N. d'ordre 40546

Université Lille 1 Sciences et Technologies

Thèse de doctorat de Mathématiques Pures

SPÉCIALISATIONS DE REVÊTEMENTS GALOSIENS

Nour GHAZI

soutenue le 30 septembre 2011 devant le jury constitué de :

Jean-Marc COUVEIGNES (Univ. Bordeaux 1).

Pierre DÈBES (Univ. Lille 1), directeur de thèse.

Bruno DESCHAMPS (Univ. du Maine).

Jean-Claude Douai (Univ. Lille 1).

Michel EMSALEM (Univ. Lille 1).

David HARARI (Univ. Paris-Sud, Orsay), rapporteur.

Umberto ZANNIER (Scuola Normale superiore di Pisa), rapporteur.

SPÉCIALISATIONS DE REVÊTEMENTS GALOISIENS

.

SPÉCIALISATIONS DE REVÊTEMENTS GALOISIENS

TABLE DES MATIÈRES

ABSTRACT

We are interested in some open questions concerning the specialization of Galois covers. The starting point is the Beckmann-Black problem. This problem asks whether a given finite Galois extension E/K of group G is the specialization of some Galois cover $f : X \to \mathbb{P}^1$ of group G defined over K at some point $t_0 \in K$? The first result is a local conclusion : if S is a finite set of finite places of K, we can find a Galois cover f of group G defined over a finite extension L/K such that for all $v \in S$, L/K is totally split in K_v and the specialization of the cover f, after scalar extension to $L_v = K_v$, is a Galois extension isomorphic to EL_v/L_v (at the same point t_0). It can be further required that f, extended to L, specializes to some Galois extension of group G isomorphic to EL/L (at the same point t_0). The second result is the same statement but with extensions EK_v/K_v replaced by local extensions E^v/K_v which do not necessarily come from a global extension E/K ; we assume that they are unramified of group $H_v \subset G$. With some hypotheses on the residue fields, this second result is related to the problem of Grunwald. The third result combines a conclusion on the Grunwald problem for arbitrary groups, an effective version of Hilbert's irreducibility theorem and a statement on the regular inverse Galois problem.

RÉSUMÉ

Dans ce travail, on s'intéresse à des questions concernant la spécialisation de revêtements galoisiens. Le point de départ est le problème de Beckmann-Black. Etant donnée une extension galoisienne E/K de groupe G, existe-t-il un revêtement galoisien $f : X \to \mathbb{P}^1$ de groupe G défini sur K qui se spécialise en E/K en un point $t_0 \in K$? Un premier résultat est une réponse locale : si S est un ensemble fini de places finies de K, on peut trouver un revêtement galoisien f de groupe G, défini sur une extension finie L/K tel que pour $v \in S$, L/K est totalement décomposée dans K_v et le revêtement f, étendu à $L_v = K_v$, se spécialise en EK_v/K_v en un point $t_0 \in K$ (fixé à l'avance). On peut demander en plus que f, vu sur L, se spécialise en une extension de groupe G isomorphe à EL/L (au même point t_0). Un deuxième résultat correspond à l'énoncé similaire mais avec les extensions EK_v/K_v remplacées par des extensions locales E^v/K_v plus générales, qui ne proviennent pas forcément d'une extension globale E/K; on suppose qu'elles sont de groupe $H_v \subset G$ et sont non ramifiées. Il y a pour ce deuxième résultat des hypothèses sur les corps résiduels. Ce deuxième énoncé est relié au problème de Grunwald. Le troisième résultat est lié à l'énoncé précédent ; il combine une conclusion de type Grunwald-Wang pour les groupes arbitraires, une version effective du théorème d'irréductibilité de Hilbert et un énoncé sur le problème inverse de Galois régulier.

INTRODUCTION

Les travaux que nous présentons dans cette thèse concernent la théorie inverse de Galois. Historiquement, le Problème Inverse de Galois est l'étude de l'énoncé suivant :

Enoncé IGP : *Étant donné un groupe fini G, il existe une extension galoisienne $E/\mathbb{Q}$ telle que* $\mathrm{Gal}(E/\mathbb{Q}) = G$.

Un argument classique de spécialisation dû à Hilbert montre que **IGP** est une conséquence de l'énoncé suivant qui constitue le Problème Inverse de Galois sous sa forme Régulière :

Enoncé RIGP : *Si G est un groupe fini, alors il existe une extension galoisienne $F/\mathbb{Q}(T)$ régulière sur $\mathbb{Q}$ (*i.e. $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$*) telle que* $\mathrm{Gal}(F/\mathbb{Q}(T)) = G$.

En effet, d'après le *théorème d'irréductibilité de Hilbert*, il existe une infinité de points $t_0 \in \mathbb{Q}$ tels que l'extension spécialisée de $F/\mathbb{Q}(T)$ en t_0, notée $F_{t_0}/\mathbb{Q}$, soit une extension galoisienne de $\mathbb{Q}$ de groupe G.

Les résultats de la thèse sont liés à ces problèmes et à cette approche. Ainsi on peut se demander si toute extension galoisienne de $\mathbb{Q}$ de groupe G donné provient par spécialisation d'une extension galoisienne de $\mathbb{Q}(T)$ de groupe G et régulière sur $\mathbb{Q}$; la stratégie par spécialisation serait alors optimale. Cette nouvelle question s'appelle le problème de Beckmann-Black :

Enoncé BB : *Étant donnés un groupe fini G et une extension galoisienne $E/\mathbb{Q}$ de groupe G, il existe une extension galoisienne $F/\mathbb{Q}(T)$ régulière sur $\mathbb{Q}$ de groupe G telle que sa spécialisation en un point $t_0 \in \mathbb{Q}$ soit isomorphe à $E/\mathbb{Q}$.*

On sait qu'une réponse positive au problème de Beckmann-Black **BB** (étendu à tout corps K à la place de $\mathbb{Q}$) implique une réponse positive au problème inverse de Galois régulier **RIGP** (Dèbes [**Dèb99**]). Nous renvoyons à l'introduction du chapitre 2 pour d'autres commentaires sur ce problème.

Notre premier résultat est une forme faible de l'énoncé **BB**, qui combine une conclusion locale et une conclusion globale. Plus exactement, on fixe un groupe fini G, un point $t_0 \in \mathbb{Q}$ et une extension $E/\mathbb{Q}$ galoisienne de groupe G. On montre alors que, pour tout ensemble fini S de nombres premiers p, il existe un corps de nombres L totalement décomposé dans $\mathbb{Q}_p$, pour tout $p \in S$, et une extension galoisienne $F/L(T)$ régulière sur L de groupe G telle que :

(1) l'extension spécialisée de $F/L(T)$ en t_0 est une extension galoisienne de groupe G isomorphe à EL/L.
(2) $F_{t_0}\mathbb{Q}_p/\mathbb{Q}_p \cong E\mathbb{Q}_p/\mathbb{Q}_p$, pour tout $p \in S$.

Au vu de la condition (2), on peut se demander si on peut obtenir un énoncé similaire où les extensions locales $E\mathbb{Q}_p/\mathbb{Q}_p$ sont remplacées par des extensions plus générales $E^p/\mathbb{Q}_p$ (ne provenant pas d'une extension donnée $E/\mathbb{Q}$). C'est ce que nous faisons dans la deuxième partie de cette thèse qui est une collaboration avec mon directeur de thèse P. Dèbes. La question est reliée au problème de Grunwald qui porte sur l'énoncé suivant :

Enoncé Gr : *Étant donnés un groupe fini G et un ensemble fini de nombres premiers p donnés avec des extensions galoisiennes $E^p/\mathbb{Q}_p$ de groupe $H_p \subset G$, il existe une extension galoisienne $E/\mathbb{Q}$ de groupe G telle que $E\mathbb{Q}_p/\mathbb{Q}_p \cong E^p/\mathbb{Q}_p$ pour tout $p \in S$.*

Nous renvoyons à l'introduction du chapitre 3 pour plus de commentaires sur le problème de Grunwald.

Pour des raisons techniques, nous nous intéressons au *problème de Grunwald non-ramifié i.e.* on suppose que les extensions $E^p/\mathbb{Q}_p$ sont galoisiennes et non-ramifiées.

Notre résultat principal établit un lien entre le problème de Grunwald non-ramifié et le théorème d'irréductibilité de Hilbert. On obtient le théorème suivant. Pour tout groupe fini G, il existe une constante m ne dépendant que de G telle que : pour tout ensemble fini S de nombres premiers $p \geq m$ donnés avec des extensions locales $E^p/\mathbb{Q}_p$ non-ramifiées ($p \in S$), il existe un corps de nombres L totalement décomposé dans $\mathbb{Q}_p$ ($p \in S$) et une extension galoisienne $F/L(T)$ de groupe G régulière sur L vérifiant la propriété suivante, que nous appelons "propriété de Hilbert-Grunwald" :

(H-Gr) *Il existe une infinité de points $t_0 \in \mathbb{Q}$ telle que l'extension spécialisée de $F/\mathbb{Q}(T)$ en t_0 satisfait les deux conclusions suivantes :*

(1) *$F_{t_0}/\mathbb{Q}$ est une extension galoisienne de groupe G.*
(2) *$F_{t_0}\mathbb{Q}_p/\mathbb{Q}_p \cong E_p/\mathbb{Q}_p$, pour tout $p \in S$.*

On montre de plus que L peut-être pris égal à $\mathbb{Q}$ lui-même si on dispose d'une extension $F/\mathbb{Q}(T)$ de groupe G, régulière sur $\mathbb{Q}$; nous montrons en fait que la propriété **(H-Gr)** est satisfaite pour toute telle extension $F/\mathbb{Q}(T)$ (la constante m dépendant alors de $F/\mathbb{Q}(T)$).

Nous donnons ensuite quelques applications de ces résultats. Nous apportons notamment quelques précisions à l'énoncé **RIGP** sur $\mathbb{Q}_p$. On sait qu'il est vrai d'après Harbater, nous pouvons ajouter que, pour p assez grand (comparé à $|G|$), il existe des réalisations $F/\mathbb{Q}_p(T)$ qui ont bonne réduction. Nous donnons aussi une condition nécessaire liée à des questions analytiques en théorie des nombres (formes effectives du théorème de Čebotarev) pour que l'énoncé **RIGP** soit vrai sur $\mathbb{Q}$ pour un groupe fini G donné.

Cette thèse se décompose en trois chapitres. Dans le premier, on donne les outils dont on a besoin dans la suite de ce travail. On s'intéresse, dans le chapitre 2, au problème de Beckmann-Black : on introduit ce problème et on montre notre premier résultat. On présente dans le chapitre 3 le problème de Hilbert-Grunwald et on donne une preuve de notre deuxième résultat et de ses applications.

Remerciements.— Je remercie chaleurement mon directeur de thèse professeur Pierre Dèbes d'avoir accepté d'encadrer ce travail de thèse. Pour sa patience... son aide... sa connaissance... ses précieux conseils... et ses encouragements, j'exprime mes profonds remerciements à mon prof Pierre Dèbes. Je voudrais remercier aussi les rapporteurs de cette thèse d'avoir pris sur leur précieux temps pour juger ce travail. Je tiens aussi à remercier l'ensemble des membres du jury pour avoir accepté de participer à la soutenance de ma thèse.

CHAPITRE 1

PRÉLIMINAIRES

Soient K un corps, G un groupe fini et B une variété lisse projective géométriquement intègre définie sur K. On note $\overline{K}$ la clôture algébrique de K et K^{sep} sa clôture séparable. On note $K((T))$ le corps des séries formelles de Laurent à coefficients dans K et on note G_K le groupe de Galois absolu de K. Pour plus de détails sur ce chapitre, voir [**Dèb09**, chapter 3] et [**DD97**].

1.1. Invariants des revêtements

Rappelons qu'un revêtement $f : X \to B$ défini sur K est un morphisme fini défini sur K, étale au-dessus d'un ouvert non vide de B avec X une variété normale géométriquement irréductible.

1.1.1. Corps de base algébriquement clos. — Supposons que K soit algébriquement clos.

1.1.1.1. Généralités. — Il y a une correspondance bijective entre les revêtements et les extensions de corps des fonctions (à isomorphisme près) : à un revêtement $f : X \to B$, on associe l'extension finie séparable $K(X)/K(B)$ des corps de fonctions de X et de B et inversement, à une extension finie séparable $F/K(B)$, on associe le morphisme $X \to B$ obtenu en normalisant B dans F; le morphisme $X \to B$ est fini [**Mil80**, prposition 1.1] et on vérifie que ces deux correspondances sont inverse l'une de l'autre. Pour simplifier les notations, on note $F := K(X)$ et $\widehat{F}/K(B)$ la clôture galoisienne de $F/K(B)$. On associe à $F/K(B)$ les invariants suivants :

- son degré : $d = [F : K(B)]$.
- son groupe : le groupe $\text{Gal}(\widehat{F}/K(B))$. On peut voir ce groupe comme plongé dans S_d. En effet, le groupe $\text{Gal}(\widehat{F}/K(B))$ opère fidèlement sur

les d-plongements de F dans $K(B)^{\text{sep}}$. En numérotant ces différents plongements, on peut voir $\text{Gal}(\widehat{F}/K(B))$ comme sous-groupe de S_d. De plus, si le revêtement f est galoisien *i.e.* $F/K(B)$ est une extension galoisienne, alors l'action $\text{Gal}(F/K(B)) \to S_d$ est l'action par translation à gauche, qu'on appelle la *représentation régulière à gauche* de $\text{Gal}(F/K(B))$.

- son diviseur de branchement D : la somme formelle des diviseurs premiers[(1)] de B qui sont ramifiées dans le revêtement $f : X \to B$. On suppose que D est à croisements normaux. Cela assure que f est plat.

1.1.1.2. Cas $B = \mathbb{P}^1$. — Dans ce cas, on note plus simplement $\mathbf{t} = \{t_1, \ldots, t_r\}$ le diviseur de branchement. Si, de plus, la caractéristique de K est 0, on peut également introduire le type de ramification :

On fixe un système cohérent $(\zeta_n)_{n\geq 1}$ de racines de l'unité *i.e.* ζ_n est une racine n-ième primitive de l'unité et $\zeta_{nm}^n = \zeta_m$, pour tous $n, m \geq 1$. Si l'extension $F/K(T)$ est galoisienne de groupe G, pour tout $j = 1, \ldots, r$, on peut associer une classe de conjugaison C_j du groupe G de la façon suivante. Les groupes d'inertie associés à t_j sont conjugués et cycliques d'ordre égal à l'indice de ramification e_j de t_j dans $F/K(T)$. Fixons I_j un de ces groupes d'inertie. On dit que $\sigma \in I_j$ est un *générateur distingué* de I_j si $\frac{\sigma(\pi)}{\pi} = \zeta_{e_j}$, où $\pi = (T - t_j)^{\frac{1}{e_j}}$ et σ est vu comme un élément du groupe de Galois de l'extension $FK((T-t_j)) = K((T-t_j))^{\frac{1}{e_j}}$ de $K((T-t_j))$. Les générateurs distingués des groupes d'inertie au-dessus de t_j sont dans la même classe de conjugaison C_j de G. L'uplet non ordonné $\mathbf{C} = \{C_1, \ldots, C_r\}$ (avec des répétitions éventuelles) est appelé *le type de ramification* de $F/K(T)$.

Dans le cas où l'extension $F/K(T)$ n'est pas galoisienne, le type de ramification est défini comme étant celui de sa clôture galoisienne $\widehat{F}/K(T)$ et les classes de conjugaison sont les classes induites par les classes C_i dans S_d via le plongement de $\text{Gal}(\widehat{F}/K(T))$ dans S_d.

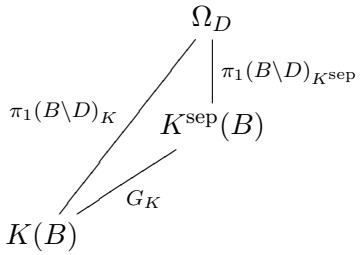
1.1.2. Corps de base quelconque. — Par la correspondance revêtements-extensions, les revêtements $f : X \to B$ définis sur K correspondent aux extensions $F/K(B)$ séparables régulières sur K (*i.e.* $F \cap \overline{K} = K$). On définit alors les invariants de $F/K(B)$ (ou de $f : X \to B$) comme étant ceux de $FK^{\text{sep}}/K^{\text{sep}}(B)$.

(1) Par diviseur premier, on entend un fermé intègre de codimension 1.

Dans la suite, on dit que $F/K(B)$ est une G-*extension de groupe* H[(2)] si $F/K(B)$ est galoisienne, F/K est régulière et un isomorphisme entre $\mathrm{Gal}(F/K(B))$ et H est donné. On dit que $F/K(B)$ est une *simple extension* si $F/K(B)$ est une extension finie séparable régulière sur K. On parlera de "G-revêtement" et de "simple revêtement" pour les notions correspondantes en termes de revêtements.

1.2. Groupe fondamental

Soit D un diviseur effectif réduit et K-rationnel de B, c'est-à-dire une somme formelle de diviseurs premiers de B globalement invariante par l'action de G_K. On fixe une clôture séparable $K(B)^{\mathrm{sep}}$ de $K(B)$ (ce qui correspond au choix d'un point de base générique dans $B \setminus D$). Notons Ω_D l'extension galoisienne maximale de $K^{\mathrm{sep}}(B)$ non-ramifiée au-dessus de $B \setminus D$. Le groupe fondamental géométrique $\pi_1(B \setminus D)_{K^{\mathrm{sep}}}$ de $B \setminus D$ est le groupe de Galois de l'extension $\Omega_D/K^{\mathrm{sep}}(B)$. De plus, l'extension $\Omega_D/K(B)$ est galoisienne car D est globalement invariante par l'action de G_K. Par définition, son groupe de Galois est le K-groupe fondamental de $B \setminus D$ que l'on note $\pi_1(B \setminus D)_K$.



Via la théorie de Galois, on a une suite exacte de groupes fondamentaux. De plus, tout point K-rationnel $t_0 \in B(K) \setminus D$ définit naturellement une section, notée s_{t_0}, de cette suite exacte :

$$1 \longrightarrow \pi_1(B \setminus D)_{K^{\mathrm{sep}}} \longrightarrow \pi_1(B \setminus D)_K \longrightarrow G_K \longrightarrow 1, \quad s_{t_0} : G_K \to \pi_1(B \setminus D)_K$$

(2) La lettre majuscule G dans G-extension indique que le groupe de Galois fait partie de la donnée. Le groupe de Galois pourra être noté G; nous aurons alors des G-extensions de groupe G.

1.3. Correspondance entre extensions et représentations du groupe fondamental

Soit $F/K(B)$ une simple extension de degré d. On associe à cette extension les invariants mentionnés dans le §1.1. L'extension $F/K(B)$ correspond à un morphisme $\phi : \pi_1(B \setminus D)_K \to S_d$ transitif tel que sa restriction à $\pi_1(B \setminus D)_{K^{\text{sep}}}$ reste transitif (car F/K est régulier). Le morphisme ϕ s'obtient à partir de l'extension en considérant l'action de $\pi_1(B \setminus D)_K$ sur l'ensemble des $K(B)$-plongements de F dans Ω_D.

Si $F/K(B)$ est une G-extension de groupe G, elle correspond à un morphisme surjectif $\phi : \pi_1(B \setminus D)_K \to G$. De plus, la G-extension $FK^{\text{sep}}/K^{\text{sep}}(B)$ de groupe G correspond à la restriction $\overline{\phi} : \pi_1(B \setminus D)_{K^{\text{sep}}} \to G$ de ϕ à $\pi_1(B \setminus D)_{K^{\text{sep}}}$. Ce morphisme $\overline{\phi}$ reste surjectif car F/K est régulier.

Réciproquement, soit $\phi : \pi_1(B \setminus D)_K \to S_d$ un morphisme. Considérons le sous-corps $F = {\Omega_D}^{\pi_1(1)}$ de Ω_D fixé par le sous-groupe $\pi_1(1) \subset \text{Ker}(\phi)$ des éléments x tels que $\phi(x)$ fixe 1. L'extension $F/K(B)$ est une simple extension correspondant à ϕ. Si $\phi : \pi_1(B \setminus D)_K \to G$ est un épimorphisme, alors l'extension $F/K(B)$ avec $F = {\Omega_D}^{\text{Ker}(\phi)}$ est une G-extension de groupe G.

