THE GALOIS CORRESPONDENCE

KEITH CONRAD

1. Introduction

Let L/K be a field extension. A *K-automorphism* of L is a field automorphism $\sigma\colon L \to L$ which fixes the elements of K: $\sigma(c) = c$ for all $c \in K$. The set of K-automorphisms of L is a group under composition and is denoted $\mathrm{Aut}(L/K)$. Its identity element is the identity function on L. Studying properties of L/K through properties of the group $\mathrm{Aut}(L/K)$ is the basic theme of Galois theory.

Example 1.1. Two $\mathbf{R}$-automorphisms of $\mathbf{C}$ are the identity $z \mapsto z$ and complex conjugation $z \mapsto \overline{z}$. We will show they are the only ones. If $\sigma\colon \mathbf{C} \to \mathbf{C}$ is an $\mathbf{R}$-automorphism, then for any real a and b we have $\sigma(a+bi) = \sigma(a)+\sigma(b)\sigma(i) = a+b\sigma(i)$, so σ is determined by $\sigma(i)$ and

$$\begin{aligned} i^2 = -1 &\Longrightarrow \sigma(i^2) = \sigma(-1) \\ &\Longrightarrow \sigma(i)^2 = -1 \\ &\Longrightarrow \sigma(i) = \pm i. \end{aligned}$$

If $\sigma(i) = i$, then $\sigma(z) = z$ for all $z \in \mathbf{C}$ and if $\sigma(i) = -i$, then $\sigma(z) = \overline{z}$ for all $z \in \mathbf{C}$.

From any intermediate field $K \subset F \subset L$ we get a subgroup

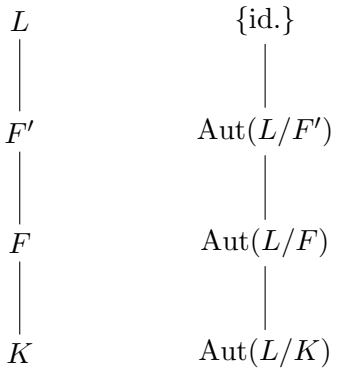
$$\mathrm{Aut}(L/F) = \{\sigma \in \mathrm{Aut}(L/K) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in F\} \tag{1.1}$$

in $\mathrm{Aut}(L/K)$. In the other direction, from any subgroup H of $\mathrm{Aut}(L/K)$ we get a field

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}, \tag{1.2}$$

which lies between K and L. (Check L^H really is a field.) Both (1.1) and (1.2) concern the equation $\sigma(\alpha) = \alpha$, but they quantify it in different ways, one over α and the other over σ.

The correspondences $F \rightsquigarrow \mathrm{Aut}(L/F)$ and $H \rightsquigarrow L^H$ between intermediate fields in the extension L/K and subgroups of $\mathrm{Aut}(L/K)$ is inclusion-reversing: if $F \subset F'$ then $\mathrm{Aut}(L/F') \subset \mathrm{Aut}(L/F)$, while if $H \subset H'$ then $L^{H'} \subset L^H$.



It is straightforward to check that

$$F \subset L^{\mathrm{Aut}(L/F)}, \quad H \subset \mathrm{Aut}(L/L^H). \tag{1.3}$$

That is, F is contained in the set of elements fixed by the automorphisms of L which fix F and H is contained in the set of automorphisms of L which fix the elements fixed by H. (This is practically a tautology, but you may need to read through that two times to see it.) What we are after is a description of those finite extensions L/K where the two inclusions in (1.3) become equalities for all intermediate fields F between K and L and all subgroups H of $\mathrm{Aut}(L/K)$, so the correspondences we have described between intermediate fields between K and L and subgroups of $\mathrm{Aut}(L/K)$ are inverses of each other. The description is due to Galois.

For instance, at a minimum we want the numbers fixed by all K-automorphisms of L to be just the elements of K: $L^{\mathrm{Aut}(L/K)} = K$. Equivalently, any element of L not in K should be moved by some K-automorphism of L.

Not every finite extension has this property. For instance, $\mathrm{Aut}(L/K)$ could be trivial with $[L : K] > 1$, so $L^{\mathrm{Aut}(L/K)} = L \neq K$. The following two examples of this possibility contain the *core* difficulties we want to avoid.

Example 1.2. The extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ has prime degree, so the only intermediate fields are $\mathbf{Q}$ and $\mathbf{Q}(\sqrt[3]{2})$. The group $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$ is trivial: if $\sigma \in \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$ then the equation $\sqrt[3]{2}^3 = 2$ implies $\sigma(\sqrt[3]{2})^3 = 2$ after applying σ to both sides, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ because $X^3 - 2$ has only one root in $\mathbf{Q}(\sqrt[3]{2})$. Since σ fixes $\mathbf{Q}$ pointwise and fixes $\sqrt[3]{2}$, it fixes every element of $\mathbf{Q}(\sqrt[3]{2})$.

Example 1.3. The extension $\mathbf{F}_p(u^{1/p})/\mathbf{F}_p(u)$ has prime degree, so the only intermediate fields are the top and bottom fields. The automorphism group is trivial, since $u^{1/p}$ is a root of the polynomial $X^p - u$ and this polynomial has only one root in characteristic p.

The problem in Example 1.2 is that $X^3 - 2$ has 3 roots in a splitting field over $\mathbf{Q}$ but the field $\mathbf{Q}(\sqrt[3]{2})$ is missing some of these roots. This difficulty will be avoided by restricting our attention to *normal* field extensions (to be defined later). Example 1.3 has a problem of a different sort: the polynomial $X^p - u$ has only one root at all in a splitting field. No matter how much we enlarge $\mathbf{F}_p(u^{1/p})$, $u^{1/p}$ will continue to be sent to itself by any $\mathbf{F}_p(u)$-automorphism even though $u^{1/p} \notin \mathbf{F}_p(u)$. The trouble here is connected with inseparability. We will eventually want to focus on *separable* extensions.

2. Field automorphisms and permutations of roots

Definition 2.1. The roots of a common irreducible polynomial in $K[X]$ are called K-*conjugates*.

Example 2.2. The numbers $\pm\sqrt{2}$ are $\mathbf{Q}$-conjugate since they both have minimal polynomial $X^2 - 2$ over $\mathbf{Q}$, but they are not $\mathbf{R}$-conjugate since $\sqrt{2}$ has minimal polynomial $X - \sqrt{2}$ and $-\sqrt{2}$ has minimal polynomial $X + \sqrt{2}$.

Example 2.3. In $\mathbf{C}$ the numbers i and $-i$ are $\mathbf{R}$-conjugates, as are (more generally) $a + bi$ and $a - bi$. The name "complex conjugate" should be "real conjugate" from this point of view, since $a + bi$ and $a - bi$ have the same minimal polynomial over $\mathbf{R}$, but not $\mathbf{C}$ (unless $b = 0$), but it's too late to change the name.

Theorem 2.4. *If $\sigma \in \mathrm{Aut}(L/K)$ and $f(X) \in K[X]$, then $\sigma(f(\alpha)) = f(\sigma(\alpha))$ for all $\alpha \in L$. In particular, a K-automorphism of L permutes the roots of $f(X)$ in L.*

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

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

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

Corollary 2.5. *The group $\mathrm{Aut}(L/K)$ permutes K-conjugates in L.*

Proof. Let $\alpha \in L$ have minimal polyomial $\pi(X)$ in $K[X]$. Apply Theorem 2.4 to the roots of $\pi(X)$ in L. □

Example 2.6. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. A K-automorphism of L sends $\sqrt{2}$ to $\sqrt{2}$ or $-\sqrt{2}$, because $\sqrt{2}$ has minimal polynomial $X^2 - 2 \in \mathbf{Q}[X]$, whose roots in L are $\pm\sqrt{2}$. A K-automorphism of L can't send $\sqrt{2}$ to $\sqrt{3}$, for instance, since $\sqrt{3}$ is not a root of $X^2 - 2$. While Corollary 2.5 puts a constraint on where a K-automorphism of L could send $\sqrt{2}$ (to roots of $X^2 - 2$), it does not assure us that all those options are in fact possible.

Example 2.7. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2})$. The field L contains $\sqrt{2} = \sqrt[4]{2}^2$, and a K-automorphism of L can only send $\sqrt{2}$ to $\pm\sqrt{2}$ by the same argument as in the previous example. But in fact it is impossible for a K-automorphism of L to send $\sqrt{2}$ to $-\sqrt{2}$.

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

Example 2.8. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[3]{2}, \omega)$, where ω is a nontrivial cube root of unity. The polynomial $X^3 - 2$ has 3 roots in L: $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. Any K-automorphism of L permutes these 3 roots. Are all six permutations of these 3 roots realized by K-automorphisms of L?

Example 2.9. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2}, i)$. The polynomial $X^4 - 2$ has all four roots in L: $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. These four roots have $4! = 24$ permutations. Is every permutation of these four numbers the restriction of some K-automorphism of L?

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

3. Bounding the automorphism group

For any finite extension L/K, we will show the group $\mathrm{Aut}(L/K)$ is finite and then try to bound its size.

