§ 5 Galois extensions

Let $f(x) \in K[x]$ be a polynomial with splitting field K_f/K. Recall that our goal for the course is to use the group theoretic properties of $\mathrm{Gal}(K_f/K)$ to understand the properties of f.

So far, we have attached a Galois group to any field extension L/K. In this section, we will see that a certain class of field extensions, the *Galois* extensions, will be the right extensions to study.

Normal extensions and Galois extensions

Example 5.1 Consider the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. This field extension behaves badly in a number of ways:

1. The minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $f(x) = x^4 - 2$. The field $\mathbb{Q}(\sqrt[4]{2})$ does not contain all of the roots of f: it contains neither $i\sqrt[4]{2}$ nor $-i\sqrt[4]{2}$.

   In particular, the field extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ does not capture all of the information coming from the polynomial f. Indeed, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not the splitting field of *any* polynomial.

2. The Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{\mathrm{id}, \mathrm{conj}\},$$

   where id is the identity, and $\mathrm{conj} : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$.

   However, if we consider $\mathbb{Q}(\sqrt[4]{2})$ as an extension of $\mathbb{Q}(\sqrt{2})$, then the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \mathrm{conj}\},$$

   and hence,

   $$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})) = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}).$$

   In particular, the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ does not capture all of the information of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Rather, it only sees the subextension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

3. The order of the Galois group of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is 2, which is smaller than the degree $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$.

Based on this example, the right extensions to study will be those without these bad properties.

Definition 5.2 A finite extension $K \subseteq L$ is *normal* if for every $\ell \in L$, the minimal polynomial f of ℓ over K splits into linear factors in L.

Equivalently, if $f(x) \in K[x]$ is a polynomial, then L either contains all the roots of f or none of the roots of f. ▲

Examples 5.3 1. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, since it does not contain all the roots of $x^4 - 2$.

2. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal. Indeed, every element of $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2},\ a, b \in \mathbb{Q}$, and the second root of the minimal polynomial of $a + b\sqrt{2}$ is $a - b\sqrt{2}$.

3. A similar argument shows that every extension L/K of degree 2 is normal. In particular, the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is normal.

Definition 5.4 A finite extension $K \subseteq L$ of fields is *Galois* if

$$|\mathrm{Gal}(L/K)| = [L : K].$$

▲

Examples 5.5 1. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois.

2. The extension $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cubed root of unity, is Galois.

3. Every extension L/K of degree 2 is Galois. Indeed, we can write $L = K(\sqrt{\beta})$ for some $\beta \in L$, and
$$\mathrm{Gal}(L/K) = \{\mathrm{id}, \mathrm{conj}\},$$
where id is the identity, and $\mathrm{conj} : \sqrt{\beta} \mapsto -\sqrt{\beta}$, so
$$|\mathrm{Gal}(L/K)| = [L : K] = 2.$$

Definition 5.6 Let L be a field, and let S be a finite set of automorphisms L. The *fixed field* of S

$$L^S = \{x \in L : \theta(x) = x \text{ for all } \theta \in S\}.$$

▲

(To see that L^S is a field, use the subfield criterion, noting that by definition $L^S \subseteq L$.)

Examples 5.7 1. If $L = \mathbb{Q}(\sqrt[4]{2})$, then

$$L^{\mathrm{Gal}(L/\mathbb{Q})} = L^{\{\mathrm{id},\mathrm{conj}\}} = \mathbb{Q}(\sqrt{2}).$$

2. If $L = \mathbb{Q}(\sqrt{2}))$, then

$$L^{\mathrm{Gal}(L/\mathbb{Q})} = L^{\{\mathrm{id},\mathrm{conj}\}} = \mathbb{Q}.$$

We have the following theorem:

Theorem 5.8 *Let $K \subseteq L$ be a finite extension of fields. Assume that $K, L \subseteq \mathbb{C}$. The following are equivalent:*

1. *L/K is Galois;*
2. *L is the splitting field of an irreducible polynomial $f \in K[x]$;*
3. *L/K is normal;*
4. *$K = L^{\mathrm{Gal}(L/K)}$.*

This equivalence is one of our first indications that a statement purely about fields ("L is the splitting field of a polynomial over K") is equivalent to a statement about the Galois group ("$|\mathrm{Gal}(L/K)| = [L : K]$"). We will prove that $(1) \implies (2) \implies (3) \implies (1)$ and that $(1) \iff (4)$. We first prove $(1) \implies (2)$.