1.4. Spécialisation

Soient $F/K(B)$ une G-extension de groupe G et $t_0 \in B(K) \setminus D$ un point K-rationnel. Soit $\phi : \pi_1(B \setminus D)_K \to G$ le morphisme surjectif correspondant à $F/K(B)$ (voir §1.3). Notons s_{t_0} la section de la suite de groupes fondamentaux correspondant au point t_0 (voir §1.2).

$$\begin{array}{ccccccccc} & & & & & \overset{s_{t_0}}{\curvearrowleft} & & & \\ 1 & \longrightarrow & \pi_1(B \setminus D)_{K^{\text{sep}}} & \longrightarrow & \pi_1(B \setminus D)_K & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \overline{\phi}} & & \downarrow{\scriptstyle \phi} & & & & \\ & & G & = & G & & & & \end{array}$$

La spécialisation, F_{t_0}/K, de $F/K(B)$ en le point t_0 est définie comme le corps résiduel de F en un premier au-dessus de t_0 dans l'extension $F/K(B)$; elle est définie à conjugaison près par des éléments de $\text{Gal}(F/K(B))$. La spécialisation F_{t_0}/K correspond au morphisme $\phi \circ s_{t_0}$ qu'un appelle *le morphisme de spécialisation* en t_0. Plus précisément, F_{t_0} est le corps fixé dans K^{sep} par $\ker(\phi \circ s_{t_0})$. En particulier, la spécialisation F_{t_0}/K est une extension galoisienne de groupe $\text{Im}(\phi \circ s_{t_0}) \subset G$.

Si $f : X \to B$ est un G-revêtement défini sur K de groupe G et $t_0 \in B(K) \setminus D$, la spécialisation de f en t_0 est celle de l'extension $K(X)/K(B)$.

1.5. Espace de Hurwitz

Supposons que G soit un groupe fini et $r > 2$ un entier. On note $\mathrm{H}_r(G)$ l'espace des modules de toutes les G-extensions de groupe G ayant exactement r points de branchement. L'espace $\mathrm{H}_r(G)$ est une variété lisse définie sur $\mathbb{Q}$ telle que pour tout corps k algébriquement clos de caractéristique 0, les points k-rationnels de $\mathrm{H}_r(G)$ correspondent aux classes d'isomorphisme de G-extensions $F/k(T)$ de groupe G définies sur k ayant r points de branchement (voir [**FV91**]).

Pour $\mathbf{C} = \{C_1, \ldots, C_r\}$ un r-uplet non ordonné de classes de conjugaison de G, on note $\mathrm{H}_r(G, \mathbf{C}) \subseteq \mathrm{H}_r(G)$ le sous-ensemble des points correspondant aux G-extensions de groupe G ayant exactement r points de branchement et de type de ramification $\mathbf{C}$. L'ensemble $\mathrm{H}_r(G, \mathbf{C})$ est une réunion de composantes irréductibles de $\mathrm{H}_r(G)$. Voir [**Völ96**] pour plus de détails.

1.6. Revêtement tordu

On généralise des résultats démontrés dans [**Dèb99**, §2] dans le cas de revêtements de $\mathbb{P}^1$. On fixe :

- un G-revêtement $f : X \to B$ de groupe G défini sur K qui correspond à une G-extension $K(X)/K(B)$ de groupe G.
- une extension galoisienne E/K de groupe H où H est un sous-groupe de G.

Considérons la suite exacte de groupes fondamentaux (voir §1.2) :

$$1 \longrightarrow \pi_1(B \setminus D)_{K^{\mathrm{sep}}} \longrightarrow \pi_1(B \setminus D)_K \longrightarrow G_K \longrightarrow 1$$

On note $\phi : \pi_1(B \setminus D)_K \to G$ le morphisme surjectif correspondant à f (voir §1.3). De son coté, E/K correspond à un morphisme $\varphi : G_K \to G$.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(B \setminus D)_{K^{\mathrm{sep}}} & \longrightarrow & \pi_1(B \setminus D)_K & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \overline{\phi}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \varphi} & & \\ & & G & = & G & = & G & & \end{array}$$

Pour $t_0 \in B(K)\backslash D$, on note s_{t_0} la section associée de $r : \pi_1(B \setminus D)_K \to G_K$. D'autre part, on peut voir f comme un simple revêtement : en termes de groupes fondamentaux, on compose ϕ par la représentation régulière à gauche $\gamma : G \to S_d$, où $d = |G|$. Le morphisme $\gamma\phi : \pi_1(B \setminus D)_K \to S_d$ est une représentation transitive qui correspond à f, vu comme simple revêtement.

On définit maintenant une représentation transitive :

$$\widetilde{\phi} : \pi_1(B \setminus D)_K \to S_d$$

par la formule suivante (voir [**Dèb99**]) : pour tout $y \in \pi_1(B \setminus D)_K$, on pose :

$$\widetilde{\phi}(y) = (\gamma\phi)(y)(\delta\varphi^* r)(y)$$

où $\delta : G \to S_d$ est la représentation régulière à droite de G dans S_d et $\varphi^* : G_K \to G$ est défini par $\varphi^*(g) = \varphi(g)^{-1}$.

La représentation $\widetilde{\phi}$ définit un simple revêtement $\widetilde{f^\varphi} : \widetilde{X^\varphi} \to B$ qui est un K-modèle du simple revêtement $f \otimes_K K^{\mathrm{sep}}$ (*i.e.* on a $\widetilde{f^\varphi} \otimes_K K^{\mathrm{sep}} \simeq f \otimes_K K^{\mathrm{sep}}$). On appelle $\widetilde{f^\varphi}$ *le revêtement tordu* de f par φ. Le revêtement $\widetilde{f^\varphi}$ a la propriété suivante :

Théorème 1.6.1. — *Fixons $t_0 \in B(K) \setminus D$. Alors le morphisme de spécialisation $\phi s_{t_0} : G_K \to G$ est conjugué dans G à φ si et seulement s'il existe $x_0 \in \widetilde{X^\varphi}(K)$ tel que $\widetilde{f^\varphi}(x_0) = t_0$.*

Démonstration. — Le morphisme $\widetilde{\phi^\varphi} s_{t_0}$ correspond à l'action de G_K sur la fibre de $\widetilde{f^\varphi}$ au-dessus de t_0. Pour tout $\tau \in G_K$, on a $\widetilde{\phi^\varphi}(s_{t_0}(\tau)) = \gamma\phi(s_{t_0}(\tau))\delta\varphi^*(\tau)$. Le terme $\gamma\phi(s_{t_0}(\tau))$ correspond à la multiplication à gauche par $\phi(s_{t_0}(\tau))$ et $\delta\varphi^*(\tau)$ à la multiplication à droite par $\varphi^{-1}(\tau)$. On déduit que si les permutations $\widetilde{\phi^\varphi}(s_{t_0}(\tau))$ ($\tau \in G_K$) ont un point fixe commun, disons $\omega \in G$, alors $\phi(s_{t_0}(\tau)) = \omega\varphi(\tau)\omega^{-1}$. On déduit que l'extension spécialisée de f en t_0 est conjuguée à φ. Ce qui termine la preuve de la partie indirecte du théorème.

Pour la partie directe, on suppose que l'extension spécialisée de f en le point t_0 est donnée pas l'épimorphisme $\varphi : G_K \to G$ à conjugaison près, c'est-à-dire, il existe $w \in G$ tel que $\phi s_{t_0} = w\varphi w^{-1}$. On déduit que, pour tout $\tau \in G_K$, on a $\widetilde{\phi^\varphi}(s_{t_0}(\tau))(g) = w\varphi(\tau)w^{-1}g\varphi(\tau)^{-1}$ ($g \in G$). Ce qui implique que $\widetilde{\phi^\varphi}(s_{t_0}(\tau))$ fixe w, lequel correspond à un point $x_0 \in \widetilde{X^\varphi}(K)$ dans la fibre de t_0. D'où le résultat. □

Remarque 1.6.2. — D. Harari nous a indiqué que le théorème 1.6.1 peut s'interpréter en termes de G-torseurs et de cohomologie étale non abélienne

[**HS02**, §4]. Le revêtement f a une classe $[f]$ dans $H^1(U,G)$ (où $U = B \setminus D$) et de même φ peut se voir dans $H^1(K,G)$ (ce dernier ensemble consiste en les morphismes de G_K dans G à conjugaison près). On a un torseur tordu X^φ (qui n'est plus G-revêtement en général si G n'est pas commutatif) $X^\varphi \to U$ sous le K-groupe algébrique fini G^φ. La condition "il existe $x_0 \in \widetilde{X^\varphi}(K)$ tel que $\widetilde{f^\varphi}(x_0) = t_0$" signifie que $[X^\varphi](t_0) = 0$, ce qui est équivalent à $[X](t_0) = \varphi$ ou encore à la condition que "le morphisme de spécialisation $\phi s_{t_0} : G_K \to G$ est conjugué dans G à φ".

1.7. Premières applications

Le théorème 1.6.1 sera un outil de base dans le chapitre 3. Mais nous pouvons dès à présent en donner quelques applications.

1.7.1. Corps PAC. — Rappelons qu'un corps k est dit PAC si toute variété géométriquement irréductible définie sur k possède un point k-rationnel ; de façon équivalente le sous-ensemble des points k-rationnels est Zariski-dense. Les corps algébriquement clos, les corps séparablement clos sont PAC. Il existe de nombreux autres exemples de corps PAC ; pour tout $\sigma \in G_{\mathbb{Q}}$ sauf dans un ensemble de mesure de Haar nulle, le corps $\overline{\mathbb{Q}}^\sigma$ est PAC. Le corps $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ (où $\mathbb{Q}^{\mathrm{tr}}$ est le corps des nombres algébriquement totalement réels) est un autre exemple concret de corps PAC. Voir [**FJ04**] pour plus d'information sur les corps PAC.

On a le résultat suivant qui a été démontré dans [**Dèb99**] pour les revêtements de $\mathbb{P}^1$.

Corollaire 1.7.1. — *Soit K un corps PAC. Alors tout G-revêtement $f : X \to B$ de groupe G défini sur K possède la propriété suivante. Toute extension galoisienne E/K de groupe $H \subset G$ est la spécialisation de f en un point $t_0 \in B(K) \setminus D$. De plus, les points t_0 ayant cette propriété forment un ensemble Zariski-dense de $B(K) \setminus D$.*

Démonstration. — C'est une conséquence immédiate du théorème 1.6.1 et de la propriété PAC : la variété $\widetilde{X^\varphi}$ a un sous-ensemble Zariski dense de points K-rationnels. □

1.7.2. Résultat de Ekedahl et Colliot-Thélène. — Une autre conséquence du théorème 1.6.1 est le résultat suivant, déjà obtenu par Colliot-Thélène [**Ser92**] et Ekedahl [**Eke90**]. Rappelons qu'une variété B définie sur un corps de nombres K a la propriété d'approximation faible-faible s'il existe

un ensemble fini Σ de places de K tel que l'ensemble $B(K)$ est dense dans $\prod_{v\in W} B(K_v)$, pour tout ensemble fini W de places disjoint de Σ.

Corollaire 1.7.2. — *Soient K un corps de nombres et B une variété de dimension arbitraire définie sur K qui vérifie la propriété d'approximation faible-faible. Alors pour tout G-revêtement $f : X \to B$ défini sur K de groupe G, il existe un sous-ensemble Zariski-dense de points $t_0 \in B(K) \setminus D$ tels que la spécialisation de f en t_0 soit de groupe G (c'est-à-dire B a la propriété de spécialisation de Hilbert).*

On peut aussi relier cet énoncé à un résultat d'Harari [**Har07**, §4] : pour que G soit groupe de Galois sur K, il suffit que G vérifie la propriété dite AHF (approximation hyper-faible). Nous montrons par ailleurs un peu plus loin (corollaire 3.4.2) que si G est, comme dans le corollaire 1.7.2, groupe de Galois d'un G-revêtement défini sur K, alors G vérifie la propriété AHF.

Dans la démonstration du corollaire 1.7.2, on va utiliser le lemme suivant qui est un résultat classique de théorie des groupes dû à Jordan [**Jor72**] et que nous réutiliserons plusieurs fois dans les chapitres suivants.

Lemme 1.7.3. — *Pour un groupe fini G, il n'y a pas de sous-groupe propre de G qui coupe toutes les classes de conjugaison de G.*

Démonstration du corollaire 1.7.2.— Par [**Ser92**, §3], les deux propriétés "approximation faible-faible" et "spécialisation de Hilbert" sont birationnelles. Il suffit donc de montrer ce résultat pour B une variété lisse projective géométriquement intègre. On note D le diviseur de ramification de f et on note $\phi : \pi_1(B \setminus D, t)_K \to G$ le morphisme surjectif correspondant à f (voir §1.3). Pour montrer la propriété de spécialisation de Hilbert, il suffit de montrer :

(∗) le morphisme $\phi s_{t_0} : G_K \to G$ est surjectif pour tous points t_0 dans un sous-ensemble Zariski-dense de $B(K) \setminus D$, où s_{t_0} est la section de la suite de groupes fondamentaux correspondant à t_0 (voir §1.2).

Pour toute place v de K, notons ϕ_v la restriction de ϕ à $\pi_1(B \setminus D, t)_{K_v}$; ϕ_v est le morphisme correspondant à $f \otimes_K K_v$. Pour montrer (∗) il suffit, via le lemme 1.7.3 et la propriété d'approximation faible-faible de B, de montrer que :

(∗∗) Pour tout $g \in G$, il existe une infinité de places v de K telles que, pour tout point t_0 dans un ouvert v-adique non-vide de $B(K_v) \setminus D$, l'image $\mathrm{Im}(\phi_v s_{t_0})$ contient un certain conjugué de $\langle g \rangle$.

Fixons $g \in G$. Soit $\varphi_g : G_K \to \langle g \rangle$ un morphisme surjectif (*i.e.* une extension galoisienne de K de groupe isomorphe à $\langle g \rangle$). Par le théorème de Čebotarev, on sait que, pour une infinité de places v de K, la restriction de φ_g à G_{K_v} est surjective et non-ramifiée. Notons $\widetilde{f^{\varphi_g}} : \widetilde{X^{\varphi_g}} \to B$ le revêtement tordu de f par φ_g. Toutes les places précédentes sauf un nombre fini vérifient $\widetilde{X^{\varphi_g}}(K_v) \neq \emptyset$; on utilise ici l'argument classique suivant qui sera repris par la suite : si $\widetilde{X^{\varphi_g}}$ a bonne réduction en v et le corps résiduel κ_v de v est suffisamment grand, la fibre spéciale de $\widetilde{X^{\varphi_g}}$ a des points κ_v-rationnels (par Lang-Weil) qui se relèvent en des points K_v-rationnels sur $\widetilde{X^{\varphi_g}}$ (par Hensel). En utilisant le théorème 1.6.1, on obtient que pour tout $t_0 \in B(K_v) \setminus D$ image par $\widetilde{f^{\varphi_g}}$ d'un point dans $\widetilde{X^{\varphi_g}}(K_v)$, l'extension spécialisée de $f \otimes_K K_v$ en t_0 contient un certain conjugué de $\langle g \rangle$. D'où le résultat $(**)$.

1.7.3. Corps finis. — On va montrer l'énoncé suivant :

Corollaire 1.7.4. — *Il existe une fonction $C(u, v)$ dépendant de deux variables vérifiant la propriété suivante. Soit $f : X \to \mathbb{P}^1$ un G-revêtement de groupe G avec r points de branchement défini sur un corps fini $\mathbb{F}_q$ tel que $q \geq C(r, |G|)$. Alors toute extension finie de $\mathbb{F}_q$ de groupe isomorphe à un sous-groupe de G est la spécialisation de f en un certain point $t_0 \in \mathbb{P}^1(\mathbb{F}_q) \setminus D$.*

Démonstration. — Notons g le genre de X. En utilisant la borne de Lang-Weil, on peut affirmer que si q est choisi de telle sorte que $q + 1 - 2g\sqrt{q} > |G|r$, alors X, ainsi que tout $\mathbb{F}_q$-modèle de $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, possède un point $\mathbb{F}_q$-rationnel ne se situant pas au-dessus d'un point de D. Par la formule de Riemann-Hurwitz, on peut borner g par un terme ne dépendant que de r et de $|G|$. L'inégalité précédente est garantie par une condition du type $q \geq C(r, |G|)$.

Soit $E/\mathbb{F}_q$ une extension cyclique de groupe $\langle \sigma \rangle \subset G$, où $\sigma \in G$. On note $\varphi : G_{\mathbb{F}_q} \to G$ le morphisme correspondant à cette extension cyclique et $\widetilde{f^{\varphi}} : \widetilde{X^{\varphi}} \to \mathbb{P}^1$ le revêtement tordu de f par φ. Comme $\widetilde{f^{\varphi}}$ est un $\mathbb{F}_q$-modèle de $f \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, alors il existe $x_0 \in \widetilde{X^{\varphi}}(\mathbb{F}_q)$ tel que $t_0 := \widetilde{f^{\varphi}}(x_0) \in \mathbb{P}^1 \setminus D$. Par le théorème 1.6.1, on peut conclure que l'extension spécialisée de f en t_0 est isomorphe à $E/\mathbb{F}_q$.

□

1.7.4. Corps de nombres. — Soient K un corps de nombres et $f : X \to \mathbb{P}^1$ un G-revêtement défini sur K avec X une courbe du genre ≥ 2. Alors une extension galoisienne E/K de groupe de Galois $H \subset G$ ne peut-être la spécialisation de f qu'en un nombre fini de points $t_0 \in \mathbb{P}^1(K) \setminus D$. En effet, pour

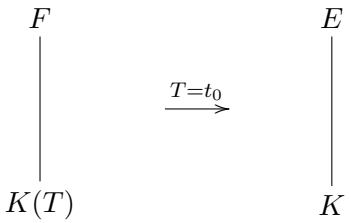
tous les revêtements tordus $\widetilde{f^{\varphi}} : \widetilde{X^{\varphi}} \to \mathbb{P}^1$ de f par un morphisme $\varphi : G_K \to G$ correspondant à E/K, le genre de $\widetilde{X^{\varphi}}$ est ≥ 2. D'après le théorème de Faltings, il n'y a qu'un nombre fini de points K-rationnels sur la variété $\widetilde{X^{\varphi}}$. Comme on n'a qu'un nombre fini de revêtements tordus à considérer, on peut conclure en utilisant le théorème 1.6.1.

CHAPITRE 2

PROBLÈME DE BECKMANN-BLACK

2.1. Introduction

Une question ouverte en théorie inverse de Galois est le problème de **B**eckmann-**B**lack (noté **BB**). Plus précisément, si on se donne un corps K, un groupe fini G et une extension galoisienne E/K de groupe G, la question de **BB** est la suivante : existe-il une G-extension $F/K(T)$ de groupe G telle que sa spécialisation en un point non-ramifié $t_0 \in \mathbb{P}^1(K)$ soit isomorphe à E/K ?



Le problème de **BB** a une réponse positive dans les situations suivantes :

- Le groupe G est le groupe symétrique S_d : Beckmann [**Bec94**] si le corps de base est un corps des nombres et Black [**Bla99**] pour un corps arbitraire K.
- G est un groupe abélien : Beckmann [**Bec94**] et Black [**Bla98**] si le corps de base K est un corps de nombres, Dèbes [**Dèb99**] pour un corps arbitraire K.
- G est le groupe diédral D_n d'ordre $2n$ avec n impair : Black [**Bla98**].
- G est un groupe fini et K est un corps PAC : Dèbes [**Dèb99**]. Par définition, on dit qu'un corps K est PAC si toute variété géométriquement irréductible définie sur K possède une infinité de points K-rationnels. De plus, Dèbes a prouvé un énoncé plus fort : il a montré que toute extension

galoisienne E/K de groupe G est la spécialisation de toute G-extension de $K(T)$ de groupe G en une infinité de points non-ramifiés $t_0 \in \mathbb{P}^1(K)$.

- G est un groupe fini et le corps de base K est un corps ample *i.e.* toute courbe $\mathcal{C}$ lisse géométriquement irréductible définie sur K possède une infinité de points K-rationnels si elle en possède au moins un : Colliot-Thélène [**CT00**] en caractéristique 0, Moret-Bailly [**MB01a**] et Haran-Jarden [**HJ98**] en général.

2.1.1. Résultat principal. — L'objet de ce chapitre est de montrer le résultat suivant :

Théorème 2.1.1. — *Soient G un groupe fini, H un sous-groupe de G, K un corps de nombres, E/K une extension galoisienne de groupe H, $t_0 \in \mathbb{P}^1(K)$ un point fixé et S un ensemble fini de places de K. Alors il existe :*

- *une extension finie L/K totalement décomposée dans K_v pour tout $v \in S$.*
- *une G-extension $F/L(T)$ de groupe G telle que l'extension spécialisée F_{t_0}/L en le point $T = t_0$ vérifie les propriétés suivantes :*
  (1) *L'extension spécialisée F_{t_0}/L est une extension galoisienne de groupe H isomorphe à EL/L.*
  (2) *L'extension complétée $F_{t_0}K_v/K_v$ est isomorphe à EK_v/K_v pour tout $v \in S$.*

Le cas particulier $S = \emptyset$ avec $G = H$ affirme que **BB** possède une réponse positive sur une extension finie du corps de base. La conclusion (2) dans le cas $S \neq \emptyset$ affirme que **BB** est vraie localement *i.e.* après une extension des scalaires à certains complétés de K donnés à l'avance. Le théorème 2.1.1 montre que ces deux conditions, locale et globale, peuvent être combinées.

