THE GALOIS CORRESPONDENCE AT WORK

KEITH CONRAD

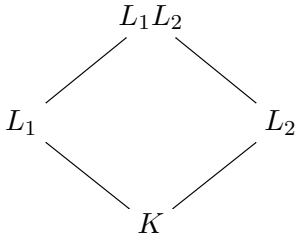
1. Examples

Theorem 1.1. *Let L_1 and L_2 be Galois over K. There is an injective homomorphism*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

given by $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$. In particular, if L_1/K and L_2/K are finite abelian extensions then L_1L_2 is a finite abelian extension of K.

Proof. A composite of Galois extensions is Galois, so L_1L_2/K is Galois.



Any $\sigma \in \mathrm{Gal}(L_1L_2/K)$ restricted to L_1 or L_2 is an automorphism since L_1 and L_2 are both Galois over K. So we get a function $R\colon \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ by $R(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2})$. We will show R is an injective homomorphism.

To show R is a homomorphism, it suffices to check the separate restriction maps $\sigma \mapsto \sigma|_{L_1}$ and $\sigma \mapsto \sigma|_{L_2}$ are each homomorphisms from $\mathrm{Gal}(L_1L_2/K)$ to $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$. For σ and τ in $\mathrm{Gal}(L_1L_2/K)$ and any $\alpha \in L_1$,

$$(\sigma\tau)|_{L_1}(\alpha) = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)),$$

and $\tau(\alpha) \in L_1$ since L_1/K is Galois, so $\sigma(\tau(\alpha)) = \sigma|_{L_1}(\tau|_{L_1}(\alpha)) = (\sigma|_{L_1} \circ \tau|_{L_1})(\alpha)$. Thus $(\sigma\tau)|_{L_1}(\alpha) = (\sigma|_{L_1} \circ \tau|_{L_1})(\alpha)$ for all $\alpha \in L_1$, so $(\sigma\tau)|_{L_1} = \sigma|_{L_1} \circ \tau|_{L_1}$. The proof that $(\sigma\tau)|_{L_2} = \sigma|_{L_2} \circ \tau|_{L_2}$ is the same.

The kernel of R is trivial, since if σ is the identity on L_1 and L_2 then it is the identity on L_1L_2. Thus R embeds $\mathrm{Gal}(L_1L_2/K)$ into the direct product of the Galois groups of L_1 and L_2 over K.

If the groups $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$ are abelian, their direct product is abelian. Therefore the embedded subgroup $\mathrm{Gal}(L_1L_2/K)$ is abelian. □

The analogue of the end of Theorem 1.1 for finite cyclic extensions is false: a compositum of two cyclic Galois extensions need not be a cyclic extension. For instance, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ and $\mathbf{Q}(\sqrt{3})/\mathbf{Q}$ are cyclic extensions but $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$ is not a cyclic extension: its Galois group is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

2. Galois groups of composites and translates

We already saw in Theorem 1.1 that if L_1/K and L_2/K are finite Galois extensions then $\mathrm{Gal}(L_1L_2/K)$ embeds into the direct product $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ by

$$\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2}).$$

When is this embedding an isomorphism? If it is not an isomorphism, what is its image?

Theorem 2.1. *Let L_1 and L_2 be Galois over K.*

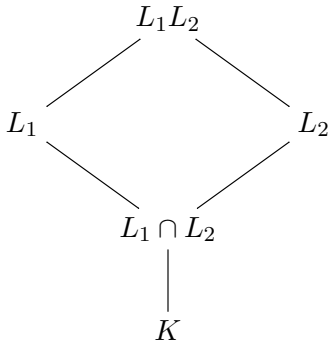
a) *The embedding*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

given by $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ is an isomorphism if and only if $L_1 \cap L_2 = K$. In particular, $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ if and only if $L_1 \cap L_2 = K$.

b) *The image of the embedding in part a is the set of compatible pairs of automorphisms: $\{(\tau_1, \tau_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) : \tau_1 = \tau_2 \text{ on } L_1 \cap L_2\}$.*

Proof. a) The embedding is an isomorphism if and only if $[L_1L_2 : K] = [L_1 : K][L_2 : K]$, or equivalently $[L_1L_2 : L_2] = [L_1 : K]$. We will show this equality occurs if and only if $L_1 \cap L_2 = K$.



To compare $[L_1L_2 : L_2]$ and $[L_1 : K]$, we will compare Galois groups having these sizes. Consider the restriction homomorphism

$$\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/K), \quad \text{where} \quad \sigma \mapsto \sigma|_{L_1}. \tag{2.1}$$

Any automorphism in the kernel of (2.1) fixes L_1 and L_2, so also L_1L_2. Thus the kernel is trivial. The image of (2.1) has the form $\mathrm{Gal}(L_1/E)$ for some field E with $K \subset E \subset L_1$. The field E is the set of elements of L_1 fixed by $\mathrm{Gal}(L_1L_2/L_2)$ acting on L_1. An element of L_1L_2 is fixed by $\mathrm{Gal}(L_1L_2/L_2)$ if and only if it lies in L_2, so the image of (2.1) is the elements of L_1 that lie in L_2. This is $L_1 \cap L_2$, so $E = L_1 \cap L_2$. Thus the image of (2.1) is $\mathrm{Gal}(L_1/L_1 \cap L_2)$, so

$$\mathrm{Gal}(L_1L_2/L_2) \cong \mathrm{Gal}(L_1/L_1 \cap L_2) \quad \text{by } \sigma \mapsto \sigma_{L_1}. \tag{2.2}$$

In particular, $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$, and this is $[L_1 : K]$ if and only if $L_1 \cap L_2 = K$.

b) Let $H = \{(\tau_1, \tau_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) : \tau_1 = \tau_2 \text{ on } L_1 \cap L_2\}$. The image of the embedding $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ lies in H (why?). We will check the image has the same size as H, so the groups coincide.

To count $|H|$, for each $\tau_2 \in \mathrm{Gal}(L_2/K)$ count those $\tau_1 \in \mathrm{Gal}(L_1/K)$ for which $\tau_1|_{L_1 \cap L_2} = \tau_2|_{L_1 \cap L_2}$. The restriction map $\mathrm{Gal}(L_1/K) \to \mathrm{Gal}(L_1 \cap L_2/K)$, where $\tau_1 \mapsto \tau_1|_{L_1 \cap L_2}$, is

surjective with kernel $\mathrm{Gal}(L_1/L_1 \cap L_2)$, so each element of $\mathrm{Gal}(L_1 \cap L_2/K)$ is $\tau_1|_{L_1 \cap L_2}$ for $|\mathrm{Gal}(L_1/L_1 \cap L_2)|$ values of τ_1 in $\mathrm{Gal}(L_1/K)$. Thus

$$\begin{aligned} |H| &= \sum_{\tau_2 \in \mathrm{Gal}(L_2/K)} |\{\tau_1 \in \mathrm{Gal}(L_1/K) : \tau_1|_{L_1 \cap L_2} = \tau_2|_{L_1 \cap L_2}\}| \\ &= \sum_{\tau_2 \in \mathrm{Gal}(L_2/K)} |\mathrm{Gal}(L_1/L_1 \cap L_2)| \\ &= |\mathrm{Gal}(L_2/K)| \cdot |\mathrm{Gal}(L_1/L_1 \cap L_2)| \\ &= [L_2 : K][L_1 : L_1 \cap L_2] \\ &= [L_2 : K][L_1L_2 : L_2] \text{ by the end of the proof of part a} \\ &= [L_1L_2 : K] \\ &= |\mathrm{Gal}(L_1L_2/K)|. \end{aligned}$$

□

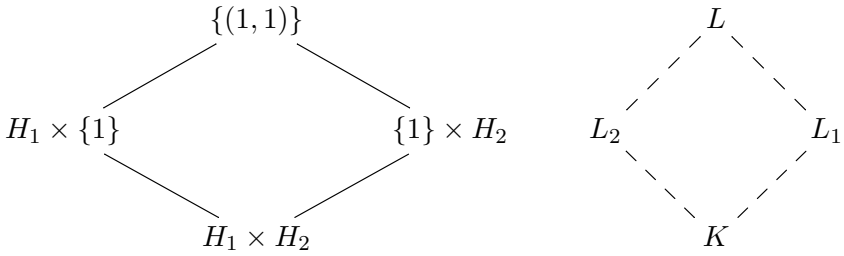
Part b says that elements of $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$ that are equal on $L_1 \cap L_2$ extend together (uniquely) to an element of $\mathrm{Gal}(L_1L_2/K)$: there is one automorphism in $\mathrm{Gal}(L_1L_2/K)$ that restricts on L_1 and L_2 to our original choices.

Example 2.2. Let $L_1 = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $L_2 = \mathbf{Q}(\sqrt[4]{2}, i)$. Both are Galois over $\mathbf{Q}$, we know their Galois groups, and $L_1 \cap L_2 = \mathbf{Q}(\sqrt{2})$. Define $\tau_1 \in \mathrm{Gal}(L_1/\mathbf{Q})$ and $\tau_2 \in \mathrm{Gal}(L_2/\mathbf{Q})$ by the conditions

$$\tau_1(\sqrt{2}) = -\sqrt{2}, \quad \tau_1(\sqrt{3}) = \sqrt{3}, \quad \tau_2(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad \tau_2(i) = i.$$

These agree on $\sqrt{2}$ since $\tau_2(\sqrt{2}) = \tau_2(\sqrt[4]{2})^2 = -\sqrt{2}$, so there is a unique $\sigma \in \mathrm{Gal}(L_1L_2/\mathbf{Q})$ that restricts to τ_1 on L_1 and τ_2 on L_2.