Lemma 5.9 Suppose $K \subseteq L$ is an extension of fields. If L/K is Galois, then L is the splitting field of an irreducible polynomial over K.

PROOF. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K. We know:

- $[L : K]$ is equal to the degree of f (Theorem 2.2),
- $|\mathrm{Gal}(L/K)|$ is equal to the number of distinct roots of f in L (Corollary 3.12).

So we see that $[L : K] = |\mathrm{Gal}(L/K)|$ implies that the number of roots of f in L is equal to the degree of f, i.e., if f factorises over L into distinct linear factors. We have therefore shown that if L/K is Galois, then L is the splitting field of a polynomial over K. ⊠

Next, we prove that $(2) \implies (3)$.

Lemma 5.10 Let L be the splitting field of an irreducible polynomial over K. Then L/K is normal.

PROOF. Suppose L is the splitting field of a polynomial $f \in K[x]$. Let $g \in K[x]$ be any other polynomial with a root $\alpha \in L$. Suppose that β is another root of g. We need to show that $\beta \in L$.

By Theorem 3.11, there is an isomorphism $\theta : K(\alpha) \to K(\beta)$ which fixes K and maps $\alpha \mapsto \beta$.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Then it is a fact that we can define a homomorphism

$$\varphi : K(\alpha, \alpha_1, \ldots, \alpha_n) \to K(\beta, \alpha_1, \ldots, \alpha_n)$$

that maps $\alpha \mapsto \beta$. Note that φ is a map $L \to L(\beta)$.

But by APR (Theorem 3.10), φ must map each of the roots of f to another root of f. Since L is generated by the roots of f, it follows that $\varphi(L) \subseteq L$. Hence $L(\beta) = L$, so $\beta \in L$, as required. ⊠

We now prove that $(3) \implies (1)$.

Lemma 5.11 Suppose $K \subseteq L$ is an extension of fields, and that $K, L \subseteq \mathbb{C}$. If L/K is normal, then L/K is Galois.

PROOF.

By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K. We know:

- $[L : K]$ is equal to the degree of f (Theorem 2.2);
- $|\mathrm{Gal}(L/K)|$ is equal to the number of distinct roots of f in L (Corollary 3.12).

Since L/K is normal and $\alpha \in L$, L must contain all the roots of f. Hence,

$$|\mathrm{Gal}(L/K)| = \#\{\text{roots of } f\} = \deg(f) = [L : K],$$

so L/K is Galois. ⊠

We complete the proof of Theorem 5.8 by proving $(1) \iff (4)$.

PROOF OF THEOREM 5.8.

We'll first show that $(1) \implies (4)$. Assume that L/K is Galois, and let $G = \mathrm{Gal}(L/K)$. We need to show that $L^G = K$.

Consider the Galois group $\mathrm{Gal}(L/L^G)$. Then $G \subseteq \mathrm{Gal}(L/L^G)$. Indeed, G acts on L and fixes L^G.

However, we have $K \subseteq L^G \subset L$. So

$$|G| \leqslant \mathrm{Gal}(L/L^G) \leqslant [L : L^G] \leqslant [L : K].$$

Since L/K is Galois, $|G| = [L : K]$, and hence $[L : L^G] = [L : K]$. so $L^G = K$ as required.

We'll now show that $(4) \implies (1)$. Write $G = \mathrm{Gal}(L/K)$ and suppose that $L^G = K$. We need to show that L/K is Galois. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = K(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over K.

