GALOIS THEORY AT WORK

KEITH CONRAD

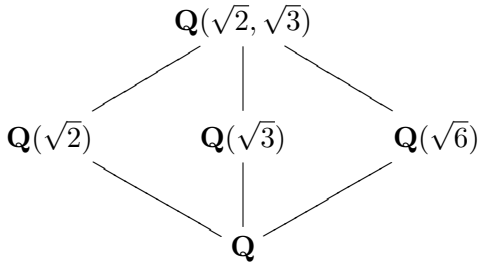
1. Examples

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

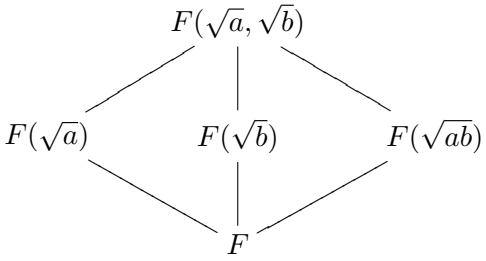
$$(X-(\sqrt{2}+\sqrt{3}))(X-(-\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X-(-\sqrt{2}-\sqrt{3})) = X^4-10X^2+1.$$

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

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

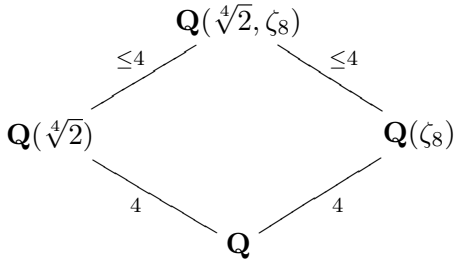
(Viewing elements of $\mathbf{Q}(\sqrt[4]{2},i)$ as complex numbers, s acts on them like complex conjugation.) The group $\langle r,s\rangle$ is isomorphic to D_4, where r corresponds to a 90 degree rotation of the square and s corresponds to a reflection across a diagonal. What is the subgroup H of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

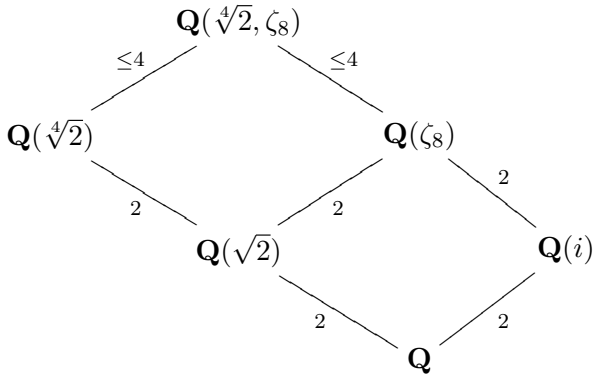
Any $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, \zeta_8)/\mathbf{Q})$ is determined by its values

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

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 which 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.

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.

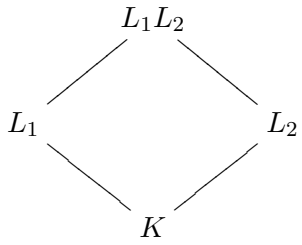
Since the quotient of a cyclic group by any subgroup is cyclic, if L/K is cyclic then F/K is cyclic too. □

Theorem 1.8. *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 1.8 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. 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.

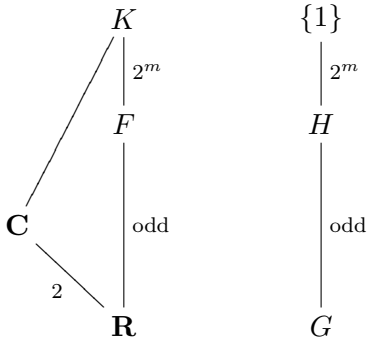
The first property is a consequence of the intermediate value theorem. The second property can be explained by writing a nonzero complex number as $re^{i\theta}$ and then its square roots are $\pm\sqrt{r}e^{i\theta/2}$. (For example, $i = e^{i\pi/2}$ and a square root of i is $e^{i\pi/4} = \frac{1}{\sqrt{2}}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

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

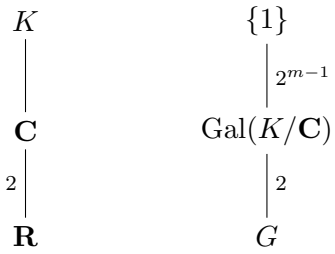
Proof. We need to show any irreducible in $\mathbf{C}[X]$ has degree 1. If $\pi(X) \in \mathbf{C}[X]$ is irreducible and α is a root, then $[\mathbf{C}(\alpha) : \mathbf{C}] = \deg \pi$, so our task is the same as showing the only finite extension of $\mathbf{C}$ is $\mathbf{C}$ itself.

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. □

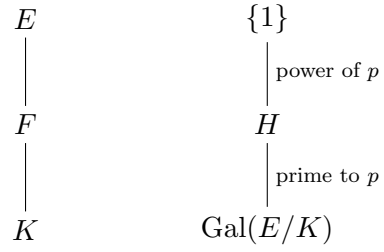
The next application, which is an amusing technicality, is taken from [6, p. 67].

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 which 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 [6, p. 67].

3. Applications to Minimal Polynomials

Theorem 3.1. *Let L/K be a finite Galois extension. For a monic irreducible polynomial $f(X)$ in $L[X]$, its roots have minimal polynomial in $K[X]$ equal to the product of all the different values of $(\sigma f)(X)$ as σ runs over $\mathrm{Gal}(L/K)$.*

When $\alpha \in L$ and $f(X) = X - \alpha$ 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 α be a root of $f(X)$ and write $\pi(X)$ for the minimal polynomial of α over K. Since $f(X)$ 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. Now the divisibility relation $F(X) \mid \pi(X)$ 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 $\mathbf{Q}(\sqrt{2})$. The minimal polynomial over $\mathbf{Q}$ of the roots of $X^2 - \sqrt{2}$ is

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

which is no surprise.

It is natural to ask if there is a converse to Theorem 3.1: if $f(X) \in L[X]$ and the product of the different polynomials $(\sigma f)(X)$, as σ runs over $\mathrm{Gal}(L/K)$, is irreducible in $K[X]$, is $f(X)$ irreducible in $L[X]$? This is too good to be true, since when $f(X) \in K[X]$ it says that an irreducible in $K[X]$ has to be irreducible in $L[X]$. That's ridiculous, since it violates the whole point of splitting fields: irreducibles in $K[X]$ can't stay irreducible over all finite Galois extensions of K! (For example, take $L/K = \mathbf{Q}(\sqrt{2})/\mathbf{Q}$ and $f(X) = X^4 - 2$.) But there is a kernel of truth in this false statement. We just have to make sure $f(X)$ honestly lives over L rather than a smaller subfield.

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 dumb counterexample where $f(X) \in K[X]$, since in that case the coefficients of f don't generate L (assuming $L \neq K$, of course).

Proof. If σ is not the identity in $\mathrm{Gal}(L/K)$, then one of the coefficients of $f(X)$ is not fixed by σ, since the coefficients generate L/K. Therefore different σ in $\mathrm{Gal}(L/K)$ have different polynomials $(\sigma f)(X)$: if $\sigma f = \tau f$ then $(\tau^{-1}\sigma)f = f$, so $\tau^{-1}\sigma$ is the identity, so $\sigma = \tau$. Thus the product being considered in the theorem is

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

We want to show that if $F(X)$ is irreducible in $K[X]$ then $f(X)$ is irreducible in $L[X]$. We will prove the contrapositive. Suppose $f(X) = g(X)h(X)$ 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 $K[X]$. 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 $L[X]$ and its coefficients generate L over K and $\pi(X) := \prod_{\sigma \in \mathrm{Gal}(L/K)} (\sigma f)(X)$ 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 $\pi(X)$ 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 $\pi(X)$ and $K(\alpha)/K$ is separable since $\pi(X)$ is separable over K. Therefore $L(\alpha)/K$ is separable, so $L(\alpha)$ has a Galois closure over K.

A Galois extension of K which contains $L(\alpha)$ must contain all the K-conjugates of α and hence must contain the splitting field of $\pi(X)$ over K. Conversely, the splitting field of $\pi(X)$ over K is a Galois extension of K which 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 $\pi(X)$ 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 $\pi(X)$ 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 $\gamma^2-\gamma-2$. (We will see a numerical criterion to check cubic extensions are Galois in Example 4.27, but that criterion will not tell us what the $\mathbf{Q}$-conjugates are.) 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

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

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 $\pi(X)$ 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 $\pi(X)$ over $\mathbf{Q}$ has degree $684 = 3 \cdot 6^3$.

4. Galois groups as permutation groups

For a separable polynomial $f(X) \in K[X]$ of degree n, the Galois group of $f(X)$ over K is defined to be the Galois group of a splitting field for $f(X)$ over K. We do not require $f(X)$ to be irreducible over K.

Example 4.1. The polynomial $X^4 - 2$ has splitting field $\mathbf{Q}(\sqrt[4]{2}, i)$ over $\mathbf{Q}$, so the Galois of $X^4 - 2$ over $\mathbf{Q}$ is isomorphic to D_4. The splitting field of $X^4 - 2$ over $\mathbf{R}$ is $\mathbf{C}$, so the Galois group of $X^4 - 2$ over $\mathbf{R}$ is cyclic of order 2.