Remark 2.3. Theorem 2.1a admits a converse. Suppose L/K is a finite Galois extension and $\mathrm{Gal}(L/K) \cong H_1 \times H_2$ for groups H_1 and H_2.

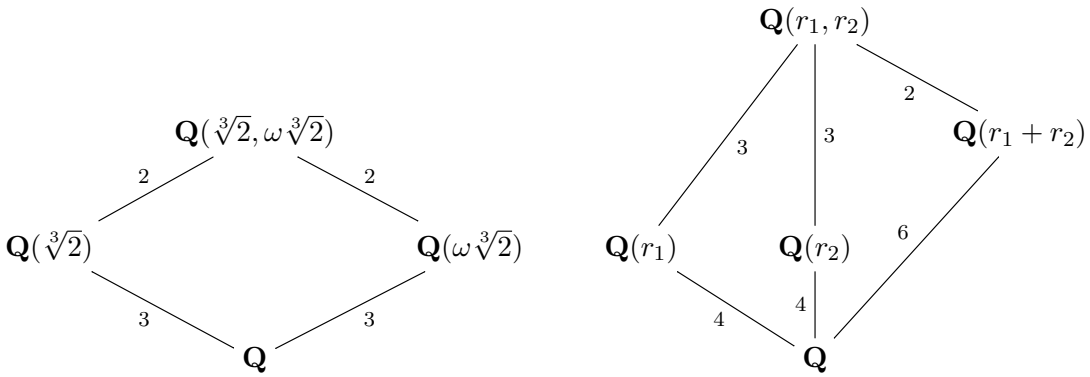


Let L_1 be the field fixed by $\{1\} \times H_2$ and L_2 be the field fixed by $H_1 \times \{1\}$. Since $H_1 \times \{1\}$ and $\{1\} \times H_2$ are normal subgroups of $H_1 \times H_2$, L_1 and L_2 are Galois over K with $\mathrm{Gal}(L_1/K) \cong (H_1 \times H_2)/(\{1\} \times H_2) \cong H_1$ and $\mathrm{Gal}(L_2/K) \cong H_2$. The subgroup corresponding to L_1L_2 is $(\{1\} \times H_2) \cap (H_1 \times \{1\}) = \{(1, 1)\}$, so $L_1L_2 = L$. The subgroup corresponding to $L_1 \cap L_2$ is $H_1 \times H_2$ (why?), so $L_1 \cap L_2 = K$.

That $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ if and only if $L_1 \cap L_2 = K$ remains true if we remove the Galois hypothesis from just one of L_1/K and L_2/K, as we'll see in Theorem 2.6 below. But if we remove the Galois hypothesis from both L_1/K and L_2/K then there are counterexamples. Here are two.

Example 2.4. If $K = \mathbf{Q}$, $L_1 = \mathbf{Q}(\sqrt[3]{2})$, and $L_2 = \mathbf{Q}(\omega\sqrt[3]{2})$, then $L_1 \cap L_2 = K$ but $[L_1L_2 : K] = 6 \neq [L_1 : K][L_2 : K]$. See the field diagram below on the left.

Example 2.5. If $K = \mathbf{Q}$, $L_1 = \mathbf{Q}(r_1)$, and $L_2 = \mathbf{Q}(r_2)$ where r_1 and r_2 are two roots of $X^4 + 8X + 12$ then $L_1 \cap L_2 = K$, but $[L_1L_2 : K] = 12 \neq [L_1 : K][L_2 : K]$. See the field diagram below on the right. If we change L_2 to $\mathbf{Q}(r_1 + r_2)$ then we still have $L_1 \cap L_2 = K$ and $[L_1L_2 : K] = 12 \neq [L_1 : K][L_2 : K]$.



Theorem 2.6. *Let L/K be a finite Galois extension and F/K be an arbitrary field extension such that L and F lie in a common field.*

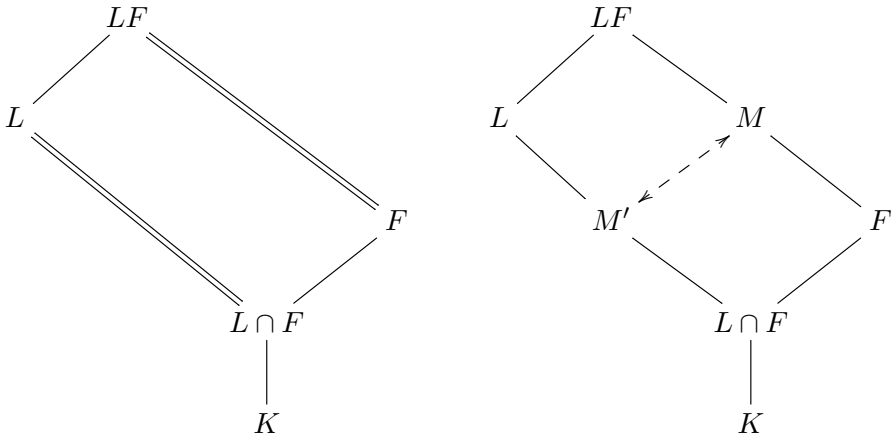
a) *The extension LF/F is finite Galois and* $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L\cap F)$ *by restriction. In particular, $[LF : F] = [L : L \cap F]$.*

   If F/K is finite then $[LF : K] = [L : K][F : K]/[L \cap F : K]$, so we have $[LF : K] = [L : K][F : K]$ if and only if $L \cap F = K$.

b) *The sets of intermediate fields $\{M : F \subset M \subset LF\}$ and $\{M' : L \cap F \subset M' \subset L\}$ are in bijection by $M \mapsto L \cap M$, with inverse $M' \mapsto M'F$.*

   In particular, every field between F and LF has the form $F(\alpha)$ where $\alpha \in L$, and if M and M' correspond by the bijection then M/F is Galois if and only if $M'/L\cap F$ is Galois, in which case $\mathrm{Gal}(M/F) \cong \mathrm{Gal}(M'/L \cap F)$ *by restriction.*

The field diagram for part a looks like the one on the left below, where parallel lines emphasize the field extensions whose Galois groups we will identify. Think of LF/F as the result of translating L/K by F (that is, taking the composite of both L and K with F).



We say Theorem 2.6 describes Galois extensions under "translation" by a field extension.

Proof. a) Since L/K is finite Galois, L is a splitting field over K of a separable polynomial $f(X) \in K[X]$. Then LF is a splitting field over F of $f(X)$, which is separable over L, so LF/F is Galois. To show $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L\cap F)$ by restricting the domain from LF to L, we essentially repeat the proof of Theorem 2.1a. Consider the restriction homomorphism

$$\mathrm{Gal}(LF/F) \to \mathrm{Gal}(L/K), \quad \text{where} \quad \sigma \mapsto \sigma|_L. \tag{2.3}$$

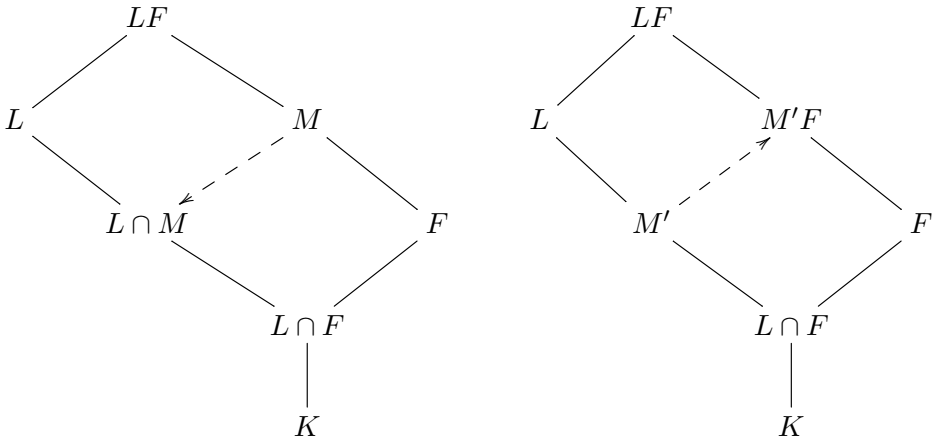
This has a trivial kernel: an automorphism in $\mathrm{Gal}(LF/F)$ that is trivial on L is trivial on LF since it is automatically trivial on F. Therefore (2.3) is injective. The image of (2.3) is a subgroup of $\mathrm{Gal}(L/K)$, so the image has the form $\mathrm{Gal}(L/E)$ for some field E between K and L. By Galois theory E is the fixed field of the image of (2.3), so $E = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(LF/F)\}$. An element of LF is fixed by $\mathrm{Gal}(LF/F)$ precisely when it belongs to F, so $E = L \cap F$. Therefore the image of (2.3) is $\mathrm{Gal}(L/L\cap F)$.

