétification π_0^{\natural} , le sous-groupe de $\hat{\mathfrak{S}}(\pi)$ des automorphismes à lacets qui fixent π_0^{\natural} est noté $\hat{\mathfrak{S}}(\pi_0^{\natural})$. C'est donc l'image inverse d'un sous-groupe de $\hat{\mathfrak{Z}}(\pi)$, noté $\hat{\mathfrak{Z}}(\pi_0^{\natural})$.¹³ On a donc une inclusion de structures d'extensions:

$$(10) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi & \longrightarrow & \hat{\mathfrak{S}}(\pi_0^{\natural}) & \longrightarrow & \hat{\mathfrak{Z}}(\pi_0^{\natural}) \longrightarrow 1 \\ & & & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \pi & \longrightarrow & \hat{\mathfrak{S}}(\pi) & \longrightarrow & \hat{\mathfrak{Z}}(\pi) \longrightarrow 1. \end{array}$$

(On montre par voie arithmético-géométrique que l'inclusion $\hat{\mathfrak{Z}} \rightarrow \hat{\mathfrak{Z}}$ n'est jamais un isomorphisme). On trouve ainsi une application

$$(11) \quad \text{Discrét}'(\pi) \rightarrow \text{sous-groupes fermés de } \hat{\mathfrak{Z}}(\pi),$$

$$[\pi_0^{\natural} \longmapsto \hat{\mathfrak{Z}}(\pi_0^{\natural})]$$

évidemment compatible à l'action de $\hat{\mathfrak{S}}(\pi)$ (transport de structure) – opérant à droite via $\hat{\mathfrak{Z}}(\pi)$ et ses automorphismes intérieurs sur lui-même.³

On trouve ainsi une classe de conjugaison bien déterminée de sous-groupes fermés de $\hat{\mathfrak{Z}}(\pi)$, qu'on appelle ses sous-groupes de Teichmüller “géométriques”. Il se pourrait d'ailleurs que $\hat{\mathfrak{Z}}_{g,v}$ soit son propre normalisateur dans $\hat{\mathfrak{Z}}_{g,v}$ ce qui équivaut à l'assertion que (11) est

¹³NB. L'ensemble des classes de discrétification de π se décrit en termes de groupes *extérieurs* définis par π comme $\text{Isomext}_{\text{lac}}(\hat{\pi}_{g,v}, \pi)$ divisé par $\hat{\mathfrak{Z}}_{g,v}$; on a d'ailleurs une application de degré 2 $\text{Isomext}(\hat{\pi}_{g,v}, \pi)/\hat{\mathfrak{Z}}_{g,v}^+ \rightarrow \text{Isomext}(\hat{\pi}_{g,v}, \pi)/\hat{\mathfrak{Z}}_{g,v}$, ce qui permet pour toute classe de discrétification de définir ses deux *orientations* et de parler des classes de discrétification *orientées*.

A. GROTHENDIECK

bijective: la donnée d'une classe de discrétifications de π serait équivalente à celle d'un sous-groupe de Teichmüller géométrique dans son groupe de Teichmüller étendu $\hat{\mathfrak{Z}}$.¹⁴

Notons qu'on a des homomorphismes canoniques

$$(12) \quad \hat{\mathfrak{Z}} \xrightarrow{\chi} \hat{\mathbb{Z}}^*$$

$$(13) \quad \hat{\mathfrak{Z}} \rightarrow \mathfrak{S}_I$$

(où $I = I(\pi)$ est l'ensemble des classes de conjugaison des sous-groupes à lacets de π), induisant sur $\hat{\mathfrak{Z}}(\pi_0^h)$ des homomorphismes correspondants – d'où la définition des sous-groupes $\hat{\mathfrak{Z}}^!, \hat{\mathfrak{Z}}^+, \hat{\mathfrak{Z}}^{!+}$ et de même pour $\hat{\mathfrak{Z}}$. Notons que χ ne prend sur $\hat{\mathfrak{Z}}$ que les valeurs ± 1 .⁴

Le sous-groupe $\hat{\mathfrak{Z}}^+$ des automorphismes extérieurs du groupe à lacets profinis π , fixant une classe de discrétifications π_0^h et de multiplicateur $+1$, joue un rôle très particulier. A l'opposé de ce qu'on peut conjecturer sur $\hat{\mathfrak{Z}}$ (dont $\hat{\mathfrak{Z}}^+$ est un sous-groupe ouvert d'indice 2), on supposerait plutôt que $\hat{\mathfrak{Z}}^+$ est invariant dans $\hat{\mathfrak{Z}}$ [voir note en bas de page précédente]. En tout état de cause, les sous-groupes ainsi définis dans $\hat{\mathfrak{Z}}$ via classes de discrétification de π (peut-être n'y en a-t-il qu'un seul et unique!)⁵ s'appelleront les sous-groupes de Teichmüller géométriques *stricts*. Le choix d'un tel sous-groupe de $\hat{\mathfrak{Z}}$ est, en tout état de cause, un élément de structure nettement plus faible que celui d'une classe de discrétification, et même que celui d'un sous-groupe de Teichmüller géométrique (pas strict). Pour préciser les relations entre ces deux notions, rappelons d'abord que $\hat{\mathfrak{Z}}^+ = \Sigma$ se déduit de $\hat{\mathfrak{Z}}$ comme noyau de $\chi|_{\hat{\mathfrak{Z}}} : \hat{\mathfrak{Z}} \rightarrow \{\pm 1\}$. D'autre part (pour un sous-groupe de Teichmüller géométrique strict choisi $\hat{\mathfrak{Z}}^+$), considérons

$$(14) \quad \mathcal{N}_\Sigma = \mathcal{N} = \text{Norm}_{\hat{\mathfrak{Z}}}(\Sigma)$$

où $\Sigma = \hat{\mathfrak{Z}}^+$ ($[\mathcal{N}_\Sigma \text{ est}]$ peut-être toujours égal à $\hat{\mathfrak{Z}}$ tout entier), évidemment (si Σ provient d'un $\hat{\mathfrak{Z}}$)

$$(15) \quad \Sigma = \hat{\mathfrak{Z}}^+ \subset \hat{\mathfrak{Z}} \subset \mathcal{N}_\Sigma.$$

¹⁴c'est complètement déconnant et ultra-faux; un moment d'égarement! Cela apparaît clairement par la suite...La question judicieuse (avec laquelle j'ai dû sur le coup confondre) c'est si $\hat{\mathfrak{Z}}$ est *invariant* dans $\hat{\mathfrak{Z}}$, i.e. si le normalisateur est $\hat{\mathfrak{Z}}$ tout entier.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Le groupe profini \mathcal{N}/Σ associé à Σ se note Π_Σ (si Σ est unique, on note Π_π), et les $\hat{\mathfrak{Z}}$ donnant naissance au même Σ correspondent à une classe de conjugaison d'éléments d'ordre 2 de Π_Σ . Il est clair en tous cas qu'on a une application injective

$$\{\text{ensemble des sous-groupes de Teichmüller géométriques } \hat{\mathfrak{Z}} \text{ dans } \hat{\mathfrak{Z}}^+ \text{ tels que } \hat{\mathfrak{Z}}^+ = \Sigma\}$$

↓

$$(16) \quad \{\text{ensemble des éléments d'ordre 2 dans } \Pi_\Sigma\}$$

et que son image est stable par conjugaison. Montrons que deux éléments de l'image sont conjugués dans Π_Σ . En effet, soient $\hat{\mathfrak{Z}}, \hat{\mathfrak{Z}}' \supset \Sigma$ tels que $\Sigma = \hat{\mathfrak{Z}}^+ = \hat{\mathfrak{Z}}'^+$. Il existe $g \in \hat{\mathfrak{Z}}$ tel que $\hat{\mathfrak{Z}}' = \text{Int}(g)\hat{\mathfrak{Z}}$, et on aura alors $\hat{\mathfrak{Z}}'^+ = \text{Int}(g)\hat{\mathfrak{Z}}^+$, i.e. $g \in \mathcal{N}$, OK.

Les éléments d'ordre 2 ainsi obtenus dans Π_Σ s'appellent les involutions canoniques. On en donnera une interprétation conjecturale remarquable plus bas. L'ensemble $\hat{\mathfrak{Z}}/\mathcal{N}$ s'identifie à l'ensemble des sous-groupes de Teichmüller géométriques stricts (une fois choisi l'élément "origine" Σ).⁶ Plus intrinsèquement, on aura:

$$\{\text{Ensemble des sous-groupes de Teichmüller géométriques stricts de } \hat{\mathfrak{Z}}(\pi)\}$$

↑

$$(17) \quad \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi)/\mathcal{N}_{g,\nu}$$

où on pose, comme de juste,

$$(18) \quad \mathcal{N}_{g,\nu} = \text{Norm}_{\hat{\mathfrak{Z}}_{g,\nu}}(\hat{\mathfrak{Z}}_{g,\nu}^+)$$

(peut-être égal à $\hat{\mathfrak{Z}}_{g,\nu}$ tout entier!).

Considérons maintenant le *topos modulaire sur* \mathbb{Q} des courbes algébriques de type (g, ν) , noté $\mathcal{M}_{g,\nu,\mathbb{Q}}$ ou simplement $\mathcal{M}_{g,\nu}$. Si nous choisissons un revêtement universel $\overline{\mathcal{M}}_{g,\nu}$ (d'où un revêtement universel de $\text{Spec } \mathbb{Q}$, i.e. une clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q}), on peut préciser le $\pi_1(\mathcal{M}_{g,\nu,\mathbb{Q}})$ comme le groupe des $\mathcal{M}_{g,\nu,\mathbb{Q}}$ -automorphismes de ce revêtement et l'appeler le

A. GROTHENDIECK

groupe de *Teichmüller arithmétique* de type (g, ν) (relatif au choix de $\widetilde{\mathcal{M}}_{g, \nu, \mathbb{Q}}$). On aura donc une suite exacte

$$(19) \quad 1 \rightarrow \pi_1(\mathcal{M}_{g, \nu, \overline{\mathbb{Q}}}) \rightarrow \pi_1(\mathcal{M}_{g, \nu}) \rightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow 1,$$

(où $\overline{\mathbb{Q}}$ et les points base sont explicités comme il a été dit). Notons que par la théorie transcendante de Teichmüller on a un isomorphisme (défini modulo l'opération induite par $\pi_1(\mathcal{M}_{g, \nu})$ sur $\pi_1(\mathcal{M}_{g, \nu, \overline{\mathbb{Q}}})$):

$$(20) \quad \pi_1(\mathcal{M}_{g, \nu, \overline{\mathbb{Q}}}) \simeq \hat{\mathfrak{Z}}_{g, \nu}^+$$

(où $\hat{\mathfrak{Z}}_{g, \nu}^+$ est le compactifié profini de $\mathfrak{Z}_{g, \nu}^+$).

Considérons d'autre part le schéma $\mathcal{U}_{g, \nu}$ sur $\mathcal{M}_{g, \nu}$, courbe de type (g, ν) “universelle”. On a donc, en choisissant un revêtement universel $\widetilde{\mathcal{U}}_{g, \nu}$ de celle-ci *au-dessus* du revêtement universel choisi $\widetilde{\mathcal{M}}_{g, \nu}$ de $\mathcal{M}_{g, \nu}$, un diagramme commutatif:

$$(21-22) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi & \longrightarrow & \pi_1(\mathcal{U}_{g, \nu}) & \longrightarrow & \pi_1(\mathcal{M}_{g, \nu}) \longrightarrow 1 \\ & & \downarrow \wr & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \pi & \longrightarrow & \hat{\mathfrak{S}}(\pi) & \longrightarrow & \hat{\mathfrak{Z}}(\pi) \longrightarrow 1 \end{array}$$

et de même pour $\mathcal{U}_{g, \nu, \overline{\mathbb{Q}}} \rightarrow \mathcal{M}_{g, \nu, \overline{\mathbb{Q}}}$:

$$(21') \quad 1 \rightarrow \pi \rightarrow \pi_1(\mathcal{U}_{g, \nu, \overline{\mathbb{Q}}}) \rightarrow \pi_1(\mathcal{M}_{g, \nu, \overline{\mathbb{Q}}}) \rightarrow 1.$$

On a bien sûr un isomorphisme de groupes à lacets

$$(23) \quad \pi \simeq \hat{\pi}_{g, \nu}$$

dont on voudrait déterminer l'indétermination de façon précise.⁷

Notons $\mathcal{M}_{g, \nu, \mathbb{C}}$ le topos modulaire de Teichmüller complexe, défini à l'aide de la surface $C^\infty \mathcal{U}_{g, \nu}$; il est muni du revêtement universel canonique $\widetilde{\mathcal{M}}_{g, \nu, \mathbb{C}}$ (§21; $\widetilde{\mathcal{M}}_{g, \nu, \mathbb{C}} \simeq E_g/A_{g, \nu}^o$) de groupe d'automorphismes $\mathfrak{Z}_{g, \nu}^+$ justement - $\mathcal{U}_{g, \nu, \mathbb{C}}$ étant lui aussi muni d'un revêtement universel au-dessus du précédent, ($\widetilde{\mathcal{U}}_{g, \nu, \mathbb{C}} = E_g/A_{g, \nu+1}^o$). Ceci donne naissance aux suites exactes des groupes discrets (dans le contexte topologique général)

$$(24) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi_{g, \nu} & \longrightarrow & \mathfrak{S}_{g, \nu}^+ & \longrightarrow & \mathfrak{Z}_{g, \nu}^+ \longrightarrow 1 \\ & & \downarrow \wr & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \pi_{g, \nu} & \longrightarrow & \text{Aut}_{\text{lac}}(\pi_{g, \nu}) & \longrightarrow & \text{Autext}_{\text{lac}}(\pi_{g, \nu}) \longrightarrow 1 \end{array}$$

(la première suite s'envoyant dans la seconde par un isomorphisme de structures d'extensions [avec les identifications] $\mathfrak{S}_{g,v}^+ = \pi_1(\mathcal{U}_{g,v,\mathbb{C}})$ et $\mathfrak{Z}_{g,v}^+ = \pi_1(\mathcal{M}_{g,v,\mathbb{C}})$) qui par passage aux complétés profinis donne la suite exacte analogue pour les multiplicités algébriques sur \mathbb{C} .

$$(25) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \hat{\pi}_{g,v} & \longrightarrow & \hat{\mathfrak{S}}_{g,v} & \longrightarrow & \hat{\mathfrak{Z}}_{g,v}^+ \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & \hat{\pi}_{g,v} & \longrightarrow & \text{Aut}_{\text{lac}}(\hat{\pi}_{g,v}) & \longrightarrow & \text{Autext}_{\text{lac}}(\hat{\pi}_{g,v}) \longrightarrow 1. \end{array}$$

Cette situation provient d'ailleurs canoniquement d'une situation analogue sur $\overline{\mathbb{Q}}_0 = \text{cl\`oture algébrique de } \mathbb{Q} \text{ dans } \mathbb{C}$, le choix de $\widetilde{\mathcal{U}_{g,v,\mathbb{C}}}$ définissant un $\widetilde{\mathcal{U}_{g,v,\overline{\mathbb{Q}}_0}}$, d'où un $\mathcal{M}_{g,v,\overline{\mathbb{Q}}_0}$. Pour définir un isomorphisme entre cette suite (25) et la suite exacte (21') (munie canoniquement de deux homomorphismes dans (22)) il faut

1) choisir un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$ – l'indétermination est dans $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; ceci permet d'identifier $\overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}}_0$;

2) Choisir un isomorphisme (sur $\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_0$) de $(\widetilde{\mathcal{U}_{g,v}})_0$ (construit par voie transcendant sur \mathbb{C} et descendu à $\overline{\mathbb{Q}}_0$) avec $\widetilde{\mathcal{U}_{g,v,\overline{\mathbb{Q}}}}$ – l'indétermination est dans $\pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}})$. En résumé, on a une classe d'isomorphismes de (21) et (25), définie modulo automorphismes intérieurs dans le groupe profini $\pi_1(\mathcal{U}_{g,v})$. Une fois choisi l'isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$, les isomorphismes correspondants transforment la *classe de discrétifications orientée* standard de $\hat{\pi}_{g,v}$ en exactement une classe de discrétifications orientée de π .

Changeant le choix de l'isomorphisme en son complexe conjugué, on trouve la quasi-discrétification orientée opposée.⁸

On voit d'autre part que l'image de $\pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}}) \subset \pi_1(\mathcal{M}_{g,v})$ dans $\hat{\mathfrak{Z}}(\pi)$ n'est autre que le $\hat{\mathfrak{Z}}^+$ correspondant à une quelconque des classes de quasi-rigidification discrètes choisies – le sous-groupe ne dépend pas du choix de cette classe – ce qui ne fait qu'exprimer que l'image de $\pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}})$ dans $\hat{\mathfrak{Z}}(\pi)$, considérée comme sous-groupe de l'image du groupe plus grand $\pi_1(\mathcal{M}_{g,v})$, y est invariante – ce qui résulte du fait que $\pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}})$ est invariant dans $\pi_1(\mathcal{M}_{g,v,\mathbb{Q}})$. Ainsi π est muni canoniquement (non d'une quasi-rigidification discrète orientée, ce qui dépend du choix d'un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$, i.e. d'un plongement $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$), mais du moins d'un groupe de Teichmüller géométrique strict $\Sigma \subset \hat{\mathfrak{Z}}(\pi)$, à savoir l'image de $\pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}})$ (isomorphe à $[\cdot\cdot\cdot]$)⁹ Ceci posé, on a un homomorphisme canonique d'extensions

de groupes

$$(26) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi_1(\mathcal{M}_{g,v,\overline{\mathbb{Q}}}) & \longrightarrow & \pi_1(\mathcal{M}_{g,v}) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1 \\ & & \downarrow \wr & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \Sigma & \longrightarrow & \mathcal{N}_\Sigma & \longrightarrow & \Pi_\Sigma \longrightarrow 1, \end{array}$$

où $\mathcal{N}_\Sigma = \mathrm{Norm}_{\hat{\mathfrak{Z}}(\pi)}(\Sigma)$ et Π_Σ est le groupe des automorphismes extérieurs “arithmétiques” de π (muni de Σ).

Pour le choix d’un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$, i.e. d’un plongement $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, l’image de la conjugaison complexe de $\mathrm{Gal}(\overline{\mathbb{Q}}_0/\mathbb{Q})$ n’est autre que l’élément d’ordre 2 de Π_Σ associé au sous-groupe de Teichmüller géométrique, associé à la quasi-discrétification (orientée, mais peu importe) canonique sur π (définie par $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$).

La conjecture naturelle ici, c’est que

$$(27) \quad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \Pi_\Sigma$$

du groupe de Galois vers les automorphismes extérieurs arithmétiques de (π, Σ) soit un isomorphisme. On peut la compléter par la conjecture, encore plus hardie, que de plus Σ est invariant dans $\hat{\mathfrak{Z}}(\pi)$ ($\Leftrightarrow \Sigma_{g,v}$ invariant dans $\hat{\mathfrak{Z}}_{g,v}$), ce qui signifierait donc que $\mathcal{N}_\Sigma = \hat{\mathfrak{Z}}$, ou encore que ¹⁵

$$(28) \quad \pi_1(\mathcal{M}_{g,v}) \xrightarrow{\sim} \hat{\mathfrak{Z}}(\pi) = \mathrm{Autext}_{\mathrm{lac}}(\pi)$$

et $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ s’identifierait au quotient “arithmétique” du groupe des automorphismes extérieurs à lacets de π .

Soit maintenant \mathcal{U} une courbe algébrique de type g, v sur $\overline{\mathbb{Q}}$. Elle est définie par un point de $\mathcal{M}_{g,v,\overline{\mathbb{Q}}}$ sur $\mathrm{Spec} \overline{\mathbb{Q}}$, et comme fibre de $\mathcal{U}_{g,v}$ en ce point. Choisissons un revêtement universel de \mathcal{U} , d’où un groupe $\pi(\mathcal{U})$, canoniquement isomorphe au groupe π ci-dessus, une fois choisi un isomorphisme entre $\widetilde{\mathcal{U}_{g,v}}$ et le revêtement universel de $\mathcal{U}_{g,v}$ déduit de $\widetilde{\mathcal{U}}$, ce qui donne une indétermination dans $\pi_1(\mathcal{U}_{g,v,\overline{\mathbb{Q}}}) \simeq \hat{\mathfrak{S}}^+$. Ainsi, une fois choisi un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$, on trouve sur $\pi_1(\mathcal{U})$ une quasi-discrétification orientée [voir ⁸] (évidente d’ailleurs à définir directement, par voie transcendante), changée en son opposée par changement de l’isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$ par conjugaison complexe. D’autre part, le sous-groupe $\hat{\mathfrak{Z}}^+$ de $\hat{\mathfrak{Z}}(\pi)$,

¹⁵conjectural!

correspondant à cette quasi-discrétification (orientée, peu nous chaut) ne dépend pas du choix de l'isomorphisme en question $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$, il est canoniquement associé à π en tant que groupe fondamental d'un \mathcal{U} sur un corps algébriquement clos (N.B. on pourrait prendre un corps algébriquement clos de caractéristique zéro quelconque, pas la peine que ce soit sur $\overline{\mathbb{Q}}$, cf. plus bas).

Si la conjecture sur Π est vérifiée, il en résulterait que la donnée d'un groupe profini à lacets π de type (g, ν) , muni d'un groupe de Teichmüller géométrique strict $\Sigma \subset \hat{\mathfrak{Z}}(\pi)$ (ce qui peut-être n'est pas une structure supplémentaire du tout – Σ serait uniquement déterminé par π !) équivaudrait à la donnée d'une extension algébriquement close $\overline{\mathbb{Q}}$ de \mathbb{Q} (dont le groupe de Galois serait $\mathcal{N}_{\hat{\mathfrak{Z}}_0}(\Sigma)/\Sigma = \Pi_{\Sigma}$) et le Π_0 -torseur $\text{Isom}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}}_0)$ s'identifierait à l'ensemble $(\subset \text{Isom}(\hat{\pi}_{g,\nu}, \pi)/\hat{\mathfrak{Z}}_{g,\nu}^0)$ des quasi-rigidifications *orientées* donnant naissance à $\pi...$ et d'un revêtement universel de $\mathcal{U}_{g,\nu,\overline{\mathbb{Q}}}$ ou simplement d'un revêtement universel $\widetilde{\mathcal{U}}_{g,\nu}$ de $\mathcal{U}_{g,\nu} = \mathcal{U}_{g,\nu,\mathbb{Q}}$.¹⁶ La donnée d'un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}}_0$ revient donc à celle d'une quasi-rigidification orientée sur π compatible avec Σ (condition peut-être automatiquement satisfaite...). Ceci dit, la donnée d'une courbe algébrique de type g, ν sur un corps algébriquement clos $\overline{\mathbb{Q}}$, et d'un revêtement universel de celle-ci reviendrait à la donnée d'une donnée précédente (à savoir un revêtement universel d'un $\mathcal{M}_{g,\nu}$, *plus* un point de $\mathcal{M}_{g,\nu,\overline{\mathbb{Q}}}$ sur $\overline{\mathbb{Q}}$ définissant un revêtement universel)¹⁷, et cette dernière donnée s'identifierait à un germe de scindage dans l'extension

$$1 \rightarrow \pi_1(\mathcal{M}_{g,\nu,\overline{\mathbb{Q}}}) \rightarrow \pi_1(\mathcal{M}_{g,\nu}) \rightarrow \pi_1(\mathbb{Q}) \rightarrow 1.$$

L'interprétation profinie (en termes des groupes *extérieurs* à lacets π) est alors un (π, Σ) , et un germe de scindage de

$$1 \rightarrow \Sigma \rightarrow \mathcal{N}_{\Sigma} \rightarrow \Pi_{\Sigma} \rightarrow 1.$$

Si on veut une courbe sur une sous-extension finie K' de $\overline{\mathbb{Q}}/\mathbb{Q}$, correspondant à un sous-groupe d'indice fini $\Gamma' \subset \Pi_{\Sigma}$, il s'agira d'un scindage partiel $\Gamma' \rightarrow \mathcal{N}_{\Sigma}$.

Mais sûrement, si cette description des courbes algébriques anabéliennes est pleinement fidèle, elle n'est pas 2-fidèle, i.e. il faut des conditions sur ce scindage, qu'il faudra examiner par la suite.

¹⁶si on se donne seulement π comme groupe extérieur, avec Σ , ce qui revient à la donnée d'un revêtement universel de $\mathcal{M}_{g,\nu}$.

¹⁷NB. Si on renonce à choisir $\widetilde{\mathcal{U}}$, ceci revient à travailler avec les groupes à lacets *extérieurs*.

La description d'une courbe algébrique de type g, ν sur un corps fixé, de type fini sur \mathbb{Q} , K quelconque, muni d'une extension algébriquement close \bar{K} (donc $\Pi = \text{Gal}(\bar{K}/K) \rightarrow \Pi_0 = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, où $\bar{\mathbb{Q}}$ est la clôture algébrique de \mathbb{Q} dans \bar{K}), en termes de $\Pi \leftarrow \Pi_0$, serait la suivante: donnée d'un groupe extérieur à lacets π de type g, ν , d'un sous-groupe de Teichmüller Σ dans $\hat{\mathfrak{Z}}(\pi)$, d'un isomorphisme $\bar{\mathbb{Q}} \simeq$ corps défini par cette situation (ayant comme groupe de Galois $\mathcal{N}_\Sigma/\Sigma$, de sorte qu'on trouve un isomorphisme $\Pi_0 \simeq \mathcal{N}_\Sigma/\Sigma$), enfin d'un relèvement de $\Pi \rightarrow \Pi_0$ (qui décrit une action arithmétiquement extérieure de Π sur (π, Σ)) en une action extérieur $\Pi \rightarrow \mathcal{N}_\Sigma$ de Π sur (π, Σ) avec des conditions qu'il faudra essayer de dégager (nécessaires et suffisantes conjecturalement) sur ce relèvement.

Notons que tout plongement $\bar{K} \hookrightarrow \mathbb{C}$ définit canoniquement sur le groupe extérieur $\pi = \pi_1(\mathcal{U}_{\bar{K}})$ une quasi-discrétification orientée, remplacée par l'opposée quand on remplace le plongement par le complexe conjugué. Je dis que ces quasi-discrétifications définissent toutes Σ comme groupe des automorphismes et que la quasi-discrétification définie par $\bar{K} \hookrightarrow \mathbb{C}$ ne dépend que de sa restriction en $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ – de façon plus précise, c'est celle qu'on définit directement à l'aide de $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, i.e. de $\bar{\mathbb{Q}} \simeq \bar{\mathbb{Q}}_0$. Mais il y a lieu d'examiner aussi la façon d'obtenir des *discrétifications*. Ainsi, si un \mathcal{U} est défini sur $\bar{\mathbb{Q}}_0$, [c'est] un π extérieur de type (g, ν) , muni d'une quasi-discrétification orientée $\pi_0^{\text{h}+}$, et d'un germe de scindage de

$$1 \rightarrow \Sigma \rightarrow \mathcal{N}_\Sigma \rightarrow \Pi_\Sigma \rightarrow 1,$$

où $\Sigma = \text{Autext}_{\text{lac}}(\pi, \pi_0^{\text{h}+})$, qui fait opérer extérieurement le noyau du groupe défini par Π_Σ sur π , les points rationnels sur $\bar{\mathbb{Q}}_0$ correspondant aux classes de π -conjugaison des germes de relèvement de cette opération extérieure en une vraie opération. Supposons donc donné un tel point, i.e. on a un sous-groupe ouvert $\Pi \subset \Pi_\Sigma$ qui opère bel et bien sur π , l'opération définie mod automorphismes intérieurs (lui-même unique car $\pi^\Gamma = \{1\}$!) Dans cette situation, il faudrait définir dans $\pi \simeq \pi_1(\mathcal{U}_p, P)$ une *discrétification orientée* $\pi_0 \subset \pi$, et pas seulement une quasi-discrétification orientée! (Bien sûr, elle doit être dans la classe qu'on s'est donnée d'avance de discrétifications orientées, qu'on avait justement notée $\pi_0^{\text{h}+}$. On y reviendra – ainsi qu'à la situation analogue sur un corps de base K de type quelconque...)

Je réfère au début du § suivant (§27) pour le changement de terminologie, la “quasi-discrétification” devenant une “prédiscrétification”. Mais il y a lieu d'introduire aussi une notion plus fine, correspondant au cas d'un π_1 (profini) d'une variété algébrique X définie sur un corps algébriquement clos \bar{K} , quand on plonge \bar{K} dans \mathbb{C} : il y a une discrétification

mod automorphismes intérieurs – on l'appellera une *prédiscrétification stricte*. Dans le cas d'un π à lacets, l'espace homogène sous $\hat{\mathfrak{Z}}(\pi)$ de celles-ci s'identifie à

$$\mathrm{Isom}_{\mathrm{lac}}(\hat{\pi}_{g,v}, \pi) / (\hat{\pi}_{g,v} \cdot \mathfrak{Z}_{g,v}) \simeq \mathrm{Isom}_{\mathrm{ext}_{\mathrm{lac}}}(\hat{\pi}_{g,v}, \pi) / \mathfrak{Z}_{g,v},$$

et cette action également ne dépend que du groupe profini à lacets extérieur défini par $\pi_{g,v}$, et équivaut à celle d'une "base extérieure" de π mod action de $\mathfrak{Z}_{g,v}$, i.e. d'un isomorphisme de π avec le $\hat{\pi}_{g,v}$ "type", mod action de $\mathfrak{Z}_{g,v}$. L'application

$$\text{Bases extérieures de } \pi \rightarrow \text{Prédiscrétifications de } (\pi)$$

fait donc du membre de gauche un toreur relatif à droite sur celui de droite, de groupe $\mathfrak{Z}_{g,v}$.

Une prédiscrétification de (π, Σ) correspond à un choix d'un isomorphisme de la clôture algébrique $\overline{\mathbb{Q}}_{(\pi, \Sigma)} = \overline{\mathbb{Q}}$ associé à (π, Σ) , avec $\overline{\mathbb{Q}}_0$. Quand on se donne (π, Σ) comme correspondant à une courbe algébrique sur $\overline{\mathbb{Q}}$, i.e. qu'on se donne un germe de relèvement de Π_Σ dans $\mathcal{N}_\Sigma \subset \hat{\mathfrak{Z}}(\pi)$, i.e. un germe d'actions extérieures de Π_Σ sur π , toute prédiscrétification doit donner naissance à une discrétification stricte et même à une discrétification quand on remonte un germe d'action ("admissible") de Π_Σ sur π ...

§ 27. — CHANGEMENT DE TYPE (g, ν)

(a) Bouchage de trous

Je vais changer de terminologie, en appelant prédiscrétification ce que j'avais appelé (un peu péjorativement!) quasi-discrétification. En effet, on prévoit qu'une prédiscrétification – compatible avec Σ – qui revient moralement au plongement (modulo la conjugaison complexe) dans \mathbb{C} de la clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} canoniquement associé à $(\pi, \Sigma(\subset \hat{\mathfrak{Z}}(\pi)))$, donne naissance, dès que l'action extérieure arithmétique de $\Pi_\Sigma = \mathcal{N}_\Sigma/\Sigma$ sur π est relevée en un germe d'action sur π , à une vraie discrétification de π . Itou pour les prédiscrétifications orientées. Le groupe $\mathcal{N}_\Sigma/\Sigma$ mérite aussi un nom – je vais l'appeler le *groupe de Teichmüller arithmétique* associé à (π, Σ) ¹⁸, et ses éléments seront appelés les automorphismes arithmétiquement extérieurs de π – déduits d'un automorphisme extérieur (normalisant Σ) en négligeant les automorphismes extérieurs “géométriques” (i.e. justement ceux dans Σ) – comme les automorphismes extérieurs ordinaires étaient décrits en négligeant les automorphismes intérieurs de π . On fera attention que le caractère “multiplicateur”

$$\chi : \hat{\mathfrak{Z}}(\pi) \rightarrow \hat{\mathbb{Z}}^*$$

est trivial sur Σ , par construction de Σ , et passe à Π_Σ :

$$\chi_\Sigma : \Pi_\Sigma \rightarrow \hat{\mathbb{Z}}^*.$$

¹⁸moralement, $\Sigma = \hat{\mathfrak{Z}}^+$, mais il n'y a pas de $\hat{\mathfrak{Z}}^!$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Bien sûr, ce caractère s'appellera encore “multiplicateur”, ou “caractère cyclotomique”. Si notre conjecture fondamentale est vraie¹, ce caractère identifie $(\Pi_\Sigma)_{\text{ab}}$ à \hat{Z}^* . Par contre, si $I = I(\pi)$, l'homomorphisme canonique

$$\hat{\mathfrak{Z}} \rightarrow \mathfrak{S}_I$$

n'est pas trivial sur Σ , mais induit un homomorphisme surjectif:

$$\Sigma \rightarrow \mathfrak{S}_I,$$

d'où un sous-groupe $\Sigma^!$ tel que

$$\Sigma/\Sigma^! \xrightarrow{\sim} \mathfrak{S}_I.^{19}$$

On voit de suite que tout $\gamma \in \hat{\mathfrak{Z}}$ qui normalise Σ normalise $\Sigma^! = \Sigma \cap \hat{\mathfrak{Z}}^!$, d'où $\Sigma^!$ est aussi invariant dans \mathcal{N}_Σ . Soit $\mathcal{N}_\Sigma^! = \mathcal{N}_\Sigma \cap \hat{\mathfrak{Z}}^!$, on a un diagramme cartésien de sous-groupes de $\hat{\mathfrak{Z}}$:

$$\begin{array}{ccc} \mathcal{N}^! & \xrightarrow{\mathfrak{S}_I} & \mathcal{N} \\ \Pi_\Sigma \uparrow & & \uparrow \Pi_\Sigma \\ \Sigma^! & \xrightarrow{\mathfrak{S}_I} & \Sigma \end{array}$$

donnant un homomorphisme injectif $\mathcal{N}/\Sigma^! \xrightarrow{\sim} \mathcal{N}/\mathcal{N}^! \times \mathcal{N}/\Sigma$ (ici $\mathcal{N}/\mathcal{N}^! = \mathfrak{S}_I$, $\mathcal{N}/\Sigma = \Pi_\Sigma$ et $\Sigma/\Sigma^! \xrightarrow{\sim} \mathcal{N}/\mathcal{N}^! \simeq \mathfrak{S}_I$), dont on voit de suite qu'il est bijectif

$$\mathcal{N}/\Sigma^! \xrightarrow{\sim} \mathcal{N}/\mathcal{N}^! \times \mathcal{N}/\Sigma \simeq \mathfrak{S}_I \times \Pi_\Sigma,$$

et on a par suite aussi

$$\mathcal{N}^!/\Sigma^! \xrightarrow{\sim} \mathcal{N}/\Sigma = \Pi_\Sigma,$$

i.e. le groupe Π_Σ des automorphismes arithmétiquement extérieurs de (π, Σ) peut se décrire aussi via les automorphismes extérieurs induisant l'identité sur I .

Dans le cas $(g, \nu) = (0, 3)$, on a $\Sigma^! = \{1\}$, donc $\Sigma \xrightarrow{\sim} \mathfrak{S}_3$. \mathcal{N} est le normalisateur de \mathfrak{S}_3 dans $\hat{\mathfrak{Z}}$, $\mathcal{N}^! \xrightarrow{\sim} \Pi_\Sigma$ est son centralisateur, et \mathcal{N} s'identifie au produit direct des deux.

Soit maintenant $I' \subset I$, $\nu' = \text{card}(I')$, et considérons le groupe extérieur π' déduit de π par “bouchage de trous” en $I \setminus I'$, d'où un homomorphisme

$$\pi \rightarrow \pi'.$$

¹⁹ moralement, $\Sigma^! \simeq \hat{\mathfrak{Z}}^{!+}$

A. GROTHENDIECK

Considérons les bases de π pour lesquelles, les ν' premiers l_i soient dans des groupes à lacets $L_{i'}$ ($i' \in I'$) – on les appelle adaptées à I' ; elles forment un toreur $\subset \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi)$ sous le sous-groupe $\hat{\mathfrak{S}}_{g;(\nu,\nu')}$ de $\hat{\mathfrak{S}}_{g,\nu} = \text{Aut}_{\text{lac}}(\hat{\pi}_{g,\nu})$, formé des $u \in \hat{\mathfrak{S}}_{g,\nu}$ dont l'image dans \mathfrak{S}_I invarie l'ensemble des ν' premiers éléments (ou encore l'ensemble complémentaire des $\nu - \nu'$ derniers).

Pour une telle base, on trouve une base correspondante de π' . La donnée de (π, I') équivaut à celle d'un toreur sous $\hat{\mathfrak{S}}_{g;(\nu,\nu')}$, celle d'un π' à la donnée d'un toreur sous $\hat{\mathfrak{S}}_{g,\nu'}$, et le passage de π à π' est décrit par le changement de groupe d'opérateurs

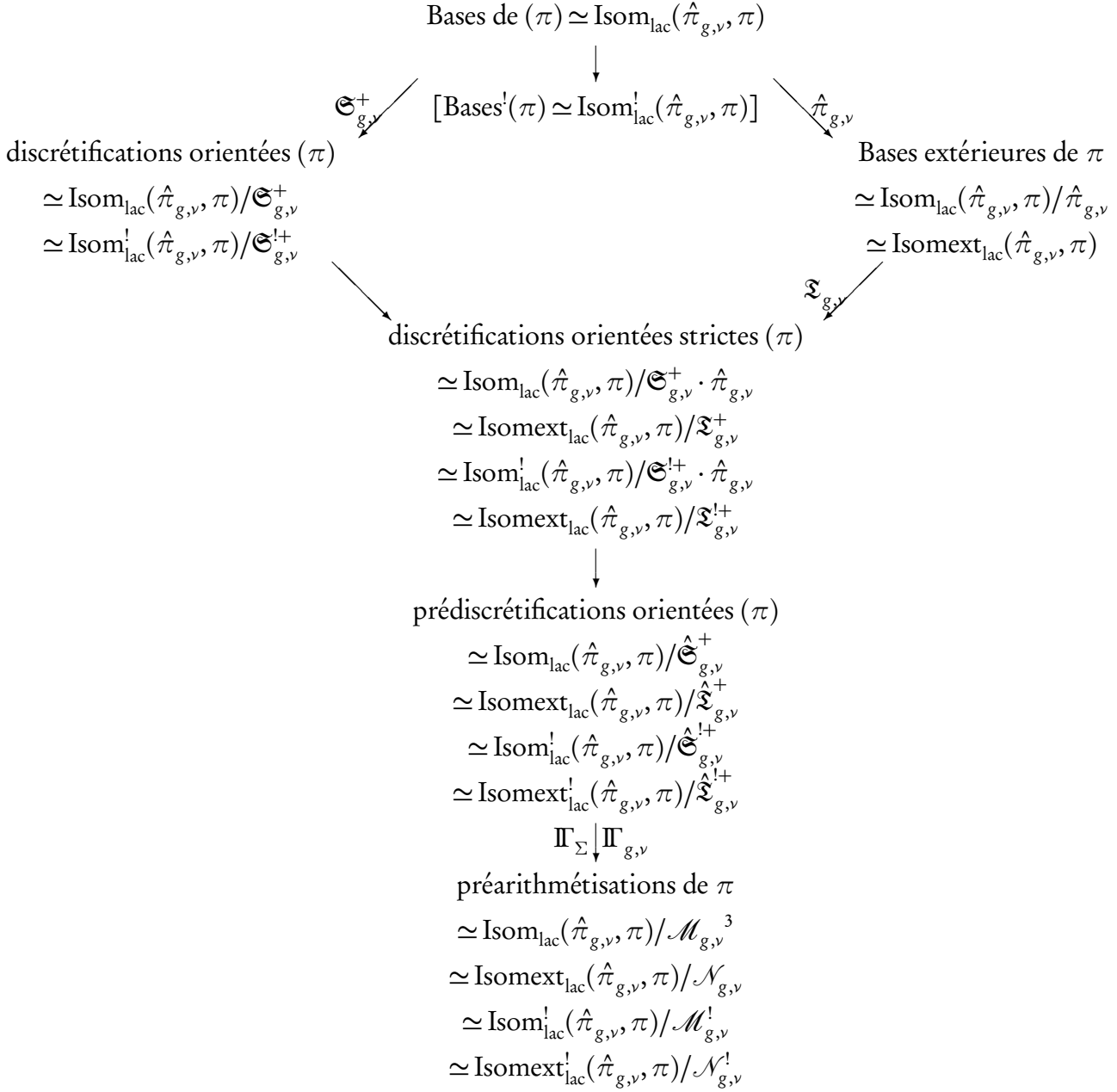
$$\hat{\mathfrak{S}}_{g;(\nu,\nu')} \rightarrow \hat{\mathfrak{S}}_{g,\nu'}.^{20}$$

Cet homomorphisme envoie $\hat{\mathfrak{S}}_{g;(\nu,\nu')}$ dans $\hat{\mathfrak{S}}_{g,\nu'}$, et même $\mathfrak{S}_{g;(\nu,\nu')}$ dans $\mathfrak{S}_{g,\nu'}$, aussi π dans π' . Il s'ensuit que toute prédiscrétification de π en définit une de π' , de même pour les prédiscrétifications strictes, discrétifications, bases extérieures “adaptées à I' ”. Enfin, si on a une “préarithmétisation”² de π , i.e. un $\Sigma \subset \hat{\mathfrak{Z}}(\pi)$, en déduit-on une préarithmétisation de π' – i.e. (par exemple) si deux prédiscrétifications de π sont compatibles i.e. ont le même groupe $\Sigma \subset \hat{\mathfrak{Z}}(\pi)$ d'automorphismes extérieurs, en est-il de même de leurs images?

Pour y voir plus clair, on va écrire sous forme de diagramme les ensembles remarquables associés à π , et ceci de deux façons, l'une sans utiliser de structure particulière sur $I = I(\pi)$, l'autre en utilisant un ordre total, ce qui permet, dans le toreur $\text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi)$ sous $\hat{\mathfrak{S}}_{g,\nu}$, de définir le sous-toreur sous $\hat{\mathfrak{S}}_{g,\nu}^!$ qu'on peut noter $\text{Isom}_{\text{lac}}^!(\hat{\pi}_{g,\nu}, \pi)$.

²⁰D'où aussi: toute base, toute discrétification, discrétification orientée de π en définit une de π' , itou pour les classes de π, π' conjugaison i.e. pour les prédiscrétifications (éventuellement orientées) strictes, et aussi pour les adhérences des classes i.e. pour les prédiscrétifications et prédiscrétifications orientées. Il n'y a que le cas des arithmétisations qui demande une analyse plus fine.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS



A. GROTHENDIECK

NB: On pose

$$\Pi_{g,\nu} = \mathcal{N}_{g,\nu} / \Sigma_{g,\nu} = \mathcal{N}_{g,\nu}^! / \Sigma_{g,\nu}^!$$

(où $\Sigma_{g,\nu} = \hat{\mathfrak{Z}}_{g,\nu}^+$, $\Sigma_{g,\nu}^! = \hat{\mathfrak{Z}}_{g,\nu}^{!+}$). On peut aussi le décrire comme le groupe Π_Σ associé à un groupe extérieur profini à lacets π muni d'une prédiscrétification orientée α (sans plus). Si on a deux tels couples (π, α) , (π', α') , d'où Π_Σ et $\Pi_{\Sigma'}$ ($\Sigma = \text{Autext}_{\text{lac}}(\pi, \alpha)$, $\Sigma' = \text{Autext}_{\text{lac}}(\pi', \alpha')$), on trouve en effet un isomorphisme *canonique*:

$$\Pi_\Sigma \xrightarrow{\sim} \Pi_{\Sigma'}$$

en prenant n'importe quel isomorphisme extérieur à lacets u de π avec π' transformant α en α' et l'isomorphisme associé $\Pi_\Sigma \rightarrow \Pi_{\Sigma'}$ ne dépend évidemment pas du choix de u .

Ceci posé, les couples (π, Σ) d'un groupe profini à lacets de type (g, ν) , muni d'une préarithmétisation, avec comme morphismes les isomorphismes arithmétiquement extérieurs (relatifs à Σ et $\Sigma' \dots$), forment un groupoïde connexe $\Pi_{g,\nu}$, ayant un objet "origine" défini à isomorphisme unique près comme étant $(\hat{\pi}_{g,\nu}, \Sigma_{g,\nu})$, où au choix n'importe quel (π, Σ_α) provenant d'un (π, α) (α une prédiscrétification orientée de π), et dont le groupe des automorphismes est justement $\Pi_{g,\nu}$.

On constate qu'à l'exception des deux espaces homogènes (sous $\hat{\mathfrak{S}}(\pi)$, mais pas nécessairement sous $\hat{\mathfrak{S}}(\pi, I')$, voire sous $\hat{\mathfrak{S}}^!(\pi)$) Bases(π) et Bases ext(π), les quatre autres sont en fait des espaces homogènes sous $\hat{\mathfrak{S}}^!$, et s'expriment comme quotients du $\hat{\mathfrak{S}}_{g,\nu}^!$ -torseur $\text{Isom}^!(\hat{\pi}_{g,\nu}, \pi)$, par les quatre sous-groupes $\mathfrak{S}_{g,\nu}^!$, $\mathfrak{S}_{g,\nu}^! \cdot \hat{\pi}_{g,\nu}$, $\hat{\mathfrak{S}}_{g,\nu}^!$, $\mathcal{M}_{g,\nu}^!$ (ce dernier défini comme image inverse de $\mathcal{N}_{g,\nu}^!$ dans $\hat{\mathfrak{S}}_{g,\nu}^!$, tout comme $\mathcal{M}_{g,\nu}$ est défini comme image inverse de $\mathcal{N}_{g,\nu}$). On trouve d'autre part, si $I' = \{i_0, \dots, i_{\nu'-1}\}$, un homomorphisme $\hat{\mathfrak{S}}_{g,\nu}^! \rightarrow \hat{\mathfrak{S}}_{g,\nu'}^!$, envoyant $\mathfrak{S}_{g,\nu}^!$ dans $\mathfrak{S}_{g,\nu'}^!$, en envoyant $\pi_{g,\nu}$ dans $\pi_{g,\nu'}$, donc $\hat{\pi}_{g,\nu}$ dans $\hat{\pi}_{g,\nu'}$, $\hat{\mathfrak{S}}_{g,\nu}^!$ dans $\hat{\mathfrak{S}}_{g,\nu'}^!$, et le sous-groupe $\mathfrak{S}_{g,\nu}^! \cdot \hat{\pi}_{g,\nu}$ de $\hat{\mathfrak{S}}_{g,\nu}^!$ dans le sous-groupe $\mathfrak{S}_{g,\nu'}^! \cdot \hat{\pi}_{g,\nu'}$ de $\hat{\mathfrak{S}}_{g,\nu'}^!$. Enfin, comme $\Sigma_{g,\nu}^!$ s'envoie dans $\Sigma_{g,\nu'}^!$, $\mathcal{N}_{g,\nu}^!$ s'envoie dans le normalisateur de $\Sigma_{g,\nu'}^!$ dans $\hat{\mathfrak{Z}}_{g,\nu'}^!$, je dis que ce n'est autre que $\mathcal{N}_{g,\nu'}^!$. Changeant de notation, ceci revient au

Lemme: ²¹ $\mathcal{N}_\Sigma^! = \text{Norm}_{\hat{\mathfrak{Z}}^!}(\Sigma^!) (= \text{Norm}_{\hat{\mathfrak{Z}}}(\Sigma^!) \cap \hat{\mathfrak{Z}}^!)$.

²¹pas prouvé

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

Evidemment on a $\mathcal{N}_\Sigma^! \subset \text{Norm}_{\hat{\mathfrak{Z}}}(\Sigma^!) \cap \hat{\mathfrak{Z}}^!$; inversement soit $g \in \hat{\mathfrak{Z}}^!$ qui normalise $\Sigma^!$, montrons qu'il normalise Σ , i.e. qu'il est $\in \mathcal{N}$ (donc $\in \mathcal{N}^! = \mathcal{N} \cap \hat{\mathfrak{Z}}^!$)....

C'est pas clair. J'ai pourtant envie de prouver la

Conjecture: L'application canonique

$$\text{Prédiscrét}^+(\pi) \rightarrow \text{Prédiscrét}^+(\pi')$$

est *bijective*. Pour que deux prédiscrétifications orientées α, β de π aient même groupe d'automorphismes extérieurs $\Sigma_\alpha = \Sigma_\beta$, il faut qu'il en soit ainsi pour leurs images $\Sigma_{\alpha'}$ et $\Sigma_{\beta'}$, i.e. que $\Sigma_{\alpha'} = \Sigma_{\beta'}$, de sorte que la bijection précédente induit une bijection

$$\text{Préarithmétisation}(\pi) \xrightarrow{\sim} \text{Préarithmétisation}(\pi').$$

Enfin, les bijections précédentes sont compatibles avec l'homomorphisme des groupes d'opérateurs $\hat{\mathfrak{Z}}(\pi, I') \rightarrow \hat{\mathfrak{Z}}(\pi')^4$, a fortiori avec $\hat{\mathfrak{Z}}^!(\pi) \rightarrow \hat{\mathfrak{Z}}^!(\pi')$, ce qui implique qu'elle induit (pour une préarithmétisation $\Sigma \subset \hat{\mathfrak{Z}}(\pi)$ donnée de π , donnant $\Sigma' \subset \hat{\mathfrak{Z}}(\pi')$ dans π' avec $\Sigma^! \rightarrow \Sigma'^!$)⁵ un homomorphisme $\mathcal{N}_\Sigma^! \rightarrow \mathcal{N}_{\Sigma'}^!$, et l'homomorphisme correspondant

$$\Pi_\Sigma = \mathcal{N}_\Sigma^! / \Sigma^! \rightarrow \Pi_{\Sigma'} = \mathcal{N}_{\Sigma'}^! / \Sigma'^!$$

est un isomorphisme.

Pour s'en convaincre il suffit de regarder le cas où $I' = \{i\}$ (et si on note $\pi = \pi_{g,\nu}$, I' réduit au dernier élément de I). On a alors un homomorphisme

$$\hat{\mathfrak{Z}}(\pi, i) \rightarrow \hat{\mathfrak{E}}(\pi')^6$$

(les automorphismes *extérieurs* à lacets de π fixant i définissent des automorphismes bien déterminés de π' – pas seulement extérieurs, i.e. $\hat{\mathfrak{E}}(\pi, i) \rightarrow \hat{\mathfrak{E}}(\pi')$ est trivial sur π , et passe donc au quotient en $\hat{\mathfrak{Z}}(\pi, i) \rightarrow \hat{\mathfrak{E}}(\pi, i)$).

J'admets, en analogie avec le cas discret, que cet homomorphisme est un *isomorphisme*, de sorte qu'on a une suite exacte²²

$$1 \rightarrow \pi' \rightarrow \hat{\mathfrak{Z}}(\pi, i) \rightarrow \hat{\mathfrak{E}}(\pi, i) \rightarrow 1$$

²²rappelons qu'on suppose π anabélien, i.e. $2g + \nu \geq 3$

A. GROTHENDIECK

ou encore

$$1 \rightarrow \hat{\pi}_{g,\nu-1} \rightarrow \hat{\mathfrak{Z}}_{g;(\nu,\nu-1)} \rightarrow \hat{\mathfrak{E}}_{g,\nu-1} \rightarrow 1$$

qui contient la suite exacte

$$1 \rightarrow \pi_{g,\nu-1} \rightarrow \mathfrak{Z}_{g;(\nu,\nu-1)} \rightarrow \mathfrak{E}_{g,\nu-1} \rightarrow 1$$

comme sous-suite exacte. Il est commode de travailler plutôt avec

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi_{g,\nu-1} & \longrightarrow & \mathfrak{Z}_{g,\nu}^{!+} & \longrightarrow & \mathfrak{E}_{g,\nu-1}^{!+} \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \hat{\pi}_{g,\nu-1} & \longrightarrow & \hat{\mathfrak{Z}}_{g,\nu}^{!+} & \longrightarrow & \hat{\mathfrak{E}}_{g,\nu-1}^{!+} \longrightarrow 1 \\ & & \parallel & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \hat{\pi}_{g,\nu-1} & \longrightarrow & \hat{\mathfrak{Z}}_{g,\nu}^! & \longrightarrow & \hat{\mathfrak{E}}_{g,\nu-1}^! \longrightarrow 1. \end{array}$$

L'application $\text{Prédiscrét}^+(\pi) \rightarrow \text{Prédiscrét}^+(\pi')$ s'identifie alors à $\hat{\mathfrak{Z}}_{g,\nu}^! / \hat{\mathfrak{Z}}_{g,\nu}^{!+}$, on lit sur le diagramme que c'est $\simeq \hat{\mathfrak{E}}_{g,\nu-1}^! / \hat{\mathfrak{E}}_{g,\nu-1}^{!+}$, d'où la bijectivité sur les ensembles de prédiscrétifications orientées.

Dans le groupe $\hat{\mathfrak{Z}}_{g,\nu}^! = \mathfrak{Z}$, on a un sous-groupe invariant $\hat{\pi}_{g,\nu-1} = \pi'$, et un sous-groupe $\Sigma (= \hat{\mathfrak{Z}}_{g,\nu}^{!+})$ entre π' et \mathfrak{Z} , donnant un sous-groupe $\Sigma' \simeq \hat{\mathfrak{E}}_{g,\nu-1}^{!+}$ dans $\mathfrak{Z}' = \mathfrak{Z}/\pi' (\simeq \hat{\mathfrak{E}}_{g,\nu-1}^!)$, et on sait bien qu'alors $\mathfrak{Z}/\Sigma \simeq \mathfrak{Z}'/\Sigma'$, et que le normalisateur \mathcal{N} de Σ dans \mathfrak{Z} est l'image inverse du normalisateur \mathcal{N}' de Σ' dans \mathfrak{Z}' , de sorte que $\mathcal{N}/\Sigma \simeq \mathcal{N}'/\Sigma'$, ce qui prouve ce qu'on voulait.

Corollaire: On a des isomorphismes canoniques:

$$\Pi_{g,\nu} \xrightarrow{\sim} \Pi_{g,\nu-1} \xrightarrow{\sim} \dots$$

de sorte que si $g \geq 2$, on a canoniquement $\Pi_{g,\nu} \simeq \Pi_{g,0}$; d'autre part $\Pi_{1,\nu} \simeq \Pi_{1,1}$ ($g = 1, \nu \geq 1$), $\Pi_{0,\nu} \simeq \Pi_{0,3}$ ($\nu \geq 3$).²³

NB: Le “fait” admis est loin d'être évident – même que $\hat{\mathfrak{Z}}_{g;(\nu,\nu-1)} \rightarrow \hat{\mathfrak{Z}}_{g,\nu-1}$ soit surjectif ou que $\hat{\mathfrak{Z}}_{g;(\nu,\nu-1)} \rightarrow \hat{\mathfrak{E}}_{g,\nu-1}$ soit injectif, est loin d'être évident, et est peut-être tout à fait faux! Le fait admis revient à un énoncé d'existence d'un foncteur en sens inverse “forage de trous” qui en tout état de cause reste incompris.

²³On voit aussi que Σ invariant dans $\hat{\mathfrak{Z}}$ équivaut à Σ' invariant dans $\hat{\mathfrak{Z}}'$.

§ 28. — CHANGEMENT DE TYPE (g, ν) (SUITE)

(b) passage à un revêtement fini

Soit π un groupe profini à lacets de type (g, ν) , anabélien comme toujours, π' un sous-groupe d'indice fini. On sait (ou on vérifie, par passage au cas discret) que muni des traces sous π des sous-groupes à lacets de π , π' est un groupe à lacets. Ses sous-groupes à lacets sont aussi les sous-groupes L' tels que

a) $L' = \text{Centr}_{\pi}(L') \cap \pi'$

b) $L = \text{Centr}_{\pi}(L')$ est un sous-groupe à lacets dans π .

On pose $d(L') = [L : L']$, et on a ainsi une fonction $d : I' = I(\pi') \rightarrow \mathbb{N}^*$, et une application $I' \xrightarrow{\varphi} I$, telles que $\forall i \in I$, on ait:

$$(1) \quad \sum_{\substack{i' \in I' \\ i' \text{ au dessus de } i}} d(i') = n \quad (\text{où } n = [\pi : \pi']).$$

On aura la formule de Hurwitz

$$(2) \quad 2g' - 2 = n(2g - 2) + \sum_{i' \in I'} (d(i') - 1),$$

où la somme à droite est égale à $(n \text{ card}(I) - \text{card}(I'))$, i.e.

$$(3) \quad 2g' - 2 + \text{card}(I') = n(2g - 2 + \text{card}(I)).$$

(NB. $2g - 2 + \text{card}(I)$ est l'opposé de la caractéristique d'Euler-Poincaré à supports compacts

A. GROTHENDIECK

de la courbe dont π est le groupe fondamental...²⁴

De façon évidente, toute discrétification de π en définit une de π' – et il en est de même pour les discrétifications orientées, modulo un peu de cohomologie, ce qui revient à dire, dans le cas discret par exemple, que $T \simeq H_!^2(\mathcal{U}, \mathbb{Z}) \rightarrow H_!^2(\mathcal{U}', \mathbb{Z}) \simeq T'$ peut s'écrire sous la forme $n\theta^{-1}$, où θ est un isomorphisme bien déterminé (l'isomorphisme trace) $T' \xrightarrow{\sim} T$.

Il n'est pas clair pour moi à première vue si l'application

$$\text{Discrét}(\pi) \rightarrow \text{Discrét}(\pi')$$

est surjective, ou injective. L'injectivité pour tout π' d'indice fini dans π signifierait que deux discrétifications π_0, π'_0 de π qui sont commensurables, i.e. telles que $\pi_0 \cap \pi'_0$ soit d'indice fini dans π_0 et dans π'_0 , sont égales.

Supposons que π' soit un sous-groupe invariant dans π , et posons $G = \pi/\pi'$.

Conjecture: L'application $\text{Discrét}(\pi) \rightarrow \text{Discrét}(\pi')$ est injective, et son image est formée des discrétifications $\pi'_0 \subset \pi'$ telles que $G \rightarrow \text{Autext}_{\text{lac}}(\pi') \simeq \text{Autext}_{\text{lac}}(\hat{\pi}'_0) \simeq \hat{\mathfrak{Z}}(\hat{\pi}'_0)$ se factorise par $\mathfrak{Z}(\pi'_0) = \text{Autext}_{\text{lac}}(\pi'_0)$ (et en fait, même par $\mathfrak{Z}(\pi'_0)^+$). En d'autres termes, $\forall g \in \pi, \exists h \in \pi'$ tel que $\text{Int}(hg)(\pi'_0) \subset \pi'_0$, i.e. $\pi' \cdot \pi_0 = \pi$, où π_0 est le normalisateur de π'_0 dans π .

La condition pour qu'un π'_0 soit dans l'image est évidemment nécessaire. Montrons qu'elle est suffisante, et que le π_0 donnant naissance à π'_0 par $\pi_0 \cap \pi'$ est unique. On a une action extérieure de G sur π'_0 , qui définit l'action extérieure sur $\hat{\pi}'_0 \simeq \pi'$, or π se récupère canoniquement à partir de cette dernière (car $\text{Centre}(\hat{\pi}') = 1$), et on voit que c'est le complété profini de l'extension π_0 de G par π'_0 , définie par l'action extérieure de G sur π'_0 . On a donc bien une discrétification généralisée π_0 de π , au sens de la seule structure de groupe profini, et elle induit π'_0 – mais il faut voir qu'elle est compatible avec la structure à lacets de π . Mais celle-ci s'explicite, à partir de la structure à lacets de π' , en prenant les sous-groupes à lacets L' de π' , et leurs centralisateurs dans π . Faisant itou pour $\pi_0 \supset \pi'_0$, on devrait trouver une structure à lacets sur π_0 , donnant lieu aux mêmes d_i . J'ai l'impression que ça ne doit pas être très vache à prouver – ce serait comme si on savait déjà que toute extension “sans torsion” d'un groupe fini par un groupe à lacets est de façon canonique un groupe à lacets...

²⁴NB. Dire qu'on est dans le cas anabélien signifie que $-\text{EP}_1$ [i.e. l'opposé de la caractéristique d'Euler-Poincaré à support compact] est ≥ 1 , et cette relation est donc conservée par passage à un revêtement. L'entier $-\text{EP}_1$ mesure par sa positivité stricte le degré d'anabélianité en quelque sorte..

Corollaire: En tout cas, l'application

$$\text{Discrét}(\pi) \rightarrow \text{Discrét}(\pi')$$

est *injective*.

NB: Elle ne doit pas toujours être bijective, car il doit y avoir une action extérieure d'un G sur un $\hat{\pi}'_0$, i.e. un homomorphisme $G \rightarrow \hat{\mathfrak{Z}}(\hat{\pi}'_0)$, qui ne se factorise pas par $\mathfrak{Z}(\pi'_0)$, et qui pourtant est aussi bonne du point de vue groupe profini que celles provenant d'un π et d'un sous-groupe invariant π' . En fait, partons d'une telle situation *discrète* $\pi_0 \supset \pi'_0$, d'où $G = \pi_0/\pi'_0$ et $G \rightarrow \text{Autext}_{\text{lac}}(\pi'_0) = \mathfrak{Z}(\pi'_0) \subset \hat{\mathfrak{Z}}(\hat{\pi}'_0)$, et *conjuguons* G par un élément γ de $\hat{\mathfrak{Z}}(\pi'_0)$, de façon à trouver $G \rightarrow \hat{\mathfrak{Z}}(\hat{\pi}'_0)$ qui ne se factorise pas par $\mathfrak{Z}(\pi'_0)$. On trouve une extension π^{\natural} de G par $\hat{\pi}'_0$, *isomorphe* à $\hat{\pi}_0$ (en tant qu'extension de G par $\hat{\pi}'_0$), donc la structure à lacets de $\hat{\pi}'_0$ en définit une sur π^{\natural} (de façon à être induite par cette dernière), mais pourtant la discrétification choisie π_0 de $\hat{\pi}_0$ n'est pas induite par une de π . Pour faire la construction, il suffit de trouver un élément $\gamma \in \hat{\mathfrak{Z}}(\pi'_0)$ tel que $\text{Int}(\gamma) \cdot G \not\subset \mathfrak{Z}$ i.e. tel que G ne stabilise pas $\gamma^{-1}(\pi'_0) \subset \hat{\pi}'_0$. Un tel γ existe toujours...

