



HAL
open science

Unsolvability of the Quintic Formalized in Dependent Type Theory

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

► **To cite this version:**

Sophie Bernard, Cyril Cohen, Assia Mahboubi, Pierre-Yves Strub. Unsolvability of the Quintic Formalized in Dependent Type Theory. ITP 2021 - 12th International Conference on Interactive Theorem Proving, Jun 2021, Rome / Virtual, France. hal-03136002v2

HAL Id: hal-03136002

<https://inria.hal.science/hal-03136002v2>


Submitted on 20 Apr 2021 (v2), last revised 2 May 2021 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

1 **Unsolvability of the Quintic Formalized in** 2 **Dependent Type Theory**

3 **Sophie Bernard** ✉
4 Université Côte d’Azur, Inria, France

5 **Cyril Cohen** ✉ 🏠 
6 Université Côte d’Azur, Inria, France

7 **Assia Mahboubi** ✉
8 Inria, France
9 Vrije Universiteit Amsterdam, The Netherlands

10 **Pierre-Yves Strub** ✉
11 École polytechnique, France

12 — **Abstract** —

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

18 **2012 ACM Subject Classification** Theory of computation → Type theory; Theory of computation
19 → Logic and verification; Theory of computation → Constructive mathematics

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

22 **Digital Object Identifier** 10.4230/LIPIcs.ITP.2021.3

23 **Supplementary Material** <https://github.com/math-comp/Abel> version 1.1.2.

24 **1** **Introduction**

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

36 In fact, we developed a formal proof of the more general theorem – attributed to Galois [9]
37 in his memoir from 1830 – which provides an explicit necessary and sufficient condition
38 for the existence of solutions by radical, and we also formalize an example of non-solvable
39 quintic, obtained as a corollary of the latter. This Galois theorem is an emblematic result of
40 Galois theory, which studies field extensions of commutative fields via a correspondence with
41 groups of permutations of roots of polynomials.

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



© Sophie Bernard and Cyril Cohen and Assia Mahboubi and Pierre-Yves Strub;
licensed under Creative Commons License CC-BY 4.0

12th International Conference on Interactive Theorem Proving (ITP 2021).

Editors: Liron Cohen and Cezary Kaliszyk; Article No. 3; pp. 3:1–3:18

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

44 Components library [25], for the purpose of the formal proof of the Odd Order theorem [12].
 45 As there is no published description of this material, we provide where needed a description
 46 of the material from this contribution that we rely on.

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

51 **2** Background and outline

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

115 **3 Formal definitions**

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

120 In fact, we also assume this extension to be *normal*, that is, that L is the splitting field
 121 of a certain polynomial in $F_0[X]$. We will thus use letters E, F, K for sub-fields of L that are
 122 themselves extensions over F_0 . This formalization choice can be compared to the use of an
 123 ambient `finGroupType` in the formalization of finite group theory [12, 16].

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

```
126 Variables (F0 : fieldType) (L : splittingFieldType F0).
127 Implicit Types (E F K : {subfield L}).
128
```

3:4 A Coq proof of Abel – Ruffini theorem

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

133 Of course, when F/E is itself a field extension, it remains possible to see F as a vector
 134 space over E : for instance `\dim_E F` refers to the dimension of F as a vector space over E , i.e.,
 135 to the degree $[F : E]$ of the extension. Note that as a rule of thumb, notations are designed
 136 so as to be well-formed as often as possible. For example, `\dim_E F` is actually defined as
 137 the Euclidean quotient of $[F : F_0]$ by $[E : F_0]$, and thus does not require `E` to be included
 138 in `F`. These formalization choices, inherited from the design of the `Mathematical Components`
 139 library for linear algebra [11], significantly contribute to reduce the bureaucratic workload in
 140 proofs.

141 In this work, we benefit from the formalized basic concepts and results in Galois theory
 142 available in the `Mathematical Components` library [12], notably from the available proof of the
 143 fundamental theorem of Galois theory. The corresponding libraries actually introduce the
 144 vocabulary related to field extensions and Galois groups. In particular, `'Gal(F/E)` refers to
 145 the Galois group of a field extension F/E . Here as well, this notation is well formed for any
 146 `E, F : {subfield L}`, regardless of any inclusion property, and actually refers to $\text{Gal}(F/E \cap F)$
 147 and is a group, regardless of whether F/E is a Galois extension.

