Unsolvability of the Quintic Formalized in Dependent Type Theory

Sophie Bernard, Cyril Cohen, Assia Mahboubi, Pierre-Yves Strub

Unsolvability of the Quintic Formalized in Dependent Type Theory

Sophie Bernard
Université Côte d'Azur, Inria, France

Cyril Cohen
Université Côte d'Azur, Inria, France

Assia Mahboubi
Inria, France
Vrije Universiteit Amsterdam, The Netherlands

Pierre-Yves Strub
École polytechnique, France

Abstract

In this paper, 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.

2012 ACM Subject Classification Theory of computation → Type theory; Theory of computation → Logic and verification; Theory of computation → Constructive mathematics

Keywords and phrases Galois theory, Coq, Mathematical Components, Dependent Type Theory, Abel-Ruffini, General quintic

Digital Object Identifier 10.4230/LIPIcs.ITP.2021.3

Supplementary Material `https://github.com/math-comp/Abel` version 1.1.2.

1 Introduction

This article presents a formal study of the existence of solutions by radicals of polynomial equations. Solutions by radicals are the ones that can be expressed from the coefficients of a polynomial using operations of addition, multiplication, subtraction, division, and extraction of roots. More precisely we study the case of polynomial equations of degree greater than 4. As opposed to the case of lower degree, there is no solution by radicals to general polynomial equations of degree five or higher with arbitrary coefficients. This theorem, also known as the Abel-Ruffini theorem, is attributed to Abel for his work [14, volume 1, chapter III] published in 1826. Ruffini is credited for a first formulation and proof [21] from 1799. Abel writes about Ruffini: "[...]; but his memoir is so complicated that it is very hard to assess the correctness of his reasoning. It seems to me that his reasoning is not always satisfactory." [14, volume 2, chapter XVIII]

In fact, we developed a formal proof of the more general theorem – attributed to Galois [8] in his memoir from 1830 – which provides an explicit necessary and sufficient condition for the existence of solutions by radical, and we also formalize an example of non-solvable quintic, obtained as a corollary of the latter. This Galois theorem is an emblematic result of Galois theory, which studies field extensions of commutative fields via a correspondence with groups of permutations of roots of polynomials.

This formalization endeavor builds on an existing library covering elementary results in Galois theory, developed by Georges Gonthier and Russell O'Connor in the Mathematical

Components library [25], for the purpose of the formal proof of the Odd Order theorem [11]. As there is no published description of this material, we provide where needed a description of the material from this contribution that we rely on.

The formalized proof is constructive, and relies on nothing but the axioms and rules of the foundational framework implemented by Coq. The code of this formalization is available on `https://github.com/math-comp/Abel` version 1.1.2. Every numbered definition, lemma or theorem in this paper is our contribution, and we hyperlinked red underlined definitions.

2 Background and outline

Throughout this section, we consider a field K of characteristic 0 and a polynomial $P \in K[X]$. We study the solvability by radicals of the equation $P(X) = 0$, also termed the solvability by radicals of P. An easy case is when all the roots of P are in K, i.e., when F *splits* P. In the general case, the idea is to consider successive *field extensions* F over K, i.e., fields F such that $K \subset F$. These extensions are built so as to gradually encompass all the roots of P.

In the rest of the paper, we write F/K to denote that F is a field extension over K. Given such an extension, the larger field F is a K-vector space and we can consider its dimension – called the *degree of the extension* and written $[F : K]$. A field extension is said to be *finite* when its degree is finite. In the present paper, all the field extensions under consideration are finite and we sometimes simply refer to them as "field extensions". If $x_0, \ldots, x_n$ are elements of F, we denote by $K(x_1, \ldots, x_n)$ the smallest field which contains K and x_i for all $i \leq n$. Note that both $K(x_1, \ldots, x_n)/K$ and $F/K(x_1, \ldots, x_n)$ are field extensions. The *splitting field* of $P \in F[X]$ is the smallest field extension of F which splits P.

Let F/K be a field extension. An element x of F is said to be *algebraic over* K if it is a root of some nonzero polynomial with coefficients in K. The field extension F/K is called *algebraic* when all its elements are algebraic over K. Moreover if F is a splitting field for some polynomial in $K[X]$, the extension F/K is said to be *normal*. Last, the *minimal polynomial* of an element x of F is the monic polynomial of minimal degree among all the nonzero polynomials with coefficients in K and having x as a root.

▶ **Definition 1** (radical, solvable by radicals)**.** *Let F/K be a field extension. F/K is called a* simple radical extension *if there exists $x \in F$ and a positive integer $n \in \mathbb{N}^*$ such that $x^n \in K$ and $F = K(x)$. A* radical series *is a tower $F_0 \subset \cdots \subset F_n$ where F_k/F_{k-1} is a simple radical extension for $k \in \{1, \ldots, n\}$. A field extension F/K is a* radical extension *if there is a radical series $K = F_0 \subset \cdots \subset F_n = F$. It is a* solvable by radicals extension *if there is a radical extension E/K such that $F \subset E$.*

A polynomial $P \in K[X]$ is solvable by radicals *if it splits in a radical extension of K.*

The crux of the method is, given a splitting field F of a polynomial P over K, to study the field automorphisms of F that fix K point-wise, thereby permuting the roots P.

More generally, given a field (finite) extension F/K, the set of automorphisms of F that fix K point-wise is always a group. We call it $\mathrm{Gal}(F/K)$, the *Galois group* of the extension F/K. Moreover, if $\mathrm{Gal}(F/K)$ fixes *exactly* K, the extension F/K is then said to be a *Galois extension*. In this case, the order of the Galois group $\mathrm{Gal}(F/K)$ is equal to the degree of the extension $[F : K]$. Some properties of $\mathrm{Gal}(F/K)$ hold without F/K being Galois, e.g., the inclusion $\mathrm{Gal}(F/M) \subset \mathrm{Gal}(F/K)$ when $M \subset K$. Every Galois extension is a normal extension and since we assumed K has characteristic zero, every normal extension F/K is a Galois extension.

The first theorem that has been formally proven in this paper states that the Galois group of a polynomial P contains all the information about the solvability of the corresponding polynomial equation:

▶ **Theorem 2** (Galois). *A polynomial $P \in F[X]$ is solvable by radicals if and only if its Galois group is solvable.*

We recall that a group G is *solvable* if it is close to being abelian, in the sense that there exists a normal series $\{e\} = G_0 \triangleleft \cdots \triangleleft G_n = G$ of G, whose factors G_{k+1}/G_k are all abelian.

Proof. Lemma 11 from Section 4 addresses the right to left direction. Lemma 19 from Section 5 shows the converse direction. Section 6.1 proves the theorem for $F = \mathbb{Q}$. Finally Section 8.3 explains how to generalize this both in constructive and classical logic contexts. ◀

In other words, Theorem 2 reduces the problem of the solvability by radicals of a polynomial to the analysis of the solvability of its Galois group and allows us to deduce the following one:

▶ **Theorem 3** (Abel-Ruffini). *There is no solution by radicals to general polynomial equations of degree five or higher.*

Proof. It suffices to show that there is a polynomial over $\mathbb{Q}$ which is not solvable by radicals because otherwise the general solution would apply. Theorem 22 in Section 6.3 shows that the polynomial $X^5 - 4X + 2$ is not solvable by radicals. ◀

For the sake of clarity, and unless otherwise stated, in the rest of the paper we focus on the specific case where the base field K has characteristic zero. For instance, the base field of Theorem 3 is simply $\mathbb{Q}$, the field of rational numbers. However, in the formal development, we have striven to provide definitions that are general enough to also apply to the positive characteristic case. Typically, in the case of nonzero characteristic, a normal (hence algebraic) extension F/E is Galois only in the case where it is also *separable* – i.e. if for any $x \in F$, the minimal polynomial of x is separable, i.e., has only simple roots. A substantial amount of our formal development thus applies to the case of positive characteristic as well. We discuss this more in details in Section 9.

