C. R. Acad. Sci. Paris, t. 311, Série I, p. 273-276, 1990

Théorie des nombres/*Number Theory*

Extensions de corps globaux à ramification et groupe de Galois donnés

Laurent MORET-BAILLY

Résumé — Si K est un corps de nombres (ou un corps de fonctions d'une variable sur un corps fini) et G un groupe fini, on construit deux extensions finies $E \subset F$ de K telles que l'extension F/E soit galoisienne de groupe G, ait une structure locale donnée au-dessus d'un ensemble fini donné de places de K, et soit non ramifiée en-dehors de ces places. On utilise pour cela un théorème d'existence de solutions d'équations en entiers algébriques satisfaisant à des conditions locales sur un ensemble fini de places.

Global field extensions with given Galois group and ramification

Abstract — *If* K *is a number field, or a* 1*-variable function field over a finite field, and* G *is a finite group, we construct two finite extensions* $E \subset F$ *of* K, *such that the extension* F/E *is Galois with group* G, *has a prescribed local structure over a given finite set of places of* K, *and is unramified elsewhere. We achieve this by using an existence theorem for algebraic integer solutions of polynomial equations, satisfying local conditions at a finite set of places.*

Dans tout ce qui suit, K désigne un corps de nombres ou un corps de fonctions d'une variable sur un corps fini. On note M_K l'ensemble des places de K, et Σ une partie finie de M_K. Pour $v \in M_K$, on note K_v le complété de K en v.

1. ÉNONCÉ DU THÉORÈME. — 1.1. Fixons un groupe fini G et, pour chaque $v \in \Sigma$, une K_v-algèbre finie K'_v, galoisienne de groupe G, c'est-à-dire une K_v-algèbre étale munie d'une action de G faisant de Spec K'_v un G-torseur sur Spec K_v (il reviendrait au même de se donner pour chaque $v \in \Sigma$ un sous-groupe D_v de G, défini à conjugaison près, et une extension M_v de K_v, galoisienne de groupe D_v; on retrouve K'_v comme l'anneau $\mathrm{Hom}_{D_v}(G, M_v)$ des applications D_v-équivariantes de G dans M_v).

1.2. THÉORÈME. — *Avec les notations de* 1.1, *il existe :*

— *une extension finie* E *de* K, décomposée *en chaque* $v \in \Sigma$ (*de sorte que, pour toute place w de* E *au-dessus de v,* E_w *s'identifie à* K_v)*;*

— *une extension finie* F *de* E, *galoisienne de groupe* G, *non ramifiée hors de* Σ, *et telle que, pour tout w comme ci-dessus, la* K_v*-algèbre galoisienne* $F \otimes_E E_w$ *soit isomorphe* (*avec l'action de* G) *à* K'_v.

2. RAPPELS SUR LES DONNÉES DE SKOLEM. — 2.1. Soit S une partie finie non vide de M_K, contenant Σ et les places archimédiennes. Soit R l'anneau des S-entiers de K, et posons B = Spec R. On identifiera comme d'habitude l'ensemble $|B|$ des points fermés de B à $M_K - S$.

On désigne par $f : X \to B$ un B-schéma de type fini; on suppose que f est surjectif, que sa fibre générique X_K est géométriquement irréductible sur K, et que X est irréductible.

On se donne enfin, pour chaque $v \in \Sigma$, une extension finie galoisienne L_v du complété K_v de K en v, et un ouvert non vide Ω_v de $X(L_v)$ (pour la topologie déduite de v), formé de points lisses et invariant sous $\mathrm{Gal}(L_v/K_v)$.

Note présentée par Jean-Pierre SERRE.

0764-4442/90/03110273 $ 2.00

2.2. DÉFINITION ([1], 1.2). — *On appelle* donnée de Skolem *un couple*

$$\mathscr{S} = (X \xrightarrow{f} B, \{(L_v, \Omega_v)\}_{v \in \Sigma})$$

vérifiant les conditions de 2.1. *On dit que* $\mathscr{S}$ *est* complète *si* $\Sigma = S$ (*i. e. si* $\Sigma \cup |B| = M_K$), incomplète *sinon.*

On appelle point entier *de* $\mathscr{S}$ *un fermé irréductible* Y *de* X, *fini et surjectif sur* B, *tel que, pour tout* $v \in \Sigma$, $Y \otimes_R L_v$ *soit formé de points* L_v*-rationnels appartenant à* Ω_v.

