Le théorème de Tamagawa I.

Tamás Szamuely

Le présent exposé contient un rapport sur la première partie de la démonstration par Tamagawa de la conjecture anabélienne de Grothendieck pour les courbes hyperboliques affines, précédé d'une introduction succincte à ce cercle d'idées. Le rôle du rédacteur s'est surtout limité à transformer la pagode richement ornementée de Tamagawa en une sorte de cube style Bauhaus. A part les techniques de géométrie algébrique, la bonne compréhension du texte nécessite une certaine familiarité avec les théorèmes classiques de la théorie des corps de classes.

C'est un plaisir de remercier Jean-Louis Colliot-Thélène et Philippe Gille pour leur lecture attentive d'une version préliminaire.

1 Introduction au monde anabélien

La théorie du groupe fondamental en géométrie algébrique telle qu'on la voit aujourd'hui a été introduite par Grothendieck vers 1960 dans son séminaire [SGA1] comme une généralisation commune de la théorie du groupe fondamental des variétés complexes et de la théorie de Galois. En effet, il a associé de façon fonctorielle à tout schéma connexe X muni d'un point géométrique $\bar{x}$ un groupe profini $\pi_1(X, \bar{x})$, qui pour une variété complexe n'est autre que le complété profini de son groupe fondamental topologique, et pour le spectre d'un corps k, son groupe de Galois absolu $Gal(k)$. De plus, si X est un schéma géométriquement connexe, de type fini au-dessus d'un corps k, la fonctorialité du groupe fondamental conduit à une suite exacte naturelle

$$1 \to \pi_1(\overline{X}, \bar{x}) \to \pi_1(X, \bar{x}) \to Gal(k) \to 1, \tag{1}$$

le schéma $\overline{X}$ étant celui obtenu à partir de X par extension de scalaires à la clôture algébrique $\bar{k}$ de k. Le groupe $\pi_1(\overline{X}, \bar{x})$ s'appelle le groupe fondamental *géométrique* de X.

Le groupe $\pi_1(X, \bar{x})$ agit sur $\pi_1(\overline{X}, \bar{x})$ par conjugaison, induisant une représentation $\pi_1(X, \bar{x}) \to Aut(\pi_1(\overline{X}, \bar{x}))$. La restriction de cette représentation à $\pi_1(\overline{X}, \bar{x})$ a pour image le sous-groupe distingué $Inn(\pi_1(\overline{X}, \bar{x}))$ des automorphismes intérieurs. Par passage au quotient, nous obtenons donc une représentation

$$\rho: \ Gal(k) \to Out(\pi_1(\overline{X}, \bar{x})),$$

où $Out(\pi_1(\overline{X}, \bar{x})) = Aut(\pi_1(\overline{X}, \bar{x}))/Inn(\pi_1(\overline{X}, \bar{x}))$ est le groupe des *automorphismes extérieurs* de $\pi_1(\overline{X}, \bar{x})$. Dans le cas où le centre de $\pi_1(\overline{X}, \bar{x})$ est trivial, le morphisme $\pi_1(\overline{X}, \bar{x}) \to Inn(\pi_1(\overline{X}, \bar{x}))$ est bijectif, et a fortiori, $\pi_1(X, \bar{x})$ s'identifie au produit fibré $Aut(\pi_1(\overline{X}, \bar{x})) \times_{Out(\pi_1(\overline{X}, \bar{x}))} Gal(k)$. Dans ce cas, le groupe fondamental géométrique et la représentation ρ déterminent donc la classe de l'extension (1). Si k est un sous-corps de $\mathbf{C}$, le groupe fondamental apparaît ainsi comme un objet "transcendant" muni d'une action de Galois.

Quand, vingt ans plus tard dans sa solitude montpelliéraine, Grothendieck est revenu à l'une de ses premières amours, il a eu la vision que certains schémas, dits *anabéliens*, sont déterminés à isomorphisme près par ces données. Plus précisément, on peut résumer (d'après [2], [3], [11], [19]) sa conjecture comme suit.

Soit k un corps de type fini sur $\mathbf{Q}$, et X_1, X_2 deux schémas géométriquement connexes de type fini sur k. Tout k-morphisme $\phi: \ X_1 \to X_2$ induit un morphisme de groupes profinis $\pi_1(\phi): \ \pi_1(X_1) \to \pi_1(X_2)$ compatible avec les projections sur $Gal(k)$. (Pour alléger la notation, on n'indique plus les points géométriques). En général, étant donné deux groupes profinis G_1 et G_2 munis de projections vers un troisième groupe G, notons $Hom^*_G(G_1, G_2)$ l'ensemble des morphismes de G_1 dans G_2 compatibles avec la projection vers *G à un automorphisme intérieur de G près.* La composition avec les automorphismes intérieurs de G_1 (resp. G_2) munit alors l'ensemble $Hom^*_G(G_1, G_2)$ d'une action à droite de G_1 (resp. d'une action à gauche de G_2). Ici l'orbite d'un morphisme *surjectif* sous G_1 est la même que sous G_2. En particulier, les orbites sous G_1 et G_2 des *G-isomorphismes* $G_1 \to G_2$ sont les mêmes; on note $Isom^{ext}_G(G_1, G_2)$ leur ensemble. Dans le cas général, les orbites sous G_1 et G_2 peuvent différer et on définit l'ensemble $Hom^{ext}_G(G_1, G_2)$ des homomorphismes extérieurs comme le quotient de $Hom^*_G(G_1, G_2)$ sous l'action intérieure de G_2. On obtient ainsi la catégorie $\mathbf{Prof}^{ext}_G$ des groupes profinis G-augmentés avec les homomorphismes extérieurs. Revenant à notre situation concrète, la conjecture de Grothendieck peut se formuler ainsi:

Conjecture 1.1 (Grothendieck [3]) *Soit k un corps de type fini sur $\mathbf{Q}$. Il existe une sous-catégorie pleine $\mathcal{A}$ de la catégorie des schémas géométriquement connexes de type fini sur k dont le foncteur $\pi_1(\,)$ induit un plongement pleinement fidèle dans la catégorie $\mathbf{Prof}^{ext}_{Gal(k)}$. Cette sous-catégorie, dite la catégorie des k-schémas anabéliens, doit comprendre:*

- *le spectre de k;*

- *les k-courbes hyperboliques (i.e. les k-courbes lisses dont le groupe fondamental géométrique a un centre trivial, mais il n'est pas trivial lui-même);*

- *les fibrations lisses en schémas anabéliens au-dessus d'une base anabélienne.*

Grothendieck considère également les espaces de modules de courbes pointées (ou de variétés abéliennes polarisées) comme objets anabéliens; comme ils n'entrent pas dans la catégorie des k-schémas de type fini, nous avons préféré les omettre ici. Par contre, notons, suivant Grothendieck, que par la théorie des bons voisinages d'Artin, la conjecture sous sa forme ci-dessus impliquerait que tout point d'un k-schéma lisse admet une base de voisinages formée de schémas affines anabéliens. Ce dernier énoncé peut être perçu comme un analogue conjectural du fait que tout point d'une variété algébrique complexe possède une base de voisinages ouverts (pour la topologie complexe) constituée d'espaces d'Eilenberg-Maclane $K(\pi, 1)$.