3 Formal definitions

Throughout this paper, and unless explicitly mentioned, we consider a (finite) field extension L/F_0, which will serve as an ambient larger locus, fixing a common type for the elements of the various fields at stake. As discussed in Section 2, the reader can safely assume that L has characteristic zero.

In fact, we also assume this extension to be *normal*, that is, that L is the splitting field of a certain polynomial in $F_0[X]$. We will thus use letters E, F, K for sub-fields of L that are themselves extensions over F_0. This formalization choice can be compared to the use of an ambient `finGroupType` in the formalization of finite group theory [11, 16].

In Coq, these assumptions amount to opening a section sharing variables `F0` and `L`, as well as implicit type declarations for letters `E,F,K`:

```
Variables (F0 : fieldType) (L : splittingFieldType F0).
Implicit Types (E F K : {subfield L}).
```

Considering a normal ambient field extension L/F_0 ensures, without loss of generality, that the ambient L is large enough so that for each subfield E of L, it is possible to find a Galois extension F/E, where F is a subfield of L.

Of course, when F/E is itself a field extension, it remains possible to see F as a vector space over E: for instance `\dim_E F` refers to the dimension of F as a vector space over E, i.e., to the degree $[F : E]$ of the extension. Note that as a rule of thumb, notations are designed so as to be well-formed as often as possible. For example, `\dim_E F` is actually defined as the Euclidean quotient of $[F : F_0]$ by $[E : F_0]$, and thus does not require `E` to be included in `F`. These formalization choices, inherited from the design of the Mathematical Components library for linear algebra [10], significantly contribute to reduce the bureaucratic workload in proofs.

In this work, we benefit from the formalized basic concepts and results in Galois theory available in the Mathematical Components library [11], notably from the available proof of the fundamental theorem of Galois theory. The corresponding libraries actually introduce the vocabulary related to field extensions and Galois groups. In particular, `'Gal(F/E)` refers to the Galois group of a field extension F/E. Here as well, this notation is well formed for any `E,F : {subfield L}`, regardless of any inclusion property, and actually refers to $\mathrm{Gal}(F/E \cap F)$ and is a group, regardless of whether F/E is a Galois extension.

We lack space to further comment on all the Coq definitions involved in the present formal proof, but we provide in Figure 1 a correspondence table between the Mathematical Components syntax and the related mathematical objects.

4 From solvable Galois groups to solvable extensions

In this section, we consider E and F two sub-fields of an ambient common normal extension L and we study sufficient conditions for the field extension F/E to be solvable by radical. As these conditions may involve assumptions of primitive roots of unity, we thus enrich the formal context given in Section 3 with the following declarations:

```
Implicit Types (w : L) (n : nat).
```

First, we prove the result in the case of an abelian Galois extension, that is, a Galois extension which Galois group is abelian. In this case, we can prove that the extension is radical.

▶ **Lemma 4.** *An abelian Galois extension F/E of degree n is radical as soon as E contains a primitive n^{th} root of unity.*

```
Lemma abelian_radical_ext w E F (n := \dim_E F) : n.-primitive_root w →
  w \in E → galois E F → abelian 'Gal(F / E) → radical.-ext E F.
```

Proof. The proof goes by exhibiting a basis (r_i) of F, seen as a vector space over E, such that for any u in $G = \mathrm{Gal}(F/E)$ and for any $i \in \{1, \ldots, n\}$, $u(r_i) = \lambda r_i$, where λ is some n^{th} root of unity. Indeed, as in this case $u(r_i^n) = r_i^n$, we have $r_i^n \in E$ for any i, which concludes the proof.

Let u be an element of G. Since $|G| = [F : E] = n$, by Lagrange's theorem of finite group theory, we have $u^n = \mathrm{id}$. Therefore the minimal polynomial of u in E divides the polynomial $X^n - 1$. But since the latter is square-free and splits over E (for E contains a primitive n^{th} root of unity), so is the minimal polynomial of u, and u is thus diagonalizable. Moreover, since G is abelian, all its elements are co-diagonalizable. As a consequence, there exists a

`R : ringType`	R is a ring, whose elements are the terms `x : R`
`p %= q`	the polynomials P and Q are equal up to a unit of R
`'X`	$X \in R[X]$ the indeterminate
`x *: p`	the polynomial xP with $x \in R$ and $P \in R[X]$
`x%:P`	the constant polynomial $x \in R[X]$
`p ^^ f`	the image of $P \in R[X]$ by a ring morphism $f : R \to R'$
`F0 : fieldType`	F_0 is a field, whose elements are the terms `x : L`
`prime n`	the natural number $n \in \mathbb{N}$ is prime
`n != 0 :> F0`	n is nonzero in F_0
`has_char0 F0`	F_0 has characteristic 0
`n.-primitive_root w`	ω is a primitive n^{th} root of unity
	(we use the ASCII character `w` for the greek letter ω)
`x : L`	x is an element of the field L
`E, F, K : {subfield L}`	E, F, K are subfields of L, with base field F_0
`\dim_E F`	the dimension of F over E, i.e., the degree $[F : E]$
`x \in E`	x is in the subset E of L
`E ≤ F`	$E \subset F$, i.e., E is a subfield of F
`1 : {subfield L}`	F_0, seen as a subfield of L
`{:L} : {subfield L}`	L, seen as a subfield of L
	by definition we always have `x \in {: L}` for `x : L`
`<<E ; x>> : {subfield L}`	$E(x)$, the smallest field generated by E and $x \in L$
`<<E & s>> : {subfield L}`	$E(s)$, the smallest field generated by E and the sequence s
`E :&: F : {subfield L}`	$E \cap F$, the field $\{x \mid x \in E \wedge x \in F\}$
`E * F : {subfield L}`	the compositum EF, the field $\{xy \mid x \in E, y \in F\}$
`iota : 'AHom(L,L')`	$\iota : L \to L'$ is an F_0-algebra morphism
`iota @: E`	$\iota(E)$, the image of E by ι, a subfield of L'
`splittingFieldFor E p F`	$F = E(\vec{x})$ where $p \in L[X]$ has roots $\vec{x}$ and coefficients in E
`L : splittingFieldType F0`	L is a splitting field extension of the field F_0, as a type; this is equivalent to the existence of `p` with coefficients in `L`, such that `splittingFieldFor 1 p {:L}`
`minPoly E x : {poly L}`	the minimal polynomial of x over E
`normalField E F : {subfield L}`	the subfield extension F/E is normal
`separable E F : {subfield L}`	the subfield extension F/E is separable
`galois E F : {subfield L}`	the subfield extension F/E is Galois
`radical E x n`	$x^n \in E$ with $n > 0$, i.e., the element x is radical in E
`pradical E x p`	$x^p \in E$ and p is prime
`r.-ext E F`	F/E is `r`, where `r` is either `radical` or `pradical`
`solvable_by r E F`	F/E is solvable by `r`, where `r` is either `radical` or `pradical`
`'Gal(F/E)`	the Galois group of the subfield extension F/E
`phi @* G`	the image of the group G by the morphism φ
`abelian G`	G is abelian
`solvable G`	G is solvable

