The Abel–Ruffini theorem and the unsolvability of the quintic

Lawrence C. Paulson

Abstract

This entry proves the *Abel–Ruffini theorem* — a polynomial equation solvable by radicals has a solvable Galois group — and applies it to a concrete quintic to conclude that the general quintic is not solvable by radicals. We follow the corresponding *mathlib* formalisation [2].

The forward direction — *solvable by radicals implies solvable Galois group* — is assembled on the session `New_Algebra`: cyclotomic and Kummer extensions have solvable (indeed abelian) Galois groups, solvability is preserved by the tower correspondence, and the normal closure of a radical tower is again a radical tower obtained by splicing the Galois conjugates of the original tower.

For the concrete witness we study the rational quintic $\Phi = x^5 - 4x + 2$ and show that the Galois group of its splitting field over $\mathbb{Q}$ is not solvable. We prove that Φ is irreducible over $\mathbb{Q}$ (Eisenstein's criterion at 2) and, using the AFP entry `Sturm_Sequences` [1], show that it has exactly three real roots and one conjugate pair of non-real roots. Complex conjugation therefore acts on the five roots as a transposition, while irreducibility makes the Galois action transitive; a transitive subgroup of S_5 containing a transposition is the whole of S_5, which is not solvable. Combining the two halves yields the headline result that Φ is not solvable by radicals.

Contents

1 Cyclotomic and Kummer extensions have abelian Galois groups 4

2 Roots of unity form a cyclic group 4

2.1 The set of nth roots of unity 4

2.2 The primitive root generates: powers exhaust the roots of unity . 4

2.3 Closure properties: a subgroup of the multiplicative group 5

2.4 Divisibility: fewer roots of unity sit among more 5

3 Cyclotomic and Kummer extensions have abelian Galois groups 6

3.1 Automorphisms map the carrier into itself 6

3.2 Abelian criterion for a simple normal extension 6

3.3 Cyclotomic extensions are abelian . . . 7
3.4 Kummer extensions are abelian . . . 7

4 The forward Abel–Ruffini direction: assembling the radical tower 8
4.1 A single radical step, with roots of unity present, is a full splitting field . . . 8
4.2 A Kummer step is both solvable and stable . . . 8
4.3 A cyclotomic step is solvable, stable, and supplies the roots of unity 9
4.4 A chain of Kummer steps is a solvable tower . . . 9
4.5 Solvability descends to a stable subfield with surjective restriction 10
4.6 The forward theorem . . . 11
4.7 From a roots-of-unity-free chain to a valid Kummer chain . . . 11
4.8 Extracting Kummer witnesses from a radical tower . . . 12
4.9 Extracting a nondegenerate witness list from a bare radical tower 13
4.10 A radical tower over a roots-of-unity base has a solvable Galois group . . . 14
4.11 Unconditional descent to a stable splitting subfield . . . 14

5 The normal radical closure of a radical tower 14
5.1 A Galois conjugate of a radical tower is a radical tower . . . 15
5.2 The family of all conjugates is a family of towers over the base . 15
5.3 The spliced tower's top contains every tower of the family . . . 15
5.4 The normal radical closure exists . . . 16
5.5 Every element of a radical tower top is algebraic over the base . 16
5.6 A splitting field is normal and has a finite Galois group . . . 17
5.7 Prepending a cyclotomic step . . . 17
5.8 A radical tower embeds in a solvable normal radical top . . . 17
5.9 Polynomial helpers: products over a subfield and their roots . . . 18
5.10 Witness-level normal closure: bounded-exponent Kummer chain for the conjugate family . . . 19
5.11 The normal radical closure of a radical tower is a solvable splitting field . . . 20

6 A Concrete Quintic with Galois Group S_5 21
6.1 Eisenstein's irreducibility criterion . . . 21
6.2 The polynomial and its real roots . . . 22
6.3 The real polynomial and its real roots . . . 23
6.4 The complex roots: three real and one conjugate pair . . . 23
6.5 Irreducibility of the quintic over the rationals . . . 25

6.6 The Galois group of the quintic is not solvable 25
6.7 The main theorem 25

7 The quintic $x^5 - 4x + 2$ is not solvable by radicals **26**
7.1 The main theorem 26

1 Cyclotomic and Kummer extensions have abelian Galois groups

theory *Cyclotomic-Kummer*
imports *HOL−Analysis.Complex-Transcendental*
HOL−New-Algebra.Subfield
HOL−New-Algebra.Galois-Degree
begin

2 Roots of unity form a cyclic group

For the complex numbers there is an *explicit* primitive nth root of unity, *unity-root* n = *exp* (*complex-of-real* (*2* ∗ *pi*) ∗ i / n), and every nth root of unity is one of its powers. Thus the group of nth roots of unity is *cyclic*, generated by *unity-root* n.

2.1 The set of nth roots of unity

definition *roots-of-unity* :: *nat* ⇒ *complex set*
where *roots-of-unity* $n \equiv \{z.\ z \hat{} n = 1\}$

A distinguished primitive nth root of unity.

definition *unity-root* :: *nat* ⇒ *complex*
where *unity-root* $n \equiv$ *exp* (*2* ∗ *of-real pi* ∗ i / *of-nat* n)

lemma *roots-of-unity-iff* [*simp*]: $z \in$ *roots-of-unity* $n \longleftrightarrow z \hat{} n = 1$
⟨*proof*⟩

lemma *one-in-roots-of-unity* [*simp*, *intro*]: *1* ∈ *roots-of-unity* n
⟨*proof*⟩

lemma *finite-roots-of-unity*:
assumes $n > 0$ **shows** *finite* (*roots-of-unity* n)
⟨*proof*⟩

lemma *card-roots-of-unity*:
assumes $n > 0$ **shows** *card* (*roots-of-unity* n) = n
⟨*proof*⟩

2.2 The primitive root generates: powers exhaust the roots of unity

The jth power of *unity-root* n is *exp* (*2*πij / n), the standard parametrisation of the nth roots of unity.

lemma *unity-root-power*:
unity-root $n \hat{} j$ = *exp* (*2* ∗ *of-real pi* ∗ i ∗ *of-nat* j / *of-nat* n)

⟨*proof*⟩

Each power of the primitive root is indeed an nth root of unity.

lemma *unity-root-pow-mem*:
assumes $n > 0$ **shows** *unity-root* $n \mathbin{\hat{}} j \in$ *roots-of-unity* n
⟨*proof*⟩

Cyclicity. The nth roots of unity are exactly the powers $\{(\textit{unity-root}\ n)^j \mid j.\ j < n\}$ of the primitive root: the group is cyclic.

theorem *roots-of-unity-eq-powers*:
assumes $n > 0$
shows *roots-of-unity* $n = \{\textit{unity-root}\ n \mathbin{\hat{}} j \mid j.\ j < n\}$
⟨*proof*⟩

corollary *roots-of-unity-subset-powers*:
assumes $n > 0$ **and** $z \in$ *roots-of-unity* n
shows $\exists j < n.\ z =$ *unity-root* $n \mathbin{\hat{}} j$
⟨*proof*⟩

2.3 Closure properties: a subgroup of the multiplicative group

lemma *unity-root-mem* [*simp*, *intro*]:
assumes $n > 0$ **shows** *unity-root* $n \in$ *roots-of-unity* n
⟨*proof*⟩

lemma *roots-of-unity-mult-closed*:
assumes $x \in$ *roots-of-unity* n **and** $y \in$ *roots-of-unity* n
shows $x * y \in$ *roots-of-unity* n
⟨*proof*⟩

lemma *roots-of-unity-nonzero*:
assumes $n > 0$ **and** $z \in$ *roots-of-unity* n **shows** $z \neq 0$
⟨*proof*⟩

lemma *roots-of-unity-inverse-closed*:
assumes $z \in$ *roots-of-unity* n **shows** *inverse* $z \in$ *roots-of-unity* n
⟨*proof*⟩