2.3. THÉORÈME ([1], théorème 1.3). — *Toute donnée de Skolem incomplète admet un point entier.*

2.4. *Remarque.* — Dans [1], le B-schéma X est supposé séparé; cette restriction est inutile car on peut toujours se ramener au cas séparé en remplaçant X, comme expliqué dans *loc. cit.*, 1.10.1, par un ouvert non vide (par exemple affine) de X.

3. EXTENSION À CERTAINES DONNÉES DE SKOLEM COMPLÈTES.

3.1. THÉORÈME. — *Soit* $\mathscr{S} = (X \xrightarrow{f} B, \{(L_v, \Omega_v)\}_{v \in \Sigma})$ *une donnée de Skolem. On suppose vérifiée la condition suivante :*

(∗) *Pour tout ensemble fini* T_K *de points fermés lisses de* X_K, *il existe un sous-schéma* Z_K *de* X_K, propre et géométriquement irréductible *sur* K, *contenant* T_K, *et lisse sur* K *aux points de* T_K.

Alors $\mathscr{S}$ *admet un point entier.*

3.2. *Remarque.* — La condition (∗) ci-dessus est notamment vérifiée dans les deux cas suivants :

(i) X_K est propre sur K;

(ii) il existe une immersion ouverte $j : X_K \to \bar{X}_K$, où $\bar{X}_K$ est une K-variété projective et où $\bar{X}_K - j(X_K)$ est de codimension $\geqq 2$ dans $\bar{X}_K$.

3.3. *Démonstration de* 3.1. — Traitons d'abord le cas où X_K est propre sur K. Il existe alors un ouvert non vide U de B tel que $f^{-1}(U)$ soit propre sur U; soit b un point fermé de U et posons $B' = B - \{b\}$, $X' = f^{-1}(B')$. Alors la donnée de Skolem $\mathscr{S}' = (X' \to B', \{(L_v, \Omega_v)\}_{v \in \Sigma})$ est incomplète; donc admet d'après 2.3 un point entier Y'. Si Y désigne l'adhérence de Y' dans X, le choix de b implique que Y est fini surjectif sur B donc est un point entier de $\mathscr{S}$.

Dans le cas général, on construit comme dans [1], 2.2, un fermé T de X, quasi-fini et surjectif sur B, tel que T_K soit formé de points lisses de X_K et que, pour tout $v \in \Sigma$, on ait $T(L_v) \cap \Omega_v \neq \varnothing$. La condition (∗) appliquée à T_K fournit un fermé Z_K de X_K. Soit Z l'adhérence de Z_K dans X et posons, pour tout $v \in \Sigma$, $\Omega'_v = \Omega_v \cap Z_{\text{lisse}}(L_v)$. Alors, $(Z \to B, \{(L_v, \Omega'_v)\}_{v \in \Sigma})$ est une donnée de Skolem. Comme Z_K est propre elle admet un point entier Y, qui est aussi un point entier de $\mathscr{S}$. ■

4. DÉMONSTRATION DU THÉORÈME 1.2.

— On reprend les notations du paragraphe 1.

4.1. Établissons d'abord la variante plus faible de 1.2 obtenue en exigeant seulement que F soit une E-algèbre étale (pas nécessairement un corps). On peut supposer Σ non vide (en lui ajoutant le cas échéant une place v_0 et en prenant par exemple $K'_{v_0} = (K_{v_0})^G$). Soit R l'anneau des Σ-entiers de K, et posons $B = \operatorname{Spec} R$. Soit U le plus grand ouvert de $(\mathbb{P}^2_B)^G$ sur lequel G opère librement par permutation des facteurs, et notons X le B-schéma quotient U/G. Alors X vérifie les conditions de 2.1, ainsi que la condition (ii) de 3.2 [en posant $\bar{X}_K = (\mathbb{P}^2_K)^G/G$] donc aussi la condition (∗) de 3.1.

On vérifie aisément que, pour tout B-schéma T, la donnée d'un B-morphisme de T dans X équivaut à celle d'un G-torseur T′ sur T, muni d'un T-plongement de T′ dans $\mathbb{P}^2_T$. Pour tout $v \in \Sigma$, soit Ω_v l'ensemble des $x \in X(K_v)$ tels que le torseur correspondant sur Spec K_v (qui n'est autre que la fibre en x du morphisme naturel $U \to X$) soit isomorphe à Spec K'_v. Alors Ω_v est un *ouvert* de $X(K_v)$: en effet le faisceau I des isomorphismes de G-torseurs sur X_{K_v} entre U_{K_v} et le torseur constant $X \times_B \mathrm{Spec}\, K'_v$ est représentable par un schéma étale sur X_{K_v}, de sorte que l'application naturelle $I(K_v) \to X(K_v)$, qui a pour image Ω_v, est ouverte. D'autre part, Ω_v est *non vide* car il résulte du théorème de l'élément primitif (et du fait que K_v est infini) que Spec K'_v est plongeable dans la droite affine $\mathbb{A}^1_{K_v}$, *a fortiori* dans $\mathbb{P}^2_{K_v}$.

