22. Galois theory

The main result here is that inside nice [1] finite-degree field extensions L of k, the intermediate fields K are in (inclusion-reversing) bijection with subgroups H of the **Galois group**

$$G = \mathrm{Gal}(L/k) = \mathrm{Aut}(L/k)$$

of *automorphisms* of L over k, by

$$\text{subgroup } H \leftrightarrow \text{ subfield } K \text{ fixed by } H$$

This is depicted as

$$G\left\{\begin{array}{c} \left.\begin{array}{c} L \\ | \\ K \end{array}\right\} H \\ | \\ k \end{array}\right.$$

For K the fixed field of subgroup H there is the equality

$$[L:K] = |H|$$

Further, if H is a *normal* subgroup of G, then

$$\mathrm{Gal}(K/k) \approx G/H$$

[1] Namely **Galois** field extensions, which are by definition both **separable** and **normal**, defined momentarily.

In the course of proving these things we also elaborate upon the situations in which these ideas apply.

Galois' original motivation for this study was solution of equations in radicals (roots), but by now that classical problem is of much less importance than the general structure revealed by these results.

Also, notice that much of our earlier discussion of finite fields, cyclotomic polynomials, and roots of unity amounted to explicit examples of the statements here. In fact, there are few computationally accessible examples beyond those we have already discussed.

This whole discussion is more technical than the previous examples, but this is not surprising, considering the scope.

1. *Field extensions, imbeddings, automorphisms*

A more flexible viewpoint on field extensions, imbeddings, and automorphisms will be useful in what follows. Some of this is review.

A **field extension** K of a given field k is a field which is a k-algebra. That is, in addition to being a field, K is a k-module, *and* with the commutativity property

$$\xi(\alpha\cdot\eta) \;=\; \alpha\cdot(\xi\,\eta) \qquad\qquad \text{(for } \alpha\in k \text{ and } \xi,\eta\in K)$$

and with the *unital* property

$$1_k\cdot\xi \;=\; \xi \qquad\qquad \text{(for all } \xi\in K)$$

Note that the unital-ness promises that the map

$$\alpha\longrightarrow\alpha\cdot 1_K$$

gives an isomorphism of k to a subfield of K. Thus, when convenient, we may identify k with a subfield of K. However, it would be inconvenient if we did not have the flexibility to treat field extensions of k as k-algebras in this sense.

A field K is *algebraically closed* if, for every polynomial $f(x)\in K[x]$ of positive degree n, the equation $f(x)=0$ has n roots in K.

An *algebraic closure* $\overline{k}$ of a field k is an algebraically closed field extension $\overline{k}$ of k such that every element of $\overline{k}$ is *algebraic* over k. We proved that algebraic closures exist, and are essentially unique, in the sense that, for two algebraic closures K_1 and K_2 of k, there is a field isomorphism $\sigma: K_1\longrightarrow K_2$ which is the identity map on k.

It is immediate from the definition that an algebraic closure $\overline{k}$ of a field k is an algebraic closure of any intermediate field $k\subset K\subset\overline{k}$.

As a matter of traditional terminology, when K and L are field extensions of k and $\varphi: K\longrightarrow L$ is a k-algebra map, we may also say that $\varphi: K\longrightarrow L$ is a field map *over* k.

Next, for an irreducible $f(x)\in k[x]$, and for β a root of $f(x)=0$ in a field extension K of k, there is a k-algebra map $k(\alpha)\longrightarrow K$ such that $\sigma\alpha=\beta$. To prove this, first note that, by the universal property of $k[x]$, there is a unique k-algebra homomorphism $k[x]\longrightarrow\overline{k}$ sending x to β. The kernel is the ideal generated by the minimal polynomial of β, which is $f(x)$. That is, this map factors through $k[x]/f$, which isomorphic to $k(\alpha)$.

In particular, an algebraic extension $k(\alpha)$ of k can be imbedded by a k-algebra map into an algebraic closure $\overline{k}$ of k in at least one way. In fact, for each root β of $f(x)=0$ in $\overline{k}$, there is a k-algebra homomorphism $k(\alpha)\longrightarrow\overline{k}$ sending α to β. Conversely, any β in $\overline{k}$ which is the image $\sigma\alpha$ of α under a k-algebra homomorphism σ must be a root of $f(x)=0$: compute

$$f(\beta)=f(\sigma\alpha)=\sigma\Big(f(\alpha)\Big)=\sigma(0)=0$$

As a corollary of this last discussion, we see that any k-algebra automorphism of $k(\alpha)$ must send α to another root of its minimal polynomial over k, of which there are at most

$$\deg f \;=\; [k(\alpha):k]$$

An induction based on the previous observations will show that any *finite* (hence, algebraic) field extension K of k admits at least one k-algebra homomorphism $\sigma : K \longrightarrow \overline{k}$ to a given algebraic closure $\overline{k}$ of k. [2] This is proven as follows. Using the finiteness of K over k, there are finitely-many elements $\alpha_1, \ldots, \alpha_n$ in K such that

$$K \;=\; k(\alpha_1, \alpha_2, \ldots, \alpha_n) \;=\; k(\alpha_1)(\alpha_2)\ldots(\alpha_n)$$

Then there is a k-algebra imbedding of $k(\alpha_1)$ into $\overline{k}$. Classically, one would say that we will *identify* $k(\alpha_1)$ with its image by this map. It is better to say that we give K a $\sigma(k(\alpha_1))$-algebra structure by

$$\sigma(\beta)\cdot\xi \;=\; \beta\cdot\xi \qquad\qquad (\text{for } \beta\in k(\alpha_1) \text{ and } \xi \in K)$$

Since $\overline{k}$ is an algebraic closure of $\sigma k(\alpha_1)$, the same principle shows that there is a $k(\alpha_1)$-linear field homomorphism of $k(\alpha_1, \alpha_2)$ to $\overline{k}$. Continuing inductively, we obtain a field homomorphism of K to $\overline{k}$.

Then a similar argument proves that, given a finite extension L of a finite extension K of k, any k-algebra imbedding of K into an algebraic closure $\overline{k}$ *extends* to an imbedding of L into $\overline{k}$. To see this, let $\sigma : K \longrightarrow \overline{k}$ be given. View the finite field extension L of K as a finite field extension of σK as indicated above. Since $\overline{k}$ is also an algebraic closure of K, there is at least one K-algebra imbedding of L into $\overline{k}$.

2. *Separable field extensions*

The notion of *separability* of a field extension has several useful equivalent formulations. We will rarely be interested in non-separable field extensions. Happily, in characteristic 0, *all* extensions are separable (see below). Also, even in positive characteristic, all finite extensions of *finite* fields are separable. That is, for our purposes, non-separable field extensions are a pathology that we can avoid. Indeed, the results of this section can be viewed as proving that we can avoid non-separable extensions by very mild precautions.

A finite (hence, algebraic) field extension K of k is **separable** if the number of (nonzero) field maps

$$\sigma : K \longrightarrow \overline{k}$$

of K to an algebraic closure $\overline{k}$ of k is equal to the degree $[K:k]$.

[2.0.1] **Proposition:** Let $k(\alpha)$ be a field extension of k with α a zero of an irreducible monic polynomial f in $k[x]$. Then $k(\alpha)$ is separable over k if and only if f has no repeated factors. [3]

Proof: As noted much earlier, the only possible images of α in $\overline{k}$ are zeros of the irreducible polynomial $f(x)$ of α over k, since

$$f(\sigma\alpha) = \sigma\big(f(\alpha)\big) = \sigma(0) = 0$$

because σ is a field homomorphism fixing the field k, in which the coefficients of f lie. We have already seen that

$$[k(\alpha):k] \;=\; \deg f$$

[2] In fact, *any* algebraic extension K of k imbeds into an algebraic closure of k, but the proof requires some equivalent of the Axiom of Choice, such as Well-Ordering, or Zorn's Lemma.

[3] In many examples one easily tests for repeated factors by computing the *gcd* of f and its derivative.

regardless of separability. Thus, there are *at most* $[k(\alpha) : k]$ imbeddings of $k(\alpha)$ into $\overline{k}$. If the roots are *not* distinct, then there are strictly fewer than $[k(\alpha) : k]$ imbeddings into $\overline{k}$.

We recall the earlier argument that every root β of $f(x) = 0$ in $\overline{k}$ can be hit by some imbedding of $k(\alpha)$. Because the polynomial ring $k[x]$ is the free k-algebra on one generator, there is a homomorphism

$$\sigma_o : k[x] \longrightarrow \overline{k}$$

sending x to β and the identity on k. The kernel is the ideal generated by the minimal polynomial of β over k, which is f. Thus, this homomorphism factors through the quotient $k(\alpha) \approx k[x]/f$. ///

[2.0.2] **Example:** The simplest example of a *non*-separable extension is $\mathbb{F}_p(t^{1/p})$ over $\mathbb{F}_p(t)$, where $\mathbb{F}_p$ is the field with p elements and t is an indeterminate. The minimal polynomial for $\alpha = t^{1/p}$ is

$$x^p - t = (x - t^{1/p})^p$$

It is reasonable to view this as an avoidable pathology.

Now we give an iterated version of the first proposition:

[2.0.3] **Proposition:** A finite field extension $k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of k is separable if and only each intermediate extension

$$k(\alpha_1, \alpha_2, \ldots, \alpha_i) \;/\; k(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$$

is separable.