De plus, l'addendum ci-dessous du théorème 2.1.1 donne deux conclusions supplémentaires. La première précise certaines propriétés de la G-extension $F/L(T)$ et permet une interprétation modulaire du résultat. La deuxième se place dans le cas plus général où K est un corps hilbertien[(1)] de caractéristique 0. Rappelons que tout corps de type fini sur $\mathbb{Q}$ est un corps hilbertien.

Théorème 2.1.1 (addendum) : *On a les conclusions supplémentaires suivantes :*

[(1)] Un corps K est dit hilbertien si pour tout polynôme irréductible unitaire $f(T, Y) \in K(T)[Y]$, il existe une infinité de points $t \in K$ tels que le polynôme spécialisé $f(t, Y)$ est irréductible dans $K[Y]$.

(3) *On peut demander que la G-extension $F/L(T)$ ait un nombre r de points de branchement et un type de ramification $\boldsymbol{C}^{(2)}$ indépendants de S.*
(4) *Dans le cas particulier où $S = \emptyset$, la conclusion globale* (1) *est satisfaite si K est un corps hilbertien de caractéristique* 0.

Ainsi d'après (3), il existe un espace de Hurwitz $\mathrm{H}_r(G, \mathbf{C})^{(3)}$ ne dépendant pas de S tel que l'extension $F/L(T)$ correspond à un point dans cet espace. On peut comparer ce résultat avec le résultat principal de B. Deschamps selon lequel pour tout groupe fini G, il existe un espace de Hurwitz $\mathrm{H}_r(G, \mathbf{C})$ qui a des points p-adiques pour tout p [**Des95**]. Plus précisément, on construira une courbe $\mathcal{C}$ dans l'espace de Hurwitz $\mathrm{H}_r(G, \mathbf{C})$ tel que, pour tout S, il existe une G-extension $F/L(T)$ comme dans le théorème 2.1.1 qui correspond à un point sur cette courbe.

2.2. Preuve du théorème principal

Soient G un groupe fini, K un corps de caractéristique 0, $t_0 \in \mathbb{P}^1(K)$ un point fixé et E/K une extension galoisienne de groupe $H \subset G$.

2.2.1. BB sur une courbe. — Le point de départ est l'énoncé suivant :

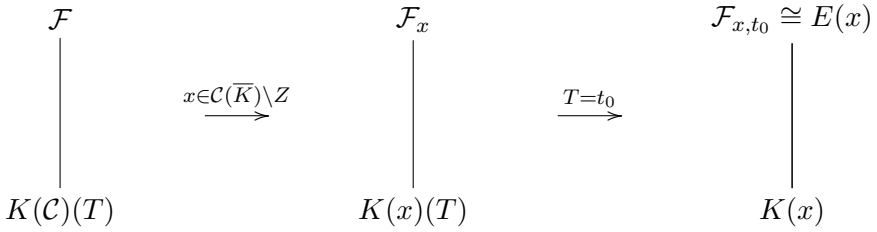
Proposition 2.2.1. — *Sous les hypothèses du théorème 2.1.1, il existe :*

1. *une courbe projective lisse géométriquement irréducible $\mathcal{C}$ définie sur K avec un point K-rationnel,*
2. *une G-extension $\mathcal{F}/K(\mathcal{C})(T)$ de groupe G définie sur le corps de fonctions $K(\mathcal{C})$ non-ramifiée au-dessus de $T = t_0$,*

ayant la propriété suivante : il existe un fermé propre de Zariski Z tel que, pour tout $x \in \mathcal{C}(\overline{K}) \setminus Z$, l'extension spécialisée de $\mathcal{F}/K(\mathcal{C})(T)$ en x est une G-extension, $\mathcal{F}_x/K(x)(T)$, de groupe G qui est non-ramifiée au-dessus de $T = t_0$ et dont l'extension spécialisée, $\mathcal{F}_{x,t_0}/K(x)$, au point $T = t_0$ est une extension galoisienne isomorphe à $E(x)/K(x)$.

Le diagramme suivant illustre ces doubles spécialisations :

(2) Pour la définition, voir §1.1.1.2
(3) Pour plus de détails, voir §1.5.



La proposition 2.2.1 est une traduction arithmétique du théorème 2.7 de l'article [**MB01a**] qui utilise un point de vue géométrique. On expliquera au §2.3, en utilisant un point de vue arithmétique, comment la proposition 2.2.1 se déduit du fait que l'énoncé **BB** est vrai pour le corps complet (donc ample) $K((X))$ de séries formelles de Laurent à coefficients dans K.

On note r le nombre des points de branchement de $\mathcal{F}/K(\mathcal{C})(T)$, $\mathbf{t} = \{t_1, \ldots, t_r\} \in \mathbb{P}^1(\overline{K(\mathcal{C})})$ son diviseur de branchement et $\mathbf{C} = \{C_1, \ldots, C_r\}$ son type de ramification.

2.2.2. Preuve du théorème 2.1.1. — Comme K est un corps de nombres, par le théorème de densité de Čebotarev [**FJ04**, théorème 5.6], il existe, pour tout $g \in H$, une infinité de places v_g de K, en dehors de S, non-ramifiées dans E/K et telles que le groupe de décomposition, $\mathrm{Gal}(E_v/K_v)$, soit conjugué dans H à $\langle g \rangle$. De plus, on peut choisir pour chaque $g \in H$ une de ces places, notons la v_g, de telle sorte que toutes les places v_g ainsi obtenues ($g \in H$) soient distinctes deux à deux. On note S' l'ensemble de toutes ces places v_g et on pose $S'' = S \cup S'$.

Soit $K^{\mathrm{tot}S''}$ le corps des nombres algébriques totalement S''-adiques *i.e.* le corps des éléments $x \in \overline{K}$ dont le polynôme minimal sur K est totalement décomposé dans K_v pour tout $v \in S''$. Comme $\mathcal{C}$ possède un point K-rationnel et $K \subseteq K^{\mathrm{tot}S''}$, l'ensemble $\mathcal{C}(K^{\mathrm{tot}S''})$ est non vide. En utilisant le fait que $K^{\mathrm{tot}S''}$ est un corps ample [**MB89**], on obtient qu'il existe une infinité de points $K^{\mathrm{tot}S''}$-rationnels sur la courbe $\mathcal{C}$.

Fixons $x \in \mathcal{C}(K^{\mathrm{tot}S''}) \setminus Z$, et L une clôture galoisienne de $K(x)/K$. On note $\mathcal{F}_x L$ par F. D'après la proposition 2.2.1, l'extension $F/L(T)$ est une G-extension de groupe G telle que sa spécialisation F_{t_0}/L en le point t_0 est une extension galoisienne isomorphe à EL/L. Comme $L \subseteq K^{\mathrm{tot}S''} \subseteq K_v$, l'extension $F_{t_0}K_v/K_v$ est isomorphe à E_v/K_v (pour tout $v \in S$). Cela termine la preuve de (2).

Il reste à montrer que F_{t_0}/L est une extension galoisienne de groupe H. On sait d'abord que $\mathrm{Gal}(F_{t_0}/L)$ est un sous-groupe de H. De plus, pour tout $v \in S''$, le groupe $\mathrm{Gal}(F_{t_0}/L)$ contient $\mathrm{Gal}(F_{t_0}K_v/K_v)$ à conjugaison près. En particulier, pour tout $g \in G$, il existe $\sigma_v \in H$ tel que $\langle g \rangle^{\sigma_v} \subseteq H$. Via le lemme 1.7.3, on a $H = \mathrm{Gal}(F_{t_0}/L)$. D'où la fin de la preuve du théorème 2.1.1.

2.2.3. Preuve du théorème 2.1.1 (addendum). — Quitte à grossir le fermé de Zariski Z, on peut affirmer que $F/L(T)$ possède le même nombre de points de branchement et même type de ramification que $\mathcal{F}/K(\mathcal{C})(T)$. On déduit que le corps L et l'extension $F/L(T)$ dépendent de S, mais que le nombre de points de branchement et le type de ramification de $F/L(T)$ n'en dépendent pas. De plus, l'extension $F/L(T)$, qu'on vient de construire, correspond à un point sur la courbe $\mathcal{C}$ dans l'espace de Hurwitz $H_r(G, \mathbf{C})$. Cela achève la preuve de (3).

Pour montrer (4), on suppose que K est un corps hilbertien de caractéristique 0. En utilisant la proposition 2.2.1, on obtient la propriété suivante : pour tout $x \in \mathcal{C}(\overline{K}) \setminus Z$, il existe une G-extension $F/K(x)(T)$ de groupe G définie sur $K(x)$ telle que l'extension spécialisée en $T = t_0$ est une extension galoisienne isomorphe à $E(x)/K(x)$. Pour atteindre notre but, il suffit de trouver un point $x \in \mathcal{C}(\overline{K}) \setminus Z$ tel que les deux extensions $K(x)/K$ et E/K soient linéairement disjointes (alors $E(x)/K(x)$ sera une extension galoisienne de groupe H).

On note $h(w, z) = 0$ une équation affine de $\mathcal{C}$ où $h(W, Z) \in K[W, Z]$ est un polynôme irréductible dans $\overline{K}[W, Z]$. Comme E est une extension finie d'un corps hilbertien K, on peut trouver une infinité de points $w_0 \in K$ (dans K lui-même et pas seulement dans E) tels que $h(w_0, Z) \in K[Z]$ soit irréductible dans $E[Z]$ [**Völ96**, corollaire 1.8].

Pour chaque w_0, on choisit $z_0 \in \overline{K}$ tel que $h(w_0, z_0) = 0$. Comme Z est un ensemble fini et qu'on a une infinité de points $w_0 \in K$ vérifiant la propriété mentionnée au-dessus, on peut affirmer qu'il existe une infinité de points $x := (w_0, z_0) \in \mathcal{C}(\overline{K}) \setminus Z$ (avec $w_0 \in K$) tels que $h(w_0, Z) \in K[Z]$ soit irréductible sur $E[Z]$. On déduit que $[K(x) : K] = deg_Z(h) = [E(x) : E]$. D'où $K(x)/K$ et E/K sont linéairement disjoints.

2.3. Preuve de la proposition 2.2.1

La preuve se décompose en plusieurs étapes.

2.3.1. Première étape : Application de BB sur $K((X))$. — On sait que le problème de Beckmann-Black **BB** a une réponse positive si le corps de base est un corps complet. Ce résultat a été montré par Colliot-Thélène [**CT00**] en caractéristique 0 et dans le cas général par Moret-Bailly [**MB01a**] et Haran-Jarden [**HJ98**] en utilisant des techniques de recollement (patching) et de déformation. On va appliquer ce résultat dans le cas où le corps de base est le corps des séries formelles de Laurent $K((X))$ à coefficients dans K. On donnera au §2.4 une preuve de ce résultat qui reprend celle de Haran-Jarden.

Comme E/K est une extension galoisienne de groupe H, l'extension $E((X))/K((X))$ est une extension galoisienne de groupe H. D'après l'énoncé **BB** sur $K((X))$, on a la conclusion suivante qui constitue le but de cette première étape :

Il existe une G-extension $F_{K((X))}/K((X))(T)$ de groupe G non-ramifiée au-dessus de t_0 telle que l'extension spécialisée en t_0 soit une extension galoisienne de groupe H isomorphe à $E((X))/K((X))$. De plus, la construction de $F_{K((X))}$ montre qu'on peut supposer que les points de branchement $\boldsymbol{t}$ de $F_{K((X))}/K((X))(T)$ sont dans $\mathbb{P}^1(\overline{N})$ où N est le hensélisé de $K(X)$ dans $K((X))$ pour la valuation X-adique, c'est-à-dire, le corps constitué des éléments de $K((X))$ qui sont algébriques sur $K(X)$.

$$\begin{array}{ccc} F_{K((X))} & & E((X)) \\ \Big| & \xrightarrow{T=t_0\in\mathbb{P}^1(K)} & \Big| \\ K((X))(T) & & K((X)) \end{array}$$

Notons $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K((X))} \to G$ l'épimorphisme correspondant à la G-extension $F_{K((X))}/K((X))(T)$. On a le diagramme :

$$\begin{array}{ccccccccc} & & & & & \overset{s_{t_0}}{\curvearrowleft} & & & \\ 1 & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{K((X))}} & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K((X))} & \longrightarrow & G_{K((X))} & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle \overline{\phi}} & & \Big\downarrow{\scriptstyle \phi} & & & & \\ & & G & = & G & & & & \end{array}$$

où la section s_{t_0} est celle qui correspond au point rationnel non-ramifié t_0. Par construction, le sous-corps de $\overline{K((X))}$ fixé par $\ker(\phi \circ s_{t_0})$ est isomorphe à $E((X))$; en particulier, l'image du morphisme $\phi \circ s_{t_0}$ est exactement H.

2.3.2. Deuxième étape : Descente sur le corps hensélien $N = K((X)) \cap \overline{K(X)}$. — L'énoncé suivant est le but de cette étape :

Lemme 2.3.1. — *Il existe une G-extension $F_N/N(T)$ définie sur N de groupe G telle que $F_N K((X)) = F_{K((X))}$ et que la spécialisation, $F_{N,t_0}/N$, en le point t_0 soit une extension galoisienne de groupe H isomorphe à EN/N.*

$$\begin{array}{ccc} F_N & & EN \\ \Big| & \xrightarrow{T=t_0 \in \mathbb{P}^1(K)} & \Big| \\ N(T) & & N \end{array}$$

Démonstration. — La restriction $\gamma : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K((X))} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_N$ est un isomorphisme. Pour cela voir par exemple l'argument de [**DD04**, théorème 3.4] : on note d'abord que la restriction $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{K((X))}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{N}}$[(4)] est un isomorphisme (via le théorème d'existence de Riemann), puis que la restriction $\rho : G_{K((X))} \to G_N$ est aussi un isomorphisme (via le lemme de Krasner).

De plus, comme t_0 est un point dans $\mathbb{P}^1(K) \setminus \mathbf{t}$, il induit une section, que l'on note aussi s_{t_0}, de $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_N \to G_N$.

$$\begin{array}{ccccccccc} & & & & & \overset{s_{t_0}}{\curvearrowleft} & & & \\ 1 & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{K((X))}} & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{K((X))} & \longrightarrow & G_{K((X))} & \longrightarrow & 1 \\ & & \Big\downarrow \cong & & \Big\downarrow \gamma & & \cong \Big\downarrow \rho & & \\ 1 & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_{\overline{N}} & \longrightarrow & \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_N & \longrightarrow & G_N & \longrightarrow & 1 \\ & & & & & \underset{s_{t_0}}{\curvearrowleft} & & & \end{array}$$

(4)Ici on s'est fixé une clôture algébrique $\overline{K((X))}$ de $K((X))$, $\overline{K(X)}$ désigne la clôture algébrique de $K(X)$ dans $\overline{K((X))}$, on prend ensuite $N = K((X)) \cap \overline{K(X)}$ et $\overline{N}$ est la clôture algébrique de N dans $\overline{K((X))}$.

On déduit qu'il existe une G-extension $F_N/N(T)$ définie sur N de groupe G telle que $F_N K((X)) = F_{K((X))}$: cette extension $F_N/N(T)$ correspond au morphisme surjectif $\phi_N = \phi \circ \gamma^{-1} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t})_N \to G$. De plus, la spécialisation $F_{N,t_0}/N$, de $F_N/N(T)$ en le point t_0 est une extension galoisienne de groupe H telle que $F_{N,t_0}K((X))$ soit égale à la spécialisation de $F_{K((X))}$ en t_0. Par construction de $F_{K((X))}$, on obtient que $F_{N,t_0}K((X)) = E((X))$. D'autre part, comme ρ est un isomorphisme, alors $F_{N,t_0} = EN$. □

2.3.3. Troisième étape : Descente sur la courbe $\mathcal{C}$. — On va montrer l'énoncé suivant :

Lemme 2.3.2. — *Il existe une extension finie $M/K(X)$ avec $M \subset N$ satisfaisant la propriété suivante :*

(i) *Il existe une G-extension $F_M/M(T)$ de groupe G tel que $F_M N = F_N$.*
(ii) *La spécialisation $F_{M,t_0}/M$ de $F_M/M(T)$ en le point t_0 est une extension galoisienne de groupe H et telle que $F_{M,t_0} = EM$.*

Le fait que $M \subseteq N \subset K((X))$, impliquera que M est régulière sur K. On pourra donc dire que M est le corps des fonctions d'une courbe projective lisse géométriquement irréductible $\mathcal{C}$ définie sur K *i.e.* $M = K(\mathcal{C})$. De plus, on pourra déduire de $M = K(\mathcal{C}) \subset N \subset K((X))$ qu'il existe un point K-rationnel sur $\mathcal{C}$ (celui qui, vu comme place du corps $K(\mathcal{C})$, correspond à la valuation X-adique restreinte à N), *i.e.* $\mathcal{C}(K) \neq \emptyset$.

Démonstration. — Soit $y(T)$ un élément primitif de $F_N/N(T)$ entier sur $N[T]$ (qu'on obtient par exemple en multipliant un élément primitif par le *ppcm* des dénominateurs des coefficients de son polynôme minimal sur $N(T)$). Tout conjugué de $y(T)$ sur $N(T)$ s'écrit comme une fonction rationnelle en T et $y(T)$ à coefficients dans N. Soit M_1 le corps engendré par $K(X)$ et tous les coefficients de toutes ces fonctions rationnelles et les coefficients du polynôme minimal de $y(T)$ sur $N(T)$. Ce corps, M_1, est une extension finie de $K(X)$ contenue dans N, et par construction $F_{M_1} = M_1(T, y(T))$ satisfait la condition (i) (en remplaçant M par M_1).

Montrons comment obtenir la condition (ii). On sait que $y(T)$ peut être représenté par une série formelle de la forme :

$$\sum\nolimits_{j\geq 0} a_j (T - t_0)^j \in \overline{M_1}[[T - t_0]]$$

Ceci est possible car t_0 est un point non-ramifié dans $F_{M_1}/M_1(T)$. De plus, on a $F_{M_1,t_0} = M_1(\underline{a})$, où $\underline{a} = \{a_0, a_1, ...\}$. Comme $F_{M_1,t_0}/M_1$ est une extension

finie, on peut trouver un sous-ensemble fini a_I of $\underline{a}$ tel que $M_1(\underline{a}) = M_1(a_I)$. On déduit que :

$$N(a_I) = F_{N,t_0} = EN$$

En particulier, on peut trouver un ensemble fini $N_0 \subset N$ tel que

$$M_1(N_0)(a_I) \subset M_1(N_0)E$$

Finalement, soit α un élément primitif de E/K. Comme $N(a_I) = F_{N,t_0} = EN$, il existe un sous-ensemble fini $N_1 \subset N$ tel que $\alpha \in M_1(N_1)(a_I)$.

On note $M = M_1(N_0 \cup N_1)$ et $F_M = F_{M_1}M$. Il est facile de voir que $M(a_I) = EM$ et donc $F_{M,t_0} = EM$. La conclusion du lemme 2.3.2 est satisfaite pour les corps M et F_M qu'on vient de trouver. □

Posons $M = K(\mathcal{C})$ comme expliqué plus haut et $F = F_M$. Le lemme 2.3.2 peut être réécrit en ces termes : il existe une G-extension $F/K(\mathcal{C})(T)$ de groupe G telle que $K(\mathcal{C})N = F_N$ et $EK(\mathcal{C})/K(\mathcal{C})$ soit la spécialisation de $F/K(\mathcal{C})(T)$ en le point t_0.

$$\begin{array}{ccc} F & & EK(\mathcal{C}) \\ | & \xrightarrow{T=t_0 \in \mathbb{P}^1(K)} & | \\ K(\mathcal{C})(T) & & K(\mathcal{C}) \end{array}$$

2.3.4. Quatrième étape : Spécialisation en des points de la courbe $\mathcal{C}$. — Comme l'extension $F/K(\mathcal{C})(T)$ est une extension régulière, on peut appliquer le théorème de Bertini-Noether [**FJ04**, proposition 8.8]. Ce qui permet d'affirmer qu'il existe un fermé propre de Zariski Z dans $\mathcal{C}$ avec la propriété suivante : pour tout $x \in \mathcal{C}(\overline{K}) \setminus Z$, l'extension spécialisée de $F/K(\mathcal{C})(T)$ au point x est une G-extension $F_x/K(x)(T)$ de groupe G, non-ramifiée au-dessus du point $T = t_0$. De plus, la spécialisation, $F_{t_0}/K(\mathcal{C})$ de $F/K(\mathcal{C})(T)$ en $T = t_0$ est isomorphe à $E(\mathcal{C})/K(\mathcal{C})$. Cela, avec la régularité de l'extension $K(\mathcal{C})/K$, entraine que la spécialisation $F_{x,t_0}/K(x)$ de $F_x/K(x)(T)$ en $T = t_0$ est $K(x)$-isomorphe à $EK(x)/K(x)$.

