Séminaires & Congrès
5, 2001, p. 147–159

MODULES GALOISIENS SUR LES COURBES : UNE INTRODUCTION

par

Niels Borne

***Résumé.* —** Cet article est une introduction aux modules galoisiens sur les courbes. On commence par présenter un résultat de S. Nakajima concernant l'espace des différentielles holomorphes, et ses conséquences sur l'étude du groupe fondamental étale. On montre ensuite comment la connaissance de la structure du groupe de Grothendieck équivariant d'une courbe permet de résoudre partiellement le problème du calcul des modules galoisiens.

***Abstract* (Galois modules on curves : an introduction). —** To start with, we introduce a result of S. Nakajima concerning the space of holomorphic differentials, and its consequences on the study of the étale fundamental group. We then show how the knowledge of the structure of the equivariant Grothendieck group of a curve allows to solve partly the problem of the computation of Galois modules.

1. Le problème de Hecke et le groupe fondamental des courbes

1.1. Le problème de Hecke classique. — Le premier théorème de la théorie des modules galoisiens sur les courbes est dû à Chevalley et Weil en 1934 (voir [**4**]). Ce résultat est une réponse à un problème qu'avait posé Hecke (voir [**11**]), et que les auteurs ont reformulé de la manière suivante :

***Problème 1.1* (Hecke, 1928)**. — *Soit X une courbe algébrique sur $\mathbb{C}$ munie d'une action d'un groupe fini G. Comment décomposer l'espace des formes différentielles $H^0(X, \Omega_X)$ sur la courbe comme une somme directe de représentations indécomposables du groupe G ?*

Chevalley et Weil vont étendre le problème au cas des différentielles de degré quelconque. Par souci de simplicité, on énonce ici leur résultat dans un cas particulier.

***Classification mathématique par sujets* (2000). —** 14H37, 14C40.
***Mots clefs.* —** Automorphismes des courbes, Théorèmes de Riemann-Roch.

***Théorème 1.2* (Chevalley-Weil, 1934).** — *Soit X une courbe algébrique sur $\mathbb{C}$ munie d'une action libre d'un groupe fini G (i.e. le stabilisateur de tout point est trivial). Soit de plus $\pi : X \to Y = X/G$ le quotient et g_Y le genre de la courbe algébrique Y. On note $\mathbb{C}$ (resp. $\mathbb{C}[G]$) la représentation triviale (resp. régulière) de G. On a des isomorphismes entre représentations :*

(i) $H^0(X, \Omega_X) \simeq \mathbb{C} \oplus \mathbb{C}[G]^{\oplus g_Y - 1}$

(ii) $H^0(X, \Omega_X^{\otimes l}) \simeq \mathbb{C}[G]^{\oplus (2l-1)(g_Y-1)}$ *pour tout entier* $l > 1$

La version générale du théorème est valable sans hypothèse sur l'action, et a une forme analogue, avec des termes supplémentaires traduisant l'existence de points fixes. Comme on sait décomposer $\mathbb{C}[G]$ en somme de représentations indécomposables, cet énoncé répond complètement au problème de Hecke.

1.2. Le problème de Hecke modulaire. — On peut remarquer que le théorème de Chevalley-Weil implique le fait suivant : si une courbe algébrique sur $\mathbb{C}$ admet un revêtement galoisien non trivial, alors elle est de genre strictement positif, autrement dit le groupe fondamental de la droite projective sur $\mathbb{C}$ est nul (en fait, la formule de Riemann-Hurwitz suffit à le démontrer, et la formule (i) du théorème ci-dessus en est une version équivariante). Ceci est bien entendu un renseignement très faible sur le groupe fondamental des courbes algébriques sur $\mathbb{C}$, qui est par ailleurs bien connu. Cependant, le lien entre le problème de Hecke et le groupe fondamental est beaucoup plus intéressant dans un autre contexte, qu'on va exposer maintenant.

Dans la suite de cet article, la lettre X désignera une courbe algébrique projective et lisse sur un corps algébriquement clos k, avec une prédilection pour la caractéristique positive. On dira simplement que X est une courbe, et on supposera X munie d'une action fidèle d'un groupe fini G respectant sa structure algébrique et fixant le corps k. D'une part, on peut formuler un problème de Hecke sur k, et d'autre part on dispose du groupe fondamental algébrique du quotient $Y = X/G$ qui classe les revêtements algébriques étales de Y.

Lorsque le corps k considéré est de caractéristique nulle, la situation est totalement analogue au cas des courbes algébriques sur $\mathbb{C}$: le problème de Hecke admet exactement la même réponse, et le groupe fondamental étale est connu grâce au travaux de Grothendieck (voir SGA1). Par contre, en caractéristique positive, des différences apparaissent : on n'a que des renseignements partiels sur le groupe fondamental (voir par exemple l'introduction de [**17**] pour un résumé), et bien que le problème de Hecke soit résolu dès que l'action est modérée (voir [**12**], Theorem 3), l'analogue de la formule de Chevalley-Weil n'est plus valable en général, mais seulement lorsque la caractéristique de k ne divise pas l'ordre de G.

