Séminaires & Congrès
5, 2001, p. 63–99

ESPACES DE HURWITZ

par

Michel Emsalem

***Résumé.* —** La catégorie des revêtements algébriques de la droite projective à invariants fixés (nombre de points de branchement, groupe de monodromie etc.) est une gerbe au dessus de son espace des modules grossiers. On esquisse ici différentes constructions de ces espaces de Hurwitz sur $\mathbb{Z}$, et l'on montre des applications arithmétiques de ces constructions : solution du problème inverse de Galois régulier sur $\mathbb{Q}_p$ ou plus généralement sur un corps large, propriétés arithmétiques du corps des modules d'un revêtement, existence de modèles ayant bonne réduction.

***Abstract* (Hurwitz spaces). —** The category of algebraic covers of the projective line with fixed invariants (number of branch points, monodromy group...) is a gerbe over its moduli space. We sketch differents constructions of these Hurwitz spaces over $\mathbb{Z}$, giving some arithmetic applications: solution of the regular inverse Galois problem over $\mathbb{Q}_p$ or more genrally over a large field, arithmetic properties of field of moduli of an algebraic cover, existence of models with good reduction.

1. Introduction

Le but de ces exposés est de présenter différentes constructions des espaces de modules de revêtements de la droite projective (appelés espaces de Hurwitz en référence à l'article original d'Hurwitz paru en 1891, où l'auteur définit une structure de variété complexe sur l'espace des revêtements dits « simples » de degré d de la sphère de Riemann [Hur]). Dans la suite on ne se limitera pas aux revêtements « simples » : on traitera la question des modules pour des revêtements généraux de la droite projective, et aussi des G-revêtements (c'est à dire des revêtements galoisiens de la droite projective donnés avec leurs groupes d'automorphismes). Pour disposer d'un espace de taille raisonnable, il faudra se fixer le degré, le nombre de points de branchement, et des invariants d'inertie.

***Classification mathématique par sujets* (2000). —** 14H30, 14D22, 11G99.
***Mots clefs.* —** Revêtements algébriques, espace des modules, gerbes, corps des modules, ramification, groupe de Galois, monodromie.

Pour les applications arithmétiques que l'on a en vue, on aura besoin de faire de ces espaces de Hurwitz des variétés algébriques, définies naturellement sur un corps de nombres (déterminé par des conditions combinatoires liées aux invariants de l'inertie, et dans la pratique souvent le corps $\mathbb{Q}$ des nombres rationnels) ; les points de l'espace de Hurwitz rationnels sur un corps K algébriquement clos de caractéristique 0 sont en correspondance biunivoque avec les classes d'isomorphisme de (G-) revêtements de la droite projective définis sur K [Fr1], [FrVö].

Une des applications les plus connues concerne le problème de Galois régulier sur $\mathbb{Q}$, qui consiste à se demander si un groupe fini G donné est le groupe de Galois d'une extension régulière de $\mathbb{Q}(t)$. Cette question peut s'exprimer en termes d'espaces de Hurwitz : la réponse positive à la question est équivalente à l'existence d'un espace de Hurwitz associé au groupe G possédant un point rationnel sur $\mathbb{Q}$. On verra que cette remarque conduit à la réalisation de certains groupes finis sur $\mathbb{Q}$ (en particulier sous les conditions de rigidité) [Fr1], [MaMa], [Th]. Elle permet aussi de montrer que le problème a une réponse positive pour tout groupe fini si on le pose sur certains corps assez gros à la place de $\mathbb{Q}$ [De2], [DeFr], [CT], [Mo-Ba1].

Les espaces de Hurwitz sont des *espaces de modules grossiers* : il n'existe pas en général de famille de Hurwitz universelle sur l'espace de Hurwitz. Mais de telles familles existent localement (au sens analytique sur $\mathbb{C}$, au sens étale de façon plus générale). Ces familles définissent une *gerbe* au-dessus de l'espace de Hurwitz ; à tout point géométrique h de l'espace de Hurwitz correspond une classe d'isomorphisme de (G-) revêtements dans la catégorie considérée définis sur un corps algébriquement clos de caractéristique 0. La gerbe des modèles de cette classe d'isomorphisme est la spécialisation au point h de la gerbe de Hurwitz. En particulier, le corps des modules de cette classe d'isomorphisme est le corps résiduel de h [DeDoEm].

