Sur la R-équivalence de torseurs sous un groupe fini *

Laurent Moret-Bailly †

IRMAR (Institut de Recherche Mathématique de Rennes, UMR 6625 du CNRS)
Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex
Laurent.Moret-Bailly@univ-rennes1.fr
http://www.maths.univ-rennes1.fr/~moret/

*Accepté pour publication au *Journal of Number Theory* le 20 septembre 2002.

†L'auteur est membre du réseau européen « Arithmetic Algebraic Geometry » (contrat HPRN-CT-2000-00120).

Résumé

On donne des critères de R-équivalence pour les torseurs sous un schéma en groupes fini constant sur un corps. En particulier, un énoncé de dévissage galoisien permet, en utilisant la notion de bitorseur, de formaliser et de généraliser un théorème de Philippe Gille dans le cas des corps locaux : ce dernier est notamment étendu aux corps locaux supérieurs.

Abstract

We give criteria for R-equivalence of torsors under finite constant group schemes over a field. In particular, using bitorsors, we obtain a Galois dévissage result which formalises and generalises a theorem of Philippe Gille in the case of local fields; for instance, Gille's theorem is shown to extend to higher local fields.

Classification AMS 2000 : 12G05, 14G20, 18G50.

1 Introduction

1.1 R-équivalence.

Soient K un corps et A l'anneau semi-local de la droite affine $\mathbb{A}^1_K$ en $\{0,1\}$. On rappelle que si H est un K-schéma en groupes, deux H-torseurs X et Y sur K (*i.e.* sur $\operatorname{Spec} K$, et pour la topologie fppf) sont dits *élémentairement R-équivalents* s'il existe un H-torseur sur $\operatorname{Spec} A$ induisant (à isomorphisme près) X en 0 et Y en 1. La R-équivalence est par définition la relation d'équivalence engendrée par la R-équivalence élémentaire, sur la classe des H-torseurs sur K. Elle induit naturellement une relation d'équivalence, encore appelée R-équivalence, sur l'ensemble $\mathrm{H}^1(K,H)$ des *classes d'isomorphie* de H-torseurs sur K (le lien avec la définition de $\mathrm{H}^1(K,H)$ par cocycles est établi, avec toute la généralité voulue, dans [Gir], III, 3.6.4 et 3.6.5, ainsi, pour la cohomologie galoisienne, que dans [D-G], III, § 5, n$^{\mathrm{os}}$ 3 et 4).

On a en particulier des sous-ensembles

$$\mathrm{R}_{\mathrm{el}}(K,H) \subset \mathrm{R}(K,H) \subset \mathrm{H}^1(K,H)$$

où $\mathrm{R}(K,H)$ (resp. $\mathrm{R}_{\mathrm{el}}(K,H)$) est l'ensemble des classes de H-torseurs R-équivalents (resp. élémentairement R-équivalents) au torseur trivial.

D'autre part, si L est une extension de K, on note comme d'habitude $\mathrm{H}^1(L/K,H) \subset \mathrm{H}^1(K,H)$ l'ensemble des classes de H-torseurs trivialisés par L.

Dans ce qui suit, on considérera surtout des schémas en groupes finis étales sur K, et des torseurs sous iceux ; si l'on fixe une clôture séparable K_{s} de K et que l'on pose $\mathrm{Gal}_K = \mathrm{Gal}\,(K_{\mathrm{s}}/K)$, on peut identifier un K-schéma fini étale X au Gal_K-ensemble fini $X(K_{\mathrm{s}})$, ce que nous ferons systématiquement. Noter que Gal_K lui-même, ainsi que ses sous-groupes distingués et ses quotients, peut être considéré comme un K-schéma en groupes profini, lorsqu'on le munit de son action sur lui-même par conjugaison.

1.2 Notations.

Soient K, K_s et Gal_K comme ci-dessus, et soit $M \subset K_s$ une extension galoisienne de K, non nécessairement finie, de groupe Π (qui est donc un groupe profini, quotient de Gal_K par un sous-groupe fermé distingué). On suppose donnée une suite exacte

$$1 \longrightarrow \Gamma \longrightarrow \Pi \longrightarrow \pi \longrightarrow 1 \tag{1.2.1}$$

de groupes profinis (ici et dans la suite, tous les morphismes de groupes profinis sont supposés continus) ; on note $M_0 \subset M$ le corps des invariants de Γ, de sorte que $\pi = \mathrm{Gal}\,(M_0/K)$.

Enfin on se donne un groupe fini G, que l'on voit comme K-schéma en groupes constant.

1.3 Théorème. *Avec les notations de* 1.2*, on suppose que :*

(i) *la suite exacte* (1.2.1) *de groupes profinis est* scindée *;*

(ii) *on a* $\mathrm{H}^1(M_0/K, G) \subset \mathrm{R}(K, G)$ *;*

(iii) *pour tout K-schéma en groupes H quotient de Γ, dont le groupe sous-jacent est isomorphe à un sous-groupe de G, on a* $\mathrm{H}^1(M/K, H) \subset \mathrm{R}(K, H)$.

Alors on a $\mathrm{H}^1(M/K, G) \subset \mathrm{R}(K, G)$.

1.4 Remarques sur les hypothèses.

1.4.1 Comme le lecteur pourra le constater (voir la preuve du théorème 8.5 et plus précisément le diagramme (8.5.2)) on peut remplacer l'hypothèse (i) par la suivante, plus faible : pour tout morphisme continu $\theta : \Pi \to G$, le morphisme naturel $\overline{\theta} : \pi \to \theta(\Pi)/\theta(\Gamma)$ (déduit de θ par passage au quotient) se relève en un morphisme continu $\pi \to \theta(\Pi)$.

1.4.2 La preuve utilise de façon cruciale l'identification de $\mathrm{H}^1(M/K, G)$ (pour G constant) avec le quotient de $\mathrm{Hom}\,(\Pi, G)$ par la conjugaison. De ce fait, elle ne s'étend pas aux schémas en groupes étales généraux, à l'exception, de manière assez formelle, de certaines *formes intérieures* de groupes constants. Plus précisément, avec les hypothèses de 1.3, soit de plus X un G-torseur (à droite, disons) *trivialisé par M* et soit G' le K-schéma en groupes $\underline{\mathrm{Aut}}_G(X)$: alors on a une bijection de $\mathrm{H}^1(K, G)$ avec $\mathrm{H}^1(K, G')$, associant au G-torseur à droite Y le K-schéma fini étale $\underline{\mathrm{Isom}}_G(X, Y)$, muni de l'action à droite évidente de G'. On voit facilement que cette bijection respecte la R-équivalence et envoie $\mathrm{H}^1(M/K, G)$ sur $\mathrm{H}^1(M/K, G')$, de sorte que l'on déduit encore de 1.3 que $\mathrm{H}^1(M/K, G') \subset \mathrm{R}(K, G')$.

1.4.3 On peut préciser l'énoncé en tenant compte de la filtration naturelle sur l'ensemble pointé $\mathrm{H}^1(K, H)$. Pour $n \in \mathbb{N}$, définissons $\mathrm{R}_n(K, H) \subset \mathrm{H}^1(K, H)$ comme suit : $\mathrm{R}_0(K, H)$ est réduit à la classe triviale, et $\mathrm{R}_{n+1}(K, H)$ est l'ensemble des classes de H-torseurs élémentairement R-équivalents à un torseur de $\mathrm{R}_n(K, H)$. Si l'on remplace l'inclusion de 1.3 (ii) par $\mathrm{H}^1(M_0/K, G) \subset \mathrm{R}_m(K, G)$ et celle de 1.3 (iii) par $\mathrm{H}^1(M/K, H) \subset \mathrm{R}_n(K, H)$, alors on peut conclure que $\mathrm{H}^1(M/K, G) \subset \mathrm{R}_{m+n}(K, G)$. Ceci résulte facilement du théorème de dévissage 8.5 et de la remarque 6.4.

1.4.4 Dans la situation de 1.3, on pourrait envisager une relation plus fine que la R-équivalence, à savoir la « $\mathrm{R}_{M/K}$-équivalence », définie comme la relation d'équivalence *dans* $\mathrm{H}^1(M/K, G)$ engendrée par la R-équivalence élémentaire. Si l'on note $\mathrm{R}(M/K, G)$ l'ensemble des G-torseurs $\mathrm{R}_{M/K}$-équivalents au torseur trivial, le lecteur pourra constater que si l'on remplace dans 1.3 l'hypothèse (ii) par $\mathrm{H}^1(M_0/K, G) \subset \mathrm{R}(M/K, G)$, et (iii) par $\mathrm{H}^1(M/K, H) \subset \mathrm{R}(M/K, H)$, alors on conclut que $\mathrm{H}^1(M/K, G) \subset \mathrm{R}(M/K, G)$. On peut de plus combiner cette variante de 1.3 avec celle de 1.4.3 ci-dessus.

1.4.5 On n'a pas inclus dans l'énoncé les remarques 1.4.3 et 1.4.4 qui précèdent, pour la raison suivante : dans les applications les plus importantes, K est un corps valué hensélien, donc est fertile (pour toute K-variété V lisse connexe, $V(K)$ est vide ou dense dans V), et dans ce cas le théorème 2 de [MB 2] montre que la R-équivalence dans $\mathrm{H}^1(K, G)$ coïncide avec la R-équivalence élémentaire, ce qui entraîne en outre que sa restriction à $\mathrm{H}^1(M/K, G)$ coïncide avec la $\mathrm{R}_{M/K}$-équivalence. On voit donc que 1.4.3 et 1.4.4 sont sans objet dans ce cas.

Le théorème 1.3 sera établi au § 8 ; auparavant, au § 3, nous en déduirons le suivant :

1.5 Théorème. *Soit K le corps des fractions d'un anneau de valuation discrète hensélien, à corps résiduel k de caractéristique $p \geq 0$, et soit G un groupe fini* d'ordre non divisible par p.

On suppose que $\mathrm{R}(k, G) = \mathrm{H}^1(k, G)$. *Alors* $\mathrm{R}(K, G) = \mathrm{H}^1(K, G)$ (et donc $\mathrm{R}_{\mathrm{el}}(K, G) = \mathrm{H}^1(K, G)$ d'après [MB 2], cf. remarque 1.4.5).

