ASTÉRISQUE 294

SÉMINAIRE BOURBAKI
VOLUME 2002/2003
EXPOSÉS 909-923

Société Mathématique de France 2004
Publié avec le concours du Centre National de la Recherche Scientifique

Association des collaborateurs de Nicolas Bourbaki, École normale supérieure,
45, rue d'Ulm, F-75230 Paris Cedex 05.
Url : `http://www.bourbaki.ens.fr/`

Mots clefs et classification mathématique par sujets **(2000)**

Exposé n° 909. — Unités cyclotomiques, paires de Wieferich. — 11D61, 11R18, 11J86, 11R27, 11R33, 11Y50.
Exposé n° 910. — Irrationalité, fonction zêta de Riemann, série hypergéométrique, approximant de Padé, théorème d'Apéry, approximation rationnelle, polylogarithme. — 11J72, 11G55, 11M06, 33C20, 41A21.
Exposé n° 911. — Équations des ondes non linéaires, optique géométrique, instabilité. — 35L30.
Exposé n° 912. — Polyèdres flexibles, volume, places. — 52C25, 52B10, 52B45.
Exposé n° 913. — Représentations unitaires, 1-cohomologie, groupes algébriques simples, réseaux, applications harmoniques, spectres de graphes. — 22D10, 22E40, 22E41, 05C50, 53C43.
Exposé n° 914. — Variété de Fano, variété rationnellement connexes par chaînes, points rationnels, groupe fondamental, cohomologie rigide, pentes. — 14M20, 14J45, 14G15, 14G05, 14H30, 14Cxx ,14F30.
Exposé n° 915. — Théorie des ensembles, hypothèse du continu, forcing, axiome de grand cardinal. — 03Exx.
Exposé n° 916. — Théorie géométrique des groupes, groupes hyperboliques, marches aléatoires, petite simplification. — 20F65, 20P05.
Exposé n° 917. — Primalité, sommes de Jacobi, courbes elliptiques, courbes hyperelliptiques, multiplication complexe, corps finis. — 11A41, 11Y11, 11Y16.
Exposé n° 918. — Systèmes hyperboliques, méthode de viscosité. — 35F20, 35F25, 35B25, 35B35.
Exposé n° 919. — Courbe elliptique, fonction L p-adique. — 11-02, 11F11, 11F67, 11F80, 11F85, 11G05, 11G16, 11G40, 11R33, 11R39, 11R56, 11S80, 11S99, 14F30, 14F42, 14G10, 14G35, 14G40.
Exposé n° 920. — Nombres de Betti L^2, feuilletage, facteur de type II_1, groupe fondamental d'un facteur de type II_1. — 46L35, 57R30.
Exposé n° 921. — Amibes de variétés algébriques, amibes non archimédiennes, géométrie tropicale, invariants de Gromov-Witten. — 14P25, 14N10, 32A60, 32Q55, 14N35.
Exposé n° 922. — Formule du premier ordre, théorie élémentaire, problème de Tarski, groupe libre, groupe limite, action de groupe sur les arbres. — 03C60, 20E05, 20E08.
Exposé n° 923. — Groupe de Galois absolu, corps de fonctions, géométrie anabélienne. — 12F10, 14E20, 14H25, 14J20.

SÉMINAIRE BOURBAKI
VOLUME 2002/2003
EXPOSÉS 909-923

***Résumé.* —** Comme les précédents volumes de ce séminaire, celui-ci contient quinze exposés de synthèse sur des sujets d'actualité : trois exposés de théorie des nombres, deux sur les équations aux dérivées partielles, trois sur la théorie des groupes, un sur les polyèdres, un sur la cohomologie p-adique, un sur la théorie des ensembles, un sur la conjecture de Birch et Swinnerton-Dyer, un sur les nombres de Betti L^2 et facteurs de type II_1, un de géométrie algébrique, un sur les groupes de Galois des corps de type fini.

***Abstract* (Séminaire Bourbaki, volume 2002/2003, exposés 909-923)**

As in the preceding volumes of this seminar, one finds here fifteen survey lectures on topics of current interest: three lectures on number theory, two on partial differential equations, three on group theory, one on polyedras, one on p-adic cohomology, one on set theory, one on the Birch and Swinnerton-Dyer conjecture, one on L^2 Betti numbers and type II_1 factors, one on algebraic geometry, one on Galois groups of fields of finite type.