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

4 From solvable Galois groups to solvable extensions

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

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

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

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

```
164 Lemma abelian_radical_ext w E F (n := \dim_E F) : n.-primitive_root w →  

  165 w \in E → galois E F → abelian 'Gal(F / E) → radical.-ext E F.
```

168 **Proof.** The proof goes by exhibiting a basis (r_i) of F , seen as a vector space over E , such
 169 that for any u in $G = \text{Gal}(F/E)$ and for any $i \in \{1, \dots, n\}$, $u(r_i) = \lambda r_i$, where λ is some n^{th}
 170 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
 171 the proof.

172 Let u be an element of G . Since $|G| = [F : E] = n$, by Lagrange's theorem of finite group
 173 theory, we have $u^n = \text{id}$. Therefore the minimal polynomial of u in E divides the polynomial
 174 $X^n - 1$. But since the latter is square-free and splits over E (for E contains a primitive n^{th}
 175 root of unity), so is the minimal polynomial of u , and u is thus diagonalizable. Moreover,
 176 since G is abelian, all its elements are co-diagonalizable. As a consequence, there exists a

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

■ **Figure 1** Correspondence between Coq syntax and mathematical vocabulary

3:6 A Coq proof of Abel – Ruffini theorem

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

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

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

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

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

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

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

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

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

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

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

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

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

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


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

224 Since F/E is a Galois extension, then so is $FE(\omega)/E(\omega)$. Let m be the degree of
 225 $FE(\omega)/E(\omega)$. By Lemma 6, $\text{Gal}(FE(\omega)/E(\omega))$ is isomorphic to $\text{Gal}(F/F \cap E(\omega))$, which is
 226 thus of order m as well. But since $\text{Gal}(F/F \cap E(\omega))$ is a subgroup of $\text{Gal}(F/E)$, its order m
 227 divides n , the order of $\text{Gal}(F/E)$. Consider $\omega' = \omega^{\frac{n}{m}}$. It is an element of $E(\omega)$, and thus of
 228 $FE(\omega)$, and a primitive root of unity. We can apply Lemma 5 on the extension $FE(\omega)/E(\omega)$,
 229 and the m^{th} primitive root of unity ω' as soon as we show that $\text{Gal}(FE(\omega)/E(\omega))$ is solvable.
 230 Which is the case because it is isomorphic to $\text{Gal}(F/F \cap E(\omega))$, itself solvable as a subgroup
 231 of $\text{Gal}(F/E)$. ◀

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

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

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

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

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

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

```
246 Lemma ext_solvable_by_radical w E F (n := \dim_E (normalClosure E F)) :
247 n.-primitive_root w → solvable_ext E F → solvable_by_radical E F.
```

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

253 5 From solvable by radicals extensions to solvable extensions

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

258 ▶ **Lemma 12.** Suppose that L contains ω , an n^{th} primitive root of unity for n a positive
 259 integer. Consider E a sub-field of L and $x \in L$ such that $x^n \in E$. Then, the extension
 260 $E(\omega, x)/E$ is Galois. In particular if $\omega \in E$, then $E(x)/E$ is Galois.

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


3:8 A Coq proof of Abel – Ruffini theorem

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

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

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

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

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

```
275 Lemma minPoly_pradical (p : nat) (w x : L) (E : {subfield L}):
276   p.-primitive_root w → prime p → w \in E → x \notin E → x ^+ p \in E →
277   minPoly E x = 'X^p - (x ^+ p)%:P.
278
```

280 **Proof.** Let $P \in E[X]$ be the minimal polynomial of x over E . By minimality, P divides
 281 any polynomial over E that cancels x . In particular, P divides $X^p - x^p = \prod_{i < p} (X - x\omega^i)$.
 282 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
 283 x , S contains x , therefore $|S|$ is positive. It suffices to show $|S| \geq p$, because then $S = I_p$
 284 and $P = X^p - x^p$. Since $|S|$ is positive, it is sufficient to prove that p divides $|S|$.

