GALOIS THEORY AT WORK: CONCRETE EXAMPLES

KEITH CONRAD

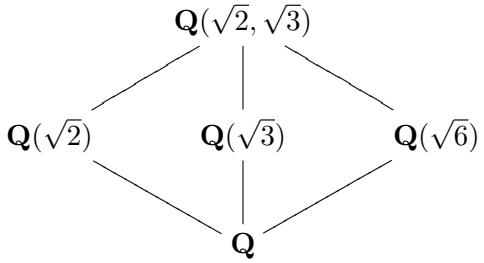
1. Examples

Example 1.1. The field extension $\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}$ is Galois of degree 4, so its Galois group has order 4. The elements of the Galois group are determined by their values on $\sqrt{2}$ and $\sqrt{3}$. The $\mathbf{Q}$-conjugates of $\sqrt{2}$ and $\sqrt{3}$ are $\pm\sqrt{2}$ and $\pm\sqrt{3}$, so we get at most four possible automorphisms in the Galois group. See Table 1. Since the Galois group has order 4, these 4 possible assignments of values to $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$ all really exist.

$\sigma(\sqrt{2})$	$\sigma(\sqrt{3})$
$\sqrt{2}$	$\sqrt{3}$
$\sqrt{2}$	$-\sqrt{3}$
$-\sqrt{2}$	$\sqrt{3}$
$-\sqrt{2}$	$-\sqrt{3}$

Table 1

Each nonidentity automorphism in Table 1 has order 2. Since $\mathrm{Gal}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$ contains 3 elements of order 2, $\mathbf{Q}(\sqrt{2},\sqrt{3})$ has 3 subfields K_i such that $[\mathbf{Q}(\sqrt{2},\sqrt{3}) : K_i] = 2$, or equivalently $[K_i : \mathbf{Q}] = 4/2 = 2$. Two such fields are $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$. A third is $\mathbf{Q}(\sqrt{6})$ and that completes the list. Here is a diagram of all the subfields.



In Table 1, the subgroup fixing $\mathbf{Q}(\sqrt{2})$ is the first and second row, the subgroup fixing $\mathbf{Q}(\sqrt{3})$ is the first and third row, and the subgroup fixing $\mathbf{Q}(\sqrt{6})$ is the first and fourth row (since $(-\sqrt{2})(-\sqrt{3}) = \sqrt{2}\sqrt{3}$).

The effect of $\mathrm{Gal}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$ on $\sqrt{2}+\sqrt{3}$ is given in Table 2. The 4 values are all different, since $\sqrt{2}$ and $\sqrt{3}$ are linearly independent over $\mathbf{Q}$. Therefore $\mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbf{Q}$ must be

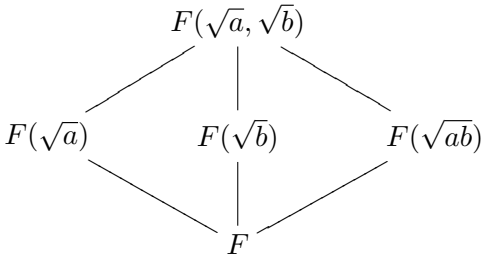
$$(X-(\sqrt{2}+\sqrt{3}))(X-(-\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X-(-\sqrt{2}-\sqrt{3})) = X^4-10X^2+1.$$

In particular, X^4-10X^2+1 is irreducible in $\mathbf{Q}[X]$ since it's a minimal polynomial over $\mathbf{Q}$.

$\sigma(\sqrt{2})$	$\sigma(\sqrt{3})$	$\sigma(\sqrt{2}+\sqrt{3})$
$\sqrt{2}$	$\sqrt{3}$	$\sqrt{2}+\sqrt{3}$
$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{2}-\sqrt{3}$
$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{2}+\sqrt{3}$
$-\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{2}-\sqrt{3}$

TABLE 2

By similar reasoning if a field F does not have characteristic 2 and a and b are nonsquares in F such that ab is not a square either, then $[F(\sqrt{a},\sqrt{b}) : F] = 4$ and all the fields between F and $F(\sqrt{a},\sqrt{b})$ are as in the following diagram.



Furthermore, $F(\sqrt{a},\sqrt{b}) = F(\sqrt{a}+\sqrt{b})$. The argument is identical to the special case above.

