SÉMINAIRES ET CONGRÈS 13

GROUPES DE GALOIS ARITHMÉTIQUES ET DIFFÉRENTIELS

édité par

Daniel Bertrand

Pierre Dèbes

Société Mathématique de France 2006

D. Bertrand

Institut de Mathématiques de Jussieu (UMR 7586), Université Pierre et Marie Curie, Case 247, 4 Place Jussieu, 75252 Paris Cedex 05, France.

E-mail : `bertrand@math.jussieu.fr`

P. Dèbes

Laboratoire Paul Painlevé (UMR 8524), U.F.R. Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France.

E-mail : `Pierre.Debes@univ-lille1.fr`

***Classification mathématique par sujets* (2000). —** 03B35, 11Fxx, 11Gxx, 11R58, 11Yxx, 12Exx, 12Fxx, 12Gxx, 12Hxx, 12Jxx, 13Nxx, 14Dxx, 14-04, 14F05, 14Gxx, 14Hxx, 18A25, 20B05, 20Cxx, 20D25, 20Exx, 20Fxx, 20Gxx, 20Jxx, 32J25, 32S40, 33C05, 34Axx, 34M55, 35Cxx, 53Cxx, 65E05, 65Y20, 68Q15.

***Mots clefs*. —** Algorithmes, correspondance de Riemann-Hilbert, dessins d'enfants, équations différentielles p-adiques, espaces de Hurwitz, formes modulaires, géométrie anabélienne, groupe de Galois différentiel, groupe fondamental, groupes de tresse, espaces de modules, problème de Galois inverse, revêtement des courbes, théorie de Galois, tours modulaires.

GROUPES DE GALOIS ARITHMÉTIQUES ET DIFFÉRENTIELS

édité par Daniel Bertrand, Pierre Dèbes

Résumé. — Ce volume constitue les actes du colloque sur les groupes de Galois arithmétiques et différentiels qui s'est déroulé au CIRM de Luminy (France) du 8 au 13 Mars 2004. Le but était de rendre compte du rapprochement en cours entre les deux théories, et de le développer. Le volume, à l'image du colloque, aborde des thèmes communs aux deux théories : espaces de modules (de courbes, de revêtements, de connexions), questions arithmétiques (corps de définition, théorie de la descente), groupes fondamentaux, problèmes inverses, méthodes de déformation, calculs et réalisations explicites de groupes de Galois, aspects algorithmiques.

***Abstract* (Arithmetic and differential Galois groups).** — On March 8-13, 2004, a meeting was organized at the Luminy CIRM (France) on arithmetic and differential Galois groups, reflecting the growing interactions between the two theories. The present volume collects the proceedings of this conference. It covers the following themes: moduli spaces (of curves, of coverings, of connexions), including the recent developments on modular towers; the arithmetic of coverings and of differential equations (fields of definition, descent theory); fundamental groups; the inverse problems and methods of deformation; and the algorithmic aspects of the theories, with explicit computations or realizations of Galois groups.

TABLE DES MATIÈRES

RÉSUMÉS DES ARTICLES

Cet article s'intéresse aux opérateurs différentiels de deuxième et troisième ordre. Nous introduisons une notion d'opérateur standard, et montrons que tout opérateur différentiel de groupe de Galois différentiel fini est image inverse d'un opérateur standard. Nous donnons aussi un algorithme concernant certaines extensions de corps, associées à des solutions algébriques d'une équation de Riccati.

Le but est de compléter des résultats de M.F. Singer concernant la variation des groupes de Galois différentiels. Soit C un corps algébriquement clos, de caractéristique 0. On considère des familles de connections de rang n sur la droite projective, paramétrisées par des schémas X sur C. Soit $G \subset \mathrm{GL}_n$ un sous-groupe algébrique. On montre que $X(=G)$, l'ensemble des points fermés de X avec G comme groupe de Galois différentiel, est constructible pour toute famille si et seulement si le groupe G satisfait une condition introduite par M.F. Singer. Pour la démonstration, des techniques concernant des familles de fibrés vectoriels et des connections sont développées.