Example 4.2. The Galois group of $X^3 - 2$ over $\mathbf{Q}$ is S_3.

Example 4.3. The Galois group of $(X^2 - 2)(X^2 - 3)$ over $\mathbf{Q}$ is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Its Galois group over $\mathbf{R}$ is trivial.

We will develop a method, using permutations, to study Galois groups of polynomials. It is particularly effective when the Galois group turns out to be a symmetric or alternating group.

Writing $f(X) = (X - r_1) \cdots (X - r_n)$, the splitting field of $f(X)$ over K is $K(r_1, \ldots, r_n)$. Each σ in the Galois group of $f(X)$ over K permutes the r_i's and σ is completely determined by this permutation since the r_i's generate the splitting field over K. A permutation of the r_i's can be viewed as a permutation of the subscripts $1, 2, \ldots, n$.

Example 4.4. Consider the Galois group of $X^4 - 2$ over $\mathbf{Q}$. The polynomial has 4 roots: $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$. Take as generators of $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ the automorphisms r and s from Example 1.2. The effect of the Galois group on $\sqrt[4]{2}$ and i is in Table 3.

Automorphism	1	r	r^2	r^3	s	rs	r^2s	r^3s
Value on $\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
Value on i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

TABLE 3

Passing from $\sqrt[4]{2}$ and i to the four roots of $X^4 - 2$, the effect of r on the roots of $X^4 - 2$ is

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

which is a 4-cycle, while the effect of s on the roots of $X^4 - 2$ is

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

which swaps $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$ while fixing $\sqrt[4]{2}$ and $-\sqrt[4]{2}$. So s is a 2-cycle on the roots.

Indexing the roots of $X^4 - 2$ as

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = i\sqrt[4]{2}, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -i\sqrt[4]{2}, \tag{4.1}$$

the automorphism r acts on the roots like (1234) and the automorphism s acts on the roots like (24). With this indexing of the roots, the Galois group of $X^4 - 2$ over $\mathbf{Q}$ becomes the following group of permutations in S_4.

Automorphism	1	r	r^2	r^3	s	rs	r^2s	r^3s
Permutation	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

TABLE 4

Example 4.5. If we label the roots of $(X^2 - 2)(X^2 - 3)$ as

$$r_1 = \sqrt{2}, \quad r_2 = -\sqrt{2}, \quad r_3 = \sqrt{3}, \quad r_4 = -\sqrt{3},$$

then the Galois group of $(X^2 - 2)(X^2 - 3)$ over $\mathbf{Q}$ becomes the following subgroup of S_4:

$$(1), \quad (12), \quad (34), \quad (12)(34). \tag{4.2}$$

Numbering the roots of $f(X)$ in a different way can identify the Galois group with a different subgroup of S_n.

Example 4.6. Labeling $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$ in this order as $\alpha_2, \alpha_4, \alpha_3, \alpha_1$ identifies the Galois group of $X^4 - 2$ over $\mathbf{Q}$ with the subgroup of S_4 in Table 5, which is not the subgroup of S_4 in Table 4.

Automorphism	1	r	r^2	r^3	s	rs	r^2s	r^3s
Permutation	(1)	(1243)	(14)(23)	(1342)	(14)	(13)(24)	(23)	(12)(34)

TABLE 5

Example 4.7. If we label $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ in this order as r_2, r_4, r_1, r_3 then the Galois group of $(X^2-2)(X^2-3)$ over $\mathbf{Q}$ turns into the following subgroup of S_4:

$$(1), \quad (13), \quad (24), \quad (13)(24). \tag{4.3}$$

This is not the same subgroup as (4.2).

In general, associating to each σ in the Galois group of $f(X)$ over K its permutation on the roots of $f(X)$, viewed as a permutation of the subscripts of the roots when we list them as $r_1, \ldots, r_n$, is a homomorphism from the Galois group to S_n. This homomorphism is injective since an element of the Galois group which fixes each r_i is the identity on the splitting field. Thinking about the Galois group of a polynomial with degree n as a subgroup of S_n is the original viewpoint of Galois. (The description of Galois theory in terms of field automorphisms is due to Dedekind and, with more abstraction, Artin.)

Two different choices for indexing the roots of $f(X)$ can lead to different subgroups of S_n, but they will be conjugate subgroups. For instance, the subgroups in Tables 4 and 5 are conjugate by the permutation $\binom{1234}{2431} = (124)$, which is the permutation turning one indexing of the roots into the other, and the subgroups (4.2) and (4.3) are conjugate by $\binom{1234}{2413} = (1243)$. So although the Galois group of $f(X)$ over K does not have a canonical embedding into S_n in general, its image in S_n is well-defined *up to an overall conjugation*. For example, without fixing an indexing of the roots, it doesn't make sense to ask if a particular permutation like (132) is in the Galois group as a subgroup of S_n, but it does make sense to ask if the Galois group contains a permutation with a particular cycle type (like a 3-cycle).

Although we can speak about Galois groups of irreducible or reducible polynomials, like $X^4 - 2$ or $(X^2-2)(X^3-2)$ over $\mathbf{Q}$, the Galois group of an irreducible polynomial turns out to have a special property, called transitivity, when we turn the Galois group into a subgroup of S_n. A subgroup $G \subset S_n$ is called *transitive* when, for any $i \neq j$ in $\{1, 2, \ldots, n\}$, there is a permutation in G sending i to j.

Example 4.8. The subgroups of S_4 in Tables 4 and 5 are transitive. This corresponds to the fact that for any two roots of $X^4 - 2$ there is an element of its Galois group over $\mathbf{Q}$ taking the first root to the second.

Example 4.9. The subgroup of S_4 in (4.2) is not transitive since no element of the subgroup takes 1 to 3. This corresponds to the fact that an element of $\mathrm{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ can't send $\sqrt{2}$ to $\sqrt{3}$.

Being transitive is not a property of an abstract group. It is a property of subgroups of S_n.[1] A conjugate subgroup of a transitive subgroup of S_n is also transitive since conjugation on S_n amounts to listing the numbers from 1 to n in a different order.

Theorem 4.10. *Let $f(X) \in K[X]$ be a separable polynomial of degree n.*

(a) *If $f(X)$ is irreducible in $K[X]$ then its Galois group over K has order divisible by n.*
(b) *The polynomial $f(X)$ is irreducible in $K[X]$ if and only if its Galois group over K is a transitive subgroup of S_n.*

[1]More generally, it is a property of groups equipped with a specific action on a set. Subgroups of S_n have a natural action on the set $\{1, 2, \ldots, n\}$.

Proof. (a) For a root r of $f(X)$ in K, $[K(r) : K] = n$ is a factor of the degree of the splitting field over K, which is the size of the Galois group over K.

(b) First suppose $f(X)$ is irreducible. For two roots r_i and r_j of $f(X)$, we can write $r_j = \sigma(r_i)$ for some σ in the Galois group of $f(X)$ over K. Therefore the Galois group, as a subgroup of S_n, sends i to j, so it is a transitive subgroup. Now suppose $f(X)$ is reducible (so $n \geq 2$). It is a product of distinct irreducibles since it is separable. Let r_i and r_j be roots of different irreducible factors of $f(X)$. These irreducible factors are the minimal polynomials of r_i and r_j over K. For any σ in the Galois group of $f(X)$ over K, $\sigma(r_i)$ has the same minimal polynomial over K as r_i, so we can't have $\sigma(r_i) = r_j$. Therefore, as a subgroup of S_n, the Galois group of $f(X)$ does not send i to j, so it is not a transitive subgroup of S_n. □

Here is our first application of these ideas to computing Galois groups.

Theorem 4.11. *Let $f(X) \in \mathbf{Q}[X]$ be an irreducible polynomial of prime degree p with all but two roots in $\mathbf{R}$. The Galois group of $f(X)$ over $\mathbf{Q}$ is isomorphic to S_p.*

Proof. Let $L = \mathbf{Q}(r_1, \ldots, r_p)$ be the splitting field of $f(X)$ over $\mathbf{Q}$. The permutations of the r_i's by $\mathrm{Gal}(L/\mathbf{Q})$ provide an embedding $\mathrm{Gal}(L/\mathbf{Q}) \hookrightarrow S_p$ and $\#\,\mathrm{Gal}(L/\mathbf{Q})$ is divisible by p by Theorem 4.10, so $\mathrm{Gal}(L/\mathbf{Q})$ contains an element of order p by Cauchy's theorem. In S_p, the only permutations of order p are p-cycles (why?). So the image of $\mathrm{Gal}(L/\mathbf{Q})$ in S_p contains a p-cycle.

We may take L to be a subfield of $\mathbf{C}$, since $\mathbf{C}$ is algebraically closed. Complex conjugation restricted to L is a member of $\mathrm{Gal}(L/\mathbf{Q})$. Since $f(X)$ has only two non-real roots by hypothesis, complex conjugation transposes two of the roots of $f(X)$ and fixes the others. Therefore $\mathrm{Gal}(L/\mathbf{Q})$ contains a transposition of the roots of $f(X)$. (This is the reason for the hypothesis about all but two roots being real.)

