# Formalizing Galois Theory

Thomas Browning and Patrick Lutz

# The road to Galois theory

**Ongoing:** Abel-Ruffini

**Fall 2020:** Galois theory project

**Summer 2020:**
Berkeley Lean Seminar

**December 2018:** Starts with project by students at Imperial (especially Kenny Lau)

Contributors 5

# Summary: Imperial project

- December 2018—September 2020
- Included several Imperial students, a lot of work done by Kenny Lau
- Set up many basic definitions: Algebra, subalgebra, field extensions, fixed field of a group action, …
- Constructed splitting fields and algebraic closure
- Proved several key theorems

```
/-- Auxiliary construction to a splitting field of a polynomial. Uses induction on the degree. -/
def splitting_field_aux (n : ℕ) : Π {α : Type u} [field α], by exactI Π (f : polynomial α),
  f.nat_degree = n → Type u :=
nat.rec_on n (λ α _ _ _, α) $ λ n ih α _ f hf, by exactI
ih f.remove_factor (nat_degree_remove_factor' hf)
```

```
/-- The canonical algebraic closure of a field, the direct limit of adding roots to the field for each polynomial over the field. -/
def algebraic_closure : Type u :=
ring.direct_limit (algebraic_closure.step k) (λ i j h, algebraic_closure.to_step_of_le k i j h)
```

# Summary: Imperial project

Three theorems especially important for the Galois correspondence

- **Theorem (linear independence of characters):** if $E/F$ is a field extension and $H$ is a subgroup of $\mathrm{Aut}(E/F)$ then $[E : E^H] \leq |H|$
- **Theorem:** if $E/F$ is a field extension and $K$ is an intermediate field then $|\mathrm{Aut}(E/K)| \leq [E : K]$
- **Theorem:** if $E$ is a field and $G$ is a group action on $E$ then $E/E^G$ is Galois

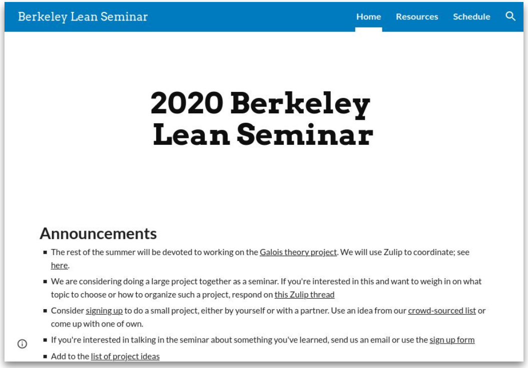
```
lemma dim_le_card : vector_space.dim (fixed_points G F) F ≤ fintype.card G :=

instance separable : is_separable (fixed_points G F) F :=

instance normal : normal (fixed_points G F) F :=
```

# Summary: Berkeley Lean Seminar

- Natural number game, Patrick Massot tutorial, small independent projects
- **Attendance:** 35 (week 1) → 8 (week 12)
- **Places where we lost people:** downloading Lean/VS Code, after the natural number game, Massot exercise 0080




- **Some projects:** De Bruijn–Erdős theorem, Bolzano-Weierstrass theorem, Chinese remainder theorem
- At the end, a few of us decided to work on Galois theory
- We'd be happy to discuss what we learned running this seminar

Contributors 5

# Summary: Galois theory project

- Adjoining elements to fields
- Primitive element theorem

```
theorem exists_primitive_element [finite_dimensional F E] (F_sep : is_separable F E) :
  ∃ α : E, F⟮α⟯ = ⊤ :=
```

- Galois correspondence

```
def intermediate_field_equiv_subgroup [finite_dimensional F E] [is_galois F E] :
  intermediate_field F E ≃o order_dual (subgroup (E ≃ₐ[F] E)) :=
```

- $E/F$ is Galois (i.e. normal and separable) $\leftrightarrow$ The fixed field of $\mathrm{Aut}(E/F)$ is $F$

  $\leftrightarrow |\mathrm{Aut}(E/F)| = [E : F]$

  $\leftrightarrow$ $E$ is the splitting field of a separable polynomial

```
theorem tfae [finite_dimensional F E] :
  tfae [is_galois F E,
    intermediate_field.fixed_field (⊤ : subgroup (E ≃ₐ[F] E)) = ⊥,
    fintype.card (E ≃ₐ[F] E) = findim F E,
    ∃ p : polynomial F, p.separable ∧ p.is_splitting_field F E] :=
```

# This has been done before

```
Lemma splitting_galoisField K E :
  reflect (exists p, [/\ p \is a polyOver K, separable_poly p
                     & splittingFieldFor K p E])
          (galois K E).
Proof.
apply: (iffP and3P) => [[sKE sepKE nKE]|[p [Kp sep_p [r Dp defE]]]].
  rewrite (eq_adjoin_separable_generator sepKE) // in nKE *.
  set a := separable_generator K E in nKE *; exists (minPoly K a).
  split; first 1 [exact: minPolyOver | exact/separable_generatorP].
  have [r /= /allP Er splitKa] := normalFieldP nKE a (memv_adjoin _ _).
  exists r; first by rewrite splitKa eqpxx.
  apply/eqP; rewrite eqEsubv; apply/andP; split.
    by apply/Fadjoin_seqP; split => //; apply: subv_adjoin.
  apply/FadjoinP; split; first exact: subv_adjoin_seq.
  by rewrite seqv_sub_adjoin // -root_prod_XsubC -splitKa root_minPoly.
have sKE: (K <= E)%VS by rewrite -defE subv_adjoin_seq.
split=> //; last by apply/splitting_normalField=> //; exists p; last exists r.
rewrite -defE; apply/separable_Fadjoin_seq/allP=> a r_a.
by apply/separable_elementP; exists p; rewrite (eqp_root Dp) root_prod_XsubC.
Qed.
```