Example 1.2. The extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ is not Galois, but $\mathbf{Q}(\sqrt[4]{2})$ lies in $\mathbf{Q}(\sqrt[4]{2},i)$, which is Galois over $\mathbf{Q}$. We will use Galois theory for $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ to find the intermediate fields in $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$.

The Galois group of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ equals $\langle r,s\rangle$, where

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

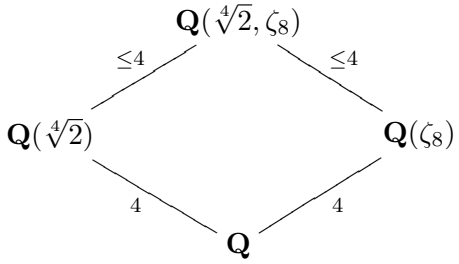
(Viewing elements of $\mathbf{Q}(\sqrt[4]{2},i)$ as complex numbers, s acts on them like complex conjugation.) The group $\langle r,s\rangle$ is isomorphic to D_4, where r corresponds to a 90 degree rotation of the square and s corresponds to a reflection across a diagonal. What is the subgroup H of $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ corresponding to $\mathbf{Q}(\sqrt[4]{2})$?

$$\begin{array}{cc} \mathbf{Q}(\sqrt[4]{2},i) & \{1\} \\ \Big|2 & \Big|2 \\ \mathbf{Q}(\sqrt[4]{2}) & H \\ \Big|4 & \Big|4 \\ \mathbf{Q} & D_4 \end{array} \tag{1.1}$$

Since s is a nontrivial element of the Galois group that fixes $\mathbf{Q}(\sqrt[4]{2})$, $s \in H$. The size of H is $[\mathbf{Q}(\sqrt[4]{2},i) : \mathbf{Q}(\sqrt[4]{2})] = 2$, so $H = \{1,s\} = \langle s\rangle$. By the Galois correspondence for $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$, fields strictly between $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}$ correspond to subgroups of the Galois group strictly between $\langle s\rangle$ and $\langle r,s\rangle$. From the known subgroup structure of D_4, the only subgroup lying strictly between $\langle s\rangle$ and $\langle r,s\rangle$ is $\langle r^2,s\rangle$. Therefore only one field lies strictly between $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}$. Since $\mathbf{Q}(\sqrt{2})$ is such a field it is the only one.

Remark 1.3. While Galois theory provides the most systematic method to find intermediate fields, it may be possible to argue in other ways. For example, suppose $\mathbf{Q} \subset F \subset \mathbf{Q}(\sqrt[4]{2})$ with $[F : \mathbf{Q}] = 2$. Then $\sqrt[4]{2}$ has degree 2 over F. Since $\sqrt[4]{2}$ is a root of $X^4 - 2$, its minimal polynomial over F has to be a quadratic factor of $X^4 - 2$. There are three monic quadratic factors with $\sqrt[4]{2}$ as a root, but only one of them, $X^2 - \sqrt{2}$, has coefficients in $\mathbf{Q}(\sqrt[4]{2})$ (let alone in $\mathbf{R}$). Therefore $X^2 - \sqrt{2}$ must be the minimal polynomial of $\sqrt[4]{2}$ over F, so $\sqrt{2} \in F$. Since $[F : \mathbf{Q}] = 2$, $F = \mathbf{Q}(\sqrt{2})$ by counting degrees.

Example 1.4. Let's explore $\mathbf{Q}(\sqrt[4]{2}, \zeta_8)$, where $\zeta_8 = e^{2\pi i/8}$ is a root of unity of order 8, whose minimal polynomial over $\mathbf{Q}$ is $X^4 + 1$. Both $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(\zeta_8)$ have degree 4 over $\mathbf{Q}$. Since $\zeta_8^2 = i$, $\mathbf{Q}(\sqrt[4]{2}, \zeta_8)$ is a splitting field over $\mathbf{Q}$ of $(X^4 - 2)(X^4 + 1)$ and therefore is Galois over $\mathbf{Q}$. What is its Galois group? We have the following field diagram.



Thus $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}]$ is at most 16. We will see the degree is *not* 16: there are some hidden algebraic relations between $\sqrt[4]{2}$ and ζ_8.