Proof: The notation means to consider the large field as obtained by repeatedly adjoining single elements:

$$k(\alpha_1, \alpha_2, \ldots, \alpha_n) = k(\alpha_1)(\alpha_2)\ldots(\alpha_n)$$

Let

$$[k(\alpha_1, \ldots, \alpha_i) \;:\; k(\alpha_1, \ldots, \alpha_{i-1})] \;=\; d_i$$

Since degrees multiply in towers,

$$[K : k] = d_1 \cdot_2 \cdot \ldots \cdot d_n$$

An imbedding of K into an algebraic closure $\overline{k}$ of k can be given by first imbedding $k(\alpha_1)$, then extending this to an imbedding of $k(\alpha_1, \alpha_2)$, and so on, noting that an algebraic closure of k is an algebraic closure of any of these finite extensions. There are at most d_1, d_2, $\ldots$, d_n such imbeddings at the respective stages, with equality achieved if and only if the intermediate extension is separable. ///

Now a version which de-emphasizes elements:

[2.0.4] **Proposition:** If K is a finite separable extension of k and L is a finite separable extension of K, then L is a finite separable extension of k.

Proof: By the finiteness, we can write

$$K = k(\alpha_1, \ldots, \alpha_m)$$

By the separability assumption on K/k, by the previous proposition, each intermediate extension

$$k(\alpha_1, \ldots, \alpha_i) \;/\; k(\alpha_1, \ldots, \alpha_{i-1})$$

is separable. Further, write

$$L = k(\alpha_1, \ldots, \alpha_m, \alpha_{n+1}, \ldots, \alpha_{m+n})$$

The separability hypothesis on K/L and the previous proposition imply that all the further intermediate extensions are separable. Then apply the previous proposition in the opposite order to see that L/k is separable. ///

[2.0.5] **Proposition:** If K and L are finite separable extensions of k inside a fixed algebraic closure $\overline{k}$ of k, then their compositum KL (inside $\overline{k}$) is a finite separable extension of k.

Proof: By the previous proposition, it suffices to prove that the compositum KL is separable over K. Let $L = k(\beta_1, \ldots, \beta_n)$. By the second proposition, the separability of L/k implies that all the intermediate extensions

$$k(\beta_1, \ldots, \beta_i) \;/\; k(\beta_1, \ldots, \beta_{i-1})$$

are separable. Thus, the minimal polynomial f_i of β_i over $k(\beta_1, \ldots, \beta_{i-1})$ has no repeated factors. Since the minimal polynomial of β_i over $K(\beta_1, \ldots, \beta_{i-1})$ is a factor of f_i, it has no repeated factors. Going back in the other direction again, this means that

$$K(\beta_1, \ldots, \beta_i) \;/\; K(\beta_1, \ldots, \beta_{i-1})$$

is separable, for every i. Then L/K is separable. ///

3. *Primitive elements*

The following finiteness result is stronger than one might suspect, and gives further evidence that finite separable extensions are well-behaved.

[3.0.1] **Proposition:** Let K be a finite field extension of k. There is a single generator α such that $K = k(\alpha)$ if and only if there are only finitely-many fields between k and K.

Proof: First, suppose that $K = k(\alpha)$. Let E be an intermediate field, and let $g(x) \in E[x]$ be the minimal polynomial of α over E. Adjoining the *coefficients* of g to k gives a field F between k and E. Since g is irreducible in $E[x]$, it is certainly irreducible in the smaller $F[x]$. Since $K = k(\alpha) = F(\alpha)$, the degree of K over E is equal to its degree over F. By the multiplicativity of degrees in towers, $E = F$. That is, E is uniquely determined by the monic polynomial g. Since g divides f, and since there are only finitely-many monic divisors of f, there are only finitely-many possible intermediate fields.

Conversely, assume that there are only finitely-many fields between k and K. For k *finite*, the intermediate fields are k vector subspaces of the finite-dimensional k vector space K, so there are only finitely-many. Now consider *infinite* k. It suffices to show that for any two algebraic elements α, β over k, there is a single γ such that $k(\alpha, \beta) = k(\gamma)$. Indeed, let $\gamma = \alpha + t\beta$ with $t \in k$ to be determined. Since there are finitely-many intermediate fields and k is infinite, there are $t_1 \neq t_2$ such that

$$k(\alpha + t_1\beta) \;=\; k(\alpha + t_2\beta)$$

Call this intermediate field E. Then

$$(t_2 - t_1)\beta = (\alpha + t_1\beta) - (\alpha + t_2\beta) \in E$$

We can divide by $t_1 - t_2 \in k^\times$, so $\beta \in E$, and then $\alpha \in E$. Thus, the singly-generated E is equal to $k(\alpha, \beta)$. The finite-dimensional extension K is certainly finitely generated, so an induction proves that K is singly generated over k. ///

[3.0.2] **Remark:** There can be infinitely-many fields between a base field and a finite extension, as the example of the degree p^2 extension $\mathbb{F}_p(s^{1/p}, t^{1/p})$ of $\mathbb{F}_p(s,t)$ with independent indeterminates s, t showed earlier.

In classical terminology, a single element α of K such that $K = k(\alpha)$ is called a **primitive elements** for K over k.

[3.0.3] **Corollary:** Let K be a finite separable extension of k. Then there are finitely-many fields between K and k, and K can be generated by a single element over k.

Proof: The issue is to show that a separable extension with two generators can be generated by a single element. Let $E = k(\alpha, \beta)$, with α, β separable over k. Let X be the set of distinct imbeddings of E into $\overline{k}$ over k, and put

$$f(x) \;=\; \Pi_{\sigma \neq \tau, \text{ in } X}(\sigma\alpha + x \cdot \sigma\beta - \tau\alpha - x\tau\beta)$$

This f is not the 0 polynomial, so there is $t \in \overline{k}$ such that $f(t) \neq 0$. Then the $\sigma(\alpha + t\beta)$ are n distinct field elements. Thus, $k(\alpha + t\beta)$ has degree at least n over k. On the other hand, this n is the degree of $k(\alpha, \beta)$ over k, so $k(\alpha, \beta) = k(\alpha + t\beta)$. ///

4. *Normal field extensions*

In contrast to separability, the condition that a finite field extension K of k be *normal* is *not* typical. [4] There are several different useful characterizations of the property.

A finite field extension K of k is **normal** if all k-algebra homomorphisms of K into a fixed algebraic closure $\overline{k}$ of k have the same *image*.

[4.0.1] **Remark:** Thus, in discussions of a normal extensions, it is not surprising that an algebraic closure can serve a useful auxiliary role.

[4.0.2] **Example:** To illustrate that normal extensions are arguably atypical, note that the field extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ is *not* normal, since one imbedding into a copy of $\overline{\mathbb{Q}}$ inside $\mathbb{C}$ sends the cube root to a *real* number, while two others send it to *complex* (non-real) numbers.

[4.0.3] **Example:** All cyclotomic extensions of $\mathbb{Q}$ are normal. Indeed, let ζ be a primitive n^{th} root of unity. We have already seen that *every* primitive n^{th} root of unity is of the form ζ^k where k is relatively prime to n. Since any mapping of $\mathbb{Q}(\zeta)$ to an algebraic closure of $\mathbb{Q}$ sends ζ to a primitive n^{th} root of unity, the image is unavoidably the same.

[4.0.4] **Remark:** Note that the key feature of roots of unity used in the last example was that by adjoining *one* root of an equation to a base field we include *all*. This motivates:

[4.0.5] **Proposition:** Let $f(x)$ be the minimal polynomial of a generator α of a finite field extension $k(\alpha)$ of k. The extension $k(\alpha)/k$ is normal if and only if every root β of $f(x) = 0$ lies in $k(\alpha)$, if and only if $f(x)$ factors into linear factors in $k(\alpha)[x]$.

Proof: The equivalence of the last two conditions is elementary. As we have seen several times by now, the k-algebra imbeddings $\sigma : k(\alpha) \longrightarrow \overline{k}$ are in bijection with the roots of $f(x) = 0$ in $\overline{k}$, with each root getting hit by a unique imbedding. If $k(\alpha)/k$ is normal, then $k(\sigma(\alpha)) = k(\tau(\alpha))$ for any two roots $\sigma(\alpha)$ and $\tau(\alpha)$ in $\overline{k}$. That is, any one of these images of $k(\alpha)$ contains every root of $f(x) = 0$ in $\overline{k}$. Since $k(\alpha) \approx k(\sigma(\alpha))$ for any such imbedding σ, the same conclusion applies to $k(\alpha)$.

On the other hand, suppose that $f(x)$ factors into linear factors in $k(\alpha)[x]$. Then it certainly factors into linear factors in $k(\sigma(\alpha))[x]$, for every $\sigma : k(\alpha) \longrightarrow \overline{k}$. That is, any $k(\sigma(\alpha))$ contains all the roots of $f(x) = 0$ in $\overline{k}$. That is,

$$k(\sigma(\alpha)) = k(\tau(\alpha))$$

for any two such imbeddings, which is to say that the two images are the same. ///

[4.0.6] **Proposition:** If L is a finite normal field extension of k, and $k \subset K \subset L$, then L is normal over K.

Proof: An algebraic closure $\overline{k}$ of k is also an algebraic closure of any image $\sigma(K)$ of K in $\overline{k}$, since K is algebraic over k. The collection of imbeddings of L into $\overline{k}$ that extend $\sigma : K \longrightarrow \sigma(K)$ is a subset of the collection of *all* k-algebra imbeddings of L to $\overline{k}$. Thus, the fact that all the latter images are the same implies that all the former images are the same. ///

[4.0.7] **Remark:** In the situation of the last proposition, it is certainly *not* the case that K/k is normal. This is in sharp contrast to the analogous discussion regarding separability.

