S

50376
1999
127

THÈSE

présentée à

L'UNIVERSITÉ LILLE 1

par **Bounab SADI**

pour obtenir le grade de **DOCTEUR**

SPÉCIALITÉ : MATHÉMATIQUES

Préparée sous la direction de **M. Pierre DÈBES**

DESCENTE EFFECTIVE DU CORPS DE DÉFINITION DES REVÊTEMENTS

soutenue le 7 mai 1999 devant le jury formé de :

M. J-M COUVEIGNES, Professeur, Univ. de Toulouse, [rapporteur]
M. P. DÈBES, Professeur, USTL, [Directeur de thèse]
M. J-C DOUAI, Professeur, USTL, [Président de Jury]
M. M. EMSALEM, Professeur, USTL
M. U. ZANNIER, Professeur, Univ. de Venise (Italie), [rapporteur]

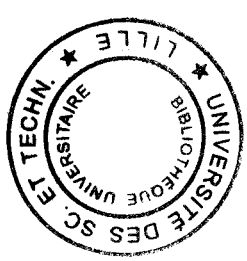
SCD LILLE 1
D 030 255985 8

50376.
1999.
127

Je voudrais remercier toutes les personnes qui m'ont accompagnées tout au long de ce travail de recherche et dont les encouragements répétés m'ont permis d'aboutir. Mes remerciements vont tout d'abord à Pierre Dèbes, mon directeur de thèse, dont les conseils et avis éclairés ont été pour moi très précieux. Je ne voudrais pas oublier de mentionner ici, mes amis et mes parents plus particulièrement qui sont témoins de ce travail aujourd'hui.

Je remercie également Michel Emsalem et Jean-Claude Douai qui ont bien voulu relire le texte, me faire part de leurs suggestions et d'avoir accepter de faire partie du jury. Je suis très touché que Umberto Zannier et Jean-Marc Couveignes aient accepté d'être rapporteurs. Je regrette que les délais trop court ne permettent pas à Jean-Marc Couveignes d être présent à la soutenance.

Je n'oublie pas les différents professeurs de mathématiques qui m'ont fortement influencés dans le choix du domaine de recherche dans lequel je travaille aujourd'hui.



Résumé

Le thème général de ce travail est la descente du corps de définition des revêtements algébriques. Dans ce contexte, il est naturel d'introduire le corps des modules d'un revêtement. Ce n'est pas toujours un corps de définition mais si c'en est un, c'est le plus petit possible. Notre travail porte plus spécifiquement sur l'obstruction à ce que le corps des modules soit un corps de définition. Dans certaines circonstances, on sait qu'il n'y a pas d'obstruction. Notre but est de préciser les énoncés de descente connus en explicitant un modèle du revêtement en question qui soit défini sur son corps des modules. Ainsi un théorème de Coombes-Harbarter montre qu'un revêtement galoisien de $\mathbf{P}_1$ est défini sur son corps des modules. Grâce à une nouvelle approche qui utilise le lemme de Dedekind, nous en donnons une forme plus précise en le sens ci-dessous: notre méthode permet de construire effectivement un modèle sur le corps des modules ; par exemple, nous pouvons donner une borne pour le degré et la hauteur des équations définissant ce modèle. Nous obtenons des résultats similaires dans le cas général de revêtements non nécessairement galoisiens, supposés définis sur leur corps des modules. Ces résultats sont cependant un peu moins précis que dans le cas galoisien.

Mots clés : revêtements galoisiens, corps de fonctions, corps de définition, corps des modules, descente.

1991 mathematics subject classification. Primary. 14G05; Secondary 14H30, 12F05.

Abstract

The general theme of this work is the descent of fields of definition of algebraic covers. On this context, it is natural to introduce the field of moduli of a cover. In general, it is not a field of definition but if it is, it is the smallest possible. Our work is more specifically devoted to the obstruction to the field of moduli being a field of definition. Under some circumstances, there is no obstruction. Our goal is to deepen the descent results already known by producing an explicit model of the cover that is difined over its field of moduli. A theorem due to Coombes and Harbater states that a Galois cover of $\mathbf{P}_1$ is difined over its field of moduli. Thanks to a new approach which uses Dedekind's lemma, we give a more precise: our method allows us to build effectively a model over the field of moduli. We can, for example, give a bound for the degree and the height of the equations defining that model. We obtain similar results in the general case of not necessarily Galois covers, which are supposed to be defined over their field of moduli. However, those results are slightly precise than in the Galois case.

Keywords: Galois covers, functions fields, fields of definition, filed of moduli, descent.

1991 mathematics subject classification. Primary. 14G05; Secondary 14H30, 12F05.

Table des matières

1 La théorie de la descente du corps de définition **8**
1.1 Corps de définition et corps des modules 8
1.1.1 Données du problème 8
1.1.2 La suite exacte de départ 9
1.1.3 Corps des modules 10
1.2 Descente de Weil 12
1.2.1 Condition de cocycle de Weil 12
1.2.2 Théorème de descente 13
1.3 Position du problème 15

2 Descente du corps de définition des revêtements galoisiens **17**
2.1 Enoncés 18
2.2 Une estimation plus intrinsèque de $\deg(P_k)$ 20
2.3 Preuve du théorème 23
2.4 Preuve du corollaire 25
2.4.1 Détermination de a 25
2.4.2 Calcul de la hauteur des éléments a et y_a . . . 26
2.5 Application 31
2.5.1 Le principe global-local 31
2.5.2 Remarque 32
2.5.3 Calcul de la borne 32

3 Descente dans le cas général **34**
3.1 Descente dans le cas fini 35
3.2 Cas général 37

Le contexte de cette thèse est celui du problème inverse de Galois. Nous énoncerons d'abord ce problème sur $\mathbf{Q}$:

Est-ce que tout groupe fini G est le groupe de Galois d'une extension $E/\mathbf{Q}$?

Le corps $\mathbf{Q}$ étant hilbertien, il suffit de résoudre la forme régulière du problème inverse de Galois sur $\mathbf{Q}$:

Est-ce que tout groupe fini G est groupe de Galois d'une extension régulière $E/\mathbf{Q}(T)$? ("régulière" signifie que $E \cap \overline{\mathbf{Q}} = \mathbf{Q}$)

De nombreux groupes finis sont réalisés sur $\mathbf{Q}$, par exemple, les groupes abéliens finis, le groupe symétrique, de nombreux groupes simples ([Mat],[MatMa]), en particulier 25 des 26 groupes sporadiques (il manque le groupe de Mathieu M_{23}). Mais on ne sait pas si tous les groupes finis sont réalisables sur $\mathbf{Q}$. Par contre à l'aide d'arguments de nature topologique on sait montrer que tout groupe fini est le groupe de Galois d'une extension de $\mathbf{C}(T)$. La géométrie algébrique permet ensuite de prouver que tout groupe fini est le groupe de Galois d'une extension de $\overline{\mathbf{Q}}(T)$ ([Se; Ch.6]). Il s'agit donc après d'un problème de descente de $\overline{\mathbf{Q}}(T)$ à $\mathbf{Q}(T)$. De façon générale, on peut énoncer la forme régulière du problème inverse de Galois sur un corps quelconque:

Est-ce que tout groupe fini est le groupe de Galois d'une extension régulière $E/k(T)$? (i.e., $E \cap \overline{k} = k$).

Actuellement aucun contre-exemple n'est connu. Le problème régulier inverse de Galois est résolu sur tous les corps k algébriquement clos. Et du fait de la condition de régularité, il suffit de le résoudre sur les corps premiers et donc en caractéristique 0 sur $\mathbf{Q}$. En fait le problème régulier est résolu sur des corps suffisamment gros, les corps "amples" par exemple ([Po], [DeDes]).

On peut traduire le problème de façon géométrique, il est équivalent à trouver un G-revêtement $f : X \to \mathbf{P}_1$ défini sur k dont le groupe d'automorphismes soit le groupe G que l'on veut réaliser. Nous appelons ici G-revêtement la donnée d'un revêtement galoisien avec ses automorphismes. Pour un revêtement non nécessai-

rement galoisien et donné sans ses automorphismes, nous emploierons l'expression "revêtement pur". Pour des énoncés valables à la fois pour des revêtements purs et des G-revêtements, nous dirons (G)-revêtements. De façon générale le problème consiste à étudier le problème de la descente du corps de définition des $(G$-$)$ revêtements dont la base est $\mathbf{P}_1$ ou plus généralement une variété B définie sur un corps k de caractéristique 0. Pour cela on étudie l'action de $G_k = \mathrm{Gal}(\overline{k}/k)$ sur les $(G$-$)$revêtements définis sur $\overline{k}$. Si f est un $(G$-$)$ revêtement défini sur $\overline{k}$ alors on définit son corps des modules comme le sous corps de $\overline{k}$ fixé par le groupe

$$\{\tau \in \mathrm{Gal}(\overline{k}/k) | f^\tau \simeq f \text{ sur } \overline{k}\}$$

(où f^τ est le $(G$-$)$revêtement f tordu par l'action de τ). On peut justifier la terminologie corps des "modules" de la façon suivante : le revêtement f correspond à un point sur un certain espace des modules; sous des hypothèses convenables, le corps des modules est égal au corps de rationalité de ce point. Une question centrale du problème est alors:

Le corps des modules d'un $(G$-$)$revêtement est-il un corps de définition ?

La réponse est non en général ([CouGr], [Cou] pour les revêtements purs et [CoHa] pour les G-revêtements). Le corps des modules est un corps contenu dans tous les corps de définition contenant k; donc si c'est un corps de définition alors c'est le plus petit contenant k. Il existe de nombreux cas où le corps des modules est un corps de définition. Ainsi le corps des modules est un corps de définition du $(G$-$)$revêtement dans les deux cas extrêmes suivants ([DeDo1]):

- Celui où l'ordre du groupe d'automorphismes est maximal. Dans la situation des revêtements purs, cela correspond au cas des revêtements galoisiens. Ce résultat sur les revêtements galoisiens est dû à Coombes et Harbater ([CoHa]); c'est l'un des thèmes principaux de cette thèse (cf Ch.2). Dans celle des G-revêtements, le groupe d'automorphismes est le centre du groupe de Galois G du revêtement en question. Ce premier cas extrême correspond donc au cas des G-revêtements de groupe abélien.

- Celui où l'ordre du groupe est minimal. Pour un revêtement pur cela signifie qu'il n'a pas d'automorphisme non trivial et pour un G-revêtement que le centre $Z(G)$ de son groupe de Galois est trivial.

Il existe aussi une mesure cohomologique de l'obstruction à ce que le corps des modules soit un corps de définition: il est démontré en général dans [DeDo1] que l'obstruction vit dans $H^2(k, Z(G))$, le second groupe de cohomologie du corps des modules k à valeur dans le centre $Z(G)$ du groupe G.

L'obstruction à ce que le corps des modules soit un corps de définition est le thème principal de cette thèse. Plus précisement, le problème que nous allons considérer sera de donner une description explicite et effective d'un k-modèle lorsque la descente sur le corps des modules k est possible; nous appelons k-modèle un revêtement défini sur k et isomorphe sur $\overline{k}$ au revêtement de départ. Pour cela nous utiliserons le langage des extensions de corps des fonctions qui est plus adapté à ce type de questions. De plus ce point de vue nous permettra de simplifier le critère de descente de Weil. Notre résultat principal concerne le théorème de Coombes-Harbater. Nous en donnerons une nouvelle approche basée uniquement sur le lemme de Dedekind. Cette approche, en plus de prouver qu'un revêtement galoisien est défini sur son corps des modules k, fournit également un k-modèle explicite du revêtement. Notre approche s'applique également à la situation des revêtements quelconques et donne des résultats plus explicites que les résultats connus jusque là. Nous terminons cette introduction par une description plus détaillée des différents chapitres où nous expliquons ce que nous entendons par résultats "explicites" et "effectifs".

Dans le Chapitre 1 nous exposerons le problème de la descente dans le langage des extensions de corps en travaillant sur les corps de fonctions plutôt que sur les variétés correspondantes. Cela permettra notamment de simplifier le critère de descente de Weil ([We]) en l'existence d'une section pour une certaine suite exacte. Ce point de vue sur le problème avait été déjà pris dans une certaine mesure dans le contexte des revêtements galoisiens par E. Dew ([Dew]).

