Galois Theory

Lectured by Alessio Corti
Scribed by Yu Coughlin

Autumn 2025

Contents

1 Motivation

In this section, fix a field $\mathbb{Q} \subset K \subset \mathbb{C}$. For some $\alpha \in \mathbb{C}$ we will use the notation:

$$K(\alpha) := \left\{ \frac{P(\alpha)}{Q(\alpha)} \in \mathbb{C} \;\middle|\; P, Q \in K[X],\ Q(\alpha) \neq 0 \right\}.$$

$K(\alpha_1, \dots, \alpha_n)$ is defined recursively.

Definition 1.0.1. Such an $\alpha \in \mathbb{C}$ is **algebraic over** K is there is some nonzero polynomial $P \in K[x]$ such that $P(\alpha) = 0$.

Consider $\mathbb{Q}(\sqrt{2})$, hours of highschool mathematics tells us we don't need to consider the entire large set of quotients, just:

$$\mathbb{Q}(\sqrt{2}) + \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

If we choose something **transcendental** (non-algebraic) like $\mathbb{Q}(\pi)$, then we must use the full quotient definition, and in this case we have $\mathbb{Q}(\pi) \cong \mathbb{Q}(X)$ the field of fractions of $\mathbb{Q}[X]$.

Definition 1.0.2. For some $f \in K[x]$ with distinct complex roots $a_1, \dots, a_n \in \mathbb{C}$, the **splitting field** of f is $L = K(\alpha_1, \dots, \alpha_n)$.

Let $K = \mathbb{Q}$ and $f = x^3 - 2$. The roots of f in $\mathbb{C}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where ω is $(1 - i\sqrt{3})/2$. So the splitting field is $L = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ which can be simplified to just $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. What are the intermediate fields between $\mathbb{Q}$ and L?

$$\begin{tikzcd}
 & & L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) & & \\
\mathbb{Q}(\sqrt[2]{3}) \arrow[urr] & \mathbb{Q}(\omega\sqrt[2]{3}) \arrow[ur] & & \mathbb{Q}(\omega^2\sqrt[2]{3}) \arrow[ul] & \\
 & & & & \mathbb{Q}(i\sqrt{3}) \arrow[uull] \\
 & & \mathbb{Q} \arrow[uull] \arrow[uul] \arrow[uur] \arrow[urr] & &
\end{tikzcd}$$

Lots of fields you might guess, like $\mathbb{Q}(i\sqrt{3}\sqrt[2]{3})$ and $\mathbb{Q}(\sqrt[2]{3} + i\sqrt{3})$ happen to already be in this diagram. But we cannot yet prove this is everything. The length of the arrows is a clue, they relate to the dimension as $\mathbb{Q}$-vector spaces and subgroups in the Galois correspondence.

Theorem 1.0.3 (Fundamental theorem of Galois theory)**.** The **Galois group** of a field extension $K \subset L$ is

$$G = \mathrm{Gal}(L/K) = \left\{ \varphi : L \xrightarrow{\sim} L \;\middle|\; \varphi|_K = \mathrm{id}_K \right\}$$

and the eponymous Galois correspondence:

$$\begin{tikzcd}
\{K \subset F \subset L\} \arrow[r, leftrightarrow, "\sim"] & \{H \leq G\} \\
F \arrow[r, mapsto] & F^\dagger := \{g \in G \mid g|_F = \mathrm{id}_F\} = G_F \\
H^* := \{\alpha \in L \mid H\alpha = \alpha\} & H \arrow[l, mapsto]
\end{tikzcd} .$$

If one knows the Galois group is a supgroup of the permutation of all the roots, then for the case $L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, there is seemingly no way to distinguish the roots, so we expect $G = S_3$, which is luckily true.

Fields are complicated and hard, there are two operations that "cavort" via a weird distributivity law, and proving the classification of subfields of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ already feels pretty impossible. Galois theory allows us to move information from the easy theory of finite groups into the world of field extensions.

Proposition 1.0.4. G is a subgroup of $\mathfrak{S}_n$, where n is the degree of f.

