THE GALOIS CORRESPONDENCE

KEITH CONRAD

1. Introduction

We call a finite extension of fields L/K *Galois* if L is the splitting field over K of a separable polynomial: some (monic) separable polynomial $f(X) \in K[X]$ splits completely over L and L is generated over K by the roots of $f(X)$.

Example 1.1. The extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is Galois since $\mathbf{Q}(\sqrt{2})$ is the splitting field over $\mathbf{Q}$ of $X^2 - 2$: $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\sqrt{2}, -\sqrt{2})$.

Example 1.2. Any quadratic extension L/K outside of characteristic 2 is Galois. Indeed, by completing the square we can write $L = K(\sqrt{d})$ for some nonsquare $d \in K^\times$, and $X^2 - d$ is separable outside characteristic 2. Thus L is a splitting field over K for $X^2 - d$.

Example 1.3. The extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$ is Galois since $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field over $\mathbf{Q}$ of $(X^2 - 2)(X^2 - 3)$.

Example 1.4. The extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is Galois, where ζ_n is a primitive nth root of unity, since $\mathbf{Q}(\zeta_n)$ is a splitting field over $\mathbf{Q}$ of $X^n - 1$: its roots are all powers ζ_n^k.

Example 1.5. The extension $\mathbf{F}_2(\sqrt{u})/\mathbf{F}_2(u)$, where u is an indeterminate, is not Galois. The field $\mathbf{F}_2(\sqrt{u})$ is a splitting field over $\mathbf{F}_2(u)$ of the polynomial $X^2 - u$, but the extension is not separable. This is a quadratic extension that is not Galois, and has characteristic 2.

Example 1.6. The polynomial $X^2 + X + 1$ is irreducible over $\mathbf{F}_2$. Letting α be one root, $\alpha + 1$ is another root (check!), so the extension $\mathbf{F}_2(\alpha)$ is Galois over $\mathbf{F}_2$ because it's the splitting field of the separable polynomial $X^2 + X + 1$ over $\mathbf{F}_2$. This is a quadratic Galois extension in characteristic 2.

Example 1.7. The extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ does not *appear* to be Galois. The field $\mathbf{Q}(\sqrt[3]{2})$ has one root of $X^3 - 2$ but not a full set of roots of $X^3 - 2$. However, this does not (yet) tell us the extension isn't Galois, since even if it's not a splitting field of $X^3 - 2$, might it be a splitting field over $\mathbf{Q}$ of some other polynomial? We'll see later that this is impossible.

For any finite extension L/K, a K-*automorphism* of L is a field automorphism $\sigma \colon L \to L$ such that $\sigma(c) = c$ for all $c \in K$.

Example 1.8. Two $\mathbf{R}$-automorphisms of $\mathbf{C}$ are the identity and complex conjugation.

For every L/K, one example of a K-automorphism is the identity function on L, and sometimes it may be the only example.

Example 1.9. For $n \geq 3$, the degree of $\mathbf{Q}(\sqrt[n]{2})/\mathbf{Q}$ is n and the only $\mathbf{Q}$-automorphism of $\mathbf{Q}(\sqrt[n]{2})$ is the identity. The reason is that $\sqrt[n]{2}$ is the *only* nth root of 2 in $\mathbf{Q}(\sqrt[n]{2})$: this field is inside $\mathbf{R}$ and there is just one real nth root of 2. (Notice that last statement is wrong when $n = 2$.) If σ is a $\mathbf{Q}$-automorphism of $\mathbf{Q}(\sqrt[n]{2})$ then applying σ to both sides of the equation $\sqrt[n]{2}^n = 2$ implies $\sigma(\sqrt[n]{2})^n = \sigma(2) = 2$, so $\sigma(\sqrt[n]{2})$ is an nth root of 2 in $\mathbf{Q}(\sqrt[n]{2})$. Therefore $\sigma(\sqrt[n]{2}) = \sqrt[n]{2}$. Since σ fixes all elements of $\mathbf{Q}$ and it fixes $\sqrt[n]{2}$, it fixes the whole field $\mathbf{Q}(\sqrt[n]{2})$.

For any finite extension L/K, the collection of all K-automorphisms of L is a group under composition. This group is finite, and when L/K is a Galois extension there is a close relationship between the fields lying between K and L and the subgroups of the group of all K-automorphisms of L. This relationship is called the Galois correspondence, and understanding it is the main subject of these notes.

2. Roots in a Galois Extension

The following theorem tells us something important about a Galois extension L/K: not only does it have a full set of roots for one irreducible polynomial (namely the one that L is a splitting field for over K), but it has a full set of roots for the minimal polynomial in $K[X]$ of any element of L.

Theorem 2.1. *If L/K is a Galois extension, then every irreducible polynomial in $K[X]$ with one root in L splits completely over L. Equivalently, the minimal polynomial in $K[X]$ of every element of L splits completely over L.*

Proof. This proof will use the symmetric function theorem: every symmetric polynomial in n variables with coefficients in K is a polynomial in the elementary symmetric functions of those n variables with coefficients in K.

Let $\pi(X)$ be irreducible in $K[X]$ with a root in L, say α. We want to show $\pi(X)$ splits completely over L. We are going to show $\pi(X)$ is a factor of a polynomial in $K[X]$ that splits completely over L, so $\pi(X)$ also splits completely over L.

By definition of L being a splitting field over K, there is some polynomial $f(X) \in K[X]$ such that $f(X) = (X - \beta_1) \cdots (X - \beta_n)$ in $L[X]$ and $L = K(\beta_1, \ldots, \beta_n) = K[\beta_1, \ldots, \beta_n]$. Write $\alpha = g(\beta_1, \ldots, \beta_n)$ for a polynomial $g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. Now consider the monic polynomial $h(X)$ whose roots are g evaluated at *all* permutations of the β_i's:

$$h(X) = \prod_{\sigma \in S_n} (X - g(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)})) \in L[X].$$

This has factor $X - \alpha$, so $h(\alpha) = 0$. By construction, the coefficients of $h(X)$ are symmetric polynomials in $\beta_1, \ldots, \beta_n$ with K-coefficients. Therefore the coefficients of $h(X)$ are polynomials in the elementary symmetric functions of $\beta_1, \ldots, \beta_n$ with K-coefficients. The elementary symmetric functions of the β_i's are the coefficients of $f(X)$ (up to sign) and thus lie in K, so each coefficient of $h(X)$ is a polynomial in elements of K with K-coefficients, and thus the coefficients of $h(X)$ are all in K: $h(X) \in K[X]$. Since $h(\alpha) = 0$ and $h(X) \in K[X]$, $h(X)$ is divisible by the minimal polynomial of α in $K[X]$, which is $\pi(X)$. Since $\pi(X) | h(X)$ and $h(X)$ splits completely in $L[X]$, $\pi(X)$ splits completely in $L[X]$. □

Example 2.2. In the Galois extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$, $\sqrt{2} + \sqrt{3}$ has minimal polynomial $X^4 - 10X^2 + 1$ and all of its roots are in the field: $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$.

3. Field automorphisms and permutations of roots

Definition 3.1. The roots of a common irreducible polynomial in $K[X]$ are called *K-conjugates.*

Example 3.2. The numbers $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ are $\mathbf{Q}$-conjugate since they all have minimal polynomial $X^4 - 2$ over $\mathbf{Q}$, but they are not all $\mathbf{R}$-conjugate: over the real numbers, $\sqrt[4]{2}$ has minimal polynomial $X - \sqrt[4]{2}$, $-\sqrt[4]{2}$ has minimal polynomial $X + \sqrt[4]{2}$, and $\pm i\sqrt[4]{2}$ has minimal polynomial $X^2 + \sqrt{2}$.

Example 3.3. In $\mathbf{C}$ the numbers i and $-i$ are $\mathbf{R}$-conjugates, as are (more generally) $a + bi$ and $a - bi$. The name "complex conjugate" should be "real conjugate" from this point of view, since $a + bi$ and $a - bi$ have the same minimal polynomial over $\mathbf{R}$, but not $\mathbf{C}$ (unless $b = 0$), but it's too late to change the name.

Theorem 3.4. *If σ is a K-automorphism of L and $f(X) \in K[X]$, then $\sigma(f(\alpha)) = f(\sigma(\alpha))$ for all $\alpha \in L$. In particular, a K-automorphism of L permutes the roots of $f(X)$ in L.*

Proof. Write $f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$, with $c_i \in K$. Then $\sigma(c_i) = c_i$, so

$$\begin{aligned}
\sigma(f(\alpha)) &= \sigma\left(c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0\right) \\
&= \sigma(c_n)\sigma(\alpha)^n + \sigma(c_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(c_1)\sigma(\alpha) + \sigma(c_0) \\
&= c_n\sigma(\alpha)^n + c_{n-1}\sigma(\alpha)^{n-1} + \cdots + c_1\sigma(\alpha) + c_0 \\
&= f(\sigma(\alpha)).
\end{aligned}$$

If $f(\alpha) = 0$ then $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so σ sends any root of $f(X)$ in L to a root of $f(X)$ in L. The roots of $f(X)$ in L are a finite set and σ is an injective function, so its effect on the roots must be a permutation: any injective function of a finite set to itself is surjective too. □

Corollary 3.5. *Each K-automorphism of L permutes each set of K-conjugates in L.*

Proof. Let $\alpha \in L$ have minimal polyomial $\pi(X)$ in $K[X]$. Apply Theorem 3.4 to the roots of $\pi(X)$ in L. □

Example 3.6. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. A K-automorphism of L sends $\sqrt{2}$ to $\sqrt{2}$ or $-\sqrt{2}$, because $\sqrt{2}$ has minimal polynomial $X^2 - 2 \in \mathbf{Q}[X]$, whose roots in L are $\pm\sqrt{2}$. A K-automorphism of L can't send $\sqrt{2}$ to $\sqrt{3}$, for instance, since $\sqrt{3}$ is not a root of $X^2 - 2$. While Corollary 3.5 puts a constraint on where a K-automorphism of L could send $\sqrt{2}$ (to roots of $X^2 - 2$), it does not assure us that all those options are in fact possible.