© Astérisque 294, SMF 2004

Résumés des exposés vii

NOVEMBRE 2002

909 Yuri F. BILU — *Catalan's conjecture [after Mihăilescu]* 1

910 Stéphane FISCHLER — *Irrationalité de valeurs de zêta [d'après Apéry, Rivoal,...]* 27

911 Guy MÉTIVIER — *Exemples d'instabilités pour des équations d'ondes non linéaires [d'après G. Lebeau]* 63

912 Jean-Marc SCHLENKER — *La conjecture des soufflets [d'après I. Sabitov]* 77

913 Alain VALETTE — *Nouvelles approches de la propriété (T) de Kazhdan* 97

MARS 2003

914 Antoine CHAMBERT-LOIR — *Points rationnels et groupes fondamentaux : applications de la cohomologie p-adique [d'après P. Berthelot, T. Ekedahl, H. Esnault, etc.]* 125

915 Patrick DEHORNOY — *Progrès récents sur l'hypothèse du continu [d'après Woodin]* 147

916 Étienne GHYS — *Groupes aléatoires [d'après Misha Gromov,...]* 173

917 François MORAIN — *La primalité en temps polynomial [d'après Adleman, Huang ; Agrawal, Kayal, Saxena]* 205

918 Frédéric ROUSSET — *Systèmes hyperboliques et viscosité évanescente [d'après S. Bianchini et A. Bressan]* 231

JUIN 2003

919 Pierre COLMEZ — *La conjecture de Birch et Swinnerton-Dyer* $\mathbf{p}$*-adique* 251

920 Alain CONNES — *Nombres de Betti* L^2 *et facteurs de type* II_1 *[d'après D. Gaboriau et S. Popa]* 321

921 Ilia ITENBERG — *Amibes de variétés algébriques et dénombrement de courbes [d'après G. Mikhalkin]* 335

922 Frédéric PAULIN — *Sur la théorie élémentaire des groupes libres [d'après Sela]* 363

923 Tamás SZAMUELY — *Groupes de Galois de corps de type fini [d'après Pop]* 403

Table par noms d'auteurs 433

Yuri F. BILU – *Catalan's conjecture* [*after Mihăilescu*]

The subject of the talk is the recent work of Mihăilescu, who proved that the equation $x^p - y^q = 1$ has no solutions in non-zero integers x, y and odd primes p, q. Together with the results of Lebesgue (1850) and Ko Chao (1865) this implies the celebrated *conjecture of Catalan (1843)*: *the only solution to* $x^u - y^v = 1$ *in integers* $x, y > 0$ *and* $u, v > 1$ *is* $3^2 - 2^3 = 1$.

Before the work of Mihăilescu the most definitive result on Catalan's problem was due to Tijdeman (1976), who proved that the solutions of Catalan's equation are bounded by an absolute effective constant.

Stéphane FISCHLER – *Irrationalité de valeurs de zêta* [*d'après Apéry, Rivoal,...*]

Les valeurs aux entiers pairs (strictement positifs) de la fonction ζ de Riemann sont transcendantes, car ce sont des multiples rationnels de puissances de π. En revanche, on sait très peu de choses sur la nature arithmétique des $\zeta(2k+1)$, pour $k \geqslant 1$ entier. Apéry a démontré en 1978 que $\zeta(3)$ est irrationnel. Rivoal a prouvé en 2000 qu'une infinité de $\zeta(2k+1)$ sont irrationnels, mais sans pouvoir en exhiber aucun autre que $\zeta(3)$. Il existe plusieurs points de vue sur la preuve d'Apéry ; celui des séries hypergéométriques permet d'obtenir à la fois les théorèmes d'Apéry et de Rivoal.

Guy MÉTIVIER – *Exemples d'instabilités pour des équations d'ondes non linéaires* [*d'après G. Lebeau*]

Le but de l'exposé est de donner un guide de lecture pour un article de Gilles Lebeau où il est montré que le problème de Cauchy pour l'équation d'onde surcritique $(\partial_t^2 - \Delta_x)u + u^p = 0$ est mal posé au sens de Hadamard dans l'espace d'énergie, pour $p \geqslant 7$ en dimension 3. La preuve repose sur des constructions d'optique géométrique et des analyses d'instabilité dans des régimes fortement non linéaires. On donnera les étapes de l'analyse en essayant de les situer dans leur contexte plus général : construction de solutions asymptotiques où équations eikonales et équations d'amplitudes sont liées, mécanismes d'instabilité linéaires et non linéaires par résonances et interactions.

