[21] N. Q. D. Thong, *Structure du groupe des similitudes*, Linear Algebra Appl. 12 (1975), 241–246.
[22] M. A. Tsfasman, *Arithmetic of singular Del Pezzo surfaces* (in Russian), Uspekhi Mat. Nauk 38, n° 6 (1983), 131–132.

Received on 13.1.1987
and in revised form on 3.10.1988 (1699)

ACTA ARITHMETICA
LIV (1990)

Sur les extensions totalement décomposées de certains corps de fonctions

par

JEAN CLAUDE DOUAI (Paris)

Soient X une courbe projective, lisse, géométriquement irréductible, définie sur un corps k complet pour une valuation discrète à corps résiduel fini k_0, K son corps des fonctions.

S. Saito et K. Kato ont défini dans [9] et [4] à partir du K_2 un groupe C_K (resp. $C_{m,K}$) (noté C_K^2 (resp. $C_{m,K}^2$) dans [4]) jouant le rôle de groupe de classes d'idèles (resp. de classes d'idèles pour la relation d'équivalence associée à un module m). Ils ont établi les suites exactes

$$0 \to (Q/Z)^r \to H^1(K, Q/Z) \to (C_K)^* \to 0, \tag{1}$$

$$0 \to (Q/Z)^r \to H^1(U_{\text{ét}}, Q/Z) \to (\varprojlim C_{m,K})^* \to 0 \tag{2}$$

où r désigne un entier lié à la réduction de X modulo l'idéal maximal de k, nul dans le cas de bonne réduction, U un ouvert non vide de X, m dans la limite projective parcourant les modules de X tels que $U \cap m$ = ensemble vide. Que deviennent ces résultats dans le cas où $k = k_0((t))$ avec k_0 algébriquement clos et non plus fini? L'objectif de ce papier est de montrer qu'il existe alors des suites exactes

$$0 \to (Q/Z)^{2g-\varepsilon} \to H^1(K, Q/Z) \to (C_K)^* \to 0, \tag{1$'$}$$

$$0 \to (Q/Z)^{2g-\varepsilon} \to H^1(U_{\text{ét}}, Q/Z) \to (\varprojlim C_{m,K})^* \to 0 \tag{2$'$}$$

du type précédent où cette fois C_K (resp. $C_{m,K}$) désigne le vrai groupe d'idèles de K (resp. des classes d'idèles pour la relation d'équivalence associé à un module m de X) mais qu'elles sont anti-analogues à (1) et (2) en ce sens que le rôle de l'entier r est joué par $2g-\varepsilon$ où g est le genre de X, ε l'invariant de Ogg associé à la réduction de X modulo t et est maximum précisément dans le cas de bonne réduction. Si $U = X$, l'exactitude de (2)′ (resp. (2)) traduit exactement le fait que les revêtements abéliens complétement décomposés de X correspondent biunivoquement aux revêtements de même nature de la courbe réduite $\mathfrak{X}_s$ où $\mathfrak{X}$ désigne un modèle régulier de X sur Spec $k_0[[t]]$ (resp. Spec O_k). Les résultats obtenus ici précisent et complétent ceux de [3].

Notations. Dans la suite, sauf mention expresse, nous désignerons par k_0 un corps aigébriquement clos, de caractéristique 0 (pour simplifier), $k = k_0((t))$ un corps de séries formelles en une variable, X une courbe algébrique, lisse, projective, irréductible, définie sur k, $K = k(X)$ son corps des fonctions.

1. Nous aurons besoin du résultat suivant qui a été établi pour un faisceau F quelconque fini de torsion dans [1] et qui étend au cas des courbes définies sur les corps quasi-finis du type $k_0((t))$ le théorème de dualité analogue pour les courbes définies sur les corps finis.

1.1. Théorème. *X étant muni de la topologie étale, soit μ_q le faisceau des racines $q^{\text{ièmes}}$ de l'unité (q entier quelconque $\geqslant 1$). Pour $i > 3$, les groupes $H^i(X, \mu_q)$ sont nuls; ils sont finis pour $0 \leqslant i \leqslant 3$, et il existe un accouplement*

$$H^i(X, \mu_q) \otimes H^{3-i}(X, \mu_q) \to Q/Z$$

qui met en dualité parfaite les groupes $H^i(X, \mu_q)$ et $H^{3-i}(X, \mu_q)$.

Remarquons que $\mu_q \simeq Z/qZ$.