Bien sûr, il n'y a pas de raison, pour deux discrétifications π_0, π_1 de π , que si π_0, π_1 sont π -conjugués (i.e. définissent la même prédiscrétification stricte de π), il en soit de même pour π'_0 et π'_1 pour l'action intérieure de π' (il faudrait que π_0, π_1 soient conjugués par π' , et pas seulement par π). Par contre, je présume que si π_0, π_1 sont "adhérents" l'un à l'autre dans l'espace des discrétifications de π , i.e. s'ils définissent une même prédiscrétification, il en est de même pour π'_0, π'_1 , et que l'application

$$(4) \quad \text{Prédiscrét}(\pi) \rightarrow \text{Prédiscrét}(\pi')$$

qu'on obtient ainsi, est encore bijective, et qu'elle passe à son tour au quotient, pour définir une application bijective

$$(5) \quad \text{Préarith}(\pi) \rightarrow \text{Préarith}(\pi'),$$

et que si Σ, Σ' se correspondent par cette dernière, on a un isomorphisme canonique

$$(6) \quad \Pi_{\Sigma} \rightarrow \Pi_{\Sigma'},$$

compatible avec les actions de ces groupes sur l'ensemble P_Σ des prédiscrétifications de π compatibles à Σ , et l'ensemble $P_{\Sigma'}$ des prédiscrétifications de π' compatibles à Σ' (qui sont respectivement des torseurs à gauche sous $\Pi_\Sigma, \Pi_{\Sigma'}$). En même temps, on trouvera donc que Σ est unique pour π , i.e. invariant dans $\hat{\mathfrak{Z}}(\pi)$, si et seulement si Σ' est unique dans π' , i.e. invariant dans $\hat{\mathfrak{Z}}(\pi')$.

En tout cas, la conjecture fondamentale qui interprète les $\Pi_{g,v}$ comme $\Pi_0 = \text{Gal}(\overline{\mathbb{Q}_0}/\mathbb{Q})$ aurait au moins comme conséquence que l'application $\text{Discrét}^+(\pi) \rightarrow \text{Discrét}^+(\pi')$ passe au quotient de deux façons, pour donner un diagramme commutatif:

$$\begin{array}{ccc} \text{Discrét}^+(\pi) & \longrightarrow & \text{Discrét}^+(\pi') \\ \downarrow & & \downarrow \\ P = \text{Prédiscrét}^+(\pi) & \longrightarrow & P' = \text{Prédiscrét}^+(\pi') \\ \downarrow & & \downarrow \\ A = \text{Arithm}(\pi) & \longrightarrow & A' = \text{Arithm}(\pi') \end{array}$$

et que le carré inférieur est cartésien (sans préjuger de l'injectivité ou de la bijectivité de l'application $A \rightarrow A'$). Donc il faudrait que si π_0, π_1 sont deux discrétifications orientées de π , qui définissent la même prédiscrétification (orientée), alors il en soit de même pour leurs traces sur π', π'_0 et π'_1 , relativement à π' . Mais déjà si π_0 et π_1 sont π -conjugués (i.e. définissent la même discrétification orientée, *stricte*), ce n'est pas tellement clair – mais si, car on aura $\pi = \pi' \cdot \pi_0$ donc si $\pi_1 = \text{int}(u) \pi_0$, écrivant $u = u' u_0$ avec $u' \in \pi', u_0 \in \pi_0$, on aura $\pi_1 = \text{int}(u') \text{int}(u_0) \pi_0 = \text{int}(u') \pi_0$, donc $\pi'_1 = \text{int}(u') \pi'_0$ donc π'_0 et π'_1 sont conjugués. Tâchons de procéder de même dans le cas général d'un $u \in \hat{\mathfrak{S}}(\pi_0)^+$ tel que $\pi_1 = u(\pi_0)$, en écrivant si possible $u = u' u_0$, avec $u' \in \hat{\mathfrak{S}}(\pi_0, \pi'_0)^+$, et $u_0 \in \mathfrak{S}(\pi_0)^+$, où on définit $\mathfrak{S}(\pi_0, \pi'_0)^+$ comme le groupe des automorphismes discrets de π_0 qui *stabilisent* π'_0 , et $\hat{\mathfrak{S}}(\pi_0, \pi'_0)^+$ est son compactifié profini. On aurait alors $\pi_1 = u'(u_0(\pi_0)) = \dot{u}'(\pi_0)$, où \dot{u}' désigne l'image de u' dans $\hat{\mathfrak{Z}}(\pi'_0)$. En tous cas, il n'y a aucun problème si π' est un sous-groupe *caractéristique* de π , car alors on a un homomorphisme discret $\mathfrak{S}(\pi_0) \rightarrow \mathfrak{S}(\pi'_0)$, définissant l'homomorphisme $\hat{\mathfrak{S}}(\hat{\pi}_0) \rightarrow \hat{\mathfrak{S}}(\hat{\pi}'_0)$. Comme les sous-groupes ouverts caractéristiques de π sont cofinaux, on est ramené (pour les questions de factorisabilité de $D(\pi) \rightarrow D(\pi')$ en $P(\pi) \rightarrow P(\pi')$ et $A(\pi) \rightarrow A(\pi')$ et de bijectivité des applications $P(\pi) \rightarrow P(\pi')$ et $A(\pi) \rightarrow A(\pi')$) au cas où π' est un sous-groupe *caractéristique*. On a alors factorisabilité de $D(\pi) \rightarrow D(\pi')$ en $P(\pi) \rightarrow P(\pi')$. Montrons que cette application est injective... Cela signifie (a) que l'image

inverse dans $\hat{\mathfrak{S}}(\hat{\pi}_0)$ de $\hat{\mathfrak{S}}(\hat{\pi}'_0)^+$ est $\hat{\mathfrak{S}}(\hat{\pi}_0)^+$, la surjectivité signifie (b) que tout élément de $\hat{\mathfrak{S}}(\hat{\pi}'_0)$ est congru mod $\hat{\mathfrak{S}}(\pi'_0)^+$ à un élément de l'image de $\hat{\mathfrak{S}}(\pi_0)$. La factorisabilité en $A(\pi) \rightarrow A(\pi')$ signifie que (c) par l'application précédente $\hat{\mathfrak{S}}(\pi_0) \hookrightarrow \hat{\mathfrak{S}}(\pi'_0)$, (NB. il est immédiat que c'est injectif) envoie $\mathcal{M}(\pi_0) = \text{Norm}_{\hat{\mathfrak{S}}(\pi_0)}(\hat{\mathfrak{S}}^+(\pi_0))$ dans $\mathcal{M}(\pi'_0)$, l'injectivité de $A(\pi) \rightarrow A(\pi')$ que (d) l'on a même que $\mathcal{M}(\pi)$ est exactement l'image inverse de $\mathcal{M}(\pi')$, la surjectivité de $A(\pi) \rightarrow A(\pi')$ que (e) tout élément de $\hat{\mathfrak{S}}(\pi'_0)$ est congru mod $\mathcal{M}(\pi'_0)$ à un élément de $\hat{\mathfrak{S}}(\pi_0)$ (c'est plus faible que (b)) – et ces conditions réunies impliquent que l'homomorphisme canonique

$$\mathcal{M}(\pi_0)/\hat{\mathfrak{S}}(\pi_0) = \Pi_{\pi_0} \rightarrow \Pi_{\pi'_0} = \mathcal{M}(\pi'_0)/\hat{\mathfrak{S}}(\pi'_0)$$

est un isomorphisme – il suffit même pour ceci d'avoir (c) (pour pouvoir définir cette application) et (a) (pour son injectivité), et (b) et le renforcement (d) de (c) (pour sa surjectivité). Donc on voit que tout est suspendu aux propriétés des homomorphismes d'inclusions de groupes:

$$(7) \quad \begin{array}{ccccc} \hat{\mathfrak{S}}^+(\pi_0) & \hookrightarrow & \mathcal{M}(\pi_0) & \hookrightarrow & \hat{\mathfrak{S}}(\pi_0) \\ \downarrow & & \downarrow ? & & \downarrow \\ \hat{\mathfrak{S}}^+(\pi'_0) & \hookrightarrow & \mathcal{M}(\pi'_0) & \hookrightarrow & \hat{\mathfrak{S}}(\pi'_0) \end{array}$$

à charge de prouver (a) et (b) (qui ne concernent que le carré composé) et (c).

Peut-être les propriétés (a), (b) et (c) sont-elles tout à fait fausses – pourtant (a) (qui correspond à l'injectivité de $P(\pi) \rightarrow P(\pi')$) semble assez plausible. La propriété (b) (qui exprimerait la surjectivité de $P(\pi) \rightarrow P(\pi')$) est beaucoup plus problématique, voir fausse. L'ennui, c'est que le groupe $\hat{\mathfrak{S}}(\pi_0)$ peut être “beaucoup plus petit” que $\hat{\mathfrak{S}}(\pi'_0)$, on s'en rend compte en passant au quotient par le sous-groupe $\hat{\pi}'_0 = \pi'$ (contenu dans le plus petit des groupes de (7), et invariant dans le plus grand), on trouve sur la deuxième ligne les groupes $\hat{\mathfrak{Z}}^+(\pi'_0)$, $\mathcal{N}(\pi'_0)$ et $\hat{\mathfrak{Z}}(\pi'_0)$, sur la première des extensions des groupes correspondants pour π_0 ($\hat{\mathfrak{Z}}^+(\pi_0)$, $\mathcal{N}(\pi_0)$ et $\hat{\mathfrak{Z}}(\pi_0)$) par le groupe fini $G = \pi_0/\pi'_0 \simeq \pi/\pi'$, notées par des $\tilde{}$, de sorte que l'on a:

$$(8) \quad \begin{array}{ccccccc} G & \hookrightarrow & \tilde{\mathfrak{Z}}^+(\pi_0) & \hookrightarrow & \tilde{\mathcal{N}}(\pi_0) & \hookrightarrow & \tilde{\mathfrak{Z}}(\pi_0) \\ & \searrow & \downarrow & & \downarrow ? & & \downarrow \\ & & \hat{\mathfrak{Z}}^+(\pi'_0) & \hookrightarrow & \mathcal{N}(\pi'_0) & \hookrightarrow & \hat{\mathfrak{Z}}(\pi'_0) \end{array}$$

A. GROTHENDIECK

qui montre que les groupes de la première ligne *normalisent* le sous-groupe $G \subset \hat{\mathfrak{Z}}^+(\pi'_0)$ (NB en fait on a $G \subset \mathfrak{Z}^+(\pi'_0)$, et π_0 se reconstitue à partir de π'_0 et de ce sous-groupe de π'_0) – on doit pouvoir montrer sans trop de mal que dans (8), $\hat{\mathfrak{Z}}^+(\pi_0)$ et $\hat{\mathfrak{Z}}(\pi_0)$ sont justement les normalisateurs de G dans $\hat{\mathfrak{Z}}^+(\pi'_0)$ et dans $\hat{\mathfrak{Z}}(\pi'_0)$ (ce qui impliquerait bien (a), d'ailleurs) – mais je ne vois aucune raison plausible que (b) soit vrai – ce qui signifierait, essentiellement, qu'il n'y a pas plus de “transcendance arithmétique” définie par le (“très gros”!) $\hat{\mathfrak{Z}}(\pi'_0) \pmod{\hat{\mathfrak{Z}}(\pi'_0)^+}$, que celle définie par le (“bien plus petit”) groupe $\hat{\mathfrak{Z}}(\pi_0) = \text{Norm}_{\hat{\mathfrak{Z}}(\pi_0)}(G)$... D'ailleurs ces conditions (a), (b) ne sont pas impératives pour que la conjecture fondamentale reliant les $\pi_{g,\nu}$ à Π_0 soit cohérente – par contre il faudrait absolument avoir (c) pour pouvoir au moins définir $A(\pi) \rightarrow A(\pi')$ et (si Σ, Σ' se correspondent) $\Pi_\Sigma \rightarrow \Pi_{\Sigma'}$, dans le cas π' caractéristique dans π (et dans tous les cas si on admet de plus (a), qui semble assez plausible, et donne les *injectivités* qu'il faut). Mais on se demande bien pourquoi un élément de $\hat{\mathfrak{Z}}(\pi'_0)$ simplement parce qu'il est dans le normalisateur R de G dans $\hat{\mathfrak{Z}}(\pi'_0)$, donc aussi R , et qu'il normalise $R \cap \hat{\mathfrak{Z}}^+(\pi'_0)$, devrait normaliser aussi $\hat{\mathfrak{Z}}^+(\pi'_0)$ lui-même! Il est vrai qu'on a fait des hypothèses draconiennes au départ (partant d'un sous-groupe *caractéristique* π'_0 de π_0) qui doivent bien se refléter par des propriétés particulières de $G \subset \mathfrak{Z}^+(\pi'_0)$. Peut-être finalement l'astuce de se ramener à des sous-groupes caractéristiques pour examiner la situation n'est-elle pas si astucieuse. Pour y voir plus clair, on pourrait déjà essayer de comprendre le cas où (sans suppose π' caractéristique), on suppose π' d'indice 2 dans π , donc invariant et $G \simeq \mathbb{Z}/2\mathbb{Z}$, ou bien on prend le noyau de l'homomorphisme canonique $\pi \rightarrow (\pi_{ab})_2 \simeq (\mathbb{Z}/2\mathbb{Z})^{2g}$ si $\nu = 0$, $\simeq (\mathbb{Z}/2\mathbb{Z})^{2g-\nu-1}$ si $\nu \geq 1$), en prenant par exemple $\pi = \hat{\pi}_{0,3}$ – situation de la courbe de Fermat $x^2 + y^2 + z^2 = 0$ (revêtement octaédral de $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$...)

Mais admettons provisoirement les hypothèses d'injectivité (relativement anodines), *plus* la condition (c), pas anodine du tout – d'où si Σ et Σ' se correspondent, un homomorphisme injectif

$$(9) \quad \Pi_\Sigma \hookrightarrow \Pi_{\Sigma'},$$

et voyons ce qu'on pourrait en tirer, en admettant même, provisoirement (pour voir) que (9) est un isomorphisme, c'est-à-dire toute la force de la conjecture principale $\Pi_0 \simeq \Pi_{g,\nu}$.

Soit π un groupe profini à lacets de type (g, ν) , π' de type (g', ν') . Appelons “corres-

pondance” entre π et π' un couple formé d’un \mathfrak{G} profini à lacets et d’homomorphismes à lacets $\mathfrak{G} \xrightarrow{p} \pi$, $\mathfrak{G} \xrightarrow{q} \pi'$ qui sont donc chacune composée d’un morphisme “bouchage de trous”, et d’un isomorphisme avec un sous-groupe d’indice fini. Soient $\mathcal{D}_p, \mathcal{D}_q \subset \mathcal{D} = I(\pi'')$ les sous-ensembles de \mathcal{D} qui correspondent aux “trous bouchés par p ” resp. par q , on suppose s’il le faut que $\mathcal{D}_p \cap \mathcal{D}_q = \emptyset$ (sinon on pourrait factoriser par un même quotient $\tilde{\pi}''$ de π''). En d’autres termes, si $\overline{\mathcal{D}}_p, \overline{\mathcal{D}}_q$ sont les complémentaires de $\mathcal{D}_p, \mathcal{D}_q$ dans \mathcal{D} (de sorte qu’on a $\overline{\mathcal{D}}_p \setminus I = I(\pi)$, $\overline{\mathcal{D}}_q \setminus I' = I(\pi')$), on a $\overline{\mathcal{D}}_p \cup \overline{\mathcal{D}}_q = \mathcal{D}$.

On va supposer maintenant π muni d’un $\Sigma \in A(\pi)$, π' muni d’un $\Sigma' \in A(\pi')$, on appellera “correspondance arithmétique” entre π et π' un quadruplet $(\mathfrak{G}, p, q, \Sigma_{\mathfrak{G}})$ où (\mathfrak{G}, p, q) sont comme dessus, et $\Sigma_{\mathfrak{G}} \in A(\mathfrak{G})$, tel que l’on ait $\Sigma_{\mathfrak{G}} = p^*(\Sigma) = q^*(\Sigma')$. Si $P_{\Sigma}, P_{\Sigma'}, P_{\Sigma_G}$ sont respectivement les toseurs sous $\Pi_{\Sigma}, \Pi_{\Sigma'}, \Pi_{\Sigma''}$ qu’on sait, on a deux diagrammes d’isomorphismes de toseurs:

$$\begin{array}{ccc} & P_{\Sigma_G} & \\ p^* \swarrow & & \searrow q^* \\ P_{\Sigma} & & P_{\Sigma'} \end{array} \quad \begin{array}{ccc} & \Pi_{\Sigma_G} & \\ p^* \swarrow & & \searrow q^* \\ \Pi_{\Sigma} & & \Pi_{\Sigma'} \end{array}$$

d’où par composition un isomorphisme

$$(P_{\Sigma}, \Pi_{\Sigma}) \xrightarrow{\sim} (P_{\Sigma'}, \Pi_{\Sigma'}).$$

On appelle “isomorphisme arithmétiquement extérieur” de (π, Σ) avec (π', Σ') , tout isomorphisme de toseurs qu’on peut obtenir de cette façon. Deux correspondances sont dites équivalentes du point de vue arithmétiquement extérieur, si elles définissent le même isomorphisme arithmétiquement extérieur. La composition est définie par composition des actions sur $(P_{\Sigma}, \Pi_{\Sigma})$ – on voit que ça provient d’une correspondance. On trouve donc un groupoïde, dont on vérifie sans peine qu’il est connexe.²⁵ Je dis que les automorphismes de (π, Σ) “sont” les automorphismes de $(P_{\Sigma}, \Pi_{\Sigma})$ définis par des éléments de Π_{Σ} . C’est facile...

Dans ce groupoïde, il y a un système transitif d’isomorphismes entre les $(\hat{\pi}_0, \Sigma_{\pi_0})$, où π_0 est un groupe discret à lacets) plus généralement entre les (π, Σ_{α}) , où $\alpha \in P(\pi)$ est un prédiscrétification de π – définissons donc un isomorphisme arithmétiquement extérieur de $\pi_{g,v}, \pi \dots$ Le groupe de ces automorphismes est noté Π_0 . Le groupoïde des courbes virtuelles

²⁵On l’appellera le groupoïde des courbes arithmétiques extérieures.

A. GROTHENDIECK

arithmétiques extérieures s'identifie donc à la catégorie des toiseurs sous Π_0 . Une prédiscretisation (on pourrait aussi l'appeler une rigidification arithmétiquement extérieure) n'est pas autre chose qu'un isomorphisme arithmétiquement extérieur entre cet élément de référence, et π .

§ 29. — CRITIQUE DE L'APPROCHE PRÉCÉDENTE

L'approche des paragraphes précédents semble finalement très brutale. J'ai même des doutes si la conjecture sur les propriétés du foncteur "bouchage de trous" est vraie telle quelle. Il est vrai que pour un groupe profini à lacets π , si on fixe $i \in I(\pi)$, on a un homomorphisme canonique

$$(1) \quad \hat{\mathfrak{Z}}(\pi, i) = \hat{\mathfrak{Z}}(\pi)_i \rightarrow \hat{\mathfrak{S}}(\pi'),$$

(où $\hat{\mathfrak{Z}}(\pi)_i$ est le stabilisateur de i dans $\hat{\mathfrak{Z}}(\pi)$), mais il est problématique si c'est un isomorphisme – et même si c'est injectif, ou si c'est surjectif. Mais, choisissant une discrétification $\pi_0 \subset \pi$, d'où itou π'_0 pour π' , l'homomorphisme précédent induit bel et bien un isomorphisme

$$(2) \quad \mathfrak{Z}(\pi_0)_i \simeq \mathfrak{S}(\pi'_0)$$

d'où

$$(3) \quad \hat{\mathfrak{Z}}(\pi_0) \xrightarrow{\sim} \hat{\mathfrak{S}}(\pi'_0)$$

et par suite, la suite exacte $1 \rightarrow \hat{\pi}'_0 \rightarrow \hat{\mathfrak{S}}(\pi'_0) \rightarrow \hat{\mathfrak{Z}}(\pi'_0) \rightarrow 1$ donne:

$$(4) \quad 1 \rightarrow \hat{\pi}'_0 \rightarrow \hat{\mathfrak{Z}}(\pi_0) \rightarrow \hat{\mathfrak{Z}}(\pi'_0) \rightarrow 1$$

et par suite on trouve un homomorphisme injectif

$$\hat{\pi}'_0 \rightarrow \hat{\mathfrak{Z}}(\pi_0)_i \hookrightarrow \hat{\mathfrak{Z}}(\pi_0)_i \simeq \hat{\mathfrak{Z}}(\pi)$$

A. GROTHENDIECK

(où $\hat{\pi}'_0 = \pi'$) donc un homomorphisme

$$(5) \quad i_{\pi_0} : \pi' \rightarrow \hat{\mathfrak{Z}}(\pi)_i$$

dont le composé avec (1) est l'injection canonique $\pi' \hookrightarrow \hat{\mathfrak{S}}(\pi')$. Remplaçant la discrétification π_0 par une autre, π_1 , on trouve a priori un autre homomorphisme $i_{\pi_1} : \pi' \rightarrow \hat{\mathfrak{Z}}(\pi)_i$. On peut supposer que $\pi_1 = u(\pi_0)$, $u \in \hat{\mathfrak{Z}}(\pi_0)_i$ et par transport de structure on trouve

$$i_{\pi_1} = i_{u(\pi_0)} = \text{Int}(u) \circ i_{\pi_0} \circ u_{\pi'}^{-1}$$

où $u_{\pi'}$ est l'automorphisme de π' défini par u via (1). Dire que i_{π_0} est indépendant du choix de la discrétification π_0 , revient aussi à dire que son image dans $\hat{\mathfrak{Z}}(\pi)_i$ est un sous-groupe invariant – et alors l'action de $\hat{\mathfrak{Z}}(\pi)_i$ sur le sous-groupe invariant $i_{\pi_0}(\pi) = i(\pi)$ via automorphismes intérieurs, n'est autre que celle définie par (1). Dans ce cas, on trouve par passage au quotient un homomorphisme

$$(6) \quad \hat{\mathfrak{Z}}(\pi)_i / \pi' \rightarrow \hat{\mathfrak{Z}}(\pi')$$

dont l'injectivité resp. surjectivité équivaudrait à celle de (1). Mais il n'est pas évident du tout qu'il en soit toujours ainsi.

S'il n'en était pas ainsi, il s'imposerait de regarder le sous-groupe de $\hat{\mathfrak{Z}}(\pi)_i$ formé des $\gamma \in \hat{\mathfrak{Z}}(\pi)_i$ qui normalisent le sous-groupe $i_{\pi_0}(\pi')$, et tels que l'action induite sur $i_{\pi_0}(\pi')$ corresponde à celle donnée par l'action (1) de $\hat{\mathfrak{Z}}(\pi)$ sur π' . Ce sous-groupe H_{π_0} (qui contient $\hat{\mathfrak{Z}}(\pi_0)_i$) dépend donc a priori de la discrétification choisie. Remplaçant π_0 par $u(\pi_0)$ (où $u \in \hat{\mathfrak{Z}}(\pi)_i$) le remplace par $\text{Int}(u) \cdot H$ – donc H tout au moins ne change pas, si on fait varier π_0 dans une classe de prédiscrétifications.

On peut faire des choix plus symétriques, en considérant *pour tout* $i \in I$ le quotient correspondant π'_i de π , d'où, pour une discrétification donnée π_0 , des homomorphismes

$$i_{\pi_0, i} : \pi'_i \rightarrow \hat{\mathfrak{Z}}(\pi)_i \subset \hat{\mathfrak{Z}}(\pi),$$

et on définit $H_{\pi_0} \subset \hat{\mathfrak{Z}}(\pi)$ comme le sous-groupe des $\gamma \in \hat{\mathfrak{Z}}(\pi)$ qui “permutent les $i_{\pi_0, i}$ entre eux” dans un sens évident. On a donc

$$(7) \quad H_{\pi_0} \cap \hat{\mathfrak{Z}}(\pi)_i = H_{\pi_0, i}$$

et

$$(8) \quad H \supset \hat{\mathfrak{Z}}(\pi_0).$$

Le point que j'ai en vue, c'est que le sous-groupe de $\hat{\mathfrak{Z}}(\pi_0)$ image de $\pi_1(M_{g,\nu})$, doit non seulement normaliser $\hat{\mathfrak{Z}}(\pi_0)^+$, mais de plus être contenu dans un H . C'est là une condition que j'ai rencontrée par la bande, à la faveur de l'hypothèse (peut-être bien hâtive) que (1) est un isomorphisme, qui impliquait (facilement) que l'on avait $H = \hat{\mathfrak{Z}}(\pi_0)$ tout entier. Il est possible que $\hat{\mathfrak{Z}}(\pi_0)$ soit un groupe à tel point démesuré et pathologique, qu'il ne pourra jamais être question de dire des choses raisonnables (et vraies) sur le groupe tout entier, (tel que la bijectivité de (1) par exemple) et qu'on soit obligé de travailler avec des sous-groupes plus petits, qui restent proches du discret (avec quand-même des aspects supplémentaires "arithmétiques", dû au $\Pi_0 = \text{Gal}(\overline{\mathbb{Q}_0}/\mathbb{Q})!$). En fait, il y a (pour $I = I(\pi) \neq \emptyset$, i.e. $\nu \neq 0$) dans le groupe $\hat{\mathfrak{Z}}(\pi_0)$ une structure simpliciale d'extensions successives, qui va être respectée par l'action extérieure du groupe de Galois, et dont il faudrait tenir compte. Elle fait partie de la "structure à l' ∞ " dans le π_1 des multiplicités modulaires $M_{g,\nu}$, qui même pour $\nu = 0$ est sans doute non triviale, et il est possible qu'il faille en tenir compte, pour arriver à mettre le doigt sur $\Pi_{\mathbb{Q}}$.

Sans essayer de donner d'emblée une description a priori de $\Pi_{\mathbb{Q}}$ "dans les $\hat{\mathfrak{Z}}_{g,\nu}$ ", on va procéder de façon plus inductive, en partant de la présence de $\Pi_{\mathbb{Q}}$ (pour des raisons arithmético-géométriques), et en essayant de dégager des propriétés de cette présence peut-être assez fortes pour finir par donner une caractérisation purement algébrique. Rappelons que, via le choix de $\mathcal{U}_{g,\nu}$ (différentiable), on avait pu construire, par voie transcendante, un $\widetilde{M_{g,\nu,\mathbb{C}}}$ et un $\widetilde{\mathcal{U}_{g,\nu,\mathbb{C}}} = \widetilde{M_{g,\nu+,\mathbb{C}}}$, d'où un $\widetilde{M_{g,\nu,\mathbb{Q}}}$, et un $\widetilde{\mathcal{U}_{g,\nu,\mathbb{Q}}}$, d'où un $\pi_1(\mathcal{U}_{g,\nu,\mathbb{Q}})$, avec une filtration en trois crans, dont les facteurs sont respectivement canoniquement isomorphes à

$$(9) \quad \hat{\pi}_{g,\nu}, \hat{\mathfrak{Z}}(\pi_{g,\nu})^+, \Pi_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}_0}/\mathbb{Q}).$$

Ce groupe s'envoie (on présume injectivement) dans $\hat{\mathfrak{S}}(\pi_{g,\nu})$, induisant un isomorphisme entre son sous-groupe $\pi_1(\mathcal{U}_{g,\nu,\overline{\mathbb{Q}_0}})$ et $\hat{\mathfrak{S}}(\pi_{g,\nu})$; désignons son image par $\mathcal{M}_{g,\nu}$. Donc c'est un sous-groupe fermé

$$(10) \quad \hat{\mathfrak{S}}_{g,\nu} \subset \mathcal{M}_{g,\nu} \subset \hat{\mathfrak{S}}_{g,\nu}$$

A. GROTHENDIECK

et $\hat{\mathfrak{S}}_{g,\nu}^+$ est normal dans $\mathcal{M}_{g,\nu}$ (mais pas $\hat{\mathfrak{S}}_{g,\nu}$!), La donnée d'un tel $\mathcal{M}_{g,\nu}$ équivaut à celle d'un $\mathcal{N}_{g,\nu}$

$$(11) \quad \hat{\mathfrak{Z}}_{g,\nu} \subset \mathcal{N}_{g,\nu} \subset \hat{\mathfrak{Z}}_{g,\nu}^+,$$

avec $\hat{\mathfrak{Z}}_{g,\nu}^+$ normal dans $\mathcal{N}_{g,\nu}$. On pose:

$$(12) \quad \Pi_{g,\nu} = \mathcal{N}_{g,\nu} / \hat{\mathfrak{Z}}_{g,\nu}^+ \simeq \mathcal{M}_{g,\nu} / \hat{\mathfrak{S}}_{g,\nu}^+.^{26}$$

On a un homomorphisme surjectif

$$(13) \quad \Pi_{\mathbb{Q}} \rightarrow \Pi_{g,\nu}$$

dont on présume qu'il est bijectif – i.e. que les $\Pi_{g,\nu}$ sont canoniquement isomorphes entre eux.

Soit maintenant π_0 un groupe discret à lacets de type g, ν , alors on définit des sous-groupes $\mathcal{M}_{\pi_0}, \mathcal{N}_{\pi_0}$:

$$(14) \quad \hat{\mathfrak{S}}(\pi_0) \subset \mathcal{M}_{\pi_0} \subset \hat{\mathfrak{S}}^+(\pi_0)$$

$$(15) \quad \hat{\mathfrak{Z}}(\pi_0) \subset \mathcal{N}_{\pi_0} = \mathcal{M}_{\pi_0} / \hat{\pi}_0 \subset \hat{\mathfrak{Z}}^+(\pi_0)$$

(et on pose $\Pi_{\pi_0} = \mathcal{M}_{\pi_0} / \hat{\mathfrak{S}}(\pi_0)$), en utilisant un isomorphisme $\pi_0 \xrightarrow{\sim} \pi_{g,\nu}$ et en procédant par transport de structure – le résultat n'en dépend pas. Plus généralement, partons d'un couple (π, α) d'un groupe π profini, muni d'une *prédiscretisation* α , qu'on peut donc interpréter comme une classe d'isomorphismes $\hat{\pi}_{g,\nu} \rightarrow \pi$, définie modulo composition à droite par un $u \in \hat{\mathfrak{S}}_{g,\nu}$. Alors par transport de structure on en déduit des groupes $\mathcal{M}_{\alpha}, \mathcal{N}_{\alpha}$

$$(16) \quad \hat{\mathfrak{S}}_{\alpha} \subset \mathcal{M}_{\alpha} \subset \hat{\mathfrak{S}}^+(\pi)$$

$$(17) \quad \hat{\mathfrak{Z}}_{\alpha} \subset \mathcal{N}_{\alpha} = \mathcal{M}_{\alpha} / \pi \subset \hat{\mathfrak{Z}}^+(\pi)$$

²⁶Dans $\Pi_{g,\nu}$, on a un élément canonique d'ordre 2 $\tau_{g,\nu}$, correspondant aux éléments de $\hat{\mathfrak{Z}}_{g,\nu} \setminus \hat{\mathfrak{Z}}_{g,\nu}^+ = \hat{\mathfrak{Z}}_{g,\nu}^-$.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

avec $\hat{\mathfrak{S}}(\pi)^+$ normal dans \mathcal{M}_α , i.e. $\hat{\mathfrak{Z}}^+(\pi)$ normal dans \mathcal{N}_α . On pose

$$(18) \quad \Gamma_\alpha = \mathcal{M}_\alpha / \hat{\mathfrak{S}}_\alpha^+ \simeq \mathcal{N}_\alpha / \hat{\mathfrak{Z}}_\alpha^+.$$

On a un élément canonique

$$(19) \quad \tau_\alpha \in \Gamma_\alpha, \quad \tau_\alpha^2 = 1, \quad \tau_\alpha \neq 1.$$

Soit maintenant π un groupe profini à lacets de type (g, ν) . On appelle *arithmétisation* de π la donnée d'un élément de

$$(20) \quad A(\pi) = \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \mathcal{M}_{g,\nu} \simeq \text{Isomext}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \mathcal{N}_{g,\nu}.$$

Soit $P(\pi)$ l'ensemble des prédiscretifications orientées de π :

$$(21) \quad P(\pi) = \text{Isom}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \hat{\mathfrak{S}}_{g,\nu}^+ \simeq \text{Isomext}_{\text{lac}}(\hat{\pi}_{g,\nu}, \pi) / \hat{\mathfrak{Z}}_{g,\nu}^+;$$

alors $\Gamma_{g,\nu}$ opère librement à droite sur $P(\pi)$, et

$$(22) \quad A(\pi) \simeq P(\pi) / \Gamma_{g,\nu}$$

– $P(\pi)$ est un toreur relatif sur $A(\pi)$, de groupe $\Gamma_{g,\nu}$. Pour $a \in A(\pi)$, soit \mathcal{M}_a le sous-groupe de $\hat{\mathfrak{S}}(\pi)$ des automorphismes de (π, a) , il opère sur le $\Gamma_{g,\nu}$ -torseur P_a des discretifications orientées de π sur a . Pour $\alpha \in P_a$, soit $\hat{\mathfrak{S}}_\alpha \subset \hat{\mathfrak{S}}(\pi)$; alors $\hat{\mathfrak{S}}_\alpha^+$ ne dépend pas de α (on le notera $\hat{\mathfrak{S}}_a^+$);²⁷ c'est aussi le noyau de l'opération de \mathcal{M}_a sur P_a . On a

$$(23) \quad \hat{\mathfrak{S}}_a^+ \subset \mathcal{M}_a \subset \hat{\mathfrak{S}}(\pi)$$

d'où encore

$$(24) \quad \hat{\mathfrak{Z}}_a^+ \subset \mathcal{N}_a \subset \hat{\mathfrak{Z}}(\pi)$$

en posant

$$(25) \quad \mathcal{N}_a = \mathcal{M}_a / \pi, \quad \hat{\mathfrak{Z}}_a^+ = \hat{\mathfrak{S}}_a^+ / \pi.$$

²⁷ mais attention, $\hat{\mathfrak{S}}_\alpha$ dépend de α , i.e. $\tau_\alpha \in \Gamma_a$ dépend de α .

A. GROTHENDIECK

On pose

$$(26) \quad \Pi_a = \mathcal{M}_a / \hat{\mathfrak{S}}_a^+ \simeq \mathcal{N}_a / \hat{\mathfrak{Z}}_a^+.$$

Alors Π_a s'identifie au commutant de $\Pi_{g,\nu}$ opérant sur P_a , i.e. à $\Pi_{g,\nu}$ “tordu” par le torseur P_a . Le choix d'un $\alpha \in P_a$ revient donc au choix d'un tel isomorphisme

$$(27) \quad \Pi_a \simeq \Pi_{g,\nu}$$

qui est changé par automorphisme intérieur si on change α ...

On a la catégorie des groupes à lacets extérieurs arithmétisés de type g, ν – c'est un groupoïde connexe, avec une origine fixée ($\hat{\pi}_{g,\nu}, a_{g,\nu}$) ($a_{g,\nu}$ arithmétisation “canonique”), dont le groupe des automorphismes est $\mathcal{N}_{g,\nu}$, extension de $\Pi_{g,\nu}$ par $\hat{\mathfrak{Z}}_{g,\nu}^+ \simeq \pi_1(M_{g,\nu,\mathbb{Q}})$ (si $\Pi_{\mathbb{Q}} \rightarrow \Pi_{g,\nu}$ est injectif!) (calculé par rapport au revêtement universel canonique de $M_{g,\nu,\mathbb{Q}}$)...

Se donner un objet de cette catégorie, c'est essentiellement la même chose (à isomorphisme unique près) que de se donner un revêtement universel $\widetilde{M_{g,\nu,\mathbb{Q}}}$ de $M_{g,\nu,\mathbb{Q}}$ – ou un torseur sous $\mathcal{N}_{g,\nu}$; on considère alors la famille de courbes de type g, ν sur $\widetilde{M_{g,\nu,\mathbb{Q}}}$

$$(28) \quad \mathcal{U}_{g,\nu} \times_{M_{g,\nu}} \widetilde{M_{g,\nu,\mathbb{Q}}} = \mathcal{U}_{g,\nu}(\widetilde{M_{g,\nu,\mathbb{Q}}})$$

comme étant “la” courbe algébrique dont le π_1 extérieur (qui est donc le π_1 de ce schéma...) soit le groupe extérieur à lacets donné.

Si on prenait les groupes à lacets arithmétisés, pas extérieurs, on aurait encore un groupoïde connexe avec “origine” ($\hat{\pi}_{g,\nu}, a_{g,\nu}$), avec un groupe d'automorphismes qui est $\mathcal{M}_{g,\nu} \simeq \pi_1(\mathcal{U}_{g,\nu,\mathbb{Q}})$. La donnée d'un objet de cette catégorie revient à la donnée d'un revêtement universel (non seulement de $M_{g,\nu,\mathbb{Q}}$, mais) de $\mathcal{U}_{g,\nu,\mathbb{Q}}$, soit $\widetilde{\mathcal{U}_{g,\nu,\mathbb{Q}}}$, qui sert de revêtement universel de référence pour la courbe relative (28), permettant alors de préciser son groupe fondamental comme un vrai groupe à lacets (pas seulement un groupe extérieur).

On peut enfin regarder aussi la catégorie des groupes profinis à lacets arithmétisés, où on prend comme morphismes les *isomorphismes arithmétiquement extérieurs*. On trouve encore un groupoïde connexe avec origine marquée ($\hat{\pi}_{g,\nu}, a_{g,\nu}$), dont le groupe des automorphismes est maintenant $\Pi_{g,\nu}$. Maintenant les groupes $\hat{\pi}_0$ (π_0 groupe à lacets discret de type g, ν) sont canoniquement isomorphe entre eux. La catégorie est (conjecturalement, admettant que

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

$\Pi_{\mathbb{Q}} \rightarrow \Pi_{g,v}$, soit un isomorphisme) équivalente à celle des revêtement universels de $\text{Spec } \mathbb{Q}$, i.e. à celle des clôtures algébriques de \mathbb{Q} , l'élément origine correspondant à $\overline{\mathbb{Q}}_0$.

Quand on se donne un π avec arithmétisation a , alors il lui correspond donc canoniquement une clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} . Le $\Pi_{\mathbb{Q}}$ -torseur des isomorphismes $\text{Isom}(\overline{\mathbb{Q}}_0, \overline{\mathbb{Q}})$, i.e. des plongements $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, est en correspondance 1-1 avec l'une (P_a) des prédiscrétifications orientées de π donnant naissance à a .

Notons que tout α définit un élément $\tau_{\alpha} \in \Pi_a$, $\tau_{\alpha}^2 = 1$ ($\tau_{\alpha} \neq 1$), d'où une application canonique

$$(29) \quad P_a \rightarrow {}_2\Pi_a.$$

On voit que cette application est compatible avec l'action du groupe ± 1 sur P_a ,

$$\tau_{\alpha} = \tau_{-\alpha}.$$

S'il est vrai que $\Pi_{\mathbb{Q}} \xrightarrow{\sim} \Pi_{g,v}$, alors (29) induit par passage au quotient une application bijective

$$(30) \quad P_a / \pm 1 \xrightarrow{\sim} \text{ensemble des éléments d'ordre 2 de } \Pi_a$$

(où $P_a / \pm 1 = P_a^{\natural} =$ ensemble des prédiscrétifications – pas orientées – sur a).

Cela provient du fait connu que dans $\Pi_{\mathbb{Q}}$, les seuls éléments d'ordre 2 sont les conjugués de τ , et que le centralisateur de τ dans $\Pi_{\mathbb{Q}}$ est réduit à $\{1, \tau\}$. On peut dire que la donnée d'une discrétification (pas orientée) α^{\natural} sous l'arithmétisation a , revient à la donnée d'une valuation archimédienne sur la clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} définie par (π, a) (i.e. d'un isomorphisme $\overline{\mathbb{Q}}_1 \simeq \overline{\mathbb{Q}}_0$ modulo conjugaison complexe).

§ 30. — PROPRIÉTÉS DES $\mathcal{N}_{g,\nu}$, $\Pi_{g,\nu}$

a) Propriétés liées aux sous-groupes finis

On aimerait dégager des propriétés, inspirées par le contexte géométrico-arithmétique, mais qui puissent se formuler de façon purement algébrique – et qui soient assez fortes peut-être pour finir par caractériser les $\mathcal{N}_{g,\nu}$.

Revenons à un (π, a) , groupe à lacets arithmétisé, heuristiquement, il correspond à la donnée d’une clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} , et (si π est donné extérieurement) d’une famille algébrique, paramétrée par un revêtement universel $\widetilde{M_{g,\nu,\overline{\mathbb{Q}}}}$ de $M_{g,\nu,\overline{\mathbb{Q}}}$, de courbes algébriques de type (g, ν) . Dans cette optique, réduire cette famille à *une* courbe algébrique – i.e. se donner une courbe algébrique de type (g, ν) sur $\overline{\mathbb{Q}}$ – doit revenir à se donner un noyau de relèvement de l’homomorphisme surjectif

$$(1) \quad \mathcal{N}_a \rightarrow \Pi_a$$

(de noyau $\hat{\mathfrak{X}}_a^+$). La donnée d’un tel relèvement sur un sous-groupe ouvert Γ' revient à la donnée d’une courbe algébrique de type g, ν , définie sur l’extension finie $K' \subset \overline{\mathbb{Q}}$ définie par Γ' . Il s’agit ici non pas de relèvements continus quelconques, mais de relèvements ayant des propriétés particulières (dont certaines fort profondes, du genre “Weil”... mais *peut-être* conséquences de propriétés beaucoup plus simples). Les propriétés à dégager devraient en tout cas être stables par passage à un sous-groupe ouvert plus petit. Parmi ces propriétés, il y aurait que ces germes de relèvements pourraient à leur tour se remonter à $\hat{\mathfrak{E}}(\pi)$ lui-même – de façon également “admissible” en un sens à préciser – et même qu’il y aurait “beaucoup”

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

de classes de π -conjugaison de tels germes de relèvements, pour un germe d'action extérieure sur π déjà donné – ce qui correspond au fait naïf que la courbe algébrique \mathcal{U} sur $\overline{\mathbb{Q}}$ définie par cette action extérieure a “beaucoup de points” rationnels sur $\overline{\mathbb{Q}}$. En fait, il suffirait, à la limite, de parler des propriétés de ces relèvements plus complets en un germe d'une vraie action de Π_a sur π (pas seulement extérieure) – dont les actions extérieures vont se déduire par composition avec

$$\mathcal{M}_a \rightarrow \mathcal{N}_a \simeq \mathcal{M}_a / \pi.$$

On suppose donc donné un sous-groupe fermé

$$\Gamma \subset \mathcal{M}_a \subset \hat{\mathfrak{S}}(\pi)$$

tel que

$$(a) \quad \Gamma \rightarrow \Pi_a = \mathcal{M}_a / \pi$$

est injectif, et a comme image un sous-groupe ouvert de Π_a – étant entendu que deux sous-groupes conjugués sous π – voire même parfois, sous \mathcal{M}_a – ne sont pas considérés comme essentiellement distincts. On considère, en même temps que Γ , ses sous-groupes ouverts Γ' . On veut surement, pour de tels sous-groupes ouverts

$$(b) \quad \pi^{\Gamma'} = \{1\}.$$

Si on désigne par $\tilde{\Gamma}$ l'image de Γ dans \mathcal{N}_a , de sorte qu'on a une extension

$$(1') \quad 1 \rightarrow \pi \rightarrow \mathcal{E} \rightarrow \tilde{\Gamma} \rightarrow 1$$

(où $\tilde{\Gamma}$ est isomorphe à Γ); on peut considérer Γ comme une section de cette extension, Γ' comme une section partielle. L'hypothèse $\pi^{\Gamma'} = \{1\}$ assure la *rigidité* de la catégorie des points de \mathcal{U} à valeurs dans $\overline{\mathbb{Q}}$, paradigée par celle des germes de scindage de l'extension (1').

On peut aussi regarder les ensembles $(\hat{\mathfrak{S}}_a^+)^{\Gamma'} = \text{Centr}_{\mathcal{M}_a}(\Gamma') \cap \hat{\mathfrak{S}}_a^+$ et $(\hat{\mathfrak{Z}}_a^+)^{\Gamma'} = \text{Centr}_{\mathcal{N}_a}(\tilde{\Gamma}') \cap \hat{\mathfrak{Z}}_a^+$; on a donc une suite exacte

$$(2) \quad 1 \rightarrow \pi^{\Gamma'} \rightarrow (\hat{\mathfrak{S}}_a^+)^{\Gamma'} \rightarrow (\hat{\mathfrak{Z}}_a^+)^{\Gamma'}$$

A. GROTHENDIECK

qui, compte tenu de l'hypothèse $\pi^{\Gamma'} = \{1\}$, donne

$$(3) \quad (\hat{\mathfrak{S}}_a^+)^{\Gamma'} \hookrightarrow (\hat{\mathfrak{Z}}_a^+)^{\Gamma'}.$$

Le deuxième membre de (3), par notre dictionnaire hypothétique, devrait être canoniquement isomorphe au groupe des automorphismes de la courbe \mathcal{U} sur K' , donc être un groupe fini, et même la limite inductive (pour Γ' décroissant) – qui est le groupe des automorphismes de \mathcal{U} sur $\overline{\mathbb{Q}}$ – est finie. Désignant par un exposant \natural le germe de groupe correspondant, on veut donc que

$$(c) \quad Z = (\hat{\mathfrak{Z}}_a^+)^{\Gamma^\natural} (= \text{Centr}_{\mathcal{N}_a}(\tilde{\Gamma}^\natural) \cap \hat{\mathfrak{Z}}_a^+) \text{ soit un groupe fini}$$

– ce qui fait pendant à (b), et exprime que les groupes d'automorphismes des points de $\mathcal{M}_{g,v,\overline{\mathbb{Q}}}$ sur $\overline{\mathbb{Q}}$ sont finis.

En fait, on voudrait que Z soit conjugué dans \mathcal{M}_a à un sous-groupe de \mathfrak{Z}^+ (si on suppose qu'on dispose d'une discrétification π_0 de π , permettant de définir \mathfrak{Z} – sinon, on peut exprimer cette propriété en disant qu'il existe une discrétification π_0 de π , compatible avec a , telle que $Z \subset \mathfrak{Z}(\pi_0) \dots$)

Considérons maintenant un sous-groupe fini quelconque $G \subset \hat{\mathfrak{Z}}_a^+$. [N.B. si on prend seulement $G \subset \mathcal{M}_a$, de sorte que l'image de G dans $\Pi_a = \mathcal{M}_a / \hat{\mathfrak{Z}}_a^+$ est un sous-groupe fini, alors s'il est vrai que $\Pi_a \simeq \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, cette image doit être d'ordre 1 ou 2, et dans le deuxième cas, doit définir un $\tau \in \Pi_a$ correspondant à une *prédiscrétification* (pas orientée) bien déterminée de π . Ce cas devrait être encore réutilisée dans la suite...] Supposons alors que [ce n'est sans doute *pas* automatique – si on ne suppose *pas* $\mathcal{N}_a = \text{Norm}_{\hat{\mathfrak{Z}}}(\hat{\mathfrak{Z}}_a^+)$], que G est contenu dans \mathfrak{Z}^+ , pour une discrétification convenable dans la classe a , et que l'action extérieure ainsi obtenue de G sur un π_0 discret de type (g, ν) soit toujours *réalisable*. Elle est donc réalisable aussi pour une action de G sur une structure complexe, donc algébrique, ce qui signifie qu'on peut trouver un germe de relèvement *admissible*

$$\Pi_a \rightarrow \mathcal{N}_a$$

qui centralise G . Considérons d'autre part

$$(4) \quad \text{Centr}_{\mathcal{N}_a}(G) \rightarrow \Pi_a$$

dont le noyau est $\text{Centr}_{\hat{\mathfrak{Z}}_a^+}(G) = \hat{\mathfrak{Z}}_a^{+G}$. Si on se plaçait dans le contexte discret (avec une discrétification $\pi_0 \subset \pi$ invariante par G) on aurait, par les conjectures standard topologiques, que $\hat{\mathfrak{Z}}_a^{+G}$ est le groupe des automorphismes, dans la catégorie isotopique, de l'action de G sur une surface \mathcal{U} de type (g, ν) , décrite par l'opération extérieure donnée de G sur π_0 . Ce groupe n'a aucune raison d'être fini – s'il l'était, l'homomorphisme (4) serait à noyau fini, donc serait un isomorphisme des noyaux des groupes, et il y aurait un germe de relèvement unique $\Pi_a^{\text{h}} \rightarrow \mathcal{M}_a$ qui centraliserait G – ce qui signifierait qu'il y a une seule façon de réaliser l'opération topologique de G sur \mathcal{U} par une opération analytique complexe, donc algébrique – or ce n'est surement pas le cas, l'ensemble des points fixes de G opérant sur l'espace de Teichmüller $\widetilde{M}_{g,\nu}$ n'est pas réduit à un point – c'est (dans le contexte algébrique) une multiplicité schématique qui peut être de dimension quelconque – elle est de dimension > 0 en tout cas, si le quotient \mathcal{U}/G n'est pas de genre 0.

A retenir en tout cas, comme propriétés plausibles:

(d) Pour tout sous-groupe fini G de $\hat{\mathfrak{Z}}_a^+$ (ou du moins si $G \subset \mathfrak{Z}^+$, quand on dispose d'une discrétification $\pi_0 \subset \pi$ dans a), regardant $\text{Centr}_{\hat{\mathfrak{Z}}}(G) = Z(G)$, $\mathcal{N}_a \cap Z(G) \rightarrow \Pi_a$ a une image ouverte (et il y a même des germes de relèvements admissibles $\Pi_a \rightarrow Z(G)$).

Ceci implique une propriété non triviale pour les $g \in \mathcal{M}_a$ en tant qu'éléments de $\hat{\mathfrak{Z}}(\pi)$, ou mieux de $\mathcal{N}' = \text{Norm}_{\hat{\mathfrak{Z}}}(\hat{\mathfrak{Z}})$ [à savoir: $\exists n \in \mathbb{N}^*$ tel que g^n soit congru mod $\hat{\mathfrak{Z}}_a^+$ à un élément de $Z(G)$...]. Considérons en effet l'image Z'_G de $Z(G) \cap \mathcal{N}'$ dans $\Gamma' = \mathcal{N}'/\hat{\mathfrak{Z}}$. On a évidemment $\Pi_a \subset \Gamma'$, et l'image de $Z(G) \cap \mathcal{N}_a$ dans Π_a n'est autre que $Z'_G \cap \Pi_a$. Dire que celle-ci est ouverte, i.e. d'indice fini, implique donc que $\forall g \in \Pi_a, \exists n \in \mathbb{N}^*$ tel que $g^n \in Z'_G$.

Notons que dans $\mathfrak{Z}(\pi_{g,\nu})$ il n'y a qu'un nombre fini de classes de conjugaison de sous-groupes finis, donc si on regarde leurs centralisateurs Z_G dans $\hat{\mathfrak{Z}}(\pi_{g,\nu})$ et leurs images dans

$$\Gamma'_{g,\nu} = \text{Norm}_{\hat{\mathfrak{Z}}_{g,\nu}}(\hat{\mathfrak{Z}}_{g,\nu}^+)/\hat{\mathfrak{Z}}_{g,\nu}^+,$$

on ne trouve qu'un nombre fini de sous-groupes de $\Gamma'_{g,\nu}$, soit $Z'_{g,\nu}$ leur intersection. On voit donc que le sous-groupe $\Pi'_{g,\nu}$ de $\Gamma'_{g,\nu}$ est tel que $\Pi'_{g,\nu} \cap Z'_{g,\nu}$ soit ouvert dans $\Pi'_{g,\nu}$.

Passons maintenant à des sous-groupes finis de $\hat{\mathfrak{E}}(\pi)$ lui-même – ou du moins de \mathcal{M}_a – ou, ce qui revient presque au même, de $\hat{\mathfrak{E}}_a^+$. On va, comme tantôt, se borner à des $G \subset \mathfrak{E}(\pi_0)$, pour une discrétification convenable $\in a$, car autrement il n'y aurait rien à dire. On

A. GROTHENDIECK

sait qu'alors G est cyclique – et correspond à une action de G sur un \mathcal{U} topologique, *avec point fixe*. On peut la réaliser de façon complexe, ce qu'on exprime en disant qu'il existe un relèvement admissible $\Pi_a^{\natural} \rightarrow \mathcal{M}_a$, qui centralise G . On sait d'ailleurs, si $G \neq 1$, que

$$(5) \quad \pi^G = \{1\}$$

(ou plutôt, on le sait dans le cas discret – on l'admet dans le contexte profini) – ce qu'on peut encore interpréter comme une propriété de rigidité – ainsi

$$\text{Centr}_{\hat{\mathfrak{E}}}(G) = \hat{\mathfrak{E}}^G \rightarrow \hat{\mathfrak{Z}}^G$$

est *injectif*, donc si on a $\Gamma \subset \mathcal{N}_a$ qui est dans l'image, alors il existe un relèvement $\Gamma \rightarrow \hat{\mathfrak{E}}$ unique qui centralise G , i.e. tel que $\Gamma \rightarrow \hat{\mathfrak{E}}^G$. Mais en fait ce qu'on saura, pour un $\Gamma \subset \mathcal{M}_a$ donné (décrivant une courbe algébrique via son action extérieure sur un π_1) c'est que $\Gamma \subset \mathcal{M}_a^G$ (i.e. l'action extérieure commute à une action extérieure donnée de G , i.e. G opère sur la courbe algébrique) – et on voudrait néanmoins en conclure que lorsqu'on a relevé $G \rightarrow \hat{\mathfrak{Z}}^+$ ou $G \rightarrow \hat{\mathfrak{E}}^+$ (i.e. quand on s'est donné un point fixe de l'action de G sur \mathcal{U}) alors l'action de Γ^{\natural} se remonte automatiquement en $\Gamma^{\natural} \rightarrow \mathcal{M}_a$ de façon à commuter.....(i.e. $\Gamma^{\natural} \rightarrow \mathcal{M}_a^G$). Est-ce là une propriété du choix de \mathcal{M}_a ou de celui du relèvement $\Gamma^{\natural} \rightarrow \mathcal{N}_a$, ou de G ??

Dans le cadre discret, sauf erreur, si on a une action fidèle discrète de G fini sur π_0 , alors $\mathfrak{E}(\pi_0)^G \rightarrow \mathfrak{Z}(\pi_0)^G$ (qui est injectif, par $\pi_0^G = 1$) est aussi surjectif. Non, il y a erreur – ça signifierait tel quel que si G opère fidèlement sur une surface topologique \mathcal{U} de type g, ν , avec un point fixe P , alors les automorphismes qui commutent à G *fixent* P (au lieu de permuter seulement les points fixes entre deux...). Donc il ne faut *pas* s'attendre à ce que tout tout élément dans \mathcal{N}_a^G , ni même dans $\hat{\mathfrak{Z}}_a^G$, se remonte à \mathcal{M}_a^G – mais plutôt ceci: pour un $G \subset \mathfrak{Z}_a(\pi_0)$ sous-groupe fini donné, les classes de π -conjugaison de “remontages” à $\hat{\mathfrak{E}}$, qui s'interprètent comme des points fixes d'une action de G sur quelque \mathcal{U} , forment un ensemble fini, sur lequel $\hat{\mathfrak{Z}}(\pi)^G$ opère de façon naturelle, et le stabilisateur d'un point P i.e. d'une classe de conjugaison de relèvements se remonte de façon unique en $\hat{\mathfrak{E}}^G$. Il faudrait réexaminer ceci de façon plus soignée par la suite. Mais il me semble qu'on ne trouve pas ici de nouvelles propriétés des $\Gamma \subset \mathcal{M}_a$ ni de \mathcal{M}_a lui-même, i.e. de Π_a comme sous-groupe profini de $\Gamma' = \text{Norm}_{\hat{\mathfrak{Z}}}(\hat{\mathfrak{Z}})/\hat{\mathfrak{Z}}$.

§ 31. — DIGRESSION SUR LES RELÈVEMENTS D'UNE ACTION EXTÉRIEURE D'UN GROUPE FINI

G sur un groupe profini à lacets π

On suppose l'action extérieure *fidèle*, i.e. $G \subset \hat{\mathfrak{Z}}(\pi) = \hat{\mathfrak{Z}}$, et que $G = G^+$. On suppose de plus qu'il existe une discrétification invariante π_0 , i.e. telle que $G \subset \mathfrak{Z}(\pi_0)$. Si on suppose G cyclique, alors sauf erreur il est prouvé que la situation est *réalisable* topologiquement (donc aussi de façon analytique complexe...)

Dans le cas discret, la signification des classes de π_0 conjugaison de relèvement $G \rightarrow \mathfrak{S}(\pi_0)$ est bien comprise, de même que pour les relèvements partiels. On trouve une réalisation canonique [si $\mathcal{U}^! \neq \emptyset$] du groupoïde fondamental associé au groupe extérieur π_0 , par un groupoïde fini $[\mathcal{U}^!]$ sur lequel G opère au sens strict, dont les points correspondent aux classes de π_0 -conjugaison de sections partielles $\neq 1$ maximales. Le groupe $\mathfrak{Z}(\pi_0)^G$ opère de façon également canonique sur ce groupoïde. Si $P \in \mathcal{U}^!$ correspond à un relèvement $G \rightarrow \mathfrak{S}(\pi_0)$, alors un élément $\dot{u} \in \mathfrak{Z}(\pi_0)^G$ est dans l'image de $\mathfrak{S}(\pi_0)^G$, i.e. peut se remonter en $u \in \mathfrak{S}(\pi_0)$ commutant à G , si et seulement si $\dot{u}(P) = P$, i.e. (si \dot{u} est remonté de façon quelconque en v), si et seulement si $v(G)$ est π_0 -conjugué à G , i.e. si et seulement s'il existe $g \in \pi_0$ tel que $v(G) = \text{int}(g)(G)$, i.e. $u \stackrel{\text{def}}{=} \text{int}(g^{-1})v$ fixe G (auquel cas bien sûr il centralise, par l'hypothèse $\dot{u} \in \mathfrak{Z}^G$). Donc notre brillante assertion est une tautologie, et donc le relèvement est unique. Comme $\mathcal{U}^!$ est fini, le stabilisateur $\mathfrak{Z}(\pi_0)_P^G$ de P dans $\mathfrak{Z}(\pi_0)^G$ est d'indice fini, et c'est donc ce sous-groupe d'indice fini qui se remonte gaillardement et canoniquement.

Que peut-on dire dans le contexte profini? Bien sûr, on a une application canonique

A. GROTHENDIECK

classes de π_0 -conjugaison		classes de π_0 -conjugaison
de relèvements de		des relèvements de
G en $G \rightarrow \mathfrak{S}(\pi_0)$	\longrightarrow	G en $G \rightarrow \hat{\mathfrak{S}}(\pi_0),$
i.e. de scindage de l'extension		i.e. de scindage de l'extension
$1 \rightarrow \pi_0 \rightarrow \mathcal{E} \rightarrow G \rightarrow 1$		$1 \rightarrow \hat{\pi}_0 = \pi \rightarrow \hat{\mathcal{E}} \rightarrow G \rightarrow 1.$

Il faudrait examiner d'abord

- a) la question de la bijectivité de cette application,
- b) si $\pi^G = 1$ (rigidité), pour $G \neq \{1\}$
(pour un relèvement donné, dans \mathcal{E} pour simplifier).

J'ai envie de conjecturer sans vergogne qu'il en est ainsi – ce qui impliquerait par exemple que pour tout tel relèvement de G , il y a un sous-groupe *ouvert* $(\mathfrak{S}^G)_p$ du groupe (peut-être vraiment immense a priori!) $\hat{\mathfrak{S}}^G$, qui se remonte canoniquement de façon à commuter à G

Il faudrait manifestement faire, en même temps qu'une théorie des opérations extérieures des groupes finis sur des groupes discrets à lacets (qui est pour le moment extrêmement conjecturale) une théorie analogue dans le cas profini – j'aurai sans doute à y revenir par la suite.

§ 32. — RETOUR SUR LES ASPECTS ARITHMÉTIQUES DU BOUCHAGE DE TROUS : RELATIONS ENTRE $\Pi_{g,\nu}$ et $\Pi_{g,\nu-1}$

Bien sûr, on a que

$$\mathcal{N}_{g,\nu} \rightarrow \mathfrak{S}_\nu$$

est surjectif (puisque $\mathfrak{Z}_{g,\nu} \rightarrow \mathfrak{S}_\nu$ l'est), donc on aura

$$(1) \quad 1 \rightarrow \mathcal{N}_{g,\nu}^! \rightarrow \mathcal{N}_{g,\nu} \rightarrow \mathfrak{S}_\nu \rightarrow 1$$

et le diagramme cartésien de sous-groupes de $\hat{\mathfrak{Z}}_{g,\nu}$:

$$(2) \quad \begin{array}{ccc} \hat{\mathfrak{Z}}_{g,\nu}^+ & \hookrightarrow & \mathcal{N}_{g,\nu} \\ \uparrow & & \uparrow \\ \hat{\mathfrak{Z}}_{g,\nu}^{!+} & \hookrightarrow & \mathcal{N}_{g,\nu}^! \end{array}$$

$[\mathcal{N}_{g,\nu} = \mathcal{N}_{g,\nu}^! \cdot \hat{\mathfrak{Z}}_{g,\nu}^+]$ donnera un isomorphisme

$$(3) \quad \mathcal{N}_{g,\nu}^! / \hat{\mathfrak{Z}}_{g,\nu}^{!+} \xrightarrow{\sim} \mathcal{N}_{g,\nu} / \hat{\mathfrak{Z}}_{g,\nu}^+ = \Pi_{g,\nu}.$$

Dans le cas d'un (π, a) , (π groupe extérieur à lacets, a une arithmétisation), on aura de même:

$$(4) \quad \mathcal{N}_a^! / \hat{\mathfrak{Z}}_a^+ \xrightarrow{\sim} \mathcal{N}_a / \hat{\mathfrak{Z}}_a^+ = \Pi_a \mathcal{N}_a = \mathcal{N}_a^! \cdot \hat{\mathfrak{Z}}_a^+.$$

Considérons maintenant pour tout $i \in I$ le stabilisateur \mathcal{N}_i de i dans \mathcal{N} , et le groupe à lacets (pas extérieur!) π_i , de type $(g, \nu - 1)$, déduit de π par “bouchage du trou i ”²⁸. On a alors,

²⁸On écrit ici \mathcal{N} etc. au lieu de \mathcal{N}_a ; on suppose $(g, \nu - 1)$ aussi anabélien, i.e. $2g + \nu \geq 4$.