We now show the only subgroup of S_p containing a p-cycle and a transposition is S_p, so $\mathrm{Gal}(L/\mathbf{Q}) \cong S_p$. By suitable labeling of the numbers from 1 to p, we may let 1 be a number moved by the transposition, so our subgroup contains a transposition $\tau = (1a)$. Let σ be a p-cycle in the subgroup. As a p-cycle, σ acts on $\{1, 2, \ldots, p\}$ by a single orbit, so some σ^i with $1 \leq i \leq p-1$ sends 1 to a: $\sigma^i = (1a\ldots)$. This is also a p-cycle, because σ^i has order p in S_p and all elements of order p in S_p are p-cycles, so writing σ^i as σ and suitably reordering the numbers $2, \ldots, p$ (which replaces our subgroup by a conjugate subgroup), we may suppose our subgroup of S_p contains the particular transposition (12) and the particular p-cycle $(12\ldots p)$. For $n \geq 2$, it is a theorem in group theory that the particular transposition (12) and n-cycle $(12\ldots n)$ generate S_n, so our subgroup is S_p. □

Remark 4.12. While S_p is generated by any transposition and p-cycle for p prime, it is not true that S_n is generated by any transposition and n-cycle for general n. For example, (13) and (1234) generate a proper subgroup of S_4 (one of the subgroups of order 8).

Example 4.13. The polynomial $X^3 - X - 1$ is irreducible in $\mathbf{Q}[X]$ since it is irreducible mod 2 or since it is a cubic without any rational roots. It has one real root (approximately 1.3247), and one root of a cubic is all but two roots, so its Galois group over $\mathbf{Q}$ is isomorphic to S_3.

Example 4.14. The polynomials $X^3 - 3X - 1$ and $X^3 - 4X - 1$ are both irreducible in $\mathbf{Q}[X]$ since they are cubics without any rational roots. Each polynomial has three real roots (check!), so we can't use Theorem 4.11 to determine their Galois groups over $\mathbf{Q}$.

Example 4.15. The quintic polynomial $X^5 - X - 1$ is irreducible in $\mathbf{Q}[X]$ since it is irreducible mod 3. It has one real root, so Theorem 4.11 does not tell us the Galois group.

Example 4.16. The quintic polynomial $X^5 - 4X - 1$ is irreducible in $\mathbf{Q}[X]$ since it is irreducible mod 3. It has three real roots, which is all but two roots, so its Galois group over $\mathbf{Q}$ is isomorphic to S_5.

The next thing we will do with Galois groups as subgroups of S_n is determine when they lie in A_n. Without fixing a labeling of the roots of $f(X)$, its Galois group is determined as a subgroup of S_n only up to conjugation, but it is still meaningful to ask if the Galois group is a subgroup of A_n since $A_n \lhd S_n$. We will introduce a numerical invariant of polynomials, called the discriminant, to determine when the Galois group is in A_n.

Definition 4.17. For a nonconstant $f(X) \in K[X]$ of degree n which factors over a splitting field as

$$f(X) = c(X - r_1) \cdots (X - r_n),$$

the *discriminant* of $f(X)$ is defined to be

$$\operatorname{disc} f = \prod_{i<j} (r_j - r_i)^2.$$

Example 4.18. The polynomial $(X-1)(X-3)(X-7)$ has discriminant $2^2 \cdot 6^2 \cdot 4^2 = 2304$.

Example 4.19. The discriminant of $X^2 + aX + b = (X - r)(X - r')$ is

$$(r - r')^2 = r^2 - 2rr' + r'^2 = (r + r')^2 - 4rr' = a^2 - 4b,$$

which is the usual discriminant of a monic quadratic polynomial.

The number $\operatorname{disc} f$ is nonzero if $f(X)$ is separable and is 0 if $f(X)$ is not separable. When $f(X)$ is separable, $\operatorname{disc} f$ is a symmetric polynomial in the r_i's, so it is fixed by $\mathrm{Gal}(K(r_1, \ldots, r_n)/K)$ and therefore $\operatorname{disc} f \in K$ by Galois theory. We have $\operatorname{disc} f \in K$ if $f(X)$ is not separable too, since in that case $\operatorname{disc} f$ is 0.

Because $\operatorname{disc} f$ is a symmetric polynomial in the roots of $f(X)$, when $f(X)$ is monic its discriminant is a polynomial in the coefficients of $f(X)$ (which are, up to sign, the elementary symmetric functions of the roots). In low-degree cases, explicit formulas for discriminants of some trinomials are

$$\begin{aligned}
\operatorname{disc}(X^2 + aX + b) &= a^2 - 4b, \\
\operatorname{disc}(X^3 + aX + b) &= -4a^3 - 27b^2, \\
\operatorname{disc}(X^4 + aX + b) &= -27a^4 + 256b^3, \\
\operatorname{disc}(X^5 + aX + b) &= 256a^5 + 3125b^4.
\end{aligned}$$

Example 4.20. The discriminant of $X^3 - X - 1$ is -23, the discriminant of $X^3 - 3X - 1$ is 81, and the discriminant of $X^3 - 4X - 1$ is 229.

More generally [10, p. 41],

$$\operatorname{disc}(X^n + aX + b) = (-1)^{n(n-1)/2}((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}),$$

and even more generally, for $0 < m < n$ and $(m, n) = 1$,

$$\operatorname{disc}(X^n + aX^m + b) = (-1)^{n(n-1)/2} b^{m-1}((-1)^{n-1} m^m (n-m)^{n-m} a^n + n^n b^{n-m}).$$

If (m, n) is not necessarily 1 then [12, Theorem 2]

$$\operatorname{disc}(X^n+aX^m+b) = (-1)^{n(n-1)/2}b^{m-1}((-1)^{n/d-1}m^{m/d}(n-m)^{(n-m)/d}a^{n/d}+n^{n/d}b^{(n-m)/d})^d,$$

where $d = (m, n)$. We will not derive these formulas here.

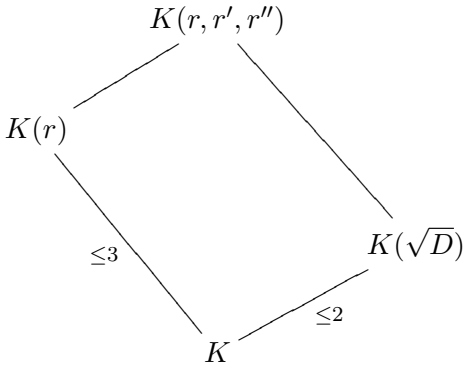
Example 4.21. Taking $m = 2$ and $n = 4$,

$$\operatorname{disc}(X^4 + aX^2 + b) = 16b(a^2 - 4b)^2.$$

Theorem 4.22. *Let K not have characteristic 2 and let $f(X)$ be a separable cubic in $K[X]$ with a root r and discriminant D. The splitting field of $f(X)$ over K is $K(r, \sqrt{D})$.*

Note we are *not* assuming $f(X)$ is irreducible here.

Proof. The roots and the discriminant of f don't change if we multiply f by a nonzero constant, so we may assume $f(X)$ is monic. Let $f(X)$ have roots r, r', and r'', so the splitting field of $f(X)$ over K is $K(r, r', r'')$.



Over $K(r)$, we can remove a linear factor and write $f(X) = (X-r)g(X)$, where $g(r) \neq 0$. Explicitly, $g(X) = (X - r')(X - r'')$. (Since f is monic, so is g.) By the quadratic formula on $g(X)$, $K(r, r', r'') = K(r, \sqrt{\operatorname{disc} g})$. It is simple to check, since f is monic, that $\operatorname{disc} f = g(r)^2 \operatorname{disc} g$, so $K(r, \sqrt{\operatorname{disc} g}) = K(r, \sqrt{\operatorname{disc} f}) = K(r, \sqrt{D})$. □

Theorem 4.23. *Let $f(X) \in K[X]$ be a separable polynomial of degree n. If K does not have characteristic 2, the embedding of the Galois group of $f(X)$ over K into S_n as permutations of the roots of $f(X)$ has image in A_n if and only if $\operatorname{disc} f$ is a square in K.*

Proof. Set $\delta = \prod_{i<j}(r_j - r_i) \neq 0$, so $\delta \in K(r_1, \ldots, r_n)$ and $\delta^2 = \operatorname{disc} f \in K$. Therefore $\operatorname{disc} f$ is a square in K if and only if $\delta \in K$.

For any $\sigma \in \operatorname{Gal}(K(r_1, \ldots, r_n)/K)$, let $\varepsilon_\sigma = \pm 1$ be its sign as a permutation of the r_i's. By one of the definitions of the sign of a permutation,

$$\sigma(\delta) = \prod_{i<j}(\sigma(r_j) - \sigma(r_i)) = \varepsilon_\sigma \prod_{i<j}(r_j - r_i) = \varepsilon_\sigma \delta,$$

so $\sigma(\delta) = \pm\delta$. Since $\delta \neq 0$ and K doesn't have characteristic 2, $\delta \neq -\delta$. We have $\sigma \in A_n$ if and only if $\varepsilon_\sigma = 1$, so $\sigma \in A_n$ if and only if $\sigma(\delta) = \delta$. Therefore the Galois group of $f(X)$ over K is in A_n if and only if δ is fixed by the Galois group, which is the same as $\delta \in K$. □

Remark 4.24. Theorem 4.23 is completely false in characteristic 2: discriminants of polynomials are always squares in characteristic 2 but S_n can occur as a Galois group. For example, if F is any field of characteristic 2, then over $F(T)$ the polynomial $X^3 + TX + T$ is separable and irreducible and its Galois group is S_3.

Theorem 4.23 lets us determine the Galois groups of irreducible cubic polynomials outside of characteristic 2.