Figure 1 Correspondence between Coq syntax and mathematical vocabulary

common basis (r_i) of eigenvectors for all elements of G, i.e., a basis (r_i) such that for all u in G, $u(r_i) = \lambda r_i$ for some eigenvalue λ in E. Since these eigenvalues are roots of the minimal polynomial $X^n - 1$ of u, we have $\lambda^n = 1$. ◀

Lemma 4 illustrates the role of linear algebra in Galois theory. However, at the start of this project, the corresponding chapter, about standard results on the diagonalization of matrices, was completely missing from the Mathematical Components library. Formalizing this chapter is one of the spin-off contributions of the present work.

The next step is to generalize the result to the case of a *solvable* Galois group: in this case the corresponding field extension is called a solvable extension. The proof goes by applying Lemma 4 to each of the (abelian) quotients involved in the corresponding normal series, and concludes by gluing radical extensions.

▶ **Lemma 5.** *A solvable Galois extension F/E of degree n is radical, as soon as E contains a primitive n^{th} root of unity.*

```
Lemma solvableWradical_ext w E F (n := \dim_E F) : n.-primitive_root w →
  w \in E → galois E F → solvable 'Gal(F / E) → radical.-ext E F.
```

Proof. We proceed by strong induction on n, the degree of the field extension. Let F/E be a Galois extension of degree n, and suppose that its Galois group G is solvable. If $n = 1$, the extension is trivial, hence G is solvable. Otherwise, by definition, G has a normal and solvable subgroup H of prime index. In particular $H \neq G$ and the quotient G/H is abelian. Let F^H be the field fixed by H (point-wise). Then, the extension F/F^H is Galois and solvable, of degree strictly smaller than n, and F^H/E is an abelian Galois extension. We conclude that F/E is radical by combining the induction hypothesis with Lemma 4. ◀

The main ingredient in the proof of Lemma 5 is the properties of the field extensions F/F^H and F^H/E. These were obtained from the theory of F^H, for H subgroup of a Galois group, already present in the Mathematical Components library.

We can relax the hypothesis that E should contain the n^{th} roots of unity, and transfer it to the ambient field, to the price of weakening the conclusion: in this case, F is only solvable by radicals. This crux of the proof relies on the properties of the Galois group of a compositum extension, which were not present in the Mathematical Components library. In particular, we use the following fact:

▶ **Lemma 6.** *Let E/K be a Galois extension and F a sub-field of E. Then:*

$$\mathrm{Gal}(KF/F) \simeq \mathrm{Gal}(K/K \cap F)$$

```
Lemma galois_isog (k K F : {subfield L}) : galois k K → k ≤ F →
  'Gal((K * F) / F) \isog 'Gal (K / K :&: F)
```

Proof. See for instance Lang's proof [15, VI, §1, Theorem 1.12]. ◀

▶ **Lemma 7.** *A solvable Galois extension F/E of degree n is solvable by radicals, as soon as E and F are sub-fields of a common normal extension L, which contains a primitive n^{th} root of unity in L.*

```
Lemma galois_solvable_by_radical w E F (n := \dim_E F) : n.-primitive_root w →
  galois E F → solvable 'Gal(F / E) → solvable_by radical E F.
```

Proof. Let F/E a Galois extension of degree n, with E, F sub-fields of F. Let $\omega \in L$ be a primitive n^{th} root of unity. The proof goes by showing that the extension $FE(\omega)/E$ is radical. Since $E(\omega)/E$ is a simple radical extension, it suffices to show $FE(\omega)/E(\omega)$ is radical.

Since F/E is a Galois extension, then so is $FE(\omega)/E(\omega)$. Let m be the degree of $FE(\omega)/E(\omega)$. By Lemma 6, $\mathrm{Gal}(FE(\omega)/E(\omega))$ is isomorphic to $\mathrm{Gal}(F/F \cap E(\omega))$, which is thus of order m as well. But since $\mathrm{Gal}(F/F \cap E(\omega))$ is a subgroup of $\mathrm{Gal}(F/E)$, its order m divides n, the order of $\mathrm{Gal}(F/E)$. Consider $\omega' = \omega^{\frac{n}{m}}$. It is an element of $E(\omega)$, and thus of $FE(\omega)$, and a primitive root of unity. We can apply Lemma 5 on the extension $FE(\omega)/E(\omega)$, and the m^{th} primitive root of unity ω' as soon as we show that $\mathrm{Gal}(FE(\omega)/E(\omega))$ is solvable. Which is the case because it is isomorphic to $\mathrm{Gal}(F/F \cap E(\omega))$, itself solvable as a subgroup of $\mathrm{Gal}(F/E)$. ◀

The final result of the section trades the assumption on the solvability of the Galois group for the solvability of the extension itself, i.e., for the solvability of the Galois group of the extension by the normal closure.

▶ **Definition 8.** *The* normal closure $\mathrm{NCl}_E(F)/E$ *of* F/E *is the smallest (for field inclusion) field extension of* F *that is normal over* E*.*

▶ **Definition 9.** *An extension* F/E *is* solvable *if* F/E *(is separable) and* $\mathrm{Gal}(\mathrm{NCl}_E(F)/E)$ *is solvable.*

▶ Remark 10. Note that in the case of zero characteristic, the separability requirement vanishes. A Galois extension F/E is solvable if and only if $\mathrm{Gal}(F/E)$ is solvable (as a group).

By definition of the normal closure, if an extension F/E is solvable, then $\mathrm{NCl}_E(F)/E$ is Galois. Therefore, solvability by radicals follows from the solvability of an extension, as an immediate corollary of Lemma 7.

▶ **Lemma 11.** *Let* F/E *be a solvable extension, and* n *the degree of the extension* $\mathrm{NCl}_E(F)/E$*.* F/E *is solvable by radicals as soon as* L *contains a primitive* n^{th} *root of unity.*

```
Lemma ext_solvable_by_radical w E F (n := \dim_E (normalClosure E F)) :
  n.-primitive_root w → solvable_ext E F → solvable_by radical E F.
```

Proof. Since F/E is solvable, $\mathrm{Gal}(\mathrm{NCl}_E(F)/E)$ is solvable. Thus Lemma 7 applies and proves that $\mathrm{NCl}_E(F)/E$ is solvable by radicals. Since $F \subset \mathrm{NCl}_E(F)$, then F/E is solvable by radical as well. ◀

5 From solvable by radicals extensions to solvable extensions

Recall that L/F_0 is an ambient normal field extension. We first establish two useful results on simple radical extensions $E(x)/E$ for E a sub-field of L. When x is a root of unity, the extension $E(x)/E$ is called a *cyclotomic* extension. A cyclotomic extension is a Galois and solvable extension.