Consider the polynomial

$$g(x) = \prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \varphi(\alpha)) \in L[x],$$

i.e. the polynomial in $L[x]$ whose roots are $\varphi(\alpha)$ for all $\varphi \in \mathrm{Gal}(L/K)$. We will show that $g(x) \in K[X]$.

Suppose that $\theta \in \mathrm{Gal}(L/K)$. Then

$$\begin{aligned} \theta(g(x)) &= \theta \left(\prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \varphi(\alpha)) \right) \\ &= \prod_{\varphi \in \mathrm{Gal}(L/K)} (x - \theta\varphi(\alpha)) \\ &= \prod_{\psi \in \mathrm{Gal}(L/K)} (x - \psi(\alpha)) \qquad \text{where } \psi = \theta\varphi \\ &= g(x). \end{aligned}$$

Hence, θ fixes all the coefficients of $g(x)$, so $g(x) \in L^G[x]$. Since $L^G = K$, we have $g(x) \in K[X]$.

But α is a root of $g(x)$, so we must have $f(x) \mid g(x)$. Hence,

$$[L : K] = \deg(f) \leqslant \deg(g) = |\mathrm{Gal}(L/K)| \leqslant [L : K],$$

from which it follows that $|\mathrm{Gal}(L/K)| = [L : K]$. Hence, L/K is Galois. ⊠

Subextensions of Galois extensions

Remember from the sketch of our plan that we are going to try to build up larger extensions from small ones. This means that it is important to consider chains of extensions.

Corollary 5.12 Suppose L/K is a Galois extension, and that $K \subseteq M \subseteq L$ is an intermediate field. Then L/M is Galois.

PROOF. Suppose that L is the splitting field of some polynomial $f \in K[x]$. Then certainly $f \in M[x]$, as $K \subseteq M$; but L splits f and is generated over K by the roots, so it is also generated over M by the roots. Thus L is the splitting field for f over M, and is therefore Galois by Theorem 5.8. ⊠

Note that any automorphism of L which fixes every element of M will certainly fix every element of K. It follows that $\mathrm{Gal}(L/M)$ is a subset (and therefore a *subgroup*) of $\mathrm{Gal}(L/K)$.

However, in general, M/K need not be Galois. We have already seen a simple example:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Let's now think about the case of field extensions $K \subseteq M \subseteq L$, in which L/K is Galois (and therefore so is L/M). Remarkably, the condition that M/K should be Galois has a simple reformulation in terms of groups.

Lemma 5.13 Let $K \subseteq M \subseteq L$ be finite extensions of fields. If M/K is Galois, then $\varphi(M) = M$ for all $\varphi \in \mathrm{Gal}(L/K)$.

PROOF. We may suppose that $M = K(\alpha)$ is the splitting field for the irreducible polynomial m_α by TPE (Theorem 2.5). The element φ must map α to another root of m_α by APR (Theorem 3.10); but this root, β say, is also in M, because M splits m_α. It then follows that $\varphi(M) \subseteq M$, and similarly $\varphi^{-1}(M) \subseteq M$, so $\varphi(M) = M$. ⊠

The situation when M/K is Galois is explained by the following theorem.

Theorem 5.14 *Let $K \subset L$ be a Galois extension, and let M be an intermediate field. Then M/K is Galois if and only if $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$. In this case, there is an isomorphism*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Gal}(M/K).$$

We will prove each direction of this if and only if statement separately.