1.2. En particulier, les groupes $H^1(X, \mu_q)$ et $H^2(X, \mu_q)$ sont des groupes finis en dualité parfaite. Il en résulte:

Corollaire. $H^2(X, \mu_q) \simeq H^1(X, Z/qZ)^* \simeq \pi_1(X)^{ab}/q \cdot \pi_1(X)^{ab}$.

Par un passage à la limite inductive, on en tire

$$H^2(X, Q/Z) \simeq \pi_1(X)^{ab} \otimes Q/Z.$$

1.3. Considérons le diagramme suivant où les lignes sont exactes

$$(*)\left\{\begin{tikzcd}[column sep=small]
(3) & K_1(k(X)) \arrow[r] \arrow[d] & \bigoplus\limits_{x \in X^1} Z \arrow[r] \arrow[d] & SK_0(X) \arrow[r] \arrow[d, dashed] & 0 \\
(4) & k(X)/(k(X))^q \arrow[r] \arrow[d, phantom, "\wr"] & \bigoplus\limits_{x \in X^1} Z/qZ \arrow[r] \arrow[d, phantom, "\wr"] & H^2(X, \mu_q) \arrow[r] & \mathrm{Br}(X)_q \\
& H^1(\mathrm{Spec}\, k(X), \mu_q) \arrow[r] & \bigoplus\limits_{x \in X^1} H^0(\mathrm{Spec}\, k(x), \mu_q) \arrow[ur] & &
\end{tikzcd}\right.$$

(X^1 = ensemble des sous-variétés de codimension 1 de X pour un schéma X quelconque).

La suite exacte (3) dans (*) correspond dans la situation k_0 algébriquement clos à la suite exacte

$$\begin{tikzcd}
K_2(k(X)) \arrow[r] & \bigoplus\limits_{x \in X^1} K_1(x) \arrow[r] \arrow[d, equal] & SK_1(X) \arrow[r] & 0 \\
& \bigoplus\limits_{x \in X^1} K_1(k(x)) & &
\end{tikzcd}$$

utilisée dans le diagramme de la page 247 de [5] pour le cas k_0 fini.

Le morphisme vertical de droite en pointillé dans le diagramme (*) se factorise par

$$(**)\left\{\begin{tikzcd}
& & SK_0(X) \simeq \mathrm{Pic}(X) \arrow[dl] \arrow[d] & & & \\
(5) & 0 \arrow[r] & \mathrm{Pic}(X)/q\,\mathrm{Pic}(X) \arrow[r] & H^2(X, \mu_q) \arrow[r] \arrow[d, phantom, "\wr"] & \mathrm{Br}(X)_q \arrow[r] & 0 \\
& & & \pi_1(X)^{ab}/q \cdot \pi_1(X)^{ab} & &
\end{tikzcd}\right.$$

1.4. Proposition. *Le conoyau de l'application $\mathrm{Pic}(X) \to H^2(X, \mu_q)$ est isomorphe à $(Z/qZ)^{2g-\varepsilon}$.*

En effet, ramenons-nous au cas q premier; par le corollaire 2.3 de [1], on sait qu'il existe une dualité entre $\mathrm{Br}(X)_q$ et le sous-groupe $(J_{k,q})_{\mathrm{div}}$ des éléments de $J_{k,q}$ qui sont divisibles (i.e. qui appartiennent à $mJ_{k,q}$ pour tout entier $m \geqslant 1$ (cf. [7], p. 194)) où J désigne la Jacobienne de X, $J_{k,q}$ les q-points rationnels sur k de J. Or par [7], p. 194, $(J_{k,q})^*_{\mathrm{div}} \simeq (Z/qZ)^{2g-\varepsilon}$ où ε est l'entier de Ogg associé à la réduction de $J \bmod (t)$ (l'isomorphisme entre $\mathrm{Br}(X)_q$ et $(Z/qZ)^{2g-\varepsilon}$ est aussi démontré dans [2]).

1.5. Corollaire. *La suite*

(6) $$0 \to \mathrm{Pic}(X) \otimes Q/Z \to \pi_1(X)^{ab} \otimes Q/Z \to (Q/Z)^{2g-\varepsilon} \to 0$$

est exacte.

1.6. Remarque. $\mathrm{Pic}(X)$ est extension de J_k par Z. Utilisant les propriétés d'un modèle minimal de Néron de J sur $\mathrm{Spec}\, k_0[[t]]$, on voit que J_k contient un sous-groupe divisible d'indice fini. Il en résulte que $\mathrm{Pic}(X) \otimes Q/Z$ est en fait isomorphe à Q/Z et $\widehat{\pi_1(X)}^{ab}$ à $(\hat{Z})^{2g+1-\varepsilon}$ (le symbole $\wedge$ désigne ici le complété). Si l'on définit $\widehat{\pi_1^0(X)}^{ab}$ à être le noyau de $\widehat{\pi_1(X)}^{ab} \to \mathrm{Gal}(\bar{k}/k) \simeq \hat{Z}$, alors $\widehat{\pi_1^0(X)}^{ab} \simeq (\hat{Z})^{2g-\varepsilon}$.