Jean-Marc SCHLENKER – *La conjecture des soufflets* [*d'après I. Sabitov*]

On sait depuis les travaux de Bricard et de Connelly qu'il existe dans l'espace euclidien des polyèdres (non convexes) qui sont flexibles : on peut les déformer continûment sans changer la forme de leurs faces. La conjecture des soufflets affirme que le volume interieur de ces polyèdres est constant au cours de la déformation. Elle a été démontrée récemment par I. Sabitov, qui a pour cela utilisé des outils algébriques inattendus dans ce contexte.

Alain VALETTE – *Nouvelles approches de la propriété (T) de Kazhdan*

Un groupe localement compact G a la propriété (T) de Kazhdan si la 1-cohomologie de tout G-module hilbertien est nulle. Cette propriété de rigidité de la théorie des représentations de G a trouvé des applications qui vont de la théorie ergodique à la théorie des graphes. Pendant près de 30 ans, les seuls exemples connus de groupes avec la propriété (T), provenaient des groupes algébriques simples sur les corps locaux, ou de leurs réseaux. La situation a radicalement changé ces dernières années : nouvelles caractérisations (Y. Shalom), nouveaux exemples (M. Gromov, Y. Shalom, A. Zuk), de sorte qu'on peut même parler de « généricité » des groupes discrets ayant la propriété (T).

Antoine CHAMBERT-LOIR – *Points rationnels et groupes fondamentaux : applications de la cohomologie p-adique* [*d'après P. Berthelot, T. Ekedahl, H. Esnault, etc.*]

Je présenterai des résultats de T. Ekedahl et H. Esnault sur les variétés projectives lisses sur un corps de caractéristique strictement positive, disons p, dont deux points peuvent être liés par une chaîne de courbes rationnelles, par exemple faiblement unirationnelles, ou de Fano. Notamment : 1) sur un corps fini, de telles variétés ont un point rationnel, résultat qui généralise le théorème de Chevalley-Warning ; 2) sur un corps algébriquement clos, de telles variétés ont un groupe fondamental fini d'ordre premier à p ; 3) sur un corps fini de cardinal q, deux variétés propres et lisses qui sont birationnelles ont même nombre de points rationnels modulo q.
Les démonstrations utilisent la cohomologie rigide, p-adique, de P. Berthelot.

Patrick DEHORNOY – *Progrès récents sur l'hypothèse du continu* [*d'après Woodin*]

Les travaux récents de Woodin ont considérablement renouvelé la théorie des ensembles en lui apportant une intelligibilité globale et en restaurant son unité. Pour la première fois, ses résultats ouvrent une perspective réaliste de résoudre le problème du continu, et, à tout le moins, ils établissent le caractère irréfutablement signifiant et précis de celui-ci.

Étienne GHYS – *Groupes aléatoires* [*d'après Misha Gromov,...*]

Quelles sont les propriétés d'un groupe de présentation finie « tiré au hasard » ? La réponse à cette question dépend bien entendu de la méthode choisie pour le tirage au sort. On peut par exemple fixer n générateurs et choisir p relations aléatoirement parmi les mots de longueur L, puis faire tendre L vers l'infini. On peut aussi choisir un graphe fini, étiqueter aléatoirement ses arêtes par des générateurs, et considérer le groupe engendré par ces générateurs, soumis aux relations lues sur les cycles du graphe. Dans cet exposé, je voudrais présenter des travaux de M. Gromov qui permettent de répondre à ces questions et qui mettent en évidence l'existence de groupes de présentation finie aux propriétés étonnantes.

François MORAIN – *La primalité en temps polynomial* [*d'après Adleman, Huang ; Agrawal, Kayal, Saxena*]

Le problème de la primalité est l'un des problèmes les plus simples et les plus anciens de la théorie des nombres. À la fin des années 1970, Adleman, Pomerance et Rumely ont donné le premier algorithme de primalité déterministe, dont le temps de calcul était presque polynomial. Il a fallu 20 années supplémentaires pour qu'Agrawal, Kayal et Saxena donnent un algorithme déterministe de temps de calcul polynomial. L'exposé présentera ces travaux, et il fera également le point sur les différents autres algorithmes inventés dans cette période.

