# 6. Galois theory

6.1. **Introduction.** The basic idea of Galois theory is to study field extensions by relating them to their automorphism groups. Recall that an $F$-automorphism of $E/F$ is defined as an automorphism $\varphi : E \to E$ that fixes $F$ pointwise, that is, $\varphi(a) = a$ for all $a \in F$. The $F$-automorphisms of $E/F$ form a group under composition (you can think of this as a subgroup of $S(E)$). We call this the *Galois group* of $E$ over $F$ and denote it by

$$\mathrm{Gal}(E/F) = \{\varphi : E \to E : \varphi \text{ is an } F\text{-automorphism }\}.$$

Now consider an intermediate field $F \subseteq L \subseteq E$; I'll write $E/L/F$ to refer to this situation, but should issue a warning that this notation is non-standard. Then we can similarly consider the $L$-automorphisms

$$\mathrm{Gal}(E/L) = \{\varphi : E \to E : \varphi \text{ automorphism, } \varphi(a) = a \text{ for all } a \in L\}.$$

This is a subgroup of $\mathrm{Gal}(E/F)$ since any such $\varphi$ in particular leaves $F \subseteq L$ invariant. Conversely, if we are given a subgroup $H \subseteq \mathrm{Gal}(E/F)$, then we can introduce

$$\mathrm{Inv}(H) = \{a \in E : \varphi(a) = a \text{ for all } \varphi \in H\}.$$

We call $\mathrm{Inv}(H)$ the *fixed field* of $H$. This *is* a field because if $a, b \in \mathrm{Inv}(H)$ and $\varphi \in H$, then for example $\varphi(a - b) = \varphi(a) - \varphi(b) = a - b$, so $a - b \in \mathrm{Inv}(H)$, and similarly $ab^{-1} \in \mathrm{Inv}(H)$ if $b \neq 0$. It is also clear that $\mathrm{Inv}(H) \supseteq F$ because the elements of $F$ are in fact fixed by all automorphisms from the bigger group $\mathrm{Gal}(E/F) \supseteq H$. So $E/\mathrm{Inv}(H)/F$, and $\mathrm{Inv}(H)$ is an intermediate field.

*Exercise* 6.1. More generally, let $S \subseteq \mathrm{Gal}(E/F)$ be an arbitrary subset. Show that $\mathrm{Inv}(S) := \{a \in E : \varphi(a) = a \text{ for all } \varphi \in S\}$ is still an intermediate field. Then show that $\mathrm{Inv}(S) = \mathrm{Inv}(H)$, with $H = \langle S \rangle$, the subgroup generated by $S$, so this doesn't really give anything new.

So given a field extension $E/F$, we can pass from an intermediate field $L$ to the subgroup $\mathrm{Gal}(E/L)$ of $\mathrm{Gal}(E/F)$, and also conversely from a subgroup $H$ to the intermediate field $\mathrm{Inv}(H)$. We will be especially interested in situations where these two operations Gal, Inv are inverses of each other.

From the definitions it is only clear that if $E/L/F$ is a field extension and $H \subseteq \mathrm{Gal}(E/F)$ is a subgroup of the Galois group, then

$$\mathrm{Inv}\,\mathrm{Gal}(E/L) \supseteq L, \qquad \mathrm{Gal}(E/\mathrm{Inv}H) \supseteq H. \tag{6.1}$$

*Exercise* 6.2. Prove this please.

**Definition 6.1.** We call an algebraic extension $E/F$ a *Galois extension* (equivalently, we say that $E$ is *Galois* over $F$) if $\operatorname{Inv}\operatorname{Gal}(E/F) = F$.

Much of the foundational material of this section also works for not necessarily algebraic extensions, and I'll present it in this way. However, later on, we will be interested in finite extensions almost exclusively, so this added generality is not really essential.

*Example* 6.1. Consider $E = \mathbb{Q}(\sqrt{2})$ as an extension of $F = \mathbb{Q}$. Since $\sqrt{2}$ generates $E$, any $\mathbb{Q}$-automorphism $\varphi$ of $E$ is already determined by what it does on $\sqrt{2}$. The minimal polynomial of $\sqrt{2} \in E$ over $\mathbb{Q}$ is given by $f = x^2 - 2 \in \mathbb{Q}[x]$. Since $\varphi$ leaves $\mathbb{Q}$ invariant, $\sqrt{2}$ can only be mapped to another zero of $f$. This gives two potential automorphisms: the identity and $\varphi(\sqrt{2}) = -\sqrt{2}$. We observed above, after Definition 5.15, that conjugates can be mapped to each other by an $F$-homomorphism; this was a consequence of Lemma 5.14. More precisely, there is an $F$-homomorphism $\varphi : F(\sqrt{2}) \to F(-\sqrt{2})$ that sends $\sqrt{2} \mapsto -\sqrt{2}$. Since $F(\sqrt{2}) = F(-\sqrt{2}) = E$, this map is an $F$-automorphism of $E$.