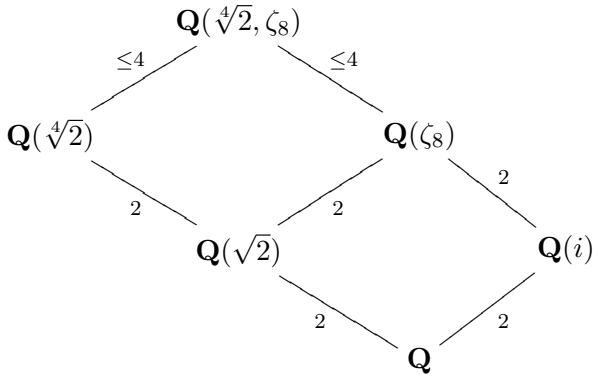
Any $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, \zeta_8)/\mathbf{Q})$ is determined by its values

$$\sigma(\zeta_8) = \zeta_8^a \quad (a \in (\mathbf{Z}/8\mathbf{Z})^\times) \quad \text{and} \quad \sigma(\sqrt[4]{2}) = i^b \sqrt[4]{2} \quad (b \in \mathbf{Z}/4\mathbf{Z}). \tag{1.2}$$

There are 4 choices each for a and b. Taking independent choices of a and b, there are at most 16 automorphisms in the Galois group. But the choices of a and b can *not* be made independently because ζ_8 and $\sqrt[4]{2}$ are linked to each other:

$$\zeta_8 + \zeta_8^{-1} = e^{2\pi i/8} + e^{-2\pi i/8} = 2\cos\left(\frac{\pi}{4}\right) = \sqrt{2} = \sqrt[4]{2}^2. \tag{1.3}$$

This says $\sqrt{2}$ belongs to both $\mathbf{Q}(\zeta_8)$ and $\mathbf{Q}(\sqrt[4]{2})$. Here is a field diagram that emphasizes the common subfield $\mathbf{Q}(\sqrt{2})$ in $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(\zeta_8)$. This subfield is the source of (1.3).



Rewriting $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ as $\zeta_8^2 - \sqrt{2}\zeta_8 + 1 = 0$, ζ_8 has degree at most 2 over $\mathbf{Q}(\sqrt[4]{2})$. Since ζ_8 is not real, it isn't inside $\mathbf{Q}(\sqrt[4]{2})$, so it has degree 2 over $\mathbf{Q}(\sqrt[4]{2})$. Therefore $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 2 \cdot 4 = 8$ and the degrees marked as "≤ 4" in the diagram both equal 2.

Returning to the Galois group, (1.3) tells us the effect of $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, \zeta_8)/\mathbf{Q})$ on $\sqrt[4]{2}$ partially determines it on ζ_8, and conversely: $(\sigma(\sqrt[4]{2}))^2 = \sigma(\zeta_8) + \sigma(\zeta_8)^{-1}$, which in the notation of (1.2) is the same as

$$(-1)^b = \frac{\zeta_8^a + \zeta_8^{-a}}{\sqrt{2}}. \tag{1.4}$$

This tells us that if $a \equiv 1, 7 \bmod 8$ then $(-1)^b = 1$, so $b \equiv 0, 2 \bmod 4$, while if $a \equiv 3, 5 \bmod 8$ then $(-1)^b = -1$, so $b \equiv 1, 3 \bmod 4$. For example, σ can't both fix $\sqrt[4]{2}$ ($b = 0$) and send ζ_8 to ζ_8^3 ($a = 3$) because (1.4) would not hold.

The simplest way to understand $\mathbf{Q}(\sqrt[4]{2}, \zeta_8)$ is to use a different set of generators. Since $\zeta_8 = e^{2\pi i/8} = e^{\pi i/4} = (1 + i)/\sqrt{2}$,

$$\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2}, i),$$

and from the second representation we know its Galois group over $\mathbf{Q}$ is isomorphic to D_4 with independent choices of where to send $\sqrt[4]{2}$ (to any fourth root of 2) and i (to any square root of -1) rather than $\sqrt[4]{2}$ and ζ_8. A different choice of field generators can make it easier to see what the Galois group looks like. We also see immediately from the second representation that $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 8$.

