This gives an extremely powerful method of studying field extensions by relating them to subgroups of finite groups. One application is an understanding of which polynomials have formulas with radicals for solving them, such as all polynomials of degrees 2, 3 and 4 have, at least in characteristic zero (see page 387).

Let $F \subseteq K$ be fields. An **F-automorphism of K** is an automorphism of K which restricts to the identity on F. For this chapter, the book uses $\iota\colon K \to K$ to denote the identity automorphism. The set of all F-automorphisms of K is denoted by $\mathrm{Gal}_{\mathbf{F}}\,\mathbf{K}$, called the **Galois group** of K over F. So, of course, Theorem 11.1 says it is a group: this is clear since the composition of isomorphisms or the inverse of an isomorphism is an isomorphism, and everything fixes F (as we discussed in Chapter 3 and again for groups). To find these groups, we need

Theorem 11.2. *Let $F \subseteq K$ be fields and $f(x) \in F[x]$. If $u \in K$ is a root of $f(x)$ and $\sigma \in \mathrm{Gal}_F K$, then $\sigma(u)$ is also a root of $f(x)$.*

Proof. $f(\sigma(u)) = \sigma(f)(u) = f(u) = 0$ since the coefficients of $f(x)$ are all fixed by σ. □

Theorem 11.4. *If $K = F(u_1, \ldots, u_n)$, then any automorphism $\sigma \in \mathrm{Gal}_F K$ is uniquely determined by its action on $u_1, u_2, \ldots, u_n$.*

Proof. This seems obvious since we know σ on F and every element of K is somehow a combination of u_i's and elements of F, but this is very intuitive, not a proof. To prove it, we use induction on n since we understand how to express the elements of a simple extension. It is trivial for $n = 0$ since $\sigma|_F = \iota$. Assume that σ is uniquely determined on $E = F(u_1, \ldots, u_{k-1})$. We will show it is determined on $E(u_k)$, which then completes the proof by induction (even if there were a countably infinite number of u_i's). We know every element of $E(u_k)$ can be written in the form $a = e_0 + e_1 u_k + \cdots + e_m u_k^m$ for some $m \geq 0,\ e_i \in E$. But then $\sigma(a) = \sigma(e_0) + \cdots + \sigma(e_m)(\sigma(u_k))^m$ is already determined. □

Corollary 11.5. *If K is the splitting field of a separable polynomial of degree n over F, then $\mathrm{Gal}_F K$ is isomorphic to a subgroup of S_n.*

Proof. By hypothesis, K is generated by the n roots of the polynomial over F. By Theorem 11.2, every automorphism of K over F permutes those roots and by Theorem 11.4, it is uniquely determined by that permutation. Thus $\mathrm{Gal}_F K$ can be thought of as just a set of permutations of the roots of the given polynomial. □

So which permutations do we get? Lets look at some examples.

1. $F = \mathbb{R}$, $K = \mathbb{C}$. K is the splitting field of the irreducible polynomial $x^2 + 1$. $\mathrm{Gal}_{\mathbb{R}} \mathbb{C}$ has two elements, the identity and conjugation, which permutes i and $-i$.

2. Example 1 of the notes for Chapter 10: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $F = \mathbb{Q}$. In examining the proof of Theorem 10.14 on lifting an isomorphism to algebraic extensions, we constructed four different elements of $\mathrm{Gal}_F K$, namely those which take $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$. By Theorem 10.2, roots of $x^2 - 2$ must go to roots of the same polynomial (and similarly for $x^2 - 3$), so these are the only possibilities. Therefore, $\mathrm{Gal}_F K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ since each of these automorphisms has order 2. This is a relatively small subgroup of S_4 which has 24 elements and suggests a theorem that what really matters is the irreducible factors of the splitting polynomial. It leaves open the question of just how many of the permutations for the roots of an irreducible polynomial actually get used. In general, not all of them, but we can prove that there are quite a few.