2.4. Appendice : BB sur $K((X))$

On donne ici une preuve, reprenant celle de Haran et Jarden [**HJ98**], de l'énoncé suivant qui est une solution du problème de Beckmann-Black

sur $K((X))$ dans le cas où l'extension de $K((X))$ à relever est de la forme $E((X))/K((X))$ avec E/K une extension galoisienne finie. Ce cas particulier suffit à nos besoins.

Théorème 2.4.1. — *Soient G un groupe fini, K un corps infini, $t_0 \in \mathbb{P}^1(K)$ et E/K une extension galoisienne de groupe $H \subset G$. Il existe une G-extension $F/K((X))(T)$ de groupe G telle que l'extension spécialisée de $F/K((X))(T)$ en t_0 soit isomorphe à $E((X))/K((X))$.*

$$\begin{array}{ccc} F & & E((X)) \\ \Big| & \xrightarrow{T=t_0} & \Big| \\ K((X))(T) & & K((X)) \end{array}$$

Le reste de cette section est la preuve de ce théorème.

2.4.1. Préliminaires. — Pour simplifier, on pose $\widehat{K} := K((X))$ et $\widehat{E} := E((X))$. L'extension $\widehat{E}/\widehat{K}$ est une extension galoisienne de groupe H non-ramifiée pour la valuation X-adique. On identifie $\gamma \in \mathrm{Gal}(\widehat{E}/\widehat{K})$ à son image dans $\mathrm{Gal}(E/K)$.

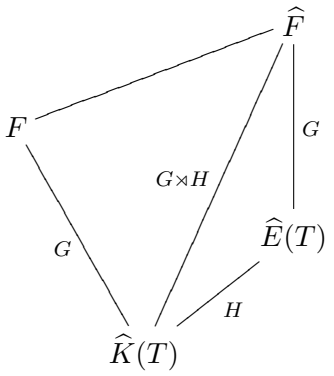
On note $H = \{h_1, \ldots, h_m\}$ et $G = \{g_1, \ldots, g_n\}$ avec $m = |H|$ et $n = |G|$. On pose $I = G \times H$ comme ensemble ; on lui donnera ensuite une structure de groupe par produit semi-direct. Le groupe H agit sur I par $(g_j, h_i)^{h_k} = (g_j, h_i h_k)$, pour $g_j \in G$ et $h_i, h_k \in H$. On identifie $(g_j, 1) \in I$ avec g_j. De plus, pour simplifier, on note $j := g_j$, pour tout $g_j \in G$. On pose $J = \{1, \ldots, n\}$. De cette façon, tout élément $i = (j, \gamma) \in I$ s'écrit de façon unique $i = j^\gamma$ $(j \in J, \gamma \in H)$.

D'autre part, on utilise la structure du groupe $G \rtimes H$ dont peut être équipé I où l'action de H sur G est définie par $g^\gamma = \gamma^{-1} g \gamma$, pour tout $\gamma \in H$ et tout $g \in G$.

Lemme 2.4.2. — *Il existe une famille $(c_i)_{i \in I}$ d'éléments de E non nuls deux à deux distincts telle que, pour tout $i \in I$ et tout $\gamma \in H$, on a $c_i^\gamma = c_{i^\gamma}$.*

Démonstration. — On choisit une famille $(c_j)_{j \in J}$ d'éléments primitifs de E/K deux à deux non conjugués sur K ; cela est possible car K est infini. Pour $i = j^\gamma$, on pose $c_i = c_j^\gamma$ pour tout $j \in J$ et $\gamma \in H$. □

La preuve est organisée de la façon suivante. D'abord, on utilisera la méthode de recollement (patching) pour trouver une G-extension $\widehat{F}/\widehat{E}(T)$ de groupe G telle que $\widehat{F}/\widehat{K}(T)$ soit une extension galoisienne de groupe $G \rtimes H$. Ensuite, on prouvera l'existence de points $b \in \widehat{K}$ telles que $\widehat{F} \subset \widehat{E}((T-b))$. Puis, on construira, à l'aide de $\widehat{F}$, une G-extension $F/\widehat{K}(T)$ de groupe G telle que $F \subset \widehat{F}$ et que tous ces points b restent des points $\widehat{E}$-rationnels sur F. On déduira que le groupe de décomposition de ces points est le groupe H.



2.4.2. Construction de l'extension $\widehat{F}$. — On utilise ici la méthode appelée "algebraic patching" par Haran et Jarden. Pour les résultats concernant les anneaux de séries convergentes, nous renvoyons à [**HJ98**].

• Pour tout $i \in I$, on pose $w_i = \frac{1}{T-c_i} \in \widehat{E}(T)$. L'ensemble

$$\widehat{E}\{w_i\} = \{\sum_{n=1}^{\infty} a_{in} w_i^n \mid a_{in} \in \widehat{E}, \lim_{n\to\infty} a_{in} = 0\}$$

est un sous-anneau de l'anneau des séries formelles $\widehat{E}[[w_i]]$. Plus généralement, l'ensemble

$$R = \widehat{E}\{w_i; i \in I\} = \{a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in} w_i^n \mid a_0 \in \widehat{E}, a_{in} \in \widehat{E}, \lim_{n\longrightarrow\infty} a_{in} = 0, i \in I\}$$

est un anneau qui est le complété de $\widehat{E}[w_i | i \in I]$ pour la valeur absolue ultramétrique définie par $|f| = \max_{i,n}\{|a_0|, |a_{in}|\}$, pour tout $f = a_0 + \sum_{i\in I}\sum_{n=1}^{\infty} a_{in} w_i^n \in R$.

On note :

- $Q = \mathrm{Fr}(R)$ le corps de fractions de R.
- $Q_D = \mathrm{Fr}(R_D)$ avec $R_D = \widehat{E}\{w_i | i \in D\}$, pour tout $D \subset I$.
- $Q_i = Q_{I\setminus\{i\}}$

- $Q_i^{'} = \mathrm{Fr}(\widehat{E}\{w_i\}) = Q_{\{i\}}$.

On a les deux résultats classiques suivants. Le premier utilise le théorème de division de Weierstrass et le deuxième un théorème de Cartan [**FvdP81**, §3.6.3].

Lemme 2.4.3. — (1) *Pour J_1 et J_2 deux sous-ensembles de I tels que $J_1 \cup J_2 \subset I$, on a :*
- *si $J_1 \cap J_2 \neq \emptyset$, alors $Q_{J_1} \cap Q_{J_2} = Q_{J_1 \cap J_2}$*
- *si $J_1 \cap J_2 = \emptyset$, alors on a $Q_{J_1} \cap Q_{J_2} = \widehat{E}(T)$.*

En particulier, on a $Q_i^{'} = \cap_{i \neq j} Q_j$ et $Q_i \cap Q_i^{'} = \widehat{E}(T)$.

(2) *$GL_n(Q) = GL_n(Q_i).GL_n(Q_i^{'})$, pour tout $i \in I$.*

• Le groupe H a une action naturelle sur Q :
pour $r = a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} (\frac{1}{T - c_i})^n \in R$ et $\gamma \in H$, on a

$$r^{\gamma} = a_0^{\gamma} + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in}^{\gamma} (\frac{1}{T - c_i^{\gamma}})^n$$

Lemme 2.4.4. — *Pour tout $i = j^{\gamma} \in I$ avec $j \in J$ et $\gamma \in H$, il existe une G-extension cyclique $F_i/\widehat{E}(T)$ de groupe $G_i = \langle g_i \rangle$ où $g_i = g_j^{\gamma}$ et telle que $F_i \subseteq Q_i^{'}$. De plus, pour tout $\gamma \in H$, on a $F_i^{\gamma} = F_{i^{\gamma}}, Q_i^{\gamma} = Q_{i^{\gamma}}$ et $G_i^{\gamma} = G_{i^{\gamma}}$. Enfin, pour tout $a \in F_i$ et tout $\tau \in G_i$, on a : $(a^{\tau})^{\gamma} = (a^{\gamma})^{\tau^{\gamma}}$.*

Démonstration. — Soit $j \in J$. Le groupe G_j est abélien, il est classique qu'il existe une G-extension $L/\widehat{E}(T)$ de groupe G_j telle que $L \subseteq \widehat{E}((T))$ (voir par exemple [**Völ96**, proposition 11.30]). Les points de branchement peuvent de plus être choisis dans $\mathbb{P}^1(\overline{K})$. Notons α un élément primitif de $L/\widehat{E}(T)$; c'est un élément de $\widehat{E}((T))$ algébrique sur $\widehat{E}(T)$. Par le théorème d'Artin [**Art68**, théorème 2.14], il existe $c_0 \in \widehat{E}^*$ tel que l'élément α converge en tout point $T = c$ où $|c| < |c_0|$.

On considère l'automorphisme de corps $\mu_c : \widehat{E}((T)) \longrightarrow \widehat{E}((T))$ défini par $\mu_c(\sum_{i=N}^{\infty} a_i T^i) = \sum_{i=N}^{\infty} (a_i c^i) T^i$. On pose $\beta = \mu_c(\alpha)$. Cet élément β est un élément primitif de $L/\widehat{E}(T)$ et $L = \widehat{E}(T)(\beta) \subseteq \mathrm{Fr}(\widehat{E}\{T\})$. L'image F_j de L via l'isomorphisme naturel entre $\mathrm{Fr}(\widehat{E}\{T\})$ et $\mathrm{Fr}(\widehat{E}\{w_j\})$ est l'extension cherchée de $\widehat{E}(T)$.

Pour $i = j^{\gamma} \in I$ $(j \in J, \gamma \in H)$, on pose $F_i = F_j^{\gamma}$ où γ agit par l'action induite du groupe H sur Q. L'extension $F_i/\widehat{E}(T)$ est une extension galoisienne de groupe $G_i = \langle g_i \rangle$. Par le choix des éléments c_i, on a $w_i^{\gamma} = (\frac{1}{T - c_i})^{\gamma} = \frac{1}{T - c_i^{\gamma}} =$

w_{i^γ}. En particulier, on a ${Q'}_j^\gamma = {Q'}_{j^\gamma}$. Ce qui implique que $F_i \subseteq Q_i'$. Le reste de l'énoncé se vérifie facilement.

□

• Comme $F_i \subseteq Q_i'$ et $Q_i' \cap Q_i = \widehat{E}(T)$ $(i \in I)$, les extensions $F_i/\widehat{E}(T)$ et $Q_i/\widehat{E}(T)$ sont linéairement disjointes $(i \in I)$. Donc $P_i = F_iQ_i$ est une G-extension de Q_i de groupe isomorphe à $G_i = \mathrm{Gal}(F_i/\widehat{E}(T))$. En utilisant 2.4.4, on obtient que, pour tout $i \in I$ et tout $\gamma \in H$, on a $P_i^\gamma = P_{i^\gamma}$ et que $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$, pour tout $a \in P_i$ et tout $\tau \in G_i$.

Considérons la Q-algèbre $N = \{\sum_{\theta\in G} a_\theta\theta | a_\theta \in Q\}$, où la loi $\times$ est donnée par $(\sum_{\theta\in G} a_\theta\theta) \times (\sum_{\theta\in G} b_\theta\theta) = \sum_{\theta\in G} a_\theta b_\theta\theta$. Le groupe G agit sur N par $(\sum_{\theta\in G} a_\theta\theta)^g = \sum_{\theta\in G} a_\theta g^{-1}\theta$ pour tout $g \in G$. Pour tout $i \in I$, on pose :

$$N_i = \{\sum_{\theta\in G} a_\theta\theta \in N \mid a_\theta \in P_i, a_\theta^\tau = a_{\theta\tau}; \forall\theta \in G, \forall\tau \in G_i\}$$

qui est une Q_i-sous-algèbre de N. On pose $\widehat{F} = \bigcap_{i\in I} N_i$.

• Le lemme suivant est le point central de la technique de "patching"

Lemme 2.4.5. — *$\widehat{F}$ est un corps et c'est une extension galoisienne de $\widehat{E}(T)$ de groupe G et non-ramifiée au-dessus de tout point qui n'est pas un point de branchement d'une des extensions $F_i/\widehat{E}(T)$, pour tout $i \in I$.*

Démonstration. — Ce résultat est classique, nous renvoyons à [**Völ96**, §11]. On vérifie d'abord que $\widehat{F}$ est un corps et que $\widehat{F}^G = \widehat{E}(T)$. On prouve ensuite que $[\widehat{F} : \widehat{E}(T)] = |G|$. C'est dans cette étape qu'intervient le lemme de Cartan (lemme 2.4.3) qui permet de construire une base de la Q-algèbre N (de cardinal $|G|$) qui soit contenue dans chaque N_i $(i \in I)$; c'est donc nécessairement une base de $\widehat{F}$ sur $\widehat{E}(T)$. L'énoncé sur la ramification ne pose pas de difficulté majeure [**Völ96**, remarque 11.24].

□

On montrera plus tard qu'il y a des points $\widehat{E}$-rationnels sur $\widehat{F}$, ce qui implique que $\widehat{F}/\widehat{E}$ est une extension régulière. On déduira que $\widehat{F}/\widehat{E}(T)$ est une G-extension de groupe G.

• On veut maintenant définir une action de H sur $\widehat{F}$. On définit d'abord une action de H sur N de la façon suivante. Pour $\gamma \in H$ et $\sum_{\theta\in G} a_\theta\theta \in N$, avec $a_\theta \in Q = \mathrm{Fr}(R)$, on pose $(\sum_{\theta\in G} a_\theta\theta)^\gamma = \sum_{\theta\in G} a_\theta{}^\gamma\theta^\gamma$.

Prouvons que $\widehat{F}$ est invariant par cette action. Pour cela, on va montrer que ${N_i}^\gamma = N_{i^\gamma}$, pour tout $\gamma \in H$ et $i \in I$. Fixons $i \in I$ et $a = \sum_{\theta \in G} a_\theta \theta \in N_i$. On a :

$$a^\gamma = \sum_{\theta \in G} a_\theta^\gamma \theta^\gamma = \sum_{\theta \in G} a^\gamma_{\theta^{\gamma^{-1}}} \theta$$

On note $b_\theta := a^\gamma_{\theta^{\gamma^{-1}}}$. On remarque que b_θ est un élément de $P_i^\gamma = P_{i^\gamma}$. Pour voir que $a^\gamma \in N_{i^\gamma}$, il reste à vérifier que, pour tout $\sigma \in G_{i^\gamma}$, on a $b_\theta^\sigma = b_{\theta\sigma}$. Comme $\sigma \in G_{i^\gamma} = G_i^\gamma$, il existe $\tau \in G_i$ tel que $\sigma = \tau^\gamma$. Donc on a :

$$b_\theta^\sigma = (a^\gamma_{\theta^{\gamma^{-1}}})^\sigma = (a^\gamma_{\theta^{\gamma^{-1}}})^{\tau^\gamma} = (a^\tau_{\theta^{\gamma^{-1}}})^\gamma = a^\gamma_{\theta^{\gamma^{-1}}{}^\tau} = a^\gamma_{(\theta\tau^\gamma)^{\gamma^{-1}}} = b_{\theta\sigma}$$

On déduit que $N_i^\gamma \subseteq N_{i^\gamma}$. Pour l'autre inclusion, on a : ${N_{i^\gamma}}^{\gamma^{-1}} \subseteq N_{(i^\gamma)^{\gamma^{-1}}} = N_i$. D'où le résultat ${N_{i^\gamma}} = N_i^\gamma$.

• Montrons que les actions de H et G sur $\widehat{F}$ définissent une action de $G \rtimes H$ sur $\widehat{F}$. Cela se ramène à montrer d'abord que :

$(*)$ Pour tout $a = \sum_{\theta \in G} a_\theta \theta \in N$, $\gamma \in H$ et $g \in G$, on a : $((a^{\gamma^{-1}})^g)^\gamma = a^{g^\gamma}$.

En effet, pour tout $g, g' \in G$ et tout $h, h' \in H$, on a $(a)^{hh'} = (a^{h'})^h$ et $(a)^{gg'} = (a^{g'})^g$. En utlisant $(*)$, on obtient que $(a^{hh'})^{gg'^h} = (a^{g'h'})^{gh}$. Il reste à montrer $(*)$:

$$\begin{aligned}((a^{\gamma^{-1}})^g)^\gamma &= ((\textstyle\sum_{\theta\in G} a_\theta^{\gamma^{-1}} \theta^{\gamma^{-1}})^g)^\gamma \\ &= (\textstyle\sum_{\theta\in G} a_\theta^{\gamma^{-1}} g^{-1}\theta^{\gamma^{-1}})^\gamma \\ &= (\textstyle\sum_{\theta\in G} a_\theta^{\gamma^{-1}} g^{-1}\gamma\theta\gamma^{-1})^\gamma \\ &= \textstyle\sum_{\theta\in G} a_\theta \gamma^{-1} g^{-1}\gamma\theta\gamma^{-1}\gamma \\ &= \textstyle\sum_{\theta\in G} a_\theta \gamma^{-1} g^{-1}\gamma\theta \\ &= (\textstyle\sum_{\theta\in G} a_\theta (g^\gamma)^{-1}\theta) \\ &= a^{g^\gamma}\end{aligned}$$

On vérifie que cette action de $G \rtimes H$ sur N laisse invariant $\widehat{F}$. Or on a $\widehat{F}^G = \widehat{E}(T)$ et $\widehat{E}(T)^H = \widehat{K}(T)$, on déduit que $\widehat{F}^{G\rtimes H} = \widehat{K}(T)$. Comme $[\widehat{F} : \widehat{K}(T)] = [\widehat{F} : \widehat{E}(T)].[\widehat{E}(T) : \widehat{K}(T)] = |G|.|H| = |G \rtimes H|$, on obtient que $\widehat{F}/\widehat{K}(T)$ est une extension galoisienne de groupe $G \rtimes H$.

2.4.3. Points $\widehat{E}$-rationnels. — On s'intéresse aux places $\widehat{E}$-rationnelles de $\widehat{F}$, lesquelles correspondent à des points $\widehat{E}$-rationnels sur le modèle projectif lisse de $\widehat{F}$. On note $\lambda : \widehat{F} \to Q$ le morphisme qui envoie $\sum a_\theta \theta$ sur a_1. Pour tout $b \in \widehat{E}$ tel que $|b| > 1$, le $\widehat{E}$-morphisme de spécialisation $\varphi_b : R \to \widehat{E}$ de T en b est bien défini (car $1 = |c_i| < |b|$, donc $|b - c_i| = |b| > 1$). L'anneau R

étant principal, le morphisme φ_b s'étend en une place $\widehat{E}$-rationnelle $\varphi_b : Q \to \widehat{E} \cup \{\infty\}$. On obtient que $\widehat{\varphi_b} := \varphi_b \circ \lambda$ est une place $\widehat{E}$-rationnelle sur $\widehat{F}$.

Comme il n'y a qu'un nombre fini de points de $\widehat{K}$ qui sont ramifiés dans $\widehat{F}/\widehat{K}(T)$ et que $\widehat{K}$ est un corps infini, il existe une infinité de points $b \in \widehat{K}$ non-ramifiés dans $\widehat{F}/\widehat{K}(T)$ tels que $|b| > 1$. Pour ces b, $\widehat{\varphi_b} := \varphi_b \circ \lambda$ est une place $\widehat{E}$-rationnelle non-ramifiée dans $\widehat{F}/\widehat{K}(T)$.

Lemme 2.4.6. — *Le groupe de décomposition $D_{\widehat{\varphi_b}}$ de $\widehat{\varphi_b}$ est le groupe H.*

Démonstration. — Pour cela, il suffit de prouver que :

(∗∗) pour tout $f \in \widehat{F}$ tel que $\widehat{\varphi_b}(f) \neq \infty$, on a $\widehat{\varphi_b}(f^\gamma) = \widehat{\varphi_b}(f)^\gamma$, pour tout $\gamma \in H$

En effet, d'après cette égalité, on a $\widehat{\varphi_b}(\widehat{F}^H) = \widehat{\varphi_b}(\widehat{F})^H = \widehat{E}^H = \widehat{K}$. L'extension $\widehat{F}^{D_{\widehat{\varphi_b}}}$ étant égale à la plus grande extension entre $\widehat{F}$ et $\widehat{K}(T)$ telle que $\widehat{\varphi_b}(\widehat{F}^{D_{\widehat{\varphi_b}}}) \subseteq \widehat{K}$, on obtient que $D_{\widehat{\varphi_b}} \subset H$. Pour l'autre inclusion, on utilise que $D_{\widehat{\varphi_b}} \cong \mathrm{Gal}(\widehat{\varphi_b}(\widehat{F})/\widehat{K})$ (car $\widehat{\varphi_b}$ est non-ramifié dans $\widehat{F}/\widehat{K}$), on remarque que $|D_{\widehat{\varphi_b}}| = [\widehat{\varphi_b}(\widehat{F}) : \widehat{K}] \geq [\widehat{E} : \widehat{K}] = |H|$ (car $\widehat{E} \subseteq \widehat{F}$ et donc $\widehat{\varphi_b}(\widehat{E}) = \widehat{E} \subseteq \widehat{\varphi_b}(\widehat{F})$).