De plus, Shoichi Nakajima a montré en 1984 que la réponse au problème de Hecke (qu'on appelera modulaire dans ce cas, en référence à la théorie de la représentation du même nom) fournit des renseignements non triviaux sur le groupe fondamental étale (voir [**15**]). Pour expliquer ce lien, on va formuler un deuxième problème, le « problème inverse » suivant.

Problème 1.3. — *Soit Y une courbe algébrique projective et lisse sur un corps algébriquement clos k, et G un groupe fini. À quelle condition existe-t-il un revêtement étale $X \to Y$ galoisien de groupe G ?*

Une courbe Y étant fixée, on note $\mathcal{G}_Y$ l'ensemble des groupes G pour lesquels le problème ci-dessus admet une réponse positive. On montre que déterminer $\pi_1^{\text{ét}}(Y)$ revient à déterminer $\mathcal{G}_Y$ (d'après [**8**], proposition 15.4, c'est une conséquence du fait que le groupe fondamental d'une courbe projective est topologiquement de type fini, ce qui résulte du théorème de spécialisation, voir SGA1, XIII, Corollaire 2.12). On suppose à présent que la caractéristique de k est strictement positive, et on la note p. Lorsque G est un p-groupe, on peut à la fois donner une réponse simple au problème de Hecke (voir ci-dessous) et déterminer si G appartient ou non à $\mathcal{G}_Y$. En effet il est connu qu'un p-groupe G appartient à $\mathcal{G}_Y$ si et seulement s'il peut être engendré par au plus h_Y générateurs, où h_Y désigne l'invariant de Hasse-Witt de la courbe Y (c'est le théorème de Shafarevitch, voir [**19**] et par exemple [**2**] pour une preuve moderne). À noter que $0 \leqslant h_Y \leqslant g_Y$.

Il n'est pas question, ici, de faire un panorama des différents travaux concernant le problème du groupe fondamental des courbes projectives en caractéristique positive, mais seulement d'évoquer son lien avec les modules galoisiens, à travers le remarquable résultat suivant :

Théorème 1.4 **(Nakajima, 1984)**. — *Soient X et Y deux courbes sur k, et $X \to Y$ un revêtement galoisien étale de groupe G. On note I l'idéal d'augmentation de l'anneau du groupe $k[G]$. On a une suite exacte courte de représentations :*

$$0 \to H^0(X, \Omega_X) \to k[G]^{\oplus g_Y} \to I \to 0$$

Cette suite exacte détermine complètement la structure de $H^0(X, \Omega_X)$ en tant que représentation de G.

Soit d_G le nombre minimal de générateurs de G. En utilisant une construction en théorie des représentations modulaires, la « loop-space operation » Ω, Nakajima peut exprimer explicitement la structure de l'espace des différentielles dans un cas particulier.

Corollaire 1.5. — *Si G est un p-groupe, l'espace des différentielles holomorphes sur X admet la décomposition en indécomposables suivante :*

$$H^0(X, \Omega_X) \simeq k[G]^{\oplus g_Y - d_G} \oplus \Omega^2 k.$$

Comme $k[G]$ est un indécomposable projectif, et $\Omega^2 k$ est un indécomposable qui ne l'est pas, ce corollaire donne la condition nécessaire : si un p-groupe G appartient $\mathcal{G}_Y$, alors $d_G \leqslant g_Y$. Pour une courbe ordinaire, $h_Y = g_Y$, et on retrouve la condition ci-dessus.

2. Généralités sur les modules galoisiens

2.1. Théorie de la représentation. — On rappelle qu'une représentation linéaire d'un groupe fini G est un morphisme $\rho : G \to \mathrm{GL}(V)$ de G dans le groupe linéaire d'un espace vectoriel V de dimension finie sur un corps k algébriquement clos donné. Si $k[G]$ désigne l'anneau du groupe, les représentations sont les $k[G]$-modules de type fini.

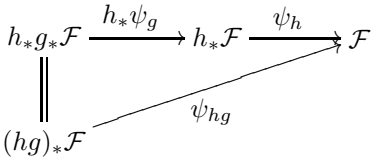
L'anneau $k[G]$ est semi-simple si et seulement si la caractéristique de k ne divise pas l'ordre de G. Dans ce cas, $k[G]$-modules indécomposables et $k[G]$-modules simples coïncident. Dans le cas général, il y a lieu de faire la distinction. Rappelons que tout $k[G]$-module admet une décomposition en $k[G]$-modules indécomposables, et le théorème de Krull-Schmidt assure l'unicité des coefficients entiers intervenant dans cette décomposition.

