A Formal Proof in Algebra: The Fundamental Theorem of Galois Theory

Sean McLaughlin
Carnegie Mellon University
School of Computer Science

March 25, 2007

Abstract
Proofs in mathematics and computer science are growing increasingly complex and difficult to understand and verify. Examples include large and complex proofs such as the Classification of Finite Simple Groups, and proofs that do extensive computer calculations such as the Appel-Haken proof of the Four Color Theorem and Hales’ proof of the Kepler Conjecture.

In response to an increasing desire for more rigorous methods of ensuring correctness, a number of computer programs called proof assistants have been designed with the sole purpose of building and checking mathematical proofs. By trusting a small base of code implementing a logic, one can have a very high degree of confidence in the correctness of results.

While many interesting and important theorems have been proved with these programs, abstract algebra is one area where relatively little progress has been made. To attempt to bridge this gap, we propose to formalize a proof of the Fundamental Theorem of Galois Theory in the Coq proof assistant.

1 Introduction
The foundations of mathematics has been an active area of research for at least the last century. Mathematicians such as Hilbert, Cantor, Frege and Russell helped form a rigorous basis for mathematical reasoning using mathematical logic. By its very nature, however, formal proof in the logical sense has always differed from the way mathematicians actually think and write about mathematics. The reason being that writing a proof in full detail from the axioms of a foundation such as set theory would be a practical impossibility. For example, it takes over 1000 pages in Russell and Whitehead’s Principia Mathematica to prove that $1 + 1 = 2$. Proofs in mathematics are thus considered to be approximations to a formal proof.

But the advent of computers make the creation and checking of proof in the style of Russell a possibility. Indeed, proof assistants such as Coq[8], Isabelle[7]
and HOL Light[6] have successfully verified a number of important mathematical results. These include the Four Color Theorem[4], the Jordan Curve Theorem[5], and the Prime Number Theorem[2].

One major area of mathematics that has received relatively little formal attention until recently is that of abstract algebra. In 2006, Georges Gonthier began a project to prove the Feit-Thompson theorem[3] of group theory in Coq. One theorem needed for that proof is the elegant Fundamental Theorem of Galois Theory[1]. I propose to formalize this theorem in the Coq proof assistant.

## 2 Galois Theory

In 1824, Niels Abel showed that, unlike the familiar case for quadratic equations, there can be no general solution to the polynomial equation

\[ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \]

if \( n \geq 5 \). In 1832, at the age of 20, Évariste Galois gave an explanation for the unsolvability of the quintic in very general terms in a letter to his friend Auguste Chevalier. The famous mathematician Hermann Weyl writes "This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind."\(^1\)

In modern mathematical language, the content of the work, now known as Galois Theory, gives a relation between field extensions and groups of field automorphisms. The fundamental theorem formalizes this relation (from Milne[11]).

**Theorem (Fundamental Theorem of Galois Theory)** Let \( E \) be a Galois extension of a field \( F \), and let \( G = \text{Gal}(E/F) \) be the Galois group of \( E \) over \( F \). The maps \( H \mapsto E^H \) and \( M \mapsto \text{Gal}(E/M) \) are inverse bijections between the set of subgroups of \( G \) and the set of intermediate fields between \( E \) and \( F \). Moreover

(a) the correspondence is inclusion reversing \( H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2} \)

(b) indexes equal degrees \( (H_1 : H_2) = [E^{H_2} : E^{H_1}] \)

(c) Given an automorphism \( \sigma \) in \( G \), \( E^{\sigma H \sigma^{-1}} = \sigma(E^H) \) and \( \text{Gal}(E/\sigma M) = \sigma \text{Gal}(E/M) \sigma^{-1} \).

(d) \( H \) is normal in \( G \) \( \iff \) \( E^H \) is normal over \( F \) in which case

\[ \text{Gal}(E^H/F) = G/H. \]

While it may seem complicated at first glance, Milne's lecture notes[11] go from the definition of a field to a complete proof of the theorem in 33 pages. The importance of the result, coupled with its relatively elementary nature, make it an attractive target for formalization. Moreover, the theorem will be needed

\(^{1}\text{Galois was killed the following day in a duel.}\)
in Gonthier’s proof of the Feit-Thompson theorem, thus making its completion of interest to the greater formalized mathematics community. In turn, a Coq formalization of the Feit-Thompson theorem, being a major part of the Classification of Finite Simple Groups, probably the longest and most complicated proof in existence, would be of interest to all mathematicians. This project would be a small contribution to that effort.

3 Project Time-line

While in my experience it is difficult to foresee the challenges that arise in doing a formal proof, here is a rough time-line of my ideal progress.

May 28th Project begins. Formalize properties of polynomials, ring structure.

June 15th Properties of fields, field extensions, algebraic elements.

July 9th Mid-term evaluations. Begin splitting field construction,

August 1st Field automorphisms, definition of the Galois group.

August 20th Begin the proof of the Fundamental Theorem

August 31st Project ends.

4 Author’s Background

I am a third year PhD student at Carnegie Mellon University in Pittsburgh, PA. My advisor is Frank Pfenning. My undergraduate degree is in mathematics from the University of Michigan, where I took a number of abstract algebra courses. I have a good amount of experience with formalizing mathematics with proof assistants. Probably my biggest project was implementing a proof producing extension of HOL Light to do quantifier elimination over the reals[10]. Last year I implemented a translation of Isabelle terms and theorems (in SML) to Ocaml functors[9] for use in HOL-Light. More recently I’m designing a system to share first order decision procedures between different theorem provers using the Ocaml module system.

In the summer of 2006 I had an internship with Georges Gonthier, the author of the Coq proof of the Four Color Theorem, where I worked on his project to formalize the Feit-Thompson theorem in Coq. Last semester I continued to use Coq to formalize semantics of programming languages in the logic programming course taught by Frank Pfenning at CMU. I thus feel I have a solid foundation both in algebra and formalized mathematics which makes me a strong candidate for the proposed project.

References:
References