Nous donnons une brève introduction à l'isomonodromie et à la sixième équation différentielle de Painlevé, ce qui conduit à des questions sur les solutions algébriques.

Les équations différentielles ordinaires possèdent un analogue arithmétique où les fonctions et leurs dérivées sont remplacées par des nombres entiers et leurs quotients de Fermat. Cet article présente les principes de cette théorie et quelques applications à la théorie des invariants pour les correspondances.

On étudie la complexité et la stabilité des calculs dans la jacobienne des courbes de grand genre sur le corps des complexes avec une attention particulière aux courbes modulaires.

Les tours modulaires ont été introduites par M. Fried. Ce sont des tours d'espaces de Hurwitz dont les niveaux correspondent aux quotients caractéristiques du p-revêtement universel de Frattini d'un groupe fini fixé, le premier p étant un diviseur de l'ordre du groupe. La tour des courbes modulaires de niveaux p^n $(n > 0)$ est l'exemple initial : le groupe fini est dans ce cas le groupe diédral d'ordre $2p$. Il y a des conjectures diophantiennes sur les tours modulaires, qui s'inspirent de la situation des courbes modulaires : l'esprit est que les points rationnels sur un corps de nombres fixé disparaissent au-delà d'un certain niveau. Dans cet article, qui est le premier d'une série de trois sur le sujet dans ce volume, après avoir revu la construction des tours modulaires, nous revenons sur ces conjectures, en examinons l'impact et expliquons quelques résultats.

On continue l'étude de la variation de la cohomologie parabolique commencée dans [**DW**]. En particulier, on donne des formules pour l'accouplement de Poincaré sur la cohomologie parabolique, et on calcule la monodromie du système de Picard-Euler, confirmant un résultat classique de Picard.

Le genre des courbes projectives est un invariant discret qui permet une première classification des relations algébriques en deux variables. On peut ainsi se concentrer sur les espaces de modules connexes $\mathcal{M}_g$ des courbes de genre g donné. Pourtant de nombreux problèmes nécessitent la donnée supplémentaire d'une fonction sur la courbe. Les espaces de modules correspondants sont les espaces de Hurwitz, dont il existe plusieurs variantes, répondant à des besoins divers. Une classe de Nielsen (§1) est un ensemble, constitué à partir d'un groupe G et d'un ensemble $\mathbf{C}$ de $r \geq 3$ classes de conjugaison de G, qui décrit la monodromie de la fonction. C'est un analogue frappant du genre.

En utilisant les revêtements de Frattini de G, chaque classe de Nielsen fournit un système projectif de classes de Nielsen dérivées, pour tout premier p divisant $|G|$. Un système projectif non vide (infini) d'orbites d'actions de tresses dans ces classes de Nielsen est une branche infinie d'un arbre de composantes. Cela correspond à un système projectif de composantes irréductibles (de dimension $r-3$) de $\{\mathcal{H}(G_{p,k}(G), \mathbf{C})\}_{k=0}^{\infty}$, la tour modulaire. La tour classique des courbes modulaires $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ (le cas le plus simple où G est le groupe diédral D_{2p}, $r = 4$ et $\mathbf{C}$ la classe d'involution répétée 4 fois) en est un avatar.

La conjecture principale (faible) dit que, si G est p-parfait, il n'y a pas de points rationnels au delà d'un niveau suffisamment élevé d'une branche de composantes. Quand $r = 4$, les tours modulaires (privées des pointes) sont des systèmes de quotients du demi-plan supérieur au-dessus de la droite projective de paramètre j. Nos thèmes.