Theorem 4.25. *Let K not have characteristic 2 and let $f(X)$ be a separable irreducible cubic in $K[X]$.*

(a) *If $\operatorname{disc} f$ is a square in K then the Galois group of $f(X)$ over K is isomorphic to A_3.*
(b) *If $\operatorname{disc} f$ is not a square in K then the Galois group of $f(X)$ over K is isomorphic to S_3.*

Proof. Since $K(r)$ is inside the splitting field, the Galois group is divisible by $[K(r) : K] = 3$. The permutations of the roots of $f(X)$ by its Galois group over K gives an embedding of the Galois group into S_3, so the image is either A_3 or S_3 since these are the only subgroups of S_3 with size divisible by 3. Theorem 4.23 says the image is in A_3 (and thus equal to A_3) if and only if $\operatorname{disc} f$ is a square in K.

This can also be proved using the formula for the splitting field of a cubic in Theorem 4.22. □

Example 4.26. In Example 4.13 we saw $X^3 - X - 1$ has Galois group S_3 over $\mathbf{Q}$. We can see again that $X^3 - X - 1$ has Galois group S_3 over $\mathbf{Q}$ since its discriminant is -23 (Example 4.20) and this is not a rational square.

Example 4.27. The Galois groups of $X^3 - 3X - 1$ and $X^3 - 4X - 1$ over $\mathbf{Q}$ were left undetermined in Example 4.14 since all of their roots are real. Now we can compute the Galois groups. From Example 4.20, $X^3 - 3X - 1$ has discriminant 81 (a square) and $X^3 - 4X - 1$ has discriminant 229 (a prime). Therefore $X^3 - 3X - 1$ has Galois group A_3 over $\mathbf{Q}$ and $X^3 - 4X - 1$ has Galois group S_3 over $\mathbf{Q}$. So although $X^3 - 3X - 1$ and $X^3 - 4X - 1$ both have all real roots, their Galois groups are not isomorphic. Any root of $X^3 - 3X - 1$ generates the splitting field over $\mathbf{Q}$, but this is not true for any root of $X^3 - 4X - 1$.

Remark 4.28. The cubics $X^3 - 2X + 1$ and $X^3 - 7X - 6$ have respective discriminants 5 and $400 = 20^2$, but this does *not* mean their Galois groups over $\mathbf{Q}$ are S_3 and A_3. Both polynomials are reducible (factoring as $(X - 1)(X^2 + X - 1)$ and $(X + 1)(X + 2)(X - 3)$). Do not forget to check that a cubic is irreducible before you use Theorem 4.25!

The following fantastic theorem of Dedekind uses factorization of a polynomial mod p to tell us when a Galois group over $\mathbf{Q}$ contains permutations with particular cycle structure.

Theorem 4.29 (Dedekind)**.** *Let $f(X) \in \mathbf{Z}[X]$ be monic irreducible over $\mathbf{Q}$ of degree n. For any prime p not dividing $\operatorname{disc} f$, let the monic irreducible factorization of $f(X)$ mod p be*

$$f(X) \equiv \pi_1(X) \cdots \pi_k(X) \bmod p$$

and set $d_i = \deg \pi_i(X)$, so $d_1 + \cdots + d_k = n$. The Galois group of $f(X)$ over $\mathbf{Q}$, viewed as a subgroup of S_n, contains a permutation of type $(d_1, \ldots, d_k)$.

The cleanest proof of Theorem 4.29 uses algebraic number theory and is beyond the scope of these notes. Proofs of Theorem 4.29 which do not directly use algebraic number theory can be found in [2, pp. 398–400] and [5, pp. 302–304], but I think these proofs are overly confusing at the expense of requiring less machinery.

Example 4.30. We compute the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ using Theorem 4.29.

This polynomial is irreducible mod 2, so it is irreducible over $\mathbf{Q}$. Let its roots be r_1, r_2, r_3, r_4. The extension $\mathbf{Q}(r_1)/\mathbf{Q}$ has degree 4, so the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ has order divisible by 4. Since the Galois group embeds into S_4, its size is either 4, 8, 12, or 24. The discriminant of $X^4 - X - 1$ is -283, which is not a rational square, so the Galois group is not a subgroup of A_4. This eliminates the possibility of the Galois group having order 12, because the only subgroup of S_4 with order 12 is A_4. (Quite generally, the only subgroup of index 2 in S_n is A_n for $n \geq 2$.) There are subgroups of S_4 with orders 4, 8, and (of course) 24 outside of A_4, so no other size but 12 is eliminated yet. We will use Theorem 4.29 to show the Galois group has order divisible by 3, and this will prove the Galois group is S_4 since 4 and 8 are not divisible by 3.

Using Theorem 4.29 with $p = 7$,

$$X^4 - X - 1 \equiv (X + 4)(X^3 + 3X^2 + 2X + 5) \bmod 7.$$

This is an irreducible factorization, so the Galois group of $X^4 - X - 1$ over $\mathbf{Q}$ contains a permutation of the roots with cycle type $(1, 3)$, which means there is a 3-cycle in the Galois group. Any 3-cycle has order 3.

This Galois group computation has an application to constructible numbers. A necessary condition for a complex number to be constructible (using only an unmarked straightedge and compass) is that the number has 2-power degree over $\mathbf{Q}$. This necessary condition is not sufficient: if r is a root of $X^4 - X - 1$ then $[\mathbf{Q}(r) : \mathbf{Q}] = 4$ and we will show r is not a constructible number by showing there is no quadratic field in $\mathbf{Q}(r)$.

Let L be a splitting field of $X^4 - X - 1$ over $\mathbf{Q}$, so the permutations of its roots by $\mathrm{Gal}(L/\mathbf{Q})$ is an isomorphism with S_4. The subgroup $\mathrm{Gal}(L/\mathbf{Q}(r))$ corresponds to a subgroup of S_4 fixing one of the four numbers, which is a group isomorphic to S_3. (The subgroups of any S_n fixing one number are all conjugate to each other, and in fact are all of the subgroups of index n in S_n.)

$$\begin{array}{ccc} L & & \{(1)\} \\ {\scriptstyle 6}\big| & & {\scriptstyle 6}\big| \\ \mathbf{Q}(r) & & S_3 \\ {\scriptstyle 4}\big| & & {\scriptstyle 4}\big| \\ \mathbf{Q} & & S_4 \end{array}$$

There is no subgroup of S_4 strictly between S_3 and S_4: if there were it would be a subgroup of index 2 and thus has to be A_4, but $S_3 \not\subset A_4$. (There is no subgroup of order 6 in A_4.) So by the Galois correspondence, there is no field properly between $\mathbf{Q}$ and $\mathbf{Q}(r)$.

Remark 4.31. For any $k \geq 2$, there are complex numbers which have degree 2^k over $\mathbf{Q}$ but are not constructible.

Example 4.32. We determine the Galois group of $X^4 + 8X + 12$ over $\mathbf{Q}$. This is reducible mod p for all small p, so the reduction mod p test doesn't help us prove the polynomial is irreducible over $\mathbf{Q}$. (In fact, the polynomial factors mod p for all p, so the reduction mod p test really doesn't apply. It's not an artifact of only looking at small primes.) Let's look

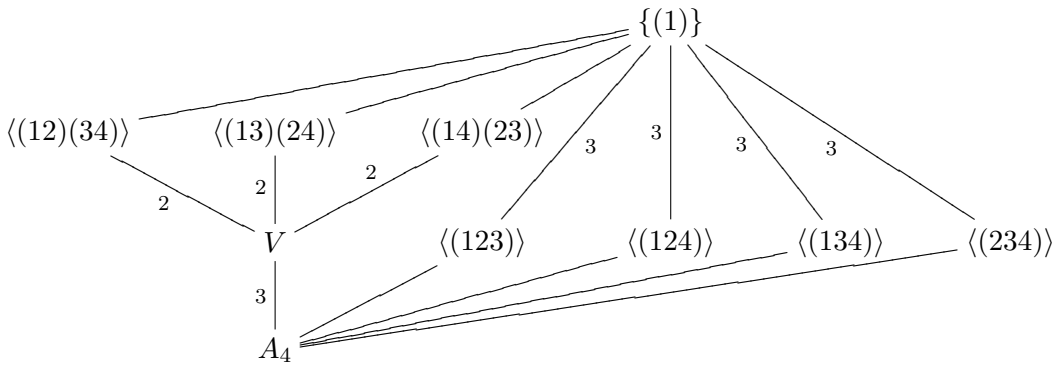
at *how* the polynomial factors into irreducibles modulo different primes:

$$\begin{aligned} X^4+8X+12 &\equiv (X+1)(X^3+4X^2+X+2) \bmod 5, \\ X^4+8X+12 &\equiv (X^2+4X+7)(X^2+13X+9) \bmod 17. \end{aligned}$$

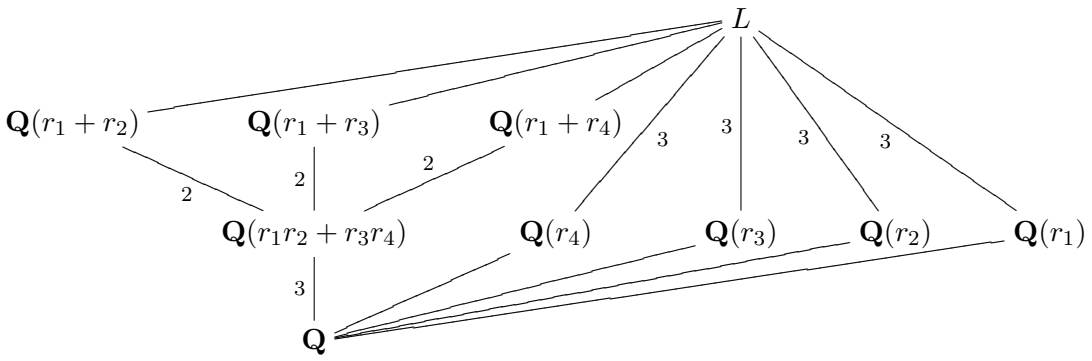
These are only consistent with $X^4+8X+12$ being irreducible over $\mathbf{Q}$ (why?).