Galois theory is in Coq's mathcomp

Proved as part of the odd order theorem project

Includes primitive element theorem and Galois correspondence (and more)

# A complete lattice for free

One of the first things we did was define the notion of adjoining a set of elements (contained in a field extension) to a field

Very useful structure defined by Anne Baanen: `intermediate_field F E`

Seems necessary to prove lots of little lemmas about the partial order on intermediate fields. But we can actually get a lot of them for free using `adjoin`

**Key trick:** `adjoin` and `coe` form a Galois insertion of `intermediate_field F E` into `set E`. Lattice instance comes for free from lattice on `set E`

# A complete lattice for free

**Key trick:** `adjoin` and `coe` form a Galois insertion of `intermediate_field F E` into `set E`. Lattice instance comes for free from lattice on `set E`

**Definition:** If $E/F$ is a field extension and $S$ is a subset of $E$ then $F(S)$ is the subfield of $E$ generated by $F$ and $S$

**Definition:** Suppose $P$ and $Q$ are two partial orders. A Galois insertion of $Q$ into $P$ is a pair of order-preserving functions $f : P \to Q$ and $g : Q \to P$ such that

- $f(p) \leq q \leftrightarrow p \leq g(q)$ (galois connection)
- and $f \circ g = id$

**Theorem:** If there is a Galois insertion from $Q$ into $P$ and if $P$ is a complete lattice then so is $Q$

# A complete lattice for free

- `adjoin` is a function `set E → intermediate_field F E`

```
/-- `adjoin F S` extends a field `F` by adjoining a set `S ⊆ E`. -/
def adjoin : intermediate_field F E :=
```

- `coe` is a function `intermediate_field F E → set E`
- Together they form a Galois insertion. The main thing required is to prove the following simple lemma

```
lemma adjoin_le_iff {S : set E} {T : intermediate_field F E} : adjoin F S ≤ T ↔ S ≤ T :=
```

- We can then define the galois insertion and get

```
instance : complete_lattice (intermediate_field F E) :=
galois_insertion.lift_complete_lattice intermediate_field.gi
```

- E.g., `sup K L = adjoin F (K ∪ L)`

# Induction scheme for intermediate fields

Two common ways to prove things about a field extension $E/F$ of finite degree

- Induction on $[E : F]$
- Pick $a_1, a_2, \ldots, a_n$ so that $E = F(a_1, a_2, \ldots, a_n)$ and use induction on $n$

Both of these have downsides in formalization

**Solution:** Define a custom induction scheme for intermediate fields

```
lemma induction_on_adjoin_finset (S : finset E) (P : intermediate_field F E → Prop) (base : P ⊥)
  (ih : ∀ (K : intermediate_field F E) (x ∈ S), P K → P ↑K⟮x⟯) : P (adjoin F ↑S) :=

lemma induction_on_adjoin [fd : finite_dimensional F E] (P : intermediate_field F E → Prop)
  (base : P ⊥) (ih : ∀ (K : intermediate_field F E) (x : E), P K → P ↑K⟮x⟯)
  (K : intermediate_field F E) : P K :=
```

# Proof of the Galois Correspondence

We used the primitive element theorem to prove the Galois correspondence.

**Definition:** If $E/F$ is a finite degree extension then an element $a$ of $E$ is a primitive element if $E = F(a)$

**Theorem (Primitive element theorem):** Every finite degree separable extension has a primitive element

**Theorem (Galois correspondence):** If $E/F$ is a finite degree Galois extension then there is an order-reversing bijection between intermediate fields of $E/F$ and subgroups of $\mathrm{Aut}(E/F)$

$H \mapsto E^H =$ elements of $E$ fixed by $H$

$K \mapsto \mathrm{Aut}(E/K) =$ elements of $\mathrm{Aut}(E/F)$ which fix $K$ pointwise

# Proof of the Galois Correspondence

The Galois correspondence follows from two numerical facts:

1. $[E : E^H] \leq |H|$ ← Proved by Kenny Lau
2. If $E/F$ is Galois and if $K$ is an intermediate field, then $|\mathrm{Aut}(E/K)| = [E : K]$