Dans le Chapitre 2, nous étudierons le cas des revêtements galoisiens. K. Coombes et D. Harbater ont montré qu'un revêtement galoisien $f : X \to \mathbf{P_1}$ défini sur $\overline{k}$ de corps des modules k est nécessairement défini sur son corps des modules. En fait leur preuve montre un résultat plus précis:

Pour tout $t_o \in \mathbf{P}_1$ non ramifié le revêtement galoisien $f : X \to \mathbf{P_1}$ a un modèle $f_k : X \to \mathbf{P}_1$ défini sur k tel que la fibre au dessus de t_o possède un point k-rationnel.

En termes de corps des fonctions nous verrons que cela est équivalent à l'existence d' une extension $E_k/k(T)$ satisfaisant

$$\begin{cases} E_k/k \text{ est régulière} \\ E_k\overline{k} = \overline{k}(X) \\ E_k \subset k((T - t_o)) \end{cases}$$

Nous donnerons une méthode qui permettra de construire un élément primitif d'une telle extension E_k. De plus dans le cas des corps de nombres cette méthode sera effective dans le sens où on pourra déterminer des bornes pour le degré et la hauteur du polynôme minimal d'un élément primitif engendrant E_k.

Nous donnerons ensuite une application à un problème de nature Locale-Globale. Si $f : X \to \mathbf{P}_1$ est un Grevêtement défini sur $\overline{\mathbf{Q}}$, on a le résultat suivant dû à P. Dèbes ([De1]): $\mathbf{Q}$ est le corps des modules de f si et seulement si f est défini sur tous les complétés $\mathbf{Q}_p$ sauf pour un nombre fini de premier p. On donnera une borne de ces nombres premiers exceptionnels. Ces résultats ont été récemment améliorés par P.Dèbes et D.Harbater qui ont décrit précisément quels sont les premiers éventuellement exceptionnels ([DeHa]). Ce sont les diviseurs de l'ordre du groupe d'automorphismes du revêtement et les nombres premiers p pour lesquels deux points de ramifications deviennent égaux modulo p. Notre résultat est moins précis qualitativement mais fournit un modèle explicite défini sur tout $\mathbf{Q}_p$ sauf un nombre fini.

Dans le chapitre 3 nous nous efforcerons de rendre explicite la descente dans le cas où le revêtement n'est pas nécessairement galoisien. Etant donné un revêtement défini sur son corps des modules k, nous donnerons une méthode générale pour déterminer un élé-

ment primitif d'un k-modèle. La différence avec le cas galoisien est que l'on devra se donner a priori une section de la suite exacte du chapitre 1.

Chapitre 1

La théorie de la descente du corps de définition

L'objet de ce chapitre est de définir les notions de corps de définition, de corps des modules, de poser le problème de la descente du corps de définition, de revoir le critère de descente de Weil ([We]) et de préciser les questions des chapitres suivants. Ces notions ont été beaucoup étudiées dans le contexte de variétés algébriques et de revêtements d'une variété B ([CoHa], [Cou], [CouGr],[DeDo1], [DeDo2], [DeEm], [Dew], [Fr], [Sh], [We], [Wol]). Nous considérons ici le cas des revêtements, mais avec un point de vue légèrement différent. Dans les chapitres suivants, notre but sera de donner des résultats de descente qui soient effectifs, c'est-à-dire, qui, en plus d'un corps de définition, donnent une description aussi précise que possible d'un modèle défini sur ce corps de définition. Dans ce but, nous préférons voir un revêtement comme une extension finie de corps de fonctions. Pour certaines applications, nous prendrons aussi $B = \mathbf{P}_1$. Mais nous n'en aurons pas besoin dans ce premier chapitre.

1.1 Corps de définition et corps des modules

1.1.1 Données du problème

Plus précisément on se donne un corps k de caractéristique 0 et une variété B projective, lisse, absolument irréductible et définie sur k.

Le corps des fonctions $k(B)$ est alors une extension régulière sur k, i.e., $\overline{k} \cap k(B) = k$. On sait alors qu'étant donné une extension F/k, on a une équivalence de catégories entre:

- la catégorie des revêtements $f : X \to B$ définis sur F où X est une variété normale irréductible définie sur F, et

- la catégorie des extensions algébriques $E/F(B)$ de degré fini du corps de fonction $F(B)$.

Le foncteur réalisant cette équivalence est le foncteur "corps des fonctions". On pose alors le problème de la descente en ces termes:

Problème:
On se fixe une extension galoisienne F/k et on se donne une extension finie $E/F(B)$ du corps des fonctions $F(B)$. Existe-t-il une extension de $E_k/k(B)$ régulière sur k (i.e. $E_k \cap \overline{k} = k$) tel que $E = E_k F$? On dit alors que E_k est un k-modèle de E et que k est un corps de définition de l'extension $E/F(B)$; c'est aussi un corps de définition du revêtement associé par l'équivalence de catégories ci-dessus.

Le cas où $F = \overline{k}$ est le cas le plus classique. On l'appelle le cas absolu; le cas plus général où F n'est pas nécessairement algébriquement clos est appelé le cas relatif.

Le chapitre 1 est une présentation de la théorie de la descente de Weil en termes de corps de fonctions. Il s'agit d'une différence de langage qui n'a rien d'essentiel. Cela permet cependant de simplifier quelques points: notamment la condition de cocycle de Weil se transforme en l'existence d'une section à une certaine suite exacte. Le langage plus géométrique des revêtements a lui l'avantage d'être plus intuitif. Nous nous efforcerons de garder le lien avec la présentation géométrique habituelle.

1.1.2 La suite exacte de départ

L'extension $E/F(B)$ donne lieu à la suite exacte:

$$1 \to \mathrm{Aut}(E/F(B)) \to \mathrm{Aut}(E/k(B)) \to G(F(B)/k(B))$$

où $\mathrm{Aut}(E/F(B))$, $\mathrm{Aut}(E/k(B))$ et $G(F/k)$ désignent respectivement les groupes des $F(B)$-automorphismes de E, des $k(B)$-automorphismes de E et le groupe de Galois de F sur k.

En effet il est clair $\mathrm{Aut}(E/F(B)) \subset \mathrm{Aut}(E/k(B))$, la seconde flèche $\mathrm{Aut}(E/k(B)) \to G(F(B)/k(B))$ n'est autre que la restriction à $F(B)$.

$$\begin{array}{ccc} F & \to & F(B) \\ \uparrow & & \uparrow \\ k & \to & k(B) \end{array}$$

On peut remarquer que $G(F(B)/k(B)) \simeq G(F/k)$, l'isomorphisme étant la restriction à F. En effet B défini sur k signifie que l'extension $k(B)/k$ est régulière, i.e, que $k(B) \cap \overline{k} = k$. En conséquence les extensions F/k et $k(B)/k$ sont linéairement disjointes, d'où $k(B) \cap F = k$ et $F(B) = k(B)F$. Donc si on choisit une k-base $(e_i)_i$ de F sur k alors $(e_i)_i$ est aussi une $k(B)$-base de $F(B)$ sur $k(B)$. Si $u \in G(F/k)$, on peut alors prolonger u à $F(B)$ en agissant sur les éléments de la base $(e_i)_i$ en posant $\overline{u}(\alpha) = \sum_i a_i u(e_i))$ où $\alpha = \sum_i a_i e_i \in F(B)$ où $a_i \in k(B)$ (on vérifie facilement que $\overline{u}$ définit un isomorphisme de corps). Il est clair que l'application $u \mapsto \overline{u}$ est l'isomorphisme réciproque de la restriction de $F(B)$ à F. On a donc la suite exacte:

$$1 \to \mathrm{Aut}(E/F(B)) \to \mathrm{Aut}(E/k(B)) \to G(F/k) \qquad (1.1)$$

1.1.3 Corps des modules

L'action d'un élément $u \in G(F/k)$ sur E dépend du prolongement $\overline{u}$ de celui-ci à une clôture algébrique de $F(B)$. On définit le groupe:

$$M(E/F(B)) = \{u \in G(F/k)/E \simeq_{F(B)} E^{\overline{u}}\}$$

Le groupe $M(E/F(B))$ est bien défini car la condition d'isomorphisme ne dépend pas du prolongement choisi $\overline{u}$. En effet si $\overline{u_1}$ et $\overline{u_2}$ sont deux prolongements de $u \in G(F/k)$ alors $\overline{u_2 u_1}^{-1}$ est un $F(B)$-isomorphisme de $E^{\overline{u_1}}$ sur $E^{\overline{u_2}}$. Donc E et $E^{\overline{u_1}}$ sont $F(B)$-isomorphes

si et seulement si E et $E^{\overline{u_2}}$ sont $F(B)$-isomorphes. On définit ensuite le corps des modules de l'extension $E/F(B)$ comme étant le sous-corps de F fixé par $M(E/F(B))$.

Remarque:

La définition précédente correspond à celle donnée plus habituellement que nous rappelons. Le groupe $G(F/k)$ agit sur les revêtements définis sur F. Si on note f^u le revêtement obtenu par l'action de u sur f alors on définit le corps des modules de f comme étant le sous-corps de F fixé par le groupe $M(f) = \{u \in G(F/k)/f^u \simeq_F f\}$. L'équivalence de catégories entre revêtements algébriques et extensions de corps de fonctions permet de dire que $M(f) = M(E/F(B))$

Proposition 1 *Soit $E/F(B)$ une extension de degré fini. Le corps k est le corps des modules de f si et seulement si la flèche de restriction de la suite exacte (1.1) est surjective. On a donc la nouvelle suite exacte:*

$$1 \to Aut(E/F(B)) \to Aut(E/k(B)) \to G(F/k) \to 1 \qquad (1.2)$$

Preuve:

Supposons que k soit le corps des modules de l'extension $E/F(B)$. Pour tout $u \in G(F/k)$ soit $\overline{u}$ un prolongement de u à une clôture algébrique de $F(B)$. Comme k est le corps des modules de l'extension $E/F(B)$, il existe un $F(B)$-isomorphisme $\psi_u : E^{\overline{u}} \to E$. On définit alors $\chi_u : E \to E$ comme le composé $\psi_u \overline{u}$. On voit que $\chi_u \in \mathrm{Aut}(E/k(B))$ pour tout $u \in G(F/k)$. De plus ψ_u étant un $F(B)$-isomorphisme de $E^{\overline{u}}$ sur E on voit que la restriction de χ_u à F est égale à u pour tout $u \in G(F/k)$. L'homomorphisme χ_u est un $k(B)$-automorphisme de E prolongeant u pour tout $u \in G(F/k)$. La dernière flèche de la suite exacte $Aut(E/k(B)) \to G(F/k)$ est donc surjective.

Réciproquement si la dernière flèche est surjective alors pour tout $u \in G(F/k)$ il existe un $k(B)$-automorphisme χ_u de E dont la restriction à F est u. Soit $\overline{u}$ un prolongement de u, il est clair que $\chi_u \overline{u}^{-1}$ est un $F(B)$-automorphisme de E sur $E^{\overline{u}}$ pour tout $u \in G(F/k)$. Donc $M(E/F(B) = G(\overline{k}/k)$ et k est le corps des modules de f.

1.2 Descente de Weil

1.2.1 Condition de cocycle de Weil

Dans ce paragraphe, on suppose que k est le corps des modules de l'extension $E/F(B)$. Pour tout $u \in G(F/k)$, on fixe un prolongement $\overline{u}$ à $\overline{E}$. Comme k est le corps des modules de l'extension $E/F(B)$, pour tout $u \in G(F/k)$, il existe un $F(B)$-isomorphisme $\psi_u : E^{\overline{u}} \to E$. On pose $\chi_u = \psi_u \overline{u}$; $\chi_u \in \mathrm{Aut}(E/k(B))$. On dira que la famille $(\psi_u)_{u \in G(F/k)}$ vérifie la condition de cocycle de Weil si la famille associée $(\chi_u)_{u \in G(F/k)}$ de $k(B)$-automorphismes de E vérifie:

$$\text{Pour tout } u, v \in G(F/k), \text{ on a } \chi_u \chi_v = \chi_{uv}$$

Si $[F : k] = \infty$, on demandera en plus que la correspondance $u \to \chi_u$ définisse une application continue $G(F/k) \to \mathrm{Aut}(E/k(B)) \subset G(\overline{k(B)}/k(B))$.