1.5.1 Remarque. Bien entendu, G est considéré ici comme groupe constant sur k et sur K respectivement.

L'hypothèse de l'énoncé est notamment vérifiée lorsque k est *fini*, comme il résulte par exemple de 2.5 plus bas. On retrouve ainsi le théorème 1 de [Gil], qui a servi de point de départ au présent travail.

Mais l'hypothèse est aussi vérifiée, trivialement, lorsque k est *séparablement clos*, et plus généralement (2.5) lorsque Gal_k est pro-cyclique.

1.5.2 Remarque. L'énoncé serait faux sans l'hypothèse sur l'ordre de G, comme le montre l'exemple suivant de Colliot-Thélène ([CT 1], Appendix) : soient $K = \mathbb{Q}_2$, $G = \mathbb{Z}/8\mathbb{Z}$, et L l'unique extension non ramifiée de degré 8 de K. Alors Spec L est un G-torseur sur K, qui n'est pas R-équivalent au torseur trivial, alors que tout G-torseur sur le corps résiduel de K l'est (cf. 2.4 (i) plus loin).

Par récurrence, on en déduit un résultat analogue pour les « corps locaux supérieurs » ; plus précisément :

1.5.3 Corollaire. *Considérons une suite de corps*

$$K = K_0,\ K_1, \ldots,\ K_n$$

où, pour chaque $i \in \{0, \dots, n-1\}$, K_i est muni d'une valuation discrète hensélienne de corps résiduel K_{i+1}, et où le groupe de Galois absolu de K_n est pro-cyclique (condition vérifiée notamment si K_n est fini ou séparablement clos).

Alors, si G est un groupe fini d'ordre premier à la caractéristique de K_n, on a $\mathrm{R}(K,G) = \mathrm{H}^1(K,G)$ (et donc encore $\mathrm{R}_{\mathrm{el}}(K,G) = \mathrm{H}^1(K,G)$, d'après [MB 2] si $n > 0$ et d'après 2.5 si $n = 0$). ∎

1.5.4 Remarque. Par exemple, on a $\mathrm{R}(K,G) = \mathrm{H}^1(K,G)$ pour tout groupe fini G, lorsque K est un corps de séries formelles de la forme $\mathbb{C}(\!(X_1)\!)\cdots(\!(X_n)\!)$; même ce cas particulier semble nouveau.

1.6 Plan de l'article.

Au § 2, nous donnons des critères simples (et sans doute plus ou moins bien connus) de R-équivalence.

Le § 3 est consacré à la preuve du théorème 1.5 à partir de 1.3.

Au § 4 on donne d'autres applications de 1.3, lorsque K est valué hensélien à corps résiduel k abélien. Ainsi, si k est fini de caractéristique différente de 2, et si G est un groupe fini quelconque, on montre que, avec les notations traditionnelles, $\mathrm{H}^1(K_{\mathrm{mod}}K_{\mathrm{ab}}/K,G) \subset \mathrm{R}_{\mathrm{el}}(K,G)$ (voir 4.3 pour un énoncé plus précis).

La preuve de 1.3 occupe le § 8 ; elle s'inspire de [Gil] et repose sur un dévissage qui est décrit dans loc. cit. en termes de cocycles, et que l'on traduit ici, de manière plus fonctorielle, dans le langage des bitorseurs. Comme ceux-ci n'ont pas encore la même popularité que les torseurs, on présente divers sorites sur cette notion (§ 5), son comportement vis-à-vis de la R-équivalence (§ 6) et le cas où l'un des groupes est constant (§ 7).

2 R-équivalence : quelques critères simples

On donne ici quelques conditions suffisantes simples de R-équivalence élémentaire pour les torseurs sous un schéma en groupes, le plus souvent fini, sur un corps.

Dans tout ce paragraphe, K désigne un corps, K_{s} une clôture séparable de K, et $\mathrm{Gal}_K = \mathrm{Gal}\,(K_{\mathrm{s}}/K)$. Tous les schémas en groupes considérés seront affines de type fini, et « G-torseur » signifie « G-torseur pour la topologie fppf ». On note $\mathrm{cd}(K)$ la dimension cohomologique de K.

Plutôt que la R-équivalence, nous considérerons ici la propriété suivante :

2.1 Définition. *Soient k un corps et G un k-schéma en groupes. On dit que G vérifie la propriété* (TVR) *(« torseur versel rationnel ») s'il existe un ouvert U d'un espace affine sur k et un $G \times_k U$-torseur $\pi : V \to U$ tels que l'application naturelle de $U(k)$ dans $\mathrm{H}^1(k,G)$ déduite de π soit* surjective.

2.1.1 Remarque. La propriété (TVR) entraîne immédiatement que $\mathrm{R}_{\mathrm{el}}(k,G) = \mathrm{H}^1(k,G)$. Lorsque k est *infini*, elle donne un peu mieux : étant donnée une famille finie $(X_1,\dots,X_r)$ de G-torseurs, il existe un ouvert U de $\mathbb{A}^1_k$, un G-torseur $f : V \to U$ et des points rationnels $u_1,\dots,u_n \in U(k)$ tels que $f^{-1}(u_i) \cong X_i$ pour tout i.

2.1.2 Remarque. Il est naturel de considérer des variantes de (TVR), notamment celle obtenue en remplaçant « ouvert d'espace affine » par « variété rationnelle ». Les considérations ci-dessous resteraient valables, mais l'énoncé 2.4 serait plus faible.

2.2 Proposition. *Soient G_i ($1 \le i \le 3$) des K-schémas en groupes.*

(i) *Si G_1 et G_2 vérifient* (TVR)*, il en est de même de $G_1 \times G_2$.*

(ii) *Soit $\varphi : G_1 \to G_2$ un morphisme de K-schémas en groupes. On suppose que l'application $\mathrm{H}^1(K,\varphi) : \mathrm{H}^1(K,G_1) \to \mathrm{H}^1(K,G_2)$ est surjective, et que G_1 vérifie* (TVR)*. Alors G_2 vérifie* (TVR)*.*

(iii) *On suppose que G_1 est un sous-groupe fermé de G_2, et que :*

  (a) *l'inclusion $G_1 \hookrightarrow G_2$ induit l'application* triviale $\mathrm{H}^1(K,G_1) \to \mathrm{H}^1(K,G_2)$ *;*

  (b) *le K-schéma G_2/G_1 est un ouvert d'espace affine.*

  Alors G_1 vérifie (TVR)*.*

(iv) *Soit L une extension finie de K, et soit H un L-schéma en groupes vérifiant* (TVR)*. Alors la restriction de Weil $\mathrm{R}_{L/K}(H)$ vérifie* (TVR)*.*

Démonstration. Les assertions (i) et (ii) sont faciles (et la réciproque de (i) est un cas particulier de (ii)).

Montrons (iii). Posons $V = G_2$, $U = G_2/G_1$ (qui est un ouvert d'espace affine par l'hypothèse (b)), et soit $\pi : V \to U$ le morphisme canonique, qui fait de V un $G_1 \times_k U$-torseur à droite pour l'action naturelle de G_1 sur G_2. Soit X un G_1-torseur (à droite) sur K : l'hypothèse (a) montre que X se plonge dans le G_2-torseur trivial, de manière compatible aux actions de G_1 ; ceci équivaut à dire que X (ainsi plongé) est une fibre de π en un point de $U(K)$.

Pour (iv), soit $V \to U$ un H-torseur comme dans la définition 2.1, où U est un ouvert d'espace affine sur L : alors on en déduit par restriction de Weil un $\mathrm{R}_{L/K}(H)$-torseur $V_1 \to U_1$, où U_1 est un ouvert d'espace affine sur K, dont on vérifie qu'il a la propriété voulue. ∎

2.3 La condition $\mathrm{Cyc}(K,G)$**.**

2.3.1 Définition. *Soit G un groupe fini. Le* 2-exposant *de G est l'ordre maximum d'un élément de 2-torsion de G.*

Si G est un groupe fini et K un corps, nous aurons à considérer la condition suivante (où l'on convient que $K(\mu_{2^e}) = K$ si $\mathrm{car}\, K = 2$) :

$\mathrm{Cyc}(K,G)$: si 2^e désigne le 2-exposant de G, l'extension $K(\mu_{2^e})/K$ est cyclique.

2.3.2 Remarque. La condition $\mathrm{Cyc}(K,G)$ est vérifiée dans chacun des cas suivants :

(i) car $K > 0$;

(ii) -1 ou -2 est un carré dans K ;

(iii) K est le corps des fractions d'un anneau local intègre hensélien à corps résiduel k de caractéristique différente de 2, tel que $\mathrm{Cyc}(k,G)$ soit vérifiée ;

(iv) G n'a pas d'élément d'ordre 8.

Remarquer d'autre part que si l est un nombre premier *impair, toute* extension de la forme $K(\mu_{l^m})/K$ est cyclique ; nous utiliserons sans commentaire cette propriété.

2.4 Théorème. *Soit G un K-schéma en groupes* commutatif. *Dans chacun des cas suivants, G vérifie* (TVR) *:*

(i) *K est de caractéristique $p > 0$, et G est un p-groupe fini constant ;*

(ii) *G est de type multiplicatif déployé par une extension métacyclique de K* (on rappelle qu'un groupe fini est dit métacyclique si ses sous-groupes de Sylow sont cycliques) *;*

(iii) *G est de type multiplicatif et* $\mathrm{cd}(K) \leq 1$ *;*

(iv) *G est fini étale et* $\mathrm{cd}(K) \leq 1$ *;*

(v) *G est fini constant, et la condition* $\mathrm{Cyc}(K,G)$ *de* 2.3 *est satisfaite.*

Démonstration. Rappelons qu'un K-schéma en groupes G est *de type multiplicatif déployé* s'il est isomorphe à un sous-schéma en groupes fermé de $\mathbb{G}_{\mathrm{m},K}^n$, pour n convenable ; il est *de type multiplicatif* si G_{K_s} est de type multiplicatif déployé comme K_s-schéma en groupes.

(i) D'après 2.2 (i), on peut supposer que $G = \mathbb{Z}/p^n\mathbb{Z}$. Soit alors W le K-schéma en groupes des vecteurs de Witt tronqués de longueur n. On a une suite exacte « d'Artin-Schreier-Witt »

$$0 \longrightarrow G \longrightarrow W \xrightarrow{\Phi-\mathrm{Id}} W \longrightarrow 0$$

où Φ est l'endomorphisme de Frobenius. Comme W est extension successive de groupes additifs $\mathbb{G}_{\mathrm{a},K}$, on a $\mathrm{H}^1(K,W) = 0$; comme W est isomorphe à $\mathbb{A}_K^n$ comme K-schéma, on conclut par 2.2 (iii).