Theorem 3.1. *For any finite extension L/K, the group $\mathrm{Aut}(L/K)$ is finite.*

Proof. Write $L = K(\alpha_1, \ldots, \alpha_n)$. Any $\sigma \in \mathrm{Aut}(L/K)$ is determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$, and $\sigma(\alpha_i)$ is restricted to lie among the finitely many K-conjugates of α_i in L. So each element of $\mathrm{Aut}(L/K)$ is determined by a finite amount of information, which makes the group $\mathrm{Aut}(L/K)$ finite. □

In the special case that L/K is a *splitting field*, we will show in Corollary 3.3 that $[L : K]$ is an upper bound on $\#\,\mathrm{Aut}(L/K)$. This will follow from a technical theorem on the number of ways to extend an isomorphism of fields to an isomorphism of splitting fields.

For any field homomorphism $\sigma\colon F \to F'$ and polynomial $f(X) = \sum_{i=0}^n c_i X^i \in F[X]$, set $(\sigma f)(X) = \sum_{i=0}^n \sigma(c_i)X^i \in F'[X]$. We call this map "applying σ to the coefficients." For $\alpha \in F$, $\sigma(f(\alpha)) = (\sigma f)(\sigma(\alpha))$. That is proved in the same way as Theorem 2.4, but unlike there the coefficients of $f(X)$ are not fixed by σ but get replaced by their σ-values. Applying σ to coefficients is a degree-preserving ring homomorphism from $F[X]$ to $F'[X]$: $\sigma(f+g) = \sigma f + \sigma g$ and $\sigma(fg) = (\sigma f)(\sigma g)$ for any f and g in $F[X]$, and trivially $\sigma(1) = 1$. If $f(X)$ splits completely in $F[X]$ then $(\sigma f)(X)$ splits completely in $F'[X]$ since linear factors gets sent to linear factors. We will be using all of this in the proof of the next theorem.

Theorem 3.2. *Let $\sigma\colon K \to K'$ be an isomorphism of fields, $f(X) \in K[X]$, L be a splitting field of $f(X)$ over K and L' be a splitting field of $(\sigma f)(X)$ over K'. Then $[L : K] = [L' : K']$, σ extends to an isomorphism $L \to L'$ and the number of such extensions is at most $[L : K]$.*

$$\begin{array}{ccc} L & \dashrightarrow & L' \\ | & & | \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Proof. (This proof is long, but it's a key result, so it's worth it.)

We argue by induction on $[L : K]$. If $[L : K] = 1$ then $f(X)$ splits completely in $K[X]$ so $(\sigma f)(X)$ splits completely in $K'[X]$. Therefore $L' = K'$, so $[L' : K'] = 1$. The only extension of σ to L in this case is σ.

Suppose $[L : K] > 1$. Since L is generated as a field over K by the roots of $f(X)$, $f(X)$ has a root $\alpha \in L$ which is not in K. Fix this α for the rest of the proof. Let $\pi(X)$ be the minimal polynomial of α over K, so α is a root of $\pi(X)$ and $\pi(X)|f(X)$ in $K[X]$. If there's going to be an isomorphism $\widetilde{\sigma}\colon L \to L'$ extending σ, then $\widetilde{\sigma}$ must send α to a root of $(\sigma\pi)(X)$:

$$\pi(\alpha) = 0 \Rightarrow \widetilde{\sigma}(\pi(\alpha)) = \widetilde{\sigma}(0) \Rightarrow (\widetilde{\sigma}\pi)(\widetilde{\sigma}(\alpha)) = 0 \Rightarrow (\sigma\pi)(\widetilde{\sigma}(\alpha)) = 0,$$

where the last step comes from $\pi(X)$ having coefficients in K (so $\widetilde{\sigma} = \sigma$ on those coefficients). So we know where the candidates for $\widetilde{\sigma}(\alpha)$ have to come from: roots of $(\sigma\pi)(X)$.

Now we show $(\sigma\pi)(X)$ has a root in L'. Since σ is an isomorphism from K to K', applying σ to coefficients is a ring isomorphism from $K[X]$ to $K'[X]$ (the inverse map is applying σ^{-1} to coefficients in $K'[X]$), so $\pi(X)|f(X) \Rightarrow (\sigma\pi)(X)|(\sigma f)(X)$. Since $\pi(X)$ is monic irreducible, $(\sigma\pi)(X)$ is also monic irreducible (a ring isomorphism preserves irreducibility). The polynomial $(\sigma f)(X)$ splits completely in $L'[X]$ by the definition of L', so its factor $(\sigma\pi)(X)$ also splits completely over L' and thus has a root in L'. Choose a root $\beta \in L'$ of $(\sigma\pi)(X)$. Set $d = \deg \pi(X) = \deg(\sigma\pi)(X)$, so $d > 1$ (because $d = [K(\alpha) : K] > 1$) and there are at most d choices for β. Consider the following field diagram, where the intermediate

fields have degree d since α and β have minimal polynomials $\pi(X)$ and $(\sigma\pi)(X)$ over K and K'.

$$\begin{array}{ccc} L & \dashrightarrow & L' \\ | & & | \\ K(\alpha) & \dashrightarrow & K'(\beta) \\ {\scriptstyle d}\,| & & |\,{\scriptstyle d} \\ K & \xrightarrow{\sigma} & K' \end{array}$$

To show there is a unique extension of σ to a field isomorphism $K(\alpha) \to K'(\beta)$ such that $\sigma(\alpha) = \beta$, first we handle uniqueness. If $\sigma' \colon K(\alpha) \to K'(\beta)$ extends σ and $\sigma'(\alpha) = \beta$, then the value of σ' is determined everywhere on $K(\alpha)$ because

$$\sigma'\left(\sum_{i=0}^{m} c_i \alpha^i\right) = \sum_{i=0}^{m} \sigma'(c_i)(\sigma'(\alpha))^i = \sum_{i=0}^{m} \sigma(c_i)\beta^i. \tag{3.1}$$

In other words, a K-polynomial in α has to go over to the corresponding K'-polynomial in β where σ is applied to the coefficients. So σ' is unique. To prove σ' exists, we will build an isomorphism from $K(\alpha)$ to $K'(\beta)$ with the help of the evaluation isomorphisms

$$K[X]/(\pi(X)) \cong K(\alpha) \quad \text{and} \quad K'[X]/((\sigma\pi)(X)) \cong K'(\beta) \tag{3.2}$$

that send X to α and to β. On the level of polynomial rings, the isomorphism $K[X] \to K'[X]$ that is σ on coefficients sends $\pi(X)$ to $(\sigma\pi)(X)$, so it identifies the ideals $(\pi(X))$ in $K[X]$ and $((\sigma\pi)(X))$ in $K'[X]$. Reducing $K[X]$ and $K'[X]$ modulo these ideals tells us

$$K[X]/(\pi(X)) \cong K'[X]/((\sigma\pi)(X)) \tag{3.3}$$

where $g(X) \bmod \pi(X) \mapsto (\sigma g)(X) \bmod (\sigma\pi)(X)$. Composition of the isomorphisms in (3.2) and (3.3) provides us with an isomorphism $K(\alpha) \to K'(\beta)$ which, by tracing through its construction, equals σ on K and sends α to β. So σ' exists and we place it in the field diagram below.

$$\begin{array}{ccc} L & \dashrightarrow & L' \\ | & & | \\ K(\alpha) & \xrightarrow{\sigma'} & K'(\beta) \\ {\scriptstyle d}\,| & & |\,{\scriptstyle d} \\ K & \xrightarrow{\sigma} & K' \end{array} \tag{3.4}$$

Now we can use induction on degrees of splitting fields by the trick of replacing the base fields K and K' with $K(\alpha)$ and $K'(\beta)$. Since L is a splitting field of $f(X)$ over K, it's also a splitting field of $f(X)$ over the larger field $K(\alpha)$. Similarly, L' is a splitting field of $(\sigma f)(X)$ over K' and thus also over $K'(\beta)$. Since $f(X)$ has its coefficients in K, $(\sigma' f)(X) = (\sigma f)(X)$. So the top square in (3.4) is similar to the square in the theorem (same polynomials and same splitting fields, with bigger base fields), except now the splitting field degrees have dropped: since $d > 1$,

$$[L : K(\alpha)] = \frac{[L : K]}{d} < [L : K].$$

By induction, $[L : K(\alpha)] = [L' : K'(\beta)]$ and σ' has an extension to a field isomorphism $L \to L'$. Since σ' extends σ, σ has an extension to an isomorphism $L \to L'$ and

$$[L : K] = [L : K(\alpha)]d = [L' : K'(\beta)]d = [L' : K'].$$

It remains to show σ has at most $[L : K]$ extensions to an isomorphism $L \to L'$. First we show every isomorphism $\widetilde{\sigma}\colon L \to L'$ extending σ arises as the extension of some intermediate isomorphism σ' of $K(\alpha)$ with a subfield of L'. From the start of the proof, $\widetilde{\sigma}(\alpha)$ has to be a root of $(\sigma\pi)(X)$. Define $\beta := \widetilde{\sigma}(\alpha)$. Since $\widetilde{\sigma}|_K = \sigma$, the restriction of $\widetilde{\sigma}$ to $K(\alpha)$ is a field homomorphism that is σ on K and sends α to β, so $\widetilde{\sigma}|_{K(\alpha)}$ is an isomorphism with image $K'(\widetilde{\sigma}(\alpha)) = K'(\beta)$. Therefore $\widetilde{\sigma}$ on L is a lift of the intermediate field isomorphism $\sigma' := \widetilde{\sigma}|_{K(\alpha)}$.

$$\begin{array}{ccc} L & \xrightarrow{\widetilde{\sigma}} & L' \\ | & & | \\ K(\alpha) & \xrightarrow{\sigma'} & K'(\beta) \\ {\scriptstyle d}\,| & & |\,{\scriptstyle d} \\ K & \xrightarrow{\sigma} & K' \end{array}$$

By induction on degrees of splitting fields, σ' lifts to at most $[L : K(\alpha)]$ isomorphisms $L \to L'$. Since σ' is determined by $\sigma'(\alpha)$, which is a root of $(\sigma\pi)(X)$, the number of maps σ' is at most $\deg(\sigma\pi)(X) = d$. The number of isomorphisms $L \to L'$ which lift σ is the number of maps σ' out of $K(\alpha)$ times the number of extensions of each σ' to an isomorphism $L \to L'$, and that total is at most $d[L : K(\alpha)] = [L : K]$. □

Here is the most important special case of Theorem 3.2.