Theorem 11.3. *Let K be a splitting field of some polynomial over F. Let $u, v \in K$. There exists an automorphism $\sigma \in \mathrm{Gal}_F K$ with $\sigma(u) = v$ iff u and v are roots of the same minimal polynomial over F.*

Proof. We know from Theorem 11.2 that if $\sigma(u) = v$, then they have the same minimal polynomial. The converse claims much more. By Corollary 10.8, there is an isomorphism $F(u) \cong F(v)$. K is also a splitting field for that same polynomial over both $F(u)$ and $F(v)$, so Theorem 10.14 says that the isomorphism extends to an isomorphism from K to K, that is, an F-automorphism σ of K. $\square$

This theorem holds for any normal extension, but the proof takes more work to handle the infinite dimensional case. (Recall Theorem 10.15: splitting field $\iff$ finite dimensional and normal). The theorem says that any root of an irreducible polynomial has an automorphism sending it to any other root. But when there are more than 3 roots, this no longer determines what happens to the other roots, so not all permutations need give automorphisms.

Example 2 of the notes for Chapter 10: $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω was a nontrivial cube root of 1 (satisfying the quadratic equation $x^2 + x + 1$). Thinking of K now as $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ we see that $\mathrm{Gal}_{\mathbb{Q}} K$ is a subgroup of S_3. It has an element of order 2 since there must be an automorphism which permutes the roots of $x^2 + x + 1$ over $\mathbb{Q}(\sqrt[3]{2})$, and it certainly cannot have order 3. There must also be some σ with $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, but it might have order 2 or 3 depending on what it does to ω. Think instead of the subfield $F = \mathbb{Q}(\omega)$ as the base field. $x^3 - 2$ is still irreducible over this field because $F(\sqrt[3]{2})$ is an extension of dimension 3 to make dimension 6 for K over $\mathbb{Q}$. Applying Theorem 11.3 again, we see that K has an automorphism σ with $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ which is the identity on F. But then $\sigma(\sqrt[3]{2}\omega) = \sigma(\sqrt[3]{2})\sigma(\omega) = \sqrt[3]{2}\omega^2$, so $\sigma^2 \neq \iota$. Therefore σ has order 3. Any subgroup of S_3 with an element of order 2 and an element of order 3 must be the whole

group, so $\mathrm{Gal}_{\mathbb{Q}} K = S_3$. Note that we could only determine this by knowing about subfields between K and $\mathbb{Q}$. We next set up a correspondence between subgroups of $\mathrm{Gal}_F K$ and fields between F and K. This is basis of Galois theory.

First we need one fact about separable extensions.

Theorem 10.18. *If K is a finite separable extension of F, then $K = F(u)$ for some $u \in K$.*

Proof. By Theorem 10.28, the theorem is true for finite fields, so we may assume that F is infinite. We know that $K = F(v_1, v_2, \ldots, v_n)$ for some v_i's in K. To show that we only need one, it suffices to show that we can always reduce two to one, for then $F(v_1, v_2) = F(w_1)$, $F(w_1, v_3) = F(w_2), \ldots$ eventually getting us down to only one element. So we assume that $K = F(v, w)$. Let $p(x), q(x) \in F[x]$ be the minimal polynomials for v, w, respectively. In some splitting field, they have distinct (since u, v are separable) roots $v = v_1, v_2, \ldots, v_m$ and $w = w_1, w_2, \ldots, w_n$. Since F is infinite, it contains an element $c \neq \dfrac{v_i - v}{w - w_j}$ for $i = 1, \ldots, m$, $j = 2, \ldots n$. Let $u = v + cw$; we will show it satisfies the theorem by showing that w (and hence v) lies in $F(u)$. Consider the polynomial $h(x) = p(u - cx) \in F(u)[x]$. $h(w) = p(v) = 0$; by our choice of c, $h(w_j) \neq 0$ for $j > 1$, as this would mean $u - cw_j = v_i$ for some i, contradicting $u = v + cw$ (solve for c). Therefore w is the only common root of $q(x)$ and $h(x)$. The minimal polynomial of w over $F(u)$ must divide both $q(x)$ and $h(x)$, hence must have degree one. That is, $w \in F(u)$. $\square$

The Galois correspondence mapping.