From the isomorphism of Galois groups, $[LF : F] = [L : L \cap F]$. When F/K is a finite extension, the formula for $[LF : K]$ follows by writing $[LF : K]$ as $[LF : F][F : K]$ and $[L : L \cap F]$ as $[L : K]/[L \cap F : K]$.

b) In the diagram below of intermediate fields (on the top) and subgroups (on the bottom)

$$\begin{array}{ccc} \{F \subset M \subset LF\} & \twoheadleftarrow\!\!\!\!\!\!\!\!\!\!\twoheadrightarrow & \{L \cap F \subset M' \subset L\} \\ \updownarrow & & \updownarrow \\ \text{subgps. of } \mathrm{Gal}(LF/F) & \longleftrightarrow & \text{subgps. of } \mathrm{Gal}(L/L \cap F) \end{array} \tag{2.4}$$

we have bijections along the left and right sides by the Galois correspondence and a bijection on the bottom from the group isomorphism in part a. Specifically, the bijection from left to right on the bottom is given by $H \mapsto H|_L$ (restricting all elements of a subgroup H of $\mathrm{Gal}(LF/F)$ to the field L). Composition of the side and bottom maps in either direction gives us bijections between the two sets of intermediate fields on the top of the diagram, and these bijections are inverses of each other. Our task is to show the bijections are given by the formulas $M \mapsto L \cap M$ and $M' \mapsto M'F$.



Start with a field M between F and LF. Let H be the subgroup it corresponds to in $\mathrm{Gal}(LF/F)$ by Galois theory, H' be the subgroup of $\mathrm{Gal}(L/L\cap F)$ corresponding to H under

the restriction isomorphism $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L\cap F)$, and M' be the field between $L\cap F$ and L corresponding to H' by Galois theory. We will show $M' = L \cap M$. By Galois theory

$$H = \{\sigma \in \mathrm{Gal}(LF/F) : \sigma(m) = m \text{ for all } m \in M\} = \mathrm{Gal}(LF/M), \quad H' = \{\sigma|_L : \sigma \in H\},$$

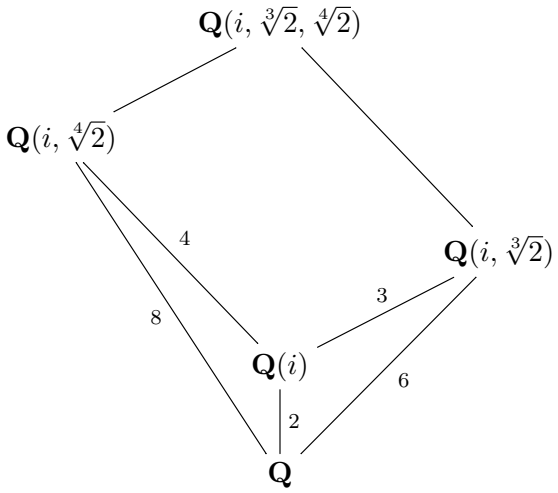
and

$$M' = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H'\} = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(LF/M)\}.$$

Since $LF = LM$, we can write $H = \mathrm{Gal}(LM/M)$, so M' is the fixed field of the restriction homomorphism $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$. By part a with M in place of F, this fixed field is $L \cap M$. Therefore $M' = L \cap M$.

Now pick M' between $L \cap F$ and L, and let M be the field it corresponds to between F and LF when we use the bijections passing through the Galois groups in (2.4) from the upper right to the upper left. We want to show $M = M'F$. Running the correspondence of (2.4) in reverse from the upper left to the upper right, we have $M' = L \cap M$ by the previous paragraph. Since our correspondence of intermediate fields is a bijection, to show $M = M'F$ it suffices to show $M' = L \cap M'F$. Obviously $M' \subset L \cap M'F$, so to prove this containment is an equality it suffices to show $[L : M'] = [L : L \cap M'F]$. By part a with $M'F$ in place of F, $[L : L \cap M'F] = [LM'F : M'F] = [LF : M'F]$, so we want to show $[LF : M'F] = [L : M']$. The field $M'F$ is intermediate in the Galois extension LF/F and the field M' is intermediate in the Galois extension $L/L\cap F$. An automorphism $\sigma \in \mathrm{Gal}(LF/F)$ is trivial on F, and thus is trivial on $M'F$ if and only if it is trivial on M', so under the restriction isomorphism $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L\cap F)$ we have $\mathrm{Gal}(LF/M'F) \leftrightarrow \mathrm{Gal}(L/M')$. In particular, $[LF : M'F] = [L : M']$. The rest of part b is left to the reader. □

Example 2.7. The extension $\mathbf{Q}(i, \sqrt[4]{2})/\mathbf{Q}$ is Galois, with group D_4. If we translate it by $\mathbf{Q}(i, \sqrt[3]{2})$ (which is *not* Galois over $\mathbf{Q}$), we get the extension $\mathbf{Q}(i, \sqrt[3]{2}, \sqrt[4]{2})/\mathbf{Q}(i, \sqrt[3]{2})$, which is Galois. To find its Galois group, start by drawing the field diagram below.



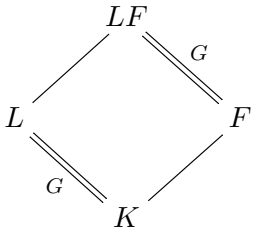
By Theorem 2.6, $\mathrm{Gal}(\mathbf{Q}(i, \sqrt[3]{2}, \sqrt[4]{2})/\mathbf{Q}(i, \sqrt[3]{2}) \cong \mathrm{Gal}(\mathbf{Q}(i, \sqrt[4]{2})/F)$, where F is the intersection of $\mathbf{Q}(i, \sqrt[4]{2})$ and $\mathbf{Q}(i, \sqrt[3]{2})$. Obviously $\mathbf{Q}(i) \subset F$, and since $[\mathbf{Q}(i, \sqrt[4]{2}) : \mathbf{Q}(i)] = 4$ and $[\mathbf{Q}(i, \sqrt[3]{2}) : \mathbf{Q}(i)] = 3$, we have $F = \mathbf{Q}(i)$.

The Galois group $\mathrm{Gal}(\mathbf{Q}(i, \sqrt[4]{2})/\mathbf{Q}(i))$ is the subgroup of $\mathrm{Gal}(\mathbf{Q}(i, \sqrt[4]{2})/\mathbf{Q})$ fixing i. This subgroup is cyclic of order 4, generated are the automorphism σ where $\sigma(i) = i$ and $\sigma(\sqrt[4]{2}) =$

$i\sqrt[4]{2}$. Therefore $\mathrm{Gal}(\mathbf{Q}(i, \sqrt[3]{2}, \sqrt[4]{2})/\mathbf{Q}(i, \sqrt[3]{2}))$ is cyclic of order 4, with generator sending $\sqrt[4]{2}$ to $i\sqrt[4]{2}$.

Theorem 2.6 did not need F/K to be finite if we're not interested in computing $[LF : K]$. Here is a worthwhile application of this level of generality.

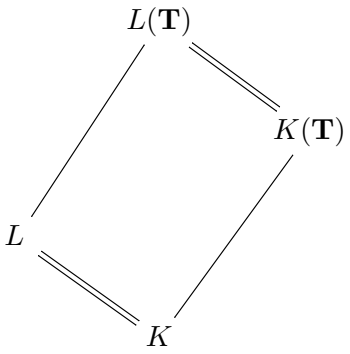
Example 2.8. If L/K is a finite Galois extension with Galois group G and F is any field extension of K lying in a common field with L and satisfying $L \cap F = K$, then LF/F is a Galois extension of F with $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F) = \mathrm{Gal}(L/K) = G$ by $\sigma \mapsto \sigma|_L$. Since σ is trivial on F, this tells us $\mathrm{Gal}(L/K)$ can be viewed as $\mathrm{Gal}(LF/F)$ by acting on L as K-automorphisms and fixing all of F. This provides a way to realize Galois groups over K as Galois groups over finite extensions of K. We will use this at the end of Section 4.



The following useful theorem is a concrete instance of Example 2.8.

Theorem 2.9. *Let L/K be a finite Galois extension and let $K(T_1, \ldots, T_n)$ be the rational function field over K in n indeterminates for $n \geq 1$. Then $L(T_1, \ldots, T_n)/K(T_1, \ldots, T_n)$ is a finite Galois extension. Its Galois group is $\mathrm{Gal}(L/K)$ acting on coefficients in $L(T_1, \ldots, T_n)$.*

Proof. The relevant field diagram is below, where we adopt the abbreviated notation $\mathbf{T}$ for the list $T_1, \ldots, T_n$.



Step 1: $L \cap K(\mathbf{T}) = K$.

It's obvious that $K \subset L \cap K(\mathbf{T})$. To prove the reverse inclusion, suppose $f(\mathbf{T}) \in L \cap K(\mathbf{T})$. Being in L, f is the root of a nonconstant polynomial $h(X) \in K[X]$, so $h(f(\mathbf{T})) = 0$ in $L(\mathbf{T})$. For each positive integer m, the substitution $T_i \mapsto T_i^m$ for all i (or $\mathbf{T} \mapsto \mathbf{T}^m$ for short) is a field homomorphism $L(\mathbf{T}) \to L(\mathbf{T})$ (not surjective for $m > 1$!) that fixes the elements of L, so $h(f(\mathbf{T}^m)) = 0$ for all m. As m varies, the rational functions $f(\mathbf{T}^m)$ take on infinitely many different values if f is nonconstant in $K(\mathbf{T})$, but that means $h(X)$ has infinitely many roots in the field $L(\mathbf{T})$, which is impossible: a nonconstant polynomial in $K[X]$ has only finitely many roots in any field extension of K. Thus f is constant in $K(\mathbf{T})$, or in other words $f \in K$.

