UNIVERSITÀ DI TRENTO
Dipartimento di Matematica

DOTTORATO

CYCLES 35 AND 36TH
SEMINARS THIRD YEAR

ADMISSION TO THE FINAL EXAMINATION - PHD PROGRAMME IN MATHEMATICS

Seminar Room of Department of Physics

The final exam seminar will take place in presence and online

Thursday 18th January 2024

10:30 Michele Battagliola - Algebraic constructions for multi party protocols with focus on threshold signatures

Abstract: Group actions are fundamental mathematical tools, with a long history of use in cryptography. Indeed, the action of finite groups at the basis of the discrete logarithm problem is behind a very large portion of modern cryptographic systems. With the advent of post-quantum cryptography, however, other group actions, like isogeny or code based ones, received interest from the cryptographic community, attracted by the possibility of translating old discrete logarithm based functionalities. In this talk we show that isomorphism problems which stem from (non-abelian) cryptographic group actions can be viable building blocks for threshold signature schemes. Moreover we show how cryptographic group actions can be used to design other multi party protocols, such as oblivious transfers.

Supervisor: Nadir Murru

10:50 Marzio Mula - Pairings and graphs of elliptic curves

Abstract: The recent attacks on the isogeny-based protocol SIDH have raised the question of whether other isogeny-based protocols, such as CSIDH, are still secure. After introducing CSIDH and its variants, we describe a strategy, based on the construction of suitable pairings, which can be combined with the SIDH attack to break some "weak" variants of CSIDH.
In the last part of the talk, we turn to graphs of elliptic curves that are not the classic isogeny graphs used in SIDH or CSIDH. We call them Hessian graphs, as they arise from the notion of Hessian variety, and we show how their regularity can also be relevant in the light of cryptographic applications.

Supervisors: Nadir Murru, Federico Pintore

11:10 Giulio Binosi - Fueter and Almansi theorems for slice regular functions of several quaternionic variables

Abstract: We broaden some definitions and give new results about the theory of slice functions of several quaternionic variables. We introduce the notions of partial spherical value and derivative for functions of several variables that extend those of one variable, recovering some of their properties and discovering new ones. This leads to a generalization of Fueter’s theorem for slice regular functions of several quaternionic variables. Furthermore, partial spherical derivatives can be use to obtain different Almansi de compositions for slice functions of several variables. The components of each decomposition, defined explicitly through partial spherical derivatives, exhibit desirable properties, such as harmonicity and circularity. As consequences of these decompositions, we give another proof of Fueter’s theorem in H^n , establish the biharmonicity of slice regular functions in every variable and, time permitting, derive some integral formulas for them.

Supervisor: Alessandro Perotti

11:30 Gloria Tabarelli - Edge-colorings and flows in Class 2 graphs

Abstract: We consider edge-colorings and flows problems in Graph Theory that are hard to solve for Class 2 graphs. Most of them are strongly related to some outstanding open conjectures, such as the Cycle Double Cover Conjecture, the Berge-Fulkerson Conjecture, the Petersen Coloring Conjecture and the Tutte’s 5-flow Conjecture. We obtain some new restrictions on the structure of a possible minimum counterexample to the former two conjectures. We prove that the Petersen graph is, in a specific sense, the only graph that could appear in the Petersen Coloring Conjecture, and we provide evidence that led to propose ananalogous of the Tutte’s 5-flow conjecture in higher dimensions.

Supervisors: Giuseppe Mazzuoccolo (Università di Verona), Peter Michael Schuster (Università di Verona)

***Contact person**: Luigi Amedeo Bianchi*

CONTATTI
Staff di Dipartimento - Matematica
tel. 0461 281508-1625-1701-3786
phd.maths@unitn.it
www.unitn.it/drmath