By the irreducibility of the polynomial, the Galois group of $X^4+8X+12$ over $\mathbf{Q}$ has size divisible by 4. The discriminant of $X^4+8X+12$ is $331776 = 576^2$, a rational square, so the Galois group is a subgroup of A_4 and therefore has size 4 or 12. From the factorization of the polynomial mod 5 above, the Galois group contains a permutation of the roots whose cycle type is $(1,3)$, which is a 3-cycle, so the Galois group has order divisible by 3, and thus its size is 12. So the Galois group of $X^4+8X+12$ over $\mathbf{Q}$ is isomorphic to A_4: the even permutations of the roots extend to automorphisms of the splitting field over $\mathbf{Q}$, while the odd permutations do not.

Let's list all the subfields of the splitting field of $X^4+8X+12$ over $\mathbf{Q}$. Here is the lattice (upside down) of subgroups of A_4.



The corresponding subfield lattice of $L = \mathbf{Q}(r_1, r_2, r_3, r_4)$ is as follows.



The normal subgroups of A_4 are $\{1\}$, V, and A_4, so the only subfield of L that is Galois over $\mathbf{Q}$ other than L and $\mathbf{Q}$ is $\mathbf{Q}(r_1r_2+r_3r_4)$. Since $[L : \mathbf{Q}(r_1)] = 3$ is prime and $r_2 \notin \mathbf{Q}(r_1)$, we have $L = \mathbf{Q}(r_1, r_2)$, so $[\mathbf{Q}(r_1, r_2) : \mathbf{Q}] = 12$.

The sums r_1+r_2, r_1+r_3, and r_1+r_4 are roots of X^6-48X^2-64 (check!) and $r_1r_2+r_3r_4$ is a root of $X^3-48X-64$. Roots of $X^3-48X-64$ are squares of roots of X^6-48X^2-64. It is left to the reader to check that $r_1r_2+r_3r_4 = (r_1+r_2)^2 = (r_3+r_4)^2$.

Example 4.33. Let's determine the Galois group of $X^5 - X - 1$ over $\mathbf{Q}$, which was left unresolved in Example 4.15. Its irreducible factorization mod 2 is

$$X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1) \bmod 2.$$

Because the polynomial is irreducible over $\mathbf{Q}$, 5 divides the size of the Galois group. From the mod 2 factorization, the Galois group contains a permutation of the roots with cycle type $(2, 3)$, which has order 6, so the Galois group has size divisible by $5 \cdot 6 = 30$. Since the Galois group is a subgroup of S_5, its size is either 30, 60, or 120.

Group theory tells us there is no subgroup of S_5 with order 30 and the only subgroup of order 60 is A_5. The discriminant is $2869 = 19 \cdot 151$, which is not a rational square, so the Galois group is not in A_5. Therefore the Galois group is S_5.

Theorem 4.11 gave us a sufficient condition for an irreducible in $\mathbf{Q}[X]$ of prime degree p to have Galois group S_p: all but 2 roots are real. This condition does not apply to $X^3 - 4X - 1$ or $X^5 - X - 1$, although by Examples 4.27 and 4.33 their Galois groups over $\mathbf{Q}$ are S_3 and S_5. Using Theorem 4.29, there is a different "all but two roots" hypothesis which also implies a Galois group is S_p.

Corollary 4.34. *Let $f(X) \in \mathbf{Z}[X]$ be monic irreducible over $\mathbf{Q}$ of prime degree p. If there is a prime number ℓ not dividing* $\operatorname{disc} f$ *such that $f(X) \bmod \ell$ has all but two roots in $\mathbf{F}_\ell$, then the Galois group of $f(X)$ over $\mathbf{Q}$ is isomorphic to S_p.*

Proof. The proof of Theorem 4.11 can be used again except for the step explaining why the Galois group of $f(X)$ over $\mathbf{Q}$ contains a transposition. In Theorem 4.11 this came from the use of complex conjugation to transpose two non-real roots, assuming there are only two non-real roots. We aren't assuming that anymore. By hypothesis the factorization of $f(X) \bmod \ell$ has all linear factors except for one quadratic irreducible factor. Therefore Theorem 4.29 says the Galois group contains a permutation of the roots with cycle type $(1, 1, \ldots, 1, 2)$, which is a transposition in S_p. □

Example 4.35. From Examples 4.13 and 4.27, the polynomials $X^3 - X - 1$ with discriminant -23 and $X^3 - 4X - 1$ with discriminant 229 each have Galois group S_3 over $\mathbf{Q}$. We can check this again with Corollary 4.34: $X^3 - X - 1 \bmod 5$ has one root and $X^3 - 4X - 1 \bmod 2$ has one root.

Example 4.36. In Example 4.16 we saw $X^5 - 4X - 1$ has Galois group S_5 over $\mathbf{Q}$ because it has all but two real roots. We can also compute the Galois group with Corollary 4.34: the discriminant is -259019 (a negative prime number) and by a computer search $X^5 - 4X - 1 \bmod 19$ has all but two roots in $\mathbf{F}_{19}$.

Example 4.37. Returning to Example 4.33, we can show the Galois group over $\mathbf{Q}$ of $X^5 - X - 1$ is S_5 in another way: $X^5 - X - 1$ has discriminant $2869 = 19 \cdot 151$ and by a computer search $X^5 - X - 1 \bmod 163$ has all but two roots in $\mathbf{F}_{163}$.

Remark 4.38. We can't use Corollary 4.34 to show $X^4 - X - 1$ has Galois group S_4 over $\mathbf{Q}$ (Example 4.30) since 4 is not prime.

If we seek an analogue of Theorem 4.11 for a Galois group to be isomorphic to A_p, using 3-cycles in place of transpositions, there is no analogue since an irreducible polynomial over $\mathbf{Q}$ can't have all but three roots in $\mathbf{R}$ (the number of non-real roots is always even). But $f(X) \bmod \ell$ could have all but three roots in $\mathbf{F}_\ell$. This suggests the next result.

Corollary 4.39. *Let $f(X) \in \mathbf{Z}[X]$ be monic irreducible over $\mathbf{Q}$ of prime degree $p \geq 3$ with* $\operatorname{disc} f$ *a perfect square. If there is a prime number ℓ not dividing* $\operatorname{disc} f$ *such that $f(X) \bmod \ell$ has all but three roots in $\mathbf{F}_\ell$, then the Galois group of $f(X)$ over $\mathbf{Q}$ is isomorphic to A_p.*

Proof. Let G be the Galois group, so G is a subgroup of A_p since $\operatorname{disc} f$ is a square. The Galois group has order divisible by p, so it contains a p-cycle. From the factorization of $f(X) \bmod \ell$ and Theorem 4.29, G contains a 3-cycle. It is a theorem of C. Jordan that for any prime $p \geq 3$, any p-cycle and any 3-cycle in S_p generate A_p, so $G \cong A_p$. □

Example 4.40. The polynomial $X^5 + 20X + 16$ has discriminant $2^{16}5^6$. It is irreducible mod 3, so it's irreducible over $\mathbf{Q}$. Modulo 7, its irreducible factorization

$$X^5 + 20X + 16 \equiv (X - 4)(X - 5)(X^3 + 2X^2 + 5X + 5) \bmod 7.$$

This has all but three roots in $\mathbf{F}_7$, so the Galois group of $X^5+20X+16$ over $\mathbf{Q}$ is isomorphic to A_5.

In Table 6 are the trinomial polynomials whose Galois group over $\mathbf{Q}$ has been computed by the methods in this section.

$f(X)$	Galois group over $\mathbf{Q}$
$X^3 - X - 1$	S_3
$X^3 - 3X - 1$	A_3
$X^3 - 4X - 1$	S_3
$X^4 - X - 1$	S_4
$X^4 + 8X + 12$	A_4
$X^5 - X - 1$	S_5
$X^5 - 4X - 1$	S_5
$X^5 + 20X + 16$	A_5

TABLE 6

It is a hard theorem of Chebotarev that the sufficient conditions for $f(X)$ to have Galois group S_p in Corollary 4.34 and A_p in Corollary 4.39 are also necessary in a strong sense: if $f(X) \in \mathbf{Z}[X]$ is monic irreducible of prime degree p with Galois group over $\mathbf{Q}$ isomorphic to S_p (resp., A_p) then there are infinitely many primes ℓ not dividing $\operatorname{disc} f$ such that $f(X) \bmod \ell$ has all but two roots (resp., all but three roots) in $\mathbf{F}_\ell$. For example, $X^5 - X - 1 \bmod \ell$ has all but two roots in $\mathbf{F}_\ell$ when $\ell = 163, 193, 227, 307, 467, \ldots$ (there is no simple pattern to this list, but it continues indefinitely), $X^5 - 4X - 1 \bmod \ell$ has all but two roots in $\mathbf{F}_\ell$ when $\ell = 19, 23, 83, 97, 149, \ldots$, and $X^5 + 20X + 16$ has all but three roots in $\mathbf{F}_\ell$ when $\ell = 7, 11, 17, 23, 29, \ldots$. In practice, it is easy to prove when a monic irreducible in $\mathbf{Z}[X]$ with prime degree p has Galois group A_p or S_p over $\mathbf{Q}$ by searching for a prime ℓ such that Corollary 4.34 or 4.39 applies. There are extensions of these ideas to polynomials of nonprime degree, so verifying an irreducible polynomial of degree n has Galois group over $\mathbf{Q}$ that is isomorphic to S_n or A_n in practice is easy.