- §3 et §4 : Identification des branches de composantes sur une tour modulaire à partir des branches de pointes $g - p'$, p et Weigel, grâce à la généralisation des structures de spin.
- §5 : Énoncé d'un ensemble de propriétés des branches de pointes impliquant la conjecture principale (faible) et réduction à un nombre limité de cas de tours pouvant encore éventuellement la mettre en défaut.
- §6 : Formulation d'une conjecture principale forte pour des tours modulaires de rang supérieur (avec des exemples) : presque tous les premiers conduisent à un système semblable à celui des courbes modulaires.

Cet article présente quelques développements récents dans l'étude des opérateurs de Lamé à monodromie finie. On décrit l'approche basée sur la théorie des pull-back développée par Klein et utilisée par Baldassarri ([**Bal81**]) pour décrire la monodromie projective. On fait ensuite le lien avec la théorie des dessins d'enfants de Grothendieck, qui amène à des descriptions et à des formules explicites. On revient également sur les résultats de Beukers and van der Waall ([**BvdW04**]) concernant la monodromie. La dernière partie est consacrée à l'étude des opérateurs de Lamé L_1 avec monodromie finie en termes des valeurs de la fonction zéta de Weierstraß correspondant à la courbe elliptique attachée à L_1 et au lien avec les formes modulaires.

Dans cette note nous donnons un bref survol de résultats récents sur le problème classique de Riemann-Hilbert pour des équations différentielles sur la sphère de Riemann. Nous mettons l'accent sur des aspects géométriques du problème faisant intervenir la notion de stabilité de fibrés vectoriels avec connexions.

Un D-module local borné est un module différentiel sur un anneau local différentiel R qui possède des bases sur R pour les solutions de congruence. Si R est muni d'une dérivation itérative, un tel D-module en plus est un module différentiel itératif (ID-module) sur R. Dans ce texte nous présentons une solution du problème inverse de Galois connexe pour les D-modules bornés sur des corps d'éléments analytiques $K\{t\}$. Dans le cas où le corps résiduel de K est algébriquement clos nous donnons en plus une solution du problème inverse pour les groupes linéaires non connexes. Finalement nous étudions la relation entre les ID-modules locaux et leurs réductions.

Dans cet article nous montrons comment retrouver une classe spéciale de valuations de corps de fonctions (qui généralisent naturellement les diviseurs premiers de Zariski) à partir de la théorie de Galois des corps de fonctions en question. Ces valuations jouent un rôle central en géométrie anabélienne birationnelle et pour d'autres questions connexes.

Cet article a pour but de donner une introduction à la théorie des espaces de Hurwitz et un aperçu des différentes méthodes pour leur construction.

Des considérations géométriques permettent d'identifier quelles propriétés nous souhaitons pour la suite canonique de groupes finis qui sont utilisés pour définir les tours modulaires. Par exemple, les groupes doivent être de centre trivial pour que les espaces de Hurwitz constituant la tour modulaire soient des espaces de modules fins. Notre suite est donnée par la série de Frattini, qui est définie inductivement : chaque groupe est le domaine d'un épimorphisme canonique, lequel a comme noyau un p-groupe abélien élémentaire, et le groupe précédent comme image. En plus de satisfaire les propriétés désirées, ce choix s'interprète naturellement en termes de théorie des représentations modulaires.

Chaque épimorphisme entre deux groupes induit (de manière covariante) un morphisme entre les espaces de Hurwitz correspondants. La factorisation de l'épimorphisme de groupes en épimorphismes irréductibles intermédiaires permet de déterminer plus simplement comment l'application entre espaces de Hurwitz se ramifie et quand les composantes connexes ont des images inverses vides. Pour cela, seuls comptent les épimorphismes intermédiaires qui ont un noyau central d'ordre p. Les plus importants de ces épimorphismes sont ceux à travers lesquels le p-revêtement universel de Frattini se factorise ; ils sont classifiés par le p-groupe élémentaire abélien des multiplicateurs de Schur.

