Galois Theory

An Information-Theoretic Perspective

A Supplement to *Galois Theory: A Self-Contained Exposition*

Abstract

This supplement reframes the central objects of Galois theory — field extensions, Galois groups, solvability — in the language of information and uncertainty. No new mathematics is introduced; every statement here is a restatement of a theorem from the main text. The goal is to make the logical structure of the theory viscerally clear: why the Galois group is the right object, why solvability is the right condition, and why A_5 is the precise obstruction to the quintic. We assume familiarity with the main exposition.

Contents

1 The Setup: Roots as Hidden Information

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n with roots $r_1, \ldots, r_n$. The roots exist — they live in the splitting field K — but they are hidden from you. You begin with knowledge only of the coefficients.

The central question of Galois theory can be rephrased as follows:

> **Information-theoretic restatement.** Can you fully determine the roots $r_1, \ldots, r_n$ by sending yourself a finite sequence of messages, where each message is a radical (an n-th root of something you already know)?

Each field extension in the tower

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_k = K$$

represents a **state of knowledge**. You start at $\mathbb{Q}$ (knowing only coefficients) and must reach K (knowing all roots). Each step $F_i \to F_{i+1}$ is one message — one piece of new information acquired by adjoining a radical.

The question is whether such a protocol exists.

2 What You Know at Each Stage

2.1 Starting at $\mathbb{Q}$: Symmetric Knowledge

At the base field $\mathbb{Q}$, you know the coefficients of f. By Vieta's formulas these are the elementary symmetric functions of the roots:

$$e_1 = \sum_i r_i, \quad e_2 = \sum_{i<j} r_i r_j, \quad \ldots, \quad e_n = r_1 r_2 \cdots r_n.$$

These functions are invariant under every permutation of the roots. Swapping r_1 and r_2, for instance, does not change any e_k.

This means: from the coefficients alone, you cannot tell the roots apart. Every permutation of $\{r_1, \ldots, r_n\}$ is consistent with your knowledge. Your uncertainty is total, and it is precisely measured by S_n — the group of all permutations.

Definition 2.1 (Galois Group as Uncertainty Set)**.** At field F_i in the tower, the **Galois group** $\mathrm{Gal}(K/F_i)$ is the set of all permutations of the roots that are consistent with everything known in F_i:

$$\mathrm{Gal}(K/F_i) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma \text{ fixes every element of } F_i\}.$$

This is not a metaphor. The Galois group is *literally* the set of worlds you cannot yet distinguish. A permutation σ remains in the group exactly as long as you have no information that could rule it out.

> **Analogy.** Think of a locked safe with a hidden combination. Your "uncertainty set" is the set of all combinations consistent with what you know. Initially (knowing nothing) it is all 10^n sequences. Each digit you learn eliminates nine-tenths of the possibilities. The "group shrinks" as you gain information. You are done when only

one combination remains.

2.2 Adjoining a Radical: Ruling Out Permutations

When you adjoin an element α to your current field, you gain information. Specifically, any automorphism σ that would change the value of α — i.e., $\sigma(\alpha) \neq \alpha$ — is now **ruled out**. It is no longer consistent with your knowledge.

The Galois group shrinks from $\mathrm{Gal}(K/F_i)$ to $\mathrm{Gal}(K/F_{i+1})$, the subgroup of permutations that also fix α.

The key diagram is:

$$\underbrace{\mathrm{Gal}(K/F_i)}_{\text{uncertainty before}} \supset \underbrace{\mathrm{Gal}(K/F_{i+1})}_{\text{uncertainty after}} \qquad \text{with quotient} \quad \frac{\mathrm{Gal}(K/F_i)}{\mathrm{Gal}(K/F_{i+1})} \cong \underbrace{\mathbb{Z}/m\mathbb{Z}}_{\text{information gained}}$$

The quotient group is the **information content** of the adjunction: it measures precisely what was ruled out.

3 The Discriminant: A First Information Gain

The discriminant of f is:

$$\Delta = \prod_{i<j} (r_i - r_j)^2.$$

Its square root $\sqrt{\Delta} = \prod_{i<j}(r_i - r_j)$ is **not** symmetric — it changes sign under any transposition of two roots.