Proof. We want to exhibit any $\sigma \in G$ as a permutation of the roots of f. Any such σ is already an automorphism, so we just need to check it sends roots to roots. If $f(\lambda) = 0$, for some $\lambda \in L$, then we can rearrange $f(\sigma(\lambda)) = \sigma(f(\lambda)) = 0$.

So we get a homomorphism $\rho : G \to \mathfrak{S}_n$. Any automorphism in the kernel must fix every root, and so all of L, thus is the identity. Therefore, ρ is injective and we get $G \leq \mathfrak{S}_n$. □

I claim this will be enough Galois theory to prove that the above diagram for $x^3 - 2$ is everything! Because in this case, G is all of $\mathfrak{S}_3$. To prove this I just have to construct enough elements. In general, constructing elements of Galois groups is very hard. We've already accepted general fields are very baroque, general automorphisms between them will surely be even less manageable. There are some easy cases.

Proposition 1.0.5. For some a not a perfect square in K, the Galois group of the field extension $K \subset K(\sqrt{a})$ will be C_2.

Proof. The automomophism $a + b\sqrt{a} \mapsto a - b\sqrt{a}$ is certainly nontrivial, this is all of $\mathfrak{S}_2$. □

Now consider the quadratic extension in the diagram above: $K = \mathbb{Q}(\sqrt[3]{2}) \subset L = K(i\sqrt{3})$, the generator of $\mathrm{Gal}(L/K)$ is τ such that $\tau(i\sqrt{3}) = -i\sqrt{3}$, this is certainly part of all of G as if it fixes $\mathbb{Q}(\sqrt[3]{2})$ it definitely fixes $\mathbb{Q}$. If we now explicitly calculate how this permutes the roots of f, we see $\tau = (2\ 3)$.

Let's now do the same with $\mathbb{Q}(\omega\sqrt[3]{2})$, we'll see the generator of this Galois group is $(1\ 3)$. I don't actually need to compute how this τ acts on the roots, certainly it fixes $\omega\sqrt[3]{2}$, and certainly it is non-trivial, so it can only be $(1\ 3)$.

These two roots generate all of $\mathfrak{S}_3$, so we have naively computed the galois group of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. BUT, we still haven't show that there are no other fields missing from our diagram, we must still simply believe in the full Galois correspondence to continue.

2 Actual Stuff

All field homomorphisms are injective[1] so I'll write $\mathrm{Emb}(K, L)$[2] for $\mathrm{Hom}(K, L)$ to remind us. Typically there is a fixed field k in the background, and all fields L come with a fixed embedding $i : k \hookrightarrow K$ which we normally supress.[3] If K, L are two such fields, we should only consider embeddings that fix k:

$$\mathrm{Emb}_k(K, L) := \{f : K \to L \mid f|_k = \mathrm{id}_k\}$$ [4]

In particular, K will be a k-vector space. We can gain a lot of information by thinking about these field extensions in term of representations over our Galois groups, we won't talk about that here though.

[1] If $\phi : K \to L$ is a field homomorphism then $\ker(\phi) \trianglelefteq K$ is either 0, making ϕ injective, or K, a contradicion as $\phi(1) = 0$.

[2] Emb stands for embedding.

[3] We normally think of $k = \mathbb{Q}$, in which case there is only ever one embedding of $\mathbb{Q}$ into any algebraic extension.

[4] more specifically, f should commute with the two embeddings.

Definition 2.0.1. A field extension $K \subset L$ is **finite** if L is finite as a K-vector space. The **degree** $[L : K]$ of the extension is $\dim_K L$.

Proposition 2.0.2 (Tower Law)**.** If $K \subset L \subset M$ is a tower of field extensions, then

$$[M : K] = [M : L][L : K].$$

Proof. TODO: finite case is just counting bases, this will suffice. □

2.1 Minimal polynomials

Definition 2.1.1. Given $K \subset L$, for all $a \in L$, the **minimal polynomial** of a in K is the monic generator of the kernel of the ring homomorphism:

$$\mathrm{ev}_a : K[X] \to L \qquad \phi(x) \mapsto \phi(a)$$

Somewhere in a previous algebra course, we have proved $K[X]$ is an Euclidean domain, so a PID.

