Unsolvability of the Quintic Formalized in Dependent Type Theory

Sophie Bernard[1], Cyril Cohen*[2], Assia Mahboubi[3,4], and Pierre-Yves Strub[5]

[1]Université Côte d'Azur – INRIA – France
[2]Université Côte d'Azur – INRIA – France
[3]Gallinette Project Team – INRIA – France
[4]Vrije Universiteit, Amsterdam – Pays-Bas
[5]LIX – Ecole Polytechnique – France

Résumé

In this talk, we describe an axiom-free Coq formalization that there does not exists a general method for solving by radicals polynomial equations of degree greater than 4. This development includes a proof of Galois' Theorem of the equivalence between solvable extensions and extensions solvable by radicals. The unsolvability of the general quintic follows from applying this theorem to a well chosen polynomial with unsolvable Galois group.

*Intervenant