Example 3.7. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2})$. The field L contains $\sqrt{2} = \sqrt[4]{2}^2$, and a K-automorphism of L can only send $\sqrt{2}$ to $\pm\sqrt{2}$ by the same argument as in the previous example. But in fact it is impossible for a K-automorphism of L to send $\sqrt{2}$ to $-\sqrt{2}$.

Each $\mathbf{Q}$-automorphism σ of $\mathbf{Q}(\sqrt[4]{2})$ sends $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$ (roots of $X^4 - 2$ in $\mathbf{Q}(\sqrt[4]{2})$ are permuted by σ), and $\sqrt{2} = \sqrt[4]{2}^2$, so $\sigma(\sqrt{2}) = \sigma(\sqrt[4]{2}^2) = \sigma(\sqrt[4]{2})^2 = (\pm\sqrt[4]{2})^2 = \sqrt{2}$. Therefore no $\mathbf{Q}$-automorphism of $\mathbf{Q}(\sqrt[4]{2})$ sends $\sqrt{2}$ to $-\sqrt{2}$ even though they have the same minimal polynomial over $\mathbf{Q}$.

Example 3.8. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[3]{2}, \omega)$, where ω is a nontrivial cube root of unity. The polynomial $X^3 - 2$ has 3 roots in L: $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. Any K-automorphism of L permutes these 3 roots. Are all six permutations of these 3 roots realized by K-automorphisms of L?

Example 3.9. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2}, i)$. The polynomial $X^4 - 2$ has all four roots in L: $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. These four roots have $4! = 24$ permutations. Is every permutation of these four numbers the restriction of some K-automorphism of L?

We will see later that for Galois extensions L/K, any two K-conjugates α and β in L are related by K-automorphism: $\beta = \sigma(\alpha)$ for some K-automorphism σ of L. This connects the study of roots of an irreducible polynomial to group theory.

4. Isomorphism of splitting fields

Theorem 4.1. *Let K be a field and $f(X) \in K[X]$ be nonconstant. Any two splitting fields of $f(X)$ over K are K-isomorphic.*

Proof. Let $n = \deg f \geq 1$ and let L_1 and L_2 be splitting fields of $f(X)$ over K, so

$$L_1 = K(\alpha_1, \dots, \alpha_n), \quad L_2 = K(\beta_1, \dots, \beta_n),$$

where the α_i's and β_j's are full sets of roots of $f(X)$. (Some α_i's and some β_j's may be repeated since $f(X)$ might not be separable.) We want to show there is a field isomorphism $L_1 \to L_2$ which fixes the elements of K.

Since L_1 and L_2 are not zero, the ring $L_1 \otimes_K L_2$ is not zero because the tensor product of nonzero vector spaces is not zero. Since L_1/K and L_2/K are algebraic, we can write $L_1 = K[\alpha_1, \dots, \alpha_n]$ and $L_2 = K[\beta_1, \dots, \beta_n]$. Thus $L_1 \otimes_K L_2$ is generated *as a K-algebra* by the $2n$ elementary tensors $\{\alpha_i \otimes 1, 1 \otimes \beta_j\}$. Pick a maximal ideal $\mathfrak{m}$ in $L_1 \otimes_K L_2$ and consider the composite map

$$L_1 \to L_1 \otimes_K L_2 \to (L_1 \otimes_K L_2)/\mathfrak{m},$$

where the first map is $x \mapsto x \otimes 1$ and the second map is the natural reduction. Both are K-algebra homomorphisms, so the composite is as well. Since L_1 is a field, the composite map is injective, so we can regard $(L_1 \otimes_K L_2)/\mathfrak{m}$ as a field extension of L_1. The α_i's are a full set of roots of $f(X)$ in L_1, so the only roots of $f(X)$ in $(L_1 \otimes_K L_2)/\mathfrak{m}$ are the $\alpha_i \otimes 1 \bmod \mathfrak{m}$. Each $1 \otimes \beta_j \bmod \mathfrak{m}$ is a root of $f(X)$, so $1 \otimes \beta_j \equiv \alpha_i \otimes 1 \bmod \mathfrak{m}$ for some i. Therefore $(L_1 \otimes_K L_2)/\mathfrak{m}$ is generated as a K-algebra by all $\alpha_i \otimes 1 \bmod \mathfrak{m}$, which proves the above map $L_1 \to (L_1 \otimes_K L_2)/\mathfrak{m}$ is surjective, and hence is a K-algebra isomorphism.

We get a K-algebra isomorphism $L_2 \to (L_1 \otimes_K L_2)/\mathfrak{m}$ in a similar way. Composing $L_1 \to (L_1 \otimes_K L_2)/\mathfrak{m}$ with the inverse of $L_2 \to (L_1 \otimes_K L_2)/\mathfrak{m}$ gives us a K-algebra isomorphism from L_1 to L_2. □

Remark 4.2. Each $\alpha_i \otimes 1$ and $1 \otimes \beta_j$ in $L_1 \otimes_K L_2$ is a solution to $f(t) = 0$. This typically gives us $2n$ solutions to $f = 0$ in $L_1 \otimes_K L_2$ when $f(X)$ is separable,[1] so we should anticipate a collapsing of these roots into each other when we reduce $L_1 \otimes_K L_2$ modulo a maximal ideal and get a field, where $f(X)$ always has at most n roots.

It might at first seem curious that the construction of a K-algebra isomorphism $L_1 \to L_2$ succeeded using any maximal ideal in $L_1 \otimes_K L_2$. In fact, different maximal ideals provide us with all the different isomorphisms. Let's look at an example before proving the general result.

Example 4.3. Two splitting fields for $X^2 - 2$ over $\mathbf{Q}$ are $L_1 = \mathbf{Q}[Y]/(Y^2 - 2)$ and $L_2 = \mathbf{Q}(\sqrt{2})$ (a subfield of $\mathbf{R}$). There are two $\mathbf{Q}$-isomorphisms $L_1 \to L_2$, determined by the identification of Y in L_1 with $\pm\sqrt{2}$ in L_2. The tensor product of L_1 and L_2 over $\mathbf{Q}$ is

$$L_1 \otimes_{\mathbf{Q}} L_2 = \mathbf{Q}[Y]/(Y^2 - 2) \otimes_{\mathbf{Q}} \mathbf{Q}(\sqrt{2}) \cong \mathbf{Q}(\sqrt{2})[Y]/(Y^2 - 2) = \mathbf{Q}(\sqrt{2})[Y]/(Y - \sqrt{2})(Y + \sqrt{2}).$$

[1] This isn't always true: if $\alpha_i \in K$ then α_i is some β_j and $\alpha_i \otimes 1 = 1 \otimes \alpha_i$.

Using the Chinese remainder theorem,

$$\mathbf{Q}(\sqrt{2})[Y]/(Y-\sqrt{2})(Y+\sqrt{2}) \cong \mathbf{Q}(\sqrt{2})[Y]/(Y-\sqrt{2}) \times \mathbf{Q}(\sqrt{2})[Y]/(Y+\sqrt{2}) \cong \mathbf{Q}(\sqrt{2})^2,$$

where Y on the left corresponds to $(\sqrt{2}, -\sqrt{2})$ on the right. The ring $\mathbf{Q}(\sqrt{2}) \times \mathbf{Q}(\sqrt{2})$ has two maximal ideals, $\{0\} \times \mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2}) \times \{0\}$. The quotient by each of these maximal ideals is isomorphic to $\mathbf{Q}(\sqrt{2})$, with one sending Y to $\sqrt{2}$ and the other sending Y to $-\sqrt{2}$.

Theorem 4.4. *With notation as in the proof of Theorem* 4.1*, the set of maximal ideals in $L_1 \otimes_K L_2$ is in bijection with the set of K-algebra isomorphisms $L_1 \to L_2$.*

Proof. We want to describe a bijection between the sets

$$\{K\text{-algebra isomorphisms } L_1 \to L_2\} \longleftrightarrow \{\text{Maximal ideals in } L_1 \otimes_K L_2\}.$$

From K-algebra isomorphism to maximal ideal: Let $L_1 \xrightarrow{\varphi} L_2$ be a K-algebra isomorphism. To construct from φ a maximal ideal in $L_1 \otimes_K L_2$, we will construct a homomorphism from $L_1 \otimes_K L_2$ onto the field L_2 and then take its kernel. The function $L_1 \times L_2 \to L_2$ where $(x, y) \mapsto \varphi(x)y$ is K-bilinear, so there is a K-linear map

$$L_1 \otimes_K L_2 \xrightarrow{f_\varphi} L_2$$

where $f_\varphi(x \otimes y) = \varphi(x)y$. This is onto since $f_\varphi(1 \otimes y) = y$. A computation shows f_φ is multiplicative on products of elementary tensors, so f_φ is a K-algebra homomorphism. Since f_φ is surjective and L_2 is a field, the kernel of f_φ is a maximal ideal. Set $M_\varphi = \ker f_\varphi$.

From maximal ideal to K-algebra isomorphism: Let $\mathfrak{m}$ be a maximal ideal in $L_1 \otimes_K L_2$. We will construct from $\mathfrak{m}$ a K-algebra isomorphism $L_1 \longrightarrow L_2$. By the proof of Theorem 4.1, the natural composite maps

$$L_1 \to L_1 \otimes_K L_2 \to (L_1 \otimes_K L_2)/\mathfrak{m} \quad \text{and} \quad L_2 \to L_1 \otimes_K L_2 \to (L_1 \otimes_K L_2)/\mathfrak{m}$$

are K-algebra isomorphisms. Call the first composite map $\psi_{1,\mathfrak{m}}$ and call the second one $\psi_{2,\mathfrak{m}}$. Set $\psi_\mathfrak{m} = \psi_{2,\mathfrak{m}}^{-1} \circ \psi_{1,\mathfrak{m}}$, so $\psi_\mathfrak{m}$ is a K-algebra isomorphism from L_1 to L_2.