Nous sommes donc dans les conditions d'application du théorème 3.1, de sorte que la donnée de Skolem $\mathscr{S} = (X \xrightarrow{f} B, \{(K_v, \Omega_v)\}_{v \in \Sigma})$ admet un point entier Y. Il est alors immédiat que le corps de fonctions E de Y, et la E-algèbre étale F fibre de $U \to X$ au point générique de Y, vérifient les conditions cherchées.

4.2. Il reste à forcer F à être un corps. Pour cela, choisissons, pour tout sous-groupe cyclique C de G (ou seulement pour toute classe de conjugaison de tels sous-groupes), un point $v(C)$ de $|B|$ [de telle sorte que $v(C) \neq v(C')$ si $C \neq C'$] et une extension $M_{v(C)}$ de $K_{v(C)}$, galoisienne de groupe C et non ramifiée (un tel choix est possible puisque le corps résiduel du point $v(C)$ est fini). Appliquons alors la construction de 4.1 en remplaçant Σ par la réunion de Σ et des $v(C)$ et en posant $K'_{v(C)} = \mathrm{Hom}_C(G, M_{v(C)})$. On obtient ainsi une extension E de K et une E-algèbre étale F [qui est encore non ramifiée aux points $v(C)$, vu le choix des $K'_{v(C)}$]. Le G-ensemble $\pi_0(\mathrm{Spec}\, F)$ est isomorphe à G/H où H est un sous-groupe de G; pour voir que F est un corps il suffit de montrer que H = G. Or, pour chaque $C \subset G$ cyclique, si w est une place de E au-dessus de $v(C)$, on a $\pi_0(\mathrm{Spec}\, F_w) \simeq G/C$, et le morphisme naturel $F \to F_w$ induit donc un G-morphisme $G/C \to G/H$, ce qui implique que H contient un conjugué de C. Le lemme bien connu suivant montre alors que H est bien égal à G :

4.3 Lemme. — *Soient* G *un groupe fini,* H *un sous-groupe de* G *rencontrant toutes les classes de conjugaison de* G. *Alors* H = G. ■

4.4. *Remarque.* — Dans la construction de 4.1, la variété X_K est K-*unirationnelle*, et, lorsqu'on lui applique la condition (*), on peut imposer à Z_K d'être une courbe K-rationnelle. On n'utilise donc, pour obtenir 1.2, que le cas particulier de 2.3 où X_K est supposée K-unirationnelle, qui se trouve déjà dans [2].

4.5. *Remarque.* — Notons [B/G] le quotient (au sens des champs) de B par l'action triviale de G (c'est-à-dire le « champ classifiant » de G sur B, *cf.* [3]). Alors le théorème 1.2 peut être vu comme un théorème d'existence de points entiers pour la donnée de Skolem complète (généralisée aux champs) $([B/G] \to B, \{(K_v, W_v)\}_{v \in \Sigma})$ où, pour $v \in \Sigma$, W_v est la sous-catégorie strictement pleine de $[B/G](K_v)$ formée des G-torseurs isomorphes à Spec K'_v. De fait, on peut généraliser aux champs algébriques (au sens d'Artin [4]) le théorème 2.3 sur les données incomplètes, ainsi que le théorème 3.1, au moins lorsque X_K est propre sur K (ce qui est le cas pour X = [B/G]).

Note remise et acceptée le 18 juin 1990.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] L. MORET-BAILLY, Groupes de Picard et problèmes de Skolem II, *Ann. scient. Ec. Norm. Sup.*, 22, 1989, p. 181-194.

[2] D. CANTOR et P. ROQUETTE, On Diophantine equations over the ring of all algebraic integers, *J. Number Theory*, 18, 1984, p. 1-26.

[3] P. DELIGNE et D. MUMFORD, The Irreducibility of the Space of Curves of Given Genus, *Pub. Math. I.H.E.S.*, 36, p. 75-109.

[4] M. ARTIN, Versal Deformations and Algebraic Stacks, *Inv. Math.*, 27, 1974, p. 165-189.

I.R.M.A.R., Université de Rennes-I,
Campus de Beaulieu, 35042 *Rennes Cedex.*