2.2. G-faisceaux. — Soit X une courbe munie d'une action d'un groupe fini G. Comme le précise Grothendieck dans le Tohoku (voir [**10**]), si l'action de G respecte la structure de X, tout faisceau sur X défini en des termes structurels va donner lieu à des représentations de X : l'espace des sections globales associé, mais aussi les différents groupes de cohomologie. Il est utile de formaliser cette notion, ce qu'il est possible de faire de la manière suivante :

Définition 2.1. — Soit $\mathcal{F}$ un faisceau (d'ensembles, de groupes, ...) sur X. On appelle G-linéarisation de $\mathcal{F}$ la donnée d'une collection $(\psi_g)_{g\in G}$ de morphismes de faisceaux $\psi_g : g_*\mathcal{F} \to \mathcal{F}$ vérifiant les conditions suivantes :

(1) $\psi_1 = \mathrm{Id}$

(2) $\psi_{hg} = \psi_h \circ h_*(\psi_g)$ (condition de cocycle), autrement dit, le diagramme suivant commute :



Un G-faisceau sur X est un faisceau muni d'une G-linéarisation.

Parmi les exemples immédiats de G-faisceaux, on peut citer les faisceaux des différentielles d'ordre l sur la courbe $\Omega_X^{\otimes l}$, ou encore les faisceaux $\mathcal{L}_X(D)$ associés aux diviseurs G-invariants D.

2.3. Problème de Riemann équivariant. — Les G-faisceaux cohérents sur une courbe (et plus généralement sur une variété) X fournissent des représentations d'origine géométrique que l'on appelle parfois les *modules galoisiens*. La question fondamentale dans l'étude de ces modules est la suivante :

Problème 2.2. — *Soit X une courbe munie d'une action d'un groupe fini G, et $\mathcal{F}$ un G-faisceau cohérent sur X. Comment décomposer $H^0(X, \mathcal{F})$ comme une somme de modules indécomposables ?*

Parmi les applications de l'étude des modules galoisiens on peut noter, outre l'étude du groupe fondamental, l'étude des singularités de l'espace des modules grossier $\mathcal{M}_g$ des courbes de genre g.

Lønsted a en effet donné une démonstration utilisant les structures galoisiennes du théorème de Rauch-Popp-Oort (voir [**14**]). Rappelons ce résultat.

Théorème 2.3 **(Rauch-Popp-Oort)**. — *Soit $\mathcal{M}_g$ l'espace des modules grossier des courbes de genre g, et P le point de $\mathcal{M}_g$ correspondant à une courbe X.*

(i) Supposons $g \geqslant 4$. Alors P est un point singulier de $\mathcal{M}_g$ si et seulement si le groupe d'automorphismes de X est non trivial.

(ii) Supposons $g = 3$. Alors si X n'est pas hyperelliptique, P est un point singulier de $\mathcal{M}_g$ si et seulement si le groupe d'automorphismes de X est non trivial ; si X est hyperelliptique, P est un point singulier de $\mathcal{M}_g$ si et seulement si le groupe d'automorphismes de X n'est pas d'ordre 2.

C'est la structure galoisienne du fibré tangent à X qui constitue l'un des point-clefs de la démonstration (voir [**14**] pour plus de détails).

3. Approche par des formules de trace

3.1. Théorie des caractères. — La théorie des caractères permet d'associer à toute représentation $\rho : G \to \mathrm{GL}(V)$ un invariant que l'on va noter provisoirement $c(V)$. Lorsque le corps de base k est de caractéristique zéro, $c(V)$ est simplement la fonction de G dans k définie par $c(V)(g) = \mathrm{tr}(\rho(g))$. Lorsque la caractéristique de k est strictement positive, il faut employer des caractères de Brauer (voir [**18**], rappelons qu'un caractère de Brauer relève la trace en caractéristique 0 sur les éléments p-réguliers). Dans la suite, le terme caractère désignera toujours un caractère de Brauer.

Lorsque $k[G]$ est semi-simple, $c(V)$ caractérise complètement V, autrement dit deux représentations sont isomorphes si et seulement si leurs caractères sont égaux. Cette assertion est fausse lorsque $k[G]$ n'est pas semi-simple, mais il est par contre exact que deux $k[G]$-modules *projectifs* de type fini ayant même caractère de Brauer sont isomorphes.

Vus comme fonctions à valeurs dans un anneau, les caractères engendrent un anneau, noté $R_k(G)$, appelé anneau des caractères virtuels. Tout caractère virtuel est la différence des caractères de deux représentations. Comme groupe, on montre que $R_k(G)$ est le groupe abélien libre engendré par les caractères des représentations irréductibles (i.e des $k[G]$-modules simples) de G.