Step 2: Study the extension $L(\mathbf{T})/K(\mathbf{T})$.

By Step 1, Theorem 2.6 says the field extension $L(\mathbf{T})/K(\mathbf{T})$ is Galois with Galois group isomorphic to $\mathrm{Gal}(L/K)$ by $\sigma \mapsto \sigma|_L$, so each element of $\mathrm{Gal}(L(\mathbf{T})/K(\mathbf{T}))$ is determined by its behavior on L. Since such an element fixes K and each $T_i \in K(\mathbf{T})$, every element of $\mathrm{Gal}(L(\mathbf{T})/K(\mathbf{T}))$ is an element of $\mathrm{Gal}(L/K)$ that acts on rational functions by fixing each T_i. Theorem 2.6 tells us all of $\mathrm{Gal}(L(\mathbf{T})/K(\mathbf{T}))$ is accounted for by the effect of different elements of $\mathrm{Gal}(L/K)$ acting on coefficients in $L(\mathbf{T})$. □

Example 2.10. The field $\mathbf{C}(T) = \mathbf{R}(T)(i)$ is quadratic over $\mathbf{R}(T)$ and $\mathrm{Gal}(\mathbf{C}(T)/\mathbf{R}(T))$ is the identity and complex conjugation acting on coefficients.

In the next theorem we continue to use $\mathbf{T}$ as shorthand for $T_1, \ldots, T_n$.

Theorem 2.11. *Let L/K be a finite Galois extension and let $\pi(\mathbf{T})$ be irreducible in $L[\mathbf{T}]$ with some coefficient in $K^\times$. Let $f(\mathbf{T})$ be the product of the different values of $\sigma(\pi(\mathbf{T}))$ as σ runs over $\mathrm{Gal}(L/K)$*

a) *The polynomial $f(\mathbf{T})$ is in $K[\mathbf{T}]$ and is irreducible there.*
b) *If $F(\mathbf{T})$ is irreducible in $K[\mathbf{T}]$ and $\pi(\mathbf{T})$ is an irreducible factor of $F(\mathbf{T})$ in $L[\mathbf{T}]$ that is scaled so it has a coefficient in $K^\times$ then, up to a constant scaling factor in L, an irreducible factoriation of $F(\mathbf{T})$ in $L[\mathbf{T}]$ is the product of the different values of $\sigma(\pi(\mathbf{T}))$ as σ runs over $\mathrm{Gal}(L/K)$.*

In practice we can scale a polynomial so its coefficient in $K^\times$ is 1. Before proving the theorem we look some examples to appreciate what the hypotheses and conclusions of the theorem are telling us and not telling us.

Example 2.12. A special case of part a for single-variable polynomials is basic to the development of Galois theory: if $\pi(T) = T - \alpha \in L[T]$ then the minimal polynomial of α over K is the product of all the different polynomials $\sigma(T - \alpha) = T - \sigma(\alpha)$ as σ runs over $\mathrm{Gal}(L/K)$. That $T - \alpha$ has leading coefficient 1 means it fits the hypothesis of part a.

Example 2.13. For the Galois extension $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$, consider $\pi(X, Y) = X + iY$ in $\mathbf{Q}(i)[X, Y]$. It is irreducible in $\mathbf{Q}(i)[X, Y]$ since it is linear and it has a coefficient equal to 1. The nontrivial element of $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ sends this polynomial to $\overline{\pi}(X, Y) = X - iY$ and $\pi\overline{\pi} = (X + iY)(X - iY) = X^2 + Y^2$, which part a of the theorem says is irreducible in $\mathbf{Q}[X, Y]$.

If $\pi(X, Y) = iX - iY = i(X - Y)$ then this is irreducible in $\mathbf{Q}(i)[X, Y]$ and the nontrivial element of $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ sends it to $\overline{\pi}(X, Y) = -iX + iY = -i(X - Y)$, with $\pi\overline{\pi} = (X - Y)^2$, which is *reducible* in $\mathbf{Q}[X, Y]$. This does not contradict part a of the theorem since $iX - iY$ does not have a coefficient in $\mathbf{Q}^\times$. If we scale $\pi(X, Y)$ to have a coefficient 1 then we get $X - Y$, which is equal to itself when applying $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ to $X - Y$, and $X - Y$ is already irreducible in $\mathbf{Q}[X, Y]$.

The polynomial $X^2 + Y^2$ is irreducible in $\mathbf{Q}[X, Y]$ and $2X + 2iY$ is an irreducible factor of it in $\mathbf{Q}(i)[X, Y]$: $X^2 + Y^2 = (2X + 2iY)(X/2 - iY/2)$. One of the coefficients of $2X + 2iY$ is in $\mathbf{Q}^\times$, so part b of the theorem says $(2X + 2iY)(2X - 2iY)$ is an irreducible factorization of $X^2 + Y^2$ in $\mathbf{Q}(i)[X, Y]$ up to a constant scaling factor. Let's check: $(2X + 2iY)(2X - 2iY)$ is $4X^2 + 4Y^2 = 4(X^2 + Y^2)$, which is not $X^2 + Y^2$ but does equal it up to a constant scaling factor.

Proof. a) For $\sigma \in \mathrm{Gal}(L/K)$, σ acting on coefficients of $L[\mathbf{T}]$ is a ring automorphism of this UFD, so it preserves irreducibility. Thus each $\sigma(\pi)$ is irreducible in $L[\mathbf{T}]$. Let the distinct

elements of $\{\sigma(\pi) : \sigma \in \mathrm{Gal}(L/K)\}$ be listed as $\{\sigma_1(\pi), \ldots, \sigma_m(\pi)\}$. The polynomials $\sigma_i(\pi)$ and $\sigma_j(\pi)$ are not scalar multiples in $L[\mathbf{T}]$: if $\sigma_i(\pi) = c\sigma_j(\pi)$ for some $c \in L^\times$, then comparing both sides at a monomial where $\pi(\mathbf{T})$ has a coefficient in $K^\times$ implies that $c = 1$, but we are assuming that $\sigma_i(\pi) \neq \sigma_j(\pi)$ for all i and j.

For $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(\sigma_i(\pi)) = (\sigma\sigma_i)(\pi)$, so each $(\sigma\sigma_i)(\pi)$ is some $\sigma_j(\pi)$. Applying σ^{-1} to $\sigma_j(\pi) = (\sigma\sigma_i)(\pi)$ returns us to $\sigma_i(\pi)$, so applying σ to the set $\{\sigma_1(\pi), \ldots, \sigma_m(\pi)\}$ is an injective mapping of the set to itself, and thus is also a surjection (the set is finite), so σ acts on the set as a permutation. This implies that the product

$$f(\mathbf{T}) = \prod_{i=1}^{m} \sigma_i(\pi) \in L[\mathbf{T}] \tag{2.5}$$

is invariant under σ: $\sigma(f) = f$ since σ applied to the polynomials $\sigma_i(\pi)$ permutes them. Thus the coefficients of $f(\mathbf{T}) \in L[\mathbf{T}]$ are each fixed by $\mathrm{Gal}(L/K)$, so the coefficients are all in K: $f(\mathbf{T}) \in K[\mathbf{T}]$.

To show $f(\mathbf{T})$ is irreducible in $K[\mathbf{T}]$, let $h(\mathbf{T})$ be a nonconstant factor of $f(\mathbf{T})$ in $K[\mathbf{T}]$. In $L[\mathbf{T}]$, (2.5) is a decomposition of $f(\mathbf{T})$ into irreducible factors, so one of them has to be a factor of $h(\mathbf{T})$, say $\sigma_i(\pi) \mid h(\mathbf{T})$ in $L[\mathbf{T}]$. Applying σ to polynomials in $L[\mathbf{T}]$ is multiplicative and thus preserves divisibility relations, so $\sigma(\sigma_i(\pi)) \mid \sigma(h)$ in $L[\mathbf{T}]$. Since h has coefficients in K we have $\sigma(h) = h$, so $(\sigma\sigma_i)(\pi) \mid h$ in $L[\mathbf{T}]$. Since $\{\sigma\sigma_i : \sigma \in \mathrm{Gal}(L/K)\} = \mathrm{Gal}(L/K)$, the definition of $\sigma_1(\pi), \ldots, \sigma_m(\pi)$ as being all the different polynomials obtained by applying $\mathrm{Gal}(L/K)$ to $\pi(\mathbf{T})$ tells us that $h(\mathbf{T})$ is divisible by every $\sigma_j(\pi)$. We showed before that the irreducibles $\sigma_j(\pi)$ in $L[\mathbf{T}]$ are *not* scalar multiples of each other in $L[\mathbf{T}]$, so $h(\mathbf{T})$ is divisible by the product of all of them! Thus $f(\mathbf{T}) \mid h(\mathbf{T})$ in $L[\mathbf{T}]$, so $\deg f \leq \deg h$: by "degree" of a polynomial in several variables we mean the largest degree of a nonzero monomial in it, and the degree does not change if the field of coefficients is made larger (like going from K to L). Therefore a nonconstant factor of $f(\mathbf{T})$ doesn't have degree less than $\deg f$, so $f(\mathbf{T})$ is irreducible in $K[\mathbf{T}]$.