We will now show $\varphi \rightsquigarrow M_\varphi$ and $\mathfrak{m} \rightsquigarrow \psi_\mathfrak{m}$ are inverses of each other: $\psi_{M_\varphi} = \varphi$ and $M_{\psi_\mathfrak{m}} = \mathfrak{m}$.

Starting with φ, that $\psi_{M_\varphi} = \varphi$ means $\psi_{1,M_\varphi} = \psi_{2,M_\varphi} \circ \varphi$ as maps $L_1 \to (L_1 \otimes_K L_2)/M_\varphi$. For

$$\psi_{1,M_\varphi} \colon L_1 \longrightarrow L_1 \otimes_K L_2 \longrightarrow (L_1 \otimes_K L_2)/M_\varphi$$

the effect is $x \mapsto x \otimes 1 \mapsto x \otimes 1 \bmod M_\varphi$. For

$$\psi_{2,M_\varphi} \circ \varphi \colon L_1 \to L_2 \longrightarrow L_1 \otimes_K L_2 \longrightarrow (L_1 \otimes_K L_2)/M_\varphi$$

the effect is $x \mapsto \varphi(x) \mapsto 1 \otimes \varphi(x) \mapsto 1 \otimes \varphi(x) \bmod M_\varphi$. Therefore we need to show $x \otimes 1 \equiv 1 \otimes \varphi(x) \bmod M_\varphi$. Recall that $M_\varphi = \ker f_\varphi$, so this congruence amounts to saying $f_\varphi(x \otimes 1) = f_\varphi(1 \otimes \varphi(x))$. From the definition of f_φ we have $f_\varphi(x \otimes 1) = \varphi(x) \cdot 1 = \varphi(x)$ and $f_\varphi(1 \otimes \varphi(x)) = \varphi(1)\varphi(x) = \varphi(x)$.

Starting with $\mathfrak{m}$, that $M_{\psi_\mathfrak{m}} = \mathfrak{m}$ means $\ker f_{\psi_\mathfrak{m}} = \mathfrak{m}$. We will show the diagram

$$\begin{tikzcd}
& L_1 \otimes_K L_2 \arrow[dl, "f_{\psi_\mathfrak{m}}"'] \arrow[dr, "\text{redn.}"] & \\
L_2 \arrow[rr, "\psi_{2,\mathfrak{m}}"'] & & (L_1 \otimes_K L_2)/\mathfrak{m}
\end{tikzcd}$$

commutes. Then since $\psi_{2,\mathfrak{m}}$ is an isomorphism, the kernels of the two maps out of $L_1 \otimes_K L_2$ would be equal, so $\ker f_{\psi_\mathfrak{m}} = \mathfrak{m}$.

To verify commutativity of the diagram, it suffices (by additivity of all the maps) to focus on elementary tensors $x \otimes y$ in $L_1 \otimes_K L_2$, where we want to check

$$\psi_{2,\mathfrak{m}}(f_{\psi_\mathfrak{m}}(x \otimes y)) \overset{?}{=} x \otimes y \bmod \mathfrak{m}.$$

The left side is

$$\begin{aligned}
\psi_{2,\mathfrak{m}}(f_{\psi_\mathfrak{m}}(x \otimes y)) &= \psi_{2,\mathfrak{m}}(\psi_\mathfrak{m}(x)y) \\
&= \psi_{2,\mathfrak{m}}(\psi_\mathfrak{m}(x))\psi_{2,\mathfrak{m}}(y) \\
&= (\psi_{2,\mathfrak{m}} \circ \psi_\mathfrak{m})(x)\psi_{2,\mathfrak{m}}(y) \\
&= \psi_{1,\mathfrak{m}}(x)\psi_{2,\mathfrak{m}}(y) \\
&= (x \otimes 1) \bmod \mathfrak{m} \cdot (1 \otimes y) \bmod \mathfrak{m} \\
&= x \otimes y \bmod \mathfrak{m}.
\end{aligned}$$

□

Theorem 4.4 tells us that counting K-isomorphisms between two splitting fields of a polynomial in $K[X]$ is the same task as counting maximal ideals in a certain (tensor product) ring. If we can compute the tensor product concretely, that provides an approach to counting K-isomorphisms of splitting fields. In particular, this would provide a way to count K-automorphisms of a splitting field over K. We'll see how to carry out this idea next.

5. Counting automorphisms

The extension $\mathbf{Q}(\sqrt[n]{2})/\mathbf{Q}$ for $n \geq 3$ has degree n but just one automorphism: the identity. In a Galois extension L/K, there are a lot of K-automorphisms of L:

Theorem 5.1. *When L/K is Galois, the number of K-automorphisms of L is $[L : K]$.*

Proof. Since L is, by definition, the splitting field of a separable polynomial, the number of K-automorphisms of L is the number of maximal ideals in the ring $L \otimes_K L$. Let's compute this ring by using the primitive element theorem.

Since L is the splitting field of a separable polynomial, we can write $L = K(\alpha_1, \ldots, \alpha_n)$ where the α_i's are the roots of a separable polynomial $f(X) \in K[X]$. Each α_i is separable over K, so by a theorem about separability every element of L is separable over K. Then the primitive element theorem implies $L = K(\gamma)$ for some γ. Let $f(X) \in K[X]$ be the minimal polynomial of γ over K, so $L \cong K[X]/(f(X))$ and $\deg f = [L : K]$. Call this degree d.

The isomorphism between L and $K[X]/(f(X))$ is best thought of as the evaluation mapping at γ from $K[X]/(f(X))$ onto L. This is a K-algebra isomorphism (meaning it fixes the elements of K). Tensoring both sides of this isomorphism with L, we get an L-algebra isomorphism (designated by $\cong_L$)

$$\begin{aligned}
L \otimes_K L &\cong_L L \otimes_K K[X]/(f(X)) \\
&\cong_L L[X]/(f(X)) \\
&\cong_L L[X]/(X - \gamma_1) \cdots (X - \gamma_d) \\
&\cong_L L[X]/(X - \gamma_1) \times \cdots \times L[X]/(X - \gamma_d) \\
&\cong_L L \times \cdots \times L.
\end{aligned}$$

Therefore $L \otimes_K L \cong L^d$, so the number of maximal ideals in $L \otimes_K L$ is the number of maximal ideals in L^d. What are the maximal ideals in L^d? One way to construct maximal ideals is to have 0 in one component and L in all the others (this is the kernel of the projection homomorphism to one component). That gives us d maximal ideals in L^d. Are there more?

In a product of commutative rings $R \times S$, the prime ideals have the form $\mathfrak{p} \times S$ and $R \times \mathfrak{q}$, where $\mathfrak{p}$ and $\mathfrak{q}$ are prime in R and S. Therefore the maximal ideals in $R \times S$ are $\mathfrak{m} \times S$ and $R \times \mathfrak{n}$ where $\mathfrak{m}$ and $\mathfrak{n}$ are maximal ideals in R and S, respectively. Extending this to a product of more than two rings, the maximal ideals in $R_1 \times \cdots \times R_n$ are ideals with ith component R_i except for one component that is a maximal ideal of that component ring. Therefore in a product of fields $F_1 \times \cdots \times F_n$ the maximal ideals are $\{0\}$ in one component and F_i in the rest. In particular, L^d has d maximal ideals, and they are the ones we already described.

Thus the number of K-automorphisms of L, which equals the number of maximal ideals in $L \otimes_K L \cong L^d$, is $d = [L : K]$. □

6. Properties of Galois extensions

Here is the first significant role for a Galois group in systematizing our understanding of the K-conjugates of an element in a Galois extension.

Theorem 6.1. *If L/K is a Galois extension then*

(1) *$\alpha \in K$ if and only if $\sigma(\alpha) = \alpha$ for all K-automorphisms σ of L,*
(2) *for each $\alpha \in L$, its K-conjugates are $\sigma(\alpha)$ as σ runs over K-automorphisms of L.*

Proof. 1) If $\alpha \in K$, then certainly α is fixed by all K-automorphisms of L. Conversely, suppose α is fixed by all K-automorphisms of L. How can we show $\alpha \in K$? Set $F = K(\alpha)$ and consider the following tower of fields.

$$\begin{tikzcd}
L \arrow[d, dash] \\
F \arrow[d, dash] \\
K
\end{tikzcd}$$

Because α is fixed by every K-automorphism of L, all elements of F are fixed by every K-automorphism of L. That means K-automorphisms of L are F-automorphisms of L. Conversely, any F-automorphism of L is a K-automorphism of L since $K \subset F$. In other words, on the field L the K-automorphisms are the same thing as the F-automorphisms.

Since L is a splitting field over K of a separable polynomial in $K[X]$, L is also a splitting field over F of the same separable polynomial now viewed in $F[X]$. Therefore L/K is Galois and L/F is Galois. From Theorem 5.1, by counting K-automorphisms of L and F-automorphisms of L (which are the same thing) we obtain $[L : K] = [L : F]$. Thus, from the tower of fields we must have $[F : K] = 1$, so $F = K$, *i.e.*, $K(\alpha) = K$. Hence $\alpha \in K$.

2) Let $\alpha \in L$. We are going to directly write down a separable polynomial in $K[X]$ with α as a root. Let the list of all K-automorphisms of L applied to α have distinct members $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. (For example, if $\alpha \in K$ then this set has one term in it even though

$[L:K]$ could be large.) We will show the polynomial with these *different* roots,

$$h_\alpha(X) = \prod_{i=1}^{m}(X - \sigma_i(\alpha)),$$

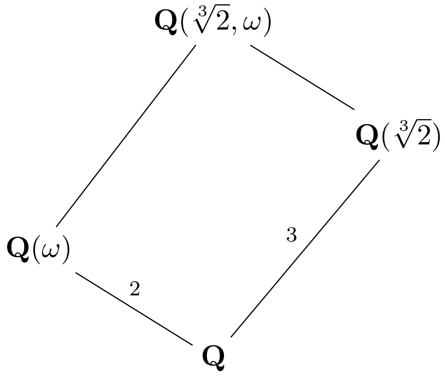
is in $K[X]$; note it is separable by construction. Why are the coefficients of $h_\alpha(X)$ in K? For any K-automorphism σ of L, each $\sigma(\sigma_i(\alpha)) = (\sigma\sigma_i)(\alpha)$ is some $\sigma_j(\alpha)$ by the definition of $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. So σ sends this finite set of roots of $h_\alpha(X)$ back to itself. It does so injectively, so it must do so surjectively too. Therefore applying σ to coefficients, which is a ring automorphism of $L[X]$, sends $h_\alpha(X)$ to $\prod_{i=1}^{m}(X - \sigma(\sigma_i(\alpha))) = \prod_{j=1}^{m}(X - \sigma_j(\alpha)) = h_\alpha(X)$. Thus each coefficient of $h_\alpha(X)$ is fixed by all K-automorphisms of L, so $h_\alpha(X) \in K[X]$ by part 1.