A. GROTHENDIECK

pour une discrétification choisie α compatible avec l'arithmétisation, un homomorphisme injectif

$$(5) \quad \pi'_i \xrightarrow{\varphi_i} \hat{\mathfrak{Z}}^{+!} \subset \mathcal{N}^! \subset \hat{\mathfrak{Z}}_i,$$

tel que le composé

$$\pi'_i \rightarrow \hat{\mathfrak{Z}}_i \rightarrow \hat{\mathfrak{G}}(\pi'_i)(\leftarrow \pi'_i)$$

soit l'inclusion canonique. Ceci posé, on veut ²⁹ que l'image de (5) (qui n'est peut-être pas invariante dans $\hat{\mathfrak{Z}}_i$) soit *invariante dans* \mathcal{N}_i , ³⁰ Cela signifie aussi que φ_i ne dépend pas du choix de la discrétification de classe α ... ou ce qui revient au même, dans $\mathcal{N}^!$ (car $\mathcal{N}_i = \mathcal{N}^! \cdot \hat{\mathfrak{Z}}_i^+$, or $\hat{\mathfrak{Z}}_i^+$ invarie cette image). Revenant à la situation universelle, cela signifie:

$$(5') \quad \mathcal{N}_{g,v}^! \subset \hat{\mathfrak{Z}}_{g,v}^+ \text{ est contenu dans le normalisateur des } \pi'_i \hookrightarrow \hat{\mathfrak{Z}}_{g,v}^{+!} \quad (1 \leq i \leq v-1),$$

qui sont donc invariants dans $\mathcal{N}_{g,v}^!$ ³¹ De plus, $\hat{\mathfrak{Z}}_{g,v}^! \xrightarrow{\psi_i} \hat{\mathfrak{G}}_{g,v-1}^!$ induit un *isomorphisme*

$$(6) \quad \mathcal{N}_{g,v}^! \xrightarrow{\sim} \mathcal{M}_{g,v-1}^!.$$

Cette assertion se décompose en deux: tout d'abord que ψ_i applique bien $\mathcal{N}_{g,v}^!$ dans $\mathcal{M}_{g,v-1}^!$ – et ceci résulte de la définition arithmético-géométrique de ces groupes – cela implique d'autre part, puisque ψ_i induit aussi un isomorphisme

$$\hat{\mathfrak{Z}}_{g,v}^+ \xrightarrow{\sim} \hat{\mathfrak{G}}_{g,v-1}^+,$$

qu'il induit un homomorphisme

$$(7) \quad \begin{array}{ccc} \Pi_{g,v} & \xrightarrow{\lambda_i} & \Pi_{g,v-1} \\ \wr & & \wr \\ \mathcal{N}_{g,v}/\hat{\mathfrak{Z}}_{g,v}^+ & & \mathcal{M}_{g,v-1}/\hat{\mathfrak{G}} \end{array}$$

et l'injectivité (resp. surjectivité) de (6) équivaut à celle de (7). D'ailleurs (7) s'insère, par construction, dans un diagramme commutatif:

$$(8) \quad \begin{array}{ccc} & \Gamma_{\mathbb{Q}} & \\ \theta \swarrow & & \searrow \theta \\ \Pi_{g,v} & \xrightarrow{\quad} & \Pi_{g,v-1} \end{array}$$

²⁹Plutôt, *il est vrai que!*

³⁰(***)

³¹Il suffit me semble-t-il de le prouver pour *un* i pour le déduire pour les autres.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

avec $\theta_{g,\nu}$ et $\theta_{g,\nu-1}$ surjectifs, donc il est bel et bien évident que (6) est *surjectif*. La bijectivité signifie que $\theta_{g,\nu}$ et $\theta_{g,\nu-1}$ ont même noyau (alors qu'a priori il se pourrait que $\theta_{g,\nu}$ ait un noyau plus petit, i.e. corresponde à une représentation de $\Pi_{\mathbb{Q}}$ “moins infidèle” que $\theta_{g,\nu-1}$). D'ailleurs, il est évident (même, a priori, sans utiliser la définition ailleurs explicitée de $\mathcal{N}_{g,\nu}$) que l'homomorphisme λ_i de (7) ne dépend pas du choix de $0 \leq i \leq \nu - 1$ – par exemple puisque l'on passe de l'un à l'autre en appliquant des opérations de $\hat{\mathfrak{Z}}^+$ (puisque $\hat{\mathfrak{Z}}^+$ opère transitivement sur I) et que $\hat{\mathfrak{Z}}^+$ opère trivialement dans $\Pi_{g,\nu} \dots$

On peut dire que (6) décrit $\mathcal{M}_{g,\nu-1}^!$ (donc $\mathcal{N}_{g,\nu-1}^!$) en termes de $\mathcal{N}_{g,\nu}$ – mais l'inverse est moins clair, faute de savoir si $\hat{\mathfrak{Z}}_{g,\nu} \xrightarrow{\psi_i} \hat{\mathfrak{S}}_{g,\nu-1}$ est injectif; si on le savait, on pourrait décrire $\mathcal{N}_{g,\nu}^!$ comme l'image inverse de $\mathcal{M}_{g,\nu-1}^! \dots$. Il ne serait pas impossible d'ailleurs que (6) soit faux, i.e. que les $\theta_{g,\nu}$ soient infidèles, mais de moins en moins quand on fait augmenter ν – en passant à la limite projective $\theta_{g,\infty}$, seulement, aurait-on (peut-être!) une représentation fidèle de $\Pi_{\mathbb{Q}}$? Mais jusqu'à indication contraire, je préfère travailler hypothétiquement avec (6), ce qui s'exprime par les suites exactes fondamentales

$$(9) \quad 1 \rightarrow \hat{\pi}_{g,\nu-1} \xrightarrow{\varphi_i} \mathcal{N}_{g,\nu}^! \xrightarrow{\psi_i'} \mathcal{N}_{g,\nu-1}^! \rightarrow 1^{32}$$

qui étend la suite exacte

$$(10) \quad 1 \rightarrow \hat{\pi}_{g,\nu-1} \xrightarrow{\varphi_i} \hat{\mathfrak{Z}}_{g,\nu}^! \xrightarrow{\psi_i'} \hat{\mathfrak{Z}}_{g,\nu-1}^! \rightarrow 1$$

(et tient lieu de la suite exacte peut-être défailante

$$?? \quad 1 \rightarrow \hat{\pi}_{g,\nu-1} \rightarrow \hat{\mathfrak{Z}}_{g,\nu}^! \rightarrow \hat{\mathfrak{Z}}_{g,\nu-1}^! \rightarrow 1 \quad ??).$$

Quand (π, a) est un groupe extérieur à lacets muni d'une arithmétisation – ce qu'on pourrait appeler une “courbe algébrique virtuelle” – alors ce qui précède permet de définir, sur chacun des π'_i de type $(g, \nu - 1)$ associés aux $i \in I(\pi)$, une arithmétisation canoniquement associée à a , soit a_i , et on trouve alors une suite exacte

$$(11) \quad 1 \rightarrow \pi'_i \rightarrow (\mathcal{N}_a)_i \xrightarrow{\psi_i} \mathcal{N}_{a_i^+} \rightarrow 1$$

telle que l'on ait

$$(12) \quad (\hat{\mathfrak{Z}}_a^+)_i = \psi_i^{-1}(\hat{\mathfrak{Z}}_{a_i^+}^+),$$

³²On pourrait l'inclure dans une suite exacte un peu plus grande, avec $(\mathcal{N}_{g,\nu})_i$ et $\mathcal{N}_{g,\nu-1} \dots$

A. GROTHENDIECK

induisant

$$(11') \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi'_i & \longrightarrow & \mathcal{N}_a^! & \xrightarrow{\phi_i^!} & \mathcal{N}_{a'_i}^! \longrightarrow 1 \\ & & & & \uparrow & & \uparrow \\ & & & & \hat{\mathfrak{Z}}_a^{+!} = \phi_i'^{-1}(\hat{\mathfrak{Z}}_{a_i}^{+!}) & & \hat{\mathfrak{Z}}_{a'_i}^{+!} \end{array}$$

et induisant par passage au quotient

$$(13) \quad \Pi_a \xrightarrow{\sim} \Pi_{a_i}.$$

De plus, l'application canonique

$$\text{Discrét}^+(\pi) \rightarrow \text{Discrét}^+(\pi'_i)$$

définit par passage aux quotients

$$(14) \quad \mathbb{P}_a \xrightarrow{\sim} \mathbb{P}_{a_i}$$

compatible avec les actions de Π_a , $\Pi_{a'_i}$ et (13).

Je ne fais ici aucune assertion sur une soi-disant bijectivité entre ensemble des arithmétisations de π , et ensemble des arithmétisations de π'_i – ce qui reviendrait à la bijectivité de

$$\hat{\mathfrak{Z}}/\mathcal{N}_a \rightarrow \hat{\mathfrak{Z}}'/\mathcal{M}_{a'} \simeq \hat{\mathfrak{Z}}'/\mathcal{N}_{a'},$$

qui n'aurait guère de raison d'être que si on admettait $\hat{\mathfrak{Z}}(\pi) \xrightarrow{\sim} \hat{\mathfrak{Z}}(\pi'_i)$, qui me semble bien problématique.

*Cependant, on trouve, par le foncteur “bouchage de trous”, une équivalence entre la catégorie des groupes profinis à lacets **extérieurs arithmétisés** de type (g, ν) , et des groupes profinis à lacets (pas extérieurs!) **arithmétisés**, de type $(g, \nu - 1)$.*

On peut se proposer d'essayer de préciser le type de propriétés qui vont caractériser $\mathcal{N}_{g,\nu}$ dans $\mathcal{N}'_{g,\nu} = \text{Norm}_{\hat{\mathfrak{Z}}_{g,\nu}}(\hat{\mathfrak{Z}}_{g,\nu}^+)$, ou encore $\Pi_{g,\nu}$ dans $\Pi'_{g,\nu} = \mathcal{N}'_{g,\nu}/\hat{\mathfrak{Z}}_{g,\nu}^+$. On a des homomorphismes naturels

$$(15) \quad \Pi'_{g,\nu} \rightarrow \text{Autext}(\hat{\mathfrak{Z}}_{g,\nu}^+) \Pi'_{g,\nu} \rightarrow \text{Autext}(\hat{\mathfrak{Z}}_{g,\nu}^{+!})$$

et je présume que $\Pi_{g,\nu}$ pourra se décrire comme image inverse d'un sous-groupe fermé convenable de l'un ou de l'autre des seconds membres, i.e. qu'on peut le décrire en termes des

propriétés d'opérations extérieures sur $\hat{\mathfrak{Z}}_{g,\nu}^+$ ou sur $\hat{\mathfrak{Z}}_{g,\nu}$. Les conditions (e) en tout cas, sont bien de ce type (propriété de normaliser des sous-groupes invariants π'_i de $\mathfrak{Z}_{g,\nu}^{+!}$). Bien sûr, on pourrait poser des conditions sur des automorphismes extérieurs (de $\hat{\mathfrak{Z}}_{g,\nu}^{+!}$, disons), qui soient stables par passage successifs à des $\hat{\mathfrak{Z}}_{g,\nu-1}^{+!}, \hat{\mathfrak{Z}}_{g,\nu'-1}^{+!}$ etc....et qui soient engendrées par les conditions (5') et (6). Mais il n'est pas dit du tout que cela suffira à décrire les $\Pi_{g,\nu} \subset \Pi'_{g,\nu}$, ne serait-ce que parce que la condition devient vide pour le cas limite $\nu = 0$ (si $g \geq 2$; ou pour les cas $g = 1, \nu = 1$, ou $g = 0, \nu = 3$). Il est possible qu'il faille faire intervenir des propriétés des π_1 des $\mathcal{M}_{g,\nu,\overline{\mathbb{Q}}}$, liées à la compactification. Ce n'est guère que dans le cas de $(g, \nu) = (0, 3)$ qu'il ne faut pas s'attendre du tout à ce genre de condition.

Appelons “courbe algébrique potentielle” (sous-entendu, sur une clôture algébrique non précisée de \mathbb{Q}) la donnée d'un groupe extérieur profini π à lacets de type (g, ν) , muni d'une arithmétisation a , et d'un germe de relèvement “admissible”

$$(16) \quad \Pi_a^{\natural} \rightarrow \mathcal{N}_a.$$

Elles forment une catégorie (pour les isomorphismes, pour le moment); si on se donne un torseur P sous $\Pi_{g,\nu}$ (ce qui, moralement, revient à se donner une clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} ...) les courbes potentielles de type (g, ν) *relatives* à ce torseur (moralement, correspondant à des courbes algébriques sur $\overline{\mathbb{Q}}$...) sont celles munies en plus d'un isomorphisme (“intérieur”)

$$(17) \quad \mathbb{P}_a \xrightarrow{\sim} P$$

(définissant un isomorphisme

$$(18) \quad \Pi_a \rightarrow \Gamma_P = \text{Aut}_{\Pi_{g,\nu}}(P).)$$

Cette fois-ci, on s'attend à trouver des ensembles d'isomorphismes *finis*, au lieu de torseurs sous des groupes profinis considérables³³.

On considère les *points* de π , comme les classes de π -conjugaison de relèvements “admissibles” de (16) en

$$(19) \quad \Pi_a^{\natural} \rightarrow \mathcal{M}_a \subset \hat{\mathfrak{Z}}(\pi)$$

³³Le cas où P est le torseur trivial est celui des π [extérieurs ?] munis d'une *prédiscretification* orientée α ; d'où une suite exacte:

$$1 \rightarrow \hat{\mathfrak{Z}}_{\alpha} \rightarrow \hat{\mathcal{N}}_{\alpha} \rightarrow \Pi_{\alpha} \rightarrow 1$$

A. GROTHENDIECK

i.e. un germe de vraie action de Π_a sur π avec $\pi^{\Pi_a} = 1$ ceci pour l'admissibilité.

Question liminaire: La connaissance de π , de $\Sigma_a = \hat{\Sigma}_a^+ \subset \hat{\Sigma}(\pi)$, et d'un sous-groupe $\Gamma \subset \hat{\Sigma}(\pi)$ (normalisant Σ_a , tel que $\Gamma' \cap \Sigma_a = \{1\}$) permet-elle de retrouver l'arithmétisation de π – et, pour commencer, de retrouver \mathcal{N}_a (dans lequel $\Gamma \cdot \Sigma$ est d'indice fini)? Il suffirait, pour pouvoir répondre par l'affirmative, de savoir que tout isomorphisme extérieur $\pi \rightarrow \pi_{g,v}$, qui envoie Σ sur $\hat{\Sigma}_{g,v} = \Sigma_{g,v}$, et tout sous-groupe d'indice fini $\Gamma' \cdot \Sigma$ de \mathcal{N}_a dans $\mathcal{N}_{g,v}$, est compatible avec les arithmétisations. Or ceci revient exactement à:

(g) (facultatif, quand-même!) Pour tout sous-groupe ouvert \mathcal{N}' de $\mathcal{N}_{g,v}$, les éléments de $\hat{\Sigma}_{g,v}$ normalisant $\hat{\Sigma}_{g,v}$ et qui transportent \mathcal{N}' dans $\mathcal{N}_{g,v}$, sont dans $\mathcal{N}_{g,v}$ (a fortiori $\mathcal{N}_{g,v}$ serait son propre normalisateur dans $\text{Norm}_{\hat{\Sigma}_{g,v}}(\hat{\Sigma}_{g,v})$).

Avec les “points de \mathcal{U} ” (définis comme classes de conjugaison de relèvements (19)) “admissibles” i.e. satisfaisant (20), on fait un groupoïde, ayant comme groupe fondamental extérieur π , et sur lequel $\Gamma \subset \mathcal{N}_a$ opère strictement (NB. pour se reposer, on se donne maintenant Γ lui-même, pas seulement un germe – moralement, cela signifie qu'on a une courbe définie sur une sous-extension finie K de $\overline{\mathbb{Q}}/\mathbb{Q}$... Les points fixes de Γ correspondent aux points rationnels sur K , les points fixes sous un sous-groupe fermé Γ' aux points rationnels sur la sous-extension K' de $\overline{\mathbb{Q}}/\mathbb{Q}$ associée à Γ' ...)

Soit maintenant $I' \subset I = I(\pi)$ une partie de I , stable par Γ . On trouve par “bouchage de trous en I' ” un groupe extérieur à lacets π' , et un homomorphisme extérieur

$$(20) \quad \pi \rightarrow \pi'.$$

D'ailleurs π' hérite d'une arithmétisation a' par π – et on aura

$$(21) \quad \Pi_a \xrightarrow{\sim} \Pi_{a'} P \simeq \mathbb{P}_a \xrightarrow{\sim} \mathbb{P}_{a'}$$

donc π' est défini sur la même P que Π_a (i.e. en faisant des trous dans \mathcal{U} pour trouver \mathcal{U}' , on n'a pas dérangé le corps de base algébrique absolu $\overline{\mathbb{Q}}$...). D'ailleurs on aura un homomorphisme canonique

$$\hat{\Sigma}(\pi) \rightarrow \hat{\Sigma}(\pi')$$

induisant

$$(22) \quad \begin{array}{ccc} \mathcal{N}_a & \longrightarrow & \mathcal{N}_{a'} \\ \uparrow & & \uparrow \\ \hat{\mathcal{Z}}_a & \longrightarrow & \hat{\mathcal{Z}}_{a'} \end{array}$$

(induisant justement $\Pi_a \rightarrow \Pi_{a'}$ par passage aux quotients), et on trouve, en composant

$$\Gamma \hookrightarrow \mathcal{N}_a \rightarrow \mathcal{N}_{a'}$$

un homomorphisme également injectif

$$(23) \quad \Gamma \hookrightarrow \mathcal{N}_{a'}$$

qui est une quasi-section de $\mathcal{N}_{a'}$ sur $\Pi_{a'}$. Donc sous réserve d'admissibilité, on trouve sur π' une structure de courbe algébrique potentielle, relative au même P .

Je suis vraiment gêné aux entournures, faute d'avoir une définition en forme d'"admissible" – je vais y revenir très vite – mais pour le moment, j'ai envie de noter que, si $I' \neq \emptyset$, le groupe extérieur π' peut se décrire par un vrai groupoïde, ayant I' comme ensemble d'objets, et sur lequel Γ opère en sens strict (ceci est de l'algèbre pure, indépendamment des histoires d'arithmétisation...) Le fait que Γ opère trivialement sur les $i' \in I'$ implique que pour tout $i' \in I'$, on a un homomorphisme canonique

$$(24) \quad \Gamma \rightarrow \pi'(i')$$

qui relève son action extérieur, d'où une classe de π' -conjugaison de relèvements de l'action extérieure de Γ sur π' en une vraie action de Γ sur π' – on espère qu'elle satisfait $\pi'^\Gamma = 1$ – et on a donc une application canonique

$$(25) \quad I' \rightarrow \text{Pts}(\pi', \alpha', \Gamma).$$

Je dis que cette application est injective. Ceci est "évident" quand on interprète "action extérieure admissible" par "réalisable par une vraie courbe algébrique", et "relèvements admissibles" par "réalisables par des vrais points rationnels sur K , corps des invariants de Γ "³⁴. Mais on voudrait bien sûr des raisons internes à la donnée des $(\mathcal{N}_{g,v})$, et des propriétés de ces

³⁴On est ramené au cas $\text{Card}(I') = 2...$

A. GROTHENDIECK

données! Ce point étant admis (en mettant entre parenthèses les deux définitions essentielles d’admissibilité, sur lesquelles on va revenir plus bas) on trouve un foncteur “bouchage de trous” (il faut faire aussi les restrictions anabéliennes habituelles):

<p>Courbes algébriques potentielles sur P relatives à un sous-groupe ouvert $\Gamma \rightarrow$ de Π_p, et munies d’un ensemble I' de points à l’infini</p>	<p>Courbes algébriques potentielles sur P relatives à Γ munies d’une partie de l’ensemble des “points invariants sous Γ”</p>
--	---

et sauf erreur, il est devenu évident que ce foncteur est une *équivalence de catégories* [pour les isomorphismes] et comme conséquence, il y a le foncteur en sens inverse: forer des trous en des “points” invariants sous Γ (ou en des points quelconques, quitte à passer à un Γ' plus petit).

Mais je me rends compte que ce n’est pas du tout évident – je vais essayer d’élucider la situation axiomatiquement. On a fixé un genre g , on suppose donné, pour v variable (tel que (g, v) anabélien) des sous-groupes fermés $\mathcal{N}_{g,v} \subset \hat{\mathfrak{Z}}_{g,v}$, normalisant $\hat{\mathfrak{Z}}_{g,v}$, et satisfaisant la condition essentielle que les $\phi_i : \hat{\mathfrak{Z}}_{g,v} \rightarrow \hat{\mathfrak{G}}_{g,v-1}$ induisent

$$\mathcal{M}_{g,v} \xrightarrow{\sim} \mathcal{M}_{g,v-1},$$

ce qui permet de définir la notion d’arithmétisation d’un π profini de type (g, v) anabélien, et la théorie du bouchage d’un nombre quelconque de trous, et du forage d’un seul trou, dans la catégorie des groupes de type (g, v) arithmétisés.

On suppose d’autre part donné une sous-catégorie pleine ³⁵ de la catégorie des groupes profinis (qui pourrait se réduire aux sous-groupes ouverts de Π_g , valeur commune des $\Pi_{g,v}$, ou des sous-groupes ouverts du groupe Π_a , a une arithmétisation), et une notion d’opérations extérieures “admissibles” de tels Γ sur des π arithmétisés. On suppose

- (1) Si Γ opère admissiblement sur π , tout sous-groupe ouvert aussi (et inversement);
- (2) ³⁶ Il suffit de la poser pour $\text{Card}(I') = 1$, i.e. bouchage d’un trou – d’ailleurs si on sait que la condition d’admissibilité ne dépend que de l’action des noyaux des groupes. Si de plus Γ invarie une partie I' de $I = I(\pi)$, alors en “bouchant I' ”, l’opération de Γ sur π' est admissible.

³⁵ On la supposera stable par passage à des sous-groupes ouverts.

³⁶ (***)

Quand on a une action *effective* (pas extérieure) de Γ sur un (π, a) de type (g, ν) , alors le foncteur “forage de trous” donne une action extérieure sur un (π°, a°) de type $(g, \nu + 1)$ et on dit que l’action de départ est admissible, si l’action *extérieure* déduite l’est. On trouve ainsi une *équivalence* entre la catégorie des systèmes $(\pi, a, \Gamma, \psi, i)$ d’un (π, a) de type $(g, \nu + 1)$, avec une opération *extérieure* admissible ψ d’un Γ dessus, et un $i \in I(\pi)$ stable par Γ , avec la catégorie des $(\pi', a', \Gamma, \psi')$ des (π', a') de type (g, ν) , avec une *vraie* action admissible ψ' de Γ dessus. La condition (2) assure que si Γ opère effectivement, de façon admissible, alors l’action extérieure déduite est admissible (mais l’inverse ne sera pas vrai – il y aura des relèvements “pathologiques” d’une action extérieure admissible donnée...). On suppose de plus

(3) Si Γ opère effectivement de façon admissible sur π , alors $\pi^\Gamma = \{1\}$.

Cela implique que la catégorie des Γ -points de π , ou si on veut des sections de $B_{\pi, \Gamma} (\simeq B_u)$ sur B_Γ , est rigide. Mais considérons la catégorie limite inductive de la catégorie des sections de $B_{\pi, \Gamma} \simeq B_u$ sur des $B_{\Gamma'}$ (Γ' sous-groupe ouvert); elle est discrète et correspond à l’ensemble

$$\text{Pt}_{ad}(B_{\pi, \Gamma^\dagger}) \simeq \varinjlim \text{Pt}_{ad}(B_{\pi, \Gamma'})$$

où l’on prend la limite inductive sur les ouverts Γ' de Γ .

Si $\text{Pt}(B_{\pi, \Gamma}) \neq \emptyset$, alors (du seul fait que $\pi^{\Gamma'} = \{1\}$ pour tout sous-groupe ouvert de Γ) le groupe extérieur π peut être décrit canoniquement par un groupoïde profini $\underline{\text{Pt}}(B_{\pi, \Gamma})$ ayant $\text{Pt}(B_{\pi, \Gamma})$ comme ensemble d’objets ³⁷, liés par le groupe extérieur π , sur lequel Γ opère en sens strict, le stabilisateur Γ_p de tout point étant ouvert, et $\Gamma_p \rightarrow \text{Aut}(P) (\simeq \pi \text{ modulo automorphismes intérieurs})$ étant continue. On a ici que si à tout $P \in \text{Pt}(B_{\pi, \Gamma})$ on associe la classe d’isomorphie de sections de $B_{\pi, \Gamma}$ sur B_Γ , on trouve une bijection – ce qui caractérise le Γ -groupoïde en question à *isomorphisme* unique près. On supposera:

(4) Si Γ opère admissiblement sur (π, a) , alors il existe un sous-groupe ouvert Γ' de Γ dont l’opération extérieure se relève en une opération effective admissible – i.e. $\text{Pt}_{ad}(B_{\Gamma, \pi}) \neq \emptyset$.

Notons que dans la situation envisagée, du bouchage d’un trou $i \in I(\pi)$ d’un π , en plus de l’homomorphisme

$$\hat{\mathfrak{Z}}(\pi)_i \xrightarrow{\psi_i} \hat{\mathfrak{C}}(\pi'_i)$$

³⁷Le groupoïde à opérateurs stricts $\underline{\text{Pt}}(B_{\pi, \Gamma})$ dépend fonctoriellement de (π, Γ) , pour des morphismes extérieurs [??].

A. GROTHENDIECK

associé, donnant par composition

$$\hat{\mathfrak{Z}}(\pi)_i \xrightarrow{\psi'_i} \hat{\mathfrak{Z}}(\pi'_i)$$

d'où une action extérieure de $\hat{\mathfrak{Z}}(\pi)$ sur π'_i , de façon que les $\pi \xrightarrow{p_i} \pi'_i$ commutent aux actions extérieures de $\hat{\mathfrak{Z}}(\pi)$, on a un homomorphisme canonique d'extensions, provenant de cette action extérieure et de l'homomorphisme $p_i : \pi \rightarrow \pi'_i$;

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi & \longrightarrow & \hat{\mathfrak{E}}(\pi)_i & \longrightarrow & \hat{\mathfrak{Z}}(\pi)_i \longrightarrow 1 \\ & & \downarrow p_i & & \downarrow \varphi_i & \nearrow [\psi_i] & \downarrow \psi'_i \\ 1 & \longrightarrow & \pi'_i & \longrightarrow & \hat{\mathfrak{E}}(\pi'_i) & \longrightarrow & \hat{\mathfrak{Z}}(\pi'_i) \longrightarrow 1 \end{array}$$

qui n'est *pas* le composé

$$\hat{\mathfrak{E}}(\pi)_i \rightarrow \hat{\mathfrak{Z}}(\pi)_i \xrightarrow{\psi_i} \hat{\mathfrak{E}}(\pi'_i)$$

(il peut se définir chaque fois qu'on a un groupe Γ , i.e. $\hat{\mathfrak{Z}}(\pi)$, qui commute extérieurement sur deux groupes extérieurs π, π' , et qu'on a un homomorphisme $p_i : \pi \rightarrow \pi'$ qui commute à l'action de Γ , et tel que le centre de π et le centralisateur de son image dans π' soient triviaux...) C'est aussi ici l'homomorphisme de "transport de structure", qui pour tout automorphisme à lacets u de π , associe l'automorphisme correspondant de π'_i . On a oublié de préciser:

(g) L'homomorphisme canonique $(\hat{\mathfrak{E}}_{g,v})_i \rightarrow \hat{\mathfrak{E}}_{g,v-1}$ associé à $i \in [0, v-1]$ envoie $(\mathcal{M}_{g,v})_i$ dans $\mathcal{M}_{g,v}$, donc il s'insère dans un homomorphisme de suites exactes:

$$(26) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \pi & \longrightarrow & \mathcal{M}_a(\pi)_i & \longrightarrow & \mathcal{N}_a(\pi)_i \longrightarrow 1 \\ & & \downarrow & & \downarrow \varphi_i & & \downarrow \\ 1 & \longrightarrow & \pi'_i & \longrightarrow & \mathcal{M}_{a'}(\pi'_i) & \longrightarrow & \mathcal{N}_{a'}(\pi'_i) \longrightarrow 1 \end{array}$$

Ceci posé, si on a une opération extérieure admissible $\Gamma \rightarrow \mathcal{N}_a(\pi)$ de Γ sur π , fixant i , donc aussi par exemple $\mathcal{N}_a(\pi) \rightarrow \mathcal{N}_{a'}(\pi')$ sur π'_i , on peut considérer que tout relèvement $\Gamma \rightarrow \mathcal{M}_a(\pi)$ pour π définit par composition un relèvement $\Gamma \rightarrow \mathcal{M}_{a'}(\pi'_i)$ pour π'_i . On conclut aisément de (2) que si le premier est admissible, le deuxième l'est. On trouve donc

$$(27) \quad \text{Pt}_{ad}(B_{\pi,\Gamma}) \rightarrow \text{Pt}_{ad}(B_{\pi'_i,\Gamma})$$

et en passant à la limite, une application de Γ -ensembles:

$$(28) \quad \mathrm{Pt}_{ad}(B_{\pi, \Gamma^{\natural}}) \rightarrow \mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma^{\natural}})$$

– qui correspond d'ailleurs à un homomorphisme de Γ -groupoïdes

$$(29) \quad \underline{\mathrm{Pt}}_{ad}(B_{\pi, \Gamma^{\natural}}) \rightarrow \underline{\mathrm{Pt}}_{ad}(B_{\pi'_i, \Gamma^{\natural}}).$$

Ceci posé, soit $P \in \mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma})$ le “point canonique” de $\mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma}) = (\mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma^{\natural}}))^{\Gamma}$. On demande:

(5) L'application (27) induit une *bijection*

$$\mathrm{Pt}_{ad}(B_{\pi, \Gamma}) \rightarrow \mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma}) \setminus \{P\}$$

ou encore (passant à la limite) une bijection de Γ -ensembles

$$\mathrm{Pt}_{ad}(B_{\pi, \Gamma^{\natural}}) \xrightarrow{\sim} \mathrm{Pt}_{ad}(B_{\pi'_i, \Gamma^{\natural}}) \setminus \{P\}.$$

Ceci signifie trois choses:

- (a) L'homomorphisme canonique $\Gamma \rightarrow \mathcal{M}_{a'}(\pi'_i)$, composé de $\Gamma \rightarrow \mathcal{N}_a(\pi)$ et de $\mathcal{N}_a(\pi) \xrightarrow{\sim} \mathcal{M}_{a'}(\pi'_i)$, n'est pas π'_i -conjugué à un homomorphisme composé $\Gamma \xrightarrow{\lambda} \mathcal{M}_a(\pi) \xrightarrow{\varphi_i} \mathcal{M}_{a'}(\pi'_i)$, où $\Gamma \xrightarrow{\lambda} \mathcal{M}_a(\pi)$ est un relèvement admissible.
- (b) Si $\lambda, \mu : \Gamma \rightarrow \mathcal{M}_a(\pi)$ sont deux relèvements admissibles de $\Gamma \rightarrow \mathcal{N}_a(\pi)$ tels que $\varphi_i \circ \lambda$ et $\varphi_i \circ \mu : \Gamma \rightarrow \mathcal{M}_{a'}(\pi'_i)$ soient π'_i -conjugués, alors λ et μ sont déjà π -conjugués.
- (c) Tout relèvement admissible de $\Gamma \rightarrow \mathcal{N}_{a'}(\pi'_i)$ en $\Gamma \rightarrow \mathcal{M}_{a'}(\pi'_i)$, provient par composition d'un relèvement admissible $\Gamma \rightarrow \mathcal{M}_a(\pi)$.

Grâce à ceci: l'équivalence de catégories entre systèmes $(\pi, a, i, \Gamma, \theta : \Gamma \rightarrow \mathcal{N}_a)$ et les systèmes $(\pi', a', \Gamma, \theta' : \Gamma \rightarrow \mathcal{N}_{a'}, P)$, où $P \in \mathrm{Pt}(B_{\pi', \Gamma^{\natural}})^{\Gamma}$, se précise de façon parfaite au niveau des points: les points Γ -rationnels de B_{π} s'identifient à l'un des pts Γ -rationnels de $B_{\pi'}$, distincts de P .

Ceci nous permet alors (ce qui n'était pas faisable dans le contexte discret!) d'étendre l'équivalence de catégories en une équivalence:

A. GROTHENDIECK

[Catégorie des systèmes $(\pi, \alpha, I', \Gamma, \theta : \Gamma \rightarrow \mathcal{N}_\alpha)$ d'un π arithmétisé par α de type (g, ν) avec $2g + (\nu - \text{card}(I')) \geq 3$, de $I' \subset I(\pi)$, d'une action *admissible* extérieure de Γ sur π telle que Γ fixe chaque point de I']

(30) | \rangle \rangle

[Catégorie des systèmes $(\pi', \alpha', I', \Gamma, \theta' : \Gamma \rightarrow \mathcal{N}_{\alpha'})$ d'un π' arithmétisé par α' de type (g, ν') [$\nu' = \nu - \text{card}(I')$] avec opération extérieure admissible de Γ dessus, et une partie $I' \subset \text{Pt}_{ad}(B_{\pi', \Gamma})$ (donc $I' \subset \text{Pt}_{ad}(B_{\pi', \Gamma})^\Gamma$), i.e. I' formé de points invariants par Γ , i.e. “ Γ -rationnels”].

On a alors un foncteur quasi-inverse: forage de trous en I' ! Il est à noter que dans cette approche, on a dû se borner au cas d'un ensemble de points $I' \subset I(\pi)$, non seulement stable par Γ , mais inclus dans I^Γ , ou encore à une partie $I' \subset \text{Pt}(B_{\pi', \Gamma^\natural})$ non seulement stable par Γ , mais même dans $\text{Pt}(B_{\pi', \Gamma^\natural})^\Gamma$. Pour montrer que sans cette restriction, le foncteur naturel correspondant est néanmoins une équivalence, on est ramené à ceci:

(6) Soit $(\pi, a, I' \subset I(\pi))$ avec (π, a) groupe à lacets extérieur profini arithmétisé de type (g, ν) , d'où (π', a') – soit Γ , avec Γ' sous-groupe ouvert opérant sur (π, a) de façon admissible ($\Gamma \rightarrow \mathcal{N}_a(\pi)$), et laissant stable I' , donc il opère de façon admissible sur (π', a') . Supposons donné un *relèvement* de cette action de Γ' en une action admissible de Γ sur $\mathcal{N}_{a'}$, qui invarie $I' \subset \text{Pt}(B_{\pi', \Gamma^\natural}) \simeq \text{Pt}(B_{\pi', \Gamma'^\natural})$ [cf. le diagramme],

$$\begin{array}{ccc} (\mathcal{N}_a)_{I'} & \xleftarrow{\quad} & \Gamma' \\ \downarrow & \swarrow & \downarrow \\ \mathcal{N}_{a'} & \xleftarrow{\quad} & \Gamma \end{array}$$

Alors il existe une action admissible unique de Γ sur (π, a) , qui prolonge celle de Γ' et qui donne naissance à celle donnée sur π' .

L'unicité est-elle de toutes façons claire? Considérons l'extension \mathcal{E} de Γ par $L = \text{Ker}((\mathcal{N}_a)_{I'} \rightarrow \mathcal{N}_a)$, image inverse de l'extension $(\mathcal{N}_a)_{I'}$ (de $\mathcal{N}_{a'}$ pas L) via $\Gamma \rightarrow \mathcal{N}_{a'}$, on a un scindage partiel de cette extension au dessus du sous-groupe Γ' de Γ , et l'assertion est que ce scindage se *prolonge, de façon unique* à Γ . On peut supposer Γ' invariant dans Γ , et on identifie Γ' à un sous-groupe de \mathcal{E} . Toutes les sections de \mathcal{E} sur Γ s'identifient à des sous-groupes, sections $\tilde{\Gamma}$ de \mathcal{E} . Pour un tel $\tilde{\Gamma}$, on a bien sûr $\tilde{\Gamma} \subset \text{Norm}_{\mathcal{E}}(\Gamma')$, d'ailleurs on a évidemment:

(31) $\text{Norm}_{\mathcal{E}}(\Gamma') \cap L = L^{\Gamma'}$

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

et je présume qu'on doit avoir $L^{\Gamma'} = 1$ (qui généralise la condition (3) plus haut...) Or cette condition implique l'unicité – savoir $\tilde{\Gamma} = \text{Norm}_{\mathcal{G}}(\Gamma')$ et l'existence signifie que

$\text{Norm}_{\mathcal{G}}(\Gamma') \rightarrow \Gamma$ est un épimorphisme (donc un isomorphisme...).

Mais il faudra essayer de préciser, dans certains contextes (au moins celui des actions arithmétiquement fidèles, i.e. $\Gamma \rightarrow \Pi_a$ injectif – qui correspond normalement au cas des courbes algébriques définies sur des extensions *algébriques* de \mathbb{Q}) – la notion d'action “admissible”. Pour ceci, on doit revenir sur la relation entre courbes (potentielles) et revêtements finis, ce qui donne aussi une façon de faire varier g .

Mais j'ai envie d'abord de reprendre sous un autre aspect (peut-être plus général) le formalisme précédent, qui peut-être aussi s'applique au cas des groupes *discrets* à lacets (je pense au formalisme des $\mathcal{U}^!$, lié aux actions extérieures de groupes finis sur de tels groupes à lacets). Soit \mathcal{X} un ensemble $\neq \emptyset$ (moralement, un ensemble de “points” d'une courbe algébriques, ou d'une surface topologique...); on suppose donné, pour toute partie finie I de \mathcal{X} , de complémentaire $\mathcal{U}_I = \mathcal{X} \setminus I$, un groupoïde $\Pi_{\mathcal{U}_I}$, ayant \mathcal{U}_I comme ensemble d'objets. De plus, pour $J \supset I$ i.e. $\mathcal{U}_J \subset \mathcal{U}_I$, on suppose donné un homomorphisme de groupoïdes

$$\Pi_{\mathcal{U}_J} \rightarrow \Pi_{\mathcal{U}_I}$$

qui sur les objets soit l'inclusion $\mathcal{U}_J \hookrightarrow \mathcal{U}_I$. On supposera la transitivité (stricte) i.e. [l'existence d']un foncteur covariant de la catégorie des parties \mathcal{U} de \mathcal{X} complémentaires de parties finies ³⁸ (avec les inclusions), vers la catégorie des groupoïdes, qui sur l'ensemble d'objets coïncide avec le foncteur évident... On suppose de plus que pour tout $i \in I$, on se donne un groupoïde Π_i (ou $\Pi_{D_i^*}$), et pour $i \in I \in \mathfrak{F}(??)$ un homomorphisme de groupoïdes

$$\Pi_{D_i^*} \rightarrow \Pi_{\mathcal{U}_I}$$

compatible avec les morphismes de transition $\pi_{\mathcal{U}_I} \rightarrow \pi_{\mathcal{U}_J}$, $I \supset J$. On suppose que pour I fixé, on trouve sur $\Pi_{\mathcal{U}_I}$ une structure de groupoïde à lacets par

$$\Pi_{D_i^*} \rightarrow \Pi_{\mathcal{U}_I}$$

³⁸Si \mathcal{X} est fini et $I = \mathcal{X}$, on suppose que cependant $\Pi_{\mathcal{U}_I} (= \Pi_{\emptyset})$ n'est pas le groupoïde vide, mais un groupoïde (qui s'envoie dans les précédents...) mais on ne pourra pas exiger la transitivité stricte Il faudrait peut-être faire des hypothèses anabéliennes sur $\Pi_{\mathcal{U}_I}$.

A. GROTHENDIECK

sans d'ailleurs exclure le cas où $I = \emptyset$, et où $(\Pi_{\mathcal{X}}$ étant connexe, disons) le genre *est* 0. On suppose de plus que si $J \supset I$ i.e. $\mathcal{U}_J \subset \mathcal{U}_I$, et pour $i \in J \setminus I$, l'homomorphisme composé

$$\Pi_{D_i^*} \rightarrow \Pi_{\mathcal{U}_J} \rightarrow \Pi_{\mathcal{U}_I}$$

soit "constant", de telle façon que $\Pi_{\mathcal{U}_I}$ se déduise de $\Pi_{\mathcal{U}_J}$ par "bouchage des trous" en $J \setminus I$.

Jusqu'à présent, tout ceci pouvait se visualiser par exemple en partant d'une surface topologique orientable X , et d'une partie \mathcal{X} de X rencontrant toute composante connexe, en prenant pour Π_I la restriction à $\mathcal{X} \setminus I$ du groupoïde fondamental de $X \setminus I$ (si $I \neq \mathcal{X}$; si $\mathcal{X} = I$, ce qui exige \mathcal{X} fini, on prendra le groupoïde fondamental de $X \setminus I = X \setminus \mathcal{X}$, qu'on aura du mal à envoyer dans les autres avec transitivité *stricte*, qu'à cela ne tienne!) Mais, on est surtout intéressé au cas \mathcal{X} infini. Où on prend X courbe algébrique sur un corps algébriquement clos, \mathcal{X} partie de X rencontrant toute composante connexe, et on définit les $\Pi_{\mathcal{U}_I}$ comme précédemment.

Soit maintenant Γ une groupe qui opère sur la situation (*strictement*, s'entend), donc sur l'ensemble \mathcal{X} , les groupoïdes $\Pi_{\mathcal{U}_I}$, les $\Pi_{D_i^*}$ (NB qu'il permute entre eux), en commutant aux homomorphismes

$$\Pi_{\mathcal{U}_I} \rightarrow \Pi_{\mathcal{U}_J} \text{ et les } \Pi_{D_i^*} \rightarrow \Pi_{\mathcal{U}_I}.$$

(On aura des difficultés, si \mathcal{X} est fini, pour $\Pi_{\mathcal{U}_I}$ quand $I = \mathcal{X}$, pour la commutation *stricte* des $\Pi_{\mathcal{U}_X} \rightarrow \Pi_{\mathcal{U}_I} \dots$ mais passons...) Nous supposons définie une notion de sous-groupe *admissible* de Γ (ils sont en tout cas $\neq \{1\}$) telle que si Γ' est admissible alors tout sous-groupe $\Gamma'' \supset \Gamma'$ aussi.

On suppose

(1°) $\forall P \in \mathcal{X}, \Gamma_P \neq \{1\}$, et Γ_P d'indice fini dans Γ (i.e. l'orbite de P finie).

Nous voulons des conditions qui assurent que \mathcal{X} et les $\Pi_{\mathcal{U}_I}$ etc. peuvent se reconstruire à isomorphisme canonique près à l'aide des données purement groupoïdiques ou topologiques (à opérateurs Γ) correspondantes. On peut le dire en langage topologique savant, mais on va l'exprimer en termes de théorie des groupes à lacets. Soit I une partie de \mathcal{X} stable par Γ , on voudrait poser des conditions qui permettent d'exprimer (pour tout tel I) la situation des groupoïdes Π_V associés aux $V \supset \mathcal{U}_I$ (i.e. les \mathcal{U}_J avec $J \subset I$), les $\Pi_{D_i^*}$ ($i \in I$) et l'opération de Γ dessus, en termes des seules opérations de Γ sur le groupe extérieur à lacets $\pi_1(\Pi_{\mathcal{U}_I})$ associé à I ou plutôt (car cela est immédiat, par l'opération de forage de trous), en sens inverse, montrer

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

comment, sous réserve d'anabélianité, disons de $\Pi_{\mathcal{X}}$ (pour fixer les idées), on peut plus ou moins reconstituer $\Pi_{\mathcal{U}_I}$ et l'action de Γ dessus..., à partir de $\Pi_{\mathcal{X}}$ (ou plutôt, du topos $B_{\Pi_{\mathcal{X}}}$), et de l'action de Γ dessus. On veut au moins une description intrinsèque des éléments de \mathcal{X} et de l'action de Γ dessus, via cette action “molle” – qui, pour \mathcal{X} connexe, revient encore à une action extérieure de Γ sur un groupe à lacets (*sans* lacets!) $\pi...$

Une première condition, sous forme faible, est que (supposant \mathcal{X} connexe, et appelant $\pi(I)$ le groupe extérieur $\pi_1(\Pi_{\mathcal{U}_I})$, pour tout partie finie I de \mathcal{X}) que pour $\pi(I)$ anabélien (ce qui sera le cas pour I “assez grand”, du moins si \mathcal{X} est infini, donc qu'on puisse prendre I de cardinal arbitrairement grand...) l'application évidente

classes de

$\pi(I)$ -conjugaison $U_I \rightarrow \text{Pt}(B_{\pi(I), \Gamma^{\natural}}) \xrightarrow{\sim} \text{degermesdescindagedel'extension } E(I)(2^{\circ}) (\text{compatible avec les actions})$ soit *injective*. Mais pour aller plus loin, il faudrait pouvoir donner une caractérisation de l'image. Notons (nous plaçant dans le contexte profini désormais) que si on se donne sur les $\pi(I)$ des arithmétisations, compatibles avec les homomorphismes extérieurs de bouchage de trous $\pi(I) \rightarrow \pi(J)$, et avec l'action de Γ sur les $\pi(I)$, on a donc un homomorphisme canonique de Γ dans le groupe commun Π des automorphismes arithmétiquement extérieurs de ces arithmétisations (et même $\Gamma \rightarrow \mathcal{M}_{\pi(\theta)=\pi}$, ce qui est déjà une donnée nettement plus forte). On peut donc supposer donnée une notion de *relèvement admissible* d'une telle action arithmétiquement extérieure, de telle façon que l'application (2°) soit une bijection

$$\mathcal{U}_I = \mathcal{X} \setminus I \xrightarrow{\sim} \text{Pt}_{ad}(B_{\pi(I), \Gamma^{\natural}}).$$

Ceci signifie d'ailleurs, pratiquement, que la notion d'admissibilité satisfait aux conditions (1°) à (6°) vues ci-dessus.

Quant à savoir ce qu'il y a lieu d'appeler opération extérieure “admissible” de Γ sur un groupe extérieur profini à lacets, cela reste pour le moment conjectural. On pourrait à titre expérimental conjecturer que la notion qui suit marcherait. Appelons “admissible” toute telle action

$$\Gamma \rightarrow \hat{\mathfrak{Z}}(\pi)$$

qui respecte une arithmétisation a , i.e. qui se factorise par le \mathcal{N}_a correspondant, telle que l'image de $\Gamma \rightarrow \mathcal{N}_a / \hat{\mathfrak{Z}} = \Pi_a$ soit ouverte, et que pour tout homomorphisme de bouchage de

A. GROTHENDIECK

trous en $i \in I(\pi)$, $\pi \rightarrow \pi'_i$, $\mathcal{N}(\pi)_i \rightarrow \mathcal{M}(\pi'_i)$, l'homomorphisme correspondant de Γ_i ni d'aucun sous-groupe ouvert Γ de Γ_i , ne normalise un L'_j , $j \in I(\pi'_i) = I \setminus \{i\}$; peut-être même faudrait-il imposer que $\pi^{(\Gamma'^+)} = \{1\}$, où Γ'^+ est le noyau de $\Gamma' \xrightarrow{\chi} \hat{\mathbb{Z}}^*$ – en tout cas on s'attend à ce que l'on ait alors $\pi^{\Gamma'} = \{1\}$, et si ce n'était le cas, il faudrait l'introduire dans la définition – pour chaque opération de bouchage de trous relatif à $I' \subset I(\pi)$, et un choix d'un $i \in I'$, permettant de définir $\Gamma_{(I',i)} \rightarrow \mathcal{M}(\pi(I'))$ ³⁹.

Notons qu'une vraie action de Γ sur π (pas seulement extérieure) qui relève une action donnée “admissible”, est elle-même admissible (en ce sens qu'elle définit une action extérieure *admissible* sur un π' de type $(g, \nu + 1)$), si et seulement si cette action ou plutôt son germe, ne normalise aucun L_i ($i \in I(\pi)$), et qu'il en soit de même pour l'action induite sur chaque $\pi(I')$ ($I' \subset I = I(\pi)$) [il suffit de prendre les $\pi(I')$ pour I' de la forme $I \setminus \{j\}$, $j \in I$, du moins si $g \neq 0$] – et qu'enfin l'action de Γ^{\natural} sur $\pi'(I)$ (déduite de π' en bouchant les trous en I , de sorte que $\pi'(I)$ a une seule classe de lacets; $\pi'(I)$ se déduit aussi de l'action effective de Γ sur $\pi(I)$ – avec 0 classe de lacets – en faisant “un trou” correspondant – relatifs à un point $i \in I$), ne normalise pas de sous-groupe lacets... Mais je présume que la première condition (action de Γ^{\natural} ne normalisant aucun des L_i) implique les autres. Mais il faut dans la définition d'admissibilité aussi tenir compte de la condition (4°), qui implique l'existence de suffisamment de relèvements...

J'en arrive (péniblement!) à une

Conjecture provisoire profinie ⁴⁰ Pour Γ groupe profini donné, une action extérieure sur un (π, a) arithmétisé anabélien de type (g, ν) est dite *admissible*, si

- a) L'homomorphisme $\Gamma \rightarrow \Pi_a$ a une image ouverte
- b) Les actions *effectives* déduites par bouchages de trous ($i' \in I' \subset I = I(\pi)$) ne normalisent pas de sous-groupe à lacets.
- c) Il existe une infinité de classes de π -conjugaison de germes de scindages de l'extension de Γ par π , qui ne normalisent aucun sous-groupe à lacets de π ⁴¹ Cette condition c) exclut

³⁹Plus généralement, pour $i \in I' \subset I = I(\pi)$ on impose que la [??] action de Γ'_i sur $\pi(I')$ correspondant à i ne normalise aucun sous-groupe L_j ($j \in I \setminus I'$). On est ramené pour ceci au cas où $I' = I \setminus \{j\}$, donc où $\pi(I')$ n'a qu'une seule classe de lacets... (si $g \geq 1$)

⁴⁰Canulé, cf. plus bas...

⁴¹(***)

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

sans doute des cas comme $\Gamma = \mathcal{N}_{g,\nu}$ avec $(g, \nu) \neq (0, 3)$, car l'extension $\mathcal{M}_{g,\nu}$ de $\mathcal{N}_{g,\nu}$ par $\hat{\pi}_{g,\nu}$ n'admet sans doute pas de germe de scindage - ce qui est équivalent (?) au fait que $\mathcal{U}_{g,\nu}$ sur $\mathbb{M}_{g,\nu}$ n'admet pas de multisection étale....

Une action effective de Γ sur π est dite effective, si l'action extérieure est effective, et si elle ne normalise aucun sous-groupe à lacets.

Ceci posé:

a) Si Γ opère effectivement de façon admissible, on a

$$\pi^\Gamma = \{1\}$$

(peut-être même $\pi^{\Gamma^+} = \{1\}$).

b) Si $i \in I$ est stable par Γ opérant extérieurement de façon admissible, alors l'action effective sur $\pi' = \pi(i)$ ne normalise aucun L'_j ($j \in I \setminus \{i\}$).

c) Si Γ opère effectivement sur π de façon admissible, en laissant fixe $i \in I$, alors l'action correspondante effective (par passage au quotient) sur $\pi' = \pi(i)$ ne normalise aucun L_j , $j \in I \setminus \{i\}$.

d) Si Γ opère effectivement sur π de façon admissible, alors l'application

$$\mathrm{Pt}_{ad}(B_{\pi, \Gamma^\natural}) \rightarrow \mathrm{Pt}_{ad}(B_{\pi', \Gamma^\natural})$$

définie par c) est *injective*, et le complémentaire de son image est égal à $\{P\}$, où P est défini par le “trou” i .

Mais cette dernière partie de l'assertion, allant au-delà de la seule *injectivité* – et caractérisant l'image, me semble maintenant tout à fait douteuse – en effet, il suffit de regarder un schéma S de paramètres, de type fini sur \mathbb{Q} (un $K(\pi, 1)$ de préférence, par exemple une courbe algébrique) et de prendre pour Γ (non le groupe fondamental de son point générique, i.e. d'un corps, mais) le groupe fondamental de S lui-même. La donnée d'une action extérieure admissible de Γ sur un π correspond moralement à celle d'une famille de courbes \mathcal{U} de type g, ν paramétré par S .⁴² La condition c) est vérifiée par exemple si \mathcal{U} provient d'une courbe algébrique sur le corps de base lui-même, donc pas de problème – et il est manifeste

⁴²Les scindages d'extensions correspondent aux section de \mathcal{U} sur S .

A. GROTHENDIECK

que la surjectivité déconne. La difficulté provient du fait que deux actions *distinctes* de \mathcal{U} sur S peuvent ne pas être *disjointes*!

Il faut pouvoir parler de sections “strictement distinctes” i.e. distinctes en tout point de S – ce qui, en traduction profinie, revient à comparer deux scindages de l’extension de Γ par π , avec les germes de scindages sur $\Pi' \subset \Pi$ de Γ (en tant qu’extension de $\Pi_{\mathbb{Q}}$ par une partie géométrique) qui correspondent aux points de S – i.e. les (germes de scindage) *admissibles* justement. On a l’impression de tourner dans un cercle vicieux ou presque – il semblerait qu’il ne faudrait pas trop vouloir avaler à la fois – traiter d’emblée *tous* les groupes profinis Γ à la fois – mais plutôt se borner d’abord à ceux qui moralement, correspondent à des π_1 de schémas de type fini sur \mathbb{Q} , des $K(\pi, 1)$ disons, ou même des variétés élémentaires à la Artin – et dans les définitions resp. conjectures se tirer par les lacets des souliers, en récurrant sur la dimension. Au premier cran donc (dimension 0) on se bornerait à des actions de groupes Γ qui soient (modulo tout au moins passage à un sous-groupe ouvert) “arithmétiquement fidèles”, par exemple $\Gamma \rightarrow \Pi_a$ injectif. Dans ce cas-là, la conjecture telle qu’elle est énoncée tantôt semble raisonnable, ou du moins pas nécessairement déconnante. Le test décisif, il est vrai, serait la possibilité d’obtenir les “courbes” ainsi définies comme des revêtements de $\mathbb{P}^1 \setminus \{0, 1, \infty\} \dots$

§ 33. — DIGRESSION TOPOLOGIQUE

Anti-involutions des surfaces orientées algébroides

(⁴³) On appelle surface algébroïde une surface U de la forme $X \setminus S$, X surface compacte orientable, S fini. Alors X est déterminée à homéomorphisme unique près comme “compactifié pur” de U ; on la note \hat{U} . Les homéomorphismes de U avec lui-même s’identifient aux homéomorphismes de X qui appliquent S dans lui-même. Les orientations de X sont en correspondance 1-1 avec celles de U . Les anti-involutions de U (supposées orientées) sont en correspondance 1-1 avec celles de X qui conservent S .

On trouve alors une équivalence entre la catégorie des surfaces orientées algébroides U munies d’une anti-involution σ , et des surfaces à bord compactes Y , munies d’une partie finie T ; à (U, σ) correspond $(\hat{U}/\sigma, (\hat{U} \setminus U)/\sigma)$ – et à (Y, T) correspond $\tilde{Y} \setminus \tilde{T}$, où \tilde{Y} est le “double orienté” de Y (qui est une surface orientée compacte), et \tilde{T} est l’image inverse de T dans \tilde{Y} .

Nous nous intéressons maintenant au cas où U est connexe de type (g, ν) , en examinant d’abord le cas $\nu = 0$, i.e. $U = \hat{U}$, $S = \emptyset$ (auquel le cas général se ramènera). La condition $\nu = 0$ correspond au cas où $T = \emptyset$ – donc les $U = X$ envisagés s’identifient aux doublements orientés de certaines variétés à bord compactes Y . Lesquelles? Evidemment il faut que Y soit *connexe*, et *non orientable* ⁴⁴. Donc Y est caractérisé, à homéomorphisme près, par son genre

⁴³Finalement je ne regarde que les surfaces compactes – pourtant le cas non compact serait aussi très intéressant à regarder – pour essayer de retrouver par voie algébrique, sur l’automorphisme extérieur d’ordre 2 du π_1 , la disposition des “points à l’infini” de la courbe sur les composantes connexes de $X^\sigma = \hat{U}$.

⁴⁴Ce n’est pas vrai que Y soit nécessairement non orientable – seulement dans le cas où $X^\sigma = \emptyset$.

A. GROTHENDIECK

γ et le nombre μ des composantes connexes du bord – il peut se déduire du plan projectif réel Y_0 en y découpant γ rondelles disjointes, et y recollant des rubans de Möbius, puis en découpant encore μ rondelles ouvertes – ce qui donne

$$\begin{aligned}\chi(Y) &= \chi(Y_0) - \gamma \chi_!(\text{rondelles ouvertes}) + \gamma \chi_!(\text{rubans de Möbius ouverts}) \\ &\quad - \mu \chi_!(\text{rondelles ouvertes})\end{aligned}$$

[où $\chi(Y_0) = 1$ et $\chi_!(\text{rondelle ouverte}) = 1$]. Or le ruban de Möbius ouvert (dédit de Y_0 en enlevant une rondelle fermée) a un $\chi_!$ égal à $\chi(Y_0) - \chi_!(\text{rondelle fermée})$, soit $1 - 1 = 0$, d'où

$$(1) \quad \chi(Y) = 1 - (\gamma + \mu),$$

pour une surface Y compacte connexe avec un bord à μ composantes non orientable de genre γ .

D'autre part, on a

$$\chi(X) = \chi(X \setminus X^\sigma);$$

or X^σ est une réunion de cercles donc son χ est nul. Or, comme $X \setminus X^\sigma$ est un revêtement étale d'ordre 2 de Y , on a

$$\chi(X \setminus X^\sigma) = 2\chi(\text{Int}(Y))$$

enfin

$$\chi(Y) = \chi(Y \setminus \partial Y) = \chi(\text{Int}(Y));$$

pour la même raison que tantôt ($\chi(\partial Y) = 0$), d'où enfin

$$(2) \quad \chi(X) = 2\chi(Y) = 2(1 - (\gamma + \mu)),$$

ou encore, puisque $\chi(X) = 2 - 2g$

$$(3) \quad g = \gamma + \mu.$$

Donc on trouve

Proposition: ⁴⁵ La catégorie des surfaces orientées connexe compactes de genre g munies d'une anti-involution σ est équivalente à celle des variétés compactes à bord *non orientables*, de type (γ, ν) (γ le genre, μ le nombre de trous), avec $\gamma + \nu = g$.

⁴⁵Non, on ne trouve qu'une sous-catégorie pleine de celle de tous les (X, σ) . Il y a d'autre part aussi les doublements orientés $\coprod_{\partial Y} Y$ des surfaces *orientables* compactes à bord non vide – si Y est de type (γ, μ) , X est de genre g avec $g = 2\gamma + \mu - 1$ (ou $\gamma \geq 0$, $\mu \geq 1$).

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Corollaire: ⁴⁶ Il y a exactement $g + 1$ classes d'isomorphisme de systèmes (X, σ) , classifiés par $\sigma \leq \mu \leq g$, où $\mu = \text{card}(\pi_0(X^\sigma))$.

Si $X = X_g$ est une surface orientée compacte de genre g , cela signifie aussi que dans le groupe $A_g = \text{Aut}(X_g)$, il y a exactement $g + 1$ classes de conjugaison d'éléments σ satisfaisant

$$(4) \quad \sigma^2 = 1, \quad \text{sg}(\sigma) = +1$$

(i.e. qui soient des anti-involutions). Elles fournissent $g + 1$ classes de conjugaison d'éléments de $A_g/A_g^\circ = \mathfrak{X}_g$, satisfaisant les mêmes relations. Nous montrerons (on l'espère!) que ces classes sont distinctes et que tout $\sigma \in \mathfrak{X}_g$ satisfaisant les relations (4) est dans l'une de ces classes.

On admettra le

Lemme: Toute anti-involution du disque unité ou de \mathbb{C} est conjugué de $z \mapsto \bar{z}$, et par suite l'ensemble de ses points fixes est homomorphe à \mathbb{R} , et en particulier est *connexe*.

Théorème: Soit U une surface orientée séparée connexe, paracompacte, *non isomorphe* à S^2 , σ une anti-involution de U , \tilde{U} un revêtement universel de U , d'où $\pi = \text{Aut}(\tilde{U}/U)$ et une extension \mathcal{E} de $\mathbb{Z}/2\mathbb{Z}$ par π , formée des automorphismes topologiques de \tilde{U} compatibles avec la relation d'équivalence définie par $\tilde{U} \setminus U$, et induisant sur U l'automorphisme id_U ou σ . Alors:

a) (Pour mémoire) U^σ est une sous-variété fermée de U de dimension 1.

b) Pour tout $x \in U^\sigma$, on trouve une classe de π -conjugaison de scindages de l'extension \mathcal{E} , à la façon habituelle, d'où une application

$$(5) \quad U^\sigma \rightarrow \text{Sc}(\mathcal{E}, \mathbb{Z}/2),$$

où $\text{Sc}(\mathcal{E}, \mathbb{Z}/2)$ désigne l'ensemble des classes de π -conjugaison de scindages de \mathcal{E} sur $\mathbb{Z}/2\mathbb{Z}$, ou encore des éléments d'ordre 2 de \mathcal{E} qui ne sont pas dans π . Cette application se factorise en une *bijection*

$$(6) \quad \pi_0(U^\sigma) \simeq \text{Sc}(\mathcal{E}, \mathbb{Z}/2).$$

⁴⁶Ça ne marche qu'en se limitant aux (X, σ) tels que X/σ non orientable – cf. ci-contre (i.e. (*)) pour le cas orientable.