[4.0.8] **Proposition:** A finite field extension K of k is normal if and only if, for every irreducible polynomial f in $k[x]$, if $f(x)$ has *one* linear factor in $K[x]$, then it factors completely into linear factors in $K[x]$.

[4] Thus, this terminology is potentially misleading, in essentially the same manner as the terminology *normal subgroups*.

Proof: First, suppose that K is normal over k, sitting inside an algebraic closure $\overline{k}$ of k. Let $\alpha \in K$ be a root in $\overline{k}$ of an irreducible polynomial $f(x) \in k[x]$. As recalled at the beginning of this chapter, given a root β of $f(x) = 0$ in $\overline{k}$, there is a k-algebra homomorphism $\sigma : k(\alpha) \longrightarrow K$ sending α to β. As recalled above, σ extends to a k-algebra homomorphism $\sigma : K \longrightarrow \overline{k}$. By the assumption of normality, $\sigma K = K$. Thus, $\beta \in K$.

For the converse, first let $K = k(\alpha)$. Let $f(x)$ be the minimal polynomial of α over k. By assumption, all the other roots of $f(x) = 0$ in $\overline{k}$ are in K. As recalled above, any k-algebra map of $k(\alpha) \longrightarrow \overline{k}$ must send α to some such root β, any k-algebra map of $k(\alpha)$ to $\overline{k}$ sends $k(\alpha)$ to K. Since $k(\alpha)$ is a finite-dimensional k-vectorspace, the injectivity of a field map implies surjectivity. That is, every k-algebra image of K in $\overline{k}$ is the original copy of K in $\overline{k}$.

For the general case of the converse, let $K = k(\alpha_1, \ldots, \alpha_n)$. Let $f_i(x)$ be the minimal polynomial of α_i over $k(\alpha_1, \ldots, \alpha_{i-1})$. Do induction on i. By hypothesis, and by the previous proposition, all the other roots of $f_i(x) = 0$ lie in K. Since any $k(\alpha_1, \ldots, \alpha_{i-1})$-linear map must send α_i to one of these roots, every image of $k(\alpha_1, \ldots, \alpha_i)$ is inside K. The induction implies that every k-algebra image of K in $\overline{k}$ is inside K. The finite-dimensionality implies that the image must be *equal* to K. ///

The idea of the latter proof can be re-used to prove a slightly different result:

[4.0.9] Proposition: Let f be a not-necessarily irreducible polynomial in $k[x]$. Let $\overline{k}$ be a fixed algebraic closure of k. Any finite field extension K of k obtained as

$$K = k(\text{all roots of } \ f(x) = 0 \ \text{ in } \ \overline{k})$$

is *normal* over k.

Proof: First, suppose K is obtained from k by adjoining all the roots $\alpha_1, \ldots, \alpha_n$ of an irreducible $f(x)$ in $k[x]$. Certainly $K = k(\alpha_1, \ldots, \alpha_n)$. Let $f_i(x)$ be the minimal polynomial of α_i over $k(\alpha_1, \ldots, \alpha_{i-1})$. Any k-algebra homomorphism $k(\alpha_1) \longrightarrow \overline{k}$ must send α_1 to some $\alpha_i \in K$, so any such image of $k(\alpha_1)$ is inside K. Do induction on i. Since $f_i(x)$ is a factor of $f(x)$, all the other roots of $f_i(x) = 0$ lie in K. Since any $k(\alpha_1, \ldots, \alpha_{i-1})$-linear map must send α_i to one of these roots, every image of $k(\alpha_1, \ldots, \alpha_i)$ is inside K. By induction, every k-algebra image of K in $\overline{k}$ is inside K. The finite-dimensionality implies that the image must be *equal* to K. Thus, K is normal over k. ///

Given a (not necessarily irreducible) polynomial f in $k[x]$, a **splitting field** for f over k is a field extension K obtained by adjoining to k all the zeros of f (in some algebraic closure $\overline{k}$ of k). Thus, the assertion of the previous proposition is that *splitting fields are normal.*

The same general idea of proof gives one more sort of result, that moves in a slightly new conceptual direction:

[4.0.10] Proposition: Let K be a normal field extensions of k. Let $f(x)$ be an irreducible in $k[x]$. Let α, β be two roots of $f(x) = 0$ in K. Then there is a k-algebra automorphism $\sigma : K \longrightarrow K$ such that

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

Proof: Let $\overline{k}$ be an algebraic closure of k, and take $K \subset \overline{k}$ without loss of generality. By now we know that there is a k-algebra map $k(\alpha) \longrightarrow \overline{k}$ sending α to β, and that this map extends to a k-algebra homomorphism $K \longrightarrow \overline{k}$. By the normality of K over k, every image of K in $\overline{k}$ is K. Thus, the extended map is an automorphism of K over k. ///

[4.0.11] Remark: For K normal over k and L normal over K, it is not necessarily the case that L is normal over k. For example, $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is normal over $\mathbb{Q}(\sqrt{2})$, but $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is *not* normal over $\mathbb{Q}$.

5. *The main theorem*

A finite field extension K of k is **Galois** if it is both separable and normal over k. Let K be a finite Galois field extension of k. The **Galois group** of K over k is the automorphism group

$$G = \mathrm{Gal}(K/k) = \mathrm{Aut}(K/k)$$

The **Galois group** of a polynomial f in $k[x]$ over k is the Galois group of the *splitting field* of f over k.

[5.0.1] **Theorem:** Let L be a finite Galois extension of k. The intermediate fields K between k and L are in *inclusion-reversing* bijection with subgroups H of the Galois group $G = \mathrm{Gal}(L/k)$ by

$$\text{subgroup } H \leftrightarrow \text{ subfield } K \text{ fixed by } H$$

For K the fixed field of subgroup H there is the equality

$$[L : K] = |H|$$

Further, H is a *normal* subgroup of G if and only if its fixed field K is Galois over k. If so, then

$$\mathrm{Gal}(K/k) \approx G/H$$

The standard picture for this is

$$G\left\{\begin{array}{c} \left.\begin{array}{c} L \\ | \\ K \end{array}\right\} H \\ | \\ k \end{array}\right.$$

[5.0.2] **Remark:** The bijection between subgroups and intermediate fields is *inclusion-reversing.*

Proof: This proof is complicated. The first part goes from intermediate fields to subgroups of the Galois group. The second part goes from subgroups to intermediate fields. Then a few odds and ends are cleaned up.

First, we prove that the pointwise-fixed field

$$L^G \;=\; \{\alpha \in L \;:\; g\cdot\alpha = \alpha \text{ for all } \; g \in G\}$$

is just k itself, as opposed to being anything larger. Suppose that $\alpha \in L$ but $\alpha \notin k$. Let $f(x)$ be the minimal polynomial of α over k. Since L is separable over k, α is separable over k, so there is a root $\beta \neq \alpha$ of $f(x)$ in $\overline{k}$. Since L is normal over k, in fact $\beta \in L$. The last proposition of the previous section shows that there is an automorphism of L sending α to β. Thus, $\alpha \notin k$. This proves that the pointwise-fixed field of L^G is k.

Upon reflection, this argument proves that for an intermediate field K between k and L, the pointwise-fixed field of $\mathrm{Gal}(L/K)$ is K itself. In symbols, $K = L^{\mathrm{Gal}(L/K)}$.

Next, we show that the map $K \longrightarrow \mathrm{Gal}(L/K)$ of intermediate fields to subgroups of the Galois group is *injective.* For an intermediate field K, L/K is Galois. We just proved that K is the fixed field of $\mathrm{Gal}(L/K)$ inside L. Likewise, for another intermediate field $K' \neq K$, the pointwise-fixed field of $\mathrm{Gal}(L/K')$ in L is K'. Thus, these two subgroups must be distinct.

Next, show that, for two intermediate fields K, K' between L and k, with $H = \mathrm{Gal}(L/K)$ and $H' = \mathrm{Gal}(L/K')$, the Galois group of L over the compositum KK' is

$$H \cap H' \;=\; \mathrm{Gal}(L/KK')$$

Indeed, every element of $H \cap H'$ leaves KK' fixed pointwise. On the other hand, every element of $\mathrm{Gal}(L/k)$ leaving KK' fixed pointwise certainly fixes both K and K'.

Next, with the notation of the previous pragraph, we claim that the pointwise-fixed field of the smallest subgroup A of G containing both H and H' is $K \cap K'$. Indeed, this fixed field must lie inside the fixed field of H, which is K, and must lie inside the fixed field of H', which is K'. Thus, the fixed field of A is contained in $K \cap K'$. On the other hand, every element of $K \cap K'$ *is* fixed by H and by H', so is fixed by the subgroup of $\mathrm{Gal}(L/k)$ generated by them.

Keeping this notation, next we claim that $K \subset K'$ if and only if $H \supset H'$. Indeed, $g \in \mathrm{Gal}(L/k)$ leaving K' fixed certainly leaves K fixed, so $g \in H$. This is one direction of the equivalence. On the other hand, when $H \supset H'$, certainly the fixed field of the larger group H is contained in the fixed field of the smaller.