Next we show $h_\alpha(X)$ is the *minimal* polynomial of α in $K[X]$. Suppose $f(X) \in K[X]$ has α as a root. We want show $\deg h_\alpha(X) \leq \deg f(X)$. Since the coefficients of $f(X)$ are in K, for any K-automorphism σ of L we have $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so $f(X)$ is divisible by $X - \sigma(\alpha)$. Running over the *distinct* values of $\sigma(\alpha)$ shows $f(X)$ is divisible by their product $h_\alpha(X)$, so $\deg h_\alpha \leq \deg f$. Thus $h_\alpha(X)$ has α as a root and is the lowest degree polynomial in $K[X]$ with that property, so it is the minimal polynomial of α over K. From the definition of $h_\alpha(X)$ and its minimality, the K-conjugates of α are $\sigma(\alpha)$ as σ runs over all the K-automorphisms of L. □

Definition 6.2. When L/K is a Galois extension, the set of all K-automorphisms of L is called the *Galois group* of L/K and it is denoted $\mathrm{Gal}(L/K)$.

Example 6.3. Let L/K be a quadratic extension not in characteristic 2, so $L = K(\sqrt{d})$ for some $d \in K^\times$. This is Galois, so it has 2 K-automorphisms: one is the identity and one is not. A K-automorphism of $K(\sqrt{d})$ is determined by its value on $\sqrt{d}$, which is $\pm\sqrt{d}$. The nontrivial element of $\mathrm{Gal}(L/K)$ is frequently called the conjugation of L. For example, the elements of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ are the identity and complex conjugation.

Example 6.4. The field $\mathbf{Q}(\sqrt[3]{2}, \omega)$ is a splitting field over $\mathbf{Q}$ for $X^3 - 2$, which is separable since any irreducible in $\mathbf{Q}[X]$ is separable. So $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is a Galois extension. By Theorem 5.1, the number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is $[\mathbf{Q}(\sqrt[3]{2}, \omega) : \mathbf{Q}] = 6$. (For comparison, recall from Example 1.9 with $n = 3$ that the number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is 1, even though the field extension has degree 3: there is just nowhere for $\sqrt[3]{2}$ to go in $\mathbf{Q}(\sqrt[3]{2})$ except to itself.) We will give two ways to think about $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$.



For the first way, each σ in $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$ is determined by its effect on the 3 roots of X^3-2, which are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, since these roots generate the top field over the bottom field (note $\omega = \omega\sqrt[3]{2}/\sqrt[3]{2}$ is a ratio of two cube roots of 2). There are at most 6 permutations of these 3 roots, and since we know there are 6 automorphisms every permutation of the roots comes from an automorphism of the field extension. Therefore $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q}) \cong S_3$ with S_3 thought of as the symmetric group on the set of 3 roots of X^3-2.

For another viewpoint, any σ in the Galois group is determined by the two values $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}\}$ and $\sigma(\omega) \in \{\omega,\omega^2\} = \{\omega,\omega^{-1}\}$. Therefore there are at most $3\cdot 2 = 6$ possibilities for σ. Since 6 is the number of automorphisms, all of these possibilities really work: any choice of a root of X^3-2 for $\sigma(\sqrt[3]{2})$ and a nontrivial cube root of unity for $\sigma(\omega)$ does come from an automorphism σ. Two particular automorphisms in the Galois group are r and s, where $r(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $r(\omega) = \omega$, and $s(\sqrt[3]{2}) = \sqrt[3]{2}$ and $s(\omega) = \omega^2$. The following table shows we can get 6 automorphism from products (compositions) of r and s.

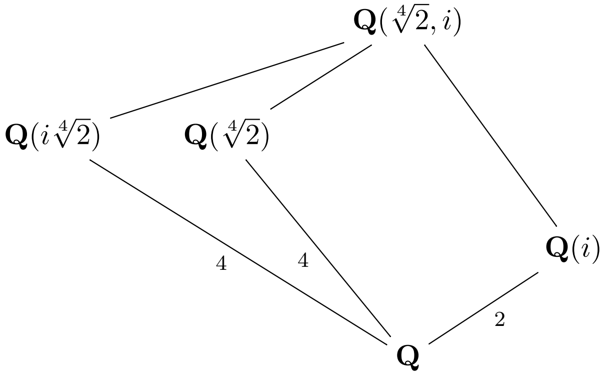
σ	id	r	r^2	s	rs	r^2s
$\sigma(\sqrt[3]{2})$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
$\sigma(\omega)$	ω	ω	ω	ω^2	ω^2	ω^2

Table 1

The 6 automorphisms in the table are different since their effects on $\sqrt[3]{2}$ or ω are not the same, so these 6 automorphisms fill up the Galois group. Check that r^3 is the identity and s^2 is the identity, and $sr = r^2s$, so our group of order 6 is generated by elements of order 3 (namely r) and 2 (namely s) with $sr = r^2s$. This makes the Galois group look like D_3.

That we found two different models for $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$, as S_3 and as D_3, is no surprise since both of these groups are nonabelian and any two nonabelian groups of size 6 are isomorphic.

Example 6.5. The extension $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ is Galois by the same reasoning as in the previous example: the top field is the splitting field over $\mathbf{Q}$ for X^4-2, which is separable. The diagram below shows some of the intermediate fields, but these are not all the intermediate fields. For instance, $\mathbf{Q}(\sqrt{2})$ is inside $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$. (This is not the only missing subfield.)


$\mathbf{Q}(\sqrt[4]{2},i)$
$\mathbf{Q}(i\sqrt[4]{2})$
$\mathbf{Q}(\sqrt[4]{2})$
$\mathbf{Q}(i)$
4
4
2
$\mathbf{Q}$

Although any element of $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ permutes the 4 roots of X^4-2, not all 24 permutations of the roots are realized by the Galois group. (This is a contrast to

$\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$, where all 6 permutations of the three roots of X^3-2 *are* realized as automorphisms in the Galois group.) For example, $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ add to 0, so under a field automorphism these two roots go to roots which are also negatives of each other. No field automorphism of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ could send $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ and $-\sqrt[4]{2}$ to $\sqrt[4]{2}$ because that doesn't respect the algebraic relation $x+y=0$ which holds for $x=\sqrt[4]{2}$ and $y=-\sqrt[4]{2}$.

To figure out what $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ is concretely, we think about an automorphism σ by what it does to $\sqrt[4]{2}$ and i, rather than what it does to all the fourth roots of 2. Since $\sigma(\sqrt[4]{2})$ has to be a root of X^4-2 (4 possible values) and $\sigma(i)$ has to be a root of X^2+1 (2 possible values), there are at most $4\cdot 2=8$ automorphisms of $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$. Because $[\mathbf{Q}(\sqrt[4]{2},i):\mathbf{Q}]=8$, $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ has size 8 and therefore all assignments of $\sigma(\sqrt[4]{2})$ and $\sigma(i)$ to roots of X^4-2 and X^2+1, respectively, *must* be realized by field automorphisms. Let r and s be the automorphisms of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ determined by[2]

$$r(\sqrt[4]{2})=i\sqrt[4]{2},\quad r(i)=i,\quad s(\sqrt[4]{2})=\sqrt[4]{2},\quad s(i)=-i.$$

By taking powers and products (that is, composites) of automorphisms, we obtain the following table of 8 different automorphisms of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$. (They are different because they don't have the same effect on both $\sqrt[4]{2}$ and i, which generate the field extension).

σ	id	r	r^2	r^3	s	rs	r^2s	r^3s
$\sigma(\sqrt[4]{2})$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

TABLE 2

A calculation at $\sqrt[4]{2}$ and i shows $r^4=\mathrm{id}$, $s^2=\mathrm{id}$, and $rs=sr^{-1}$, so $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ is isomorphic (not equal, just isomorphic!) to D_4, where D_4 can be viewed as the 8 symmetries of the square whose vertices are the four complex roots of X^4-2: r is rotation by 90 degrees counterclockwise and s is complex conjugation, which is a reflection across one diagonal of this square. (Strictly speaking, r and s as automorphisms are only defined on $\mathbf{Q}(\sqrt[4]{2},i)$, not on all complex numbers. While r looks like a rotation by 90 degrees on the four roots of X^4-2, it is not really a rotation on most elements of $\mathbf{Q}(\sqrt[4]{2})$, since r is not multiplication by i everywhere. For example, $r(1)$ is 1 rather than i, and $r(i)$ is i rather than -1. The function s, however, does coincide with complex conjugation on all of $\mathbf{Q}(\sqrt[4]{2},i)$.)