A Galois extension is said to have a given group-theoretic property (being abelian, non-abelian, cyclic, *etc.*) when its Galois group has that property.

Example 1.5. Any quadratic extension of $\mathbf{Q}$ is an abelian extension since its Galois group has order 2. It is also a cyclic extension.

Example 1.6. The extension $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is called non-abelian since its Galois group is isomorphic to S_3, which is a non-abelian group. The term "non-abelian" has nothing to do with the field operations, which of course are always commutative.

Theorem 1.7. *If L/K is a finite abelian extension then every intermediate field is an abelian extension of K. If L/K is cyclic then every intermediate field is cyclic over K.*

Proof. Every subgroup of an abelian group is a normal subgroup, so every field F between L and K is Galois over K and $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$. The quotient of an abelian group by any subgroup is abelian, so $\mathrm{Gal}(F/K)$ is abelian.

Since the quotient of a cyclic group by any subgroup is cyclic, if L/K is cyclic then F/K is cyclic too. □

2. Applications to Field Theory

We will prove the complex numbers are algebraically closed (the "Fundamental Theorem of Algebra") using Galois theory and a small amount of analysis. We need one property of the real numbers, one property of the complex numbers, and two properties of finite groups:

(1) Every odd degree polynomial in $\mathbf{R}[X]$ has a real root. In particular, no polynomial of odd degree greater than 1 in $\mathbf{R}[X]$ is irreducible.
(2) Every number in $\mathbf{C}$ has square roots in $\mathbf{C}$.
(3) The first Sylow theorem (existence of Sylow subgroups).

(4) A nontrivial finite p-group has a subgroup of index p.

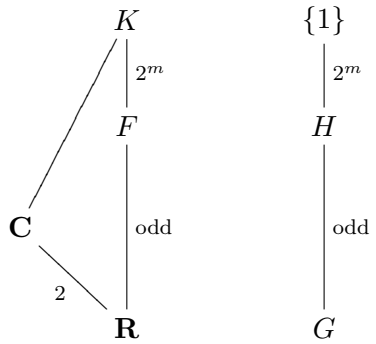
The first property is a consequence of the intermediate value theorem. The second property follows from writing a nonzero complex number as $re^{i\theta}$ and then its square roots are $\pm\sqrt{r}e^{i\theta/2}$. (For example, $i = e^{i\pi/2}$ and a square root of i is $e^{i\pi/4} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$.) It is a nice exercise to find a square root of $a + bi$ in terms of a and b. The third property is proved as part of the Sylow theorems. The fourth property is often proved in the context of showing finite p-groups are solvable; this can be found in most group theory textbooks.

Theorem 2.1. *The complex numbers are algebraically closed.*

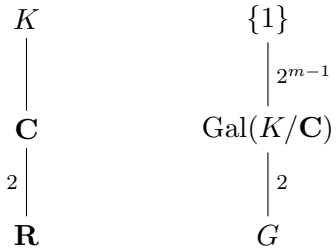
Proof. We need to show any irreducible in $\mathbf{C}[X]$ has degree 1. If $\pi(X) \in \mathbf{C}[X]$ is irreducible and α is a root, then $[\mathbf{C}(\alpha) : \mathbf{C}] = \deg \pi$, so our task is the same as showing the only finite extension of $\mathbf{C}$ is $\mathbf{C}$ itself.

Let $E/\mathbf{C}$ be a finite extension. Since E is a finite extension of $\mathbf{R}$, and we're in characteristic 0, we can enlarge $E/\mathbf{R}$ to a finite Galois extension $K/\mathbf{R}$. Since $\mathbf{R} \subset \mathbf{C} \subset K$, $[K : \mathbf{R}]$ is even.

Let $2^m \geq 2$ be the highest power of 2 dividing the size of $G = \mathrm{Gal}(K/\mathbf{R})$. There is a subgroup H of G with order 2^m (Property 3). Let F be the corresponding fixed field, so $[F : \mathbf{R}]$ is odd.



Every $\alpha \in F$ has degree over $\mathbf{R}$ dividing $[F : \mathbf{R}]$, so $[\mathbf{R}(\alpha) : \mathbf{R}]$ is odd. That means the minimal polynomial of α in $\mathbf{R}[X]$ has odd degree. Irreducible polynomials in $\mathbf{R}[X]$ of odd degree have degree 1 (Property 1), so $[\mathbf{R}(\alpha) : \mathbf{R}] = 1$. Thus $\alpha \in \mathbf{R}$, so $F = \mathbf{R}$. Therefore $G = H$ is a 2-group.