2.4 Divisibility: fewer roots of unity sit among more

If n divides N then every nth root of unity is an Nth root of unity: from $z \mathbin{\hat{}} n = 1$ and $N = n * k$ we get $z \mathbin{\hat{}} N = (z \mathbin{\hat{}} n) \mathbin{\hat{}} k = 1$. Hence one primitive Nth root of unity supplies the roots of unity for every exponent dividing N — the fact that lets a single cyclotomic step serve a whole radical tower.

lemma *roots-of-unity-dvd-mono*:
fixes z :: *complex*
assumes *dvd*: n *dvd* N **and** z: $z \mathbin{\hat{}} n = 1$

shows $z \mathbin{\hat{}} N = 1$
⟨*proof*⟩

corollary *roots-of-unity-subset-dvd*:
assumes n *dvd* N
shows *roots-of-unity* $n \subseteq$ *roots-of-unity* N
⟨*proof*⟩

3 Cyclotomic and Kummer extensions have abelian Galois groups

Both the cyclotomic extension $F(\zeta)$ (adjoining a primitive root of unity) and the Kummer extension $F(a)$ with $a^n \in F$ and the nth roots of unity already in F have *abelian* Galois groups, hence *solvable* ones. Both follow from one criterion: the Galois group of a simple normal extension is abelian as soon as its automorphisms commute on the generator, and an F-automorphism of $F\ a$ is determined by its value at a."

3.1 Automorphisms map the carrier into itself

An F-automorphism of *eval-img F a* keeps its value at a inside the carrier (it is extensional into *eval-img F a*).

lemma *field-auto-gen-closed*:
fixes F :: *complex set* **and** a :: *complex*
assumes *Subfield F* $\sigma \in$ *field-auto* (*eval-img F a*) *F*
shows $\sigma\ a \in$ *eval-img F a*
⟨*proof*⟩

3.2 Abelian criterion for a simple normal extension

If any two F-automorphisms of *eval-img F a* commute at the generator a, then *field-auto* (*eval-img F a*) *F* is an abelian group. Determinacy (*field-auto-determined-by-gen*) upgrades commutation at a to full commutation, since both *compose E* σ τ and *compose E* τ σ are automorphisms agreeing at a.

lemma *galois-abelian-of-gen-commute*:
fixes F :: *complex set* **and** a :: *complex*
assumes *sfF*: *Subfield F* **and** *alg*: *algebraic-over F a*
and *comm-gen*: $\bigwedge\sigma\ \tau.\ \sigma \in$ *field-auto* (*eval-img F a*) *F* $\Longrightarrow\ \tau \in$ *field-auto* (*eval-img F a*) *F*
$\Longrightarrow\ \sigma\ (\tau\ a) = \tau\ (\sigma\ a)$
shows *Abelian-Group* (*field-auto* (*eval-img F a*) *F*) (*compose* (*eval-img F a*)) (*identity* (*eval-img F a*))
⟨*proof*⟩

Consequently such a Galois group is *solvable*.

theorem *galois-solvable-of-gen-commute*:
fixes F :: *complex set* **and** a :: *complex*
assumes *sfF*: *Subfield* F **and** *alg*: *algebraic-over* F a
and *comm-gen*: $\bigwedge\sigma\ \tau.\ \sigma \in$ *field-auto* (*eval-img* F a) $F \Longrightarrow \tau \in$ *field-auto* (*eval-img* F a) F
$\Longrightarrow \sigma\ (\tau\ a) = \tau\ (\sigma\ a)$
shows *Group.solvable* (*field-auto* (*eval-img* F a) F) (*compose* (*eval-img* F a)) (*identity* (*eval-img* F a))
⟨*proof*⟩

3.3 Cyclotomic extensions are abelian

The polynomial $X^n - 1$ over F, and the fact that an automorphism sends an nth root of unity to an nth root of unity.

lemma *field-auto-maps-unity-root*:
fixes F :: *complex set* **and** z :: *complex*
assumes *sfF*: *Subfield* F **and** n: $n > 0$ **and** *alg*: *algebraic-over* F z
and s: $\sigma \in$ *field-auto* (*eval-img* F z) F **and** *root*: $z\ \hat{}\ n = 1$
shows $(\sigma\ z)\ \hat{}\ n = 1$
⟨*proof*⟩

Cyclotomic case. If ζ is a *primitive* nth root of unity — every nth root of unity is a power of it — then $F\ \zeta$ has an abelian Galois group: each automorphism sends ζ to a power ζ^k, and powers commute.

theorem *cyclotomic-galois-solvable*:
fixes F :: *complex set* **and** ζ :: *complex*
assumes *sfF*: *Subfield* F **and** n: $n > 0$ **and** *alg*: *algebraic-over* F ζ
and *root*: $\zeta\ \hat{}\ n = 1$
and *primitive*: $\bigwedge w.\ w\ \hat{}\ n = 1 \Longrightarrow \exists k.\ w = \zeta\ \hat{}\ k$
shows *Group.solvable* (*field-auto* (*eval-img* F ζ) F) (*compose* (*eval-img* F ζ)) (*identity* (*eval-img* F ζ))
⟨*proof*⟩

3.4 Kummer extensions are abelian

Kummer case. If F already contains the nth roots of unity and $a^n \in F$, then $F\ a$ has an abelian Galois group. An automorphism sends a to another root of $X^n - a^n$, so $\sigma\ a = a * (\sigma\ a\ /\ a)$ where the ratio $\sigma\ a\ /\ a$ is an nth root of unity, hence lies in F and is fixed by every automorphism. Two such automorphisms therefore commute at a.

theorem *kummer-galois-solvable*:
fixes F :: *complex set* **and** a :: *complex*
assumes *sfF*: *Subfield* F **and** n: $n > 0$ **and** *alg*: *algebraic-over* F a
and *anF*: $a\ \hat{}\ n \in F$
and *roots-in-F*: $\bigwedge w.\ w\ \hat{}\ n = 1 \Longrightarrow w \in F$
and *a-nz*: $a \neq 0$
shows *Group.solvable* (*field-auto* (*eval-img* F a) F) (*compose* (*eval-img* F a)) (*identity* (*eval-img* F a))

⟨*proof*⟩

end

4 The forward Abel–Ruffini direction: assembling the radical tower

theory *Radical-Solvable*
imports *Cyclotomic-Kummer*
HOL−New-Algebra.Normal-Closure
HOL−New-Algebra.Galois-Restriction-Splitting
HOL−New-Algebra.Radical-Extension
begin

We assemble the pieces — the solvable Kummer/cyclotomic steps, the stability engine and the tower assembly — into "a radical tower over a field containing enough roots of unity has a solvable Galois group".

4.1 A single radical step, with roots of unity present, is a full splitting field

When F contains the nth roots of unity and $a^n \in F$, the simple Kummer extension *eval-img F a* already contains *all* roots of $X^n - a^n$ (the others are $\zeta * a$ for roots of unity $\zeta \in F$), so it *equals* the field generated by that full root set.

lemma *kummer-step-full-root-set*:
fixes F :: *complex set* **and** a :: *complex*
assumes *sfF*: *Subfield F* **and** n: $n > 0$ **and** *anF*: $a \mathbin{\hat{}} n \in F$ **and** *a-nz*: $a \neq 0$
and *roots-in-F*: $\bigwedge w.\ w \mathbin{\hat{}} n = 1 \Longrightarrow w \in F$
shows *eval-img F a* = *generate-field* ($F \cup \{r.\ poly\ (monom\ 1\ n - [:a \mathbin{\hat{}} n:])\ r = 0\}$)
⟨*proof*⟩

4.2 A Kummer step is both solvable and stable

Packaging the previous facts: inside an ambient field K that contains the full root set of $X^n - a^n$, and with the nth roots of unity present in F, the Kummer extension *eval-img F a* supplies *both* ingredients that *solvable-tower* needs for a step: its relative Galois group is solvable (*kummer-galois-solvable*), and it is stable under *field-auto K F* (*root-generated-stable*, since it is a full root-set field by *kummer-step-full-root-set*).