Now, following Artin, we go from subgroups of the Galois group to intermediate fields. That is, we prove that every subgroup of a Galois group is the Galois group of the top field L over an intermediate field. Let E be an arbitrary field, and B a group of field automorphisms of E, with $|B| = n$. Let $K = E^B$ be the pointwise-fixed field of B inside E. Then E/K is Galois, with Galois group B. To see this, let $\alpha \in E$ and let $b_1, \ldots, b_n \in B$ be a *maximal* collection of elements of B such that the $b_i\alpha$ are *distinct*. Certainly α is a root of the polynomial

$$f(x) \;=\; \Pi_{i=1}^{n}\,(x - b_i\alpha)$$

For any $b \in B$ the list $bb_1\alpha, \ldots, bb_n\alpha$ must be merely a permutation of the original list $b_1\alpha, \ldots, b_n$, or else the maximality is contradicted. Thus, the polynomial f^b obtained by letting $b \in B$ act on the coefficients of f is just f itself. That is, the coefficients lie in the pointwise-fixed field $K = E^B$. By construction, the roots of f are distinct. This shows that every element of E is separable of degree at most n over K, and the minimal polynomial over K of every $\alpha \in E$ splits completely in E. Thus, E is separable and normal over K, hence, Galois. By the theorem of the primitive element, $E = K(\alpha)$ for some α in E, and $[E : K] \leq n$ since the degree of the minimal polynomial of α over K is *at most* n. On the other hand, we saw that the number of automorphisms of $E = K(\alpha)$ over $K(\alpha)$ is *at most* the degree of the extension. Thus, B is the whole Galois group.

Incidentally, this last discussion proves that the order of the Galois group is equal to the degree of the field extension.

Finally, for an intermediate field K between k and L, as shown earlier, the top field L is certainly separable over K, and is also normal over K. Thus, L is Galois over K. The last paragraph does also show that $\mathrm{Gal}(L/K)$ is the subgroup of $\mathrm{Gal}(L/k)$ pointwise-fixing K.

Finally, we must prove that an intermediate field K between k and L is *normal* over the bottom field k if and only if its pointwise-fixer subgroup N in $G = \mathrm{Gal}(L/k)$ is a normal subgroup of G. First, for K normal over k, any element of G stabilizes K, giving a group homomorphism $G \longrightarrow \mathrm{Gal}(K/k)$. The kernel is a normal subgroup of G, and by definition is the subgroup of G fixing K. On the other hand, if K is *not* normal over k, then there is an imbedding σ of K to $\overline{k}$ whose image is *not* K itself. Early on, we saw that such an imbedding extends to L, and, since L is normal over k, the image of L is L. Thus, this map gives an element σ of the Galois group $\mathrm{Gal}(L/k)$. We have $\sigma K \neq K$. Yet it is immediate that $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/\sigma K)$ are conjugate by σ. By now we know that these pointwise-fixer groups are unequal, so neither one is normal in $\mathrm{Gal}(L/k)$.

This finishes the proof of the main theorem of Galois theory. ///

6. *Conjugates, trace, norm*

Let K/k be a finite Galois field extension with Galois group. For $\alpha \in K$, the **(Galois) conjugates** of α over k are the images $\sigma\alpha$ for $\sigma \in G$.

The **(Galois) trace** from K to k is the map

$$\text{trace}_{K/k}\,\alpha \;=\; \text{tr}_{K/k} \;=\; \sum_{\sigma \in G} \sigma\alpha \qquad\qquad (\text{for } \alpha \in K)$$

The **(Galois) norm** from K to k is the map

$$\text{norm}_{K/k}\,\alpha \;=\; N_{K/k} \;=\; \Pi_{\sigma \in G}\sigma\alpha \qquad\qquad (\text{for } \alpha \in K)$$

Of course, usually an element α in K has a non-trivial *isotropy subgroup* in G, so there may be fewer *distinct* conjugates of α than conjugates altogether. For that matter, sometimes *conjugates* insinuates that one is to take distinct conjugates.

When K is the splitting field over k of the minimal polynomial $f(x) \in k[x]$ for α separable algebraic over k,

$$f(x) \;=\; \Pi_{\sigma \in G}(x - \sigma\alpha) \;=\; x^n - \text{tr}_{K/k}\alpha\, x^{n-1} + \ldots + (-1)^n \cdot N_{K/k}\alpha$$

where $n = [K : k]$. The other symmetric polynomials in α do not have names as common as the trace and norm.

7. *Basic examples*

A Galois extension is called **cyclic** if its Galois group is cyclic. Generally, any adjective that can be applied to a *group* can be applied to a *Galois field extension* if its Galois group has that property.

[7.0.1] **Example:** Let $k = \mathbb{F}_q$ be a **finite** field $\mathbb{F}_q$ with q elements. Although the result was not couched as Galois theory, we have already seen (essentially) that every extension K of k is *cyclic*, generated by the Frobenius automorphism

$$\mathrm{Frob}_q : \alpha \longrightarrow \alpha^q$$

Thus, without citing the main theorem of Galois theory, we already knew that

$$[K : k] = |\mathrm{Gal}(K/k)|$$

[7.0.2] **Example:** Let $k = \mathbb{Q}$, and ζ a primitive n^{th} root of unity. Again, the result was not portrayed as Galois theory, but we already saw (essentially) that $K = \mathbb{Q}(\zeta)$ is an *abelian* Galois extension, with

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/n)^\times$$

by

$$(\zeta \longrightarrow \zeta^a) \longleftarrow a$$

[7.0.3] **Example:** *(Kummer extensions)* Fix a prime p, let $k = \mathbb{Q}(\zeta)$ where ζ is a primitive p^{th} root of unity, and take a to be *not* a p^{th} power in $k^\times$. Let K be the splitting field over $\mathbb{Q}(\zeta)$ of $x^p - a$. Then $K = k(\alpha)$ for any p^{th} root α of a,

$$[K : \mathbb{Q}(\zeta)] = p$$

and the Galois group is

$$\mathrm{Gal}(K/\mathbb{Q}(\zeta)) \approx \mathbb{Z}/p \quad \text{(with addition)}$$

by

$$(\alpha \longrightarrow \zeta^\ell \cdot \alpha) \longleftarrow \ell$$

(Proof of this is left as an exercise.)

[7.0.4] **Example:** Fix a prime p, let $k = \mathbb{Q}$ and take a to be *not* a p^{th} power in $\mathbb{Q}^\times$. Let K be the splitting field over $\mathbb{Q}(\zeta)$ of $x^p - a$. Then $K = k(\alpha, \zeta)$ for any p^{th} root α of a, and for ζ a primitive p^{th} root of unity. We have

$$[K : \mathbb{Q}] = p(p-1)$$

and the Galois group is a semi-direct product

$$\mathrm{Gal}(K/\mathbb{Q}) \approx \mathbb{Z}/p \times_f (\mathbb{Z}/p)^\times$$

(Proof of this is left as an exercise at the end of this section.)

[7.0.5] **Example:** Let $t_1, \ldots, t_n$ be independent indeterminates over a field E. Let $K = E(t_1, \ldots, t_n)$ be the field of fractions of the polynomial ring $E[t_1, \ldots, t_n]$. Let the permutation group $G = S_n$ on n things act on K by permutations of the t_i, namely, for a permutation π, let

$$\sigma_\pi(t_i) = t_{\pi(i)}$$

We prove below that the fixed field in K of G is the field

$$k = E(s_1, \ldots, s_n)$$

generated by the elementary symmetric polynomials s_i in the t_i.

[7.0.6] **Remark:** The content of the last example is that **generic** polynomials of degree n have Galois groups S_n, even though various *particular* polynomials may have much smaller Galois groups.

8. *Worked examples*

[22.1] Show that $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$.

We must show that all imbeddings $\sigma : \mathbb{Q}(\sqrt{2}) \longrightarrow \overline{\mathbb{Q}}$ to an algebraic closure of $\mathbb{Q}$ have the same image. Since (by Eisenstein and Gauss) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, it is the minimal polynomial for any square root of 2 in any field extension of $\mathbb{Q}$. We know that (non-zero) field maps $\mathbb{Q}(\alpha) \longrightarrow \overline{\mathbb{Q}}$ over $\mathbb{Q}$ can only send roots of an irreducible $f(x) \in \mathbb{Q}[x]$ to roots of the same irreducible in $\overline{\mathbb{Q}}$. Let β be a square root of 2 in $\overline{\mathbb{Q}}$. Then $-\beta$ is another, and is the *only* other square root of 2, since the irreducible is of degree 2. Thus, $\sigma(\sqrt{2}) = \pm\beta$. Whichever sign occurs, the image of the whole $\mathbb{Q}(\sqrt{2})$ is the same. ///

[22.2] Show that $\mathbb{Q}(\sqrt[3]{5})$ is not normal over $\mathbb{Q}$.

By Eisenstein and Gauss, $x^3 - 5$ is irreducible in $\mathbb{Q}[x]$, so $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. Let α be one cube root of 5 in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Also, observe that $x^3 - 5$ has no repeated factors, since its derivative is $3x^2$, and the *gcd* is readily computed to be 1. Let β be *another* cube root of 5. Then $(\alpha/beta)^3 = 1$ and $\alpha/beta \neq 1$, so that ratio is a primitive cube root of unity ω, whose minimal polynomial over $\mathbb{Q}$ we know to be $x^2 + x + 1$ (which is indeed irreducible, by Eisenstein and Gauss). Thus, the cubic field extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ cannot contain β, since otherwise it would have a quadratic subfield $\mathbb{Q}(\omega)$, contradicting the multiplicativity of degrees in towers.