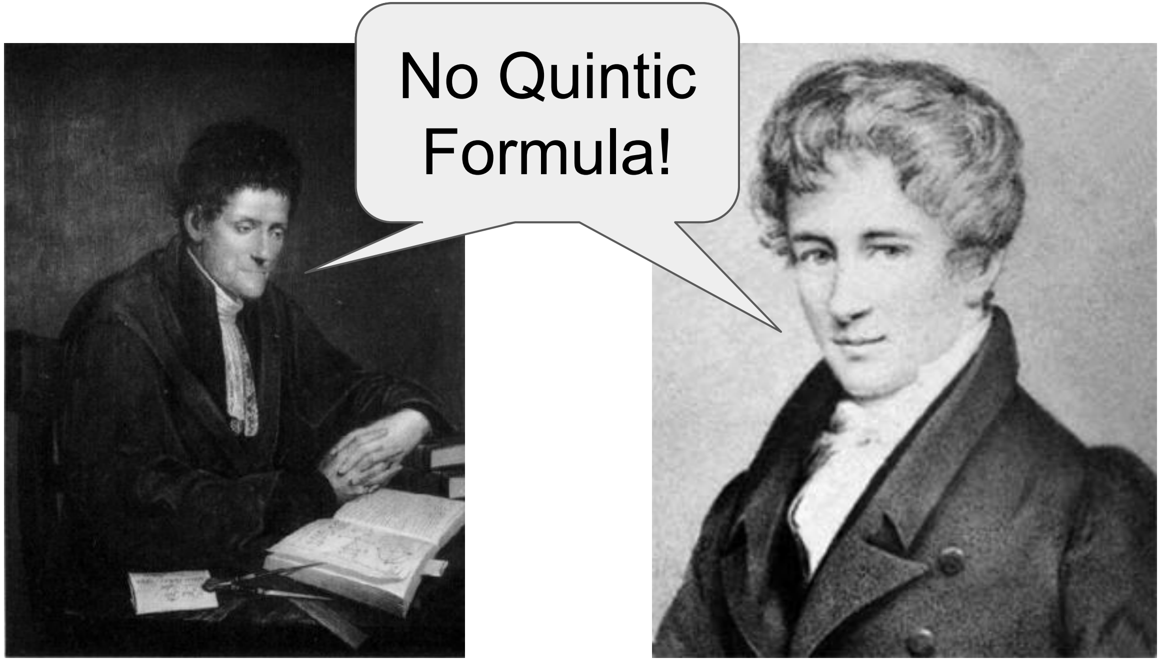
Can be proved using the primitive element theorem

**Proof of (2):**

- Show that $E/F$ Galois $\rightarrow$ $E/K$ Galois
- Let $a$ be a primitive element for $E/K$, $m(x)$ the minimal polynomial for $a$ over $K$
- $E = K(a) = K[x]/(m)$
- Replace $E$ by $K[x]/(m)$ in (2) and show that both sides are equal to $\mathrm{degree}(m)$

# Abel-Ruffini theorem

There is a quadratic formula, a cubic formula, and a quartic formula …



14. **Euler's Summation of 1 + (1/2)^2 + (1/3)^2 + ....**
HOL Light, John Harrison: statement
Isabelle, Manuel Eberl: statement
Metamath, Mario Carneiro: statement
Coq, not in contribs, Jean-Marie Madiot: statement
Mizar, Karol Pak & Artur Kornilowicz: statement

15. **Fundamental Theorem of Integral Calculus**
HOL Light, John Harrison: statement
Isabelle, Jacques D. Fleuriot: statement
Metamath, Mario Carneiro: statement
*Coq, C-CoRN, Luís Cruz-Filipe:* statement
Mizar, Noboru Endou & Katsumi Wasaki & Yasunari Shidama: statement
ProofPower, Rob Arthan: statement
PVS, NASA library, Ricky Butler
ACL2, Matt Kaufmann

16. *Insolvability of General Higher Degree Equations*

17. **De Moivre's Theorem**
HOL Light, John Harrison: statement
Isabelle, Jacques D. Fleuriot: statements
Metamath, Steve Rodriguez: statement
Coq, contrib, Frédérique Guilhot: statement
Mizar, Takashi Mitsuishi & Noboru Endou & Keiji Ohkubo: statement
Lean, Abhimanyu Pallavi Sudhir: statement
ProofPower, Rob Arthan: statement

18. **Liouville's Theorem and the Construction of Transcendental Numbers**
HOL Light, John Harrison: statements
Isabelle, Manuel Eberl: statement
Metamath, Stefan O'Rear: statement
*Coq, C-CoRN, Valentin Blot:* statement
Mizar, Artur Kornilowicz, Adam Naumowicz & Adam Grabowski: statement
Lean, Jujian Zhang: statement

# Abel-Ruffini theorem

- There is no formula using only radicals and field operations for roots of polynomials of degree ≥ 5
- Can be proved using Galois theory
- One of the five remaining theorems on Freek's list
- Not clear why it hasn't been done yet
- There is currently also a project underway to formalize it in Coq

# Abel-Ruffini overview: main idea

If a complex number is solvable by radicals … $\sqrt{\sqrt{-3}+\sqrt[3]{2}}$

Then adjoining one radical at a time gives a tower of fields …

$$\mathbb{Q}\left(\sqrt{-3}, \sqrt[3]{2}, \sqrt{\sqrt{-3}+\sqrt[3]{2}}\right) \qquad D_6$$

$$\mathbb{Q}\left(\sqrt{-3}, \sqrt[3]{2}\right) \qquad S_3$$

$$\mathbb{Q}\left(\sqrt{-3}\right) \qquad C_2$$

$$\mathbb{Q} \qquad 1$$

Each step is abelian, so the Galois group stays solvable

So $\sqrt{\sqrt{-3}+\sqrt[3]{2}}$ has solvable Galois group

# Abel-Ruffini overview: more details

**A few caveats to the previous slide:**

- Need the final field to be a Galois extension so it's not always enough to adjoin just the radicals appearing in the formula
- Prove that the final field has solvable Galois group by working backwards, showing its Galois group over each intermediate field is solvable (we will take a different route)

**Proof sketch of Abel-Ruffini theorem:**

- Show that if a complex number is solvable by radicals then it is contained in a Galois field extension with solvable Galois group (idea from previous slide)
- Find an algebraic complex number whose Galois group is $S_5$
- Show $S_5$ is not solvable

# The plan for Abel-Ruffini

Define “solvable by radicals”

If $E/F$ is a field extension, an element of $E$ is solvable by radicals if it can be written as a formula involving elements of $F$, field operations, and radicals

This is naturally an inductive type with constructors corresponding to elements of $F$, each of the field operations, and taking radicals

# The plan for Abel-Ruffini

Define “solvable by radicals”

Solvable groups

We defined a solvable group in terms of the derived series.