Corollary 3.3. *If L is a splitting field over K of a polynomial in $K[X]$, then $\#\operatorname{Aut}(L/K) \leq [L : K]$.*

Proof. Apply Theorem 3.2 with $K' = K$, $L' = L$, and σ the identity function on K. Extensions of the identity function on K to isomorphisms $L \to L$ are precisely the elements of $\operatorname{Aut}(L/K)$. (Notice, incidentally, that to make the induction work in the proof of Theorem 3.2 we must allow a general isomorphism of base fields even if our main application of interest is the case $K = K'$ and σ equal to the identity on K.) □

Now we will add a separability assumption and get a stronger conclusion: the upper bound in Theorem 3.2 is reached.

Theorem 3.4. *Let $\sigma\colon K \to K'$ be an isomorphism of fields, $f(X) \in K[X]$, L be a splitting field of $f(X)$ over K and L' be a splitting field of $(\sigma f)(X)$ over K'. If $f(X)$ is separable then there are $[L : K]$ extensions of σ to an isomorphism $L \to L'$.*

Proof. The theorem is clear if $[L : K] = 1$, so we may assume $[L : K] > 1$. We maintain the same meaning for α, $\pi(X)$, and d as in the previous proof.

Because $f(X)$ is separable, $(\sigma f)(X)$ is separable too. One way to show this is with the characterization of separability in terms of relative primality to the derivative: we can write

$$f(X)u(X) + f'(X)v(X) = 1 \tag{3.5}$$

for some $u(X)$ and $v(X)$ in $K[X]$. Applying σ to coefficients commutes with forming derivatives (that is, $\sigma(f') = (\sigma f)'$), so if we apply σ to coefficients in (3.5) then we get

$$(\sigma f)(X)(\sigma u)(X) + (\sigma f)'(X)(\sigma v)(X) = 1,$$

so $(\sigma f)(X)$ and its derivative are relatively prime in $K'[X]$. This last polynomial identity proves $(\sigma f)(X)$ is separable. Any factor of a separable polynomial is separable, so $(\sigma\pi)(X)$ is separable and therefore has d roots in L' since it splits completely over L'.

From the proof of Theorem 3.2, the number of extensions of $\sigma\colon K \to K'$ to an isomorphism σ' of $K(\alpha)$ with a subfield of L' is the number of roots of $(\sigma\pi)(X)$ in L', so separability tells us the number of maps σ' is d (and not just at most d).

$$\begin{array}{ccc} L & \dashrightarrow & L' \\ | & & | \\ K(\alpha) & \xrightarrow{\sigma'} & K'(\beta) \\ {\scriptstyle d}\,| & & |\,{\scriptstyle d} \\ K & \xrightarrow{\sigma} & K' \end{array}$$

In the diagram above, $[L : K(\alpha)] < [L : K]$ and L is a splitting field of $f(X)$ over $K(\alpha)$, so by induction on the degree of a splitting field (along with the new separability hypothesis), σ' has $[L : K(\alpha)]$ extensions to an isomorphism $L \to L'$. Since there are d choices for σ', the total number of extensions of σ to an isomorphism $L \to L'$ is $d[L : K(\alpha)] = [L : K]$. □

Corollary 3.5. *If L/K is the splitting field of a separable polynomial then $\#\operatorname{Aut}(L/K) = [L : K]$.*

Proof. Apply Theorem 3.4 with $K' = K$, $L' = L$, and σ the identity function on K. □

Example 3.6. The extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$ is a splitting field of $(X^2 - 2)(X^2 - 3)$. Its degree is 4, so $\#\operatorname{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}) = 4$. We will use this *a priori* count to find all the automorphisms.

Since $\sqrt{2}$ and $\sqrt{3}$ generate the extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$, any $\sigma \in \operatorname{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$ is determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$, which are $\pm\sqrt{2}$ and $\pm\sqrt{3}$. Combining the choices in all possible ways, we get at most 4 choices for σ. See Table 1. Because general theory says there are 4 choices for σ, every possibility in Table 1 must work. Notice that we could not draw that conclusion without knowing in advance how many σ's 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

Example 3.7. The extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ has degree 4. It is not the splitting field of $X^4 - 2$. We will show the group $\operatorname{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ has order 2, which is smaller than the degree of the extension.

In Example 2.7 we saw that any $\mathbf{Q}$-automorphism of $\mathbf{Q}(\sqrt[4]{2})$ fixes $\sqrt{2}$, and therefore fixes every number in $\mathbf{Q}(\sqrt{2})$. So $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}) \subset \mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2}))$. The reverse inclusion is obvious (yes?), so $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}) = \mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2}))$. While $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ does not appear to be a splitting field, the quadratic extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})$ is a splitting field: it's the splitting field for $T^2 - \sqrt{2}$, with roots $\pm\sqrt[4]{2}$, so $\#\,\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})) = 2$. What are the two automorphisms? They're determined by where they send $\sqrt[4]{2}$, and this number can only go to $\pm\sqrt[4]{2}$ (the roots of $X^2 - \sqrt{2}$). Since these are just two possibilities, and we know there are two automorphisms, both choices work. Explicitly, the automorphism of $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ sending $\sqrt[4]{2}$ to $\sqrt[4]{2}$ is the identity and the automorphism of $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ sending $\sqrt[4]{2}$ to $-\sqrt[4]{2}$ has the formula $x + y\sqrt[4]{2} \mapsto x - y\sqrt[4]{2}$ with $x, y \in \mathbf{Q}(\sqrt{2})$.

We're interested in those finite extensions L/K where

$$\#\,\mathrm{Aut}(L/K) = [L : K]. \tag{3.6}$$

Corollary 3.5 says this happens if L is the splitting field over K of a separable polynomial. It is a significant fact that the converse is true as well

Theorem 3.8. *If L/K is a finite extension and $\#\,\mathrm{Aut}(L/K) = [L : K]$ then*

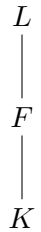
1. $L^{\mathrm{Aut}(L/K)} = K$,
2. *L/K is separable (that is, every number in L has a separable minimal polynomial in $K[X]$),*
3. *for $\alpha \in L$, its K-conjugates are $\sigma(\alpha)$ as σ runs over $\mathrm{Aut}(L/K)$,*
4. *every irreducible polynomial in $K[X]$ with a root in L splits in $L[X]$,*
5. *L is the splitting field over K of a separable polynomial.*

Proof. First we show (5) is a consequence of (2) and (4). Write $L = K(\alpha_1, \ldots, \alpha_n)$ and let $\pi_i(X)$ be the minimal polynomial of α_i in $K[X]$. By (2), each $\pi_i(X)$ is separable in $K[X]$. By (4), each $\pi_i(X)$ splits completely over L since $\pi_i(X)$ has a root α_i in L. Therefore L is a splitting field over K of the product of the $\pi_i(X)$'s *without repetition*, and that product is separable.

Now we turn to the proof of the first four conditions. Set

$$F = L^{\mathrm{Aut}(L/K)},$$

so F consists of the elements of L which are fixed by $\mathrm{Aut}(L/K)$. Eventually we will see $F = K$, but for now we can just say this is a field between K and L.



Since $K \subset F \subset L$, $\mathrm{Aut}(L/F) \subset \mathrm{Aut}(L/K)$. Any element of $\mathrm{Aut}(L/K)$ fixes each element of F by the definition of F, so $\mathrm{Aut}(L/K) \subset \mathrm{Aut}(L/F)$. Therefore $\mathrm{Aut}(L/K) = \mathrm{Aut}(L/F)$, so (by definition) $L^{\mathrm{Aut}(L/F)} = F$. In other words, we've proved (1) with F in place of K. We are going to prove (2), (3), and (4) with F in place of K, and only then will we prove $F = K$ (part (1)), after which we get (2), (3), and (4) as in the theorem using K.

To show L/F is separable, pick any $\alpha \in L$. We are going to directly write down a separable polynomial in $F[X]$ with α as a root. Let $\{\sigma(\alpha) : \sigma \in \mathrm{Aut}(L/F)\}$ have distinct members $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. (For example, if $\alpha \in F$ then this set has one term in it even though $\mathrm{Aut}(L/F)$ could be large.) We will show the polynomial with these *different* roots,

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

is in $F[X]$; note it is separable by construction. Why are the coefficients of $h_\alpha(X)$ in F? For any $\sigma \in \mathrm{Aut}(L/F)$, each $\sigma(\sigma_i(\alpha)) = (\sigma\sigma_i)(\alpha)$ is some $\sigma_j(\alpha)$ by the definition of $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. So σ sends this finite set back to itself. It does so injectively, so it must do so surjectively too. Therefore applying σ to coefficients, which is a ring automorphism of $L[X]$, sends $h_\alpha(X)$ to

$$\prod_{i=1}^{m}(X - \sigma(\sigma_i(\alpha))) = \prod_{j=1}^{m}(X - \sigma_j(\alpha)) = h_\alpha(X).$$

Thus $h_\alpha(X) \in L^{\mathrm{Aut}(L/F)}[X] = F[X]$.