Adjoining $\sqrt{\Delta}$ to $\mathbb{Q}$ gives you one piece of information: the sign of $\prod_{i<j}(r_i - r_j)$. Concretely:

- Any odd permutation (a transposition, or product of an odd number of transpositions) would negate $\sqrt{\Delta}$.
- Since you now *know* the value of $\sqrt{\Delta}$, any odd permutation is **inconsistent** with your knowledge.
- Odd permutations are ruled out.

The uncertainty set shrinks:

$$S_n \longrightarrow A_n.$$

The quotient is $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$: you gained exactly one bit of information — the parity of the roots' ordering.

Interpretation. The discriminant carries exactly one binary piece of information about the roots: their sign structure. Adjoining $\sqrt{\Delta}$ uses that one bit to halve the uncertainty set.

4 What a Cyclic Quotient Means Informationally

Each step in a radical tower adjoin α with $\alpha^n \in F_i$. The automorphisms that are ruled out are those that send α to one of the other n-th roots: $\omega\alpha, \omega^2\alpha, \ldots, \omega^{n-1}\alpha$, where $\omega = e^{2\pi i/n}$.

These n possible values are **equally spaced** in an algebraic sense — they form a cyclic orbit of size n under multiplication by ω. The ambiguity that was present before adjoining α was: which of these n values is α? This ambiguity is generated by a single operation (multiply by ω), applied up to n times.

> **Cyclic quotient = single-generator uncertainty.** A cyclic quotient $\mathbb{Z}/n\mathbb{Z}$ at step i means the remaining uncertainty at that step has a single fundamental ambiguity, repeated n times. Adjoining the radical collapses all n possibilities to one.

This is informationally **clean**: one radical, one type of ambiguity, completely resolved in one step.

Compare with a non-cyclic quotient: the remaining uncertainty would have two or more independent generators — it would require more than one radical to fully resolve.

5 The Galois Group as a Complete Uncertainty Budget

The full tower of uncertainties is:

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\}$$

where $G_i = \mathrm{Gal}(K/F_i)$. You begin with total uncertainty $G_0 = \mathrm{Gal}(K/\mathbb{Q})$ and must reach $G_k = \{e\}$ — only the identity permutation remains, meaning the roots are fully determined.

Each step reduces uncertainty:

$$\text{information gained at step } i \;=\; G_i/G_{i+1}.$$

For this to be achievable by radicals, each quotient G_i/G_{i+1} must be cyclic — since each radical resolves exactly one cyclic layer.

> **Solvability restated.** The polynomial f is solvable by radicals if and only if the total uncertainty $G = \mathrm{Gal}(K/\mathbb{Q})$ can be decomposed into a sequence of cyclic uncertainty layers:
>
> $$G = G_0 \supset G_1 \supset \cdots \supset \{e\}, \qquad G_i/G_{i+1} \text{ cyclic for all } i.$$
>
> This is exactly the definition of G being a **solvable group**.

The word "solvable" is not a coincidence. A solvable group is precisely one whose uncertainty can be communicated in cyclic messages. The algebraic and informational definitions are the same thing.

6 The Protocol Interpretation

A solution by radicals is a **communication protocol**:

Step 1. Identify the next layer of uncertainty $G_i/G_{i+1} \cong \mathbb{Z}/m\mathbb{Z}$.

Step 2. Construct the radical α that carries exactly the information needed to resolve this layer.

Step 3. Adjoin α: the uncertainty set shrinks from G_i to G_{i+1}.

Step 4. Repeat until $G_k = \{e\}$.