(ii) est la proposition 1 de [Gil]. Rappelons l'argument. Soit M une extension finie de K déployant G. D'après ([CT-S 2], proposition 1.3), il existe une suite exacte

$$1 \longrightarrow G \longrightarrow S \xrightarrow{\pi} E \longrightarrow 1$$

dans laquelle :

– E est un K-tore quasi-trivial, *i.e.* produit de restrictions de Weil $\mathrm{R}_{L_i/K}\mathbb{G}_{\mathrm{m},L_i}$ où les L_i sont des extensions finies séparables de K ; en particulier E est un ouvert d'espace affine sur K ;

– le tore S (ainsi d'ailleurs que E) est déployé par M, et S est « flasque » ; si M/K est métacyclique, cela implique que $\mathrm{H}^1(K,S)$ est trivial ([CT-S 1], cor. 3).

On conclut donc à nouveau par 2.2 (iii).

(iii) L'argument est le même que pour (ii), sans l'extension métacyclique M ; ici c'est l'hypothèse $\mathrm{cd}(K) \leq 1$ qui assure que $\mathrm{H}^1(K,S) = 1$ (un tore est un groupe divisible).

(iv) (signalé par Philippe Gille) : On écrit G comme quotient d'un « Gal_K-module de permutation », c'est-à-dire d'un produit P de restrictions de Weil $\mathrm{R}_{L_i/K}(C_i)$ où les L_i sont des extensions finies séparables de K et où $C_i = (\mathbb{Z}/n_i\mathbb{Z})_{L_i}$. L'hypothèse sur K implique alors que l'application naturelle $\mathrm{H}^1(K,P) \to \mathrm{H}^1(K,G)$ est surjective ; appliquant successivement les assertions (ii), (i) et (iv) de 2.2, on est ramené au cas où $G = \mathbb{Z}/l^m\mathbb{Z}$ (avec l premier). On conclut par (i) si $l = \mathrm{car}\, K$, et par (iii) sinon.

(v) Par décomposition en produit, on se ramène encore au cas où $G = \mathbb{Z}/l^m\mathbb{Z}$ (l premier). On conclut par (i) si $l = \mathrm{car}\, K$, et par (ii) sinon (G est déployé par $K(\mu_{l^m})$). ∎

Voici enfin une application aux groupes non nécessairement commutatifs, lorsque K est par exemple un corps fini :

2.5 Corollaire. *Soit G un groupe fini, vu comme K-schéma en groupes constant. On suppose que Gal_K est commutatif, et que la condition $\mathrm{Cyc}(K,G)$ de 2.3 est satisfaite. Alors $\mathrm{R}_{\mathrm{el}}(K,G) = \mathrm{H}^1(K,G)$.*

Démonstration. Les G-torseurs sont classifiés par les homomorphismes $\mathrm{Gal}_K \to G$, à conjugaison près. Tout G-torseur est donc induit par un torseur sous un sous-groupe commutatif H de G. Comme $\mathrm{Cyc}(K,H)$ est clairement satisfaite, il suffit d'appliquer 2.4 (v). ∎

3 Le cas « premier à p » : preuve du théorème 1.5

3.1 Notations.

Soient K, K_{s} et Gal_K comme dans 1.1 ; on suppose en outre que K est le corps des fractions d'un anneau de valuation discrète hensélien Λ, de corps résiduel k ; on note p l'exposant caractéristique de k.

La fermeture intégrale de Λ dans K_{s} est un anneau de valuation, dont le corps résiduel est une clôture algébrique $\overline{k}$ de k. On note k_{s} la clôture séparable de k dans $\overline{k}$, et l'on pose $\mathrm{Gal}_k = \mathrm{Gal}\,(k_{\mathrm{s}}/k)$. On a une suite exacte canonique

$$1 \longrightarrow I \longrightarrow \mathrm{Gal}_K \longrightarrow \mathrm{Gal}_k \longrightarrow 1 \tag{3.1.1}$$

et le groupe d'inertie I est lui-même objet d'un dévissage

$$1 \longrightarrow P \longrightarrow I \longrightarrow I_{\mathrm{mod}} \longrightarrow 1 \tag{3.1.2}$$

où P est l'unique (pro-)p-sylow de I, et I_{mod} l'« inertie modérée ». Ce dernier groupe s'identifie canoniquement à $\widehat{\mathbb{Z}}(1)(k_{\mathrm{s}}) = \varprojlim_{n\geq 1} \mu_n(k_{\mathrm{s}})$; l'isomorphisme respecte les actions de Gal_K (par conjugaison sur I_{mod}, par l'action sur les racines de l'unité sur $\widehat{\mathbb{Z}}(1)(k_{\mathrm{s}})$). Le groupe $\widehat{\mathbb{Z}}(1)(k_{\mathrm{s}})$ s'identifie aussi canoniquement à la partie première à p de $\widehat{\mathbb{Z}}(1)(K_{\mathrm{s}})$.

On a donc une suite de sous-groupes de Gal_K, et la suite correspondante de sous-corps de K_{s} :

$$\begin{array}{ccccc} \mathrm{Gal}_K & \supset & I & \supset & P \\ K & \subset & K_{\mathrm{nr}} & \subset & K_{\mathrm{mod}}. \end{array} \tag{3.1.3}$$

Pour démontrer le théorème 1.5, nous appliquerons 1.3 en prenant pour suite exacte (1.2.1) la suite

$$1 \longrightarrow I_{\mathrm{mod}} \longrightarrow \mathrm{Gal}(K_{\mathrm{mod}}/K) \longrightarrow \mathrm{Gal}_k \longrightarrow 1. \tag{3.1.4}$$

La preuve reposera sur les trois lemmes qui suivent, et qui montrent respectivement que les trois conditions de 1.3 sont satisfaites.

3.2 Lemme. *La suite exacte* (3.1.4) *de groupes profinis est scindée.*

Démonstration. Soit ϖ une uniformisante de Λ, et soit $L \subset K_{\mathrm{s}}$ le corps de décomposition de tous les polynômes $X^n - \varpi$, où n parcourt les entiers premiers à p. On vérifie alors sans mal que L/K est totalement et modérément ramifiée, donc $L \subset K_{\mathrm{mod}}$ et $L \cap K_{\mathrm{nr}} = K$. D'autre part il est bien connu que $L\,K_{\mathrm{nr}} = K_{\mathrm{mod}}$: voir par exemple [C-F], I, § 8, Corollary 1 of Proposition 1 (c'est là un avatar du « lemme d'Abhyankar »). Ceci implique que le sous-groupe $\mathrm{Gal}(K_{\mathrm{mod}}/L)$ de $\mathrm{Gal}(K_{\mathrm{mod}}/K)$ s'envoie isomorphiquement sur $\mathrm{Gal}(K_{\mathrm{nr}}/K) = \mathrm{Gal}_k$, donc scinde la suite exacte de l'énoncé. ∎

3.3 Lemme. *Soient F un corps, F_{s} une clôture séparable de F, et A un F-schéma en groupes fini étale isomorphe (comme groupe avec action de $\mathrm{Gal}(F_{\mathrm{s}}/F)$) à un quotient de $\widehat{\mathbb{Z}}(1)(F_{\mathrm{s}})$. Alors, $\mathrm{R}_{\mathrm{el}}(F, A) = \mathrm{H}^1(F, A)$.*

Démonstration. L'hypothèse implique que A est isomorphe à $\mu_{n,F}$, pour un entier n premier à car (F). La théorie de Kummer implique immédiatement que tout torseur sous un tel groupe est élémentairement R-équivalent au torseur trivial (c'est d'ailleurs un cas particulier de 2.4 (ii)). ∎

3.4 Lemme. *Soient Λ, K et k comme en* 3.1. *Soit G un Λ-schéma en groupes fini étale d'ordre inversible dans Λ, et soient $\mathscr{X}$ et $\mathscr{Y}$ deux G-torseurs sur* Spec Λ.

Si les G_k-torseurs $\mathscr{X}_k$ et $\mathscr{Y}_k$ sont élémentairement R-équivalents (resp. R-équivalents), alors il en est de même des G_K-torseurs $\mathscr{X}_K$ et $\mathscr{Y}_K$. (Bien entendu la notation G_k désigne $G \times_{\mathrm{Spec}\,(\Lambda)} \mathrm{Spec}\,(k)$, etc.)

Démonstration. Il suffit de traiter le cas de la R-équivalence élémentaire. Il existe alors un revêtement ramifié $f_0 : C_0 \to \mathbb{P}^1_k$, où C_0 est une k-courbe projective lisse munie d'une action de G_k qui fait de f_0 un G_k-torseur au-dessus d'un ouvert de $\mathbb{P}^1_k$ contenant 0 et 1, de telle sorte que $f_0^{-1}(0) \cong \mathscr{X}_k$ et $f_0^{-1}(1) \cong \mathscr{Y}_k$ comme G_k-torseurs. Vu l'hypothèse sur l'ordre de G, f_0 est automatiquement modérément ramifié ; soit $D_0 \subset \mathbb{P}^1_k$ son lieu de ramification, qui est un sous-schéma de $\mathbb{P}^1_k$ étale sur $\operatorname{Spec} k$. Choisissons un diviseur $D \subset \mathbb{P}^1_\Lambda$ étale sur $\operatorname{Spec} \Lambda$ et relevant D_0. La théorie des déformations des revêtements modérés ([Fu], th. 4.8, ou [MB 1], prop. 7.2.7) implique l'existence d'un unique revêtement modéré $f : C \to \mathbb{P}^1_\Lambda$, relevant f_0, dont le diviseur de ramification est D. Vu l'unicité, f est automatiquement un G-revêtement, et $f^{-1}(0)$ (resp. $f^{-1}(1)$) est un G-torseur sur $\operatorname{Spec} \Lambda$ relevant $\mathscr{X}_k$ (resp. $\mathscr{Y}_k$) donc isomorphe à $\mathscr{X}$ (resp. à $\mathscr{Y}$), ce qui achève la démonstration. ∎

3.5 Preuve du théorème 1.5.

Outre les notations ci-dessus, on se donne un groupe fini G d'ordre premier à p. On suppose que $\mathrm{R}(k, G) = \mathrm{H}^1(k, G)$, et l'on veut en déduire que $\mathrm{R}(K, G) = \mathrm{H}^1(K, G)$.