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

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

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

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

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

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

```
299 Lemma map_gal_inj : 'injm (map_gal iota).
300 Lemma img_map_gal : map_gal iota @* 'Gal(F / E) = 'Gal(iota @: F / iota @: E).
302
```

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

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

```

308 Lemma normalField_aimg : normalField (iota @: E) (iota @: F) = normalField E F.
309 Lemma separable_aimg : separable (iota @: E) (iota @: F) = separable E F.
310 Lemma galois_aimg : galois (iota @: E) (iota @: F) = galois E F.
311 Lemma solvable_ext_aimg : solvable_ext (iota @: E) (iota @: F) = solvable_ext E F.
312 Lemma aimg_normalClosure :
313   iota @: normalClosure E F = normalClosure (iota @: E) (iota @: F).
314

```

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

319 ► **Lemma 16.** *Let L/F_0 be an ambient normal field extension and n a natural number
 320 coprime with the characteristic of F_0 . There is an ambient normal field extension L'/F_0 ,
 321 a primitive n^{th} root of unity $\omega \in L'$ and an F_0 -algebra morphism $\iota : L \rightarrow L'$, such that
 322 $\iota(L)(\omega) = L'$.*

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

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

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

```

328 Lemma radical_solvable_ext (p : nat) (x : L) (E : {subfield L}) :
329   prime p → p != 0 => FO → x ^+ p \in E → solvable_ext E <<E; x>>.
330

```

332 **Proof.** Without loss of generality, we can assume the existence of $\omega \in L$ a primitive p^{th} root
 333 of unity. Indeed, Lemma 16 gives the existence of a field extension L' and an embedding
 334 $\iota : L \rightarrow L'$, where L' contains a p^{th} primitive root of unity (since $p \neq 0$ in F_0). Now we may
 335 prove $\iota(E(x))/\iota(E)$ is Galois and “transfer” the result to $E(x)/E$ using Lemma 15.

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

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

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

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

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

3:10 A Coq proof of Abel – Ruffini theorem

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

```
355 Lemma radical_ext_solvable_ext (E F : {subfield L}) : has_char0 L → E ≤ F →  
356 solvable_by_radical E F → solvable_ext E F.  
357
```

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

363 Note that this proof goes by induction on the length of the tower. Curiously, some
364 references (such as the French wikipedia page on the Abel-Ruffini Theorem as of 2021-04-20)
365 do not rely on solvable extensions, or define it as “being Galois and solvable” instead of
366 “having a Galois field extension that is solvable”. Unfortunately, under such variations, we
367 lack a transitivity property analogue to Lemma 18, which dooms to failure any attempt
368 of a similar proof by induction. Actually, we conjecture¹ that there is a tower of cyclic
369 extensions of height two $\mathbb{Q}^{\text{ab}} \subset K \subset L$ where both K/\mathbb{Q}^{ab} and L/K are simple radical
370 Galois extensions, but where L/\mathbb{Q}^{ab} is not Galois (even though \mathbb{Q}^{ab} contains all roots of
371 unity). Such a counterexample would imply that any proof by induction where the induction
372 hypothesis has the form “ E_n/E_0 is Galois and [...]” is bound to fail.

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

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

384 6 Galois and Abel-Ruffini theorems

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

388 6.1 Galois’ theorem

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

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

¹ <https://mathoverflow.net/questions/381824>

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

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

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

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

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

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

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

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

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

425 6.2 Irreducible rational polynomials of Prime Degree with exactly Two 426 Non Real Roots

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

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

435 **Proof.** Let $P \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p , a sequence $s = (s_i)_i$ of
 436 its roots, and $G = \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ its Galois group. We define a group morphism $\varphi : G \rightarrow \mathfrak{S}_p$,
 437 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
 438 group of P to a permutation of the indices of the sequence s that is compatible with the
 439 action of u on the roots s of P . Now, it suffices to show that φ is injective and surjective to
 440 conclude.