Theorem 5.15 *Let $K \subset L$ be a Galois extension, and let M be an intermediate field. Then if M/K is Galois, $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, and there is an isomorphism*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Gal}(M/K).$$

PROOF. If M/K is Galois, then $\varphi(M) = M$ for all $\varphi \in \mathrm{Gal}(L/K)$, by the preceding Lemma. That is, given $m \in M$, $\varphi(m) \in M$ also. Since any θ in $\mathrm{Gal}(L/M)$ will fix all elements of M, we see that $\theta(\varphi(m)) = \varphi(m)$ for all $m \in M$, $\theta \in \mathrm{Gal}(L/M)$ and $\varphi \in \mathrm{Gal}(L/K)$. Therefore $\varphi^{-1}\theta\varphi(m) = m$, and so $\varphi^{-1}\theta\varphi$

fixes every element of M. It follows that $\varphi^{-1}\theta\varphi \in \mathrm{Gal}(L/M)$, and therefore $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$.

For the second part, define a map

$$\begin{array}{rcl} \Phi : \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) \\ \varphi & \mapsto & \varphi|_M \end{array}$$

where $\varphi|_M$ is the restriction of φ to $M \to M$ (recall that $\varphi(M) = M$). So $\varphi|_M \in \mathrm{Gal}(M/K)$, as required. The map that sends each φ to $\varphi|_M$ is easily seen to be a group homomorphism, and its kernel consists of all φ such that $\varphi|_M(m) = m$ for all $m \in M$, i.e., $\varphi \in \mathrm{Gal}(L/M)$.

Then the first isomorphism theorem for groups gives:

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Im}\,\Phi \subseteq \mathrm{Gal}(M/K).$$

However, if we compare the sizes of the two sides, bearing in mind that L/K and L/M are both Galois (by Corollary 5.12):

$$|\mathrm{Im}\,\Phi| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M/K)|$$

using the Degrees Theorem 2.3, and so $\mathrm{Im}\,\Phi = \mathrm{Gal}(M/K)$. ⊠

Theorem 5.16 *Suppose that L/K is Galois, and let M be an intermediate field. If $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, then M/K is Galois.*

Proof. Note that

$$\begin{array}{ll} & \mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K) \\ \iff & \varphi^{-1}\theta\varphi \in \mathrm{Gal}(L/M) \text{ for all } \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi^{-1}\theta\varphi(m) = m \text{ for all } m \in M, \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \theta\varphi(m) = \varphi(m) \text{ for all } m \in M, \theta \in \mathrm{Gal}(L/M), \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi(M) \subseteq L^{\mathrm{Gal}(L/M)} \text{ for all } \varphi \in \mathrm{Gal}(L/K) \\ \iff & \varphi(M) \subseteq M \text{ for all } \varphi \in \mathrm{Gal}(L/K) \text{ by Theorem 5.8} \\ \iff & \varphi(M) = M \text{ for all } \varphi \in \mathrm{Gal}(L/K) \end{array}$$

As in Theorem 5.15, define

$$\begin{array}{rcl} \Phi : \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) \\ \theta & \mapsto & \theta_M \end{array}$$

where $\theta_M(m) = \theta(m)$ for $m \in M$. As $\theta(M) = M$, $\theta_M \in \mathrm{Gal}(M/K)$, as required. Also, one easily sees that Φ is a group homomorphism. Further, its kernel is $\mathrm{Gal}(L/M)$. The first isomorphism theorem gives

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Im}\,\Phi \subseteq \mathrm{Gal}(M/K).$$

and, as in the proof of Theorem 5.15,

$$[M : K] \geq |\mathrm{Gal}(M/K)| \geq \left|\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}\right| = \frac{[L : K]}{[L : M]} = [M : K],$$

and so $[M : K] = |\mathrm{Gal}(M/K)|$, and M/K is therefore Galois. ⊠

§ 6 The Galois correspondence

Before we look at the principal application, to the insolubility of the quintic, we will look at the Galois correspondence. The main theorem of the theory is that a polynomial is soluble if and only if the Galois group of its splitting field has a particular property (also called solubility). One result, that there exist polynomials whose Galois groups are not soluble, does not require the Galois correspondence. However, the converse, that if the Galois group of a polynomial is soluble, then the polynomial is soluble, does require the correspondence.