Comme on l'a annoncé plus haut, on applique 1.3 en prenant pour M le corps K_{mod}, et pour suite exacte (1.2.1) la suite (3.1.4). Celle-ci est bien scindée d'après le lemme 3.2. Noter que *tout* G-torseur sur K est modérément ramifié, donc trivialisé par M. L'extension M_0 de 1.3 n'est autre que K_{nr}.

La condition (iii) de 1.3 est vérifiée d'après le lemme 3.3. Vérifions la condition (ii) : il s'agit donc de voir que tout G-torseur $X \to \operatorname{Spec} K$ *non ramifié* est dans $\mathrm{R}(K, G)$. Un tel torseur se prolonge canoniquement en un G-torseur $\mathscr{X} \to \operatorname{Spec} \Lambda$, de fibre spéciale un G-torseur $X_0 \to \operatorname{Spec} k$. Par hypothèse, X_0 est dans $\mathrm{R}(k, G)$. Le lemme 3.4 permet donc de conclure. ∎

3.6 Remarque. Le lemme 3.4 n'apparaît pas dans [Gil]. Lorsque le corps résiduel k est fini, Gille utilise un autre argument pour vérifier (au langage près) la condition (ii) de 1.3 : puisque $\mathrm{Gal}_k \cong \widehat{\mathbb{Z}}$, l'étude des G-torseurs non ramifiés se ramène à celle des $\mathbb{Z}/n\mathbb{Z}$-torseurs, où n est premier à p, et un tel torseur est élémentairement R-équivalent au torseur trivial d'après 2.4 (ii).

C'est encore le fait que $\mathrm{Gal}_k \cong \widehat{\mathbb{Z}}$, plutôt que le lemme 3.2, qu'utilise Gille pour voir que la suite (1.2.1) est scindée.

3.7 Remarque. L'exemple de Colliot-Thélène cité plus haut (1.5.2) montre encore que l'hypothèse sur l'ordre du groupe dans 3.4 ne peut être supprimée.

4 Cas d'un corps résiduel abélien

4.1 Notations.

On reprend les hypothèses et notations de 3.1. Si A et B sont deux sous-groupes fermés de Gal_K, on conviendra de noter $[A,B]$ le sous-groupe *fermé* de Gal_K engendré par les commutateurs $[a,b]$ ($a \in A$, $b \in B$). On pose alors

$$\begin{aligned} P_0 &:= P \cap [I, \mathrm{Gal}_K] = \mathrm{Ker}\,(I \xrightarrow{\mathrm{can}} I/[I,\mathrm{Gal}_K] \times I_{\mathrm{mod}}) \\ M &:= (K_{\mathrm{s}})^{P_0}. \end{aligned} \tag{4.1.1}$$

Le diagramme (3.1.3) se complète donc en :

$$\begin{array}{ccccccccccc} \mathrm{Gal}_K & \supset & I & \supset & P & \supset & P \cap [\mathrm{Gal}_K, \mathrm{Gal}_K] & \supset & P_0 & \supset & [I,I] \\ K & \subset & K_{\mathrm{nr}} & \subset & K_{\mathrm{mod}} & \subset & K_{\mathrm{mod}} K_{\mathrm{ab}} & \subset & M & \subset & (K_{\mathrm{nr}})_{\mathrm{ab}} \end{array}$$

où l'on remarque que $[I,I] \subset P$ puisque I_{mod} est commutatif, d'où l'inclusion $[I,I] \subset P_0$.

En passant au quotient par P_0 la suite (3.1.1), on obtient une suite exacte de groupes profinis

$$1 \longrightarrow \Gamma \longrightarrow \Pi \longrightarrow \pi \longrightarrow 1 \tag{4.1.2}$$

avec :

$$\begin{aligned} \Gamma &= I/P_0 = \mathrm{Im}\,(I \xrightarrow{\mathrm{can}} I/[I,\mathrm{Gal}_K] \times I_{\mathrm{mod}}) \\ \Pi &= \mathrm{Gal}\,(M/K) \\ \pi &= \mathrm{Gal}_k = \mathrm{Gal}\,(K_{\mathrm{nr}}/K). \end{aligned}$$

4.2 Remarque. Γ s'identifie à un sous-groupe de $I/[I,\mathrm{Gal}_K] \times \prod_{l \neq p} \mathbb{Z}_l(1)(K_{\mathrm{s}})$; il est donc commutatif (ceci équivaut d'ailleurs à la propriété $[I,I] \subset P_0$, déjà observée). De plus, le noyau $U := \mathrm{Gal}\,(K_{\mathrm{s}}/K_{\mathrm{cycl}})$ du caractère cyclotomique opère trivialement sur Γ ; autrement dit, l'image U/P_0 de U dans Π centralise Γ. Ceci équivaut encore à dire que $[I,U] \subset P_0$, et l'on peut vérifier qu'en fait $P_0 = [I,I][I,U] = [I,IU]$.

4.3 Théorème. *Avec les notations de* 4.1*, on se donne un groupe fini G, et l'on suppose que :*

(i) $\pi = \mathrm{Gal}_k$ *est commutatif ;*

(ii) *la suite* (4.1.2) *est scindée ;*

(iii) *la condition* $\mathrm{Cyc}(K,G)$ *de* 2.3 *est satisfaite.*

Alors, on a $\mathrm{H}^1(M/K,G) \subset \mathrm{R}(K,G)$ (et donc $\mathrm{H}^1(M/K,G) \subset \mathrm{R}_{\mathrm{el}}(K,G)$ d'après [MB 2], cf. la remarque 1.4.5).

4.3.1 Remarques. (1) Les conditions (i) et (ii) du théorème sont notamment vérifiées lorsque le groupe $\pi = \mathrm{Gal}_k$ est un quotient sans torsion de $\widehat{\mathbb{Z}}$, et en particulier lorsque k est fini ou séparablement clos (et aussi lorsque $k = \mathbb{C}(\!(t)\!)$, mais voir (2) ci-dessous).

(2) Lorsque G est d'ordre premier à p, on n'obtient ici rien de mieux que le théorème 1.5 : en effet on voit tout de suite que $\mathrm{Cyc}(K, G)$ implique $\mathrm{Cyc}(k, G)$, de sorte que, d'après 2.5, l'hypothèse de 1.5 est vérifiée. En dehors de cette situation, le cas particulier le plus simple de 4.3 est 4.3.2 ci-dessous, que l'on peut d'ailleurs facilement extraire de la démonstration de [Gil].

4.3.2 Corollaire. *On suppose que p est un nombre premier impair et que K est une extension finie de $\mathbb{Q}_p$. Alors tout G-torseur modérément ramifié est dans* $\mathrm{R}(K, G)$.

Démonstration. Les conditions (i) et (ii) de 4.3 sont vérifiées (remarque 4.3.1 (1)), et (iii) l'est aussi puisque $p > 2$ (remarque 2.3.2 (iii)). ∎

4.4 Démonstration de 4.3.

Nous supposerons que $p > 1$, sinon la remarque 4.3.1 (2) s'applique.

On applique le théorème 1.3 en prenant pour suite (1.2.1) la suite (4.1.2), qui est scindée par hypothèse. Le corps M_0 de 1.3 est encore K_{nr}.

Vérifions la condition (ii) de 1.3. Le raisonnement est le même que dans la preuve de 2.5 : un G-torseur trivialisé par M_0 correspond à un morphisme continu $\pi \to G$. Comme π est commutatif par hypothèse, un tel torseur est induit par un torseur sous un sous-groupe commutatif H de G. Comme $\mathrm{Cyc}(K, H)$ est vérifiée, on peut appliquer 2.4 (v).

Vérifions la condition (iii) de 1.3. Soit donc H un quotient fini de Γ, dont le groupe sous-jacent est un sous-groupe de G. Alors H est commutatif (4.2) et l'on peut donc supposer que c'est un l-groupe, pour l premier.

Si $l = p$, alors la structure de Γ montre que H est un quotient de $I/[I, \mathrm{Gal}_K]$; or l'action de Gal_K sur $I/[I, \mathrm{Gal}_K]$ est triviale de sorte que H est constant. La conclusion résulte donc de 2.4 (v).

Si $l \neq p$, alors H est un sous-quotient de $A \times \mathbb{Z}_l(1)$, où A est la composante l-primaire de $I/[I, \mathrm{Gal}_K]$ (A est donc, comme ci-dessus, un schéma en groupes constant). Donc H est de type multiplicatif, déployé par $K(\mu_{l^n})$ pour n assez grand. C'est là une extension *cyclique* de K : c'est clair si $l \neq 2$, et si $l = 2$ alors $p > 2$ de sorte que la remarque 2.3.2 (iii) s'applique (on utilise ici l'hypothèse $p > 1$ faite au début). On conclut par 2.4 (ii). ∎

5 Bitorseurs : généralités

On rappelle ci-dessous les principales propriétés des bitorseurs ; pour plus de détails, voir par exemple [Gir] ou [Br].

5.1 Définition des bitorseurs.

Soient G' et G deux groupes d'un topos T (par exemple deux schémas en groupes sur un corps). Rappelons ([Gir], [Br]) qu'un (G', G)-*bitorseur* est la donnée d'un objet X de T, muni d'une action à gauche de G' et d'une action à droite de G, ces deux actions faisant respectivement de X un G'-torseur à gauche et un G-torseur à droite, et de plus commutant entre elles. En général un tel bitorseur sera noté (G', X, G), sans notation particulière pour les actions.

On voit immédiatement, dans ces conditions, que G' (resp. G) s'identifie canoniquement au faisceau $\underline{\mathrm{Aut}}_G(X)$ des G-automorphismes de X (resp. à $\underline{\mathrm{Aut}}_{G'}(X)^\circ$, groupe opposé au faisceau des G'-automorphismes de X), de sorte que, par exemple, tout G-torseur à droite Y détermine canoniquement un bitorseur $(\underline{\mathrm{Aut}}_G(Y), Y, G)$, et que tout bitorseur est de cette forme, à isomorphisme canonique près (voir ci-dessous pour la notion d' isomorphisme).