From now on we assume that K is a finite-dimensional extension of F. We will define a mapping from intermediate fields (fields between F and K) to subgroups of $\mathrm{Gal}_F K$. Assume that $F \subseteq E \subseteq K$. To E, we associate the group $\mathrm{Gal}_E K$, the group of automorphisms of K which fix E, and hence also fix its subfield F. Thus we may think of $\mathrm{Gal}_E K$ as a subgroup of $\mathrm{Gal}_F K$. Our problem now is to discover the conditions under which this mapping is surjective and injective. Given a subgroup of $\mathrm{Gal}_F K$, we can find an intermediate field as follows: for $H \subseteq \mathrm{Gal}_F K$, let $E_H = \{\, a \in K \mid \sigma(a) = a \text{ for all } \sigma \in H \,\}$. E_H is a field because σ preserves operations. The main theorem we want says that these ways of going from groups to fields and fields to groups are inverses to one another when K is normal and separable over F.

First note that $K \mapsto \mathrm{Gal}_K K = \{e\}$ and $F \mapsto \mathrm{Gal}_F K$. The mapping reverses inclusions. Note how it works with our example of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$ over $\mathbb{Q}$.

Lemma 11.7. *Let H be a subgroup of $\mathrm{Gal}_F K$ with fixed field E. Then K is a simple, normal, separable extension of E.*

Proof. Let $u \in K$ with minimal polynomial $p(x)$ over E. Every automorphism in H carries u to some root of $p(x)$, so there are finitely many images, say $u = u_1, \ldots, u_t \in K$; H permutes these roots. Let $f(x) = \prod(x - u_i)$. The u_i are distinct, so $f(x)$ is separable. For any $\sigma \in H$, $\sigma(f(x))$ just permutes the roots of $f(x)$ so carries it to itself. That is, all the coefficients of $f(x)$ are in the fixed field E. u is a root of the separable polynomial $f(x) \in E[x]$, so u is separable over E. u was arbitrary, so K is a separable extension of E. By Theorem 10.18, $K = E(u)$ for some $u \in K$. Choosing $f(x)$ as above, it splits in K, so K is a normal extension of E. $\square$

Theorem 11.8. *Let H be a subgroup of $\operatorname{Gal}_F K$ with fixed field E. Then $H = \operatorname{Gal}_E K$ and $|H| = [K : E]$. Therefore the Galois correspondence is always surjective. (Equivalently, we could say that $H \mapsto E_H \mapsto \operatorname{Gal}_{E_H} K$ is the identity.)*

Proof. By Lemma 11.7, $K = E(u)$ for some u; u has a minimal polynomial $p(x)$ of degree $n = [K : E]$ (by Theorem 10.7). Distinct elements of $\operatorname{Gal}_E K$ map u to distinct roots of $p(x)$ (since an automorphism of $E(u)$ fixing E is determined by where it sends u). Thus $|\operatorname{Gal}_E K| \leq n$. Furthermore, elements of H fix E, so $H \subseteq \operatorname{Gal}_E K$ and we have

$$|H| \leq |\operatorname{Gal}_E K| \leq n = [K : E].$$

Let $f(x)$ be as in the previous proof. Then H has at least t elements, as those count the distinct images of u under elements of H. Since $p(x)$ is the minimal polynomial, it divides $f(x)$, hence

$$[K : E] = n = \deg p(x) \leq \deg f(x) = t \leq |H|.$$

Combining these inequalities gives $|H| = |\operatorname{Gal}_E K|$, so that $H = \operatorname{Gal}_E K$. $\square$

The injectivity of the Galois correspondence needs another condition. For example, if $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[3]{2})$, then the Galois group $\operatorname{Gal}_{\mathbb{Q}} K$ is the identity, the same as for $\operatorname{Gal}_K K$. If K is a finite, normal, separable extension of F, we call it a **Galois extension**.