Since

$$\mathbb{Q}(\alpha) \approx \mathbb{Q}[x]/\langle x^3 - 5\rangle \approx \mathbb{Q}(\beta)$$

we can map a copy of $\mathbb{Q}(\sqrt[3]{5})$ to either $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\beta)$, sending $\sqrt[3]{5}$ to either α or β. But inside $\overline{\mathbb{Q}}$ the two fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are distinct sets. That is, $\mathbb{Q}(\sqrt[3]{5})$ is not normal. ///

[22.3] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{13})$ where ζ_{13} is a primitive 13^{th} root of unity.

We already know that the Galois group G of the extension is isomorphic to $(\mathbb{Z}/13)^\times$ by

$$a \longrightarrow (\sigma_a : \zeta \longrightarrow \zeta^a)$$

and that group is cyclic. Thus, the subgroups are in bijection with the divisors of the order, 12, namely 1,2,3,4,6,12. By the main theorem of Galois theory, the intermediate fields are in bijection with the *proper* subgroups, which will be the fixed fields of the subgroups of orders $2, 3, 4, 6$. We have already identified the quadratic-over-$\mathbb{Q}$ subfield of any cyclotomic field $\mathbb{Q}(\zeta_p)$ with a primitive p^{th} root of unity ζ_p with p *prime*, via Gauss sums, as $\mathbb{Q}(\sqrt{\pm p})$ with the sign being the quadratic symbol $(-1/p)_2$. Thus, here, the subgroup fixed by the subgroup of order 6 is quadratic over $\mathbb{Q}$, and is $\mathbb{Q}(\sqrt{13})$.

We claim that the subfield fixed by $\zeta \longrightarrow \zeta^{\pm 1}$ is $\mathbb{Q}(\xi)$, where $\xi = \zeta + \zeta^{-1}$ is obtained by averaging ζ over that group of automorphisms. First, ξ is not 0, since those two powers of ζ are linearly independent over $\mathbb{Q}$. Second, to show that ξ is not accidentally invariant under any *larger* group of automorphisms, observe that

$$\sigma_a(\xi) = \zeta^a + \zeta^{-a} = \zeta^a + \zeta^{13-a}$$

Since $\zeta^1, \zeta^2, \ldots, \zeta^{11}, \zeta^{12}$ are a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta)$, an equality $\sigma_a(\xi) = \xi$ is

$$\zeta^a + \zeta^{13-a} = \sigma_a(\xi) = \xi = \zeta + \zeta^{12}$$

which by the linear independence implies $a = \pm 1$. This proves that this ξ generates the sextic-over-$\mathbb{Q}$ subextension.

To give a second description of ξ by telling the irreducible in $\mathbb{Q}[x]$ of which it is a zero, divide through the equation satisfied by ζ by ζ^6 to obtain

$$\zeta^6 + \zeta^5 + \ldots + \zeta + 1 + \zeta^{-1} + \ldots + \zeta^{-6} = 0$$

Thus,

$$\begin{aligned} \xi^6 + \xi^5 + (1 - \binom{6}{1})\xi^4 + (1 - \binom{5}{1})\xi^3 + (1 - \binom{6}{2} + 5 \cdot \binom{4}{1})\xi^2 \\ + (1 - \binom{5}{2} + 4 \cdot \binom{3}{1})\xi + (1 - \binom{6}{3} + 5 \cdot \binom{4}{2} - 6\binom{2}{1}) \\ = \ \xi^6 + \xi^5 - 5\xi^4 - 4\xi^3 + 6\xi^2 + 3\xi - 1 \ = \ 0 \end{aligned}$$

To describe ξ as a root of this sextic is an alternative to describing it as $\xi = \zeta + \zeta^{-1}$. Since we already know that ξ is of degree 6 over $\mathbb{Q}$, this sextic is necessarily irreducible.

The quartic-over-$\mathbb{Q}$ intermediate field is fixed by the (unique) order 3 subgroup $\{1, \sigma_3, \sigma_9\}$ of automorphisms. Thus, we form the average

$$\alpha = \zeta + \zeta^3 + \zeta^9$$

and claim that α generates that quartic extension. Indeed, if σ_a were to fix α, then

$$\zeta^2 + \zeta^{3a} + \zeta^{9a} = \sigma_a(\alpha) = \alpha = \zeta + \zeta^3 + \zeta^9$$

By the linear independence of $\zeta^2, \zeta^2, \ldots, \zeta^{12}$, this is possible only for a among $1, 3, 9$ modulo 13. This verifies that this α exactly generates the quartic extension.

To determine the quartic irreducible of which α is a root, we may be a little clever. Namely, we first find the irreducible *quadratic* over $\mathbb{Q}(\sqrt{13})$ of which α is a root. From Galois theory, the non-trivial automorphism of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}(\sqrt{13})$ is (the restriction of) σ_4, since 4 is of order 6 in $(\mathbb{Z}/13)^\times$. Thus, the irreducible of α over $\mathbb{Q}(\sqrt{13})$ is

$$(x - \alpha)(x - \sigma_4\alpha)$$

in

$$\alpha + \sigma_4\alpha = \zeta + \zeta^3 + \zeta^9 + \zeta^4 + \zeta^{12} + \zeta^{10} \in \mathbb{Q}(\sqrt{13})$$

the exponents appearing are exactly the non-zero squares modulo 13, so

$$\alpha + \sigma_4\alpha = \sum_{\ell:\ \left(\frac{\ell}{13}\right)_2 = 1} \zeta^\ell = \frac{1}{2} \cdot \left(\sum_{1 \le \ell \le 12} \left(\frac{\ell}{13}\right)_2 \zeta^\ell \ + \sum_{1 \le \ell \le 12} \zeta^\ell \right) = \frac{\sqrt{13} - 1}{2}$$

from discussion of Gauss sums. And

$$\alpha \cdot \sigma_4\alpha = 3 + \zeta^5 + \zeta^{11} + \zeta^7 + \zeta^2 + \zeta^8 + \zeta^6 \in \mathbb{Q}(\sqrt{13})$$

The exponents are exactly the non-squares modulo 13, so this is

$$3 - \frac{1}{2} \cdot \left(\sum_{1 \le \ell \le 12} \left(\frac{\ell}{13}\right)_2 \zeta^\ell \ - \sum_{1 \le \ell \le 12} \zeta^\ell \right) = 3 - \frac{\sqrt{13} + 1}{2} = \frac{-\sqrt{13} + 5}{2}$$

Thus, the quadratic over $\mathbb{Q}(\sqrt{13})$ is

$$x^2 - \frac{\sqrt{13} - 1}{2} x + \frac{-\sqrt{13} + 5}{2}$$

It is interesting that the discriminant of this quadratic is

$$\sqrt{13} \cdot \frac{3-\sqrt{13}}{2}$$

and that (taking the *norm*)

$$\frac{3-\sqrt{13}}{2} \cdot \frac{3+\sqrt{13}}{2} = -1$$

To obtain the quartic over $\mathbb{Q}$, multiply this by the same expression with $\sqrt{13}$ replaced by its negative, to obtain

$$(x^2+\frac{x}{2}+\frac{5}{2})^2 - 13(\frac{x}{2}+\frac{1}{2})^2 = x^4+\frac{x^2}{4}+\frac{25}{4}+x^3+5x^2+\frac{5x}{2}-\frac{13x^2}{4}-\frac{13x}{2}-\frac{13}{4}$$
$$= \; x^4+x^3+2x^2-4x+3$$

Finally, to find the cubic-over-$\mathbb{Q}$ subfield fixed by the subgroup $\{1, \sigma_5, \sigma{-1}, \sigma_8\}$ of the Galois group, first consider the expression

$$\beta = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$$

obtained by averaging ζ by the action of this subgroup. This is not zero since those powers of ζ are linearly independent over $\mathbb{Q}$. And if

$$\zeta^a + \zeta^{5a} + \zeta^{12a} + \zeta^{8a} = \sigma_a(\beta) = \beta = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$$

the the linear independence implies that a is among $1, 5, 12, 8$ mod 13. Thus, β is not accidentally invariant under a larger group.

Of course we might want a second description of β by telling the irreducible cubic it satisfies. This was done by brute force earlier, but can also be done in other fashions to illustrate other points. For example, we know *a priori* that it *does* satisfy a cubic.

The linear coefficient is easy to determine, as it is the negative of

$$\beta + \sigma_2(\beta) + \sigma_2^2(\beta) = (\zeta+\zeta^5+\zeta^{12}+\zeta^8) + (\zeta^2+\zeta^{10}+\zeta^{11}+\zeta^3) + (\zeta^4+\zeta^7+\zeta^9+\zeta^6) = -1$$

since the powers of ζ are ζ^i with i running from 1 to 12. Thus, the cubic is of the form x^3+x^2+ax+b for some a, b in $\mathbb{Q}$.