Since $\mathbf{Q}(\sqrt[4]{2},i)$ is a Galois extension of $\mathbf{Q}$, the minimal polynomial over $\mathbf{Q}$ of any element in $\mathbf{Q}(\sqrt[4]{2},i)$ splits completely over $\mathbf{Q}(\sqrt[4]{2},i)$. For example, let $\alpha=\sqrt[4]{2}+\sqrt{2}+1$. The $\mathbf{Q}$-conjugates of α are found by applying $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ to α and seeing what different numbers come out. This amounts to replacing $\sqrt[4]{2}$ in the expression for α by the 4 different fourth roots of 2 and replacing $\sqrt{2}=\sqrt[4]{2}^2$ in the expression for α by the squares of those respective fourth roots of 2. We obtain the list

$$\sqrt[4]{2}+\sqrt{2}+1,\quad i\sqrt[4]{2}-\sqrt{2}+1,\quad -\sqrt[4]{2}+\sqrt{2}+1,\quad -i\sqrt[4]{2}-\sqrt{2}+1.$$

Although $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ has size 8, the Galois orbit of α only has size 4: each $\mathbf{Q}$-conjugate of α is the value of 2 different elements of the Galois group (complex conjugation s does not change α, so every σ and σs have the same value at α). Therefore $\mathbf{Q}(\alpha)/\mathbf{Q}$ has degree 4. Since $\alpha\in\mathbf{Q}(\sqrt[4]{2})$, so $\mathbf{Q}(\alpha)\subset\mathbf{Q}(\sqrt[4]{2})$, a degree comparison implies $\mathbf{Q}(\alpha)=\mathbf{Q}(\sqrt[4]{2})$.

[2] These are not the same r and s as the previous example, since they are defined on different fields, although you could think of s in both cases as complex conjugation if you wish.

The next theorem shows Galois extensions are ubiquitous, especially in characteristic 0.

Theorem 6.6. *Every finite separable extension of a field can be enlarged to a finite Galois extension of the field. In particular, any finite extension of a field with characteristic* 0 *can be enlarged to a finite Galois extension.*

Proof. Write the extension as $K(\alpha_1, \ldots, \alpha_n)/K$ where each α_i is separable over K. The product of the different minimal polynomials for the α_i's is a separable polynomial in $K[X]$. Enlarging $K(\alpha_1, \ldots, \alpha_n)$ to a splitting field of this separable polynomial over K is a Galois extension of K. □

Example 6.7. The non-Galois extensions $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ live inside the Galois extensions $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$.

Remark 6.8. When L/K is Galois and F is in between them, then L/F is Galois: a separable polynomial in $K[X]$ that L is a splitting field for over K also exhibits L as a splitting field over F. The bottom part of a tower F/K *need not* be Galois when L/K is, and moreover if L/F and F/K are Galois the extension L/K need not be Galois. These are illustrated by the two towers in the diagrams below.

$$\begin{tikzcd}
L \arrow[d, dash] & \mathbf{Q}(\sqrt[4]{2}, i) \arrow[d, dash, "2"'] & \mathbf{Q}(\sqrt[4]{2}) \arrow[d, dash, "2"'] \\
F \arrow[d, dash] & \mathbf{Q}(\sqrt[4]{2}) \arrow[d, dash, "4"'] & \mathbf{Q}(\sqrt{2}) \arrow[d, dash, "2"'] \\
K & \mathbf{Q} & \mathbf{Q}
\end{tikzcd}$$

In the tower on the right, each pair of successive field extensions is quadratic (and thus Galois) but the overall extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ is not Galois. We have to enlarge $\mathbf{Q}(\sqrt[4]{2})$ further to $\mathbf{Q}(\sqrt[4]{2}, i)$ to get a Galois extension of the base field $K = \mathbf{Q}$.

It is an important issue to decide when an intermediate field is Galois over the base. We will do that as part of the fundamental theorem of Galois theory in Section 7.

Theorem 6.9. *If L_1 and L_2 are finite Galois extensions of K inside a common field then L_1L_2 is a Galois extension of K.*

Proof. Both L_1 and L_2 are splitting fields of separable polynomials in $K[X]$. Then L_1L_2 is a splitting field for the product of the two polynomials with any common factors used only once. This polynomial is separable, so L_1L_2/K is Galois. □

7. The fundamental theorem

We defined Galois extensions by building them up: L/K is Galois when L is the splitting field of a separable polynomial over $K[X]$, and in that case the number of K-automorphisms of L is $[L : K]$. Now we go the other way, by carving a Galois extension into a field using a finite group of automorphisms of the field. Let E be a field and H be a *finite* group of automorphisms of E. Then

$$E^H = \{x \in E : \sigma(x) = x \text{ for all } \sigma \in H\}$$

is a subfield of E.

Example 7.1. Let $E = \mathbf{C}$ and $H = \{\mathrm{id}, c\}$, where $c(z) = \overline{z}$ is complex-conjugation. Then $E^H = \mathbf{R}$.

Theorem 7.2 (Artin)**.** *Let E be a field and H be a finite group of automorphisms of E. If $[E : E^H]$ is finite then E/E^H is a Galois extension and* $\mathrm{Gal}(E/E^H) = H$.

Proof. First we show E/E^H is a separable extension, by an idea already used in the proof of Theorem 6.1. Pick any $\alpha \in E$. Let the finite set $\{\sigma(\alpha) : \sigma \in H\}$ be listed according to its *distinct* elements as

$$\{\sigma_1(\alpha), \dots, \sigma_m(\alpha)\}.$$

Clearly α is a root of $h_\alpha(X) = \prod_{i=1}^m (X - \sigma_i(\alpha))$, and the roots of this polynomial are distinct and all lie in E. The degree of $h_\alpha(X)$ is $m \leq \#H$. The coefficients of $h_\alpha(X)$ all lie in E^H by the same reasoning used in the proof of Theorem 6.1 to show the polynomial $h_\alpha(X)$ there has all of its coefficients fixed by the K-automorphisms of L, so E/E^H is a finite extension which is separable over E^H (that is, every element of E has a minimal polynomial in $E^H[X]$ which is separable) and each $\alpha \in E$ has degree at most $\#H$ over E^H.

So far we have not used the hypothesis that $[E : E^H]$ is finite. Now we do. Since E/E^H is a finite separable extension of degree at most $\#H$, by the primitive element theorem $E = E^H(\alpha)$ for some α, so $[E : E^H] = [E^H(\alpha) : E^H] \leq \deg h_\alpha(X) \leq \#H$. Since $h_\alpha(X)$ splits over E, E/E^H is a Galois extension, so $\#\,\mathrm{Gal}(E/E^H) = [E : E^H] \leq \#H$. Since H is a subgroup of $\mathrm{Gal}(E/E^H)$, $\#H \leq \#\,\mathrm{Gal}(E/E^H)$, so we get equality throughout:

$$\#\,\mathrm{Gal}(E/E^H) = [E : E^H] = \#H.$$

Thus $\mathrm{Gal}(E/E^H) = H$. □

We will use Theorem 7.2 once: in the proof of Theorem 7.4.

Remark 7.3. The proof of Theorem 7.2 in [1, pp. 569–571] and [3, pp. 220-222] is different from the one here (which is based on [2, pp. 263-264]). The proofs in [1] and [3] involve solving systems of linear equations.

Here is the fundamental theorem of Galois theory. Galois discovered the concept of normal subgroups from their role in the last part of the theorem.

Theorem 7.4 (Galois)**.** *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then the inclusion-reversing mappings $F \rightsquigarrow \mathrm{Gal}(L/F)$ and $H \rightsquigarrow L^H$ between the intermediate fields between K and L and the subgroups of G are inverses of each other and satisfy the following properties when F and H correspond ($F = L^H, H = \mathrm{Gal}(L/F)$):*

(a) $\#H = [L : F]$ *and* $[F : K] = [G : H]$,

(b) *two intermediate fields F and F', with corresponding subgroups H and H', are isomorphic over K if and only if H and H' are conjugate subgroups of G; in particular,* $\mathrm{Gal}(L/\sigma(F)) = \sigma\mathrm{Gal}(L/F)\sigma^{-1}$ *for* $\sigma \in G$,

(c) *F/K is Galois if and only if $H \lhd G$, in which case the restriction map $G \to \mathrm{Gal}(F/K)$, where $\sigma \mapsto \sigma|_F$, is surjective with kernel H, so $G/H \cong \mathrm{Gal}(F/K)$.*

In (7.1) we indicate the relations of part a in a diagram, where $F = L^H$ and $H = \mathrm{Gal}(L/F)$ correspond to each other. Because inclusion relations are reversed, the group diagram appears upside-down, with the larger subgroups near the bottom (having a fixed field which is closer to K).

$$\begin{tikzcd} L \arrow[d, dash] & \{1\} \arrow[d, dash, "{[L:F]}"] \\ F \arrow[d, dash] & H \arrow[d, dash, "{[F:K]}"] \\ K & G \end{tikzcd} \tag{7.1}$$

Proof. First we check the correspondences are inverses: from fields to subgroups to fields, we need $F^{\mathrm{Gal}(L/F)} = F$, and from subgroups to fields to subgroups requires $\mathrm{Gal}(L/L^H) = H$. The first equality follows from the first part of Theorem 6.1 and the second equality comes from Theorem 7.2. (We know L/L^H is finite since $K \subset L^H \subset L$ and $[L : K] < \infty$.)

For (a), since F and H correspond we have $F = L^H$, so $\#H = [L : F]$ by Theorem 7.2. The other equality in (a) follows from this: $[G : H] = \#G/\#H = [L : K]/[L : F] = [F : K]$.

For (b), first we observe that two intermediate fields F and F' are K-isomorphic if and only if $F' = \sigma(F)$ for some $\sigma \in G$. Indeed, if $F' = \sigma(F)$ for some $\sigma \in G$ then σ is a K-isomorphism from F to F'. Conversely, if F and F' are K-isomorphic let $\varphi\colon F \to F'$ be a K-isomorphism. We want to show φ, which is defined on F, is the restriction to F of some $\sigma \in G$. By the primitive element theorem, $F = K(\gamma)$ for some γ, so $K \subset F(\varphi(\gamma)) \subset F'$. Since φ fixes K, $\varphi(\gamma) \in F'$ has the same minimal polynomial over K as γ, so γ and $\varphi(\gamma)$ have the same degree over F, which means $F' = F(\varphi(\gamma))$ since $[F : K] = [F' : K]$. Since $\varphi(\gamma)$ is a K-conjugate of γ in L, by Theorem 6.1 we have $\varphi(\gamma) = \sigma(\gamma)$ for some $\sigma \in G$. Since σ and φ agree on K and on γ, they agree on $K(\gamma) = F$. That proves $\sigma|_F = \varphi$, so $F' = \varphi(F) = \sigma(F)$. Let's look at an example for a moment to see what this is saying.

