

## Curriculum Vitae de Felix Ulmer

Né : mai 1961 à Ulm (R.F.A.)  
Nationalité : français et allemand  
Situation de famille : marié, 2 enfants  
Fonction actuelle : professeur des universités  
Etablissement actuel : Université de Rennes 1, UFR de Mathématiques  
Laboratoire : IRMAR, UMR 6625 du CNRS

7.1980 Baccalauréat Série C à Strasbourg

9.1980 - 5.1986 Études de Mathématiques à Universität Freiburg

6.1986 - 3.1988 Analyste systèmes, IndustrieanlagenBetriebsgesellschaft mbH (I.A.B.G.) à Ottobrunn (R.F.A.).

4.1988 - 9.1988 Chercheur, *Gesellschaft für Mathematik und Datenverarbeitung (GMD)* à Bonn.

10.1988 - 7.1991 Enseignant chercheur assistant, Département d'Informatique, Universität Karlsruhe.

7.1991 Thèse, Universität Karlsruhe, rapporteurs : J. Calmet et M.F. Singer

8.1991 - 7.1993 Visiting Assistant Professor du département de Mathématiques de North Carolina State University

8.1993-12.1993 Visiting Assistant Professor du département de Mathématiques de Cornell University.

Depuis 1.1994 Professeur, UFR de Mathématiques, Université de Rennes 1.

9.2002-8.2003 Congé CRCT. Membre du *Mathematical Science Research Institute* à Berkeley de janvier à juin 2003.

6.2007-5.2011 Directeur IRMAR (UMR 6625)

## 1 Activités administratives

- Membre élu du conseil de l'Université franco-allemande, depuis janvier 2009.
- Directeur du laboratoire IRMAR, UMR 6625 du CNRS, juin 2007- mai 2011.
- Directeur adjoint de l'UFR de Mathématiques 2006-2007.
- Membre élu du conseil d'administration de l'Université de Rennes 1 2004-2008.
- Représentant de l'IRMAR au conseil de l'école doctorale MATISSE 2004-2007.
- Membre élu du conseil de l'UFR de Mathématiques 2004-2007.
- Membre élu du conseil scientifique de l'IRMAR 2000-2004.

## 2 Encadrement doctoral

1. Olivier CORMIER a soutenu sa thèse "*Résolution des équations différentielles linéaires d'ordre 4 et 5 : application à la théorie de Galois classique*" en novembre 2001 à Rennes.
2. Axelle PERSON a soutenu sa thèse "*Solving homogeneous linear differential equations of order 4 in terms of equations of smaller order*" en juillet 2002 à Raleigh North Carolina. Co-tutelle codirigée avec M.F. Singer Axelle Faughn enseigne à *Western Carolina University in Cullowhee*.
3. Philippe GAILLARD a soutenu sa thèse "*Applications de la théorie de Galois différentielle aux équations différentielles linéaires d'ordre 4*" en novembre 2004 (début septembre 2000) à Rennes. Codirection avec M.F. Singer. Actuellement enseignant en Math. Sup. Bio à Amien.
4. Colas BARDAVID a soutenu sa thèse "*Schémas différentiels : approche géométrique et approche fonctorielle*" en juin 2010 (début septembre 2006) à Rennes. Actuellement Post-Doctoral Fellow at the *Institute of Mathematical Sciences, Chennai, Inde*
5. Lionel CHAUSSADE a soutenu sa thèse *Codes correcteurs avec les polynômes tordus* en novembre 2010 (début septembre 2007) à Rennes. Actuellement professeur en classe préparatoire MPSI au lycée Clémenceau à Nantes.

## 3 Comités scientifiques

- conférence *Mathematical Methods in Computer Science*, Karlsruhe 2008
- Journées nationales de calcul formel 2008 et 2009, CIRM, Luminy.
- *10-th Rhine Workshop on Computer Algebra* Basel 2006.
- *International Conference on Symbolic and Algebraic Computation* (ISSAC-05) Beijing, (ISSAC-96) Zürich, (ISSAC-93) Kiev.
- *International Mathematica Symposium* (IMS-03) Imperial College, (IMS-01) Tokyo, (IMS-99) Castle of Hagenberg (IMS-97) Rovaniemi (IMS-95), Southampton.