Next we show $h_\alpha(X)$ is the minimal polynomial of α in $F[X]$. Suppose $f(X) \in F[X]$ has α as a root. We will show $h_\alpha(X)|f(X)$. For any $\sigma \in \mathrm{Aut}(L/F)$, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so $f(X)$ is divisible by $X - \sigma(\alpha)$. Running over the *distinct* values of $\sigma(\alpha)$ shows $f(X)$ is divisible by their product $h_\alpha(X)$, so $h_\alpha(X)$ is the minimal polynomial of α in $F[X]$. From the definition of $h_\alpha(X)$ and its minimality, the F-conjugates of α are $\sigma(\alpha)$ as σ runs over $\mathrm{Aut}(L/F)$, which is (3) with F in place of K.

To show any irreducible $\pi(X) \in F[X]$ with a root in L splits in $L[X]$, let $\gamma \in L$ be a root of $\pi(X)$. Since $\pi(X)$ is irreducible over F, it is the minimal polynomial of γ in $F[X]$, so by our previous construction of minimal polynomials we have $\pi(X) = h_\gamma(X)$. From the definition of $h_\gamma(X)$, this polynomial splits completely in $L[X]$.

So far we have proved (2), (3), and (4) with F in place of K. The reasoning at the start of the proof that (2) and (4) imply (5) shows, with F in place of K, that L is a splitting field over F of a separable polynomial. Therefore $\#\,\mathrm{Aut}(L/F) = [L : F]$ by Corollary 3.5. Since $\mathrm{Aut}(L/K) = \mathrm{Aut}(L/F)$ and by hypothesis $\#\,\mathrm{Aut}(L/K) = [L : K]$, we have $[L : K] = [L : F]$. Since $K \subset F \subset L$, the degree formula implies $F = K$. Now (1), (2), (3), and (4) are true for K, so we're done. □

Condition (4) in Theorem 3.8 has a name.

Definition 3.9. An algebraic extension L/K is called *normal* if any irreducible in $K[X]$ with a root in L splits completely in $L[X]$.

Example 3.10. Any quadratic extension, separable or not (*e.g.*, even in characteristic 2) is normal. If $[L : K] = 2$ then any element of L has a minimal polynomial in $K[X]$ of degree 1 or 2, so only monic irreducibles in $K[X]$ of degree 1 or 2 could have a root in L. Skipping over the trivial linear case, if $X^2 + bX + c \in K[X]$ has the root $r \in L$, so $r^2 + br + c = 0$, then

$$X^2 + bX + c = (X - r)(X + b + r).$$

Therefore this polynomial has a full set of roots in L: r and $-b - r$.

By Theorem 3.8, if $\#\,\mathrm{Aut}(L/K) = [L : K]$ then L/K is normal because the minimal polynomial of any $\alpha \in L$ over K is $h_\alpha(X)$, which splits completely over L by its definition.

Corollary 3.5 tells us now that *the splitting field of a separable polynomial is a normal extension.*

Example 3.11. The extensions $\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q}$, $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$, and $\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}$ are normal since $\mathbf{Q}(\sqrt[3]{2},\omega)$ is a splitting field over $\mathbf{Q}$ of X^3-2, $\mathbf{Q}(\sqrt[4]{2},i)$ is a splitting field over $\mathbf{Q}$ of X^4-2, and $\mathbf{Q}(\sqrt{2},\sqrt{3})$ is a splitting field over $\mathbf{Q}$ of $(X^2-2)(X^2-3)$. That is, for any number in one of the fields $\mathbf{Q}(\sqrt[3]{2},\omega)$, $\mathbf{Q}(\sqrt[4]{2},i)$, or $\mathbf{Q}(\sqrt{2},\sqrt{3})$, all of its $\mathbf{Q}$-conjugates are also in the field.

Example 3.12. The extensions $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ are *not* normal: X^3-2 and X^4-2 are irreducible in $\mathbf{Q}[X]$ and they have no multiple roots, but X^3-2 has only one root in $\mathbf{Q}(\sqrt[3]{2})$ and X^4-2 has only two roots in $\mathbf{Q}(\sqrt[4]{2})$.

Since an irreducible polynomial in $K[X]$ with a root in L is the minimal polynomial over K of that root, L/K is normal if and only if for each $\alpha \in L$ the minimal polynomial of α over K splits completely in $L[X]$.

The following theorem, which we will not need, lets us recognize normal extensions in practice. The proof will use the theorem that symmetric polynomials are polynomials in the elementary symmetric functions.

Theorem 3.13. *For a finite extension L/K, the following are equivalent:*

(1) *L/K is normal,*
(2) *L is the splitting field over K of a polynomial in $K[X]$.*

Proof. To show (1) implies (2), write $L = K(\alpha_1,\dots,\alpha_r) = K[\alpha_1,\dots,\alpha_r]$ and let $f_i(X) \in K[X]$ be the minimal polynomial of α_i in $K[X]$. Since L/K is normal, each $f_i(X)$ splits completely in $L[X]$ (because it has a root in L). Therefore L is a splitting field over K of $f_1(X)\cdots f_r(X)$.

To show (2) implies (1) we will use the symmetric function theorem: every symmetric polynomial in n variables with coefficients in K is a polynomial in the elementary symmetric functions of those n variables with coefficients in K. Let $\pi(X) \in K[X]$ be irreducible with a root in L, say α. We want to show $\pi(X)$ splits completely over L. We are going to show $\pi(X)$ is a factor of a polynomial in $K[X]$ which splits completely over L, so $\pi(X)$ splits completely over L.

From (2), there is a polynomial $f(X) \in K[X]$ for which L is a splitting field. Let $n = \deg f(X)$ and factor $f(X)$ in $L[X]$ as $(X-\beta_1)\cdots(X-\beta_n)$. Write $\alpha = g(\beta_1,\dots,\beta_n)$ for a polynomial $g(X_1,\dots,X_n) \in K[X_1,\dots,X_n]$. Now consider the polynomial whose roots are g evaluated at all permutations of the β_i's:

$$h(X) = \prod_{\sigma\in S_n} (X - g(\beta_{\sigma(1)},\dots,\beta_{\sigma(n)}))$$

This has the factor $X-\alpha$, so $h(\alpha) = 0$. By construction, the coefficients of $h(X)$ are symmetric polynomials in $\beta_1,\dots,\beta_n$ with coefficients in K. Therefore the coefficients of $h(X)$ are polynomials in the elementary symmetric functions of $\beta_1,\dots,\beta_n$ with coefficients in K. Those elementary symmetric functions are the coefficients of $f(X)$ (up to sign) and thus lie in K, so $h(X) \in K[X]$. Since $h(\alpha) = 0$, $h(X)$ is divisible by the minimal polynomial of α in $K[X]$, which is $\pi(X)$. Since $\pi(X)|h(X)$ and $h(X)$ splits completely in $L[X]$, also $\pi(X)$ splits completely in $L[X]$. □

It should not be expected that the polynomial $h(X)$ constructed in the proof will be the minimal polynomial of α over K since it has degree $n!$, which is not sensitive to the choice

of α. (In fact, $h(X)$ will be the minimal polynomial only if $K(\alpha) = L$ and $[L : K] = n!$. In particular, if $K(\alpha) \neq L$ then $h(X)$ is not the minimal polynomial.)

Example 3.14. The splitting field of $X^4 - 2$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt[4]{2}, i)$, so Theorem 3.13 tells us $\mathbf{Q}(\sqrt[4]{2}, i)$ is a normal extension of $\mathbf{Q}$. We will use the method of proof of the theorem to find a monic polynomial in $\mathbf{Q}[X]$ with root $\alpha = (1+i)\sqrt[4]{2}$. First we have to write α in terms of the roots of $X^4 - 2$. Set

$$\beta_1 = \sqrt[4]{2}, \quad \beta_2 = -\sqrt[4]{2}, \quad \beta_3 = i\sqrt[4]{2}, \quad \beta_4 = -i\sqrt[4]{2}.$$

Then $\alpha = \sqrt[4]{2} + i\sqrt[4]{2} = \beta_1 + \beta_3$. A monic polynomial in $\mathbf{Q}[X]$ with root α is

$$h(X) = \prod_{\sigma \in S_4} (X - (\beta_{\sigma(1)} + \beta_{\sigma(3)})).$$

The degree of this polynomial is 24, while $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}] = 8$, so $h(X)$ is definitely not going to be the minimal polynomial and you really don't want to compute $h(X)$ by hand.

There is an *ad hoc* trick in this case that gets us a polynomial over $\mathbf{Q}$ with root α of smaller degree. Since $\alpha^2 = (2i)\sqrt{2}$, $\alpha^4 = -8$, so α is a root of $X^4 + 8$. And it turns out that $h(X) = (X^4 + 8)^6$.