Remarques:

(a) L'existence d'une famille $(\psi_u)_{u \in G(F/k)}$ vérifiant la condition de cocycle ne dépend pas du choix des prolongements des morphismes u à une clôture algébrique de E. En effet si $\overline{u}'$ est un autre prolongement de u à $\overline{E}$ $(u \in G(F/k))$, la famille $(\psi'_u)_{u \in G(F/k)}$ déduite de la famille $(\psi_u)_{u \in G(F/k)}$ par la formule $\psi'_u = \psi_u \overline{u}(\overline{u}')^{-1}$ vérifie la condition de cocycle: on a en fait $\chi_u = \psi_u \overline{u} = \psi'_u \overline{u}'$ $(u \in G(F/k))$.

$$\begin{array}{ccc} & \overset{u'}{\to} & \\ E & \to & E^{\overline{u'}} \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle \psi_{u'}} \\ E^{\overline{u}} & \to & E \\ & \underset{\psi_u}{\to} & \end{array}$$

(b) La condition $\chi_u \chi_v = \chi_{uv}$ correspond à la condition de cocycle énoncée par Weil (celle donnée plus bas) de la façon suivante. Dans la situation géométrique un revêtement $f : X \to B$ est donné et E est le corps des fonctions $F(X)$ de X sur F. Si k est le corps des modules de f, on dispose de $F(B)$-isomorphismes $\varphi_u : X \to X^u$. L'action de $u \in G(F/k)$ sur X est celle qui consiste à faire agir u sur les coefficients des équations définissant localement X. Les isomorphismes notés précedemment ψ_u correspondent alors aux isomorphismes $\varphi_u^* : F(X^u) \to F(X)$ associés aux φ_u via le foncteur corps des fonctions. La condition de cocycle énoncée par Weil est:

Pour tout $u, v \in G(F/k)$ on a $\varphi_v^u \varphi_u = \varphi_{uv}$

où φ_v^u est l'isomorphisme φ_v tordu par l'action de $u \in G(F/k)$.
Si $\varphi_v^u \varphi_u = \varphi_{uv}$ alors $\varphi_{uv}^* = \varphi_u^*(\varphi_v^u)^* = \varphi_u^*(\varphi_v^*)^u$ où $*$ représente le foncteur corps des fonctions et l'action de u est l'action par conjugaison induite au niveau des corps de fonctions par l'action sur les coefficients des équations.

$$\begin{array}{ccc} & \overset{\varphi_v^*}{} & \\ F(X^v) & \to & F(X) \\ u \downarrow & & \downarrow u \\ F((X^v)^u) & \to & F(X^u) \\ & \underset{(\varphi_v^u)^*}{} & \end{array}$$

Si maintenant on pose $\chi_u = \varphi_u^* u$, on a bien

$$\chi_{uv} = \varphi_{uv}^* uv = \varphi_u^*(\varphi_v^*)^u uv = \varphi_u^* u \varphi_v^* v = \chi_u \chi_v$$

1.2.2 Théorème de descente

Théorème 1 *Soit $E/F(B)$ une extension finie de corps des modules k. Avec les notations précédentes, les énoncés suivants sont équivalents:*

(i) Il existe une famille $(\psi_u)_{u \in G(F/k)}$ telle que la condition de cocycle soit vérifiée.
(ii) Il existe une section continue à l'homomorphisme:
$Aut(E/k(B)) \to G(F/k)$.
(iii) Il existe une extension $E_k/k(B)$ tel $E_k F = E$ et $E_k \cap \overline{k} = k$.
(i.e. E_k est un k-modèle de E)

Exemples
(1) Supposons que $\mathrm{Aut}(E/F(B)) = \{1\}$. Dans la situation géométrique cela correspond à supposer que le revêtement $f : X \to B$ n'a pas d'automorphismes. Dans ce cas, la flèche $\mathrm{Aut}(E/k(B)) \to G(F/k)$ est un isomorphisme. La condition *(ii)* est satisfaite; le corps des modules est alors un corps de définition ([Fr]).

(2) Si $G(F/k)$ est un groupe profini projectif (e.g $F = \overline{k}$ et $cd(k) \leq 1$), alors (ii) est satisfaite; le corps k est donc un corps de définition ([DeDo1]).

(3) Si $G(F/k)$ est fini d'ordre premier à $\mathrm{Aut}(E/F(B))$, alors la suite exacte se scinde (Schur-Zassenhauss), le corps des modules est dans ce cas un corps de définition.

(4) Le théorème de Coombes-Harbater ([CoHa]) se déduit aussi directement du théorème 1 Nous y reviendrons au chapitre 3 (cf Remarque). Ce résultat sera aussi l'objet du chapitre 2 où nous en donnerons une forme explicite.

Preuve

Montrons que $(i) \Rightarrow (ii)$. L'existence d'une famille $(\psi_u)_{u \in G(F/k)}$ vérifiant la condition de cocycle de Weil se traduit par l'existence d'une famille associée $(\chi_u)_{u \in G(F/k)}$ de $k(B)$-automorphismes de E vérifiant $\chi_{uv} = \chi_u \chi_v$. On obtient un morphisme $\chi : G(F/k) \to \mathrm{Aut}(E/k(B))$. Ce morphisme χ est une section de $\mathrm{Aut}(E/k(B) \to G(F/k)$ car la restriction de $\chi_u = \psi_u \overline{u}$ à F est u.

La réciproque $(ii) \Rightarrow (i)$ est également immédiate. Si χ est une section, la famille (ψ_u) définie par $\psi_u = \chi(u)\overline{u}^{-1}$ est une famille de $F(B)$-isomorphisme satisfaisant la condition de cocycle de Weil.

Montrons que $(ii) \Rightarrow (iii)$.

$$\begin{array}{ccc} E & \leftarrow & E_k = E^{Im\chi} \\ \uparrow & & \uparrow \\ F(B) & \leftarrow & k(B) \end{array}$$

On pose $E_k = E^{Im\chi}$ où $Im\chi$ désigne l'image de l'homomorphisme $\chi : G(F/k) \to \mathrm{Aut}(E/k(B))$. Montrons que $E_k F = E$. Soit $\sigma \in \mathrm{Aut}(E/k(B))$ tel que $\sigma = id$ sur $E_k.F \subset E$. Alors $\sigma \in Im\chi$ car σ fixe E_k. D'autre part $\sigma \in \mathrm{Aut}(E/F(B)$ fixe F et $k(B)$. D'où $\sigma \in Im\chi \cap \mathrm{Aut}(E/F(B)) = 1$. Donc $\sigma = id$ sur E. D'après la correspondance de Galois on a $E = E_k.F$.

Montrons que les extensions E_k et F sont linéairement disjointes sur k, pour cela il suffit de montrer que $E_k \cap F = k$. Si $x \in E_k \cap F$ alors x est fixé par $Im\chi$ car $E_k = E^{Im\chi}$ et x est fixé par $\mathrm{Aut}(E/F(B))$ car $F \subset F(B)$. Donc x est fixé par tout élément de $\mathrm{Aut}(E/k(B))$; en effet les sous-groupes $Im\chi$ et $\mathrm{Aut}(E/F(B))$ engendrent $\mathrm{Aut}(E/k(B))$ car χ est une section de $\mathrm{Aut}(E/k(B)) \to$

$G(F/k)$ dont le noyau est $\mathrm{Aut}(E/F(B))$. En conclusion, x est un élément de F fixé par tout élément de $\mathrm{Aut}(E/k(B))$, donc par tout élément de $G(F/k)$. Donc $x \in k$. On obtient donc $E_k \cap F = k$.

Montrons que $(iii) \Rightarrow (ii)$. On suppose qu'il existe une extension E_k vérifiant $E_k.F = E$ et $E_k \cap F = k$. On peut alors considérer le morphisme restriction $\phi : G(E/E_k) \to G(F(B)/k(B))$. Ce morphisme est injectif car si $\sigma \in G(E/E_k)$ est trivial sur E_k et sur $F(B)$ alors σ est trivial sur $E = E_k F$. Ce morphisme est surjectif car si $\tau \in G(F(B)/k(B))$ alors on peut prolonger τ à E. On choisit une $k(B)$-base $(a_i)_i$ de E_k et une $k(B)$-base $(e_j)_j$ de $F(B)$ avec $e_1 = 1$. Alors $(a_i e_j)_{i,j}$ est une $k(B)$-base de E car les extensions E_k et $F(B)$ sont linéairement disjointes sur $k(B)$. On définit alors le prolongement de τ en posant $\tau(\sum_{i,j} \alpha_{i,j} a_i e_j) = \sum_{i,j} \alpha_{i,j} a_i \tau(e_j)$ (on vérifie qu'on définit bien ainsi un isomorphisme de corps). De plus grâce au choix de $e_1 = 1$, il est clair que l'isomorphisme ainsi prolongé vaut l'identité sur E_k.

On définit alors la section χ en composant ϕ^{-1} avec l'inclusion de $i : G(E/E_k) \subset Aut(E/k(B))$. On pose donc $\chi = io\phi^{-1}$. Ce qui prouve le théorème.

1.3 Position du problème

Le théorème 1 assure l'existence d'un k-modèle mais ne permet pas d'en déterminer explicitement. Dans les chapitres suivants on donne dans certains cas une méthode de descente qui sera effective.

Dans le chapitre 2 on se restreindra au cas où $F = \overline{k}$, l'extension $E/\overline{k}(B)$ sera galoisienne et la base B sera $\mathbf{P}_1$ la droite projective définie sur k. Dans ce cas on a $k(B) = k(T)$ et donc le problème se pose de la façon suivante:

Problème général:

Etant donnée une extension finie $E/\overline{k}(T)$ dont on sait que k est le corps des modules, comment trouver explicitement un modèle sur k, i.e., une extension $E_k/k(T)$ telle que $E_k\overline{k} = E$ et $E_k \cap \overline{k} = k$?

Pour obtenir des modèles explicites définis sur le corps des modules nous partirons d'un modèle explicite défini sur $\overline{k}$. Il reste à

préciser ce que nous entendons par modèle explicite. Ce sera la donnée aussi précise que possible:

- du polynôme minimal $P(T,Y)$ d'un élément primitif de l'extension en question ($E/\overline{k}(T)$ ou $E_k/k(T)$). Dans le cas où k est un corps de nombres, nous donnerons une borne pour le degré d'un polynôme définissant l'extension $E_k/k(T)$, ou bien
- d'une série de Laurent $y \in \overline{k}((T-t_o))$ engendrant l'extension en question (dans un certain plongement $E \subset \overline{k}((T-t_o))$ où t_o est rationnel sur k). Partant d'une série $y \in \overline{k}((T-t_o))$ tel que $\overline{k}(T,y) = E$, nous donnerons une formule donnant $y_k \in \overline{k}((T-t_o))$ tel que $E_k = k(T,y_k)$.

Dans le chapitre 3, nous nous dispenserons de l'hypothèse galoisienne. Nous obtiendrons aussi une description assez précise d'un élément primitif d'un k-modèle $E_k/k(T)$. Cette description ne sera pas cependant aussi satisfaisante que dans le cas galoisien dans la mesure où elle dépendra de la section χ, qui n'est pas connue explicitement en général (voir Ch.3 remarque).

Chapitre 2

Descente du corps de définition des revêtements galoisiens

Dans ce chapitre k est un corps de caractéristique 0 et $f : X \to \mathbf{P}_1$ un revêtement défini sur $\overline{k}$ où X est une courbe projective lisse irréductible. On a vu au chapitre 1 que le groupe de Galois $G(k) := Gal(\overline{k}/k)$ agit sur les variétés algébriques définies sur $\overline{k}$. Si on note $f^\tau : X^\tau \to \mathbf{P}_1$ le revêtement obtenu par l'action de $\tau \in G(k)$ sur f, on définit alors le corps des modules absolu de f comme le sous-corps de $\overline{k}$ fixé par tous les k-automorphismes τ de $\overline{k}$ tels que f et f^τ soient isomorphes comme revêtements. Le corps des modules de f est une extension algébrique de k contenue dans tous les corps de définition de f contenant k. En général le corps des modules n'est pas un corps de définition: des contre-exemples sont donnés dans [CouGr] et [Cou]. Un théorème de Coombes-Harbater [CoHa] montre cependant que c'est le cas pour les revêtements galoisiens. Pour un exposé plus complet sur la notion de corps des modules, voir [DeDo1] et [DeDo2].