## 4 Activités de recherche/programme de recherche

Mon activité de recherche est centrée sur l'étude, théorique et algorithmique, des équations différentielles linéaires ordinaire, et, plus récemment, l'application des polynômes tordus aux codes correcteurs d'erreurs.

J'ai étudié la question de l'intégrabilité des équations différentielles linéaires et plus précisément l'existence de solutions Liouvilliennes. La méthode présentée dans [14] est une amélioration de *l'algorithme de Kovacic* pour les équations d'ordre deux. Dans [13,7] cette méthode est généralisée aux équations d'ordres arbitraires. Le résultat livre une équivalence entre les solutions Liouvilliennes et les invariants homogènes du groupe de Galois différentiel qui se factorisent comme produits de formes linéaires. Dans [11] cette équivalence est utilisée pour donner un algorithme réaliste pour le calcul des solutions d'une équation d'ordre 3. Les équations d'ordre quatre sont un cas important pour l'application du critère de non intégrabilité de systèmes Hamiltoniens de Morales-Ramis. La recherche des solutions Liouvilliennes des équations d'ordre quatre est étudié dans les thèses de mes étudiants Olivier Cormier et Philippe Gaillard.

Le groupe de Galois différentiel est un groupe algébrique linéaire qui reflète la structure algébrique d'une équation différentielle linéaire. Les articles [25] et [18] donnent des algorithmes qui permettent de déterminer la structure des groupes de Galois différentiels des équations d'ordre 2 et 3. En 1886 A. Hurwitz a construit une équation différentielle linéaire d'ordre 3 pour le groupe simple à 168 éléments. Dans [9] on étend la méthode à tous les groupes finis et on l'applique à la construction d'exemples d'équations différentielles dont le groupe de Galois est un groupe primitif fini de degré 2 et 3. La méthode est valable en fait pour tout ordre et tout groupe fini. Une fois l'équation différentielle construite, il est possible de calculer le polynôme minimal d'une solution algébrique, contribuant ainsi au problème inverse en théorie de Galois classique (en général sur  $Q(\alpha)[x]$  mais souvent sur  $Q[x]$ ). Pour la construction d'équations différentielles l'utilisation de tous les caractères fidèles est possible. Alors que l'utilisation des caractères de permutation est souvent plus difficile car de degrés très grands. La correspondance entre polynômes et équations différentielles linéaires est également exploitée dans [8] où elle est utilisée pour factoriser des polynômes de  $Q(x)[y]$  sur  $\overline{Q}(x)[y]$ , calculer leur groupe de Galois géométrique et le genre de la courbe qu'ils définissent.

En collaboration avec Frank Loray et Marius van der Put nous avons résolu de manière constructive le problème inverse pour la famille de systèmes *de Lamé* de rang deux attachés à une courbe elliptique. Dans [3] nous donnons une construction simple et efficace de telles familles à groupe de monodromie fini donné. Ces familles sont par construction isomonodromiques et il est connu, voir par exemple les travaux de Hitchin, qu'elles livrent une solution algébrique de l'équation de Painlevé P VI. L'article montre comment construire ces familles à partir d'une solution algébrique

de P VI, autrement dit à rebours de la technique usuelle de Hitchin.

Dans [5], avec D. Boucher et W. Geiselmann, nous avons introduit des codes cycliques *tordus* en utilisant des polynômes générateurs dans des anneaux (non commutatifs) de polynômes tordus sur  $\mathbb{F}_q$ , aussi appelés anneaux de Ore du type automorphisme. Pour un automorphisme  $\theta \neq \text{id}$  de  $\mathbb{F}_q$  on définit une structure d'anneau sur  $\mathbb{F}_q[X, \theta] = \{a_n X^{n-1} + \dots + a_1 X + a_0 \mid a_i \in \mathbb{F}_q \text{ et } n \in \mathbb{N}\}$ . L'addition est l'addition usuelle des polynômes et la multiplication est définie via la règle  $Xa = \theta(a)X$  ( $a \in \mathbb{F}_q$ ) qui est étendue à tout  $\mathbb{F}_q[X, \theta]$  par associativité et distributivité. Ces anneaux de polynômes sont euclidiens à droite et à gauche. Lorsque l'ordre de  $\theta$  divise  $n$ , l'idéal engendré par  $X^n - 1$  est un idéal bilatère. Les diviseurs à droite  $g \in \mathbb{F}_q[X, \theta]$  de  $X^n - 1$  engendrent alors des idéaux à gauche ( $g$ ) dans  $\mathbb{F}_q[X, \theta]/(X^n - 1)$ . L'idéal ( $g$ ) livre un sous espace vectoriel de  $(\mathbb{F}_q)^n$  et donc un code linéaire sur  $\mathbb{F}_q$  avec une structure fort riche. Nous obtenons ainsi une nouvelle classe de codes  $\theta$ -cycliques  $\mathcal{C}_\theta$  qui contient strictement la classe des codes cycliques. Ces codes sont caractérisés par la propriété suivante

