Unsolvability of the Quintic Formalized in Dependent Type Theory

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

Thierry Coquand's 60th Birthday Workshop
August 26th, 2022

Abel-Ruffini's Theorem

Question: **« Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »**

Abel-Ruffini's Theorem

Question: **« Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »**

Cardan and Ferrari ($\sim$ 1550) methods provide general solutions respectively for degrees 3 and 4.

Abel-Ruffini's Theorem

Question: **« Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »**

Cardan and Ferrari ($\sim$ 1550) methods provide general solutions respectively for degrees 3 and 4.

The answer for degree 5 is **no**, this is **Abel-Ruffini's theorem.**

- it is attributed to Abel for his work published in 1826.
- Ruffini is credited for a first formulation and proof in 1799.

Abel-Ruffini's Theorem

Question: « Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

Abel-Ruffini's Theorem

Question: « Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

The answer is provided by Galois's Theorem:
« If and only if the Galois group of the polynomial is solvable »

Abel-Ruffini's Theorem

Question: « Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

The answer is provided by Galois's Theorem:
« If and only if the Galois group of the polynomial is solvable »

In particular, to show Abel-Ruffini's theorem from Galois' Theorem, it suffices to exhibit one polynomial of degree 5 with unsolvable Galois Group.

Abel-Ruffini's Theorem

Question: « Is it possible to write roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

The answer is provided by Galois's Theorem:
« If and only if the Galois group of the polynomial is solvable »

In particular, to show Abel-Ruffini's theorem from Galois' Theorem, it suffices to exhibit one polynomial of degree 5 with unsolvable Galois Group.

It thus suffices to prove that $X^5 - 4X + 2$ *has Galois group* $\mathfrak{S}_5$*, which is unsolvable.*

The formal development

The formal development contains the following end-results:

- Galois's Theorem: the equivalence between solvability by radicals and having a solvable Group.
- Abel-Ruffini's Theorem: $X^5 - 4X + 2$ has Galois group $\mathfrak{S}_5$, which is unsolvable.
- The fact that *solvability by radicals* corresponds to « writing roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

The formal development

The formal development contains the following end-results:

- Galois's Theorem: the equivalence between solvability by radicals and having a solvable Group.
- Abel-Ruffini's Theorem: $X^5 - 4X + 2$ has Galois group $\mathfrak{S}_5$, which is unsolvable.
- The fact that *solvability by radicals* corresponds to « writing roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

All our proofs are constructive: **solvability by radicals is decidable**.

The formal development

The formal development contains the following end-results:

- Galois's Theorem: the equivalence between solvability by radicals and having a solvable Group.
- Abel-Ruffini's Theorem: $X^5 - 4X + 2$ has Galois group $\mathfrak{S}_5$, which is unsolvable.
- The fact that *solvability by radicals* corresponds to « writing roots of polynomials solely with addition, subtraction, product, division and n^{th} roots? »

All our proofs are constructive: **solvability by radicals is decidable**.

In this talk, we only consider polynomials with coefficients in $\mathbb{Q}$, which entails: « normal extensions » = « Galois extensions ».

Formalization setup

We use the Coq proof assistant together with the Mathematical Components library.

The latter already contained many results about finite group theory, linear algebra and Galois theory (and much more).

Figure 1. of the paper
`https://hal.inria.fr/hal-03136002/document`
gives a condensed translation between Mathematical Components notations and mathematical concepts.

Statement of Abel-Ruffini's theorem

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

Statement of Abel-Ruffini's theorem

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

---

where `solvable_by_radical_poly p` is equivalent to

```
{L : splittingFieldType rat &
  {iota : {rmorphism L -> algC} & { rs : seq L |
    p ^^ in_alg L %= \prod_(x <- rs) ('X - x%:P) /\
    solvable_by radical 1 <<1 & rs>>}}}.
```

Statement of Abel-Ruffini's theorem

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

---

where `solvable_by_radical_poly p` is equivalent to

```
{L : splittingFieldType rat &
  {iota : {rmorphism L -> algC} & { rs : seq L |
    p ^^ in_alg L %= \prod_(x <- rs) ('X - x%:P) /\
    solvable_by radical 1 <<1 & rs>>}}}.
```

