Cuso Graduate Colloquium, Fribourg, 15-16 September 2016

Abstracts of the talks

Optimal representations for trace-zero subgroups
Giulia Bianco *(Université de Neuchâtel)*
Abstract: Trace-zero subgroups are particular groups arising from elliptic curves defined over a finite field $\mathbb{F}_q$. Such groups turn out to have relevant applications to cryptography. Led by this motivation, one is interested in finding optimal representations for them, that is, to represent their elements with the smallest possible number of $\mathbb{F}_q$-coordinates, in order to save data space. In our talk, we first give an overview on trace-zero subgroups and optimal representations. Then we describe a specific optimal representation for trace-zero subgroups proposed by M. Massierer and E. Gorla. In the end, we present our contribution in this field: exploiting the representation cited before, we construct an efficient algorithm to compute the scalar product in trace-zero subgroups.

Topology and dynamics
Lucas Dahinden *(Université de Neuchâtel)*
Abstract: Often it is nice to know how "complicated" a mechanical system is. I will outline how algebraic topology helps to give lower bounds to the complexity of Hamiltonian dynamics in the cotangent bundle.

Lattices and box spaces
Thiebout Delabie *(Université de Neuchâtel)*
Abstract: In geometric group theory, we can look at quotients of groups and try to deduce properties of the group. A lot of these properties can be deduced from the large scale geometry of "box spaces", that are metric spaces created using these quotients. It is therefore interesting to see what box spaces have the same large scale structure. We will look at one of these results and reduce it to a result in euclidean geometry.

Quantum Ising model and conformal invariance
Jhih-Huang Li *(Université de Genève)*
Abstract: In this talk, we will study the quantum Ising model via its geometric representation, the so-called FK-representation. Then, a short introduction towards the conformal invariance will be given, which is an important notion for planar models in statistical physics. In the end, we will briefly discuss the conformal invariance of our model by looking at its interface.

On the Landau-Lifshitz-Gilbert equation
Jonathan Rochat *(École Polythecnique Fédérale de Lausanne)*
Abstract: The Landau-Lifshitz-Gilbert Equation describes the dynamics of ferromagnetism, where strong non-linearity and non-convexity are hard to tackle. This equation is commonly used in micromagnetics to model the effects of a magnetic field on ferromagnetic materials. We present in this talk a fully implicit finite element scheme to solve this problem and some numerical examples.

Towards hyperelliptic curve cryptography
Marius Vuille *(École Polythecnique Fédérale de Lausanne)*
Abstract: Nowadays communication strongly relies on the use of efficient and secure cryptosystems. In this talk, I will present the idea of public key cryptography, together with its most commonly used cryptosystems such as RSA, Diffie-Hellman

and El Gamal. In a second part I will explain the role of elliptic curves for establishing the discrete logarithm problem (DLP), and then its natural generalisation to higher genus curves, which leads to my research topic, the efficient computation of isogenies in genus 3.

Algebraic Duistermaat-Heckman phenomena
Dimitri Wyss *(École Polythecnique Fédérale de Lausanne)*
Abstract: Given a nice action of a compact Lie group G on a compact symplectic manifold M, the Duistermaat-Heckman theorem expresses the natural (Liouville) volume of the symplectic reduction M/G in terms of local data around the fixed points of the action of G on M. Using explicit examples I will explain how to obtain similar formulas for algebraic varieties over finite fields, even though there is no general DH theorem in this context.

Abstract of the colloquium

From puzzles to moduli spaces
Hugo Parlier *(Université de Fribourg)*
Abstract: How do you measure distance between shapes? What is the distance between different Rubik's cubes? How many ways can you cover a chess board with dominos? The talk will be about finding and exploring geometry in unexpected places and how puzzles illustrate more sophisticated mathematical objects such as moduli spaces.