On the other hand, proving a Galois group is small (not S_n or A_n) is a completely separate matter, which we will not discuss here.

5. Trace and Norm

For any finite extension of fields L/K, the trace and norm functions are defined in terms of the trace and determinant of multiplication maps on L. When L/K is Galois, the trace and norm on L/K can be described using the Galois group.

Theorem 5.1. *If L/K is a finite Galois extension with Galois group G, the characteristic polynomial of $\alpha \in L$ is $\chi_{\alpha,L/K}(X) = \prod_{\sigma\in G}(X - \sigma(\alpha))$. In particular,*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma\in G}\sigma(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \prod_{\sigma\in G}\sigma(\alpha).$$

Proof. Since L/K is Galois, the minimal polynomial of α in $K[X]$ splits in $L[X]$. Call its different roots $\alpha_1, \ldots, \alpha_d$, so $d = [K(\alpha) : K]$ and by a general property of characteristic polynomials,

$$\chi_{\alpha,L/K}(X) = ((X - \alpha_1)\cdots(X - \alpha_d))^{n/d},$$

where $n = [L : K]$.

For any $\sigma \in G$, $\sigma(\alpha)$ is some α_i, and by Galois theory every α_i is $\sigma(\alpha)$ for some σ. Since $\sigma(\alpha) = \sigma'(\alpha)$ if and only if $\sigma = \sigma'\tau$ for some $\tau \in \mathrm{Gal}(L/K(\alpha))$, each α_i has the form $\sigma(\alpha)$ for $[L : K(\alpha)] = n/d$ values of σ in G. Therefore

$$\chi_{\alpha,L/K}(X) = ((X - \alpha_1)\cdots(X - \alpha_d))^{n/d} = \prod_{\sigma\in G}(X - \sigma(\alpha)).$$

The desired identities for the trace and norm fall out from this by looking at the coefficients of the polynomial on the right. □

Example 5.2. If $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{d})$ for a nonsquare d in $\mathbf{Q}^\times$, the two elements of $\mathrm{Gal}(L/K)$ are determined by $\sigma_1(\sqrt{d}) = \sqrt{d}$ and $\sigma_2(\sqrt{d}) = -\sqrt{d}$, so

$$\mathrm{Tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$$

and

$$\mathrm{N}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Also

$$\chi_{a+b\sqrt{d},\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(X) = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) = X^2 - 2aX - (a^2 - db^2).$$

Example 5.3. For $\alpha \in \mathbf{F}_{p^n}$,

$$\mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \text{ and } \mathrm{N}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(\alpha) = \alpha\alpha^p\cdots\alpha^{p^{n-1}}.$$

6. Relations among Galois groups

We already saw in Theorem 1.8 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

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

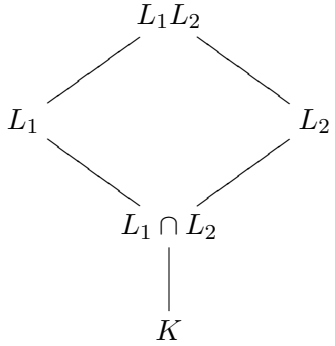
When is this embedding an isomorphism?

Theorem 6.1. *Let L_1 and L_2 be Galois over K. 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 $L_1 \cap L_2 = K$.

Proof. 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 $L_1 \cap L_2 = K$.

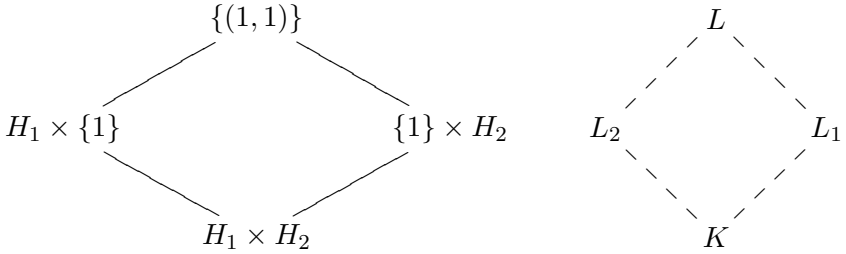


Consider the restriction homomorphism

$$\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/K), \quad \text{where} \quad \sigma \mapsto \sigma|_{L_1}. \tag{6.1}$$

Any automorphism in the kernel fixes L_1 and L_2, so also L_1L_2. Thus the kernel is trivial. To find the image we compute the fixed field of the image inside L_1. It is the elements of L_1 fixed by $\mathrm{Gal}(L_1L_2/L_2)$. The elements of L_1L_2 fixed by $\mathrm{Gal}(L_1L_2/L_2)$ are the elements of L_2 (by the Galois correspondence), so the image of (6.1) is the elements of L_2 in L_1. This is $L_1 \cap L_2$, so by the Galois correspondence the image of (6.1) is $\mathrm{Gal}(L_1/L_1 \cap L_2)$. Thus $\mathrm{Gal}(L_1L_2/L_2) \cong \mathrm{Gal}(L_1/L_1 \cap L_2)$, so in particular $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$. This is $[L_1 : K]$ if and only if $L_1 \cap L_2 = K$. □

Remark 6.2. Theorem 6.1 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 $L_1 \cap L_2 = K$ is a statement that makes sense without Galois hypotheses on L_1/K and L_2/K, but it isn't true that generally. Here are two counterexamples (the first one is the easiest and should be memorized).

Example 6.3. 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 $[L_1L_2 : K] = 6 \neq [L_1 : K][L_2 : K]$.

Example 6.4. If $K = \mathbf{Q}$, $L_1 = \mathbf{Q}(r)$, and $L_2 = \mathbf{Q}(r')$ where r and r' are two roots of $X^4 + 8X + 12$ then $L_1 \cap L_2 = K$ but $[L_1L_2 : K] = 12 \neq [L_1 : K][L_2 : K]$.

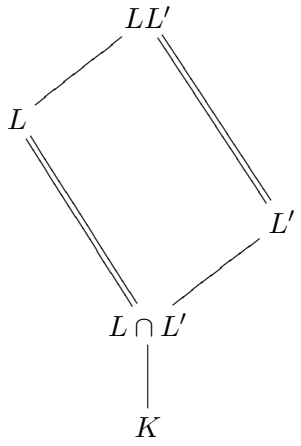
In these counterexamples, neither extension is Galois. What if just one is Galois?

Theorem 6.5. *For a finite Galois extension L/K and an arbitrary finite extension L'/K, the extension LL'/L' is finite Galois and $\mathrm{Gal}(LL'/L') \cong \mathrm{Gal}(L/L \cap L')$ by restriction. In particular,*

$$[LL' : L'] = [L : L \cap L'], \quad [LL' : K] = \frac{[L : K][L' : K]}{[L \cap L' : K]}.$$

In particular, $[LL' : K] = [L : K][L' : K]$ if and only if $L \cap L' = K$.

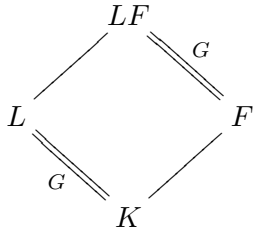
Proof. The field diagram looks like the following, where we use parallel lines to emphasize the field extensions whose Galois groups we will identify.



Since L/K is finite Galois, L is a splitting field over K of a separable polynomial $f(X) \in K[X]$. Then LL' is a splitting field over L' for $f(X)$, so LL'/L' is Galois. By the ideas from the proof of Theorem 6.1, the restriction homomorphism $\mathrm{Gal}(LL'/L') \to \mathrm{Gal}(L/K)$ is injective and the fixed field of its image is $\mathrm{Gal}(L/L \cap L')$, so $\mathrm{Gal}(LL'/L') \cong \mathrm{Gal}(L/L \cap L')$. (That L'/K may not be Galois is irrelevant.)

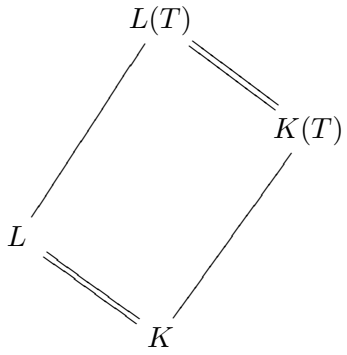
From the isomorphism of Galois groups, $[LL' : L'] = [L : L \cap L']$. The formula for $[LL' : K]$ follows by writing it as $[LL' : L'][L' : K]$. □

Example 6.6. If L/K is Galois with Galois group G and F/K is any finite extension with $L \cap F = K$, then LF/F is a Galois extension of F with $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L \cap F) = \mathrm{Gal}(L/K) = G$. This provides a way to realize Galois groups over K as Galois groups over finite extensions of K. We will return to this point at the end of Section 8.