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

3:12 A Coq proof of Abel – Ruffini theorem

- 444 ■ φ is surjective: it suffices to show that there is a transposition τ and an element of order
- 445 p in $\varphi(G)$. Indeed, since p is prime number we have $\mathfrak{S}_p = \langle \tau, c \rangle$.
- 446 ■ Since P has exactly two non real roots, there are $i < j < p$ such that, $s_i = s_j^*$ and
- 447 $s_k = s_k^*$ if $k \notin \{i, j\}$. The complex conjugation (\cdot^*) belongs to G and $\varphi(\cdot^*) = (i\ j) = \tau$.
- 448 ■ The natural number p divides $[\mathbb{Q}(P) : \mathbb{Q}]$ because P is irreducible. Since p is prime
- 449 and divides G , by Cauchy's theorem, there is an element of order p in G .
- 450 ◀

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

454 6.3 $X^5 - 4X + 2$ is not solvable by radicals

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

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

```
458 Theorem example_not_solvable_by_radicals :
459   ¬ solvable_by_radical_poly ('X^5 - 4 *: 'X + 2 : {poly rat}).
460
```

462 **Proof.** By Theorem 2, it suffices to show the galois group of $\mathbb{Q}(Q)/\mathbb{Q}$ is not solvable, where
 463 $Q = X^5 - 4X + 2$.

- 464 ■ By Lemma 21, it suffices to show Q is irreducible and has exactly two non real roots.
- 465 Irreducibility is directly given by Eisenstein criterion. Q has at least three real roots
- 466 in \mathbb{Q} because there are at least three sign changes: $Q(-2)Q(-1) < 0$, $Q(-1)Q(1) < 0$,
- 467 and $Q(1)Q(2) < 0$. Finally since the derivative $Q' = 5X^4 - 4$ has exactly two real roots
- 468 $(\pm\sqrt{\frac{2}{5}})$, it means Q has at most three real roots, hence exactly three.
- 469 ■ To show \mathfrak{S}_5 is not solvable it suffices to show its normal subgroup \mathfrak{A}_5 is not solvable
- 470 either. We conclude by contradiction with the fact that \mathfrak{A}_5 is simple of order $5 \times 4 \times 3$
- 471 and a simple solvable group must have prime order.
- 472 ◀

473 7 Solvability by radicals is what you think

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

478 More formally, for a field F , we define the grammar of radical expressions \mathbb{E}_F over F as
 479 the set of terms that can be recursively defined from the symbols $0, 1, x \in F, +, -, *, \cdot^{-1},$
 480 $\sqrt[n]{\cdot}$ 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
 481 unity):

$$482 \quad e \in \mathbb{E} ::= 0 \mid 1 \mid e_1 + e_2 \mid -e \mid e_1 * e_2 \mid e^{-1} \mid \sqrt[n]{e} \mid \omega_n \quad (n \in \mathbb{N}^*)$$

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

```

486 Variables (F : fieldType) (iota : F → algC).
487 Fixpoint algT_eval (f : algterm F) : algC :=
488   match f with
489   | Base x      => iota x
490   | 0          => 0
491   | 1          => 1
492   | f1 + f2    => algT_eval f1 + algT_eval f2
493   | - f        => - algT_eval f
494   | f1 * f2    => algT_eval f1 * algT_eval f2
495   | f ^-1      => (algT_eval f)^-1
496   | f ^+ n     => (algT_eval f) ^+ n
497   | n.+1-root f => n.+1.-root (algT_eval f)
498   | j.+1-primroot => primroot j.+1
499   end.
500

```

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

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

```

508 Lemma solvable_formula (p : {poly rat}) : p != 0 →
509   solvable_by_radical_poly p ↔
510   {in root (p ^^ ratr), ∀ x, ∃ f : algterm rat, algR_eval ratr f = x}.
511

```

513 8 Classical reasoning in a constructive setting

514 8.1 Boolean reflection and effective Galois theory

515 The present contribution takes over the main design choices deployed in `Mathematical`
516 `Components` library, and in particular its use of boolean reflection [18] for formalizing effective
517 mathematics. Notably, the defining signature of algebraic structures, like rings or fields,
518 involve boolean predicates, e.g., for comparison or discrimination of units. More generally,
519 decidable predicates, that is predicates for which excluded-middle holds constructively,
520 are formalized as boolean predicates. Consequently, equivalences between such boolean
521 propositions are stated as equalities, as for instance in Lemma 15. Besides often saving the
522 user from the technicalities of setoid rewriting, boolean specifications are provably proof-
523 irrelevant, by Hedberg’s theorem [14], and this feature is extensively used for defining and
524 using proof-irrelevant dependent pairs.