So $\operatorname{Gal}(E/F) = \{1, \varphi\}$, with $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$, $a, b \in \mathbb{Q}$. It now follows that $E = \mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$ because if $\varphi(t) = t$ for $t = a + b\sqrt{2} \in E$, then $b = 0$, so no element $t \notin \mathbb{Q}$ of $E$ is fixed by $\varphi$.

*Exercise* 6.3. The automorphism $\varphi$ has a simple structure from an algebraic point of view. However, show that $\varphi$ is discontinuous everywhere on its domain $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$.

*Example* 6.2. Now let's discuss $E = \mathbb{Q}(2^{1/3})$ in the same style. As before, any $\varphi \in \operatorname{Gal}(E/\mathbb{Q})$ must map $2^{1/3}$ to one of its conjugates. The minimal polynomial of $2^{1/3}$ is $f = x^3 - 2$, which has only this one root, $2^{1/3}$, in $E$ (the other two roots in $\mathbb{C}$ are non-real). Thus we must map $\varphi(2^{1/3}) = 2^{1/3}$; in other words $\operatorname{Gal}(E/\mathbb{Q}) = 1$. Thus $\operatorname{Inv}\operatorname{Gal}(E/\mathbb{Q}) = E$, and $E/\mathbb{Q}$ is not a Galois extension.

This happened because the minimal polynomial of the adjoined element $2^{1/3}$ did not split in $E$ and we ran out of conjugates that $2^{1/3}$ could have been mapped to by an element of the Galois group. If we instead consider a splitting field $L = \mathbb{Q}(2^{1/3}, 2^{1/3}e^{2\pi i/3})$ of $f$, then $L$ contains (by construction) all three roots $a_1 = 2^{1/3}$, $a_2 = 2^{1/3}e^{2\pi i/3}$, $a_3 = 2^{1/3}e^{4\pi i/3}$ of $f = x^3 - 2$. Since $L = \mathbb{Q}(a_1, a_2)$, an automorphism is determined by what it does on $a_1, a_2$, and one can now show that all 6 conceivable choices $a_1 \mapsto a_j$, $a_2 \mapsto a_k$, with $j \neq k$ drawn from $1, 2, 3$, actually produce a $\mathbb{Q}$-automorphism.

*Exercise* 6.4. (a) Show that for any choice of $a_j \neq a_k$, we have that $L = \mathbb{Q}(a_j, a_k)$, $a_j \notin \mathbb{Q}(a_k)$.

(b) Show that for any choice of $a_j \neq a_k$, there is a $\varphi \in \mathrm{Gal}(L/\mathbb{Q})$ with $\varphi(a_1) = a_j$, $\varphi(a_2) = a_k$. *Suggestion:* Use part (a) and apply Lemma 5.14 twice, first to $\mathbb{Q}(a_1)$ and $\mathbb{Q}(a_j)$, and then to the full extensions.

(c) Deduce that $L/\mathbb{Q}$ is Galois.

As an example of the notions just discussed in an abstract setting, let us finally take a look at $\mathrm{Gal}(L/E)$. Recall that $L/E/\mathbb{Q}$, so $E$ is an intermediate field of $L/\mathbb{Q}$. We already know that $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, which, as we just saw, contains the six automorphisms corresponding to the six possible choices in $a_1 \mapsto a_j$, $a_2 \mapsto a_k$.

Now a $\varphi \in \mathrm{Gal}(L/E)$ must fix $E = \mathbb{Q}(a_1)$, so must send $a_1 \mapsto a_1$; conversely, any such map fixes all of $E$, of course. So $\mathrm{Gal}(L/E)$ contains the following two automorphism: (1) $a_1 \mapsto a_1$, $a_2 \mapsto a_2$, and this is just the identity; (2) $a_1 \mapsto a_1$, $a_2 \mapsto a_3$.