The Fundamental Theorem of Galois Theory

The aim of the fundamental theorem of Galois theory is to compare, in the case where L/K is Galois, intermediate subfields $K \subseteq M \subseteq L$ and subgroups of $\mathrm{Gal}(L/K)$. The answer is as nice as one could hope for, although the proof (see Theorem 14.2) is quite long.

Definition 6.1 Let L/K be a Galois extension, and let H be a subgroup of $\mathrm{Gal}(L/K)$. Then we write L^H for

$$L^H = \{\ell \in L \mid \theta(\ell) = \ell \text{ for all } \theta \in H\},$$

the *fixed field* of H. ▲

(To see that L^H is a field, use the subfield criterion, noting that by definition $L^H \subseteq L$.)

Theorem 6.2 (Fundamental Theorem of Galois Theory) *Let L be a Galois extension of K, and let $G = \mathrm{Gal}(L/K)$. There is a bijection from*

$$\mathscr{S} := \{\textit{subgroups of } G\}$$

to

$$\mathscr{F} := \{\textit{intermediate fields } K \subseteq M \subseteq L\}$$

given by $H \mapsto L^H$ with inverse $M \mapsto \mathrm{Gal}(L/M)$.

Moreover, the correspondence is inclusion reversing, that is,

$$H_1 \supseteq H_2 \iff L^{H_1} \subseteq L^{H_2},$$

and indexes equal degrees, that is,

$$\frac{|H_1|}{|H_2|} = [L^{H_2} : L^{H_1}].$$

Finally, normal subgroups of G correspond to intermediate fields $K \subseteq M \subseteq L$ such that M/K is Galois.

Terminology: for any inclusion of subgroups of any group, $\frac{|H_1|}{|H_2|}$ is called the *index of H_2 in H_1*. It is the number of cosets $h_1 H_2$ for $h_1 \in H_1$.

PROOF. Let H be a subgroup of G, and let M be an intermediate subfield $K \subseteq M \subseteq L$. To prove that $\mathscr{S}$ and $\mathscr{F}$ are in bijection, we need to show that the maps we've constructed are mutually inverse, i.e. that

- $L^{\mathrm{Gal}(L/M)} = M$;
- $\mathrm{Gal}(L/L^H) = H$.

For the first part, by Corollary 5.12, L/M is Galois. Hence, by part (4) of Theorem 5.8, $L^{\mathrm{Gal}(L/M)} = M$.

For the second part, first observe that $H \subseteq \mathrm{Gal}(L/L^H)$—indeed, H acts on L and fixes L^H. We will show that $|\mathrm{Gal}(L/L^H)| \leqslant |H|$, so that this inclusion is an equality. Our argument will mimic the proof of $(4) \implies (1)$ in Theorem 5.8.

Let $M = L^H$. Then by Corollary 5.12, L/M is Galois. By TPE (Theorem 2.5), there exists an $\alpha \in L$ such that $L = M(\alpha)$. Let $f(x)$ denote the minimal polynomial of α over M.

Consider the polynomial

$$g(x) = \prod_{\varphi \in H} (x - \varphi(\alpha)) \in L[x],$$

i.e. the polynomial in $L[x]$ whose roots are $\varphi(\alpha)$ for all $\varphi \in H$. We will show that $g(x) \in M[X]$.

Suppose that $\theta \in H$. Then

$$\begin{aligned} \theta(g(x)) &= \theta\left(\prod_{\varphi \in H} (x - \varphi(\alpha))\right) \\ &= \prod_{\varphi \in H} (x - \theta\varphi(\alpha)) \\ &= \prod_{\psi \in H} (x - \psi(\alpha)) \qquad \text{where } \psi = \theta\varphi \\ &= g(x). \end{aligned}$$

Hence, θ fixes all the coefficients of $g(x)$, so $g(x) \in L^H[x] = M[x]$. But α is a root of $g(x)$, so we must have $f(x) \mid g(x)$. Hence,

$$[L : M] = \deg(f) \leqslant \deg(g) = |H|,$$

from which it follows that $\mathrm{Gal}(L/M) = H$, as required.