Example 7.5. For the extension $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ (see Example 6.5), the intermediate fields $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$ are isomorphic over $\mathbf{Q}$ since each is the adjuncation to $\mathbf{Q}$ of one root of $X^4 - 2$. There is a $\mathbf{Q}$-isomorphism $\varphi\colon \mathbf{Q}(\sqrt[4]{2}) \to \mathbf{Q}(i\sqrt[4]{2})$ where $\varphi(\sqrt[4]{2}) = i\sqrt[4]{2}$. Some $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ restricts to φ on $\mathbf{Q}(\sqrt[4]{2})$. What is it? Using the notation of Example 6.5, $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, so r is one choice for σ. Another choice is rs, since $rs(\sqrt[4]{2}) = r(\sqrt[4]{2}) = i\sqrt[4]{2}$.

Returning to the proof of Theorem 7.4b, write any K-isomorphic copy of F in L as $\sigma(F)$ for some $\sigma \in G$. For any $\tau \in G$,

$$\begin{aligned} \tau \in \mathrm{Gal}(L/\sigma(F)) &\iff \tau(\sigma(\alpha)) = \sigma(\alpha) \text{ for all } \alpha \in F, \\ &\iff \sigma^{-1}\tau\sigma(\alpha) = \alpha \text{ for all } \alpha \in F, \\ &\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/F) = H \\ &\iff \tau \in \sigma H \sigma^{-1}, \end{aligned}$$

so $\mathrm{Gal}(L/\sigma(F)) = \sigma H \sigma^{-1} = \sigma\,\mathrm{Gal}(L/F)\sigma^{-1}$.

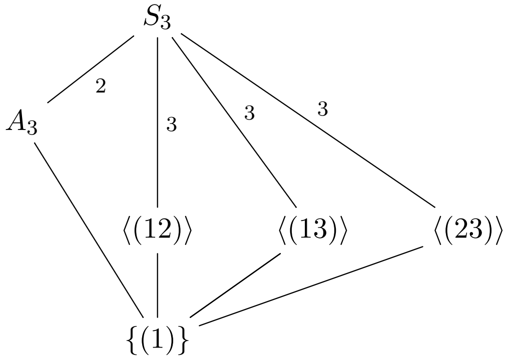
To prove (c), note that an intermediate extension F/K is separable since every element of a Galois extension is separable over the base field K. Since F is inside the Galois extension L/K, the K-conjugates of any element of F are its orbit under $\mathrm{Gal}(L/K)$ (Theorem 6.1). Therefore F/K is Galois if and only if $\sigma(F) \subset F$ for all $\sigma \in G$. Since $\sigma(F)$ and F have the same degree over K, the inclusion $\sigma(F) \subset F$ is the same as $\sigma(F) = F$. Therefore

$$\begin{aligned} F/K \text{ is Galois} &\iff \sigma(F) = F \text{ for all } \sigma \in G \\ &\iff \sigma H \sigma^{-1} = H \text{ for all } \sigma \in G \\ &\iff H \lhd G. \end{aligned}$$

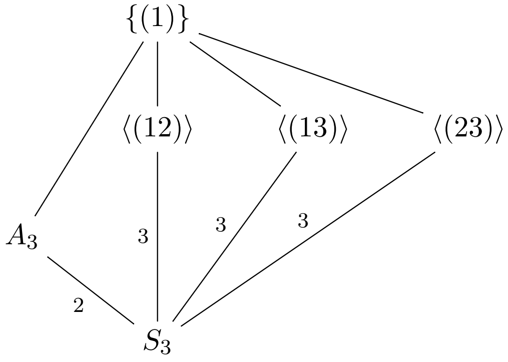
Restricting elements in $\mathrm{Gal}(L/K)$ to F defines a map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ which is a group homomorphism (check). Its kernel is $\mathrm{Gal}(L/F) = H$, so we get an embedding $G/H \hookrightarrow \mathrm{Gal}(F/K)$. The size of G/H is $[G : H] = [F : K]$, which equals $\# \mathrm{Gal}(F/K)$ since F/K is Galois. So $G/H \cong \mathrm{Gal}(F/K)$. $\square$

The bijection in Theorem 7.4 is called the *Galois correspondence.*

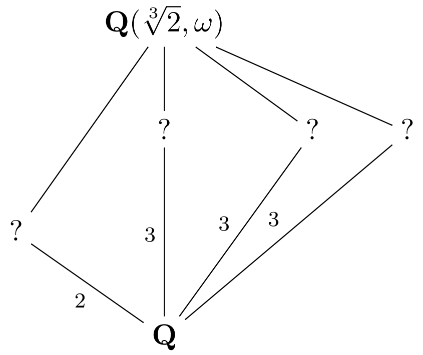
Example 7.6. The extension $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ has Galois group isomorphic to S_3 (Example 6.4). This group has 3 subgroups of order 2 and one subgroup (just A_3) of order 3. In the diagram we have indicated the indices in S_3 of subgroups.



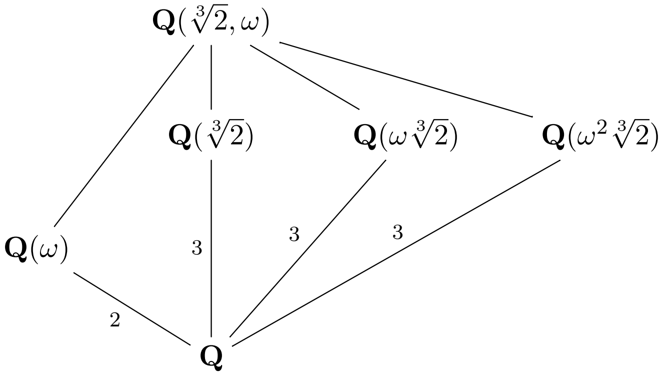
Let's flip this upside down, so larger groups are on the bottom.



By the Galois correspondence, the arrangement of subfields of $\mathbf{Q}(\sqrt[3]{2}, \omega)$ looks the same, with indices of a subgroup in the Galois group turning into degrees of a subfield over $\mathbf{Q}$.

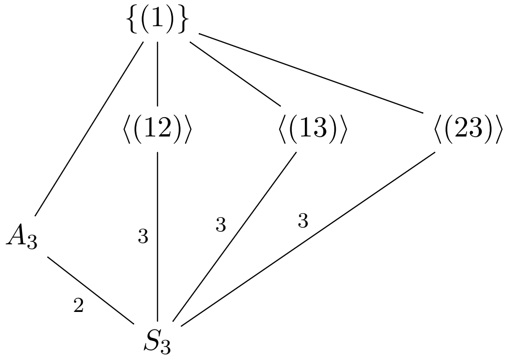


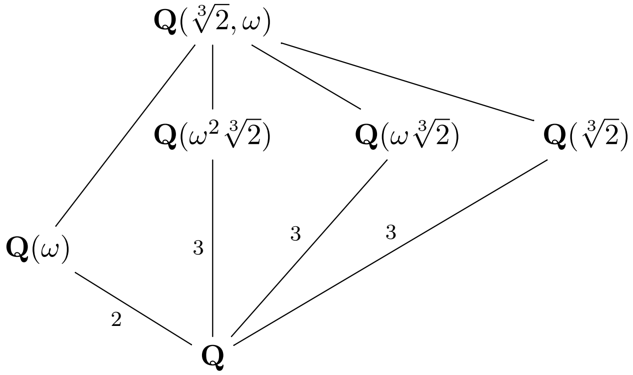
So there is one quadratic subfield and three cubic subfields. It is easy to write down enough such fields by inspection: $\mathbf{Q}(\omega)$ is quadratic and $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(\omega\sqrt[3]{2})$, and $\mathbf{Q}(\omega^2\sqrt[3]{2})$ are all cubic. (These three cubic fields are distinct since two different cube roots of 2 can't lie in the same cubic field.) So these are the only (proper) intermediate fields, and the field diagram looks like this:


$\mathbf{Q}(\sqrt[3]{2},\omega)$
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\omega\sqrt[3]{2})$
$\mathbf{Q}(\omega^2\sqrt[3]{2})$
$\mathbf{Q}(\omega)$
3
3
3
2
$\mathbf{Q}$

The subgroups of S_3 with order 2 are not normal, and likewise the cubic fields are not Galois over $\mathbf{Q}$. The subgroup A_3 is normal, and the quadratic field $\mathbf{Q}(\omega)$ is Galois over $\mathbf{Q}$.

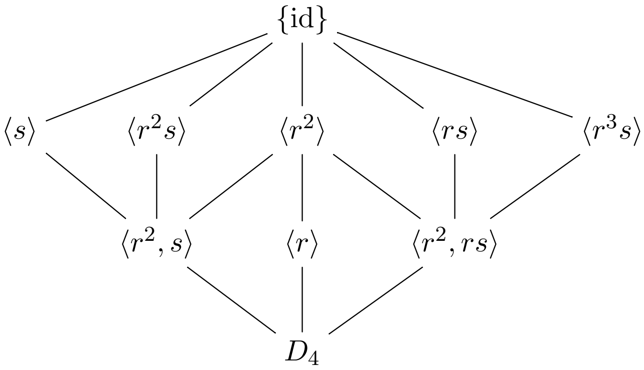
We were somewhat cavalier about the way we just wrote down the cubic fields without really paying attention to which ones should correspond to which subgroups of index 3 (order 2) in the Galois group. But we can't be more careful at this stage (beyond keeping track of indices of subgroups and degrees of subfields) because we didn't really keep track here of *how* $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$ is isomorphic to S_3. We simply used the subgroup structure of S_3 to figure out the subfield structure of $\mathbf{Q}(\sqrt[3]{2},\omega)$. If we want to match specific subgroups with specific subfields through the Galois correspondence, we have to think about S_3 as the Galois group in a definite way. There are three roots of X^3-2 being permuted by the Galois group (in all 6 possible ways), so if we label the roots abstractly as 1, 2, and 3 then we can see what the correspondence should be. Label $\sqrt[3]{2}$ as 1, $\omega\sqrt[3]{2}$ as 2, and $\omega^2\sqrt[3]{2}$ as 3. Then (12) fixes $\omega^2\sqrt[3]{2}$, and therefore $\mathbf{Q}(\omega^2\sqrt[3]{2})$ is contained in the fixed field $\mathbf{Q}(\sqrt[3]{2},\omega)^{\langle(12)\rangle}$. The subgroup $\langle(12)\rangle$ has index 3 and $\mathbf{Q}(\omega^2\sqrt[3]{2})/\mathbf{Q}$ has degree 3, so $\mathbf{Q}(\omega^2\sqrt[3]{2})$ is the full fixed field of $\langle(12)\rangle$. In a similar way, $\langle(13)\rangle$ has fixed field $\mathbf{Q}(\omega\sqrt[3]{2})$ and $\langle(23)\rangle$ has fixed field $\mathbf{Q}(\sqrt[3]{2})$. So the subgroup and subfield diagrams are aligned if we draw them as follows:



