

# Rapport scientifique sur l'Ecole du CIMPA Géométrie Algébrique et Applications

Robert Rolland

5 janvier 2001

## 1 Généralités, Organisation

L'école du CIMPA intitulée "**Géométrie Algébrique et Applications aux Codes Correcteurs et à la Cryptographie**" a eu lieu à la Havane du 20 Novembre 2000 au 1<sup>er</sup> Décembre 2000.

Les Directeurs scientifiques étaient Jorge Estrada Sarlabous (ICIMAF, Cuba) et Robert Rolland (IML, France).

L'organisation locale confiée à l'ICIMAF et à l'Université de la Havane était sous la direction de Jorge Estrada Sarlabous.

Le CIMPA était représenté par Richard Grin.

L'organisation locale a été parfaite et a permis l'accueil des participants et leur travail dans des conditions optimales. Nos partenaires cubains, professeurs, étudiants, administratifs ont montré qu'ils étaient très intéressés par cette coopération avec le CIMPA. De ce point de vue, je pense que cette expérience peut inciter le CIMPA à organiser d'autres écoles à Cuba.

## 2 Les enseignements

Ainsi cette école s'est déroulée sur deux semaines. Huit enseignants sont intervenus. Chacun a disposé de quatre plages de 1H30 réparties sur une semaine (soit 6 heures de cours chacun). Quatre participants à l'école ont

exposé leurs travaux. En outre il était très facile d'avoir des conversations scientifiques avant ou après les cours. Ceci a été grandement facilité par le fait que les enseignants étaient présents dans une large mesure aux cours de leurs collègues et donc se trouvaient fréquemment sur le site de l'école.

Voici la liste des cours (par ordre chronologique) qui ont eu lieu :

Joseph Oesterlé : Lattices and Sphere packing

Rolf-Peter Holzapfel : Algebraic Geometry over Algebraically Closed Fields

Jorge Estada Sarlabous : Introduction to Cryptography

Pierre Barthelemy : Networks Security

Gilles Lachaud : Algebraic Geometry over Finite Fields

Robert Rolland : Linear Block Coding Theory

Jean-Pierre Cherdieu : Zeta functions and curves over finite fields

Ernesto Reinaldo Barreiro : Elliptic Cryptography, jacobians of curves and cryptography

Voici la liste des exposés des participants :

José de Jesús Angel Angel : Description de algoritmos criptograficos

Miriam Abdon : A Characterization of Certain Maximal Curves

Luciane Quoos : A Construction of Curves over Finite Fields

Nicolae Florin : On the Zeta Function of a Family of Picard Curves

### **3 Les participants**

Nous avons eu 22 participants répartis par pays de la façon suivante

Cuba (6) Mexique (5) Brésil (2) Argentine (1) Costa Rica (1) Chine (1) Italie (3) Algérie (1) Roumanie (2)

Le niveau était élevé, de nombreux participants ayant déjà leur PhD, d'autres étant sur le point de le soutenir.

### **4 Dérroulement des cours**

Nous avons dans notre enseignement choisi de montrer notre domaine sous ses aspects les plus théoriques jusqu'à ses parties les plus concrètes et les plus appliquées.

Il me semble important de montrer l'extrême intérêt de la pensée abstraite dans le développement scientifique et technologique. Les recherches abstraites

actuelles sont les bases d'applications d'aujourd'hui, de demain ou d'après demain. Ce point de vue n'est pas toujours facile à soutenir vis à vis des entreprises ou des décideurs politiques, même dans les pays riches, qui bénéficient pourtant sans bien souvent s'en rendre compte des résultats abstraits des générations antérieures. Il est encore plus difficile à soutenir dans les pays qui ont des difficultés économiques. Aussi est-il important d'aider les jeunes chercheurs qui ont choisi cette direction.

## **5 Les contacts pris et le suivi**

Nous avons été reçus par le service culturel de l'Ambassade de France. En ce qui concerne le suivi de cette école il nous a été conseillé de prendre contact avec Alcatel, entreprise française bien implantée à Cuba, ce que nous avons fait. Nous allons essayer avec le soutien d'Alcatel et d'entreprises cubaines d'organiser un Workshop sur le thème de cette école. D'autre part nous ferons une demande de bourses pour des participants qui s'orientent dans ce secteur. Nous gardons le contact avec les jeunes chercheurs qui veulent travailler dans ce domaine. Ainsi une des participantes doit faire une conférence au séminaire de l'équipe ATI de l'Institut de Mathématiques de Luminy. Deux d'entre eux sont invités pour un exposé dans le cadre du colloque AGCT 8 qui aura lieu au CIRM au mois de Mai 2001. Pour ceux qui sont moins avancés nous gardons un contact par e-mail pour répondre à leurs questions.

Une ou plusieurs pages web consacrées à cette école seront bientôt mises en place. On y trouvera en particulier tous les cours.