Regardons quelques cas particuliers de plus près. La conjecture implique que pour deux k-schémas anabéliens de même dimension, l'ensemble des $Gal(k)$-isomorphismes extérieurs de leurs groupes fondamentaux est en bijection avec l'ensemble de leurs k-isomorphismes. C'est maintenant connu en dimension 1:

Théorème 1.2 ([6], [16]) *Soient X_1 et X_2 deux courbes hyperboliques définies sur un corps k de type fini sur $\mathbf{Q}$. Alors l'application naturelle*

$$Isom_{Schémas/k}(X_1, X_2) \to Isom_G^{ext}(\pi_1(X_1), \pi_1(X_2))$$

est bijective.

Le théorème est dû à A. Tamagawa dans le cas affine – c'est l'objet principal de cet exposé. Le cas projectif a été démontré par S. Mochizuki avec des méthodes de géométrie logarithmique (il a ensuite prouvé un résultat plus puissant en utilisant la théorie de Hodge p-adique).

Il existe également une version "absolue" du théorème: les isomorphismes entre schémas (pas nécessairement définis sur k) correspondent bijectivement aux isomorphismes extérieurs (sans augmentation) entre groupes fondamentaux. Cela résulte de la combinaison du théorème avec la version "birationnelle" suivante de la conjecture de Grothendieck, prouvée par Pop ([10]):

les isomorphismes de corps de type fini sur $\mathbf{Q}$ *correspondent bijectivement aux isomorphismes extérieurs de leurs groupes de Galois absolus.* Pop a également démontré une version de ce théorème en caractéristique positive. Notons que ses résultats ont d'importants précurseurs dans le travail de Neukirch, Uchida ([8], [18]) et autres dans les années 70; ces auteurs ont traité le cas des corps globaux classiques. Comme on le verra, leurs techniques jouent un rôle important dans la démonstration de Tamagawa.

En conclusion de notre petit tour du monde anabélien, mentionnons un autre cas particulier de la conjecture ci-dessus qui attend toujours sa démonstration: selon Grothendieck, l'ensemble des points k-rationnels d'une k-courbe hyperbolique devrait être en bijection avec l'ensemble des classes de conjugaison de sections de l'augmentation galoisienne dans la suite exacte (1). On n'en sait rien pour l'instant, mais Tamagawa a un analogue intéressant sur les corps finis (cf. le chapitre 4).

Disons enfin quelques mots sur la macrostructure de la preuve de Tamagawa. D'abord, il établit la variation suivante sur le thème principal:

Théorème 1.3 (Tamagawa, [16], Theorem 4.3) *Soient F_1, F_2 des corps finis, U_1 et U_2 deux courbes hyperboliques affines définies respectivement sur F_1 et sur F_2. Notons $\pi_1^t(U_i)$ le groupe fondamental modéré d'une compactification lisse de U_i, i. e. le quotient de $\pi_1(U_i)$ classifiant les revêtements étales de U_i modérément ramifiés à l'infini. Alors l'application naturelle*

$$Isom_{Schémas}(U_1, U_2) \to Isom^{ext}(\pi_1^t(U_1), \pi_1^t(U_2))$$

est bijective.

Il s'agit ici d'un énoncé "absolu" – la raison étant qu'il est possible de repérer le groupe de Galois d'un corps fini F parmi les quotients du groupe fondamental modéré d'une courbe au-dessus de F (cf. la prop. 3.2). La méthode suivie pour l'établir doit beaucoup à celle d'Uchida dans la version "birationnelle" du théorème, nous avons donc jugé utile de donner au chapitre suivant un bref résumé de cette preuve très élégante. Notons au passage que l'article [16] de Tamagawa contient également un énoncé où les $\pi_1^t(U_i)$ sont remplacés par les $\pi_1(U_i)$ – ce théorème vaut d'ailleurs pour des courbes affines quelconques.

La démonstration du théorème 1.2 procède alors en choisissant un modèle affine lisse V du corps de base k et des V-modèles $\mathcal{U}_i$ des courbes U_i ainsi que de leurs compactifications lisses, puis en appliquant le théorème 1.3 aux spécialisations des modèles $\mathcal{U}_1, \mathcal{U}_2$ en des points fermés de V. Ici le théorème d'irréductibilité de Hilbert ainsi qu'une version "anabélienne" du critère de bonne réduction de Serre-Tate jouent un rôle fondamental. Tout cela sera expliqué en détail dans l'exposé de David Harari – pour notre part, nous nous limitons désormais au cas d'un corps de base fini.

2 Ce que fait Uchida

Pour préparer la voie à la démonstration de Tamagawa, nous esquissons dans ce chapitre le principe de la démonstration du résultat suivant.

Théorème 2.1 (Uchida [18]) *Soient F_1, F_2 des corps finis. Étant donné pour $i = 1, 2$ une courbe propre lisse X_i définie sur F_i, de corps de fonctions $F_i(X_i)$, l'application naturelle*

$$Isom(F_1(X_1), F_2(X_2)) \to Isom^{ext}(Gal(F_1(X_1)), Gal(F_2(X_2)))$$

est une bijection.

Bien entendu, c'est la surjectivité qui est la partie intéressante du théorème. Voici comment on l'établit.