Ce chapitre présente une nouvelle approche du théorème de Coombes-Harbater. Le résultat que nous obtenons en donne une forme plus précise: nous expliquons comment à partir d'équations définissant un revêtement galoisien f donné, on peut explicitement trouver

un modèle de f défini sur son corps des modules. De plus, dans le cas des revêtements définis sur $\overline{\mathbf{Q}}$, le résultat est effectif: nous donnons une borne pour le degré et la hauteur des équations définissant le nouveau modèle. Notre approche diffère de celle de Coombes et Harbater en ce qu'elle s'appuie non pas sur le critère de descente de Weil (comme dans [CoHa]) mais plus simplement sur le lemme de Dedekind. Notre approche fournit donc aussi une nouvelle preuve du théorème de Coombes et Harbater. Enfin comme dans [De1], notre résultat s'étend sous certaines conditions à des corps de caractéristique quelconque (cf. §2 Remarque).

2.1 Enoncés

Théorème 2 (Coombes-Harbater [CoHa] [De1]) *Soit k un corps de caractéristique 0 et $f : X \to \mathbf{P}_1$ un revêtement galoisien défini sur $\overline{k}$. Si k est le corps des modules de f alors k est un corps de définition du revêtement f. De plus il existe un modèle $f_k : X_k \to \mathbf{P}_1$ défini sur k avec un point k-rationnel non ramifié sur X_k.*

La preuve donnée dans [CoHa] utilise le critère de descente de Weil ([We]). Pour tout $\tau \in G(k)$, il existe un isomorphisme de revêtement $\varphi_\tau : X \to X^\tau$ (par définition du corps des modules). En général, il n'y a pas unicité de φ_τ. Mais d'après le critère de descente de Weil, k est un corps de définition si et seulement si on peut trouver une famille $(\varphi_\tau)_{\tau \in G(k)}$ vérifiant $\varphi_v^u \varphi_u = \varphi_{uv}$ $(u, v \in G(k))$. Coombes et Harbater montrent qu'une telle famille existe en utilisant le fait que le groupe de Galois du revêtement agit simplement et transitivement sur chaque fibre non ramifiée, ce qui permet de "rigidifier" le choix de chaque φ_τ. Cependant [CoHa] ne fournit pas explicitement la famille $(\varphi_\tau)_{\tau \in G(k)}$ et donc ne donne pas explicitement un k-modèle du revêtement. Au contraire, notre méthode, qui n'utilise pas le critère de Weil, fournit une description explicite du corps des fonctions $E_k/k(T)$ d'un k-modèle du revêtement.

Le revêtement f correspond via le foncteur corps des fonctions à une extension algébrique E de $\overline{k}(T)$. De plus cette extension est galoisienne. Notons G son groupe de Galois. Expliquons l'action de $G(k)$ sur le corps de fonctions E. Si $\tau \in G(k)$ alors τ se prolonge

en un $k(T)$-automorphisme d'une clôture algébrique de $k(T)$. Si on note $\overline{\tau}$ ce prolongement alors on peut définir $E^{\tau} := E^{\overline{\tau}}$ car cette définition ne dépend pas du prolongement $\overline{\tau}$. En effet si $\overline{\tau_1}$ et $\overline{\tau_2}$ sont deux prolongements de $\tau \in G(k)$ alors on a $\overline{\tau_1}^{-1}\overline{\tau_2} \in G(\overline{k}(T)/\overline{k}(T))$. Or E est une extension galoisienne de $\overline{k}(T)$ donc $E^{\overline{\tau_1}^{-1}\overline{\tau_2}} = E$, d'où on a $E^{\overline{\tau_1}} = E^{\overline{\tau_2}}$. Quant à l'hypothèse "$f$ et f^{τ} sont isomorphes", elle équivaut à dire que les corps de fonctions E^{τ} et E sont $\overline{k}(T)$-isomorphes et donc puisque l'extension $E/\overline{k}(T)$ est galoisienne, que ces corps sont égaux.

Soit y un élément primitif de E sur $\overline{k}(T)$ et $P(T,Y)$ le polynôme minimal de y sur $\overline{k}(T)$. Pour tout $t_0 \in k$ non racine du discriminant $\Delta(T)$ de $P(T,Y)$ relativement à Y, il existe un plongement s_{t_0} : $E \to \overline{k}((T-t_0))$.
On peut maintenant traduire les hypothèses du théorème de Coombes-Harbater:

(i) $E/\overline{k}(T)$ est galoisienne.
(ii) $E = E^{\tau}$ pour tout $\tau \in G(\overline{k}/k)$

La conclusion du théorème se traduit en disant qu'il existe une extension algébrique $E_k/k(T)$ vérifiant les conditions:

(a) E_k/k est régulière ($i.e.$, $E_k \cap \overline{k} = k$)
(b) $E_k\overline{k} = E$
(c) $E_k \subset k((T-t_0))$

Nous allons expliquer comment déterminer explicitement une telle extension E_k.

On définit le corps K_0 comme le corps engendré sur k par les coefficients de $P(T,Y)$. Soit

$$y = \sum_{m \geq 0} y_m (T-t_0)^m$$

un développement dans $\overline{\mathbf{k}}[[T-t_0]]$ de l'élément primitif y. Posons $K = K_0(y_0)$. Le corps K est une extension algébrique de degré fini qui contient tous les coefficients y_m. En effet les coefficients de la série y se détermine de proche en proche à l'aide d'une formule de récurrence dépendant des coefficients du polynôme $P(T,Y)$. De plus on peut supposer que y est entier sur $K_0[T]$. On notera $Tr_{K/k}$ l'application trace de K dans k.

Théorème 3 *On suppose que la série formelle*

$$y = \sum_{m \geq 0} y_m (T - t_0)^m \in K((T - t_0))$$

engendre une extension $E = \overline{k}(t)(y)$ *vérifiant les conditions* (i) *et* (ii) *ci-dessus. Alors il existe* $a \in K$ *tel que*

$$y_a = \sum_{m \geq 0} Tr_{K/k}(a y_m)(T - t_0)^m \in k((T - t_0))$$

soit un élément primitif de E *sur* $\overline{k}(T)$*. De plus l'extension* $k(T)(y_a)/k(T)$ *est régulière sur* k*. C'est à dire que l'extension* $E_k = k(T)(y_a)$ *vérifie les conditions* (a),(b),(c) *ci-dessus.*

La condition (c) correspond à la conclusion du théorème 1 qu'il existe un point k-rationnel non ramifié sur X_k (au dessus de t_0).

Corollaire 1 *Si* k *est un corps de nombres et si on note* $P_k(T, Y) \in k[T, Y]$ *le polynôme minimal de* y_a *sur* $k(T)$ *alors on a*

$$\begin{cases} deg(P_k) & \leq & (2D)^d \\ h(P_k) & \leq & 5d^2(2D)^{2d} h(P) \end{cases}$$

où $D = deg(P)$, $d = [K : k] \leq D[K_0 : k]$ *et* $h(P)$ *est la hauteur logarithmique de Weil du polynôme* P *(cf. §3.2).*

Exemple
Considérons l'extension $E = \overline{\mathbf{Q}}(T)(y)$ sur $\overline{\mathbf{Q}}(T)$ où $y = 1 + i + i\sqrt{1+T}$. D'après la preuve du théorème (voir §2), l'élément a peut être ici pris égal à i. Ainsi, $y_i = iy + \overline{iy} = -2 - 2\sqrt{1+T}$ est un élément primitif de l'extension de départ dont le polynôme minimal est à coefficients dans $\mathbf{Q}$. Ce polynôme est $Y^2 + 4Y - 4T$.

2.2 Une estimation plus intrinsèque de $\deg(P_k)$

Dans le corollaire 1 $\deg(P_k)$ est le degré d'une équation polynômiale définissant un modèle sur le corps des modules du revêtement. Le corollaire 1 donne une borne en fonction de $D = \deg(P)$ et $[K :$

$k]$. On peut en déduire une borne en fonction de paramètres plus intrinsèques liés au revêtement $f : X \to \mathbf{P}_1$, à savoir le genre de X, l'ordre $|G|$ du groupe G des automorphismes du revêtement ($|G|$ est aussi le degré du revêtement) et l'ordre $|\mathrm{Aut}(G)|$ du groupe des automorphismes de G.

- Par construction, le corps K de la section 2.1 est le corps de rationalité d'un modèle $f_K : X_K \to \mathbf{P}_1$ du revêtement $f : X \to \mathbf{P}_1$ et d'un point de X_K au dessus d'un point non ramifié $t_o \in \mathbf{P}_1(k)$. D'après [DeDo1; Cor.3.5 p 320], on peut demander que K vérifie:

$$[K : k] \leq |\frac{\mathrm{Nor}_{S_d} G}{\mathrm{Cen}_{S_d} G}| = |\mathrm{Aut}(G)|$$

.

Ici $\mathrm{Nor}_{S_d} G$ et $\mathrm{Cen}_{S_d} G$ désignent respectivement le normalisateur et le centralisateur de G dans la représentation $G \hookrightarrow S_d$ associée à l'action de G sur une fibre non ramifiée du revêtement. Comme le revêtement est supposé galoisien, on a $\mathrm{Nor}_{S_d} G \simeq \mathrm{Cen}_{S_d} \times \mathrm{Aut}(G)$ (eg. [DeDo1, Prop.3.1 p316]) ce qui justifie l'égalité plus haut.

- Ensuite on peut prendre pour D le degré du polynôme minimal P d'un élément primitif arbitraire de l'extension $K(X_K)/K(T)$. On a $\deg(P) \leq \deg_T(P) \deg_Y(P) = \deg_T(P)|G|$. Nous allons montrer qu'il existe un élément primitif pour lequel

$$\deg_T(P) \leq \frac{(2g+1)|G| \log |G|}{\log 2}$$

Cela combiné au corollaire 1 nous permettra de conclure qu'il existe une équation polynômiale $P_k(T, Y) = 0$ définissant un k-modèle du revêtement avec

$$\deg(P_k) \leq (4(2g+1)|G|^2 \log |G|)^{\mathrm{Aut}(G)}$$

L'estimation de $\deg_T(P)$ utilise le lemme suivant, qui nous a été indiquée par U. Zannier.

Lemme 1 *Soit $\varphi : C \to C'$ un morphisme non constant de courbes projectives lisses, défini sur un corps K et de degré $\rho > 1$. Soit $\delta' \geq 1$ le degré d'un diviseur effectif $\Delta' = m'_1 + \ldots + m'_{\delta'}$ sur C' défini sur K. Alors il existe $f \in K(C) - K(C')$ tel que* $\deg_C(f) \leq (2g+1)\rho\delta'$

où $\deg_C(f) = [\overline{K}(C) : \overline{K}(f)]$ *désigne le degré de la fonction* f *sur la courbe* C *et* g *le genre de* C.

Preuve: Soit $\Delta = \varphi^*(\Delta') = M_1 + \ldots + M_\delta$ le diviseur image réciproque de Δ' par φ; Δ est un diviseur effectif sur C défini sur K et de degré $\delta = \rho\delta'$.

Soit $n = 2g + 1$. Considérons les K-espaces vectoriels

$$\mathcal{L}_C(n\Delta) = \{f \in K(C)/(f)_C + n\Delta \geq 0\} \subset K(C)$$

$$\mathcal{L}_{C'}(n\Delta') = \{f \in K(C')/(f)_{C'} + n\Delta' \geq 0\} \subset K(C') \subset K(C)$$

On a $2g - 2 - \deg(n\Delta) < 0$ (resp. $2g' - 2 - \deg(n\Delta') < 0$) (où $g' \leq g$ est le genre de C'. D'après le théorème de Riemann-Roch, $\mathcal{L}_C(n\Delta)$ et $\mathcal{L}_{C'}(n\Delta')$ sont des K-espaces vectoriels de dimensions respectives $l_C(n\Delta) = n\delta + 1 - g$ et $l_{C'}(n\Delta') = n\delta' + 1 - g'$. De l'inégalité $n > g$ on déduit que

$$l_C(n\Delta) - l_{C'}(n\Delta') = n\delta'(\rho - 1) - (g - g') > 0$$

En conséquence, il existe $f \in \mathcal{L}_C(n\Delta) - \mathcal{L}_{C'}(n\Delta')$. Alors $f \in K(C)$ mais $f \notin K(C')$: en effet si $f \in K(C')$ alors $f \in \mathcal{L} - C(n\Delta) \cap K(C') \subset \mathcal{L}_{C'}(n\Delta')$, ainsi que le précise l'argument ci-dessous.