theorem *kummer-step-solvable-and-stable*:
fixes K F :: *complex set* **and** a :: *complex*
assumes K: *Subfield K* **and** *sfF*: *Subfield F* **and** *FK*: $F \subseteq K$
and n: $n > 0$ **and** *anF*: $a \mathbin{\hat{}} n \in F$ **and** *a-nz*: $a \neq 0$
and *roots-in-F*: $\bigwedge w.\ w \mathbin{\hat{}} n = 1 \Longrightarrow w \in F$
and *aK*: $a \in K$

shows *Group.solvable* (*field-auto* (*eval-img F a*) *F*) (*compose* (*eval-img F a*)) (*identity* (*eval-img F a*))
  ∧ *eval-img F a* ⊆ *K*
  ∧ (∀ σ ∈ *field-auto K F*. σ ‘ *eval-img F a* = *eval-img F a*)
  ∧ *Subfield* (*eval-img F a*)
⟨*proof*⟩

4.3 A cyclotomic step is solvable, stable, and supplies the roots of unity

Adjoining the primitive nth root of unity *unity-root n* to F: the extension *eval-img F* (*unity-root n*) has a solvable (abelian) Galois group (*cyclotomic-galois-solvable*), is the full root-set field of $X^n - 1$ (hence stable by *root-generated-stable*), and — crucially — *contains all the nth roots of unity*, establishing the invariant that the subsequent Kummer step needs.

theorem *cyclotomic-step-solvable-and-stable*:
  fixes *K F* :: *complex set*
  assumes *K*: *Subfield K* **and** *sfF*: *Subfield F* **and** *FK*: *F* ⊆ *K* **and** *n*: *n* > *0*
    and *zK*: *unity-root n* ∈ *K*
  shows *Group.solvable* (*field-auto* (*eval-img F* (*unity-root n*)) *F*)
      (*compose* (*eval-img F* (*unity-root n*))) (*identity* (*eval-img F* (*unity-root n*)))
  ∧ *eval-img F* (*unity-root n*) ⊆ *K*
  ∧ (∀ σ ∈ *field-auto K F*. σ ‘ *eval-img F* (*unity-root n*) = *eval-img F* (*unity-root n*))
  ∧ *Subfield* (*eval-img F* (*unity-root n*))
  ∧ (∀ *w*. *w* ^ *n* = *1* ⟶ *w* ∈ *eval-img F* (*unity-root n*))
⟨*proof*⟩

4.4 A chain of Kummer steps is a solvable tower

An element whose nth power lies in F is algebraic over F (it is a root of the nonzero F-polynomial $X^n - a^n$).

lemma *radical-algebraic*:
  fixes *F* :: *complex set*
  assumes *sfF*: *Subfield F* **and** *n*: *n* > *0* **and** *anF*: *a* ^ *n* ∈ *F*
  shows *algebraic-over F a*
⟨*proof*⟩

The chain of fields built from a list of *Kummer witnesses* (a, n) (each contributing a step $F \rightsquigarrow F(a)$).

fun *kummer-fields* :: *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *complex set list* **where**
  kummer-fields F [] = []
| *kummer-fields F* ((*a*, *n*) # *ws*) = *eval-img F a* # *kummer-fields* (*eval-img F a*) *ws*

Validity of a witness chain over F: each step has positive exponent, a nonzero base a with $a^n \in F$, and the nth roots of unity already present in the current field.

fun *kummer-valid* :: *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *bool* **where**
  kummer-valid F [] = *True*
| *kummer-valid F* ((*a*, *n*) # *ws*) =
    (*n* > *0* ∧ *a* ≠ *0* ∧ *a* ^ *n* ∈ *F* ∧ (∀ *w*. *w* ^ *n* = *1* ⟶ *w* ∈ *F*) ∧
     kummer-valid (*eval-img F a*) *ws*)

The top field of the chain (the ambient splitting field).

definition *ktop* :: *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *complex set* **where**
  ktop F ws ≡ *last* (*F* # *kummer-fields F ws*)

lemma *ktop-Nil* [*simp*]: *ktop F* [] = *F*
  ⟨*proof*⟩

lemma *ktop-Cons* [*simp*]: *ktop F* ((*a*, *n*) # *ws*) = *ktop* (*eval-img F a*) *ws*
  ⟨*proof*⟩

The chain is increasing, so the base is contained in the top.

lemma *ktop-facts*:
  fixes *F* :: *complex set*
  shows *Subfield F* ⟹ *kummer-valid F ws* ⟹ *F* ⊆ *ktop F ws* ∧ *Subfield* (*ktop F ws*)
⟨*proof*⟩

The top field is a subfield.

lemma
  assumes *Subfield F kummer-valid F ws*
  shows *F-subset-ktop*: *F* ⊆ *ktop F ws* **and** *subfield-ktop*: *Subfield* (*ktop F ws*)
  ⟨*proof*⟩

The chain is a solvable tower. By induction on the witness list: each Kummer step is solvable and stable inside the ambient top field.

theorem *kummer-chain-solvable-tower*:
  Subfield F ⟹ *kummer-valid F ws* ⟹ *solvable-tower* (*ktop F ws*) *F* (*kummer-fields F ws*)
⟨*proof*⟩

The Galois group of a valid Kummer chain is solvable.

corollary *kummer-chain-galois-solvable*:
  assumes *sfF*: *Subfield F* **and** *valid*: *kummer-valid F ws*
  shows *Group.solvable* (*field-auto* (*ktop F ws*) *F*) (*compose* (*ktop F ws*)) (*identity* (*ktop F ws*))
  ⟨*proof*⟩

4.5 Solvability descends to a stable subfield with surjective restriction

Descent to an intermediate Galois group. Let $F \subseteq E \subseteq K$ with E stable under *field-auto K F*, and suppose restriction $\lambda\sigma.\ \mathit{restrict}\ \sigma\ E$ maps *field-auto K F*

onto field-auto E F (the *normality* input: every F-automorphism of E extends to one of K). Then if *field-auto K F* is solvable, so is *field-auto E F* — it is a homomorphic image.

This is the group-theoretic heart of the forward direction: the quintic's Galois group would be a *quotient* of the solvable Galois group of a radical extension, hence solvable — contradicting its non-solvability. The surjectivity hypothesis is exactly what *normality of K over F* supplies (and what a full normal-closure construction would discharge).

theorem *galois-solvable-descends*:
  fixes *K E F* :: *complex set*
  assumes *K*: *Subfield K* **and** *sfE*: *Subfield E* **and** *sfF*: *Subfield F*
    and *FE*: $F \subseteq E$ **and** *EK*: $E \subseteq K$
    and *stable*: $\bigwedge\sigma.\ \sigma \in$ *field-auto K F* $\Longrightarrow \sigma$ ‘ $E = E$
    and *onto*: $(\lambda\sigma.$ *restrict* σ *E*$)$ ‘ *field-auto K F* = *field-auto E F*
    and *solvK*: *Group.solvable* (*field-auto K F*) (*compose K*) (*identity K*)
  shows *Group.solvable* (*field-auto E F*) (*compose E*) (*identity E*)
⟨*proof*⟩

4.6 The forward theorem

The forward Abel–Ruffini theorem. Suppose a set S lies in a field E that sits inside the top *ktop F ws* of a valid Kummer chain over F (so E is contained in a radical extension), with E stable under the ambient Galois group and restriction onto *field-auto E F* surjective (the normality conditions). Then *field-auto E F* is solvable.