Theorem 11.9. *Let K be a Galois extension of F and E an intermediate field. Then E is the fixed field of the subgroup $\operatorname{Gal}_E K$. Therefore the Galois correspondence is injective for Galois extensions. (Equivlaently, we could say that $E \mapsto \operatorname{Gal}_E K \mapsto E_{\operatorname{Gal}_E K}$ is the identity.)*

Proof. Let $E_0 \supseteq E$ be the fixed field of $\operatorname{Gal}_E K$. Assume that $u \notin E$. We show that some automorphism in $\operatorname{Gal}_E K$ moves u, so $u \notin E_0$. K is a Galois extension of E since it is for F (normal $\iff$ splitting field; separable—use same polynomial). Let $p(x)$ be the minimal polynomial of u; its roots are all distinct and in K. If v is any other root, then there exists $\sigma \in \operatorname{Gal}_E K$ with $\sigma(u) = v$ by Theorem 11.3, and hence $u \notin E_0$. $\square$

Corollary 11.10. *K is Galois over F iff F is the fixed field of $\operatorname{Gal}_F K$.*

Proof. ($\Longrightarrow$) is Theorem 11.9 with $E = F$. ($\Longleftarrow$) Lemma 11.7 with $E = F$. $\square$

Fundamental Theorem of Galois Theory. *If K is a Galois extension of F, then there is a bijection between the set of all intermediate fields between F and K and the set of all subgroups of $\operatorname{Gal}_F K$ given by assigning to each intermediate field E, the subgroup $\operatorname{Gal}_E K$. This satisfies $[K : E] = |\operatorname{Gal}_E K|$ and $[E : F] = [\operatorname{Gal}_F K : \operatorname{Gal}_E K]$.*

Furthermore, E is a normal extension of F iff the corresponding subgroup $\operatorname{Gal}_E K$ is a normal subgroup of $\operatorname{Gal}_F K$, in which case $\operatorname{Gal}_F E \cong \operatorname{Gal}_F K / \operatorname{Gal}_E K$.

Proof. The previous two theorems prove the bijective correspondence. By Theorem 11.8, $[K : E] = |\operatorname{Gal}_E K|$. Taking $E = F$ gives $[K : F] = |\operatorname{Gal}_F K|$, so that $[K : E][E : F] = [K : F] = |\operatorname{Gal}_F K| = |\operatorname{Gal}_E K|[\operatorname{Gal}_F K : \operatorname{Gal}_E K]$; division gives $[E : F] = [\operatorname{Gal}_F K : \operatorname{Gal}_E K]$.

Assume $\operatorname{Gal}_E K \lhd \operatorname{Gal}_F K$. Let $p(x) \in F[x]$ be irreducible with a root u in E. Since K is normal over F, $p(x)$ splits in K. Let v be a root of $p(x)$ in K. There exists $\sigma \in \operatorname{Gal}_F K$ with $\sigma(u) = v$. For any $\tau \in \operatorname{Gal}_E K$, normality implies that $\tau\sigma = \sigma\tau_1$ for some $\tau_1 \in \operatorname{Gal}_E K$. Now $\tau(v) = \tau(\sigma(u)) = \sigma(\tau_1(u)) = \sigma(u) = v$, so $v \in E$. Therefore, all roots of $p(x)$ are in E and E is a normal extension of F.