Example 3.15. For u transcendental over $\mathbf{F}_p$, the extension $\mathbf{F}_p(u^{1/p})/\mathbf{F}_p(u)$ of degree p is normal since $\mathbf{F}_p(u^{1/p})$ is a splitting field over $\mathbf{F}_p(u)$ of $X^p - u$.

4. Galois extensions

In Section 3 we saw that a finite extension L/K satisfying $\#\operatorname{Aut}(L/K) = [L : K]$ also satisfies further conditions: $L^{\operatorname{Aut}(L/K)} = K$ and L/K is both separable and normal. With no new work, it turns out these properties are all equivalent to each other.

Theorem 4.1. *For a finite extension L/K, the following are equivalent:*

(a) $\#\operatorname{Aut}(L/K) = [L : K]$,
(b) $L^{\operatorname{Aut}(L/K)} = K$,
(c) *L/K is separable and normal,*
(d) *L is the splitting field over K of a separable polynomial in $K[X]$.*

Proof. That (a) implies (b) was shown in the proof of Theorem 3.8. Also in the proof of Theorem 3.8, we showed the condition $L^{\operatorname{Aut}(L/F)} = F$ implies L/F is separable and normal using the $h_\alpha(X)$ construction. If we make the hypothesis that $L^{\operatorname{Aut}(L/K)} = K$, then running through that same argument with K in place of F shows (b) implies (c). The first paragraph of the proof of Theorem 3.8 shows (c) implies (d). Corollary 3.5 says (d) implies (a). □

Theorem 4.1 implies a sharper form of the inequality in Corollary 3.3, which is applicable to all finite extensions (not just splitting fields).

Corollary 4.2. *If L/K is any finite extension then $\#\operatorname{Aut}(L/K) | [L : K]$.*

Proof. Since L/K is finite, $\operatorname{Aut}(L/K)$ is a finite group by Theorem 3.1. Let $F = L^{\operatorname{Aut}(L/K)}$. Then $\operatorname{Aut}(L/K) = \operatorname{Aut}(L/F)$, so $F = L^{\operatorname{Aut}(L/F)}$. By Theorem 4.1, $\#\operatorname{Aut}(L/F) = [L : F]$, so $\#Aut(L/K) = [L : F]$, which is a factor of $[L : K]$. □

Corollary 4.3. *If L/K is a finite extension which is either inseparable or not normal then $\#\operatorname{Aut}(L/K) < [L : K]$.*

Proof. By Corollary 4.2, $\#\operatorname{Aut}(L/K) \leq [L:K]$. From Theorem 4.1, if L/K is inseparable or not normal then $\#\operatorname{Aut}(L/K) \neq [L:K]$, so $\#\operatorname{Aut}(L/K) < [L:K]$. □

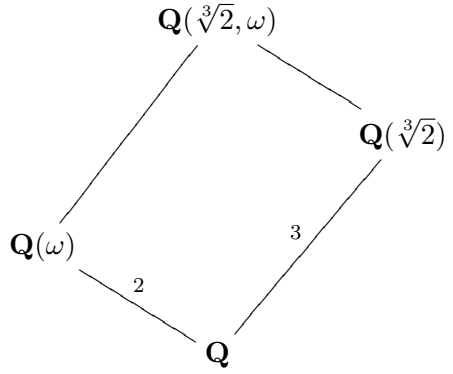
Corollary 4.3 explains why the inequality $\#\operatorname{Aut}(\mathbf{F}_p(u^{1/p})/\mathbf{F}_p(u)) < [\mathbf{F}_p(u^{1/p}) : \mathbf{F}_p(u)]$ from Example 1.3 can't be turned into an equality by enlarging the top field $\mathbf{F}_p(u^{1/p})$. The inseparability of $u^{1/p}$ over $\mathbf{F}_p(u)$ is a fatal obstruction.

Definition 4.4. A finite extension L/K is called *Galois* when it satisfies the equivalent properties of Theorem 4.1. When L/K is a Galois extension, the group $\operatorname{Aut}(L/K)$ is denoted $\operatorname{Gal}(L/K)$ and is called the *Galois group* of the extension.

For a finite Galois extension L/K, Theorem 4.1 tells us $\#\operatorname{Gal}(L/K) = [L:K]$ and $L^{\operatorname{Gal}(L/K)} = K$.

Example 4.5. Any quadratic extension L/K outside of characteristic 2 is Galois. Indeed, by completing the square we can write $L = K(\sqrt{d})$ for some nonsquare $d \in K^\times$, and $X^2 - d$ is separable outside characteristic 2. Thus L is a splitting field over K for $X^2 - d$. The Galois group has size 2, so it has one non-identity automorphism. An automorphism in $\operatorname{Gal}(K(\sqrt{d})/K)$ is determined by its value $\pm\sqrt{d}$ on $\sqrt{d}$. The nontrivial element of $\operatorname{Gal}(L/K)$ is frequently called the conjugation of L. For example, the elements of $\operatorname{Gal}(\mathbf{C}/\mathbf{R})$ are the identity and complex conjugation.

Example 4.6. The field $\mathbf{Q}(\sqrt[3]{2}, \omega)$ is a splitting field over $\mathbf{Q}$ for $X^3 - 2$, which is separable since any irreducible in $\mathbf{Q}[X]$ is separable. So $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is a Galois extension. By Theorem 4.1, the number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ is $[\mathbf{Q}(\sqrt[3]{2}, \omega) : \mathbf{Q}] = 6$. (For comparison, recall from Example 1.2 that the number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is 1, even though the field extension has degree 3: there is just nowhere for $\sqrt[3]{2}$ to go in $\mathbf{Q}(\sqrt[3]{2})$ except to itself.) We will give two ways to think about $\operatorname{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$.



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

For another viewpoint, any σ in the Galois group is determined by the two values $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ and $\sigma(\omega) \in \{\omega, \omega^2\}$. Therefore there are at most $3 \cdot 2 = 6$ possibilities for

σ. Since 6 is the number of automorphisms, all of these possibilities really work: any choice of a root of $X^3 - 2$ for $\sigma(\sqrt[3]{2})$ and a nontrivial cube root of unity for $\sigma(\omega)$ does come from an automorphism σ. Write $\sigma(\omega) = \omega^{a_\sigma}$ where $a_\sigma \in (\mathbf{Z}/(3))^\times$ and $\sigma(\sqrt[3]{2}) = \omega^{b_\sigma}\sqrt[3]{2}$ where $b_\sigma \in \mathbf{Z}/(3)$. For two automorphisms σ and τ,

$$\sigma(\tau(\omega)) = \sigma(\omega^{a_\tau}) = \sigma(\omega)^{a_\tau} = \omega^{a_\sigma a_\tau}$$

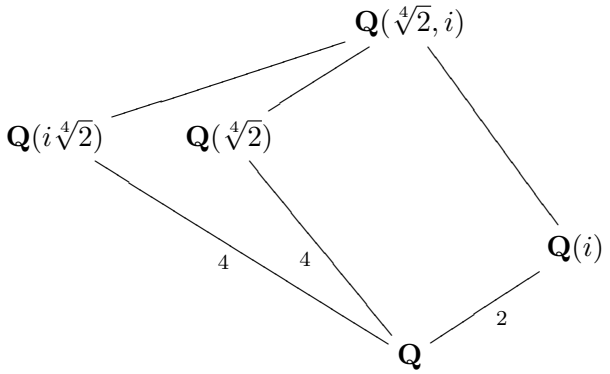
and

$$\sigma(\tau(\sqrt[3]{2})) = \sigma(\omega^{b_\tau}\sqrt[3]{2}) = \sigma(\omega)^{b_\tau}\sigma(\sqrt[3]{2}) = \omega^{a_\sigma b_\tau}\omega^{b_\sigma}\sqrt[3]{2} = \omega^{a_\sigma b_\tau + b_\sigma}\sqrt[3]{2}.$$

Looking at the exponents of ω on the right side of these two equations, composition of σ and τ behaves like multiplication of invertible matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with entries in $\mathbf{Z}/(3)$, since $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa' & ab'+b \\ 0 & 1 \end{smallmatrix}\right)$. So $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$ is isomorphic to the group $\mathrm{Aff}(\mathbf{Z}/(3))$ of mod 3 invertible matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ by $\sigma \mapsto \left(\begin{smallmatrix} a_\sigma & b_\sigma \\ 0 & 1 \end{smallmatrix}\right)$.

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

Example 4.7. The extension $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ is Galois by the same reasoning as in the previous example: the top field is the splitting field over $\mathbf{Q}$ for X^4-2, which is separable. The diagram below shows some of the intermediate fields, but these are not all the intermediate fields. For instance, $\mathbf{Q}(\sqrt{2})$ is inside $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$. (This is not the only missing subfield.)



Although any element of $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ permutes the 4 roots of $X^4 - 2$, not all 24 permutations of the roots are realized by the Galois group. (This is a contrast to $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$.) For example, $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ add to 0, so under a field automorphism these two roots go to roots which are also negatives of each other. No field automorphism of $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ could send $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ and $-\sqrt[4]{2}$ to $\sqrt[4]{2}$ because that doesn't respect the algebraic relation $x + y = 0$ which holds for $x = \sqrt[4]{2}$ and $y = -\sqrt[4]{2}$.

