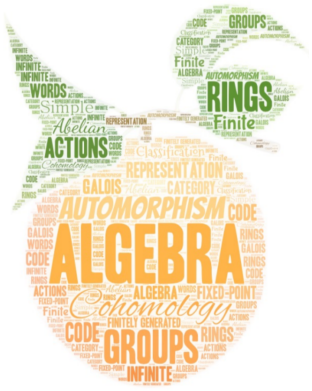
Al@Bicocca seminar

You are all welcome to the next bite of the series

“Al@Bicocca”

which is meant to give you a small taste of the Algebra at Bicocca and beyond



25 May 2026
15.00 (CEST)

Sandro Mattarei
Università degli Studi di Milano–Bicocca

Additive subgroups and inversion in finite fields

Abstract: The inversion map in a finite field plays a role in various cryptographic algorithms, one reason being its “high nonlinearity”. The set of inverses of the nonzero elements of an additive subgroup of a finite field might be expected to be a “highly nonlinear” subset, aside from trivial cases. In this talk I will provide concrete expressions to this expectation, in the form of certain bounds. Some interesting geometric configurations arise as exceptional cases.

Online venue: Webex
University of Milano-Bicocca
Viale dell’Innovazione, 10
Edificio U9
Milano (IT)
Aula U9-01

Organizers:
Jessica Anzanello
Julian Feuerpfeil
Marco Barbieri
Simone Blumer
Nicola Grittini
Francesco Matucci

Website