Chaining *kummer-chain-galois-solvable* (the radical top has a solvable Galois group) with *galois-solvable-descends* (solvability descends to the stable subfield). This is the complete forward direction modulo the single classical input — normality of the ambient radical field, i.e. surjectivity of restriction — which a full normal-closure construction supplies.

theorem *radical-extension-galois-solvable*:
  fixes *F E* :: *complex set* **and** *ws* :: (*complex* × *nat*) *list*
  assumes *sfF*: *Subfield F* **and** *sfE*: *Subfield E*
    and *valid*: *kummer-valid F ws*
    and *FE*: $F \subseteq E$ **and** *EK*: $E \subseteq$ *ktop F ws*
    and *stable*: $\bigwedge\sigma.\ \sigma \in$ *field-auto* (*ktop F ws*) *F* $\Longrightarrow \sigma$ ‘ $E = E$
    and *onto*: $(\lambda\sigma.$ *restrict* σ *E*$)$ ‘ *field-auto* (*ktop F ws*) *F* = *field-auto E F*
  shows *Group.solvable* (*field-auto E F*) (*compose E*) (*identity E*)
⟨*proof*⟩

4.7 From a roots-of-unity-free chain to a valid Kummer chain

A *pre-Kummer chain* over F bounded by N: each step has positive exponent n *dividing* N, a nonzero base a with $a^n \in F$. This is the roots-of-unity-*free* data

of a radical tower (a raw radical step, tagged with its exponent), with the mild global bound that all exponents divide a common N.

fun *pre-kummer-valid* :: *nat* ⇒ *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *bool* **where**
  pre-kummer-valid N F [] = *True*
| *pre-kummer-valid N F* ((*a*, *n*) # *ws*) =
    (*n* > *0* ∧ *n dvd N* ∧ *a* ≠ *0* ∧ *a* ^ *n* ∈ *F* ∧ *pre-kummer-valid N* (*eval-img F a*) *ws*)

If the base field already contains all Nth roots of unity, a pre-Kummer chain bounded by N is a genuine Kummer chain: at each step the nth roots of unity (with *n dvd N*) are among the Nth roots of unity (*roots-of-unity-dvd-mono*), which persist up the tower since each field contains its predecessor.

lemma *pre-kummer-valid-imp-kummer-valid*:
  Subfield F ⟹ (∀ *w*. *w* ^ *N* = *1* ⟶ *w* ∈ *F*) ⟹ *pre-kummer-valid N F ws* ⟹ *kummer-valid F ws*
⟨*proof*⟩

The Galois group of a pre-Kummer chain, once the roots of unity are adjoined, is solvable. If F contains the Nth roots of unity and *ws* is a pre-Kummer chain bounded by N, then *field-auto* (*ktop F ws*) *F* is solvable.

corollary *pre-kummer-chain-galois-solvable*:
  assumes *sfF*: *Subfield F* **and** *rou*: ∀ *w*. *w* ^ *N* = *1* ⟶ *w* ∈ *F*
    and *pre*: *pre-kummer-valid N F ws*
  shows *Group.solvable* (*field-auto* (*ktop F ws*) *F*) (*compose* (*ktop F ws*)) (*identity* (*ktop F ws*))
  ⟨*proof*⟩

4.8 Extracting Kummer witnesses from a radical tower

A *nondegenerate* radical tower is one whose every step can be realised by a *nonzero* radical whose exponent divides a common bound N. (Adjoining *0* adds nothing, so this is no real restriction for reaching a target set; and any finite family of exponents divides their common multiple.) We record this as the existence of a witness list.

definition *realises-tower* :: *nat* ⇒ *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *complex set list* ⇒ *bool*
  where *realises-tower N F ws Fs* ≡ *pre-kummer-valid N F ws* ∧ *kummer-fields F ws* = *Fs*

If a radical tower is realised by a nondegenerate witness list over a base F containing the Nth roots of unity, then its top field has a solvable Galois group over F. The top field of the realised chain coincides with the tower top.

lemma *ktop-eq-tower-top*:
  assumes *kummer-fields F ws* = *Fs*
  shows *ktop F ws* = *tower-top F Fs*
  ⟨*proof*⟩

theorem *radical-tower-galois-solvable*:
  assumes *sfF*: *Subfield F* **and** *rou*: $\forall\, w.\ w \mathbin{\hat{}} N = 1 \longrightarrow w \in F$
    and *real*: *realises-tower N F ws Fs*
  shows *Group.solvable* (*field-auto* (*tower-top F Fs*) *F*)
        (*compose* (*tower-top F Fs*)) (*identity* (*tower-top F Fs*))
⟨*proof*⟩

Conversely, a nondegenerate witness chain *is* a radical tower in the sense of *radical-tower*: each Kummer step $F \rightsquigarrow F(a)$ is a radical step, since *eval-img F a* = *generate-field* $(F \cup \{a\})$ with $a^n \in F$. Thus the notion of a realised tower is faithful to the project's *radical-tower*.

4.9 Extracting a nondegenerate witness list from a bare radical tower

The nondegeneracy conditions of a witness list, without the common divisibility bound: each step has positive exponent, a nonzero base, and its power in the current field.

fun *wit-valid* :: *complex set* ⇒ (*complex* × *nat*) *list* ⇒ *bool* **where**
  wit-valid F [] = *True*
| *wit-valid F* ((*a*, *n*) # *ws*) =
    (*n* > *0* ∧ *a* ≠ *0* ∧ *a* ^ *n* ∈ *F* ∧ *wit-valid* (*eval-img F a*) *ws*)

Given a common bound N divisible by every step exponent, a nondegenerate witness list is a pre-Kummer chain.

lemma *wit-valid-imp-pre-kummer-valid*:
  wit-valid F ws ⟹ (∀ *x* ∈ *set ws*. *snd x dvd N*) ⟹ *pre-kummer-valid N F ws*
⟨*proof*⟩

Every radical tower has a nondegenerate witness list. Walking the tower: each radical step $F \rightsquigarrow G$ either uses a nonzero radical (G = *eval-img F a*) or is a no-op ($G = F$, which occurs when the existential witness is *0*); in the latter case the trivial witness (*1*, *1*) reproduces F (as *eval-img F 1* = *F*).

lemma *radical-tower-witnesses*:
  Subfield F ⟹ *radical-tower F Fs* ⟹ ∃ *ws*. *wit-valid F ws* ∧ *kummer-fields F ws* = *Fs*
⟨*proof*⟩

lemma *pre-kummer-valid-imp-radical-tower*:
  Subfield F ⟹ *pre-kummer-valid N F ws* ⟹ *radical-tower F* (*kummer-fields F ws*)
⟨*proof*⟩

4.10 A radical tower over a roots-of-unity base has a solvable Galois group

The forward theorem for a bare radical tower. If F contains *enough* roots of unity — namely the Nth roots of unity for N the product of the (extracted) step exponents — then the top of any radical tower over F has a solvable Galois group over F. This reduces the forward direction over F to the single remaining hypothesis that F contains the required roots of unity — which a cyclotomic pre-step $F \rightsquigarrow F(\zeta_N)$ supplies (and which, over $\mathbb{Q}$, is the only reason the base must first be enlarged).

theorem *radical-tower-solvable-of-roots*:
  assumes *sfF*: *Subfield F* **and** *tower*: *radical-tower F Fs*
    and *rou*: $\bigwedge ws.$ *wit-valid F ws* $\Longrightarrow$ *kummer-fields F ws* $=$ *Fs*
      $\Longrightarrow \forall w.\ w\ \widehat{}\ (\mathit{prod\text{-}list}\ (\mathit{List.map}\ \mathit{snd}\ \mathit{ws})) = 1 \longrightarrow w \in F$
  shows *Group.solvable* (*field-auto* (*tower-top F Fs*) *F*)
      (*compose* (*tower-top F Fs*)) (*identity* (*tower-top F Fs*))
⟨*proof*⟩

4.11 Unconditional descent to a stable splitting subfield

Combining the splitting-field image theorem *galois-restriction-image-of-splitting-field* with the descent theorem *galois-solvable-descends* discharges the former surjectivity obligation when K is a splitting field over E. This is where the "deep gap" closes.

theorem *galois-splitting-subfield-solvable*:
  fixes *K E F* :: *complex set* **and** *Phi* :: *complex poly*
  assumes *sfE*: *Subfield E* **and** *sfF*: *Subfield F* **and** *FE*: $F \subseteq E$
    and *Phi*: *Phi* $\in$ *poly-over F*
    and *split*: *splitting-field E Phi K*
    and *stable*: $\bigwedge \sigma.\ \sigma \in$ *field-auto K F* $\Longrightarrow \sigma$ ‘ $E = E$
    and *solvK*: *Group.solvable* (*field-auto K F*) (*compose K*) (*identity K*)
  shows *Group.solvable* (*field-auto E F*) (*compose E*) (*identity E*)
⟨*proof*⟩

end

5 The normal radical closure of a radical tower

theory *Radical-Normal-Closure*
  imports *Radical-Solvable*
    HOL−New-Algebra.Algebraic-Transitivity
    HOL−New-Algebra.Galois-Transitivity
begin

To descend solvability of a radical extension onto a *quotient* Galois group we must first replace the radical tower by one whose top is *normal* over the base —

the "normal radical closure". The construction (as in the standard textbook argument, and in Mathlib's *FieldTheory.AbelRuffini*): the conjugates of a radical tower are again radical towers (*radical-tower-image*), and splicing the finitely many conjugates together (*radical-tower-spliced*) yields one radical tower whose top is stable under the ambient Galois group. These blocks develop the conjugate/splice reasoning; the quintic-specific assembly and the contradiction live in the joint session theory.