$$(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}_\theta \quad \Rightarrow \quad (\theta(a_{n-1}), \theta(a_0), \theta(a_1), \dots, \theta(a_{n-2})) \in \mathcal{C}_\theta.$$

L'avantage de l'anneau non commutatif  $\mathbb{F}_q[X, \theta]$  est que la factorisation n'est pas unique à ordre et à inversibles près. Il en découle un nombre impressionnant de codes. Dans [5] de nouveaux codes ont été obtenus, dont la distance minimale améliore celle de certains meilleurs codes connus.

Dans [2] nous montrons que le dual d'un code  $\theta$ -cyclique est encore  $\theta$ -cyclique et un nouveau code [38, 19, 11] a été obtenu, dont la distance minimale améliore celle des meilleurs codes autoduaux connus. Dans [1] nous montrons comment prescrire une borne inférieure pour le rang ou la distance d'un code tordu en définissant des codes "BCH tordus". Pour imposer une distance minimale  $\delta$  on exige que le polynôme générateur  $g \in \mathbb{F}_q[X, \theta]$  soit divisible à droite par

$$(X - \alpha), (X - \alpha^2), \dots, (X - \alpha^{\delta-1}),$$

avec  $\alpha$  dans une extension de corps de  $\mathbb{F}_q$ . Ici encore la non commutativité livre un grand nombre de facteurs à droite et nous obtenons ainsi de nouveaux codes, dont la distance minimale améliore celle de certains meilleurs codes linéaires connus. Ces codes "BCH tordus" sont particulièrement intéressants, car on peut les décoder efficacement avec une version non commutative de l'algorithme de Berlekamp-Welsch.

Dans [22] nous généralisons l'approche aux codes  $Rg/Rf \subset R/Rf$  qui sont des modules sur  $R = \mathbb{F}_q[X, \theta]$ . Nous obtenons ainsi plus de codes pour les petites dimensions. A un détail technique près, le dual d'un "module code tordu" est un module code tordu si et seulement si  $g$  divise  $X^n - c$  avec  $n$  la longueur du code et  $c \in \mathbb{F}_q$ . En particulier un code auto-dual est toujours "consta-cyclique tordu".

Mon objectif est la généralisation de ces codes et l'étude de leurs propriétés.

## Travaux et publications

[http://perso.univ-rennes1.fr/felix.ulmer/fu\\_papers.html](http://perso.univ-rennes1.fr/felix.ulmer/fu_papers.html)