*Exercise* 6.5. We observed above that $\mathrm{Gal}(L/E)$ is always a subgroup of $\mathrm{Gal}(L/F)$ for an intermediate field $L/E/F$. Please verify that the two maps from $\mathrm{Gal}(L/E)$ that we just obtained indeed form a subgroup.

*Exercise* 6.6. What is $\mathrm{Gal}(L/\mathbb{Q})$ in this example (please find a familiar group that this Galois group is isomorphic to)?

*Exercise* 6.7. Consider $E/\mathbb{Q}$, where $E = \mathbb{Q}(2^{1/4}, i)$ is the splitting field of $f = x^4 - 2$. Find $[E : \mathbb{Q}]$ and show that $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$ and that $E$ is Galois over $\mathbb{Q}$.

*Exercise* 6.8. Consider $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. (a) Show that $f$ is irreducible; (b) show that if $r \in \mathbb{C}$ is a root of $f$, then so is $r^2 - 2$; (c) conclude that $\mathbb{Q}(r)$ is a splitting field for any such $r$; (d) find $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$.

*Exercise* 6.9. Show that every homomorphism $\varphi : F \to F$ fixes the prime field $P$ of $F$ pointwise. Conclude that $\mathrm{Aut}(F) = \mathrm{Gal}(F/P)$, if $F$ is viewed as an extension of its prime field.

*Exercise* 6.10. Show that $\mathbb{R}$ does not have any non-trivial (that is, $\varphi(a) \neq a$ for some $a \in \mathbb{R}$) automorphisms. *Hint:* Show that if $a < b$, then $\varphi(a) < \varphi(b)$ for any homomorphism. For this, start out with the case $a = 0$ and try to characterize the condition that $b > 0$ algebraically.

6.2. **The Galois connection.** We now return to the general situation and explore the *Galois connection* between (sub)groups of $F$-automorphisms and fixed (sub)fields in more detail. As we already discussed, we can move back and forth between these objects with the help of the operations Gal and Inv. It will be useful to temporarily simplify the notation, as follows: let $E/F$ be a field extension, and let $G = \mathrm{Gal}(E/F)$. Then, if $L$ is an intermediate field, $E/L/F$, we write $L^* := \mathrm{Gal}(E/L)$; as we observed above, $L^*$ is a subgroup of $G$. Similarly, if $H \subseteq G$ is a subgroup, then we write $H^* := \mathrm{Inv}\, H$; this is an intermediate field $E/H^*/F$.

So $*$ can mean either Gal or Inv, and which operation is meant depends on the context. There is no danger of confusion, however, because Gal is applied to intermediate fields while Inv must be applied to subgroups of automorphisms, so only one of the two possible interpretations of $*$ makes sense in any given situation.

**Proposition 6.2.** *Let $L \subseteq K$ be intermediate fields of a field extension $E/K/L/F$, and let $J \subseteq H \subseteq G := \mathrm{Gal}(E/F)$ be subgroups. Then:*
*(a) $K^* \subseteq L^*$ and $H^* \subseteq J^*$;*
*(b) $L^{**} \supseteq L$ and $H^{**} \supseteq H$;*
*(c) $L^{***} = L^*$ and $H^{***} = H^*$.*

*Proof.* Part (a) is clear from the definitions: for example, if $\varphi \in K^* = \mathrm{Gal}(E/K)$, then $\varphi(a) = a$ for all $a \in K$, so in particular this holds for all $a \in L \subseteq K$, and thus $\varphi \in L^* = \mathrm{Gal}(E/L)$. Part (b) is (6.1) restated in our new notation and was discussed in Exercise 6.2.

As for part (c), notice that $L^{***} = (L^*)^{**} \supseteq L^*$ by (b), but also $L^{**} \supseteq L$ by (b) again and thus $L^{***} \subseteq L^*$ by (a). The proof of $H^{***} = H^*$ is completely analogous. □

**Lemma 6.3.** *Let $E/K/L/F$ be a field extension, and suppose that $K/L$ is of finite degree. Then $[L^* : K^*] \leq [K : L]$.*

In particular, this can be applied to $K = E$, $L = F$ if $E/F$ is finite, and since $E^* = \mathrm{Gal}(E/E) = 1$, so $[L^* : E^*] = |L^*|$, it then says that $|\mathrm{Gal}(E/F)| \leq [E : F]$.