It follows that the two maps $H \mapsto L^H$ and $M \mapsto \mathrm{Gal}(L/M)$ are inverse bijections.

For the other part, observe that if $H_1 \supseteq H_2$, we have $L^{H_1} \subseteq L^{H_2}$ (anything in L fixed by H_1 will be fixed by H_2); conversely, if $L^{H_1} \subseteq L^{H_2}$, the first part of the theorem shows that then $\mathrm{Gal}(L/L^{H_1}) \supseteq \mathrm{Gal}(L/L^{H_2})$, and also that $\mathrm{Gal}(L/L^{H_i}) = H_i$, so that $H_1 \supseteq H_2$.

For the assertion about indexes and degrees, first observe that it is immediate if $H_2 = 1$. In this case, $L^{H_2} = L$, and

$$(H_1 : 1) = |H_1| = |\mathrm{Gal}(L/L^{H_1})| = [L : L^{H_1}].$$

Now consider the general case. We use the special case above to see that $|H_i| = [L : L^{H_i}]$. But also we have:

$$|H_1| = |H_2|(H_1 : H_2) \quad \text{and} \quad [L : L^{H_1}] = [L : L^{H_2}][L^{H_2} : L^{H_1}]$$

(by the Degrees Theorem 2.3). Comparing these gives the result.

⊠

Example 6.3 We are now going to look at the Galois theory of the polynomial $x^3 - 2$. Its splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity, so this is Galois over $\mathbb{Q}$. Let's first look at all of the subfields of this field. I claim that the *subfield lattice* is:

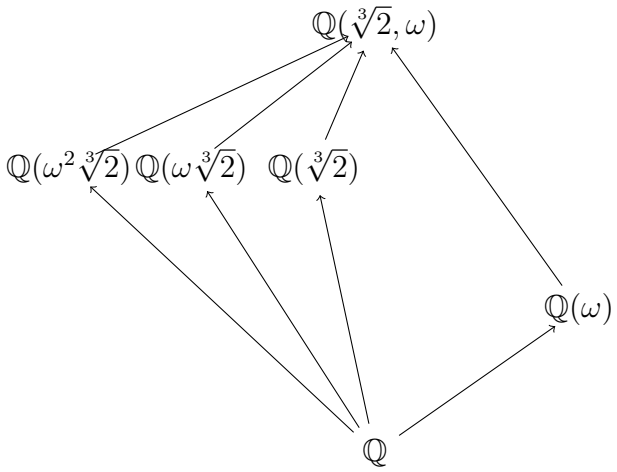

Figure 1: Lattice of subfields of $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

(One pictures the lattice of subfields of a field L by drawing a line between two subfields K and M whenever $K \subset M$ and there are no subfields strictly between K and M. Further, one arranges it so that M is higher up on the page than K.)

$\mathbb{Q}$-auto	effect on $\sqrt[3]{2}$	effect on ω	permutation
1	$\sqrt[3]{2}$	ω	id
φ	$\sqrt[3]{2}$	ω^2	(2 3)
ψ	$\omega\sqrt[3]{2}$	ω	(1 2 3)
$\psi\varphi$	$\omega\sqrt[3]{2}$	ω^2	(1 2)
ψ^2	$\omega^2\sqrt[3]{2}$	ω	(1 3 2)
$\varphi\psi$	$\omega^2\sqrt[3]{2}$	ω^2	(1 3)

Table 1

The idea of Galois theory is that this is reflected by the group theoretical structure of the subgroups of the Galois group. We have already seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ is S_3. Now S_3 has the (upside-down) subgroup lattice shown in Figure 2.