A. GROTHENDIECK

c) Soit Z_i une composante connexe de U^σ , correspondant à un scindage $\sigma_i \in \mathcal{E}^-$ d'ordre 2. Alors

$$(7) \quad \pi^{\sigma_i} = \{1\} \quad \text{si et seulement si} \quad Z_i \simeq \mathbb{R}.$$

d) Si $Z_i \not\simeq \mathbb{R}$, i.e. $Z_i \simeq S^1$, alors, pour une orientation choisie de Z_i , désignant par g_i l'élément de $\pi = \pi_1(U)$ qu'il définit (défini à conjugaison près), et par $\varphi_i : \mathbb{Z} \rightarrow \pi$ l'homomorphisme $\varphi_i(n) = g_i^n$ de \mathbb{Z} dans π , on a :

1°) φ_i est injectif;

2°) quitte à remplacer φ_i par un conjugué, on a

$$(8) \quad \pi^{\sigma_i} = \text{Im } \varphi_i.$$

Démonstration. On trouve l'application (5) en prenant, pour tout $x \in U^\sigma$, l'opération canonique de $\mathbb{Z}/2\mathbb{Z}$ sur le revêtement universel $\tilde{U}(x)$ ponctuée en x , et en prenant les opérations correspondantes sur \tilde{U} , déduites par les isomorphismes $\tilde{U} \simeq \tilde{U}(x)$. On voit que les opérations σ' obtenues sur \tilde{U} (pour x fixé) sont celles pour lesquelles $\tilde{U}^{\sigma'}$ a un point au-dessus de x – donc l'ensemble des x qui donnent naissance à la classe d'un σ' , sont les éléments de l'image de $\tilde{U}^{\sigma'}$ par la projection $\tilde{U} \rightarrow U$. Comme par le lemme $\tilde{U}^{\sigma'}$ est non vide et connexe, il s'ensuit que son image dans U^σ l'est aussi – on va voir que son image est exactement une composante connexe de U^σ – ce qui à la fois prouvera la factorisabilité de (5) par $\pi_0(U^\sigma)$ (assez triviale de toutes façons) et le fait que l'application déduite de (6) est *bijective*.

Soit \tilde{Z}_i un revêtement universel de Z_i , et prenons le revêtement universel correspondant \tilde{U}_i de U , de sorte qu'on a

$$(9) \quad \begin{array}{ccc} \tilde{Z}_i & \longrightarrow & \tilde{U}_i \\ \downarrow & & \downarrow \\ Z_i & \longrightarrow & U \end{array}$$

et par fonctorialité σ opère aussi sur ce diagramme (en opérant trivialement sur Z_i, \tilde{Z}_i), soit σ_i son opération sur \tilde{U}_i . On voit donc que \tilde{Z}_i s'envoie dans $\tilde{U}_i^{\sigma_i}$, qui s'envoie donc *sur* Z_i – ce qui achève déjà de prouver b).

Considérons l'image de \tilde{Z}_i dans $\tilde{U}_i|Z_i$; c'est une partie *ouverte* et fermée (comme image d'un homomorphisme de revêtements étales sur la même composante Z_i), donc c'est a fortiori une partie ouverte et fermée de $\tilde{U}_i^{\sigma_i}$, et comme cet espace est connexe, il lui est égal. De

plus $\tilde{Z}_i \rightarrow \tilde{U}^{\sigma_i}$ fait de Z_i un revêtement étale de son image $\tilde{U}_i^{\sigma_i}$ dans $\tilde{U}^{\sigma_i}|_{Z_i}$, et comme \tilde{U}^{σ_i} est simplement connexe, on trouve finalement

$$(10) \quad \tilde{Z}_i \xrightarrow{\sim} \tilde{U}_i^{\sigma_i}.$$

Lorsque Z_i est simplement connexe, i.e. $\tilde{Z}_i \simeq Z_i$, cela signifie aussi que $\tilde{U}_i^{\sigma_i}$ est un homéomorphisme (donc $\tilde{Z}_i = Z_i \rightarrow \tilde{U}_i^{\sigma_i}$ est l'homéomorphisme inverse). Comme, pour $x \in Z_i$ et $\tilde{x} \in (\tilde{U}_i^{\sigma_i})_x$, les \tilde{x}' de $\tilde{U}_i^{\sigma_i}$ au-dessus de x sont les éléments de la forme $\tilde{x}\gamma$, avec $\gamma \in \pi_i^{\sigma_i}$ ($\pi_i = \text{Aut}(\tilde{U}_i/U)$), il s'ensuit que l'on a bien

$$(11) \quad \pi_i^{\sigma_i} = 1$$

ce qui est essentiellement la formule (7). Dans le cas Z_i non simplement connexe, posant

$$(12) \quad T_i = \text{Aut}(\tilde{Z}_i/Z_i) \simeq \pi_1(Z_i; \tilde{Z}_i)$$

on trouve un homomorphisme canonique

$$(13) \quad \varphi_i : T_i \rightarrow \pi_i$$

et l'injectivité dans (10) équivaut au fait que (13) est injectif. Bien entendu, le choix d'un générateur g_i° de T_i équivaut au choix d'une orientation de Z_i , et $g_i = \varphi_i(g_i^\circ) \in \pi$ est alors l'élément correspondant de $\pi_1(U)$ dont il est question dans l'énoncé (moins précis, car on n'y parle que de classe de conjugaison). Il est clair que σ_i (opérant trivialement sur T_i , et sur π_i par transport de structure) commute à l'homomorphisme injectif φ_i , donc φ_i induit $T_i \rightarrow \pi_i^{\sigma_i}$. Je dis que c'est en fait un *isomorphisme*

$$(14) \quad \varphi_i : T_i \xrightarrow{\sim} \pi_i^{\sigma_i}$$

– il reste à prouver la surjectivité. Mais si $\gamma \in \pi_i^{\sigma_i}$, alors $\tilde{x}\gamma \in \tilde{U}_i^{\sigma_i}$, donc $\tilde{x}\gamma \in \varphi_i(\tilde{Z}_i)$ ce qui signifie que $\tilde{x}\gamma = \tilde{x}\varphi_i(g)$ pour $g \in T_i$, donc $\gamma \in \text{Im } \varphi_i$, cqfd.

Corollaire 1: Soit $\sigma_i \in \mathfrak{S}_g$ ($1 \leq i \leq g$), correspondant à une anti-involution σ_i de X_g telle que $\text{Card } \pi_0(X_g^{\sigma_i}) = i$ et X_g/σ non orientable. Alors

a) Il y a exactement i classes de π_g -conjugaison d'automorphismes effectifs d'ordre 2 de π_g dans la classe σ_i (ce qui prouve que si $i \neq j$, σ_i et σ_j ne sont pas conjugués dans \mathfrak{S}_g ...);

A. GROTHENDIECK

b) Si $u_i \in \mathfrak{S}_g = \text{Aut}_{\text{lac}}(\pi_g)$ est d'ordre 2 dans la classe σ_i , alors

$$(14) \quad \pi_g \simeq \mathbb{Z};$$

c) Si $u_i, u'_i \in \mathfrak{S}_g$ sont d'ordre 2, de classe σ_i , alors $\exists h \in \mathfrak{S}_g^+$ tel que

$$(15) \quad u'_i = h u_i h^{-1} = \text{int}(h) u_i.$$

(NB. Nécessairement, l'image de h dans \mathfrak{Z}_g^+ sera dans $(\mathfrak{Z}_g^+)^{\sigma_i} = \text{Centr}_{\mathfrak{Z}_g}(\sigma_i)^+$.)

Démonstration. a) et b) sont des cas particuliers du théorème, appliqué à une anti-involution σ_i de X_g , avec $\pi_0(X_g^{\sigma_i})$ de cardinal i . Soit $Y_{g,i} = X_g^{\sigma_i}$ surface compacte à bord non orientable connexe de type $(g-i, i)$; il est bien connu et immédiat que le groupe des automorphismes d'une telle variété est transitif sur $\pi_0(\partial Y)$, donc en remontant à (X_g, σ_i) , que le groupe des automorphismes de (X_g, σ_i) est transitif sur $\pi_0(X_g^{\sigma_i})$, qu'on peut interpréter aussi comme l'ensemble des classes de π_g -conjugaison de u_i , comme dans b), c). Cela implique donc qu'il existe $\dot{h} \in \mathfrak{Z}_g^+$, commutant à σ_i , tel que – désignant par h un relèvement dans \mathfrak{S}_g^+ – on ait $u'_i \pi$ -conjugué à $\text{int}(h)u_i$, ce qui signifie aussi qu'on peut (quitte à modifier h) le choisir de façon qu'on ait (15).

Corollaire 2: Sous les conditions du corollaire précédent, posant $\pi_g^{u_i} = T (\simeq \mathbb{Z})$, on a un diagramme de suites exactes

$$(16) \quad \begin{array}{ccccccc} 1 & \longrightarrow & T & \longrightarrow & \mathfrak{S}_g^{+u_i} & \longrightarrow & \mathfrak{Z}_g^{+\sigma_i} \\ & & \parallel & & \downarrow & & \downarrow \\ 1 & \longrightarrow & T & \longrightarrow & \mathfrak{S}_g^{u_i} & \longrightarrow & \mathfrak{Z}_g^{\sigma_i} \end{array}$$

et l'indice de $\mathfrak{S}_g^{+u_i}$ dans $\mathfrak{Z}_g^{+\sigma_i}$ (et de $\mathfrak{S}_g^{u_i}$ dans $\mathfrak{Z}_g^{\sigma_i}$) est i .

Comme les deux dernières flèches verticales sont des inclusions de sous-groupes d'indice 2, il suffit de traiter l'assertion concernant $\mathfrak{S}_g^+, \mathfrak{Z}_g^+$. Or $\mathfrak{Z}_g^{+\sigma_i}$ opère trivialement sur l'ensemble des classes de π -conjugaison de u'_i , d'après c); d'autre part le stabilisateur dans $\mathfrak{Z}_g^{+\sigma_i}$, pour cette action, de u_i , est formé des $\dot{\gamma} \in \mathfrak{Z}_g^{+\sigma_i}$ tels que $\text{int}(\gamma)u_i$ soit π -conjugué à u_i , i.e. tels qu'il existe $\alpha \in \pi$, avec $\text{int}(\gamma)u_i = \text{int}(\alpha)u_i$, i.e. $\alpha^{-1}\gamma \in \mathfrak{S}_g^{+u_i}$, ce qui signifie que $\dot{\gamma}$ est dans l'image de $\mathfrak{S}_g^{+u_i}$, cqfd.

J'ai envie de construire une figure géométrique où on puisse mettre en évidence simultanément des anti-involutions topologiques qui donnent naissance aux $\sigma_i \in \mathfrak{Z}_g$ (à conjugaison

près, et aux divers $u_i \in \mathfrak{S}_g$ associés à un σ_i (ce qui sera alors facile, par la recette générale). Nous savons que $\sigma_i \in \mathfrak{S}_g$ s'obtient en regardant un X_g comme doublement orienté d'un $Y = Y_{g-i,i}$, donc en partant du plan projectif réel Y_0 , en y faisant g trous, dont on rebouche $g-i$ par des rubans de Möbius, en laissant les i autres trous tels quels. Soient D_j ($1 \leq j \leq g$) les disques disjoints fermés correspondant aux "trous" donc

$$(17) \quad V_{0,j} = Y_0 \setminus \cup_j D_j^\circ$$

est une variété à bord (non orientable), contenue à la fois dans Y_0 et dans $Y = Y_{g-i,i}$, et coïncidant même avec Y en les points de

$$\partial Y = \bigcup_{g-i+1 \leq j \leq g} \partial D_j.$$

Soit X_0 la sphère orientée qui revêt Y_0 , et $U_0 = X_0 \setminus V_0$ sa restriction sur $\cup D_j$, c'est donc le complémentaire d'une réunion de $2g$ disques

$$(18) \quad U_0 = X_0 \setminus \bigcup_{1 \leq j \leq g} \Delta_j$$

où $\Delta_j \rightarrow D_j$ est un revêtement trivial à 2 feuillets de D_j ($\Delta_j = \Delta'_j \amalg \Delta''_j \simeq D_j \times \varepsilon_j$, où ε_j est un ensemble à 2 éléments qui s'identifie à l'ensemble des deux orientations de D_j ,...). Soit d'autre part M_j ($1 \leq j \leq g-i$) le ruban de Möbius dont le bord a été recollé à V_0 par un homomorphisme

$$(19) \quad \partial M_j \simeq \partial D_j.$$

Soit

$$(20) \quad M = \coprod_{1 \leq j \leq g-i} M_j$$

de sorte que

$$(21) \quad Y_{g-i,i} = V_0 \amalg_{\partial M} M.$$

Soit donc $X = X_g$ le doublement orienté de $Y_{g-i,i}$ défini par (21), soit $\tilde{M} = \coprod_{1 \leq j \leq g} \tilde{M}_j$ l'image inverse de M dedans, qui est un revêtement étale de degré 2 de M :

$$(22) \quad X_{g,i} = X_g \setminus \text{Int}(\tilde{M}),$$

A. GROTHENDIECK

et on aura

$$(23) \quad X_g = X_{g,i} \amalg_{\partial \tilde{M}} \tilde{M}$$

pour un homéomorphisme bien déterminé de $\partial \tilde{M}$ avec une partie ouverte et fermée de $\partial X_{g,i}$. D'ailleurs, on aura une application continue canonique:

$$(24) \quad \mathcal{U}_0 \rightarrow X_{g,i}$$

qui définit un homéomorphisme de $X_{g,i}$ avec la surface obtenue en contractant les $\partial \Delta_j \subset \mathcal{U}_0$ ($\partial \Delta_j = (\partial D_j) \times \varepsilon_j$), pour $g-i+1 \leq j \leq g$ à l'aide des projections $\partial \Delta_j \simeq (\partial D_j) \times \varepsilon_j \rightarrow D_j$.

D'autre part, chaque \tilde{M}_j ($1 \leq j \leq g-i$), revêtement des orientations du ruban du Möbius, est isomorphe au cylindre $S^1 \times I$, et son anti-involution canonique est sans point fixe, et s'identifie à $(z, t) \rightarrow (-z, -t)$ (où S^1 est identifié aux nombres complexes de module 1, et I à $[-1, +1]$). D'ailleurs, X_0 orienté avec son anti-involution de revêtement de Y_0 s'identifie à la sphère ordinaire (dans un espace vectoriel euclidien de dimension 3), avec l'anti-involution $x \mapsto -x$. En résumé:

Proposition: On peut obtenir (pour $1 \leq i \leq g$ fixé) les couples (X_g, σ_i) , à homéomorphisme près, en prenant la sphère (euclidienne orientée) X_0 , avec son antipodisme standard τ , en prenant un ensemble de $2g$ disques D_j ($j \in J$) mutuellement disjoints, stable par τ , et une partie $I' \subset J/\tau = I$ (I de cardinal g) avec $\text{card}(I') = i$, et en procédant ainsi: pour tout $j \in I$, soient $\Delta_j = D'_j \cup D''_j$ la réunion des deux disques correspondants, et $S_j = \partial \Delta_j / \tau$, de sorte que S_j est un cercle; soit

$$T_j = S_j \times I^{\varepsilon_j}$$

(où $I = [-1, +1]$, $\varepsilon_j = \{j \in I \mid j \text{ sur } i\} \simeq$ l'ensemble des orientations de S_i , I^{ε_j} tordu par ε_j , de sorte qu'on a un homéomorphisme canonique:

$$(25) \quad \partial T_j \simeq \partial \Delta_j,$$

de sorte que $X_g = \mathcal{U}_0 \amalg_{\partial \Delta} T$ (où $\Delta = \coprod_1^g \Delta_j$, $T = \coprod_1^g T_j$) est *orientée*. [NB. T_j est canoniquement orienté et l'isomorphisme (25) *respecte* comme il se doit l'orientation, i.e. $\partial T \simeq \partial V_0$ la renverse.] Ceci posé, l'antipodisme τ induit sur chaque $\tilde{M}_i \simeq S_j \times \varepsilon_j$ l'anti-involution canonique provenant de cette expression des ∂T_i , qui échange les deux composantes connexes. Pour tout $j \in I$, on prolonge $\dot{\tau}|_{\partial T_j}$ à T_j en deux anti-involutions $\dot{\tau}_j, \dot{\tau}'_j$ de T_j de telle façon que

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

a) $\dot{\tau}_j$ soit sans points fixes,

b) $\dot{\tau}'_j$ ait un ensemble de points fixes homéomorphe à S_j par la projection $T_j^{\dot{\tau}'_j} \rightarrow S_j$ (cf. plus bas pour des choix particuliers explicites – on verra qu'on peut même supposer $T_j^{\dot{\tau}'_j} = S_j \times \{0\}$).

Soit, pour toute partie $I' \subset I$, $\tau_{I'}$ l'anti-involution de $X_g = V_0 \amalg_{\partial T} T$ (où $V_0 = X_0 \setminus \bigcup_{j \in J} D'_j$) qui coïncide avec τ sur V_0 , avec τ'_j sur T_j pour $j \in I'$, avec τ_j pour $j \in I \setminus I'$. Alors on a

$$(26) \quad X_g^{(\tau_{I'})} = \bigcup_{j \in I'} (S_j \times \{0\})$$

donc si $\text{card}(I') = i$ ($0 \leq i \leq g$), alors $\tau_{I'}$ est un σ_i .

Choix de $\dot{\tau}_j, \dot{\tau}'_j$. On choisit un isomorphisme $S_j \simeq U \stackrel{\text{def}}{=} \{z \in \mathbb{C} \mid |z| = 1\}$, d'où une orientation de S_j , et une bijection $\varepsilon_j \simeq \{\pm 1\}$, d'où $I^{\varepsilon_j} \simeq I = [-1, +1]$ et on prend

$$(27) \quad \dot{\tau}(z, t) = (-z \exp(i\pi t), -t) \dot{\tau}'(z, t) = (z, -t).$$

[NB. Pour la définition des $\dot{\tau}'_j$, on n'a pas besoin du choix d'un isomorphisme $S_j \simeq U$.]

On a bien $\dot{\tau}^2 = \dot{\tau}'^2 = id$, $\dot{\tau}|\partial\tau = \dot{\tau}'|\partial\tau = \tau|\partial\tau$.

D'ailleurs on note que:

$$(\dot{\tau}'\dot{\tau})^2 = \dot{\tau}'\dot{\tau}\dot{\tau}'\dot{\tau} = ((z, t) \mapsto (z \exp(2i\pi t), t)).$$

Ce n'est pas l'application identique – l'ensemble de ses points fixes est égal à l'ensemble des (z, t) tels que $t \in \{-1, 0, +1\}$ – i.e.

$$(28) \quad T_j^{(\dot{\tau}'_j\dot{\tau}_j)^2} = S_j \times [\partial I^{\varepsilon_j} \cup \{0\}].$$

Soit

$$(29) \quad \dot{\rho}_j = \dot{\tau}'_j\dot{\tau}_j, [(z, t) \mapsto (-z \exp(i\pi t), t)]$$

– c'est un automorphisme de T_j qui est l'identité sur ∂T_j . Pour toute partie I' de $I = J/\tau$, soit

$$(30) \quad \rho_{I'} = \text{l'automorphisme de } X_g \text{ qui est l'identité sur } V_0 = X_g \setminus \bigcup_{j \in I \setminus I'} T_j,$$

A. GROTHENDIECK

et qui est ρ_j sur T_j pour $j \in I'^{47}$.

On aura donc

$$(32) \quad \tau_{I'} \tau_{I''} = \rho_{I'_0} \rho_{I''_0}^{-1}$$

où $I'_0 = I' \setminus I' \cap I''$, $I''_0 = I'' \setminus I' \cap I''$; d'autre part on aura évidemment

$$(33) \quad [\rho_J, \rho_K] = 1 \text{ pour } J, K \subset I.$$

Remarque: Au lieu d'un isomorphisme $S_j \simeq \mathbb{U}$ supposons donné plutôt sur S_j une structure de torseur sous $\mathbb{U}^{\varepsilon_j}$ (\mathbb{U} tordu par ε_j , grâce à l'automorphisme d'ordre 2, $z \mapsto z^{-1} = \bar{z}$ de \mathbb{U}). On peut donc définir

$$(36 \text{ [sic]}) \quad \exp : \mathbb{R}^{\varepsilon_j} \rightarrow \mathbb{U}^{\varepsilon_j}$$

où $I_j^\varepsilon \subset \mathbb{R}^{\varepsilon_j}$, de façon évidente, d'où des anti-involutions $\dot{\tau}_j, \dot{\tau}'_j : T_j \xrightarrow{\sim} T_j$ par les formules (27).

Si par exemple on choisit des disques D'_j tels que leurs bords soient des *cercles* euclidiens, alors il y a sur chaque $\partial D'_j$ une structure de torseur sous un groupe $\mathbb{U}^{\varepsilon_j}$, invariante par antipodisme, et qui passe donc au quotient. Dès lors tout automorphisme de $(X_0, (D'_j))$ qui respecte cette structure supplémentaire de torseur – et notamment tout automorphisme qui respecte la structure *métrique*, opère sur X_g en commutant au système des τ_j, τ'_j au sens évident.

Egalement, si on retient sur X la structure conforme seulement, et si on choisit dans chaque D_j un “centre” a_j , de façon compatible avec l'involution, alors le choix des $a_j \in \text{Int}(D'_j)$ définit une structure de torseur sur M_j et ces structures sont invariantes par transformations conformes qui respectent l'ensemble de points a_j . [NB. On ne suppose plus nécessairement que (∂D_j) soit un cercle, seulement que ∂D_j pas trop sauvage. Si ∂D_j est un cercle cette définition coïncide avec la précédente si et seulement si a_j est le centre du cercle.]

Pour définir τ_j sur T_j , il suffit de nettement moins de données que d'une structure de torseur topologique sur T_j . Ecrivant, pour $(z, t) \in S_j \times I^{\varepsilon_j}$

$$(37) \quad \tau_j(z, t) = (u_t(z), -t)$$

⁴⁷Posant $\rho_j = \rho_{\{j\}}$, on aura simplement $\rho_J = \prod_{j \in J} \rho_j$. Sauf erreur, ρ_j engendre le groupe $\text{ST}^{!+}(T_j)(??) \simeq \mathbb{Z}$, donc les ρ_j engendrent un groupe $\simeq \mathbb{Z}^I$. NB. On a $\rho_j = \tau_{\{j\}} \tau_\emptyset$.

où $u_t : S_j \xrightarrow{\sim} S_j$ est un homéomorphisme dépendant continûment de t , écrivant que $\tau_j|_{\partial T_j} = \tau|_{\partial T_j}$ on trouve la condition

a) $u_t = \text{id}$ si $t \in \partial I^{\varepsilon_j} \simeq \varepsilon_j$ (ça s'écrit, si S_j est orienté, $u_1 = u_{-1} = 0$);

écrivant que $\tau_j^2 = \text{id}$, on trouve la condition

b) $u_{-t} = u_t^{-1}$ ($t \in I^{\varepsilon_j}$),

et écrivant que $T_j^{\tau_j} = \emptyset$ on trouve la condition

c) u_0 sans points fixes.

Si une orientation est choisie, les $j \mapsto u_j$ satisfaisant a), b), c) correspondent aux applications $[0, 1] \rightarrow \text{Aut}(S_j)$ par $t \mapsto u_t$, telles que $u_1 = \text{id}$, u_0 sans point fixe et d'ordre 2 (le cas envisagé plus haut est celui-ci où $t \mapsto u_{1-t}$ provient d'une représentation continue $\mathbb{R} \mapsto \text{Aut}(S_j)$).

Remarques: On peut se proposer de déterminer la structure de toutes les anti-involutions τ , sur un cylindre orienté $T \simeq S \times I^{\varepsilon_j}$ ($\varepsilon = \text{Or}(S)$) qui n'ont pas de point fixe sur le bord – ce qui implique déjà que τ permute les deux composantes connexes du bord. Plus généralement, les anti-involutions τ d'une surface à bord orientée X , n'ayant pas de point fixe sur ∂X , correspondent aux variétés à bord munies d'une partie à la fois ouverte et fermée $(\partial Y)'$ de ∂Y – en associant à une telle $(Y, (\partial Y)')$ son “doublement” orienté relativement à $(\partial Y)'$ – à X, σ correspondant $(X/\sigma, \text{Im} X^\sigma \rightarrow X/\sigma)$. Si X est connexe compact, Y est compacte *non orientable*⁴⁸; supposons que son type soit (γ, j) , et soit $i = \text{card}(\pi_0((\partial Y)')) = \text{card}(\pi_0(X^\sigma))$. Donc $0 \leq i \leq j$, et $\chi(Y) = 1 - (\gamma + j)$, et on voit de suite que

$$\chi(X) = \chi_!(X \setminus (X|\partial Y)) = \chi_!(X|\text{Int}(Y))$$

(car le χ d'un cercle est nul)

$$= 2\chi_!(\text{Int}(Y)) = 2\chi(Y) = 2(1 - (\gamma + j));$$

donc si X est de type (g, ν) , on aura $\chi(X) = 2 - 2g, 2 - 2g - \nu = 2(1 - (\gamma + j))$, i.e.

$$(38) \quad g + \nu/2 = \gamma + j$$

⁴⁸Pas vrai! Si Y est orientable de type (γ, j) , avec $0 \leq i \leq j$, on aura $g + \nu/2 = 2\gamma + j - 1, \nu = 2(j - i)$, i.e. $i = j - \nu/2$ comme dans le cas ci-contre [celui du texte qui suit].

A. GROTHENDIECK

(cela exige que ν soit pair, ce qui était évident a priori, car σ doit permuter les éléments de $\pi_0(\partial X)$ entre eux, sans y avoir de points fixes...). Mais j'ai oublié de noter que ν est déterminé en fonction de (γ, j, i) où $i = \text{card}((\partial Y)')$ par

$$(39) \quad \nu = 2(j - i),$$

i.e. $i = j - \nu/2$. Donc il faut ici (pour $g = 0, \nu = 2$) chercher (γ, j, i) avec $\gamma \in \mathbb{N}, 0 \leq i \leq j \in \mathbb{N}$, tels que l'on ait $\nu = 2(j - i)$, i.e. $j - i = 1$ i.e. $i = j - 1$, et $\gamma + j = 1$, ce qui donne la seule possibilité (comme $i \geq 0$, donc $j \geq 1$)

$$\text{a) } \gamma = 0, j = 1, i = 0.$$

Le cas a) correspond au cas où $T^\sigma = \emptyset$; il se déduit du plan projectif réel en y faisant un trou à bord (d'où ruban de Möbius), et en prenant le doublement orienté.

Le cas où $T^\sigma \neq \emptyset$ donnera nécessairement un quotient Y orienté, on doit avoir que pour son type $(\gamma, [??])$, le seul cas:

$$\text{b) } \gamma = 0, j = 2, i = 1 \text{ (quotient orienté)}$$

déduit de la sphère à deux trous, i.e. du cylindre, en prenant le doublement orienté par rapport à *un* des trous.

C'est bien les deux cas donnés respectivement par $\dot{\tau}$ et $\dot{\tau}'$ dans les formules (27).

Je voudrais maintenant construire une situation sous les conditions de la proposition mettant en évidence un maximum de symétries – il est vrai que l'on pourrait travailler avec tous les automorphismes de X_0 commutant à l'antipodisme τ , invariant l'ensemble des D_j , et respectant (disons) des structures de torseur topologique sur l'ensemble des ∂D_j – ou ce qui revient naturellement au même (à indétermination de multiplication par 2 près) ⁴⁹ les automorphismes de Y_0 qui invarient $D = \cup_{i \in I} D_i$, et respectent des structures de torseur sur les composantes connexes ∂D_j de ∂D . On prévoit que (travaillant modulo isotopie) on aura un groupe qui sera voisin d'un groupe de tresses, et sans doute calculable sans grand mal – et en le mettant ensemble avec le groupe engendré par les opérateurs précédents, on trouvera peut-être un démarrage pour engendrer par exemple \mathfrak{Z}_g par générateurs (anti-involutifs) et relations.

⁴⁹Non, *sans* indétermination, en relevant à la sphère de façon à repsecter l'orientation.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Considérons le sous-groupe \mathcal{G} de $A_g = \text{Aut}(X_g)$ engendré par les $\tau_{I'}$, $I' \subset I$. Soit \mathcal{H} le sous-groupe engendré par les ρ_j , ($j \in I$). On a

$$\tau_{I'} \rho_j \tau_{I'} = \tau_{I'} (\tau_{\{j\}} \tau_{\emptyset}) \tau_{I'} = (\tau_{I'} \tau_{\{j\}}) (\tau_{\emptyset} \tau_{I'}) \in \mathcal{H}$$

par la formule (32) donc \mathcal{H} est un sous-groupe invariant. Les formules (32) montrent que \mathcal{G}/\mathcal{H} est un groupe *commutatif*, et même qu'il est isomorphe à ± 1 par le caractère d'orientation tous les τ'_I sont égaux mod \mathcal{H}).

Considérons comme élément de référence de \mathcal{H} l'élément

$$(40) \quad \tau = \tau_{\emptyset}$$

(anti-involution sans points fixes de X_g). On trouve alors par (32) que pour $I' \subset I$,

$$(41) \quad \tau_{I'} = \rho_{I'} \tau = \left(\prod_{j \in I'} \rho_j \right) \cdot \tau^{50},$$

d'ailleurs on aura, pour $j \in I$,

$$\tau \rho_i \tau = \tau_{\emptyset} (\tau_{\{i\}} \tau_{\emptyset}) \tau_{\emptyset} = \tau_{\emptyset} \tau_{\{i\}} = \rho_i^{-1}$$

$$(42) \quad \tau \rho_i \tau^{-1} = \rho_i^{-1}.$$

Ainsi \mathcal{G} apparait comme le produit semi-direct de $\mathcal{H} \simeq \mathbb{Z}^I$, et de $\{\pm 1\} \simeq \{1, \tau\}$ y opérant par la symétrie $\rho \mapsto \rho^{-1}$. Donc pour *tout* $\rho \in \mathcal{H}$, on a $(\tau \rho)^2 = 1$, i.e. pour tout $\sigma \in \mathcal{H}^{-1}$, σ est une *anti-involution*. Comme σ coïncide avec τ sur $V_0 = X_g \setminus \cup_{i \in I} \text{Int}(T_i)$, on voit que l'ensemble des points fixes de σ est contenu dans $\cup_{i \in I} \text{Int}(T_i)$, et pour calculer l'indice de σ , i.e. $\text{card}(\pi_0(X_g^\sigma))$, il suffit de prendre la somme des indices dans les T_j . Or dans T_j , on a par (29) $\rho_j(z, t) = (-z \exp(i\pi t), t)$, et par récurrence,

$$(43) \quad \rho_j^{n_j}(z, t) = ((-1)^{n_j} z \exp(i\pi n_j t), t)$$

donc

$$(44) \quad \tau \rho_j^{n_j}(z, t) = ((-1)^{n_j+1} z \exp(i\pi(n_j+1)t), -t)$$

⁵⁰On veut du reste, comme $\tau^2 = 1$, $\tau_{I'}^2 = 1$, que $\tau_{I'} = \tau_{I'}^{-1} = \tau \rho_{I'}^{-1}$ donc $\tau \rho_{I'} \tau = \rho_{I'}^{-1}$, ce qui est (42).

A. GROTHENDIECK

et $(z, t) \in T_j$ est point fixe de $\tau \rho_j^{n_j}$ si et seulement si $t = 0$, et n_j est *impair*, donc

$$T_j^{\tau \rho_j^{n_j}} = \emptyset \text{ si}$$

n_j pair $S_j \times \{0\}$ si n_j impair (45)

donc

Indice de $u = \tau \prod_j \rho_j^{n_j} = (46) \quad = \text{cardinal de l'ensemble } I'_n \text{ des } j \in I \text{ tels que } n_j \text{ soit impair.}$

Il en résulte pour des raisons générales que u est conjugué dans $A_g = \text{Aut}(X_g)$ (par un élément de A_g^+) à $\tau_{I'} = \rho_{I'} \tau = \tau \rho_{I'}^{-1}$, ou aussi $\rho_{I'}^{-1} \tau = \tau \rho_{I'}$.

Mais si $\tau \rho', \tau \rho'' \in \mathcal{G}$, $(\rho', \rho'' \in \mathcal{H})$, et si $\rho \in \mathcal{H}$, la relation

$$\rho(\tau \rho') \rho^{-1} = \tau \rho''$$

équivalent à

$$\tau \rho \tau \rho' \rho^{-1} = \rho''$$

(où $\tau \rho \tau = \rho^{-1}$), i.e. $\rho^2 = \rho' \rho''^{-1}$; donc $\tau \rho'$ et $\tau \rho''$ sont conjugués par un élément de \mathcal{H} si et seulement si $\rho' \rho''^{-1} \in \mathcal{H}^2$ – ce qui précise l'observation précédente...

La façon la plus riche en symétries simples pour disposer les $2g$ trous antipodiques D_j me semble la suivante. On considère la sphère euclidienne, avec l'action du groupe diédral \mathbb{D}_{2g} – par exemple quand c'est la sphère de Riemann qui est considérée comme riemannienne, par le choix de antipodisme comme étant

$$\tau z = -\frac{1}{\bar{z}}; (47)$$

on prend l'action type du groupe diédral (avec comme pôles les points $0, \infty$, et comme équateur le cercle unité $U = \{z \in \mathbb{C} \mid |z| = 1\}$), en écrivant \mathbb{D}_n comme $\subset O(2, \mathbb{R})$, comme produit semi-direct de $\{\pm 1\}$ par $\mu_n(\mathbb{C}) = \mu_n$, le couple (ξ, α) ($\xi \in \mu_n, \alpha \in \{\pm 1\}$) opérant par $(\xi, \alpha)(z) = \xi z^\alpha$. On peut d'ailleurs l'élargir en un groupe $\tilde{\mathbb{D}}_n \simeq \mathbb{D}_n \times \mathbb{Z}/2\mathbb{Z}$, où le deuxième facteur $\mathbb{Z}/2\mathbb{Z}$ est engendré par l'antipodisme (47) (qui commute à \mathbb{D}_n – de même d'ailleurs que l'anti-involution $z \mapsto 1/\bar{z}$, qui a comme ensemble de points fixes U et n'est autre que la symétrie par rapport à l'équateur, leur composé $z \mapsto -z$ étant la symétrie par rapport à l'axe des pôles...) donc on regarde les transformations

$$u_{\xi, \alpha, \beta} = u_{\xi, \alpha} \tau^\beta, \quad \xi \in \mu_n, \alpha \in \{\pm 1\}, \beta \in \mathbb{Z}/2\mathbb{Z},$$

donc

$$u_{\xi, \alpha, \beta} z = u_{\xi, \alpha}(z) = \xi z^\alpha s i$$

$$\beta = 0 u_{\xi, \alpha}(\frac{-1}{z}) = -\xi \bar{z}^{-\alpha} s i \beta = 1$$

maison sera appelée

τ renverse l'orientation, donc est à manier avec réserve pour ce qui concerne le “transport de structure” dans la situation présente. Ici $n = 2g$, \mathbb{D}_{2g} est d'ordre $4g$, et $\tilde{\mathbb{D}}_n$ d'ordre $8g$. On prend sur l'équateur une trajectoire de $\mu_n = \mu_{2g}$, par exemple justement l'ensemble μ_{2g} , de racines $2g$ -ièmes de l'unité lui-même (en tant que sous-ensemble de la sphère) comme l'ensemble des “centres” des disques D'_i . On choisit un disque D'_0 autour du point P_0 (assez petit pour ce qui va suivre)⁵¹, et on prend les transformés de D'_0 par les $\xi \in \mu_n$. Ces choix étant faits, la surface X_g est déterminée sans ambiguïté, et le groupe \mathbb{D}_{2g} y opère par transport de structure, en permutant entre eux les g cylindres T_i , correspondant aux éléments de $J/\tau = J/\{\pm 1\}$, i.e. aux paires d'éléments antipodiques de S , i.e. aux “diagonales” du polygone à 2μ côtés qu'ils déterminent sur l'équateur. Le groupe \mathbb{D}_{2g} normalise le groupe G ; de façon précise on aura, pour $u \in \mathbb{D}_{2g}$,

$$u \tau_{I'} u^{-1} = \tau_{u(I')}(49)$$

pour $I' \subset I = J/\tau$, en tenant compte de l'opération de \mathbb{D}_{2g} sur I . On aura donc en particulier, désignant par $\tau_g = \tau_\emptyset$ l'extension de l'antipodisme de la sphère X_0 (ou plutôt de $\tau|_{V_0}$) en un antipodisme sans points fixes de X_g , noté τ précédemment

$$u \tau_g u^{-1} = \tau_g(50)$$

i.e. τ_g commute à l'action de \mathbb{D}_n , et

$$u \rho_j u^{-1} = \rho_{u(j)}.(51)$$

On peut donc dire que \mathbb{D}_{2g} opère sur \mathcal{G} , d'où un produit semi-direct $\mathbb{D}_{2g} \cdot \mathcal{G}$, qui opère donc sur X_g .

Quant à la question de prolonger de même l'action sur X_0 de $\tilde{\mathbb{D}}_{2g}$ tout entier en une action sur X_g , ça a été fait sans crier gare, à τ_{X_0} correspondant naturellement $\tau_{X_g} = \tau_g$, qui a

⁵¹Il faut simplement que D'_0 ne rencontre pas $\xi D'_0$, où $\xi = \exp(2i\pi/2g)$.

A. GROTHENDIECK

en effet le bon goût de commuter à l'action de \mathbb{D}_{2g} . [Il pourrait sembler plus naturel, il est vrai, dans un esprit de “transport de structure (envers et contre tout?)”, de faire correspondre à τ_{X_0} l'opération τ_I donnée par (27), qui en chaque T_j serait égal à τ_j (et sur V_0 , bien sûr, coïncide avec τ_{X_0}), $\tau_j(z, t) = (z, -t)$, l'ensemble des points fixes de τ_I étant formé des g cercles médians $S_j \times \{0\}$ des g tubes T_j . On aura par (41) $\tau_I = \rho_I \tau_g$, donc τ_I commute également à \mathbb{D}_n , puisque τ et $\rho_I = \prod_{i \in I} \rho_i$ y commutent. Mais il ne semble pas important pour le moment quelle convention nous adoptons.] On peut donc dire aussi que le groupe $\tilde{\mathbb{D}}_{2g}$ opère sur \mathcal{H} – cette opération prolongeant celle de τ_g , identifié maintenant à un élément de $\tilde{\mathbb{D}}_{2g}$, i.e. à l'antipodisme dans $\tilde{\mathbb{D}}_{2g}$ – et le produit semi-direct

$$\tilde{\mathbb{D}}_{2g} \cdot \mathcal{H} \supset \mathcal{G} = \langle 1, \tau_g \rangle \cdot \mathcal{H} \quad (52)$$

opère sur X_g .

Il faudrait maintenant, dans cette voie:

1) Expliciter l'action extérieure de ce produit semi-direct sur le groupe fondamental π_g , avec une attention toute particulière à l'action du groupe $(\mathbb{Z}/2\mathbb{Z})^3 \subset \tilde{\mathbb{D}}_{2g}$ qui stabilise un des cylindres T_j – qui dans l'espace euclidien de dimension 3 s'interprète comme le groupe des changements de signe relatif au système d'axes orthonormés correspondant.

2) Etendre l'action sur π_g du groupe de Teichmüller (plus ou moins) “spécial” de données chacun des T_j , en l'action d'un groupe analogue d'un ensemble plus grand obtenu en lui rajoutant une “lanière” L (d'où un tore à un trou, et son groupe de Teichmüller spécial, qui s'introduisent de façon naturelle)⁵² voire l'ensemble encore plus grand obtenu en mettant également la lanière antipodique L' (cet ensemble se présente comme un cylindre $(L \cup L')$ ou “buse”, où on aurait mis un tube (T_j) en travers, et a la structure topologique d'un tore à deux trous). Il est possible qu'il faille considérer de près ce dernier, pour étudier les relations entre les éléments de \mathfrak{X}_g provenant des ensembles précédents.... Un travail amusant sera de se débrouiller pour écrire les générateurs du groupe π_g , et surtout la fameuse relation, dans une disposition géométrique relative des “anses”, qui est une disposition “panachée” – et non plus sagement à la queue-leu-leu!

⁵²C'est essentiellement un $SL(2, \mathbb{Z})$ – plutôt une extension centrale remarquable de $SL(2, \mathbb{Z})$ par \mathbb{Z} , qui rappelle celle de $SL(2, \mathbb{R})$ par \mathbb{Z} ... (revêtement universel de $SL(2, \mathbb{R})$).

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

En attendant d'entrer ainsi dans le vif de la structure du groupe de Teichmüller, je vais déjà essayer de décrire des générateurs et relations pour le sous-groupe intéressant qu'on vient d'écrire, $\tilde{\mathbb{D}}_{2g} \cdot \mathcal{H}$. Je vais prendre les sempiternels générateurs $\varepsilon_0, \varepsilon_1$ de \mathbb{D}_{2g} ⁵³,

$$\varepsilon_0^2 = \varepsilon_1^2 = 1, \quad (\varepsilon_0 \varepsilon_1)^{2g} = 1$$

et y joindre $\tau = \tau_g$, et $\rho_0 \tau = \tau'$ ($\rho_0 = \rho_{j_0}$, j_0 point marqué de $I = J/\tau$) satisfaisant

$$\tau^2 = \tau'^2 = 1,$$

$$(\tau \varepsilon_0)^2 = (\tau \varepsilon_1)^2 = 1$$

exprimant la commutation de τ à $\varepsilon_0, \varepsilon_1$;

$$(\varepsilon_1 \tau')^2 = 1,$$

i.e. ε_1 commute à τ' ,

$$((\varepsilon_0 \varepsilon_1)^g \tau')^2 = 1$$

(l'involution $(\varepsilon_0 \varepsilon_1)^g$ commute à τ'); sauf erreur, ça fait un ensemble de générateurs et relations pour $\tilde{\mathbb{D}}_{2g} \cdot \mathcal{H}$ – en résumé $\varepsilon_0, \varepsilon_1, \tau, \tau'$:

$$\varepsilon_0^2 = \varepsilon_1^2 = \tau^2 = \tau'^2 = 1(\tau \varepsilon_0)^2 = (\tau \varepsilon_1)^2 = (\tau' \varepsilon_1)^2 = 1(\varepsilon_0 \varepsilon_1)^{2g} = 1(\tau'(\varepsilon_0 \varepsilon_1)^g)^2 = 1. (52)$$

C'est peut-être pas très astucieux comme choix de générateurs, en ce sens que $\varepsilon_0, \varepsilon_1$ ne sont pas du tout sur le même pied que τ, τ' – ce ne sont pas des *anti*-involutions. Il vaudrait mieux prendre $\varepsilon'_0 = \tau \varepsilon_0, \varepsilon'_1 = \tau \varepsilon_1$, de façon à obtenir:

$$\varepsilon_0'^2 = \varepsilon_1'^2 = \tau^2 = \tau'^2 = 1(\tau \varepsilon_0')^2 = (\tau \varepsilon_1')^2 = (\tau'(\tau \varepsilon_1'))^2 = 1(\varepsilon_0' \varepsilon_1')^{2g} = 1(\tau'(\varepsilon_0' \varepsilon_1')^g)^2 = 1. (52 \text{ bis})$$

Ce sont essentiellement les “mêmes” relations sauf la dernière de la deuxième ligne.

Peut-être ce petit jeu avec le tout petit groupe $\tilde{\mathbb{D}}_n$ opérant sur \mathcal{H} est un peu une amusette – le groupe $\mathcal{H} \simeq \mathbb{Z}^g$ dans \mathfrak{X}_g suggère beaucoup la situation d'un tore maximal dans un groupe semi-simple; on a vraiment envie d'en avoir une caractérisation intrinsèque dans \mathfrak{X}_g – ou dans \mathfrak{S}_g , ce qui est possible puisqu'en tant que groupe de transformations topologiques effectives, il laisse fixe les points de $V_0 \subset X_g$ – par exemple les deux pôles, qu'on peut prendre comme

⁵³NB. ε_0 bouge le sommet du repère, ε_1 l'arête et pas le sommet, donc $\varepsilon_1(j_0) = j_0$.

A. GROTHENDIECK

points base pour construire revêtement universel et groupe fondamental. Ce sont peut-être les sous-groupes abéliens-libres maximaux. On aimerait étudier le normalisateur – est-ce exactement ce qui provient des automorphismes de $X_g \setminus \cup T_i^\circ \simeq V_0$? Les $SL(2, \mathbb{Z})$ associés aux “lanières” à travers le tube T_j , jouent-ils un rôle analogue à celui des groupes $SL(2, K)$ où $GP(1, K)$ “de rang 1” dans la théorie des groupes algébriques réductifs? Si *** ne “mord” pas à la situation, la soumettre peut-être à ***, qui est à l’aise tant avec les groupes discrets et leurs générateurs et relations, qu’avec la théorie des semi-simples – et la topologie...

§ 33bis. — ÉTUDE DES REVÊTEMENTS FINIS - RELATION ENTRE
LES $\mathcal{N}_{g,\nu}$, $\Gamma_{g,\nu}$ POUR g VARIABLE

Soient π un groupe extérieur à lacets profini arithmétisé de type (g, ν) , π' un sous-groupe connexe de π , d'où une application injective

$$\text{Discrét}(\pi) \hookrightarrow \text{Discrét}(\pi');$$

on voudrait prouver qu'elle est compatible avec la relation d'équivalence de l'arithmétisation, de sorte que toute arithmétisation de π en donne une de π' , et de même pour les prédiscrétifications. On voudrait établir en même temps que les applications

$P^+(\pi) \rightarrow P^+(\pi')$ sur les prédiscrétifications orientées et $A(\pi) \rightarrow A(\pi')$ sur les arithmétisations sont injectives. Pour prouver ces points, on est ramené au cas où π' invariant caractéristique (cf. §28, diagramme (7)). Choissant une discrétification π_0 de π , donc π'_0 de π' , on trouve donc $\hat{\mathfrak{S}}(\pi_0) \rightarrow \hat{\mathfrak{S}}(\pi'_0)$ et on a:

L'homomorphisme $\hat{\mathfrak{S}}(\pi_0) \rightarrow \hat{\mathfrak{S}}(\pi'_0)$ envoie $\mathcal{M}(\pi_0)$ dans $\mathcal{M}(\pi'_0)$.

On aura donc un diagramme (variante de celui du §28):

$$\begin{array}{ccccc} \hat{\mathfrak{S}}^+(\pi_0) & \hookrightarrow & \mathcal{M}(\pi_0) & \hookrightarrow & \hat{\mathfrak{S}}(\pi_0) \\ \downarrow & & \downarrow & & \downarrow \\ \hat{\mathfrak{S}}^+(\pi'_0) & \hookrightarrow & \mathcal{M}(\pi'_0) & \hookrightarrow & \hat{\mathfrak{S}}(\pi'_0) \end{array} \quad (1)$$

qui implique qu'une discrétification π_1 sur π qui donne même prédiscrétification orientée que π_0 (resp. même arithmétisation) définit une discrétification π'_1 de π' qui donne même prédiscrétification orientée (resp. même arithmétisation) que π'_0 .

A. GROTHENDIECK

Donc on a bien $P^+(\pi) \rightarrow P^+(\pi')$, $A(\pi) \rightarrow A(\pi')$ et il faut encore exprimer l'injectivité, qui revient aux relations

$$\hat{\mathfrak{S}}^+(\pi_0) = \hat{\mathfrak{S}}^+(\pi'_0) \cap \hat{\mathfrak{S}}(\pi_0), \quad \mathcal{M}(\pi_0) = \mathcal{M}(\pi'_0) \cap \hat{\mathfrak{S}}(\pi_0) \quad (2)$$

i.e. un automorphisme à lacets de π qui, sur π' , appartient à $\hat{\mathfrak{S}}(\pi'_0)$, resp. à $\mathcal{M}(\pi'_0)$, est déjà dans $\hat{\mathfrak{S}}(\pi_0)$, resp. dans $\mathcal{M}(\pi'_0)$.

L'assertion repérée étant admise, l'assertion non repérée signifie aussi que l'homomorphisme canonique:

$$\Pi_a = \mathcal{M}_a(\pi) / \hat{\mathfrak{S}}_a^+(\pi) \rightarrow \Pi'_a = \mathcal{M}'_a(\pi') / \hat{\mathfrak{S}}_{a'}^+(\pi') \quad (3)$$

est *injectif*. Par construction (via $\Pi_{\mathbb{Q}}$), c'est aussi surjectif, donc on trouverait: l'homomorphisme canonique (3) est bijectif et on trouverait aussi une bijection

$$P_a(\pi) \rightarrow P'_a(\pi') \quad (4)$$

entre arithmétisation de π de type a et arithmétisation de π' de type a' , *compatible* avec l'isomorphisme (3).

Enfin, ces résultats dans les cas π' invariant caractéristique s'étendraient aussitôt au cas d'un $\pi' \subset \pi$ ouvert quelconque.

Procédant par exemple comme dans le §28 à coups de "correspondances" arithmétiques extérieures entre "courbes potentielles", on trouve un groupoïde connexe (ponctué par les $\hat{\pi}_{g,\nu}$, par exemple, qui y sont canoniquement isomorphes), dont le π_1 extérieur est la valeur commune des $\Pi_{g*} = \Pi_{g,\nu}$. Pour trouver un isomorphisme canonique entre $\Pi_{g,\nu}$ et $\Pi_{g',\nu'}$, on choisit une correspondance entre $\pi_{g,\nu}$ et $\pi_{g',\nu'}$, par exemple on regarde l'un et l'autre (quitte à passer de g, ν à $g, \tilde{\nu}$ avec $\tilde{\nu} \geq \nu$, et de même pour g', ν' à $g', \tilde{\nu}'$ avec $\tilde{\nu}' \geq \nu'$) comme des sous-groupes [d'indices] finis du même $\pi_{0,3}$, d'où $\Pi_{0,3} \xrightarrow{\sim} \Pi_{g,\tilde{\nu}}, \Pi_{0,3} \xrightarrow{\sim} \Pi_{g',\tilde{\nu}'}$.

On aimerait maintenant voir ce qui, dans le yoga précédent, est indépendant de toute conjecture. Par exemple, le fait que les homomorphismes surjectifs canoniques

$\Pi_{g,\nu} \rightarrow \Pi_{g,\nu'}$ (g le même, ν' constant) n'est pas établi. Cependant, si on savait que dans la situation du (π, π') avec π' invariant caractéristique, on a $\hat{\mathfrak{S}}(\pi'_0) \cap \hat{\mathfrak{S}}^+(\pi_0) = \hat{\mathfrak{S}}^+(\pi_0)$ (qui est un énoncé de nature relativement anodine sur des groupes à lacets profinis), on concluerait à la *bijectivité* de $\Pi_{\pi_0} \rightarrow \Pi_{\pi'_0}$ dans cette situation, et on en concluerait que le noyau de $\Pi_{\mathbb{Q}} \rightarrow$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

$\Pi_{0,3}$ s'envoie *trivialement* dans les $\Pi_{g,\nu}$ pour tout ν – i.e. qu'il s'envoie dans les $\Pi_{g,\nu}$ par *l'intermédiaire* de $\Pi_{0,3}$ – et que de plus $\Pi_{0,3} \rightarrow \Pi_{g,\nu}$ est un *isomorphisme* pour tout (g, ν) avec ν assez grand – il suffit que la surface de type (g, ν) (ou de type (g, ν') avec un $\nu' \leq \nu$) puisse s'obtenir comme revêtement étale de $X_{0,3}$, i.e. que $\pi_{g,\nu'}$ se réalise (avec sa structure à lacets) comme sous-groupe d'indice fini de $\pi_{0,3}$. Alors, considérant un $\pi'' = \pi_{g'',\nu''} \subset \pi_{g,\nu'}$ d'indice fini et contenu dans $\pi_{0,3}$, on aura un diagramme commutatif:

$$\begin{array}{ccc} \Pi_{0,3} & \xrightarrow{\sim} & \Pi_{g'',\nu''} \\ \uparrow & & \uparrow \wr \\ \Pi_{\mathbb{Q}} & \longrightarrow & \Pi_{g,\nu'} \end{array}$$

d'où notre assertion $\Pi_{0,3} \xrightarrow{\sim} \Pi_{g,\nu'}$ et a fortiori l'homomorphisme surjectif $\Pi_{0,3} \rightarrow \Pi_{g,\nu}$ qui le factorise ($\nu \geq \nu'$) est bijectif. Notons par exemple que les $\Pi_{0,\nu} \rightarrow \Pi_{0,3}$ ($\nu \geq 3$) sont alors bijectifs. Mais on notera qu'en tout état de cause, on ne trouve de résultat pour un g, ν que si $\nu \geq 3$ – donc ceci ne dit rien sur la fidélité éventuelle, par exemple de $\Pi_{0,3} \rightarrow \Pi_{g,0} = \Pi_g$ ($g \geq 2$), ou $\Pi_{0,3} \rightarrow \Pi_{1,1} = \Pi_1$.

Soit une courbe algébrique \mathcal{U} de type g, ν ⁵⁴, définie sur un sous-corps K fini sur \mathbb{Q} de $\overline{\mathbb{Q}_0}$, donc elle définit une action extérieure du sous-groupe ouvert $\Gamma = \Gamma_K \subset \Gamma_{\mathbb{Q}}$ sur $\pi_1(\mathcal{U}_{\overline{\mathbb{Q}_0}})$. Quitte à agrandir K , et à agrandir ν ou ν' (i.e. faire des trous) pour trouver \mathcal{U}' on peut supposer que \mathcal{U}' est un revêtement étale de $(\mathcal{U}_{0,3})_K$. On pose $\pi' = \pi_1(\mathcal{U}'_{\overline{\mathbb{Q}_0}})$, $\pi = \pi_1(\mathcal{U}_{\overline{\mathbb{Q}}})$. Soit alors θ le noyau de

$$\Gamma (\subset \Pi_{\mathbb{Q}}) \longrightarrow \Pi_{0,3},$$

il opère donc par automorphismes intérieurs sur $\hat{\pi}_{0,3}$, donc l'image de $\theta' = \Gamma' \cap \theta$ dans le groupe des automorphismes extérieurs de $\pi' \subset \hat{\pi}_{0,3}$ est un sous-groupe fini – a fortiori son image dans $\Pi_{\pi'}$, et dans $\mathcal{N}(\pi)$, et dans Π_{π} . Il en est de même (choisissant un point base rationnel sur K dans \mathcal{U}') de l'opération effective sur $\pi_1(\mathcal{U}, P)$ car il suffit d'appliquer le résultat précédent à $\mathcal{U} \setminus \{P\}$. On en conclut aussi que les noyaux des homomorphismes $\Pi_{0,\nu} \rightarrow \Pi_{0,3}$ ($\nu \geq 3$) sont *finis*. On voit facilement que pour tout V.A. [Valuation Arithmétique] A définie sur K , l'opération de θ' sur $\prod_{\ell} T_{\ell}(A)$ se fait à travers un groupe quotient fini.

Il devient très difficile de s'imaginer comment il pourrait se faire que θ' n'opère pas en fait trivialement! J'ai même l'impression que je peux montrer, grâce au résultat du russe que

⁵⁴On ne fait plus d'hypothèse conjecturale (telle que l'injectivité dans (3)).

A. GROTHENDIECK

m'a signalé Deligne, que $\Pi_{\mathbb{Q}} \rightarrow \Pi_{0,3}$ est un isomorphisme! Cela signifierait que les actions extérieures de $\Pi_{\mathbb{Q}}$ sur des $\pi_1 \simeq \overline{\pi_{g,\nu}}$ peuvent s'interpréter (au moins pour ν assez grand, g étant fixé) comme des scindages de l'extension $\mathcal{N}_{g,\nu}$ de $\Pi_{g,\nu}$ par $\hat{\mathfrak{Z}}_{g,\nu}$ – ou de l'extension $\mathcal{M}_{g,\nu}$ de $\Pi_{g,\nu}$ par $\hat{\mathfrak{S}}_{g,\nu}$, quand il s'agit d'actions effectives.

Bien entendu, la question essentielle qui se pose alors (admettant $\Pi_{\mathbb{Q}} \simeq \Pi_{0,3}$) est de caractériser $\Pi_{0,3}$ algébriquement, ainsi que les $\mathcal{N}_{g,\nu}$ – et de donner une description algébrique également des scindages “admissibles” – i.e. correspondant bel et bien à des courbes algébriques sur des corps de nombres algébriques, que ce sont exactement les actions relevant l'action extérieure donnée, qui ne normalisent aucun sous-groupe à lacets, ou encore telle que $\hat{\pi}_{0,3}^{\Gamma''+}$ (mais il est concevable qu'il faille y ajouter de conditions plus subtiles, faisant intervenir les Frobenius...). On peut se proposer de trouver une description des actions *extérieures* “admissibles”, sans avoir à passer par des actions effectives admissibles – et à s'embarasser d'en donner une définition plus ou moins plausible. La difficulté bien sûr provient du fait que si Γ'' opère *extérieurement* sur $\hat{\pi}_{0,3}$, il n'opère pas extérieurement pour autant sur un sous-groupe ouvert donné π' de $\hat{\pi}_{0,3}$. Mais on va supposer justement qu'il *existe* une telle action, de telle façon que $\pi' \rightarrow \hat{\pi}_{0,3}$ soit compatible avec les actions extérieures, et que l'action de Γ' sur π se déduise (modulo isomorphisme) de [??].

Pour ce deuxième point, on a une réponse immédiate (supposant connus déjà les $\mathcal{N}_{g,\nu}$). Soit un (π, a) de type g, ν , avec relèvement partiel de Π_a en $\Gamma'_a \hookrightarrow \mathcal{N}_a$. Elle sera admissible si et seulement si on peut trouver un (π', a') de type (g, ν') et un plongement de π' comme sous-groupe d'indice fini de $\hat{\pi}_{0,3}$ compatible avec a' , et un sous-groupe ouvert Γ'' de $\Pi_{0,3}$, et une action effective admissible de Γ'' sur $\hat{\pi}_{0,3}$ qui relève l'action extérieure donnée, et qui invarie π' , de façon qu'à isomorphisme près, (π, a) , et le germe d'action de Γ' dessus se déduise de (π', a') par l'action de Γ'' dessus, par “bouchage” d'un paquet de trous (et oubli d'une action effective au profit de l'action extérieure). Il faut dans cette approche de simplement savoir préciser algébriquement ce qu'on entend par action “admissible” de $\Gamma'' \subset \Pi_{0,3}$ sur $\hat{\pi}_{0,3}$ – sous-entendant que ça doit correspondre aux points de $\mathcal{U}_{0,3}$ rationnels sur le corps de nombres défini par Γ'' . On peut conjecturer celle-ci, par “bouchage de trous”.

Il semble qu'on puisse sur le même principe donner une description des $\mathcal{N}_{g,\nu}$ (donc de $\Pi_{g,\nu}$) en termes de $\Pi_{0,3}$. Utilisant les homomorphismes de transition $\hat{\mathfrak{Z}}_{g,\nu} \rightarrow \hat{\mathfrak{Z}}_{g,\nu'}$, il suffit de le faire, quand g est fixé, pour des ν grands – assez grands pour qu'il existe une courbe

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

algébrique de type g, ν sur \mathbb{Q} qui soit un revêtement étale de $\mathcal{U}_{0,3}$ sur \mathbb{Q} . On considère donc un plongement correspondant de $\pi_{g,\nu}$ dans $\pi_{0,3}$, et on décrète que si on peut faire opérer extérieurement $\Pi_{0,3}$ dans $\pi_{g,\nu}$, de façon que $\pi_{g,\nu} \rightarrow \pi_{0,3}$ commute à ces actions extérieures, *alors* le sous-groupe de $\hat{\mathfrak{Z}}_{g,\nu}$ engendré par $\hat{\mathfrak{Z}}_{g,\nu}$ et $\Pi_{0,3}$ est $\mathcal{N}_{g,\nu}$.

§ 34. — DESCRIPTION HEURISTIQUE PROFINIE DE LA
CATÉGORIE DES COURBES ALGÉBRIQUES
DÉFINIES SUR DES SOUS-EXTENSIONS FINIES K DE $\overline{\mathbb{Q}_0}/\mathbb{Q}$ (I.E. DE
 $\mathbb{C}/\mathbb{Q})$)

On se borne aux courbes géométriques connexes (par commodité) anabéliennes (par nécessité provisoire), cf. plus bas sur la façon de se débarrasser de cette restriction. La donnée d'un revêtement de $\mathcal{U}_{\overline{\mathbb{Q}_0}}$ définit une structure d'extension

$$1 \rightarrow \pi \rightarrow \Sigma \rightarrow \Gamma^+ \rightarrow 1(1)$$

ou encore on a un homomorphisme

$$\mathcal{E} \rightarrow \Pi(2)$$

(image Γ ouverte, de noyau appelé π) où $\Gamma \subset \Pi_{\mathbb{Q}} \simeq \Pi_{0,3}$ est le sous-groupe ouvert correspondant à K . Se donner une telle extension (moyennant $\text{Centre}(\pi) = 1$) revient à se donner une action extérieure de Γ' sur π . Une première question: faut-il mettre la structure à lacets de π dans les données de l'objet (1) (ou (2)) censé décrire \mathcal{U}/K ?

Conjecture: Ce n'est pas la peine – la structure à lacets de π est la seule structure à lacets invariante par l'action extérieure de Γ (ou de Γ^{\natural}). Les sous-groupes à lacets L_i sont les sous-groupes maximaux dans π , tels que $\text{Norm}_{\mathcal{E}}(L_i) \rightarrow \Gamma$ ait comme image un sous-groupe ouvert de Γ ⁵⁵. Je présume aussi que tout homomorphisme entre extensions \mathcal{E} de Γ^+ par un π , \mathcal{E}'

⁵⁵et tout sous-groupe $\neq \{1\}$ de π qui a cette propriété est contenu dans un unique L_i ...

de Γ par un π' (\mathcal{E} , \mathcal{E}' provenant de courbes algébriques \mathcal{U} , \mathcal{U}') et tel que l'image de \mathcal{E} dans \mathcal{E}' soit ouverte respecte nécessairement la structure à lacets, et en fait provient d'un homomorphisme (unique, on le sait) de courbes algébriques.

En tout cas, si on admet la description des sous-groupes à lacets, il sera clair que l'image par μ d'un L_i sera ou bien (1), ou bien contenu dans un unique L_j ...

Ceci signifierait que le foncteur des courbes algébriques sur K ([avec comme] morphismes les morphismes dominants) vers les groupes profinis extérieurs sur lesquels Γ opère, serait pleinement fidèle. Le foncteur “extension du corps de base” de K à K' correspond au foncteur restriction d'un groupe extérieur (ou d'une structure d'extension) de Γ à Γ' (sous-groupe ouvert). Les revêtements étales finis de \mathcal{U} correspondent aux \mathcal{E} -ensembles ($\widetilde{\mathcal{U}}$ étant choisi)...