525 The present development heavily relies on the effective perspective provided by the
526 underlying linear algebra component [11]. In this library, vector spaces of finite dimension
527 and their sub-spaces, always come with an explicit basis, and are in fact internally represented
528 as matrices. This way, most properties of linear algebra in finite dimension are effective,
529 thanks to variants of Gaussian elimination: computing the dimension of a sub-space, testing
530 whether a family of vectors is free, whether it generates a given sub-space, testing the inclusion
531 or the equality between sub-spaces, etc. When a larger vector space is in fact an algebra
532 (resp. a field extension) over a given base field, it is decidable whether a given subspace is in
533 fact a sub-algebra U (resp. a sub-field U): it suffices to test whether pairwise products of
534 elements of the basis of U belong to U . Note however that effectivity does not mean that
535 the computations are necessarily tractable in practice: turning these effective definition into
536 formally verified algebra that can be executed on concrete entries would require a non-trivial
537 additional effort [8, 24].

3:14 A Coq proof of Abel – Ruffini theorem

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

544 8.2 Non-effective results

545 However, important properties in commutative algebra, such as testing a polynomial in
546 $F[X]$ for irreducibility for F an arbitrary field, remain non-effective, even in the case of a
547 field F with a decidable equality. As a consequence, in a constructive setting, some facts
548 like Lemma 16 cannot be proved as such. The way out is to change their statement for a
549 classically equivalent one, typically, a double-negated version, so as to restore constructive
550 provability. For this purpose, we use the `classically` monadic predicate [12]: for any $P : \text{Prop}$,
551 `classically P` is equivalent to the double-negation $\neg(\neg P)$. For instance, the construction of a
552 larger normal field extension performed in Lemma 16 is not effective in general. Here is a
553 typical example of non-effective statement:

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

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

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

567 8.3 Stating Galois' theorem in characteristic zero

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

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

```
575 Theorem AbelGalois (F0 : fieldType) (L : splittingFieldType F0) (w : L)  
576 (E F : {subfield L}) : (E ≤ F) -> has_char0 L ->  
577 (\dim_E (normalClosure E F)).-primitive_root w ->  
578 solvable_by_radical E F ↔ solvable_ext E F.
```

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

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

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

598 **9 Conclusion**

599 **Comparison to related formalization in Coq**

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

607 These hierarchies are designed using Coq’s canonical structures mechanism [22], more
 608 precisely with the packed class methodology [10], in order to achieve ad-hoc polymorphism [13,
 609 17]. This inference mechanism is crucial to combine the different components of the library:
 610 finite group theory, linear algebra, theory of field extensions and Galois theory. Inference of
 611 structures is used at almost every single line of code and its efficiency is crucial for making
 612 amenable such a development.

613 **Comparison to related formalization in other systems**

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

618 A formalization of field extensions and algebraic closure [7] was carried out in the
 619 `Isabelle/HOL` theorem prover. Despite the lack of dependent types, this library comes with a
 620 definition of the algebraic closure of an abstract field as opposed to the a more elementary
 621 construction for a fixed field such as \mathbb{Q} . However, it is unclear whether the methodology used
 622 there can be further extended for the formalization of Galois theory. At least, dependent
 623 types play a central role in the design choices at stake in the present development.

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

625 Last, there exists an unfinished development related to the formalization of Galois theory
 626 and unsolvability of the quintic in `LEGO` [2]. However, only the unsolvability of the symmetric
 627 group [4] has been formally addressed.

628 **Comparison to the pen and paper literature**

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

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

640 The proof of unsolvability of $X^5 - 4X + 2$ involves counting its real roots. The most common
 641 way of doing this relies on building *sign tables*. However, the **Mathematical Components**
 642 library does not give any formal treatment of sign tables and we had to roll out our own
 643 solution. Fortunately, the **MathComp-Real-Closed** [6] library provides results related to the
 644 study of the variations of a polynomial with coefficients in an algebraically closed field. This
 645 allowed us to give lower and upper bounds on the number of reals without having to formalize
 646 sign tables. However, we expect that a formal treatment of sign tables to be a useful addition
 647 to the **Mathematical Components** library.