En effet, pour tout $M \in C$, si $m = \varphi(M)$, on a avec des notations évidentes $ord_{C,M}(f) = e_{M/m} ord_{C',m}(f)$ où $e_{M/m}$ est l'indice de ramification de φ en M au dessus de m. On a d'autre part $v_M(\Delta) = e_{M/m} v_m(\Delta')$ où $v_M(\Delta)$ (resp. $v_m(\Delta')$) désigne le coefficient de M (resp. m) dans le diviseur Δ (resp. Δ').

On a donc que,

$$\text{si } ord_{C,M}(f)_C + n v_M(\Delta) \geq 0 \text{ pour tout } M \in C$$
$$[i.e., f \in \mathcal{L}_C(n\Delta)]$$

$$\text{alors } ord_{C',m}(f)_{C'} + n v_m(\Delta') \geq 0 \text{ pour tout } m = \varphi(M) \in C'$$
$$[i.e., f \in \mathcal{L}_{C'}(n\Delta')]$$

Enfin, on a $\deg_C(f) \leq \deg(n\Delta) = n\delta = n\rho\delta'$. Ce qui prouve le lemme.

Pour en déduire l'estimation précédente, on procède de la façon suivante. Le lemme, appliqué à $C = X_K$, $C' = \mathbf{P}_1$ et $\Delta' = (t_o)$ fournit $f_1 \in K(X_K) - K(T)$ tel que $\deg(f_1) \leq (2g+1)|G|$.

Le lemme appliqué à $C = X_K$ et C' un modèle projectif lisse du corps des fonctions $K(T, f_1)$ et $\Delta' = f_1^*((t_o))$ fournit $f_2 \in K(X_K) - K(T, f_1)$ tel que $\deg(f_2) \leq (2g+1)|G|$.

Comme $[K(X_K) : K(T)] < \infty$, après un certain nombre, disons k, d'applications successives du lemme, on obtient des fonctions $f_1, \ldots, f_k$ vérifiant:

$$\begin{cases} f_i \in K(X_K) - K(T, f_1, ..., f_{i-1}) \\ \deg(f_i) \leq (2g+1)|G| \\ K(X_K) = K(T, f_1, ..., f_k) \end{cases}$$

Puisque $[K(T, f_1, ..., f_i) : K(T, f_1, ..., f_{i-1}] \geq 2$ pour $i = 1, ..., k$ on aura $k \leq \dfrac{\log |G|}{\log 2}$. Comme K est infini, il existe $c_1, ..., c_k \in K$ tel que $K(X_K) = K(T, c_1 f_1 + ... + c_k f_k)$. Posons $f = c_1 f_1 + ... + c_k f_k$ alors $K(X_K) = K(T, f)$ et on a alors

$$\deg f \leq \sum_{i=1}^{i=k} \deg(f_i) \leq \frac{(2g+1)|G| \log |G|}{\log 2}$$

Pour conclure, il reste à voir que si P est le polynôme minimal de f sur $K(T)$, alors $\deg(f) = \deg_T(P)$.

2.3 Preuve du théorème

On note $\tau_1, ..., \tau_d$ les k plongements de K dans $\overline{k}$. On a alors pour tout $a \in K$

$$y_a = \sum_{i=1}^{d} (ay)^{\tau_i} = \sum_{m \geq 0} Tr_{K/k}(ay_m)(T - t_0)^m$$

L'action des k-plongements τ_i se faisant sur les coefficients de la série ay. Il résulte de l'hypothèse $E^\tau = E$ pour tout $\tau \in G(k)$ que $y^{\tau_i} \in E$ pour $i = 1, ..., d$ et donc que $y_a \in E$. De plus il est clair que $y_a \in k((T - t_0))$ car $Tr_{K/k}(ay_m) \in k$, pour tout $m \geq 0$.

Lemme 2 *Pour tous σ et σ' de $G(E/\overline{k}(T))$ distincts il existe $a \in K$ tel que les termes constants des séries $\sigma(y_a)$ et $\sigma'(y_a)$ soient distincts.*

Preuve

On considère $\sigma, \sigma' \in G(E/\overline{k}(T))$ tels que $\sigma \neq \sigma'$. On note c_i le terme constant de la série $\sigma(y^{\tau_i}) - \sigma'(y^{\tau_i})$ pour $i = 1, ..., d$. La famille $(c_i)_i$ d'éléments de $\overline{k}$ n'est pas réduite à 0. En effet y est un élément primitif de E donc $\sigma(y) \neq \sigma'(y)$. Comme t_0 est supposé non racine du discriminant $\Delta(T)$ de $P(T,Y)$, $\sigma(y)$ et $\sigma'(y)$ vues comme séries en $T - t_0$ sont déterminées par leurs termes constants, qui sont donc distincts. On considère l'application

$$\sum_{i=1}^{i=d} c_i \tau_i$$

de K dans $\overline{k}$. Elle est non nulle d'après le lemme de Dedekind car les k-plongements sont linéairement indépendants sur $\overline{k}$. Il existe donc $a \in K$ tel que

$$\sum_{i=1}^{i=d} c_i a^{\tau_i} \neq 0$$

De la définition des c_i, on déduit

$$\text{terme constant}(\sum_{i=1}^{i=d} \sigma(a^{\tau_i} y^{\tau_i})) \neq \text{terme constant}(\sum_{i=1}^{i=d} \sigma'(a^{\tau_i} y^{\tau_i}))$$

Ce qui prouve le lemme.

D'après le lemme, pour tous $\sigma, \sigma' \in G(E/\overline{k}(T))$ il existe $a \in K$ tel que $\sigma(y_a) \neq \sigma'(y_a)$. Il faut remarquer que a dépend de σ, σ'. L'argument suivant montre que a peut être choisi indépendamment de σ, σ'. L'ensemble

$$H_{\sigma,\sigma'} = \{a \in K / \text{terme constant}(\sigma(y_a)) = \text{terme constant}(\sigma'(y_a))\}$$

est un sous k-espace vectoriel de K strictement inclus dans celui-ci. Comme k est infini, K n'est pas la réunion des $\frac{n(n-1)}{2}$ sous-espaces $H_{\sigma,\sigma'}$. En prenant a hors de cette réunion on a $\sigma(y_a) \neq \sigma'(y_a)$ pour tout $\sigma \neq \sigma'$. L'élément y_a est donc un élément primitif de E sur $\overline{k}(T)$ car il possède exactement n conjugués distincts.

L'cxtension $E_k = k(T)(y_a)$ de $k(T)$ satisfait donc la conclusion (b) du théorème 2. La conclusion (c) est vraie par construction. Quant à la régularité de l'extension E/k elle résulte de:

$$k(T)(y_a) \cap \overline{k} \subset k((T - t_0)) \cap \overline{k} = k$$

On a ainsi construit l'extension $E_k = k(T)(y_a)$ qui correspond au corps des fonctions d'un modèle f_k défini sur k du revêtement galoisien f.

Remarque
On utilise l'hypothèse $car(k) = 0$ en deux endroits:
- pour l'existence de t_0 tel que $\Delta(t_0) \neq 0$
- pour l'existence de $a \notin \cup H_{\sigma,\sigma'}$
En fait l'hypothèse k infini suffit.
Si k est fini, on peut plus généralement considérer les $k(T)$-espaces

$$H_{\sigma,\sigma'} \otimes_k K(T)$$

et prendre $a \in K(T)$ qui est infini. Le problème est que l'on est pas assuré de l'existence d'un point t_0 où f ne serait pas ramifié.
En conclusion le théorème 2 s'étend au cas où k est infini ou k est fini et il existe $t_0 \in k$ tel que $\Delta(t_0) \neq 0$.

2.4 Preuve du corollaire

2.4.1 Détermination de a

On peut se demander comment déterminer l'élément a du théorème 2? Nous allons voir qu'on peut prendre

$$a = n_1 e_1 + ... + n_d e_d$$

où $n_1, ..., n_d \in \mathbf{Z}$ et $e_1, ..., e_d$ est une base de K sur k.

En effet dans la preuve du Théorème, on a choisi $a \in K$ tel que l'égalité suivante n'ait pas lieu:

$$\text{terme constant}(\sum_{i=1}^{i=d} \sigma(y^{\tau_i} a^{\tau_i})) = \text{terme constant}(\sum_{i=1}^{i=d} \sigma'(y^{\tau_i} a^{\tau_i}))$$

pour tous $\sigma, \sigma' \in G$. On a vu qu'il suffit de prendre $a \notin \cup H_{\sigma,\sigma'}$ où la réunion est prise sur les paires $\sigma, \sigma' \in G$ avec $\sigma \neq \sigma'$. Il s'agit donc de trouver a hors d'un nombre fini de sous-espaces stricts du k-espace K. On fixe une base $(e_1, ..., e_d)$ de K sur k. On pose alors $\Gamma = \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_d$ qui est un réseau de K. On pose alors

$$C_p = \{x \in \Gamma : x = n_1e_1 + \cdots + n_de_d, \mid n_i \mid \leq p\}$$

On a $\mathrm{Card}(C_p) = (2p+1)^d$.

Lemme 3 *Soit H un hyperplan de K vu comme k-espace vectoriel, alors $Card(H \cap C_p) \leq (2p+1)^{d-1}$.*

Preuve: On considère une équation $a_1x_1 + \cdots + a_nx_n = 0$ de l'hyperplan H dans la base $e_1, \cdots, e_d$ de K sur k. On peut supposer que $a_1 \neq 0$. Si $(x_1, \cdots, x_d) \in H \cap C_p$ alors on a donc $2p+1$ choix possibles pour chacun des x_i $i = 2, ..., d$ car les x_i sont des entiers vérifiant $\mid x_i \mid \leq p$. L'équation laisse alors au plus une seule possibilité pour x_1. D' où $\mathrm{Card}(H \cap C_p) \leq (2p+1)^{d-1}$.

Donc si on a N hyperplans $H_1, \cdots, H_N$ alors on a l'inégalité

$$\mathrm{Card}(\bigcup_{i=1}^{i=N} (H_i \cap C_p)) \leq N(2p+1)^{d-1}$$

Et donc si $[\frac{N}{2}] + 1 \leq p$, où $[x]$ désigne la partie entière de x, on a alors

$$\mathrm{Card}(C_p) > \mathrm{Card}(\bigcup_{i=1}^{i=N} H_i \cap C_p)$$

On applique cela à ce qui précède: on a $\frac{n(n-1)}{2} = N$ sous-espaces $H_{\sigma,\sigma'}$. Il existe $a = n_1e_1 + \cdots + n_de_d$ avec la condition $|n_i| \leq [\frac{n(n-1)}{4}] + 1$ tel que $a \notin \cup H_{\sigma,\sigma'}$. Et cet élément a vérifie la conclusion du Théorème 2.

2.4.2 Calcul de la hauteur des éléments a et y_a

On suppose désormais que k est un corps de nombres. On rappelle les notations suivantes:

Pour $p \geq 2$ on notera $H(\alpha_1, \cdots, \alpha_p)$ la hauteur de Weil d'un p-uplet où $\alpha_1, \cdots, \alpha_p$ sont des nombres algébriques, qui est définie par

$$H(\alpha_1, \cdots, \alpha_p) = [\prod_{v \in M_F} sup_{i=1,\ldots,p} |\alpha|_i]^{\frac{1}{[F:Q]}}$$

où F est un corps de nombres contenant les éléments α_i et où v parcourt M_F un ensemble de valeurs absolues indépendantes vérifiant la formule du produit([La]). On définit la hauteur d'un nombre algébrique $\alpha \in \overline{\mathbf{Q}}$ par $H(1, \alpha)$. Si $P(T, Y)$ est un polynôme à coefficients dans un corps de nombres alors on définit la hauteur de P comme la hauteur du p-uplet formé par ses coefficients. De plus on notera

$$h(\alpha_1, \cdots, \alpha_p) = \log H(\alpha_1, \cdots, \alpha_p)$$

la hauteur logarithmique de Weil. Si y est une fonction algébrique entière sur $\overline{k}[T]$, on définira sa hauteur $H(y)$ comme la hauteur de son polynôme minimal sur $\overline{k}[T]$.