We know that $\beta = \zeta+\zeta^5+\zeta^{12}+\zeta^8$ is a zero of this equation, and from

$$\beta^3 + \beta^2 + a\beta + b = 0$$

we can determine a and b. Expanding β^3 and β^2, we have

$$\big(\zeta^3+\zeta^2+\zeta^{10}+\zeta^{11}$$
$$+3(\zeta^7+\zeta^4+\zeta+\zeta^{12}+\zeta^{10}+\zeta^4+\zeta^9+\zeta^3+\zeta^5+|zeta^8+\zeta^6+\zeta^2)$$
$$+6(\zeta^5+\zeta+\zeta^8+\zeta^{12}\big)$$
$$+\big(\zeta^2+\zeta^{10}+\zeta^{11}+\zeta^3+2(\zeta^6+1+\zeta^9+\zeta^4+1+\zeta^7)\big)$$
$$+a\cdot(\zeta+\zeta^5+\zeta^{12}+\zeta^8)+b=0$$

Keeping in mind that

$$\zeta^{12} = -(1+\zeta+\zeta^2+\ldots+\zeta^{10}+\zeta^{11})$$

using the linear independence of $1, \zeta, \zeta^2, \ldots, \zeta^{10}, \zeta^{11}$ by looking at the coefficients of 1, ζ, ζ^2, ζ^3, $\ldots$ we obtain relations, respectively,

$$\begin{array}{rcl} -3-6+2\cdot 2-a+b & = & 0 \\ 0 & = & 0 \\ 1-6+1-a & = & 0 \\ 1-6+1-a & = & 0 \\ \ldots & & \end{array}$$

From this, $a = -4$ and $b = 1$, so

$$x^3 + x^2 - 4x + 1$$

is the cubic of which $\beta = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$ is a zero. ///

[8.0.1] **Remark:** It is surprising that the product of β and its two conjugates is -1.

[22.4] Find all fields intermediate between $\mathbb{Q}$ and a splitting field of $x^3 - x + 1$ over $\mathbb{Q}$.

First, we check the irreducibility in $\mathbb{Q}[x]$. By Gauss this is irreducible in $\mathbb{Q}[x]$ if and only if so in $\mathbb{Z}[x]$. For irreducibility in the latter it suffices to have irreducibility in $(\mathbb{Z}/p)[x]$, for example for $\mathbb{Z}/3$, as suggested by the exponent. Indeed, an earlier example showed that for prime p and $a \neq 0 \bmod p$ the polynomial $x^p - x + a$ is irreducible modulo p. So $x^3 - x + 1$ is irreducible mod 3, so irreducible in $\mathbb{Z}[x]$, so irreducible in $\mathbb{Q}[x]$.

Even though we'll see shortly that in characteristic 0 irreducible polynomials always have distinct zeros, we briefly note why: if $f = g^2 h$ over an extension field, then $\deg \gcd(f, f') > 0$, where as usual f' is the derivative of f. If $f' \neq 0$, then the *gcd* has degree at most $\deg f' = \deg f - 1$, and is in $\mathbb{Q}[x]$, contradicting the irreducibility of f. And the derivative can be identically 0 if the characteristic is 0.

Thus, any of the three distinct zeros α, β, γ of $x^3 - x + 1$ generates a cubic extension of $\mathbb{Q}$.

Now things revolve around the discriminant

$$\Delta = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 = -27\cdot 1^3 - 4\cdot(-1)^3 = -27 + 4 = -23$$

from the computations that show that the discriminant of $x^3 + bx + c$ is $-27c^2 - 4b^3$. From its explicit form, if two (or all) the roots of a cubic are adjoined to the groundfield $\mathbb{Q}$, then the square root of the discriminant also lies in that (splitting) field. Since -23 is *not* a square of a rational number, the field $\mathbb{Q}(\sqrt{-23})$ is a subfield of the splitting field.

Since the splitting field K is normal (and in characteristic 0 inevitably separable), it is Galois over $\mathbb{Q}$. Any automorphism σ of K over $\mathbb{Q}$ must permute the 3 roots among themselves, since

$$\sigma(\alpha)^3 - \sigma(\alpha) + 1 = \sigma(\alpha^3 - \alpha + 1) = \sigma(0) = 0$$

Thus, the Galois group is a *subgroup* of the permutation group S_3 on 3 things. Further, the Galois group is *transitive* in its action on the roots, so cannot be merely of order 1 or 2. That is, the Galois group is either cyclic of order 3 or is the full permutation group S_3. Since the splitting field has a quadratic subfield, via the main theorem of Galois theory we know that the order of the Galois group is *even*, so is the full S_3.

By the main theorem of Galois theory, the intermediate fields are in inclusion-reversing bijection with the proper subgroups of S_3. Since the discriminant is not a square, the 3 subfields obtained by adjoining the different roots of the cubic are distinct (since otherwise the square root of the discriminant would be there), so these must give the subfields corresponding to the 3 subgroups of S_3 of order 2. The field $\mathbb{Q}(\sqrt{-23})$ must correspond to the single remaining subgroup of order 3 containing the 3-cycles. There are no other subgroups of S_3 (by Lagrange and Sylow, or even by direct observation), so there are no other intermediate fields. ///

[22.5] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{21})$ where ζ_{21} is a primitive 21st root of unity.

We have already shown that the Galois group G is isomorphic to

$$(\mathbb{Z}/21)^\times \approx (\mathbb{Z}/7)^\times \times (\mathbb{Z}/3)^\times \approx \mathbb{Z}/6 \oplus \mathbb{Z}/2 \approx \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

(isomorphisms via Sun-Ze's theorem), using the fact that $(\mathbb{Z}/p)^\times$ for p prime is *cyclic*.

Invoking the main theorem of Galois theory, to determine all intermediate fields (as fixed fields of subgroups) we should determine all subgroups of $\mathbb{Z}/3\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2$. To understand the collection of all subgroups, proceed as follows. First, a subgroup H either contains an element of order 3 or not, so H either contains that copy of $\mathbb{Z}/3$ or not. Second, $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ is a two-dimensional vector space over $\mathbb{F}_2$, so its proper subgroups correspond to one-dimensional subspaces, which correspond to non-zero vectors (since the scalars are just $\{0, 1\}$), of which there are exactly 3. Thus, combining these cases, the complete list of *proper* subgroups of G is

$$\begin{array}{rcc}
H_1 &=& \mathbb{Z}/3 \oplus 0 \oplus 0 \\
H_2 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus 0 \\
H_3 &=& \mathbb{Z}/3 \oplus 0 \oplus \mathbb{Z}/2 \\
H_4 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \cdot (1,1) \\
H_5 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \\
H_6 &=& 0 \oplus \mathbb{Z}/2 \oplus 0 \\
H_7 &=& 0 \oplus 0 \oplus \mathbb{Z}/2 \\
H_8 &=& 0 \oplus \mathbb{Z}/2 \cdot (1,1) \\
H_9 &=& 0 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2
\end{array}$$

At worst by trial and error, the cyclic subgroup of order 3 in $(\mathbb{Z}/21)^\times$ is $\{1, 4, 16\}$, and the $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ subgroup is $\{1, 8, 13, -1\}$.

An auxiliary point which is useful and makes things conceptually clearer is to verify that in $\mathbb{Q}(\zeta_n)$, where $n = p_1 \ldots p_t$ is a product of *distinct* primes p_i, and ζ_n is a primitive n^{th} root of unity, the powers

$$\{\zeta^t : 1 \le t < n, \ \text{ with } \ \gcd(t, n) = 1\}$$

is (as you might be hoping[5]) a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_n)$.

Prove this by induction. Let ζ_m be a primitive m^{th} root of unity for any m. The assertion holds for n prime, since for p prime

$$\frac{x^p - 1}{x - 1}$$

is the minimal polynomial for a primitive p^{th} root of unity. Suppose the assertion is true for n, and let p be a prime not dividing n. By now we know that the np^{th} cyclotomic polynomial is irreducible over $\mathbb{Q}$, so the degree of $\mathbb{Q}(\zeta_{np})$ over $\mathbb{Q}$ is (with Euler's totient function φ)

$$[\mathbb{Q}(\zeta_{np})\mathbb{Q}] = \varphi(np) = \varphi(n) \cdot \varphi(p) = [\mathbb{Q}(\zeta_n)\mathbb{Q}] \cdot [\mathbb{Q}(\zeta_p)\mathbb{Q}]$$

since p and n are relatively prime. Let a, b be integers such that $1 = an + bp$. Also note that $\zeta = \zeta_n \cdot \zeta_p$ is a primitive np^{th} root of unity. Thus, in the explicit form of Sun-Ze's theorem, given $i \bmod p$ and $j \bmod n$ we have

$$an \cdot i + bp \cdot j = \begin{cases} \ \ i & \bmod p \\ j \bmod n & \end{cases}$$

Suppose that there were a linear dependence relation

$$0 = \sum_i c_\ell \, \zeta_{np}^\ell$$

[5] For $n = 4$ and $n = 9$ the assertion is definitely false, for example.

with $c_i \in \mathbb{Q}$ and with ℓ summed over $1 \leq \ell < np$ with $\gcd(\ell, np) = 1$. Let $i = \ell \bmod p$ and $j = \ell \bmod n$. Then

$$\zeta_{np}^{ani+bpj} = \zeta_n^j \cdot \zeta_p^i$$

and

$$0 = \sum_{i=1}^{p} \zeta_p^i \left(\sum_j c_{ani+bpj}\, \zeta_n^j \right)$$

where j is summed over $1 \leq j < n$ with $\gcd(j, n) = 1$. Such a relation would imply that $\zeta_p, \ldots, \zeta_p^{p-1}$ would be linearly dependent over $\mathbb{Q}(\zeta_n)$. But the minimal polynomial of ζ_p over this larger field is the same as it is over $\mathbb{Q}$ (because the degree of $\mathbb{Q}(\zeta_n, \zeta_p)$ over $\mathbb{Q}(\zeta_n)$ is still $p - 1$), so this implies that all the coefficients are 0. ///

[22.6] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{27})$ where ζ_{27} is a primitive 27^{th} root of unity.