- If $H$ is a subgroup of $G$, $[H, H]$ is the subgroup generated by its commutators $[g, h] = ghg^{-1}h^{-1}$
- Derived series of a group: $G^{(0)} = G$, $G^{(1)} = [G^{(0)}, G^{(0)}]$, … $G^{(n+1)} = [G^{(n)}, G^{(n)}]$
- $G$ is solvable if $G^{(n)} = \bot$ for some $n$

Various facts about solvable groups needed: abelian groups are solvable, quotients of solvable groups are solvable, etc…

# The plan for Abel-Ruffini

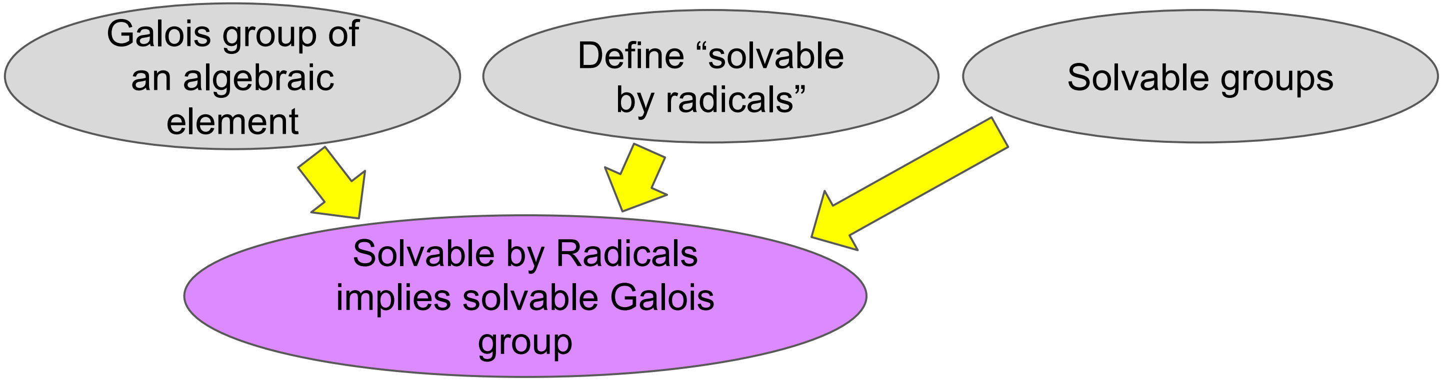
Galois group of an algebraic element

Define “solvable by radicals”

Solvable groups

```
def gal (p : polynomial F) := p.splitting_field ≃ₐ[F] p.splitting_field
gal (minimal_polynomial (is_integral α))
```

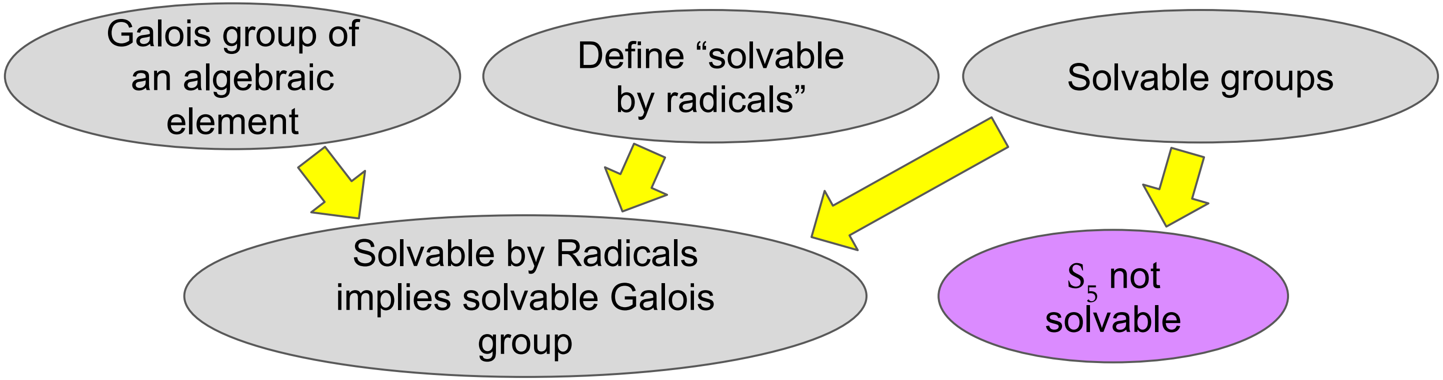
# The plan for Abel-Ruffini




Proved by induction on the “solvable by radicals” type.

Hardest part is radical case. The key lemma is: If $F$ has all the $n^{th}$ roots of unity and if $a$ is in $F$ then $a^{1/n}$ has abelian Galois group.