Si l'on a en tête des applications arithmétiques plus fines, qui impliquent en particulier les réductions (bonnes ou mauvaises) des revêtements en des premiers, on doit traiter du problème des modules, non plus sur $\mathbb{Q}$, mais sur $\mathbb{Z}$. C'est ce que fait Fulton dans [Fu] pour les revêtements simples, avec comme conséquence l'irréductibilité de l'espace des modules de courbes de genre g. Cette construction a été généralisée par Wewers [We1] pour des revêtements quelconques. On présentera avec un peu plus de détails l'esquisse d'une construction de la gerbe de Hurwitz, ainsi qu'une présentation de cette gerbe utile dans les applications arithmétiques, suivant une méthode proposée par Bertin [Be], méthode qui reprend en les adaptant au contexte des (G-) revêtements la construction des espaces de modules de courbes de [DeMu].

Ces espaces de Hurwitz sur $\mathbb{Z}$ fournissent par exemple une preuve simple d'un théorème de Beckmann : les seuls nombres premiers qui se ramifient dans le corps des modules d'un (G-) revêtement sont les premiers où il y a mauvaise réduction et ceux qui divisent l'ordre du groupe de monodromie. Une étude plus fine de la gerbe de Hurwitz permet de montrer qu'en les premiers v n'appartenant pas à l'ensemble

fini de mauvaises places mentionné ci-dessus, le (G-) revêtement a un bon modèle sur l'extension non ramifiée maximale du complété K_v du corps K de rationalité du lieu de branchement en v [Em2]. Si l'on suppose de plus que le corps des modules du (G-) revêtement est $\mathbb{Q}$ par exemple, on en déduit qu'il en existe un bon modèle sur $\mathbb{Q}_p$ [DeHa]. En utilisant certaines familles de revêtements, plutôt que l'espace de Hurwitz lui-même, et un résultat de Moret-Bailly, [DeDoMo-Ba] montre que sous les mêmes hypothèses que précédemment, c'est à dire si le corps des modules du (G-) revêtement est $\mathbb{Q}$ et le nombre premier p n'est pas mauvais, le (G-) revêtement admet un modèle sur le corps $\mathbb{Q}^{tp}$ (les nombres algébriques dont tous les conjugués sont dans $\mathbb{Q}_p$).

Une étape supplémentaire consiste à traiter aussi des revêtements dégénérés, c'est à dire à compléter l'espace de Hurwitz en interprétant son bord [Be], [We1]. On mentionnera comme application le fait qu'une certaine composante irréductible de l'espace de Hurwitz introduite par Fried est définie sur $\mathbb{Q}$. On peut mentionner d'autres applications, dont il ne sera pas question dans ce texte, par exemple l'utilisation du bord de l'espace de Hurwitz pour réaliser certains groupes ([We2]) ou l'étude de la ramification de certains mauvais premiers dans le corps des modules ([EmFl]).

Enfin nous n'avons pas traité des questions concernant la gerbe de Hurwitz en les premiers qui divisent l'ordre du groupe de monodromie et qui ont été l'objet d'un certain nombre de travaux [BeMéz1], [BeMéz2], [GrMa], [HaSt], [He], [Sa2].

2. Espaces des modules grossiers, espace des modules fins

Un espace des modules pour une catégorie $\mathcal{C}$ est *grosso modo* un espace qui paramètre les classes d'isomorphisme d'objets de la catégorie $\mathcal{C}$. Ce paragraphe a pour but de préciser cette notion et de l'appliquer à la catégorie des revêtements algébriques ramifiés de la droite projective $\mathbb{P}^1$.

2.1. Catégorie fibrée au-dessus de la catégorie des schémas. — Les objets auxquels nous aurons affaire sont des objets algébriques relatifs, par exemple des variétés algébriques définies sur un *corps* ou un *anneau*, de façon plus générale des objets algébriques au-dessus d'un *schéma* S. De plus on a une notion de changement de base (par exemple l'extension de scalaires d'un corps k à une extension k' de k). La notion de *catégorie fibrée* introduite par A. Grothendieck [SGA1] formalise cette situation.