### 1) Articles de revues :

- [1] *Linear codes using skew polynomials with automorphisms and derivations*,  
Prépublication HAL 00597127  
À paraître dans : *Designs, Codes and Cryptography*
- [2] *Skew codes of prescribed distance or rank* (avec L. Chausade et P. Loidreau)  
*Designs, Codes and Cryptography*, vol. **50**, 267-284 (2009)
- [3] *Coding with skew polynomial rings* (avec D. Boucher)  
*Journal of Symbolic Computation*, vol. **44**, pp.1644-1656 (2009)  
Special issue on *Gröbner Bases Techniques in Cryptography and Coding Theory*
- [4] *The Lamé family of connections on the projective line*  
(avec F. Loray et M. van der Put)  
*Annales de la Faculté des Sciences de Toulouse*, vol. **17**, 371-409 (2008)
- [5] *Skew Constacyclic Codes over Galois Rings* (avec D. Boucher et P. Solé)  
*Advances in Mathematics of Communications*, vol. **2**, pp. 273-292 (2008)
- [6] *Skew Cyclic Codes* (avec D. Boucher et W. Geiselmann)  
*Appl. Algebra in Eng. Comm. and Comp.*, vol. **18** pp. 379-389 (2007)
- [7] *Note on Algebraic solutions of differential equations with known finite Galois group*  
*Appl. Algebra in Eng. Comm. and Comp.* vol. **16** , pp. 205-218 (2005)
- [8] *Liouvillian solutions of third order differential equations*  
*Journal of Symbolic Computation* vol. **36**, pp. 855-889 (2003)
- [9] *Linear Differential Operators for Polynomial Equations*  
(avec O. Cormier, M.F. Singer et B.M. Trager).  
*Journal of Symbolic Computation* , vol. **34**, pp. 355-398 (2002)
- [10] *Differential equations and finite groups* (avec M. van der Put)  
*Journal of Algebra*, vol. **226**, pp. 920-966 (2000)
- [11] *How to Solve Linear Differential Equations : An Outline.*  
*Programming and Computer Software*, vol. **26**, pp. 17-22 (2000)
- [12] *Liouvillian solutions of linear differential equations of order three and higher*  
(avec M. van Hoeij, J.F. Ragot et J.A. Weil)  
*Journal of Symbolic Computation*, vol. **28**, pp. 589-609 (1999)
- [13] *Constructing a Third Order Linear Differential Equation* (avec W. Geiselman).  
*Theoretical Computer Science*, vol. **187**, pp. 3-6 (1997)

- [14] *Linear Differential Equations and Products of Linear Forms* (avec M.F. Singer)  
J. of Pure and Applied Algebra, vol. **117-118** , pp. 353-379 (1997)
- [15] *Note on Kovacic's algorithm* (avec J.A. Weil)  
Journal of Symbolic Computation, vol. **22**, pp. 179-200 (1996)
- [16] *Necessary conditions for liouvillian solutions of (third order) linear differential equations* (avec M.F. Singer)  
Appl. Algebra in Eng. Comm. and Comp., vol. **6**, pp. 1-22 (1995)
- [17] *Irreducible linear differential equations of prime order*  
Journal of Symbolic Computation, vol. **18**, pp. 385-401 (1994)
- [18] *Liouvillian and algebraic solutions of second and third order linear differential equations* (avec M.F. Singer)  
Journal of Symbolic Computation, vol. **16**, pp. 37-73 (1993)
- [19] *Galois groups of second and third order linear differential equations*  
(avec M.F. Singer)  
Journal of Symbolic Computation, vol. **16**, pp. 1-36 (1993)
- [20] *On liouvillian solutions of linear differential equations*  
Appl. Algebra in Eng. Comm. and Comp., vol. **2**, pp. 171-193 (1992)

## 2) Articles dans des actes de conférences avec comité de lecture

- [20] *A note on the dual codes of module skew codes* (avec D. Boucher)  
Proceedings of the 13th IMA Conference of Cryptography and Coding, Oxford (2011), Lecture Notes in Computer Science, 7089, 23-243 (2011)
- [21] *Key exchange and encryption schemes based on non-commutative skew polynomials* (avec D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta), Proceedings PQCrypto, 3rd Int. Workshop on Post-Quantum Cryptography, Darmstadt, Lecture Notes in Computer Science, 6061, 126-141 (2010).
- [22] *Codes as modules over skew polynomial rings* (avec D. Boucher),  
Proceedings of IMA conference on Cryptography and Coding, Cirencester  
Springer Lectures Notes in Computer Science 5921, pp. 38-55 (2009)
- [23] *Fourth order linear differential equations with imprimitive group*, (avec D. Boucher et P. Gaillard), Proceedings ISSAC, Philadelphia  
ACM Press, pp. 45-49 (2003)
- [24] *Computing the Galois group of a polynomial using linear differential equations*,  
(avec O. Cormier et M.F. Singer). Proceedings of ISSAC, St Andrews  
ACM Press, pp. 78-85 (2000)
- [25] *On a third order linear differential equations whose differential Galois group is the simple group of 168 elements* (avec M.F. Singer),