b) We have a divisibility relation $\pi(\mathbf{T}) \mid F(\mathbf{T})$ in $L[\mathbf{T}]$. Applying each $\sigma \in \mathrm{Gal}(L/K)$ to this relation implies $\sigma(\pi) \mid \sigma(F)$ in $L[\mathbf{T}]$, so $\sigma(\pi) \mid F$ since F has coefficients in K. Each $\sigma(\pi)$ is irreducible, and by an argument in part a the condition that π has a coefficient in $K^\times$ implies the different $\sigma(\pi)$'s (as σ varies in $\mathrm{Gal}(L/K)$) are not scalar multiples of each other in $L[\mathbf{T}]$. Thus $F(\mathbf{T})$ is divisible in $L[\mathbf{T}]$ by the product of the distinct $\sigma(\pi)$'s. From part a, the product of the distinct $\sigma(\pi)$'s is irreducible in $K[\mathbf{T}]$. Call this product $f(\mathbf{T})$, so $f(\mathbf{T}) \in K[\mathbf{T}]$ and $f(\mathbf{T}) \mid F(\mathbf{T})$ in $L[\mathbf{T}]$. We want to show $f(\mathbf{T}) \mid F(\mathbf{T})$ in $K[\mathbf{T}]$.

The ratio $F(\mathbf{T})/f(\mathbf{T})$ is in $L[\mathbf{T}] \cap K(\mathbf{T})$. It should be plausible that $L[\mathbf{T}] \cap K(\mathbf{T}) = K[\mathbf{T}]$. This can be proved in a simple way if $n = 1$ (single-variable polynomials) using the Euclidean property of such polynomials, but multivariable polynomials over a field are not Euclidean. Instead we can argue using the notion of an integral ring extension, as follows. (If you don't know what integral extensions are, just accept that $L[\mathbf{T}] \cap K(\mathbf{T}) = K[\mathbf{T}]$.) Since L/K is a finite extension of fields, $L[\mathbf{T}]$ is an integral extension of $K[\mathbf{T}]$, so a polynomial in $L[\mathbf{T}] \cap K(\mathbf{T})$ is a rational function over K that is integral over $K[\mathbf{T}]$. The ring $K[\mathbf{T}]$ is a UFD and UFDs are integrally closed, so a rational function in $K(\mathbf{T})$ that's integral over $K[\mathbf{T}]$ must be in $K[\mathbf{T}]$. Therefore $L[\mathbf{T}] \cap K(\mathbf{T}) = K[\mathbf{T}]$, so $f(\mathbf{T}) \mid F(\mathbf{T})$ in $K[\mathbf{T}]$.

Since $f(\mathbf{T})$ and $F(\mathbf{T})$ are irreducible in $K[\mathbf{T}]$, the relation $f(\mathbf{T}) \mid F(\mathbf{T})$ in $K[\mathbf{T}]$ implies $F(\mathbf{T}) = cf(\mathbf{T})$ for some $c \in K^\times$ (because $f(\mathbf{T})$ is not constant). □

We end this section with a substantial numerical application of Theorem 2.6, taking up the next few pages.

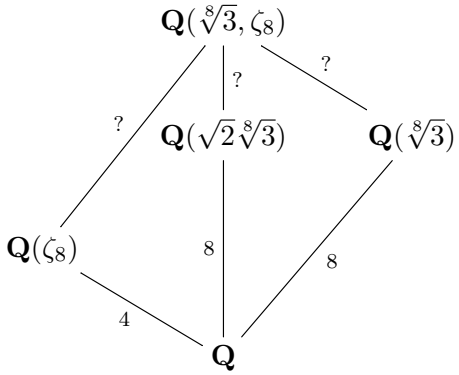
Example 2.14. We will prove the fields $\mathbf{Q}(\sqrt[8]{3})$ and $\mathbf{Q}(\sqrt{2}\sqrt[8]{3})$ are not isomorphic by placing them in a common Galois extension of $\mathbf{Q}$ and showing the subgroups they correspond to in the Galois group are not conjugate.

The minimal polynomial of $\sqrt[8]{3}$ over $\mathbf{Q}$ is $X^8 - 3$ and the minimal polynomial of $\sqrt{2}\sqrt[8]{3}$ is $X^8 - 48 = X^8 - 16 \cdot 3$. The splitting field of $X^8 - 3$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt[8]{3}, \zeta_8)$. We have $\sqrt{2} \in \mathbf{Q}(\zeta_8)$ since

$$\zeta_8 = e^{2\pi i/8} = \frac{1+i}{\sqrt{2}} \Longrightarrow \zeta_8 + \zeta_8^{-1} = \frac{2}{\sqrt{2}} = \sqrt{2},$$

so $\mathbf{Q}(\sqrt[8]{3}, \zeta_8) = \mathbf{Q}(\sqrt{2}\sqrt[8]{3}, \zeta_8)$. This Galois extension of $\mathbf{Q}$ contains both $\mathbf{Q}(\sqrt[8]{3})$ and $\mathbf{Q}(\sqrt{2}\sqrt[8]{3})$.

To compute $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$, we will first determine $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}]$.



From the field diagram above, we guess $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}] = 32$, but we should be cautious about this because we might similarly think $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 4 \cdot 4 = 16$ but in fact $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 8$. (Indeed, $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2}, i)$ since $i = \zeta_8^2$ and $\zeta_8 = (1+i)/\sqrt{2} = (1+i)/\sqrt[4]{2}^2$, and writing the field as $\mathbf{Q}(\sqrt[4]{2}, i)$ makes it easy to see it has degree 8 over $\mathbf{Q}$). By Theorem 2.6a with $K = \mathbf{Q}$, $L = \mathbf{Q}(\zeta_8)$, and $F = \mathbf{Q}(\sqrt[8]{3})$,

$$[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}] = \frac{32}{[\mathbf{Q}(\sqrt[8]{3}) \cap \mathbf{Q}(\zeta_8) : \mathbf{Q}]}.$$

The intersection $\mathbf{Q}(\sqrt[8]{3}) \cap \mathbf{Q}(\zeta_8)$ is inside $\mathbf{R}$ since $\mathbf{Q}(\sqrt[8]{3}) \subset \mathbf{R}$, and the only real subfields of $\mathbf{Q}(\zeta_8)$ are $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{2})$, so if $\mathbf{Q}(\sqrt[8]{3}) \cap \mathbf{Q}(\zeta_8)$ is not $\mathbf{Q}$ then it must be $\mathbf{Q}(\sqrt{2})$. That would put $\sqrt{2}$ inside of $\mathbf{Q}(\sqrt[8]{3})$, and there should be a strong feeling in you that $\sqrt{2} \notin \mathbf{Q}(\sqrt[8]{3})$.

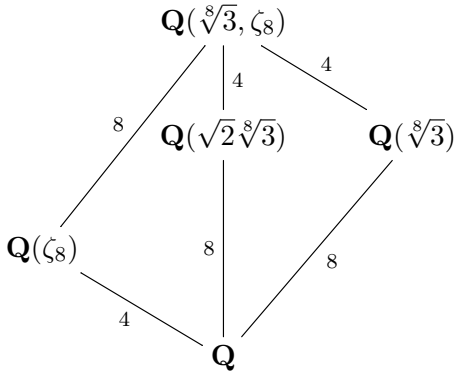
How do we prove $\sqrt{2} \notin \mathbf{Q}(\sqrt[8]{3})$? One way is to show the only quadratic subfield of $\mathbf{Q}(\sqrt[8]{3})$ is $\mathbf{Q}(\sqrt{3})$ and then recall that $\mathbf{Q}(\sqrt{2}) \neq \mathbf{Q}(\sqrt{3})$. That is left to you. What we will do instead is look at quartic subfields of $\mathbf{Q}(\sqrt[8]{3})$. An obvious one is $\mathbf{Q}(\sqrt[4]{3})$. If $\sqrt{2} \in \mathbf{Q}(\sqrt[8]{3})$ then $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\sqrt[8]{3})$, so $\mathbf{Q}(\sqrt[8]{3})$ would have *two* quartic subfields: $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbf{Q}(\sqrt[4]{3})$. (These quartic fields are definitely not equal, since the first one is Galois over $\mathbf{Q}$ and the second one is not.) We're going to prove $\mathbf{Q}(\sqrt[4]{3})$ is the only quartic subfield of $\mathbf{Q}(\sqrt[8]{3})$, giving a contradiction.[1]

[1]Methods from algebraic number theory provide another way to show that $\sqrt{2} \notin \mathbf{Q}(\sqrt[8]{3})$.