Il reste à montrer (∗∗). On fixe $\gamma \in H$ et $f = \sum_{\theta \in G} a_\theta \theta \in \widehat{F} \subseteq N$. Alors $\lambda(f^\gamma) = \lambda(\sum_{\theta \in G} a_\theta^\gamma \theta^\gamma) = a_1^\gamma = (\lambda(\sum_{\theta \in G} a_\theta \theta))^\gamma = \lambda(f)^\gamma$. D'autre part, pour tout élément $r = a_0 + \sum_{i \in I} \sum_{n=0}^{\infty} a_{in} (\frac{1}{T - c_i})^n \in R$, on a :

$$\begin{aligned} \varphi_b(r^\gamma) &= \varphi_b({a_0}^\gamma + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in}^\gamma (\frac{1}{T - {c_i}^\gamma})^n) \\ &= {a_0}^\gamma + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in}^\gamma (\frac{1}{b - {c_i}^\gamma})^n \end{aligned}$$

et comme $b \in \widehat{K}$, on obtient que :

$$\varphi_b(r^\gamma) = (a_0 + \sum_{i \in I} \sum_{n=1}^{\infty} a_{in} (\frac{1}{b - c_i})^n)^\gamma = \varphi_b(r)^\gamma$$

□

Pour résumer, on a construit une G-extension $\widehat{F}/\widehat{E}(T)$ de groupe G telle que $\widehat{F}/\widehat{K}(T)$ soit une extension galoisienne de groupe $G \rtimes H$. De plus, on a prouvé qu'il existe des places $\widehat{\varphi_b}$ de $\widehat{F}$ (correspondant à des points b sur le modèle projectif lisse de $\widehat{F}$); ces places sont $\widehat{E}$-rationnelles non-ramifiées sur $\widehat{K}(T)$ et de groupe de décomposition égal à H. On déduit que le corps résiduel de $\widehat{\varphi_b}$ est un corps entre $\widehat{K}$ et $\widehat{E}$ (car $\widehat{\varphi_b}(\widehat{F}) = \widehat{E}$) de degré égal au cardinal de

H (car $D_{\widehat{\varphi_b}} = H$). Ce corps résiduel est donc $\widehat{E}$ et l'extension spécialisée de $\widehat{F}/\widehat{K}(T)$ en le point b est isomorphe à $\widehat{E}/\widehat{K}$.

2.4.4. Construction de F. — On a un morphisme surjectif

$$\rho : G \rtimes H \to G; (g, h) \to gh$$

On pose $F = \widehat{F}^M$, où $M = \mathrm{Ker}(\rho)$. L'extension $F/\widehat{K}(T)$ est une extension galoisienne, de groupe égal à G (car ρ surjective). Notons ψ_b la restriction de $\widehat{\varphi_b}$ sur F. Donc $\rho(D_{\widehat{\varphi_b}}) = \rho(H) = \rho(H \times \{1\}) = H$ est le groupe de décomposition de ψ_b dans l'extension $F/\widehat{K}(T)$.

Comme $b \in \widehat{K}$, le corps résiduel de ψ_b est une extension galoisienne de $\widehat{K}$ contenue dans $\widehat{\varphi_b}(\widehat{F}) = \widehat{E}$ tel que le groupe de décomposition de ψ_b soit H. On déduit que la place ψ_b est une place $\widehat{E}$-rationnelle du corps résiduel $\widehat{E}/\widehat{K}$ et donc l'extension spécialisée de $F/\widehat{K}(T)$ au point b est isomorphe à $\widehat{E}/\widehat{K}$.

Par un changement de variable T en $T - b + t_0$, on obtient qu'il existe une extension galoisienne $F/\widehat{K}(T)$ de groupe G telle que l'extension spécialisée de $F/\widehat{K}(T)$ en le point t_0 soit isomorphe à $\widehat{E}/\widehat{K}$.

Il reste à vérifier que $F/\widehat{K}(T)$ est une extension régulière. Il suffit de montrer que $[F : \widehat{K}(T)] = [F\widehat{K}^{\mathrm{sep}} : \widehat{K}^{\mathrm{sep}}(T)]$, où $\widehat{K}^{\mathrm{sep}}$ est la clôture séparable de $\widehat{K}$.

On remarque d'abord que $F = \widehat{F}^M$ et $\widehat{F}^G = \widehat{E}(T)$ sont linéairement disjoints sur $\widehat{K}(T)$, puisque $F \cap \widehat{E}(T) = \widehat{F}^{M.G} = \widehat{F}^{G \rtimes H} = \widehat{K}(T)$. Donc on a $[F : \widehat{K}(T)] = [F\widehat{E} : \widehat{E}(T)]$. D'autre part, le corps $\widehat{F} = F\widehat{E}$ est régulier sur $\widehat{E}$, alors $[\widehat{F} : \widehat{E}(T)] = [\widehat{F}\widehat{K}^{\mathrm{sep}} : \widehat{K}^{\mathrm{sep}}(T)]$. On déduit que $[F : \widehat{K}(T)] = [F\widehat{E} : \widehat{E}(T)] = [F\widehat{K}^{\mathrm{sep}} : \widehat{K}^{\mathrm{sep}}(T)]$. D'où le résultat et la fin de la preuve du théorème 2.4.1.

CHAPITRE 3

PROBLÈME DE HILBERT-GRUNWALD

Le problème et les résultats principaux sont présentés au §3.1.1. Les deux sections suivantes sont consacrées aux preuves. On termine par des applications au §3.4.

3.1. Résultats principaux

3.1.1. Le problème de Grunwald. — Soient K un corps, G un groupe fini et S un ensemble fini de valuations discrètes de K. Pour chaque $v \in S$, on fixe une extension galoisienne E^v/K_v du complété K_v de groupe $H_v \subset G$. Le problème de Grunwald est le suivant : existe-t-il une extension galoisienne E/K de groupe G telle que, pour tout $v \in S$, l'extension complétée EK_v/K_v soit isomorphe à E^v/K_v? Plus précisément, étant donné un morphisme[(1)] $\varphi_v : G_{K_v} \to G$ pour tout $v \in S$, la question est de trouver un morphisme surjectif $\varphi : G_K \to G$ tel que le morphisme composé de φ avec la restriction $G_{K_v} \to G_K$ donne le morphisme φ_v, pour tout $v \in S$.

Dans le cas où K est un corps de nombres, le problème de Grunwald a une réponse positive dans les cas suivants :

- Le groupe G est cyclique d'ordre impair. C'est le théorème de Grunwald-Wang ; l'énoncé initial de Grunwald ne comportait pas la restriction "ordre impair", Wang a donné un contre exemple avec $G = \mathbb{Z}/8\mathbb{Z}$ [**Wan48**], voir aussi [**JNW08**, (9.2.8)].
- Le groupe G est résoluble d'ordre premier avec le nombre de racines de l'unité dans K. C'est un résultat de Neukirch ([**Neu79**] et [**JNW08**, (9.5.5)]).

(1) Ici tous les morphismes de groupes profinis sont continus.

Plus généralement, le problème de Grunwald concerne l'image du morphisme suivant (le morphisme de Grunwald) :

$$Gr_{K,S} : \mathrm{Epi}(G_K, G) \to \prod\nolimits_{v\in S} \mathrm{Hom}(G_{K_v}, G)^{\equiv}$$

Ici on note par $\mathrm{Epi}(G_K, G)$ l'ensemble de tous les morphismes surjectifs de G_K vers G et le symbole $\equiv$ dans $\mathrm{Hom}(G_{K_v}, G)^{\equiv}$ signifie qu'on considère les morphismes de G_{K_v} vers G à conjugaison près dans G.

Définition 3.1.1. — Un élément $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v\in S}$ de $\prod_{v\in S}\mathrm{Hom}(G_{K_v}, G)$ est appelé *problème de Grunwald*. Etant donnée une extension L/K galoisienne totalement décomposée dans K_v pour tout $v \in S$, on dit que $\varphi \in \mathrm{Epi}(G_L, G)$ est une L-solution du problème de Grunwald $\underline{\varphi}$ si $Gr_{L,S}(\varphi) = \underline{\varphi}$[(2)]. De plus, le problème de Grunwald $\underline{\varphi}$ est dit non-ramifié si $\mathrm{Gal}(\overline{K_v}/{K_v}^{\mathrm{ur}}) \subset Ker(\varphi_v)$ pour tout $v \in S$ (où ${K_v}^{\mathrm{ur}}$ est l'extension maximale non ramifée de K_v).

On remarque que $\underline{\varphi}$ ne change pas si on fait une extension des scalaires de K à une extension L comme ci-dessus.

3.1.2. Théorèmes principaux. — Pour toute place v d'un corps de nombres K, on note le cardinal du corps résiduel de K_v par q_v et sa caractéristique par p_v.

La constante $C(r, |G|)$, qui est mentionnée dans le théorème suivant, dépend de l'ordre du groupe G et du nombre r de points de branchement du revêtement ; elle est définie plus précisément au §3.2.

Théorème 3.1.2. — *Soient K un corps de nombres, S un ensemble fini de places finies de K et G un groupe fini. On suppose que pour tout $v \in S$, $p_v \nmid |G|$ et $q_v \geq C(r, |G|)$. Soit $f : X \to \mathbb{P}^1$ un G-revêtement de groupe G défini sur K tel que la propriété de bonne réduction suivante soit satisfaite :*

(Bonne-réduction)[(3)] *pour tout $v \in S$, le diviseur de branchement $\boldsymbol{t} = \{t_1, \ldots, t_r\}$ est étale et v n'est pas une place de ramification verticale pour f.*

[(2)] Il y a un petit abus de notation pour écrire $Gr_{L,S}(\varphi) = \underline{\varphi}$, car il y a plusieurs places de L au-dessus de chaque place de S. Pour le justifier, il faut noter que L/K est totalement décomposé dans K_v pour tout $v \in S$ et que les homomorphismes $G_{K_v} \to G$ dans l'ensemble d'arrivée de $Gr_{L,S}$ sont considérés à conjugaison près dans G.

[(3)] Un critère classique pour la bonne réduction : si $\mathbf{t}$ est un diviseur étale et $p_v \nmid |G|$, alors f a bonne réduction en v après une extension finie L/K [**Ful69**]. De plus, s'il n'y a pas de ramification verticale, alors on peut prendre $L = K$. D'autre part, "$\mathbf{t}$ est étale" signifie que deux points de branchement distincts ne coalescent pas en v. On dit que deux points t_i et t_j coalescent en v si et seulement si : ou bien $|\, t_i \,|_{\overline{v}} \leq 1, |\, t_j \,|_{\overline{v}} \leq 1$ et $|\, t_i - t_j \,|_{\overline{v}} < 1$ ou bien $|\, t_i \,|_{\overline{v}} \geq 1, |\, t_j \,|_{\overline{v}} \geq 1$ et $|\, t_i - t_j \,|_{\overline{v}} < 1$ où $\overline{v}$ est un prolongement de v sur $\overline{K}$. De

Alors f a la propriété de spécialisation de Hilbert-Grunwald suivante :

(HGr-spec) Pour tout problème de Grunwald non-ramifié $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v\in S}$, il existe des points $t_0 \in \mathbb{P}^1(K) \setminus \boldsymbol{t}$ tels que la spécialisation de f en $T = t_0$ soit une extension galoisienne de groupe G qui soit une K-solution du problème de Grunwald $\underline{\varphi}$. De plus, l'ensemble de ces points t_0 contient un sous-ensemble $\mathbb{P}^1(K) \cap \prod_{v\in T} U_v$ avec $U_v \subset \mathbb{P}^1(K_v)$ un ouvert non vide $(v \in T)$ et $T \supset S$ un ensemble fini de places de K.

La propriété de Hilbert-Grunwald apparait déjà dans un travail de Plans et Vila [**PV05**] mais seulement pour des G-extensions qui sont construites par la méthode de rigidité.

La constante $c(G)$ dans le théorème suivant ne dépend que du groupe G (voir §3.3).

Théorème 3.1.3. — *Soient K un corps de nombres, S un ensemble fini de place de K et G un groupe fini. On suppose que $p_v \not| 6|G|$ et $q_v \geq c(G)$ $(v \in G)$. Alors il existe une extension galoisienne L/K totalement décomposée dans K_v $(v \in S)$ et un G-revêtement $f : X \to \mathbb{P}^1$ de groupe G défini sur L tel que ce G-revêtement vérifie les conditions (Bonne-réduction) et (HGr-spec) avec K remplacé par L.*

3.1.3. Compléments aux théorèmes principaux. —

(*a*) On montrera une version plus générale du théorème 3.1.2 où $\mathbb{P}^1$ sera remplacé par une variété de dimension arbitraire et K par le corps des fractions d'un anneau de Dedekind (voir §3.2 et §3.2.2).

(*b*) Les deux théorèmes 3.1.2 et 3.1.3 restent vrais si le corps de base K est un corps de fonctions $\kappa(x)$ d'une variable sur un corps κ qui est ou bien un corps PAC avec "beaucoup d'extensions cycliques" ou bien un corps fini "assez gros" (voir §3.4.5).

(*c*) Le revêtement $f : X \to \mathbb{P}^1$ du théorème 3.1.3 dépend de S. Mais notre construction nous permettra de fixer le nombre r de points de branchement et le type de ramification $\mathbf{C}$. Ainsi le revêtement f correspond à un point de l'espace de Hurwitz $\mathrm{H}_r(G, \mathbf{C})$ indépendant de S. De plus, on prouvera que ces points sont dans une certaine composante (de type **HM** [**Fri95**] [**DE06**]) définie sur K de l'espace de Hurwitz .

façon géométrique, cela signifie que $\mathbf{t}$ s'étend en un schéma étale au-dessus de $\mathrm{Spec}(\mathcal{O}_v)$. La définition de "ramification verticale" est rappelée au §3.2.1.2.

(*d*) Dans le cas où G est un groupe de centre trivial, la condition "v n'est pas un premier de ramification verticale" (dans l'hypothèse (Bonne-réduction)) est automatique si $\mathbf{t}$ est étale et $p_v \not| |G|$ [**Bec91**]. On utilisera cela pour montrer le théorème 3.1.3.

Les théorèmes 3.1.2 et 3.1.3 ont des applications liées à plusieurs sujets :

- Le théorème d'irréductibilité de Hilbert. Le revêtement f de nos énoncés possède beaucoup de spécialisations dans son corps de définition qui préservent son groupe de Galois G (voir §3.4.1).
- Le problème de Grunwald-Wang (voir §3.4.2).
- Le Problème Régulier Inverse de Galois sur $\mathbb{Q}$ (RIGP). On donnera une condition nécessaire (peut-être toujours réalisée) pour qu'un groupe fini puisse être réalisé comme groupe de Galois d'une G-extension de $\mathbb{Q}(T)$ (voir §3.4.3).
- Le Problème Régulier Inverse de Galois sur un corps p-adique. On peut construire, pour toute valuation v de K telle que $p_v \not|6|G|$ et $q_v \geq c(G)$, un G-revêtement f de groupe G défini sur K_v et tel que v soit une place de bonne réduction pour f (voir §3.4.4).

3.2. Preuve du théorème 3.1.2

La preuve du théorème 3.1.2 comporte deux parties : une première partie locale, où le corps de base est un corps valué complet et une seconde partie où on globalise les résultats locaux.

3.2.1. Situation locale. — On va étudier le théorème dans le contexte plus général des revêtements d'une variété de dimension arbitraire.

3.2.1.1. Le résultat local. — On se donne :

- k le corps de fractions d'un anneau de valuation discrète complet A. On note $\mathfrak{p}$ l'idéal de valuation et $\kappa = A/\mathfrak{p}$ le corps résiduel. On suppose, de plus, que κ est parfait de caractéristique $p \geq 0$.
- B une variété projective géométriquement intègre de dimension arbitraire définie sur k. De plus, on suppose qu'elle possède un modèle, $\mathcal{B}$, intègre lisse projectif défini sur A. En particulier, $\mathcal{B}$ est régulière [**Gro67**, proposition 17.5.8].
- $f : X \to B$ un G-revêtement de groupe G défini sur k. On note $k(X)/k(B)$ la G-extension de groupe G correspondant à f et $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ le morphisme correspondant à la normalisation de $\mathcal{B}$ dans $k(X)$ ($\mathcal{F}$ est

un morphisme fini [**Mil80**, proposition 1.1]), $\mathcal{F}_0 : \mathcal{X}_0 \to \mathcal{B}_0$ la fibre spéciale et $\mathcal{D}$ la fermeture de Zariski de D dans $\mathcal{B}$ où D est le diviseur de branchement de f.

3.2.1.2. Définitions. — Rappelons que k^{sep} désigne une clôture séparable de k et $\overline{\kappa}$ une clôture algébrique (en fait également séparable) du corps parfait κ.

Un morphisme fini et plat $\mathcal{F}' : \mathcal{X}' \to \mathcal{B}$ avec $\mathcal{X}'$ normal est appelé *un A-modèle de* $(f\otimes_k k^{sep}, \mathcal{F}_0\otimes_\kappa\overline{\kappa})$ si :

- $\mathcal{F}'\otimes_A k$ est un k-revêtement et est k^{sep}-isomorphe à $f\otimes_k k^{\text{sep}}$.
- la fibre spéciale $\mathcal{F}'_0 : \mathcal{X}'_0 \to \mathcal{B}_0$ est un κ-revêtement et est $\overline{\kappa}$-isomorphe à $\mathcal{F}_0\otimes_\kappa\overline{\kappa}$.

On dit que $\mathfrak{p}$ *n'est pas un premier de ramification verticale pour* f si $\mathcal{F} : \mathcal{X} \to \mathcal{B}$ est non-ramifié au-dessus de $\mathfrak{p}$ *i.e.* $\mathcal{F}$ est non-ramifié au-dessus de la fibre spéciale $\mathcal{B}_0$.

Un homomorphisme $\varphi : G_k \to G$ est dit *non-ramifié en* $\mathfrak{p}$ si le groupe d'inertie au-dessus de $\mathfrak{p}$ est contenu dans $\ker(\varphi)$.

Nos hypothèses font également intervenir la propriété pour un diviseur d'être à croisements normaux. Nous prenons comme définition celle donnée dans [**Gro71**, page 277] dont nous utiliserons des résultats.

Théorème 3.2.1. — *Soient $f : X \to B$ un G-revêtement de groupe G défini sur k et $\varphi : G_k \to G$ un morphisme non-ramifié en $\mathfrak{p}$. Supposons que $p \nmid |G|$ et que :*

(Bonne-réduction) $\mathcal{D}$ est un diviseur lisse, $\mathcal{D}\cup\mathcal{B}_0$ est régulier à croisements normaux sur A et $\mathfrak{p}$ n'est pas un premier de ramification verticale pour f.

(κ-assez-gros) pour tout A-modèle $\mathcal{F}' : \mathcal{X}' \to \mathcal{B}$ de $(f\otimes_k k^{sep}, \mathcal{F}_0\otimes_\kappa\overline{\kappa})$, il existe des points κ-rationnels sur $\mathcal{X}'_0$ qui ne sont pas au-dessus de l'ensemble fermé $\mathcal{D}_0\otimes_\kappa\overline{\kappa}$.

Alors il existe $t_0 \in B(k)\setminus D$ tel que la spécialisation de f en t_0 soit isomorphe à l'extension E/k correspondant au morphisme φ. De plus, l'ensemble des points t_0 ayant cette propriété contient la préimage d'un ensemble non vide $M \subset \mathcal{B}_0(\kappa)\setminus\mathcal{D}_0$ via l'application $\mathcal{B}(A) \to \mathcal{B}_0(\kappa)$.

Démonstration. — On note $\widetilde{f^\varphi} : \widetilde{X^\varphi} \to B$ le revêtement tordu de f par φ (voir §1.6). On note $\widetilde{\mathcal{F}^\varphi} : \widetilde{\mathcal{X}^\varphi} \to \mathcal{B}$ le morphisme correspondant à la normalisation de $\mathcal{B}$ dans $k(\widetilde{X^\varphi})$. Par définition, on a $\widetilde{\mathcal{F}^\varphi}\otimes_A k = \widetilde{f^\varphi}$, donc $\widetilde{\mathcal{F}^\varphi}\otimes_A k$ est k^{sep}-isomorphe à $f\otimes_k k^{\text{sep}}$.