▶ **Lemma 12.** *Suppose that* L *contains* ω*, an* n^{th} *primitive root of unity for* n *a positive integer. Consider* E *a sub-field of* L *and* $x \in L$ *such that* $x^n \in E$*. Then, the extension* $E(\omega, x)/E$ *is Galois. In particular if* $\omega \in E$*, then* $E(x)/E$ *is Galois.*

```
Lemma galois_cyclo_radical (n : nat) (w x : L) (E : {subfield L}):
    p.-primitive_root w → p > 0 → x ^+ p \in E → galois E << <<E; w>> ; x >>.
```

Proof. If $x \in E$, the conclusion is immediate. We can thus suppose that $x \neq 0$ and $n > 1$. In this case, the polynomial $P = X^p - x^n \in E[X]$ is separable, since it has n distinct roots, of the form $x\omega^i$, for $i = 0 \dots n-1$. Moreover,

$$\begin{aligned} E(x, x\omega, \dots, x\omega^{n-1}) &= E(x, x\omega)(x\omega^2, \dots, x\omega^{n-1}) && \text{since } n > 0 \\ &= E(\omega, x)(x\omega^2, \dots, x\omega^{n-1}) && \text{since } x \neq 0 \\ &= E(\omega, x) && \text{since } x\omega^i \in E(\omega, x) \end{aligned}$$

It follows that $E(\omega, x)$ is a splitting field of P, and therefore that $E(\omega, x)/E$ is Galois. ◀

▶ **Lemma 13.** *Suppose that L contains ω, a p^{th} primitive root of unity for p a prime number. Consider E a subfield of L and $x \in L$ such that $x^p \in E$, but $x \notin E$. Then, the minimal polynomial of x over E is $X^p - x^p$.*

As a consequence, $\mathrm{Gal}(E(x)/E)$ *is of prime order and is thus cyclic, hence abelian (and solvable).*

```
Lemma minPoly_pradical (p : nat) (w x : L) (E : {subfield L}):
    p.-primitive_root w → prime p → w \in E → x \notin E → x ^+ p \in E →
  minPoly E x = 'X^p - (x ^+ p)%:P.
```

Proof. Let $P \in E[X]$ be the minimal polynomial of x over E. By minimality, P divides any polynomial over E that cancels x. In particular, P divides $X^p - x^p = \prod_{i<p}(X - x\omega^i)$. Hence there is a subset S of $I_p = \{i \mid i < p\}$ such that $P = \prod_{i \in S}(X - x\omega^i)$. Since P cancels x, S contains x, therefore $|S|$ is positive. It suffices to show $|S| \geq p$, because then $S = I_p$ and $P = X^p - x^p$. Since $|S|$ is positive, it is sufficient to prove that p divides $|S|$.

First, note that p divides any k such that $x^k \in E$. Indeed, if k and p were coprime, Bézout's identity would provide $m, n \in \mathbb{Z}$ such that $km + pn = 1$. As a consequence, we would have $x = (x^k)^m + (x^p)^n \in E$, contradicting our assumption that $x \notin E$.

Now the constant coefficient of P is $x^{|S|}\Omega$, where $\Omega = \prod_{i \in S} \omega^i$ is a nonzero element of E, hence $x^{|S|} \in E$ and p divides $|S|$. ◀

In order to get rid of the assumption that the ambient L contains a suitable root of the unity, we prove that the normal closure of a subfield of L, as well as the Galois group of an extension in L, are preserved up to isomorphism when L is extended with some roots of unity.

Consider L/F_0 and L'/F_0 two normal extensions, $\iota : L \to L'$ an F_0-algebra morphism, and F/E a field extension in L.

▶ **Lemma 14.** *There is a group isomorphism* $\mathrm{Gal}(F/E) \to \mathrm{Gal}(\iota(F)/\iota(E))$*, which we also denote ι.*

In Coq the group (iso)morphism corresponding to ι is called `map_gal`.

```
Lemma map_gal_inj : 'injm (map_gal iota).
Lemma img_map_gal : map_gal iota @* 'Gal(F / E) = 'Gal(iota @: F / iota @: E).
```

The properties of this morphism are key to the preservation of normal extensions, separable extensions, Galois extensions, normal closures and solvable extensions under the associated algebra isomorphism.

▶ **Lemma 15.** *The extension $\iota(F)/\iota(E)$ is normal (resp. separable, Galois, solvable) if and only if F/E is normal (resp. separable, Galois, solvable), and* $\iota(\mathrm{NCl}_E(F)) = \mathrm{NCl}_{\iota(E)}(\iota(F))$.

```
Lemma normalField_aimg   : normalField (iota @: E) (iota @: F)  = normalField E F.
Lemma separable_aimg     : separable (iota @: E) (iota @: F)    = separable E F.
Lemma galois_aimg        : galois (iota @: E) (iota @: F)       = galois E F.
Lemma solvable_ext_aimg  : solvable_ext (iota @: E) (iota @: F) = solvable_ext E F.
Lemma aimg_normalClosure :
  iota @: normalClosure E F = normalClosure (iota @: E) (iota @: F).
```

The combination of Lemma 15 with Lemma 16 makes possible to extend, if needed, the ambient field with a primitive root of unity so as to prove that a certain extension is normal (resp. separable, Galois, or solvable).

▶ **Lemma 16.** *Let L/F_0 be an ambient normal field extension and n a natural number coprime with the characteristic of F_0. There is an ambient normal field extension L'/F_0, a primitive n^{th} root of unity $\omega \in L'$ and an F_0-algebra morphism $\iota : L \to L'$, such that $\iota(L)(\omega) = L'$.*

We can now state and prove properties of simple (prime) radical extensions which do not require any assumption on the presence of a root of unity.

▶ **Lemma 17.** *Let p be prime number such that $p \neq 0$ in F_0. Let $x \in L$ and E a subfield of L such that $x^p \in E$. The extension $E(x)/E$ is solvable.*

Note that because of the definition of a solvable extension, $E(x)/E$ need not be Galois.

```
Lemma pradical_solvable_ext (p : nat) (x : L) (E : {subfield L}) :
  prime p → p != 0 :> F0 → x ^+ p \in E → solvable_ext E <<E; x>>.
```

Proof. Without loss of generality, we can assume the existence of $\omega \in L$ a primitive p^{th} root of unity. Indeed, Lemma 16 gives the existence of a field extension L' and an embedding $\iota : L \to L'$, where L' contains a p^{th} primitive root of unity (since $p \neq 0$ in F_0). Now we may prove $\iota(E(x))/\iota(E)$ is Galois and "transfer" the result to $E(x)/E$ using Lemma 15.