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

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

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

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

TABLE 2

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

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

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

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

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

Theorem 4.8. *Every finite separable extension of a field can be enlarged to a finite Galois extension of the field. In particular, any finite extension of a field with characteristic* 0 *can be enlarged to a finite Galois extension.*

Proof. Write the extension as $K(\alpha_1, \ldots, \alpha_n)/K$ where each α_i is separable over K. The product of the different minimal polynomials for the α_i's is a separable polynomial in $K[X]$. Enlarging $K(\alpha_1, \ldots, \alpha_n)$ to a splitting field of this polynomial over K is a Galois extension of K by Theorem 4.1. □

Example 4.9. The non-Galois extensions $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ live inside the Galois extensions $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ and $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$.

Corollary 4.10. *A finite inseparable extension can not be extended to a finite Galois extension.*

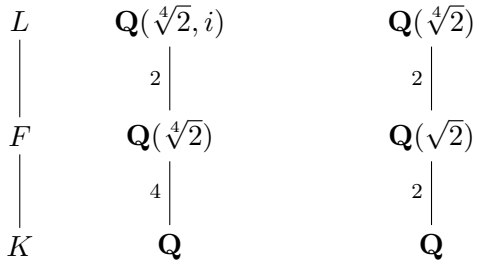
Proof. Any element of a Galois extension is separable over the base field. □

In the remainder of this section we tabulate some properties of Galois extensions.

Theorem 4.11. *If L/K is a finite Galois extension and $L \supset F \supset K$ then L/F is a Galois extension.*

Proof. We will use the characterization of Galois extensions as separable normal extensions. When $L \supset F \supset K$, separability and normality are both preserved in the passage from L/K to L/F because the minimal polynomial over F of any element of L divides its minimal polynomial over K. □

Remark 4.12. The bottom part of the tower F/K *need not* be Galois when L/K is, and moreover if L/F and F/K are Galois the extension L/K need not be Galois. These are illustrated by the two towers in the diagrams below.

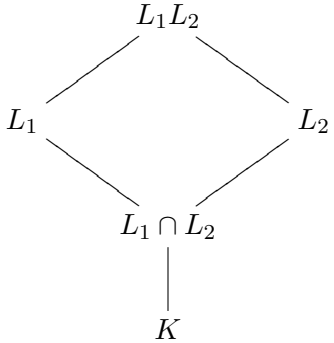


In the tower on the right, each pair of successive field extensions is quadratic (and thus Galois) but the overall extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ is not Galois. We have to enlarge $\mathbf{Q}(\sqrt[4]{2})$ further to $\mathbf{Q}(\sqrt[4]{2}, i)$ to get a Galois extension of the base field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

It is an important issue to decide when an intermediate field is Galois over the base. We will do that as part of the fundamental theorem of Galois theory in Section 5.

Theorem 4.13. *If L_1 and L_2 are finite Galois extensions of K inside a common field then L_1L_2 and $L_1 \cap L_2$ are both finite Galois extensions of K.*

Proof. By Theorem 4.1, L_1 and L_2 are both splitting fields for a separable polynomial in $K[X]$. Then L_1L_2 is a splitting field for the product of the two polynomials with common factors used only once. This polynomial is separable, so L_1L_2/K is Galois.



To show $L_1 \cap L_2$ is Galois over K we take the viewpoint that Galois extensions are separable normal extensions. Every element of L_1 is separable over K, so the subfield $L_1 \cap L_2$ is separable over K. To show $L_1 \cap L_2$ is normal over K, pick $\alpha \in L_1 \cap L_2$. It has a full set of K-conjugates in L_1 and in L_2 since each of these are normal extensions of K. These two sets of K-conjugates are the same, since otherwise the minimal polynomial of

α in $K[X]$ has more roots in L_1L_2 than its degree. Therefore the K-conjugates of α lie in $L_1 \cap L_2$. □

The property $L^{\mathrm{Aut}(L/K)} = K$ characterizes Galois extensions of K among the *finite* extensions of K, by Theorem 4.1. But there are many field extensions L/K of infinite degree where $L^{\mathrm{Aut}(L/K)} = K$. First there are infinite Galois extensions of K. There are also transcendental (*i.e.*, non-algebraic) extensions of K with this property. An example is a rational function field $L = K(u)$. It can be shown that the group $\mathrm{Aut}(K(u)/K)$ consists of all linear-fractional substitutions $f(u) \mapsto f((au+b)/(cu+d))$ where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. (Scaling a, b, c, d by a common $\lambda \in K^\times$ defines the same substitution, so the group $\mathrm{Aut}(K(u)/K)$ is isomorphic to $\mathrm{GL}_2(K)/K^\times$ rather than to $\mathrm{GL}_2(K)$.) Further examples of this situation arise in algebraic geometry.

5. The fundamental theorem

So far we have looked at the passage from a finite extension field L/K to the finite group $\mathrm{Aut}(L/K)$. When L is a splitting field over K of a polynomial in $K[X]$ then $\#\,\mathrm{Aut}(L/K) \leq [L:K]$ (Corollary 3.3). Now we go the other way, from a group of automorphisms of a field to field extension. Let E be a field and H be a *finite* group of automorphisms of E. Then

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

is a subfield of E.

Example 5.1. Let $E = \mathbf{C}$ and $H = \{\mathrm{id}, c\}$, where $c(z) = \overline{z}$ is complex-conjugation. Then $E^H = \mathbf{R}$.

Theorem 5.2 (Artin)**.** *Let E be a field and H be a finite group of automorphisms of E. If $[E : E^H]$ is finite then E/E^H is a Galois extension and* $\mathrm{Gal}(E/E^H) = H$.

Proof. First we show E/E^H is a separable extension, by an idea already used in the proof of Theorem 3.8. Pick any $\alpha \in E$. Let the finite set $\{\sigma(\alpha) : \sigma \in H\}$ be listed according to its *distinct* elements as

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

Clearly α is a root of $h_\alpha(X) = \prod_{i=1}^m (X - \sigma_i(\alpha))$, and the roots of this polynomial are distinct and all lie in E. The degree of $h_\alpha(X)$ is $m \leq \#H$. The coefficients of $h_\alpha(X)$ all lie in E^H by the same reasoning used in the proof of Theorem 3.8 to show $h_\alpha(X)$ there has coefficients in $L^{\mathrm{Aut}(L/K)}$, so E/E^H is an algebraic extension which is separable over E^H (that is, every element of E has a minimal polynomial in $E^H[X]$ which is separable) and each $\alpha \in E$ has degree at most $\#H$ over E^H.

So far we have not used the hypothesis that $[E : E^H]$ is finite. Now we do. Since E/E^H is a finite separable extension of degree at most $\#H$, by the primitive element theorem $E = E^H(\alpha)$ for some α, so $[E : E^H] = [E^H(\alpha) : E^H] \leq \deg h_\alpha(X) \leq \#H$. Since $h_\alpha(X)$ splits over E, E/E^H is a Galois extension (Theorem 4.1d), so $\#\,\mathrm{Gal}(E/E^H) = [E : E^H] \leq \#H$. Since H is a subgroup of $\mathrm{Gal}(E/E^H)$, $\#H \leq \#\,\mathrm{Gal}(E/E^H)$, so we get equality throughout:

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

Thus $\mathrm{Gal}(E/E^H) = H$. □

The finiteness hypothesis on $[E : E^H]$ in Theorem 5.2 is actually automatic.

Theorem 5.3 (Artin)**.** *Let E be a field and H be a finite group of automorphisms of E. The extension E/E^H is finite.*

Proof. From the first part of the proof of Theorem 5.2, where finiteness of $[E : E^H]$ is not used, every element of E is separable over E^H with bounded degree (at most $\#H$), so there is an $\alpha \in E$ such that $[E^H(\alpha) : E^H]$ is maximal. We are going to show $E = E^H(\alpha)$. For any $\beta \in E$, $E^H(\alpha) \subset E^H(\alpha, \beta) \subset E$. Since $E^H(\alpha, \beta)$ is a finite separable extension of E^H, by the primitive element theorem $E^H(\alpha, \beta) = E^H(\gamma)$ for some γ. Then $[E^H(\alpha) : E^H] \leq [E^H(\gamma) : E^H]$, and this inequality must be an equality because of the maximality defining $[E^H(\alpha) : E^H]$. Hence $E^H(\alpha) = E^H(\alpha, \beta)$ (one field is inside the other and they have the same degree over E^H), which implies $\beta \in E^H(\alpha)$. This holds for all $\beta \in E$, so $E = E^H(\alpha)$. Therefore $[E : E^H] = [E^H(\alpha) : E^H] < \infty$. □

We will use Theorem 5.2 once: in the proof of Theorem 5.6. Finiteness of $[E : E^H]$ in that application will be known in advance, so Theorem 5.3 is not needed in our development of Galois theory. (However, it is useful to understand some examples in Galois theory.)

Remark 5.4. The proof of Theorem 5.3 showed: if E/F is separable and every element of E has bounded degree over F then $[E : F] < \infty$. This can *fail* if E/F is inseparable. Consider $E = \mathbf{F}_p(u_1^{1/p}, u_2^{1/p}, \dots)$, with independent indeterminates $u_1, u_2, \dots$, as an extension of $F = \mathbf{F}_p(u_1, u_2, \dots)$. We have $[E : F] = \infty$, but every $\alpha \in E$ satisfies $\alpha^p \in F$, so $[F(\alpha) : F] \leq p$ for all $\alpha \in E$.

Remark 5.5. The proof of Theorems 5.2 and 5.3 in [1, pp. 569–571] and [3, pp. 220-222] is different from the one here (which is based on [2, pp. 263-264]). The proofs in [1] and [3] involve solving systems of linear equations.