Pour décrire l'image essentielle de ce foncteur, on n'est pas réduit aux conjectures. On part de l'extension canonique $\mathcal{E}_{0,3}$ de $\Pi_{0,3} = \Pi$ par $\hat{\pi}_{0,3}$, on prend un sous-groupe ouvert \mathcal{E}' de $\mathcal{E}_{0,3}$, d'image $\Gamma \subset \Pi_{0,3}$, noyau $\pi' \subset \hat{\pi}_{0,3}$, et dans la structure à lacets canonique de π' de genre g (induite par celle de $\pi_{0,3}$), on prend un $I \subset I(\pi')$ tel que $2g + \text{card}(I) \geq 3$, stable par Γ , et on “bouche les trous” en $I(\pi') \setminus I$. De même, pour décrire quand une action effective, relevant une action extérieure admissible, est elle-même admissible – i.e. peut-être obtenue à partir d'une courbe algébrique \mathcal{U} , *ponctuée* par un point rationnel sur K . Ceci ne signifie pas pour autant, que si \mathcal{U} est donnée par une action extérieure de Γ sur un π , que les classes de conjugaison de relèvements admissibles de cette action proviennent bien toutes de points de \mathcal{U} rationnels sur K . Mais on voit de suite que ceci sera le cas, dès que l'on admet la pleine fidélité pour les *isomorphismes*.

(NB. Même pour les automorphismes de $\mathcal{U}_{0,3} = \mathbb{P}_{\mathbb{Q}}^1 \setminus \{0, 1, \infty\}$, cette pleine fidélité n'est pas du tout claire. Il faudrait prouver que le commutant de $\Pi_{0,3}$ dans $\hat{\mathfrak{Z}}_{0,3}$ est réduit à \mathfrak{S}_3 . La situation est moins sans espoir, quand on se donne, avec la structure de groupe profini extérieur à opérateur Γ , une arithmétisation de π (ce qui suppose qu'on a explicité une structure à lacets) invariante par Γ – donc dans $\hat{\mathfrak{Z}}(\pi)$ on dispose d'un $\mathcal{N}(\pi)$, et $\Gamma \hookrightarrow \mathcal{N}(\pi)$. Dans ce point de vue, pour un homomorphisme de Γ -groupes extérieurs (arithmétisés) $\pi' \rightarrow \pi$, il est sous-entendu qu'il est compatible avec les arithmétisations, i.e. si π'' est l'image de π' dans π , on veut que l'arithmétisation de π'' déduite de celle de π' par “passage au quotient”, soit celle induite par π . En particulier, pour les automorphismes extérieurs de π , il est sous-entendu que non seulement ils commutent à Γ , mais encore qu'ils sont dans $\mathcal{N}(\pi)$ (ce qui implique

A. GROTHENDIECK

qu'ils sont dans $\hat{\mathfrak{Z}}(\pi)$, car le centralisateur dans π de tout sous-groupe ouvert de Π_π est $\{1\}$! Dans le cas de $\mathcal{W}_{0,3}$, on a $\mathcal{N}_{0,3} \simeq \mathfrak{S}_3 \times \Pi_{0,3}$, et on sait que le centre de $\Pi_{0,3} \simeq \Pi$ est triviale – donc on trouve bien que le groupe des automorphismes de cette structure est réduit à \mathfrak{S}_3 !

Ce point de vue est néanmoins probablement superflu – car on présume que pour l'action extérieure donnée de Γ , il y a une unique arithmétisation invariante par Γ , et que les homomorphismes “admissibles” de Γ -groupes extérieurs “admissibles”, tels qu'ils ont été définis précédemment, respectent automatiquement cette arithmétisation. S'il n'en était rien, il faudrait bien entendu introduire les arithmétisations dans la structure.

Il se pose la question de trouver une description plus simpliste des actions extérieures d'un Γ sur un π qui sont “admissibles”. Ici, on va partir d'un π dont on fixe déjà une structure à lacets et une arithmétisation a (invariantes par Γ), de sorte que $\Gamma \subset \mathcal{N}(\pi)$, $\Gamma \rightarrow \Pi_\pi$ injective à image ouverte, i.e. Γ correspond à un scindage partiel (ou germe de scindage) de

$$1 \rightarrow \hat{\mathfrak{Z}}(\pi) \rightarrow \mathcal{N}(\pi) \rightarrow \Pi_\pi \rightarrow 1.$$

Soit (g, ν) le type de π ; si $g \geq 1$ le critère la plus simple, c'est que les “ Γ^\natural -points” de π' déduits de π en bouchant tous les trous, soient distincts. (NB. Si $g = 1$, en bouchant tous les trous on tombe dans un cas abélien – mais ça ne fait rien). Si $g = 0$, il n'y a pas de condition pour $\nu = 3$, et si $\nu > 3$, mettant à part une partie $I' \subset I(\pi)$ avec $\text{card}(I') = 3$, la condition c'est qu'en bouchant les trous en $I \setminus I'$, les Γ^\natural -points de π déduits des points de $I \setminus I'$ soient distincts.

On notera que dans cette optique conjecturale, dans les cas limites $(g, 0)$ ($g \geq 2$), $(1, 1)$, $(0, 3)$, on n'impose aucune condition a priori sur les relèvements. C'est peut-être très brutal – et il se pourrait qu'on trouve des relèvements qui ne correspondent pas à une courbe algébrique – i.e. qui en fait ne sont *pas* admissibles, même s'ils le paraissent.

Pour y comprendre quelque chose, il me semble qu'il faut revenir à une interprétation des germes de scindages dits “admissibles” d'une extension telle que

$$1 \rightarrow \hat{\mathfrak{Z}}_{g,\nu} \rightarrow \mathcal{N}_{g,\nu} \rightarrow \Pi_{g,\nu} \rightarrow 1$$

où $\Pi_{g,\nu} \simeq \Pi_{\mathbb{Q}} \simeq \Pi_{0,3}$, comme correspondants aux points algébriques d'une *variété* (plutôt ici, une multiplicité) modulaire $\mathcal{M}_{g,\nu,\mathbb{Q}}$, dont $\mathcal{N}_{g,\nu}$ est le groupe fondamental arithmétique, et $\hat{\mathfrak{Z}}_{g,\nu}$ le groupe fondamental géométrique. J'aimerais examiner cette situation de plus près, par la suite. Pour le moment, il semble prudent de ne pas faire de conjectures hâtives pour une

description *directe* (i.e. *pas* via $\mathcal{U}_{0,3}$) des opérations extérieures “admissibles”. On travaillera donc pour le moment avec cette notion sous la forme constructive (via $\mathcal{U}_{0,3}$).

Si on a un π extérieur de type (g, ν) avec opération extérieure admissible de $\Gamma \subset \mathbb{I}$, on prévoit qu’il y aura une prédiscrétification stricte canonique sur π (pas invariante pas Γ , bien sûr – mais telle que l’arithmétisation correspondante le soit). On va même, pour une action effective admissible de Γ^\natural sur π (relevant l’action extérieure donnée), définir une discrétification orientée correspondante canonique $\pi_0 \subset \pi$ (remplacée par une conjuguée, quand on conjugue le relèvement $\Gamma^\natural \rightarrow \mathcal{E}$ par un $g \in \pi$) – toutes ces discrétifications orientées (correspondant aux différents “points” de B_{π, Γ^\natural}) définissent une même prédiscrétification orientée – et même une même prédiscrétification orientée *stricte*.

L’action effective de Γ^\natural sur π peut s’obtenir (à isomorphisme près) comme suit: on prend un sous-groupe ouvert $\mathcal{E}' \subset \mathcal{E}_{0,3}$, d’où extension $1 \rightarrow \pi' \rightarrow \mathcal{E}' \rightarrow \Gamma' \rightarrow 1$ avec $\pi' \subset \hat{\pi}_{0,3}$, donc $\pi' = \hat{\pi}'_0$ ($\pi'_0 = \pi' \cap \pi_{0,3}$). On a une opération de Γ' sur $I(\pi') = I(\pi'_0)$, on la prend triviale (quitte à passer à un sous-groupe ouvert de Γ'), on choisit $i \in I' \subset I(\pi')$, on bouche les trous en I' , d’où π , avec discrétification orientée π_0 , et une action extérieure de Γ' dessus, qui est relevée en une action effective grâce à i . On trouvera bien ainsi un “réseau” – une discrétification orientée dans π – je dis qu’il ne dépend pas des choix qui ont été faits – en particulier, que les automorphismes de $(\pi, a, \Gamma^\natural)$ transforment π_0 en lui-même. De plus, si on a deux points x, y de B_{π, Γ^\natural} , d’où $\pi(x), \pi(y)$, parmi les classes de chemins de x à y (qui font un bitorseur sous $\pi(y), \pi(x)$) il y a en a pour lesquelles $\pi(x) \rightarrow \pi(y)$ envoie $\pi_0(x)$ dans $\pi_0(y)$ – quand on se limite à ceux-ci, on trouve un sous-groupe du groupe fondamental $\Pi(\pi, \Gamma^\natural)$, qui est cette fois-ci un groupe *connexe* à lacets. On fera attention que Γ n’opère *pas* sur ce groupe, bien qu’il opère sur l’ensemble de ses objets.

§ 35. — L'INJECTIVITÉ DE $\Pi_{\mathbb{Q}} \rightarrow \text{Autext}_{\text{lac}}(\hat{\pi}_{0,3})$

Théorème 1: ⁵⁶ Soit $\Pi = \text{Gal}(\overline{\mathbb{Q}}_0/\mathbb{Q})$, où $\overline{\mathbb{Q}}_0$ est la clôture algébrique de \mathbb{Q} dans \mathbb{C} , considérons l'homomorphisme canonique

$$\Pi \xrightarrow{\Theta} \hat{\mathfrak{Z}}_{0,3} = \text{Autext}_{\text{lac}}(\hat{\pi}_{0,3}). (1)$$

Cet homomorphisme est *injectif*.

Démonstration.

Lemme 1: Soit $x \in \mathbb{Q}$, $x \neq 0, 1$ i.e. $x \in \mathcal{U}_{0,3}(\mathbb{Q})$; choisissons un chemin sur $\mathbb{P}^1(\mathbb{C})$ de $P = -\bar{j}$ (point base pour définir $\pi_{0,3} = \pi_1(\mathcal{U}_{0,3}(\mathbb{C}), P)$, (NB. $\mathcal{U}_{0,3} = \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$), d'où un isomorphisme $\pi_1(\mathcal{U}_{0,3}(\overline{\mathbb{Q}}_0), x) \simeq \hat{\pi}_{0,3}$, et par transport de structure une action effective de Π sur $\hat{\pi}_{0,3}$ (pas seulement extérieure). Alors $K = \text{Ker } \Theta$ opère trivialement sur $\hat{\pi}_{0,3}$.

Démonstration. Il suffit de voir que l'opération *extérieure* de K sur $\pi_1(\overline{V})$ où $V = \mathcal{U}_{0,3} \setminus \{x\}$, est triviale. D'après le résultat de Belyi, il existe un morphisme (*défini sur* \mathbb{Q} , ceci est essentiel)

$$\mathbb{P}^1\mathbb{Q} \rightarrow \mathbb{P}^1\mathbb{Q},$$

étale au-dessus de $\mathcal{U}_{0,3} = \mathbb{P}^1\mathbb{Q} \setminus \{0, 1, \infty\}$, et tel que $x \mapsto 0$. Soit \mathcal{U}' le revêtement étale de $\mathcal{U}_{0,3} = \mathcal{U}$ induit, $\pi' = \pi_1(\overline{\mathcal{U}'})$ son groupe fondamental géométrique, sur lequel Π donc $K \subset \Pi$ opère extérieurement. Alors $\pi(\overline{V})$ est un quotient de π' , avec respect des opérations extérieures de Π , et il suffit de prouver que K opère trivialement sur π' . Mais π' s'identifie à

⁵⁶Démontré modulo le lemme 2 plus bas.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

un sous-groupe ouvert de $\hat{\pi}_{0,3} = \pi$ (avec respect des opérations extérieures de K), sur lequel l'opération extérieure de K est triviale. Il s'ensuit que l'opération extérieure de K sur π' se fait à travers un groupe quotient *fini*.

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi' & \longrightarrow & \mathcal{E}'_K & \longrightarrow & K \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & \pi & \longrightarrow & \mathcal{E}_K & \longrightarrow & K \longrightarrow 1 \end{array}$$

[En effet, l'action extérieure de K se fait à travers l'action effective du groupe extérieur \mathcal{E}_K , laquelle par construction de K se fait par un homomorphisme $\mathcal{E}_K \rightarrow \Pi/\mathcal{Z}$ ($\mathcal{Z} = \text{Centre}(\pi)$), et l'action de \mathcal{E}'_K induite se fait par le composé $\mathcal{E}'_K \rightarrow \mathcal{E}_K \rightarrow \pi/\mathcal{Z}$, dont l'image est dans \mathcal{N}/\mathcal{Z} , où \mathcal{N} est le normalisateur de π' dans π . Donc l'image de K dans $\text{Autext}(\pi')$ est contenue dans celle de $\mathcal{N}/\mathcal{Z} \rightarrow \text{Autext}(\pi')$, or \mathcal{N}/π' est fini.]

Repassant à $\pi_1(\overline{V})$, on voit donc que l'image de K dans $\text{Autext}(\pi_1(\overline{V}))$ est finie, donc l'image de K dans $\text{Aut}(\hat{\pi}_{0,3})$ est finie. Elle est d'ailleurs formée d'automorphismes intérieurs, donc le lemme 1 sera conséquence du

Lemme 2: Tout automorphisme intérieur d'ordre fini de $\hat{\pi}_{0,3}$ (groupe profini libre à deux générateurs) est trivial. De façon plus précise: $\hat{\pi}_{0,3}$ a un centre réduit à $\{1\}$, et tout élément de $\hat{\pi}_{0,3}$ d'ordre fini est réduit à 1.

Ceci est un énoncé d'algèbre profini pure, que je reporte pour plus tard, pour en terminer avec la partie "géométrique" de la démonstration du théorème.

Lemme 3: Pour tout ouvert non vide $V \subset \mathbb{P}^1\mathbb{Q}$, considérant l'action extérieure de Π sur $\pi_1(\overline{V})$, la restriction de celle-ci à K est triviale.

Quitte à passer à un ouvert plus petit, on peut supposer par Belyi que V est un revêtement étale de $\mathcal{U}_{0,3}$ – et le raisonnement précédent montre alors que l'action extérieure de K se fait via un groupe quotient fini – mais cela n'est pas suffisant pour notre propos, et n'implique pas par lui-même que cette action soit triviale. D'ailleurs, au point où j'en suis, on aurait pu remplacer \mathcal{U} par n'importe quelle courbe algébrique quasi projective lisse géométriquement connexe – pour trouver que K opère sur le groupe extérieur $\pi_1(\overline{V})$ via un groupe fini. Mais ici l'hypothèse $V \subset \mathbb{P}^1\mathbb{Q}$ implique qu'il existe $y \in V(\mathbb{Q})$, soit $x \in \mathcal{U}(\mathbb{Q})$ son image dans $\mathcal{U} = \mathcal{U}_{0,3}$. Prenant y, x comme points base pour les groupes fondamentaux, on trouve

A. GROTHENDIECK

maintenant un homomorphisme effectif de groupes fondamentaux

$$\pi' = \pi_1(\overline{V}, y) \hookrightarrow \pi(\simeq \hat{\pi}_{0,3}) = \pi_1(\overline{\mathcal{U}}, x),$$

compatible avec une action *effective* de Π sur ces groupes. Par le lemme 1 l'action induite de K sur $\pi = \pi_1(\overline{\mathcal{U}}, x)$ est triviale, donc aussi son action sur le sous-groupe π' . A fortiori l'action extérieure est triviale, cqfd.

On peut maintenant prouver le

Lemme 4: $K = \{1\}$ (i.e. le théorème!)

En effet, sous les conditions du lemme 2, l'action de Π sur l'ensemble $I = S(\overline{\mathbb{Q}}_0)$, où $S = \mathbb{P}_{\mathbb{Q}}^1 \setminus V$, est déduite de l'action extérieure de Π sur $\pi_1(\overline{V})$ si $\text{card}(I) \geq 2$, comme l'action sur les classes de conjugaison de “sous-groupes lacets”. Comme K opère trivialement sur le groupe extérieur, il opère trivialement sur I . Ceci étant vrai pour tout V , on voit que l'action de K sur $\mathbb{P}^1(\overline{\mathbb{Q}}_0) = \overline{\mathbb{Q}}_0 \cup \{\infty\}$ est triviale, i.e. son action sur $\overline{\mathbb{Q}}_0$ l'est, donc $K = \{1\}$, cqfd.

Ouf!

Il reste à reporter la démonstration du lemme 2, que je vais reformuler sous une forme plus générale:

Théorème 2: Soit π un groupe profini libre sur un ensemble fini I de cardinal ≥ 2 . Alors:

- a) Le centre de π est égal à $\{1\}$.
- b) Il n'y a pas dans π d'élément d'ordre fini autre que 1.

Finalement je cale sur a) – tout comme je ne vois pas pourquoi le centre de Π (et de tout sous-groupe ouvert) doit être réduit à $\{1\}$. Consulter Deligne à ce sujet!

Pour b), voici un expédient. Soit K un corps algébriquement clos de caractéristique 0, et considérons le corps des fonctions $L = K(X)$ de $\mathcal{U} = \mathbb{P}_K^1 \setminus \{n+1 \text{ points}\}$ ($n = \text{card}(I)$). Alors $\pi \simeq \pi_1(\mathcal{U})$, et c'est un quotient de $\mathcal{E}_L = \text{Gal}(\overline{L}/L)$. Comme π est libre, $\mathcal{E}_L \rightarrow \pi$ se relève en $\pi \rightarrow \mathcal{E}_L$, et il suffit de voir que \mathcal{E}_L n'a pas d'élément d'ordre fini $\neq 1$. Mais d'après Artin, il n'y a pas d'automorphisme d'ordre fini $\neq 1$ d'un corps algébriquement clos \overline{L} , sauf dans le cas où \overline{L} est extension quadratique d'un corps ordonné maximal R , qui soit le corps des invariants de τ (donc τ d'ordre 2 exactement).

Mais en l'occurrence on aurait $R \supset L$, et $L \supset K$, or dans K l'élément -1 est un carré, donc R ne peut être ordonné – absurde!

Corollaire 1 du théorème 1: Soit X une courbe algébrique (lisse, géométriquement connexe, quasi-projective), sur k extension finie de \mathbb{Q} . (Je présume que l'action extérieure de $\mathcal{E}_k^{\bar{k}}$ sur $\pi_1(X_{\bar{k}})$ est fidèle si \mathcal{U} anabélien – à défaut de pouvoir le prouver, j'énonce:) Alors il existe une partie ouverte non vide V de X telle que l'action extérieure de $\mathcal{E}_k^{\bar{k}}$ sur $\pi_1(V_{\bar{k}})$ soit fidèle.

Démonstration. D'après Belyi, on sait qu'on peut trouver $V \subset X$ qui soit un revêtement étale de $\mathcal{U} = (\mathcal{U}_{0,3})_k$, je dis que ce V là convient. Soit donc K le noyau de l'opération extérieure de $\Gamma = \mathcal{E}_k^{\bar{k}}$ sur $\pi' = \pi_1(V_{\bar{k}})$. Soit y un point fermé de V , rationnel sur l'extension finie k' de k correspondant à un sous-groupe ouvert $\Gamma' = \mathcal{E}_{k'}^{\bar{k}}$ de Γ , soit $K' = \Gamma' \cap K$. Soit x l'image de y dans \mathcal{U} : on a

$$\pi' = \pi_1(V_{\bar{k}}, y) \hookrightarrow \pi = \pi_1(\mathcal{U}_{\bar{k}}, x),$$

et par construction l'action extérieure de K' sur π' est triviale, donc K' opère sur π' par automorphismes intérieurs. Or on a le

Lemma 5: ⁵⁷ Soit π un groupe profini à lacets, π' un sous-groupe ouvert; alors tout automorphisme u de π qui laisse stable π' et induit sur π' un automorphisme intérieur (resp. l'identité) est intérieur (resp. l'identité).

Admettons pour l'instant ce lemme – il en résulte que les éléments de K' , qui opèrent sur π en induisant sur π' des automorphismes intérieurs, induisent sur π lui-même des automorphismes intérieurs, i.e. que l'action extérieure de K' sur π est triviale. D'après le théorème 1, on sait d'autre part que l'action extérieure de Γ' sur π est fidèle, donc $K' = \{1\}$. Il en résulte que K est *fini*. Mais par Artin on sait que les seuls sous-groupes finis $\neq \{1\}$ de Γ sont ceux engendrés par une “conjugaison complexe” τ , correspondant à un sous-corps ordonné maximal entre k et \bar{k} . Mais pour un tel τ on a $\chi(\tau) = -1$, donc l'action extérieure de τ ne peut être triviale – on gagne. En fait, la démonstration a montré ceci:

Corollaire: Soient k un corps de caractéristique 0, \mathcal{U} une courbe algébrique (lisse etc.) sur k , telle que $\mathcal{E}_k^{\bar{k}} = \Gamma$ opère fidèlement sur $\pi_1(\mathcal{U}_{\bar{k}})$ (opération extérieure). Alors pour tout

⁵⁷prouvé seulement modulo vérification de (2), (4) ci-dessous – pour le Corollaire 1; (2) est d'ailleurs suffisant...

A. GROTHENDIECK

revêtement étale géométriquement connexe V de \mathcal{U} , l'opération extérieure de Γ sur $\pi_1(V_{\bar{k}})$ est également fidèle.

Reste à prouver le lemme 5. Il suffit de le prouver dans le cas “respé” – l'autre s'en déduit aussitôt. Si π a au moins une classe de lacets (cas d'une courbe algébrique affine i.e. non propre), alors π est libre – et le lemme 5 est valable justement pour de tels groupes. Si $(l_i)_{1 \leq i \leq \nu}$ est un système de générateurs, soit L_i le sous-groupe fermé engendré par l_i , nous admettrons que $\forall n \in \mathbb{N}^*$

$$L_i = \text{Centr}_\pi(L_i^n) \text{ }^{58}.(2)$$

Ceci posé, si l'automorphisme u de π induit l'identité sur π' , $\exists n \in \mathbb{N}^*$ tel que $\forall 1 \leq i \leq \nu$, $u(l_i^n) = l_i^n$, donc $u(l_i)$ centralise $l_i^n = u(l_i)^n$, donc par (2) on a $u(l_i) \in L_i$, i.e. $u(L_i) \subset L_i$, mais on a $\text{Aut}(L_i) \simeq \hat{\mathbb{Z}}^*$, et un automorphisme d'un $\hat{\mathbb{Z}}$ -module libre de rang 1 est connu quand on le connaît sur ${}_u L_i \xleftarrow{\sim} L_i$. Donc $\forall i$ on a $u(l_i) = l_i$, donc $u = \text{id}$, cqfd.

Dans le cas où π n'est pas libre, prenons un bon $(x_i, y_i)_{1 \leq i \leq g}$ – de sorte que π soit défini par la relation génératrice

$$\prod_1^g [x_i, y_i] = 1.(3)$$

Soient Λ_i, Λ'_i les sous-groupes fermés engendrés par x_i, y_i . (Ils sont d'ailleurs tous conjugués sous $\text{Aut}(\pi) \dots$). J'admets que ces groupes sont $\simeq \hat{\mathbb{Z}}$ (i.e. que les homomorphismes surjectifs $\hat{\mathbb{Z}} \rightarrow \Lambda_i, \hat{\mathbb{Z}} \rightarrow \Lambda'_i$ envoyant 1 dans les x_i, y_i sont injectifs – c'est d'ailleurs trivial en passant à π_{ab}) et qu'on a, en analogie avec (2), pour tout $n \in \mathbb{N}^*$

$$\text{Centr}_\pi(\Lambda_i^n) = \Lambda_i, \quad \text{Centr}_\pi(\Lambda_i'^n) = \Lambda'_i,$$

et on termine comme ci-dessus.

Remarque: Le résultat le plus fort de fidélité dans la direction du présent paragraphe, concernant des actions de Π et de ses sous-groupes ouverts, serait le suivant: si V est une courbe algébrique anabélienne sur l'extension finie k de \mathbb{Q} , avec la clôture algébrique \bar{k} , alors non seulement l'action extérieure de $\mathcal{E}_k^{\bar{k}} = \Gamma$ sur $\pi_1(V_{\bar{k}})$ devrait être fidèle, i.e.

$$\Gamma \rightarrow \hat{\mathfrak{Z}}(\pi) \text{ }^{59}$$

⁵⁸pas prouvé!

⁵⁹Cet homomorphisme se factorise automatiquement par le sous-groupe $\mathcal{N}(\pi)$ qui normalise $\hat{\mathfrak{Z}}(\pi)$.

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

injective, mais même l'homomorphisme composé

$$\Gamma \rightarrow \mathcal{N}(\pi) \rightarrow \mathcal{N}(\pi)/\hat{\mathfrak{Z}}^+(\pi) \simeq \Pi_\pi$$

devrait être injectif (auquel cas ce sera même un isomorphisme, puisqu'il est surjectif par construction même de $\mathcal{N}(\pi)$, Π_π ...). Des raisonnements heuristiques faits précédemment (moins convaincants sans doute que ceux du présent paragraphe!) semblent indiquer que ce serait le cas au moins lorsque V est un revêtement étale de $\mathcal{U} = (\mathcal{U}_{0,3})_k$, auquel cas en effet l'homomorphisme $\Gamma \rightarrow \Pi_\pi$ s'insère dans un diagramme commutatif

$$\begin{array}{ccccc} & & \Gamma & & \\ & \swarrow & \downarrow & \searrow & \\ \Pi_{\pi_0} & & \Pi_\pi & \longrightarrow & \Pi_{\pi'} \end{array}$$

où $\pi_0 = \pi_1(\mathcal{U}_k)$, de sorte que π est un sous-groupe ouvert de π_0 , et π' est un sous-groupe ouvert convenable, *caractéristique* dans π_0 . Si on pouvait montrer que $\Pi_{\pi_0} \rightarrow \Pi_{\pi'}$ est injectif (ce qui est plus ou moins une histoire d'algèbre profinie), il en serait de même du composé $\Gamma \hookrightarrow \Pi_{\pi_0} \rightarrow \Pi_{\pi'}$, donc aussi de $\Gamma \rightarrow \Pi_\pi$. Donc modulo cette hypothèse sur les groupes profinis, et utilisant Belyi, on trouve que pour toute courbe algébrique V sur k , il existe $V' \subset V$ ouvert non vide, tel que

$$\Gamma \rightarrow \Pi_{\pi'}$$

(où $\pi' = \pi_1(V'_k)$) soit injectif. Quant à savoir si $\Gamma \rightarrow \Pi_\pi$ est lui-même déjà injectif – ou ce qui revient au même, si $\Gamma \rightarrow \Pi_g$ pour $g \geq 2$ et $\Gamma \rightarrow \Pi_{1,1}$ sont injectifs, je n'ai pas de raison heuristique plausible pour m'en convaincre à présent – peut-être est-ce tout à fait faux? L'argument plus ou moins convaincant rappelé précédemment (à supposer qu'on arrive à le justifier) montrerait seulement que si $\Gamma \rightarrow \Pi_\pi$ est injectif pour *un* π (ce qui ne dépend que de son type (g, ν)) alors il l'est pour les π' ouverts dans π . On le sait à présent (modulo peu de chose, tout au moins) pour les types $(0, \nu)$ ($\nu \geq 3$) exactement – ni plus ni moins – et on pourrait peut-être le déduire pour les types (g, ν) qui s'en déduisent par “revêtement fini”. Mais il est clair déjà qu'on n'obtient pas les types $(g, 0)$ comme cela ($g \geq 2$), ni même aucun (g, ν) avec $g \geq 1, \nu \in \{0, 1, 2\}$. C'est dire qu'on est loin du compte... Le premier cas bien intéressant serait donc le cas $(1, 1)$ (tore à un trou!), où $\hat{\mathfrak{Z}}_{1,1}^+ \simeq \mathrm{SL}(2, \mathbb{Z})^\wedge$ opérant extérieurement sur $\hat{\pi}_{1,1}$ (groupe libre à deux générateurs, encore – comme par hasard – l'action “arithmétique” de $\Pi_\mathbb{Q}$ sur $\hat{\pi}_{1,1}$ (i.e. l'action extérieure *mod* $\hat{\mathfrak{Z}}_{1,1}^+ \simeq \mathrm{SL}(2, \mathbb{Z})^\wedge$) est-elle fidèle?

§ 36. — L'ISOMORPHISME $\Pi_{\mathbb{Q}} \xrightarrow{\sim} \Pi_{1,1}$

(⁶⁰) Soit $\pi'_{0,3}$ le groupe quotient de $\Pi_{0,3}$ défini par les relations

$$l_1^2 = l_\infty^3 = 1; (1)$$

c'est donc le groupe “cartographique orienté pour structures triangulées”, les $\pi'_{0,3}$ -ensembles finis correspondant aux cartes orientées finies (pouvant avoir des boucles aplaties) dont les faces sont des triangles ou des mono-angles. L'opération extérieure de $\Pi_{\mathbb{Q}}$ (mais non celle de \mathfrak{S}_3 !) sur $\hat{\pi}_{0,3}$ passe au quotient en une action sur $\hat{\pi}'_{0,3}$. On peut améliorer le théorème 1 du paragraphe précédent par la

Proposition:

L'action extérieure de $\Pi_{\mathbb{Q}}$ sur $\hat{\pi}'_{0,3}$ est fidèle.

Pour le montrer, on va plonger $\pi_{0,3}$ comme sous-groupe d'indice fini dans $\pi'_{0,3}$, d'où un plongement analogue

$$\hat{\pi}_{0,3} \hookrightarrow \hat{\pi}'_{0,3}$$

qui sera compatible avec l'action extérieure de $\Pi_{\mathbb{Q}}$.

Considérons pour cela le schéma quotient $Y = \mathbb{P}_{\mathbb{Q}}^1 / \mathfrak{S}_3 = X / \mathfrak{S}_3$ avec les trois points a_0, a_1, a_∞ de Y , rationnels sur \mathbb{Q} , a_0 correspondant à la trajectoire $\{0, 1, \infty\}$, a_1 à la trajectoire $\{-1, \frac{1}{2}, 2\}$ et a_∞ à la trajectoire $\{j, \bar{j}\}, (j = \exp \frac{2i\pi}{3})$ de \mathfrak{S}_3 (ce qui épuise l'ensemble des trajectoires “singulières” géométriques). On sait que Y est une droite projective (sur $\overline{\mathbb{Q}}$ a priori),

⁶⁰Les réflexions du présent paragraphe, un peu cahin caha, seront reprises de façon moins pesante au paragraphe suivant.

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

qu'on épingle par a_0, a_1, a_∞ comme points $0, 1, \infty$, donc $Y \simeq \mathbb{P}_\mathbb{Q}^1$; l'homomorphisme $X \rightarrow Y$ s'identifie donc à un morphisme bien déterminé

$$f : X = \mathbb{P}_\mathbb{Q}^1 \rightarrow \mathbb{P}_\mathbb{Q}^1 = Y(3)$$

qui fait de X un revêtement galoisien de Y , de groupe \mathfrak{S}_3 , étale au dessus de $\mathbb{P}_\mathbb{Q}^1 \setminus \{0, 1, \infty\}$, avec comme indices de ramifications en ces points 2,2,3. Du point de vue de la géométrie des cartes (se plaçant sur le corps de base \mathbb{C}), on considère la carte déterminée sur X par le triangle sphérique $(0, 1, \infty)$ (sur l'axe réel comme équateur) – qui est donc la carte pondérée universelle – comme image inverse de la carte universelle (ayant un seul sommet 0, une seule arête repliée $0 \rightarrow 1$, une seule face, de centre ∞). Tout revêtement étale topologique de $\mathcal{U}_{0,3}(\mathbb{C}) \subset X$ donne ainsi un revêtement étale topologique de $\mathcal{U}_{0,3}(\mathbb{C}) \subset Y$, ayant au dessus de 1 la ramification 2, au dessus de l'infini la ramification 3 exactement, ce qui correspond au foncteur “oubli” de la pondération, où une carte triangulaire pondérée est considérée comme une carte tout court. Du point de vue des groupes fondamentaux, on trouve ainsi une équivalence de catégories:

$$(4) \quad \begin{array}{c} \text{Revêtements étales de } X \setminus \{0, 1, \infty\} = \mathcal{U}_{0,3} \simeq \pi_{0,3}\text{-ensembles} \\ \downarrow \wr \\ \text{Revêtements de } Y \setminus \{0, 1, \infty\} = \mathcal{U}_{0,3} / (\text{l'objet } X \setminus \{0, 1, \infty\} \text{ de la dite catégorie}) \\ \simeq \pi'_{0,3}\text{-ensembles}/E \end{array}$$

où:

- les revêtements de $Y \setminus \{0, 1, \infty\}$ considérés sont ceux dont la ramification est subordonnée à la signature $2\{1\} + 3\{\infty\}$,
- E est le $\pi'_{0,3}$ -ensemble correspondant à l'objet $X \setminus \{0, 1, \infty\}$ de la catégorie des revêtements étales de $Y \setminus \{0, 1, \infty\}$ à ramification subordonnée à $2\{1\} + 3\{\infty\}$.

Ici, le point base de $Y \setminus \{0, 1, \infty\}$ choisi pour décrire les revêtements (à ramification subordonnée à...) par un groupe fondamental à ramification, étant encore $P = -\bar{j}$, on aura:

$$E = f_{\mathbb{C}}^{-1}(P)(5)$$

et on peut expliciter ainsi la catégorie $(\pi'_{0,3}\text{-ens.})/E$, où E est un espace homogène, isomorphe au quotient de $\pi'_{0,3}$ par le sous-groupe $\pi_{0,3}^{\prime 0}$, noyau de l'homomorphisme surjectif idoine,

$$\pi'_{0,3} \rightarrow \mathfrak{S}_3$$

A. GROTHENDIECK

$$(6) \quad \begin{aligned} l_0 &\mapsto \text{éléments d'ordre 2} \\ l_1 &\mapsto \text{éléments d'ordre 2} \\ l_\infty &\mapsto \text{éléments d'ordre 3} \end{aligned}$$

[en marge:] A calculer!.

On choisit un $Q_0 \in E$ comme “origine” de E – pour pouvoir identifier E comme $\pi'_{0,3}$ -ensemble à $\pi'_{0,3}/\pi'^0_{0,3} \simeq \mathfrak{S}_3$ – alors $\text{Ens}(\pi'_{0,3})/E$ s’identifie, par le foncteur $F \rightarrow F_{Q_0}$, à $\text{Ens}(\pi'^0_{0,3})$.

On trouve donc en résumé une équivalence de catégories (dépendant du choix de Q_0)

$$\pi_{0,3} - \text{ensembles} \xrightarrow{\sim} \pi'^0_{0,3} - \text{ensembles}$$

qui est elle-même décrite par un bitorseur sous $(\pi'^0_{0,3}, \pi_{0,3})$ et, à isomorphisme (non unique!) près par un isomorphisme

$$\pi_{0,3} \xrightarrow{\sim} \pi'^0_{0,3},$$

les isomorphismes ainsi obtenus (pour des origines variables du bitorseur) formant exactement une classe de conjugaison par $\pi'^0_{0,3}$, i.e. un *isomorphisme extérieur* $\pi_{0,3} \xrightarrow{\sim} \pi'^0_{0,3}$. Quand de plus le choix de Q_0 varie, on trouve un composé $\pi_{0,3} \rightarrow \pi'^0_{0,3} \rightarrow \pi'_{0,3}$ exactement une classe de $\pi'_{0,3}$ -conjugaison, i.e. un homomorphisme extérieur.

J’ai beaucoup turbiné pour pas grand chose – à défaut d’avoir écrit les fonctorialités [?] très générales [??] pour les “groupes fondamentaux avec ramification”. Par exemple le bifoncteur I mystérieux de tantôt est formé des classes de chemins de $P \in X(\mathbb{C}) \setminus \{0, 1, \infty\}$ (point base pour calculer $\pi_{0,3}$) vers Q_0 (jouant le rôle d’un nouveau point base, ayant le mérite de s’envoyer sur celui – P – qui sert à calculer $\pi'_{0,3}$, groupe fondamental à ramification sur $Y(\mathbb{C}) \setminus \{0, 1, \infty\} \dots$). Il serait peut-être plus commode de définir directement un foncteur en sens inverse,

$$(7) \quad \begin{aligned} \text{Revêtements de } Y(\mathbb{C}) \setminus \{0, 1, \infty\} &\longrightarrow \text{Revêtements étales de } X(\mathbb{C}) \setminus \{0, 1, \infty\} \\ &\text{subordonnés à la signature } 2\{1\} + 3\{\infty\} \end{aligned}$$

par image inverse, suivi d’une *normalisation*.

Ici on utilise le fait que l’objet $X(\mathbb{C}) \setminus \{0, 1, \infty\}$ de la catégorie des revêtements à ramification maximum imposée, réalise justement un maximum sur les points $1, \infty$ où la condition intervient. On trouve que le foncteur correspondant

$$\pi'_{0,3} - \text{ensembles} \rightarrow \pi_{0,3} - \text{ensembles} (7 \text{ bis})$$

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

a les propriétés d'exactitude d'un foncteur associé à un morphisme de topos galoisiens

$$B_{\pi_{0,3}} \rightarrow B\pi'_{0,3}$$

(commute aux limites inductives, exact à gauche) et est donc défini par un $(\pi_{0,3}, \pi'_{0,3})$ -ensemble qui soit un toreur (à droite) pour $\pi'_{0,3}$ ⁶¹. Le choix d'une origine pour ce toreur définit alors aussi un homomorphisme correspondant $\pi_{0,3} \rightarrow \pi'_{0,3}$.

Revenons à la situation arithmétique sur \mathbb{Q} , où on dispose non seulement des groupes fondamentaux géométriques profinis $\hat{\pi}_{0,3}, \hat{\pi}'_{0,3}$, mais aussi d'extensions

$$\begin{array}{ccccccc} 1 & \longrightarrow & \hat{\pi}_{0,3} & \longrightarrow & \mathcal{E}_{0,3} & \longrightarrow & \Pi \longrightarrow 1 \\ 1 & \longrightarrow & \hat{\pi}'_{0,3} & \longrightarrow & \mathcal{E}'_{0,3} & \longrightarrow & \Pi \longrightarrow 1 \end{array} \quad (8)$$

qui s'interprètent comme des groupes fondamentaux de $\mathcal{U}_{0,3}$, resp. de $\mathcal{U}_{0,3}$ avec ramification subordonnée à $2\{1\} + 3\{\infty\}$. Les raisonnements précédents s'étendent à ce cadre et fournissent donc un homomorphisme d'extension

$$\begin{array}{ccccccc} 1 & \longrightarrow & \hat{\pi}_{0,3} & \longrightarrow & \mathcal{E}_{0,3} & \longrightarrow & \Pi \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & \hat{\pi}'_{0,3} & \longrightarrow & \mathcal{E}'_{0,3} & \longrightarrow & \Pi \longrightarrow 1 \end{array} \quad (9)$$

défini modulo composition par un automorphisme intérieur de $\pi'_{0,3}$ [$\hat{\pi}_{0,3} \rightarrow \hat{\pi}'_{0,3}$ s'insère dans une suite exacte

$$1 \rightarrow \hat{\pi}_{0,3} \rightarrow \hat{\pi}'_{0,3} \rightarrow \mathfrak{S}_3 \text{ (9 bis)}$$

et itou pour les groupes discrets, $1 \rightarrow \pi_{0,3} \rightarrow \pi'_{0,3} \rightarrow \mathfrak{S}_3$].

Ceci dit, soit K le noyau de l'opération extérieure de Π sur $\pi'_{0,3}$. On voit alors que l'opération extérieure de K sur le sous-groupe ouvert $\hat{\pi}_{0,3}$ se fait par un groupe fini (en fait par l'intermédiaire de $\hat{\pi}'_{0,3}/\hat{\pi}_{0,3} \simeq \mathfrak{S}_3 \dots$) – ce qui implique, par le théorème 1 du paragraphe précédent, que le groupe K lui-même est fini. Donc par Artin on a $K = 1$ ou $K = (1, \tau)$, τ la conjugaison complexe. Mais comme $\chi(\tau) = -1$, il est évident que l'opération extérieure de τ sur $\pi'_{0,3}$ (où même sur $\pi'_{0,3,ab} (\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ n'est pas triviale. Cela prouve la proposition.

⁶¹Ce bitorseur est aussi l'ensemble des $Y_{\mathbb{C}} \setminus \{0\}$ homomorphismes du “revêtement universel” à ramification imposée de cet espace sur le revêtement universel ordinaire de $X(\mathbb{C}) \setminus \{0, 1, \infty\}$.

A. GROTHENDIECK

J'ai envie maintenant d'interpréter $\pi'_{0,3}$ comme $\mathfrak{Z}_{1,1}^+ / (\text{centre})$ (le centre est isomorphe à $\{\pm 1\}$), et itou pour $\hat{\pi}'_{0,3} \simeq \hat{\mathfrak{Z}}_{1,1} / \{\pm 1\}$, isomorphisme qui soit compatible avec l'action extérieure de Π . On a (pour mémoire)

$$\mathfrak{Z}_{1,1} \xrightarrow{\sim} GL(2, \mathbb{Z}), (10)$$

l'isomorphisme étant obtenu ainsi

$$\mathfrak{Z}_{1,1} \xrightarrow{\sim} \mathfrak{Z}_{1,0} \xrightarrow{\sim} \text{Autext}(\pi_{1,0}) \simeq \text{Autext}(\mathbb{Z}^2) \simeq GL(2, \mathbb{Z}) (11)$$

[où le premier isomorphisme est celui de bouchage de trou].

On a donc

$$\mathfrak{Z}_{1,1}^+ \simeq SL(2, \mathbb{Z}) (12)$$

et

$$\text{Centre}(\mathfrak{Z}_{1,1}) \simeq \{\pm 1\} (13)$$

(s'identifie au groupe des homothéties de $SL(2, \mathbb{Z})$). Il est connu qu'on a dans $SL(2, \mathbb{Z}) / \{\pm 1\}$ deux générateurs λ_2, λ_3 satisfaisant respectivement

$$\lambda_3^3 = 1, \lambda_2^2 = 1 (14)$$

et tels que ces relations soient une *présentation* de $SL(2, \mathbb{Z}) / \{\pm 1\}$. Sauf erreur ces éléments proviennent d'éléments u_4, u_6 de $SL(2, \mathbb{Z})$ lui-même, satisfaisant

$$u_6^6 = 1, u_4^4 = 1, (15)$$

et qui correspondent aux seuls éléments d'ordres 6 et 4 (à conjugaison et passage à l'inverse près). En fait, tout élément d'ordre fini de $SL(2, \mathbb{Z})$ est conjugué à une puissance de u_4 ou u_6 . Les sous-groupes engendrés respectivement par u_4 et u_6 , cycliques d'ordre 4 et 6, sont les groupes des automorphismes des deux courbes elliptiques exceptionnelles (dîtes “anharmoniques”) (en caractéristique 0).

Je n'ai pas de formule sous la main pour “placer” u_4 et u_6 , de façon qu'ils engendrent le groupe $SL(2, \mathbb{Z})$ modulo son centre (ce qui implique sans doute qu'ils engendrent $SL(2, \mathbb{Z})$) – mais on fera attention à la relation supplémentaire, s'ajoutant à (15)

$$u_4^2 = u_6^3 (16)$$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

(c'est justement l'élément -1 du centre de $SL(2, \mathbb{Z})$). Je n'ai peut-être pas besoin de la formule explicite pour u_4 et u_6 . On définit alors

$$\pi'_{0,3} \xrightarrow{\sim} SL(2, \mathbb{Z}) / \{\pm 1\} \quad (17)$$

par

$$l'_1 \mapsto \lambda_2, \quad l'_\infty \mapsto \lambda_3 \quad (18)$$

(donc $l'_0 \mapsto (\lambda_3 \lambda_2)^{-1} = \lambda_2 \lambda_3^{-1} = \lambda_2 \lambda_3^2$), où l'_0, l'_1, l'_∞ sont les générateurs de $\pi'_{0,3}$ correspondants à ceux l_0, l_1, l_∞ de $\pi_{0,3}$, avec les relations de définition

$$l'_\infty l'_1 l'_0 = 1, \quad l_1'^2 = 1, \quad l_\infty'^3 = 1, \quad (19)$$

de sorte que $\pi'_{0,3}$ est bien le groupe de générateurs l'_1, l'_∞ satisfaisant à $l_1'^2 = 1, l_\infty'^3 = 1$.

Je veux maintenant me convaincre que l'homomorphisme correspondant à (17),

$$\hat{\pi}'_{0,3} \rightarrow SL(2, \mathbb{Z}) / \{\pm 1\} \simeq \hat{\mathfrak{Z}}_{1,1}^+ / \{\pm 1\} \quad (20)$$

est compatible avec l'opération extérieure de $\Pi = \Pi_{\mathbb{Q}}$. Pour ceci, j'ai envie de définir directement le composé avec $\hat{\pi}_{0,3} \rightarrow \hat{\pi}'_{0,3}$, i.e. $\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^+ / \{\pm 1\}$, et même de le relever en un homomorphisme

$$\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^+ \quad (21)$$

Au niveau des groupes discrets, on définit bien

$$\pi_{0,3} \rightarrow SL(2, \mathbb{Z}) \quad (22)$$

$$\text{par } l_1 \mapsto u_4, \quad l_\infty \mapsto u_6, \quad l_0 \mapsto (u_6 u_4)^{-1} = u_4^{-1} u_6^{-1},$$

et $SL(2, \mathbb{Z}) \simeq \mathfrak{Z}_{1,1}^+$ s'identifie au quotient de $\pi_{0,3}$ par le sous-groupe engendré par les éléments

$$l_1^4, l_\infty^6, (l_1^2)(l_\infty^3)^{-1}.$$

D'ailleurs $\pi_{0,3}$ peut s'interpréter comme un groupe de Teichmüller $\mathfrak{Z}_{0,4}^{!+}$ ⁶², et (22) comme un homomorphisme

$$\mathfrak{Z}_{0,4}^{!+} \rightarrow \mathfrak{Z}_{1,1}^+ \quad (23)$$

⁶²En effet $\mathfrak{Z}_{g,\nu}^!$ est extension de $\mathfrak{Z}_{g,\nu-1}^!$ par $\pi_{g,\nu-1}$ (si $(g, \nu-1)$ anabélien) et itou pour les \mathfrak{Z}^+ ; $\mathfrak{Z}_{0,3}^{!+} = \{1\}$!

A. GROTHENDIECK

dont je soupçonne qu'il se prolonge en un homomorphisme

$$\mathfrak{S}_{0,4}^! \rightarrow \mathfrak{S}_{1,1} \simeq SL(2, \mathbb{Z})(24)$$

[le premier membre étant] une extension de $(1, \tau)$ par $\pi_{0,3}$, qui n'est autre que le groupe cartographique triangulé pondéré non orienté.

J'interprète le premier membre de (23) comme le π_1 "géométrique transcendant" du topos modulaire $\mathbb{M}_{0,4}^!$, classifiant les droites projectives avec quatre points distincts numérotés de 1 à 4; et le deuxième membre de (23) est le π_1 transcendant du topos modulaire $\mathbb{M}_{1,1}$, classifiant les courbes elliptiques (avec une origine fixée). On devrait donc pouvoir définir, au niveau des multiplicités modulaires sur \mathbb{Q} ,

$$(\mathbb{M}_{0,4}^!)_{\mathbb{Q}} \rightarrow (\mathbb{M}_{1,1})_{\mathbb{Q}}, (25)$$

qui donnerait naissance à (23).

Mais on voit de suite qu'on a un isomorphisme canonique

$$\mathbb{M}_{0,4}^! \simeq \mathcal{U}_{0,3}(26)$$

(je laisse tomber les indices \mathbb{Q}), et la donnée de (25) revient donc aussi à la donnée d'une famille de courbes elliptiques sur $\mathcal{U}_{0,3}$. Mais si λ est la "variable $\in \mathcal{U}_{0,3}$ ", en prenant "le" revêtement quadratique E_λ de \mathbb{P}^1 ramifié en $0, 1, \infty, \lambda$, on trouve une courbe elliptique, avec quatre points marqués – au dessus de $0, 1, \infty, \lambda$ – dont on peut prendre le point au dessus de 0 comme origine – alors les trois autres points sont les trois points d'ordre 2, indexés respectivement par $1, \infty, \lambda$.

De façon plus précise: sur un schéma de base quelconque S , sauf que 2 y soit inversible (caractéristique résiduelle différente de 2), on a un foncteur qui va de la catégorie des systèmes (E, α, β) d'une courbe elliptique (homogène) relative sur S , et α, β deux sections de E formant une base de ${}_2E$, en tant que schéma localement constant en \mathbb{F}_2 – modules (ou système local de \mathbb{F}_2 -modules) de S (donnant naissance à $\gamma = \alpha + \beta$, comme troisième larron – de sorte que (β, γ) etc. sont en fait aussi des bases)⁶³ – vers la catégorie des fibrés en droites projectives P sur S , avec quatre sections $u_0, u_1, u_\infty, \lambda$ marquées distinctes en chaque point,

⁶³Il revient au même de dire que l'on a trois sections α, β, γ de ${}_2E$ sur S , qui sont distinctes en tout $s \in S$ et partant $\neq 1$.

en associant à E le quotient $E/\pm 1$, muni des sections $u_0, u_1, u_\infty, \lambda$ qui sont images respectivement de $0, \alpha, \beta, \gamma = \alpha + \beta$; et ce foncteur est *presque* une équivalence de catégories. Ce qui lui manque pour l'être, c'est que pour une courbe elliptique relative E , la symétrie $x \rightarrow -x$ de E – qui est un automorphisme non trivial – opère trivialement sur l'objet correspondant $E/\{\pm 1\}$ ⁶⁴. Donc il faut prendre le champ sur (Sch) , déduit de celui des courbes elliptiques en commençant par prendre $\text{Isom}(E, F)' = \text{Isom}(E, F)/\pm 1$, puis on prendra le champ associé à un préchamp (les objets sur S sont les “courbes elliptiques relatives à symétrie près sur S ”). Le champ est représentable par une multiplicité modulaire $M'_{1,1}$, ayant comme groupe fondamental géométrique $SL(2, \mathbb{Z})'/\{\pm 1\}$ justement, déduit par exemple des variétés modulaires à rigidification de Jacobi déchelonné n , $M_{1,1}[n]$ – avec un groupe $SL(2, \mathbb{Z}/n\mathbb{Z})$ opérant dessus, de sorte que

$$M_{1,1} \simeq (M_{1,1}[n], SL(2, \mathbb{Z}/n\mathbb{Z})) \quad (27)$$

et en outre que le sous-groupe central $\{\pm 1\}$ de $SL(2, \mathbb{Z}/n\mathbb{Z})$ opère trivialement sur $M_{1,1}[n]$; donc on peut faire opérer le groupe quotient $SL(2, \mathbb{Z}/n\mathbb{Z})' = SL(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$, et poser

$$M'_{1,1} = (M_{1,1}[n], SL(2, \mathbb{Z}/n\mathbb{Z})') \quad (28)$$

(ce qui manifestement ne dépend pas du choix de n , $n \geq 2$). On trouve ainsi un homomorphisme

$$M'_{0,4} \simeq \mathcal{U}_{0,3} \longrightarrow M'_{1,1}, \quad (29)$$

qui fait de $M'_{0,4}$ un revêtement galoisien de groupe \mathfrak{S}_3 de $M'_{1,1}$, et de façon plus précise

$$M'_{0,4} \xrightarrow{\sim} M_{1,1}[2]' \rightarrow M'_{1,1} \quad (30)$$

[la deuxième flèche définissant un] revêtement galoisien de groupe $SL(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$, le groupe fondamental géométrique de $M_{1,1}[2]$ étant d'ailleurs isomorphe au noyau de l'homomorphisme $SL(2, \mathbb{Z})^\wedge \rightarrow SL(2, \mathbb{Z}/2\mathbb{Z})$ qui factorise l'homomorphisme canonique $SL(2, \mathbb{Z})^\wedge \rightarrow SL(2, \mathbb{Z}/2\mathbb{Z})$.

Passant aux groupes fondamentaux pour $M'_{0,4} = \mathcal{U}_{0,3}$ et $M'_{1,1}$, on trouve un homomor-

⁶⁴Les pages qui suivent sont inutilement compliquées, avec l'introduction de $\mathbb{M}'_{1,1}, \mathfrak{Z}'_{1,1}$ etc. il suffit d'y aller brutalement avec la courbe elliptique $y^2 = \sqrt{x(x-1)(x-\lambda)}$ sur $\mathcal{U}_{0,3}$, pour avoir $\mathcal{U}_{0,3} \rightarrow \mathbb{M}_{1,1}$; cf. plus bas...

phisme de suites exactes

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \hat{\pi}_{0,3} = \mathfrak{Z}_{0,4}^! & \longrightarrow & \mathcal{E}_{0,3} = \mathcal{N}_{0,4} & \longrightarrow & \Pi \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \wr \\
 1 & \longrightarrow & \hat{\mathfrak{Z}}_{1,1}^{'+} & \longrightarrow & \mathcal{E}'_{1,1} & \longrightarrow & \Pi \longrightarrow 1
 \end{array} \quad (31)$$

([avec] $\hat{\mathfrak{Z}}_{1,1}^{'+} = \hat{\mathfrak{Z}}_{1,1}^+ / \{\pm 1\} \simeq SL(2, \mathbb{Z}) / \{\pm 1\}$), qui identifie $\mathcal{E}_{0,3}$ à un sous-groupe ouvert d'indice 6 dans $\mathcal{E}'_{1,1} = \mathcal{E}_{1,1} / \{\pm 1\}$, et itou pour $\hat{\pi}_{0,3}$ dans $\hat{\mathfrak{Z}}_{1,1}^{'+}$. On trouve ainsi un isomorphisme

$$\hat{\pi}_{0,3} \xrightarrow{\sim} \text{Ker}(\mathfrak{Z}_{1,1}^{'+} \rightarrow \mathfrak{S}_3) \simeq (\text{Ker}(\mathfrak{Z}_{1,1}^+ \rightarrow \mathfrak{S}_3)) / \{\pm 1\} \quad (32)$$

compatible avec les actions extérieures de Π . On peut dire aussi qu'on a une structure d'extension

$$1 \rightarrow \hat{\pi}_{0,3} \rightarrow \mathfrak{Z}_{1,1}^{'+} \rightarrow \mathfrak{S}_3 \rightarrow 1 \quad (33)$$

(i.e. $1 \rightarrow \hat{\pi}_{0,3} \rightarrow SL(2, \mathbb{Z}) / \{\pm 1\} \rightarrow SL(2, \mathbb{Z} / 2\mathbb{Z}) \rightarrow 1$) compatible avec les actions de Π (Π opérant trivialement sur \mathfrak{S}_3).

Je finis par m'apercevoir que ce qu'on obtient ici est loin de (22) – cet homomorphisme (22) n'a rien d'injectif, par contre il est surjectif, et ses valeurs sont, non dans $SL(2, \mathbb{Z}) / \{\pm 1\}$, mais dans $SL(2, \mathbb{Z})$ lui-même! Il faudra donc que je revienne encore sur une façon de donner un sens arithmético-géométrique remarquable à (22), et son extension aux groupes profinis correspondants. Pour le moment, je m'en tiens à exploiter un peu (33). Tout d'abord je note que les arguments faits dans le cadre schématique marchent aussi dans le cas transcendant, analytique complexe, et fournissent alors

$$\pi_{0,3} \xrightarrow{\sim} \text{Ker}(\mathfrak{Z}_{1,1}^{'+} \rightarrow \mathfrak{S}_3) = \text{Ker}(SL(2, \mathbb{Z}) / \{\pm 1\} \rightarrow SL(2, \mathbb{Z} / 2\mathbb{Z})) \quad (34)$$

compatible avec (32), ou encore une suite exacte,

$$1 \rightarrow \pi_{0,3} \rightarrow \mathfrak{Z}_{1,1}^{'+} = SL(2, \mathbb{Z}) / \pm 1 \rightarrow \mathfrak{S}_3 = SL(2, \mathbb{Z} / 2\mathbb{Z}) \rightarrow 1. \quad (35)$$

On aimerait interpréter (35) et (33), comme correspondant aux suites exactes analogues liées au diagramme (9), reliant $\pi_{0,3}$ et $\pi'_{0,3}$ – en identifiant $\pi'_{0,3}$ à $\mathfrak{Z}_{1,1}^{'+}$, $\hat{\pi}'_{0,3}$ à $\hat{\mathfrak{Z}}_{1,1}^{'+}$. J'y reviendrai tantôt.

Remarque: On peut se demander si l'homomorphisme

$$\hat{\pi}_{0,3} \rightarrow SL(2, \mathbb{Z}) / \{\pm 1\} \simeq \hat{\mathfrak{Z}}_{1,1}^+ / \{\pm 1\}$$

se remonte ⁶⁵Oui, on peut remonter, et c'est plus ou moins trivial... cf. plus bas... (de façon plus ou moins naturelle) en un homomorphisme

$$\hat{\pi}_{0,3} \rightarrow SL(2, \mathbb{Z})^\wedge \simeq \hat{\mathfrak{Z}}_{1,1}^+,$$

et itou pour les groupes discrets

$$\pi_{0,3} \rightarrow SL(2, \mathbb{Z}) \simeq \mathfrak{Z}_{1,1}^+.$$

Bien sûr, comme $\pi_{0,3}$ et $\hat{\pi}_{0,3}$ sont libres (avec deux générateurs) on peut toujours remonter – d'exactlyment *quatre* façons d'ailleurs (qui nécessairement, dans le cadre profini, respectent les réseaux discrets). Mais peut-on le faire en respectant les opérations de Π ? Il suffirait pour cela qu'on puisse remonter $\mathcal{U}_{0,3} \rightarrow M'_{1,1}$ en $\mathcal{U}_{0,3} \rightarrow M_{1,1}$ (NB. $M_{1,1}$ est une $\mathbb{Z}/2\mathbb{Z}$ -gerbe au dessus de $M'_{1,1}$), et je suspecte, d'après le yoga “anabélien” que j'essaye de développer, que l'inverse doit être vrai ⁶⁶ – que tout relèvement de $\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^+$ commutant aux opérations de Π est défini par un tel relèvement $\mathcal{U}_{0,3} \rightarrow M_{1,1}$. Or l'existence d'un tel relèvement $\mathcal{U}_{0,3} \rightarrow M_{1,1}$ signifierait exactement l'existence d'une famille de courbes elliptiques sur $\mathcal{U}_{0,3}$, avec rigidification de Jacobi d'échelon 2, qui corresponde à l'invariant tautologique λ . Je doute qu'il en existe une, comme je doute que le relèvement en termes de groupes profinis à opération puisse se faire.

A vrai dire, comme $\hat{\mathfrak{Z}}_{1,1}^+ = SL(2, \mathbb{Z})^\wedge$ n'a plus de centre trivial, il n'est plus raisonnable de vouloir “tout exprimer” par les opérations extérieures de Π sur $\hat{\mathfrak{Z}}_{1,1}^+$, il faut plutôt revenir à l'extension $\mathcal{E}_{1,1} = \mathcal{E}_{M_{1,1}}$ de Π par $\hat{\mathfrak{Z}}_{1,1}^+$, et la question est si l'homomorphisme

$$\mathcal{E}_{0,3} \longrightarrow \mathcal{E}'_{1,1} = \mathcal{E}_{1,1}/\{\pm 1\}$$

se remonte en

$$\mathcal{E}_{0,3} \xrightarrow{?} \mathcal{E}_{1,1},$$

ce qui est plus fort que de trouver un relèvement $\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^+$, compatible avec les opérations extérieures de Π . Pour apprécier cette différence, je note que Π opère sur l'ensemble E des quatre relèvements $\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^+$ (interprétés comme homomorphismes extérieurs), et la question posée sous la forme faible est s'il existe un élément de E invariant par Π . S'il n'existait

⁶⁵(*)

⁶⁶Pas tout fait, cf. page suivante pour une formulation plus raisonnable...

A. GROTHENDIECK

pas, il y aurait en tous cas un sous-groupe ouvert de Π , d'indice 2 ou 4, qui laisserait invariant un élément – donc, quitte à passer à l'extension finie correspondante de \mathbb{Q} , on trouve un relèvement, et quitte à passer à une extension un peu plus grande, les *quatre* relèvements possibles commutent à l'action extérieure de Π . Par contre, rien ne prouve que l'on puisse trouver un “germe de relèvement” de $\mathcal{E}_{0,3} \rightarrow \mathcal{E}'_{1,1}$ en $\mathcal{E}_{0,3}^{\flat} \rightarrow \mathcal{E}_{1,1}^{\flat}$ (germes pris par rapport aux sous-groupes ouverts de $\mathcal{E}_{0,3}$ contenant $\hat{\pi}_{0,3}$, ou même tous les sous-groupes ouverts). L'obstruction à remonter sur $\mathcal{E}_{0,3}$ lui-même, i.e. à *scinder* une certaine extension de $\mathcal{E}_{0,3}$ par $\{\pm 1\}$, est

$$\alpha \in H^2(\mathcal{E}_{0,3}, \mathbb{Z}/2\mathbb{Z}), (36)$$

et rien ne dit que cette classe de cohomologie puisse s'effacer, en passant à un sous-groupe ouvert de $\mathcal{E}_{0,3}$.

Mais en termes géométriques, les courbes elliptiques relatives cherchées sur $\mathcal{U}_{0,3}$ forment les sections d'un champ sur $(\mathcal{U}_{0,3})'_{\text{ét}}$ – qui est une $\mathbb{Z}/2\mathbb{Z}$ -gerbe – l'obstruction se trouve donc dans un groupe de Brauer,

$$\beta \in H^2(\mathcal{U}_{0,3}, \mathbb{Z}/2\mathbb{Z}), (37)$$

ou comme $\mathcal{U} = \mathcal{U}_{0,3}$ est une courbe algébrique affine sur un corps (il suffirait qu'elle ne soit pas de type 0,0), il s'en suit que l'homomorphisme canonique (à coefficients de torsion quelconques)

$$H^*(\mathcal{E}_{\mathcal{U}}, -) \longrightarrow H^*(\mathcal{U}, -)$$

est un isomorphisme. D'ailleurs, il doit être plus ou moins trivial que β est l'image de α – ce qui confirme l'intuition que si le relèvement est possible au niveau des groupes fondamentaux profinis (arithmético-géométriques), il l'est aussi au niveau des multiplicités modulaires elles-mêmes, donc qu'on a une existence d'une courbe elliptique relative sur $\mathcal{U}_{0,3}$ qui...