On veut donc majorer la hauteur logarithmique du polynôme minimal P_k de y_a. Plusieurs résultats nous seront utiles.

Proposition 2 ([La]; Prop.2.12 p.61) *Si* $P_1, P_2 \in \overline{\mathbf{Q}}[Y_1, \cdots, Y_n]$, *alors*

$$h(P_1) \leq h(P_1) + h(P_2) \leq h(P_1 P_2) + n \deg(P_1 P_2)$$

En utilisant l'inégalité précédente on voit que pour majorer la hauteur de y_a il suffit de majorer la hauteur d'un polynôme $\hat{R}(T, Y) \in \overline{k}(T, Y)$ qui annule y_a. On a $y_a = \sum_{i=1}^{i=d} (ay)^{\tau_i}$ et on connait des polynômes qui annulent chacun des termes de cette somme. En effet si $P(T, Y)$ est le polynôme minimal de y sur $\overline{k}(T)$ et si on note

$$P(T, Y) = a_0 + a_1 Y + \cdots + a_{n-1} Y^{n-1} + Y^n$$

où $a_0, \cdots, a_{n-1} \in \overline{k}[T]$, alors ay a pour polynôme minimal

$$R(T, Y) = a_0 a^n + a_1 a^{n-1} Y + \cdots + a_{n-1} a Y^{n-1} + Y^n \text{ où } n = \deg_Y P$$

Et donc $(ay)^{\tau_i}$ a pour polynôme minimal

$$R^{\tau_i} = a_0^{\tau_i} (a^{\tau_i})^n + \cdots + a_{n-1}^{\tau_i} a^{\tau_i} Y^{n-1} + Y^n$$

On va construire un polynôme qui annule y_a à l'aide de résultants. On introduit les notations suivantes:
Soient $f(Y) = a_pY^p + \cdots + a_0$ avec $a_p \neq 0$ et $g(Y) = b_qY^q + \cdots + b_0$ avec $b_q \neq 0$ deux polynômes à coefficients dans un anneau commutatif A, on note $R_Y(f,g)$ leur résultant, on définit leur résultant réduit $\hat{R}_Y(f,g)$ par la formule:

$$R_Y(f,g) = a_p^q b_q^p \hat{R}_Y(f,g)$$

Si $F(T,Y_1,...,Y_m,Z) \in K[T,Y_1,...,Y_m,Z]$ et $P_i(T,Y_i) \in K[T,Y_i]$, on définit de proche en proche les polynômes $\hat{R}_i$ par:

$$\begin{cases} \hat{R}_1 &= \hat{R}_{Y_1}(F,P_1) \\ \hat{R}_i &= \hat{R}_{Y_i}(\hat{R}_{i-1},P_i) \text{ pour } i = 2,...,m \end{cases}$$

Proposition 3 ([De2]) *Pour $i = 1,...,m$ les polynômes $\hat{R}_i$ sont dans $K[T,Y_{i+1},...,Y_m,Z]$. En particulier, $\hat{R}_m \in K[T,Z]$. De plus si on se donne $z \in \overline{K}[T]$ une racine de $\hat{R}_m$ (i.e., $\hat{R}_m(T,z) = 0$), alors il existe $y_1,...,y_m$ dans $\overline{K}(T)$ tel que*

$$\begin{cases} P_1(T,y_1) &= 0 \\ &\vdots \\ P_m(T,y_m) &= 0 \\ F(T,y_1,...,y_m,z) &= 0 \end{cases}$$

Réciproquement, si on se donne $y_1,...,y_m$ et z tel que y_i soit racine de P_i pour $i = 1,...,m$ et tel que $F(T,y_1,...,y_m,z) = 0$ alors z est racine de $\hat{R}_m$ (i.e., $\hat{R}_m(T,z) = 0$).

Preuve: Il suffit de voir que $\hat{R}_m(T,z) = 0$ si et seulement si $\hat{R}_{m-1}$ et P_m ont une racine commune. Donc si et seulement s'il existe $y_m \in \overline{K}(T)$ tel que $P_m(T,y_m) = 0$ et $\hat{R}_{m-1}(T,y_m) = 0$. De même $\hat{R}_{m-1}(T,y_m) = 0$ si et seulement si P_{m-1} et $\hat{R}_{m-2}$ ont une racine commune. Et on continue ainsi de suite.

Lemme 4 ([De2]) *Soit $A,B \in K[Y_1,...,Y_n]$ deux polynômes tel que $\deg_{Y_1}(A) > 0$ et $\deg_{Y_1}(B) > 0$. Soit $R = R_{Y_1}(A,B)$ alors on a*

$$\begin{cases} \deg(R) & \leq & 2\deg(A)\deg(B) \\ h(R) & \leq & \deg(A)h(B)\deg(B)h(A) + n\deg(AB)\log(\deg(AB)) \end{cases}$$

Ce lemme permet de majorer la hauteur et le degré de $\hat{R}_m(T,Z)$ car ce polynôme apparait comme un résultant itéré. On en déduit alors la proposition suivante:

Proposition 4 ([De2]) *Avec les mêmes hypothèses sur les polynômes que la proposition 3 et si de plus $h(P_i) \leq C, \deg(P_i) \leq D$ pour $i = 1, ..., m$ et si $deg(F) \leq \delta$ où C, D, δ sont des réels alors*

$$\begin{cases} \deg(\hat{R}_m) & \leq & (2D)^m\delta \\ h(\hat{R}_m) & \leq & \delta D^{m-1}2^m C + D^m h(F) + 7m\delta^2(2D)^{2m} \end{cases}$$

En appliquant les résultats ci-dessus à $m = d = [K : k]$, $P_i(T, Y_i) = R^{\tau_i}(T, Y_i)$, $y_i = (ay)^{\tau_i}$, $i = 1, ..., d$, $F(T, Y_1, ..., Y_m, Z) = Y_1 + \cdots + Y_m - Z$, $\delta = deg(F) = 1$, $D = deg(R^{\tau_i}) = \deg(P)$, et $C = h(ay)$, on obtient

$$\begin{cases} \hat{R}_m(T, y_a) & = & 0 \\ \deg(\hat{R}_m) & \leq & (2D)^d \\ h(\hat{R}_m) & \leq & 2^d D^{d-1} C + 2(d+2)(2D)^{2d} \end{cases}$$

En utilisant la proposition 2 on obtient les majorations suivantes du degré et de la hauteur du polynôme P_k

$$(1) \begin{cases} \deg(P_k) & \leq & (2D)^d \\ h(P_k) & \leq & (2D)^d(C+2) + 4d(2D)^{2d} \end{cases}$$

Rappelons que C est la hauteur logarithmique de ay. Il reste donc à exprimer la hauteur de cet élément en fonction de a et de $h(y) = h(P)$. Il faut donc déterminer la hauteur du polynôme $R(T, Y)$ en fonction de celle de a et du polynôme $P(T, Y)$.

Si on note $a_{i,j}$ les coefficients des $a_i(T)$, qui sont des éléments de K, on a

$$H(ay) = (\prod_{v \in M_K} \sup_{i,j} |a^{n-i} a_{i,j}|_v)^{\frac{1}{[K:Q]}}$$

Or on a pour tout $v \in M_K$

$$sup_{i,j}|a^{n-i}a_{i,j}|_v \leq (sup_{i=1,...n}|a|_v^{n-i})(sup_{i,j}|a_{i,j}|_v)$$

et donc

$$H(ay) \leq (\prod_{v\in M_K} \max(1,|a|_v))^{\frac{n}{[K:Q]}} H(y) = H(a)^n H(y)$$

d'où

$$(2) \qquad C \leq nh(a) + h(y)$$

Il nous reste à majorer le terme $h(a)$ en fonction de $h(P)$ et de $\deg(P)$. On a vu que $a = n_1e_1 + \cdots + n_de_d$ avec $n_i \in \mathbf{Z}$ et $|n_i| \leq N$, on en déduit

$$\begin{cases} |a|_v \leq \max_{i=1,...,d} |e_i|_v & \text{si v est non archimédienne} \\ |a|_v \leq Nd \max_{i=1,...,d} |e_i|_v & \text{si v est archimédienne} \end{cases}$$

Et donc

$$(3) \begin{cases} h(a) \leq \log(Nd) + \sum_{v\in M_K} \log(\max(1,|e_i|_v)) \\ \qquad \leq \log(Nd) + h(1,e_1,...,e_d) \end{cases}$$

Il reste à choisir une base $(e_1,...,e_d)$ et à majorer le terme $h(1,e_1,...,e_d)$. On sait que $K = K_0(y_0)$ où K_0 est le corps engendré par les coefficients $a_{i,j}$ de $P(T,Y)$ sur k et y_0 est le terme constant de la série y. On sait aussi que y_0 est racine du polynôme $P(t_0,Y)$ avec la condition t_0 non racine du discriminant $\Delta(T)$ de $P(T,Y)$. Un au moins des nombres $0,1,...,\deg(\Delta)$ n'est pas racine de $\Delta(T)$. Donc on peut choisir $t_0 \in \{0,1,...,\deg(\Delta)\}$ tel que

$$(4) \qquad t_0 \leq \deg\Delta \leq (\deg(P))^2$$

Les éléments de la forme $a_{i,j}y_0^p$ où $0 \leq p \leq n-1$, $0 \leq i \leq n$, $0 \leq j \leq m$ forment une partie génératrice de l'espace vectoriel K sur k. On peut donc choisir les e_i parmi ces éléments. On a

$$P(t_0,Y) = \sum_{i=0}^{i=n} \sum_{j=0}^{j=m} a_{i,j}t_0^j Y^i$$

On note $|P_{t_0}|_v$ le maximum des valeurs absolues v-adiques des coefficients de $P(t_0,Y)$ et $|P|_v$ le maximum des valeurs absolues

v-adiques des coefficients de $a_{i,j}$ de $P(T,Y)$. En utilisant la forme locale de l'inégalité de Liouville ([La]; voir [De3, Ch1] pour la forme utilisée ici) on obtient

$$\begin{cases} |y_0|_v & \leq & |P_{t_0}| \leq |P|_v \max(1,|t_0|_v)^m \\ & \leq & |P|_v \max(1,|t_0|_v)^m \text{si } v \text{ est non archimédienne} \\ |y_0|_v & \leq & 2|P_{t_0}|_v \leq 2|P|_v \max(1,|t_0|_v)^m \\ & \leq & 2|P|_v \max(1,|t_0|_v)^m \text{si } v \text{ est archimédienne} \end{cases}$$

Les mêmes majorations valent pour les $a_{i,j}$ car $|a_{i,j}|_v \leq |P|_v$. On en déduit que

$$\begin{array}{rcl} h(1,e_1,...,e_d) & = & \frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} \log \max(1,|e_1|,...,|e_d|) \\ & \leq & \sum_{v \in S_\infty} \log(2|P|_v) + \frac{n}{[K:\mathbf{Q}]} \sum_{v \notin S_\infty} \log(|P|_v) \\ & & + \sum_{v \in M_K} m \log \max(1,|t_0|_v) \\ (5) & \leq & n(mh(t_0) + \log 2 + h(P)) \end{array}$$

Finalement, reportées dans (1), les inégalités (2)-(5) et $N = \frac{n(n-1)}{2}$ fournissent

$$\begin{cases} \deg(P_k) & \leq & (2D)^d \\ h(P_k) & \leq & 4d(2D)^{2d} h(P) \end{cases}$$

Ce qui prouve le Corollaire.

2.5 Application

2.5.1 Le principe global-local

Les résultats de la section précédente vont nous permettre de donner une forme effective du résultat suivant, démontré initialement dans [De1] où il est appelé principe global-local.