This statement is immediately plausible because if $a \in E \backslash F$, then we know that an automorphism can map $a$ only to one of its conjugates, and there are at most $\deg f_a$ of these (if we are unlucky, there are fewer, if $f_a$ doesn't split in $E$ or has multiple roots). This already settles the case $E = F(a)$, and in general, we would hope to be able to apply this step several times to deduce the result.

*Proof.* We organize the formal proof as an induction on $n = [K : L]$. If $n = 1$, then $K = L$, so $L^* = K^*$ and the claim becomes trivial.

Now assume that $n > 1$ and that the inequality holds for extensions $K'/L'$ of with $[K' : L'] < n$. If there is an intermediate field $M$ properly between $K$ and $L$, then $[K : M], [M : L] < n$, so the induction hypothesis can be applied to these extensions and we obtain that

$$[L^* : K^*] = [L^* : M^*][M^* : K^*] \leq [M : L][K : M] = [K : L].$$

Here, we use Exercise 2.37 for the first equality and Theorem 5.4 for the second one. (In fact, we use a version of Exercise 2.37 for potentially infinite groups.)

If there are no such intermediate fields $M$, then we can take any $a \in K \setminus L$, and we will have that $K = L(a)$ (otherwise $M = L(a)$ would be a proper intermediate field). Let $f_a \in L[x]$ be the minimal polynomial of $a$ over $L$. We then know that $\deg f_a = n$. Now consider a coset $\varphi K^* = \varphi \operatorname{Gal}(E/K) \in L^*/K^*$, $\varphi \in L^* = \operatorname{Gal}(E/L)$, and let $\varphi\psi$, $\psi \in K^*$, be an arbitrary element of this coset (also recall that the group operation in $L^*$ is composition, so this is the composition of the automorphisms $\varphi$, $\psi$). Since $\psi \in \operatorname{Gal}(E/K)$ fixes $K = L(a)$, we have that $(\varphi \circ \psi)(a) = \varphi(a)$. So all automorphisms from a fixed coset $\varphi K^*$ send $a$ to the same image. This image $\varphi(a)$ must be another root of $f_a$ because the coefficients of $f_a$ are in $L$ and are thus fixed by $\varphi$.

Moreover, if we now consider two distinct cosets $\varphi_j K^*$, then $\varphi_1$, $\varphi_2$ do *not* send $a$ to the same image: if they did, it would follow that $\varphi_1(b) = \varphi_2(b)$ for all $b \in K = L[a]$, so $\varphi_2^{-1}\varphi_1 \in \operatorname{Gal}(E/K) = K^*$ and hence $\varphi_1 K^* = \varphi_2 K^*$. So the representatives of a given coset can be described as *exactly* those automorphisms from $L^*$ that send $a$ to a certain fixed image. In particular, this says that there can be at most as many cosets as there are potential images of $a$, and we observed earlier that these are restricted to the roots of $f_a$, which is a degree $n$ polynomial. Thus $[L^* : K^*] \leq n$, as claimed. □

**Lemma 6.4.** *Let $E/F$ be a field extension, and write $G = \operatorname{Gal}(E/F)$. Suppose that $J, H$ are subgroups of $G$ with $J \subseteq H \subseteq G$ and that $[H : J]$ is finite. Then $[J^* : H^*] \leq [H : J]$.*

If $G$ is a finite group, then this can be applied to $J = 1$, $H = G$, and then it says $[E : \operatorname{Inv}(G)] \leq |G|$. If $E/F$ is also Galois, so $\operatorname{Inv}(G) = F$, then it follows that $[E : F] \leq |\operatorname{Gal}(E/F)|$, and when this is combined with the previous Lemma, we obtain that a finite Galois extension satisfies $[E : F] = |\operatorname{Gal}(E/F)|$. We already observed this situation in some of the concrete examples we discussed above. Later, we will see that this identity characterizes the Galois extensions among the finite extensions.

*Proof.* Fix representatives $\varphi_1 = 1, \varphi_2, \ldots, \varphi_n$ of the (left) cosets $\varphi J \subseteq H$; in other words, $H$ is the disjoint union of the $\varphi_k J$, $k = 1, \ldots, n$. If we had $[J^* : H^*] > [H : J] = n$, then we could find elements $a_1, \ldots, a_{n+1} \in J^* \subseteq E$ that are linearly independent over $H^* = \operatorname{Inv}(H)$.