1. Fixons une clôture séparable Ω_i de $F_i(X_i)$. Tout point fermé de X_i induit alors des valuations discrètes (à valeurs dans $\mathbf{Q}$) sur Ω_i. On montre d'abord, suivant Neukirch, que ces valuations correspondent bijectivement à leurs groupes de décomposition. Le fait non-trivial ici est que deux valuations de Ω_i ne peuvent pas admettre le même groupe de décomposition. Cela résulte d'un théorème classique, dû à F. K. Schmidt [12], d'après lequel un corps non-séparablement clos ne peut être muni que d'une seule valuation discrète hensélienne. (Pour une démonstration élégante de ce théorème dans un cadre légèrement plus général, voir [7], Lemma 8.)

2. Toujours d'après Neukirch, on prouve ensuite qu'un sous-groupe fermé D de $Gal(F_i(X_i))$ est le groupe de décomposition d'une valuation discrète de Ω_i si et seulement si il possède la propriété suivante: étant donné un nombre premier l, le groupe de cohomologie galoisienne $H^2(G, \mathbf{Z}/l\mathbf{Z})$ est isomorphe à $\mathbf{Z}/l\mathbf{Z}$ ou 0 pour tout sous-groupe ouvert G de D, selon la présence ou non des racines l-ièmes de l'unité dans le corps fixé par G. Cela se déduit après passage à la limite de la suite exacte d'Albert-Brauer-Hasse-Noether en théorie des corps de classes globale.

3. Il résulte donc des numéros précédents que tout isomorphisme entre $Gal(F_1(X_1))$ et $Gal(F_2(X_2))$ induit une bijection entre les valuations discrètes des Ω_i (et a fortiori entre les points fermés des X_i) ainsi que des isomorphismes sur leurs groupes de décomposition. Si D_i est un tel groupe de décomposition, il est le groupe de Galois d'un complété K_i de $F_i(X_i)$, qui est un corps de séries de Laurent sur une extension finie E_i de F_i. Par la théorie des corps de classes locale, le groupe multiplicatif de E_i est isomorphe au sous-groupe de torsion de l'abélianisé de D_i. Comme E_i est également le corps résiduel de K_i, en appliquant cet argument à un sous-groupe d'indice fini de D_i, on peut décider si ce sous-groupe fixe une extension non ramifiée ou pas en regardant la torsion de son abélianisé. Ainsi, on voit que l'on a isomorphisme sur les sous-groupes d'inertie des D_i. En considérant des extensions de Kummer totalement ramifiées, Uchida parvient également à établir une bijection entre les éléments de Frobenius des D_i. Comme l'image de l'application de réciprocité locale est engendrée par les sous-groupes d'inertie et les Frobenius, on obtient des isomorphismes entre les groupes multiplicatifs des complétés des $F_i(X_i)$ en leurs points fermés correspondants.

4. Le numéro précédent fournit donc un isomorphisme entre les groupes d'idèles des corps $F_i(X_i)$. Mais le groupe d'idèles d'un corps de fonctions est le domaine de l'application de réciprocité globale et le groupe multiplicatif du corps est son noyau. Nous obtenons ainsi un isomorphisme $F_1(X_1)^\times \cong F_2(X_2)^\times$. Uchida vérifie enfin qu'en rajoutant les éléments 0 nous arrivons à une bijection *additive* entre $F_1(X_1)$ et $F_2(X_2)$.

La démonstration du théorème 1.3 par Tamagawa poursuit la même philosophie: caractérisation galoisienne des groupes de décomposition, bijection entre les points fermés des "revêtements modérés universels", utilisation de la théorie des corps de classes locale et globale pour établir des isomorphismes sur les groupes d'idèles, puis les groupes multiplicatifs des corps de fonctions; enfin, récupération des courbes en utilisant la bijection entre les points. Mais pour l'analogue des étapes 1 et 2, il doit appliquer une méthode complètement différente – en fait, le groupe de décomposition d'un point non ramifié du revêtement universel dans le groupe fondamental modéré d'une courbe étant isomorphe à $\hat{\mathbf{Z}}$, il n'est pas possible de le distinguer cohomologiquement parmi les innombrables sous-groupes procycliques. Le substitut de Tamagawa sera discuté dans les deux chapitres suivants. Le reste de l'argument, d'un esprit proche de celui des points 3. et 4, fera l'objet du chapitre 5.

3 Caractérisation d'invariants

Nous avons vu lors du survol de la méthode d'Uchida que la démonstration procède en reconstituant d'abord de nombreux invariants des corps de fonctions à partir de leurs groupes de Galois. Dans ce chapitre, nous nous proposons de faire un travail analogue en partant du groupe fondamental modéré.

Dans la suite, soient U une courbe affine lisse définie sur un corps fini F, X une compactification lisse de U, de genre g et de corps de fonctions K. Notons S le fermé complémentaire de U dans X et n le cardinal de $S(\bar{F})$, i.e. le nombre des "points géométriques à l'infini".

Convention 3.1 *Disons qu'un sous-quotient (fonctoriel en U) G_U de $\pi_1^t(U)$ (resp. un invariant Φ_U attaché à U) est* **repérable** *si tout isomorphisme $\pi_1^t(U) \cong \pi_1^t(V)$, où V est une autre courbe lisse sur un corps fini, induit un isomorphisme $G_U \cong G_V$ (resp. une égalité $\Phi_U = \Phi_V$). De même, un morphisme entre deux sous-quotients repérables est repérable s'il est compatible aux isomorphismes $\pi_1^t(U) \cong \pi_1^t(V)$; une propriété d'un sous-quotient ou d'un morphisme est repérable si elle n'est pas affectée par ces isomorphismes.*

Proposition 3.2 *Le groupe de Galois absolu $Gal(F)$ et le groupe fondamental modéré géométrique $\pi_1^t(\bar{U})$ sont repérables.*

C'est ce fait qui explique pourquoi on dispose d'un analogue "absolu" de la conjecture anabélienne pour les courbes sur les corps finis.

Démonstration. Ces groupes se capturent déjà au niveau de l'abélianisé $\pi_1^t(U)^{ab}$ de $\pi_1^t(U)$. En effet, comme $Gal(F)$ est isomorphe à $\hat{\mathbf{Z}}$, il est abélien et en tant que tel quotient de $\pi_1^t(U)^{ab}$. Nous allons montrer que le noyau $\pi_1^t(U)_0^{ab}$ de la projection $\pi_1^t(U)^{ab} \to Gal(F)$ est fini, ce qui établit la proposition car il permet de récupérer $Gal(F)$ comme $\pi_1^t(U)^{ab}$ modulo torsion, puis $\pi_1^t(\bar{U})$ comme le noyau de $\pi_1^t(U) \to Gal(F)$.