2. Extensions complètement décomposées. Soit $\mathfrak{X}$ un modèle régulier de X sur $\mathrm{Spec}\, k_0[[t]]$, i.e. un schéma de dimension 2 régulier muni d'un morphisme propre $\mathfrak{X} \to \mathrm{Spec}\, k_0[[t]]$ plat tel que $\mathfrak{X} \underset{\mathrm{Spec}\, k_0[[t]]}{\otimes} k \simeq X$. Désignons par $\mathfrak{X}_s$ la fibre spéciale de $\mathfrak{X}$ et par $\pi_1(X)^{\mathrm{c.s.}}$ le groupe quotient de $\pi_1(X)^{ab}$ qui classifie les revêtements (abéliens) complètement décomposés de X (cf. la définition 2.1, chap. II de [9]). L'exactitude de (6) traduit la propriété arithmétique suivante:

2.1. Proposition. *Il existe un isomorphisme $\pi_1(X)^{\mathrm{c.s.}} \simeq \pi_1(\mathfrak{X}_s)^{\mathrm{c.s.}}$.*

Cette proposition correspond dans notre cas à la proposition 2.2, chap. II de [9].

On sait qu'il existe un homomorphisme surjectif de $\pi_1(X)^{\mathrm{c.s.}}$ vers $\pi_1(\mathfrak{X}_s)^{\mathrm{c.s.}}$. Nous allons montrer qu'il y a une suite exacte

(6)* $$0 \to H^1(\mathfrak{X}_s, Q/Z) \to H^1(X, Q/Z) \to \mathrm{Hom}(\mathrm{Pic}(X), Q/Z) \to 0.$$

(6)* sera la suite duale de (6) et l'analogue dans la situation k_0 algébriquement clos de la suite exacte

$$0 \to E_{\mathfrak{X}_s} \to H^1(X, Q/Z) \to \mathrm{Hom}(SK_1(X), Q/Z)$$

considéré dans la proposition 2, § 2, p. 246 de [5] pour le cas k_0 fini.

Dans (6)*, l'inclusion de $H^1(\mathfrak{X}_s, Q/Z)$ dans $H^1(X, Q/Z)$ est induite par l'homomorphisme surjectif $\pi_1(X)^{ab} \to \pi_1(\mathfrak{X}_s)^{ab}$ et le 3ième homomorphisme de (6)* par l'homomorphisme $0 \to \mathrm{Pic}(X) \otimes Q/Z \to H^2(X, Q/Z)$ déduit des suites exactes de Kummer (5). Pour établir l'exactitude de (6)*, nous devons montrer que tout élément χ de $H^1(X, Q/Z)$ annulant $\mathrm{Pic}(X)$ vient d'un élément $\tilde{\chi}$ de $H^1(\mathfrak{X}_s, Q/Z)$. Pour chaque point fermé x de $\mathfrak{X}_s$, χ induit un élément χ_x de $H^1(K_x, Q/Z)$ où K_x est le corps des fractions de $\hat{\mathcal{O}}_{\mathfrak{X},x}$ (complété de l'anneau local $\mathcal{O}_{\mathfrak{X},x}$). Pour chaque $\mathfrak{p} \in P = \mathrm{Spec}(\mathcal{O}_{\mathfrak{X},x})^1$, soit $K_{x,\mathfrak{p}}$ la complétion de K_x pour la valuation $\mathfrak{p}$-adique. Il existe une partie finie S de P telle que tous les idéaux de $P-S$ proviennent de X par l'opération $\mathfrak{p} \to x$, $x \in \{\bar{\mathfrak{p}}\}$, $\mathfrak{p} \in X^1$. Puisque χ annule $\mathrm{Pic}(X)$, χ annule le groupe des classes d'idèles de K et, pour tout $\mathfrak{p} \in X^1$, le groupe $K_\mathfrak{p}^*$ (cf. par exemple pour une situation analogue la proposition 6.6, chap. IV de [6]); donc χ_x annule le sous-groupe $\prod_{\mathfrak{p} \in P-S} K_{x,\mathfrak{p}}^*$ du groupe des idèles de K_x, le symbole $\prod$ indiquant qu'il s'agit d'un produit restreint par rapport aux sous-groupes $U_{x,\mathfrak{p}}$ des unités de $K_{x,\mathfrak{p}}$. D'autre part χ_x annule le sous-groupe des idèles principaux de K_x; or, les idèles principaux sont denses dans $\prod_{\mathfrak{p} \in S} K_{x,\mathfrak{p}}^*$, donc χ_x annule le groupe des idèles de K_x. Par la loi de réciprocité appliquée au corps local de dimension 1 à corps résiduel quasi-fini $K_{x,\mathfrak{p}}$, on sait que $K_{x,\mathfrak{p}}^*$ s'identifie à un sous-groupe dense de $\mathrm{Gal}(K_{x,\mathfrak{p}}^{ab}/K_{x,\mathfrak{p}})$. Pour tout $\mathfrak{p} \in P$, l'image $\chi_{x,\mathfrak{p}}$ de χ_x dans $H^1(K_{x,\mathfrak{p}}, Q/Z)$ est donc nulle. Ainsi χ_x est non ramifié en un $\mathfrak{p}$ quelconque de P et vient d'un élément de $H^1(\hat{\mathcal{O}}_{\mathfrak{X},x}, Q/Z) = H^1(x, Q/Z) = 0$, d'où $\chi_x = 0$. χ est donc non ramifié en un point fermé quelconque de $\mathfrak{X}$ et vient d'un élément $\tilde{\chi}$ de $H^1(\mathfrak{X}, Q/Z) \simeq H^1(\mathfrak{X}_s, Q/Z)$.