---

where we reuse MATHEMATICAL COMPONENTS concepts:

- `splittingFieldType rat` is the type of normal field extension of $\mathbb{Q}$
- `{rmorphism L -> algC}` is the type of ring morphisms to $\overline{\mathbb{Q}}$
- `1` is the base field (here the embedding of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$)
- `<<1 & v>>` is the field extension $\mathbb{Q}(v_0, \ldots, v_n)$

Solvability 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 $F_0 \subseteq \ldots \subseteq F_n$ 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 $K = F_0 \subseteq \ldots \subseteq F_n = F$.

It is a *solvable by radicals extension* if there is a radical extension E/K such that $F \subseteq E$.

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

Statement of Galois' theorem

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

---

where we reuse Mathematical Components concepts:

- `{poly F}` is the type of polynomials over F,
- `solvable G` means the group G is solvable,
- `'Gal( F / E )` is the Galois Group of the field extension F/E
- `1` is the base field (here the embedding of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$)
- `{: numfield p}` is the number field $\mathbb{Q}(p) \subseteq \overline{\mathbb{Q}}$.

The polynomial $X^5 - 4X + 2$

We show

```
Lemma isog_gal :
  'Gal ({:numfield p} / 1) \isog 'Sym_('I_d).
```

---

when the polynomial `p` has prime degree `d` and two non real roots.

The polynomial $X^5 - 4X + 2$

We show

```
Lemma isog_gal :
  'Gal ({:numfield p} / 1) \isog 'Sym_('I_d).
```

---

when the polynomial `p` has prime degree `d` and two non real roots.

We study the sign variations of $X^5 - 4X + 2$ to show it indeed has at least three real roots, and its derivative to show it has at most three.

The polynomial $X^5 - 4X + 2$

We show

```
Lemma isog_gal :
  'Gal ({:numfield p} / 1) \isog 'Sym_('I_d).
```

---

when the polynomial `p` has prime degree `d` and two non real roots.

We study the sign variations of $X^5 - 4X + 2$ to show it indeed has at least three real roots, and its derivative to show it has at most three.

Finally we show the symmetric group of a type of cardinality greater than 4 is never solvable:

```
Lemma solvable_SymF : 4 < #|T| -> solvable 'Sym_T =
    false.
```

Making sure `solvable_by_radicals` is what we mean

```
Lemma solvable_formula (p : {poly rat}) : p != 0 ->
  solvable_by_radical_poly p <->
  {in root (p ^^ ratr), forall x,
     exists f : algterm rat, algT_eval ratr f = x}.
```

Where

```
Fixpoint algT_eval (f : algterm F) := 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.
```

Focus: « solvable by radicals $\Rightarrow$ solvable »

French wikipedia page:

- **Pour tout *i* de 1 à *k*, l'extension $K(\alpha_1, \dots, \alpha_i)$ de *K* est galoisienne et de groupe résoluble.**

  Notons F_i l'extension $K(\alpha_1, \dots, \alpha_i)$ de *K* et G_i son groupe de Galois.

  L'extension F_1 de *K* est cyclotomique, donc galoisienne et abélienne.

  Soit $i > 1$. Supposons que l'extension F_{i-1} de *K* est galoisienne et que G_{i-1} est résoluble. D'après le point précédent, l'extension F_i de F_{i-1} est galoisienne et de groupe *H* abélien. Par conséquent, l'extension F_i de *K* est galoisienne et G_i est résoluble, comme extension de G_{i-1} par *H*.

Focus: « solvable by radicals $\Rightarrow$ solvable »

French wikipedia page:

- **Pour tout *i* de 1 à *k*, l'extension $K(\alpha_1, \ldots, \alpha_i)$ de K est galoisienne et de groupe résoluble.**

  Notons F_i l'extension $K(\alpha_1, \ldots, \alpha_i)$ de K et G_i son groupe de Galois.
  L'extension F_1 de K est cyclotomique, donc galoisienne et abélienne.
  Soit $i > 1$. Supposons que l'extension F_{i-1} de K est galoisienne et que G_{i-1} est résoluble. D'après le point précédent, l'extension F_i de F_{i-1} est galoisienne et de groupe H abélien. Par conséquent, l'extension F_i de K est galoisienne et G_i est résoluble, comme extension de G_{i-1} par H.