Cet article, le deuxième de trois sur les tours modulaires dans ce volume, revient, à l'intention des arithméticiens-géomètres, sur la théorie des groupes nécessaire à cette théorie, pour aboutir à l'état actuel des connaissances sur les p-groupes de multiplicateurs de Schur de notre suite de groupes.

Ceci est une discussion informelle de la façon dont le problème de la construction des variétés algébriques avec diverses comportements topologiques, motive la recherche des méthodes formelles dans l'écriture des mathématiques vérifée sur machine. Aussi incluse est une discussion brève de mes travaux sur la formalisation de la théorie des catégories dans un environnement « ZFC » en utilisant l'assistant de preuves Coq.

ABSTRACTS

Algorithms and Moduli Spaces for Differential Equations
MAINT BERKENBOSCH 1

This article discusses second and third order differential operators. We will define standard operators, and prove that every differential operator with finite differential Galois group is a so-called pullback of some standard operator. We will also give an algorithm concerning certain field extensions, associated with algebraic solutions of a Riccati equation.

Families of linear differential equations on the projective line
MAINT BERKENBOSCH & MARIUS VAN DER PUT 39

The aim is to extend results of M.F. Singer on the variation of differential Galois groups. Let C be an algebraically closed field of characteristic 0. One considers certain families of connections of rank n on the projective line parametrized by schemes X over C. Let $G \subset \mathrm{GL}_n$ be an algebraic subgroup. It is shown that $X(=G)$, the set of closed points with differential Galois group G, is constructible for all families if and only if G satisfies a condition introduced by M.F. Singer. For the proof, techniques for handling families of vector bundles and connections are developed.

Brief introduction to Painlevé VI
PHILIP BOALCH 69

We will give a quick introduction to isomonodromy and the sixth Painlevé differential equation, leading to some questions regarding algebraic solutions.

Ordinary differential equations have an arithmetic analogue in which functions are replaced by integer numbers and the derivative operator is replaced by a Fermat quotient operator. This paper reviews the basics of this theory and explains some of the applications to the invariant theory of correspondences.

This paper is concerned with the complexity and stability of arithmetic operations in the jacobian variety of curves over the field of complex numbers, as the genus grows to infinity. We focus on modular curves.

Modular towers have been introduced by M. Fried. They are towers of Hurwitz spaces, with levels corresponding to the characteristic quotients of the p-universal Frattini cover of a fixed finite group and with p a prime divisor of the order of the group. The tower of modular curves of levels p^n $(n > 0)$ is the original example: the finite group is then the dihedral group of order $2p$. There are diophantine conjectures on modular towers, inspired by modular curves: the spirit is that over a number field, rational points do not exist beyond a certain level. In this paper, which is the first of a series of three on this topic in this volume, after defining modular towers, we discuss the significance of these conjectures and explain some results.

We continue our study of the variation of parabolic cohomology ([**DW**]) and derive an exact formula for the underlying Poincaré duality. As an illustration of our methods, we compute the monodromy of the Picard-Euler system and its invariant Hermitian form, reproving a classical theorem of Picard.

The genus of projective curves discretely separates decidedly different two variable algebraic relations. So, we can focus on the connected moduli $\mathcal{M}_g$ of genus g curves. Yet, modern applications require a data variable (function) on such curves. The resulting spaces are versions, depending on our need from this data variable, of *Hurwitz spaces*. A *Nielsen class* (§1) is a set defined by $r \geq 3$ conjugacy classes $\mathbf{C}$ in the data variable monodromy G. It gives a striking genus analog.

Using Frattini covers of G, every Nielsen class produces a projective system of related Nielsen classes for any prime p dividing $|G|$. A nonempty (infinite) projective system of braid orbits in these Nielsen classes is an infinite $(G, \mathbf{C})$ *component (tree) branch*. These correspond to projective systems of irreducible (dim $r-3$) components from $\{\mathcal{H}(G_{p,k}(G), \mathbf{C})\}_{k=0}^{\infty}$, the $(G, \mathbf{C}, p)$ Modular Tower (**MT**). The classical modular curve towers $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ (simplest case: G is dihedral, $r = 4$, $\mathbf{C}$ are involution classes) are an avatar.