5.2 Morphismes de bitorseurs.

Soient $\mathscr{X}_1 = (G'_1, X_1, G_1)$ et $\mathscr{X}_2 = (G'_2, X_2, G_2)$ deux bitorseurs. Nous appellerons *morphisme* de $\mathscr{X}_1$ vers $\mathscr{X}_2$ un triplet $\Phi = (\varphi' : G'_1 \to G'_2, u : X_1 \to X_2, \varphi : G_1 \to G_2)$ de morphismes de T, tel que φ' et φ soient des morphismes de groupes et que u soit φ'-équivariant à gauche et φ-équivariant à droite.

On obtient ainsi une catégorie notée $\mathrm{Bitors}\,(T)$.

Il arrive que l'on ait besoin d'imposer les morphismes φ', φ (avec les notations ci-dessus), ou seulement l'un d'eux : on dira donc que Φ est un (φ', φ)-morphisme, ou un $(\varphi', *)$-morphisme, ou un $(*, \varphi)$-morphisme. De même, on parlera de $(G', *)$-bitorseurs, et de $(*, G)$-bitorseurs.

Si $\Phi = (\varphi', u, \varphi)$ est un morphisme de bitorseurs, il est équivalent de dire que φ' est injectif (resp. surjectif) comme morphisme de T, ou que u l'est, ou que φ l'est ; nous dirons alors que Φ est injectif (resp. surjectif). De même, Φ est un isomorphisme dans $\mathrm{Bitors}\,(T)$ si et seulement si φ' (ou u, ou φ) en est un dans T.

Tout morphisme Φ s'écrit de manière essentiellement unique sous la forme $\beta \circ \alpha$, où β est injectif et α surjectif. Bien entendu, le bitorseur source de β n'est autre, à isomorphisme canonique près, que $(\mathrm{Im}\,\varphi', \mathrm{Im}\,u, \mathrm{Im}\,\varphi)$; il sera appelé l'*image* de Φ.

5.3 Trivialisations.

Si G est un groupe de T, le G-*bitorseur trivial* est par définition le (G, G)-bitorseur $\mathrm{Triv}(G) = (G, G, G)$ où G opère à droite et à gauche sur lui-même par translations.

Si (G', X, G) est un bitorseur, il revient au même de dire que le G'-torseur à gauche X est trivial, ou que le G-torseur à droite X est trivial, ou que l'objet X de T a une section ; de plus ces conditions sont vérifiées localement dans T.

Si ces conditions sont vérifiées, nous commettrons l'abus (courant déjà pour les torseurs) de dire que « le bitorseur (G', X, G) est trivial ».

De façon plus précise, le choix d'une section x de X détermine un isomorphisme de G-torseurs à droite $u : G \to X$, donné par $g \mapsto xg$. Celui-ci se prolonge en un $(*, \mathrm{Id}_G)$-isomorphisme de la forme $(\mathrm{conj}\,(x), u, \mathrm{Id}_G) : \mathrm{Triv}(G) \to (G', X, G)$, où $\mathrm{conj}\,(x) : G \to G'$ est un isomorphisme de groupes de T qui mérite le nom de « conjugaison par x » ; de fait, si (G', X, G) est le bitorseur trivial (G, G, G), on vérifie tout de suite que $\mathrm{conj}\,(x) : G \to G$ est l'automorphisme intérieur $g \mapsto xgx^{-1}$.

5.4 Bitorseurs et classes de conjugaison.

La propriété qui précède (que l'on exprime couramment en disant que G' est une « forme intérieure » de G) a une conséquence importante : à tout bitorseur (G', X, G) est associée une bijection canonique entre l'ensemble des sous-objets de G invariants par conjugaison et l'ensemble des sous-objets de G' invariants par conjugaison. En particulier, si H est un *sous-groupe distingué* de G, il lui correspond canoniquement un sous-groupe distingué H' de G', caractérisé par la propriété que $X/H = H'\backslash X$; noter que l'on a alors un morphisme canonique $(G', X, G) \to (G'/H', X/H, G/H)$.

5.5 Changement de groupe structural.

Soient $\mathscr{X} = (G'_1, X_1, G_1)$ un bitorseur et $\varphi : G_1 \to G_2$ un morphisme de groupes de T. Il existe alors un $(*, G_2)$-bitorseur $\mathscr{X}^{\varphi} = (G'_2, X_2, G_2)$ et un $(*, \varphi)$-morphisme $\Phi = (\varphi', u, \varphi) : \mathscr{X} \to \mathscr{X}^{\varphi}$ qui est universel au sens suivant : tout $(*, \varphi)$-morphisme $\mathscr{X} \to \mathscr{Y}$ se factorise de façon unique sous la forme $\mathscr{X} \xrightarrow{\Phi} \mathscr{X}^{\varphi} \xrightarrow{\Theta} \mathscr{Y}$ où Θ est un $(*, \mathrm{Id}_{G_2})$-(iso)morphisme.

(En d'autres termes, le foncteur $(G', X, G) \mapsto G$ fait de $\mathrm{Bitors}\,(T)$ une catégorie cofibrée en groupoïdes au-dessus de la catégorie des groupes de T.)

En tant que G_2-torseur à droite, X_2 n'est autre que le torseur déduit de X_1 par le changement de groupe structural φ : c'est donc le produit contracté $X_1 \times^{G_1} G_2$, quotient de $X_1 \times G_2$ par l'action de G_1 donnée par $((x_1, g_2), g_1) \mapsto (x_1 g_1, \varphi(g_1)^{-1} g_2)$.

Noter que dans cette construction, le groupe G'_2 et le morphisme $\varphi' : G'_1 \to G'_2$ dépendent de X_1 (et pas seulement de φ et de G'_1). Cependant, φ' est « localement isomorphe à φ » : plus précisément, le choix d'une trivialisation de $\mathscr{X}$ détermine des isomorphismes $\psi_1 : G_1 \xrightarrow{\sim} G'_1$ et $\psi_2 : G_2 \xrightarrow{\sim} G'_2$ tels que $\varphi'\psi_1 = \psi_2\varphi$. On voit ainsi, notamment, que si (G', X, G) est un bitorseur et H un sous-groupe de G tel que X soit induit (comme G-torseur à droite) par un H-torseur, alors il est induit comme G'-torseur à gauche par un torseur sous un sous-groupe H' de G', localement isomorphe à H.

Enfin, on a bien entendu une opération similaire du côté gauche : si $\varphi' : G'_1 \to G'_2$ est un morphisme de groupes, elle fournit un $(G'_2, *)$-bitorseur noté ${}^{\varphi'}\mathscr{X}$ et un $(\varphi', *)$-morphisme universel $\mathscr{X} \to {}^{\varphi'}\mathscr{X}$.

5.6 Cas particulier : passage au quotient.

Soient $\mathscr{X} = (G', X, G)$ un bitorseur, $H \xhookrightarrow{j} G$ un sous-groupe *distingué* de G, et $\varphi : G \to G/H$ le morphisme canonique. On a alors, d'après 5.3, un sous-groupe distingué H'

de G' et un morphisme $\mathscr{X} \to (G'/H', X/H, G/H)$. Bien entendu, celui-ci n'est autre que le morphisme $\mathscr{X} \to \mathscr{X}^{\varphi}$ défini ci-dessus. Le bitorseur $(G'/H', X/H, G/H)$ pourra être noté, indifféremment, $\mathscr{X}/H$ ou $H'\backslash\mathscr{X}$. On vérifie, sans surprise, la propriété suivante :

5.6.1 Lemme. *Avec les notations de* 5.6*, les conditions suivantes sont équivalentes :*

(i) *le bitorseur $\mathscr{X}/H$ est trivial ;*

(ii) *le G-torseur à droite X est induit par un H-torseur ;*

(iii) *le G'-torseur à gauche X est induit par un H'-torseur ;*

(iv) *il existe un (H', H)-bitorseur Y et un $(*, j)$-morphisme $(H', Y, H) \to \mathscr{X}$.* ∎

5.7 Composition de bitorseurs.

La catégorie $\mathrm{Bitors}\,(T)$ possède un « produit » partiellement défini, qui fait tout son charme : si $\mathscr{X}_1 = (G_1, X_1, G_2)$ et $\mathscr{X}_2 = (G_2, X_2, G_3)$ sont dans $\mathrm{Bitors}\,(T)$, le produit contracté $X_1 \times^{G_2} X_2$ admet une structure naturelle de (G_1, G_3)-bitorseur. On notera

$$\mathscr{X}_1 \wedge \mathscr{X}_2 = (G_1, X_1 \times^{G_2} X_2, G_3)$$

le bitorseur ainsi obtenu. La loi $\wedge$ admet une contrainte d'associativité (des isomorphismes $(\mathscr{X}_1 \wedge \mathscr{X}_2) \wedge \mathscr{X}_3 \xrightarrow{\sim} \mathscr{X}_1 \wedge (\mathscr{X}_2 \wedge \mathscr{X}_3)$ assortis de compatibilités) ; les bitorseurs triviaux sont neutres à droite et à gauche, et tout bitorseur $\mathscr{X} = (G', X, G)$ admet un inverse, à savoir $\mathscr{X}^{-1} = (G, X^{-1}, G')$, où $X^{-1} = X$ muni de l'action à gauche (resp. à droite) de G (resp. G') donnée par $(g, x) \mapsto xg^{-1}$ (resp. $(x, g') \mapsto {g'}^{-1}x$).

5.7.1 Lemme. *Soient $\mathscr{X}_1 = (G_1, X_1, G_2)$, $\mathscr{X}_2 = (G_2, X_2, G_3)$, $\mathscr{Y} = (H', Y, H)$ des bitorseurs (avec $\mathscr{X}_1$ et $\mathscr{X}_2$ composables), et*

$$\Phi : \mathscr{X}_1 \wedge \mathscr{X}_2 \longrightarrow \mathscr{Y}$$

un morphisme.

Il existe alors un groupe G_2' de T, et un morphisme de groupes $\varphi_2 : G_2 \to G_2'$ tels que Φ se factorise sous la forme

$$\mathscr{X}_1 \wedge \mathscr{X}_2 \xrightarrow{\Phi_1 \wedge \Phi_2} \mathscr{X}_1^{\varphi_2} \wedge {}^{\varphi_2}\mathscr{X}_2 \xrightarrow{\Psi} \mathscr{Y}$$

où $\Phi_1 : \mathscr{X}_1 \to \mathscr{X}_1^{\varphi_2}$ et $\Phi_2 : \mathscr{X}_2 \to {}^{\varphi_2}\mathscr{X}_2$ sont les morphismes canoniques, et où Ψ est un isomorphisme.