Let $\mathbf{Q} \subset F \subset \mathbf{Q}(\sqrt[8]{3})$ with $[F : \mathbf{Q}] = 4$, so $[\mathbf{Q}(\sqrt[8]{3}) : F] = 2$. Then $\sqrt[8]{3}$ has two F-conjugates: itself and some other number. That other number is another 8th root of 3, so it is some $\zeta_8^c \sqrt[8]{3}$, where $1 \leq c \leq 7$. Then the minimal polynomial of $\sqrt[8]{3}$ over F is

$$(X - \sqrt[8]{3})(X - \zeta_8^c \sqrt[8]{3}) = X^2 - (1 + \zeta_8^c)\sqrt[8]{3}X + \zeta_8^c \sqrt[4]{3}.$$

The coefficients on the right must be in F, and $F \subset \mathbf{Q}(\sqrt[8]{3}) \subset \mathbf{R}$, so $\zeta_8^c \sqrt[4]{3}$ is real. The only real powers of ζ_8 are ± 1. Since $1 \leq c \leq 7$, we must have $\zeta_8^c = -1$. Therefore the constant term $\zeta_8^c \sqrt[4]{3} = -\sqrt[4]{3}$ is in F. Since $[F : \mathbf{Q}] = 4$ and $\sqrt[4]{3}$ has degree 4 over $\mathbf{Q}$, $F = \mathbf{Q}(\sqrt[4]{3})$. This completes the proof that $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}] = 32$ and we fill in all the degrees in the field diagram below.



Now we compute $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$, which has size 32 from our field degree calculation. Each σ in this Galois group is determined by its values on $\sqrt[8]{3}$ and ζ_8. Under the Galois group, $\sqrt[8]{3}$ goes to an 8th root of 3 and ζ_8 goes to a primitive 8th root of unity, so $\sigma(\zeta_8) = \zeta_8^a$ and $\sigma(\sqrt[8]{3}) = \zeta_8^b \sqrt[8]{3}$, where $a \in (\mathbf{Z}/8\mathbf{Z})^\times$ and $b \in \mathbf{Z}/8\mathbf{Z}$. Thus each element of the Galois group gives us two exponents mod 8, a and b, with a mod 8 being invertible. There are 4 choices for a and 8 choices for b, which allows for at most $4 \cdot 8 = 32$ possible σ's. Since the number of σ's is 32, every pair of choices for a and b really works: for each $a \in (\mathbf{Z}/8\mathbf{Z})^\times$ and $b \in \mathbf{Z}/8\mathbf{Z}$, there is a unique $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$ such that $\sigma(\zeta_8) = \zeta_8^a$ and $\sigma(\sqrt[8]{3}) = \zeta_8^b \sqrt[8]{3}$. Write this σ as $\sigma_{a,b}$, so

$$\sigma_{a,b}(\zeta_8) = \zeta_8^a, \quad \sigma_{a,b}(\sqrt[8]{3}) = \zeta_8^b \sqrt[8]{3}. \tag{2.6}$$

To understand the Galois group in terms of the parameters a and b, check that

$$\sigma_{a,b} \circ \sigma_{a',b'} = \sigma_{aa',b+ab'}.$$

The way the parameters combine on the right is exactly the way the matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

multiply, so there is an isomorphism from

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/8\mathbf{Z})^\times, \quad b \in \mathbf{Z}/8\mathbf{Z} \right\} \tag{2.7}$$

to $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$ given by $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto \sigma_{a,b}$. The mod 8 matrix group (2.7) will be our concrete model for $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$.

Now that we computed the Galois group of a Galois extension of $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt[8]{3})$ and $\mathbf{Q}(\sqrt{2}\sqrt[8]{3})$, we are ready to show $\mathbf{Q}(\sqrt[8]{3}) \not\cong \mathbf{Q}(\sqrt{2}\sqrt[8]{3})$ by showing their corresponding subgroups in $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$ are not conjugate.

In the matrix model (2.7) of $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$, the subgroup fixing $\mathbf{Q}(\sqrt[8]{3})$ is

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/8\mathbf{Z})^\times \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix} \right\} \tag{2.8}$$

because every $\sigma_{a,0}$ fixes $\sqrt[8]{3}$ (set $b = 0$ in (2.6)), there are 4 such automorphisms, and $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}(\sqrt[8]{3})] = 32/8 = 4$. To find the subgroup fixing $\mathbf{Q}(\sqrt{2}\sqrt[8]{3})$, we need to find the (a, b)-solutions to $\sigma_{a,b}(\sqrt{2}\sqrt[8]{3}) = \sqrt{2}\sqrt[8]{3}$. In terms of $\sqrt[8]{3}$ and ζ_8,

$$\sqrt{2}\sqrt[8]{3} = (\zeta_8 + \zeta_8^{-1})\sqrt[8]{3},$$

so

$$\sigma_{a,b}(\sqrt{2}\sqrt[8]{3}) = (\zeta_8^a + \zeta_8^{-a})\zeta_8^b\sqrt[8]{3}.$$

Therefore

$$\sigma_{a,b}(\sqrt{2}\sqrt[8]{3}) = \sqrt{2}\sqrt[8]{3} \iff (\zeta_8^a + \zeta_8^{-a})\zeta_8^b\sqrt[8]{3} = (\zeta_8 + \zeta_8^{-1})\sqrt[8]{3} \iff (\zeta_8^a + \zeta_8^{-a})\zeta_8^b = \zeta_8 + \zeta_8^{-1}.$$

The number of (a, b)-solutions is $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}(\sqrt{2}\sqrt[8]{3})] = 32/8 = 4$, and by inspection 4 solutions are $(a, b) = (\pm 1, 0)$ and $(\pm 3, 4)$, so the matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ fixing $\sqrt{2}\sqrt[8]{3}$ are

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pm 3 & 4 \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix} \right\}. \tag{2.9}$$

It remains to show that the mod 8 matrix groups (2.8) and (2.9) are not conjugate inside of (2.7). These subgroups are abstractly isomorphic to each other since they are are each isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, so we can't rule out them being conjugate from being non-isomorphic as abstract groups. To rule out conjugacy, we really must look at conjugation on these subgroups.

Suppose $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$ is a matrix in (2.7) that conjugates (2.8) to (2.9). For any $a \in (\mathbf{Z}/8\mathbf{Z})^\times$,

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & (1-a)y \\ 0 & 1 \end{pmatrix}. \tag{2.10}$$

(Since x cancels out on the right side, we could take $x = 1$ from now on.) In particular,

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & -2y \\ 0 & 1 \end{pmatrix}.$$

Therefore the only conjugate of $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in (2.9) is $\left(\begin{smallmatrix} 3 & 4 \\ 0 & 1 \end{smallmatrix}\right)$, so $-2y \equiv 4 \bmod 8$, so $y \equiv 2 \bmod 4$. Since

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & -4y \\ 0 & 1 \end{pmatrix},$$

the only conjugate of $\left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in (2.9) is $\left(\begin{smallmatrix} 5 & 4 \\ 0 & 1 \end{smallmatrix}\right)$, so $-4y \equiv 4 \bmod 8$, which implies $y \equiv 1 \bmod 2$. We have incompatible congruences on y, so (2.8) and (2.9) are nonconjugate subgroups in (2.7). (Each element of (2.8) can be conjugated within the group (2.7) to an element of (2.9), but there is not *one* element of the group (2.7) that conjugates all of (2.8) to (2.9).)

3. Generating a Composite Field with a Sum

From the proof of the primitive element theorem, if α and β are separable over K then $K(\alpha,\beta) = K(\alpha + c\beta)$ for all but finitely many $c \in K$. It is natural to ask if there is a condition that assures us we can use $c = 1$, so $\alpha + \beta$ generates $K(\alpha,\beta)$.

Theorem 3.1. *If K has characteristic 0 and $K(\alpha,\beta)/K$ is a finite extension such that $K(\alpha)/K$ and $K(\beta)/K$ are both Galois and $K(\alpha) \cap K(\beta) = K$, then $K(\alpha,\beta) = K(\alpha+\beta)$.*

Proof. Our argument is taken from [8, p. 65]. Let $H = \mathrm{Gal}(K(\alpha,\beta)/K(\alpha+\beta))$. We will show this group is trivial.

Pick $\sigma \in H$, so $\sigma(\alpha+\beta) = \alpha+\beta$. Therefore

$$\sigma(\alpha) - \alpha = \beta - \sigma(\beta).$$

Since $K(\alpha)$ and $K(\beta)$ are Galois over K, $\sigma(\alpha) \in K(\alpha)$ and $\sigma(\beta) \in K(\beta)$, so $\sigma(\alpha)-\alpha \in K(\alpha)$ and $\beta - \sigma(\beta) \in K(\beta)$. This common difference is therefore in $K(\alpha) \cap K(\beta) = K$. Write $\sigma(\alpha) - \alpha = t$, so

$$\sigma(\alpha) = \alpha + t, \quad \sigma(\beta) = \beta - t.$$

Applying σ repeatedly, $\sigma^j(\alpha) = \alpha + jt$ for all integers j. Choose $j \geq 1$ such that σ^j is the identity (for instance, let $j = [K(\alpha,\beta) : K]$). Then $\alpha = \alpha + jt$, so $jt = 0$. Since we are in characteristic 0 and j is a positive integer, we must have $t = 0$, so $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$. Therefore σ is the identity on $K(\alpha,\beta)$. □

Example 3.2. The fields $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$ are both Galois over $\mathbf{Q}$ and their intersection is $\mathbf{Q}$, so Theorem 3.1 tells us $\mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. This can also be seen more simply by checking $\sqrt{2}+\sqrt{3}$ is not fixed by any element of $\mathrm{Gal}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$ other than the identity.

If we drop the Galois hypothesis in Theorem 3.1 completely, then the proof of Theorem 3.1 falls apart and the theorem need not be true anymore.