Pour appliquer la condition (κ-assez-gros), nous allons prouver que $\widetilde{\mathcal{F}^{\varphi}}$ est un A-modèle de $(f\otimes_k k^{\mathrm{sep}}, \mathcal{F}_0\otimes_\kappa\overline{\kappa})$. Pour cela, il faut montrer que $\widetilde{\mathcal{F}^{\varphi}}$ est étale (plat et non-ramifié) et que la fibre spéciale, $\widetilde{\mathcal{F}_0^{\varphi}} : \widetilde{\mathcal{X}_0^{\varphi}} \to \mathcal{B}_0$, est un κ-revêtement tel que $\widetilde{\mathcal{F}_0^{\varphi}}\otimes_\kappa\overline{\kappa}$ soit isomorphe à $\mathcal{F}_0\otimes_\kappa\overline{\kappa}$.

— Montrons que $\widetilde{\mathcal{F}^{\varphi}}$ est plat. On utilise le critère suivant [**GM71**, corollaire 2.3.5] :

Si un revêtement est modérément ramifié le long d'un diviseur régulier à croisements normaux, alors ce revêtement est plat.

Comme $p \not| |G|$, alors $\widetilde{\mathcal{F}^{\varphi}}$ est modérément ramifié. Ainsi le k-revêtement $\widetilde{f^{\varphi}} : \widetilde{X^{\varphi}} \to B$ est plat car il est modérément ramifié et son diviseur de ramification D est un diviseur régulier à croisements normaux sur k (car d'après l'hypothèse (Bonne-réduction), il est régulier à croisements normaux sur A).

De plus, $\widetilde{f^{\varphi}}$ est étale au-dessus de $B\setminus D$ [**Mil80**, théorème 3.21]. Or $B\setminus D = \mathcal{B}\setminus(\mathcal{D}\cup\mathcal{B}_0)$. On déduit que $\widetilde{\mathcal{F}^{\varphi}}$ est non-ramifié au-dessus de $\mathcal{B}\setminus(\mathcal{D}\cup\mathcal{B}_0)$ et que le diviseur de ramification de $\widetilde{\mathcal{F}^{\varphi}}$ est contenu dans le fermé $\mathcal{D}\cup\mathcal{B}_0$. Donc pour montrer que $\widetilde{\mathcal{F}^{\varphi}}$ est plat, il suffit d'appliquer le critère précédent en remarquant que $p \not| |G|$ et que le diviseur de ramification $\mathcal{D}\cup\mathcal{B}_0$ est un diviseur régulier à croisements normaux sur A (d'après l'hypothèse (Bonne-réduction)).

— Montrons que $\widetilde{\mathcal{F}^{\varphi}}$ est non-ramifié au-dessus de $\mathcal{B}\setminus\mathcal{D}$. Comme $\widetilde{f^{\varphi}}$ est non-ramifié au-dessus de $B\setminus D$, alors, via le théorème de pureté de Nagata-Zariski, il suffit de vérifier que $\mathfrak{p}$ est non-ramifié dans $\widetilde{\mathcal{F}^{\varphi}}$.

Montrons que $\mathfrak{p}$ est non-ramifié dans $\widetilde{\mathcal{F}^{\varphi}}$. D'abord, $\mathfrak{p}$ est non-ramifié dans E/k; plus exactement, il est non-ramifié dans la clôture intégrale, ${A'}_E$, de A dans E. D'autre part, comme $\mathfrak{p}$ n'est pas un premier de ramification verticale pour f, alors $\mathfrak{p}$ est non-ramifié dans la normalisée de $\mathcal{B}$ dans $k(X)$. Comme E/k est non-ramifié, d'après [**Bec91**, lemme 2.1] l'idéal au-dessus de p (dans ${A'}_E/A$) est non-ramifié dans la normalisée de $\mathcal{B}\otimes_A {A'}_E$ dans $E(X)$. Cela entraîne que $\mathfrak{p}$ est non-ramifié dans la normalisée de $\mathcal{B}$ dans $E(X)$. Or $k(\widetilde{X^{\varphi}}) \subset E(X) = E(\widetilde{X^{\varphi}})$. On obtient donc que $\mathfrak{p}$ est non-ramifié dans la normalisée de $\mathcal{B}$ dans $k(\widetilde{X^{\varphi}})$, c'est-à-dire que $\mathfrak{p}$ est non-ramifié dans $\widetilde{\mathcal{F}^{\varphi}}$. D'où le résultat.

— Montrons que la fibre spéciale $\widetilde{\mathcal{F}_0^{\varphi}} : \widetilde{\mathcal{X}_0^{\varphi}} \to \mathcal{B}_0$ est un κ-modèle de $\mathcal{F}_0^{\mathrm{sep}} = \mathcal{F}_0\otimes_\kappa\overline{\kappa}$. Plus exactement, nous allons vérifier que $\widetilde{\mathcal{F}_0^{\varphi}}$ est fini, étale sur $(\mathcal{B}\setminus\mathcal{D})_0$, que la variété $\widetilde{\mathcal{X}_0^{\varphi}}$ est géométriquement irréductible et que $\widetilde{\mathcal{F}_0^{\varphi}}\otimes_\kappa\overline{\kappa}$ est isomorphe à ${\mathcal{F}_0}^{\mathrm{sep}}$.

D'après un résultat de Grothendieck [**Gro71**, exposé XIII], on a une équivalence de catégories entre la catégorie des revêtements de $\mathcal{B}$ modérément ramifiés sur $\mathcal{D}$ et la catégorie des revêtements de la fibre spéciale de $\mathcal{B}_0$ modérément ramifiés au-dessus de $\mathcal{D}_0$. En appliquant ce critère à $\widetilde{\mathcal{F}^{\varphi}}$, on obtient que $\widetilde{\mathcal{F}_0^{\varphi}} : \widetilde{\mathcal{X}_0^{\varphi}} \to \mathcal{B}_0$ est fini, plat, étale au-dessus de $(\mathcal{B} \setminus \mathcal{D})_0$ et $\widetilde{\mathcal{X}_0^{\varphi}}$ est normal et irréductible (sur κ). Il reste à voir que $\widetilde{\mathcal{X}_0^{\varphi}}$ est géométriquement irréductible, c'est-à-dire $\widetilde{\mathcal{X}_0^{\varphi}}$ est irréductible sur $\overline{\kappa}$, et que $\mathcal{F}_0^{\mathrm{sep}}$ est isomorphe à $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$.

On note A^{sep} la clôture intégrale de A dans k^{sep} et $\mathcal{F}^{\mathrm{sep}} : \mathcal{X}^{\mathrm{sep}} \to \mathcal{B}^{\mathrm{sep}}$ la normalisée de $\mathcal{B}^{\mathrm{sep}} = \mathcal{B} \otimes_A A^{\mathrm{sep}}$ dans $k^{\mathrm{sep}}(X)$. Comme $\mathcal{F}^{\mathrm{sep}}$ est un revêtement modérément ramifié le long du diviseur de branchement $(\mathcal{B} \setminus \mathcal{D}) \otimes_A A^{\mathrm{sep}}$, alors, par le résultat précédent de Grothendieck, on obtient que $\mathcal{F}_0^{\mathrm{sep}} : \mathcal{X}_0^{\mathrm{sep}} \to \mathcal{B}_0^{\mathrm{sep}}$ est un revêtement modérément ramifié. En particulier, $\mathcal{X}_0^{\mathrm{sep}}$ est irréductible. Si on montre que $\mathcal{F}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ sont isomorphes, alors $\mathcal{X}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{X}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ seront isomorphes. Et on déduira que $\widetilde{\mathcal{X}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ est irréductible, *i.e.* $\widetilde{\mathcal{X}_0^{\varphi}}$ est géométriquement irréductible.

Il reste donc à prouver que $\mathcal{F}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ sont isomorphes. Comme $\widetilde{\mathcal{F}^{\varphi}}$ est étale sur $\mathcal{B} \setminus \mathcal{D}$, il existe un ouvert non vide $U = \mathrm{Spec}(\beta) \subset \mathcal{B} \setminus \mathcal{D}$ qui rencontre $\mathcal{B}_0$ tel que la clôture intégrale $\beta'_{k(\widetilde{X^{\varphi}})}$ de β dans $k(\widetilde{X^{\varphi}})$ soit un β-module libre de rang $[k(\widetilde{X^{\varphi}}) : k(B)]$. En diminuant U, on peut supposer que l'ensemble ouvert $U \otimes_A A^{\mathrm{sep}} = \mathrm{Spec}(\beta \otimes_A A^{\mathrm{sep}})$ de $(\mathcal{B} \setminus \mathcal{D}) \otimes_A A^{\mathrm{sep}}$ vérifie la propriété suivante : la clôture intégrale $(\beta \otimes_A A^{\mathrm{sep}})'_{k^{\mathrm{sep}}(X)}$ de $\beta \otimes_A A^{\mathrm{sep}}$ dans $k^{\mathrm{sep}}(X)$ est un $\beta \otimes_A A^{\mathrm{sep}}$-module libre de rang $[k^{\mathrm{sep}}(\widetilde{X^{\varphi}}) : k^{\mathrm{sep}}(B)]$. On choisit une base $f_1, \ldots, f_d$ du β-module $\beta'_{k(\widetilde{X^{\varphi}})}$. C'est aussi une base du $\beta \otimes_A A^{\mathrm{sep}}$-module $(\beta \otimes_A A^{\mathrm{sep}})'_{k^{\mathrm{sep}}(X)}$: en effet, son discriminant est inversible dans β (et donc dans $\beta \otimes_A A^{\mathrm{sep}}$), de plus, on a $k^{\mathrm{sep}}(X) = k^{\mathrm{sep}}(\widetilde{X^{\varphi}})$ et $[k(\widetilde{X^{\varphi}}) : k(B)] = [k^{\mathrm{sep}}(\widetilde{X^{\varphi}}) : k^{\mathrm{sep}}(B)]$. On déduit que $(\mathcal{F}^{\mathrm{sep}})^{-1}(U \otimes_A A^{\mathrm{sep}})$ et $(\widetilde{\mathcal{F}^{\varphi}})^{-1}(U) \otimes_A A^{\mathrm{sep}}$ sont isomorphes au-dessus de l'ouvert $U \otimes_A A^{\mathrm{sep}}$. Cela implique que $\mathcal{F}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ sont birationnellement isomorphes. De plus, comme $\mathcal{X}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{X}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ sont normaux, en utilisant l'équivalence de catégories entre corps des fonctions et revêtements, on peut conclure que $\mathcal{F}_0^{\mathrm{sep}}$ et $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ sont isomorphes (pas seulement birationnellement isomorphes). En utilisant le même argument pour $\varphi = 1$, on obtient que $\mathcal{F}_0^{\mathrm{sep}}$, $\widetilde{\mathcal{F}_0^{\varphi}} \otimes_{\kappa} \overline{\kappa}$ et $\mathcal{F}_0 \otimes_{\kappa} \overline{\kappa}$ sont isomorphes. D'où le résultat.

Maintenant on peut appliquer l'hypothèse (κ-assez-gros) car on vient de montrer que $\widetilde{\mathcal{F}^{\varphi}}$ est un A-modèle de $(f \otimes_k k^{\mathrm{sep}}, \mathcal{F}_0 \otimes_{\kappa} \overline{\kappa})$. On obtient qu'il existe

des points κ-rationnels sur $\widetilde{\mathcal{X}_0^{\varphi}}$ qui ne sont pas au-dessus de $\mathcal{D}_0$. Notons M l'ensemble $\widetilde{\mathcal{F}_0^{\varphi}}(\widetilde{\mathcal{X}_0^{\varphi}}(\kappa)) \setminus \mathcal{D}_0$.

Fixons $\overline{t_0} \in M$ et $\overline{x} \in \widetilde{\mathcal{X}_0^{\varphi}}(\kappa)$ au-dessus de $\overline{t_0}$. Comme la variété $\mathcal{B}$ est lisse, par le lemme de Hensel, il existe $t_0 \in \mathcal{B}(A)$ un relèvement de $\overline{t_0}$. Plus précisément, tous ces relèvements t_0 sont dans une même classe $U \subset \mathcal{B}(A)$ modulo $\mathfrak{p}$ pour la topologie $\mathfrak{p}$-adique. D'autre part, le morphisme $\widetilde{\mathcal{F}^{\varphi}} : \widetilde{\mathcal{X}^{\varphi}} \to \mathcal{B}$ est étale au voisinage de t_0. Par une nouvelle application du lemme de Hensel, on déduit qu'il existe $x \in \widetilde{X^{\varphi}}(A)$ un relèvement de $\overline{x}$. Par le théorème 1.6.1, on peut conclure que la spécialisation de f en t_0 est une extension galoisienne isomorphe à E/k. De plus, l'ensemble de ces points t_0 contient un ouvert non vide U de $\mathcal{B}(A) \setminus \mathcal{D}$.

□

3.2.1.3. Remarque sur l'hypothèse (κ-assez-gros). — L'hypothèse (κ-assez-gros) est satisfaite dans les deux situations suivantes :

- κ est PAC (par la définition d'un corps PAC).
- κ est un corps fini de cardinal q plus grand qu'une constante $C(f, \mathcal{B})$ qui est explicitée ci-dessous et qui ne dépend que de f et $\mathcal{B}$. Dans le cas particulier $B = \mathbb{P}^1$, cette constante ne dépend que de r et de $|G|$. Cela résulte de l'énoncé suivant :

La borne de Lang-Weil.— *Soit V une variété propre géométriquement irréductible de dimension $d \geq 1$ définie sur κ où κ est un corps fini de cardinal q. Alors il existe une constante β dépendant seulement de $V_{\overline{\kappa}} = V \otimes_{\kappa} \overline{\kappa}$ telle que $|\#V(\kappa) - q^d| \leq \beta\sqrt{q^{2d-1}}$. Pour tout premier $l \neq p$, la constante β peut-être choisie égale à la plus grande dimension $\beta_l(V_{\overline{\kappa}})$ du groupe de cohomologie l-adique $H^i(V_{\overline{\kappa}}, \mathbb{Q}_l)$ pour $i = 0, 1, \ldots, 2d$, (vu comme $\mathbb{Q}_l$-espace vectoriel).*

Ce résultat est une conséquence du travail de Grothendieck et Deligne sur la conjecture de Weil [**Del74**, §1] et [**Del80**]. Pour tout $l \neq p$, Grothendieck a défini les groupes de cohomologie l-adique $H^i(V_{\overline{\kappa}}, \mathbb{Q}_l)$ qui sont des $\mathbb{Q}_l$-espaces vectoriels de dimension finie pour lesquels on a la formule suivante :

$$\#V(\kappa) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F, H^i(V_{\overline{\kappa}}, \mathbb{Q}_l))$$

où $\mathrm{Tr}(F, H^i(V_{\overline{\kappa}}, \mathbb{Q}_l)$ est la trace du Frobenius agissant sur $H^i(V_{\overline{\kappa}}, \mathbb{Q}_l)$. Par le théorème de Deligne [**Del80**, théorème 3.3.1], les valeurs propres de l'action du Frobenius sur ces groupes de cohomologies ont des valeurs absolues $\leq \sqrt{q^i}$. De plus, pour $i = 2d$, on a $\mathrm{Tr}(F, H^{2d}(V_{\overline{\kappa}}, \mathbb{Q}_l)) = q^d$.

Pour déduire l'hypothèse (κ-assez-gros) dans le cas d'un corps fini, on fixe un A-modèle $\mathcal{F}' : \mathcal{X}' \to \mathcal{B}$ de $(f\otimes_k k^{\mathrm{sep}}, \mathcal{F}_0\otimes_\kappa\overline{\kappa})$. En utilisant la borne de Lang-Weil, on obtient que le nombre total de points κ-rationnels sur la variété $V = \mathcal{X}_0'$ est minoré par $q^d - \beta_l(V_{\overline{\kappa}})\sqrt{q^{2d-1}}$, où $\beta_l(V_{\overline{\kappa}}) = \beta_l(\mathcal{X}_0'\otimes_\kappa\overline{\kappa})$.

On veut maintenant évaluer le nombre N de points κ-rationnels au-dessus des composantes irréductibles définies sur κ de $\mathcal{D}_0\otimes_\kappa\overline{\kappa}$. L'hypothèse (bonne-réduction) avec l'hypothèse $p \not| |G|$ implique qu'il y a une correspondance entre les composantes irréductibles de $\mathcal{D}_0\otimes_\kappa\overline{\kappa}$ et celles de $D\otimes_k k^{\mathrm{sep}}$. On note $r(D)$ le nombre de ces composantes. En appliquant la borne de Lang-Weil, on obtient que $N \leq |G|r(D)(q^{d-1} + b_l(\mathcal{D})\sqrt{q^{2(d-1)-1}}) \leq |G|r(D)(1+b_l(\mathcal{D}))q^{d-1}$ où $b_l(\mathcal{D})$ est le maximum de tous les $\beta_l(V_{\overline{\kappa}})$ avec V variant dans l'ensemble de toutes les composantes irréductibles de $\mathcal{D}_0\otimes_\kappa\overline{\kappa}$.

Ainsi le nombre de points κ-rationnels non-ramifiés sur la variété $\mathcal{X}_0'$ est plus grand qu'une expression de la forme : $q^d - \beta_l(V_{\overline{\kappa}})\sqrt{q^{2d-1}} - |G|r(D)(1 + b_l(\mathcal{D}))q^{d-1}$. Cette borne est positive si $q > c$, où c est une constante choisie de la façon suivante : pour chaque $l \neq p$, il existe une constante c_l dépendant de $r(D), |G|, \beta_l(\mathcal{X}_0\otimes_\kappa\overline{\kappa})$ et $b_l(\mathcal{D})$. Il suffit de choisir pour c une constante plus grande qu'un de ces c_l pour obtenir l'hypothèse (κ-assez-gros). On note cette constante c par $C(f, \mathcal{B})$; elle ne dépend que de f et de $\mathcal{B}$.

Pour $B = \mathbb{P}^1$ et $\mathcal{B} = \mathbb{P}^1_A$. On a $b_l(\mathcal{D}) = 0$ et $\beta_l(\mathcal{X}_0\otimes_\kappa\overline{\kappa})$ est borné par une constante dépendant du genre de $\mathcal{X}_0\otimes_\kappa\overline{\kappa}$ qui est égal au genre g de X. Or par la formule de Riemann-Hurwitz, il existe un majorant de g qui dépend seulement de r et $|G|$. On déduit que pour tout $l \neq p$, la constante c_l peut-être choisie ne dépendant que de r et $|G|$ et indépendante de l. La constante c est alors de la forme $C(r, |G|)$. Plus précisément, on sait que $\#\mathcal{X}_0(\kappa) - (q+1) \geq 2g\sqrt{q}$ et il suffit donc de choisir q de telle sorte que $q + 1 - 2g\sqrt{q} > r|G|$ (car ici $N \leq r|G|$).

3.2.1.4. Le cas des revêtements de $B = \mathbb{P}^1$. — On a la conséquence suivante :

Corollaire 3.2.2. — *Soit k le corps de fractions d'un anneau de valuation discrète complet A. On note $\mathfrak{p}$ l'idéal de valuation et κ le corps résiduel $A/\mathfrak{p}$. Supposons de plus que κ soit parfait de caractéristique p. On se donne $f : X \to \mathbb{P}^1$ un G-revêtement défini sur k de groupe G de diviseur de branchement $\boldsymbol{t}$ et un morphisme non-ramifié $\varphi : G_k \to G$. Supposons que $p \not| |G|$ et que :*

(Bonne-réduction) Le diviseur de branchement $\boldsymbol{t} = \{t_1, \ldots, t_r\}$ est étale et $\mathfrak{p}$ n'est pas un premier de ramification verticale pour f.

(κ-assez-gros) Le corps κ est fini de cardinal $q > C(r, |G|)$ où $C(r, |G|)$ est une constante définie au §3.2.1.3.

Alors il existe $t_0 \in \mathbb{P}^1(k) \setminus \boldsymbol{t}$ tel que la spécialisation de f en t_0 soit conjuguée, dans G, au morphisme $\varphi : G_k \to G$. De plus, l'ensemble de t_0 ayant cette propriété contient un ouvert non-vide de $\mathbb{P}^1(k) \setminus \boldsymbol{t}$.

Démonstration. — Ce corollaire est un cas particulier du théorème 3.2.1 où $B = \mathbb{P}^1$. Il suffit de vérifier que l'hypothèse (Bonne-réduction) se réécrit sous la forme indiquée ici, c'est-à-dire que $\mathcal{D} \cup \mathcal{B}_0$ est un diviseur à croisements normaux sous les conditions données ici.