Soit $\mathbf{m}$ le diviseur sur X correspondant à la somme des points fermés de S. Par la théorie des corps de classes telle qu'elle est exposée dans [14], le groupe $\pi_1^t(U)_0^{ab}$ est isomorphe au groupe des F-points de la jacobienne généralisée $J_{\mathbf{m}}$ associée au "module" $\mathbf{m}$. Mais ce dernier groupe est fini.

Proposition 3.3 *Si U n'est pas la droite affine, la caractéristique p de F est repérable.*

Démonstration. Pour un nombre premier l, notons $\pi_1^t(\bar{U})^{(l)}$ le plus grand pro-l-quotient de $\pi_1^t(\bar{U})$ et $r(l)$ son nombre minimal de générateurs. D'après [13], cor. au prop. 25, $r(l)$ est égal à la dimension du $\mathbf{Z}/l\mathbf{Z}$-espace vectoriel $H^1(\pi_1^t(\bar{U})^{(l)}, \mathbf{Z}/l\mathbf{Z})$. Pour $l \neq p$, cette dimension vaut $2g+n-1$ par comparaison avec la théorie transcendante ([SGA1]). Pour $l = p$, le groupe $H^1(\pi_1^t(\bar{U})^{(p)}, \mathbf{Z}/p\mathbf{Z})$ classifie les revêtements galoisiens de X de groupe $\mathbf{Z}/p\mathbf{Z}$, étales sur U et modérément ramifiés sur S. Comme l'indice de ramification doit diviser p, ils sont étales partout, et on a affaire au groupe $H^1(\pi_1^t(\bar{X})^{(p)}, \mathbf{Z}/p\mathbf{Z})$, ou encore à $H^1_{\text{ét}}(\bar{X}, \mathbf{Z}/p\mathbf{Z})$. Comme $\bar{X}$ est propre sur un corps algébriquement clos de caractéristique p, ce groupe n'est autre que le noyau de l'application d'Artin-Schreier $F : H^1(\bar{X}, O_{\bar{X}}) \to H^1(\bar{X}, O_{\bar{X}})$ (cf. [5], prop. 4.12). A fortiori, $r(p) \leq g < 2g+n-1$ sauf pour $g = 0$. Ainsi, $r(p)$ se distingue comme la seule valeur de $r(l)$ différente de $2g+n-1$.

Dans cette preuve, nous avons utilisée les rudiments de la théorie du p-rang; pour une étude plus approfondie, voir l'exposé d'Irene Bouw dans ce volume.

On suppose désormais que U est *hyperbolique.*

Proposition 3.4 *Le Frobenius engendrant $Gal(F)$, le cardinal q de F, le cardinal n de $S(\bar{F})$ ainsi que le genre g de X sont repérables.*

Démonstration. Gardons les notations de la démonstration précédente et fixons un nombre premier $l \neq p$. D'après [4], démonstration du th. 1, le $Gal(F)$-module $\pi_1^t(\bar{U})^{(l),ab}$ se dévisse en une suite exacte

$$0 \to T_l(\mathbf{G}_m(\bar{F})) \to T_l(\mathbf{G}_m^n(\bar{F})) \to \pi_1^t(\bar{U})^{(l),ab} \to T_l(Pic_X^0(\bar{F})) \to 0$$

où pour un groupe abélien A, $T_l(A)$ désigne son module de Tate l-adique. Considérons d'abord le cas où $n > 1$. Par le théorème de Weil sur les variétés abéliennes et la suite exacte ci-dessus, les valeurs propres du Frobenius sur $\pi_1^t(\bar{U})^{(l),ab}$ sont q (avec multiplicité $(n-1)$) ainsi que $2g$ entiers algébriques de valeur absolue $q^{1/2}$. De plus, ces propriétés caractérisent le Frobenius parmi les autres éléments de $Gal(F)$, d'où la proposition dans ce cas.

Sinon, les valeurs propres que l'on trouve ont toutes la même valeur absolue. Le cas où l'on est en difficulté est quand les valeurs propres sont toutes égales à un nombre premier car on ne peut pas savoir si on a affaire à une courbe de genre 0 avec beaucoup de points géométriques à l'infini ou bien à une courbe de genre positif avec un seul point. Comme le centre de $\pi_1^t(\bar{U})$ est supposé non trivial, on peut exclure les cas $g = 0, n \leq 2$. Sinon, passons à un revêtement défini par un sous-groupe ouvert de $\pi_1^t(U)$ et regardons les valeurs propres dans cette situation. On peut alors décider, en utilisant la formule de Hurwitz, si g était au moins deux (et a donc considérablement augmenté) ou bien il était 0 – le casse-tête d'origine est ainsi résolu.

Proposition 3.5 *Le groupe $\pi_1(X)$ comme quotient de $\pi_1^t(U)$ est repérable.*

Démonstration. Soient H un sous-groupe d'indice fini de $\pi_1^t(U)$, g_H le genre du revêtement correspondant de X. D'après la formule de Hurwitz, ce revêtement est étale si et seulement si

$$2g_H - 2 = [\pi_1^t(\bar{U}) : \pi_1^t(\bar{U}) \cap H](2g-2).$$

L'intersection des H ayant cette propriété est précisément le noyau de la surjection $\pi_1^t(U) \to \pi(X)$.

Proposition 3.6 *Le nombre des points rationnels de X au-dessus d'une extension finie F' de F est repérable.*

Démonstration. C'est de nouveau une application du théorème de Weil. Si le degré de l'extension est m, faisons la somme des valeurs propres de la m-ième puissance de Frobenius sur $\pi_1(\bar{X})^{(l),ab}$. En rajoutant le nombre des F'-points, nous devons obtenir $1+q^m$. Comme les valeurs propres du Frobenius et l'entier q sont repérables, le nombre des points est également repérable.

4 Les substituts des théorèmes de Schmidt et de Neukirch

Gardant les conventions et hypothèses du chapitre précédent, nous allons maintenant repérer les groupes de décomposition des points du "revêtement modéré universel" dans $\pi_1^t(U)$, obtenant ainsi des énoncés analogues aux deux premières étapes de la démonstration d'Uchida esquissée au chapitre 2.