648 On the same subject, the library **MathComp-Real-Closed** contains a quantifier elimination
 649 procedure and a root counting procedure. In theory, in order to obtain the number of real
 650 roots, it would have been possible to simply run this procedure on the targeted polynomial.
 651 However, in practice, due to the very inefficient nature of the involved datatypes (starting
 652 from the use of unary natural numbers), the methodology proved to be too inefficient. A
 653 possible future work would be to extend COQEAL [8, 5] to make effective these procedures.

654 **The case of positive characteristic**

655 Even if a large part of our development is independent from the characteristic of the fields
 656 under consideration, for the sake of simplifying, we sometime restricted ourselves to the case
 657 of characteristic zero – as this is the case in the file `abel.v` for example. For instance, we
 658 specialized the notion of radical extension to fields of characteristic zero, which is enough to
 659 show the unsolvability of a polynomial over \mathbb{Q} . However, we expect that the zero-characteristic
 660 assumption could be dropped in the near future. For example, the definition of radical
 661 extensions in a field of an arbitrary characteristic p could be generalized by following the
 662 definition from Lang [15, VI, §7, Remark], thus adding a second kind of radical extensions
 663 $K(a)/K$ such that $a^p - a \in K$. The proof that cyclic extensions of degree p are of that form
 664 would then rely on the additive version of Hilbert Theorem 90. (The multiplicative version
 665 is already formalized – it could be used in place of Lemma 4 – and we do not expect any
 666 difficulty in formalizing its additive counterpart.)

667 **Reasoning up to isomorphisms**

668 A substantial amount of proof scripts is devoted to the transfer of properties from one object
 669 to an isomorphic one (See Lemma 15 for an example). This part is largely left implicit on
 670 paper and it is indeed quite mundane. It would be interesting to see if the ongoing work
 671 around *Homotopy Type Theory* [26, 24, 3] could apply here.

672 ——— **References** ———

- 673 1 Niels Henrik Abel. *Œuvres complètes de Niels Henrikl Abel, mathématicien*. C. Gröndahl,
674 1881. URL: <https://www.abelprize.no/c54178/artikkel/vis.html?tid=54181>.
- 675 2 Peter Aczel. Galois: a theory development project. *manuscript*, University of Manchester,
676 1993.
- 677 3 Carlo Angiuli, Evan Cavallo, Anders Mörtberg, and Max Zeuner. Internalizing representation
678 independence with univalence. *Proc. ACM Program. Lang.*, 5(POPL), January 2021. doi:
679 10.1145/3434293.
- 680 4 Gilles Barthe. A formal proof of the unsolvability of the symmetric group over a set with five
681 or more elements.
- 682 5 Cyril Cohen, Maxime Dénès, and Anders Mörtberg. Refinements for Free! In *Certified*
683 *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.
- 684 6 Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered
685 fields to quantifier elimination. *Logical Methods in Computer Science*, 8(1:02):1–40, February
686 2012. URL: <https://hal.inria.fr/inria-00593738>, doi:10.2168/LMCS-8(1:02)2012.
- 687 7 Paulo Emilio de Vilhena and Lawrence C. Paulson. Algebraically closed fields in isabelle/hol.
688 In Nicolas Peltier and Viorica Sofronie-Stokkermans, editors, *Automated Reasoning*, pages
689 204–220, Cham, 2020. Springer International Publishing.
- 690 8 Maxime Dénès, Anders Mörtberg, and Vincent Siles. A refinement-based approach to com-
691 putational algebra in COQ. In Lennart Berlinger and Amy Felty, editors, *ITP - 3rd Inter-*
692 *national Conference on Interactive Theorem Proving - 2012*, volume 7406 of *Lecture Notes*
693 *In Computer Science*, pages 83–98, Princeton, United States, August 2012. Springer. URL:
694 <https://hal.inria.fr/hal-00734505>, doi:10.1007/978-3-642-32347-8_7.
- 695 9 Evariste Galois. *Mémoire sur les conditions de résolubilité des équations par radicaux.*,
696 volume XI of *Journal de mathématiques pures et appliquées*. Joseph Liouville, 1846.
697 URL: [https://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_](https://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubiblite.pdf)
698 [resolubiblite.pdf](https://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubiblite.pdf).
- 699 10 François Garillot, Georges Gonthier, Assia Mahboubi, and Laurence Rideau. Packaging
700 Mathematical Structures. working paper or preprint, March 2009. URL: [https://hal.inria.](https://hal.inria.fr/inria-00368403)
701 [fr/inria-00368403](https://hal.inria.fr/inria-00368403).
- 702 11 Georges Gonthier. Point-Free, Set-Free Concrete Linear Algebra. In Marko C. J. D. van
703 Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem*
704 *Proving - ITP 2011*, volume 6898 of *Lecture Notes in Computer Science*, pages 103–118,
705 Berg en Dal, Netherlands, August 2011. Radboud University of Nijmegen, Springer. URL:
706 <https://hal.inria.fr/hal-00805966>, doi:10.1007/978-3-642-22863-6_10.
- 707 12 Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot,
708 Stéphane Le Roux, Assia Mahboubi, Russell O’Connor, Sidi Ould Biha, Ioana Pasca, Laurence
709 Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of
710 the Odd Order Theorem. In Sandrine Blazy, Christine Paulin, and David Pichardie, editors,
711 *ITP 2013, 4th Conference on Interactive Theorem Proving*, volume 7998 of *LNCS*, pages
712 163–179, Rennes, France, July 2013. Springer. URL: <https://hal.inria.fr/hal-00816699>,
713 doi:10.1007/978-3-642-39634-2_14.
- 714 13 Georges Gonthier, Beta Ziliani, Aleksandar Nanevski, and Derek Dreyer. How to make
715 ad hoc proof automation less ad hoc. *SIGPLAN Not.*, 46(9):163–175, September 2011.
716 doi:10.1145/2034574.2034798.
- 717 14 Michael Hedberg. A coherence theorem for Martin-Löf’s Type Theory. *J. Funct. Program.*,
718 8(4):413–436, July 1998. URL: <http://dx.doi.org/10.1017/S0956796898003153>, doi:10.
719 1017/S0956796898003153.
- 720 15 Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.
- 721 16 Assia Mahboubi. The rooster and the butterflies. In Jacques Carette, David Aspinall, Christoph
722 Lange, Petr Sojka, and Wolfgang Windsteiger, editors, *Intelligent Computer Mathematics -*
723