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

Theorem 5.6 (Galois)**.** *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then the inclusion-reversing mappings $F \rightsquigarrow \mathrm{Gal}(L/F)$ and $H \rightsquigarrow L^H$ between the intermediate fields between K and L and the subgroups of G are inverses of each other and satisfy the following properties when F and H correspond ($F = L^H, H = \mathrm{Gal}(L/F)$):*

(a) *$\#H = [L : F]$ and $[F : K] = [G : H]$,*
(b) *two intermediate fields F and F', with corresponding subgroups H and H', are isomorphic over K if and only if H and H' are conjugate subgroups of G; in particular, $\mathrm{Gal}(L/\sigma(F)) = \sigma\mathrm{Gal}(L/F)\sigma^{-1}$ for $\sigma \in G$,*
(c) *F/K is Galois if and only if $H \lhd G$, in which case the restriction map $G \to \mathrm{Gal}(F/K)$, where $\sigma \mapsto \sigma|_F$, is surjective with kernel H, so $G/H \cong \mathrm{Gal}(F/K)$.*

In (5.1) we indicate the relations of part a in a diagram, where $F = L^H$ and $H = \mathrm{Gal}(L/F)$ correspond to each other. Because inclusion relations are reversed, the group diagram appears upside-down, with the larger subgroups near the bottom (having a fixed field which is closer to K).

$$\begin{array}{ccc} L & & \{1\} \\ | & & |_{[L:F]} \\ F & & H \\ | & & |_{[F:K]} \\ K & & G \end{array} \tag{5.1}$$

Part c explains why normal field extensions get their name: in the context of a finite Galois extension L/K, where every intermediate field is separable over the base field, the intermediate fields which are normal (equivalently, Galois) over the base are those whose corresponding subgroups in $\mathrm{Gal}(L/K)$ are normal subgroups.

Proof. First we check the correspondences are inverses: going from fields to subgroups to fields, we need $F^{\mathrm{Gal}(L/F)} = F$, and going from subgroups to fields to subgroups requires $\mathrm{Gal}(L/L^H) = H$. The first equality follows from Theorems 4.1 and 4.11 (L/F is Galois) and the second equality comes from Theorem 5.2. (We know in advance that L/L^H is finite since $K \subset L^H \subset L$ and $[L : K] < \infty$.)

For (a), since F and H correspond we have $F = L^H$, so $\#H = [L : F]$ by Theorem 5.2. The other equality in (a) follows from this: $[G : H] = \#G/\#H = [L : K]/[L : F] = [F : K]$.

For (b), first we observe that two intermediate fields F and F' are K-isomorphic if and only if $F' = \sigma(F)$ for some $\sigma \in G$. Indeed, if $F' = \sigma(F)$ for some $\sigma \in G$ then σ is a K-isomorphism from F to F'. Conversely, if F and F' are K-isomorphic let $\varphi\colon F \to F'$ be a K-isomorphism. We want to show φ, which is defined on F, is the restriction to F of some $\sigma \in G$. By the primitive element theorem, $F = K(\gamma)$ for some γ, so $K \subset F(\varphi(\gamma)) \subset F'$. Since φ fixes K, $\varphi(\gamma) \in F'$ has the same minimal polynomial over K as γ, so γ and $\varphi(\gamma)$ have the same degree over F, which means $F' = F(\varphi(\gamma))$ since $[F : K] = [F' : K]$. Since $\varphi(\gamma)$ is a K-conjugate of γ in L, by Theorem 3.8 we have $\varphi(\gamma) = \sigma(\gamma)$ for some $\sigma \in G$. Since σ and φ agree on K and on γ, they agree on $K(\gamma) = F$. That proves $\sigma|_F = \varphi$, so $F' = \varphi(F) = \sigma(F)$. Let's look at an example for a moment to see what this is saying.

Example 5.7. For the extension $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$, whose Galois group was worked out in Example 4.7, the intermediate fields $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$ are isomorphic over $\mathbf{Q}$ since each is the adjuncation to $\mathbf{Q}$ of one root of $X^4 - 2$. There is a $\mathbf{Q}$-isomorphism $\varphi\colon \mathbf{Q}(\sqrt[4]{2}) \to \mathbf{Q}(i\sqrt[4]{2})$ where $\varphi(\sqrt[4]{2}) = i\sqrt[4]{2}$. Some $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ restricts to φ on $\mathbf{Q}(\sqrt[4]{2})$. What is it? Using the notation of Example 4.7, $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, so r is one choice for σ. Another choice is rs, since $rs(\sqrt[4]{2}) = r(\sqrt[4]{2}) = i\sqrt[4]{2}$.

Returning to the proof of Theorem 5.6b, write any K-isomorphic copy of F in L as $\sigma(F)$ for some $\sigma \in G$. For any $\tau \in G$,

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

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

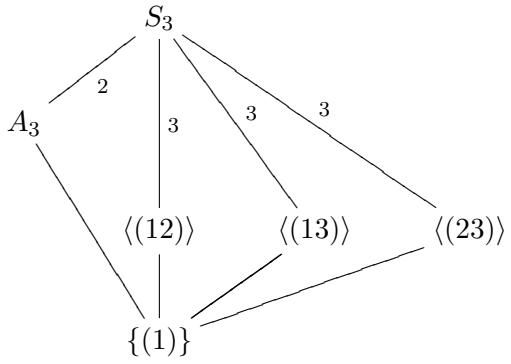
To prove (c), note that an intermediate extension F/K is automatically separable since every element of a Galois extension is separable over the base field K. Therefore F/K is Galois if and only if F/K is normal. Since F is inside the Galois extension L/K, the K-conjugates of any element of F are its orbit under $\mathrm{Gal}(L/K)$ (Theorem 3.8). Therefore F/K is normal if and only if $\sigma(F) \subset F$ for all $\sigma \in G$. Since $\sigma(F)$ and F have the same degree over K, the inclusion $\sigma(F) \subset F$ is the same as $\sigma(F) = F$. Therefore

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

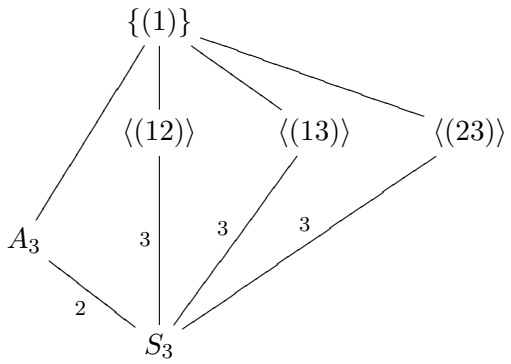
Restricting elements in $\mathrm{Gal}(L/K)$ to F defines a map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ which is a group homomorphism (check). Its kernel is $\mathrm{Gal}(L/F) = H$, so we get an embedding $G/H \hookrightarrow \mathrm{Gal}(F/K)$. The size of G/H is $[G : H] = [F : K]$, which equals $\#\,\mathrm{Gal}(F/K)$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

The bijection in Theorem 5.6 is called the *Galois correspondence*. Only for finite *Galois* extensions does it hold. Why? Because the special case $L^{\mathrm{Aut}(L/K)} = K$ of the correspondence is a property in Theorem 4.1 characterizing Galois extensions among finite extensions.

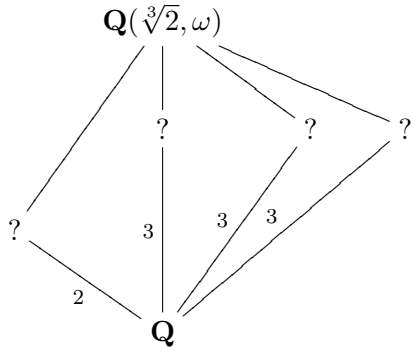
Example 5.8. The extension $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ has Galois group isomorphic to S_3 (Example 4.6). This group has 3 subgroups of order 2 and one subgroup (just A_3) of order 3. In the diagram we have indicated the indices in S_3 of subgroups.



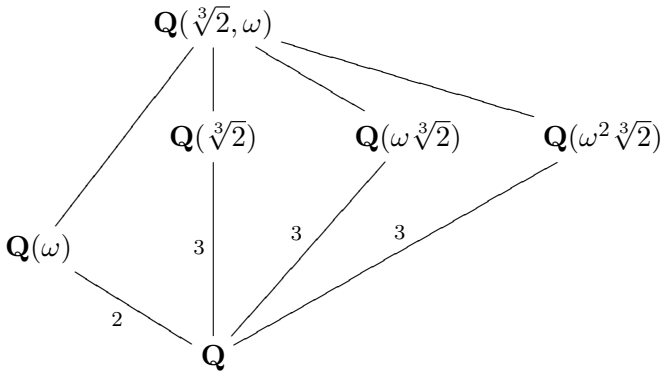
Let's flip this upside down, so larger groups are on the bottom.