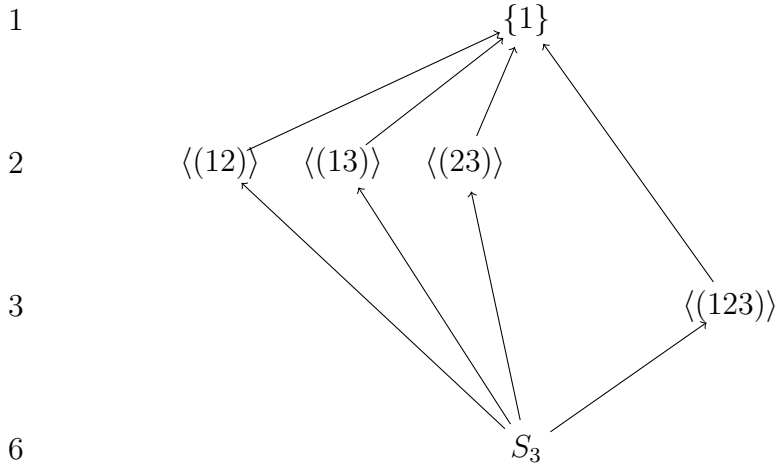

Figure 2: Subgroup lattice of S_3.

Note that the pictures look alike!

So the Galois correspondence is between the six subfields of $\mathbb{Q}(\sqrt[3]{2},\omega)$ and the six subgroups of S_3.

We now check that the above pictures correspond.

Table 1 shows the isomorphism $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) \cong S_3$.

Thus, if we consider the subfield $\mathbb{Q}(\omega)$ of $\mathbb{Q}(\sqrt[3]{2},\omega)$, then we can see that $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(123)\rangle}$. This is because $\psi(\omega) = \omega$. Note that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Now we use the Galois correspondence to see that the degree equals the index, and so we see that we have an equality $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(123)\rangle}$.

In a similar way, we can identify the fixed field of each subgroup of S_3, and they correspond as in the picture. (Exercise: which of the fields are Galois extensions of $\mathbb{Q}$?) ⊠

Example 6.4 Let $L = \mathbb{Q}(\sqrt[4]{2}, i)$, the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Thus $\mathbb{Q} \subseteq L$ is Galois. $[L : \mathbb{Q}] = 8$, as $[L : \mathbb{Q}(\sqrt[4]{2})] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Then $|\mathrm{Gal}(L/\mathbb{Q})| = 8$.

Now $\sqrt[4]{2}$ has minimal polynomial $x^4 - 2$, whose roots are $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ and $-i\sqrt[4]{2}$. Further, i has minimal polynomial $x^2 + 1$, whose roots are $\pm i$.

The eight possible $\mathbb{Q}$-automorphisms of M are given in the following table:

$\mathbb{Q}$-auto	effect on $\sqrt[4]{2}$	effect on i	permutation	remarks
1	$\sqrt[4]{2}$	i	id	
r	$i\sqrt[4]{2}$	i	(1 2 3 4)	$r^4 = 1$
r^2	$-\sqrt[4]{2}$	i	(1 3)(2 4)	
r^3	$-i\sqrt[4]{2}$	i	(1 4 3 2)	
s	$\sqrt[4]{2}$	$-i$	(2 4)	$s^2 = 1$
rs	$i\sqrt[4]{2}$	$-i$	(1 2)(3 4)	
r^2s	$-\sqrt[4]{2}$	$-i$	(1 3)	
r^3s	$-i\sqrt[4]{2}$	$-i$	(1 4)(2 3)	$r^3s = sr$

It follows that $\mathrm{Gal}(L/\mathbb{Q}) = \langle r, s \mid r^4 = s^2 = 1, r^3s = sr\rangle \cong D_4$. The (upside-down) subgroup lattice of D_4 is shown in Figure 3.

The subfield lattice of L is shown in Figure 4.