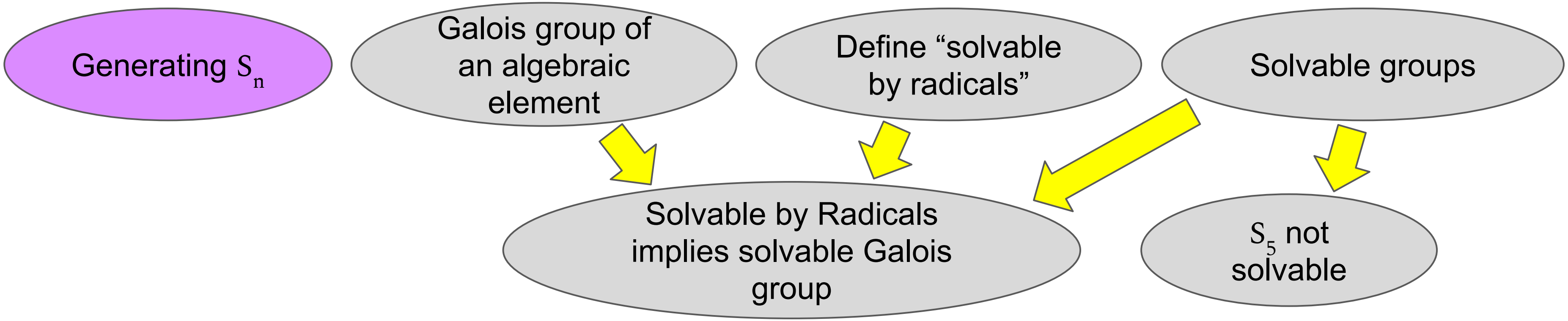
# The plan for Abel-Ruffini




Traditionally a consequence of the fact that $A_5$ is simple

But it’s possible to give an easier direct proof

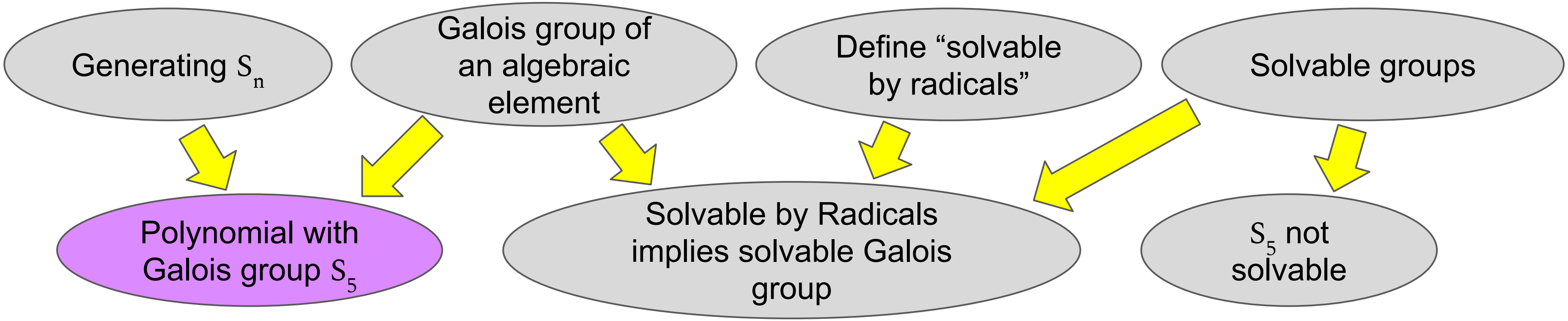
# The plan for Abel-Ruffini




If $p$ is prime then any $p$ cycle and transposition together generate $S_p$:

- Take a power of the cycle so that the transposition swaps two adjacent elements of the cycle
- Cycle and adjacent transposition → All adjacent transpositions
  → All transpositions → All of $S_n$