The (weak) Main Conjecture 1.2 says, if G is *p-perfect*, there are no rational points at high levels of a component branch. When $r = 4$, **MT**s (minus their cusps) are systems of upper half plane quotients covering the j-line. Our topics.

- §3 and §4: Identifying component branches on a **MT** from *g-p′, p and Weigel cusp branches* using the **MT** generalization of *spin structures*.
- §5: Listing cusp branch properties that imply the (weak) Main Conjecture and extracting the small list of towers that could possibly fail the conjecture.
- §6: Formulating a (strong) Main Conjecture for higher rank **MT**s (with examples): almost all primes produce a modular curve-like system.

This survey paper contains recent developments in the study of Lamé operators having finite monodromy group. We present the approach based on the pull-back theory of Klein, that allowed the description of the projective monodromy groups by Baldassarri ([**Bal81**]), as well as the connection with Grothendieck's theory of dessins d'enfants, that leads to explicit properties and formulae. The results of Beukers and van der Waall ([**BvdW04**]) concerning the full monodromy group are also presented. The last section describes the Lamé operators L_1 with finite monodromy in terms of the values of the Weierstraß zeta function corresponding to the elliptic curve associated to L_1, as well as the connection with the modular forms.

In this note we give a brief survey of recent results on the classical Riemann-Hilbert problem for differential equations on the Riemann sphere. We emphasize geometrical aspects of the problem involving the notion of stability of vector bundles with connections.

An integral (or bounded) local D-module is a differential module over a local D-ring R having congruence solution bases over R. In case R is equipped with an iterative derivation, such a D-module is an iterative differential module (ID-module) over R. In this paper we solve the connected inverse Galois problem for integral D-modules over fields of analytic elements $K\{t\}$. In case the residue field of K is algebraically closed, we are able to additionally solve the non-connected inverse Galois problem. Further we study the behaviour of ID-modules by reduction of constants.

In this paper we show how to recover a special class of valuations (which generalize in a natural way the Zariski prime divisors) of function fields from the Galois theory of the functions fields in discussion. These valuations play a central role in the birational anabelian geometry and related questions.

This paper is intended to serve as a general introduction to the theory of Hurwitz spaces and as an overview over the different methods for their construction.

Geometric considerations identify what properties we desire of the canonical sequence of finite groups that are used to define modular towers. For instance, we need the groups to have trivial center for the Hurwitz spaces in the modular tower to be fine moduli spaces. The Frattini series, constructed inductively, provides our sequence: each group is the domain of a canonical epimorphism, which has elementary abelian p-group kernel, having the previous group as its range. Besides satisfying the desired properties, this choice is readily analyzable with modular representation theory.

Each epimorphism between two groups induces (covariantly) a morphism between the corresponding Hurwitz spaces. Factoring the group epimorphism into intermediate irreducible epimorphisms simplifies determining how the Hurwitz-space map ramifies and when connected components have empty preimage. Only intermediate epimorphisms that have central kernel of order p matter for this. The most important such epimorphisms are those through which the universal central p-Frattini cover factors; the elementary abelian p-Schur multiplier classifies these.

This paper, the second of three in this volume on the topic of modular towers, reviews for arithmetic-geometers the relevant group theory, culminating with the current knowledge of the p-Schur multipliers of our sequence of groups.

This is an informal discussion of how the construction problem in algebraic geometry, that is the problem of constructing algebraic varieties with various topological behaviors, motivates the search for methods of doing mathematics in a formal, machine-checked way. I also include a brief discussion of some of my work on the formalization of category theory within a ZFC-like environment in the Coq proof assistant.