Conversely, assume that E is a normal extension of F. We want a surjective homomorphism $\theta\colon \operatorname{Gal}_F K \to \operatorname{Gal}_F E$ with kernel $\operatorname{Gal}_E K$. This will complete the proof. Let $\sigma \in \operatorname{Gal}_F K$ and restrict it to E. We want to know that the image lies in E; this follows from the normality of E over F, as any element $u \in E$ must be mapped to another root of its irreducible polynomial over F—but they are all in E. Thus σ restricts to an element of $\operatorname{Gal}_F E$, giving us our homomorphism θ. $\ker\theta$ is $\operatorname{Gal}_E K$ by definition. θ is surjective by Theorem 10.14 which says that any automorphism of E fixing F can be extended to the splitting field K (of some polynomial since we have a finite, normal extension). $\square$

See picture, page 384, for how this all works with $\mathbb{Q}(\sqrt[3]{2}, \omega)$, the splitting field of $x^3 - 2$.

Finite fields Let $K = \mathbb{F}_{p^n}$. K is a Galois extension of $\mathbb{Z}_p$ since $x^{p^n} - x$ has only simple roots. We will compute $\operatorname{Gal}_{\mathbb{Z}_p} K$. Let $\sigma(x) = x^p$ for $x \in K$. We have already seen that σ preserves addition. It clearly preserves multiplication, hence is a homomorphism. The kernel is zero since K is a field, and it is surjective since it is injective on a finite set. Therefore σ is an automorphism of K. Furthermore, $x^p = x$ has the p solutions $0, 1, 2, \ldots, p-1$, so the fixed field is $\mathbb{Z}_p$. Thus σ generates a subgroup of $\operatorname{Gal}_{\mathbb{Z}_p} K$ with fixed field $\mathbb{Z}_p$. By the fundamental theorem of Galois theory, this must be the whole group (or $\langle\sigma\rangle$ would have a larger fixed field). Thus $\operatorname{Gal}_{\mathbb{Z}_p} K$ is a cyclic group of order $[K : \mathbb{Z}_p] = n$.

For any intermediate field $F = \mathbb{F}_{p^m}$, $|\operatorname{Gal}_{\mathbb{Z}_p} K| = n = |\operatorname{Gal}_F K||\operatorname{Gal}_{\mathbb{Z}_p} F| = |\operatorname{Gal}_F K|m$, so again we see that $m \mid n$. And $\operatorname{Gal}_F K$ is the subgroup of $\operatorname{Gal}_{\mathbb{Z}_p} K$ generated by σ^m which carries $x \mapsto x^{p^m}$ (so that the order is n/m).

Greek geometric problems: squaring the circle, duplicating the cube, trisecting an angle.

16th century algebra problem: find a formula with radicals to solve any polynomial equation. See page 387 for quadratic and cubic formulas. A fourth degree formula also exists.

None of these are possible. The basis for this is work by Abel and Galois. The main ideas are the following:

(1) A **radical extension** of a field F is an extension K built up by a chain of simple extensions of polynomials of the form $x^n - a$. A polynomial equation $f(x) = 0$ is **solvable by radicals** if some radical extension contains a splitting field for F.
(2) A group G is **solvable** if it has a chain of subgroups $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \langle e \rangle$ such that each $G_i \lhd G_{i-1}$ and G_{i-1}/G_i is abelian.
(3) **(Galois' criterion)** Let F be a field of characteristic 0, $f(x) \in F[x]$. $f(x) = 0$ is solvable by radicals iff the Galois group of the splitting field K, $\operatorname{Gal}_F K$, is a solvable group.
(4) S_5 is not a solvable group, therefore polynomials such as $2x^5 - 10x + 5$, whose Galois group is S_5 are not solvable by radicals. That is, no general formula exists for degree greater than four.
(5) Compass and straight-edge constructions can only construct points in the plane that involve square roots. Thus constructible real numbers correspond to radical extensions involving only sequences of quadratic extensions—with corresponding groups having order a power of 2. Squaring the circle involves constructing π, which is transcendental. Duplicating the cube involves constructing the side of a cube of twice the volume, that is a root of $x^3 - 2$, not possible with a group of order a power of 2. Trisecting an angle of 60° involves finding a root of $x^3 - 3x - 1$ (see page 460).