The group $\mathrm{Gal}(K/\mathbf{C})$ has order 2^{m-1}. If $m \geq 2$ then $\mathrm{Gal}(K/\mathbf{C})$ has a subgroup of index 2 (Property 4), whose fixed field has degree 2 over $\mathbf{C}$. Any quadratic extension of $\mathbf{C}$ has the form $\mathbf{C}(\sqrt{d})$ for some nonsquare $d \in \mathbf{C}^\times$. But every nonzero complex number has square roots in $\mathbf{C}$ (Property 2), so $[\mathbf{C}(\sqrt{d}) : \mathbf{C}]$ is 1, not 2. We have a contradiction. Thus $m = 1$, so $K = \mathbf{C}$. Since $\mathbf{C} \subset E \subset K$, we conclude that $E = \mathbf{C}$. □

Theorem 2.2. *If L/K be Galois with degree p^m, where p is a prime, then there is a chain of intermediate fields*

$$K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = K$$

where $[F_i : F_{i-1}] = p$ for $i \geq 1$ and F_i/K is Galois.

Proof. The group $\mathrm{Gal}(L/K)$ is a finite group of order p^m. One of the consequences of finite p-groups being solvable is the existence of a rising chain of subgroups from the trivial subgroup to the whole group where each subgroup has index p in the next one and each subgroup is *normal* in the whole group. Now apply the Galois correspondence. □

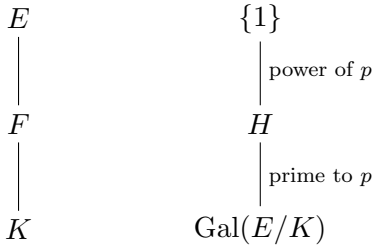
The next application, which is an amusing technicality, is taken from [2, p. 67].

Theorem 2.3. *Let p be a prime number. If K is a field of characteristic 0 such that every proper finite extension of K has degree divisible by p then every finite extension of K has p-power degree.*

Aside from examples resembling $K = \mathbf{R}$ (where $p = 2$ works), fields that fit the conditions of Theorem 2.3 are not easy to describe at an elementary level. But the technique of proof is a pleasant use of elementary group theory.

Proof. Let L/K be a finite extension. We want to show $[L : K]$ is a power of p. Since K has characteristic 0, L/K is separable, so we can embed L in a finite Galois extension E/K. Since $[L : K]|[E : K]$, it suffices to show $[E : K]$ is a power of p, i.e., show finite Galois extensions of K have p-power degree.

By the first Sylow theorem, $\mathrm{Gal}(E/K)$ contains a p-Sylow subgroup, say H. Let $F = E^H$, so $[F : K]$ is the index of H in $\mathrm{Gal}(E/K)$. This index is prime to p by the definition of a Sylow subgroup, so $[F : K]$ is prime to p.



Every proper finite extension of K has degree divisible by p, so $[F : K] = 1$. Thus $F = K$ and $[E : K] = [E : F] = \#H$ is a power of p. □

Remark 2.4. Theorem 2.3 is true when K has positive characteristic, but then one has to consider the possibility that K has inseparable extensions and additional reasoning is needed. See [2, p. 67].

3. Applications to Minimal Polynomials

When L/K is a Galois extension and $\alpha \in L$, the Galois group $\mathrm{Gal}(L/K)$ provides us with a systematic way to describe all the roots of the minimal polynomial of α over K: they are the different elements of the Galois orbit $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$. If we let $\mathrm{Gal}(L/K)$ act on $L[X]$, and not just L, by acting on polynomial coefficients, then we can relate minimal polynomials of the same number over different fields using a Galois group.

Theorem 3.1. *Let L/K be a finite Galois extension and α lie in some extension of L with minimal polynomial $f(X)$ in $L[X]$. The minimal polynomial of α in $K[X]$ is the product of all the different values of $(\sigma f)(X)$ as σ runs over* $\mathrm{Gal}(L/K)$.