- 724 *MKM, Calculemus, DML, and Systems and Projects 2013, Held as Part of CICM 2013, Bath,*
 725 *UK, July 8-12, 2013. Proceedings*, volume 7961 of *Lecture Notes in Computer Science*, pages
 726 1–18. Springer, 2013. doi:10.1007/978-3-642-39320-4_1.
- 727 **17** Assia Mahboubi and Enrico Tassi. Canonical structures for the working coq user. In Sandrine
 728 Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving*,
 729 pages 19–34, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
- 730 **18** Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Zenodo, January 2021. doi:
 731 10.5281/zenodo.4457887.
- 732 **19** The mathlib Community. The lean mathematical library. In *Proceedings of the 9th ACM*
 733 *SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020*, page
 734 367–381, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/
 735 3372885.3373824.
- 736 **20** R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra*. Universitext.
 737 Springer New York, 1987.
- 738 **21** P. Ruffini. *Teoria generale delle equazioni: in cui si dimostra impossibile la soluzione algebrica*
 739 *delle equazioni generali di grad superiore al quarto*. Number pt. 1 in Nineteenth Century
 740 Collections Online (NCCO): Science, Technology, and Medicine: 1780-1925. Nella stamperia
 741 di S. Tommaso d’Aquino, 1799.
- 742 **22** Amokrane Saibi. Typing algorithm in type theory with inheritance. In *Proceedings of the 24th*
 743 *ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 292–301,
 744 1997.
- 745 **23** Christoph Schwarzweiler. On roots of polynomials over $F[X]/(p)$. *Formaliz. Math.*, 27(2):93–100,
 746 2019. doi:10.2478/forma-2019-0010.
- 747 **24** Nicolas Tabareau, Éric Tanter, and Matthieu Sozeau. Equivalences for free: univalent
 748 parametricity for effective transport. *Proc. ACM Program. Lang.*, 2(ICFP):92:1–92:29, 2018.
 749 doi:10.1145/3236787.
- 750 **25** The Mathematical Components Team. The Mathematical Components library. <https://github.com/math-comp/math-comp>, 2007.
 751
- 752 **26** The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of*
 753 *Mathematics*. <https://homotopytypetheory.org/book>, Institute for Advanced Study, 2013.