Il est vrai qu'il est bien connu qu'une classe de cohomologie (37) à coefficients de torsion s'efface, en passant à une extension finie du corps de base (\mathbb{Q} en l'occurrence). En fait, on a une suite spectrale

$$H^*(\mathcal{U}_{0,3}, \mathbb{Z}/2\mathbb{Z}) \leftarrow E_2^{p,q} = H^p(\mathbb{Q}, H^q(\overline{\mathcal{U}_{0,3}}, \mathbb{Z}/2\mathbb{Z})), (38)$$

et ici $H^q(\overline{\mathcal{U}_{0,3}}) = 0$ pour $q \geq 2$, donc on trouve une suite exacte

$$\dots E_2^{0,1} = H^q(\mathbb{Q}, H^1(\overline{\mathcal{U}})) \rightarrow E_2^{2,0} = H^q(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(\mathcal{U}_{0,3}) \rightarrow$$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

$$\rightarrow E_2^{1,1} = H^p(\mathbb{Q}, H^1(\overline{\mathcal{U}}) \simeq \mathbb{F}_2^2) \rightarrow E_2^{3,0} = H^3(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \rightarrow \dots$$

Je me rends compte enfin que l'existence d'un relèvement – i.e. de la courbe elliptique hypothétique sur $\mathcal{U}_{0,3}$ – est tout à fait triviale, il suffit de le définir par l'équation

$$y = \sqrt{x(x-1)(x-\lambda)},$$

$$\text{i.e. } y^2 - x(x-1)(x-\lambda) = F(x, y; \lambda) = 0,$$

ce qui définit une courbe plane affine, ou passer en coordonnées projectives

$$F(x, y, z; \lambda) = y^2 z - x^3 + (1 + \lambda)x^2 z - \lambda x z^2 = 0.$$

Je ne vais pas approfondir la question ici, dans quelle mesure ce choix est “naturel”.

Il donne en tous cas un homomorphisme tout ce qu'il y a de précis

$$\mathbb{M}_{0,4}^! \simeq \mathcal{U}_{0,3} \longrightarrow \mathbb{M}_{1,1}, (39)$$

d'où un homomorphisme d'extensions

$$\begin{array}{ccccccc} 1 & \longrightarrow & \hat{\pi}_{0,3} = \mathfrak{Z}_{0,4}^{!+} & \longrightarrow & \mathcal{E}_{0,3} = \mathcal{N}_{0,4}^! & \longrightarrow & \Pi \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & \hat{\mathfrak{Z}}_{1,1}^+ = SL(2, \mathbb{Z})^\wedge & \longrightarrow & \mathcal{E}_{1,1} = \mathcal{N}_{1,1} & \longrightarrow & \Pi \longrightarrow 1 \end{array} \quad (39)$$

défini modulo automorphisme intérieur par un élément de $\hat{\mathfrak{Z}}_{1,1}^+ = SL(2, \mathbb{Z})^\wedge$, et au niveau des groupes discrets,

$$\pi_{0,3} \longrightarrow \hat{\mathfrak{Z}}_{1,1}^+$$

et même,

$$\pi_{0,3} \hookrightarrow \Gamma_2 = \text{Ker}(\hat{\mathfrak{Z}}_{1,1}^+ = SL(2, \mathbb{Z})^\wedge \rightarrow \mathfrak{S}_3 = SL(2, \mathbb{Z}/2\mathbb{Z})) (42)$$

(et itou pour les groupes profinis). Ici $\pi_{0,3}$ est tel que le sous-groupe de congruence du deuxième membre [?], soit Γ_2 soit produit direct [??] sous-groupe $\pi_{0,3}$ et de son centre $\{\pm 1\}$. Mais en fait, il y a exactement quatre sous-groupes dans Γ_2 qui réalisent cette décomposition. Pour ne pas faire de jaloux, on pourrait regarder l'intersection des quatre, qui est un sous-groupe de Γ_2 d'indice un diviseur de $24=16$ [?] ⁶⁷; c'est l'intersection des noyaux de quatre homomorphismes $\Gamma_2 \rightarrow \text{Centre}(\Gamma_2) = \{\pm 1\}$. En tant que sous-groupe de $\pi_{0,3}$, il est d'indice un

⁶⁷NB. Ça doit être le noyau de $SL(2, \mathbb{Z}) \rightarrow SL(2, \mathbb{Z}/4\mathbb{Z})$.

diviseur de 8 [c'est vrai et c'est même trivial...] – ça ne m'étonnerait pas que ce soit justement le groupe des commutateur de $\pi_{0,3}$, qui est d'indice 4 – il y a là toute une situation à élucider...

Bien entendu, il faudrait aussi expliciter l'homomorphisme (42) (défini modulo automorphismes intérieurs) par ses valeurs sur les générateurs l_0, l_1, l_∞ – j'y reviendrai peut-être tantôt⁶⁸.

Théorème:

L'action extérieure naturelle de $\Pi_{\mathbb{Q}}$ sur $\hat{\mathfrak{Z}}_{1,1}^+$, et même sur $\mathfrak{Z}_{1,1}' = \mathfrak{Z}_{1,1}^+ / \{\pm 1\}$, est fidèle.

On utilise le fait qu'on a un homomorphisme extérieur injectif

$$\hat{\pi}_{0,3} \hookrightarrow \hat{\mathfrak{Z}}_{1,1}^{'+},$$

compatible avec l'action de Π , en procédant comme pour la proposition du début (où $\hat{\pi}_{0,3}'$ jouait le rôle de $\hat{\mathfrak{Z}}_{1,1}^{'+}$).

Corollaire:

Les homomorphismes canoniques (surjectifs)

$$\Pi_{\mathbb{Q}} \rightarrow \Pi_{1,\nu} \quad (\nu \geq 1), (43)$$

sont injectifs, donc des isomorphismes.

Il suffit de le prouver pour $\Pi_{\mathbb{Q}} \rightarrow \Pi_{1,1}$ (puisque $\Pi_{1,1}$ est un quotient de $\Pi_{1,\nu}$, $\nu \geq 1$...), or on a un homomorphisme canonique $\Pi_{1,1} \rightarrow \text{Autext } \hat{\mathfrak{Z}}_{1,1}^+$ et on peut considérer le composé,

$$\Pi_{\mathbb{Q}} \rightarrow \Pi_{1,1} \rightarrow \text{Autext } \hat{\mathfrak{Z}}_{1,1}^+ \rightarrow \text{Autext } \mathfrak{Z}_{1,1}^{'+};$$

par le théorème précédent ce composé est injectif, donc aussi $\Pi_{\mathbb{Q}} \rightarrow \Pi_{1,1}$, cqfd.

Remarque: On a vraiment l'impression, avec la proposition du début, et le résultat précédent baptisé "théorème", d'avoir démontré deux fois la même chose, et avec la même démonstration encore! Donc il est temps, après ce détour, de s'assurer qu'il en est bien ainsi, i.e. que l'homomorphisme $\hat{\pi}_{0,3} \rightarrow \hat{\mathfrak{Z}}_{1,1}^{'+}$ qu'on vient d'utiliser s'identifie bel et bien à l'homomorphisme

⁶⁸Il n'est pas clair si $\pi_{0,3}$ est invariant en tant que sous-groupe de $\mathfrak{Z}_{1,1}^+ = SL(2, \mathbb{Z})$, i.e. stable par l'action extérieure de \mathfrak{S}_3 sur $SL(2, \mathbb{Z})$ – je présume que oui, puisque \mathfrak{S}_3 agit aussi extérieurement sur $\pi_{0,3}$ a priori... $\mathfrak{Z}_{1,1}^+ / \pi_{0,3}$ serait une extension centrale intéressante de \mathfrak{S}_3 par $\{\pm 1\}$...

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

$\hat{\pi}_{0,3} \rightarrow \hat{\pi}'_{0,3}$, moyennant un isomorphisme convenable (qui reste à décrire) commutant aux actions extérieures de Π , qu'on se proposait de construire (cf. (10) à (20)) – et on l'a perdu en route, en essayant de trouver $\pi'_{0,3} \xrightarrow{\sim} \mathfrak{F}_{1,1}^{'+}$ par factorisation dans l'homomorphisme composé $\pi_{0,3} \rightarrow \pi'_{0,3} \rightarrow \mathfrak{F}_{1,1}^{'+}$ [la première flèche étant donnée par la surjection canonique] – et on s'est en un sens fourvoyé, car l'homomorphisme “naturel” $\pi_{0,3} \rightarrow \mathfrak{F}_{1,1}^{'+}$ sur lequel on est tombé n'était *pas* du tout celui qu'on avait en vue: j'étais à côté de mes pompes. Donc il me faut revenir à la charge!

§ 37. — THÉORIE DES MODULES DES COURBES ELLIPTIQUES VIA LEGENDRE

(rigidification d'échelon 2)

Je me rends compte que j'ai pas mal compliqué des choses pourtant bien simples, au paragraphe précédent. D'abord un remords de topologie des surfaces:

Proposition: ⁶⁹ Soit X une surface topologique paracompacte, G un groupe discret opérant proprement sur X ; on suppose que pour tout $x \in X$, le stabilisateur G_x opère fidèlement sur un voisinage de x (de sorte que G opère fidèlement – en fait les deux doivent être équivalents) en préservant l'orientation locale (donc G_x est un groupe cyclique) de sorte que $Y = X/G$ est une surface topologique paracompacte. Considérons l'ensemble $X' = \{x \in X \mid G_x \neq (1)\}$ – qui est une partie discrète de X stable sous G – et l'image $Y' \subset Y$ de X' – partie discrète de Y – et la “signature” sur (Y, Y') , pour laquelle le coefficient d_y ($y \in Y'$) est l'indice de ramification $\text{ord}(G_x)$ en les $x \in X$ au dessus de y . Pour tout G -revêtement X' de X , considérons alors $X'/G = Y'$ comme espace au dessus de Y . Alors:

a) Y' est une surface topologique, revêtement ramifié de Y , subordonné à la signature $\underline{d} = \underline{d}(X/Y)$.

⁶⁹**Variante:** \mathcal{G} opère sur X avec sous-groupe *invariant* G satisfaisant les conditions ci-contre [i.e. ci-dessus] on a alors, posant $Y = X/G$ avec opération de $\mathcal{G}/G = \mathcal{H}$ dessus: $\underline{\text{Rev}}(X, \mathcal{G}) \simeq \underline{\text{Rev}}((Y, \underline{d}), \mathcal{H})$, qui donne $\pi_1(X, \mathcal{G}, x) \xrightarrow{\sim} \pi_1((Y, \underline{d}, \mathcal{H}), y)$. Application: $\mathfrak{S}_{0,3} \simeq \mathfrak{Z}'_{1,1} (\simeq GL(2, \mathbb{Z})^+ / \pm 1)$ (où $\mathfrak{S}_{0,3}$ est une extension de $\mathfrak{S}_{0,3} = \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ par $\pi_{0,3}$).

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

b) Le foncteur $X' \mapsto Y' = X'/G$ est une équivalence de catégories:

$$\text{Rev}(X, G) \xrightarrow{\sim} \text{Rev}_{\underline{d}}(Y).(1)$$

N.B. On peut expliciter un foncteur quasi-inverse, en associant à tout revêtement ramifié Y' de Y compatible avec \underline{d} , le (X, G) - revêtement “normalisé” (en un sens topologique facile à expliciter) de $X \times_Y Y'$. On a un énoncé analogue pour les schémas localement noethériens réguliers de dimension 1, où le foncteur quasi-inverse s’obtient en normalisant $X \times_Y Y'$.

Corollaire: Soient $x \in X \setminus X'$, y son image dans Y . On suppose Y connexe (i.e. que G opère transitivement sur l’ensemble des composantes connexes de X). Alors on a un isomorphisme canonique

$$\pi_1(X, G, x) \xrightarrow{\sim} \pi_1((Y, \underline{d}), y)(2)$$

d’où, pour X connexe, une suite exacte canonique

$$1 \rightarrow \pi_1(X, x) \rightarrow \pi_1((Y, \underline{d}), y) \rightarrow G \rightarrow 1.(3)$$

N.B. On a un corollaire analogue dans le contexte schématique, X et Y étant des schémas réguliers de dimension 1 – ou, le cas échéant, des schémas relatifs lisses de dimension relative 1 sur un S , mais dans ce cas il faudrait (si j’en ai besoin) faire un peu attention de préciser l’énoncé en forme raisonnable.

Exemple: Prenons $X = \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\} = \mathcal{U}_{0,3}(\mathbb{C})$, $G = \mathfrak{S}_3$ opérant de façon habituelle, donc (avec les conventions du paragraphe précédent), identifiant $\mathbb{P}^1(\mathbb{C})/(G = \mathfrak{S}_3)$ à $\mathbb{P}^1(\mathbb{C})$, avec:

$$\begin{aligned} (0, 1, \infty) &\mapsto 0 & d_0 &= 2 \\ (2, -1, 1/2) &\mapsto 1 & d_1 &= 2(4) \\ (j, \bar{j}) &\mapsto \infty & d_\infty &= 3, \end{aligned}$$

on trouve $Y = \mathbb{P}^1(\mathbb{C}) \setminus \{0\}$, et $\underline{d} = 2\{1\} + 3\{\infty\}$. On trouve donc un isomorphisme canonique:

$$\pi_1((\mathcal{U}_{0,3}(\mathbb{C}), \mathfrak{S}_3), x) \simeq \pi_1((\mathbb{P}^1(\mathbb{C}) \setminus \{0\}, \underline{d}), y), (5)$$

où malheureusement on ne peut prendre $x = P = j$; il faut prendre $x \in \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty, 2, -1, -1/2, j, \bar{j}\}$ et le plus commode sera de prendre x tel que $y = f(x)$ soit le

A. GROTHENDIECK

point base typique $Q = y$ pour calculer le π_1 à ramification – pour un tel x on trouve donc un isomorphisme canonique

$$\pi_1((\mathcal{U}_{0,3}(\mathbb{C}), \mathfrak{S}_3), x) \simeq \pi'_{0,3}(5 \text{ bis})$$

et en choisissant une \mathfrak{S}_3 -classe de chemins du point base initial $P = y$ sur $X = \mathcal{U}_{0,3}(\mathbb{C})$ vers x , d'où un isomorphisme correspondant du premier membre de (5 bis) avec $\pi_{0,3}$, on trouve un isomorphisme canonique

$$\pi_1((\mathcal{U}_{0,3}(\mathbb{C}), \mathfrak{S}_3), P) \simeq \pi'_{0,3}(6)$$

(qui change par automorphisme intérieur quand on modifie le choix d'une \mathfrak{S}_3 -classe de chemins), d'où la suite exacte

$$1 \rightarrow \pi_{0,3} \rightarrow \pi'_{0,3} \rightarrow \mathfrak{S}_3 \rightarrow 1, (7)$$

qui n'est autre que (9 bis) du paragraphe précédent, mais interprétée ici de façon bien plus transparente comme suite exacte d'homotopie pour \mathfrak{S}_3 opérant sur $\mathcal{U}_{0,3}(\mathbb{C})$. Et on trouve de même, dans le cadre arithmético-géométrique, travaillant sur le schéma $\mathcal{U}_{0,3} = \mathcal{U}_{0,3,\mathbb{Q}}$ et son quotient $\mathcal{U}_{0,3}/\mathfrak{S}_3 \simeq \mathbb{P}_{\mathbb{Q}}^1 \setminus \{0\}$, avec la signature $2\{1\} + 3\{\infty\}$ dessus, le diagramme de suites exactes:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
 1 & \longrightarrow & \hat{\pi}_{0,3} = \hat{\mathfrak{Z}}_{0,4}^+ & \longrightarrow & \hat{\pi}'_{0,3} & \longrightarrow & \mathfrak{S}_3 \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \parallel \\
 1 & \longrightarrow & \mathcal{E}_{0,3} = \mathcal{N}_{0,4}' & \longrightarrow & \mathcal{E}'_{0,3} & \longrightarrow & \mathfrak{S}_3 \longrightarrow 1(8) \\
 & & \downarrow & & \downarrow & & \\
 & & \Pi_{0,4} = \Pi_{\mathbb{Q}} & = & \Pi_{\mathbb{Q}} & & \\
 & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & &
 \end{array}$$

Nous voulons maintenant mettre en relation $\mathcal{U}_{0,3}$, avec l'action de \mathfrak{S}_3 dessus, avec la multiplicité modulaire $M_{1,1}$ pour les courbes elliptiques (indices \mathbb{Q} sous-entendus). C'est dommage d'ailleurs de travailler seulement sur \mathbb{Q} - je vais travailler plutôt sur $\mathbb{Z}[\frac{1}{2}]$ - i.e. en caractéristique résiduelle différente de 2.

Au paragraphe précédent j’ai identifié, un peu vaseusement, $\mathcal{U}_{0,3} = M_{0,4}^!$ à $M_{1,1}[2]'$ (sous lequel $M_{1,1}[2]$ est une gerbe liée par $\mathbb{Z}/2$). Les ennuis techniques (plutôt les complications conceptuelles) tiennent au fait que pour les courbes elliptiques (plus généralement pour les variétés abéliennes de dimension quelconque), si n est un entier ≥ 3 , la “rigidification de Jacobi d’échelon n ” est bel et bien une rigidification, i.e. tout automorphisme d’une courbe elliptique relative E qui induit l’identité sur ${}_nE$ – sous schéma noyau de $n \operatorname{id}_E$ – est l’identité; mais il n’en est plus de même pour $n = 2$, où n est l’identité id_E au-dessus d’une partie ouverte fermée de S et $-\operatorname{id}_E$ sur le complémentaire. Ceci suggère, pour une meilleure compréhension, de coiffer $M_{1,1}[2]$ par un $M_{1,1}[n]$, où n est un multiple de 2; donc $M_{1,1}[n]$ sera un schéma ordinaire de type fini sur $\operatorname{Spec} \mathbb{Z}$ (son image dans $\operatorname{Spec} \mathbb{Z}$ sera l’ouvert $\operatorname{Spec} \mathbb{Z}[\frac{1}{n}]$) et au-dessus de $\operatorname{Spec} \mathbb{Z}[\frac{1}{n}]$, le topos modulaire $M_{1,1}$ se récupère comme

$$M_{1,1} \simeq (M_{1,1}[n], GL(2, \mathbb{Z}/n\mathbb{Z}) = \Gamma_n)(9)$$

au-dessus de $\operatorname{Spec} \mathbb{Z}[\frac{1}{n}]$.⁷⁰ Ici $M_{1,1}[n]$ est le schéma qui représente le foncteur sur (Sch):

$S \mapsto$ ensemble des courbes elliptiques relatives sur S

munies d’un isomorphisme $(\mathbb{Z}/n\mathbb{Z})_S^2 \rightarrow {}_nE$ ⁷¹

sur lequel le groupe $\Gamma_n = GL(2, \mathbb{Z}/n\mathbb{Z}) = \operatorname{Aut}((\mathbb{Z}/n\mathbb{Z})^2)$ opère de façon évidente. Le schéma modulaire “grossier” (par opposition à la multiplicité ou topos modulaire) est décrit au-dessus de $\mathbb{Z}/n\mathbb{Z}$ par

$$\widetilde{M}_{1,1} \simeq M_{1,1}[n]/\Gamma_n(10)$$

au-dessus de $\mathbb{Z}[\frac{1}{n}]$.

N.B. Le schéma $\widetilde{M}_{1,1}$ sur $\operatorname{Spec} \mathbb{Z}$ peut se décrire comme “l’enveloppe représentable” du foncteur non-représentable

$S \mapsto$ classes d’isomorphisme de courbes elliptiques relatives sur S ...

– itou sur un schéma de base (par exemple \mathbb{Q} ou $\operatorname{Spec} \mathbb{Z}[\frac{1}{n}]$), quelconque...

Il faut faire attention qu’en tant que schéma sur $\mathbb{Z}[\frac{1}{n}]$ (ou sur \mathbb{Q} , en passant à la fibre générique), $M_{1,1}[n]$ n’est pas relativement connexe (i.e. n’est pas à fibres géométriquement connexes). En effet, un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})_S^2 \simeq {}_nE$$

⁷⁰Attention, c’est bien $GL(2, \mathbb{Z}/n\mathbb{Z})$ et non $SL(2, \mathbb{Z}/n\mathbb{Z})$ qu’il faut prendre ici.

⁷¹Ce foncteur est représentable si et seulement si $n \geq 3$ (donc il ne l’est pas pour $n = 1, 2$).

A. GROTHENDIECK

implique par passage à la seconde puissance extérieure, un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})_S \xrightarrow{\sim} \bigwedge_{\mathbb{Z}/n\mathbb{Z}}^2 E \simeq \mu_n^{\otimes -1}(S)$$

d'où un isomorphisme

$$\mathbb{Z}/n\mathbb{Z} \simeq \mu(S)$$

qui s'identifie (prenant l'image de 1 mod n) à une section de $\mu_n^*(S)$ où μ_n^* est le $(\mathbb{Z}/n\mathbb{Z})^*$ -torseur relatif sur $\text{Spec } \mathbb{Z}[\frac{1}{n}]$ des “racines primitives n -ièmes de 1”. On a donc un morphisme canonique

$$M_{1,1}[n] \rightarrow \mu_n^*(11)$$

et c'est ce morphisme qui est à fibres géométriques connexes en caractéristique 0. Passant à la limite sur n variable, on trouve *sur* \mathbb{Q}

$$M_{1,1}[\infty] = \varprojlim M_{1,1}[n] \rightarrow \mu_\infty^* \simeq \text{Spec } \Sigma(12)$$

où le dernier isomorphisme est canonique et $\Sigma \subset \mathbb{C}$ est la sous-extension cyclotomique maximale de $\overline{\mathbb{Q}_0}$.

On récupère les $M_{1,1}[n']$, pour $n'|n$, $n' \neq 1, 2$, à partir de $M_{1,1}[n]$ avec l'action de Γ_n dessus par

$$M_{1,1}[n'] \simeq M_{1,1}[n] \times_{\Gamma_n} \Gamma_{n'} \simeq M_{1,1}[n]/K_{n,n'}(13)$$

sur $\text{Spec } \mathbb{Z}[\frac{1}{n}]$, où

$$K_{n,n'} = \text{Ker}(\Gamma_n \rightarrow \Gamma_{n'}).^{72}(14)$$

Si on applique cependant cette formule dans les cas non licites $n'=1$ ou 2 , on trouve pour le cas $n'=1$, non $M_{1,1}$ mais $\widetilde{M}_{1,1}$ (schéma modulaire grossier), et pour $n'=2$, non $M_{1,1}[2]$ (qui n'est pas non plus un schéma), mais ce qu'on avait appelé au paragraphe précédent $M_{1,1}[2]'$.

On peut expliciter $M_{1,1}$ et $\widetilde{M}_{1,1}$ sur $\text{Spec } \mathbb{Z}$ tout entier en termes des $M_{1,1}[n]$ en les décrivant au-dessus des schémas ouverts $\text{Spec}(\mathbb{Z}[\frac{1}{n}])$, $\text{Spec}(\mathbb{Z}[\frac{1}{n'}])$ qui recouvrent $\text{Spec}(\mathbb{Z})$ (i.e. pour $(n, n')=1$) par (9) et (10) en y prenant d'abord n puis n' , et en “recollant” au-dessus de $\text{Spec}(\mathbb{Z}[\frac{1}{nn'}])$, par ces mêmes formules appliquées à nn' ...

On a d'ailleurs (pour mémoire)

⁷² $K_{n,n'}$ opère *librement* sur le schéma si $n'|n$, $n' \neq 1, 2$ mais pas bien sûr si $n' = 1$ ou 2 .

Théorème: $\widetilde{M}_{1,1} \simeq \mathbb{E}_{\mathbb{Z}}^1$ (sur $\text{Spec } \mathbb{Z}$).

On peut épingler un tel isomorphisme (défini à priori modulo le groupe affine entier $X \mapsto \pm X + n, n \in \mathbb{Z}$), en notant qu’il y a dans $\widetilde{M}_{1,1}$ deux sections privilégiées sur \mathbb{Z} , dont les valeurs au point générique correspondent aux deux classes d’isomorphisme de courbes elliptiques en caractéristique 0 (sur \mathbb{C} par exemple) qui ont des automorphismes différents de id , $-\text{id}$ – les deux groupes d’automorphismes qu’on obtient sont d’ailleurs $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ (très facile, par exemple par voie transcendante). Ce sont ce qu’on appelle sauf erreur les courbes elliptiques “anharmoniques”. Sur un

$M_{1,1}[n]$, le groupe des automorphismes rationnels sur k d’une courbe elliptique décrite par un point x de $M_{1,1}[n](k)$ s’identifie canoniquement au stabilisateur de x dans Γ_n :

$$\text{Aut}(E_x) \simeq (\Gamma_n)_x. (15)$$

Bien sûr on a des énoncés idoines sur un schéma de base quelconque, pas nécessairement un corps. Cela montre déjà que les automorphismes des courbes elliptiques sont liés de façon essentielle à la *ramification* de Γ_n opérant sur $M_{1,1}[n]$. On trouve ainsi:

Proposition: (Sur $\text{Spec } \mathbb{Q}$, si $n \neq 1, 2$) Il y a exactement deux orbites de Γ_n opérant sur $M_{1,1}[n]$ qui sont “critiques”, et qui correspondent à des stabilisateurs isomorphes respectivement à $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$, qui sont les groupes d’automorphismes des courbes elliptiques (“anharmoniques”) correspondantes.

On montre que Γ_n n’opère pas fidèlement sur $M_{1,1}[n]$ – le noyau de cette opération est le sous-groupe central $\{\pm 1\}$, image du groupe correspondant de $GL(2, \mathbb{Z})$ – il correspond au groupe des automorphismes “universels” $\pm \text{id}_E$ des courbes elliptiques E . Le groupe quotient

$$\Gamma'_n := \Gamma_n / \{\pm 1\} (16)$$

opère fidèlement, et on peut regarder le “topos mixte” $(M_{1,1}[n], \Gamma'_n)$ – on trouve aussitôt qu’il ne *dépend pas* (à équivalence canonique près) *du choix de n* [à cela près que l’ouvert de $\text{Spec } \mathbb{Z}$ sur lequel “il a un sens” dépend de $n...$] ⁷³ – et en fait, on a:

$$(M_{1,1}[n], \Gamma'_n) \simeq M'_{1,1} (17)$$

⁷³ donc à condition de se placer au dessus d’un schéma de base tel $\text{Spec}(\mathbb{Z}[\frac{1}{nn'}])$ où n, n' sont tous deux inversibles...

au-dessus de $\text{Spec } \mathbb{Z}[\frac{1}{n}]$, où la multiplicité schématique modulaire $M'_{1,1}$ est décrite, en termes de courbes elliptiques “définies modulo symétries”, comme au paragraphe précédent.

Remarque: La proposition précédente semble dépendre de n , mais on voit a priori (grâce au fait que les $\Gamma_{n,n'}, n'|n, n' \neq 1, 2$ opèrent librement) que si elle est valable pour *un* n , elle est valable pour tous.

Notons aussi

Corollaire de la Proposition: En caractéristique 0, les stabilisateurs *dans* Γ'_n (le groupe qui opère fidèlement sur $(M_{1,1}[n])$ des points des deux orbites critiques sont respectivement $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.⁷⁴

On a supposé ici que $n \neq 1, 2$, mais rien ne nous empêche de regarder aussi

$$M_{1,1}[2]' \stackrel{\text{def}}{=} M_{1,1}[2m]/\Gamma_{2m,2} = M_{1,1}[2m]/\Gamma_{2m,2} \quad (18)$$

(où m est un entier quelconque ≥ 2). L'action de $\Gamma_2 \simeq GL(2, \mathbb{Z}/2\mathbb{Z}) \simeq SL(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3 \simeq \Gamma_{2m}/\Gamma_{2m,2}$. Il n'est plus vrai, certes, que $\Gamma_{2m,2}$ opère librement sur $M_{1,1}[2m]$ – car $\Gamma_{2m,2}$ contient l'élément $-1 \in \Gamma_{2m}$ correspondant à la symétrie universelle $-\text{id}_E$ – i.e. à l'élément -1 de $GL(2, \mathbb{Z})$. Mais le résultat général de rigidité rappelé au début implique que

$$\Gamma_{2m,2} := \Gamma'_{2m,2}/\pm 1 \simeq \text{Ker}(\Gamma'_{2m} \rightarrow \Gamma'_2 \simeq \mathfrak{S}_3)$$

opère encore *librement* sur $M_{1,1}[2m]$ – et cela implique que le corollaire de la proposition est valable encore pour l'action de $\Gamma'_2 (\simeq \Gamma_2 \simeq \mathfrak{S}_3)$ sur $M_{1,1}[2]'$.

Digression terminologique: $M_{1,1} = M_{1,1}[1]$ et les $M_{1,1}[n]$, $n \in \mathbb{N}^*$, sont définies a priori comme des *multiplicités* schématiques modulaire, i.e. a) comme des topos localement annelés localement isomorphes au topos étale d'un schéma (en l'occurrence de type fini sur $\text{Spec } \mathbb{Z}$, ou sur \mathbb{Q} si on travaille en caractéristique 0) et b) définis, à équivalence près définie elle-même à isomorphisme unique près, comme “représentant” les foncteurs correspondants

$S \mapsto$ catégorie des courbes elliptiques relatives sur S , avec rigidification

$$\begin{aligned} & \text{d'échelon } n, \text{ i.e. isomorphisme } (\mathbb{Z}/n\mathbb{Z})_S \simeq_n E \\ & = \mathcal{E}ll_n(S) \end{aligned}$$

donc par construction, on a pour tout schéma S une équivalence:

$$\mathcal{E}ll_n(S) \xrightarrow{\sim} \text{Hom}(S, (M_{1,1}[n]))$$

⁷⁴valable pour $n \geq 2$, cf. plus bas.

[où les homomorphismes sont des homomorphismes de topos localement annelés, i.e. homomorphismes de multiplicités).] Pour que les catégories $\mathcal{E}ll_n(S)$ soient *discrètes*, ou encore que $(M_{1,1}[n])$ soit un schéma, ou encore que les automorphismes d'une courbe elliptique respectant une rigidification de Jacobi d'échelon n soient l'identité, il faut et il suffit que $n \geq 3$, i.e. $n \neq 1, 2$. Donc $M_{1,1}[2]$ n'est pas un schéma, mais $M_{1,1}[2]'$ en est un, et $M_{1,1}[2] \rightarrow M_{1,1}[2]'$ est un isomorphisme local (décrit entièrement par une $\mathbb{Z}/2\mathbb{Z}$ -gerbe sur $M_{1,1}[2]'$). Il faut quand même prendre la peine de définir:

$$M_{1,1}[2] \xrightarrow{\text{“théor.”}} (M_{1,1}[2m], \Gamma_{2m,2}) \rightarrow M_{1,1}[2]' \xrightarrow{\text{“défini”}} M_{1,1}[2m]/\Gamma'_{2m,2} (20)$$

(on a aussi $M_{1,1}[2m]/\Gamma'_{2m,2} = M_{1,1}[2m]/\Gamma_{2m,2}$) comme l'homomorphisme canonique de “passage au quotient grossier” qui a un sens chaque fois qu'un groupe discret (disons) G opère sur un schéma (disons) X , comme un morphisme

$$(X, G) \rightarrow X/G = Y (21)$$

dont le foncteur image inverse (faisceaux sur $Y = X/G \rightarrow G$ -faisceaux sur X) est évident. Ici on a un sous-groupe invariant z de G qui opère trivialement sur X , tel que G/z opère librement, ce qui signifie que le morphisme (21) se factorise en

$$(X, G) \rightarrow (X, G/z =: G') \rightarrow Y = X/G = X/G' (22)$$

de sorte que le morphisme de multiplicité (21) s'identifie aussi, simplement, à:

$$(M_{1,1}[2m], \Gamma_{2m,2}) \rightarrow (M_{1,1}[2m], \Gamma'_{2m,2}) \simeq M_{1,1}[2]' (23).$$

Par contre, si on veut descendre jusqu'à $M_{1,1}[1]' = M'_{1,1}$, en passant au quotient (au sens “grossier”) dans $M_{1,1}[n]$ par Γ'_n , l'homomorphisme

$$(M_{1,1}[n], \Gamma'_n) = M'_{1,1} \rightarrow M_{1,1}[n]/\Gamma'_n = \widetilde{M}_{1,1} (24)$$

n'est plus un “isomorphisme”, i.e. n'est plus une équivalence, car Γ'_n n'opère pas librement – il a (même en caractéristique 0) de la ramification de degrés 2, 3. [Si cependant en excluant les courbes elliptiques anharmoniques, ça marcherait – ce n'est “qu'au voisinage” de ces courbes elliptiques que (24) n'est pas un isomorphisme...].

A. GROTHENDIECK

En fait les raisonnements du paragraphe précédent établissent un isomorphisme (valable sur $\text{Spec}\mathbb{Z}[\frac{1}{2}]$)⁷⁵

$$M_{1,1}[2]' \simeq M_{0,4}^! \simeq \mathcal{U}_{0,3}(25)$$

et cet isomorphisme est compatible avec les opérations de

$$\Gamma_2' \simeq \Gamma_2 = GL(2, \mathbb{Z}/2\mathbb{Z}) = SL(2, \mathbb{Z}/2\mathbb{Z})(26)$$

sur $M_{1,1}[2]'$ d'une part, de \mathfrak{S}_3 sur $\mathcal{U}_{0,3}$ d'autre part, quand on considère l'isomorphisme

$$\Gamma_2 = GL(2, \mathbb{F}_2) \xrightarrow{\sim} \mathfrak{S}_3(27)$$

qui associe, à tout automorphisme de \mathbb{F}_2^2 , son action sur les trois éléments non nuls $\underline{\alpha} = (1, 0)$, $\underline{\beta} = (0, 1)$ et $\underline{\gamma} = (1, 1) = \underline{\alpha} + \underline{\beta}$ (de sorte qu'on a d'ailleurs)

$$\gamma = \alpha + \beta, \alpha = \beta + \gamma, \beta = \gamma + \alpha.(28)$$

Il faudrait expliciter cette compatibilité, en considérant l'action naturelle de \mathfrak{S}_4 sur $M_{0,4}^!$, $M_{0,n}^!$ étant la multiplicité modulaire définie par

(29) $\underline{\text{Hom}}_{\text{multipl}}(S, M_{0,n}^!) \simeq$ catégorie des courbes relatives sur S , localement isomorphes à \mathbb{P}_S^1 et munies de n sections mutuellement disjointes numérotées S_1, S_2, \dots, S_n .

N.B. C'est représentable bel et bien par une multiplicité si et seulement si $n \geq 3$, i.e. si le champ des groupoïdes qu'on veut représentés est "rigide",⁷⁶ et alors cette multiplicité est même un schéma, isomorphe d'ailleurs canoniquement au sous-schéma

$\underline{\text{Mon}}(I_{n-3}, \mathcal{U}_{0,3}) \subset \mathcal{U}_{0,3}^{I_{n-3}}$, où ici $I_{n-3} = \{i \in \mathbb{N} \mid 3 \leq i \leq n\}$ – ainsi $M_{0,3}^! \simeq \text{Spec } \mathbb{Z}$ (schéma fini), et $M_{0,4}^! \simeq \mathcal{U}_{0,3} = \mathbb{P}_{\mathbb{Z}}^1 \setminus \{\text{sections } 0, 1, \infty\} = \text{Spec } \mathbb{Z}[T][1/\{T(T-1)\}]$.

Mais on fera attention qu'il y a une opération naturelle de \mathfrak{S}_n sur $M_{0,n}^!$, donc sur $\underline{\text{Mon}}(I_{n-3}, \mathcal{U}_{0,3})$ – alors que l'on ne voit a priori que l'action de $\mathfrak{S}_3 \times \mathfrak{S}_{n-3}$ sur ce dernier: l'isomorphisme canonique

$$M_{0,n}^! \simeq \underline{\text{Mon}}((I_{n-3}, \mathcal{U}_{0,3}) \subset \mathcal{U}_{0,3}^{I_{n-3}} \text{ (où } I_{n-3} = \{i \in \mathbb{N} \mid 3 < i \leq n\}))(30)$$

⁷⁵L'image de $M_{1,1}[2]'$ dans $\text{Spec } \mathbb{Z}$ est $\text{Spec } \mathbb{Z}[\frac{1}{2}]$ tandis que celle de $M_{0,4}^! \simeq \mathcal{U}_{0,1}$ est $\text{Spec } \mathbb{Z}$ tout entier.

⁷⁶Si on veut une représentabilité pour $n = 0, 1, 2$, il ne suffit plus de travailler avec une topologie étale – il faut des topologies fppf par exemple.

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

ne tient compte que des opérations naturelles du sous-groupe

$$\mathfrak{S}_3 \times \mathfrak{S}_{n-3} \subset \mathfrak{S}_n (31)$$

de \mathfrak{S}_n sur $M_{0,n}^!$, et pas de celle de \mathfrak{S}_n tout entier. Dans le cas de $n = 4$, l'opération de $\Gamma'_2 = GL(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$ sur $M_{0,4}^!$ qui nous intéresse est celle qui correspond au sous-groupe $\mathfrak{S}_1 \times \mathfrak{S}_3$ qui fixe le premier élément (correspondant à la section nulle d'une courbe elliptique) et qui permute les trois suivants (correspondant aux trois éléments d'ordre 2 d'une courbe elliptique générique en caractéristique différente de 2, qui sont les trois autres points fixes de $x \mapsto -x$), alors que l'opération naïve de \mathfrak{S}_3 sur $\mathcal{U}_{0,3}$ correspond au sous-groupe $\mathfrak{S}_3 \times \mathfrak{S}_1$ dans \mathfrak{S}_4 , qui fixe les trois premiers éléments. Petite question de gymnastique schématique (indépendante maintenant de la géométrie des courbes elliptiques, mais histoire de géométrie projective de dimension 1): comment passer d'une de ces actions de \mathfrak{S}_3 à l'autre? On a envie de prouver que ce sont les mêmes !

Notons que si I est un ensemble à 4 éléments, alors il lui est associé un ensemble à 3 éléments de "partitions de type (2,2)", $P_{2,2}(I) = \tilde{I}$, et l'homomorphisme

$$\mathfrak{S}_I \simeq \mathfrak{S}_4 \rightarrow \mathfrak{S}_{\tilde{I}} \simeq \mathfrak{S}_3 (32)$$

est surjectif – son noyau est un sous-groupe isomorphe (non canoniquement) à $\mathbb{F}_2 \times \mathbb{F}_2$ – donc un groupe commutatif $V(I)$ annulé par 2, i.e. un espace vectoriel sur \mathbb{F}_2 , et en tant que tel de dimension 2. En fait, $V(I)$ opérant sur I fait de I un $V(I)$ -torseur – donc I est muni canoniquement d'une structure de plan affine sur \mathbb{F}_2 , et $V(I) \subset \mathfrak{S}_I$ est le groupe de ses translations. \mathfrak{S}_I s'interprète comme le groupe des automorphismes affines de I (*toute* permutation de I est affine – il y a sur l'ensemble I une et une seule structure de plan affine sur \mathbb{F}_2), et $\mathfrak{S}_{\tilde{I}}$ comme le groupe $\text{Aut}(V(I))$ – ce qui suggère d'interpréter \tilde{I} comme l'ensemble des trois éléments non nuls de $V(I)$, et en fait, on constate que l'on a une bijection canonique

$$\tilde{I} \xrightarrow{\sim} V(I)^* \stackrel{\text{def}}{=} V(I) \setminus \{0\} (33)$$

en associant à une partition $I = I' \cup I''$, avec I', I'' de cardinal 2, la seule permutation de I qui invarie I', I'' et induit sur chacun une permutation non triviale (les éléments de \mathfrak{S}_I obtenus ainsi sont les *permutations paires d'ordre 2*, qui avec l'identité forment donc le sous-groupe $V(I)$).

A. GROTHENDIECK

On trouve, si $i \in I$, d'où $I \setminus \{i\}$ de cardinal 3, une application canonique

$$I \setminus \{i\} \rightarrow \tilde{I} \quad (34)$$

en associant à $j \in I \setminus \{i\}$ la partition de I en $\{i, j\}$ et en son complémentaire. Cette bijection étant compatible avec le transport de structure, on en conclut que l'isomorphisme correspondant

$$\mathfrak{S}_{I \setminus \{i\}} \simeq \mathfrak{S}_{\tilde{I}} \quad (35)$$

est aussi le composé

$$\mathfrak{S}_{I \setminus \{i\}} \hookrightarrow \mathfrak{S}_I \rightarrow \mathfrak{S}_{\tilde{I}}, \quad (35)$$

($\mathfrak{S}_{I \setminus \{i\}}$ étant le stabilisateur de i dans \mathfrak{S}_I) donc les quatre sous-groupes symétriques d'indice 3 $\mathfrak{S}_{I \setminus \{i\}}$ de \mathfrak{S}_I ($i \in I$) sont canoniquement isomorphe à $\mathfrak{S}_{\tilde{I}}$ – donc entre eux, par des isomorphismes qui sont d'ailleurs déduits des bijections canoniques

$$I \setminus \{i\} \xrightarrow{\sim} I \setminus \{j\} \quad (i \neq j, i, j \in I), \quad (37)$$

égales à la *transposition* (non à l'identité) sur $I \setminus \{i, j\}$. Cette bijection en effet est le composé

$$I \setminus \{i\} \xrightarrow{\sim} \tilde{I} \xrightarrow{\sim} I \setminus \{j\},$$

et pour i, j variables, ces isomorphismes forment un système transitif d'isomorphismes.

Revenant à l'action de \mathfrak{S}_4 sur $M_{0,4}^!$, la clef de la compréhension est donnée par ceci:

Proposition: Considérons le sous-groupe $V(I)$ de \mathfrak{S}_I formé de l'identité et des involutions paires. Alors l'action de $V(I)$ sur $M_{0,I}^!$ ⁷⁷ est triviale, donc \mathfrak{S}_I agit sur $M_{0,I}^!$ par l'intermédiaire de $\mathfrak{S}_I/V(I) = \mathfrak{S}_{\tilde{I}}$.

Corollaire: Soit $i \in I$, alors l'action de $\mathfrak{S}_{I \setminus \{i\}} \subset \mathfrak{S}_I$ sur $M_{0,I}^!$ est déduite de celle de $\mathfrak{S}_{\tilde{I}}$ via l'isomorphisme $\mathfrak{S}_{I \setminus \{i\}} \xrightarrow{\sim} \mathfrak{S}_I$ provenant de $I \setminus \{i\} \xrightarrow{\sim} \tilde{I}$.

En particulier, pour $I = [1, 2, 3, 4]$, pour comparer l'action de $\mathfrak{S}_{\{1,2,3\}}$ et de $\mathfrak{S}_{\{2,3,4\}}$ sur $M_{0,4}^! \simeq \mathcal{U}_{0,3}$ – où la première est l'action standard de \mathfrak{S}_3 sur $\mathcal{U}_{0,3}$, la deuxième celle de \mathfrak{S}_3 sur $M1, 1[2]'$, on utilise l'isomorphisme

$$\mathfrak{S}_{\{1,2,3\}} \simeq \mathfrak{S}_{\{2,3,4\}} \quad (38)$$

⁷⁷N.B. $M_{0,I}^!$ se définit en termes de I , pour tout ensemble I de cardinal ≥ 3 comme $M_{0,4}^!$

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

explicité dans (37), correspondant à la bijection

$$1 \mapsto 4, 2 \mapsto 3, 3 \mapsto 2$$

des ensembles d'indices, qui correspond donc à l'automorphisme

$$\text{int}(\sigma_1) : \mathfrak{S}_3 \rightarrow \mathfrak{S}_3 \quad (39)$$

en identifiant maintenant les deux ensembles d'indices $[1, 2, 3], [2, 3, 4]$ à $[0, 1, \infty]$, et en désignant par $\sigma_i \in \mathfrak{S}_{\{0,1,\infty\}}$ (pour $i \in \{0, 1, \infty\}$) la transposition des éléments $\neq i$. Donc

Corollaire: L'isomorphisme canonique

$$\mathcal{U}_{0,3} \xrightarrow{\varphi} M_{1,1}[2]' \quad (\text{sur } \mathbb{Z}[\frac{1}{2}]),$$

quand on fait opérer $\mathfrak{S}_3 = \mathfrak{S}_{\{0,1,\infty\}}$ sur l'un et l'autre membre, est compatible avec ces opérations, *via* l'automorphisme $\text{int}(\sigma_1)$, i.e.

$$\varphi(u \cdot x) = (\sigma_1 u \sigma_1^{-1}) \cdot \varphi(x) \quad (40)$$

Il faut quand même démontrer la proposition 4, qui équivaut bien sûr à ceci:

Corollaire: Soit X une droite projective relative sur un schéma S , I un ensemble à quatre éléments, $(S_i)_{i \in I}$ une famille de sections mutuellement disjointes, et σ une involution paire de I (correspondant à une partition $I = \{i_1, i_2\} \cup \{i_3, i_4\}$ par $\sigma i_1 = i_2, \sigma i_2 = i_1, \sigma i_3 = i_4, \sigma i_4 = i_3$). Alors il existe un automorphisme (évidemment unique) u de X , tel que $u \circ s_i = s_{\sigma i}$.

Démonstration: On peut supposer que $X = \mathbb{P}_S^1, s_1 = 0, s_2 = \infty$; donc s_3, s_4 s'identifient à des sections de \mathcal{O}_S^* ; on prendra u défini par

$$u(z) = \frac{\lambda}{z}, \quad \lambda \in \Gamma(S, \mathcal{O}_X^*)$$

qui échange 0 et ∞ , et la condition pour échanger s_3, s_4 s'écrit $\frac{\lambda}{s_3} = s_4, \frac{\lambda}{s_4} = s_3$, i.e. $\lambda = s_3 s_4$ (N.B. il suffirait que (s_1, s_2, s_3) et (s_1, s_2, s_4) soient mutuellement disjointes – pas la peine que s_3, s_4 soient mutuellement disjointes...)

Plaçons nous à nouveau sur \mathbb{Q} (pour fixer les idées), et considérons les groupes fondamentaux des multiplicités modulaires $M_{1,1}, M'_{1,1}$. On part de

$$M_{1,1} \simeq (M_{1,1}[n], \Gamma_n)$$

A. GROTHENDIECK

$$n \geq 3 M'_{1,1} \simeq (M_{1,1}[n], \Gamma'_n = \Gamma_n / \pm 1) \quad n \geq 2 \quad (41)$$

(ou pour

$n=2$ on remplace $M_{1,1}[2]$ par $M_{1,1}[2]'$), qui donne des isomorphismes de groupes extérieurs

$$\begin{array}{ccc} \pi_1(M_{1,1}) \simeq \pi_1(M_{1,1}[n], \Gamma_n) & (n \geq 3) & \\ \downarrow & \downarrow & \\ \pi_1(M'_{1,1}) \simeq \pi_1(M_{1,1}[n], \Gamma'_n) & (n \geq 2) & \end{array} \quad (42)$$

(où comme au (41) si $n = 2$), et comme $M_{1,1}[n]$ est connexe (même s'il n'est pas géométriquement connexe)⁷⁸, on trouve

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi_1(M_{1,1}[n]) & \longrightarrow & \pi_1(M_{1,1}) & \longrightarrow & \Gamma_n \longrightarrow 1 \\ & & \downarrow \wr & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \pi_1(M_{1,1}[n]) & \longrightarrow & \pi_1(M'_{1,1}) & \longrightarrow & \Gamma'_n \longrightarrow 1 \end{array} \quad (43)$$

qui permet de reconstruire $\pi_1(M_{1,1})$, en tant qu'extension de Γ_n , quand on connaît $\pi_1(M'_{1,1})$ comme extension de Γ'_n , par image inverse via $\Gamma_n \rightarrow \Gamma'_n$. On trouve comme de juste

Proposition: $\pi_1(M_{1,1})$ est une extension centrale de $\pi_1(M'_{1,1})$ par $\{\pm 1\}$.

D'autre part, on a les suites exactes d'homotopie sur $\text{Spec } \mathbb{Q}$

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi_1(\overline{M_{1,1}}) & \longrightarrow & \pi_1(M_{1,1}) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \pi_1(\overline{M'_{1,1}}) & \longrightarrow & \pi_1(M'_{1,1}) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1 \end{array} \quad (44)$$

(avec les isomorphismes $\pi_1(\overline{M_{1,1}}) \simeq \mathfrak{S}_{1,1}^+$, $\pi_1(M_{1,1}) \simeq \mathfrak{S}_{1,1} \simeq \mathcal{N}_{1,1}$) et la théorie transcendante fournit des isomorphismes extérieurs canoniques⁷⁹

$$\pi_1(\overline{M_{1,1}}) \simeq SL(2, \mathbb{Z})^\wedge, \quad \pi_1(\overline{M'_{1,1}}) \simeq SL(2, \mathbb{Z})^\wedge = SL(2, \mathbb{Z})^\wedge / \pm 1, \quad (45)$$

On a la compatibilité essentielle suivante entre (43), (44), (45): la commutativité de

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi_1(\overline{M_{1,1}}) \simeq SL(2, \mathbb{Z})^\wedge & \longrightarrow & \pi_1(M_{1,1}) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1 \\ & & \downarrow \text{surj} & & \downarrow & & \downarrow \chi_n \\ 1 & \longrightarrow & SL(2, \mathbb{Z}/n\mathbb{Z}) \hookrightarrow \Gamma_n = GL(2, \mathbb{Z}/n\mathbb{Z}) & \xrightarrow{\det} & (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & 1 \end{array} \quad (46)$$

⁷⁸c'est le théorème de Kronecker d'irréductibilité de l'équation cyclotomique.

⁷⁹Attention; ne pas confondre $SL(2, \mathbb{Z})^\wedge$ avec $SL(2, \hat{\mathbb{Z}})$!!!

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

(où χ_n est le caractère cyclotomique).

Passant à la limite sur n , ceci donne un diagramme commutatif

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \pi_1(\overline{M_{1,1}}) \simeq SL(2, \mathbb{Z})^\wedge & \longrightarrow & \pi_1(M_{1,1}) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1 \\
 & & \downarrow \text{surj} & & \downarrow & & \downarrow \chi \\
 1 & \longrightarrow & SL(2, \hat{\mathbb{Z}}) \hookrightarrow & GL(2, \hat{\mathbb{Z}}) & \longrightarrow & \hat{\mathbb{Z}}^* & \longrightarrow 1
 \end{array} \quad (47)$$

diagramme sur lequel nous allons revenir.

Pour l'instant je vais exploiter le deuxième isomorphisme (42) pour $n = 2$:

$$\pi_1(M'_{1,1}) = \mathcal{N}'_{1,1} \simeq \pi_1(M_{1,1}[2]', \Gamma_2 = \mathfrak{S}_3) \simeq \pi_1(\mathcal{U}_{0,3}, \mathfrak{S}_3), \quad (48)$$

où le dernier isomorphisme correspond à l'isomorphisme $\text{int}(\sigma_1) : \mathfrak{S}_3 \xrightarrow{\sim} \mathfrak{S}_3$, explicité dans (40). On trouve donc bien, comme prévu au paragraphe précédent – et de façon entièrement conceptuelle, l'isomorphisme d'extension

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \pi_1(\overline{M'_{1,1}}) & \longrightarrow & \pi_1(M'_{1,1}) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1 \\
 & & \downarrow \wr & & \downarrow \wr & & \parallel \\
 1 & \longrightarrow & \pi_1(\overline{\mathcal{U}_{0,3}}, \mathfrak{S}_3) & \longrightarrow & \pi_1(\mathcal{U}_{0,3}, \mathfrak{S}_3) & \longrightarrow & \Pi_{\mathbb{Q}} \longrightarrow 1
 \end{array} \quad (49)$$

où l'on a $\pi_1(\overline{M'_{1,1}}) = \hat{\mathfrak{X}}_{1,1}^{'+} \simeq SL(2, \mathbb{Z})^\wedge$, $\pi_1(M'_{1,1}) \simeq \mathcal{N}'_{1,1}$, $\pi_1(\overline{\mathcal{U}_{0,3}}, \mathfrak{S}_3) \simeq \hat{\pi}'_{0,3}$ et $\pi_1(\mathcal{U}_{0,3}, \mathfrak{S}_3) \simeq \mathcal{E}'_{0,3}$. D'ailleurs, reprenant ces réflexions dans le contexte transcendant, on voit que cet isomorphisme

$$\hat{\pi}_{0,3}/\{l_1^2, l_\infty^3\} = \hat{\pi}'_{0,3} \xrightarrow{\sim} \pi_1(\overline{M'_{1,1}}) = SL(2, \mathbb{Z})^\wedge = SL(2, \mathbb{Z})'/\pm 1 \quad (50)$$

est associé à un isomorphisme

$$\pi_{0,3}/\{l_1^2, l_\infty^3\} = \pi'_{0,3} \xrightarrow{\sim} SL(2, \mathbb{Z})' = SL(2, \mathbb{Z})/\pm 1 \quad (51)$$

déduit de l'isomorphisme de multiplicités analytiques complexes

$$M'_{1,1}{}^{\text{an}} \simeq (\mathcal{U}_{0,3}^{\text{an}}, \mathfrak{S}_3). \quad (52)$$

Il faudrait quand même expliciter l'homomorphisme (51) – qui n'est défini que modulo automorphisme intérieur, a priori, par des formules explicites – alors que sa définition ici sort de

A. GROTHENDIECK

façon purement conceptuelle, “géométrique” (au sens de la géométrie algébrique relative, des courbes rationnelles et elliptiques sur des espaces analytiques arbitraires). C’est là un calcul clef, sûrement instructif, qui ne devrait pas présenter de difficulté particulière...

J’ai un peu laissé tomber en chemin dans tout ça le schéma modulaire “grossier” $\widetilde{M}_{1,1}$, après avoir affirmé qu’il est isomorphe à $\mathbb{E}_{\mathbb{Z}}^1$ et qu’il y a deux sections marquées, dont les valeurs en caractéristique 0 correspondent aux deux classes d’isomorphisme de courbes elliptiques anharmoniques. En termes de l’isomorphisme

$$\widetilde{M}_{1,1} \simeq M_{1,1}[2]'/\Gamma_2' \simeq \mathcal{U}_{0,3}/\mathfrak{S}_3 \quad (53)$$

(valable sur $\text{Spec } \mathbb{Z}[\frac{1}{2}]$), on trouve bien, au dessus de $S = \text{Spec } \mathbb{Z}[\frac{1}{2}]$, que $\widetilde{M}_{1,1}$ se déduit d’un schéma relatif Y qui est localement (au sens étale) isomorphe à \mathbb{P}_S^1 , en enlevant une section s , dont l’existence implique déjà que Y est globalement isomorphe à \mathbb{P}_S^1 – donc $Y \setminus s(S)$ isomorphe à \mathbb{E}_S^1 . Dans cette approche, on a donc envie de désigner par ∞ (non par 0, comme en théorie des cartes !) cette section, qui correspond aux “points à l’infini” $(0, 1, \infty)$ de $\mathcal{U}_{0,3}$, ou encore au “point à l’infini” de $\widetilde{M}_{1,1}$. Il est d’ailleurs facile de vérifier a priori (par la compactification de Deligne-Mumford de $M_{1,1}$ et de $\widetilde{M}_{1,1}$) que $\widetilde{M}_{1,1}$ sur $\text{Spec } \mathbb{Z}$ tout entier est de la forme $Y \setminus \text{Im } s$, où Y est lisse et propre sur $\text{Spec } \mathbb{Z}$ tout entier, et s une section – dès lors ce qu’on connaît par exemple sur la fibre géométrique, et le fait que \mathbb{Z} est principal, impliquent que $Y \simeq \mathbb{P}_{\mathbb{Z}}^1$, et qu’on a donc $\widetilde{M}_{1,1} \simeq \mathbb{E}_{\mathbb{Z}}^1$. Pour choisir cet isomorphisme, on utilise les deux sections de $\mathbb{E}_{\mathbb{Z}}^1$, correspondant aux courbes anharmoniques. Ces deux sections *ne sont pas disjointes*, elles se rencontrent en caractéristique 2 et en caractéristique 3 (pour ce qui se passe en caractéristique $\neq 2$, i.e. sur $\text{Spec } \mathbb{Z}[\frac{1}{2}]$, on le voit bien par l’isomorphisme (53) – car en caractéristique 3 les deux orbites $(2, -1, \frac{1}{2})$ et (j, \bar{j}) coïncident et se collapsent en un seul et même point). Mais prenant l’une de ces sections comme section nulle (sauf erreur c’est celle qui correspond à la courbe elliptique la plus riche en symétries, à savoir le groupe $\mathbb{Z}/6\mathbb{Z}$, qu’on prend – c’est une question de convention bien sûr – c’est donc aussi l’orbite $\{j, \bar{j}\}$, correspondant à un stabilisateur isomorphe à $\mathbb{Z}/3\mathbb{Z}$), cela détermine l’isomorphisme $\widetilde{M}_{1,1} \simeq \mathbb{E}_{\mathbb{Z}}^1$ au signe près. L’autre section devient alors un entier de la forme $\pm 2^a 3^b$ ($a, b \in \mathbb{N}^*$ – entiers bien déterminés dont je ne sais pas la valeur par coeur), et on achève de normaliser en exigeant que le signe soit *plus*. Donc

Théorème: (pour mémoire – c’est bien connu)

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

Il y a un isomorphisme unique

$$\widetilde{M}_{1,1} \simeq \mathbb{E}_{\mathbb{Z}}^1(54)$$

qui en caractéristique 0 donne à la courbe anharmonique de groupe d'automorphisme $\mathbb{Z}/6\mathbb{Z}$ l'invariant 0, et à celle de groupe $\mathbb{Z}/4\mathbb{Z}$ un invariant > 0 (qui sera nécessairement $2^a 3^b$, avec $a, b \in \mathbb{N}^*$ bien déterminés, mais par moi oubliés... $b = 3$, cf. ci-dessous).

En termes de l'isomorphisme

$$\widetilde{M}_{1,1} \simeq \mathcal{U}_{0,3}/\mathfrak{S}_3 \subset \mathbb{P}^1/\mathfrak{S}_3$$

valable sur $\text{Spec } \mathbb{Z}[\frac{1}{2}]$, ceci correspond à un isomorphisme entre $\mathbb{P}^1/\mathfrak{S}_3$ et \mathbb{P}^1 qui à l'orbite $(0, 1, \infty)$ associe ∞ (non 0), et à l'orbite (j, \bar{j}) associe 0 (non ∞), à l'orbite $(2, -1, \frac{1}{2})$ le fameux $2^a 3^b$ (et non 1). La fonction (invariant modulaire)

$$\mathcal{J}(\lambda) \in \mathbb{Q}(\lambda)(55)$$

qui réalise cet isomorphisme, i.e. le morphisme

$$\mathbb{P}_{\mathbb{Z}}^1 \xrightarrow{\mathcal{J}} \mathbb{P}_{\mathbb{Z}}^1(56)$$

correspondant (de degré 6, avec $\mathcal{J} \circ u = \mathcal{J}, u \in \mathfrak{S}_3$) est donc lié à celle inspirée de la théorie des cartes, soit $f(\lambda)$, par

$$\mathcal{J}(\lambda) = 2^a 3^b f(\lambda)^{-1}(57).$$

D'ailleurs, $f(\lambda)$ (ou $\mathcal{J}(\lambda)$) se calcule aisément par la connaissance de ses zéros et de ses pôles, avec leurs multiplicités, et la “normalisation” pour la valeur de f (ou de \mathcal{J}) sur une des sections $2, -1, \frac{1}{2}$; on trouve immédiatement

$$f(z) = \frac{3^3}{2^2} \frac{z^2(z-1)^2}{(z^2 - z + 1)^3}, (58)$$

donc,

$$\mathcal{J}(z) = 2^{a+2} 3^{b-3} \frac{(z^2 - z + 1)^3}{z^2(z-1)^2}. (59)$$

Comme $\mathcal{J}(\lambda)$ doit garder un sens en caractéristique 3, et ne peut pas être constante, ceci montre d'ailleurs que $b = 3$, donc (59) s'écrit aussi

$$\mathcal{J}(z) = 2^{a+2} \frac{(z^2 - z + 1)^3}{z^2(z-1)^2},$$

A. GROTHENDIECK

mais on se rappellera que cette formule n'est pertinente – ne permet de calculer l'invariant d'une courbe elliptique – que si la caractéristique est différente de 2, heureusement! Pour décrire

$$M_{1,1} \longrightarrow \mathbb{E}_{\mathbb{Z}}^1(60)$$

(et en particulier pour déterminer l'autre invariant modulaire critique $2^a 3^3$, i.e. pour déterminer a) aussi au voisinage de 2 – disons en caractéristique différente de 3 – il faut une étude des courbes elliptiques qui ne passe plus par la représentation (de Legendre, sauf erreur) $y^2 = \sqrt{x(x-1)(x-\lambda)}$, ou encore, par la rigidification de Jacobi d'échelon 2, mais par celle d'échelon 3.

Remarques: on voit tout de suite que le quotient $\mathbb{P}_{\mathbb{Z}}^1/\mathfrak{S}_3$ s'identifie à $\mathbb{P}_{\mathbb{Z}}^1$ de façon unique en prenant comme images des orbites $(0, 1, \infty)$ et (j, \bar{j}) les sections 0 et ∞ (par exemple, en suivant la convention qui correspond à la théorie des cartes), et en prenant comme image de l'orbite $(2, -1, \frac{1}{2})$ un nombre rationnel qui soit > 0 .

Ceci est possible a priori, car on note que les orbites $(0, 1, \infty)$ et (j, \bar{j}) ne coïncident en aucune caractéristique, donc correspondent à des sections disjointes de $Y = \mathbb{P}_{\mathbb{Z}}^1/\mathfrak{S}_3$, tandis que l'orbite constante $(2, -1, \frac{1}{2})$ coïncide avec la première en caractéristique 2, avec la deuxième en caractéristique 3 (et ce sont là les deux seules coïncidences qui peuvent arriver).

On voit donc a priori que la troisième section sera de la forme $2^\alpha/3^\beta$, avec $\alpha, \beta \in \mathbb{N}^*$. Le calcul explicite est d'ailleurs évident; l'homomorphisme composé

$$\mathbb{P}_{\mathbb{Z}}^1 \xrightarrow{f_1} \mathbb{P}_{\mathbb{Z}}^1/\mathfrak{S}_3 \simeq \mathbb{P}_{\mathbb{Z}}^1(61)$$

doit être de la forme $f_1 = c f$, avec la constante $c \in \mathbb{Q}$ choisie de telle façon que $c f$ se réduise bien en toute caractéristique (ce qui détermine c modulo le signe), et que $f_1(-1) = c f(-1) = c > 0$ (ce qui lève l'indétermination du signe). On trouve alors

$$f_1(\lambda) = \frac{\lambda^2(\lambda-1)^2}{(\lambda^2-\lambda+1)^2} = \frac{2^2}{3^3} f(\lambda), (62)$$

donc

$$f_1(-1) = \frac{2^2}{3^3} \quad (\text{donc } \alpha = 2, \beta = 3). (63)$$

Mais on fera attention qu'au voisinage de la caractéristique 2, ces calculs ne se rapportent plus à $\widetilde{M}_{1,1}$ et $\widehat{M}_{1,p}$ où la configuration des trois sections n'est pas la même qu'ici...