Plus précisément, fixons une clôture séparable du corps de fonctions K et considérons la sous-extension maximale $\tilde{K}$ non ramifiée sur U et modérément ramifiée au-dessus de S. Le schéma $\tilde{X}$ obtenu en normalisant X dans $\tilde{K}$ est la limite projective des normalisés de X dans des sous-extensions finies de $\tilde{K}|K$, et a fortiori un point fermé $\tilde{x}$ de $\tilde{X}$ peut être identifié à une suite cohérente de points fermés de revêtements finis modérés de X. Si x est le point de X au-dessous de $\tilde{x}$, notons K_x le complété de K par rapport à la valuation v_x

associée à x. Avec cette notation, le point $\tilde{x}$ correspond à une extension de v_x sur $\tilde{K}$ et le complété de $\tilde{K}$ par rapport à cette valuation est l'extension maximale non ramifiée (resp. modérément ramifiée) de K_x si $x \in U$ (resp. $x \in S$). Ce sont les groupes de décomposition de points de $\tilde{X}$ dans $\pi_1^t(U)$ que l'on aimerait caractériser.

Pour ce faire, Tamagawa a eu l'idée de recourir à l'outil technique suivant. Nous avons vu que la suite exacte (1) donne lieu à une représentation de $Gal(F)$ dans $Out(\pi_1(\overline{X}))$. Le groupe des commutateurs de $\pi_1(\overline{X})$ étant caractéristique, par passage au quotient nous obtenons une action bien définie de $Gal(F)$ sur $\pi_1(\overline{X})^{ab}$ et a fortiori sur $\pi_1(\overline{X})^{ab}/l^m$ pour tout nombre premier l et entier positif m. Or en vertu de [5], th. III.3.9 et cor. III.4.18, ce dernier $Gal(F)$-module est isomorphe au sous-groupe de l^m-torsion de $Pic^0(\overline{X})$ que nous noterons $Pic^0(\overline{X})\{l^m\}$ dans la suite (ce fait a déjà été implicitement utilisé pour $l \neq p$ dans la démonstration de la prop. 3.3). Soient maintenant G un sous-groupe ouvert de $Gal(F)$, et s_1, s_2 deux homomorphismes $G \to \pi_1(X)$ qui scindent la surjection $\pi_1(X) \to Gal(F)$ au-dessus de G. Pour chaque $\sigma \in G$, l'élément $s_1(\sigma)s_2(\sigma)^{-1}$ vit dans $\pi_1(\overline{X})$, on peut donc considérer son image dans $\pi_1(\overline{X})^{ab}$. Un calcul facile montre que la fonction $G \to \pi_1(\overline{X})^{ab}$ ainsi obtenue est un 1-cocycle. Notons α_m son image dans le groupe $H^1(G, \pi_1(\overline{X})^{ab}/l^m) = H^1(G, Pic^0(\overline{X})\{l^m\})$.

Remarque 4.1 Donnons une interprétation du cocycle α_m en utilisant la cohomologie étale. Pour simplicité, nous ne traitons que le cas $G = Gal(F)$. Le dual du morphisme induit par une section s_i sur le quotient $\pi_1(\overline{X})^{ab}/l^m$ est un morphisme $H^1_{\text{ét}}(X, \mathbf{Z}/l^m\mathbf{Z}) \to H^1(G, \mathbf{Z}/l^m\mathbf{Z})$ scindant le morphisme naturel $H^1(G, \mathbf{Z}/l^m\mathbf{Z}) = H^1_{\text{ét}}(F, \mathbf{Z}/l^m\mathbf{Z}) \to H^1_{\text{ét}}(X, \mathbf{Z}/l^m\mathbf{Z})$. En écrivant la suite exacte des termes de bas degré de la suite spectrale de Hochschild-Serre, on obtient

$$0 \to H^1(G, \mathbf{Z}/l^m\mathbf{Z}) \to H^1_{\text{ét}}(X, \mathbf{Z}/l^m\mathbf{Z}) \to H^0(G, H^1_{\text{ét}}(\overline{X}, \mathbf{Z}/l^m\mathbf{Z})) \to H^2(G, \mathbf{Z}/l^m\mathbf{Z}),$$

le dernier groupe étant 0 car F est un corps fini. Par ce qui a été dit plus haut, le dual de la différence $s_1 - s_2$ s'annule donc sur l'image du morphisme de gauche dans la suite exacte ci-dessus, et a fortiori induit un morphisme $H^0(G, H^1_{\text{ét}}(\overline{X}, \mathbf{Z}/l^m\mathbf{Z})) \to H^1(G, \mathbf{Z}/l^m\mathbf{Z}) \cong \mathbf{Z}/l^m\mathbf{Z}$. Mais on a des isomorphismes

$$H^0(G, H^1_{\text{ét}}(\overline{X}, \mathbf{Z}/l^m\mathbf{Z}))^* \cong H^1(G, H^1_{\text{ét}}(\overline{X}, \mathbf{Z}/l^m\mathbf{Z})^*) \cong H^1(G, H^1_{pl}(\overline{X}, \mu_{l^m}))$$

où l'étoile indique le groupe abélien dual et le souscript *pl* la cohomologie plate. Le premier isomorphisme provient de la dualité de Tate pour un module galoisien sous le groupe de Galois d'un corps fini, le deuxième de la dualité de Poincaré pour $l \neq p$ (en utilisant le théorème de comparaison [5], th. III.3.9) et de la dualité d'Artin-Milne [1] pour $l = p$. Enfin, le dernier groupe n'est autre que $H^1(G, Pic^0(\overline{X})\{l^m\})$, toujours d'après [5], cor. III.4.18.

Disposant de cette interprétation, c'est un exercice sans grande difficulté de vérifier la compatibilité suivante:

Lemme 4.2 *Dans la situation ci-dessus, supposons que les sections s_1, s_2 proviennent de points x_1, x_2 de X rationnels sur $\bar{F}^G$. Alors le cocycle α_m coïncide avec l'image du zéro-cycle $(x_1 - x_2) \in Pic^0(\overline{X})^G$ par le morphisme composé*

$$Pic^0(\overline{X})^G \to Pic^0(\overline{X})^G / l^m Pic^0(\overline{X})^G \to H^1(G, Pic^0(\overline{X})\{l^m\})$$

où le deuxième morphisme provient de la suite exacte de cohomologie associée à la suite exacte courte

$$0 \to Pic^0(\overline{X})\{l^m\} \to Pic^0(\overline{X}) \xrightarrow{l^m} Pic^0(\overline{X}) \to 0$$

existant à cause de la divisibilité de $Pic^0(\overline{X})$.