Proposition 5 (Dèbes [De1]) *Soit k un corps de nombres et $f : X \to \mathbf{P}_1$ un G-revêtement (i.e, un revêtement galoisien donné avec ses automorphismes) défini sur $\overline{\mathbf{Q}}$. Alors les propositions suivantes sont équivalentes:*

- k est le corps des modules de f.

- Le G-revêtement peut être défini sur tout k_v pour toute place v, sauf un nombre fini.

Supposons $k = \mathbf{Q}$ pour simplifier, on va donner une borne qui majore les nombres premiers p pour lesquels f n'est pas défini sur $\mathbf{Q}_p$.

2.5.2 Remarque

Le principe global-local a été récemment précisé. Soit f est un G-revêtement de corps des modules k. P. Dèbes et D. Harbater ont décrit précisement quels sont les nombres premiers exceptionnels pour lesquels le G-revêtement f peut ne pas être défini sur $\mathbf{Q}_p$. Ce sont les diviseurs premiers de l'ordre du groupe G et les nombres premiers p pour lesquels des points de ramification sont égaux modulo p [DeHa]. Dans un travail récent [Em] M. Emsalem étend ce résultat aux revêtements purs (i.e, non nécessairement galoisiens et sans leurs automorphismes). Ces résultats sont plus précis que celui que nous allons donner. Notre approche peut garder un intérêt cependant dans la mesure où elle fournit des modèles explicites. Nous la donnons rapidement.

2.5.3 Calcul de la borne

Rappelons le principe de la démonstration du résultat ci-dessus donnée dans [De1]. Supposons donné un G-revêtement $f : X \to \mathbf{P}_1$ défini sur $\overline{\mathbf{Q}}$ de corps des modules égal à $\mathbf{Q}$. Appelons $P(T,Y)$ le polynôme minimal d'un élément primitif sur $\overline{\mathbf{Q}}$ du corps de fonction $\overline{\mathbf{Q}}(X)$ de f tel que y soit entier sur $\overline{\mathbf{Q}}[T]$. D'après le théorème de Coombes-Harbater, f a un modèle défini sur $\mathbf{Q}$ en tant que simple revêtement, à savoir celui donné par le polynôme $P_{\mathbf{Q}}(T,Y)$ du Théorème 2. On choisit $t_0 \in \mathbf{Z}$ non racine du discriminant $\Delta(T)$ de $P_{\mathbf{Q}}(T,Y)$ et on note $\Delta = \Delta(t_0)$ le discriminant de $P(t_0,Y)$.

Soit p un nombre premier ne divisant pas Δ. D'après le lemme de Hensel, les racines de $P_{\mathbf{Q}}(t_0,Y)$ engendrent des extensions non ramifiées de $\mathbf{Q}_p$, on peut alors conclure que le G-revêtement f est défini sur $\mathbf{Q}_p$. En effet on note $\mathbf{Q}_p^{nr}$ l'extension algébrique non ramifée maximale de $\mathbf{Q}_p$. Si on étend les scalaires à $\overline{\mathbf{Q}_p}$, le G-revêtement f a pour corps des modules $\mathbf{Q}_p$. De plus, le polynôme $P_{\mathbf{Q}}(T,Y)$ induit

un modèle $f_{\mathbf{Q}}$ de f dont la fibre au-dessus de t_0 ne consiste qu'en des points $\mathbf{Q}_p^{nr}$-rationnels: cela fait de $f_{\mathbf{Q}}$ un modèle défini sur $\mathbf{Q}_p^{nr}$ comme G-revêtement. Le groupe $G(\mathbf{Q}_p^{nr}/\mathbf{Q}_p)$ étant projectif, on peut conclure, en utilisant le lemme 8.2 de [De1], que le G-revêtement f est défini sur $\mathbf{Q}_p$.

Déterminons une majoration de $\Delta(t_0)$. On a vu que l'on pouvait choisir t_0 parmi $0, 1, ..., \deg \Delta$ pour que t_0 ne soit pas racine de $\Delta(T)$. On a d'autre part

$$h(\Delta(t_0)) \leq h(\Delta) + h(t_0) + \log(\deg(\Delta))$$

et donc

$$(1) \quad |\Delta(t_0)| \leq \deg(\Delta) e^{\deg(\Delta) h(\Delta)}.$$

En utilisant les inégalités du corollaire ainsi que (1), on obtient

$$|\Delta(t_0)| \leq 2(2D)^d e^{20d(2D)^{4d} h(P)}.$$

On peut donc conclure que le G-revêtement f est défini sur $\mathbf{Q}_p$ pour tout nombre premier p vérifiant

$$p > 2(2D)^d e^{20d(2D)^{4d} h(P)}.$$

Chapitre 3

Descente dans le cas général

Soit k un corps de caractéristique 0 et F/k une extension galoisienne (éventuellement de degré infini). On considère un revêtement $f : X \to B$ défini sur F. Avec les mêmes hypothèses qu'au chapitre 1, cela équivaut à se donner une extension $E/F(B)$ algébrique de degré fini. On supposera que k est le corps des modules de cette extension. L'extension $E/F(B)$ donne lieu à la suite exacte:

$$1 \to \mathrm{Aut}(E/F(B)) \to \mathrm{Aut}(E/k(B)) \to G(F/k) \to 1$$

Le théorème 1 montre qu'il existe une section $\chi : G(F/k) \to \mathrm{Aut}(E/k(B))$ si et seulement si le revêtement f est défini sur k. En termes de corps des fonctions cela signifie qu'il existe une extension $E_k/k(B)$ tel que $E_kF = E$ et $E_k \cap F = k$. Pour le reste de ce chapitre, on suppose que k est effectivement un corps de définition et on se fixe une section $\chi : G(F/k) \to \mathrm{Aut}(E/k(B))$. On sait de plus que le k-modèle correspondant E_k est le sous-corps de E fixé par l'image de la section χ:

$$E_k = E^{Im\chi}$$

L'objet de ce chapitre est de donner une construction effective de ce k-modèle. Plus précisément, on va déterminer un élément primitif de E_k. On va procéder en deux temps, suivant que l'extension F/k est finie ou pas.

3.1 Descente dans le cas fini

Dans un premier cas nous supposerons que l'extension F/k est galoisienne de degré fini. Les données du problème sont les suivantes:

- On note y un élément primitif de $E/F(B)$.
- $G(F/k) = \{\tau_1, \ldots, \tau_d\}$ est un groupe fini d'ordre d.
- $Im(\chi) = \{\chi(\tau_1), \ldots, \chi(\tau_d)\}$ est un sous groupe d'ordre d de $\mathrm{Aut}(E/k(B))$.

Théorème 4 *Si F/k est une extension galoisienne de degré fini. Il existe $a \in F$ tel que $y_a = \sum_{i=1}^{i=d} (ay)^{\chi(\tau_i)}$ soit un élément primitif de E_k sur $k(B)$*

Comme $Im(\chi) \subset \mathrm{Aut}(E/k(B))$ on a $(ay)^{\chi(\tau_i)} \in E$ pour tous $a \in F$ et tous $\chi(\tau_i) \in Im(\chi)$, donc $y_a \in E$. De plus $(y_a)^{\chi(\tau_i)} = y_a$ pour tous $\chi(\tau_i) \in Im(\chi)$ donc $y_a \in E_k$, pour tout $a \in F$. Notons $\sigma_1, ..., \sigma_n$ les $F(B)$-plongements distincts de E dans une clôture algébrique $\overline{k(B)}$ de E. Pour démontrer le théorème 4, il suffit de trouver $a \in F$ tel que les conjugués $\sigma_i(y_a)$ soient deux à deux distincts.

On se fixe d'abord deux plongements distincts σ_l, σ_k. On pose $c_i = \sigma_l(y^{\chi(\tau_i)}) - \sigma_k(y^{\chi(\tau_i)})$ pour tout $\chi(\tau_i) \in Im(\chi)$. La famille (c_i) pour $i = 1, ..., d$ est une famille d'éléments de $\overline{k(B)}$ non réduite à 0 car si on prend $\tau_1 = 1$ on a alors $\chi(1) = 1$ et donc $c_1 = \sigma_l(y) - \sigma_k(y) \neq 0$. On utilise alors le lemme suivant, qu'il faut voir comme une variante du Théorème de Dedekind.

Lemme 5 *L'homomorphisme $\sum_{i=1}^{i=d} c_i\chi(\tau_i) : F \to \overline{k(B)}$ qui à $a \in F$ associe $\sum_{i=1}^{i=d} c_i a^{\chi(\tau_i)}$ est non nul.*

Preuve du lemme:

On fait un raisonnement par l'absurde. On suppose qu'il existe une relation de longueur minimale non nulle $\sum_{i\in I} c_i\chi(\tau_i) = 0$. On aurait alors pour tous $a, b \in F$

$$\sum_{i\in I} c_i a^{\chi(\tau_i)} = 0 \text{ et } \sum_{i\in I} c_i (ab)^{\chi(\tau_i)} = 0$$

On a donc pour tous $a, b \in F$ et pour $s \in I$ fixé

$$\sum_{i \in I} c_i a^{\chi(\tau_i)} b^{\chi(\tau_i)} - \sum_{i \in I} c_i a^{\chi(\tau_i)} b^{\chi(\tau_s)} = 0$$

Ce qui permet de dire que pour tous $a, b \in F$ on a

$$\sum_{i \in I - \{s\}} c_i (b^{\chi(\tau_i)} - b^{\chi(\tau_s)}) a^{\chi(\tau_i)} = 0$$

Par minimalité de la première relation on en déduit alors que les coefficients $b^{\chi(\tau_i)} - b^{\chi(\tau_s)}$ de la dernière relation sont tous nuls pour tout $b \in F$. Ce qui contredit le fait que les homomorphismes $\chi(\tau_i)$ sont distincts sur F. Ce qui prouve le lemme.

En utilisant le lemme il existe $a \in F$ tel que $\sum_{i=1}^{i=d} c_i a^{\chi(\tau_i)} \neq 0$. En remplaçant c_i on obtient

$$\sum_{i=1}^{i=d} (\sigma_l(y^{\chi(\tau_i)}) - \sigma_k(y^{\chi(\tau_i)})) a^{\chi(\tau_i)} \neq 0$$

$$\sum_{i=1}^{i=d} \sigma_l(y^{\chi(\tau_i)}) a^{\chi(\tau_i)} \neq \sum_{i=1}^{i=d} \sigma_k(y^{\chi(\tau_i)}) a^{\chi(\tau_i)}$$

$$\sum_{i=1}^{i=d} \sigma_l(ay)^{\chi(\tau_i)} \neq \sum_{i=1}^{i=d} \sigma_k(ay)^{\chi(\tau_i)}$$

$$\sigma_l(y_a) \neq \sigma_k(y_a).$$

On voit que le lemme permet de prouver l'existence d'un élément $a \in F$ tel que $\sigma_l(y_a) \neq \sigma_k(y_a)$. Cet élément dépend du choix des plongements σ_l, σ_k. Cependant, par le raisonnement habituel suivant, on peut trouver $a \in F$ indépendant de l et k. Le lemme montre que pour $l \neq k$ l'ensemble $V_{\sigma_l,\sigma_k} = \{a \in F / \sigma_i(y_a) = \sigma_j(y_a)\}$ est un sous k-espace de F strictement inclus dans celui-ci. Le corps k étant infini, il existe $a \in F$ n'appartenant à aucun des sous-espaces V_{σ_l,σ_k} où $1 \leq l < k \leq n$. Ce qui prouve l'existence de $a \in F$ tel que tous les conjugués de y_a soient distincts et donc le théorème est démontré.

3.2 Cas général

Essentiellement, on va se ramener au cas précédent. L'idée de départ est de dire que l'extension $E/F(B)$ admet un F_o-modèle $E_{F_o}/F_o(B)$ avec F_o/k une sous extension finie de F/k. Il y a cependant une difficulté: n'importe quel F_o-modèle ne conviendra pas. En effet il n'est pas nécessaire que la descente de F_o à k soit possible bien que celle de f à k le soit: si $E_k/k(B)$ est un k-modèle, il peut arriver que l'extension $E_k \otimes_k F_o(B)$ ne soit pas isomorphe à $E_{F_o}/F_o(B)$ sur $F_o(B)$; les deux extensions sont isomorphes sur $F(B)$ (après extensions des scalaires), mais l'isomorphisme n'est pas forcément défini sur F_o. Autrement dit, il peut arriver que la descente de F à k soit possible mais qu'elle ne passe pas par n'importe quel F_o-modèle.