In the proof of Theorem 6.5, the assumption that L'/K is finite was only used at the very end, to compute $[LL' : K]$. The rest of the proof goes through if L'/K is infinite, not necessarily even algebraic, and here is a worthwhile application of that generality.

Theorem 6.7. *Let L/K be a finite Galois extension and let $L' = K(T)$ be the rational function field over K in the indeterminate u. Then $LL' = L(T)$.*



Proof. The intersection $K(T) \cap L$ is K because the only elements of $K(T)$ which are algebraic over K are the elements of K themselves. (If a nonconstant rational function $f(T)$ were algebraic over K then T would be algebraic over K since T is algebraic over $K(f(T))$.) Therefore Theorem 6.5 says the extension $L(T)/K(T)$ of rational function fields is Galois with $\mathrm{Gal}(L(T)/K(T)) \cong \mathrm{Gal}(L/K)$ by $\sigma \mapsto \sigma|_L$. □

The way the inverse of this isomorphism works is that elements of $\mathrm{Gal}(L/K)$ act on $L(T)$ by acting on coefficients, keeping T fixed. For instance, $\mathbf{C}(T) = \mathbf{R}(T)(i)$ is a quadratic extension of $\mathbf{R}(T)$ and $\mathrm{Gal}(\mathbf{C}(T)/\mathbf{R}(T))$ is the identity and complex conjugation acting on coefficients.

Corollary 6.8. *Let L/K be a finite Galois extension and $f(X) \in L[X]$ be monic, separable, and irreducible.*

Returning to Theorem 6.1 again, it is natural to ask *how* the Galois group of a composite of finite Galois extensions lies in the direct product of the Galois groups. What is the image of the embedding?

Theorem 6.9. *When L_1 and L_2 are finite Galois extensions of K, the image of the embedding $\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ which sends σ to $(\sigma|_{L_1}, \sigma|_{L_2})$ is the compatible automorphisms: $\{(\tau_1, \tau_2) : \tau_1 = \tau_2 \text{ on } L_1 \cap L_2\}$.*

Proof. 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. We will check the image has the same size as H, so the groups coincide.

To count $\#H$, we count for each $\tau_1 \in \mathrm{Gal}(L_1/K)$ how many $\tau_2 \in \mathrm{Gal}(L_2/K)$ have $\tau_2|_{L_1 \cap L_2} = \tau_1|_{L_1 \cap L_2}$. The restriction map $\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1 \cap L_2/K)$, where $\tau_2 \mapsto \tau_2|_{L_1 \cap L_2}$, is a surjective homomorphism with kernel $\mathrm{Gal}(L_2/L_1 \cap L_2)$, so each element of $\mathrm{Gal}(L_1 \cap L_2/K)$ has the form $\tau_2|_{L_1 \cap L_2}$ for $\#\,\mathrm{Gal}(L_2/L_1 \cap L_2)$ values of τ_2 in $\mathrm{Gal}(L_2/K)$.

Thus

$$\begin{aligned}
\#H &= \sum_{\tau_1 \in \mathrm{Gal}(L_1/K)} \#\{\tau_2 \in \mathrm{Gal}(L_2/K) : \tau_1|_{L_1\cap L_2} = \tau_2|_{L_1\cap L_2}\} \\
&= \#\,\mathrm{Gal}(L_1/K) \cdot \#\,\mathrm{Gal}(L_2/L_1\cap L_2) \\
&= [L_1 : K][L_2 : L_1 \cap L_2] \\
&= \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]} \\
&= [L_1L_2 : K] \text{ by Theorem 6.5} \\
&= \#\,\mathrm{Gal}(L_1L_2/K).
\end{aligned}$$

□

What this is saying is that if we have elements of $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$, as long as they are equal on $L_1 \cap L_2$ they extend together (uniquely) to an element of $\mathrm{Gal}(L_1L_2/K)$: there is one automorphism in $\mathrm{Gal}(L_1L_2/K)$ which restricts on L_1 and L_2 to our original choices.

Example 6.10. 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 understand 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

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

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

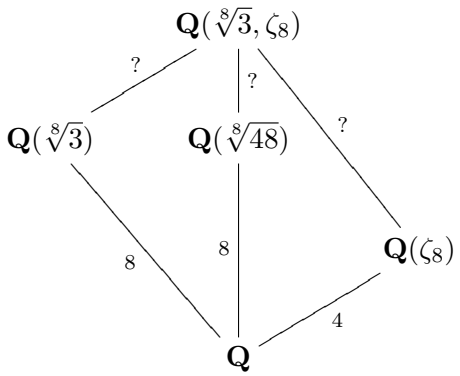
Example 6.11. As a substantial numerical application of Theorem 6.5, taking up the rest of this section, we will prove the fields $\mathbf{Q}(\sqrt[8]{3})$ and $\mathbf{Q}(\sqrt[8]{48})$ are not isomorphic by placing them in a common Galois extension of $\mathbf{Q}$ and showing the subgroups they correspond 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 $\sqrt[8]{48}$ is $X^8 - 48 = X^8 - 16 \cdot 3$. The splitting field of $X^8 - 3$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt[8]{3}, \zeta_8)$. Since $48 = 2^4 \cdot 3$, $\sqrt[8]{48} = \sqrt{2}\sqrt[8]{3}$. 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 $\mathbf{Q}(\sqrt[8]{3}, \zeta_8) = \mathbf{Q}(\sqrt[8]{48}, \zeta_8)$. This Galois extension of $\mathbf{Q}$ contains both $\mathbf{Q}(\sqrt[8]{3})$ and $\mathbf{Q}(\sqrt[8]{48})$.

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, we guess $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}] = 32$, but we should be cautious about this from our experience with $\mathbf{Q}(\sqrt[4]{2}, \zeta_8)$ in Example 1.4. To show the degree is 32, use Theorem 6.5 with $K = \mathbf{Q}$, $L = \mathbf{Q}(\zeta_8)$, and $L' = \mathbf{Q}(\sqrt[8]{3})$, which tells us

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

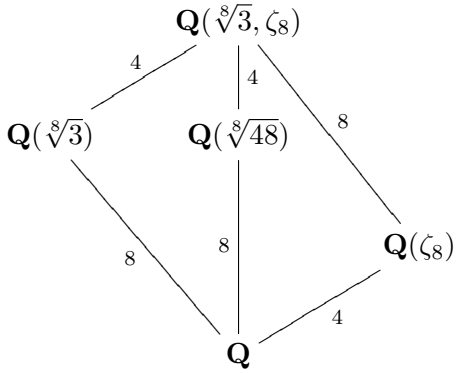
Therefore we want to show $\mathbf{Q}(\sqrt[8]{3}) \cap \mathbf{Q}(\zeta_8) = \mathbf{Q}$. The intersection is inside $\mathbf{R}$ since $\mathbf{Q}(\sqrt[8]{3}) \subset \mathbf{R}$, and the only real subfields of $\mathbf{Q}(\zeta_8)$ are $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{2})$, so if $\mathbf{Q}(\sqrt[8]{3}) \cap \mathbf{Q}(\zeta_8)$ 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 idea is to show the only quadratic subfield of $\mathbf{Q}(\sqrt[8]{3})$ is $\mathbf{Q}(\sqrt{3})$, because we know $\mathbf{Q}(\sqrt{2}) \neq \mathbf{Q}(\sqrt{3})$. That is left to you. What we will do instead is look at quartic subfields of $\mathbf{Q}(\sqrt[8]{3})$. 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.[2]

We adopt the method of Remark 1.3. 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

[2]There are methods from algebraic number theory which make it obvious that $\sqrt{2} \notin \mathbf{Q}(\sqrt[8]{3})$.

$b \in \mathbf{Z}/8\mathbf{Z}$, 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

$$\sigma_{a,b}(\zeta_8) = \zeta_8^a, \quad \sigma_{a,b}(\sqrt[8]{3}) = \zeta_8^b \sqrt[8]{3}. \tag{6.2}$$

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

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/8\mathbf{Z})^\times, \quad b \in \mathbf{Z}/8\mathbf{Z} \right\} \tag{6.3}$$

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 (6.3) 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 $\mathbf{Q}(\sqrt[8]{48})$, we are ready to show $\mathbf{Q}(\sqrt[8]{3}) \ncong \mathbf{Q}(\sqrt[8]{48})$ by showing their corresponding subgroups in $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$ are not conjugate.