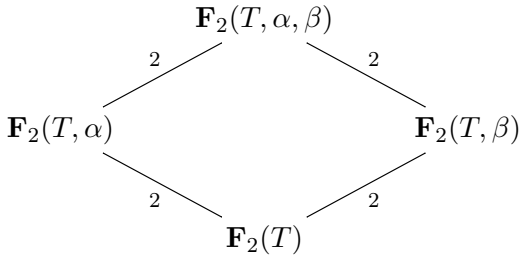
Example 3.3. Both $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\omega\sqrt[3]{2})$ are not Galois over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt[3]{2}) \cap \mathbf{Q}(\omega\sqrt[3]{2}) = \mathbf{Q}$. The field $\mathbf{Q}(\sqrt[3]{2},\omega\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2},\omega)$ has degree 6 over $\mathbf{Q}$, but $\sqrt[3]{2}+\omega\sqrt[3]{2} = -\omega^2\sqrt[3]{2}$ (because $1+\omega+\omega^2 = 0$), which generates the field $\mathbf{Q}(\omega^2\sqrt[3]{2})$ of degree 3 over $\mathbf{Q}$. So $\mathbf{Q}(\sqrt[3]{2},\omega\sqrt[3]{2}) \neq \mathbf{Q}(\sqrt[3]{2}+\omega\sqrt[3]{2})$.

Example 3.4. Let r and r' be two roots of $X^4+8X+12$. The extensions $\mathbf{Q}(r)$ and $\mathbf{Q}(r')$ have degree 4 over $\mathbf{Q}$, $\mathbf{Q}(r) \cap \mathbf{Q}(r') = \mathbf{Q}$, and $[\mathbf{Q}(r,r') : \mathbf{Q}] = 12$. The sum $r+r'$ has degree 6 over $\mathbf{Q}$ (it is a root of $X^6 - 48X^2 - 64$), so $\mathbf{Q}(r,r') \neq \mathbf{Q}(r+r')$.

In the proof of Theorem 3.1 we used the condition that K has characteristic 0 in one place: to know that if $jt = 0$ in K where j a positive integer then $t = 0$. The choice of j comes from $\sigma^j = \mathrm{id}$, so j can be chosen as $[K(\alpha,\beta) : K]$. Therefore Theorem 3.1 is valid in characteristic p as long as $[K(\alpha,\beta) : K] \not\equiv 0 \bmod p$. What if $[K(\alpha,\beta) : K]$ is divisible by p? First of all, there are no problems when K is a finite field. That is, Theorem 3.1 is true when K is any finite field. See Jyrki Lahtonen's answer at [10]. But if $K = \mathbf{F}_p(T)$, the simplest infinite field of characteristic p, counterexamples to Theorem 3.1 occur.

Example 3.5. Consider $K = \mathbf{F}_2(T)$, $\alpha^2+\alpha+1 = 0$, and $\beta^2+\beta+T = 0$. The polynomials X^2+X+1 and X^2+X+T are separable and irreducible over K (check these quadratics have no root in $\mathbf{F}_2(T)$), so α and β have degree 2 over K and generate Galois extensions of K (their K-conjugates are $\alpha+1$ and $\beta+1$). The field $K(\alpha) = \mathbf{F}_2(T,\alpha) = \mathbf{F}_2(\alpha)(T)$

is a field of rational functions over $\mathbf{F}_2(\alpha)$ and $X^2 + X + T$ has no root in it (why?), so $[K(\alpha, \beta) : K(\alpha)] = 2$. Therefore $[K(\alpha, \beta) : K] = 4$ and $K(\alpha) \cap K(\beta) = K$. We have the following field diagram.



Unlike the conclusion of Theorem 3.1, $K(\alpha, \beta) \neq K(\alpha + \beta)$ because $\alpha + \beta$ has degree 2 over K: $(\alpha + \beta)^2 + (\alpha + \beta) = \alpha^2 + \beta^2 + \alpha + \beta = T + 1$. An example of a primitive element of $K(\alpha, \beta)/K$ is $\alpha + T\beta$: its Galois orbit over $\mathbf{F}_2(T)$ has order 4. A similar example occurs over $\mathbf{F}_p(T)$ for any prime p, where $\alpha^p - \alpha + 1 = 0$ and $\beta^p - \beta + T = 0$.

If K has characteristic 0 and just one of $K(\alpha)$ or $K(\beta)$ in Theorem 3.1 is Galois, the proof of the theorem no longer works but the theorem is still true! Isaacs [4] found that Theorem 3.1 is true when K has characteristic 0 with a weaker condition in place of the Galois hypotheses.

Theorem 3.6. *If K has characteristic 0 and $K(\alpha, \beta)/K$ is a finite extension such that $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$ then $K(\alpha, \beta) = K(\alpha + \beta)$.*

Proof. See [4] or [5, pp. 363–368]. The hypothesis on field degrees in those references is that the degrees $[K(\alpha) : K]$ and $[K(\beta) : K]$ are relatively prime, but the only use of this in the proof is to guarantee that $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$ and this degree formula can be true even without the two factors being relatively prime. □

The degree hypothesis in Theorem 3.6 is equivalent to $K(\alpha) \cap K(\beta) = K$ when one of $K(\alpha)$ or $K(\beta)$ is Galois over K (Theorem 2.6), so Theorem 3.1 is true when only one of $K(\alpha)$ or $K(\beta)$ is Galois over K.

Example 3.7. Theorem 3.6 implies $\mathbf{Q}(\sqrt[3]{2}, \omega) = \mathbf{Q}(\sqrt[3]{2} + \omega)$ and $\mathbf{Q}(\sqrt[4]{2}, i) = \mathbf{Q}(\sqrt[4]{2} + i)$.

Example 3.8. We know $\mathbf{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) \neq \mathbf{Q}(\sqrt[3]{2} + \omega\sqrt[3]{2})$ and this example does not fit Theorem 3.6 since $[\mathbf{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) : \mathbf{Q}] = 6$ while $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}][\mathbf{Q}(\omega\sqrt[3]{2}) : \mathbf{Q}] = 9$.

Example 3.9. Letting r and r' be two roots of $X^4 + 8X + 12$, we can't decide if $\mathbf{Q}(r, r')$ equals $\mathbf{Q}(r + r')$ from Theorem 3.6 since $[\mathbf{Q}(r, r') : \mathbf{Q}] = 12$ and $[\mathbf{Q}(r) : \mathbf{Q}][\mathbf{Q}(r') : \mathbf{Q}] = 16$. The two fields are not the same since $\mathbf{Q}(r + r')$ has degree 6 over $\mathbf{Q}$.

Example 3.10. Does $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2} + \zeta_8)$? Since $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2}, i)$ (see Example 2.14) we have $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 8$, and also $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}][\mathbf{Q}(\zeta_8) : \mathbf{Q}] = 16$, so we can't answer the question with Theorem 3.6. The Galois orbit of $\sqrt[4]{2} + \zeta_8$ over $\mathbf{Q}$ has size 8, so in fact $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2} + \zeta_8)$. (The minimal polynomial of $\sqrt[4]{2} + \zeta_8$ over $\mathbf{Q}$ is $X^8 - 8X^5 - 2X^4 + 16X^3 + 32X^2 + 24X + 9$.) Thus the degree hypothesis of Theorem 3.6 is sufficient to imply $K(\alpha, \beta) = K(\alpha + \beta)$ in characteristic 0, but it is not necessary.

In [4] and [5], a version of Theorem 3.6 is proved in characteristic p under extra technical hypotheses. That some extra hypothesis is needed can be seen from Example 3.5; it has the degree hypothesis of Theorem 3.6 but not the conclusion.

4. The inverse Galois problem

The *inverse Galois problem* asks which finite groups arise as Galois groups of a given field. For instance, the only Galois groups over $\mathbf{R}$ are the trivial group and a group of order 2. The most important case of the inverse Galois problem is base field $\mathbf{Q}$: it is conjectured that every finite group is a Galois group over $\mathbf{Q}$, but this is still not solved.

It is important to remember that the inverse Galois problem is about finite *Galois* extensions of fields. Every finite extension of fields E/F has an automorphism group $\mathrm{Aut}(E/F)$, but this might be smaller in size than $[E:F]$ in which case E/F is not a Galois extension. For instance, $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ have degree 3 and 4, while $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$ is trivial and $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ has order 2. In 1980, M. Fried [1] proved that every finite group G is isomorphic to $\mathrm{Aut}(K/\mathbf{Q})$ for some finite extension $K/\mathbf{Q}$ – in fact, for infinitely many $K/\mathbf{Q}$ – but this doesn't solve the inverse Galois problem over $\mathbf{Q}$ since the fields K need not be Galois over $\mathbf{Q}$. A simpler proof of this result, avoiding an appeal to the Hilbert irreducibility theorem, was given later by W-D. Geyer [2].

The inverse Galois problem is solved over $\mathbf{C}(T)$: each finite group is a Galois group over $\mathbf{C}(T)$, and this is proved by methods of complex analysis (Riemann surfaces). If the base field is arbitrary, then every finite group is the Galois group of some field extension. We will explain this using Cayley's theorem to embed every finite group in a symmetric group.