Le diviseur $\mathbf{t}$ est de la forme $\{t_1, \ldots, t_r\}$. On peut supposer que ces points t_i $(i = 1, \ldots, r)$ sont dans A. Le diviseur $\mathcal{D}$ correspond à un polynôme de la forme $D(T) = \delta \prod_{i=1}^{r} (T - t_i)$ avec $\delta \in A \setminus \mathfrak{p}$. Supposons par l'absurde que $\mathcal{D}$ n'est pas à croisements normaux. Alors $D'(T)$ est 0 modulo $\mathfrak{p}$, et donc $D(T)$ modulo $\mathfrak{p}$ a une racine double. On déduit qu'il existe deux points t_i et t_j de $\{t_1, \ldots, t_r\}$ qui sont égaux modulo $\mathfrak{p}$ ce qui contredit le fait que $\mathcal{D}$ est étale. □

3.2.2. Situation globale. — Les énoncés principaux de cette section sont les corollaires 3.2.4 et 3.2.3. Ils permettent en particulier de déduire le théorème principal 3.1.2 (voir remarque (a) du §3.2.2.1).

On reste dans le cas d'un revêtement d'une variété projective de dimension arbitraire. On se donne :

- G un groupe fini et K le corps des fractions d'un anneau de Dedekind R.
- S un ensemble fini de places finies de K (correspondant à des idéaux premiers de R). Pour toute place v, on note K_v la complétion de K pour cette place, R_v l'anneau de valuation, $\mathfrak{p}_v$ l'idéal de valuation et κ_v le corps résiduel $R_v/\mathfrak{p}_v$. On note q_v le cardinal et p_v la caractéristique du corps résiduel.
- B une variété projective lisse géométriquement intègre définie sur K qui possède un modèle intègre $\mathcal{B}$ défini sur R tel que $\mathcal{B}_v = \mathcal{B} \otimes_R R_v$ soit lisse sur R_v pour tout $v \in S$.
- $f : X \to B$ un G-revêtement de groupe G défini sur K. On note D le diviseur de branchement de f et on pose $\mathcal{D}$ et $\mathcal{D}_v$ sa fermeture de Zariski dans $\mathcal{B}$ et $\mathcal{B}_v$ respectivement.

De plus, on suppose que les hypothèses suivantes sont satisfaites :

(Bonne-réduction) *Pour tout $v \in S$, $p_v \not| |G|$, $\mathcal{D}_v$ est un diviseur lisse, $\mathcal{D}_v \cup (\mathcal{B}_v)_0$ est régulier à croisements normaux sur R_v et $\mathfrak{p}_v$ n'est pas un premier de ramification verticale pour $f \otimes_K K_v$.*

(Hypothèse sur les corps résiduels) *Pour tout $v \in S$, le corps κ_v est un corps fini de cardinal $q_v > C(f, \mathcal{B})$; où $C(f, \mathcal{B})$ est la constante définie ci-dessous.*

(Hypothèse sur B) *La variété B vérifie la propriété d'approximation faible relativement à S* i.e. *l'ensemble $B(K)$ est dense dans $\prod_{v \in S} B(K_v)$.*

La constante $C(f, \mathcal{B})$ est déterminée de la façon suivante : on fixe un premier $l \neq p_v$ pour tout $v \in S$. Au §3.2.1.3, on a défini, pour tout $v \in S$, une constante c_l ne dépendant que de $r(D), |G|, \beta_l(\mathcal{X}_0 \otimes_{\kappa_v} \overline{\kappa_v})$ et de $b_l(\mathcal{D} \otimes_{\kappa_v} \overline{\kappa_v})$. Ici les $\mathcal{X}_0 \otimes_{\kappa_v} \overline{\kappa_v}$ viennent d'une variété globale qui est la normalisée de $\mathcal{B}$ dans $K(X)$. Par une propriété standard des groupes de cohomologie l-adique [**Gro73**], la $\mathbb{Q}_l$-dimension de $H^i(\mathcal{X}_0 \otimes_{\kappa_v} \overline{\kappa_v}, \mathbb{Q}_l)$ peut-être bornée par une constante dépendant seulement de X (donc dépendant de f et ne dépendant pas de v). Idem pour $b_l(\mathcal{D} \otimes_{\kappa_v} \overline{\kappa_v})$. On déduit que la constante c_l peut-être choisie de la forme $C(f, \mathcal{B})$ (c'est-à-dire ne dépendant que de f et de $\mathcal{B}$). On prend $q_v \geq C(f, \mathcal{B})$, pour tout $v \in S$. En particulier, si $B = \mathbb{P}^1$, alors en utilisant la remarque 3.2.1.3, cette constante ne dépend que de $|G|$ et de r.

Pour tout $v \in S$, on note $f_v : X_v \to B_v$ le G-revêtement défini sur K_v de groupe G qui vient de f par une extension des scalaires de K à K_v. Fixons un problème de Grunwald non-ramifié $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v \in S}$. Avec nos hypothèses (Bonne-réduction) et (Hypothèse sur les corps résiduels), on peut appliquer le théorème local 3.2.1 à f_v et φ_v, pour tout $v \in S$. On déduit qu'il existe un ouvert non vide $U_v \in B(K_v) \setminus D$ tel que la spécialisation de f_v en chaque point $t_v \in U_v$ soit une extension galoisienne qui correspond au morphisme $\varphi_v : G_{K_v} \to G$, pour tout $v \in S$ (à conjugaison près par un élément de G).

Or la variété B vérifie la propriété d'approximation faible relativement à S, donc l'ensemble $B(K) \cap \prod_{v \in S} U_v$ est non vide. Fixons t_0 dans cet ensemble $B(K) \cap \prod_{v \in S} U_v$. Le point t_0 a la même propriété de spécialisation que les points t_v ($v \in S$). Ce qui implique que, pour chaque $v \in S$, la spécialisation de $f_v = f \otimes_K K_v$ en le point t_0 est une extension galoisienne qui correspond au morphisme $\varphi_v : G_{K_v} \to G$, à conjugaison près par un élément de G. Donc, le groupe de Galois de $\mathrm{Gal}(K(X)_{t_0}/K)$ contient un certain conjugué de $H_v = \varphi_v(G_{K_v})$ dans G *i.e.* pour tout $v \in S$, il existe $g_v \in G$ tel que le conjugué ${H_v}^{g_v} = g_v H_v g_v^{-1}$ soit contenu dans $\mathrm{Gal}(K(X)_{t_0}/K)$.

On souhaite se placer dans des situations où $\mathrm{Gal}(K(X)_{t_0}/K) = G$. On sait d'abord, par la définition de spécialisation, que $\mathrm{Gal}(K(X)_{t_0}/K) \subseteq G$. Pour l'autre inclusion, on a deux cas selon le groupe G et le problème de Grunwald considérés :

⋆ Supposons que la condition suivante soit satisfaite :

(𝔤-complet) *Si C_v est une classe de conjugaison d'un générateur du groupe cyclique $H_v = \varphi_v(G_{K_v})$*[4]*, alors l'ensemble $\{C_v, v \in S\}$ est $\mathfrak{g}$-complet* i.e. *il n'y a pas de sous-groupe propre de G qui coupe toutes les classes de conjugaison C_v ($v \in S$).*

On obtient alors que $\mathrm{Gal}(K(X)_{t_0}/K) = G$ et on peut conclure qu'on a l'énoncé suivant :

Corollaire 3.2.3. — *Si en plus des hypothèses du §3.2.2, (𝔤-complet) est satisfait, alors la propriété suivante de Hilbert-Grunwald est satisfaite :*

(HGr-spec) Pour tout problème de Grunwald non-ramifié $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v\in S}$, il existe un ensemble non vide de la forme $B(K) \cap \prod_{v\in S} U_v$, où U_v est un ouvert de $B(K_v) \setminus D$, tel que, pour tout $t_0 \in B(K) \cap \prod_{v\in S} U_v$, la spécialisation de f en t_0 est une extension galoisienne de groupe G qui est une K-solution du problème de Grunwald $\underline{\varphi}$.

⋆ Supposons que la condition (𝔤-complet) ne soit pas vérifiée. Pour obtenir la condition (HGr-spec), on doit modifier les hypothèses de la façon suivante :

(Hypothèse sur les corps résiduels) *En plus des valuations de S, il existe une infinité de valuations v de K telles que le corps résiduel κ_v soit un corps fini de cardinal $q_v \geq C(f, \mathcal{B})$.*

(Hypothèse sur B) *La variété B vérifie la propriété d'approximation faible* i.e. *l'ensemble $B(K)$ est dense dans $\prod_{v\in W} B(K_v)$, pour tout ensemble fini W de places de K.*

Avec ces modifications, on va trouver t_0 vérifiant $\mathrm{Gal}(K(X)_{t_0}/K) = G$. Pour cela, on choisit, pour chaque $g \in G$, une place v_g de telle sorte que :

- v_g n'appartient pas à S et les places v_g sont deux à deux distinctes.

[4] H_v est cyclique car v est supposée non ramifiée.

- le localisé $\mathcal{B}_{v_g} = \mathcal{B} \otimes_R R_{v_g}$ est lisse et v_g vérifie la condition (bonne-réduction). Cela est possible si la condition (bonne-réduction) est vraie sur le corps K; c'est le cas, par exemple, si $S \neq \emptyset$ ou si $B = \mathbb{P}^1$. En effet, il n'y a alors qu'un nombre fini de valuations de K qui ne vérifient pas ces deux conditions.
- le corps résiduel κ_{v_g} est fini de cardinal plus grand que la constante $C(f, \mathcal{B})$.

On note $S_0 = \{v_g; g \in G\}$. Pour tout $g \in G$, il existe une (unique) extension cyclique non-ramifiée E_{v_g}/K_{v_g} de groupe $\langle g \rangle$. En effet, les extensions cycliques non-ramifiées de K_{v_g} correspondent aux extensions du corps fini κ_{v_g}; or chaque groupe cyclique est le groupe de Galois d'une (unique) extension de tout corps fini. On applique le théorème local 3.2.1 pour $f_{v_g} = f \otimes_K K_{v_g}$ et $\varphi_{v_g} : G_{K_{v_g}} \to G$, où φ_{v_g} est le morphisme correspondant à l'extension cyclique non-ramifiée E_{v_g}/K_{v_g} $(g \in G)$. On obtient qu'il existe des points $t_{v_g} \in B(K_{v_g}) \setminus D$ tels que la spécialisation de f_{v_g} en t_{v_g} soit une extension galoisienne de groupe conjugué, dans G, à $H_{v_g} = \varphi_{v_g}(G_{K_{v_g}}) = \langle g \rangle$. De plus, l'ensemble de ces points t_{v_g} contient un ouvert non vide U_{v_g} de $B(K_{v_g}) \setminus D$.

Notons $T = S \cup S_0$. Comme B vérifie la propriété d'approximation faible, alors l'ensemble $B(K) \cap (\prod_{v \in T} U_v)$ est non-vide. Si t_0 est un point dans cet ensemble, alors t_0 vérifie la même propriété de spécialisation que t_v, pour tout $v \in T$. Notons $K(X)_{t_0}/K$ l'extension spécialisée de f en t_0. Le groupe $\mathrm{Gal}(K(X)_{t_0}/K)$ contient un certain conjugué de $\langle g \rangle$, pour tout $g \in G$. Via le lemme de Jordan (lemme 1.7.3), on déduit que $\mathrm{Gal}(K(X)_{t_0}/K) = G$ et que la spécialisation $K(X)_{t_0}/K$ est une K-solution de notre problème de Grunwald de départ. On a donc montré le résultat suivant :

Corollaire 3.2.4. — *Sous les hypothèses suivantes et si $S \neq \emptyset$ ou $B = \mathbb{P}^1$:*

(Bonne-réduction) Pour tout $v \in S$, $p_v \not| |G|$, $\mathcal{D}_v$ est un diviseur lisse, $\mathcal{D}_v \cup (\mathcal{B}_v)_0$ est régulier à croisements normaux sur R_v et $\mathfrak{p}_v$ n'est pas un premier de ramification verticale pour $f \otimes_K K_v$,

(Hypothèse sur les corps résiduels) il existe une infinité de valuations v de K telles que le corps résiduel κ_v soit un corps fini de cardinal $q_v \geq C(f, \mathcal{B})$,

(Hypothèse sur B) La variété B vérifie la propriété d'approximation faible i.e. *l'ensemble $B(K)$ est dense dans $\prod_{v\in W} B(K_v)$, pour tout ensemble fini W de places finies de K,*

on a la propriété suivante de Hilbert-Grunwald :

(HGr-spec) Pour tout problème non-ramifié de Grunwald $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v\in S}$, il existe un ensemble non vide de la forme $B(K) \cap \prod_{v\in T} U_v$, où $T \supset S$ est un ensemble fini de places et où U_v est un ouvert de $B(K_v) \setminus D$, tel que la spécialisation de f en t_0 est une extension galoisienne de groupe G qui est une K-solution de $\underline{\varphi}$, pour tout $t_0 \in B(K) \cap \prod_{v\in T} U_v$.

3.2.2.1. Remarques. —

(*a*) Cas où $B = \mathbb{P}^1$ et K est un corps de nombres. Les hypothèses du corollaire 3.2.4 sont clairement vérifiées. En particulier, on sait que $\mathbb{P}^1$ est une variété projective qui vérifie la propriété d'approximation faible ; c'est le théorème d'Artin-Whaples [**Lan78**, page 285]. Ce qui précède fournit une preuve complète du théorème 3.1.2.

(*b*) Cas où les corps résiduels sont PAC. La preuve de la situation globale marche si on remplace l'hypothèse (Hypothèse sur les corps résiduels) par l'hypothèse suivante :

(Corps résiduels PAC) *pour toute valuation v de K, le corps résiduel κ_v est PAC et tout groupe cyclique est un quotient de G_{κ_v}, pour tout v.*

En effet, d'après la remarque 3.2.1.3, on sait qu'on peut appliquer le théorème local 3.2.1 pour le G-revêtement f_v et le morphisme φ_v, pour tout $v \in S$. De plus, la stratégie de globalisation (voir §3.2.2) reste possible dans ce cas grâce à l'hypothèse que tout groupe cyclique est un quotient de G_{κ_v}. Dans le §3.4.5 on donnera une application de cette remarque.

3.3. Preuve du théorème 3.1.3

On se donne un groupe fini G, un corps de nombres K et un ensemble fini S de places de K tels que pour tout $v \in S$, on a $p_v \not| 6|G|$ et $q_v \geq c(G)$ où $c(G)$ est une constante qui ne dépend que de G (définie un peu plus loin).

La preuve du théorème 3.1.3, due à Dèbes, se décompose en plusieurs étapes :

3.3.1. Première étape. — Réduction au cas d'un groupe de centre trivial.

Supposons que $Z(G) \neq \{1\}$. En utilisant [**FV91**, lemme 2], on peut trouver un morphisme surjectif $\epsilon : \widetilde{G} \to G$ tel que $Z(\widetilde{G}) = \{1\}$. En effet, on peut prendre $\widetilde{G} = \Gamma^d \rtimes G$ le produit en couronnes de Γ et G où Γ est un groupe non-abélien simple fini, $d = |G|$ et G agit sur Γ^d en permutant les facteurs de Γ^d via la représentation régulière de G. On prend par exemple, $\Gamma = PSL_2(\mathbb{F}_3)$. Comme aucun des premiers p_v ne divise $6|G|$, alors p_v ne divise pas $|\widetilde{G}|$ $(v \in S)$. Si $Z(G) = \{1\}$, alors on prend $\widetilde{G} = G$.

Dans les étapes $2, 3, 4$ et 5 ci-dessous, nous démontrons le théorème 3.1.3 dans le cas où le groupe est le groupe de centre trivial $\widetilde{G}$. Nous expliquons dans l'étape 6 comment en déduire le théorème 3.1.3 dans le cas général du groupe G; un point crucial sera que le morphisme ϵ est scindé.

3.3.2. Deuxième étape. — On construit un espace de Hurwitz de G-revêtements de groupe $\widetilde{G}$ qui possède une composante irréductible définie sur $\mathbb{Q}$.

La construction suivante est due à Fried. On note $C_1, \ldots, C_s$ une liste de toutes les classes de conjugaison non-triviales de $\widetilde{G}$. Soit $\widetilde{C}$ un uplet obtenu par réunion de toutes les paires $(C_1, {C_1}^{-1}) \ldots (C_s, {C_s}^{-1})$, chacune apparaissant au moins deux fois dans $\widetilde{C}$. On note $\mathrm{H}_r(\widetilde{G}, \widetilde{C})$ l'espace de Hurwitz de tous les G-revêtements de $\mathbb{P}^1$ de groupe $\widetilde{G}$ avec $r = 4s$ points de branchement et de type de ramification $\widetilde{C}$. D'après [**Fri95**], $\mathrm{H}_r(\widetilde{G}, \widetilde{C})$ a une certaine composante (appelée composante de type **HM**) définie sur $\mathbb{Q}$ (voir aussi [**DE06**]).

3.3.3. Troisième étape. — Points rationnels sur la réduction de $\mathrm{H}_r(\widetilde{G}, \widetilde{C})$.

D'après [**Wew98**], $\mathbf{H}_r(\widetilde{G}, \widetilde{C})$ est un schéma lisse et de type fini sur $\mathbb{Z}[1/|\widetilde{G}|]$. Pour toute place v telle que $p_v \not| |\widetilde{G}|$, la composante **HM** a bonne réduction en v. En particulier, la composante **HM** a bonne réduction en toute place $v \in S$. Donc la fibre spéciale $\mathbf{HM}_{v,0}$ de $\mathbf{HM} \otimes_{\mathbb{Z}[1/|\widetilde{G}|]} R_v$ est géométriquement irréductible.

Le corps résiduel κ_v est un corps fini. D'après les estimations de Lang-Weil, il existe une constante $C(r, |\widetilde{G}|)$ ne dépendant que de r et de $|\widetilde{G}|$ (et donc de G seulement) telle que si q_v est supérieur à cette constante, alors il existe des points κ_v-rationnels non-ramifiés sur $\mathbf{HM}_{v,0}$.

Ces points correspondent à des G-revêtements de groupe $\widetilde{G}$, de type de ramification $\widetilde{C}$ et de corps des modules κ_v. Ces G-revêtements sont en fait

définis sur κ_v car le corps des modules est un corps de définition dans le cas où le corps de base est un corps fini [**DD97**, corollaire 3.3].

3.3.4. Quatrième étape. — Relèvement des κ_v-revêtements.

Comme $\mathrm{H}_r(\widetilde{G},\widetilde{C})$ est un schéma lisse, on peut appliquer le lemme de Hensel sur $\mathrm{H}_r(\widetilde{G},\widetilde{C})$. On déduit que, pour tout $v\in S$, on peut relever les points κ_v-rationnels de l'étape précédente en des points K_v-rationnels de la composante **HM** de $\mathrm{H}_r(\widetilde{G},\widetilde{C})$. Ces points K_v-rationnels, qui correspondent à des G-revêtements de groupe $\widetilde{G}$, sont dans une composante **HM**. On note U_v le sous-ensemble ouvert de $\mathbf{HM}(K_v)$ pour la topologie v-adique qui correspond aux G-revêtements définis sur K_v avec diviseur de ramification étale en v. Les points K_v-rationnels qu'on vient de construire sont dans U_v.

3.3.5. Cinquième étape. — Approximation.

En utilisant la propriété locale-globale de $K^{\mathrm{tot}S}$ [**MB89**] [**MB01b**], on trouve des points $K^{\mathrm{tot}S}$-rationnels sur la composante **HM** qui sont dans U_v pour tout $v\in S$. D'après [**DDMB04**, corollaire 1.4], ce point correspond à un G-revêtement $\widetilde{f}:\widetilde{X}\to\mathbb{P}^1$ défini sur $K^{\mathrm{tot}S}$. Par notre construction, ce G-revêtement $\widetilde{f}$ est défini sur une extension galoisienne L de K qui est totalement décomposée dans K_v, pour tout $v\in S$. De plus, le diviseur de ramification de $\widetilde{f}$ est étale en tout point $v\in S$. Comme on a $Z(\widetilde{G})=\{1\}$ et $p_v\not|\,|G|$, alors en utilisant [**Bec91**, proposition 2.3], on peut affirmer que v n'est pas un premier de ramification verticale pour $\widetilde{f}$, pour tout $v\in S$. On déduit que la condition (Bonne-réduction) du théorème global §3.2.2 est satisfaite.