We know that the Galois group G is isomorphic to $(\mathbb{Z}/27)^\times$, which we also know is *cyclic*, of order $(3-1)3^{3-1} = 18$, since 27 is a power of an odd prime (namely, 3). The subgroups of a cyclic group are in bijection with the divisors of the order, so we have subgroups precisely of orders $1, 2, 3, 6, 9, 18$. The proper ones have orders $2, 3, 6, 9$. We can verify that $g = 2$ is a generator for the cyclic group $(\mathbb{Z}/27)^\times$, and the subgroups of a cyclic group are readily expressed in terms of powers of this generator. Thus, letting $\zeta = \zeta_{27}$, indexing the alphas by the order of the subgroup fixing them,

$$\begin{array}{rcc}
\alpha_2 & = & \zeta + \zeta^{-1} \\
\alpha_3 & = & \zeta + \zeta^{2^6} + \zeta^{2^{12}} \\
\alpha_6 & = & \zeta + \zeta^{2^3} + \zeta^{2^6} + \zeta^{2^9} + \zeta^{2^{12}} + \zeta^{2^{15}} \\
\alpha_9 & = & \zeta + \zeta^{2^2} + \zeta^{2^4} + \zeta^{2^6} + \zeta^{2^8} + \zeta^{2^{10}} \zeta^{2^{12}} + \zeta^{2^{14}} + \zeta^{2^{16}}
\end{array}$$

But there are some useful alternative descriptions, some of which are clearer. Since ζ_{27}^3 is a primitive 9^{th} root of unity ζ_9, which is of degree $\varphi(9) = 6$ over $\mathbb{Q}$, this identifies the degree 6 extension generated by α_3 $(3 \cdot 6 = 18)$ more prettily. Similarly, ζ_{27}^9 is a primitive cube root of unity ζ_3, and $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ from earlier examples. This is the quadratic subfield also generated by α_9. And from

$$0 = \frac{\zeta_9^9 - 1}{\zeta_9^3 - 1} = \zeta_9^6 + \zeta_9^3 + 1$$

we use our usual trick

$$\zeta_9^3 + 1 + \zeta_9^{-3} = 0$$

and then

$$(\zeta_9 + \zeta_9^{-1})^3 - 3(\zeta_9 + \zeta_9^{-1}) - 1 = 0$$

so a root of

$$x^3 - 3x - 1 = 0$$

generates the degree 3 field over $\mathbb{Q}$ also generated by α_6. ///

[22.7] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Before invoking the main theorem of Galois theory, note that it really is true that $[K : \mathbb{Q}] = 2^3$, as a special case of a more general example we did earlier, with an arbitrary list of primes.

To count the proper subgroups of the Galois group $G \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$, it is useful to understand the Galois group as a 3-dimensional vector space over $\mathbb{F}_2$. Thus, the proper subgroups are the one-dimensional subspace and the two-dimensional subspaces, as vector spaces.

There are $2^3 - 1$ non-zero vectors, and since the field is $\mathbb{F}_2$, this is the number of subgroups of order 2. Invoking the main theorem of Galois theory, these are in bijection with the intermediate fields which are of degree 4 over $\mathbb{Q}$. We can easily think of several quartic fields over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{5})$, $\mathbb{Q}(\sqrt{3},\sqrt{5})$, $\mathbb{Q}(\sqrt{6},\sqrt{5})$, $\mathbb{Q}(\sqrt{10},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{15})$, and the least obvious $\mathbb{Q}(\sqrt{6},\sqrt{15})$. The argument that no two of these are the same is achieved most efficiently by use of the automorphisms σ,τ,ρ of the whole field which have the effects

$$\begin{array}{ccc} \sigma(\sqrt{2}) = -\sqrt{2} & \sigma(\sqrt{3}) = \sqrt{3} & \sigma(\sqrt{5}) = \sqrt{5} \\ \tau(\sqrt{2}) = \sqrt{2} & \tau(\sqrt{3}) = -\sqrt{3} & \tau(\sqrt{5}) = \sqrt{5} \\ \rho(\sqrt{2}) = \sqrt{2} & \rho(\sqrt{3}) = \sqrt{3} & \rho(\sqrt{5}) = -\sqrt{5} \end{array}$$

which are restrictions of automorphisms of the form $\zeta \longrightarrow \zeta^a$ of the cyclotomic field containing all these quadratic extensions, for example $\mathbb{Q}(\zeta_{120})$ where ζ_{120} is a primitive 120^{th} root of unity.

To count the subgroups of order $4 = 2^2$, we might be a little clever and realize that the two-dimensional $\mathbb{F}_2$-vectorsubspaces are exactly the kernels of non-zero linear maps $\mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$. Thus, these are in bijection with the non-zero vectors in the $\mathbb{F}_2$-linear dual to $\mathbb{F}_2^3$, which is again 3-dimensional. Thus, the number of two-dimensional subspaces is again $2^3 - 1$.

Or, we can count these two-dimensional subspaces by counting ordered pairs of two linearly independent vectors (namely $(2^3-1)(2^3-2) = 42$) and dividing by the number of changes of bases possible in a two-dimensional space. The latter number is the cardinality of $GL(2,\mathbb{F}_2)$, which is $(2^2-1)(2^2-2) = 6$. The quotient is 7 (unsurprisingly).

We can easily write down several quadratic extensions of $\mathbb{Q}$ inside the whole field, namely $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{30})$. That these are distinct can be shown, for example, by observing that the effects of the automorphisms σ,τ,ρ differ. ///

[22.8] Let a,b,c be independent indeterminates over a field k. Let z be a zero of the cubic

$$x^3 + ax^2 + bx + c$$

in some algebraic closure of $K = k(a,b,c)$. What is the degree $[K(z):K]$? What is the degree of the splitting field of that cubic over K?

First, we prove that $f(x) = x^3+ax^2+bx+c$ is irreducible in $k(a,b,c)[x]$. As a polynomial in x with coefficients in the ring $k(a,b)[c]$, it is monic and has *content* 1, so its irreducibility in $k(a,b,c)[x]$ is equivalent to its irreducibility in $k(a,b)[c][x] \approx k(a,b)[x][c]$. As a polynomial in c it is monic and linear, hence irreducible. This proves the irreducibility in $k(a,b,c)[x]$. Generally, $[K(z):K]$ is equal to the degree of the minimal polynomial of z over K. Since f is irreducible it *is* the minimal polynomial of z over K, so $[K(z):K] = 3$.

To understand the degree of the *splitting field*, let the three roots of $x^3+ax^2+bx+c = 0$ be z,u,v. Then (the discriminant)

$$\Delta = (z-u)^2(u-v)^2(v-z)^2$$

certainly lies in the splitting field, and is a *square* in the splitting field. But if Δ is *not* a square in the ground field K, then the splitting field contains the quadratic field $K(\sqrt{\Delta})$, which is of degree 2 over K. Since $\gcd(2,3) = 1$, this implies that the splitting field is of degree at least 6 over K. But $f(x)/(x-z)$ is of degree 2, so the degree of the splitting field cannot be *more* than 6, so it is *exactly* 6 if the discriminant is *not* a square in the ground field K.

Now we use the fact that the a,b,c are indeterminates. Gauss' lemma assures us that a polynomial A in a,b,c is a square in $k(a,b,c)$ if and only it is a square in $k[a,b,c]$, since the reducibilities of $x^2 - A$ in the two rings are equivalent. Further, if A is square in $k[a,b,c]$ then it is a square in any homomorphic image of $k[a,b,c]$. If the characteristic of k is not 2, map $a \longrightarrow 0$, $c \longrightarrow 0$, so that $f(x)$ becomes $x^3 + bx$. The zeros of this are 0 and $\pm\sqrt{b}$, so the discriminant is

$$\Delta = (0-\sqrt{b})^2(0+\sqrt{b})^2(-\sqrt{b}-\sqrt{b})^2 = b \cdot b \cdot 4b = 4b^3 = (2b)^2 \cdot b$$

The indeterminate b is not a square. (For example, x^2-b is irreducible by Gauss, using Eisenstein's criterion.) That is, because this image is not a square, we know that the genuine discriminant is not a square in $k(a,b,c)$ without computing it.

Thus, the degree of the splitting field is always 6, for characteristic not 2.

For characteristic of k equal to 2, things work differently, since the cubic expression $(z-u)(u-v)(v-z)$ is already invariant under any group of permutations of the three roots. But, also, in characteristic 2, separable quadratic extensions are not all obtained via square roots, but, rather, by adjoining zeros of *Artin-Schreier* polynomials x^2-x+a. ... ///

[22.9] Let $x_1,\ldots,x_n$ be independent indeterminates over a field k, with elementary symmetric polynomials $s_1,\ldots,s_n$. Prove that the Galois group of $k(x_1,\ldots,x_n)$ over $k(s_1,\ldots,s_n)$ is the symmetric group S_n on n things.

Since $k[x_1,\ldots,x_n]$ is the free (commutative) k-algebra on those n generators, for a given permutation p we can certainly map $x_i \longrightarrow x_{p(i)}$. Then, since this has trivial kernel, we can extend it to a map on the fraction field $k(x_1,\ldots,x_n)$. So the permutation group S_n on n things does act by automorphisms of $k(x_1,\ldots,x_n)$. Certainly such permutations of the indeterminates leaves $k[s_1,\ldots,s_n]$ pointwise fixed, so certainly leaves the fraction field $k(s_1,\ldots,s_n)$ pointwise fixed.