Now consider the system of linear equations, in $E$,

$$\sum_{k=1}^{n+1} \varphi_j(a_k)x_k = 0, \qquad j = 1, \ldots, n. \tag{6.2}$$

Since this is a homogeneous system of $n$ equations for $n+1$ unknowns, it has non-trivial solutions $(x_1, \ldots, x_{n+1}) \neq (0, \ldots, 0)$. Among these, fix one with the smallest possible number of non-zero entries. By relabeling, we may assume that $x = (b_1, \ldots, b_N, 0, \ldots, 0)$, with $b_j \neq 0$. We may further assume that $b_1 = 1$ (if not, divide by $b_1$). We also know that not all $b_j$ are in $H^*$ because if they were, then (6.2) for $j = 1$ would show that the $a_j$ are linearly dependent over $H^*$, contrary to our assumption. For convenience, let's assume that $b_2 \notin H^*$. So there exists $\varphi \in H$ with $\varphi(b_2) \neq b_2$.

Now apply this automorphism $\varphi$ to all equations from (6.2). Recall that $\varphi\varphi_j$, $j = 1, \ldots, n$, still represent exactly the elements of $H/J$ (and each coset once); for example, this follows because a group acts on its left cosets in this way by left multiplication. Moreover, any automorphism $\psi \in \varphi_j J$ from a given coset sends $a_k$ to the same image because the $a_k$ were taken from $J^*$, so are fixed by the automorphisms from $J$. These remarks show that $y_j := \varphi(x_j)$ still solves (6.2); we have only reordered the equations. Now $y = (1, \varphi(b_2), \ldots, \varphi(b_N), 0, \ldots, 0)$ and $\varphi(b_2) \neq b_2$ by our choice of $\varphi$, so $x - y$ is a non-trivial solution of (6.2) with fewer non-zero entries than $x$, contrary to our choice of $x$. □

Let us now elaborate some on the observations we already made above, following the statement of Lemma 6.4. We would like to identify situations in which the inequalities from Lemmas 6.3, 6.4 become equalities. We introduce some additional terminology. Given a field extension $E/L/F$, we call an intermediate field $L$ *closed* if $L^{**} = L$. Similarly, a subgroup $H \subseteq \mathrm{Gal}(E/F)$ is called closed if $H^{**} = H$. So closed objects have the property that going back and forth with the Galois connection brings us back to the original object. An extension $E/F$ was defined to be Galois if (in the new terminology) $F$ is closed.

Intermediate fields can fail to be closed, as we saw in the examples above: consider again $E/F = \mathbb{Q}(2^{1/3})/\mathbb{Q}$ and $L = \mathbb{Q}$. Then $L^{**} = E$ since $L^* = \mathrm{Gal}(E/F) = 1$. (Finite subgroups of Galois groups are always closed, as we will see in a moment.) Proposition 6.2(c) implies that intermediate fields and subgroups of the form $X^*$ (in other words, everything that is obtained by applying Gal or Inv) are closed.

**Theorem 6.5.** *Let $E/K/L/F$ be a field extension. (a) If $L$ is closed and $[K : L]$ is finite, then $K$ is also closed and $[L^* : K^*] = [K : L]$.*

*(b) Write $G = \mathrm{Gal}(E/F)$. Let $J, H$ be subgroups of $G$ with $J \subseteq H \subseteq G$. If $J$ is closed and $[H : J]$ is finite, then $H$ is also closed and $[J^* : H^*] = [H : J]$.*

The following special cases are of particular interest.

**Corollary 6.6.** *(a) Let $E/F$ be a field extension. Then all finite subgroups of $\mathrm{Gal}(E/F)$ are closed.*
*(b) Let $K$ be an intermediate field of the Galois extension $E/F$. If $[K : F]$ is finite, then $K$ is closed, and thus $E$ is Galois over $K$.*

To prove part (a) of the Corollary, apply Theorem 6.5(b) to the finite subgroup $H \subseteq \mathrm{Gal}(E/F)$ and $J = 1$, and observe that $J = 1$ is closed. Similarly, part (b) follows by applying Theorem 6.5(a) with $L = F$. Notice that $L = F$ is closed here because $E$ was assumed to be Galois over $F$.