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

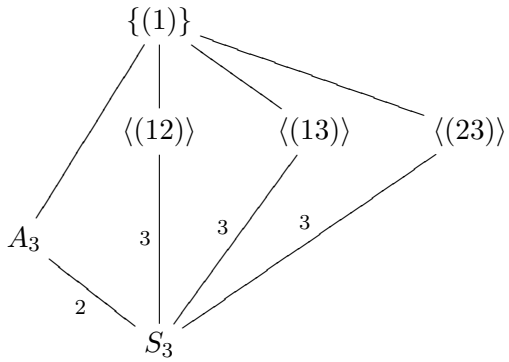


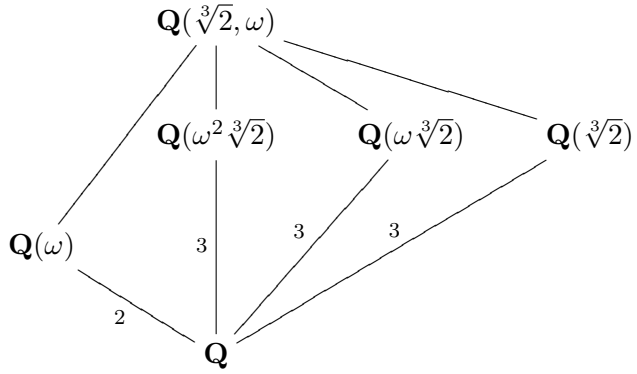
So there is one quadratic subfield and three cubic subfields. It is easy to write down enough such fields by inspection: $\mathbf{Q}(\omega)$ is quadratic and $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(\omega\sqrt[3]{2})$, and $\mathbf{Q}(\omega^2\sqrt[3]{2})$ are all cubic. (These three cubic fields are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



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

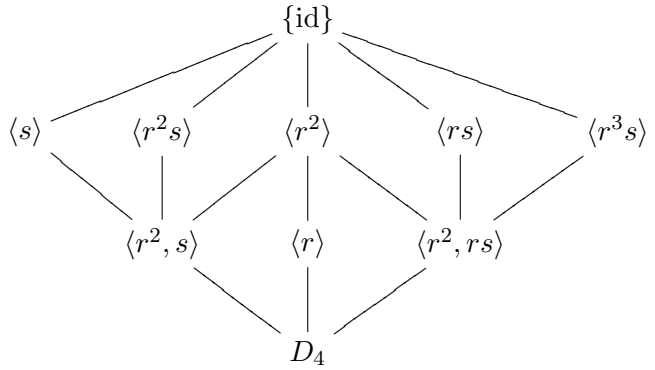
We were somewhat cavalier about the way we just wrote down the cubic fields without really paying attention to which ones should correspond to which subgroups of index 3 (order 2) in the Galois group. But we can't be more careful at this stage (beyond keeping track of indices of subgroups and degrees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



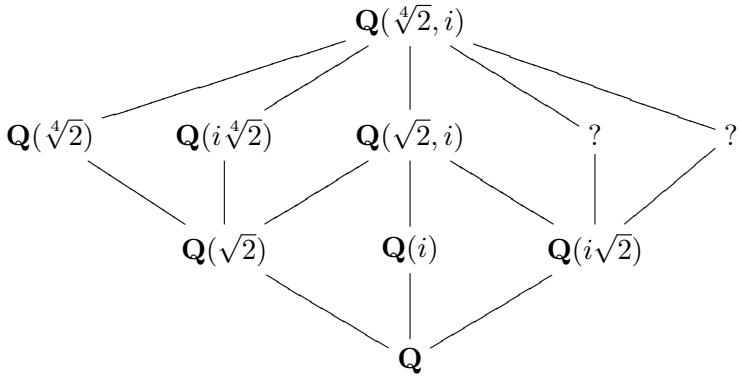


Example 5.9. The extension $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ has Galois group isomorphic to D_4 according to the permutations which the Galois group induces on the fourth roots of 2. Generators are r and s where $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, $r(i) = i$ and $s(\sqrt[4]{2}) = \sqrt[4]{2}$, $s(i) = -i$ (s is complex conjugation). See Table 2 in Example 4.7.

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



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



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

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

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

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

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

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

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

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

so

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

Therefore

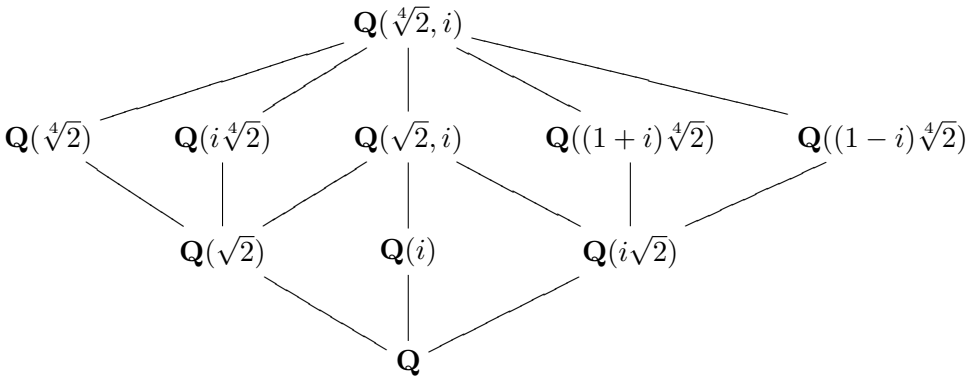
$$\alpha = a + b(\sqrt[4]{2} + i\sqrt[4]{2}) + d(\sqrt[4]{2}^3 - i\sqrt[4]{2}^3) + gi\sqrt{2}.$$

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

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

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

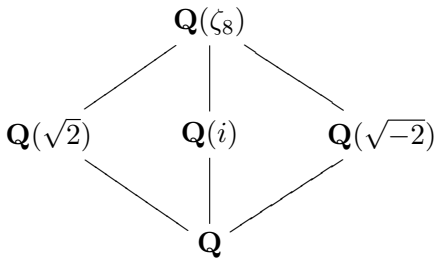
of $\langle r^3 s\rangle$ is $(1-i)\sqrt[4]{2}$. Now we have a complete field diagram.



Example 5.10. Let $\zeta_8 = e^{2\pi i/8}$ be a root of unity of order 8. The field $\mathbf{Q}(\zeta_8)$ is Galois over $\mathbf{Q}$, being the splitting field of $X^8 - 1$. We will use the Galois correspondence to find all the fields between $\mathbf{Q}$ and $\mathbf{Q}(\zeta_8)$.

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

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



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

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

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

Example 5.11. Let F be any field and $T_1, \ldots, T_n$ be indeterminates over F. The T_i's are roots of the polynomial

$$(X - T_1)(X - T_2)\cdots(X - T_n) = X^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n, \tag{5.2}$$

where

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

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

Let $K = F(s_1, \ldots, s_n)$, so $K \subset L^{S_n} \subset L$. Thus $[L : K] \geq [L : L^{S_n}] = \#S_n = n!$. At the same time, the T_i's are all roots of the same degree n polynomial (5.2) in $K[X]$, so L/K is a splitting field of a polynomial of degree n, which means $[L : K] \leq n!$. Hence $[L : K] = n! = [L : L^{S_n}]$, which forces $L^{S_n} = K$: every symmetric rational function in $T_1, \ldots, T_n$ over F is a rational function of the elementary symmetric functions $s_1, \ldots, s_n$.

Here are two theorems which follow from the Galois correspondence.

Theorem 5.12. *Let L/K be a finite Galois extension and F and F' be K-isomorphic intermediate fields corresponding to H and H' in $\mathrm{Gal}(L/K)$. The K-isomorphisms from F to F' in $\mathrm{Gal}(L/K)$ are the restrictions $\sigma|_F$ where $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\sigma H \sigma^{-1} = H'$.*

Proof. In the proof of Theorem 5.6b, we showed any K-isomorphism $\varphi\colon F \to F'$ can be extended to some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma H \sigma^{-1} = H'$. Then $\varphi = \sigma|_F$.

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

Theorem 5.12 says σ conjugates H to H' if and only if it maps F to F', which should be simple to remember.

Theorem 5.13. *Let L/K be finite Galois and F and F' be intermediate fields with corresponding subgroups H and H'.*

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

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

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

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

6. Primitive Elements

Galois theory provides a method to prove a number is a primitive element in a Galois extension.

Theorem 6.1. *When L/K is a finite Galois extension and $\gamma \in L$, the degree $[K(\gamma) : K]$ is the size of the Galois orbit of γ. In particular, γ is a primitive element for L/K if and only if $\#\{\sigma(\gamma) : \sigma \in \mathrm{Gal}(L/K)\} = [L : K]$.*

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

Example 6.2. In $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$, $\sqrt[4]{2} + i$ has 8 different values under the Galois group (see Table 3), since i, $\sqrt[4]{2}$, and $i\sqrt[4]{2}$ are linearly independent over $\mathbf{Q}$. (They are part of a $\mathbf{Q}$-basis for the field extension.) Thus $\mathbf{Q}(\sqrt[4]{2}, i) = \mathbf{Q}(\sqrt[4]{2} + i)$.

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

TABLE 3

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

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

TABLE 4

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

Example 6.3. Let F be any field and $T_1, \ldots, T_n$ be indeterminates over F. Let $L = F(T_1, \ldots, T_n)$, on which S_n acts by permutations of $T_1, \ldots, T_n$. From Example 5.11, the fixed field for S_n is $K = F(s_1, \ldots, s_n)$, where the s_i's are the elementary symmetric polynomials in the T_i's.

The extension L/K must have a primitive element, and here is an explicit choice: $T_1T_2^2\cdots T_n^n$. To show this works, we take our cue from Theorem 6.1 and look at the S_n-orbit. For any $\sigma \in S_n$,

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

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

References

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