Par passage à la limite projective, on obtient la cohomologie continue $H^1_{cont}(G, T_l Pic^0(\overline{X})) = \varprojlim H^1(G, Pic^0(\overline{X})\{l^m\})$. Et le lemme ci-dessus implique le

Corollaire 4.3 *L'image du cocycle $\sigma \mapsto s_1(\sigma) s_2(\sigma)^{-1}$ dans le groupe $H^1_{cont}(G, T_l Pic^0(\overline{X}))$ provient de $\varprojlim Pic^0(\overline{X})^G / l^m Pic^0(\overline{X})^G$.*

Nous pouvons maintenant démontrer l'analogue suivant du théorème de F. K. Schmidt cité au chapitre 2.

Proposition 4.4 *Deux points différents $\tilde{x}_1 \neq \tilde{x}_2$ de $\tilde{X}$ ne peuvent pas admettre le même groupe de décomposition dans $\pi_1^t(U)$.*

Démonstration. Supposons que ce soit quand même le cas. Prenons un sous-groupe ouvert H définissant un revêtement X_H de X dont $\tilde{x}_1$, $\tilde{x}_2$ induisent deux points fermés distincts $x_1 \neq x_2$. La courbe X étant supposée hyperbolique, on a ou bien $g > 0$ ou alors $n > 2$, ce qui permet de choisir H de sorte que le genre de X_H soit non nul. L'hypothèse implique que les points x_1, x_2 admettent le même groupe de décomposition D dans $\pi_1(X_H)$;

soit G son image dans $Gal(F)$. Par sa définition même, le groupe G fixe les points x_1 et x_2. A fortiori, les sections s_1 et s_2 correspondantes sont toutes les deux identiques à l'inverse de l'isomorphisme $D \to G$, donc leur quotient est trivial. En appliquant le corollaire précédent à X_H à la place de X, on trouve que le zéro-cycle $x_1 - x_2$ est infiniment l-divisible dans $Pic^0(\overline{X_H})^G$ pour tout l, i.e. il est infiniment divisible. Mais le groupe $Pic^0(\overline{X_H})^G$ étant fini, il ne contient pas d'éléments infiniment divisibles non triviaux. Ainsi, le zéro-cycle $x_1 - x_2$ est linéairement équivalent à zéro, ce qui est impossible car le genre de X_H est supposé différent de 0.

Soit maintenant G un sous-groupe d'indice fini de $Gal(F)$. Appelons, suivant Tamagawa, *section géométrique* tout homomorphisme $s : G \to \pi_1^t(U)$ scindant la surjection $\pi_1^t(U) \to Gal(F)$ au-dessus de G dont l'image est contenue dans le groupe de décomposition d'un point fermé $\tilde{x}$ de $\tilde{X}$.

Proposition 4.5 *Soit $s : G \to \pi_1^t(U)$ une section géométrique. Alors il n'existe qu'un seul sous-groupe de décomposition de $\pi_1^t(U)$ contenant $s(G)$.*

Démonstration. Soient $\tilde{x}_1$, $\tilde{x}_2$ des points de $\tilde{X}$ dont les groupes de décomposition D_1, D_2 contiennent $s(G)$. Prenons un sous-groupe H comme dans la démonstration précédente. Quitte à le restreindre, on peut supposer que $s(G) \cap H$ et les groupes $D_i \cap H$ pour $i = 1, 2$ ont même image dans $Gal(F)$. Les images $\bar{D}_i$ des $D_i \cap H$ dans $\pi_1(X_H)$ sont isomorphes à $\hat{\mathbf{Z}}$, donc s'injectent dans $Gal(F)$. De plus, l'image de $s(G)$ dans $\pi_1(X)$ est contenue dans $\bar{D}_1 \cap \bar{D}_2$ et se projette sur le même sous-groupe de $Gal(F)$ que les $\bar{D}_i$. A fortiori, $\bar{D}_1 = \bar{D}_2$ et, par la démonstration précédente, $\tilde{x}_1 = \tilde{x}_2$.

Proposition 4.6 *Une section s de la surjection $\pi_1^t(U) \to Gal(F)$ au-dessus de G est géométrique si et seulement si pour tout sous-groupe ouvert H de $\pi_1^t(U)$ contenant $s(G)$, le revêtement correspondant X_H de X a un point sur $\bar{F}^G$.*

Démonstration. L'implication non triviale résulte du fait qu'une limite projective d'ensembles finis non vides est non vide.

Appliquant la prop. 3.6 à la courbe X_H, on obtient le

Corollaire 4.7 *Les sections géométriques sont repérables parmi les morphismes $G \to \pi_1^t(U)$ scindant la surjection $\pi_1^t(U) \to Gal(F)$ au-dessus du sous-groupe ouvert G.*

Appelons deux sections géométriques $s_1 : G_1 \to \pi_1^t(U)$, $s_2 : G_2 \to \pi_1^t(U)$ *équivalentes* si leur image tombe dans le même sous-groupe de décomposition de $\pi_1^t(U)$.

Proposition 4.8 *Fixons une section géométrique $s : G \to \pi_1^t(U)$. Alors les sections géométriques équivalentes à s sont repérables.*

Démonstration. En effet, soit $s_1 : G \to \pi_1^t(U)$ une autre section géométrique. Par la démonstration de la prop. 4.5, s_1 est équivalente à s si et seulement si on peut trouver un sous-groupe ouvert H de $\pi_1^t(U)$ tel que les images de $s(G)$ et $s_1(G_1)$ soient les mêmes dans $\pi_1(X_{H'})$ pour tout sous-groupe $H' \subset H$ ouvert dans $\pi_1^t(U)$. D'après la proposition 3.5, cette dernière propriété est repérable.

Nous pouvons maintenant démontrer le résultat principal de ce chapitre.

Théorème 4.9 *Tout sous-groupe de décomposition dans $\pi_1^t(U)$ est engendré par les images d'une classe d'équivalence de sections géométriques. Par conséquent, les sous-groupes de décomposition sont repérables. De plus, on peut repérer si un sous-groupe de décomposition est au-dessus d'un point de U ou pas.*

Démonstration. Étant donné un sous-groupe de décomposition D, considérons la projection $p : D \to Gal(F)$. L'image G est un sous-groupe d'indice fini de $Gal(F) \cong \hat{\mathbf{Z}}$, donc libre de rang 1, et par conséquent la projection p admet une section $s : G \to D$. Cette section est unique si et seulement si D est au-dessus d'un point de U car dans ce cas D est lui-même isomorphe à $\hat{\mathbf{Z}}$. Sinon, D contient un sous-groupe d'inertie modéré non trivial I. Prenons un générateur topologique $g \in G$. Pour tout élément $i \in I$, il existe alors une section de p envoyant g sur $s(g)i$. Ainsi, les sections engendrent D. La repérabilité résulte de la proposition précédente.