Démonstration. Écrivons $\Phi = (\varphi_1, u, \varphi_3) : \mathscr{X}_1 \wedge \mathscr{X}_2 \to (H', Y, H)$. Considérons le morphisme canonique $\Phi_2 : \mathscr{X}_2 \to \mathscr{X}_2^{\varphi_3}$: il est de la forme $(\varphi_2, u_2, \varphi_3)$ où $\varphi_2 : G_2 \to G_2'$ est un morphisme de groupes ; le bitorseur $\mathscr{X}_2^{\varphi_3}$ s'identifie aussi à ${}^{\varphi_2}\mathscr{X}_2$. Le morphisme canonique $\Phi_1 \wedge \Phi_2 : \mathscr{X}_1 \wedge \mathscr{X}_2 \to \mathscr{X}_1^{\varphi_2} \wedge {}^{\varphi_2}\mathscr{X}_2$ est par construction un $(*, \varphi_3)$-morphisme, comme Φ, de sorte que $\mathscr{Y}$ et $\mathscr{X}_1^{\varphi_2} \wedge {}^{\varphi_2}\mathscr{X}_2$ s'identifient tous deux à $(\mathscr{X}_1 \wedge \mathscr{X}_2)^{\varphi_3}$. Le lemme en résulte. ∎

5.8 Bitorseurs d'isomorphismes.

Soit G un groupe de T ; considérons deux $(*, G)$-bitorseurs (G', X, G) et (G'', Y, G). Alors $\underline{\mathrm{Isom}}_G(X, Y)$ admet une structure naturelle de (G'', G')-bitorseur, et l'on a un isomorphisme canonique de (G'', G')-bitorseurs

$$(G'', \underline{\mathrm{Isom}}_G(X, Y), G') \xrightarrow{\sim} (G'', Y, G) \wedge (G', X, G)^{-1}. \tag{5.8.1}$$

En combinant ceci avec le lemme 5.6.1, on obtient le résultat suivant, qui nous servira plus loin :

5.8.1 Lemme. *Soient $\mathscr{X} = (G', X, G)$, $\mathscr{Y} = (G'', Y, G)$ deux $(*, G)$-bitorseurs, H un sous-groupe distingué de G, $H' \subset G'$ et $H'' \subset G''$ les sous-groupes qui lui correspondent canoniquement via $\mathscr{X}$ et $\mathscr{Y}$ respectivement (cf.* 5.3*). On suppose que $\mathscr{X}/H$ et $\mathscr{Y}/H$ sont isomorphes. Alors le (G'', G')-bitorseur $\mathscr{Y} \wedge \mathscr{X}^{-1}$ provient par changement de groupe structural d'un (H'', H')-bitorseur.* ∎

6 Bitorseurs et R-équivalence

6.1 Notations.

Soit K un corps, dont on fixe une clôture séparable K_s. Nous allons appliquer les notions ci-dessus au topos K_et des faisceaux sur le petit site étale de K (qui est équivalent au topos des $\mathrm{Gal}\,(K_\mathrm{s}/K)$-ensembles).

Si G est un K-schéma en groupes fini étale, nous noterons

$$(X, G) \overset{\mathrm{R_{el}}}{\sim} (Y, G), \quad \text{resp.} \quad (G, X') \overset{\mathrm{R_{el}}}{\sim} (G, Y')$$

la R-équivalence élémentaire entre deux G-torseurs à droite X et Y (resp. deux G-torseurs à gauche X' et Y'). De même nous noterons

$$(X, G) \overset{\mathrm{R}}{\sim} (Y, G), \quad \text{resp.} \quad (G, X') \overset{\mathrm{R}}{\sim} (G, Y')$$

la R-équivalence. La notation (G, G) désignera le G-torseur trivial (à droite ou à gauche, suivant le contexte).

Dans ce qui suit, tous les schémas en groupes et (bi)torseurs considérés sont finis étales sur K.

6.2 Proposition. (Bitorseurs et R-équivalence élémentaire)

(i) *Soient H, G, G', G'', G''' des K-schémas en groupes finis étales, (G', X, G), (G'', Y, G), (G, Z, G''') des bitorseurs et $\varphi : G \to H$ un morphisme de K-groupes. Alors on a les implications suivantes :*

(a) $(X, G) \overset{\mathrm{R_{el}}}{\sim} (Y, G) \iff (G, X^{-1}) \overset{\mathrm{R_{el}}}{\sim} (G, Y^{-1})$;

(b) $(X,G) \overset{\mathrm{R_{el}}}{\sim} (Y,G) \implies (X \times^G H, H) \overset{\mathrm{R_{el}}}{\sim} (Y \times^G H, H)$;

(c) $(X,G) \overset{\mathrm{R_{el}}}{\sim} (Y,G) \implies (X \times^G Z, G''') \overset{\mathrm{R_{el}}}{\sim} (Y \times^G Z, G''')$;

(d) $(X,G) \overset{\mathrm{R_{el}}}{\sim} (G,G) \iff (G',X) \overset{\mathrm{R_{el}}}{\sim} (G',G')$;

(e) $(X,G) \overset{\mathrm{R_{el}}}{\sim} (Y,G) \iff (G'', \underline{\mathrm{Isom}}_G(X,Y)) \overset{\mathrm{R_{el}}}{\sim} (G'',G'') \iff (\underline{\mathrm{Isom}}_G(X,Y), G') \overset{\mathrm{R_{el}}}{\sim} (G',G')$

ainsi que l'analogue de (c) *pour le produit contracté à gauche, et les analogues de* (b) *et* (e) *pour les torseurs à gauche.*

(ii) *Notons* $\mathfrak{R}_{\mathrm{el}}$ *la classe des bitorseurs* (G',X,G) *tels que* $(X,G) \overset{\mathrm{R_{el}}}{\sim} (G,G)$ *(ou tels que* $(G',X) \overset{\mathrm{R_{el}}}{\sim} (G',G')$*, ce qui revient au même d'après* (i) (d)*). Alors* $\mathfrak{R}_{\mathrm{el}}$ *possède les propriétés suivantes :*

(a) $\mathfrak{R}_{\mathrm{el}}$ *contient les bitorseurs triviaux* $\mathrm{Triv}(G)$;

(b) $\mathfrak{R}_{\mathrm{el}}$ *est stable par inverse : si* $\mathscr{X} \in \mathfrak{R}_{\mathrm{el}}$*, alors* $\mathscr{X}^{-1} \in \mathfrak{R}_{\mathrm{el}}$;

(c) $\mathfrak{R}_{\mathrm{el}}$ *est « stable par morphismes » : si* $\mathscr{X} \in \mathfrak{R}_{\mathrm{el}}$ *et si* $\Phi : \mathscr{X} \to \mathscr{Y}$ *est un morphisme, alors* $\mathscr{Y} \in \mathfrak{R}_{\mathrm{el}}$.

(iii) *La R-équivalence élémentaire de torseurs est déterminée par la classe* $\mathfrak{R}_{\mathrm{el}}$ *de* (ii) *: de façon précise (pour les torseurs à droite) si* $\mathscr{X} = (G',X,G)$ *et* $\mathscr{Y} = (G'',Y,G)$ *sont deux* $(*,G)$*-bitorseurs, les propriétés suivantes sont équivalentes :*

(a) $(X,G) \overset{\mathrm{R_{el}}}{\sim} (Y,G)$;

(b) $\mathscr{Y} \wedge \mathscr{X}^{-1} \in \mathfrak{R}_{\mathrm{el}}$;

(c) $\mathscr{Y}$ *est de la forme* $\mathscr{Z} \wedge \mathscr{X}$*, avec* $\mathscr{Z} \in \mathfrak{R}_{\mathrm{el}}$.

Démonstration. (i) Les assertions (a), (b) et (c) résultent immédiatement des définitions. Pour montrer (d), on applique (c) en prenant $(G'',Y,G) = (G,G,G)$ et $(G,Z,G''') = (G,X^{-1},G')$: on obtient $(G',G') \overset{\mathrm{R_{el}}}{\sim} (X^{-1},G')$ d'où $(G',X) \overset{\mathrm{R_{el}}}{\sim} (G',G')$ d'après (a).

On en déduit (e) en utilisant (5.8.1).

Finalement, (ii) (resp. (iii)) n'est qu'une reformulation des propriétés (a), (b) et (c) (resp. (e)) de (i). ∎

6.3 Proposition. (Bitorseurs et R-équivalence) *Notons encore* $\mathfrak{R}_{\mathrm{el}}$ *la classe de bitorseurs définie en* 6.2 (ii).

(i) *Soit* $\mathscr{X} = (G',X,G)$ *un bitorseur. Les conditions suivantes sont équivalentes :*

(a) $(X,G) \overset{\mathrm{R}}{\sim} (G,G)$;

(b) $(G',X) \overset{\mathrm{R}}{\sim} (G',G')$;

(c) $\mathscr{X}$ *est (à isomorphisme près) de la forme* $\mathscr{X}_1 \wedge \mathscr{X}_2 \wedge \cdots \wedge \mathscr{X}_n$*, où les* $\mathscr{X}_i$ *sont dans* $\mathfrak{R}_{\mathrm{el}}$.

(ii) *Soit $\mathfrak{R}$ la classe des bitorseurs $\mathscr{X} = (G', X, G)$ vérifiant les conditions de* (i)*. Alors $\mathfrak{R}$ vérifie les analogues des propriétés de* 6.2 (ii) *(elle contient les bitorseurs triviaux, et est stable par inverse et par morphismes), et est de plus stable par la composition de bitorseurs (lorsqu'elle est définie). Plus précisément, $\mathfrak{R}$ est la plus petite classe de bitorseurs stable par isomorphisme et par composition, et contenant $\mathfrak{R}_{\mathrm{el}}$.*

(iii) *Soient $\mathscr{X} = (G', X, G)$ et $\mathscr{Y} = (G'', Y, G)$ deux $(*, G)$-bitorseurs. Les conditions suivantes sont équivalentes (où $\mathfrak{R}$ est la classe de bitorseurs définie en* (ii)*) :*

(a) $(X, G) \overset{\mathrm{R}}{\sim} (Y, G)$;

(b) $\mathscr{Y} \wedge \mathscr{X}^{-1} \in \mathfrak{R}$;

(c) *$\mathscr{Y}$ est de la forme $\mathscr{Z} \wedge \mathscr{X}$, avec $\mathscr{Z} \in \mathfrak{R}$.*

Démonstration. L'assertion (i) résulte de la définition et de 6.2 (iii), et entraîne facilement les autres. ∎

6.4 Remarque. On peut évidemment préciser (i) de la façon suivante : si, pour $n \in \mathbb{N}$ donné, l'on définit $\mathrm{R}_n(K, G)$ commme en 1.4.3, on a l'équivalence : $(X, G) \in \mathrm{R}_n(K, G) \Leftrightarrow \mathscr{X}$ est de la forme $\mathscr{X}_1 \wedge \mathscr{X}_2 \wedge \cdots \wedge \mathscr{X}_n$, où les $\mathscr{X}_i$ sont dans $\mathfrak{R}_{\mathrm{el}}$.