5.1 A Galois conjugate of a radical tower is a radical tower

lemma *radical-tower-conjugate*:
  fixes N F :: *complex set* **and** Fs :: *complex set list* **and** σ :: *complex* $\Rightarrow$ *complex*
  assumes N: *Subfield N* **and** *sfF*: *Subfield F*
    and *tower*: *radical-tower F Fs* **and** *topN*: *tower-top F Fs* $\subseteq N$
    and s: $\sigma \in$ *field-auto N F*
  shows *radical-tower F* (*List.map* ((') σ) *Fs*)
⟨*proof*⟩

5.2 The family of all conjugates is a family of towers over the base

Applying a list σs of F-automorphisms to a radical tower yields a family of radical towers over F — the input shape that *radical-tower-spliced* consumes.

lemma *conjugate-towers-over*:
  fixes N F :: *complex set* **and** Fs :: *complex set list*
    and σs :: (*complex* $\Rightarrow$ *complex*) *list*
  assumes N: *Subfield N* **and** *sfF*: *Subfield F*
    and *tower*: *radical-tower F Fs* **and** *topN*: *tower-top F Fs* $\subseteq N$
    and *ss*: *set* $\sigma s \subseteq$ *field-auto N F*
  shows *all-towers-over F* (*List.map* ($\lambda\sigma$. *List.map* ((') σ) *Fs*) σs)
  ⟨*proof*⟩

5.3 The spliced tower's top contains every tower of the family

Base-changing a tower *Ts* (over F) onto a larger base B can only enlarge its top.

lemma *tower-top-basechange-superset*:
  assumes $F \subseteq B$
  shows *tower-top F Ts* $\subseteq$ *tower-top B* (*List.map* (λH. *generate-field* ($B \cup H$)) *Ts*)
  ⟨*proof*⟩

In the spliced tower *spliced B Tss* over B, the top field contains the top of *every* tower of the family (measured over the common base F). This is what makes the splice top a compositum of the conjugates.

lemma *spliced-top-contains-towers*:

assumes *Subfield B* **and** *Subfield F* **and** $F \subseteq B$ **and** *all-towers-over F Tss*
shows $\forall$ *Ts* $\in$ *set Tss*. *tower-top F Ts* $\subseteq$ *tower-top B* (*spliced B Tss*)
⟨*proof*⟩

5.4 The normal radical closure exists

The top of a conjugated tower is the conjugate of the top: since σ fixes F setwise, *tower-top F* (*map* ((‘) σ) *Fs*) = σ ‘ *tower-top F Fs* (the last field of the mapped list is the image of the last field; for the empty tower both sides are σ ‘ $F = F$).

lemma *tower-top-conjugate*:
assumes *sF*: σ ‘ $F = F$
shows *tower-top F* (*List.map* ((‘) σ) *Fs*) = σ ‘ *tower-top F Fs*
⟨*proof*⟩

The normal radical closure exists (complex form). Given a radical tower *Fs* over F inside an ambient field N, and any list σs of F-automorphisms of N, splicing the conjugate family yields a single radical tower over F whose top B contains the conjugate σ ‘ *tower-top F Fs* of the original top for every $\sigma \in$ *set* σs.

theorem *radical-normal-closure-exists*:
fixes *N F* :: *complex set* **and** *Fs* :: *complex set list*
and σs :: (*complex* $\Rightarrow$ *complex*) *list*
assumes *N*: *Subfield N* **and** *sfF*: *Subfield F*
and *tower*: *radical-tower F Fs* **and** *topN*: *tower-top F Fs* $\subseteq$ *N*
and *ss*: *set* $\sigma s \subseteq$ *field-auto N F*
defines *Tss* $\equiv$ *List.map* ($\lambda\sigma$. *List.map* ((‘) σ) *Fs*) σs
shows *radical-tower F* (*spliced F Tss*)
($\forall \sigma \in$ *set* σs. σ ‘ *tower-top F Fs* $\subseteq$ *tower-top F* (*spliced F Tss*))
⟨*proof*⟩

5.5 Every element of a radical tower top is algebraic over the base

Algebraicity of a witness (Kummer/radical) chain over its base. Every element of the top *ktop F ws* of a nondegenerate witness list is algebraic over the base F.

theorem *ktop-algebraic-over-base*:
fixes *F* :: *complex set*
shows *Subfield F* $\Longrightarrow$ *wit-valid F ws* $\Longrightarrow$ *y* $\in$ *ktop F ws* $\Longrightarrow$ *algebraic-over F y*
⟨*proof*⟩

Recast for a bare radical tower (via its witness list): every element of *tower-top F Fs* is algebraic over F.

theorem *radical-tower-top-algebraic*:
fixes *F* :: *complex set*
assumes *sfF*: *Subfield F* **and** *tower*: *radical-tower F Fs*
shows $\forall$ *y* $\in$ *tower-top F Fs*. *algebraic-over F y*
⟨*proof*⟩

5.6 A splitting field is normal and has a finite Galois group

theorem *splitting-field-finite-galois*:
fixes F :: *complex set* **and** *Phi* :: *complex poly*
assumes *sfF*: *Subfield F* **and** *Phi*: *Phi* $\in$ *poly-over F* **and** *Phinz*: *Phi* $\neq$ *0*
defines $N \equiv$ *generate-field* $(F \cup \{r.\ \textit{poly Phi } r = 0\})$
shows *Subfield N F* $\subseteq$ *N finite* (*field-auto N F*)
⟨*proof*⟩

5.7 Prepending a cyclotomic step

Adjoining a root of unity is a radical step. So a radical tower *Fs* over the cyclotomic base *eval-img F* (*unity-root N*) extends, by prepending that base as a first step, to a radical tower over F itself: *eval-img F* (*unity-root N*) # *Fs*.

lemma *radical-step-cyclotomic*:
fixes F :: *complex set*
assumes *sfF*: *Subfield F* **and** N: $N > 0$
shows *radical-step F* (*eval-img F* (*unity-root N*))
⟨*proof*⟩

Prepending the cyclotomic step to a tower over the cyclotomic base yields a radical tower over F.

lemma *radical-tower-cyclotomic-prepend*:
fixes F :: *complex set*
assumes *sfF*: *Subfield F* **and** N: $N > 0$
and *tower*: *radical-tower* (*eval-img F* (*unity-root N*)) *Fs*
shows *radical-tower F* (*eval-img F* (*unity-root N*) # *Fs*)
⟨*proof*⟩

5.8 A radical tower embeds in a solvable normal radical top

Witness validity is monotone in the base. If *ws* is a nondegenerate witness list over F and $F \subseteq B$ with B a subfield, then *ws* is also a nondegenerate witness list over B: the closure conditions $a^n \in F$ persist to B, and the running field *eval-img B a* still contains B (hence F).