When $\alpha \in L$, so $f(X) = X - \alpha$, we recover the construction of the minimal polynomial of α in $K[X]$ as $\prod_{j=1}^{r}(X - \sigma_j(\alpha))$, where $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ are the distinct values of $\sigma(\alpha)$ as σ runs over $\mathrm{Gal}(L/K)$.

Proof. Let $\pi(X)$ denote the minimal polynomial of α over K. Since $\pi(\alpha) = 0$ and $f(X)$ is the minimal polynomial of α over L, $f(X) \mid \pi(X)$ in $L[X]$. For any $\sigma \in \mathrm{Gal}(L/K)$, $f(X) \mid \pi(X) \Rightarrow (\sigma f)(X) \mid \pi(X)$ because $(\sigma\pi)(X) = \pi(X)$.

Note $(\sigma f)(X) = (\sigma_i f)(X)$ for some i. Each $\sigma_i f$ is monic irreducible in $L[X]$ and therefore $\sigma_i f$ and $\sigma_j f$ are relatively prime when $i \neq j$. Thus $\pi(X)$ is divisible by $F(X) := \prod_{i=1}^{r}(\sigma_i f)(X)$. For any $\sigma \in \mathrm{Gal}(L/K)$, the set of polynomials $(\sigma\sigma_i f)(X)$ are the same as all $(\sigma_i f)(X)$ except it may be in a different order, so

$$(\sigma F)(X) = \prod_{i=1}^{r}(\sigma\sigma_i f)(X) = \prod_{i=1}^{r}(\sigma_i f)(X) = F(X),$$

so the coefficients of $F(X)$ are in K. Since $F(X) \mid \pi(X)$ and $F(\alpha) = 0$, the meaning of minimal polynomial implies $F(X) = \pi(X)$. □

Example 3.2. Consider $X^2 - \sqrt{2}$ in $\mathbf{Q}(\sqrt{2})[X]$. It is irreducible since $\sqrt{2}$ is not a square in $\mathbf{Q}(\sqrt{2})$: if $(a + b\sqrt{2})^2 = \sqrt{2}$ with $a, b \in \mathbf{Q}$ then $a^2 + 2b^2 = 0$, so $a = b = 0$, a contradiction. The different values of $\sigma(X^2 - \sqrt{2}) = X^2 - \sigma(\sqrt{2})$ as σ runs over $\mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ are $X^2 - \sqrt{2}$ and $X^2 + \sqrt{2}$, so the minimal polynomial over $\mathbf{Q}$ of the roots of $X^2 - \sqrt{2}$ is

$$(X^2 - \sqrt{2})(X^2 + \sqrt{2}) = X^4 - 2.$$

Since a minimal polynomial over a field is just an irreducible polynomial over that field (with a particular root), we can formulate Theorem 3.1 in terms of irreducible polynomials without mentioning roots: if $f(X)$ is monic irreducible in $L[X]$ then the product of the different $(\sigma f)(X)$, as σ runs over $\mathrm{Gal}(L/K)$, is irreducible in $K[X]$. Consider a potential converse: if $f(X)$ is monic in $L[X]$ and the product of the different polynomials $(\sigma f)(X)$, as σ runs over $\mathrm{Gal}(L/K)$, is irreducible in $K[X]$, then $f(X)$ is irreducible in $L[X]$. This is *false*: use $L/K = \mathbf{Q}(\sqrt{2})/\mathbf{Q}$ and $f(X) = X^2 - 2$. Here $(\sigma f)(X) = X^2 - 2$ for either σ, so the product of different $(\sigma f)(X)$ is $X^2 - 2$, which is irreducible in $K[X]$ but reducible in $L[X]$. Yet there is a kernel of truth in this false converse. We just have to make sure $f(X)$ doesn't live over a proper subfield of L.

Theorem 3.3. *Let L/K be a finite Galois extension. Suppose $f(X)$ is monic in $L[X]$ and its coefficients generate L over K. If the product of the different polynomials $(\sigma f)(X)$, as σ runs over* $\mathrm{Gal}(L/K)$*, is irreducible in $K[X]$, then $f(X)$ is irreducible in $L[X]$.*

This avoids the previous counterexample $f(X) = X^2 - 2$ with $L/K = \mathbf{Q}(\sqrt{2})/\mathbf{Q}$, since the coefficients of $f(X)$ do not generate $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$.