In order to prove $E(x)/E$ is solvable, it suffices to find a Galois extension of $E(x)$ that is solvable. Because of Lemma 12, $E(\omega, x)/E$ is Galois. Now both $E(\omega)/E$ (because it is cyclotomic) and $E(\omega, x)/E(\omega)$ (by Lemma 13) are Galois and solvable. Hence, $\mathrm{Gal}(E(\omega, x)/E(\omega))$ is a normal subgroup of $\mathrm{Gal}(E(\omega)/E)$, therefore $E(\omega, x)/E$ is solvable. ◀

The final lemma of this section is often stated in the literature in the following way: "If F/E is Galois and solvable by radicals then $\mathrm{Gal}(F/E)$ is solvable". While this is true, this does not allow for a proof by induction as such since intermediate extensions of the radical series of F/E need not be Galois over E. Rigorous proofs must strengthen the induction. One way to do so is by introducing the notion of solvable extension which, contrarily to the notion of Galois extension, is transitive:

▶ **Lemma 18** (solvability of extensions is transitive)**.** *If F/E and K/F are solvable extensions, then K/E is solvable.*

Proof. We essentially follow the proof from Lang [15, VI, §7, Proposition 7.1], except that instead of in-lining the definition of the normal closure in a particular case, we define and study normal closures for their own interest, which eventually results in a shorter proof. ◀

We are now ready to state the final and main result of this section, and to avoid assuming that the extension F/E is Galois, in addition to being solvable by radicals. The proof is a straightforward induction on the height of the radical series.

▶ **Lemma 19.** *If F/E is solvable by radicals then F/E is a solvable extension.*

```
Lemma radical_ext_solvable_ext (E F : {subfield L}) : has_char0 L → E ≤ F →
  solvable_by radical E F → solvable_ext E F.
```

Proof. Let F/E be a solvable by radicals extension, it is also solvable by prime radicals, so there exists a prime radical extension tower $E = E_0 \subset E_1 \subset \ldots \subset E_n$ such that $F \subset E_n$. Since every intermediate extension E_{i+1}/E_i is solvable, by Lemma 17, we conclude by induction and by Lemma 18 that E_n/E_0 is solvable. Since $F \subset E_n$, F/E is also solvable. ◀

Note that this proof goes by induction on the length of the tower. Curiously, some references (such as the French wikipedia page on the Abel-Ruffini Theorem as of 2021-04-20) do not rely on solvable extensions, or define it as "being Galois and solvable" instead of "having a Galois field extension that is solvable". Unfortunately, under such variations, we lack a transitivity property analogue to Lemma 18, which dooms to failure any attempt of a similar proof by induction. Actually, we conjecture[1] that there is a tower of cyclic extensions of height two $\mathbb{Q}^{\mathrm{ab}} \subset K \subset L$ where both $K/\mathbb{Q}^{\mathrm{ab}}$ and L/K are simple radical Galois extensions, but where $L/\mathbb{Q}^{\mathrm{ab}}$ is not Galois (even though $\mathbb{Q}^{\mathrm{ab}}$ contains all roots of unity). Such a counterexample would imply that any proof by induction where the induction hypothesis has the form "E_n/E_0 is Galois and [...]" is bound to fail.

Hence, some references end up applying Galois' fundamental theorem in a context where a premise – that some extension is Galois – does not hold. And those who exhibit a correct proof without relying on solvable extensions must reconstruct a radical series gradually, by adding all possible conjugates over the smallest field of the tower, at each step, which is exactly what is factored out in the definition of a solvable extension and in Lemma 18.

Moreover, all the proofs we found in the literature – including the ones relying on solvable extensions, such as in *Algebra*, Lang [15, VI, §7, Theorem 7.2] – delve into details about picking an appropriate primitive root of unity ω (e.g., using the least common multiple of all the prime exponents involved in the radical series) and reconstruct the full radical extension starting with the cyclotomic field extension $E(\omega)/E$ before starting an induction. We observe here that this detour is completely unnecessary when using solvable extensions.

6 Galois and Abel-Ruffini theorems

In this section we specialize results to $\mathbb{Q}$, which is sufficient to obtain the unsolvability of the general quintic. For possible generalizations of the results stated here, we refer to the discussions in Sections 8 and 9.

6.1 Galois' theorem

For a given polynomial in $P \in \mathbb{Q}[X]$, splitting fields for P over $\mathbb{Q}$ always exist, are isomorphic to each other and embed in the algebraic numbers (noted $\bar{\mathbb{Q}}$ in math style and `algC` in Coq) and though this embedding can be seen as a number field. We pick such a splitting field and call it $\mathbb{Q}(P)$, *the* splitting field of P. We pose the convention $\mathbb{Q}(0) = \mathbb{Q}$.

We write `numfield p` for $\mathbb{Q}(P)$ in Coq, it has type `splittingFieldType rat`, and there is a morphism `numfield_inC : {rmorphism numfield p → algC}` embedding $\mathbb{Q}(P)$ in $\bar{Q}$. There is also a function `numfield_roots : {poly rat} → seq (numfield p)` which lists the roots of P.

[1] https://mathoverflow.net/questions/381824

A polynomial P is solvable by radical if there is a field L that splits P, and such that L/K is solvable by radical. Note that L need not be $\mathbb{Q}(P)$, indeed the radicals involved in the decomposition of L may not belong to $\mathbb{Q}(P)$.

▶ **Definition 20.** *A nonzero polynomial $P \in \mathbb{Q}[X]$ is solvable by radicals if there is a field extension L and a subfield K of L which is a splitting field for P, and such that the extension $K/\mathbb{Q}$ is solvable by radicals.*

In Coq we use a slightly different definition (see Section 8) which we prove equivalent to the mathematical one.

```
Lemma solvable_poly_ratP (p : {poly rat}) : p != 0 →
  solvable_by_radical_poly p ↔
  ∃ L : splittingFieldType rat, ∃ K : {subfield L},
    splittingFieldFor 1 (p ^^ in_alg L) K ∧ solvable_by radical 1 K.
```

We can now recall Theorem 2 (Galois) and prove it formally for $F = \mathbb{Q}$:

▶ **Theorem 2** (Galois). *A polynomial $P \in F[X]$ is solvable by radicals if and only if its Galois group is solvable.*

```
Theorem AbelGaloisPolyRat (p : {poly rat}) :
  solvable_by_radical_poly p ↔ solvable 'Gal({: numfield p} / 1).
```

Proof. First notice that by Remark 10 the right hand side of the equivalence "$\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is solvable", is the same as $\mathbb{Q}(P)/\mathbb{Q}$ is a solvable extension. The left to right side is then a trivial application of Lemmas 19. And the right to left side consists in first extending $\mathbb{Q}(P)$ with a $[\mathbb{Q}(P) : \mathbb{Q}]^{\text{th}}$ primitive root of unity before applying Lemma 11. ◀

Now, in order to prove the Abel-Ruffini theorem, it suffices to exhibit a polynomial of degree 5 which Galois group is unsolvable. As in the literature, we pick $\mathfrak{S}_5$ and prove a certain class of polynomials has Galois group $\mathfrak{S}_5$: the irreducible rational polynomials with Prime Degree and Two Non Real Roots.

6.2 Irreducible rational polynomials of Prime Degree with exactly Two Non Real Roots

▶ **Lemma 21.** *Irreducible polynomials $P \in \mathbb{Q}[X]$ of prime degree p with exactly two non real roots have a Galois group over $\mathbb{Q}$ isomorphic to $\mathfrak{S}_p$.*

```
Lemma PDTNRR.isog_gal (p : {poly rat}) :
    irreducible_poly p → prime (size p).-1 →
    count [pred x | numfield_inC p x \isn't Creal] (numfield_roots p) = 2 →
  'Gal({: numfield p} / 1) \isog 'Sym_('I_(size p).-1)
```

Proof. Let $P \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p, a sequence $s = (s_i)_i$ of its roots, and $G = \mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ its Galois group. We define a group morphism $\varphi : G \to \mathfrak{S}_p$, so that $\forall i < p,\ \forall u \in G,\ s_{\varphi(u)(i)} = u(s_i)$. In other words φ maps an element u of the Galois group of P to a permutation of the indices of the sequence s that is compatible with the action of u on the roots s of P. Now, it suffices to show that φ is injective and surjective to conclude.