Each x_i is a zero of

$$f(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \ldots + (-1)^n s_n$$

so certainly $k(x_1,\ldots,x_n)$ is *finite* over $k(s_1,\ldots,s_n)$. Indeed, $k(x_1,\ldots,x_n)$ is a splitting field of $f(X)$ over $k(s_1,\ldots,s_n)$, since no smaller field could contain $x_1,\ldots,x_n$ (with or without $s_1,\ldots,s_n$). So the extension is *normal* over $k(s_1,\ldots,s_n)$. Since the x_i are mutually independent indeterminates, certainly no two are equal, so $f(X)$ is separable, and the splitting field is separable over $k(s_1,\ldots,s_n)$. That is, the extension is Galois.

The degree of $k(x_1,\ldots,x_n)$ over $k(s_1,\ldots,s_n)$ is *at most* $n!$, since x_1 is a zero of $f(X)$, x_2 is a zero of the polynomial $f(X)/(X-x_1)$ in $k(x_1)[X]$, x_3 is a zero of the polynomial $f(X)/(X-x_1)(X-x_2)$ in $k(x_1,x_2)[X]$, and so on. Since the Galois group contains S_n, the degree is *at least* $n!$ (the order of S_n). Thus, the degree is exactly $n!$ and the Galois group is exactly S_n.

Incidentally, this proves that $f(X) \in k(s_1,\ldots,s_n)[X]$ is irreducible, as follows. Note first that the degree of the splitting field of *any* polynomial $g(X)$ of degree d is at most $d!$, proven best by induction: given one root α_1, in $k(\alpha_1)[X]$ the polynomial $g(X)/(X-\alpha_1)$ has splitting field of degree at most $(d-1)!$, and with that number achieved *only* if $g(X)/(X-\alpha_1)$ is *irreducible* in $k(\alpha_1)[X]$. And $[k(\alpha_1):k] \le d$, with the maximum achieved if and only if $g(X)$ is irreducible in $k[X]$. Thus, by induction, the maximum possible degree of the splitting field of a degree d polynomial is $d!$, and for this to occur it is *necessary* that the polynomial be irreducible.

Thus, in the case at hand, if $f(X)$ were *not* irreducible, its splitting field could not be of degree $n!$ over $k(s_1,\ldots,s_n)$, contradiction. ///

[22.10] Let K/k be a finite separable extension, $\overline{k}$ an algebraic closure of k, and $\sigma_1,\ldots,\sigma_n$ distinct field homomorphisms of K to $\overline{k}$. These σ are *linearly independent* over $\overline{k}$, in the following sense. If $\alpha_1,\ldots,\alpha_n \in \overline{k}$ are such that for all $\beta \in K$

$$\alpha_1\,\sigma_1(\beta) + \ldots + \alpha_n\,\sigma_n(\beta) \;=\; 0$$

then all α_i are 0.

Renumbering if necessary, let

$$\alpha_1\,\sigma_1(\beta) + \ldots + \alpha_n\,\sigma_n(\beta) \;=\; 0$$

be the *shortest* such relation with all α_i nonzero. Let $\gamma \in K^\times$ be a *primitive element* for K/k, that is, $K = k(\gamma)$. Then all the $\sigma_i(\gamma)$ are distinct. Replacing β by $\gamma\cdot\beta$ in the displayed relation and dividing by

$\sigma_1(\gamma)$ gives another relation

$$\alpha_1\,\sigma_1(\beta) + \frac{\alpha_2 \cdot \sigma_2(\gamma)}{\sigma_1(\gamma)}\,\sigma(\beta) + \ldots + \frac{\alpha_n\,\sigma_n(\gamma)}{\sigma_1(\gamma)}\sigma_n(\beta) \;=\; 0$$

Since the ratios $\chi_i(\gamma)/\chi_1(\gamma)$ are not 1 for $i > 1$, subtraction of this relation from the first relation gives a shorter relation, contradiction. ///

[22.11] Let K be a finite separable extension of a field k. Show that the Galois trace tr $: K \longrightarrow k$ is not the 0 map.

Let $\sigma_1, \ldots, \sigma_n$ be the distinct field homomorphisms of K into a chosen algebraic closure $\overline{k}$ of k. The trace is

$$\mathrm{tr}\,(\beta) \;=\; \sigma_1(\beta) + \ldots + \sigma_n(\beta) \;=\; 1 \cdot \sigma_1(\beta) + \ldots + 1 \cdot \sigma_n(\beta)$$

The previous example shows that this linear combination of the imbeddings σ_i is not the 0 map. ///

[22.12] Let K/k be a finite separable extension. Show that the *trace pairing*

$$\langle , \rangle \;:\; K \times K \longrightarrow k$$

defined by

$$\langle \alpha, \beta \rangle \;=\; \mathrm{tr}_{K/k}(\alpha \cdot beta)$$

is *non-degenerate*.

That is, we must prove that, for any non-zero $\alpha \in K$, there is $\beta \in K$ such that $\mathrm{tr}\,(\alpha\beta) \neq 0$. The previous example shows that the trace of a primitive element γ is non-zero. Thus, given $\alpha \neq 0$, let $\beta = \gamma/\alpha$. ///

Exercises

[22.13] Show that any quadratic extension of $\mathbb{Q}$ is normal over $\mathbb{Q}$.

[22.14] Take an integer d which is not a cube or a rational number. Show that $\mathbb{Q}(\sqrt[3]{d})$ is *not* normal over $\mathbb{Q}$.

[22.15] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{11})$ where ζ_{11} is a primitive 13^{th} root of unity.

[22.16] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_8)$ where ζ_8 is a primitive 27^{th} root of unity.

[22.17] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$.

22.[8.0.1] What is the Galois group of $x^3 - x - 1$ over $\mathbb{Q}$?

22.[8.0.2] What is the Galois group of $x^3 - 2$ over $\mathbb{Q}$?

22.[8.0.3] What is the Galois group of $x^3 - x - 1$ over $\mathbb{Q}(\sqrt{23})$?

22.[8.0.4] What is the Galois group of $x^4 - 5$ over $\mathbb{Q}$, over $\mathbb{Q}(\sqrt{5}$, over $\sqrt{-5}$, over $\mathbb{Q}(i)$, and over $\mathbb{Q}(\sqrt{2})$?

22.[8.0.5] Let K/k be a finite separable extension. Show that for every intermediate field $k \subset E \subset K$, the extensions E/k and K/E are separable.

22.[8.0.6] Show that $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is normal over $\mathbb{Q}(\sqrt{2})$, but $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ is *not* normal over $\mathbb{Q}$.

22.[8.0.7] Find all subfields of the splitting field over $\mathbb{Q}$ of x^4+2.

22.[8.0.8] Let k be a field. Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of $k^\times$. Suppose that $c_1, \ldots, c_n$ in k are such that for all positive integers ℓ

$$\sum_i c_i \, \alpha_i^\ell = 0$$

Show that all the c_i are 0.

22.[8.0.9] Let K be a finite normal field extension of a field k. Let P be a monic irreducible in $k[x]$. Let Q and R be two monic irreducible factors of P in $K[x]$. Show that there is $\sigma \in \mathrm{Aut}(K/k)$ such that $Q^\sigma = R$ (with σ acting on the coefficients).

22.[8.0.10] Show that every finite algebraic extension of a finite field is normal and separable, hence Galois.

22.[8.0.11] Show that any cyclotomic field (that is, an extension of $\mathbb{Q}$ obtained by adjoining a root of unity) is normal and separable, hence Galois.

22.[8.0.12] Fix a prime p. Let k be a field *not* of characteristic p, containing a primitive p^{th} root of unity ζ. Let $a \in k$ *not* be a p^{th} power of any element of k, and let α be a p^{th} root of α. Prove that the *Kummer extension* $K = k(\alpha)$ is normal and separable, hence Galois. Prove that the Galois group is cyclic of order p, given by automorphisms

$$\alpha \longrightarrow \zeta^\ell \cdot \alpha \qquad\qquad (\text{for } 0 \le \ell < p)$$

22.[8.0.13] Let $t_1, \ldots, t_n$ be independent indeterminates over a field E. Let $K = E(t_1, \ldots, t_n)$ be the field of fractions of the polynomial ring $E[t_1, \ldots, t_n]$. Let

$$k = E(s_1, \ldots, s_n)$$

be the subfield generated by the elementary symmetric polynomials s_i in the t_i. Prove that the extension K/k is normal and separable, hence Galois. (Then, from our earlier discussion, its Galois group is the permutation group on n things.)

22.[8.0.14] Show that the Galois trace $\sigma : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ is

$$\sigma(\alpha) \;=\; \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}}$$

22.[8.0.15] Show that the Galois norm $\nu : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ is

$$\nu(\alpha) \;=\; \alpha^{\frac{q^n-1}{q-1}}$$

22.[8.0.16] Let k be a finite field, and K a finite extension. Show that trace and norm maps $K \longrightarrow k$ are surjective.

22.[8.0.17] Let k be a finite field with q elements. Fix a positive integer n. Determine the order of the largest cyclic subgroup in $GL(n,k)$.

22.[8.0.18] Let m and n be coprime. Let ζ be a primitive m^{th} root of unity. Show that the cyclotomic polynomial $\varphi_n(x)$ is irreducible in $\mathbb{Q}(\zeta)[x]$.

22.[8.0.19] (*Artin*) Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. Let k be a maximal subfield of $\overline{\mathbb{Q}}$ not containing $\sqrt{2}$. Show that every finite extension of k is cyclic.

22.[8.0.20] (*Artin*) Let σ be an automorphism of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$, with fixed field k. Show that every finite extension of k is cyclic.