*Proof of Theorem 6.5(a).* We have that

$$[K : L] = [K : L^{**}] \leq [K^{**} : L^{**}] \leq [L^* : K^*] \leq [K : L]; \tag{6.3}$$

here, we've used that $L = L^{**}$ and $K \subseteq K^{**}$, and then we apply Lemmas 6.3 and 6.4. More explicitly, Lemma 6.3 shows us that the final inequality holds and $[L^* : K^*]$ is finite, and this fact in turn lets us use Lemma 6.4 to obtain the previous estimate. It then follows that all inequalities in (6.3) are equalities and $K^{**} = K$. □

*Exercise* 6.11. Prove part (b) in the same way.

Next, we would like to analyze which intermediate fields correspond to *normal* subgroups under the Galois connection. We introduce one more piece of terminology: we call an intermediate field $L$, with $E/L/F$ a field extension, *stable* if $\varphi(L) \subseteq L$ for all $\varphi \in \mathrm{Gal}(E/F)$. This requirement is somewhat reminiscent of being a fixed field, but it is much weaker: we only ask that $\varphi(a) \in L$ again for every $a \in L$, but we do not insist that $a$ gets mapped to itself.

If $L$ is stable and $\varphi \in G = \mathrm{Gal}(E/F)$, then $\varphi^{-1} \in G$ also, so $\varphi^{-1}(L) \subseteq L$ as well. Equivalently, $L \subseteq \varphi(L)$, so a stable intermediate field will in fact satisfy $\varphi(L) = L$ for all $\varphi \in G$.

**Lemma 6.7.** *(a) If $L$ is stable, then $L^* \trianglelefteq G$; (b) if $H \trianglelefteq G$, then $H^*$ is stable.*

*Proof.* (a) Let $\varphi \in L^* = \mathrm{Gal}(E/L)$ and $\psi \in G = \mathrm{Gal}(E/F)$. If $a \in L$, then also $\psi^{-1}(a) \in L$, as just observed, and $\varphi$ fixes the elements of $L$, so $\psi\varphi\psi^{-1}(a) = \psi\psi^{-1}(a) = a$. This says that $\psi\varphi\psi^{-1} \in L^*$, as required.

Part (b) is similar: if $a \in H^* = \mathrm{Inv}(H)$ and $\varphi \in G = \mathrm{Gal}(E/F)$, then for any $\psi \in H$, we have that $\varphi^{-1}\psi\varphi \in H$ as well, so $\psi\varphi(a) =$

$\varphi\varphi^{-1}\psi\varphi(a) = \varphi(a)$. This says that $\varphi(a) \in H^*$, so we have established that $H^*$ is stable, as claimed. □

The following formula is also useful and throws light from a slightly different angle on these issues. Consider again an intermediate field $E/L/F$, and write $G = \mathrm{Gal}(E/F)$, $H = L^* = \mathrm{Gal}(E/L)$. Let $\varphi \in G$. Then

$$\varphi H \varphi^{-1} = \varphi(L)^* = \mathrm{Gal}(E/\varphi(L)). \tag{6.4}$$

This confirms one more time that $H \trianglelefteq G$ if $L$ is stable (= part (a) of the Lemma).

*Exercise* 6.12. Prove (6.4).

**Theorem 6.8.** *Suppose that $E/F$ is a Galois extension, $f \in F[x]$ is irreducible (over $F$) and $f(a) = 0$ for some $a \in E$. Then $E$ contains a splitting field of $f$, and $f$ does not have multiple roots in $E$.*

The last statement means that (as expected, probably) the linear factors $x - c$ of $f$ in $E[x]$ are all distinct. We'll discuss multiple roots in some detail in the next section.

*Proof.* The coefficients of $f$ are from $F$, so any $\varphi \in G = \mathrm{Gal}(E/F)$ leaves these invariant. It follows that $\varphi(f(a)) = f(\varphi(a)) = 0$ also. Let $a_1 = a, a_2, \ldots, a_k$ be the complete list of the elements of the form $\varphi(a)$, $\varphi \in G$, and put $g(x) = \prod_{j=1}^{k}(x - a_j)$. (Why is this list finite?) Each $\varphi \in G$ permutes the $a_j$; in fact, $G$ acts on $\{a_1, \ldots, a_k\}$, by restricting automorphisms $\varphi \in G$ to this set. It follows that if we extend $\varphi \in G$ to $E[x]$ by sending $x \mapsto x$, then $\varphi(g(x)) = g(x)$. Since this holds for all $\varphi \in G$, the coefficients of $g$ (when multiplied out) lie in the fixed field $G^*$ of $G$, which is $F$, since we assumed $E$ to be Galois over $F$.