Proof. Since the coefficients of $f(X)$ generate L/K any σ in $\mathrm{Gal}(L/K)$ that is not the identity changes at least one off the coefficients of $f(X)$. (Otherwise the coefficients lie in the field fixed by σ, which is a nontrivial subgroup of $\mathrm{Gal}(L/K)$ and a nontrivial subgroup has a fixed field smaller than L.) It follows that for any distinct σ and τ in $\mathrm{Gal}(L/K)$, the

polynomials $(\sigma f)(X)$ and $(\tau f)(X)$ are different: if $\sigma f = \tau f$ then $(\tau^{-1}\sigma)f = f$, so $\tau^{-1}\sigma$ fixes the coefficients of f and therefore $\sigma = \tau$. Thus the hypothesis of the theorem is that

$$F(X) := \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma f)(X).$$

is irreducible in $K[X]$, where the product runs over *all* of $\mathrm{Gal}(L/K)$, and we want to show $f(X)$ is irreducible in $L[X]$. We will prove the contrapositive. Suppose $f(X)$ is reducible in $L[X]$, so $f(X) = g(X)h(X)$ in $L[X]$ where $g(X)$ and $h(X)$ are nonconstant. Then

$$F(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma f)(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma g)(X) \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma h)(X) = G(X)H(X),$$

where $G(X)$ and $H(X)$ are in $K[X]$ (why?). Since $g(X)$ and $h(X)$ have positive degree, so do $G(X)$ and $H(X)$, and therefore $F(X)$ is reducible in $K[X]$. □

Example 3.4. Consider $X^n - \sqrt{2}$ in $\mathbf{Q}(\sqrt{2})[X]$. Its coefficients generate $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$. Since

$$(X^n - \sqrt{2})(X^n + \sqrt{2}) = X^{2n} - 2$$

is irreducible over $\mathbf{Q}$, $X^n - \sqrt{2}$ is irreducible in $\mathbf{Q}(\sqrt{2})[X]$ for all n. The same kind of argument shows $X^n - (1 + 2\sqrt{2})$ is irreducible over $\mathbf{Q}(\sqrt{2})[X]$ for all n.

Corollary 3.5. *Let L/K be a finite Galois extension. Suppose $f(X)$ is monic in $L[X]$, its coefficients generate L/K, and $F(X) := \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma f)(X)$ is separable and irreducible in $K[X]$. Then each $(\sigma f)(X)$ is irreducible in $L[X]$ and if α is a root of $f(X)$ then the Galois closure of $L(\alpha)/K$ is the splitting field of $F(X)$ over K.*

Proof. The irreducibility of $f(X)$ in $L[X]$ follows from Theorem 3.3. The polynomials $(\sigma f)(X)$ satisfy the same hypotheses as $f(X)$, so they are all irreducible over L as well. The minimal polynomial of α over K is $F(X)$ and $K(\alpha)/K$ is separable since $F(X)$ is separable over K. Therefore $L(\alpha)/K$ is separable, so $L(\alpha)$ has a Galois closure over K.

A Galois extension of K that contains $L(\alpha)$ must contain all the K-conjugates of α and hence must contain the splitting field of $F(X)$ over K. Conversely, the splitting field of $F(X)$ over K is a Galois extension of K that contains α as well as all the roots of $f(X)$, so the extension contains the coefficients of $f(X)$. Those coefficients generate L/K, so the splitting field of $F(X)$ over K contains $L(\alpha)$. □

There is nothing deep going on in this corollary. The point is that since the coefficients of f generate L, L is already inside the Galois closure of $K(\alpha)/K$, so just by forming the splitting field of $F(X)$ over K we pick up L inside it.