lemma *wit-valid-exps-pos*:
fixes F :: *complex set*
shows *wit-valid F ws* $\Longrightarrow \forall x \in$ *set ws. snd x* > 0
⟨*proof*⟩

lemma *eval-img-mono-base*: $F \subseteq B \Longrightarrow$ *eval-img F a* $\subseteq$ *eval-img B a*
⟨*proof*⟩

lemma *mono-base-lemma*:
fixes F :: *complex set*
shows *Subfield B* $\Longrightarrow F \subseteq B \Longrightarrow$ *wit-valid F ws* $\Longrightarrow$ *ktop F ws* $\subseteq$ *ktop B ws* $\wedge$ *wit-valid B ws*

⟨*proof*⟩

lemma *ktop-mono-base*:
fixes F :: *complex set*
shows *Subfield* $B \Longrightarrow F \subseteq B \Longrightarrow$ *wit-valid* F *ws* $\Longrightarrow$ *ktop* F *ws* $\subseteq$ *ktop* B *ws*
⟨*proof*⟩

lemma *wit-valid-mono-base*:
fixes F :: *complex set*
shows *Subfield* $B \Longrightarrow F \subseteq B \Longrightarrow$ *wit-valid* F *ws* $\Longrightarrow$ *wit-valid* B *ws*
⟨*proof*⟩

A radical tower over a subfield F embeds into a field N that is a *solvable* radical top over F: prepend a cyclotomic step $F \rightsquigarrow F(\zeta_{N0})$ (with N_0 the product of the extracted witness exponents), realise the tower over the enlarged base by the same witnesses, and combine solvability over the cyclotomic base with solvability of the cyclotomic step via the tower step.

theorem *radical-tower-embeds-solvable-top*:
fixes F :: *complex set*
assumes *sfF*: *Subfield* F **and** *tower*: *radical-tower* F *Fs*
obtains N *Gs* **where** *Subfield* N **and** $F \subseteq N$ **and** *tower-top* F *Fs* $\subseteq N$
and *radical-tower* F *Gs* **and** *tower-top* F *Gs* $= N$
and *Group.solvable* (*field-auto* N F) (*compose* N) (*identity* N)
⟨*proof*⟩

5.9 Polynomial helpers: products over a subfield and their roots

lemma *poly-over-prod-list*:
assumes *Subfield* K
shows $(\bigwedge p.\ p \in$ *set ps* $\Longrightarrow p \in$ *poly-over* $K) \Longrightarrow$ *prod-list ps* $\in$ *poly-over* K
⟨*proof*⟩

lemma *poly-prod-list-root-iff*:
fixes *ps* :: $'a$ :: *idom poly list*
shows *poly* (*prod-list ps*) $y = 0 \longleftrightarrow (\exists\, p \in$ *set ps*. *poly* p $y = 0)$
⟨*proof*⟩

lemma *prod-list-poly-nonzero*:
fixes *ps* :: $'a$ :: *idom poly list*
shows $(\bigwedge p.\ p \in$ *set ps* $\Longrightarrow p \neq 0) \Longrightarrow$ *prod-list ps* $\neq 0$
⟨*proof*⟩

Each radical base *fst* w of a witness list lies in the Kummer top.

lemma *ktop-facts*:
fixes F :: *complex set*
shows *Subfield* $F \Longrightarrow$ *wit-valid* F *ws* $\Longrightarrow F \subseteq$ *ktop* F *ws* $\wedge$ *set* (*List.map fst ws*) $\subseteq$ *ktop* F *ws*
⟨*proof*⟩

The base is contained in the Kummer top of a nondegenerate witness list (the chain is increasing; roots of unity are not needed for this).

lemma
assumes *Subfield F wit-valid F ws*
shows *F-subset-ktop-wit*: $F \subseteq$ *ktop F ws* **and** *ktop-witness-bases-subset*: *set* (*List.map fst ws*) $\subseteq$ *ktop F ws*
⟨*proof*⟩

5.10 Witness-level normal closure: bounded-exponent Kummer chain for the conjugate family

The image of a simple extension under a field homomorphism on a superfield is the generated field of the image — unconditionally (no algebraicity of the image needed).

lemma *eval-img-image-hom*:
assumes *hom*: *field-hom-on N f* **and** *sfF*: *Subfield F* **and** *FN*: $F \subseteq N$
and *alg*: *algebraic-over F a* **and** *aN*: $a \in N$
shows *f ‘ eval-img F a = generate-field* (*f ‘ F* $\cup$ {*f a*})
⟨*proof*⟩

lemma *ktop-append*: *ktop F* (*xs* @ *ys*) = *ktop* (*ktop F xs*) *ys*
⟨*proof*⟩

lemma *pre-kummer-valid-append*:
pre-kummer-valid N0 F xs $\Longrightarrow$ *pre-kummer-valid N0* (*ktop F xs*) *ys*
$\Longrightarrow$ *pre-kummer-valid N0 F* (*xs* @ *ys*)
⟨*proof*⟩

Conjugating and base-changing a witness list, at the witness level. Let σ be a field homomorphism on the ambient N fixing G setwise via σ ‘ $G = G$. Given a witness list *ws* over G whose top lies in N and whose exponents divide N_0, and a base B (a subfield of N) containing σ ‘ G, there is a witness list *cw* over B — with the *same exponents* — that is N_0-bounded (*pre-kummer-valid*) and whose Kummer top contains the conjugate σ ‘ *ktop G ws*.

lemma *base-conj-witnesses*:
fixes *N* :: *complex set* **and** σ :: *complex* $\Rightarrow$ *complex*
assumes *N*: *Subfield N* **and** *hom*: *field-hom-on N σ* **and** *homN*: σ ‘ $N \subseteq N$
shows $\bigwedge G\ B$. *Subfield G* $\Longrightarrow$ *Subfield B* $\Longrightarrow$ $G \subseteq N \Longrightarrow B \subseteq N \Longrightarrow \sigma$ ‘ $G \subseteq B$
$\Longrightarrow$ *wit-valid G ws* $\Longrightarrow$ *ktop G ws* $\subseteq N \Longrightarrow$ ($\forall x \in$ *set ws. snd x dvd N0*)
$\Longrightarrow \exists$ *cw. pre-kummer-valid N0 B cw* $\wedge$ σ ‘ *ktop G ws* $\subseteq$ *ktop B cw*
$\wedge$ $B \subseteq$ *ktop B cw* $\wedge$ *ktop B cw* $\subseteq N$
⟨*proof*⟩

Folding the conjugate witnesses over the whole Galois group. Given a base tower *ws* over G, a cyclotomic base *Fz* (a subfield of N containing σ ‘ G for every σ in the list), we accumulate the conjugate witness lists of σ ‘ *ktop G ws* for all σ into one N_0-bounded pre-Kummer chain over *Fz* whose top stays inside N and

contains every conjugate σ ‘ *ktop G ws*. Induction on the list, appending each *base-conj-witnesses* chain with *pre-kummer-valid-append* / *ktop-append*.

lemma *conj-family-witnesses*:
fixes *N Fz G* :: *complex set* **and** *ws* :: (*complex* × *nat*) *list*
assumes *N*: *Subfield N* **and** *sfG*: *Subfield G* **and** *GN*: $G \subseteq N$
and *wv*: *wit-valid G ws* **and** *topGN*: *ktop G ws* $\subseteq N$ **and** *dvd*: $\forall x \in$ *set ws*. *snd x dvd N0*
shows $\bigwedge$*Fz*. *Subfield Fz* $\Longrightarrow$ *Fz* $\subseteq N \Longrightarrow G \subseteq$ *Fz* $\Longrightarrow$ ($\forall \sigma \in$ *set* σs. $\sigma \in$ *field-auto N G*)
$\Longrightarrow \exists$ *CW*. *pre-kummer-valid N0 Fz CW* $\wedge$ *Fz* $\subseteq$ *ktop Fz CW* $\wedge$ *ktop Fz CW* $\subseteq N$
$\wedge$ ($\forall \sigma \in$ *set* σs. σ ‘ *ktop G ws* $\subseteq$ *ktop Fz CW*)
⟨*proof*⟩

The Kummer top of a pre-Kummer chain is a subfield (each step is a simple algebraic extension; roots of unity are not needed).