3.3.6. Sixième étape. — La propriété de Hilbert-Grunwald.

On fixe une constante $c(G)$ de telle sorte que $c(G)\geq C(r,|\widetilde{G}|)$ et qu'on puisse appliquer l'inégalité de Lang-Weil dans la troisième étape. Par construction, le morphisme surjectif $\epsilon:\widetilde{G}\to G$ est scindé, on note $s:G\to\widetilde{G}$ une section. Si $\underline{\varphi}:(\varphi_v:G_{K_v}\to G)_{v\in S}$ est un problème de Grunwald non-ramifié de groupe G, alors $s\underline{\varphi}:(s\varphi_v:G_{K_v}\to\widetilde{G})_{v\in S}$ est un problème de Grunwald non-ramifié du groupe $\widetilde{G}$. D'après le cas global (voir §3.2.2), le revêtement $\widetilde{f}$ vérifie la conclusion de Hilbert-Grunwald (HGr-spec) pour $(\widetilde{G},S,s\underline{\varphi})$. On note $\widetilde{F}/L(T)$ la G-extension de groupe $\widetilde{G}$ correspondant à $\widetilde{f}$ et F le sous-corps de $\widetilde{F}$ qui est fixé par le noyau de ϵ. On déduit que $F/L(T)$ est une G-extension de groupe G et on note $f:X\to\mathbb{P}^1$ le G-revêtement correspondant à $F/L(T)$.

Le revêtement f est un G-revêtement de groupe G défini sur L, où L/K est une extension galoisienne totalement décomposée, et qui vérifie les conditions (Bonne-réduction) et (HGr-spec) pour $(G, S, \underline{\varphi})$. D'où le résultat.

3.3.7. Complément. — La même preuve marche pour $K = \kappa(x)$ où κ est un corps de caractéristique $p \not| 6|G|$ tel que :

(i) κ est PAC et tout groupe cyclique est un quotient de G_κ, ou
(ii) κ est un corps fini de cardinal $q \geq c(G)$.

En effet, pour tout $v \in S$, on peut également trouver, dans la troisième étape, des G-revêtements de corps des modules κ. D'après [**DD97**, corollaire 3.3], le corps des modules est bien aussi un corps de définition. Voir aussi §3.2.2.1 où on a expliqué comment d'autres arguments de la preuve du théorème 3.1.2 doivent être adaptés au cas de corps résiduels PAC.

3.4. Applications

On va donner quelques applications du théorème 3.1.2 et du théorème 3.1.3.

3.4.1. Théorème d'irréductibilité de Hilbert effectif. — On se place dans le cas où $B = \mathbb{P}^1$ et $K = \mathbb{Q}$ (pour simplifier). On fixe un problème de Grunwald non-ramifié $\underline{\varphi} = (\varphi_v)_{v\in S}$ tel que $p_v \not| |G|, p_v \geq C(r, |G|)$ et que la condition (Bonne-réduction) du théorème 3.1.2 soit satisfaite pour tout $v \in S$. Par le théorème 3.1.2, la conclusion (HGr-spec) implique qu'il existe des points $t_0 \in \mathbb{P}^1(\mathbb{Q})$ tels que le groupe de Galois de la spécialisation $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ soit exactement G, ce qui correspond à la conclusion du théorème d'irréductibilité de Hilbert.

De plus, on peut choisir ces points t_0 de la forme $(am + b)_{m\in\mathbb{Z}}$ où $a = a_0 \prod_{v\in S} p_v$ avec $a_0 \in \mathbb{N}$ ne dépendant que de f et b un entier qui vient de la propriété d'approximation faible (voir aussi [**Fri74**] où ce type de conclusion apparait déjà). De plus, par l'effectivité de notre méthode, on obtient une borne pour le plus petit entier $t_0 \geq 0$ tel que l'extension spécialisée $\mathbb{Q}(X)_{t_0}/\mathbb{Q}$ soit une extension galoisienne de groupe G qui ne dépend que de $|G|, r$ et des plus petits premiers $p \not| |G|$ tel que la condition (Bonne-réduction) du théorème 3.1.2 soit satisfaite.

3.4.2. Lien avec le problème de Grunwald-Wang. — Une conséquence immédiate du théorème 3.1.3 est la version suivante du théorème de Grunwald-Wang.

Corollaire 3.4.1. — *Soient K un corps de nombres, G un groupe fini et S un ensemble fini de places de K tel que $p_v \not| |G|$ et $q_v \geq c(G)$, pour tout $v \in S$. Alors tout problème de Grunwald non-ramifié $\underline{\varphi} = (\varphi_v : G_{K_v} \to G)_{v\in S}$ a une L-solution où L est une extension galoisienne de K totalement décomposée dans K_v, pour tout $v \in S$.*

De plus d'après le théorème 3.1.2, on peut prendre $L = K$ si on sait réaliser G comme groupe de Galois d'un G-revêtement défini sur K. Dans ce cas, on prend p_v assez grand de telle sorte que la condition (Bonne-réduction) soit satisfaite. Ainsi un tel G-revêtement permet de résoudre tout problème de Grunwald non-ramifié $\underline{\varphi}$ avec $p_v \gg 1$ ($v \in S$). Autrement dit, on a le résultat suivant :

Corollaire 3.4.2. — *Supposons que G soit un groupe de Galois régulier sur K. Alors il a la propriété de Grunwald non-ramifiée suivante : pour tout ensemble fini S de places de K avec $p_v \gg_G 1$,*

(Gr-nr) l'ensemble $\prod_{v\in S} Hom_{ur}(G_{K_v}, G)^{\equiv}$ est dans l'image de l'application de Grunwald $Gr_{K,S} : Epi(G_K, G) \to \prod_{v\in S} Hom(G_{K_v}, G)^{\equiv}$, où $Hom_{ur}(G_{K_v}, G)^{\equiv}$ est l'ensemble de tous les morphismes non-ramifiés $\varphi_v \in Hom(G_{K_v}, G)$ vus à conjugaison près par des éléments de G.

La condition sur p_v ne peut pas être totalement éliminée dans cet énoncé (et donc dans le théorème 3.1.2) : Le contre-exemple de Wang affirme que le problème de Grunwald non-ramifié à une réponse négative pour la valuation 2-adique et le groupe $G = \mathbb{Z}/8\mathbb{Z}$ [**Wan48**].

3.4.3. Lien avec le problème régulier inverse de Galois (RIGP). — Si $E/\mathbb{Q}$ est une extension galoisienne, on note $\pi^E_{\mathrm{ntd}}(x)$ le nombre de nombres premiers $p \leq x$ qui ou bien ne sont pas totalement décomposés dans $E/\mathbb{Q}$ ou bien sont ramifiés dans $E/\mathbb{Q}$. D'après le théorème de densité de Čebotarev, on sait que : pour une extension galoisienne $E/\mathbb{Q}$ de groupe G, on a :

$$\pi^E_{\mathrm{ntd}}(x) \sim_E (1 - \frac{1}{|G|}) \frac{x}{\log x}$$

De plus, Lagarias et Odlyzko ont donné, dans [**LO77**], une version effective du théorème de Čebotarev. Ils ont prouvé que pour toute extension galoisienne $E/\mathbb{Q}$ de groupe G, on a :

$$\pi^E_{\mathrm{ntd}}(x) \geq \pi(x) - \frac{2}{|G|} \frac{x}{\log x}, si \log x \geq \beta |G| \log^2 |d_E|$$

où β est une constante absolue et $\pi(x)$ est le nombre des premiers $\leq x$.

On a la conséquence suivante du théorème 3.1.3 :

Corollaire 3.4.3. — *Soit G un groupe fini. Supposons qu'il existe deux fonctions $l(x)$ et $m(x)$ qui tendent vers l'infini quand $x \to \infty$ telles que la propriété suivante soit satisfaite : si $E/\mathbb{Q}$ est une extension galoisienne de groupe G et de discriminant d_E, on a :*

$(*)$ $\pi_{ntd}^{E}(x) \geq m(x)$, *si* $\log|d_E| \leq xl(x)$

Alors il n'existe pas de G-extension de groupe G défini sur $\mathbb{Q}$.

D'après le résultat de Lagarias et Odlyzko, la condition $(*)$ avec $\log|d_E| \leq xl(x)$ remplacé par $\beta|G|\log^2|d_E| \leq \log x$ est satisfaite pour tout groupe G. Si on trouve un seul groupe G qui vérife $(*)$, alors on peut affirmer que le problème RIGP a une réponse négative pour ce groupe.

Démonstration. — Fixons $l(x)$ et $m(x)$ deux fonctions qui tendent vers l'infini quand $x \to \infty$ vérifiant la condition $(*)$. Supposons par l'absurde qu'il existe une G-extension $F/\mathbb{Q}(T)$ de groupe G. On note r le nombre de points de branchement de cette G-extension. On fixe $p_0 > \max(|G|, C(r,|G|))$ un entier tel que la condition (Bonne-réduction) du théorème principal 3.1.2 soit satisfaite pour tout $p \geq p_0$. On choisit p_1 un entier tel que $p_1 \geq p_0$ et que l'intervalle $[p_0, p_1]$ contient au moins $|G|$ nombres premiers.

Pour tout $x > p_1$, on considère S_x l'ensemble de tous les premiers p tels que $p_1 < p < x$. On considère le problème de Grunwald $\underline{\varphi} = (\varphi_p)_{p\in S_x}$ pour lequel $\varphi_p : G_{\mathbb{Q}_p} \to G$ est trivial. Par le théorème 3.1.2, il existe des spécialisations $F_{t_0}/\mathbb{Q}$ de $F/\mathbb{Q}(T)$ en $t_0 \in \mathbb{Q}$ (où t_0 dépend de x) qui sont solution du problème de Grunwald $\underline{\varphi}$. On déduit que $F_{t_0}/\mathbb{Q}$ est non-ramifié et totalement décomposé dans $\mathbb{Q}_p$, pour tout $p \in S_x$.

De plus, par les même arguments de §3.2.2, on peut, en ajoutant à S_x les $|G|$ premiers dans $[p_0, p_1]$, assurer que $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) = G$. Ainsi l'extension $F_{t_0}/\mathbb{Q}$ est galoisienne de groupe G et vérifie $\pi_{\mathrm{ntd}}^{F_{t_0}}(x) \leq \pi(p_1)$. Cela contredit $(*)$, si on montre que $\log|d_{F_{t_0}}| \leq xl(x)$ pour tout x assez grand.

Comme expliqué dans 3.4.1, on peut choisir $t_0 \in \mathbb{N}$ tel que $t_0 \leq c_1 \prod_{p\in S_x} p$, avec c_1 dépendant de $F/\mathbb{Q}(T)$. D'autre part, si $P(T,Y)$ est le polynôme irréductible d'un élément primitif entier de $F/\mathbb{Q}(T)$ et $\triangle(T) \in \mathbb{Z}[T]$ le discriminant de $P(T,Y)$, alors on a $|d_{F_{t_0}}| \leq |\triangle(t_0)| \leq c_2|t_0|^{c_3}$ avec c_2 et c_3 deux constantes dépendant de $F/\mathbb{Q}(T)$. Pour $x \to \infty$, on a $\log(\prod_{p\in S_x} p) \sim x$. On

déduit que $\log|d_{F_{t_0}}| \leq c_4 x$ avec c_4 dépendant de $F/\mathbb{Q}(T)$. Ce qui implique que $\log|d_{F_{t_0}}| \leq xl(x)$, pour x assez grand. □

3.4.4. Lien avec RIGP sur les corps p-adiques. — Soient K un corps de nombres et G un groupe fini. On fixe un ensemble fini S de places de K tel que $p_v \not| 6|G|$ et $q_v \geq c(G)$ pour tout $v \in S$, où $c(G)$ est la constante définie dans la preuve du théorème 3.1.3. D'après [**Har87**], [**Dèb95**] et [**Pop96**], on sait que RIGP a une réponse positive pour tout corps ample. On déduit qu'il existe un G-revêtement de groupe G défini sur $K^{\mathrm{tot}S}$. Mais la méthode utilisée (patching) conduit à des extensions pour lesquelles toute place v de S est une place de mauvaise réduction pour f.

Au contraire notre théorème 3.1.3, permet de construire un G-revêtement $f : X \to \mathbb{P}^1$ de groupe G défini sur $K^{\mathrm{tot}S}$ qui satisfait la condition (Bonne-réduction) pour tout $v \in S$. Plus précisément, on a l'énoncé suivant :

Corollaire 3.4.4. — *Soient K et G comme précédemment. Pour tout ensemble fini S de places de K tel que $p_v \not| 6|G|$ et $q_v \geq c(G)$, il existe un G-revêtement $f : X \to \mathbb{P}^1$ de groupe G défini sur K^{totS} tel que toute place v dans S soit une place de bonne réduction pour f.*

3.4.5. Corps de fonctions en une variable. — Supposons que $B = \mathbb{P}^1$, et κ soit ou bien un corps PAC ou bien un corps fini de cardinal assez grand. On note $K = \kappa(x)$ le corps de fonctions d'une variable x sur un corps κ. On pose p la caractéristique de κ. Fixons un ensemble fini de points x_v de $\mathbb{P}^1(\kappa)$ et notons S l'ensemble des valuations v de K correspondant à ces points. Pour tout $v \in S$, on fixe E^v/κ une extension galoisienne de groupe $H_v \subset G$ et on note $\varphi^v : G_\kappa \to G$ le morphisme correspondant. L'extension $E^v((x - x_v))/\kappa((x - x_v))$ est non-ramifiée.

Soit $f : X \to \mathbb{P}^1$ un G-revêtement de groupe G défini sur $K = \kappa(x)$ avec r points de branchement. Supposons que $p \not||G|$ et que les conditions suivantes soient satisfaites :

(Bonne-réduction) *pour tout $v \in S$, le diviseur de branchement $\boldsymbol{t} = \{t_1, \ldots, t_r\}$ est étale et v n'est pas un premier de ramification verticale pour f.*

(Hypothèse sur le corps résiduel) *On suppose que κ vérifie une de ces deux conditions :*

- *ou bien κ est PAC et tout groupe cyclique est un quotient de G_κ.*
- *ou bien κ est un corps fini de cardinal $q \geq C(r, |G|)$.*

Dans ce contexte, en utilisant §3.2.2 si κ est fini et §3.3.7 si κ est PAC, on obtient l'énoncé suivant :

Corollaire 3.4.5. — *Avec les hypothèses (Bonne-réduction) et (Hypothèse sur le corps résiduel), le G-revêtement f vérifie la conclusion de spécialisation de Hilbert-Grunwald suivante :*

(HGr-spec) Il existe des spécialisations $K(x)_{t_0(x)}/\kappa(x)$ de f en des points $t_0(x) \in \mathbb{P}^1(\kappa(x))\backslash \boldsymbol{t}$ de groupe G telles que le corps résiduel de $\kappa(x)(X)_{t_0(x)}/\kappa(x)$ en $x = x_v$ soit isomorphe à E^v/κ, pour tout $v \in S$. De plus, l'ensemble des points $t_0(x)$ ayant cette propriété contient un ouvert non vide de la forme $\mathbb{P}^1(\kappa(x)) \cap \prod_{v\in T} U_v$ avec $U_v \subset \mathbb{P}^1(\kappa((x - x_v)))$ et T un ensemble fini de places de K tel que $T \supset S$.

D'autre part, le théorème 3.1.3 affirme l'existence de tels revêtements f mais définis sur une extension galoisienne de $K = \kappa(x)$ totalement décomposée dans K_v, pour tout $v \in S$ (voir §3.2.2.1, cas (b)).

BIBLIOGRAPHIE

[Art68] Emil Artin. Algebraic numbers and algebraic functions. *Nelson*, 1968.

[Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419 :27–53, 1991.

[Bec94] Sybilla Beckmann. Is every extension of $\mathbf{Q}$ the specialization of a branched covering ? *J. Algebra*, 164 :430–451, 1994.

[Bla98] Elena V. Black. Arithmetic lifting of Dihedral extensions. *J. Algebra*, 203 :12–29, 1998.

[Bla99] Elena V. Black. Deformations of Dihedral 2-group extensions of fields. *Trans. Amer. Math. Soc.*, 351 :3229–3241, 1999.

[CT00] Jean-Louis Colliot-Thélène. Rational connectedness and Galois cover of projective line. *Ann. of Math*, 151 :359–373, 2000.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers : field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30 :303–338, 1997.

[DD04] Pierre Dèbes and Bruno Deschamps. Corps ψ-libres et théorie inverse de Galois infinie. *J. Reine Angew. Math.*, 574 :197–218, 2004.

[DDMB04] Pierre Dèbes, Jean-Claude Douai, and Laurent Moret-Bailly. Descent varieties for algebraic covers. *J. Reine Angew. Math.*, 574 :51–78, 2004.

[DE06] Pierre Dèbes and Michel Emsalem. Harbater-Mumford components and Hurwitz towers. *J. Math. Inst. Jussieu*, 5(3) :351–371, 2006.

[Dèb95] Pierre Dèbes. Covers of $\mathbb{P}^1$ over the p-adics. *In Recent developments in the Inverse Galois Problem*, 186 :217–238, 1995.

[Dèb99] Pierre Dèbes. Galois covers with prescribed fibers : the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Paris*, 28 :273–286, 1999.

[Dèb09] Pierre Dèbes. Arithmétique des revêtement de la droite. *Cours de Master 2, univ. Lille1*, 2009. math.univ-lille1.fr/ pde/.

[Del74] Pierre Deligne. La conjecture de Weil I. *Publ. Math. IHES*, 43 :273–308, 1974.

[Del80] Pierre Deligne. La conjecture de Weil II. *Publ. Math. IHES*, 52 :137–252, 1980.

[Des95] Bruno Deschamps. Existence de points p-adiques, pour tout p, sur un espace de Hurwitz. *In recent developments in the Inverse Galois Problem*, 186 :239–274, 1995.

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreductibility theorem. *Sém. théorie des nombres, Paris 1988-1989*, 91 :241–248, 1990.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. first edition 1986.

[Fri74] Michael D. Fried. On Hilbert's irreductibility theorem. *J. Number Theory*, 6 :211–231, 1974.

[Fri95] Michael D. Fried. Introduction to modular towers : generalizing dihedral group–modular curve connections. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 111–171. Amer. Math. Soc., Providence, RI, 1995.

[Ful69] William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. of Math.*, 90 :542–575, 1969.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4) :771–800, 1991.

[FvdP81] Jean Fresnel and Marius van der Put. Géométrie analytique rigide et applications. *Birkhauser*, 1981.

[GM71] Alexandre Grothendieck and Jacob P. Murre. *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, volume 208 of *LNM*. Springer, 1971.

[Gro67] Alexandre Grothendieck. EGA Etude locale des schémas et des morphismes de schémas. *Publ. Math. IHES*, 32 :329–351, 1967.

[Gro71] Alexandre Grothendieck. *Revêtements étales et groupe fondamental*, volume 224 of *LNM*. Springer, 1971.

[Gro73] Alexandre Grothendieck. SGA 5 Cohomologie l-adique et fonctions L. *LNM, Springer-Verlag*, 589, 1973.

[Har87] David Harbater. Galois coverings of the arithmetic line. *Lecture Notes in Math.*, 1240 :165–195, 1987.

[Har07] David Harari. Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini. *Bull. Soc. Math. France*, 135 :49–564, 2007.

[HJ98] Dan Haran and Moshe Jarden. Regular split embedding problems over complete valued fields. *Forum Mathematicum*, 10 :329–351, 1998.

[HS02] David Harari and Alexei Skorobogatov. Non-abelian cohomology and rational points. *Compositio Math*, 130 :241–273, 2002.

[JNW08] Alexander Schmidt Jurgen Neukirch and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren de mathematischen wissenschaften*. Springer, 2008.

[Jor72] Camille Jordan. Recherches sur les substitutions. *J. Liouville*, (17) :351–367, 1872.

[Lan78] Serge Lang. *Algebra*. World Student Series. Addison-Wesley, 1978.

[LO77] Jeffrey C. Lagarias and Andrew M. Odlyzko. Effective versions of the Chebotarev density theorem. *In algebraic number fields*, pages 409–464, 1977.

[MB89] Laurent Moret-Bailly. Groupes de Picard et problèmes de Skolem II. *Annales Sci. E.N.S.*, 22 :181–194, 1989.

[MB01a] Laurent Moret-Bailly. Construction de revêtements de courbes pointées. *J. Algebra*, 240 :505–534, 2001.

[MB01b] Laurent Moret-Bailly. Problèmes de Skolem sur les champs algébriques. *Comp. Math.*, 125 :1–30, 2001.

[Mil80] James S. Milne. *Etale cohomology*. Volume 33 of Princeton Mathematical Series. Princeton University Press, 1980.

[Neu79] Jurgen Neukirch. On solvable number fields. *Invent. Math*, 53 :135–164, 1979.

[Pop96] Florian Pop. Embedding problems over large fields. *Annals of Math*, 144 :1–35, 1996.

[PV05] Bernat Plans and Nuria Vila. Galois covers of $\mathbf{P}^1$ over $\mathbf{Q}$ with prescribed local or global behavior by specialization. *J. Théorie des nombres bordeaux*, 17 :271–282, 2005.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett, Boston, London, 1992.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996.

[Wan48] Shianghaw Wang. A counter-example to Grunwald's theorem. *Annals of Mathematics*, 49 :1008–1009, 1948.

[Wew98] Stefan Wewers. Construction of Hurwitz spaces. *PhD Thesis, Essen*, 1998.