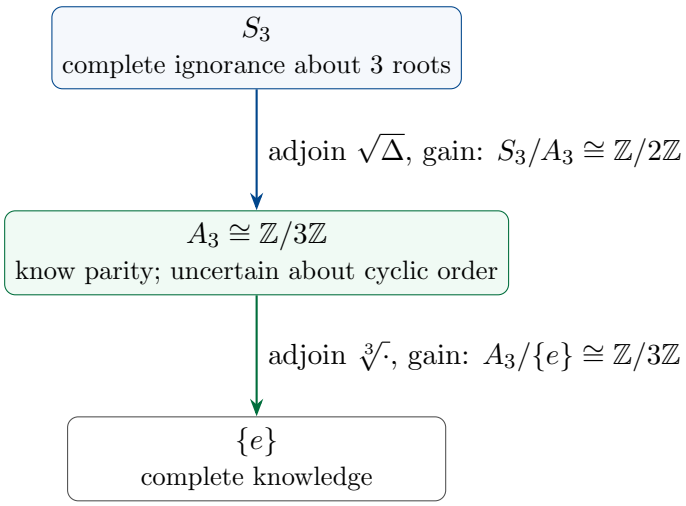
The protocol terminates in finitely many steps if and only if the group is solvable. Each "message" in the protocol is one radical.

Analogy with 20 questions. The game of 20 Questions is solvable because every binary question eliminates half the search space, and after enough binary steps, the space is exhausted. A polynomial is "solvable" in the same sense: each radical is a question with a cyclic (n-valued) answer, and the game terminates if the Galois group can be fully resolved by such questions. An unsolvable polynomial is one where some residual ambiguity cannot be addressed by any such question.

7 The Cubic and Quartic: Protocols Made Explicit

7.1 The Cubic (S_3)

Starting uncertainty: S_3 — complete ignorance about three roots.



Two radicals. Two cyclic layers. Two clean information gains. This is Cardano's formula, described in the language of uncertainty reduction.

The discriminant tells you the sign structure of the roots. The cube root then pins down their cyclic position. Together, they fully determine all three roots.

7.2 The Quartic (S_4)

The quartic requires a longer protocol, passing through A_4 and the Klein four-group $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$:

$$S_4 \supset A_4 \supset V_4 \supset \mathbb{Z}/2\mathbb{Z} \supset \{e\}$$

with quotients $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ — all cyclic.
At each step:

- $S_4 \to A_4$: adjoin $\sqrt{\Delta}$, learn parity.
- $A_4 \to V_4$: adjoin a cube root, learn the coarser cyclic structure.
- $V_4 \to \mathbb{Z}/2\mathbb{Z}$: adjoin a square root, resolve one sign ambiguity.
- $\mathbb{Z}/2\mathbb{Z} \to \{e\}$: adjoin another square root, resolve the last sign.

This is Ferrari's method. Four radicals, four cyclic layers, four information gains.

8 Why A_5 Is the Obstruction

8.1 The Simplicity of A_5

For $n \geq 5$, the alternating group A_n is **simple**: it has no normal subgroups other than $\{e\}$ and itself.

In uncertainty terms: A_n is an **irreducible uncertainty**. There is no element α you could adjoin that would partially resolve it — that is, rule out some but not all permutations in A_n while leaving a proper normal subgroup intact.

Why not? Because any such α would be fixed by a proper normal subgroup $H \trianglelefteq A_n$. But A_n is simple: the only proper normal subgroup is $\{e\}$. So α would either be fixed by all of A_n (meaning it was already in your field — no information gained) or fixed by only $\{e\}$ (meaning it distinguishes all $|A_n|$ possibilities at once — not a radical step, which can resolve at most a cyclic layer).

> **The core obstruction.** A radical can only resolve a cyclic layer of uncertainty. A_5 contains no cyclic layers — it is simple. Therefore no radical can make progress against the uncertainty represented by A_5. Every adjunction either gains nothing or gains everything, and gaining everything at once requires a degree-$|A_5| = 60$ extension in a single step, which is not a radical.

8.2 Formalizing the Obstruction

The derived series of S_5 is:

$$S_5 \supset A_5 \supset A_5 \supset \cdots$$

The series stalls at A_5 because $[A_5, A_5] = A_5$ — the commutator subgroup of A_5 is A_5 itself. There is no abelian (let alone cyclic) quotient available. The group cannot be "peeled" further.

In protocol terms: you can reduce from S_5 to A_5 in one step (adjoin $\sqrt{\Delta}$, gain one bit). But then you are stuck. No radical carries information about the A_5-uncertainty. The protocol cannot continue.

Impossibility. For a polynomial with Galois group S_5: you can learn the parity of the roots. Then you are permanently stuck. The remaining uncertainty — represented by A_5 — is informationally atomic, and radicals cannot address it.