But a Galois extension of a Galois extension is not necessarily Galois anymore (e.g. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$).

Focus: « solvable by radicals $\Rightarrow$ solvable »

French wikipedia page:

- **Pour tout *i* de 1 à *k*, l'extension $K(\alpha_1, \ldots, \alpha_i)$ de *K* est galoisienne et de groupe résoluble.**

  Notons F_i l'extension $K(\alpha_1, \ldots, \alpha_i)$ de *K* et G_i son groupe de Galois.
  L'extension F_1 de *K* est cyclotomique, donc galoisienne et abélienne.
  Soit $i > 1$. Supposons que l'extension F_{i-1} de *K* est galoisienne et que G_{i-1} est résoluble. D'après le point précédent, l'extension F_i de F_{i-1} est galoisienne et de groupe *H* abélien. Par conséquent, l'extension F_i de *K* est galoisienne et G_i est résoluble, comme extension de G_{i-1} par *H*.

But a Galois extension of a Galois extension is not necessarily Galois anymore (e.g. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$).
Books such *Algebra* (Lang 2003), fix this by defining a *Solvable extension* F/E as an extension such that there exists a Galois extension L/E of solvable Galois group. This makes the notion of solvable extension transitive (non trivial proof) and fixes the proof.

Focus: « solvable by radicals $\Rightarrow$ solvable »

In order to factor the code maximally when talking about solvable extensions, we had to introduce a function which is seldom introduced in the literature:

Definition

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.

This simplifies the definition and theory of solvable extensions:

Definition

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

Focus: « solvable by radicals $\Rightarrow$ solvable »

Other books do not necessarily introduce this notion of solvable extension. They ensure that all extensions stay Galois by adding to the original radical extensions additional elements at every layer. This is a very subtle process that his carefully described in many courses, and amounts to inlining the proof of transitivity of solvable extensions.

Focus: « solvable by radicals $\Rightarrow$ solvable »

Other books do not necessarily introduce this notion of solvable extension. They ensure that all extensions stay Galois by adding to the original radical extensions additional elements at every layer. This is a very subtle process that his carefully described in many courses, and amounts to inlining the proof of transitivity of solvable extensions.

Fun fact: even *Algebra* (Lang 2003) starts a proof by adding primitive roots of the unity to the original radical extension, while we show this is useless when using solvable extensions.

Focus: existence of splitting fields

Before specializing to the rationals, we actually proved a more general result:

```
Lemma AbelGaloisPoly (F : fieldType) (p : {poly F}) :
    has_char0 F ->
  solvable_ext_poly p <-> solvable_by_radical_poly p.
```

Then we encounter a problem that we worked around with Thierry in 2011 in *A constructive version of Laplace's proof on the existence of complex roots*: the left to right direction would require the construction of a splitting field of an arbitrary field, which is not constructive because irreducibility of polynomials is undecidable in general.

Focus: existence of splitting fields

constructively

Loose definition:

```
Definition solvable_by_radical_poly
    (F : fieldType) (p : {poly F}) :=
  forall (L : splittingFieldType F) (rs : seq L),
    p ^^ in_alg L %= \prod_(x <- rs) ('X - x%:P) ->
  forall w : L, (\dim <<1 & rs>>).-primitive_root w ->
      solvable_by radical 1 <<1 & rs>>.
```

Focus: existence of splitting fields

constructively

Loose definition:

```
Definition solvable_by_radical_poly
    (F : fieldType) (p : {poly F}) :=
  forall (L : splittingFieldType F) (rs : seq L),
    p ^^ in_alg L %= \prod_(x <- rs) ('X - x%:P) ->
  forall w : L, (\dim <<1 & rs>>).-primitive_root w ->
      solvable_by radical 1 <<1 & rs>>.
```