So $g \in F[x]$. Moreover, $g$ is monic, $g(a) = 0$, and $\deg g \le \deg f$ since the linear factors of $g$ are also linear factors of $f$ (in $E[x]$). However, $f$ is irreducible and thus its monic version $cf$ is the minimal polynomial of $a$. We conclude that $cf = g$, and our claims follow. □

**Theorem 6.9.** *Suppose that the extension $E/F$ is Galois. Then an intermediate field $L$ is Galois over $F$ precisely if $L$ is stable.*

Notice that here we are dealing with a slightly different scenario than previously considered: we make the intermediate field the new extension field and keep the ground field the same, rather than the other way around.

*Proof.* If $L$ is stable and $a \in L \setminus F$, then $\varphi(a) \neq a$ for some $\varphi \in \mathrm{Gal}(E/F)$, since $E/F$ is Galois. Since $L$ is stable, $\varphi(L) = L$, so the restriction of $\varphi$ to $L$ is in $\mathrm{Gal}(L/F)$, and thus $a \notin \mathrm{Inv}\,\mathrm{Gal}(L/F)$. This shows that $\mathrm{Inv}\,\mathrm{Gal}(L/F) = F$, as claimed.

Conversely, suppose now that $L/F$ is Galois. Take any $a \in L$, $\varphi \in \mathrm{Gal}(E/F)$, and consider the minimal polynomial $f \in F[x]$ of $a$; here, we are for the first time making use of the fact that Galois extensions are by definition algebraic. We see as in the proof of Theorem 6.8 that $\varphi(a) \in E$ is another (or perhaps the same) root of $f$. Moreover, Theorem 6.8 says that $f$ splits in $L$, so this field must contain this root. Thus $\varphi(a) \in L$; we have shown that $L$ is stable, as claimed. □

We have now collected quite a few facts about the Galois connection, and our patience finally pays off. We are ready to combine these to produce the *Fundamental Theorem of Galois Theory:*

**Theorem 6.10.** *Let $E/F$ be a finite Galois extension, and write $G = \mathrm{Gal}(E/F)$. Then the operation* Gal *sets up a bijection between the intermediate fields $L$ of $E/F$ and the subgroups $H$ of $G$, with inverse* Inv. *If $J \subseteq H \subseteq G$ are two such subgroups, then $[H : J] = [J^* : H^*]$; in particular, $|\mathrm{Gal}(E/F)| = [E : F]$.*

*For any intermediate field $L$, the extension $E/L$ is also Galois. Moreover, $L$ is Galois over $F$ if and only if $H \trianglelefteq G$, with $H = L^* = \mathrm{Gal}(E/L)$; in this case, $\mathrm{Gal}(L/F) \cong G/H$.*

When the Galois connection becomes a bijection, like here, it is more common to refer to it as the *Galois correspondence.*

*Proof.* We know from Corollary 6.6 that all subgroups of $G$ and all intermediate fields are closed. This shows that Gal and Inv are inverses of each other. In particular, these operations are injective, or, to spell this out more explicitly, suppose that $L^* = K^*$ for two intermediate fields $L, K$. Then $L = L^{**} = K^{**} = K$, so Gal is injective, as claimed, and of course the proof for Inv is completely analogous. The Galois correspondence is surjective because any subgroup $H = H^{**} = (H^*)^*$ is in the range of $* = \mathrm{Gal}$, and similarly for intermediate fields. The formula $[H : J] = [J^* : H^*]$ then follows from Theorem 6.5(b).

We already know that $E/L$ is always Galois, for any intermediate field $L$; this was stated above as Corollary 6.6(b). By combining Lemma 6.7 with Theorem 6.9, we then see that $L/F$ is Galois precisely if $H \trianglelefteq G$; here, we make use of the fact that $L^{**} = L$, which is needed when we apply Lemma 6.7(b).

To prove the statement about $G/H$, we first show that this quotient group is isomorphic to a *subgroup* of $\mathrm{Gal}(L/F)$. Consider the restriction homomorphism $\Phi : G \to \mathrm{Gal}(L/F)$ that sends an automorphism $\varphi \in G = \mathrm{Gal}(E/F)$ to its restriction $\varphi|_L$ to $L$. This *is* an element of

$\mathrm{Gal}(L/F)$ because $L$ is stable. It's also easy to check that $\Phi$ indeed is a (group) homomorphism. What is the kernel of $\Phi$? Obviously, $\Phi(\varphi) = \varphi\big|_L = 1$ precisely if $\varphi$ fixes all elements of $L$ or, equivalently, if $\varphi \in \mathrm{Gal}(E/L) = L^* = H$. So $G/H = G/\ker(\Phi) \cong \Phi(G) \subseteq \mathrm{Gal}(L/F)$, as claimed.