- In : Proceedings of AAEECC, Puerto Rico  
**Springer Lectures Notes in Computer Science** 673, pp. 316-324 (1993)
- [26] *Liouvillian solutions of third order linear differential equations : New bounds and necessary conditions* (avec M.F. Singer), Proceedings ISSAC Berkeley  
**ACM Press**, pp. 57-62 (1992)
- [27] *On algebraic solutions of linear differential equations with primitive unimodular Galois group*, In : Proceedings of AAEECC-9, New Orleans  
**Springer Lectures Notes in Computer Science** 539, pp. 446-455 (1991)
- [28] *On liouvillian solutions of homogeneous linear differential equations* (avec J. Calmet), In : Proceedings of ISSAC, Tokyo 1990  
**ACM Press**, pp. 236-243 (1990)

### 3) Chapitres de livres, autres

- [27] *Some methods to solve linear differential equations in closed form* (avec J.A. Weil), à paraître dans les actes de **Algebraic Theory of Differential Equations**, Edinburgh 2006, éditeurs : M. MacCallum et A.V. Mikhailov  
**London Mathematical Society Lecture Note Series**, No. 357 (2008)
- [28] *Fehler korrigierende Codes*  
 Computeralgebra Rundbrief GI-DMV-GAMM, April, 32-34 (2008)  
 Sonderheft zum Jahr der Mathematik 2008
- [29] *Note on Kovacic's algorithm* (avec J.A. Weil),  
**ACM SIGSAM Bulletin**, Volume 29 , Issue 2, 10-11 (April 1995)
- [30] *Entwurf von Algorithmen zur Berechnung Liouvillescher Lösungen von linearen gewöhnlichen Differentialgleichungen*, Thèse Universität Karlsruhe 1991,  
 Verlag Dr. Kovac, Hamburg 1991, ISBN 3-925630-93-7

## 5 Communications séminaires/congrès, invitations

- *SAGE Days 24*, Linz, july 2010
- *Algebraic Methods in Dynamical Systems* Bedlewo, Mai 2010
- *12th IMA International Conference on Cryptography and Coding*, Cirencester, décembre 2009
- *Noncommutative rings and their applications*, Lens, juillet 2009.
- AMS Meeting, Raleigh, avril 2009.
- *Colloquium*, Angers, mars 2008
- *Journées "Codage et Cryptographie"*, Carcans, mars 2008.
- *Journées 2007 de l'ANR GECKO*, Nice, novembre 2007.
- *Colloquium*, Erlangen, juin 2007
- *Journées annuelles "calcul formel" de la DMV*, Kaiserslautern, mai 2007
- "Mariusfest" - "Intercity Seminar", Groningen, avril 2007
- IRISA de Rennes, *Séminaire 68NQRT*, octobre 2006.
- *Journées "Codage et Cryptographie"*, Eymoutiers, octobre 2006.
- *Algebraic Theory of Differential Equations*, Edinburgh, août 2006
- *Colloque en mémoire de Manuel Bronstein*, Nice, juillet 2006
- Université de Paris 6, *exposé au groupe de travail*, avril 2006
- Université de Nice, *séminaire*, avril 2006
- *Journées Calcul Formel*, CIRM luminy, novembre 2005
- FoCM 2005 conference in Santander, Spain, juillet 2005
- Université de Strasbourg, *séminaire*, février 2005
- Intercity Number Theory Seminar, Université Groningen, octobre 2004
- Université Nanjin, *séminaire*, Septembre 2004
- *Kolchin Seminar in Differential Algebra*, Hunter College New York, déc. 2003
- *Galois Theory and Differential Equations*, Oberflockenbach, octobre 2003
- Colloquium, San Diego State University, mai 2003
- Computational Algebra Seminar, University of Berkeley, mars 2003
- Invité pour 5 mois au Mathematical Science Research Institute, 2003
- Colloque Mathématiques Effectives, Poitiers, septembre 2002
- Invité pour un mois au Mathematical Science Research Institute, mars 2002
- INRIA Sophia Antipolis, *séminaire*, juin 2001
- Conférence *Differential Galois Theory*, Banach Center, Bedlewo, mai 2001
- Invité pour une semaine à *Université de Torun*, janvier 2001
- AMS Meeting, Columbia University, novembre, 2000
- Université de Graz, *séminaire*, juin 2000
- Journées "Équations différentielles et calcul formel" à Lille, Mars 2000
- Université de Haute Bretagne à Brest, *séminaire*, février 2000
- Invité un mois à *North Carolina State University*, janvier 2000