Théorème 5 (Cas général) *On suppose donnée une section* χ : $G(F/k) \to Aut(E/k(B))$ *continue.*

(a) Il existe des sous-extensions galoisiennes finies F_o/k *de* F/k *pour lesquelles il existe un* F_o*-modèle* $E_{F_o}/F_o(B)$ *de* $E/F(B)$ *et un homomorphisme* $\chi_o : G(F_o/k) \to Aut(E_{F_o}/k(B))$ *rendant commutatif le diagramme:*

$$\begin{array}{ccc} & \chi & \\ G(F/k) & \to & Aut(E/k(B)) \\ p\downarrow & & \downarrow \\ G(F_o/k) & \to & Aut(E_{F_o}/k(B)) \end{array}$$

(b) Soient F_o, E_{F_o} *et* χ_o *comme ci-dessus. Soit* y *un élément primitif de* $E_{F_o}/F_o(B)$ *alors il existe* $a \in F_o$ *tel que* $y_a = \sum_{\tau \in G(F_o/k)} a^\tau y^{\chi_o(\tau)}$ *soit un élément primitif de* $E_k/k(B)$.

Remarque:
Tout modèle défini sur une sous-extension finie de k ne convient pas nécessairement pour (a). En particulier, on sait qu'il existe au moins un k-modèle $E_k/k(B)$. Si la conclusion de (a) est valable avec ce k-modèle et donc pour $F_o = k$, nécessairement $\chi(\tau)$ est l'identité sur E_k pour tout $\tau \in G(F/k)$. Cela n'est pas vrai en général: on prend E_k l'extension donnée par le polynôme $Y^2 + 1 +$

$T = 0$ et $\chi : G(\overline{k}/k) \to \mathrm{Aut}(E/k(T))$ donné par l'action de $G(\overline{k}/k)$ sur les éléments de E vu comme sous-corps de $\overline{k}((T))$ engendré par $i\sqrt{1+T} = i + \frac{iT}{2} + ...$

Preuve du Théorème 5

(a) Soient K_o/k une sous-extension finie de F/k et $E_{K_o}/K_o(B)$ un K_o-modèle de $E/F(B)$. Soit y un élément primitif de l'extension $E_{K_o}/K_o(B)$ i.e $(E_{K_o} = K_o(B)(y))$. L'élément y n'a qu'un nombre fini de conjugués sur $k(B)$. Nous en tirons deux conséquences:

- L'ensemble $I_y = \{\tau \in G(F/K_o)/\chi(\tau)(y) = y\}$ est un sous-groupe d'indice fini de $G(F/K_o)$. Le sous corps fixé F^{I_y} est donc de degré fini sur K_o et donc sur k.

- Il existe une extension finie L_o/K_o tel que pour tout $\tau \in G(F/K_o)$, $\chi(\tau)(y) \in L_o(B)(y)$. (Puisque $\chi(\tau)(E) = E$ et $E = FE_{K_o} = F(B)(y)$, on sait a priori que $\chi(\tau)(y) \in F(B)(y)$).

Soient F_o la clôture galoisienne sur K_o du corps $F^{I_y}L_o$ et $E_{F_o} = F_oE_{K_o} = F_o(B)(y)$. Pour tout $\tau \in G(F/k)$ quelconque, on a

$$\chi(\tau)(E_{F_o}) = \chi(\tau)(F_o(B)(y)) = F_o(B)(\chi(\tau)(y)) = F_o(B)(y) = E_{F_o}.$$

(la dernière égalité résultant de $\chi(\tau)(y) \in L_o(B)(y) \subset F_o(B)(y)$).

Donc $\chi(\tau)$ induit un automorphisme de l'extension $E_{F_o}/k(B)$. D'autre part, si $\tau \in G(F/k)$ est l'identité sur F_o, alors $\tau \in I_y$ (puisque $F^{I_y} \subset F_o$ et I_y est fermé (car χ est continu)) et donc $\chi(\tau)(y) = y$ ce qui donne que $\chi(\tau)$ est l'identité sur $F_o(B)(y)$. L'homomorphisme

$$\begin{array}{c} G(F/k) \to \mathrm{Aut}(E_{F_o}/k(B)) \\ \tau \longmapsto \chi(\tau)|E_{F_o} \end{array}$$

se factorise donc par $G(F_o/k)$ pour donner le résultat voulu.

(b) Soit $a \in F_o$ arbitraire. Il est clair que y_a est dans $F_o(B)(y) \subset E$. Montrons que $y_a \in E_k = E^{Im\chi}$. Soit $\sigma \in G(F/k)$. On a

$$\begin{array}{rcl} \chi(\sigma)(y_a) & = & \sum_{\tau \in G(F_o/k)} (a^\tau)^{\chi(\sigma)} (y^{\chi_o(\tau)})^{\chi(\sigma)} \\ \chi(\sigma)(y_a) & = & \sum_{\tau \in G(F_o/k)} (a^\tau)^\sigma y^{\chi(\sigma)\chi_o(\tau)} \\ \chi(\sigma)(y_a) & = & \sum_{\tau \in G(F_o/k)} (a^\tau)^{p(\sigma)} (y^{\chi_o(p(\sigma))\chi_o(\tau)}) \\ \chi(\sigma)(y_a) & = & \sum_{\tau \in G(F_o/k)} a^{p(\sigma)\tau} y^{\chi_o(p(\sigma)\tau)} \\ \chi(\sigma)(y_a) & = & y_a \end{array}$$

La fin de la preuve (b) se fait comme pour le cas fini en remplaçant F par F_o. Ce qui prouve le théorème.

Remarques:

(1) Effectivité des théorèmes 4 et 5.

Les théorèmes 4 et 5 donnent une formule explicite pour un élément primitif d'un k-modèle $E_k/k(T)$ de l'extension de départ. Ce résultat n'est cependant pas aussi satisfaisant que celui du théorème 3 dans le cas galoisien. Les théorèmes 4 et 5 ne sont vraiment effectifs qu'à partir du moment où on connait explicitement une section χ et un F_o-modèle $E_{F_o}/F_o(B)$ comme dans le théorème 5.

(2) Le cas galoisien en suivant l'approche générale.

Le théorème de Coombes-Harbater se déduit assez directement, dans sa partie qualitative du théorème 1 du Ch.1. Rappelons que pour montrer que le corps des modules k de l'extension $E/\overline{k}(T)$, supposée galoisienne, est un corps de définition, il suffit de montrer que l'épimorphisme

$$\mathrm{Aut}(E/k(T)) \to G(\overline{k}/k)$$

admet une section. Pour tout $t_o \in k$, non ramifié dans l'extension $E/\overline{k}(T)$ le corps E se plonge dans $\overline{k}((T-t_o))$. D'autre part, tout élément $\tau \in G(\overline{k}/k)$ se prolonge naturellement en un k-automorphisme de $\overline{k}((T-t_o))$; on dispose donc d'un monomorphisme

$$G(\overline{k}/k) \to \mathrm{Aut}(\overline{k}((T-t_o))).$$

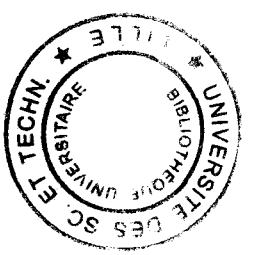
Enfin, le fait que k est le corps des modules, combiné au fait que $E/\overline{k}(T)$ est galoisien entraine que l'action de tout $\tau \in G(\overline{k}/k)$ sur E via le plongement $E \hookrightarrow \overline{k}((T-t_o))$ vérifie $E^\tau = E$. La flèche précédente induit donc un monomorphisme

$$\chi : G(\overline{k}/k) \to \mathrm{Aut}(E/k(T))$$

qui est clairement une section de la surjection de départ. De plus, dans ce cas la section χ est connue explicitement: pour tout $\tau \in G(\overline{k}/k)$, $\chi(\tau)$ opère sur E en agissant sur les coefficients des séries formelles représentant les éléments de E via un plongement $E \hookrightarrow \overline{k}((T-t_o))$. De plus il y a naturellement un F_o-modèle $E_{F_o}/F_o(T)$ comme dans le $a)$ du théorème 5. En effet, soient y un élément

primitif de l'extension $E/\overline{k}(T)$ et E_{F_o} la clôture normale du corps engendré sur k par les coefficients de la série représentant y dans $E \subset \overline{k}((T-t_o))$. L'extension $F_o(T,y)/F_o(T)$ est un F_o-modèle de l'extension $E/\overline{k}(T)$ vérifiant (a). (La régularité provient de $F_o(T,y) \cap \overline{k} \subset F_o((T-t_o)) \cap \overline{k} = F_o$). Si on applique la formule du théorème 5 dans ce contexte, on retrouve la formule du théorème 3 du chapitre 2.

Références

[CoHa] K. Coombes and D. Harbater, Hurwitz families and arithmetic surfaces, Duke Math. J., **52** (1985), 821-839.
[Cou] J-M. Couveignes, Quelque revêtements défini sur $\mathbf{Q}$, Manuscripta Mathematica, **94/4**, (1997), 409-445.
[CouGr] J-M. Couveignes and L. Granboulan, Dessins from a geometric point of view, in The grothendieck theory of Dessins d'enfants, Leila Schneps ed., Camb. U. Press, (1995), 79-113.
[De1] P. Dèbes , G-covers of $\mathbf{P_1}$ over the p-adics , Contemporary Mathematics ,**186**, 217-238 , (1995).
[De2] P. Dèbes , Hilbert subsets and s-integral points , Manuscripta mathematica , **89** , 107-137, (1996).
[De3] P. Dèbes, Valeurs algébriques de fonctions algébriques et théorème d'irréductibilité de Hilbert, Thèse 3ème cycle, Publ. Univ. Paris 6, (1984).
[DeDes] P. Dèbes and B. Deschamps, The regular inverse Galois problem over large fields, London Math. Soc., Lecture note series **243**, in geometric galois action 2, Edited by P. Lochak and L. Schneps, 119-138.
[DeDo1] P. Dèbes et J-C. Douai, Algebraic covers: field of moduli versus field of definition, Ann. Sci. E.N.S., 4^e série, **30**, (1997), 303-338.
[DeDo2] P. Dèbes et J-C. Douai, Local-global principles for algebraic covers, Israel J. Math., **103**, (1998), 237-257.
[DeEm] P Dèbes and M. Emsalem, On fields of moduli of curves, Journal of algebra **211**, 42-56, (1999).
[DeHa] P. Dèbes and D. Harbater , Fields of definition of p-adics covers, J. fur die reine und angen. Math., **498** (1998), 223-236
[Em] M. Emsalem, On reduction of covers of arithmetic surfaces, preprint, (1997).
[Dew] E. Dew, Fields of moduli of arithmetic covers, Thesis, (1991).
[Fr] M. Fried, Fields of definition of function fields and Hurwitz families, groups as Galois groups, Communication in Algebra **1** (1997), 17-82.
[FrJa] M. Fried and M. Jarden , Field arithmetic, Springer Verlag, (1986).

[La] S. Lang , Fundamentals of diophantine geometry , Springer Verlag (1983).
[Mat] B.H Matzat, Kontruktive Galoistheorie ,LNM **1284**, Spinger, (1987).
[MatMa] B.H Matzat and G. Malle, Inverse Galois theorie, (1996).
[Pop] F. Pop, Embedding problems over large fields, Annals of math., **144**, 1-35, (1996).
[Se] J.-P. Serre, Topics in Galois theory, Notes written by Henry Darmon, Jones and Bartlett Publ., Boston, (1992).
[Sh] G. Shimura, On field of rationality for an abelian variety, Nagoya Math. J. **45**,(1971), 167-178.
[We] A. Weil , The field of definition of a variety , Oeuvres complètes (Collected papers) , Springer-Verlag , 291-306.
[Wo] J. Wolfart, the "obvious" part of Belyi's theorem and Riemann surfaces with many automorphisms, preprint, (1995).