8.3 No Finite Protocol Exists

The argument generalizes. For any polynomial f whose Galois group G contains a copy of A_5 in its derived series, the derived series will stall at that copy. The total uncertainty cannot be decomposed into cyclic layers. No finite sequence of radicals suffices.

Since the *generic* degree-n polynomial for $n \geq 5$ has Galois group S_n, and S_n contains A_n (which is simple and non-abelian for $n \geq 5$), there is no general formula for degree ≥ 5.

9 The Fundamental Theorem, Informationally

The Fundamental Theorem of Galois Theory states a bijection:

$$\{\text{subgroups of } \mathrm{Gal}(K/F)\} \longleftrightarrow \{\text{intermediate fields } F \subseteq E \subseteq K\}.$$

In information terms: every **partial state of knowledge** (an intermediate field E) corresponds to a **residual uncertainty set** (the subgroup $\mathrm{Gal}(K/E)$ of permutations still consistent with knowing E). The correspondence is perfect and invertible.

The order-reversing property is natural: **more knowledge** (larger E) means **fewer consistent permutations** (smaller $\mathrm{Gal}(K/E)$).

The normality condition has a clean reading too: $H \trianglelefteq \mathrm{Gal}(K/F)$ if and only if the corresponding intermediate field K^H is itself a Galois extension of F. In information terms: the partial knowledge represented by K^H is *unambiguous* relative to the base — there is a well-defined Galois group (and hence a well-defined uncertainty structure) for the sub-problem K^H/F.

10 A Dictionary

Algebraic object	**Informational meaning**
Base field $\mathbb{Q}$	Initial state: only symmetric knowledge
Splitting field K	Terminal state: all roots known
Intermediate field F_i	Current state of knowledge
$[F_{i+1} : F_i] = m$	Size of the information gain at step i
$\mathrm{Gal}(K/F_i)$	Current uncertainty set: permutations not yet ruled out
$\sigma \in \mathrm{Gal}(K/F_i)$	A "possible world" consistent with current knowledge
$\lvert\mathrm{Gal}(K/F_i)\rvert$ large	High uncertainty about the roots
$\lvert\mathrm{Gal}(K/F_i)\rvert = 1$	Complete knowledge: roots fully determined
Adjoining α	Receiving one piece of information
Quotient $G_i/G_{i+1} \cong \mathbb{Z}/m$	One cyclic message: m-valued, single-generator
Solvable group	Uncertainty decomposable into cyclic layers
Non-solvable group	Uncertainty contains an irreducible block
A_n simple ($n \geq 5$)	Irreducible block: no cyclic layers to peel
Radical extension	Protocol using only cyclic messages
f solvable by radicals	Protocol exists for f
f not solvable by radicals	No protocol exists; A_n blocks all progress
Normal subgroup	Sub-uncertainty with a well-defined own structure
Quotient group	Information content of one protocol step

11 The Deepest Statement

We can now state the content of Galois theory as precisely as possible in informational language.

A polynomial f has roots that are hidden from you. You can acquire information about them by adjoining radicals — each radical is a message with a cyclic structure. You are done when your uncertainty set is $\{e\}$.

Galois's theorem, informational form.

A polynomial is solvable by radicals if and only if its total uncertainty — the Galois group — admits a finite decomposition into cyclic uncertainty layers.

The polynomial is *not* solvable by radicals if and only if its Galois group contains an irreducible block of uncertainty that no cyclic message can address.

For $n \geq 5$: the alternating group A_n is that irreducible block. It is simple — it has no internal structure that a radical can resolve. A radical either gains nothing (the element was already known) or gains everything (impossible in one step). There is no middle ground. No protocol exists.

This is not a limitation of our cleverness. It is a structural property of the symmetry group of the roots. The roots of a general quintic are not inaccessible because the formula is complicated; they are inaccessible because the symmetry group of the problem contains a component — A_5 — whose internal structure is incompatible with the structure of any radical.

The question "can we solve this polynomial?" turns out to be the question "does this group decompose into cyclic layers?" — and Galois showed these two questions are the same question.