2.2. Corollaire. *La suite exacte (6)* s'écrit*

$$0 \to (Q/Z)^{2g-\varepsilon} \to H^1(X, Q/Z) \to \mathrm{Hom}(\mathrm{Pic}(X), Q/Z) \to 0$$

et si $U = X$, elle n'est autre que la suite exacte (2)' de l'introduction.

2.3. Corollaire. *Rang de $\pi_1(X)^{c.s.}$ = Rang de $\pi_1^0(X)^{ab} = 2g-\varepsilon$.*

2.4. Corollaire. *Désignons par $Ш^2(\mu_q)$ le noyau de l'application*

$$H^2(K, \mu_q) \to \prod_{x \in X^1} H^2(K_x, \mu_q).$$

Alors le rang du Z/qZ-module $Ш^2(\mu_q)$ est indépendant de q et égal à $2g-\varepsilon$, i.e. au rang de $\pi_1(X)^{c.s.}$.

Nous avons vu au cours de la démonstration de la proposition 1.4 que $\mathrm{Br}(X)_q \simeq (Z/qZ)^{2g-\varepsilon}$.

2.5. Dans le cas où le corps résiduel k_0 (supposé contenir les racines q-ièmes de l'unité) est fini et non plus algébriquement clos, il résulte du théorème 4 de [4] que $(Z/qZ)^r$ (où r est l'entier qui apparait dans les suites exactes (1) et (2) de l'introduction) est le noyau $Ш^3(\mu_q)$ de l'application

$$H^3(K, \mu_q) \to \prod_{\mathfrak{p} \in X^1} H^3(K, \mu_q).$$

Le rang du (Z/qZ)-module $Ш^3(\mu_q)$ est donc égal au rang du groupe $\pi_1(X)^{c.s.}$ (cf. aussi le théorème 2.4 de [9]). L'analogie avec le corollaire 2.4 est donc totale. Nous montrerons dans un autre article que cette situation est tout à fait générale: si X est définie sur un corps local de dimension N au sens de Parshin (voir par exemple [8] pour la définition d'un tel corps), elle provient d'une dualité entre $H^{N+2}(X, \mu_q)$ et $H^1(X, Z/qZ)$ généralisant le théorème 1.1 et conduit à un théorème du type de Tate–Poitou généralisant celui de [1].

2.6. Proposition. *Nous avons les suites exactes*

$$(7) \qquad 0 \to (Q/Z)^{2g-\varepsilon} \to H^1(U_{\text{ét}}, Q/Z) \to (\varinjlim C_{m,K})^* \to 0,$$

$$(8) \qquad 0 \to (Q/Z)^{2g-\varepsilon} \to H^1(K, Q/Z) \to (C_K)^* \to 0$$

où C_K désigne le groupe des classes d'idèles de K, $C_{m,K}$ le groupe des classes de diviseurs de X pour la relation de m-équivalence, m parcourant les modules de X tels que $U \cap (\mathrm{Supp}(m))$ = vide.

(7) et (8) s'obtiennent de manière standard compte tenu du corollaire 2.2.