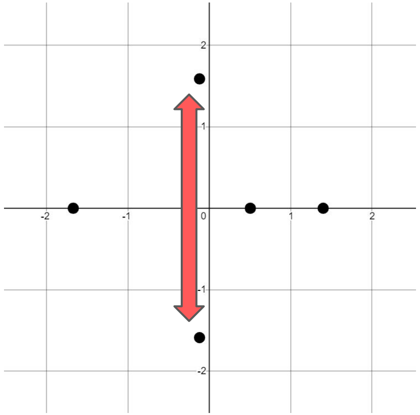
# The plan for Abel-Ruffini

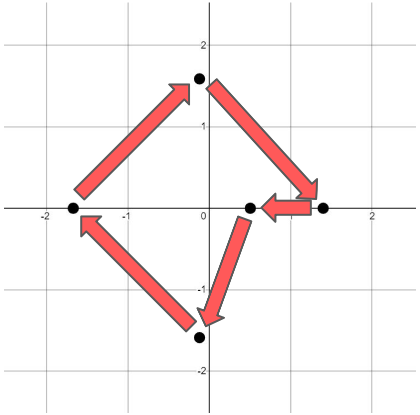



Ex: $x^5 - 6x + 3$

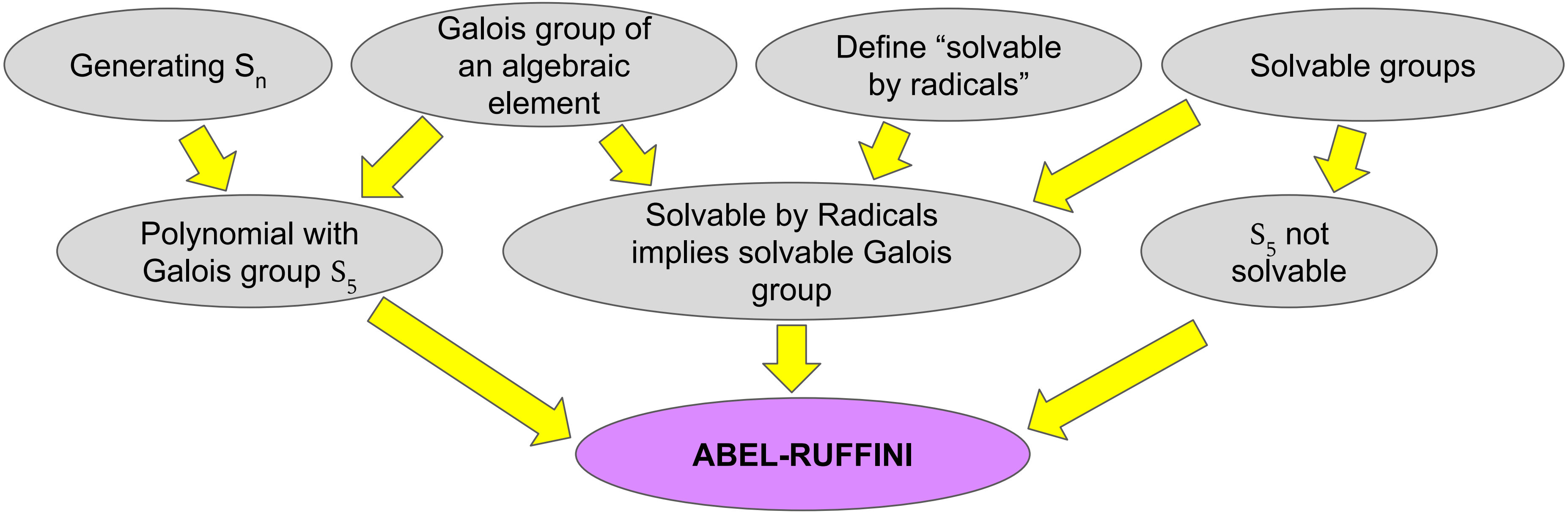
3 real roots

2 conjugate roots

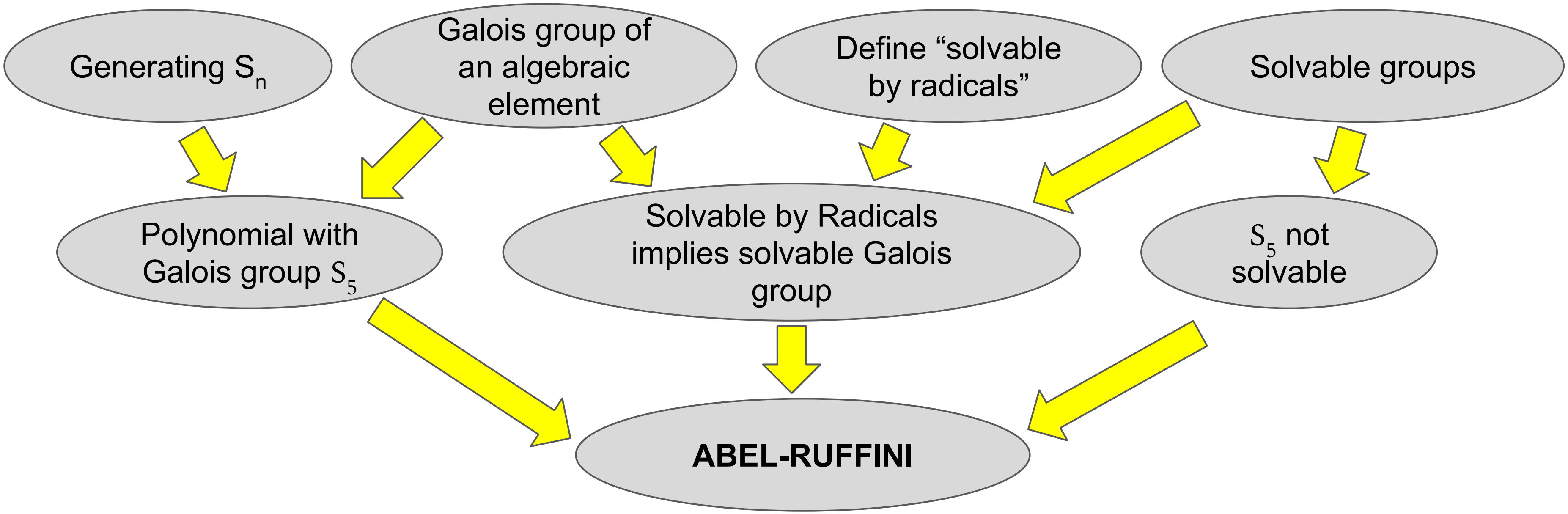




# The plan for Abel-Ruffini

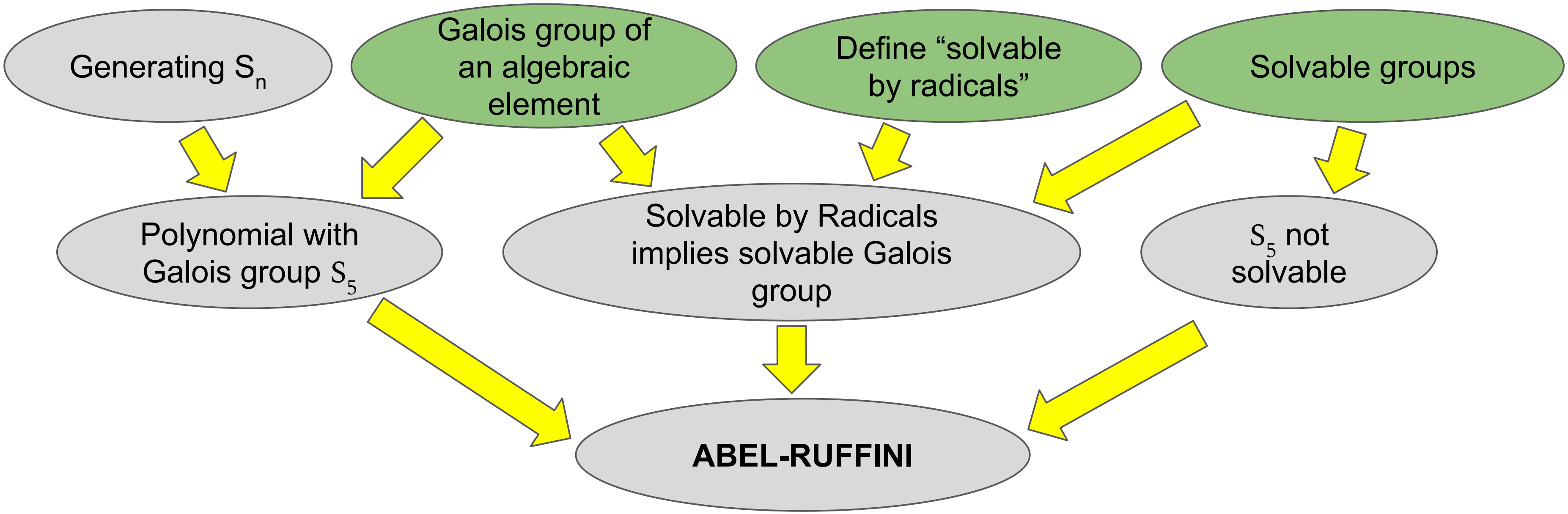


# The plan for Abel-Ruffini



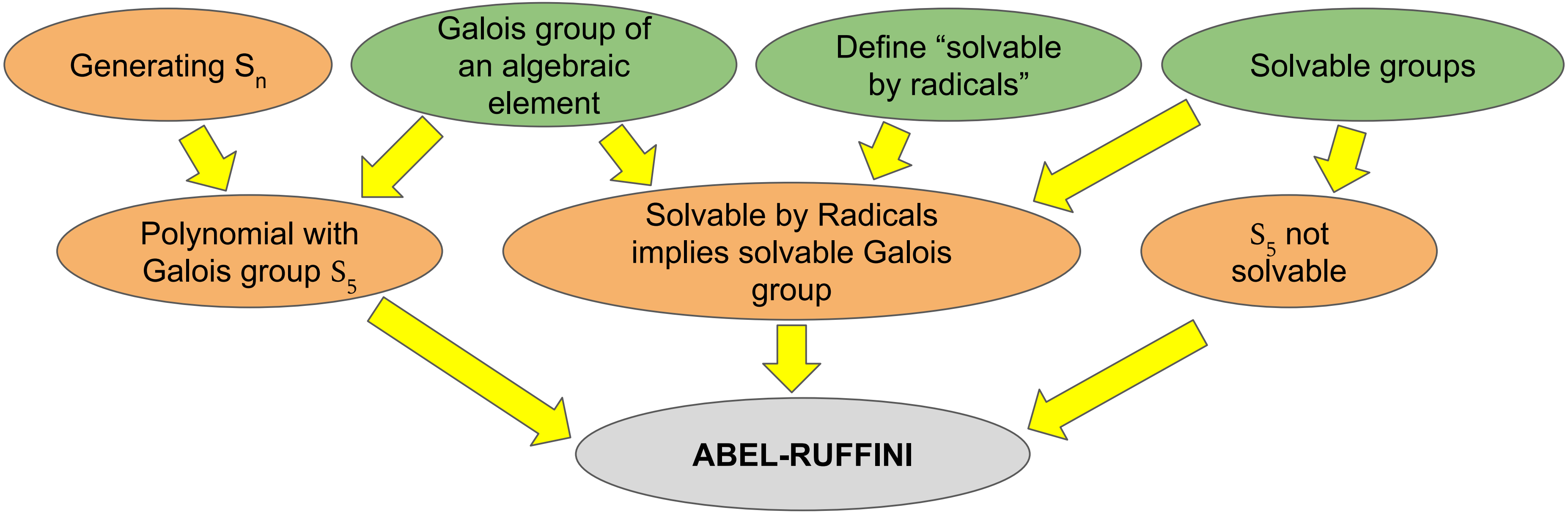

**What is the current status of this project?**

# The plan for Abel-Ruffini



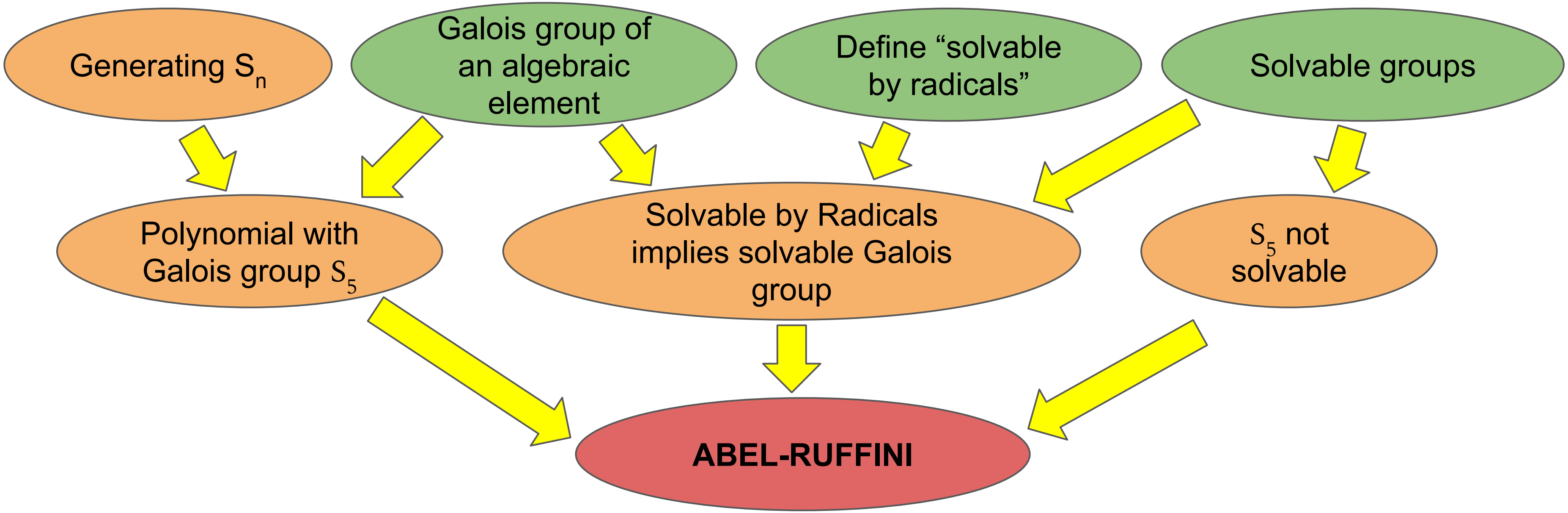

**What is the current status of this project?**

# The plan for Abel-Ruffini




**What is the current status of this project?**

# The plan for Abel-Ruffini




**What is the current status of this project?**

# The SBR type

Inductively define “solvable by radicals”

```
inductive is_SBR : E → Prop
| base (a : F) : is_SBR (algebra_map F E a)
| add (a b : E) : is_SBR a → is_SBR b → is_SBR (a + b)
| neg (α : E) : is_SBR α → is_SBR (-α)
| mul (α β : E) : is_SBR α → is_SBR β → is_SBR (α * β)
| inv (α : E) : is_SBR α → is_SBR α⁻¹
| rad (α : E) (n : ℕ) (hn : n ≠ 0) : is_SBR (α^n) → is_SBR α
```

# The SBR type

Bundle into an `intermediate_field`

```