- φ is injective: let u be such that $\varphi(u) = \mathrm{id}$, it suffices to show that $u = \mathrm{id}$. Let $x \in \mathbb{Q}(P)$, x can be decomposed as a multivariate polynomial μ over $\mathbb{Q}$ applied to the sequence s, i.e., $x = \mu(s)$. Then $u(x) = u(\mu(s)) = \mu\left((u(s_i))_i\right) = \mu\left((s_{\varphi(u)(i)})_i\right) = \mu(s) = x$.

- φ is surjective: it suffices to show that there is a transposition τ and an element of order p in $\varphi(G)$. Indeed, since p is prime number we have $\mathfrak{S}_p = \langle \tau, c \rangle$.
  - Since P has exactly two non real roots, there are $i < j < p$ such that, $s_i = s_j^\star$ and $s_k = s_k^\star$ if $k \notin \{i, j\}$. The complex conjugation $(\cdot^\star)$ belongs to G and $\varphi(\cdot^\star) = (i\ j) = \tau$.
  - The natural number p divides $[\mathbb{Q}(P) : \mathbb{Q})]$ because P is irreducible. Since p is prime and divides G, by Cauchy's theorem, there is an element of order p in G.

◀

In Coq we did not link the theory of multivariate polynomials with the theory of field automorphism yet, instead we simply iterate on the sequence s and use univariate polynomials in each s_i.

6.3 $X^5 - 4X + 2$ is not solvable by radicals

There is no general formula for solving equations of degree greater than four (Theorem 3) because if there were, the equation $x^5 - 4x + 2 = 0$ would be solvable.

▶ **Theorem 22** (Insolvability of the quintic). *$X^5 - 4X + 2$ is not solvable by radicals.*

```
Theorem example_not_solvable_by_radicals :
  ¬ solvable_by_radical_poly ('X^5 - 4 *: 'X + 2 : {poly rat}).
```

Proof. By Theorem 2, it suffices to thow the galois group of $\mathbb{Q}(Q)/\mathbb{Q}$ is not solvable, where $Q = X^5 - 4X + 2$.

- By Lemma 21, it suffices to show Q is irreducible and has exactly two non real roots. Irreducibility is directly given by Eisenstein criterion. Q has at least three real roots in $\bar{\mathbb{Q}}$ because there are at least three sign changes: $Q(-2)Q(-1) < 0$, $Q(-1)Q(1) < 0$, and $Q(1)Q(2) < 0$. Finally since the derivative $Q' = 5X^4 - 4$ has exactly two real roots $(\pm\sqrt{\frac{2}{\sqrt{5}}})$, it means Q has at most three real roots, hence exactly three.
- To show $\mathfrak{S}_5$ is not solvable it suffices to show its normal subgroup $\mathfrak{A}_5$ is not solvable either. We conclude by contradiction with the fact that $\mathfrak{A}_5$ is simple of order $5 \times 4 \times 3$ and a simple solvable group must have prime order.

◀

7 Solvability by radicals is what you think

We now link the solvability by radical, as defined above, to the existence or not of analytic expressions for computing the roots of a given polynomial. Most of the time, this last step is considered mundane and is left to the reader. Here we give a formal treatment to it, both for intellectual satisfaction but also as a hint that our definition of a radical extension is correct.

More formally, for a field F, we define the grammar of radical expressions $\mathbb{E}_F$ over F as the set of terms that can be recursively defined from the symbols 0, 1, $x \in F$, $+$, $-$, $*$, $\cdot^{-1}$, $\sqrt[n]{\cdot}$ and ω_n where $\sqrt[n]{e}$ (resp. ω_n) stands for a n^{th}-root of e (resp. a n^{th}-primitive root of unity):

$$e \in \mathbb{E} ::= 0 \mid 1 \mid e_1 + e_2 \mid -e \mid e_1 * e_2 \mid e^{-1} \mid \sqrt[n]{e} \mid \omega_n \quad (n \in \mathbb{N}^*)$$

In Coq, as expected, we encode this set using an algebraic datatype. We then give an interpretation for terms in $\mathbb{E}$ in terms of algebraic numbers and w.r.t. an evaluation function `(iota : F → algC)`:

```
Variables (F : fieldType) (iota : F → algC).
Fixpoint algT_eval (f : algterm F) : algC :=
  match f with
  | Base x          => iota x
  | 0               => 0
  | 1               => 1
  | f1 + f2         => algT_eval f1 + algT_eval f2
  | - f             => - algT_eval f
  | f1 * f2         => algT_eval f1 * algT_eval f2
  | f ^-1           => (algT_eval f)^-1
  | f ^+ n          => (algT_eval f) ^+ n
  | n.+1-root f     => n.+1.-root (algT_eval f)
  | j.+1-prim1root => prim1root j.+1
  end.
```

It is worth mentioning that, in the listing above, the expressions on the left of `=>` are syntax whereas the ones on the right of `=>` are semantic, i.e., values in the type `algC` of algebraic numbers.

We now have all the necessary ingredients to state and prove the equivalence between being a solvable by radical polynomials and having roots expressible as a radical expression, as defined above:

```
Lemma solvable_formula (p : {poly rat}) : p != 0 →
  solvable_by_radical_poly p ↔
  {in root (p ^^ ratr), ∀ x, ∃ f : algterm rat, algR_eval ratr f = x}.
```

8 Classical reasoning in a constructive setting

8.1 Boolean reflection and effective Galois theory

The present contribution takes over the main design choices deployed in Mathematical Components library, and in particular its use of boolean reflection [18] for formalizing effective mathematics. Notably, the defining signature of algebraic structures, like rings or fields, involve boolean predicates, e.g., for comparison or discrimination of units. More generally, decidable predicates, that is predicates for which excluded-middle holds constructively, are formalized as boolean predicates. Consequently, equivalences between such boolean propositions are stated as equalities, as for instance in Lemma 15. Besides often saving the user from the technicalities of setoid rewriting, boolean specifications are provably proof-irrelevant, by Hedberg's theorem [13], and this feature is extensively used for defining and using proof-irrelevant dependent pairs.

The present development heavily relies on the effective perspective provided by the underlying linear algebra component [10]. In this library, vector spaces of finite dimension and their sub-spaces, always come with an explicit basis, and are in fact internally represented as matrices. This way, most properties of linear algebra in finite dimension are effective, thanks to variants of Gaussian elimination: computing the dimension of a sub-space, testing whether a family of vectors is free, whether it generates a given sub-space, testing the inclusion or the equality between sub-spaces, etc. When a larger vector space is in fact an algebra (resp. a field extension) over a given base field, it is decidable whether a given subspace is in fact a sub-algebra U (resp. a sub-field U): it suffices to test whether pairwise products of elements of the basis of U belong to U. Note however that effectivity does not mean that the computations are necessarily tractable in practice: turning these effective definition into formally verified algebra that can be executed on concrete entries would require a non-trivial additional effort [7, 24].