The first isomorphism theorem for rings now tells us:

$$K[X]/(f) \cong \mathrm{im}(\mathrm{ev}_a) \subset L$$

so $\mathrm{im}(\mathrm{ev}_a)$ is an integral domain, and thus f is prime so irreducible, and so (f) is maximal and $\mathrm{im}(\mathrm{ev}_a)$ is a field. Thus $K[a]$, the K-algebra generated by a, is the same as $K(a)$ the field generated by a as defined earlier.[5]

Conversely, if $f \in K[X]$ is monic and irreducible, and L is the field $K[X]/(f)$, then $K \subset L$ is a finite field extension. If we set $a := [X] \in L$, then $L = K[a] = K(a)$, and $f(x)$ is the minimal polynomial of a. The degree of such an extension $[K : K(a)]$ is equal to the degree of the minimal polynomial.

Finally, for a field extension $K \subset L$ and all $a \in L$ we will always have:

$$\mathrm{Emb}_K(K(a), L) = \{\text{roots of } f \text{ in } L\}$$

2.2 Splitting fields

The construction of a splitting field of a K-irreducible polynomial as $L = K[X]/(f)$ is still important. When $L \subset \mathbb{C}$ we can adjoin sufficiently many roots of f and have a nice constructive form, but we are still interested fields that are not part of $\mathbb{C}$.

For example, consider $\mathbb{F}_2$ and the irreducible polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$, we can form $L = \mathbb{F}_2[X]/(X^2 + X + 1)$ which he know has degree 2 of $\mathbb{F}_2$ so has 4 elements. Are there any other fields of 4 elements? If one exists it is certianly of characteristic 2 so contains $\mathbb{F}_2$, any remaining element not contained in $\mathbb{F}_2$ has a minimal polynomial of degree 2 which must be irreducible, this can only be $X^2 + X + 1$ so there is only one such field of size 4 up to isomorphism. We can call this $\mathbb{F}_4$.[6] In general, we know the theory of finite fields to be somewhat well behaved and all formed in a similar fashion. What about infinite fields of finite characteristic? Consider

$$K := \mathbb{F}_2(t) = \mathrm{Frac}(\mathbb{F}_2[t]) = \left\{ \frac{P(t)}{Q(t)} \;\middle|\; P(t), Q(t) \in \mathbb{F}_2[t],\ Q(t) \not\equiv 0 \right\}$$

and the polynomial $X^2 - t \in K[X]$, which is irreducible. We can certianly prove this is irreducible by naively constructing a root and finding a contradiction. Or we can endeavor to learn some irreducibility conditions for general polynomials.

Proposition 2.2.1 (Eisenstein criterion)**.** If $f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ and there exists some prime $p \in \mathbb{Z}$ such that $p \mid a_i$ and $p^2 \nmid a_n$, then f is irreducible.

Corollary 2.2.2. By Gauss' lemma we know this implies f is also irreducible over $\mathbb{Q}[X]$.

[5] This is somehow not very constructive, our proofs that $K[X]$ is a PID normally goes by the ACC, we have no algorithm for computing a^{-1} in $K[a]$.

[6] There is a certainly a Galois action that swaps the two roots of $X^2 + X + 1$, so while our field is defined only up to non-unique isomorphism. Is $\mathbb{C}$ the same? can we distinguish i from $-i$?

But the Eisenstein criterion is “totally rubbish” and in practice will rarely work.[7] We could now use the Gauss lemma to simplify our naive strategy as we only have to search $\mathbb{F}_2[t][X]$, but in fact the analogue between $\mathbb{Z}$ and $K[X]$ holds for the Eisenstein criterion, and by using $p = t \in \mathbb{F}_2[t]$, we deduce $X^2 - t$ is irreducible. We can even observe $K[x]/(X^2 - t) \cong K$, which you should percieve as being very weird!

But now, in more generality:

Definition 2.2.3. Let K be a field and $f \in K[x]$ be irreducible. A **splitting field** of f over K is a field extension $K \subset L$ such that:

$$f(x) = \prod_{i=1}^{n}(X - \lambda_i) \in L[X]$$

splits completely in $L[X]$; and L is generated by $S = \{\lambda \in L \mid f(\lambda) = 0\}$ over K.