Définition 2.1. — Soit $\mathcal{S}$ la catégorie des schémas. Une catégorie fibrée au-dessus de $\mathcal{S}$ est la donnée d'une catégorie $\mathcal{C}$ munie d'un foncteur covariant $p : \mathcal{C} \to \mathcal{S}$ vérifiant les propriétés suivantes :

(1) Si, pour tout schéma S l'on note $\mathcal{C}(S) = p^{-1}(S)$ la catégorie des sections au dessus de S (les morphismes de $\mathcal{C}(S)$ sont ceux de $\mathcal{C}$ au-dessus de id_S), à

tout morphisme $f : S' \to S$ dans $\mathcal{S}$ est associé un foncteur covariant *image réciproque* $f^\star : \mathcal{C}(S) \to \mathcal{C}(S')$ et pour tout objet X de $\mathcal{C}(S)$ un morphisme *cartésien* $\alpha_X : f^\star(X) \to X$ au-dessus de f (*i.e.* tel que $p(\alpha_X) = f$).

(2) Le foncteur $f^\star$ vérifie les axiomes suivants : $\mathrm{id}^\star = \mathrm{id}$ et si f et g sont deux morphismes composables dans la catégorie $\mathcal{C}$, $(f \circ g)^\star \simeq g^\star \circ f^\star$ (*i.e.* il existe une équivalence naturelle $c_{f,g}$ de foncteurs entre $(f \circ g)^\star$ et $g^\star \circ f^\star$, ces équivalences naturelles satisfaisant une relation de cocycle pour trois morphismes f, g, h composables [SGA]).

(3) Si S est un schéma, X et Y deux objets de $\mathcal{C}(S)$ et $\lambda : Y \to X$ un morphisme dans $\mathcal{C}(S)$, alors $\lambda \circ \alpha_Y = \alpha_X \circ f^\star(\lambda)$.

Définition 2.2. — Un morphisme entre deux catégories fibrées $\mathcal{C}$ et$\mathcal{D}$ au-dessus de $\mathcal{S}_S$ est un foncteur $f : \mathcal{C} \to \mathcal{D}$ tel que pour tout objet U de la catégorie de base, f aille de $\mathcal{C}(U)$ dans $\mathcal{D}(U)$, et tel que f « commute » aux changements de bases.

Remarque 2.3

(a) On parlera de catégorie fibrée en groupoïdes lorsque, pour tout S la catégorie $\mathcal{C}(S)$ est un groupoïde, *i.e.* si tous les morphismes sont des isomorphismes. Il est facile de voir que ceci revient au fait que tous les morphismes dans la catégorie $\mathcal{C}$ sont cartésiens.

(b) Dire que le morphisme α_X est cartésien signifie que pour tout objet X'' de $\mathcal{C}(S')$ et tout morphisme $\beta : X'' \to X$ au-dessus de f, il existe un unique morphisme $\widetilde{\beta} : X'' \to f^\star(X)$ au-dessus de $\mathrm{id}_{S'}$ tel que $\alpha_X \circ \widetilde{\beta} = \beta$.

(c) La propriété $(f \circ g)^\star \simeq g^\star \circ f^\star$ énoncée dans (2) est une conséquence du fait que le produit de deux morphismes cartésiens est cartésien.

Exemple 2.4. — La catégorie $\mathcal{S}/\mathcal{S}$ des schémas au-dessus de la catégorie de base des schémas $\mathcal{S}$, est une catégorie fibrée : si $f : S' \to S$ un morphisme de schémas, $f^\star$ est simplement le foncteur qui associe à tout objet $X \to S$ de $\mathcal{S}/\mathcal{S}$ le produit fibré $X \times_S S' \to S'$.

Remarque 2.5. — Dans la définition de catégorie fibrée, au lieu de prendre comme catégorie de base la catégorie des schémas $\mathcal{S}$, on peut pour un schéma S fixé, prendre comme base la catégorie $\mathcal{S}_S$ des schémas au-dessus de S. C'est cette notion un peu plus générale qui apparaîtra le plus souvent dans la suite ; S sera par exemple $\mathrm{Spec}(\mathbb{Q})$, auquel cas la catégorie de base est celle des schémas sur un corps de caractéristique 0, ou bien $\mathrm{Spec}(\mathbb{Z}[T^{-1}])$, où T est un ensemble fini de nombres premiers. Lorsque l'on prend $S = \mathrm{Spec}(\mathbb{Z})$, on retrouve le cas particulier introduit d'abord.