lemma *subfield-ktop-pre*:
fixes *F* :: *complex set*
assumes *Subfield F* **and** *pre-kummer-valid N0 F ws*
shows *Subfield* (*ktop F ws*)
⟨*proof*⟩

If the base lies in a subfield N and every radical base of the witness list lies in N, then the whole Kummer top lies in N: each simple step *eval-img G a* = *generate-field* ($G \cup \{a\}$) stays inside N.

lemma *ktop-subset-of-bases*:
fixes *N* :: *complex set*
assumes *N*: *Subfield N*
shows $\bigwedge$*F*. *Subfield F* $\Longrightarrow$ *F* $\subseteq N \Longrightarrow$ *wit-valid F ws* $\Longrightarrow$ *set* (*List.map fst ws*) $\subseteq N$
$\Longrightarrow$ *ktop F ws* $\subseteq N$
⟨*proof*⟩

5.11 The normal radical closure of a radical tower is a solvable splitting field

Suppose *Fs* is a radical tower over F whose top contains the finite root set X of an irreducible F-polynomial P. Let Kq = *generate-field* ($F \cup X$). Then there is a normal closure N and an F-polynomial Ψ exhibiting N as the splitting field *generate-field* ($Kq \cup \{r.\ poly\ \Psi\ r = 0\}$) over Kq, with N solvable over F.

theorem *radical-tower-normal-closure-solvable*:
fixes *F* :: *complex set* **and** *P* :: *complex poly*
assumes *sfF*: *Subfield F* **and** *tower*: *radical-tower F Fs*
and *P*: $P \in$ *poly-over F* **and** *irrP*: *irreducible-over F P*
and *Xdef*: $X = \{r.\ poly\ P\ r = 0\}$ **and** *finX*: *finite X* **and** *XKq*: $X \subseteq$ *tower-top F Fs*
and *closed*: $\bigwedge q$ :: *complex poly*. $0 <$ *degree* $q \Longrightarrow \exists b.\ poly\ q\ b = 0$

defines $Kq \equiv$ *generate-field* $(F \cup X)$
obtains $N\ \Psi$ **where** *Subfield* N **and** $Kq \subseteq N$
and $\Psi \in$ *poly-over* F
and $N =$ *generate-field* $(Kq \cup \{r.\ poly\ \Psi\ r = 0\})$
and *finite* $\{r.\ poly\ \Psi\ r = 0\}$
and $\bigwedge r.\ poly\ \Psi\ r = 0 \Longrightarrow$ *algebraic-over* $Kq\ r$
and *Group.solvable* (*field-auto* $N\ F$) (*compose* N) (*identity* N)
⟨*proof*⟩

The preceding construction is the reusable bridge from a radical tower to the Galois group of the field generated by the roots of an irreducible polynomial. The normal radical top is an auxiliary object: after its solvability is established, the splitting-field restriction theorem descends solvability to the root field itself.

theorem *radical-tower-root-field-solvable*:
fixes F :: *complex set* **and** P :: *complex poly*
assumes *sfF*: *Subfield* F **and** *tower*: *radical-tower* $F\ Fs$
and *P*: $P \in$ *poly-over* F **and** *irrP*: *irreducible-over* $F\ P$
and *Xdef*: $X = \{r.\ poly\ P\ r = 0\}$ **and** *finX*: *finite* X
and *Xtop*: $X \subseteq$ *tower-top* $F\ Fs$
and *closed*: $\bigwedge q$ :: *complex poly*. $0 <$ *degree* $q \Longrightarrow \exists\, b.\ poly\ q\ b = 0$
defines $Kq \equiv$ *generate-field* $(F \cup X)$
shows *Group.solvable* (*field-auto* $Kq\ F$) (*compose* Kq) (*identity* Kq)
⟨*proof*⟩

end

6 A Concrete Quintic with Galois Group S_5

theory *Quintic-Example*
imports
HOL−New-Algebra.Complex-Field-Extension
HOL−New-Algebra.Abel-Ruffini
HOL−New-Algebra.Galois-Transitivity
HOL−Computational-Algebra.Polynomial-Factorial
Sturm-Sequences.Sturm
begin

We study the quintic $x^5 - 4x + 2$ over the rationals. It is irreducible (Eisenstein at *2*, proved here directly) and has exactly three real roots and one pair of complex-conjugate roots (the real-root count via the *sturm* method of *Sturm-Sequences.Sturm*). These are the hypotheses from which its Galois group is shown to be S_5.

6.1 Eisenstein's irreducibility criterion

A general form of Eisenstein's criterion over the integers: a polynomial satisfying the Eisenstein conditions for a prime p has no factorisation into two factors of positive degree.

lemma *sum-atMost-split*: $(\sum l{\leq}(i{::}nat).\ F\ l) = F\ i + (\sum l{<}i.\ F\ l)$
⟨*proof*⟩

lemma *eisenstein-factor-helper*:
fixes *f g h* :: *int poly* **and** *p* :: *int*
assumes *prime*: *prime p*
and *fgh*: $f = g * h$
and *lead*: ¬ *p dvd lead-coeff g*
and *mid*: $\bigwedge i.\ i < degree\ f \Longrightarrow p\ dvd\ coeff\ f\ i$
and *ph0*: ¬ *p dvd coeff h 0*
and *dg*: *0* < *degree g* **and** *dh*: *0* < *degree h*
shows *False*
⟨*proof*⟩

lemma *eisenstein-no-factor*:
fixes *f g h* :: *int poly* **and** *p* :: *int*
assumes *prime*: *prime p*
and *fgh*: $f = g * h$
and *lead*: ¬ *p dvd lead-coeff f*
and *mid*: $\bigwedge i.\ i < degree\ f \Longrightarrow p\ dvd\ coeff\ f\ i$
and *const*: ¬ $p\hat{}2$ *dvd coeff f 0*
and *dg*: *0* < *degree g* **and** *dh*: *0* < *degree h*
shows *False*
⟨*proof*⟩

6.2 The polynomial and its real roots

The quintic, as an integer polynomial; it is irreducible by Eisenstein at $2{::}'a$.

definition *PhiZ* :: *int poly*
where $PhiZ \equiv [:2,\ -4,\ 0,\ 0,\ 0,\ 1:]$

lemma *degree-PhiZ*: *degree PhiZ = 5*
⟨*proof*⟩

lemma *content-PhiZ*: *Polynomial.content PhiZ = 1*
⟨*proof*⟩

lemma *PhiZ-coeffs*:
coeff PhiZ 0 = 2 coeff PhiZ 1 = −4 coeff PhiZ 2 = 0
coeff PhiZ 3 = 0 coeff PhiZ 4 = 0 coeff PhiZ 5 = 1
⟨*proof*⟩

A degree-0 factor of *PhiZ* is a unit.

lemma *PhiZ-deg0-factor-unit*:
assumes *eq*: *PhiZ = smult c q*
shows [:*c*:] *dvd 1*
⟨*proof*⟩

theorem *irreducible-PhiZ*: *irreducible PhiZ*

⟨*proof*⟩

6.3 The real polynomial and its real roots

definition *Phi* :: *real poly*
  where *Phi* ≡ [:*2*, −*4*, *0*, *0*, *0*, *1*:]

lemma *Phi-eval*: *poly Phi x* = *x*^*5* − *4*∗*x* + *2*
  ⟨*proof*⟩

lemma *degree-Phi*: *degree Phi* = *5*
  ⟨*proof*⟩

At least three real roots, in disjoint intervals.

lemma *Phi-root-neg*: ∃ *x*. −*2* < *x* ∧ *x* < *0* ∧ *poly Phi x* = *0*
  ⟨*proof*⟩

lemma *Phi-root-01*: ∃ *x*. *0* < *x* ∧ *x* < *1* ∧ *poly Phi x* = *0*
  ⟨*proof*⟩

lemma *Phi-root-12*: ∃ *x*. *1* < *x* ∧ *x* < *2* ∧ *poly Phi x* = *0*
  ⟨*proof*⟩

The Sturm method counts the real roots: there are exactly three.