Splitting fields certainly exist, we can just progressively adjoin all roots of f until f splits completely. I claim, if:

$$\begin{tikzcd}
L_1 & & L_2 \\
& K \arrow[ul, hook] \arrow[ur, hook'] &
\end{tikzcd}$$

are two splitting fields for f, then there exists some ismorphism $\phi \in \mathrm{Emb}_K(L_1, L_2)$.

2.3 Motivation again

Back to the tower law to prove that we have a full subfield lattice:

$$\begin{tikzcd}
& & L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) & & \\
\mathbb{Q}(\sqrt[2]{3}) \arrow[urr, "2"] & \mathbb{Q}(\omega\sqrt[2]{3}) \arrow[ur, "2"] & & \mathbb{Q}(\omega^2\sqrt[2]{3}) \arrow[ul, "2"] & \mathbb{Q}(i\sqrt{3}) \arrow[ull, "3"] \\
& & \mathbb{Q} \arrow[ull, "3"] \arrow[ul, "3"] \arrow[ur, "3"] \arrow[urr, "2"] & &
\end{tikzcd}$$

TODO: I know the diagram is ugly, I don’t care right now.

By the tower law, we now know $[L : \mathbb{Q}] = 6$, so any addition subfields K must have $[K : \mathbb{Q}] = 2$ or 3. Suppose $[K : \mathbb{Q}] = 2$, for K to be distinct it must not contain $i\sqrt{3}$. So $X^2 + 3$ remains irreducible over K and we can form the extension:

$$\begin{tikzcd}
& K(i\sqrt{3}) & \\
K \arrow[ur, "2"] & & \mathbb{Q}(i\sqrt{3}) \arrow[ul, "2"] \\
& \mathbb{Q} \arrow[ul, "2"] \arrow[ur, "2"] &
\end{tikzcd}$$

But the tower law now gives us $6 = [L : \mathbb{Q}] = [L : K(i\sqrt{3})][K(i\sqrt{3}) : \mathbb{Q}] = 4[L : K(i\sqrt{3})]$ and $4 \nmid 6$.

If instead $[K : \mathbb{Q}] = 3$, for K to be distinct it must contain no roots of $X^3 - 2$, so we can form $K[X]/(X^3 - 2)$, a degree three extension, and $9 \nmid 6$.

2.4 Back to splitting fields

Lemma 2.4.1. Let f be an irreducible polynomial in $k \subset K$, and $K(a) = K[X]/(f)$, then for any $K \subset L$:

$$\mathrm{Emb}_K(K(a), L) \cong \{\text{roots of } f \text{ in } L\}$$

[7] It is like if you drop your keys on a dark street, the mathematician goes to look for your keys on the other side of the street where there is a lamp. Sure, *if* your keys happen to have reached the other end of the street, they will certainly be found. But this is unlikely, just how it is unlikely an irreducible polynomial satisfies Eisenstein.

Proof. consider the map which sends $\varphi \in \mathrm{Emb}_k(K(a), L)$ to $\varphi(a) \in L$ we know φ will commute with f so $\varphi(a)$ is a root. Indeed, this map is injective as if we have some $\phi(a) = \phi'(a)$ in L, they must now agree on all of $K(a)$. If isntead I have a root $b \in L$ of f, then the map $\mathrm{ev}_b : K[X] \to L$ must have f the generator of the kernel, so the isomorphism theorem gives us a map $K(a) = K[X]/(f) \to L$. □

We have already seen this to be true! There are three embeddings of $\mathbb{Q}(\sqrt[3]{2})$ into $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ as either $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$, or $\mathbb{Q}(\omega^2\sqrt[3]{2})$.[8]

[8] "We rrrrrrrip $\mathbb{Q}(\sqrt[3]{2})$ out of its environment, it is an animal embedded in the jungle of complex numbers". It is just isomorphic to the abstract field $\mathbb{Q}[X]/(X^3 - 2)$, which exists as three different copies in $\mathbb{C}$ "This abstract copy can be incarnated as a lion or a tiger or a zebra". We are just measuring the wasted space of the slpitting field.