PRÉFACE

Les recherches récentes en théorie de Galois des polynômes $P(T,Y)$ (ou des fonctions algébriques) d'une part et des opérateurs différentiels $L(T,\partial)$ d'autre part, ont rapproché ces deux théories. Dans les deux situations, on se fixe une base géométrique, et on s'intéresse aux extensions, algébriques ou différentielles, de cette base. Parmi les principaux résultats qui ont marqué cette convergence, on peut citer la conjecture d'Abhyankar et son analogue différentiel, le problème inverse de Galois (classique ou différentiel) sur $k(T)$ pour un corps k algébriquement clos ou assez “large”, ainsi qu'un certain nombre de réalisations explicites sur des petits corps (notamment grâce à la méthode de rigidité).

Le colloque de Luminy avait pour but de favoriser les échanges et collaborations entre chercheurs des deux domaines ; il a porté sur les thèmes suivants, communs aux deux directions :

- espaces de modules : espaces de modules de courbes et de revêtements, espaces de modules pour des connexions, compactification, tours modulaires ;
- arithmétique des revêtements et des équations différentielles : corps de définition, théorie de la descente, dessins d'enfant ;
- groupes fondamentaux, en toutes caractéristiques : conjecture d'Abhyankhar, problèmes inverses, méthodes de déformation ;
- théorie de Galois explicite : calcul de groupes de Galois, réalisation explicite de groupes, méthode de rigidité.

Les articles contenus dans ce volume reflètent ce programme, avec un accent particulier sur les questions de modules.

Ainsi, dans le cadre algébrique, le texte de M. Romagny et S. Wewers est une introduction moderne aux espaces de modules de revêtements (espaces de Hurwitz) : travaux récents sur leur construction (sur $\mathrm{Spec}(\mathbb{Z})$, compactification), applications arithmétiques ou aux questions de réduction. Les trois articles de P. Dèbes, M. Fried et D. Semmen couvrent un développement en cours des espaces de Hurwitz, la théorie des tours modulaires : construction et applications, recherche de composantes (composantes de Harbater-Mumford), conjecture de Fried sur les points rationnels, pro-points sur des corps complets.

Dans le cadre différentiel, l'article de Berkenbosch et van der Put décrit la variation du groupe de Galois dans une famille d'équations différentielles, et celui de Dettweiler et Wewers la variation de la cohomologie parabolique. On trouvera les récents progrès sur le problème de Riemann-Hilbert dans l'article de Malek, tandis que les questions d'isomonodromie sont développées dans l'article de Boalch sur Painlevé VI.

Ce dernier article présente une nouvelle construction d'équations différentielles à solutions algébriques. Ce thème, à la jonction des deux domaines depuis leur origine, fait également l'objet de l'article de Berkenbosch, qui étend le théorème de Klein aux équations d'ordre 3, et de celui de Litcanu et Zapponi, qui traite d'équations de Lamé à monodromie finie. Les courbes modulaire y apparaissent, et sont étudiées en détail dans l'article de Couveignes. L'aspect algorithmique, très présent dans ces differents textes, est abordé de façon théorique par celui de Simpson.

Le cadre différentiel n'oublie pas la caractéristique p : voir l'article de Matzat, qui fait le lien entre ces questions et les équations différentielles p-adiques et celui de Buium sur la théorie géométrique des quotients de Fermat. Enfin, du côté algébrique, l'article de Pop concerne la conjecture anabélienne pour un corps de fonctions K sur un corps algébriquement clos de caractéristique différente d'un nombre premier ℓ : on y voit comment retrouver les diviseurs de Zariski premiers à partir du pro-ℓ groupe de Galois maximal au-dessus de K.

Outre les présents éditeurs, le comité scientifique du colloque était composé d'Y. André (ENS Paris), D. Harbater (Univ. Penn.), H. Matzat (IWR Heidelberg), M. van der Put (Univ. Groningen) et M. Singer (MSRI). Nous les remercions ici pour leur collaboration. Nous remercions également pour leur travail les rapporteurs des textes publiés dans ce volume.

D. Bertrand & P. Dèbes