General theorem

```
  Lemma solvable_by_radical_polyP (F : fieldType)
    (p : {poly F}) : p != 0 -> has_char0 F ->
  solvable_by_radical_poly p <->
  classically (
    exists (L : splittingFieldType F) (rs : seq L),
      p ^^ in_alg L %= \prod_(x <- rs) ('X - x%:P) /\
      solvable_by radical 1 <<1 & rs>>).
```

Focus: existence of splitting fields

classically

```
Lemma classic_fieldExtFor (F0 : fieldType)
  (L : fieldExtType F0) (p : {poly L}) : p != 0 ->
  classically
  { L' : fieldExtType F0 & { rs : seq L' &
    { iota : 'AHom(L, L') |
      <<iota @: fullv & rs>> = fullv &
      p ^^ iota %= \prod_(r <- rs) ('X - r%:P) }}}.
```

`classically P := forall b : bool, (P -> b)-> b` was added to mathcomp by G. Gonthier (and R. O'Connor ?) in 2010 with this kind of application in mind in representation theory.

Focus: existence of splitting fields case on irreducibility

```
apply: classic_bind (@classic_EM (irreducible_poly p));
  case; last first.
```

Yields

```
  ============================
  ~ irreducible_poly p ->
  classically
    {L' : fieldExtType F0 &
    {rs : seq L' &
    {iota : 'AHom(L, L') | <<limg iota & rs>>%VS = fullv &
    p ^^ iota %= \prod_(r <- rs) ('X - r%:P)}}}

goal 2 (ID 4762) is:
 irreducible_poly p ->
 classically
   {L' : fieldExtType F0 &
   {rs : seq L' &
   {iota : 'AHom(L, L') | <<limg iota & rs>>%VS = fullv &
   p ^^ iota %= \prod_(r <- rs) ('X - r%:P)}}}
```

Focus: existence of splitting fields

leaving the monad

As soon as a goal is decidable.

```
classically
  {L' : splittingFieldType F0 & {w : L' &
  {iota : 'AHom(L, L') | <<limg iota; w>> = fullv &
      p.-primitive_root w}}} ->
solvable_ext E <<E; x>>
```

```
  L' : splittingFieldType F0
  w : L'
  f : 'AHom(L, L')
  wf : <<limg f; w>> = fullv
  rw : p.-primitive_root w
  ============================
  solvable_ext E <<E; x>>
```

Decidability of solvability of finite groups plays a big role in simplifying many statements...

Focus: changing fields

In the Mathematical Components library:

- Finite group theory is not about groups by about subgroups.
- Galois theory is not about fields but about sub-fields.

We have a base field ($\mathbb{Q}$) and a super-field extension L.
All extensions F/E are taken on subfields F and E of L.

Focus: changing fields

In the Mathematical Components library:

- Finite group theory is not about groups by about subgroups.
- Galois theory is not about fields but about sub-fields.

We have a base field ($\mathbb{Q}$) and a super-field extension L.
All extensions F/E are taken on subfields F and E of L.

Once in while, we need to extend the super-field L into L' (e.g. adjoining a root of the unity). We thus have theorems such as:

```
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.
```

Conclusion

- First formal proof of this theorem. It has been formalized in Lean since then.
- Spotted a few problems and/or detours in the literature.
  In particular, in the proof of « solvable by radicals $\Rightarrow$ solvable ».
- About 6000loc, among which $\sim$ 4500loc of reusable results to add to the Mathematical Components library.
- The case of positive characteristic is left out.
- We wonder whether techniques around HoTT would help with the few cases of reasoning up to isomorphism that we had.

The Mathematical Components library is available at `https://github.com/math-comp/math-comp/`.

The contents of the Abel-Ruffini repository `https://github.com/math-comp/Abel/` will be integrated gradually.

See `https://hal.inria.fr/hal-03136002/document` for more explanations.

Happy 61.35$^{\text{th}}$ Birthday Thierry!
Questions?