7 Bitorseurs à groupe structural constant

Dans ce paragraphe nous décrivons les bitorseurs dont l'un des deux groupes structuraux est fini constant, lorsque le topos T est galoisien, c'est-à-dire équivalent à la catégorie des ensembles avec action continue d'un groupe profini.

7.1 Π-ensembles : notations et conventions.

On se donne désormais un groupe profini Π, et l'on travaille dans la catégorie $\mathscr{C}_\Pi$ des Π-ensembles, c'est-à-dire des ensembles X munis d'une action à gauche continue de Π (pour la topologie profinie sur Π et la topologie discrète sur X). Cette catégorie est un topos ([SGA], IV, 2.4).

Si X est un Π-ensemble, son ensemble sous-jacent sera noté $|\mathsf{X}|$; le transformé de $x \in |\mathsf{X}|$ par $\sigma \in \Pi$ sera noté ${}^{\sigma}x$.

Pour éviter des confusions, nous utiliserons (sauf exceptions telles que la notation $|\mathsf{X}|$ ci-dessus) des typographies différentes pour les ensembles $(X, Y, \dots)$ et les Π-ensembles $(\mathsf{X}, \mathsf{Y}, \dots)$.

Si X et Y sont deux Π-ensembles *finis*, l'objet $\underline{\mathsf{Hom}}\,(\mathsf{X}, \mathsf{Y})$ de $\mathscr{C}_\Pi$ est l'ensemble H des applications de $|\mathsf{X}|$ dans $|\mathsf{Y}|$ muni de l'action de Π donnée par la formule

$$({}^{\sigma}f)(x) = {}^{\sigma}[f({}^{\sigma^{-1}}x)]$$

(pour $f \in H$, $\sigma \in \Pi$ et $x \in |\mathsf{X}|$). La finitude assure que cette action est bien continue. (Sans l'hypothèse de finitude, la bonne définition de l'ensemble sous-jacent à $\underline{\mathsf{Hom}}\,(\mathsf{X}, \mathsf{Y})$ est $\varinjlim_U \mathrm{Hom}_U(|\mathsf{X}|, |\mathsf{Y}|)$ où U parcourt les sous-groupes ouverts de Π).

Les objets de $\mathscr{C}_\Pi$ pour lesquels l'action de Π est triviale seront dits *constants* (ce sont les objets constants du topos $\mathscr{C}_\Pi$). L'objet constant associé à un ensemble X sera noté $\underline{\underline{X}}$.

Un Π-*groupe* est un groupe du topos $\mathscr{C}_\Pi$, c'est-à-dire un groupe muni d'une action à gauche de Π par automorphismes. Si G est un Π-groupe, on notera encore $|\mathsf{G}|$, par abus, le *groupe* sous-jacent à G. Un G-torseur à droite est alors un Π-ensemble non vide X muni d'une action à droite libre et transitive de $|\mathsf{G}|$ sur $|\mathsf{X}|$ (notée $(x,g)\mapsto xg$), la compatibilité avec les actions de Π étant donnée par la formule ${}^\sigma(xg) = ({}^\sigma x)({}^\sigma g)$ ($\sigma\in\Pi$, $x\in|\mathsf{X}|$, $g\in|\mathsf{G}|$).

On peut voir Π lui-même (ainsi que ses sous-groupes fermés distingués et ses quotients) comme un pro-Π-groupe, en le munissant de son action par automorphismes intérieurs.

Si $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ est un bitorseur dans $\mathscr{C}_\Pi$, on notera $|\mathscr{X}|$ le bitorseur ensembliste $(|\mathsf{G}'|, |\mathsf{X}|, |\mathsf{G}|)$; le foncteur $\mathscr{X}\mapsto|\mathscr{X}|$ d'oubli des actions de Π est fidèle et compatible (notamment) aux changements de groupe structural et à la composition de bitorseurs.

7.2 Π-ensembles : (bi)torseurs sous les groupes constants.

7.2.1 Notations. Considérons la sous-catégorie pleine B_Π de $\mathrm{Bitors}\,(\mathscr{C}_\Pi)$ formé des bitorseurs $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ tels que le Π-groupe G soit *constant*.

Désignons d'autre part par B'_Π la catégorie suivante :

- un objet de B'_Π est de la forme (G', X, G, θ), où (G', X, G) est un bitorseur ensembliste et où $\theta : \Pi \to G'$ est un homomorphisme continu ;
- un morphisme de (G', X, G, θ) vers (H', Y, H, ψ) est un morphisme de bitorseurs $(\varphi', u, \varphi) : (G', X, G) \to (H', Y, H)$ vérifiant $\psi\circ\varphi' = \theta : \Pi \to H'$.

7.2.2 Remarques. La catégorie B_Π est équivalente à la catégorie, en apparence plus simple, des couples (X, G) où G est un groupe et X un torseur à droite sous le groupe constant $\underline{\underline{G}}$: l'équivalence est donnée par le foncteur $(\mathsf{G}', \mathsf{X}, \mathsf{G}) \mapsto (\mathsf{X}, |\mathsf{G}|)$, de quasi-inverse $(\mathsf{X}, G) \mapsto (\mathsf{Aut}_{\underline{\underline{G}}}(\mathsf{X}), \mathsf{X}, \underline{\underline{G}})$.

De la même façon, B'_Π est équivalente à la catégorie des objets (X, G', θ) où G' est un groupe, X un G'-torseur à droite, et $\theta : \Pi \to G'$ un homomorphisme continu.

Les définitions en termes de bitorseurs expriment mieux la symétrie de la situation, et notamment le fait que l'on a un diagramme de « foncteurs d'oubli » :

$$\begin{array}{ccccc} & & \mathrm{B}'_\Pi & & (G', X, G, \theta) \\ & & \downarrow{\scriptstyle\omega'} & & \downarrow \\ \mathrm{B}_\Pi & \xrightarrow{\omega} & \mathrm{Bitors}\,(\mathrm{Ens}) & & (G', X, G) \\ \mathscr{X} & \longmapsto & |\mathscr{X}| & & \end{array}$$

7.2.3 Proposition. *Il existe une équivalence de catégories*

$$\Phi : \mathrm{B}_\Pi \to \mathrm{B}'_\Pi$$

telle que $\omega'\circ\Phi \cong \omega$.

Démonstration. Contentons-nous de décrire Φ et un quasi-inverse $\Psi : \mathrm{B}'_\Pi \to \mathrm{B}_\Pi$ de Φ.

Soit $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ un objet de B_Π, et posons $(G', X, G) = \omega(\mathscr{X}) = (|\mathsf{G}'|, |\mathsf{X}|, |\mathsf{G}|)$. Comme le Π-groupe G est constant, il est donné par l'action triviale de Π sur le groupe G. Ceci entraîne que l'action de Π sur X *commute* à celle de G, et est donc donnée par un morphisme de groupes θ de Π vers le groupe $\mathrm{Aut}_G(X)$, qui n'est autre que G', à isomorphisme canonique près. On obtient bien ainsi un objet $\Phi(\mathscr{X}) = (G', X, G, \theta)$ de B'_Π.

Inversement, soit (G', X, G, θ) un objet de B'_Π. On en déduit une action à gauche de Π sur X, via θ et l'action de G', et une action à gauche de Π sur G' par automorphismes intérieurs via θ. D'où un Π-groupe G' (qui ne dépend d'ailleurs pas de X) et un G'-torseur à gauche X. On vérifie alors immédiatement que l'action de Π sur G (identifié à $\mathrm{Aut}_{G'}(X)$) est triviale, de sorte que X est bien muni d'une structure de $(\mathsf{G}', \underline{\underline{G}})$-bitorseur. ∎

7.2.4 Remarque. Lorsque l'on adopte les descriptions de B_Π et B'_Π données en 7.2.2, en remarquant en outre qu'avec les notations habituelles, on a un isomorphisme $G \cong G'$ bien défini à conjugaison près, on retrouve la bijection bien connue entre $\mathrm{H}^1(\Pi, G)$ et le quotient de $\mathrm{Hom}\,(\Pi, G)$ par les automorphismes intérieurs de G.

7.2.5 Propriétés de l'équivalence de 7.2.3 : connexité. Rappelons qu'un objet X du topos $\mathscr{C}_\Pi$ est *connexe* si et seulement si c'est un Π-ensemble (non vide et) *transitif*.

Soient $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ un objet de B_Π, et $\Phi(\mathscr{X}) = (G', X, G, \theta)$ l'objet de B'_Π correspondant. Nous dirons que $\mathscr{X}$ est *connexe* si l'objet X de $\mathscr{C}_\Pi$ l'est : cette condition équivaut à dire que $\theta : \Pi \to G'$ est *surjectif*.

De plus, il existe toujours un objet connexe $\mathscr{Y}$ de B_Π (d'ailleurs unique à isomorphisme non unique près) et un morphisme injectif $\mathscr{Y} \to \mathscr{X}$. En effet, soit $H' \subset G'$ l'image de $\theta : \Pi \to G'$; le choix d'un élément de X détermine un sous-groupe correspondant H de G, et un morphisme $(H', Y, H) \to (G', X, G)$ de torseurs, qui de plus est un morphisme $(H', Y, H, \theta_{H'}) \to (G', X, G, \theta)$ d'objets de B'_Π où $\theta_{H'}$ est obtenu à partir de θ par restriction du but. Appliquant le foncteur Ψ on obtient le morphisme $(\mathsf{H}', \mathsf{Y}, \mathsf{H}) \to (\mathsf{G}', \mathsf{X}, \mathsf{G})$ cherché.