Frédéric ROUSSET – *Systèmes hyperboliques et viscosité évanescente* [*d'après S. Bianchini et A. Bressan*]

Le but de l'exposé est de présenter les résultats obtenus par S. Bianchini et A. Bressan sur le problème de Cauchy pour des perturbations visqueuses $\partial_t u^\varepsilon + \partial_x f(u^\varepsilon) = \varepsilon \partial_{xx} u^\varepsilon$ de systèmes strictement hyperboliques $\partial_t u + \partial_x f(u) = 0$ en une dimension d'espace. Ils ont en particulier montré l'existence globale ($t \geqslant 0$), l'unicité et la stabilité des solutions et justifié la convergence quand ε tend vers zéro pour des données initiales à petite variation totale. Leur analyse montre aussi que les solutions du système hyperbolique ainsi obtenues coïncident avec les solutions provenant d'autres types d'approximations.

Pierre COLMEZ – *La conjecture de Birch et Swinnerton-Dyer* **p** *-adique*

La conjecture de Birch et Swinnerton-Dyer prédit que l'ordre r_∞ du zéro en $s = 1$ de la fonction L d'une courbe elliptique E définie sur $\mathbf{Q}$ est égal au rang r du groupe de ses points rationnels. On sait démontrer cette conjecture si $r_\infty = 0$ ou 1, mais on n'a aucun résultat reliant r_∞ et r si $r_\infty \geqslant 2$. Nous expliquerons comment Kato démontre que la fonction L p-adique attachée à E a, en $s = 1$, un zéro d'ordre supérieur ou égal à r.

Alain CONNES – *Nombres de Betti* L^2 *et facteurs de type* II_1 [*d'après D. Gaboriau et S. Popa*]

Damien Gaboriau a montré récemment que les nombres de Betti L^2 des feuilletages mesurés à feuilles contractiles sont des invariants de la relation d'équivalence associée. Sorin Popa a utilisé ce résultat joint à des propriétés de rigidité des facteurs de type II_1 pour en déduire l'existence de facteurs de type II_1 dont le groupe fondamental est trivial.

Ilia ITENBERG – *Amibes de variétés algébriques et dénombrement de courbes* [*d'après G. Mikhalkin*]

Les *amibes* des variétés algébriques dans $(\mathbb{C}^*)^n$ sont les images de ces variétés par l'application des moments $\mathrm{Log} : (\mathbb{C}^*)^n \to \mathbb{R}^n$, $\mathrm{Log} : (z_1, \ldots, z_n) \mapsto (\log|z_1|, \ldots, \log|z_n|)$. Des résultats obtenus par G. Mikhalkin montrent l'utilité des amibes pour l'étude des variétés algébriques réelles et complexes. Les amibes peuvent être déformées en des complexes polyédraux appelés *variétés algébriques tropicales*. Cette déformation permet, en particulier, de calculer les invariants de Gromov-Witten du plan projectif et d'autres surfaces toriques en dénombrant des courbes tropicales.

Frédéric PAULIN – *Sur la théorie élémentaire des groupes libres* [*d'après Sela*]

Sela a annoncé une solution complète d'un problème de Tarski, qui demanda vers 1945 quels sont les groupes de type fini qui ont la même théorie élémentaire qu'un groupe libre. Nous discuterons des travaux de Remeslennikov, Kharlampovich-Myasnikov, Sela, Champetier-Guirardel et autres sur la structure des *groupes limites* (les groupes de type fini qui sont « limites » de groupes libres, ou encore, qui ont la même théorie universelle qu'un groupe libre). Nous indiquerons quelques outils utilisés par Sela (dont des techniques de Rips, Rips-Sela, Bestvina-Feighn et autres sur les actions de groupes sur les arbres).

Tamás SZAMUELY – *Groupes de Galois de corps de type fini* [*d'après Pop*]

Il y a quelques années, Florian Pop a démontré que tout corps de type fini sur le corps premier est déterminé à isomorphisme près par son groupe de Galois absolu (quitte à passer à une extension purement inséparable en caractéristique positive). Ce théorème, dont la généalogie remonte à des travaux de Neukirch sur les groupes de Galois de corps de nombres au début des années 1970, répond positivement à la « conjecture anabélienne birationnelle » de A. Grothendieck formulée en 1983. Dans un travail en cours, Pop étend le résultat à un corps de type fini, de dimension au moins 2, sur la *clôture algébrique* du corps premier ; le cas de dimension 2 a été également traité récemment par Bogomolov et Tschinkel. L'exposé passera en revue les résultats obtenus dans ce domaine et donnera les grandes idées des démonstrations de Pop.