We leave it as an exercise to verify the correspondence. We give just one example, namely, the field $M = \mathbb{Q}((1+i)\sqrt[4]{2})$. We first prove it is fixed by rs.

$$rs((1+i)\sqrt[4]{2}) = rs(\sqrt[4]{2}) + rs(i\sqrt[4]{2}) = i\sqrt[4]{2} + \sqrt[4]{2} = (1+i)\sqrt[4]{2}.$$

Next we check that it is not fixed by r^2:

$$r^2((1+i)\sqrt[4]{2}) = r^2(\sqrt[4]{2}) + r^2(i\sqrt[4]{2}) = -\sqrt[4]{2} - i\sqrt[4]{2} = -(1+i)\sqrt[4]{2}.$$

It follows that the subgroup of D_4 corresponding to M must be a subgroup containing rs but not r^2. A quick examination of the list of subgroups shows that the only possibility is $\{1, rs\}$. The other correspondences are similar. ⊠

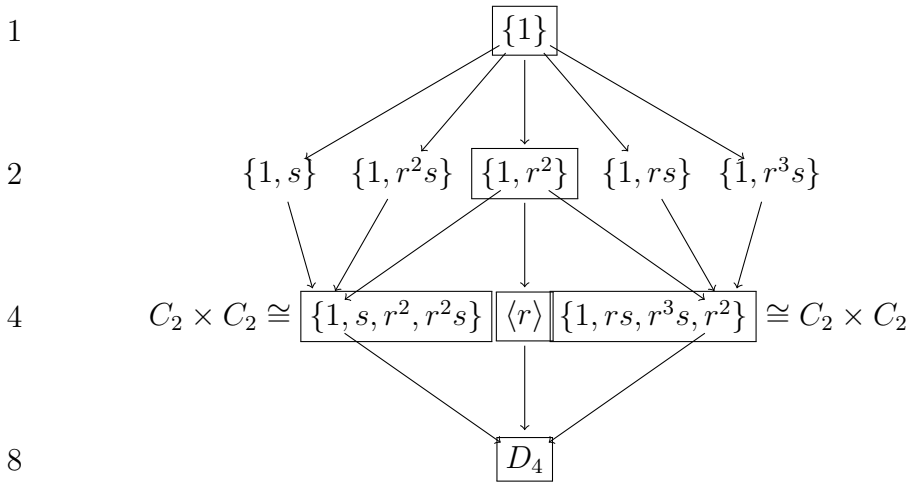

Figure 3: The subgroup lattice of D_4. The normal subgroups are boxed.

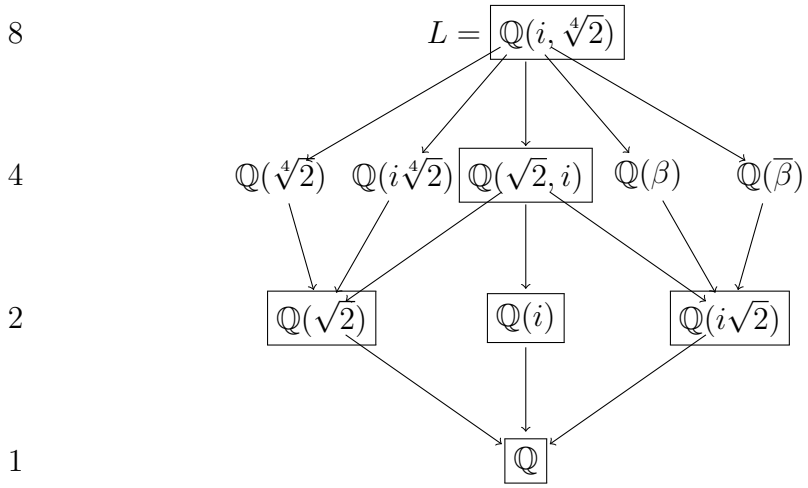

Figure 4: The subfield lattice of $L = \mathbb{Q}(i, \sqrt[4]{2})$. The subfields of L which are Galois extensions of $\mathbb{Q}$ are boxed. Note $\beta = (1+i)\sqrt[4]{2}$.