theorem *Phi-three-real-roots*: *card* {*x*::*real*. *poly Phi x* = *0*} = *3*
  ⟨*proof*⟩

6.4 The complex roots: three real and one conjugate pair

The same polynomial over the complex numbers.

definition *PhiC* :: *complex poly* **where** *PhiC* ≡ [:*2*, −*4*, *0*, *0*, *0*, *1*:]

lemma *degree-PhiC*: *degree PhiC* = *5*
  ⟨*proof*⟩

lemma *PhiC-nonzero*: *PhiC* ≠ *0*
  ⟨*proof*⟩

lemma *PhiC-eval*: *poly PhiC x* = *x*^*5* − *4*∗*x* + *2*
  ⟨*proof*⟩

lemma *pderiv-PhiC*: *pderiv PhiC* = [:−*4*, *0*, *0*, *0*, *5*:]
  ⟨*proof*⟩

lemma *pderiv-PhiC-eval*: *poly* (*pderiv PhiC*) *x* = *5*∗*x*^*4* − *4*
  ⟨*proof*⟩

The quintic is squarefree: it shares no root with its derivative. (A common root would force $x = 5/8$, which does not satisfy $5x^4 = 4$.)

lemma *PhiC-rsquarefree*: *rsquarefree PhiC*
⟨*proof*⟩

lemma *PhiC-roots-finite*: *finite* {*z*. *poly PhiC z* = *0*}
⟨*proof*⟩

Being squarefree of degree 5, it has exactly five distinct complex roots.

theorem *card-PhiC-roots*: *card* {*z*. *poly PhiC z* = *0*} = *5*
⟨*proof*⟩

The real complex-roots are the images of the real roots, hence number three.

lemma *poly-PhiC-of-real*: *poly PhiC* (*complex-of-real x*) = *complex-of-real* (*poly Phi x*)
⟨*proof*⟩

lemma *real-roots-PhiC*: {*z*. *poly PhiC z* = *0* ∧ *z* ∈ ℝ} = *complex-of-real* ‘ {*x*. *poly Phi x* = *0*}
⟨*proof*⟩

theorem *card-real-roots-PhiC*: *card* {*z*. *poly PhiC z* = *0* ∧ *z* ∈ ℝ} = *3*
⟨*proof*⟩

Conjugation maps roots to roots (the coefficients are real).

lemma *cnj-poly-PhiC*: *poly PhiC* (*cnj z*) = *cnj* (*poly PhiC z*)
⟨*proof*⟩

lemma *cnj-root-PhiC*: *poly PhiC z* = *0* ⟹ *poly PhiC* (*cnj z*) = *0*
⟨*proof*⟩

Hence exactly two non-real roots.

theorem *card-nonreal-roots-PhiC*: *card* {*z*. *poly PhiC z* = *0* ∧ *z* ∉ ℝ} = *2*
⟨*proof*⟩

lemma *cnj-notreal*: *z* ∉ ℝ ⟹ *cnj z* ∉ ℝ
⟨*proof*⟩

lemma *cnj-ne-self-of-notreal*: *z* ∉ ℝ ⟹ *z* ≠ *cnj z*
⟨*proof*⟩

The two non-real roots form a single conjugate pair, so complex conjugation transposes them while fixing the three real roots.

lemma *nonreal-roots-conj-pair*:
obtains *a* **where** {*z*. *poly PhiC z* = *0* ∧ *z* ∉ ℝ} = {*a*, *cnj a*} **and** *a* ≠ *cnj a*
and *poly PhiC a* = *0* **and** *a* ∉ ℝ
⟨*proof*⟩

Summary of the root structure feeding the Galois-group argument.

theorem *PhiC-root-structure*:

card $\{z.\ poly\ PhiC\ z = 0\} = 5\ \wedge$
card $\{z.\ poly\ PhiC\ z = 0 \wedge z \in \mathbb{R}\} = 3\ \wedge$
card $\{z.\ poly\ PhiC\ z = 0 \wedge z \notin \mathbb{R}\} = 2\ \wedge$
$(\forall z.\ poly\ PhiC\ z = 0 \longrightarrow poly\ PhiC\ (cnj\ z) = 0)$
⟨*proof*⟩

6.5 Irreducibility of the quintic over the rationals

The complex quintic is the *of-int*-image of the integer quintic, equivalently the *of-rat*-image of its rational version.

lemma *PhiC-eq-map-of-int*: $PhiC = map\text{-}poly\ of\text{-}int\ PhiZ$
⟨*proof*⟩

lemma *map-of-rat-of-int-PhiZ*:
$map\text{-}poly\ of\text{-}rat\ (map\text{-}poly\ of\text{-}int\ PhiZ :: rat\ poly) = (PhiC :: complex\ poly)$
⟨*proof*⟩

theorem *irreducible-over-Rats-PhiC*: *irreducible-over* $(\mathbb{Q} :: complex\ set)\ PhiC$
⟨*proof*⟩

6.6 The Galois group of the quintic is not solvable

The quintic has rational (indeed integer) coefficients.

lemma *PhiC-poly-over-Rats*: $PhiC \in poly\text{-}over\ (\mathbb{Q} :: complex\ set)$
⟨*proof*⟩

Relabelling an involution that swaps exactly two points yields a transposition. Here τ is an involution of the finite set X enumerated by e, fixing every point except the pair $\{a, \tau\ a\}$.

lemma *pull-involution-two-points-transpose*:
fixes $e :: nat \Rightarrow complex$ **and** $X :: complex\ set$ **and** $\tau :: complex \Rightarrow complex$ **and** $n :: nat$
assumes *ebij*: *bij-betw* $e\ \{0..<n\}\ X$
and *tauX*: $\tau\ `\ X = X$
and *invol*: $\bigwedge x.\ x \in X \Longrightarrow \tau\ (\tau\ x) = x$
and a: $a \in X$ **and** *ta*: $\tau\ a \in X$ **and** *ane*: $a \neq \tau\ a$
and *fixed*: $\bigwedge x.\ x \in X \Longrightarrow x \neq a \Longrightarrow x \neq \tau\ a \Longrightarrow \tau\ x = x$
defines $i \equiv inv\text{-}into\ \{0..<n\}\ e\ a$ **and** $j \equiv inv\text{-}into\ \{0..<n\}\ e\ (\tau\ a)$
shows *pull* $n\ e\ (restrict\ \tau\ X) = Transposition.transpose\ i\ j$
⟨*proof*⟩

6.7 The main theorem

The Galois group of the quintic $x\hat{}5 - 4x + 2$ — the group of automorphisms of its splitting subfield of *complex* fixing $\mathbb{Q}$ — is not solvable. This will imply that the quintic is not solvable by radicals.

theorem *quintic-galois-group-not-solvable*:

defines $X \equiv \{z.\ poly\ PhiC\ z = 0\}$
defines $K \equiv generate\text{-}field\ (\mathbb{Q} \cup X)$
shows $\neg\ Group.solvable\ (field\text{-}auto\ K\ \mathbb{Q})\ (compose\ K)\ (identity\ K)$
⟨*proof*⟩

end

7 The quintic $x^5 - 4x + 2$ is not solvable by radicals

theory *Abel-Ruffini-Quintic*
imports
Radical-Normal-Closure — the forward direction: the normal-closure construction
Quintic-Example — concrete non-solvability of the quintic's Galois group
begin

The two halves of the argument meet here.

7.1 The main theorem

theorem *quintic-not-solvable-by-radicals*:
$\neg$ *solvable-by-radicals* ($\mathbb{Q}$ :: *complex set*) $\{r.\ poly\ PhiC\ r = 0\}$
⟨*proof*⟩

end

References

[1] M. Eberl. Sturm's theorem. *Archive of Formal Proofs*, 2014. https://isa-afp.org/entries/Sturm_Sequences.html, Formal proof development.

[2] T. mathlib Community. mathlib: `Mathlib.FieldTheory.AbelRuffini`. https://leanprover-community.github.io/mathlib4_docs/Mathlib/FieldTheory/AbelRuffini.html. Lean 4 / mathlib formalisation of the Abel–Ruffini theorem.