In the matrix model (6.3) of $\mathrm{Gal}(\mathbf{Q}(\sqrt[8]{3}, \zeta_8)/\mathbf{Q})$, the subgroup fixing $\mathbf{Q}(\sqrt[8]{3})$ is

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/8\mathbf{Z})^\times \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix} \right\} \tag{6.4}$$

because every $\sigma_{a,0}$ fixes $\sqrt[8]{3}$ (set $b = 0$ in (6.2)), 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 $\mathbf{Q}(\sqrt[8]{48})$, we need to find the (a, b)-solutions to $\sigma_{a,b}(\sqrt[8]{48}) = \sqrt[8]{48}$. In terms of $\sqrt[8]{3}$ and ζ_8,

$$\sqrt[8]{48} = \sqrt{2}\sqrt[8]{3} = (\zeta_8 + \zeta_8^{-1})\sqrt[8]{3},$$

so

$$\sigma_{a,b}(\sqrt[8]{48}) = (\zeta_8^a + \zeta_8^{-a})\zeta_8^b \sqrt[8]{3}.$$

Therefore

$$\sigma_{a,b}(\sqrt[8]{48}) = \sqrt[8]{48} \iff (\zeta_8^a + \zeta_8^{-a})\zeta_8^b \sqrt[8]{3} = (\zeta_8 + \zeta_8^{-1})\sqrt[8]{3} \iff (\zeta_8^a + \zeta_8^{-a})\zeta_8^b = \zeta_8 + \zeta_8^{-1}.$$

The number of (a, b)-solutions is $[\mathbf{Q}(\sqrt[8]{3}, \zeta_8) : \mathbf{Q}(\sqrt[8]{48})] = 32/8 = 4$, 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 $\sqrt[8]{48}$ are

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pm 3 & 4 \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix} \right\}. \tag{6.5}$$

It remains to show that the mod 8 matrix groups (6.4) and (6.5) are not conjugate inside of (6.3). 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 (6.3) which conjugates (6.4) to (6.5). For any $a \in (\mathbf{Z}/8\mathbf{Z})^\times$,

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & (1-a)y \\ 0 & 1 \end{pmatrix}. \tag{6.6}$$

(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 (6.5) 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 (6.5) 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 (6.4) and (6.5) are nonconjugate subgroups in (6.3). (Each element of (6.4) can be conjugated within the group (6.3) to an element of (6.5), but there is not *one* element of the group (6.3) which conjugates all of (6.4) to (6.5).)

7. 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 7.1. *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 [13, 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. 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 7.2. The fields $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$ are both Galois over $\mathbf{Q}$ and their intersection is $\mathbf{Q}$, so Theroem 7.1 tells us $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$. We already saw that by Galois theory in Example 1.1.

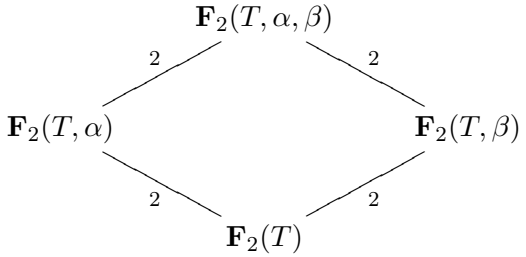
If we drop the Galois hypothesis in Theorem 7.1 completely, then the proof of Theorem 7.1 falls apart and the theorem need not be true anymore.

Example 7.3. 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 7.4. Let r and r' be two roots of $X^4 + 8X + 12$. From Example 4.32, 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 7.1 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 7.1 is valid in characteristic p as long as $[K(\alpha, \beta) : K] \not\equiv 0 \bmod p$. If the degree is a multiple of p then Theorem 7.1 has counterexamples.

Example 7.5. 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 7.1, $K(\alpha, \beta) \neq K(\alpha + \beta)$ 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 7.1 is Galois, the proof of the theorem no longer works but the theorem is still true! Isaacs [4] found that Theorem 7.1 is true when K has characteristic 0 with no Galois hypotheses at all, but a weaker hypothesis in its place:

Theorem 7.6. *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 [7, 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 7.6 is equivalent to $K(\alpha) \cap K(\beta) = K$ when one of $K(\alpha)$ or $K(\beta)$ is Galois over K (Theorem 6.5), so Theorem 7.1 is true when only one of $K(\alpha)$ or $K(\beta)$ is Galois over K.

Example 7.7. Theorem 7.6 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 7.8. 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 7.6 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 7.9. 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 7.6 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 7.10. Does $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2} + \zeta_8)$? Since $[\mathbf{Q}(\sqrt[4]{2}, \zeta_8) : \mathbf{Q}] = 8$ (by Example 1.4) and $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}][\mathbf{Q}(\zeta_8) : \mathbf{Q}] = 16$, we can't answer this with Theorem 7.6. Since $\mathbf{Q}(\sqrt[4]{2}, \zeta_8) = \mathbf{Q}(\sqrt[4]{2}, i)$, you can check the Galois orbit of $\sqrt[4]{2} + \zeta_8$ 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 7.6 is sufficient to imply $K(\alpha, \beta) = K(\alpha + \beta)$ in characteristic 0, but it is not necessary.

In [4] and [7], a version of Theorem 7.6 is proved in characteristic p under extra technical hypotheses. That some extra hypothesis is needed can be seen from Example 7.5; it has the degree hypothesis of Theorem 7.6 but not the conclusion.

8. 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 completely settled. It is known that every finite group is a Galois group over $\mathbf{C}(T)$, using complex analysis (Riemann surfaces).

If we leave the base field arbitrary, then every finite group is the Galois group of some field extension. This is a pretty use of Cayley's theorem embedding every finite group in some symmetric group.

Theorem 8.1. *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 8.1 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 classical polynomials (*e.g.*, the truncated exponential series $\sum_{k=0}^{n} X^k/k!$, has splitting field over $\mathbf{Q}$ with Galois group S_n unless $4|n$, when the Galois group is A_n). Towards the end of the 19th century, 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 [9].

It's worth emphasizing why Schur's realization of every S_n as a Galois group over $\mathbf{Q}$ does not settle the inverse Galois problem over $\mathbf{Q}$ even though every finite group is a subgroup of some symmetric group. The Galois correspondence goes backwards, so realizing a group as a Galois group over a field realizes its subgroups as Galois groups over intermediate fields (same top field, changing base field). It is the quotients of the Galois group that are realized as Galois groups over the base field. 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 every finite solvable group is a Galois group over $\mathbf{Q}$. (The proof had an error concerning the prime 2, but this was later repaired.) Most recent work on the inverse Galois problem has taken the 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 [14] (esp. Chapter 1) for a basic introduction to these ideas and [11] for a general survey.

As a nice conceptual (non-numerical) use of Theorem 6.5, let's lift the inverse Galois problem from $\mathbf{Q}$ to its finite extensions.

Theorem 8.2. *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 a finite extension $F/\mathbf{Q}$. We want to realize G as a Galois group over F. Following Example 6.6, 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 extension $L/\mathbf{Q}$ such that $G \cong \mathrm{Gal}(L/\mathbf{Q})$ and $L \cap F = \mathbf{Q}$.

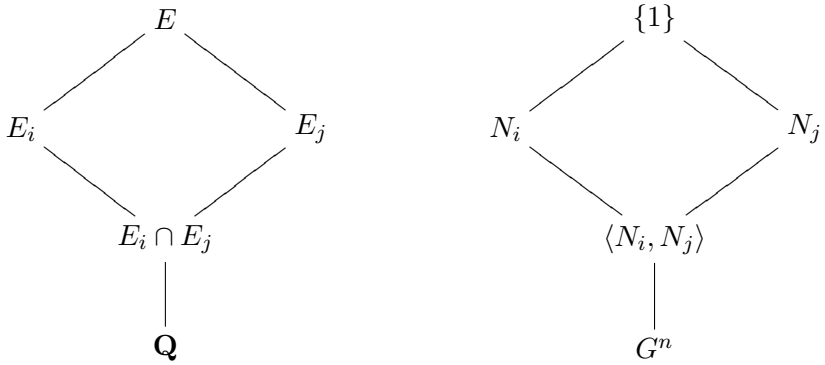
There are only finitely many fields between $\mathbf{Q}$ and F (including $\mathbf{Q}$ and F). Let the number of them be n. By hypothesis all finite groups are Galois groups over $\mathbf{Q}$, so in particular the n-fold product group G^n is a Galois group over $\mathbf{Q}$. Let $\mathrm{Gal}(E/\mathbf{Q}) \cong G^n$. 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 $E_1, \ldots, E_n$ intersects F in $\mathbf{Q}$. Then the composite of F with that E_i will realize 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 which 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 a 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 8.2 shows every finite group arises as a Galois group over F.

9. What Next?

There are two important aspects of field extensions which are missing by a study of Galois theory of finite extensions, and we briefly address them:

(1) Galois theory for infinite extensions
(2) transcendental extensions

A field extension L/K of infinite degree is called Galois when it is algebraic, separable, and normal. That 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 [8].) 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] D. Cox, "Galois Theory," Wiley, Hoboken, NJ, 2004.
[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] N. Jacobson, "Basic Algebra I," 2nd ed., Freeman, 1985.
[6] I. Kaplansky, "Fields and Rings," 2nd ed., Univ. of Chicago Press, Chicago, 1972.
[7] G. Karpilovsky, "Topics in Field Theory," North-Holland, Amsterdam, 1989.
[8] P. Morandi, "Field and Galois theory," Springer-Verlag, New York, 1996.
[9] H. Osada, *The Galois groups of the polynomials* $X^n + aX^l + b$, J. Number Theory **25** (1987), 230–238.
[10] P. Samuel, *Algebraic Theory of Numbers*, Dover, 2008.
[11] J-P. Serre, "Topics in Galois theory," Jones and Bartlett, Boston, MA, 1992.
[12] R. Swan, *Factorization of Polynomials over Finite Fields*, Pacific J. Math. **12** (1962), 1099–1106.
[13] S. Weintraub, "Galois Theory," Springer-Verlag, New York, 2005.
[14] H. Völklein, "Groups as Galois Groups – an Introduction," Cambridge Univ. Press, Cambridge, 1996.