5 Conclusion

Nous sommes maintenant suffisamment érudits pour compléter la démonstration du th. 1.3. Montrons d'abord l'énoncé de surjectivité, i.e. que tout isomorphisme $\sigma : \pi_1^t(U_1) \xrightarrow{\sim} \pi_1^t(U_2)$ provient d'un isomorphisme de schémas $U_1 \xrightarrow{\sim} U_2$.

Soit d'abord D_1 le groupe de décomposition d'un point fermé du "revêtement universel modéré" de U_1. Par la prop. 4.4, le cor. 4.7 ainsi que le th.

4.9, $\sigma(D_1)$ est le groupe de décomposition d'un unique point du revêtement universel modéré de U_2. On obtient ainsi une bijection entre les groupes de décomposition dans $\pi_1^t(U_1)$ et $\pi_1^t(U_2)$ et, toujours d'après le th. 4.9, entre les points fermés des U_i ainsi que de leurs compatifications lisses X_i.

Nous allons maintenant montrer que, tout comme chez Uchida, la connaissance des sous-groupes de décomposition et du Frobenius (cf. la prop. 3.4) permet de récupérer les groupes multiplicatifs des corps de fonctions via la théorie des corps de classes. En effet, la théorie locale enseigne qu'étant donné le complété K_P du corps de fonctions d'une F-courbe propre lisse en un point P, si nous prenons l'image réciproque du sous-groupe discret de $Gal(F)$ formé des puissances entières du Frobenius par la projection $Gal(K_P)^{ab} \to Gal(F)$, nous obtenons un sous-groupe isomorphe au groupe multiplicatif $K_P^\times$ (voir par exemple [15], chap. XIV, cor. 2 au th. 1). De plus, cet isomorphisme transforme la filtration par les groupes de ramification en la filtration sur les unités de K_P (*ibid.,* chap. XV, remarque après le th. 2). En particulier, le groupe des unités provient du sous-groupe d'inertie et l'"Einseinheitengruppe" (le groupe des unités congrus à 1) du sous-groupe d'inertie sauvage.

Retenant ce fait, prenons un point fermé P_1 de X_1 et un groupe de décomposition D_1 au-dessus de P_1. (Ceux-ci étant tous isomorphes, le choix est indifférent.) Si P_1 est dans U_1 (resp. dans $X_1 \setminus U_1$), l'image réciproque des puissances entières du Frobenius par la projection $D_1^{ab} \to Gal(F)$ est isomorphe par le paragraphe précédent à $(K_1)_{P_1}^\times / U_{P_1}$ (resp. $(K_1)_{P_1}^\times/(1+\mathbf{m}_{P_1})$), où U_{P_1} est le groupe des unités de $(K_1)_{P_1}$ et $\mathbf{m}_{P_1}$ son idéal de valuation. En faisant la somme directe des groupes ainsi obtenus pour P_1 variable, nous obtenons un "Strahlklassengruppe" correspondant au "module" défini par les points fermés de X_1 en dehors de U_1. Ce groupe s'envoie dans $\pi_1^t(U_1)^{ab}$ par l'application de réciprocité globale qui n'est autre que le produit des inverses des isomorphismes locaux discutés ci-dessus (voir [9] ou [17]). Le noyau est précisément le groupe multiplicatif du corps de fonctions K_1 de U_1 (cf. [14], chap. VI, th. 4 et prop. 24 ou encore [9], p. 415 pour l'énoncé analogue sur un corps de nombres).

L'isomorphisme σ traduit alors cette construction en la construction correspondante pour $\pi_1^t(U_2)$. Nous obtenons donc un isomorphisme $K_1^\times \xrightarrow{\sim} K_2^\times$ entre les groupes multiplicatifs des corps de fonctions. La dernière tâche sérieuse est de vérifier que cet isomorphisme s'étend en un isomorphisme *additif* entre K_1 et K_2. En effet, une fois que c'est vérifié, l'isomorphisme entre les corps de fonctions induit un isomorphisme entre les modèles propres et lisses X_1 et X_2 et nous récupérons enfin un isomorphisme entre les courbes U_1 et U_2 en enlevant les points à l'infini (qui sont repérables par ce qui précède).

L'argument par lequel Tamagawa établit l'additivité est également inspiré par ce que fait Uchida dans [18], mais il est beaucoup plus délicat. Nous devons nous contenter ici d'une esquisse, en renvoyant à son article [16] pour les détails. Tout d'abord, on peut appliquer la démarche précédente à des sous-groupes ouverts correspondants des $\pi_1^t(U_i)$, obtenant des isomorphismes entre les groupes multiplicatifs d'extensions finies des K_i. La fonctorialité de l'application de réciprocité globale assure que ces isomorphismes sont compatibles entre eux; a fortiori, un argument de passage à la limite implique l'existence d'un isomorphisme $\psi : (\overline{F}K_1)^\times \tilde{\to} (\overline{F}K_2)^\times$ entre les groupes multiplicatifs des corps de fonctions des courbes $\overline{U}_i = U_i \times \overline{F}$. Il suffit alors de montrer que ψ s'étend en un isomorphisme de corps $\overline{F}K_1 \tilde{\to} \overline{F}K_2$. Quitte à faire encore une extension finie de corps, l'hyperbolicité permet de supposer que chacune des courbes $\overline{U}_i$ admet au moins 3 points à l'infini; notons par abus de notation P_0, P_1, P_∞ un triplet correspondant sur les deux courbes. L'isomorphisme ψ induit un isomorphisme sur les sous-groupes formés des fonctions constantes inversibles; en effet, ce sont les sous-groupes divisibles maximaux des groupes $\overline{F}K_i^\times$. La première chose à montrer est que l'isomorphisme sur ces deux sous-groupes isomorphes à $\overline{F}^\times$ devient additive en rajoutant les fonctions 0.