def SBR : intermediate_field F E :=
{ carrier := is_SBR F,
  zero_mem' := by { convert is_SBR.base (0 : F), rw ring_hom.map_zero },
  add_mem' := is_SBR.add,
  neg_mem' := is_SBR.neg,
  one_mem' := by { convert is_SBR.base (1 : F), rw ring_hom.map_one },
  mul_mem' := is_SBR.mul,
  inv_mem' := is_SBR.inv,
  algebra_map_mem' := is_SBR.base }
```

# The SBR type

`SBR` has an induction scheme (coming from `is_SBR.rec`)

```
lemma induction (P : SBR F E → Prop)
(base : ∀ α : F, P (algebra_map F (SBR F E) α))
(add : ∀ α β : SBR F E, P α → P β → P (α + β))
(neg : ∀ α : SBR F E, P α → P (-α))
(mul : ∀ α β : SBR F E, P α → P β → P (α * β))
(inv : ∀ α : SBR F E, P α → P α⁻¹)
(rad : ∀ α : SBR F E, ∀ n : ℕ, n ≠ 0 → P (α^n) → P α)
(α : SBR F E) : P α :=
```

# The SBR type

**Recall:** Standard proof of Abel-Ruffini theorem is to form a tower of radical extensions. Have to worry about ending up with something Galois and proving solvability by backwards induction

**Instead:** We show by induction that if $a$ is `SBR` then the splitting field of the minimal polynomial of $a$ has solvable Galois group. Still need to do induction.

```
theorem solvable_gal_of_SBR (α : SBR F E) :