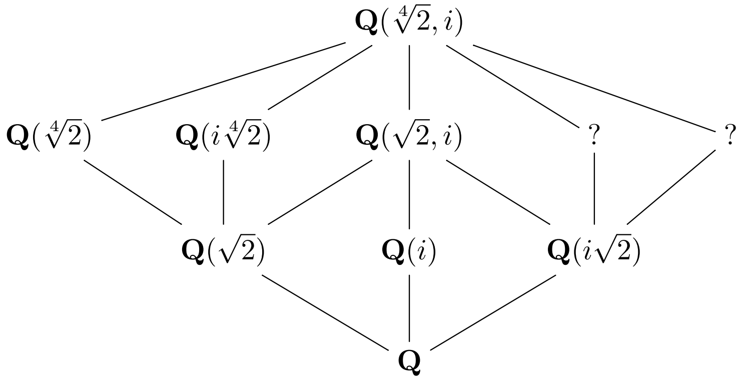

$\mathbf{Q}(\sqrt[3]{2},\omega)$
$\mathbf{Q}(\omega^2\sqrt[3]{2})$
$\mathbf{Q}(\omega\sqrt[3]{2})$
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\omega)$
3
3
3
2
$\mathbf{Q}$

Example 7.7. The extension $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ has Galois group isomorphic to D_4 according to the permutations which the Galois group induces on the fourth roots of 2. Generators are r and s where $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, $r(i) = i$ and $s(\sqrt[4]{2}) = \sqrt[4]{2}$, $s(i) = -i$ (s is complex conjugation). See Table 2 in Example 6.5.

Below is the diagram of all subgroups of D_4, written upside down.



All indices of successive subgroups here are 2, so we don't include that information in the diagram. The lattice of intermediate fields in $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ looks the same:



To check the fields have been placed correctly according to the Galois correspondence $H \rightsquigarrow \mathbf{Q}(\sqrt[4]{2},i)^H$, verify in each case that each field in the field diagram is fixed by the subgroup in the same relative position in the subgroup diagram, and the degree of the field over $\mathbf{Q}$ equals the index of the subgroup over $\mathbf{Q}$: if $F \subset \mathbf{Q}(\sqrt[4]{2},i)^H$ and $[F:\mathbf{Q}] = [D_4 : H]$ then $F = \mathbf{Q}(\sqrt[4]{2},i)^H$.

As an example, the subextension $\mathbf{Q}(i)/\mathbf{Q}$ has degree 2, so its corresponding subgroup H in D_4 has index 2. Since $r(i) = i$, $\langle r\rangle$ is a subgroup fixing i with index $8/4 = 2$, so $H = \langle r\rangle$. Thus $\mathbf{Q}(i)$ corresponds to $\langle r\rangle$. Since $\mathbf{Q}(i)$ is Galois over $\mathbf{Q}$, the restriction of an automorphism of $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ to $\mathbf{Q}(i)/\mathbf{Q}$ gives us a homomorphism $D_4 = \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ which is surjective and its kernel is the subgroup fixing $\mathbf{Q}(i)$, namely $\langle r\rangle$. So $D_4/\langle r\rangle \cong \mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$. This isomorphism with the quotient group makes sense: every element of D_4 is some r^k or $r^k s$, so modulo $\langle r\rangle$ every element of D_4 is 1 or s, and this is what we usually think of as the Galois group of $\mathbf{Q}(i)/\mathbf{Q}$: the identity and complex conjugation.

In D_4 there is only one normal subgroup of index 4, namely $\langle r^2\rangle = \{1, r^2\}$. Therefore there is only one field inside $\mathbf{Q}(\sqrt[4]{2}, i)$ of degree 4 over $\mathbf{Q}$ which is Galois over $\mathbf{Q}$. Since $\mathbf{Q}(\sqrt{2}, i)$ is such a field, that is the field corresponding to $\langle r^2\rangle$.

We have left two fields undetermined in the field diagram. They correspond to the subgroups $\langle rs\rangle$ and $\langle r^3 s\rangle$ and must have degree 4 over $\mathbf{Q}$. The smallest subgroup properly containing either of these is $\langle r^2, rs\rangle$, so we can figure out the undetermined fields by looking for an $\alpha \in \mathbf{Q}(\sqrt[4]{2}, i)$ of degree 4 over $\mathbf{Q}$ that is fixed by rs and not by r^2, and likewise find β of degree 4 over $\mathbf{Q}$ fixed by $r^3 s$ and not by r^2. Then the missing fields are $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$.

To find α, rather than blind guessing we write out a general element of $\mathbf{Q}(\sqrt[4]{2}, i)$ in a basis over $\mathbf{Q}$ and see what the condition $rs(\alpha) = \alpha$ means about the coefficients. Writing

$$\alpha = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{2}^2 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi\sqrt[4]{2}^3,$$

with rational coefficients a, b, c, d, e, f, g, h, applying rs to all terms gives

$$rs(\alpha) = a + bi\sqrt[4]{2} - c\sqrt{2} - di\sqrt[4]{2}^2 - ei + f\sqrt[4]{2} + gi\sqrt{2} - h\sqrt[4]{2}^3,$$

so

$$b = f, c = -c, e = -e, d = -h.$$

Therefore

$$\alpha = a + b(\sqrt[4]{2} + i\sqrt[4]{2}) + d(\sqrt[4]{2}^3 - i\sqrt[4]{2}^3) + gi\sqrt{2}.$$

The 4 coefficients a, b, d, g can be any rational numbers, so we have found a $\mathbf{Q}$-basis of the field fixed by $\langle rs\rangle$. To pick something simple of degree 4, we try $b = 1$ and the other coefficients equal to 0:

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

Easily $r^2(\alpha) = -\alpha$, so α is fixed by $\langle rs\rangle$ but not by $\langle r^2\rangle$, which means the field $\mathbf{Q}(\alpha)$ is inside the fixed field of $\langle rs\rangle$ but not inside the fixed field of $\langle r^2\rangle$, so $\mathbf{Q}(\alpha)$ must be the fixed field of $\langle rs\rangle$. The difference $\beta = \sqrt[4]{2} - i\sqrt[4]{2}$ is fixed by $r^3 s$ and not by r^2, so the fixed field of $\langle r^3 s\rangle$ is $(1 - i)\sqrt[4]{2}$. Now we have a complete field diagram.

$$\begin{tikzcd}
 & & \mathbf{Q}(\sqrt[4]{2}, i) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbf{Q}(\sqrt[4]{2}) \arrow[dr, dash] & \mathbf{Q}(i\sqrt[4]{2}) \arrow[d, dash] & \mathbf{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbf{Q}((1+i)\sqrt[4]{2}) \arrow[d, dash] & \mathbf{Q}((1-i)\sqrt[4]{2}) \arrow[dl, dash] \\
 & \mathbf{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbf{Q}(i) \arrow[d, dash] & \mathbf{Q}(i\sqrt{2}) \arrow[dl, dash] & \\
 & & \mathbf{Q} & &
\end{tikzcd}$$

Example 7.8. Let $\zeta_8 = e^{2\pi i/8}$ be a root of unity of order 8. The field $\mathbf{Q}(\zeta_8)$ is Galois over $\mathbf{Q}$, being the splitting field of $X^8 - 1$. We will use the Galois correspondence to find all the fields between $\mathbf{Q}$ and $\mathbf{Q}(\zeta_8)$.

Since ζ_8 is a root of $(X^8-1)/(X^4-1) = X^4+1$ and $(X+1)^4+1 = X^4+4X^3+6X^2+4X+2$ is Eisenstein at 2, so irreducible over $\mathbf{Q}$, X^4+1 is the minimal polynomial of ζ_8 over $\mathbf{Q}$. Therefore the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q})$ has order 4, which means it is either a cyclic group or a product of two groups of order 2. Which group is it?

The two nonisomorphic groups of order 4 are distinguishable from each other by the number of subgroups of order 2. If H is a subgroup of order 2 in the Galois group, with fixed field F, then $[\mathbf{Q}(\zeta_8) : F] = 2$, so $[F : \mathbf{Q}] = 4/2 = 2$. Therefore if $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q})$ is cyclic there is one quadratic field in $\mathbf{Q}(\zeta_8)$, while in the other case there are three.

$$\begin{tikzcd}
 & \mathbf{Q}(\zeta_8) \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbf{Q}(\sqrt{2}) \arrow[dr, no head] & \mathbf{Q}(i) \arrow[d, no head] & \mathbf{Q}(\sqrt{-2}) \arrow[dl, no head] \\
 & \mathbf{Q} &
\end{tikzcd}$$

In the field diagram above, we list three quadratic subfields, so $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q})$ is a product of two groups of order 2 and the fields we found are the full list of them. We find i inside $\mathbf{Q}(\zeta_8)$ since $i = \zeta_8^2$. We find $\sqrt{2}$ in $\mathbf{Q}(\zeta_8)$ from the complex representation $\zeta_8 = e^{2\pi i/8} = e^{\pi i/4} = \frac{1+i}{\sqrt{2}}$, which implies

$$\zeta_8 + \zeta_8^{-1} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} = \sqrt{2}.$$

Then $\sqrt{-2} = i\sqrt{2}$ is also in $\mathbf{Q}(\zeta_8)$.