7.2.6 Propriétés de l'équivalence de 7.2.3 : sous-groupes distingués. Soient $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ et $\Phi(\mathscr{X}) = (G', X, G, \theta)$ comme en 7.2.5. Il est clair que tout sous-groupe distingué de G (resp. de G') est invariant par l'action de Π, et définit donc un sous-groupe distingué de G (resp. de G'). Compte tenu de 5.3, on peut donc identifier canoniquement les quatre ensembles de sous-groupes distingués de G, G', G et G'. De plus cette identification ne dépend pas de θ.

8 Dévissage de bitorseurs ; preuve du théorème 1.3

8.1 Notations et hypothèses.

On reprend les notations et conventions de 7.1 sur les Π-ensembles, et l'on se donne une suite exacte de groupes profinis

$$1 \longrightarrow \Gamma \longrightarrow \Pi \longrightarrow \pi \longrightarrow 1. \tag{8.1.1}$$

Nous identifierons la catégorie $\mathscr{C}_\pi$ des π-ensembles à la sous-catégorie pleine de $\mathscr{C}_\Pi$ formée des Π-ensembles sur lesquels Γ opère trivialement.

8.2 Définition. *Si $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G})$ est un bitorseur dans $\mathscr{C}_\Pi$, nous dirons pour abréger que*

(i) *$\mathscr{X}$ est* de type π *s'il provient d'un bitorseur de $\mathscr{C}_\pi$;*

(ii) *$\mathscr{X}$ est* de type Γ *s'il existe un morphisme $\Phi : \mathscr{X}_1 = (\mathsf{H}', \mathsf{X}_1, \mathsf{H}) \to \mathscr{X}$ où H' est un quotient de Γ ;*

(iii) *$\mathscr{X}$ est* décomposable *s'il peut s'écrire, à isomorphisme près,*

$$\mathscr{X} = \mathscr{Y} \wedge \mathscr{Z}$$

où $\mathscr{Y}$ est de type Γ et où $\mathscr{Z}$ est de type π.

8.3 Remarque. Gardons les notations de 8.2.

(i) Pour que $\mathscr{X}$ soit de type π, il faut et il suffit que Γ opère trivialement sur $|\mathsf{X}|$.

(ii) Si $\mathscr{X}$ est de type Γ, le morphisme Φ de 8.2 (ii) peut être choisi *injectif* (considérer son image, définie en 5.2).

(iii) Si $\mathscr{X}$ est décomposable, alors G est nécessairement un π-groupe.

8.4 Lemme. *Soit $\Phi = (\varphi', u, \varphi) : \mathscr{X} = (\mathsf{G}', \mathsf{X}, \mathsf{G}) \to \mathscr{X}_1 = (\mathsf{G}'_1, \mathsf{X}_1, \mathsf{G}_1)$ un morphisme de bitorseurs de $\mathscr{C}_\Pi$.*

(i) *Si $\mathscr{X}$ est de type Γ, il en est de même de $\mathscr{X}_1$.*

(ii) *Si $\mathscr{X}$ est de type π, alors $\mathscr{X}_1$ est de type π si et seulement si G_1 est un π-groupe.*

(iii) *Si $\mathscr{X}$ est décomposable, alors $\mathscr{X}_1$ est décomposable si et seulement si G_1 est un π-groupe.*

Démonstration. L'assertion (i) résulte trivialement de la définition. Dans (ii) et (iii), le « seulement si » est trivial. Réciproquement, pour (ii), remarquer que $\mathscr{X}_1$ s'identifie à $\mathscr{X}^\varphi$. La partie « si » de (iii) résulte de (i) et (ii) et du lemme 5.7.1. ∎

8.5 Théorème. *Avec les hypothèses et notations de* 8.1, *on suppose de plus que la suite exacte* (8.1.1) *est* scindée.

Alors, pour tout groupe fini G, tout $(*, \underline{\underline{G}})$-bitorseur de $\mathscr{C}_\Pi$ est décomposable.

Démonstration. Soient G un groupe fini et $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \underline{\underline{G}})$ un $(*, \underline{\underline{G}})$-bitorseur. C'est un objet de la catégorie B_Π de 7.2. Par 7.2.5, il existe un morphisme $\mathscr{Y} \to \mathscr{X}$ où $\mathscr{Y}$ est un objet connexe de B_Π ; par 8.4 (iii), $\mathscr{X}$ est décomposable si $\mathscr{Y}$ l'est. On peut donc supposer $\mathscr{X}$ *connexe*. Il lui correspond par 7.2.3 un objet (G', X, G, θ) de B'_Π : rappelons que (G', X, G) est le bitorseur ensembliste $|\mathscr{X}|$ et que $\theta : \Pi \to G'$ est un morphisme continu, ici *surjectif* puisque $\mathscr{X}$ est connexe.

On déduit alors de (8.1.1) et de θ un diagramme de Π-groupes profinis, à carrés commutatifs et à lignes exactes :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma & \longrightarrow & \Pi & \xrightarrow{p} & \pi & \longrightarrow & 1 \\ & & \downarrow & & \downarrow\theta & \swarrow^{s} & \downarrow\overline{\theta} & & \\ 1 & \longrightarrow & H' & \longrightarrow & G' & \xrightarrow{q} & \overline{G'} & \longrightarrow & 1 \end{array} \tag{8.5.2}$$

où les flèches verticales sont surjectives, et où s (déduit d'un scindage de (8.1.1)) vérifie $q \circ s = \overline{\theta}$. De plus, le sous-groupe distingué H' de G' donne naissance (par 5.4) à un sous-Π-groupe H' de G' et à un sous-groupe distingué H de G. Posons alors

$$\widetilde{\theta} = s \circ p : \Pi \longrightarrow G';$$

on en déduit, par le foncteur Ψ de 7.2.3, un bitorseur

$$\mathscr{Z} = \Psi(G', X, G, \widetilde{\theta}) = (\mathsf{G}'', \mathsf{Z}, \underline{\underline{G}})$$

avec $|\mathscr{Z}| = |\mathscr{X}|$. Par construction, $\Gamma \subset \operatorname{Ker}\widetilde{\theta}$, de sorte que $\mathscr{Z}$ est de type π, et il suffit pour conclure de voir que le $(\mathsf{G}', \mathsf{G}'')$-bitorseur

$$\mathscr{Y} := \mathscr{X} \wedge \mathscr{Z}^{-1} = \underline{\mathrm{Isom}}_G(\mathscr{Z}, \mathscr{X})$$

est de type Γ. Comme on a $q \circ \widetilde{\theta} = q \circ \theta$, il est clair que les bitorseurs $\mathsf{H}'\backslash\mathscr{X} = \mathscr{X}/\underline{\underline{H}}$ et $\mathscr{Z}/\underline{\underline{H}}$ sont isomorphes. Par suite, d'après 5.8.1, il existe un $(\mathsf{H}', *)$-bitorseur $\mathscr{W}$ et un morphisme $\mathscr{W} \to \mathscr{Y}$. Comme H' est quotient de Γ, le théorème est démontré. ∎

8.6 Démonstration du théorème 1.3.

Sous les hypothèses du théorème 1.3, on identifie $\mathscr{C}_\Pi$ à la catégorie des K-schémas finis étales trivialisés par M. Notons $\mathfrak{R}$, comme en 6.3 (ii), la classe des bitorseurs $(\mathsf{G}', \mathsf{X}, \mathsf{G})$ de $\mathscr{C}_\Pi$ tels que le G-torseur X soit R-équivalent au torseur trivial.

Il s'agit de montrer que tout $(*, \underline{\underline{G}})$-bitorseur est dans $\mathfrak{R}$. Soit donc $\mathscr{X} = (\mathsf{G}', \mathsf{X}, \underline{\underline{G}})$ un tel bitorseur. D'après 8.5, on a $\mathscr{X} \cong \mathscr{Y} \wedge \mathscr{Z}$ avec $\mathscr{Y} = (\mathsf{G}', \mathsf{Y}, \mathsf{G}'')$ de type Γ et $\mathscr{Z} = (\mathsf{G}'', \mathsf{Z}, \underline{\underline{G}})$ de type π. Dans ces conditions, Z est un π-ensemble, donc $\mathscr{Z} \in \mathfrak{R}$ d'après la condition (ii) de 1.3. D'autre part, Y est induit, comme G'-torseur à gauche, par un torseur sous un quotient H' de Γ, dont le groupe sous-jacent est un sous-groupe de $|\mathsf{G}'|$ (d'après la remarque 8.3 (ii)), donc est isomorphe à un sous-groupe de G puisque $|\mathsf{G}'|$ est isomorphe à G. Donc $\mathscr{Y} \in \mathfrak{R}$, vu l'hypothèse (iii) de 1.3, d'où aussi $\mathscr{X} \in \mathfrak{R}$ puisque $\mathfrak{R}$ est stable par produit (6.3 (ii)), et le théorème est démontré. ∎

L'auteur remercie Jean-Louis Colliot-Thélène et Philippe Gille pour leurs remarques.

Références

[Br] L. Breen, *Bitorseurs et cohomologie non abélienne*, dans *The Grothendieck Festschrift I*, Progress in Math 86, 401-476, Birkhäuser (1990).

[C-F] J. W. S. Cassels et A. Fröhlich, *Algebraic Number Theory*, Academic Press, London and New York (1967).

[CT 1] J.-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*, Ann. of Math. 151 (2000), 359-373.

[CT-S 1] J.-L. Colliot-Thélène et J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. Éc. Norm. Sup. 10 (1977), 175-230.

[CT-S 2] J.-L. Colliot-Thélène et J.-J. Sansuc, *Principal Homogeneous Spaces under Flasque Tori ; Applications*, J. of Alg. 106 (1987), 148-205.

[D-G] M. Demazure et P. Gabriel, *Groupes Algébriques*, tome I, Masson-North-Holland (1970).

[Fu] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. of Math. 90 (1969), 75-109.

[Gil] P. Gille, *R-équivalence sur les G-revêtements sur les corps locaux non archimédiens*, J. Number Theory 91 (2001), 284-292.

[Gir] J. Giraud, *Cohomologie non abélienne*, Grundlehren Math. Wiss. 179, Springer (1971).

[MB 1] L. Moret-Bailly, *Construction de revêtements de courbes pointées*, J. of Alg. 240 (2001), 505-534.

[MB 2] L. Moret-Bailly, *R-équivalence simultanée de torseurs : un complément à l'article de P. Gille*, J. Number Theory 91 (2001), 293-296.

[SGA] M. Artin, A. Grothendieck et J.-L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas (SGA 4)*, tome 1, Lecture Notes in Math. 269, Springer (1972).