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

Sur la lancée de ces réflexions, il serait naturel de regarder de plus près le schéma

$$M_{1,1}[4] \text{ sur lequel agit } \Gamma_4 = GL(2, \mathbb{Z}/4\mathbb{Z}) \text{ via } \Gamma'_4 = \Gamma_4 / \pm 1 (64)$$

et l'homomorphisme

$$M_{1,1}[4] \longrightarrow M_{1,1}[2]' \simeq \mathcal{U}_{0,3}(65)$$

compatible avec

$$\Gamma'_4 = GL(2, \mathbb{Z}/4\mathbb{Z}) / \pm 1 \rightarrow \Gamma'_2 = \Gamma_2 \simeq GL(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3.^{80}$$

Un calcul immédiat, compte tenu que $(\mathbb{Z}/4\mathbb{Z})^* \simeq \{\pm 1\}$ donne

$$\text{Card } \Gamma_4 = 2 \text{Card } SL(2, \mathbb{Z}/4\mathbb{Z}) = 8 \text{Card } SL(2, \mathbb{Z}/2\mathbb{Z}) = 16 \text{Card } \Gamma_2 = 16 \times 6.$$

Donc

$$\text{Card}(\Gamma'_{4,2} = \text{Ker}(\Gamma'_4 \rightarrow \Gamma'_2)) = 8(66)$$

i.e. $M_{1,1}[4]$ est un revêtement galoisien de $M_{1,1}[2]'$ d'ordre 8. Notons qu'il n'est pas géométriquement connexe sur \mathbb{Q} , ou sur $\text{Spec } \mathbb{Z}[\frac{1}{2}]$, puisque $M_{1,1}[4]$ se trouve sur l'extension quadratique μ_4^* , de $\text{Spec } \Lambda$ où $\Lambda = \mathbb{Z}[\frac{1}{2}]$, qui n'est autre que $\Lambda(i)$. On a une factorisation de $M_{1,1}[4] \rightarrow M_{1,1}[2]'$:

$$\begin{array}{ccccc} M_{1,1}[4] & \longrightarrow & (\mathcal{U}_{0,3})_S & \xrightarrow{2} & M_{1,1}[2]' \simeq \mathcal{U}_{0,3} \\ & \searrow & \downarrow & & \downarrow \\ & & S^1 = \mu_4^* & \xrightarrow{2} & \text{Spec } \mathbb{Z}[\frac{1}{2}] = S \end{array} \quad (67)$$

[où les flèches horizontales sont galoisiennes du degré indiqué et] où maintenant

$$M_{1,1}[4] \longrightarrow M_{1,1}[2]''_S = (\mathcal{U}_{0,3})'_S$$

est un revêtement galoisien dont le groupe est le noyau de $\Gamma'_{4,2} \xrightarrow{\det} \{\pm 1\}$, ou encore celui de $SL(2, \mathbb{Z}/4\mathbb{Z})' \rightarrow SL(2, \mathbb{Z}/2\mathbb{Z})$, que nous allons désigner par $SI'_{4,2}$, qui est d'ordre 4.

⁸⁰En fait le noyau de l'homomorphisme $GL(k, A) \rightarrow GL(k, A/\mathcal{J})$ est toujours un groupe commutatif – et même un A/\mathcal{J} -module isomorphe à $(A/\mathcal{J})^4$ – si \mathcal{J} est un idéal de carré nul d'un anneau A . Donc ici $\text{Ker}(GL(2, \mathbb{Z}/4\mathbb{Z}) \rightarrow GL(2, \mathbb{Z}/2\mathbb{Z}))$ est un groupe *commutatif*, et même un espace vectoriel sur \mathbb{F}_2 ; il est isomorphe à \mathbb{F}_2^4 .

A. GROTHENDIECK

Proposition: Le groupe

$$S\Gamma_{4,2} = \text{Ker}(SL(2, \mathbb{Z}/4\mathbb{Z}) \rightarrow SL(2, \mathbb{Z}/2\mathbb{Z})) \quad (68)$$

est isomorphe à $\mathcal{T}L(2, \mathbb{F}_2)$ (groupe des matrices de trace nulle à coefficients dans \mathbb{F}_2), avec l'opération évidente de $SL(2, \mathbb{F}_2)$ dessus, et le sous-groupe $\{\pm 1\}$ correspond aux matrices scalaires – le quotient $S\Gamma'_{4,2}$ des deux est isomorphe à \mathbb{F}_2^2 (de façon idiote et pas canonique du tout!). Regardant $M_{1,1}[4]$ comme un revêtement galoisien de $M'_{1,1}[2]_{S'} = (\mathcal{U}_{0,3})_{S'}$, on trouve géométriquement “le” revêtement *abélien* universel de $\mathcal{U}_{0,3}$ de groupe annulé par 2 (et pour cause), qui a comme groupe de Galois $(\mathbb{F}_2)^{\{0,1,\infty\}}/(\text{diagonale})$.⁸¹

Enfin, tout est essentiellement tautologique, mais un calcul amusant à faire sera de redécrire l'action de $SL(2, \mathbb{F}_2)$ sur $\mathcal{T}L(2, \mathbb{F}_2)/$ (matrices scalaires), de façon à l'identifier à l'action de \mathfrak{S}_3 sur $\mathbb{F}_2^{\{0,1,\infty\}}/(\text{diagonale})$. Comme revêtement de

$$\widetilde{M_{1,1S'}} \simeq M_{1,1}[4]/S\Gamma'_4 \simeq M_{1,1}[2]_{S'}/\Gamma'_2 \quad (69)$$

$M_{1,1}[4]$ est un revêtement galoisien d'ordre 24 ($=4 \cdot 6$) de groupe $SL(2, \mathbb{Z}/4\mathbb{Z})'$. Ce serait bien qu'on n'ait pas un isomorphisme

$$SL(2, \mathbb{Z}/4\mathbb{Z})' \simeq \mathfrak{S}_4 \quad (70)$$

(où \mathfrak{S}_4 est le groupe des automorphismes de l'octaèdre), et que $M_{1,1S'}$ ne soit le revêtement de $\mathbb{P}_{S'}^1 \setminus \{0, 1, \infty\}$, avec ramification compatible avec $2\{1\} + 3\{\infty\}$, qui correspond à l'*octaèdre* dans la théorie des cartes – on devrait avoir sur $S' = \text{Spec } \mathbb{Z}[\frac{1}{2}][i]$ un isomorphisme canonique

$$M_{1,1}[4]_{S'} \simeq \text{courbe de Fermat } x^r + y^r + z^r = 0 \text{ (sur } S') \quad (71)$$

dont le groupe d'automorphismes est justement une extension de \mathfrak{S}_3 par

$$\mu_2^{\{0,1,\infty\}}/(\text{diagonale})!$$

⁸¹NB Ce sont les 4 supplémentaires de ce sous-espace $\mathbb{F}_2 \hookrightarrow \mathcal{T}L(2, \mathbb{F}_2)$ qui forment un tore sur le dual de $V = \mathcal{T}L(2, \mathbb{F}_2)$, qui devraient correspondre aux quatre relèvements en $\pi_{0,3} \hookrightarrow \mathfrak{S}_{1,1}^+ = SL(2, \mathbb{Z})$; cf. plus haut sur ces questions.

⁸²Il vaudrait mieux écrire l'équation de Fermat ici $x_0^r + x_1^r + x_\infty^r = 0$.

LA LONGUE MARCHE À TRAVERS LA THÉORIE DE GALOIS

Pour bien faire, il faudrait expliciter la relation entre courbes elliptiques E (sur un schéma S au dessus de $\mathbb{Z}[\frac{1}{2}][i]$) munies d'une rigidification de Jacobi d'échelon 4, e_1, e_2 avec $e_1 \wedge e_2 = [i]^{-1}$, et solutions "non triviales" de l'équation

$$x^r + y^r + z^r = o(72)$$

sur S , i.e. les systèmes de sections $x, y, z \in \Gamma(S, O_S^*)$ satisfaisant (72), modulo multiplication par un "scalaire" $\alpha \in \Gamma(S, O_S^*)$ – ou encore, rompant la symétrie en posant $X = x/z, Y = y/z$, les solutions de l'équation

$$X^r + Y^r = -1 (= i^2), X, Y \in \Gamma(S, O_S^*) \dots (73)$$

On a ainsi interprété $M_{1,1}[2]'$ et (modulo des vérifications et une étude un peu plus poussée) $M_{1,1}[4]$, en relation avec deux cartes triangulaires pondérées régulières – la carte "diédrale" ou carte triangulaire pondérée universelle (trois sommets $0, 1, \infty$, trois arêtes, deux faces qui sont des triangles, type $(p, q) = (3, 3)$), et la carte *octogonale*, qui est un revêtement d'ordre 4 de celle-ci (étale en dehors de $\{0, 1, \infty\}$).

Il serait bien aussi de regarder de plus près les variétés modulaires congruentielles $M_{1,1}[3]$ et $M_{1,1}[5]$, correspondant à des groupes modulaires "géométriques":

$$S\Gamma'_3 = SL(2, \mathbb{F}_3)/\pm 1 \text{ (d'ordre 12)} \subset GP(1, \mathbb{F}_3) \text{ (d'ordre 24)} \simeq \mathfrak{S}_4 \quad \text{en fait on doit avoir } S\Gamma'_4 \simeq \mathfrak{A}_4, S\Gamma'_5 = SL(2, \mathbb{F}_5)$$

Sauf erreur, ces groupes sont respectivement les groupes \mathfrak{A}_4 du *tétraèdre* orienté et celui \mathfrak{A}_5 de l'icosaèdre orienté. Si je me rappelle bien, les cas $n = 2, 3, 4, 5$ épuisent les cas de courbes modulaires congruentielles $M_{1,1}[n]$ qui soient *rationnelles*. C'est une chose remarquable qu'on trouve par exemple tous les polyèdres réguliers finis à faces des triangles [sauf un, à arêtes repliées - celui de la figure (76), cf. plus bas...]; il était clair a priori, par l'isomorphisme entre $\mathfrak{S}'_{1,1}$ et le "groupe cartographique triangulé orienté" $\pi'_{0,3}$, qu'on devrait retrouver tous les polyèdres réguliers finis à faces des triangles de cette façon, mais non pas que ce soit des sous-groupes de congruences, très exactement. Le tableau obtenu est alors le suivant:

groupe $G = S\Gamma'_n$ courbe modulaire type du polyèdre

$$D_3 \simeq \mathfrak{S}_3 \qquad M_{1,1}[2]' \text{ triangles } \mathfrak{A}_4 \qquad M_{1,1}[3] \text{ tétraèdre } \mathfrak{S}_4$$

A. GROTHENDIECK

Comme autres courbes modulaires (pas congruentielles) rationnelles galoisiennes sur $\tilde{M}_{1,1}$, il y aurait encore les quotients des précédents par les sous-groupes invariants de ST'_n , distincts du groupe entier et de 1. On trouve comme quotients possibles:

- a) Cas \mathfrak{S}_3 : le quotient $\{\pm 1\}$ (via signature).
- d) Cas \mathfrak{A}_4 : le quotient $\mathbb{Z}/3\mathbb{Z} = \mathfrak{A}_3$ (via $\mathfrak{S}_4 \rightarrow \mathfrak{S}_3$ induisant $\mathfrak{A}_4 \rightarrow \mathfrak{A}_3$).
- c) Cas \mathfrak{S}_4 : le quotient \mathfrak{S}_3 , et le quotient $\{\pm 1\}$ de celui-ci.
- (pour d il n'y a rien, \mathfrak{A}_5 étant un groupe simple).

Les courbes modulaires rationnelles obtenues se réduisent aux deux cas a) et b) (qui sont retrouvés dans c)). Dans le cas a), on trouve le revêtement quadratique de $Y = \mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\}$, qui est non ramifié en ∞ (car l'indice de ramification devrait diviser 2 et 3), qui correspond donc au revêtement $y = \sqrt{x(x-1)}$ et à la carte sphérique de type (2,1) (sommets d'indice 2, faces d'indice 1), formée d'un sommet avec une arête (équateur) délimitant deux faces qui sont des monogones.

Le cas b) est le revêtement cyclique d'ordre 3, ramifié seulement en 0 et en ∞ (en 1, l'indice de ramification doit être diviseur de 2 et de 3, donc est 1) avec carte sphérique de type (3,3), avec des arêtes qui sont des boucles repliées:

(76) 1 seul sommet, 3 arêtes repliées qui en sortent, une face triangulaire.

Les variétés modulaires sont trop proches de $\tilde{M}_{1,1}$ – avec un groupe d'automorphismes (quotient de $\Gamma'_\infty = SL(2, \mathbb{Z})$) trop petit, pour pouvoir être rigidifiantes; il faudrait que le groupe de Galois-Poincaré du revêtement soit multiple de 12 (multiple de 4 et 6!), pour que la courbe modulaire ait une chance d'être rigidifiante. Ces cas semblent donc nettement moins intéressants.

Il y aurait lieu par ailleurs, dans chacun des trois cas restants de (75) (mis à part donc le premier cas, qui correspond à $M_{1,1}[2]'$ et est à peu près compris), d'expliciter la relation entre les points des courbes rationnelles correspondantes, et entre courbes elliptiques à rigidification de Jacobi, d'échelon respectivement 3,4,5. Il y a sûrement des choses précises dans Klein, mais on aimerait faire des choses un peu plus fines, qui soient valables simultanément en toute caractéristique, i.e. sur des schémas de base généraux. Ce souci semble intuitivement lié à la question des opérations de $\Pi_{\mathbb{Q}}$ sur les classes d'isomorphismes des cartes, et plus particulièrement des cartes sphériques régulières. C'est assez extraordinaire que **, depuis trois ans que la question est là, n'y ait pas encore touché. Dieu sait qu'elle est juteuse!

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

Complément sur les rapports anharmoniques:

Soient x_1, x_2, x_3, x_4 des sections partout distinctes de \mathbb{P}_S^1 , on veut construire la section correspondante de $\mathcal{U}_{0,3} = \mathbb{P}_S^1 \setminus \{0, 1, \infty\}_S$. Soient a, b, c, d sections locales de \underline{O}_S , avec $ad - bc$ inversible, telles que:

$$u = u_{a,b,c,d} : z \mapsto \frac{az + b}{cz + d} \quad (77)$$

transforme (x_1, x_2, x_3) en $(0, 1, \infty)$ – on aura donc

$$\lambda = u(x_4). \quad (78)$$

Les conditions sur (a, b, c, d) pour $ux_1 = 0$ etc sont

$$ax_1 = 0, \quad ax_2 + b = cx_2 + d, \quad cx_3 + d = 0$$

qui donnent, si par exemple a est inversible (sinon on peut supposer c inversible), en résolvant en b, c, d [ici quelques lignes de calcul élémentaire omises]:

$$\lambda(x_1, x_2, x_3, x_4) = \frac{(x_4 - x_1)(x_2 - x_3)}{(x_2 - x_1)(x_4 - x_3)}. \quad (79)$$

En tant que fonction rationnelle en x_1, x_2, x_3, x_4 (à coefficients dans un anneau intègre fixé), λ est caractérisé par les deux propriétés:

- a) invariance par rapport à une (même) transformation homographique sur les variables x_1, x_2, x_3, x_4 , $f(ux_1, ux_2, ux_3, ux_4) = f(x_1, x_2, x_3, x_4)$, et
- b) $f(0, 1, \infty, x_4) = x_4$ (avec un grain de sel pour donner un sens au premier membre).

On a de plus

- c) une propriété remarquable de symétrie, qu'on explicite en définissant un homomorphisme de \mathfrak{S}_4 dans le groupe homographique (moralement, $GP(1)$)

$$\begin{array}{ccc} \sigma \in \mathfrak{S}_4 & \xrightarrow{\sigma \mapsto \varphi_\sigma} & GP(1) \\ & \searrow & \nearrow \\ & \mathfrak{S}_3 & \end{array}$$

de telle façon qu'on ait

$$\lambda(x_{\sigma^{-1}1}, x_{\sigma^{-1}2}, x_{\sigma^{-1}3}, x_{\sigma^{-1}4}) = \varphi_\sigma(\lambda(x_1, x_2, x_3, x_4)) \dots \quad (80)$$

§ 38. — DÉTERMINATION DE $\pi_{0,3}[\]$

§ 39. — PROPRIÉTÉS DE CONGRUENCE DE L'OPÉRATION DE $\Pi_{\mathbb{Q}}$
 SUR $\hat{\pi}_{0,3}$,
 LIÉES À L'HOMOMORPHISME $\mathcal{N}_{1,1} \longrightarrow \mathrm{GL}(2, \hat{\mathbb{Z}})$

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — RÉSUMÉ DES PREMIERS EXPOSÉS DE A. GROTHENDIECK
RÉDIGÉ PAR P. DELIGNE

§ I. — NOTES ANABÉLIENNES

§ II. — NOTES ANABÉLIENNES

§ III. — NOTES ANABÉLIENNES

§ IV. — NOTES ANABÉLIENNES

§ V. — NOTES ANABÉLIENNES

§ VI. — NOTES ANABÉLIENNES

§ VII. —STRUCTURE À L'INFINI DES $M_{g,\nu}$

I. Courbes standard

Soit k un corps algébriquement clos. Une “courbe standard” sur k est un schéma X sur k satisfaisant les conditions suivantes :

- a) X quasi-projectif, toute composante irréductible est de dim 1
- b) Tout point de X est soit lisse, soit un “point quadratique” (ordinaire) - i.e. isom (loc. ét) à la courbe $\text{Spec}(k[X, Y]/XY)$ au point 0.

Il est connu qu'on peut [] \widehat{X} de X , telle que X soit un schéma propre, [] X s'identifie à un ouvert dense de \widehat{X} , et que \widehat{X} soit lisse sur les points de $\widehat{X} \setminus X = I$. Alors \widehat{X} est une courbe projective, I est une partie finie de $\widehat{X}(k)$ contenant [] ouvert des points des lissité de \widehat{X} . [] A des points singuliers de X s'identifie à []

La donnée de X équivaut à celle des (\widehat{X}, I) , où \widehat{X} est un schéma projectif, dont toute composante irréductible est de dim 1, et dont l'ensemble singulier est formé des points [] ordinaires - et I est un sous-schéma fini étale de \widehat{X}^{lisse} , ou ce qui revient au même, une partie finie de $\widehat{X}^{lisse}(k)$.

Soit

Ainsi, à la courbe standard X nous avons associé les systèmes de données suivantes :

[]

Inversement, [] on construit une courbe standard X en passant au quotient dans $\widetilde{A}_k Y \setminus I_k$ par l'involution σ - i.e. X est universel [] pour la donnée p :

[]

soumise à $(pi)\sigma = pi$.

Ainsi la catégorie des courbes standard sur k [] apparaît comme équivalente à celle des systèmes a) b) c) ci-dessus. (pour les iso)...

N.B. On récupère \widehat{X} comme quotient de Y par σ .

Généralisation sur une base quelconque.

Une *courbe standard* sur S (multiplicité schématique, disons) [] défini constructivement en termes d'un système a), b), c) comme ci-dessus, i.e.

[]

On construit alors $\widehat{X} = Y/\sigma$, contenant $A = \widetilde{A}/\sigma$ et I comme sous-schémas fermés finis étales sur S , et [] $X = \widehat{X} \setminus I$. On peut montrer que le foncteur

$$(Y, \widetilde{A}, \widehat{I}, \sigma_{\widetilde{A}}) \mapsto X$$

des systèmes (5) (pour les iso) vers les schémas relatifs [], est *pleinement fidèle* ⁽¹⁾.

N.B. []

[]

(par abus de langage, puisque c'est non seulement le schéma relatif Y , mais Y avec la structure supplémentaire $\widetilde{A}, I, \sigma_{\widetilde{A}} \dots$).

II. Graphe associé à une courbe standard

Revenons au cas d'un corps de base k algébriquement clos, pour commencer. Soit X une courbe standard, d'où $Y, I, \widetilde{A}, \sigma_{\widetilde{A}}$.

Posons

$$S = \pi_o(Y) \simeq [] \text{ des corps irréductibles de } X(7)$$

On a alors le diagramme d'application canoniquement entre ensembles finis

$$[](8)$$

où q est de degré 2 et définit l'involution $\sigma_{\widetilde{A}}$. Les applications σ et p sont induites par les [] en passant aux π_o .

¹faux tel quel

A. GROTHENDIECK

Le système $(\tilde{A} \xrightarrow{\sigma} S, \sigma_{\tilde{A}})$ où $[\]$, peut être considéré comme définissant un *graphe*, dans S est l'un des sommets, et \tilde{A} l'un des $[\]$ l'application σ étant l'application "origine d'un $[\]$ ". Ce graphe ne dépend que de \widehat{X} , pas de X i.e. des choix de $I \subset \widehat{X}(k)$. C'est $[\]$ compte de ce choix que l'on considère, $[\]$ plus de la structure de graphe, le donnée supplémentaire

$$I \longrightarrow S(9)$$

Le graphe indique comment les composantes irréductibles de X (figurés par les sommets) se récupèrent deux à deux - les points d'intersections, i.e. les points singuliers ("doubles" $[\]$) de X , correspondant aux arêtes. Si une composante irréductible X_α correspond au sommet α des graphes, alors les $[\]$ fermés en α correspondent biunivoquement aux points doubles de X_α - donc $[\]$ X_α sont lisses $[\]$ l'extrémité.

Il est clair que tout graphe fini peut être obtenue (à iso près) par une \widehat{X} convenable - et même avec des composantes X_α de genre g_α donné (i.e. des \tilde{X}_α de genre $g_\alpha \dots$). De plus, $[\]$ $I \longrightarrow S$ (I $[\]$ fini), cela peut être réalisé par un $I \subset \widehat{X}^{lisse}$, i.e. par une courbe standard S .

La *maquette* d'une courbe standard X consiste, pour définition, en les données suivantes $[\]$

Une structure formée d'un graphe fini $G = (S, \tilde{A}, \sigma)$, d'un ensemble fini I au dessus de l'une des sommets de G , et d'une application "genre": $S \xrightarrow{g} N$, $[\]$ appelé ici une "maquette".

Proposition. — Considérons la maquette d'une courbe standard X

a) Soient $\alpha, \beta \in S$, alors α, β appartiennent à la même composante connexe de graphe G , si et seule si X_α et X_β appartiennent à la même composante connexe de X . Donc on a une bijection canonique

$$\pi_0(G_X) \simeq \pi_0(X), (11)$$

en particulier X est connexe si et seule si G_X est connexe.

b) Supposons X connexe i.e. \widehat{X} connexe, i.e. $[\]$ on a alors $[\]$ i.e. $[\]$ où $[\]$

.

III. Courbes "stables" et MD-graphes

Une courbe standard (sur k algébriquement clos) est "stable", si elle satisfait à l'un des conditions équivalentes suivantes

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

- a) $\text{Aut } X$ est fini
- b) Pour tout α , $(Y_\alpha, I_\alpha \cup \tilde{A}_\alpha)$ est anabélien i.e. $2g_\alpha + \hat{v}_\alpha \geq 3$ i.e. $2g_\alpha - 2 + \hat{v}_\alpha \geq 1$, i.e.
 - 1) Si $g_\alpha = 1$, on a $\hat{v}_\alpha \geq 1$
 - 2) Si $g_\alpha = 0$, on a $\hat{v}_\alpha \geq 3$
- c) Tout champ de vecteurs sur Y nul sur $I \cup \tilde{A}$ est nul.
- d) $\underline{\text{Aut}}_{(Y, \tilde{A}_k, I)}$ est un schéma en groupes fini étale sur k . On voit que cette condition (sous la forme b)) ne dépend que de la *maquette* de la courbe. On dit que X est une *MD-courbe* (MD, initiale de “Mumford-Deligne” ou de “modulaire”) si elle est stable, et 0-connexe (i.e. connexe non vide).

Les maquettes de telles courbes sont les maquettes 0-connexes et stables (i.e. dont les sommets de guère 1 sont de poids total ≥ 1 , et les sommets de guère 0 sont de poids total ≥ 3), on les appellera les MD-graphes.

NB. Une maquette est une MD-graphe si et seule si

- a) elle est 0-connexe (i.e. le graphe G est connexe $\neq \emptyset$)
- b) elle n'est pas réduit à un seul sommet de guère 1, de poids total 0 []
- c) les sommets []

Proposition. — Si $(G = (S, \tilde{A}, \sigma), I, \underline{g} : S \longrightarrow N)$ est une MD-graphe, son type (g, ν) est anabélien, i.e. $2g + \nu \geq 3$.

Si on avait $g = 1, \nu = 0$, alors la relation

$$g = 1 = \sum g_\alpha + h_1$$

montre que ou bien tous les g_α sont nuls et h_1 [], ou bien tous les g_α sauf une g_{α_0} sont nuls, []

[]

Soit G une maquette. On dit qu'une courbe standard sur un corps algébriquement clos est *de type* G , si sa maquette est isomorphe à G , on dit qu'elle est *G-épinglée* si on se donne un isomorphisme entre sa maquette et G (c'est donc une structure []).

A. GROTHENDIECK

Soit $(\widehat{X}, \underline{I})$ une courbe standard sur une base S quelconque, on dit qu'elle est de type G si ses fibres géométriques sont de type G . Alors les maquettes des fibres géométriques de $(\widehat{X}, \underline{I})$ forment les fibres d'une schéma en maquettes (ou un MD-graphe) sur S $(\underline{S}, \underline{\tilde{A}}, \sigma_{\underline{\tilde{A}}}, \underline{I}, \underline{\tilde{A}} \longrightarrow \underline{S}, \underline{I} \longrightarrow \underline{S}, \underline{S} \xrightarrow{g} N_S)$ (système de revêtements finis étales de S et de morphismes entre ceux-ci), localement isomorphe à la maquette G donnée. On appelle G -épinglage entre $(\widehat{X}, \underline{I})$ tout isomorphisme entre G_S et $\underline{G}(\widehat{X}, \underline{I})$. Si

$$\Gamma = \text{Aut } G(18)$$

(groupe fini), les G -épinglages de $(\widehat{X}, \underline{I})$ s'identifient aux sections d'une certain Γ_S -torseur, appelé *torseur de G -épinglages* de $(\widehat{X}, \underline{I})$.

Considérons, sur une base S fixée, le catégorie $([])$ des courbes standard G -épinglées. Pour tout $\alpha \in S$

N.B. Si $\text{card } J = \nu$, alors

$[]$ Il en est donc de même dans $M_{g,J}$, donc ainsi de M_G (pour G semi-stable) et de $M_{[G]} = (M_G, \Gamma)$.

IV. La théorie de Mumford-Deligne

Soient S une multiplicité schématique, X un schéma relatif sur S , propre sur S , \underline{I} une sous-schéma fermé de X . On dit que (X, \underline{I}) est une MD-courbe relative sur S , si X, \underline{I} sont plats de présentation finie sur S , et si pour tout point géométrique de S , la fibre $(X_{\bar{s}}, \underline{I}_{\bar{s}})$ est une MD-courbe géométrique sur $k(s)$ i.e. $X_{\bar{s}}$ est 0-connexe, de dimension 1, $[]$ c'est une fonction localement constant sur S .

Fixons nous une type numérique (g, ν) *anabélien* ($2g + \nu \geq 1$), et considérons, pour S variable, le groupoïde fibré

$$S \mapsto \widehat{M}_{g,\nu}(S) = \text{MD-courbes relatives sur } S, \text{ de type numérique égal à } (g, \nu)(24)$$

On a alors le vraiment $[]$ théorème suivant :

Théorème de Mumford-Deligne ⁽²⁾. — *Le groupoïde fibré $S \mapsto \widehat{M}_{g,\nu}/S$ sur Sch (plus généralement, sur les multiplicités schématiques...) est représentable pour une multiplicité schématique*

²On suppose $2g + \nu \geq 3$ (cas anabélien)

$\widehat{M}_{g,v}$, qui est lisse et propre sur $\text{Spec } Z$, D'autre part $M_{g,v}$ est un ouvert de Zariski de $\widehat{M}_{g,v}$, schématiquement dense fibre par fibre.

On en déduit aisément p. ex. la connexité des fibres géométriques
[]. Nous allons revenir là dessus maintenant.

V. Spécialisation des MD-graphes

Soit

VI. Morphismes de [] de graphes et de maquettes

VII. Étude des [] de $\dim \leq 2$ [] détermination des graphes correspondantes

VIII. Structure []

XI. Structure groupoïdale des multiplicités modulaires de Teichmüller variables ([] MDT-structure) : cas [],

X. Structures MDT analytiques : []

XI. Digression : [] Structure à l'infini des groupoïdes fondamentaux

XII. Digression (suite) : topos canoniques associés à une [] et leur dévisages en "topos élémentaires"

XIII. Digression sur stratification "locales" []

Une stratification globale

§ VIII. — TEICHMÜLLER

§ IX. — NOTES ANABÉLIENNES

I. Résultats de fidélité

À tout corps K , associons son topos étale B_K , qui est un topos (profini) galoisien. Le groupoïde des points de B_K est noté Π_K , il est anti-équivalent canoniquement à la catégorie des clôtures algébriques séparables de K . Si \bar{K} est une telle clôture, son groupe des K -automorphismes $\text{Gal}(\bar{K}/K)$ ou $E_{\bar{K}/K}$ s'identifie au groupe des automorphismes des points de B_K associé à \bar{K}/K (il vaut peut-être mieux de dire : à l'opposé de ce groupe - le [] des clôtures algébriques de K est comme celle des foncteurs fibres, à l'opposée de celles des points ...) Bien entendue, B_K se reconstitue à partir de Π_K , comme le topos des systèmes locaux (continues) sur Π_K - et en termes de $E_{\bar{K}/K}$, comme le topos des ensembles discrets à actions continues de $E_{\bar{K}/K}$.

Pour un homomorphisme de corps $K \longrightarrow K'$, i.e. un homomorphisme de schémas $\text{Spec } K' \longrightarrow \text{Spec } K$, on a un morphisme de topos correspondant

$$B_{K'} \longrightarrow B_K(1)$$

associé à un homomorphisme de groupoïdes fondamentaux

$$\Pi_{K'} \longrightarrow \Pi_K.(2)$$

Ceci s'exploitait en disant qu'un objet [] $\Pi_{K'}$ (i.e. point de $B_{K'}$, ou revêtement universel de $B_{K'}$, ou clôture \bar{K}' de K') en définit un des Π_K (ainsi, on prend $\bar{K} =$ clôture algébrique de K' dans \bar{K}') et pour deux points correspondants, on a un homomorphisme de groupes

A. GROTHENDIECK

fondamentaux correspondants, qui s'interprète par exemple comme

$$E_{\overline{K'}/K'} \longrightarrow E_{\overline{K}/K}(3)$$

et qui peuvent de reconstitue l'homomorphisme de topos comme une "restriction des scalaires".

L'image de (3) est le sous-groupe fermé de $E_{\overline{K}/K}$ qui correspond à la sous-extension K_1 de \overline{K}/K , clôture algébrique de K dans K' , i.e. $K_1 = \overline{K} \cap K'$.

$$\begin{array}{ccc} K & \longrightarrow & K' \\ \downarrow & & \downarrow \\ \overline{K} & \longrightarrow & \overline{K'} \end{array}$$

Quand K' est une extension de type fini de K , K_1 est une extension finie de K , et on es conduit que l'image de (3) est alors un sous-groupe d'indice fini, égale à $E_{\overline{K},K}$ si et seule si $K_1 = K$ i.e. K est séparablement algébrique clos dans K' . D'ailleurs, on montre sans mal que (si K est extension de type fini) l'homomorphisme (3) est injectif si et seule si K' est une extension algébrique de K . Donc il est bijectif si et seule si K' est une extension de K . Dans le suite nous nous bornons (précisément) aux corps de caractéristique 0, et la condition précédente signifie alors que $K \longrightarrow K'$ est un *isomorphisme*.

Ainsi, le foncteur $K \longrightarrow B_K$ ou $K \longrightarrow \Pi_K$, ou $(K, \overline{K}) \longrightarrow E_{\overline{K}/K}$, est *conservatif* quand on se limite comme morphismes de corps $K \longrightarrow K'$ (de caractéristique 0) à ceux que fait de K' une extension de type fini de K .

P. ex. Il suffit de se limiter aux extensions de type fini des corps fermées \mathbb{Q} - on trouve un foncteur conservatif de la catégorie de ces corps dans celles de groupoïdes (ou de topos), au sens: un ⁽¹⁾ morphisme de corps qui donne une équivalence de groupoïdes (ou de topos) est un *isomorphisme*.

Quand on prend des corps quelconques, le 2-foncteur $K \longrightarrow B_K$ ou $K \longrightarrow \Pi_K$ ou $(K, \overline{K}) \longrightarrow E_{\overline{K}/K}$ est cependant loin d'être fidèle. Ainsi, si K est séparablement clos, B_K est le "topos ponctuel", Π_K le groupoïde ponctuel, $E_{\overline{K}/K} \simeq 1$ - il est donc que les morphismes entre corps séparablement clos ne sont pas décrits par les morphismes entre leurs topos étales, ou groupoïdes fondamentaux! Pour cette raison, il y a lieu d'associer à un corps K un objet plus

fin que B_K ou Π_K , à savoir le système projectif des B_{K_i} , ou des Π_{K_i} , pour K_i sous-corps de K de type fini sur le corps $[\]$, et à un système (K, \bar{K}) le système projectif des $E_{\bar{K}_i/K_i}$, où \bar{K}_i est le clôture algébrique séparablement clos K_i dans \bar{K} . On $[\]$

$$\begin{cases} \Pi_K \simeq \varprojlim \Pi_{K_i} \\ B_K \simeq \varprojlim B_{K_i} \\ E_{\bar{K}/K} \simeq \varprojlim E_{\bar{K}_i/K_i} \end{cases} \quad (4)$$

i.e. on reconstitue les objets B_K , Π_K , $E_{\bar{K}/K}$ à partir des systèmes projectifs correspondant - mais l'inverse n'est pas vrai. En fait, comme le foncteur $\text{Ind}(\text{Corps type fini}) \longrightarrow \text{corps de la catégorie des systèmes inductifs de corps de type fini}$, vers celle des corps, est une équivalence de catégories (pour des raisons triviales), il s'ensuit que les foncteurs $K \longrightarrow B_K$, ou $K \longrightarrow \Pi_K$, ou $(K, \bar{K}) \longrightarrow E_{\bar{K}/K}$, étant des corps vers les propriétés idoines, avoir $[\]$ les propriétés de fidélité des foncteurs $K \longrightarrow B_K$, ou $K \longrightarrow \Pi_K$, ou $(K, \bar{K}) \longrightarrow \Gamma_{\bar{K}/K}$ $[\]$ aux corps de type fini, auxquels nous allons pour la suite nous $[\]$, $[\]$ des temps. Mais il sera nécessaire au cours de travail, de donner une description algébrique, par exemple, de pro-groupes finis associé par exemple à \mathbb{C} (plus précisément, à (\mathbb{C}, \mathbb{C}) !).

Le rôle dominant sous joué par le corps premier de caractéristique 0, \mathbb{Q} donc pour $B_{\mathbb{Q}}$ et $\Pi_{\mathbb{Q}}$, qui a un objet canonique, noté $\bar{\mathbb{Q}}_0$ - la clôture algébrique de \mathbb{Q} dans \mathbb{C} . On posera ⁽²⁾

$$\Pi_{\mathbb{Q}} = E_{\bar{\mathbb{Q}}_0/\mathbb{Q}}(5)$$

Pour tout corps K de caractéristique 0 - en particulière pour ces corps K de type fini sur \mathbb{Q} , lequel nous allons nous $[\]$ par le suite - on a donc des homomorphismes canoniques

$$B_K \longrightarrow B_{\mathbb{Q}} \quad \Pi_K \longrightarrow \Pi_{\mathbb{Q}}(6)$$

qui l'explicitait, quand on a choisi un objet de Π_K i.e. un \bar{K}/K , d'où un $\bar{\mathbb{Q}}/\mathbb{Q}$, pour un homomorphisme de groupes profinis

$$E_{\bar{K}/K} \longrightarrow \Gamma_{\bar{\mathbb{Q}}/\mathbb{Q}}(7)$$

Par le suit, on regarde toujours B_K , Π_K ou $E_{\bar{K}/K}$ comme muni de cette structure supplémentaire - ce sont les morphismes (de topos, de groupoïdes, ou de groupes profinis) "arithmétiques" dominant la situation.

²et on écrit souvent $\Gamma_{\bar{\mathbb{Q}}_0/\mathbb{Q}}$ au limite des $E_{\bar{\mathbb{Q}}_0/\mathbb{Q}}$, pour une clôture algébrique $[\]$ $\bar{\mathbb{Q}}$ de \mathbb{Q}

A. GROTHENDIECK

Un intérêt particulier s'attache à un noyau de (7), que je note $\pi_{\bar{K}/K}$ - on ⁽³⁾ l'appelle "partie géométrique" de groupe de Galois $E_{\bar{K}/K}$ par opposition au quotient $E_{\bar{K}/K}/\pi_{\bar{K}/K} = \Gamma_{\bar{K}/K} \hookrightarrow \Gamma_{\bar{\mathbb{Q}}/\mathbb{Q}}$, que j'appelle la partie "arithmétique" - celle-ci est un sous-groupe ouvert de $\Gamma_{\bar{\mathbb{Q}}/\mathbb{Q}}$, qui son [], correspond au sous-corps \hat{K} de $\bar{\mathbb{Q}}/\mathbb{Q}$, extension finie \hat{K}/\mathbb{Q} de $\bar{\mathbb{Q}}/\mathbb{Q}$, clôture algébrique de \mathbb{Q} dans K , de sorte qu'on a une suite exacte

$$\begin{array}{ccccccc} 1 & \longrightarrow & \pi_{\bar{K}/K} & \longrightarrow & E_{\bar{K}/K} & \longrightarrow & \Gamma_{\bar{K}/K} \longrightarrow 1 \quad (8) \\ & & & & & & \downarrow \\ & & & & & & \Gamma_{\bar{\mathbb{Q}}/\mathbb{Q}} \quad (6) \end{array}$$

On va donner une interprétation de ce noyau, et de la suite exacte (8), en écrivant

$$K = \varinjlim_i A_i \quad (9)$$

où les A_i sont les sous- \mathbb{Q} -algèbres de type fini de K , correspondant au système projectif des "modèles affines" $U_i = \text{Spec}(A_i)$ de K/\mathbb{Q} . Parmi les A_i , il y a d'ailleurs un système [] fermé des A_i réguliers, i.e. des U_i lisses/ \mathbb{Q} , [] comme morphismes de transition des morphismes de localisation []. On peut même, d'après Mike Artin, prendre comme U_i des schémas "élémentaires" sur K_0 , se dévissant en fibrations successives de courbes. Notons que $\text{Spec } K = \eta$ est le point générique [] des U_i , qui sont [] sur k (clôture algébrique de \mathbb{Q} dans K).

Le choix de \bar{K} définit un point géométrique $\bar{\eta}$ sur les U_i , d'où des groupes $\pi_1(U_i, \bar{\eta}) = \Gamma_i$, et [] bien connus

$$\begin{aligned} \text{Spec } K &= \varprojlim U_i \\ E_{\bar{K}/K} &= \pi_1(\eta, \bar{\eta}) \xrightarrow{\sim} \varprojlim_i [] \quad (\Gamma_i = \pi_1(U_i, \bar{\eta})) \quad (10) \end{aligned}$$

D'autre part, si on pose

$$\bar{U}_i = U_i \otimes_K \bar{\mathbb{Q}} \quad (11)$$

on a pour tout i une suite exacte d'homotopie

$$1 \longrightarrow (12)$$

³ on va noter $\Gamma = \Gamma_{\bar{K}/K}$ cette "partie arithmétique"

qui forment un système projectif de suite exactes, ou d'extensions ayant toutes même quotient Γ' , et dont les noyaux

$$\pi_i = \pi_1(\overline{U_i}, \overline{\eta})$$

sont des groupes fondamentaux "géométriques" - que [1] d'ailleurs [1], en utilisant un plongement de [1] dans \mathbb{C} (d'où un isomorphisme $\overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}_0}$), comme les [1] profinis de $\pi_1(U_i(\mathbb{C}), \overline{\eta})$, ou maintenant $\overline{\eta}$ est interprète comme un point [1] aux variétés complexes $U_i(\mathbb{C})$.

La suite exacte (8) est donc le limite projectif des suites exactes d'homotopie (12) ⁽⁷⁾, ce qui donne en particulière

$$\pi_{\overline{K}/K} \simeq \varprojlim_i (13)$$

Utilisant les fibrations des U_i (dans le cas où on s'astreint prendre de variétés élémentaires d'Artin), on trouve que tout π_i est un groupe extension successive des groupes profinis *fibres* (où [1]). Ceci redonne p. ex. que le dimension cohomologique de π_i est [1], celle de E_i est $\leq n+2$ (pour des coefficients de m -torsion, [1]) - et par passage à la limite, des [1] correspondantes pour les dimension cohomologiques de $\pi_{\overline{K}/K}$ et $E_{\overline{K}/K}$

$$\dim \text{coh} + \pi_{\overline{K}/K} \leq n, \quad \dim \text{coh} \Gamma_{\overline{K}/K} \leq n + 2(14)$$

qui sont en fait même des *égalités* (sauf erreur), et donnant donc une description cohomologique simple de degré d [1] absolu de K .

Théorème (1). — Soit K un corps extension de type fini de \mathbb{Q} , \overline{K} une clôture algébrique de K . Alors pour tout sous-groupe ouvert E de $E_{\overline{K}/K}$, son centralisateur dans $E_{\overline{K}/K}$ est réduit au groupe unité. Iton pour $\pi_{\overline{K}/K}$.

Démonstration. — Soit $\Gamma' \subset \Gamma \subset \Gamma_{\overline{\mathbb{Q}}/\mathbb{Q}}$ l'image de E dans $\Gamma = \Gamma_{\overline{K}/K}$ qui est donc un sous-groupe ouvert. L'image dans Γ des centralisateurs de E' dans E [1] centralisateur de Γ' dans Γ . Je dis qu'il est égale à 1, ce qui équivaut donc au

Corollaire. — Dans $\Gamma_{\mathbb{Q}} = \Gamma_{\overline{\mathbb{Q}}/\mathbb{Q}}$, le centralisateur de tout sous-groupe ouvert est réduit à (1).

OPS Ce sous-groupe ouvert Γ' invariant, il est bien connue ⁽⁸⁾ que son centre est réduit à 1 donc si Z est son centralisateur dans $\Gamma_{\mathbb{Q}}$, l'homomorphisme $Z \longrightarrow \Gamma_{\mathbb{Q}}/\Gamma'$ est injectif donc

⁷cette interprétation

⁸à vérifier

Z est fini. Mais on sait que les seules éléments $\neq 1$ de $\Gamma_{\mathbb{Q}}$ d'ordre fini sont les conjugués de τ , conjugaison complexe. Mais le centralisateur de τ dans $\Gamma_{\mathbb{Q}}$ est réduit à $[\]$ donc on peut contenir Γ' , donc $\tau \notin z$, donc $z = (1)$.

$[\]$ à $E \subset E_{\bar{K}/K}$, on voit donc que son centralisateur Z dans $E_{\bar{K}/K}$ est une image dans Γ réduite à $\{1\}$ donc $z \subset \pi_{\bar{K}/K}$. Soit $\pi' \subset \pi = \pi_{\bar{K}/K}$ le $[\]$ de z' sur π , c'est un sous-groupe ouvert de π , et on est ramené à voir que $\text{Centr}_{\pi}(\pi') = \{1\}$, i.e. le

Corollaire. — Soit π un groupe profini, extension successives de groupes profinis libres. Alors le centralisateur z dans π de tout sous-groupe ouvert π' de π est réduit à $\{1\}$.

Par dévissage on est ramené au cas d'un groupe profini *libre*. On sait que π' est donc libre. OPS π' invariant, ⁽⁹⁾ et on admet que le centre d'un groupe profini libre est réduit à 1.

Donc $Z \longrightarrow \pi/\pi'$ est injectif, donc Z est fini, et on admet que dans un groupe profini libre, il n'y a pas d'élément ⁽¹⁰⁾ d'ordre fini $\neq 1$ - ce qui $[\]$ la démonstration.

Scholie. — Le fait que $E_{\bar{K}/K}$ soit à centre trivial peut s'exploiter en disant que le groupoïde Π_K (ou le topos B_K) $[\]$ à équivalence près, définie à isomorphisme unique près, quand on connaît le groupe extérieure associé à $E_{\bar{K}/K}$.

Les homomorphismes $E_{\bar{K}'/K'} \longrightarrow E_{\bar{K}/K}$ associés à des homomorphismes $K \longrightarrow K'$ d'extensions de type fini de \mathbb{Q} , ayant une image ouvert dans un centralisateur réduit à 1, on voit de même que l'homomorphisme de topos $B_{K'} \longrightarrow B_K$ ou de groupoïdes $\Pi_{K'} \longrightarrow \Pi_K$, sont détermines à équivalence près (définie à isomorphisme unique près) par l'homomorphisme correspondant de groupes extérieures. Il $[\]$ en particulière ainsi de morphisme structurel $B_K \longrightarrow B_{\mathbb{Q}}$ ou $\Pi_K \longrightarrow \Pi_{\mathbb{Q}}$ qu'on peut interpréter intrinsèquement comme un homomorphisme de groupes profinis extérieures $E_K \longrightarrow E_{\mathbb{Q}}$. Mais nous $[\]$ suivre $[\]$, en exploitant le fait que $\pi_{\bar{K}/K}$ est lui associé à centre trivial. Cela signifie que l'extension de $\Gamma = \Gamma_{\bar{K}/K}$ par $\pi_{\bar{K}/K}$ est entièrement connue, à isomorphisme près, pour $\pi_{\bar{K}/K}$ et Γ fixés, en termes de l'action extérieure correspondant de Γ sur π , comme l'image inverse de l'extension universelle

$$1 \longrightarrow \text{Aut}(\pi) \longrightarrow \text{Atext}(\pi) \longrightarrow 1$$

Pour K fixé, donc k fixé, $[\]$ qu'on fixe un $\Gamma = \Gamma_{\mathbb{Q}/k}$ revient à dire qu'on fixe une clôture

⁹à vérifier

¹⁰à vérifier

algébrique de k , $[]$ qu'on fixe un $\pi_{\bar{K}/K} = \pi_1(K \otimes_K \bar{k})$ signifie $[]$ qu'on fixe un revêtement universel de $\text{Spec}(K \otimes_k \bar{k}) = \eta \otimes_k \bar{k}$, les deux ensembles reviennent à se donner le revêtement universel $\bar{\eta} = \text{Spec}(\bar{K})$ de K . Par la suite, nous décrivons (avec une fidélité qui reste à $[]$) les couples (K, \bar{K}) d'une extension K de \mathbb{Q} de type fini, et d'une clôture algébrique \bar{K} de K , par les triples (π, Γ, φ) , où $\pi = \pi_{\bar{K}, K}$ et $\Gamma = \Gamma_{\bar{K}, K}$ sont des groupes profinis, et $\varphi : \Gamma \longrightarrow [](\pi)$ une action extérieure de Γ sur π - ce qui peut de reconstituer l'extension $\mathbb{E}_{\bar{K}, K}$ de $\Gamma_{\bar{K}, K}$ par $\pi_{\bar{K}, K}$. J'ai oublié $[]$ qu'il faut *de plus* se donner Γ comme sous-groupe d'un $\Gamma_{\bar{\mathbb{Q}}/\mathbb{Q}}$ bien déterminé, i.e. qu'il faut se donner un objet de $\Pi_{\mathbb{Q}}$ et une $[]$ fidèle de Γ dessus - pour reconstruire $[]$ cas données un homomorphisme de groupoïdes profinis $\Pi_K \longrightarrow \Pi_{\mathbb{Q}}$, plus un objet de Π_K - ou encore, un morphisme de topos progaloisien $B_K \longrightarrow B_{\mathbb{Q}}$, plus un point de B_K . On peut ainsi fixer un objet de $\Pi_{\mathbb{Q}}$, i.e. un point de $B_{\mathbb{Q}}$, i.e. un $\bar{\mathbb{Q}}$, et étudier les K , avec un plongement de k (clôture algébrique de \mathbb{Q} dans K) dans $\bar{\mathbb{Q}}$ - mais $[]$ donner une clôture algébrique \bar{K} de K qui induise $\bar{\mathbb{Q}}/\mathbb{Q}$. Ils sont décrits [?]

On a ainsi plusieurs $[]$ essentiellement équivalentes, pour décrire par voie profinie une extension K de type fini de \mathbb{Q} :

- 1) Pour le topos étale B_K , en tant que topos progaloisien sur $B_{\mathbb{Q}}$;
- 2) Pour le groupoïde fondamental Π_K de ce topos (groupoïde de ces points, ou de ses revêtement universel) - en tant que groupoïde au dessus de $\Pi_{\mathbb{Q}}$;
- 3) Pour le groupe extérieur E_K , au dessus de groupe extérieur $E_{\mathbb{Q}}$ ou $\Gamma_{\mathbb{Q}}$ ($[]$) ;
- 4) En termes d'une clôture algébrique \bar{K}/K (i.e. en décrivant le couple (K, \bar{K}) plutôt que K), par un objet $\bar{\mathbb{Q}} \in (\Pi_{\mathbb{Q}})$ et un homomorphisme de groupes profinis $E \longrightarrow \Gamma_{\bar{\mathbb{Q}}, \mathbb{Q}}$;
- 5) En termes d'une clôture algébrique fixe $\bar{\mathbb{Q}}$ de \mathbb{Q} , et où $\Gamma = \Gamma_{\bar{\mathbb{Q}}, \mathbb{Q}}$ $[]$ les couples (K, i) où $i : k \longrightarrow \bar{\mathbb{Q}}$ est un plongement de la clôture algébrique k de \mathbb{Q} dans $\bar{\mathbb{Q}}$: pour le groupes extérieur $\pi_K = \pi_1(K)$, sur lequel un sous-groupe ouvert $\Gamma_K \subset \Gamma$ opère extérieurement par des groupes profinis *extérieures* $\pi_1(K) = \Gamma_K$, sur lesquels un sous-groupe ouvert Γ (non précisé $[]$) de $\Gamma_{\bar{\mathbb{Q}}, \mathbb{Q}}$ opère *extérieurement* ;
- 6) En termes d'une $\bar{\mathbb{Q}}/\mathbb{Q}$: pour le groupoïde $\Pi_{K \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}}$ $[]$.

A. GROTHENDIECK

Un homomorphisme de corps $K \longrightarrow K'$ donne ⁽¹¹⁾ $[\]$ à un homomorphisme de groupes extérieures, $\pi' \longrightarrow \pi$, où l'image de π' dans π est ouvert $[\]$ de centralisateur réduit à (1), ce qui implique $[\]$ que le morphisme de topos $B_{K' \otimes_K \overline{\mathbb{Q}}} \longrightarrow B_{K \otimes_K \overline{\mathbb{Q}}}$ est déterminé (à isomorphisme unique près) par $[\]$ homomorphisme extérieur. De plus on a des actions extérieures de $\Gamma = \Gamma_K \subset \Gamma_{K'}$ sur π' et π , de façon que $\pi' \longrightarrow \pi$ $[\]$ et ceci suffit pour reconstituer, d'une part les groupes extérieures E, E' extensions ("extérieures") de Γ $[\]$ π, π' (et, à équivalence rigide près, les $B_K, B_{K'}$ et $B_K \longrightarrow B_{\mathbb{Q}}, B_{K'} \longrightarrow B_{\mathbb{Q}}$) et de plus l'homomorphisme d'extensions extérieures $E \longrightarrow E'$ de Γ .

Remarque. — Quand $\pi \neq (1)$, i.e. K pas fini sur \mathbb{Q} , le théorème 1 peut se renforcer, sauf erreur, en écrivant que pour tout sous-groupe $\pi' \subset \pi$ ouvert *dans* π , $\text{Centr}_E(\pi') = \{1\}$.

Si z est se centralisateur, on a $z \cap \pi = (1)$ d'après le théorème 1, prouvons que l'image de z dans $\Gamma_{\overline{K}, K} \subset \Gamma_{\overline{\mathbb{Q}}, \mathbb{Q}}$ est finie (ce qui $[\]$ alors, que z est d'ordre 1 ou 2, et dans le $[\]$ cas que son image des $\Gamma_{\overline{\mathbb{Q}}, \mathbb{Q}}$ est $[\]$ pour un τ de conjugaison complexe).

$[\]$ E pour un sous-groupe ouvert assez petit (ce qui revient à poser à une extension finie de K) $[\]$ $\pi' = \pi$, alors l'image z' de z dans Γ est contenue dans le noyau de l'homomorphisme $\varphi : \Gamma \longrightarrow [\](\pi)$. $[\]$ je sais prouver que cet homomorphisme est injectif (ou est ramené aussitôt ou cas où K est de degré de $[\]$ 1, et on est ramené au cas des π_1 d'une courbe algébrique ...)

Théorème (2). ⁽¹²⁾ — *Le foncteur $K \longrightarrow \Pi_K / \Pi_{\mathbb{Q}}$ des extensions de type fini de \mathbb{Q} vers les groupoïdes profinis sur $\Pi_{\mathbb{Q}}$ est fidèle i.e. si deux homomorphismes $f, g : K \longrightarrow K'$ définissent des homomorphismes de groupoïdes sur $\Pi_{\mathbb{Q}}$ isomorphes*

$$\begin{array}{ccc} \Pi_{K'} & \xrightarrow{f^*, g^*} & \Pi_K \\ & \searrow p' & \swarrow p \\ & \Pi_{\mathbb{Q}} & \end{array}$$

(i.e. il existe un isomorphisme de foncteurs $\alpha : f^* \longrightarrow g^*$ tel que pour tout objet $\overline{\eta}'$ de $\Pi_{K'}$, le

¹¹on suppose pour simplifier que c'est

¹²En fait, ce théorème n'est pas spécial à \mathbb{Q} - il $[\]$ avait sur un corps de $[\]$ quelconque est en fait

carré

$$\begin{array}{ccc} pf^*(\overline{\eta'}) & \xrightarrow[p(\alpha)]{\sim} & pg^*(\overline{\eta'}) \\ \downarrow & & \downarrow \\ p(\overline{\eta'}) & \xrightarrow{\sim} & p'(\overline{\eta'}) \end{array}$$

est commutatif) alors $f = g$.

L'hypothèse sur f, g signifie aussi, en termes d'une clôture algébrique choisie $\overline{K'}$ de K' , donnent via f [] g deux clôtures algébriques de [] l'on peut trouver un isomorphisme [] celui-ci ⁽¹³⁾ ([]) d'identifier $E_{\overline{K}/K}$ et $E_{\tilde{K}/K}$ de telle façon que les deux homomorphismes

$$f^*, g^* : E_{\overline{K'}, K'} \longrightarrow E_{\overline{K}, K}$$

sont égaux. C'est sans doute plus claire en termes d'une clôture algébrique $\overline{\mathbb{Q}}$ fixée de \mathbb{Q} , en disant que les deux homomorphismes $f^*, g^* : E_{K'} \longrightarrow E_K$ de groupes profinis extérieures (avec opérateurs $\Gamma_{\overline{\mathbb{Q}}, \mathbb{Q}}$) sont égaux.

Écrivons comme [] $K = \varinjlim A_i$, donc $\eta = \text{Spec}(K) = \varprojlim U_i$, on a (en termes d'un point géométrique quelconque $\overline{\eta}$ de $\text{Spec} K$ i.e. en termes d'un \overline{K})

$$\pi_K = \varprojlim_i \pi_1(\overline{U}_i, \overline{\eta}), \quad \text{où} \quad \overline{U}_i = U_i \otimes_K \overline{\mathbb{Q}}$$

et il suffit de voir que pour tout i , $f|_{A_i} = g|_{A_i}$ [] le fait que $\pi_1(f_i^*) = \pi_1(g_i^*) : \pi_{K'} \longrightarrow \pi_1(U_i)$ (comme homomorphisme de groupes extérieures. On [] fixé, on a $K' = \varinjlim A_j$, où les A_j contient $f_i(A_i)$ et $g_i(A_i)$, donc

$$\pi_{K'} = \varprojlim_j \pi_1(\overline{V}_j, \overline{\eta'}), \quad \text{avec} \quad \overline{V}_j = \text{Spec}(A_j) \otimes_K \overline{\mathbb{Q}}.$$

Notons (prenant les V_j réguliers) que les homomorphismes de transition des le système projectif de $\pi_1(\overline{V}_j, \overline{\eta'})$ sont surjectifs - donc $\pi_{K'} \longrightarrow \pi_1(\overline{V}_j, \overline{\eta'})$ est surjectif, ce qui implique que l'égalité de f^* et $g^* : \pi_{K'} \longrightarrow \pi_1(\overline{U}_i)$ (comme homomorphismes extérieures) implique celle de $\pi_1(\overline{V}_j) \longrightarrow \pi_1(\overline{U}_j)$.

Donc l'égalité $f_i = g_i$ (d'où $f = g$) est conséquence de résultat plus général. “[géométrique”

¹³induisant “l'identité” sur [] clôtures algébriques []

A. GROTHENDIECK

Corollaire (1). — Soient X, Y des schémas de type fini réduits 0-connexes sur un corps algébriquement clos k , et $f, g : X \longrightarrow Y$ deux morphismes, on suppose que $\pi_1(f), \pi_1(g) : \pi_1(X) \longrightarrow \pi_1(Y)$ sont égaux (en fait $[]$ extérieurs) Alors

- a) Si Y se plonge par un $i : Y \longrightarrow G$ un groupe algébrique commutatif extension d'une V.A par un tore, il existe un $u \in Y$ (unique) tel que $g(x) = f(x) + u$ et pour tout $x \in X(h)$, i.e. $(i \circ g) = \tau_u \circ (i \circ f) (\tau_u [])$
- b) Si Y est une variété élémentaire d'Artin, avec fibres successives des courbes anabéliennes, et $X []$ et f ou g est dominant, alors $f = g$.

Démonstration. — a) L'unicité de $[]$ est $[]$ - i.e. il suffit (¹⁴) d'examiner les actions de $\pi(f)$, $\pi(g)$ sur les groupes abelianisés dans π_1 , et même sur leurs composantes l -adiques. Prenant le Jacobienne généralisée de type "extension d'une V.A par une tore" de X , on sait que

- 1°) Les morphismes $f : X \longrightarrow G$ tel que $f(\alpha) = 0$ se factorisent de façon unique par $X \xrightarrow{can} J \xrightarrow{\varphi} G$ avec φ un homomorphisme de groupes algébriques ;
- 2°) Un tel homomorphisme φ est connu quand on connaît ses actions sur les $H_1(, \mathbb{Z})$ ce qui $[]$ à la connaissance sur les points d'ordre $[]$ que soit v - on ceux-ci sont denses ...
- 3°) $H_1(X, \mathbb{Z}_l) \xrightarrow{\sim} H_1(J, \mathbb{Z}_l)$.

De ceci, on conclut (par 3°)) que $H_1(f) = H_1(g)$ implique (si $f = \varphi \circ can$, $g = \psi \circ can$) $H_1(\varphi) = H_1(\psi)$, donc par 2°) que $\varphi = \psi$, donc $f = g []$

Notons que l'on

- b) on va pourtant prouvons l'égalité sans l'hypothèse anabéliennes

$[]$ L'hypothèse que $\pi_1(f) = \pi_1(g)$ signifie donc qu'il existe $\alpha \in \pi_1(Y)$, tel que

$$\pi(f')(\gamma) = [] \pi(j)(\gamma)$$

pour tout $\gamma \in Im(\pi_1(X) \xrightarrow{\pi_1(f)} \pi_1(U))$. $[]$ cette image est un sous-groupe ouvert de $\pi_1(U)$ ($[]$ dominant !). Donc on est ramené à ceci: Soit U ouvert $\neq \varphi$ de Y , $u \in G$, tels que $\tau_u U \subset Y$ [et tels que (désignant par f, f' les morphismes $y \longrightarrow y$ et $y \mapsto y$ en de U dans Y) $\pi_1(f)$ et $\pi_1(f')$ $[]$ extérieurement en un sous-groupe ouvert de $\pi_1(U)$] alors $f = f'$ voie $u =$

¹⁴En fait, dans a) il suffit de supposer que

Finalement, je [] que [] pas à la prouve par voie géométrique [] *arithmétique*.

Corollaire (2). — *Le condition $f = g$ de corollaire précédent, est valable si on suppose que K est de caractéristique 0, X [] est dans l'une des hypothèses suivantes*

- c) *l'image de $\pi_1(F)$ est un sous-groupe ouvert de $\pi_1(Y)$, Y est une variété élémentaire d'Artin anabélienne ;*
- d) *l'image de $\pi_1(X)$ par $\pi_1(f)$ a un centralisateur dans $\pi_1(Y)$ réduit à (1), et Y se plonge dans un groupe algébrique extension d'une VA par un tore.*

Comme le centralisateur [] de un sous-groupe ouvert de $\pi_1(Y)$ ($\pi_1(Y)$ étant extension successive de groupes profinis *fibres* anabéliennes) est réduit à (1), comme un a un¹⁵ plus haut, le cas c) est un cas particulier de d), [] dans le cas d), [] X pour un ouvert d'Artin []

La situation X, Y, f, g provient, par extension de corps de [] d'une situation analogue sur un corps K extension de type fini de \mathbb{Q} . Soit \bar{K} la clôture algébrique de K dans k [] de K à \bar{K} . On a donc [] satisfaisant la condition d) avec [] trivial.

Mais ces hypothèses impliquent que les extensions $E(X/K) = \pi_1(X)$, $E(Y/K) = \pi_1(Y)$ de $E_{\bar{K},K}$ [], ainsi que les homomorphismes [] induits, sont reconstruite à partir de [] et de l'action extérieure de $E_{\bar{K},K}$ sur ces groupes. On va montrer maintenant le

Corollaire (3). — *Soient X, Y deux schémas de type fini sur un corps K extension de type fini de \mathbb{Q} , On suppose que Y se plonge dans une extension d'une V.A. par un tore, X réduit, X, Y [] 0-connexe. Soit \bar{K} une clôture algébrique de K , d'où des extensions "extérieures" $E_{X,K}, E_{Y,K}$ de $E_{\bar{K},K} = \text{Gal}(\bar{K}, K)$ [] $\pi_1(\bar{X}), \pi_1(\bar{Y})$, et pour tout morphisme $f : X \longrightarrow Y$, un morphisme [] de $E_{X,K}$ [] $E_{Y,K}$.*

Soient $f, g : X \rightrightarrows Y$ tels que [] - i.e. [] soient conjugués pour un élément de $\pi_1(Y)$ [] alors $f = g$.