Example 7.9. Let F be any field and $T_1, \dots, T_n$ be indeterminates over F. The T_i's are roots of the polynomial

$$(X - T_1)(X - T_2)\cdots(X - T_n) = X^n - s_1T^{n-1} + s_2T^{n-2} - \cdots + (-1)^n s_n, \tag{7.2}$$

where

$$s_k = \sum_{1 \le i_1 < \cdots < i_k \le n} T_{i_1} \cdots T_{i_k}$$

is the sum of the products of the T_i's taken k at a time. When S_n acts on the field $L := F(T_1, \dots, T_n)$ by permutations of the variables T_i, different permutations in S_n permute the variables in different ways. The fixed field L^{S_n} consists of the *symmetric* rational functions: those which are unchanged by any permutations of the variables $T_1, \dots, T_n$. The s_k's are symmetric, so $F(s_1, \dots, s_n) \subset L^{S_n}$. We will use Galois theory to show equality occurs here. (This can be done without Galois theory too.)

Let $K = F(s_1, \dots, s_n)$, so $K \subset L^{S_n} \subset L$. Thus $[L : K] \ge [L : L^{S_n}] = \#S_n = n!$. At the same time, the T_i's are all roots of the same degree n polynomial (7.2) in $K[X]$, so L/K is a splitting field of a polynomial of degree n, which means $[L : K] \le n!$. Hence $[L : K] = n! = [L : L^{S_n}]$, which forces $L^{S_n} = K$: every symmetric rational function in $T_1, \dots, T_n$ over F is a rational function of the elementary symmetric functions $s_1, \dots, s_n$.

Here are two theorems which follow from the Galois correspondence.

Theorem 7.10. *Let L/K be a finite Galois extension and F and F' be K-isomorphic intermediate fields corresponding to H and H' in $\mathrm{Gal}(L/K)$. The K-isomorphisms from F to F' in $\mathrm{Gal}(L/K)$ are the restrictions $\sigma|_F$ where $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\sigma H \sigma^{-1} = H'$.*

Proof. In the proof of Theorem 7.4b, we showed any K-isomorphism $\varphi \colon F \to F'$ can be extended to some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma H \sigma^{-1} = H'$. Then $\varphi = \sigma|_F$.

Conversely, for any $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma H \sigma^{-1} = \mathrm{Gal}(L/\sigma(F))$, so $\sigma H \sigma^{-1} = H'$ if and only if $\mathrm{Gal}(L/\sigma(F)) = \mathrm{Gal}(L/F')$, which is equivalent to $F' = \sigma(F)$ by the Galois correspondence. □

Theorem 7.10 says σ conjugates H to H' if and only if it maps F to F', which should be simple to remember.

Theorem 7.11. *Let L/K be finite Galois and F and F' be intermediate fields with corresponding subgroups H and H'.*

(a) $\mathrm{Gal}(L/FF') = H \cap H'$ *and* $\mathrm{Gal}(L/F \cap F') = \langle H, H' \rangle$*, where* $\langle H, H' \rangle$ *denotes the subgroup of* $\mathrm{Gal}(L/K)$ *generated by H and H'.*

(b) $F \subset F'$ *if and only if* $H' \subset H$*, in which case* $[F' : F] = [H : H']$.

Proof. For (a), we use the inclusion-reversing nature of the Galois correspondence. The composite field FF' is the smallest field containing both F and F' in L, so its corresponding subgroup $\mathrm{Gal}(L/FF')$ is the largest subgroup of $\mathrm{Gal}(L/K)$ contained in H and H', so it is $H \cap H'$. The argument for the other equation is similar.

For (b), the equivalence of the inclusions comes from the Galois correspondence. Moreover, we then have $[F' : F] = [L : F]/[L : F'] = \#H/\#H' = [H : H']$. □

8. Primitive Elements

Galois theory provides a way to show a number generates a Galois extension.

Theorem 8.1. *When L/K is a finite Galois extension and $\gamma \in L$, the degree $[K(\gamma) : K]$ is the size of the Galois orbit of γ. In particular, γ is a primitive element for L/K if and only if $\#\{\sigma(\gamma) : \sigma \in \mathrm{Gal}(L/K)\} = [L : K]$.*

Proof. Since γ is separable over K, $[K(\gamma) : K]$ is the number of roots of the minimal polynomial of γ over K, and these roots are all in L since L/K is Galois. From Galois theory, the roots of the minimal polynomial of γ over K are the orbit of γ under $\mathrm{Gal}(L/K)$. To say $L = K(\gamma)$ is equivalent to saying $\mathrm{Gal}(L/K)$ takes γ through as many elements as the degree $[L : K] = \#\,\mathrm{Gal}(L/K)$. □

Example 8.2. In $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$, $\sqrt[4]{2} + i$ has 8 different values under the Galois group (see Table 3), since i, $\sqrt[4]{2}$, and $i\sqrt[4]{2}$ are linearly independent over $\mathbf{Q}$. (They are part of a $\mathbf{Q}$-basis for the field extension.) Thus $\mathbf{Q}(\sqrt[4]{2}, i) = \mathbf{Q}(\sqrt[4]{2} + i)$.

On the other hand, $\sqrt[4]{2} + i\sqrt[4]{2}$ is *not* a primitive element for $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ since its Galois orbit has fewer than 8 values. There are 4 values, each arising twice in Table 4.

Table 4 tells us $\sqrt[4]{2}+i\sqrt[4]{2}$ has degree 4 over $\mathbf{Q}$. We directly find a fourth degree polynomial over $\mathbf{Q}$ with $\sqrt[4]{2}+i\sqrt[4]{2}$ as a root: setting $\alpha = \sqrt[4]{2}+i\sqrt[4]{2} = (1+i)\sqrt[4]{2}$, $\alpha^2 = 2i\sqrt{2}$, so $\alpha^4 = -8$. Thus $\sqrt[4]{2} + i\sqrt[4]{2}$ is a root of $X^4 + 8$. This must be the minimal polynomial of $\sqrt[4]{2} + i\sqrt[4]{2}$ over $\mathbf{Q}$, since we know this numebr has degree 4 over $\mathbf{Q}$. In particular, $X^8 + 4$ is irreducible over $\mathbf{Q}$.

σ	$\sigma(\sqrt[4]{2})$	$\sigma(i)$	$\sigma(\sqrt[4]{2}+i)$
1	$\sqrt[4]{2}$	i	$\sqrt[4]{2}+i$
r	$i\sqrt[4]{2}$	i	$i\sqrt[4]{2}+i$
r^2	$-\sqrt[4]{2}$	i	$-\sqrt[4]{2}+i$
r^3	$-i\sqrt[4]{2}$	i	$-i\sqrt[4]{2}+i$
s	$\sqrt[4]{2}$	$-i$	$\sqrt[4]{2}-i$
rs	$i\sqrt[4]{2}$	$-i$	$i\sqrt[4]{2}-i$
r^2s	$-\sqrt[4]{2}$	$-i$	$-\sqrt[4]{2}-i$
r^3s	$-i\sqrt[4]{2}$	$-i$	$-i\sqrt[4]{2}-i$

Table 3

σ	$\sigma(\sqrt[4]{2})$	$\sigma(i)$	$\sigma(\sqrt[4]{2}+i\sqrt[4]{2})$
1	$\sqrt[4]{2}$	i	$\sqrt[4]{2}+i\sqrt[4]{2}$
r	$i\sqrt[4]{2}$	i	$i\sqrt[4]{2}-\sqrt[4]{2}$
r^2	$-\sqrt[4]{2}$	i	$-\sqrt[4]{2}-i\sqrt[4]{2}$
r^3	$-i\sqrt[4]{2}$	i	$-i\sqrt[4]{2}+\sqrt[4]{2}$
s	$\sqrt[4]{2}$	$-i$	$\sqrt[4]{2}-i\sqrt[4]{2}$
rs	$i\sqrt[4]{2}$	$-i$	$i\sqrt[4]{2}+\sqrt[4]{2}$
r^2s	$-\sqrt[4]{2}$	$-i$	$-\sqrt[4]{2}+i\sqrt[4]{2}$
r^3s	$-i\sqrt[4]{2}$	$-i$	$-i\sqrt[4]{2}-\sqrt[4]{2}$

Table 4

Example 8.3. Let F be any field and $T_1,\dots,T_n$ be indeterminates over F. Let $L = F(T_1,\dots,T_n)$, on which S_n acts by permutations of $T_1,\dots,T_n$. From Example 7.9, the fixed field for S_n is $K = F(s_1,\dots,s_n)$, where the s_i's are the elementary symmetric polynomials in the T_i's.

The extension L/K must have a primitive element, and here is an explicit choice: $T_1T_2^2\cdots T_n^n$. To show this works, we take our cue from Theorem 8.1 and look at the S_n-orbit. For any $\sigma \in S_n$,

$$\sigma(T_1T_2^2\cdots T_n^n) = T_{\sigma(1)}T_{\sigma(2)}^2\cdots T_{\sigma(n)}^n.$$

If $\sigma(T_1T_2^2\cdots T_n^n) = \tau(T_1T_2^2\cdots T_n^n)$ then $T_{\sigma(1)}T_{\sigma(2)}^2\cdots T_{\sigma(n)}^n = T_{\tau(1)}T_{\tau(2)}^2\cdots T_{\tau(n)}^n$, so by comparing variables with the same exponent on both sides, we have $\sigma(1) = \tau(1),\dots,\sigma(n) = \tau(n)$, so $\sigma = \tau$. Therefore the S_n-orbit of $T_1T_2^2\cdots T_n^n$ has size $n! = [L:K]$, so $T_1T_2^2\cdots T_n^n$ is a primitive element of L/K.

References

[1] D. Dummit and R. Foote, "Abstract Algebra," 3rd ed., Wiley, New York, 2004.
[2] S. Lang, "Algebra," revised 3rd ed., Springer-Verlag, New York, 2002.
[3] J. Rotman, "Advanced Modern Algebra," Prentice-Hall, Upper Saddle River, NJ, 2002.