  is_solvable (gal (minimal_polynomial (is_integral α))) :=
```

# Proving $S_5$ is not solvable

**Recall:**

- We defined a group to be solvable if its derived series is eventually trivial
- Derived series: $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ = subgroup generated by $ghg^{-1}h^{-1}$ where $g$ and $h$ are in $G^{(n)}$
- $G^{(n)}$ is always a normal subgroup of $G$

We want to show that $S_5^{(n)}$ is never the trivial subgroup

- We can just show that it always contains $(1\ 2\ 3)$
- If $S_5^{(n)}$ contains $(1\ 2\ 3)$ then we can conjugate to get $(1\ 4\ 3)$ and $(2\ 5\ 3)$
- $(1\ 4\ 3)(2\ 5\ 3)(1\ 4\ 3)^{-1}(2\ 5\ 3)^{-1} = (1\ 4\ 3)(2\ 5\ 3)(1\ 3\ 4)(2\ 3\ 5) = (1\ 2\ 3)$

# What's next after Abel-Ruffini?

- Constructible numbers and compass-and-straightedge constructions?
- Number fields and algebraic number theory?

## Missing theorems from Freek Wiedijk's list of 100 theorems

These theorems are not yet formalized in Lean. Here is the list of the formalized theorems.

- 5: Prime Number Theorem
- 6: Godel's Incompleteness Theorem
- 8: The Impossibility of Trisecting the Angle and Doubling the Cube
- 9: The Area of a Circle