En fait, il suffit même que ls homomorphismes d'extensions [] soient égaux, [] $f = g$. (C'est à dire, [] des hypothèses *anabéliennes*, des hypothèses [] géométriques sue les actions de [], [] on peut laisser tomber les aspects anabéliens [] sur les aspects abéliens []) [].

¹⁵il faut

A. GROTHENDIECK

Il suffit de voir que $[\]$ à noyau abélien associée - l'hypothèse implique que $f(x)$ et $g(x)$ définissent le même donne de conjugaison de scindages. Donc il suffit maintenant de prouver le

Théorème (3). — *Soit X un schéma de type fini sur un corps K , extension de type fini de \mathbb{Q} , on suppose que X est géométriquement 0-connexe et se plonge dans une extension d'une V. A. par un tore (p. ex. X est une variété élémentaire d'Artin, à fibres $[\]$).*

Considérons une clôture algébrique \bar{K}/K et l'extension extérieure correspondant $E_{X/K}$ dans $E_{\bar{K}/K} = \text{Gal}(\bar{K}/K)$ par $\pi_1(\bar{X})$ ($\bar{X} = X \otimes_K \bar{K}$) et l'extension déduite de $\tilde{E}_{X/K}$ de $E_{\bar{K}/K}$ par $\pi_1(\bar{X})_{ab}$. Considérons les applications

$$X(K) \longrightarrow \text{Classes de } \pi(\bar{X}) - \text{conjugaison de scindages de } E_{X/K} \text{ sur } E_{\bar{K}/K}(*)$$

$$X(K) \longrightarrow \text{Classes de conjugaison de scindages}(**)$$

Ces applications sont *injectives*.

Démonstration. — Il suffit de le $[\]$ pour le seconde application, et on est ramené au cas où X est lui-même un groupe algébrique G , extension d'une V. A. par une tore. Alors l'application est un homomorphisme de groupes

$$G(K)(16)$$

obtenue ainsi. On considère pour tout $[\]$ la suite exacte $[\]$

$$0 \longrightarrow [\] \longrightarrow G[\] \longrightarrow G \longrightarrow 1$$

$[\]$ suite exacte de cohomologie

$[\]$

et passant à la limite, on trouve

$$0 \longrightarrow$$

le composé de (16) avec l'homomorphisme canonique

$[\]$

compte tenu de

$[\]$

[] que l'homomorphisme induite par

[]

dont le noyau [] est fermé des éléments de $G(K)$ *infinitement divisibles* dans \mathbb{Q} . [] ici K étant un corps [] de type fini le théorème de Mordell-Weil [] que $G(K)$ est un \mathbb{Z} -module de type fini - donc $G(K) \longrightarrow \varprojlim G(K)_n$ est injectif. Donc []

Remarque. —

[] x dans le “revêtement universel abélien” \tilde{G} de G construit comme \varprojlim des revêtements $G(n) \simeq G$ de G , donnée, []. L'énoncé dit que si [] est trivial - i.e. si [] mais dans ce cas [] soit [] étales.

est cependant possible que [] ...

[] aux conditions de de Corollaire 1, b), [] avec les groupes fondamentaux [], on trouve que

[]

Complément. — Retour sur une démonstration *géométrique* du Théorème 2, Corollaire 1 b). On peut supposer que ce est la Jacobienne généralisée de Y , et il suffit de montrer le

Lemme. — *Soit Y une variété élémentaire d'Artin anabélienne (sur K algébriquement clos), $Y \hookrightarrow J_Y^1$ son plongement dans sa Jacobienne généralisée, $u \in J_Y^0(k)$ et U un ouvert non [] de Y , tels que $U + u \subset Y$. Alors $u = 1$, ou encore: l'application $x \mapsto x$ [] de U dans Y est l'identité.*

Par dévissage, on es ramené au cas où Y est une courbe. Supposons le d'abord complète, de suite que $U + u \subset Y$ implique $Y + u \subset Y$ - alors la [] est bien connu (et résulte par exemple de la formation des points fixes, qui implique que [] ce qui [] $J_Y^0(k)$ est nulle. Pour que $x + u$ soit de la forme y ($y \in Y$) il faut [] que $u \in \alpha$ et y aient même image dans J_Y^1 , ce qui [] Je veut mieux, dans le cas général, présenter les choses sous forme homologique. Considérons les deux morphismes $U \hookrightarrow iY$ induisant et $J : U \longrightarrow Y$ induit par lui, je dis que $H_1(i) = H_1(j)$, ou ce qui revient au même, puisque $Y \xrightarrow{\alpha} J_Y'$ induit un isomorphisme $H_1(\alpha) : H_1(Y) \longrightarrow H_1(J_Y')$, que

Si le genre est 0, on en concluait (puisque []. Dans le cas de genre 1, on en concluait maintenant que l'image de un des J_Y^0 est égale à 1, et on [] comme précédemment. []

II. La question de pleine fidélité

Soient K, K' deux extensions de type fini de Q - est-il vrai que tout Π_Q -homomorphisme $\Pi_{K'} \longrightarrow \Pi_K$ provient d'un homomorphisme de corps $K' \longrightarrow K$? On est ramené aussitôt au cas où - une clôture algébrique \overline{Q} de Q étant choisie, d'où un $\Gamma_{\overline{Q}/Q} = K$ et K' ont des sous-corps k, k' (clôture algébrique de Q dans K resp. K') isomorphes, avec des plongements $k, k' \longrightarrow Q$ de même image, que E_K et $E_{K'}$ peuvent être considérés comme des extensions d'un même groupe $\Gamma = \Gamma_{\overline{Q}/k}$ par π_K resp. $\pi_{K'}$. La question est alors si *tout* homomorphisme de $\pi_{K'}$ dans π_K qui commute à l'action de Γ , est induit par un homomorphisme $K \hookrightarrow K'$. Pour construire ce dernier, il faudrait donc avoir une idée comment reconstruire K, K' à partir des extensions $E_K, E_{K'}$, ou encore à partir des groupes profinis extérieurs avec opération de Γ dessus. Et on pressent que le Théorème 3 du paragraphe précédent (appliqué notamment à \mathbb{P}_K^1 convenablement troué...) pourrait donner la clef d'une telle construction.

Bien sûr, des homomorphismes extérieurs quelconques $\pi_{K'} \longrightarrow \pi_K$ n'auront pas de sens géométrique - l'idée est que les opérations du groupe $\Gamma = \Gamma_{\overline{Q}/k}$ dessus soit si draconienne, qu'il n'est possible de trouver un homomorphisme extérieure qui y commute que par voie géométrique - par des plongements de corps. Donc il est essentiel ici que le corps de base ne soit pas quelconque, mais un corps tel que Q (ou, ce qui revient manifestement au même, une extension de type fini de Q). Encore faut-il se borner aux homomorphismes $\pi_{K'} \longrightarrow \pi_K$ dont on décrète d'avance que l'image soit ouverte - sinon, prenant pour $\pi_{K'}$ le groupe unité (i.e. $K' = k$), on trouverait un homomorphisme $K \longrightarrow k$ correspondant! Il faut pour le moins, pour travailler à l'aise à partir d'homomorphismes $\pi_{K'} \longrightarrow \pi_K$ (au lieu de $E_{K'} \longrightarrow E_K$) supposer que le centralisateur dans π_K de l'image de tout sous-groupe ouvert de $\pi_{K'}$ soit réduit à $\{1\}$ - on dira que l'homomorphisme en question est *anabélien* alors - de telle façon qu'à partir de cet homomorphisme (commutant à Γ) on reconstitue l'homomorphisme d'extensions E_K et $E_{K'}$, qui est l'objet vraiment essentiel. Par exemple, si justement $K' = k$, donc $E_{K'} = \Gamma$, ce qui nous intéressera, ce ne seront pas le Γ -homomorphismes de $\pi_{K'} = \{1\}$ (!) dans π_K , mais bien les *sections* de E_K sur Γ .

Question-conjecture. — Soient K, K' deux corps, extensions de type fini de Q , et un morphisme $B_{K'} \longrightarrow B_K$ de topos sur B_Q .

Les conditions suivantes sont-elles bien équivalentes [?]

- (a) L'homomorphisme provient d'un plongement de corps $K \hookrightarrow K'$.
- (b) L'image de l'homomorphisme extérieur $E_{K'} \longrightarrow E_K$ a une image ouverte.
- (c) L'homomorphisme extérieure $E_{K'} \longrightarrow E_K$ est anabélien. ⁽¹⁶⁾

NB. On sait que (a) \Rightarrow (b) \Rightarrow (c) et que (b) équivaut à $\pi_K \longrightarrow \pi_{K'}$ a une image ouverte.

Une réponse affirmative impliquerait que si $\deg K'/Q < \deg K/Q$, alors il n'y a pas de tel homomorphisme $E_{K'} \longrightarrow E_K$, compatible avec les projections dans $E_Q = \Gamma_Q$, en particulier, il en résulterait que toute section de E_K sur $\Gamma = \text{Im}(E_K \longrightarrow \Gamma_Q)$, ou sur un sous-groupe ouvert Γ' de Γ , a un centralisateur non-trivial dans E_K – et comme son centralisateur dans Γ est réduit à $\{1\}$, cela impliquerait que pour toute telle section, on aurait (si $\pi_K \neq 1$) $\pi_K^{\Gamma'} \neq \{1\}$. Or je m'aperçois que ceci est sans doute faux (cf. plus bas, numéro 3) – il faudrait renforcer (c) ci-dessus en [:]

- (c') L'homomorphisme $E_{K'}^\circ \longrightarrow E_K$ induit par $E_{K'} \longrightarrow E_K$ est anabélien (où $E_{K'}^\circ$ est le noyau de l'homomorphisme composé

$$E_{K'} \longrightarrow \Gamma_{\overline{Q}/Q} \xrightarrow{\chi \text{ caractère cyclotomique}} \hat{Z}^*).$$

Mais pour voir que cette condition est *nécessaire* pour que l'homomorphisme soit géométrique, il faudrait vérifier que pour tout sous-groupe ouvert E' d'un E_K , le centralisateur dans E_K (non seulement de E' lui-même, mais même de E'°) est réduit à 1 – ce qui résulte de la démonstration du Théorème 1, et du fait ⁽¹⁷⁾ que pour tout sous-groupe ouvert Γ' de $\Gamma = \Gamma_Q$, le centralisateur (non seulement de Γ' , mais même) de Γ'° dans Γ est réduit à $\{1\}$.

Donc, la conjecture initiale revue et corrigée donné la

Conséquence (conjecturale). — *Pour tout section de E_K sur un sous-groupe ouvert Γ' de Γ_Q , de sorte que Γ' opère (effectivement) sur π_K , on a (si K pas algébrique sur Q , i.e. $\pi_K \neq \{1\}$) $\pi_K^{\Gamma'^\circ} \neq \{1\}$.*

¹⁶(c) n'est pas assez fort, cf. plus bas ...

¹⁷à vérifier !

A. GROTHENDIECK

à vrai dire, à certains égards les Γ_K sont des groupes trop gros pour pouvoir travailler directement avec, il y a lieu de regarder Γ_K comme un \varprojlim de groupes $\Gamma_{U/Q}$ associés à des modèles affines de K – et on s’intéressera plus particulièrement à des modèles affines qui sont des variétés élémentaires – plus généralement, qui sont des $K(\pi, 1)$ (au sens profini ...). Il est possible qu’il faille d’ailleurs, dans l’énoncé de la conjecture de départ, prendre un homomorphisme extérieur $E_{K'} \longrightarrow E_K$ dont on suppose d’avance (en plus de l’hypothèse anabélienne et de la compatibilité avec les homomorphismes dans Γ_Q) qu’elle est compatible avec les *filtrations* de ces groupes, associés à ces modèles (“filtration modélique” (grossière)).

Nous allons alors, au même temps que des extension de type fini de Q , les homomorphismes entre tels, et homomorphismes de groupes profinis associés, étudier la situation analogue pour des “modèles” élémentaires anabéliens, voire des modèles $K(\pi, 1)$ généraux (On peut aussi regarder de tels modèles sur un corps K , extension de type fini de Q – mais passons pour le moment sur cette situation mixte, un peu bâtarde ...) Si U, V sont des tels modèles, tout morphisme $V \longrightarrow U$ définit un morphisme de topos galoisiens sur B_Q , $B_U \longrightarrow B_V$, et si U est élémentaire anabélien, ce morphisme est connu quand on connaît seulement $H_1(B_{\overline{U}}, Z_\ell) \longrightarrow H_1(B_{\overline{V}}, Z_\ell)$ – ce qui est beaucoup moins que la classe d’isomorphie d’homomorphismes de B_Q -topos. (En fait, sans hypothèse anabélienne sur V , dès que V se plonge dans une variété anabélienne, f est connu quand on connaît son action sur les topos étales ...). Mais quels sont les homomorphismes $B_U \longrightarrow B_V$, ou $E_U \longrightarrow E_V$, qui correspondent à des morphismes de modèles ? Avec un peu de culot, on dirait [:]

Conjecture fondamentale. — Soient U, V deux schémas de type fini sur Q , V séparé régulier, U une variété élémentaire anabélienne sur une extension finie de Q . Considérons un morphisme $B_V \longrightarrow B_U$ des topos étales sur Q – ou, ce qui revient au même, un homomorphisme de groupes extérieurs

$$f : E_V = \pi_1(V) \longrightarrow E_U = \pi_1(U),$$

compatible avec les homomorphismes extérieurs dans $\Gamma_Q = \pi_1(Q)$.⁽¹⁸⁾

Conditions équivalentes [:]

(a) Cet homomorphisme provient (à isomorphisme près) d’un morphisme $V \longrightarrow U$ sur les

¹⁸**NB** Pour l’unicité, on est ramené aussitôt au cas où V lui-même est un modèle élémentaire anabélien, si ça nous chante.

modèles (qui est donc uniquement déterminé)

(b) $f|E_V^\circ$ est anabélien, i.e. l'image par f de tout sous-groupe ouvert de E_V° a un centralisateur réduit à 1.

Pour la nécessité de (b), on est ramené aussitôt au cas où V est réduit à un point, où cela se réduit à la

Conséquence conjecturale. — Soit $\Gamma' \subset \text{Im}(E_U \longrightarrow \Gamma_Q)$ un sous-groupe ouvert, correspondant à un corps k fini sur Q , considérons un k -point de U , d'où un relèvement $\Gamma' \longrightarrow E_U$, de sorte que Γ' opère sur π_U . Ceci posé, on a $\pi_U^{\Gamma'} = \{1\}$.

On étudiera par la suite les relations entre cette “conséquence conjecturale”, et la précédente (d'apparence opposée !) concernant les E .

La conjecture fondamentale sur les modèles implique la conjecture fondamentale sur les corps, à condition de prendre soin, dans cette dernière, de se limiter aux homomorphismes compatibles aux filtrations modéliques. ⁽¹⁹⁾

Plus généralement, prenant maintenant pour U des schémas qui sont des \varprojlim des modèles élémentaires anabéliens, avec morphismes de transition des immersions ouvertes affines (pour pouvoir passer à la \varprojlim dans la catégorie des schémas), pour V un schéma \varprojlim de schémas séparés réguliers de type fini sur Q (morphismes de transition immersions ouvertes affines sans plus). Alors les morphismes *dominants* de schémas $V \longrightarrow U$ doivent correspondre aux homomorphismes extérieurs $E_V \longrightarrow E_U$ compatibles avec les projections dans $E_Q = \Gamma_Q$, et telle que l'image soit ouverte. Par exemple, on pourrait prendre pour U, V les spectres d'anneaux locaux réguliers essentiellement [?] de type fini sur Q .

—

Cette conjecture fondamentale (éventuellement revue et corrigée en cours de route ?) étant admise, la question qui se pose ensuite est de déterminer les topos (pro)galoisiens sur B_Q qui proviennent de modèles élémentaires anabéliens – ou encore, les $\pi_U = \pi_1(\overline{U})$ de tels modèles étant connus, de déterminer quelles sont [les] actions extérieures possibles de sous-groupes ouverts Γ de Γ_Q sur de tels groupes fondamentaux – et éventuellement question

¹⁹Et il vaut mieux se borner à l'équivalence de (a) et (b) – la condition (c) avec les centralisateurs risque de passer mal à la \varprojlim .

analogue pour d'autres types de groupes profinis, correspondant à des $K(\pi, 1)$ qui se réaliseraient par des variétés algébriques (sur C , disons), mais pas par des variétés élémentaires. (J'ai en vue autant des variétés modulaires, tels que, notamment, des variétés modulaires pour les courbes algébriques...) à partir de là, on reconstruirait par recollement, en termes profinis, tous les schémas lisses sur un corps de type fini sur Q (ou plutôt la catégorie de ceux-là), ou plus généralement, sur un corps quelconque – puis, sans doute, par “recollement”, la catégorie des schémas localement de type fini sur un K – tant [?] des [varier?] la catégorie des fractions qui s'en déduit en rendant inversibles les homéomorphismes universels...

Les réflexions précédentes suggèrent aussi des énoncés comme le suivant : Pour un schéma de base S localement noethérien donné ⁽²⁰⁾, les foncteurs $X \longrightarrow X_{\text{ét}}$, allant de la catégorie des schémas réduits localement de présentation finis sur S , vers la 2-catégorie des topos au-dessus de $X_{\text{ét}}$, est 1-fidèle (deux homomorphismes $f, g: X \rightrightarrows Y$ tels que les morphismes de topos $f_{\text{ét}}, g_{\text{ét}}: X_{\text{ét}} \rightrightarrows Y_{\text{ét}}$ au-dessus de Set soient isomorphes, sont égaux) et même peut-être *pleinement fidèle*, quand on passe à la catégorie des fractions de $(\text{Sch}_{\text{l.t.f.}})/S$ obtenue en rendant inversibles les homéomorphismes universels... Expriment ceci par exemple pour les automorphismes d'une courbe algébrique propre sur une extension finie de Q , on retrouverait le “fait” que tout automorphisme extérieur de E_K (K le corps des fonctions de X) qui respecte la structure à lacets [?] et qui commute à l'action de Γ , provient d'un automorphisme de X .

III. Étude des sections de E_U sur Γ

Soit U un schéma connexe lisse de type fini géométriquement 0-connexe sur le corps K , d'où $E_U \longrightarrow E_K$, et ⁽²¹⁾ on se propose d'étudier les sections mod $\pi_{U,K}$ -conjugaison – plus généralement, on [] un même topos [] les sections $E'_K \longrightarrow E_U$, où E'_K est un sous-groupe ouvert de E_K (ce qui signifie que [] fait une extension de base finie sur K). Si K de type fini sur le corps Q et si U se plonge dans un schéma sur un groupe commutatif rigide l'application

$U(K) \longrightarrow []$ d'isomorphisme section de B_U sur $B_K[[]\pi_{U,K}$ -conjugaison de sections de E_U sur E_K

est injectif. On va examiner d'entre façons “géométriques” de trouver des sections.

Supposons d'abord que U soit une courbe algébrique, que ne soit pas de type $(0, 0)$ ou $(0, 1)$, i.e. $\pi_1(\overline{U}) = \pi_{U,K} \neq \{0\}$. On a que pour tout $i \in \widehat{\overline{U}} \setminus \overline{U}$ (point à l'infini) le groupe de

²⁰ S de caractéristique 0?

²¹ On a choisie un revêtement universel \tilde{U} de U pour définir X , et E_U, E_K , et $E_U \longrightarrow E_K$.

lacs L_i fournit un scindage (des $[]$ i.e. $[]$) en prenant son centralisateur $Z(L_i)$ dans E , d'où

$$1 \longrightarrow L_i \longrightarrow Z(L_i) \longrightarrow \Gamma \longrightarrow 1(2)$$

et en prenant les scindages de cette extension. Il ne existe, p. ex. définis par une $[]$ de $\overline{O}_{\widehat{U},i}$. L'un des données de conjugaison des scindages de (2) est un $[]$

(3)

et $[]$ injectivement de l'un des données de π -conjugaison de scindages.

Proposition. — ⁽²²⁾ On suppose $(g, v) \neq (0, 0), (0, 1)$ i.e. $\pi_{\overline{U}} = \pi_{U,K} \neq (1)$. Alors les classes de π -conjugaison scindage de (1) définies pour les scindages de (2) sont distinctes de celles associés aux points de $U(K)$. Si de plus $(g, v) \neq (0, 2)$, i.e. si $[]$ est dans le cas anabélien, alors les classes de π -conjugaison de scindages de (1), associés à des scindages de (2) pour deux indices $i = i_1$ et $i = i_2$ distincts, soient distincts.

La première assertion s'obtient en "bordant" le trou i , alors la section envisagée devient la section de $U \cup \{i\} = U'$ associée au point i , et celle est donc distincte de celle associée aux $[]$ points de U' , i.e. aux points de U - a fortiori $[]$ pour le sous-groupe $[]$ par L_i . On $[]$ de même pour $[]$ que les $[]$ de scindages associées à un L_{i_1} et un L_{i_2} , $i_1 \neq i_2$, sont distinctes, $[]$ sauf le cas de type (0, 3) $[]$ on tombe sur le type (0, 1), où $[]$ de résultat d'injectivité. Mais on peut $[]$, à condition d'admettre que pour un scindage de (2), faisant opérer Γ sur π , on a

$$\pi^{\Gamma} = L_i(3)$$

(donc $\pi^{\Gamma} = (1)$, d'ailleurs) - résultat que on $[]$ plausible. $[]$ que le $[]$ de conjugaison de sections détermine le $[]$ de conjugaison de L_i , donc i .

Conjecture (A). — Soit U courbe algébrique anabélienne géométrique 0-connexe sur corps K de type fini sur Q . Alors toute section de (1) est d'une des deux types précédents, i.e. soit définie par un point de $U(K)$ ²³, Soit pas une section d'une extension (2), avec $i \in I(\pi)^{\Gamma}$ i.e. $[]$ un point de $\widehat{U} \setminus U$, rationnel sur K .

²²C'est démontré sauf pour le type (0, 3) $[]$

²³Il y a $[]$ plus $[]$

Si on obtient cette conjecture, alors on va conclurait, pour passage à la limite, en considérant le corps de fonctions L de U et $E_L \longrightarrow E_K$ (E_L peut être considéré comme un groupe à lacets “infini” (avec une infinité des classes de sous-groupes lacets $L_i \dots$) que tout scindage de cette extension provient d’une scindage d’une extension de type (2), avec $i \in I$ $\Gamma = X(K)$ ($X = \hat{U}$). Les classes conjugués de tels scindages se grouperaient donc pour paquets (en regardent les centralisateurs des sous-groupes image de Γ° par ses sections,) et un $[]$ ensemble des scindages qui est donc $[](\Gamma^\circ)$ conjugués (même s’il ne sont eux-mêmes conjugués). Donc on retrouve $[]$ une description de $X(K)$ (donc ainsi de $X(K')$ pour toute extension finie K' de K) en termes de l’extension E_L de E_K par $\pi_{L,K}$, au même temps qu’une $[]$ de reconstitue les $U = X \setminus I$ $[]$

Donc en fait c’est la structure $E_L \longrightarrow E_K$ qui est le plus riche a priori, et de loin plus commode pour le genre 0 et 1, où le considération des U de type (g, v) ($2g + v \geq 3$) $[]$ le groupe “continue” d’automorphismes... La forme “modélisque” de la conjecture précédente revient à la forme “birationalle”, quand on y précise cette $[]$ en disant que tout scindage de $E_U \longrightarrow E_K$ se revient au un scindage de $E_L \longrightarrow E_K$ (on ainsi, $[]$ un scindage de $E_V \longrightarrow E_K$, si V est un modèle $[] U$).

On ne $[]$ les conjectures précédentes (sous forme modélisque, disons) sous une forme plus géométrique, en introduisant, un même topos qu’un revêtement universel \tilde{U} de U , $[] X'$ de X $[] \tilde{U}$ (où $X = \hat{U}$). (NB je m’abstient de le noter \tilde{X} , $[]$ il n’est pas $[]$ sur X). Notons que pour $i \in I = \bar{X} - \bar{U}$, l’un des L_i des $\bar{\pi} = \pi(\bar{U})$ $[]$ en correspondance 1-1 avec $[]$ fibre X'_i de X' au dessus de i .

$$X \longrightarrow \bar{X} \longrightarrow X'$$

Donc X' peut être considéré comme le $[]$ de \tilde{U} , et de $X' \setminus I =$ ensemble des sous-groupes lacets de $\bar{\pi}$, qui apparaissent ainsi comme des “points à l’infini” des revêtements universel \tilde{U} . D’ailleurs E_U s’interprète comme le groupe de $[]$ schéma \tilde{U} $[]$, et $E_U \longrightarrow E_K$ comme l’homomorphisme de passage au quotient $[]$ (NB. \bar{K} s’identifie a la clôture algébrique de K dans $[]$, donc E_U opère sur $\text{Spec } \bar{K}$ de façon $[]$) Une section de E_U sur E_K est donc une action de E_K sur \tilde{U} , compatible avec son action sur \tilde{U} $[]$ convenable (sans doute $[] \bar{U}_i$ finis sur \bar{U} entre \bar{U} et $\bar{U} \dots$). Considérons alors la

Conjecture (B). ⁽²⁴⁾ — *Toute telle action de Γ sur \tilde{U} admet dans $X' = \widehat{\tilde{U}}$ un point fixe et un*

²⁴et même l’action induit de Γ° doit avoir un point fixe $[]$ plus bas

seul.

Ceci signifie alors

a) S'il y a un point fixe à distance finie i.e. $\tilde{X} \in \tilde{U}^T$, alors

1°) L'image de \tilde{X} dans U est uniquement déterminée - c'est essentiellement le Théorème 3 dans §1 (des α points distincts de $U(K)$ définissent des classes de conjugaison des scindages distinctes) et

2°) ²⁵ $\pi^\Gamma = (1)$ (i.e. il n'y a pas d'autre point fixe dans \tilde{U} sur ce même $x \in U(K)$), et []

3°) il n'y a pas au même temps ce point fixe à l'infini - i.e. il n'existe pas de L_i normalisé par Γ , i.e. une scindage des [] type n'est pas au même temps des deuxièmes (fait que nous avons et oublié directement, précédemment).

D'autre part, dans le cas de points fixes à l'infini, l'unicité de l'image dans X signifie qu'une même action effective [] à la fois un L_i et [] ($v \neq J$) - Fait [] établi sauf dans le cas $(g, v) = (0, 3)$ - et l'unicité au dessus d'une $i \in I$ fixé signifie que le L_i (i fixé) normalisé par Γ est unique, ce qui est un affaiblissement de la relation

$$L_i = \text{Cen} \pi^{\Gamma^\circ}$$

pour ces opérations, conjecture plus haut.

En fait, je conjecture que dans la conjecture B, il est même vrai que Γ° agissant sur $X' = \widehat{U}$ a un point fixe et un seul (ce qui est plus haut, [] point fixe [] nécessairement fixe pour Γ). Ceci implique dans le cas des points fixes à distance finie, qu'est alors $\pi^{\Gamma^\circ} = (1)$, comme il se devrait en général [] et dans le cas de points fixes à l'infini, que

$$\pi^{\Gamma^\circ} \subset \text{Norm}_\pi(L_i) = L_i$$

donc le [] $\pi^{\Gamma^\circ} = L_i$ [] !

[] tous nos beaux énoncés devraient être valables, [] un corps de base K de type fini de Q , mais [] que K est extension de type fini d'un corps cyclotomique (pas [] fini sur Q).

²⁵C'est un cas particulier []

A. GROTHENDIECK

Nous pourrions définir les *courbes de Poincaré* sur un corps algébriquement clos de \bar{K} de caractéristique 0, comme étant les courbes isomorphes à des revêtements universels de courbes algébriques anabéliennes sur K (donc courbes anabéliennes \bar{U}, \bar{V} sur \bar{K} définissent des revêtements de Poincaré isomorphes, si et seule si existe un revêtement fini étale de l'un, isomorphes à un revêtement fini étale de l'autre). Étant donné une courbe de Poincaré \widehat{U} sur \bar{K} , on définit canoniquement sa complétion $\widehat{U} [] \widehat{U}$. Ceci posé :

Conjecture (B'). — Soient K un corps de type fini sur Q (ou sur un corps cyclotomique suffise peut-être), \bar{K} une clôture algébrique de K , U une courbe de Poincaré sur \bar{K} , de complétion $\widehat{U} = X$. Considérons une action de $\Gamma = \Gamma_{\bar{K}, K}$ sur U , compatible avec sous-action sur \bar{K} , d'où une action de Γ sur X . Ceci posé : Il existe un point fixé et un seul de Γ° agissent sur X (Γ° , noyau de caractère cyclotomique $\Gamma \xrightarrow{\chi} \widehat{Z}^*$).

La différence avec la conjecture B, pour celle-ci $[], []$ d'un groupe profini π , $[]$ librement sur U de façon que $U_{/\pi}$ soit une courbe algébrique anabélienne sur \bar{K} .

Que donneraient les conjecture précédentes, quand on les applique à une situation où K est $[]$ pour un modèle S de K (disons, élémentaire anabélienne), quand U_K provient d'une courbe relative U_S sur S - de sorte qu'on a un homomorphisme de groupes

$$E_{U_S} \longrightarrow E_S(4)$$

de noyau $\pi_{\bar{U}}$, dont $E_{U_K} \longrightarrow E_K$ est déduit pour changement de base i.e. par produit fibre

$$E_{U_K} \longrightarrow E_{U_S} [] (5)$$

Ainsi, les sections de E_{U_K} sur E_K correspondant aux relèvement continus $E_K \longrightarrow E_{U_S}$ de l'homomorphisme surjectif $E_K \longrightarrow E_S$ et parmi ce relèvement, ceux qui sont triviaux sur le noyau de $E_K \longrightarrow E_S$ correspondent aux sections de E_{U_S} sur U_S . Nos conjectures impliquent donc qu'il y a existents deux sortes telles sections : 1°) celles qui correspondent à des points de U_K/K i.e à des sections rationnelles des U_S sur S - mais on va vérifier sans mal, sans doute, qu'une telle section rationnelle ne correspond effectivement à une section de l'extension (4), que si c'est une section régulière (à vérifier tantôt). 2°) Celles correspondant à des $i \in I(\bar{U}_K)$ rationnels sur K , i.e. à une section de $\widehat{U}_S \setminus U_S = S'$ (étale fini sur S) sur S . Et il faudrait étudier encore à quelle conditions une telle section définit un paquet non vide de scindages de (4) - et comment déterminer exactement tous ces scindages.

Avant d'élucider ces deux points, un peu technique, je voudrais voir dans quelle manière la conjecture **A** (ou **B**) faite des ces §, permet de reconstruire la catégorie des modèles élémentaires anabéliennes sur Q , et celle des extensions de type fini de Q et des modèles élémentaires anabéliennes sur ceux-ci, en termes des groupes extérieurs (ou topos galoisiens) associés à partir bien sûr de la donnée fondamentale de $\Gamma_Q = \Gamma_{\overline{Q}, \overline{Q}_0}$, opérant extérieurement sur $\widehat{\pi_{0,3}}$, d'où déjà l'extension $E_{0,3} = E_{U_{0,3}/Q}$, où $U_{0,3} = \mathbb{P}_Q^1 - \{0, 1, \infty\}$.

Prenons les donne de $\widehat{\pi_{0,3}}$ -conjugaison de $[]$ sections de $E_{0,3}$ sur $\Gamma_Q = \Gamma$ i.e. les "points" telles que le centralisateur de Γ^0 soit trivial (sections "admissibles") $[]$ des topos $B_{\widehat{\pi_{0,3}}, \Gamma_Q} []$ sur $B_{\Gamma_Q} []$ - on trouve un ensemble sur lequel Γ opère (qui n'est autre que $U_{0,3}(\overline{Q}_0)$, à isomorphisme canonique près). Pour tout ensemble fini I des sections, stable par $[]$ la formation "forage de trous" doit nous fournir un groupe extérieur $\pi_{0,3}(I)$, de type $[]$ sur lequel Γ opère (il voit mieux peut-être utiliser le yoga introduit par ailleurs des groupoïdes rigides - donc on peut $[]$ ainsi $[]$ de trous $0, 1, \infty$ - on trouve donc l'équivalent groupoidal de la droite projective \mathbb{P}_Q^1 , on l'appelle $[]$ - qui correspond à un groupe extérieure à lacets infini sur lequel Γ opère - en fait, ce n'est autre que E_{K_1} , où

$$K_1 = Q(T_1)(6)$$

est l'extension transcendantal pour type de degré 1 de Q .

Partant de (6), on construit de même l'équivalent groupoidal de $U_{0,3}$ et on reconstruit comme précédent, pour avoir, sont des courbes de type $(0, \nu_2)$ sur K_1 (ou sur une extension finie de K_1) sont des courbes relatives de tipe $(0, \nu_2)$ sur une courbe sur Q (ou une extension finie de Q , ou une revêtement étale fini d'une telle $U_{0\nu_1}$).

On procède $[]$ pour construire finalement tous les E_K sur E_Q ($[]$ tout corps extension de typew fini de Q , est extension finie d'une extension transcendantal $[]$) et tous les modèles élémentaires, où $[]$ chaque avec la fibration $[]$ sont une courbe de genre 0, suite un revêtement étale fini d'une telle fibration particulière. Sauf erreur, ça fait assez pour avoir un système fondamental de voisinages de tout point d'une X lisse sur un K et de reconstituer en principe les schémas lisses sur des K , pour recollements de tels morceaux avec des "immersions ouvertes". Mais $[]$ que pour faire un telle description, il en faudrait développer un langage géométrique qui celle mieux à l'intuition géométrique, que les sempiternelles extensions de groupes profinis ... ou actions extérieures, et où les points rigides (à $[]$ alors des clôtures algébriques de corps) jouent un rôle prépondérant. Je me faudra y revenir dessus - et en même

temps, expliciter les topos étales (pas seulement le “morceau $K(\pi, 1)$ ”) [] entiers des schémas décrits ici par des extensions.

Reprenons le cas de $U = U_S$ schéma relatif sur S , “élémentaire” sur S - à fibres successives anabéliennes (s’il le faut) ou de moins à π_1 non nul, S étant lui-même (pour fixer les idées) lisse sur Q , irréductible, corps de fonctions K , et reprenons la digression 5. Considérons une section rationnelle f de U sur S , définissant une section de E_{U_K} sur E_K - ou, ce qui revient au même, un relèvement de l’homomorphisme surjectif, $E_K \longrightarrow E_S$ en $E_K \longrightarrow E_{U_S}$ (composé de la section $E_U \longrightarrow E_{U_K}$ [] $E_{U_K} \longrightarrow E_{U_S}$). Je veux montrer que f est pourtant définie i.e. une section de U_S sur S , si et seule si le section de E_{U_K} sur E_K provient d’une section de E_{U_S} sur E_S , i.e. si et seule si le relèvement $E_K \longrightarrow E_{U_S}$ [] sur le noyau de $E_K \longrightarrow E_S$.

Notons que cette dernière condition est une condition “de codimension 1 sur S ” - de façon plus précis, si Z est un sous-schéma fermé de S de codimension ≥ 2 , alors, posant $S' = S \setminus Z$, on a $\pi_1(S') \xrightarrow{\sim} \pi_1(S) = E_S$ pour le “théorème de pureté” - donc le noyau de $E_K \longrightarrow E_S$ est le même que celui de $E_K \longrightarrow E_{S'}$, ou, si [] (comme S' n’est pas un “modèle”) que le sous-groupe fermé engendré pour les noyaux des $E_K \longrightarrow E_{S'_i}$, où les S'_i sont des ouvert “modèles” qui recouvrent S' . Si donc le conditions envisagés sont [] relativement aux S'_i (qui pourtant un recouvrement par S , [] S') - ce qui est [] signifie que ce section rationnelle envisagé est [] sur les S'_i , i.e. sur S' - alors celle est vérifié relativement à S - ce qui est [] signifie que le section est [] sur S . Donc, [], il faudrait [] a priori qu’une section de $U_{S'}$ sur S' [] une section de U_S sur S . [] d’une courbe relative $U_S = X_S - T$, X lisse sur S de dimension relative 1, T fini [] sur S , [] T décomposé sur S . Si X [] relatif ≥ 1 , on sait ([] Weil) que le section [] une section de X , soit D l’image inverse de T , c’est un diviseur sur S , dont le [] sur $S' = S \setminus Z$ est nul, donc (comme $\text{codim}(Z, S) \geq 1$) il est nul, OK.

(9)

(10)

avec des carrés cartésiens, et des flèches horizontales surjectives. L’homomorphisme $E_{U_S} \longrightarrow E_K$ est composé d’un relèvement $E_K \longrightarrow E_{U_{D_n}}$ de $E_K \longrightarrow E_{D_n}$ avec l’homomorphisme canonique $E_{U_{D_n}} \longrightarrow E_{U_S}$. (relèvement $E_K \longrightarrow E_{U_{D_n}}$ correspondant biunivoquement aux sections de E_{U_n} sur E_K , ou aux relèvements de $E_K \longrightarrow E_S$ ou $E_K \longrightarrow E_{U_S} \dots$).

Ceci dit ²⁶, j’ai envie de prouver que $\varphi_n : E_K \longrightarrow E_{D_n}$ [] i.e. provient d’une section de

²⁶N.B.

E_{O_n} sur O_n si et seule si la section rationnelle correspondant de U_S/S est définie en n . Ceci impliquera l'assertion précédent (que la section ϕ de E_{U_K} sur E_K provient d'une section de E_{U_S} sur E_S , si t seule si la section rationnelle correspondant isomorphe).

Mais il s'agit ici d'un énoncé en fait $[\]$ géométrique, que j'ai envie de reformuler sous forme plus générale :

Théorème. — Soit T un trait $[\]$, U un schéma relatif "élémentaire" sur T , anabélienne²⁷, K le corps des fonctions de T , On $[\]$ un revêtement universel \tilde{U} de U , d'où une clôture algébrique \bar{K} de K , et on considère l'extension $E_U = \pi_1(U; \tilde{U})$ de $E_K = \pi_1(K, \bar{K}) \simeq \text{Gal}(\bar{K}/K)$ par $\pi = \pi_1(U_{\bar{K}}, \tilde{U})$. On a donc un carre cartésien des groupes profinis

$$[\]$$

où E_S s'identifie au quotient de E_K par le sous-groupe $[\]$ engendré par un groupe d'inertie $I_{K'} \simeq T_{\infty}(\bar{K})$, cf plus haut. Soit f_K, K un point de $U_K \text{ rel}/K$, d'où une section $\Psi = \Psi_{f_K}$ de E_K sur E_{U_K} . Ceci posé les conditionnes suivantes sont équivalentes

(a) f_K se prolonge en une section de U sur S ;

(b) Ψ provient d'une section de E_U sur E_S ;

(b') le compose $E_K \xrightarrow{\Psi} E_{U_K} \longrightarrow E_U$ s'annule sur $I_{K'}$.

L'équivalence de (b) et (b'), et qu'elles soient impliquées par (a), est clair. C'est l'implication (b) \Rightarrow (a) qui demande une démonstration. On est $[\]$ au cas où T est strictement local (donc $E_K = \text{Gal}(\bar{K}/K)$ est réduit à son sous-groupes d'inertie, et $E_S = (1)$). On est ramené de prendre un $[\]$ au cas où U_S est une courbe relative élémentaire, $U = X \setminus T$, X lisse et propre. Alors f se prolonge en une section f au X sur S , et la conclusion $[\]$ que $f(S) \subset U$. Donc on est ramené $[\]$ au

Lemme. — Soit X schéma projectif lisse de donne relation 1 connexe sur S trait strictement local, soit $T \subset X$ sous-schéma, fini étale sur S , donc $T \simeq I_S$, I ensemble fini, et soit $U = X \setminus T$ (donc T est défini par une $[\](g_i)_{i \in I}$ des sections disjointes de X sur S) si g est de genre relatif,

²⁷anabélienne $[\]$ - il suffit que les fibres de ordre 1 de la fibration élémentaire de U ne soient que de type $(0,0)$ ou $(0,1)$ - i.e. à π_1 nul

$\nu = []I$, on suppose $(g, \nu) \neq (0, 1)$. Soit $i_0 \in I$, f une section de X/S distinctes des disjoints g_i , et telle que f et g_{i_0} coïncident en s (point fermé de S). Si $\eta = S \setminus s$, on a donc un morphisme $\eta \longrightarrow U$, d'où $\pi_1(\eta) \longrightarrow \pi_1(U)$. Je dis que cet homomorphisme n'est pas trivial, et même, si $\nu \geq 2$, que pour la donné $[]$ n'est pas trivial (pour $[]$ distinct de la caractéristique résiduelle).

Comme la section rationnelle de $J_{X/S}^1$ défini par f est régulière, on voit que le composé de l'homomorphisme envisagé avec $H_n(J_{X/S}^1, Z_\ell)$ est nul - i.e. le $H_1(\eta, Z_\ell)$ s'envoie dans la partie torique de $H_1(U, Z_\ell) []$, qu'est canoniquement isomorphe à T_ℓ^I / T_ℓ . (**N. B** cette partie est nulle si $\text{card } I = i$, et dans ce cas le critère homologique $[]$ insuffisant...) Il faudrait donc calculer cet homomorphisme

$$T_\ell(\simeq H_1(\eta, Z_\ell)) \longrightarrow T_\ell^I / T_\ell$$

pour constater qu'il n'est pas nul dans le cas envisagé, $\nu \geq 2$ (et traiter $[]$ le cas $\nu = 1$). Je vais dériver le résultat : soit $x = g_{i_0}(s)$, $A = \underline{O}_{X,n}$, V l'anneau de S , J_{i_0} l'idéal de l'homomorphisme $A \xrightarrow{g_{i_0}^*} V$ associé à $[]$, c'est donc une idéal inversible de A - soit de même J_f l'idéal associé à $f^* = A \longrightarrow V$, et considérons $g_{i_0}^*(J_f)$, c'est une idéal de V engendré par un générateur, et comme $g_{i_0} \neq f$, on voit que cet idéal n'est pas nul. Soit $H = []\nu / g_{i_0}^*(J_f)$, cet entier $[]$ de g_{i_0} et f , ces $[]$ comme une multiplicité d'intersection. Ceci posé, je $[]$ que l'homomorphisme

$$T_\ell \longrightarrow T_\ell^I / T_\ell$$

est le produit $[]$ des l'injections canoniques $T_\ell \longrightarrow T_\ell^I$, correspondant à l'indice i_0 . Il faudrait que $[]$.

Reste le cas $\nu = 1$, qui semble demander un traitement séparé ²⁸. $[]$ à vérifier (pour les groupes fondamentaux premiers à p) c'est que l'homomorphisme extérieur $\pi_1(U_s) \simeq \pi_1(\eta) \longrightarrow \pi_1(U)$ est égal à $K_{i_0} \circ (\mu Id_T)$, où K_{i_0} est l'homomorphisme "local"

$$[]$$

associé à l'indice i_0 . Je vais admettre à priori, qui une ne peut guère être difficile.

Pour terminer ce numéro, je veux encore étudier, dans la situation d'une U courbe relation sur une S avec $U = X \setminus T$, X lisse et propre sur S , T fini étale, avec sections g_i donnée

²⁸Ceci doit être indépendant de la $[]$ de ν !

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

de T sur S , les “sections de 2^{ème} espèce” de l’extension

$$1 \longrightarrow \pi \longrightarrow E_U \longrightarrow E_S \longrightarrow 1$$

associées ²⁹ à $i = i_0$ - que définit une classe de π -conjugaison de sous-groupes ouverts lacets L_i dans π . (On suppose qu’on a bien une telle suite exact i.e. que $\pi_2(S) \longrightarrow \pi_1(\text{fibre})$ est nul, ce qui [] le cas si $\pi_2(S) = 0$, p. ex []) si on est dans le cas d’un modèle élémentaire au dessus d’un corps de caractéristique 0 (la reconstruction de ces [] étant sans doute [], si on [] aux groupes fondamentaux premiers aux cas résiduelles...) [] L_i dans E_U s’envoie *sur* E_S , on trouve donc des scindages pour cette extension, qu’on peut regarder comme une extension

$$1 \longrightarrow T \longrightarrow N(L_i) \longrightarrow E_S \longrightarrow 1(13)$$

La classe d’isomorphisme est un élément

$$(14)$$

que je ne propos d’étudier. On [] si S est un $K(\pi, 1)$

$$(15)$$

d’ailleurs on a une suite exacte de Kummer (ou $\text{Pic}(S) = []$)

$$0 \longrightarrow \text{Pic}(S)[](16)$$

d’où par passage à la limite

$$(17)$$

Dans le cas où S est un schéma élémentaire sur un corps de type fini sur Q , $\text{Pic}(S)$ est un \mathbb{Z} -modèle de type fini (par Mordell-Weil-Néron), donc l’homomorphisme

$$\text{Pic}(S) \longrightarrow \widehat{\text{Pic}(S)} \longrightarrow H^2(S, T)(18)$$

est *injectif*.

Sous nous [] de cette condition, considérons le cas général - je dis que la classe c (14) est donc l’image de (18), de façon précise que c’est l’image de l’élément

$$g_i \in \text{Pic}(S)$$

²⁹en tous cas, même sous []

A. GROTHENDIECK

classe des faisceaux \mathcal{O}_X (on \mathcal{O}_X) de X le \mathcal{O}_X de g_i . Principe d'une vérification : \mathcal{O}_X la complété formel de X \mathcal{O}_X de $g_v(S)$, \mathcal{O}_X ou interpréter la suite exacte (13) comme la suite exacte d'homotopie de ce topos \mathcal{O}_X , au dessus de S . On a donc à prouver une histoire d'ombres...

Dans le cas "arithmétique", on voit donc que l'extension (13) est scindée si et seule si $g_i = 0$ i.e. \mathcal{O}_X , globalement sur S , \mathcal{O}_X

Quand $g_i = 0$, parmi les scindages, il y a \mathcal{O}_X provenant \mathcal{O}_X d'une base de J_i/J_i^2 qui soit \mathcal{O}_X .

L'indétermination des choix d'une telle base \mathcal{O}_X celle des choix d'une section de (13) est donc

$$(20)$$

On a ici des suites exactes de Kummer

$$\mathcal{O}_X$$

d'où par passage à la limite

$$(21)$$

Dans le "cas arithmétique" \mathcal{O}_X on trouve donc

$$\mathcal{O}_X$$

Si le genre est zéro, prenant une de ces sections de T sur S comme section à l'infini, OPS (\mathcal{O}_X à se localiser) $U_S = \mathbb{E}'_S \setminus T'$, donc f s'identifie à une section de \mathbb{E}'_S sur S' , i.e. de \underline{O}_S sur S , donc (comme $\text{codim}(2, S) \geq 2$ \mathcal{O}_X) elle se prolonge en une section de \mathbb{E}'_S . Et on \mathcal{O}_X comme précédemment, OK. Considérons donc les diviseurs irréductibles D_i sur S , ou ce qui revient au même, les points x_v de X de $\text{codim } 1$, i.e tels que \underline{O}_{x_v} soit un \mathcal{O}_X anneau de valuations discrète). Considérons son \mathcal{O}_X \overline{O}_{x_v} dans \overline{K} , \mathcal{O}_X un idéal maximal \mathcal{O}_X (ces idéaux correspondent aux points \mathcal{O}_X \tilde{S} de S dans \overline{K} au dessus de x) et considérons son stabilisateur N_n dans E_K , qui opère donc dans $k(\tilde{x}) = \overline{k(x)}$, et s'envoie en fait, on le sait, sur $\text{Gal}(\overline{k(x)}/k(x))$.

Soit $I_{\tilde{x}}$ le noyau de l'homomorphisme obtenue (\mathcal{O}_X "géométriques" de \mathcal{O}_X), donc on a une suite exacte

$$1 \longrightarrow \mathcal{O}_X \text{Gal}(\overline{k(x)}/k(x)) \longrightarrow 1(7)$$

et par Kummer une isomorphisme canonique³⁰

$$(8)$$

³⁰à corps de \mathcal{O}_X de car 0 !

On notera que si x est le $[]$ du diviseurs D , alors $k(x)$ est le corps des fonctions de D . C'est un corps de type fini sur Q .

Il est immédiat (sans supposer que le corps de base pour S soit Q) que le noyau de $E_K \longrightarrow E_S$ est le sous-groupe $[]$ engendré par les $I_{\tilde{n}}$. Donc l'hypothèse que $E_K \longrightarrow E_{U_S} []$ sur le dit noyau, signifie aussi qu'il $[]$ sur $[]$ des $I_{\tilde{n}}$. Soit alors $U_{\underline{O}_x}$ induit par U sur $\text{Spec } Q_x$, on a donc des factorisations d'ailleurs $\mathbb{G}_n(S)$ n'a pas $[]$, donc

22)

est injectif³¹. Ainsi, quand $g_i = 0$ i.e. quand (13) admet des scindages “géométriques” (et il suffit $[]$) ceux-ci forment un torseur sous $\mathbb{G}_m(S)$, qui s'identifie à une sous-torseur des $[]$ de tous les scindages de (13). Pour que la “description profinie de la géométrie algébrique absolu sur Q soit complète, il y faudrait également caractériser (en termes de cette description profinie) le sous-ensemble remarquable.

Je voudrais enfin comprendre encore comment une section d'extensions des type (1) peut se “spécialiser” en une section de type (2), donc le cas des courbes relatives. Pour ceci, je reprends la $[]$ situation

Dans la cas $[]$ où f n'est pas définie sur S , on trouve une action de 2^{nde} espèce, $[] L_i$ dans π .

À vrai dire

$[]$

(31)

J'ai l'action extérieure de T sur π n'est souvent pas triviale (je conjecture qu'elle l'est si et seule si il y a “bonne réduction”) - donc le groupe E_K n'opère pas lui même extérieurement sur π . Mais tout scindage de (30) définit une extension de E_K par π , donc une action extérieure $[]$ “admissible”, définie par une courbe algébrique ? - Sans doute pas $[]$, si ce n'est la courbe “réduit” de type (g, v) ($[]$) ? $[]$ ce pourrait être celle ci :

Conjecture-à- $[]$. — Les conditions suivantes sont équivalentes :

(a) U_η a bonne réduction sur S ;

³¹(cas “ $[]$ ”)

- (b) L'action extérieure de T sur π est triviale (ce qui signifie ainsi que tout $[]$ scindage de (31) - p. ex défini par un point de $U_{\bar{\eta}}$ $[]$ induit un homomorphisme $T \longrightarrow \pi$);
- (c) L'action de T sur $\pi_{ab} = H_1(U_{\bar{\eta}})$ est triviale ;
- (d) Iton pour
- (e) En termes de une section de (30)
- (f) En termes de une section de (30)

On a $[]$

$[]$

J'ai donc $[]$ un $[]$ général (qui je pourrais à la occasion $[]$ avec la généralité qui lui revient) pour construire des actions extérieures $[]$ de groupes E_k (K extension de type fini de Q) sur des π à lacets, qui (sans doute) $[]$ géométriques, par la considération de courbes de type (g, v) "se réduisent $[]$ ". Mais je $[]$ pas pour cette vrai à faire des actions effectives, associées à actions extérieures $[]$ géométriques $[]$ - i.e. d'une des deux types $1^\circ, 1^\circ$ $[]$ de ce n°.

IV. Sections d'extensions et anneaux de valuations généraux

D'abord une révision de notations. Si X est une schéma connexe, je note

$$E_X = \Pi_1(X)(1)$$

son groupe fondamental profini en tant que groupe extérieur, et si \tilde{X} est un revêtement universel profini de E_X , par

$$E_X^{(\tilde{X})} = \pi_1(X; \tilde{X}) = Aut_X(\tilde{X})(2)$$

son groupe fondamental précisé - qu'est un groupe profini. Si $X = \text{Spec}(A)$, où A est un anneau (le plus souvent une corps) je note E_A , et $E_A^{\tilde{A}=E_X^{(\tilde{X})}}$. Si A est une A -algèbre telle que $\text{Spec}(\tilde{A}) = \tilde{Y}$ soit une revêtement universel de X (ce qui le détermine à isomorphisme non unique près). Bien entendu, si ξ est une "point géométrique" de X , on note

$$E_X^\xi = \Pi_1(X_1\xi) = E_X^{\tilde{X}(\xi)}, (3)$$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

où $\tilde{X}(\xi)$ est le revêtement universel de X en ξ . Le choix de ξ correspond d'une $[\]$ et d'une extension séparablement close Ω de $k(x)$ ($[\]$ clôture algébrique de $k(x)$) et on note alors ainsi E_X^Ω au lieu de E_X^ξ (Ω sous entendu $[\]$ extension de $k(x)$ donc avec sa structure de $k(x)$ algèbre) $[\]$

$$E_X^\Omega = E_X^{\overline{k(x)}}, (4)$$

où $\overline{k(\alpha)}$ est la clôture algébrique de $k(\alpha)$ dans Ω . Bien sur, si $X = \text{Spec}(A)$, on note aussi E_A^Ω – notation $[\]$ utilisée $[\]$ $E_K^{\overline{K}}$, K un corps, \overline{K} une clôture algébrique $[\]$ séparable de K .

Si X est un Y -schéma, 1-connexe, on $[\]$

$$E(f) : E_X \longrightarrow E_Y, \quad \text{où } f : X \longrightarrow Y (5)$$

E_X est un foncteur en X

$$(\text{Sch conn}) \longrightarrow \text{Group ext}$$

qui se précise pour l'homomorphisme injectif des groupes profinis

$$E_X^{\tilde{X}} \longrightarrow E_Y^{\tilde{Y}} (6)$$

où \tilde{Y} est le revêtement universel de Y défini par $\tilde{X} \longrightarrow Y$ (\tilde{X} $[\]$ pouvoir écrire en fait $E_Y^{\tilde{X}}$, plus géométriquement E_Y^Z chaque fois qu'on a un Y -schéma Z 1-connexe, jouent le rôle de “foncteur fibre” pour le topos $B_{\pi(X)}$ des revêtements étales de Y .)

On peut désir que

$$(X, \tilde{X}) \mapsto E_X^{\tilde{X}} (7)$$

est un foncteur, de la catégorie des schémas 0-connexes X munis d'un revêtement universel (on $[\]$ d'un Z 1-connexe s'envoyant dans X) vers celle des groupes profinis. Ceci s'applique en particulier en regardons la sous-catégorie des (X, ξ) munis d'un point géométrique - on a donc

$$E_X^\xi \longrightarrow E_Y^\eta (8)$$

si on a un homomorphisme de schémas “géométriques profinis” $(X, \xi) \longrightarrow (Y, \eta)$. On note que tout $[\]$ géométrique de X en un $x \in X$ - i.e. une extension $[\]$ Ω de $k(x)$ $[\]$ - et l'homomorphisme (8) s'identifie ainsi à

$$E_X^{\overline{k(x)}} \longrightarrow E_Y^{\overline{k(\eta)}} (9)$$

A. GROTHENDIECK

où $\overline{k(\alpha)}$, $\overline{k(\eta)}$ sont les clôtures séparables *dans* Ω .

On posera

$$E_{X/Y}^{\tilde{X}} = \text{Ker}(E_X^{\tilde{X}} \longrightarrow E_Y^{\tilde{X}} = E_Y^{\tilde{Y}}) \quad (10)$$

C'est un foncteur par un triple $\tilde{X} \longrightarrow X \longrightarrow Y$ avec X, Y 0-connexe, \tilde{X} un revêtement universel, plus généralement, si $T \longrightarrow X$ avec 1-connexe, on pose

$$E_{X/Y}^T = \text{Ker}(E_X^T \longrightarrow E_Y^T) \quad (11)$$

(³²) on a un foncteur $[]$. Cas particulière $E_{X/Y}^\xi$, ξ un point géométrique de X , $E_{X/Y}^\Omega, E_{X/A}^{\tilde{X}}$ (si $Y = \text{Spec } A$), $E_{B/A}^{\tilde{B}}$...

$[]$ on dispose d'une "suite exacte d'homotopie universel" (en dim 2) (³³) pour $X \longrightarrow Y$, alors le donnée (pour $X \longrightarrow Y$ donné) de $T \longrightarrow X$, (avec T 1-connexe) peut s'interpréter par la donnée d'un composé

$$T \longrightarrow Y$$

et d'un relèvement en $T \longrightarrow X$, ou ce qui revient au même, d'une section de $X_T = X \times_Y T$ sur T . Ceci posé,

$$X$$

on avoir un isomorphisme $[]$ (avec l'hypothèse de "suite exacte d'homotopie" faut)

$$E_{X/Y}^T \simeq \pi_1(X_T; T) \simeq E_{X_T}^T \quad (12)$$

et on $[]$

$$1 \longrightarrow E_{X/Y}^T \longrightarrow E_X^T \longrightarrow E_Y^T \longrightarrow 1 \quad (13)$$

(Cette hypothèse $[]$ satisfait si $Y = \text{Spec } K$, K un corps, Si X est géométriquement 0-connexe sur K).

Plus généralement, si on a une suite exacte d'homotopie universel, mais pour $[]$ avec $E_X^T \longrightarrow E_Y^T$ surjectif,

On (³⁴) $[]$ une factorisation de $X \longrightarrow Y$ en

$$X \longrightarrow Y' \longrightarrow Y \quad (14)$$

³²NB. $E_{X/T}^T []$

³³Cas où $E_X^T \longrightarrow E_Y^T$ est [un] épimorphisme

³⁴Sous l'hypothèse "suite exacte d'homotopie" mais avec fibres $[]$

LA LONGUE MARCHÉ À TRAVERS LA THÉORIE DE GALOIS

avec Y' étale fini ou pro-étales fini sur Y et $E'_X \longrightarrow E_Y$, était maintenant [un] épimorphisme, [] suite exacte universel d'homotopie bien sûr. On avoir donc isomorphismes []

$$E_{X/Y}^T \xrightarrow{\sim} E_{X/Y'}^T (15)$$

qui peut donc se [] comme

$$E_{X \times_{Y'} T}^T \simeq E_{X/Y}^T (16)$$

qu'on peut noter $E_{X_T}^T$, mais en faisant attention que [] X_T [] non plus $X \times_Y T$ (qui va être disconnexe si $Y' \longrightarrow Y$ pas isomorphisme) mais $X \times_Y T$.

Bien sur, à isomorphisme []

s'identifie bel et bien au groupe de Galois $\text{Gal}(\bar{K}, K)$ de \bar{K}/K , \bar{K} est la clôture séparable de K telle que $\text{Spec } \bar{K} \simeq \tilde{Y}$. Souvent, on notons Γ , ou Γ_K , $\Gamma_K^{\bar{K}}$, au lieu de E_Y - surtout si K est algébrique sur le corps premier, et [] donc plus de “partie géométrique” à distinguer d'une “partie arithmétique”...

Soit K un corps (qui pourrait être algébriquement clos), L une extension de type fini de K , X un “modèle” propre régulière de L . Alors $E_X^{\bar{L}}$ s'identifie à un quotient de $E_L^{\bar{L}}$, *qui ne dépend pas de modèle X défini*, comme il est [] c'est la partie “universelle géométrique” [] qui classifie les schémas (finis) étales sur L qui sont “non isomorphes” sur *tout* modèle régulière (propre ou non) de L/K .

Si U est un modèle quelconque, il se plonge dans un X , et on a des homomorphismes surjectifs [] Z partie ferme de X

$$E_X^{\bar{L}} = E_L^{\bar{L}} \simeq E_U^{\bar{L}} / \text{sous-groupe fermé []}$$

Notons que $E_L^{\bar{L}}$ est limite projective de $E_U^{\bar{L}}$, pour des modèles réguliers ([]) variables

$$E_L^{\bar{L}} \simeq [] E_U^{\bar{L}}$$

et de même, bien sûr

$$\pi_{L/K}^{\bar{L}} \simeq [] \pi_{U/K}^{\bar{L}}.$$

[],

dont le choix “effectif” dépend de celui d'un revêtement universel ou encore d'un point géométrique [] de \tilde{K}_n - i.e. d'une clôture algébrique de \tilde{K}_n []

[],

A. GROTHENDIECK

est que $a \in U$.

Ceci posé, E_U^\perp se récupère à partir de E_L^\perp , comme quotient de ce dernier, en prenant *tous* les V de L [] un centre sur U (il suffit même de prendre les $V = \underline{O}_{U,n}$, où se est [] de codim 1 des U), et [] correspondants.

On peut regarder

[]

Mais il en est [] ainsi comme on voit en considérant $V_1 = V \cap L_1$, qu'est un anneau de valuations de L_1 , (³⁵) dont le corps [] fini sur K si celui de V l'est (donc $V_1 \neq L_1$) - donc V_1 correspond à une "place" des corps de fonctions d'une variable L_1 sur K . [] E_K° centralise T_{V_1}

Conjecture. — Soient K, L des extensions de type fini de \mathbb{Q} , $K \subset L$. Alors

a) Toute section de E_L sur E_K (au guère de tel, se revient au même...) normalise sur T_V associée à un anneau de valuations V de L contenant K , à corps résiduel algébrique sur K et V est uniquement (³⁶) [] cette condition [] au dessus de E_K .

b) Soit U un modèle "élémentaire" de L sur K , anabélien. Alors tout section de E_U^\perp sur E_K^\perp se relie [] une section de E_L^\perp sur E_K^\perp .

À noter que ce question 2° est [] locale [] elle doit être essentiellement "triviale", que [] vraie un [] - par contre 1°, est une question de [] globale sur U , et sans doute [] façons triviale.

La validité des ces énonces, impliquant donc, pour les sections de E_U^\perp sur E_K^\perp associées à un anneau de valuations de L/K de corps résiduel K , que l'image de E_K^\perp doit normaliser un sous-groupe [] de $\pi_{L/K}^\perp$, qui est non trivial si le valuation [] centre sur U , i.e. si le section n'est pas associé à un point K -rationnel de U , ce qui est justifiant [] des conjectures (qui prouvent d'abord [] !) de §2.

Avant de [] vers l'étude des questions 1°) et 2°) et ainsi des questions de normalisation et de centralisations [] précédemment a propos de N_V, I_V, \dots),

³⁵Il faut []

³⁶ []