Example 3.6. Consider the extension $\mathbf{Q}(\gamma)/\mathbf{Q}$, where γ is a root of $X^3 - 3X - 1$. This cubic extension is Galois and the $\mathbf{Q}$-conjugates of γ are $2 - \gamma^2$ and $\gamma^2 - \gamma - 2$. Let $f(X) = X^3 - \gamma X - 1$. The polynomials $(\sigma f)(X)$ as σ runs over the three elements of $\mathrm{Gal}(\mathbf{Q}(\gamma)/\mathbf{Q})$ are $f(X)$, $X^3 - (2 - \gamma^2)X - 1$, and $X^3 - (\gamma^2 - \gamma - 2)X - 1$. Their product is

$$F(X) = X^9 - 3X^6 - 3X^5 + 2X^3 + 3X^2 - 1,$$

which is irreducible mod 2 and thus is irreducible in $\mathbf{Q}[X]$. Therefore the polynomials $f(X)$, $X^3 - (2 - \gamma^2)X - 1$, and $X^3 - (\gamma^2 - \gamma - 2)X - 1$ are all irreducible over $\mathbf{Q}(\gamma)[X]$ and the splitting field of $F(X)$ over $\mathbf{Q}$ is the smallest Galois extension of $\mathbf{Q}$ containing $\mathbf{Q}(\gamma, \alpha)$, where α is a root of $f(X)$. According to PARI, the splitting field of $F(X)$ over $\mathbf{Q}$ has degree $684 = 3 \cdot 6^3$.

4. What Next?

There are two important aspects of field extensions that are missing by a study of Galois theory of finite extensions, and we briefly address them: Galois theory for infinite algebraic extensions and for transcendental extensions.

An algebraic extension L/K of infinite degree is called Galois when it is separable and normal. This means each element of L is the root of a separable irreducible in $K[X]$ and that every irreducible in $K[X]$ with a root in L splits completely over L. An example of an infinite Galois extension of $\mathbf{Q}$ is $\mathbf{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 1} \mathbf{Q}(\mu_{p^n})$, the union of all p-th power cyclotomic extensions of $\mathbf{Q}$, where p is a fixed prime. Even if an algebraic extension L/K is infinite, any particular element (or finite set of elements) in L lies in a finite subextension of K, so knowledge of finite extensions helps us understand infinite algebraic extensions. In fact, another way of describing an infinite Galois extension is that it is a composite of finite Galois extensions.

For an infinite Galois extension L/K, its Galois group $\mathrm{Gal}(L/K)$ is still defined as the group of K-automorphisms of L, and we can associate a subgroup of the Galois group to each intermediate field and an intermediate field to each subgroup of the Galois group just as in the finite case. However, this correspondence is no longer a bijection! This was first discovered by Dedekind, who saw in particular examples that different subgroups of an infinite Galois group could have the same fixed field. So it looks like Galois theory for infinite extensions breaks down. But it isn't really so. Krull realized that if you put a suitable topology on the Galois group then a bijection can be given between all intermediate fields and the *closed* subgroups in that topology. (See [1] and [3].) Every subgroup of the Galois group is associated to the same field as its closure in the Krull topology, and this explains Dedkind's examples of two different subgroups with the same associated field: one subgroup is the closure of the other. The Krull topology on Galois groups not only rescued Galois theory for infinite extensions, but gave a new impetus to the study of topological groups. To understand infinite Galois theory, first learn about the p-adic numbers and their topological and algebraic structure, as they are used in the simplest examples of interesting infinite Galois groups, such as $\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q})$.

Turning away from Galois extensions, the next most important class of field extensions are transcendental extensions. These are field extensions in which some element of the top field is transcendental (that is, not algebraic) over the bottom field. The simplest example of a transcendental extension of a field F is the field $F(T)$ of rational functions over F in an indeterminate T, or more generally the field $F(T_1, \ldots, T_n)$ of rational functions in n independent variables over F. This is called a pure transcendental extension. A general transcendental extension is a mixture of algebraic and transcendental parts, such as $F(x, y)$ where x is transcendental over F and $y^2 = x^3 - 1$.

Since transcendental extensions of F have infinite degree, the notion of field degree is no longer important. In its place is the concept of *transcendence degree*, which is a nonlinear analogue of a basis and measures how transcendental the extension is. The need to understand transcendental field extensions is not driven for its own sake, but for other areas of mathematics, such as algebraic geometry.

References

[1] J. Bastida, "Field extensions and Galois theory," Addison-Wesley, Reading, MA 1984.
[2] I. Kaplansky, "Fields and Rings," 2nd ed., Univ. of Chicago Press, Chicago, 1972.
[3] P. Morandi, "Field and Galois theory," Springer-Verlag, New York, 1996.