The main effect of this effective take on linear algebra in the case of (finite) field extensions is the definition of boolean functions for testing whether a (finite) field extension is normal, separable or Galois. In addition, the construction of normal closure is effective, as well as that of the Galois group of an extension. As the finite group theory component of the Mathematical Components library provides a boolean test for the solvability of finite group, solvability of an extension is decidable as well.

8.2 Non-effective results

However, important properties in commutative algebra, such as testing a polynomial in $F[X]$ for irreducibility for F an arbitrary field, remain non-effective, even in the case of a field F with a decidable equality. As a consequence, in a constructive setting, some facts like Lemma 16 cannot be proved as such. The way out is to change their statement for a classically equivalent one, typically, a double-negated version, so as to restore constructive provability. For this purpose, we use the `classically` monadic predicate [11]: for any `P : Prop`, `classically P` is equivalent to the double-negation `¬(¬P)`. For instance, the construction of a larger normal field extension performed in Lemma 16 is not effective in general. Here is a typical example of non-effective statement:

```
Lemma classic_baseCycloExt F n : (n%:R != 0 :> F) → classically
 { L' : splittingFieldType F & { w : L' & <<1; w>> = {: L'} & n.-primitive_root w }}.
```

The `classically` monad thus seals the sigma-type, which is itself an effective existential statement. However thanks to the formal definition of the `classically` predicate, a hypothesis of the form `classically P` can be used directly as if it were of the form `P` in particular for proving a boolean statement (and because `¬(¬b)` $\leftrightarrow$ `b` holds constructively).

Continuing our example, Lemma `classic_baseCycloExt` is used in the proof of Lemma 17, in order to establish that a simple extension $E(x)/E$ is solvable, which is stated formally as `solvable_ext E <<E; x>>`. Since the `solvable` predicate is boolean (see Section 8.1), lemma `classic_baseCycloExt` can be used without propagating the `classically` monad to the final formal statement of Lemma 17.

8.3 Stating Galois' theorem in characteristic zero

In a constructive setting, it is not possible to rely on the existence of an algebraic closure when needed, as is commonly assumed in the standard literature, and this even in the case of a base field F_0 with zero characteristic. Our current formal statement of Galois' theorem for arbitrary field extensions in zero characteristic thus reads:

▶ **Theorem 23.** *Let L/F_0 be a normal extension of characteristic zero and F/E a field extension in L. Suppose that $\omega \in L$ is a primitive $[\mathrm{NCl}_E(F) : E]^{th}$ root of unity. Then F/E is solvable by radicals if and only if it is solvable.*

```
Theorem AbelGalois  (F0 : fieldType) (L : splittingFieldType F0) (w : L)
    (E F : {subfield L}) : (E ≤ F) → has_char0 L →
    (\dim_E (normalClosure E F)).-primitive_root w →
  solvable_by radical E F ↔ solvable_ext E F.
```

In the literature "F solvable by radicals" is defined as the existence of a certain radical extension containing F. This definition actually allows us to get rid of the assumption on the existence of a root of unity, as in the above theorem. This assumption, which is only needed for the right-to-left implication (see Lemma 19), would indeed be encompassed by the definition of "solvable by" in the right-to-left implication.

Alas, strengthening the definition of "solvable by radicals" in order to match the variant found in the literature – and thus dropping the assumption on the existence of a root of unity – would not make the right-to-left implication a direct consequence of Lemma 11 in the current state of the formalization. It is actually not clear to us whether this would be provable at all constructively. Indeed, we know no constructive way to test the presence of a primitive root of unity in L, or to extend L with such a hypothetical primitive root of unity.

We could however use classical axioms, or the `classically` monad of Section 8.2, to recover the standard wording found in the literature. Another option would be to construct, effectively, extensions of number fields with an arbitrary algebraic element, e.g.,with a primitive root of unity. This way, results from Section 6 that have been specialized to $\mathbb{Q}$ could in principle be generalized to any number field, or, even to factorial fields [20], i.e., fields equipped with an effective irreducibility test for polynomials.

9 Conclusion

Comparison to related formalization in Coq

This work represents a significant extension of the Mathematical Components library, both in size and in contents. This background proved to be sufficiently mature so that we didn't need to change the definitions and formalization choices. This work is grounded on the three main algebraic hierarchies which are the backbone of the Mathematical Components library: hierarchies of structures (from additive groups to field extensions, and real closed fields), hierarchies of morphisms (of additive groups, rings, algebra, and fields), and hierarchies of predicates (sub-groups, vector sub-spaces, sub-algebras, sub-fields).

These hierarchies are designed using Coq's canonical structures mechanism [22], more precisely with the packed class methodology [9], in order to achieve ad-hoc polymorphism [12, 17]. This inference mechanism is crucial to combine the different components of the library: finite group theory, linear algebra, theory of field extensions and Galois theory. Inference of structures is used at almost every single line of code and its efficiency is crucial for making amenable such a development.

Comparison to related formalization in other systems

The only formalization of Galois theory we are aware of has been carried in Lean/mathlib. This work is at an early stage of development as only the Galois correspondence is currently proven. This development relies on previously defined algebraic structures by the Lean/mathlib community [19], such as fields, vector spaces, algebras and their morphisms.

A formalization of field extensions and algebraic closure [6] was carried out in the Isabelle/HOL theorem prover. Despite the lack of dependent types, this library comes with a definition of the algebraic closure of an abstract field as opposed to the a more elementary construction for a fixed field such as $\mathbb{Q}$. However, it is unclear whether the methodology used there can be further extended for the formalization of Galois theory. At least, dependent types play a central role in the design choices at stake in the present development.

The Mizar library contains core definitions and results related to field extensions [23].

Last, there exists an unfinished development related to the formalization of Galois theory and unsolvability of the quintic in LEGO [1]. However, only the unsolvability of the symmetric group [3] has been formally addressed.

Comparison to the pen and paper literature

In this paper, we give a comprehensive outline of the Abel-Ruffini theorem. This outline serves as a basis to our formal development and has only been made possible by a careful synthesis work of the numerous definitions and proofs from the literature.

We noticed several variations in the definitions of "radical extensions" and "solvable by radical" (extension), which are the same but may denote two different things: one corresponding to our definition of "radical extension" and the other corresponding to our definition "solvable by radical". Indeed both definitions are useful and we must give a precise name to each. Perhaps the most surprising takeaways from this synthesis work are the remarks that follow the proof of Lemma 19. Many references give a fine-grained description of a modification of the radical series which would give the right induction hypothesis, which can be avoided by the definition of a solvable extension.

The proof of unsolvability of X^5-4X+2 involves counting its real roots. The most common way of doing this relies on building *sign tables*. However, the Mathematical Components library does not give any formal treatment of sign tables and we had to roll out our own solution. Fortunately, the MathComp-Real-Closed [5] library provides results related to the study of the variations of a polynomial with coefficients in an algebraically closed field. This allowed us to give lower and upper bounds on the number of reals without having to formalize sign tables. However, we expect that a formal treatment of sign tables to be a useful addition to the Mathematical Components library.