Pour ce faire, Tamagawa montre d'abord par un argument de Riemann-Roch qu'il existe une fonction $x_1 \in \overline{F}K_1$ telle que pour son diviseur de pôles $(x_1)_\infty$ on ait $\dim \Gamma(\overline{X}_1, O_{\overline{X}_1}((x_1)_\infty)) = 2$ (il appelle une telle fonction *minimale*) et telle que son évaluation en les points P_0, P_1, P_∞ soit égale à $0, 1, \infty$ (dans l'ordre). Notons au passage que l'évaluation en le point i consiste à regarder d'abord l'image de x_1 dans le quotient $(\overline{F}K)^\times_{P_i}/U_{P_i} \cong \mathbf{Z}$ (où nous avons adopté des notations similaires à celles du début du chapitre), puis si c'est 0, à regarder son image dans $U_{P_i}/(1+\mathbf{m}_{P_i}) \cong \overline{F}(P_i)^\times$. Comme les P_i sont des points à l'infini, il résulte après passage à la limite des arguments du troisième paragraphe de ce chapitre que σ envoie les groupes $\overline{F}K^\times_{P_i}/U_{P_i}$ et $U_{P_i}/(1+\mathbf{m}_{P_i})$ isomorphiquement sur les sous-quotients correspondants de $\pi_1^t(\overline{U}_2)$. Par contre, on ne peut pas repérer le groupe $U_P/(1+\mathbf{m}_P)$ comme sous-quotient de $\pi_1^t(\overline{U}_1)$ si P est un point de $U_1(\overline{F})$; c'est la raison pour laquelle la démonstration de Tamagawa ne couvre pas le cas des courbes propres.

Revenant à notre fonction minimale x_1, le théorème de Riemann-Roch pour $\overline{X}_2$ (qui a le même genre que $\overline{X}_1$ d'après la prop. 3.4) implique que $x_2 = \psi(x_1)$ est une fonction minimale sur $\overline{X}_2$. De plus, par ce qu'on vient d'expliquer, elle a les mêmes évaluations en les points P_i que x_1. Prenons maintenant des fonctions constantes a_1, b_1 sur $\overline{X}_1$. La fonction $f_1 = a_1x_1 + b_1$

a le même diviseur de pôles sur $\overline{X}_1$ que x_1; il en est donc de même pour $f_2 = \psi(f_1)$ et x_2. Comme x_2 est minimale, il existe par définition des fonctions constantes a_2, b_2 sur $\overline{X}_2$ vérifiant $f_2 = a_2x_2 + b_2$. En évaluant f_2 en P_0 on obtient $b_2 = \psi(b_1)$; l'évaluation de f_2/x_2 en P_∞ donne $a_2 = \psi(a_1)$. Enfin, on a ou bien $0 \neq a_2 + b_2 = f_2(P_1) = \psi(f_1(P_1)) = \psi(a_1 + b_1)$, ou bien $f_1(P_1) = f_2(P_1) = 0$, d'où l'additivité de ψ sur les constantes. Le même type d'argument montre que l'extension de ψ par 0 induit un isomorphisme du sous-corps $\overline{F}(x)$ de $\overline{F}K_1$ sur le sous-corps $\overline{F}(\psi(x))$ de $\overline{F}K_2$ pour toute fonction minimale x sur $\overline{X}_1$. Tamagawa termine alors sa preuve en montrant que les fonctions minimales engendrent les corps $\overline{F}K_i$ au-dessus de $\overline{F}$ et les isomorphismes ci-dessus se recollent en une bijection additive $\overline{F}K_1 \xrightarrow{\sim} \overline{F}K_2$.

Enfin, l'énoncé d'injectivité du théorème 1.3 résulte également de la construction ci-dessus. En effet, un automorphisme intérieur de $\pi_1^t(U_2)$ ne fait que permuter les sous-groupes de décomposition au-dessus d'un point fermé donné de X_2. D'autre part, pour reconstituer X_2, le choix d'un tel sous-groupe était indifférent.

Bibliographie

[SGA1] A. Grothendieck, Revêtements étales et groupe fondamental, Springer LNM **224**, 1971.

[1] M. Artin, J. S. Milne, Duality in the flat cohomology of curves, *Inv. Math.* **35** (1976), 111–129.

[2] G. Faltings, Curves and their fundamental groups [following Grothendieck, Tamagawa and Mochizuki], *Séminaire Bourbaki*, année 1997/98, exposé 840.

[3] A. Grothendieck, Brief an G. Faltings (27/06/1983), in: L. Schneps and P. Lochak (eds.) *Geometric Galois Actions I*, Cambridge University Press, 1997, pp. 49–58.

[4] N. Katz, S. Lang, Finiteness theorems in geometric class field theory, *L'Enseign. Math.* **27** (1981), 285–319.

[5] J. S. Milne, *Étale cohomology*, Princeton University Press, 1981.

[6] S. Mochizuki, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, *J. Math. Sci. Univ. Tokyo*, **3** (1996), 571–627.

[7] J. Neukirch, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximalen auflösbaren Erweiterungen, *J. reine angew. Math.* **238** (1969), 135–147.

[8] ———, Über die absoluten Galoisgruppen algebraischer Zahlkörper, *Astérisque* **41–42** (1977), 67–79.

[9] ———, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[10] F. Pop, On Grothendieck's conjecture of birational anabelian geometry, preprint, 1996.

[11] ———, Glimpses of Grothendieck's anabelian geometry, in L. Schneps and P. Lochak (eds.) *Geometric Galois Actions I*, Cambridge University Press, 1997, pp. 113–126.

[12] F. K. Schmidt, Mehrfach perfekte Körper, *Math. Ann.* **108** (1933), 1–25.

[13] J.-P. Serre, *Cohomologie galoisienne* (5e éd.) Springer LNM **5**, 1994.

[14] ———, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[15] ———, *Corps locaux*, Hermann, Paris, 1962.

[16] A. Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), 135–194.

[17] J. Tate, Global class field theory, in J. W. S. Cassels and A. Fröhlich (eds.) *Algebraic Number Theory*, Academic Press, 1967, pp. 163–203.

[18] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.* **106** (1977), 589–598.

[19] V. Voevodsky, Représentations galoisiennes provenant de courbes hyperboliques (en russe), *Izv. Akad. Nauk SSSR* **55** (1991). Traduction anglaise: *Math. USSR Izvestiya* **39** (1992), 1281–1291.

Tamás Szamuely
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences,
PO Box 127,
H-1364 Budapest, Hungary
e-mail : szamuely@math-inst.hu