Galois Theory

Lectured by Alessio Corti
Scribed by Yu Coughlin

Autumn 2025

Contents

1 Motivation

Fix a field $\mathbb{Q} \subset K \subset \mathbb{C}$. For some $\alpha \in \mathbb{C}$ we will use the notation:

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

$K(\alpha_1, \ldots, \alpha_n)$ 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 $P(\alpha) = 0$.

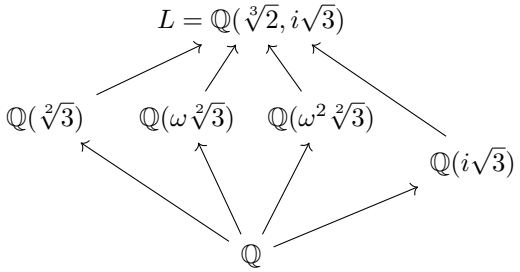
Consider $\mathbb{Q}(\sqrt{2})$, this has a simpler description than as the full quotient:

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

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 $\mathbb{Q}(\pi) \cong Q(X)$ the field of fractions of $\mathbb{Q}[X]$.

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

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?



Lots of fields you might guess, like $\mathbb{Q}(i\sqrt{3}\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2} + i\sqrt{3})$ 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:

$$\begin{aligned} \{K \subset F \subset L\} &\xleftrightarrow{\sim} \{H \leq G\} \\ F &\longmapsto F^\dagger := \{g \in G \mid g|_F = \mathrm{id}_F\} = G_F \\ H^* := \{\alpha \in L \mid H\alpha = \alpha\} &\longmapsfrom H \end{aligned} \quad .$$

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:

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

[5] This is somehow not very constructive, our proofs that $K[X]$ is a PID normally go by the ACC, we have algorithm for computing a^{-1} in $K[a]$.