On the same subject, the library MathComp-Real-Closed contains a quantifier elimination procedure and a root counting procedure. In theory, in order to obtain the number of real roots, it would have been possible to simply run this procedure on the targeted polynomial. However, in practice, due to the very inefficient nature of the involved datatypes (starting from the use of unary natural numbers), the methodology proved to be too inefficient. A possible future work would be to extend CoqEAL [7, 4] to make effective these procedures.

The case of positive characteristic

Even if a large part of our development is independent from the characteristic of the fields under consideration, for the sake of simplifying, we sometime restricted ourselves to the case of characteristic zero – as this is the case in the file `abel.v` for example. For instance, we specialized the notion of radical extension to fields of characteristic zero, which is enough to show the unsolvability of a polynomial over $\mathbb{Q}$. However, we expect that the zero-characteristic assumption could be dropped in the near future. For example, the definition of radical extensions in a field of an arbitrary characteristic p could be generalized by following the definition from Lang [15, VI, §7, Remark], thus adding a second kind of radical extensions $K(a)/K$ such that $a^p - a \in K$. The proof that cyclic extensions of degree p are of that form would then rely on the additive version of Hilbert Theorem 90. (The multiplicative version is already formalized – it could be used in place of Lemma 4 – and we do not expect any difficulty in formalizing its additive counterpart.)

Reasoning up to isomorphisms

A substantial amount of proof scripts is devoted to the transfer of properties from one object to an isomorphic one (See Lemma 15 for an example). This part is largely left implicit on paper and it is indeed quite mundane. It would be interesting to see if the ongoing work around *Homotopy Type Theory* [26, 24, 2] could apply here.

References

1. Peter Aczel. Galois: a theory development project. *manuscript, University of Manchester*, 1993.
2. Carlo Angiuli, Evan Cavallo, Anders Mörtberg, and Max Zeuner. Internalizing representation independence with univalence. *Proc. ACM Program. Lang.*, 5(POPL), January 2021. doi:10.1145/3434293.
3. Gilles Barthe. A formal proof of the unsolvability of the symmetric group over a set with five or more elements. URL: https://ftp.cs.ru.nl/CSI/CompMath.Found/sn.ps.Z.
4. Cyril Cohen, Maxime Dénès, and Anders Mörtberg. Refinements for Free! In *Certified Programs and Proofs*, pages 147 – 162, Melbourne, Australia, December 2013. URL: https://hal.inria.fr/hal-01113453, doi:10.1007/978-3-319-03545-1_10.
5. Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. *Logical Methods in Computer Science*, 8(1:02):1–40, February 2012. URL: https://hal.inria.fr/inria-00593738, doi:10.2168/LMCS-8(1:02)2012.
6. Paulo Emílio de Vilhena and Lawrence C. Paulson. Algebraically closed fields in isabelle/hol. In Nicolas Peltier and Viorica Sofronie-Stokkermans, editors, *Automated Reasoning*, pages 204–220, Cham, 2020. Springer International Publishing.
7. Maxime Dénès, Anders Mörtberg, and Vincent Siles. A refinement-based approach to computational algebra in COQ. In Lennart Beringer and Amy Felty, editors, *ITP - 3rd International Conference on Interactive Theorem Proving - 2012*, volume 7406 of *Lecture Notes In Computer Science*, pages 83–98, Princeton, United States, August 2012. Springer. URL: https://hal.inria.fr/hal-00734505, doi:10.1007/978-3-642-32347-8_7.
8. Evariste Galois. *Mémoire sur les conditions de résolubilité des équations par radicaux.*, volume XI of *Journal de mathématiques pures et appliquées*. Joseph Liouville, 1846. URL: https://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubiblite.pdf.
9. François Garillot, Georges Gonthier, Assia Mahboubi, and Laurence Rideau. Packaging Mathematical Structures. working paper or preprint, March 2009. URL: https://hal.inria.fr/inria-00368403.
10. Georges Gonthier. Point-Free, Set-Free Concrete Linear Algebra. In Marko C. J. D. van Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem Proving - ITP 2011*, volume 6898 of *Lecture Notes in Computer Science*, pages 103–118, Berg en Dal, Netherlands, August 2011. Radboud University of Nijmegen, Springer. URL: https://hal.inria.fr/hal-00805966, doi:10.1007/978-3-642-22863-6_10.
11. Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of the Odd Order Theorem. In Sandrine Blazy, Christine Paulin, and David Pichardie, editors, *ITP 2013, 4th Conference on Interactive Theorem Proving*, volume 7998 of *LNCS*, pages 163–179, Rennes, France, July 2013. Springer. URL: https://hal.inria.fr/hal-00816699, doi:10.1007/978-3-642-39634-2_14.
12. Georges Gonthier, Beta Ziliani, Aleksandar Nanevski, and Derek Dreyer. How to make ad hoc proof automation less ad hoc. *SIGPLAN Not.*, 46(9):163–175, September 2011. doi:10.1145/2034574.2034798.
13. Michael Hedberg. A coherence theorem for Martin-Löf's Type Theory. *J. Funct. Program.*, 8(4):413–436, July 1998. URL: http://dx.doi.org/10.1017/S0956796898003153, doi:10.1017/S0956796898003153.
14. Abel Niels Henrik. *Œuvres complètes de Niels Henrik Abel, mathématicien, nouvelle édition publiée aux frais de l'État norvégien par L. Sylow et S. Lie.* Imprimerie de Grøndahl & søn, 1881. URL: https://www.abelprize.no/c54178/artikkel/vis.html?tid=54181.
15. Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

16 Assia Mahboubi. The rooster and the butterflies. In Jacques Carette, David Aspinall, Christoph Lange, Petr Sojka, and Wolfgang Windsteiger, editors, *Intelligent Computer Mathematics - MKM, Calculemus, DML, and Systems and Projects 2013, Held as Part of CICM 2013, Bath, UK, July 8-12, 2013. Proceedings*, volume 7961 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2013. doi:10.1007/978-3-642-39320-4_1.

17 Assia Mahboubi and Enrico Tassi. Canonical structures for the working coq user. In Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving*, pages 19–34, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

18 Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Zenodo, January 2021. doi:10.5281/zenodo.4457887.

19 The mathlib Community. The Lean Mathematical Library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2020, page 367–381, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3372885.3373824.

20 R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer New York, 1987.

21 P. Ruffini. *Teoria generale delle equazioni: in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grad superiore al quarto*. Number pt. 1 in Nineteenth Century Collections Online (NCCO): Science, Technology, and Medicine: 1780-1925. Nella stamperia di S. Tommaso d'Aquino, 1799.

22 Amokrane Saibi. Typing algorithm in type theory with inheritance. In *Proceedings of the 24th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 292–301, 1997.

23 Christoph Schwarzweller. On roots of polynomials over F[X]/(p). *Formaliz. Math.*, 27(2):93–100, 2019. doi:10.2478/forma-2019-0010.

24 Nicolas Tabareau, Éric Tanter, and Matthieu Sozeau. Equivalences for free: univalent parametricity for effective transport. *Proc. ACM Program. Lang.*, 2(ICFP):92:1–92:29, 2018. doi:10.1145/3236787.

25 The Mathematical Components Team. The Mathematical Components library. https://github.com/math-comp/math-comp, 2007.

26 The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. https://homotopytypetheory.org/book, Institute for Advanced Study, 2013.