Theorem 4.1. *Every finite group is the Galois group of some finite Galois extension in any characteristic.*

Proof. Let F be a field. By the symmetric function theorem,

$$F(T_1,\ldots,T_n)^{S_n} = F(s_1,\ldots,s_n),$$

where the s_i's are the elementary symmetric functions of the T_i's. Therefore the field $F(T_1,\ldots,T_n)$ is Galois over $F(s_1,\ldots,s_n)$ with Galois group S_n. Any finite group G embeds into some symmetric group S_n, and thus can be interpreted as a Galois group. □

Theorem 4.1 leaves a *lot* to be desired: to realize G as a Galois group, the proof tells us to embed $G \hookrightarrow S_n$ for some n and then G is the Galois group of the extension E/E^G where $E = F(T_1,\ldots,T_n)$ and G acts on E by permuting the variables using the embedding of G in S_n. The base field $E^G = F(T_1,\ldots,T_n)^G$ of this Galois extension is rather mysterious!

Schur, in the 19th century, used number-theoretic techniques to realize every S_n and A_n as Galois groups over $\mathbf{Q}$ using splitting fields of truncated power series (*e.g.*, the splitting field over $\mathbf{Q}$ of the truncated exponential series $\sum_{k=0}^{n} X^k/k!$, has Galois group S_n unless $4 \mid n$, when the Galois group is A_n). Later Hilbert introduced geometric methods into the subject when he showed that if a finite group could be realized as a Galois group over $\mathbf{Q}(T)$ then it could be realized as a Galois group over $\mathbf{Q}$ (in infinitely many ways) by suitable specializations. The buzzword here is "Hilbert's irreducibility theorem" [3]. For instance, $X^n - X - T$ is irreducible over $\mathbf{Q}(T)$ and it turns out that its Galois group over $\mathbf{Q}(T)$ is S_n, so Hilbert's work implies that for many rational numbers t the polynomial $X^n - X - t$ is irreducible over $\mathbf{Q}$ and the Galois group is S_n. With more work, the particular choice $t = 1$ works: $X^n - X - 1$ is irreducible over $\mathbf{Q}$ and its Galois group is S_n [6].

Why does Schur's realization of every S_n as a Galois group over $\mathbf{Q}$ not settle the inverse Galois problem over $\mathbf{Q}$, even though every finite group is a subgroup of some symmetric group? The Galois correspondence reverses inclusions, so subgroups of $\mathrm{Gal}(L/K)$ have the form $\mathrm{Gal}(L/F)$ (same top field, changing base field). It is quotients of $\mathrm{Gal}(L/K)$ that have

the form $\mathrm{Gal}(F/K)$. Alas, the symmetric groups have very few quotient groups: when $n \geq 5$, the only normal subgroups of S_n are $\{(1)\}$, A_n, and S_n, so the only quotient groups of S_n are trivial, of size 2, or S_n itself.

By number-theoretic methods, Shafarevich proved in the 1950s that any finite solvable group is a Galois group over $\mathbf{Q}$. (There was an error concerning the prime 2, which was later repaired.) Most recent work on the inverse Galois problem uses a geometric approach inspired by Hilbert's ideas. As we said above, Hilbert showed that the inverse Galois problem over $\mathbf{Q}$ would be settled (by "specialization") if we can settle the inverse Galois problem over $\mathbf{Q}(T)$. See [9] (esp. Chapter 1) for a basic introduction to these ideas and [7] for a general survey.

As an application of Theorem 2.6, the inverse Galois problem for $\mathbf{Q}$ lifts to finite extensions.

Theorem 4.2. *If every finite group can be realized as a Galois group over $\mathbf{Q}$ then every finite group can be realized as a Galois group over any finite extension of $\mathbf{Q}$.*

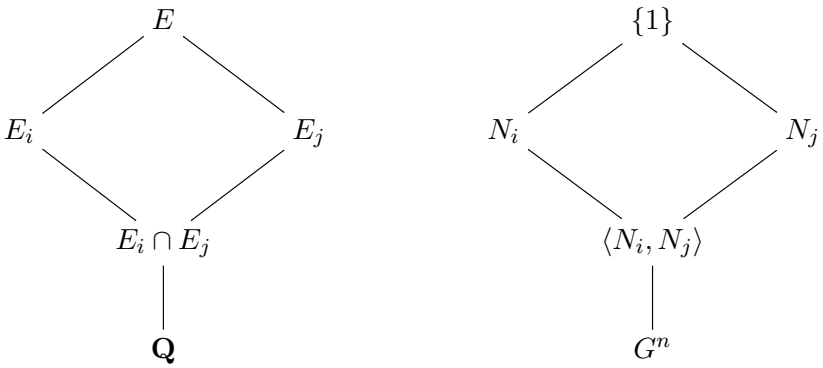
Proof. Fix a finite group G and finite extension $F/\mathbf{Q}$. Following Example 2.8, if we can realize G as a Galois group of an extension $L/\mathbf{Q}$ where $L \cap F = \mathbf{Q}$, then LF/F is Galois and $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F) = \mathrm{Gal}(L/\mathbf{Q}) \cong G$. Thus G is realized over F. So the problem is to find a finite Galois extension $L/\mathbf{Q}$ such that $G \cong \mathrm{Gal}(L/\mathbf{Q})$ and $L \cap F = \mathbf{Q}$.

There are finitely many fields between $\mathbf{Q}$ and F (including $\mathbf{Q}$ and F), say n such fields. By hypothesis all finite groups are Galois groups over $\mathbf{Q}$, so in particular the n-fold product group G^n is a Galois group over $\mathbf{Q}$. Let $\mathrm{Gal}(E/\mathbf{Q}) \cong G^n$. Inside of G^n are the normal subgroups

$$N_i = G \times G \times \cdots \times \{1\} \times \cdots \times G$$

for $1 \leq i \leq n$, where the ith coordinate is trivial and there is no restriction in other coordinates. So $N_i \cong G^{n-1}$ and $G^n/N_i \cong G$. Let E_i be the subfield of E corresponding to N_i, so $E_i/\mathbf{Q}$ is Galois with $\mathrm{Gal}(E_i/\mathbf{Q}) \cong G^n/N_i \cong G$. Each of the fields $E_1, \ldots, E_n$ realizes G as a Galois group over $\mathbf{Q}$. We are going to prove by counting that at least one of the fields E_i intersects F in $\mathbf{Q}$. Then the composite FE_i realizes G as a Galois group over F.

For $i \neq j$, $E_i \cap E_j = \mathbf{Q}$. Indeed (see the diagram below), $E_i \cap E_j$ is the largest subfield of E that lies in E_i and E_j, so by the Galois correspondence $\mathrm{Gal}(E/E_i \cap E_j)$ is the smallest subgroup of $\mathrm{Gal}(E/\mathbf{Q})$ containing $\mathrm{Gal}(E/E_i) = N_i$ and $\mathrm{Gal}(E/E_j) = N_j$. That means $\mathrm{Gal}(E/E_i \cap E_j) = \langle N_i, N_j \rangle$. From the definition of N_i and N_j, the subgroup they generate in G^n is G^n. Since $\langle N_i, N_j \rangle = G^n$, $E_i \cap E_j = \mathbf{Q}$.



Now associate to each E_i the subfield $E_i \cap F$ of F. There are n fields E_i and n subfields of F. If the correspondence from the subfields E_i to the intersections $E_i \cap F$ is a bijection

then $E_i \cap F = \mathbf{Q}$ for some i and we're done. If the correspondence is not injective then we have a repeated intersection $E_i \cap F = E_j \cap F$ for some $i \neq j$. But any element in both intersections is in $E_i \cap E_j = \mathbf{Q}$, which means $E_i \cap F = E_j \cap F = \mathbf{Q}$ and again we're done. □

The only special feature about a finite extension of the rational numbers that was used in the proof is that there are finitely many fields between it and $\mathbf{Q}$. So if every finite group arises as a Galois group over some field K and F/K is a finite extension with finitely many intermediate fields (*e.g.*, F/K is separable) then the proof of Theorem 4.2 shows every finite group arises as a Galois group over F.

References

[1] M. Fried, *A note on automorphism groups of algebraic number fields*, Proc. Amer. Math. Soc. **80** (1980), 386–388.

[2] W-D. Geyer, *Jede endliche Gruppe ist Automorphismengruppe einer endlichen Erweiterung* $K/\mathbf{Q}$, Arch. Math. (Basel), **41** (1983), 139–142.

[3] C. Hadlock, "Field Theory and its Classical Problems," Math. Assoc. America, Washington, D.C., 1978.

[4] I. M. Isaacs, *Degrees of sums in a separable field extension*, Proc. Amer. Math. Soc. **25** (1970), 638–641.

[5] G. Karpilovsky, "Topics in Field Theory," North-Holland, Amsterdam, 1989.

[6] H. Osada, *The Galois groups of the polynomials* $X^n + aX^l + b$, J. Number Theory **25** (1987), 230–238.

[7] J-P. Serre, "Topics in Galois theory," Jones and Bartlett, Boston, MA, 1992.

[8] S. Weintraub, "Galois Theory," Springer-Verlag, New York, 2005.

[9] H. Völklein, "Groups as Galois Groups – an Introduction," Cambridge Univ. Press, Cambridge, 1996.

[10] E. Solomon, Finite Field Extensions and the Sum of the Elements in Proper Subextensions (Follow-Up Question), https://math.stackexchange.com/q/144683.