2.2. Espace des modules fins. — La notion d'espace des modules fins est la plus forte. Soit comme précédemment $\mathcal{C}$ une catégorie fibrée au-dessus de la catégorie $\mathcal{S}_S$.

Définition 2.6. — Un espace des modules fins pour la catégorie $\mathcal{C}$ est un objet $X_0 \to M$ de $\mathcal{C}$ (où M est un objet de $\mathcal{S}_S$), universel au sens suivant :

pour tout objet $X \to T$ de $\mathcal{C}$ (où T est un objet de $\mathcal{S}_S$), il existe un unique morphisme f de T dans M et un unique morphisme cartésien $\alpha : X \to X_0$ au-dessus de f.

Autrement dit X_0 est une famille universelle d'espace de paramètres M : toute famille, provient, de façon unique, par image réciproque de la famille universelle.

Une conséquence immédiate de l'existence d'un espace des modules fins est que les objets de $\mathcal{C}$ ne peuvent avoir d'automorphisme non trivial. Très souvent dans la pratique, les catégories considérées ne vérifient pas cette hypothèse, et pour cette raison déjà, n'admettent pas d'espace des modules fins. Pour pallier cette difficulté, une méthode consistera à rigidifier la situation, c'est à dire à remplacer les objets de la catégorie $\mathcal{C}$, par des objets comportant des données supplémentaires, qui ne sont pas respectées par les automorphismes non triviaux.

2.3. Champs. — *Grosso modo*, un *champ* est une catégorie fibrée en groupoïdes, qui est un faisceau. Pour parler de faisceau, on a besoin que la catégorie base (catégorie des schémas ou des schémas au dessus d'un schéma donné S) soit munie d'une topologie (au sens de Grothendieck). Ce sera en général la topologie étale ou la topologie fpqc. On peut alors énoncer la définition suivante :

Définition 2.7. — Un champ est une catégorie fibrée en groupoïdes $\mathcal{C}$ au-dessus de $\mathcal{S}_S$, vérifiant les deux propriétés supplémentaires suivantes :

(i) Pour tout objet $U \to S$ de $\mathcal{S}_S$, et tout couple d'objets η et ξ de $\mathcal{C}(U)$, $\mathrm{Hom}_U(\eta, \xi)$ est un faisceau.

(ii) Dans la catégorie $\mathcal{C}$ *toute donnée de descente est effective.*

La deuxième condition est l'analogue de la condition de faisceau pour les objets. La donnée d'un objet global de $\mathcal{C}(U)$ est équivalente à une famille de donnée locales, *i.e.* d'objets ξ_i de $\mathcal{C}(U_i)$, où $(U_i)_{i\in I}$ est un raffinement de U, pourvus d'isomorphismes $f_{j,i} : \xi_{i|U_i\cap U_j} \to \xi_{j|U_i\cap U_j}$ assujettis aux conditions $f_{k,i} = f_{k,j} \circ f_{j,i}$ sur $U_i \cap U_j \cap U_k$. Pour plus de détails sur cette notion, voir l'exposé de J.-C. Douai dans ce volume [Do]. Le lecteur désireux d'approfondir la question pourra se reporter à [LaMo-Ba] et à [Vi].

Un *isomorphisme* entre deux champs $\mathcal{C}$ et $\mathcal{D}$ est un morphisme de catégories fibrées, qui réalise pour tout objet U de la base une équivalence de catégories entre $\mathcal{C}(U)$ et $\mathcal{D}(U)$.

Exemple 2.8. — Un schéma $\varphi : T \to S$ peut être considéré comme un champ particulier (à savoir $\mathcal{S}_T$, que l'on notera aussi simplement T) au-dessus de $\mathcal{S}_S$. Le foncteur de $\mathcal{S}_T \to \mathcal{S}_S$ est la composition à gauche par φ. Un morphisme de champs $T \to \mathcal{C}$ est alors simplement la donnée d'un objet de $\mathcal{C}(T)$.

Définition 2.9. — Un champ $\mathcal{C}$ est dit *représentable* s'il existe un schéma M et un morphisme $M \to \mathcal{C}$ qui est un isomorphisme de champs.