Bibliographie

[1] J. C. Douai, *Le théorème de Tate–Poitou pour les corps de fonctions des courbes définies sur les corps de séries formelles en une variable sur un corps algébriquement clos*, Communications in Algebra, présenté par S. Bloch, 15 (11) (1987), 2379–2390.

[2] — *Cohomologie des schémas en groupes sur les courbes définies sur les corps quasi-finis et loi de réciprocité*, J. Algebra 103 (1) (1986), 273–284.

[3] J. C. Douai et C. Touibi, *Courbes définies sur les corps de séries formelles et loi de réciprocité*, Acta Arith. 42 (1982), 101–106 et l'errata, ibid. 46 (1986), 197.

[4] K. Kato, *Class field theory and algebraic K-theory*, Lecture Notes in Math., 1016, 109–126, Springer-Verlag, 1983.

[5] K. Kato et S. Saito, *Unramified class field theory of arithmetical surfaces*, Ann. of Math. 118 (1983), 241–275.

[6] J. Neukirch, *Class field theory*, Grundlehren Math. Wiss. 280, Springer-Verlag, 1986.

[7] A. P. Ogg, *Cohomology of abelian varieties over function fields*, Ann. of Math. 76 (2) (1962), 185–212.

[8] A. N. Parshin, *Local class field theory*, Proc. Steklov Inst. Math. 165 (1985), Issue 3, 157–185; Translation from Trudy Mat. Inst. Steklov. 165 (1984), 143–170 (Russian).
[9] S. Saito, *Class field theory for curves over local fields*, J. Number Theory 21 (1985), 44–80.

INSTITUT HENRI POINCARÉ
PROBLÈMES DIOPHANTIENS
11, rue P. et M. Curie
75231 Paris Cedex 05, France

Reçu le 21.5.1987
et dans la forme modifiée le 23.9.1988 (1724)

ACTA ARITHMETICA
LIV (1990)

Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers

par

JEAN COUGNARD (Besançon)

1. Introduction. Etant donné un corps de nombres K, on note Z_k son anneau des entiers; si L/K est une extension algébrique de degré fini de corps de nombres, on dit que Z_L est Z_K-monogène s'il existe θ tel que $Z_L = Z_K[\theta]$.

Si $K = Q$ et L/Q cyclique de degré premier $l \geqslant 5$, M.-N. Gras a montré [9] qu'une condition nécessaire de monogénéité est que L soit un corps de rayon. On peut voir à travers les résultats de [1] que ce lien entre monogénéité et corps de rayons ne se limite pas à $k = Q$. Des travaux récents ([2], [4], [6], [7]) montrent que les conditions nécessaires sont aussi parfois suffisantes. Dans le même ordre d'idées on se propose de démontrer:

THÉORÈME 1.1. *Si k est un corps quadratique imaginaire de discriminant $d_k < -4$, $\mathfrak{f}$ un idéal entier impair de Z_k, $k^{(\mathfrak{f})}$ (resp. $k^{(2)}$) le corps de classes de k de rayon $\mathfrak{f}$ (resp. 2) alors l'anneau des entiers $k^{(\mathfrak{f})}k^{(2)}$ est monogène sur celui de $k^{(2)}$.*

En particulier, si 2 est décomposé dans k/Q, on retrouve le résultat de [4].

Lorsque $k = Q(\sqrt{-d})$ avec $d \equiv 2 \bmod 4$ on peut améliorer le théorème 1.1 en démontrant qu'alors l'anneau des entiers de $k^{(\mathfrak{f})}$ est monogène sur celui du corps de classes de Hilbert H_k de k (cf. paragraphe 12).

La méthode utilisée suit le canevas établi dans [3], le paramétrage de la courbe elliptique C/Z_k conduit au modèle de Legendre. Les résultats dépendent essentiellement des propriétés de divisibilité de la fonction de Legendre pour certains entiers quadratiques imaginaires, et des congruences satisfaites par les coordonnées des points de division d'ordre impair aux places de mauvaise réduction.

La méthode est effective car nous donnons une formule de récurrence qui permet de calculer des polynômes annulés par la première coordonnée des points de n-division (celle qui permet de construire l'élément θ tel que $Z_{k^{(2)}k^{(\mathfrak{f})}} = Z_{k^{(2)}}[\theta]$). Pour être tout à fait complet il aurait fallu prolonger ces formules à tous les points de Z_k premiers à 2.

Des résultats analogues à ceux démontrés ici viennent d'être annoncés par M. Taylor et Ph. Cassou-Noguès [5].