On the other hand, we also have that

$$|G/H| = |G|/|H| = [E : F]/[E : L] = [L : F] = |\mathrm{Gal}(L/F)|,$$

so $G/H$ is in fact isomorphic to the whole group $\mathrm{Gal}(L/F)$. □

*Exercise* 6.13. Return to the field extension $E/\mathbb{Q}$, $E = \mathbb{Q}(2^{1/3}, e^{2\pi i/3}2^{1/3})$ from Example 6.2. How many intermediate fields does the extension $E/\mathbb{Q}$ have? How many of these are Galois over $\mathbb{Q}$ (list those, please)?

6.3. **Separable and normal extensions.** We would now like to characterize Galois extensions in terms of other conditions that can (we hope) be easily verified. In fact, we will approach things from the other end: we try to identify potential problems that might prevent extensions from being Galois, and then we hope that an extension will be Galois whenever these problems can be ruled out. Eventually, we will find that Theorem 6.8 tells the whole story: the necessary conditions formulated there for an extension to be Galois will turn out to be sufficient as well.

To start our discussion of these issues, let's first observe that a *finite* extension $E/F$ is Galois if and only if $|\mathrm{Gal}(E/F)| = [E : F]$. Indeed, if $E/F$ is Galois, then the Galois group has the asserted order, as we stated above as part of the fundamental theorem. To prove the converse, apply Theorem 6.5(b) with $J = 1$, $H = G := \mathrm{Gal}(E/F)$ to deduce that $[E : L] = |G|$, with $L = G^*$, but this equals $[E : F]$ by assumption, so $F = L = F^{**}$ and $E/F$ is Galois, as claimed.

Recall also that we always have that $|G| \le [E : F]$, as we discussed in the paragraph following Lemma 6.3. So finite extensions fail to be Galois precisely if we have fewer automorphisms than expected, based on the degree of the extension.

If we focus for a moment on simple extensions $E = F(a)$ of degree $n$, so $n = \deg f_a$, then an $F$-automorphism is determined by what it does on $a$. Moreover, we must map $a$ to another (or the same) zero of $f_a$, and conversely, given such a zero $f(b) = 0$, there is a unique $F$-automorphism that sends $a \mapsto b$. The upshot of all this is that $F(a)/F$ will be Galois precisely if $f_a$ has $n$ distinct zeros in $F(a)$.

Recall again Example 6.2 in this context: we saw that $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois, and indeed the minimal polynomial $f(x) = x^3 - 2$ of $2^{1/3}$

has no other zeros in $\mathbb{Q}(2^{1/3})$, so there is only one automorphism (the identity).

A related problem is conceivable: the minimal polynomial $f_a$ could have zeros of higher multiplicity, and then there won't be the required $n$ distinct zeros in $F(a)$ even if this field is a splitting field of $f_a$. Here, we say that the root $b$ of the polynomial $f$ has *multiplicity* $m \geq 1$ if $f(x) = (x-b)^m g(x)$ with $g(b) \neq 0$. A root of multiplicity $m = 1$ is called *simple.*

So, to summarize: we have found two potential obstacles to a finite field extension being Galois. Minimal polynomials of elements of the extension field (over the ground field) could fail to split, and they could have roots of multiplicity $> 1$. We'll look at this second problem first.

A useful tool to study higher order zeros is the formal *derivative* of a polynomial $f = \sum a_j x^j \in F[x]$. As expected, we define it as

$$f'(x) := a_1 + 2a_2 x + \ldots + n a_n x^{n-1}; \tag{6.5}$$

we've made use of the usual (additive) exponential notation $2a_2 = a_2 + a_2$ etc. Definition (6.5) is of course motivated by the familiar calculus techniques that would apply to $f \in \mathbb{R}[x]$; however, from a formal point of view, it's just a formula that we pull out of a hat to define a new polynomial $f' \in F[x]$.

A computation now establishes that this formal derivative still obeys analogs of the sum and product rules:

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'$$

*Exercise* 6.14. Prove this please. Also, show that $(x-a)^m$ has derivative $m(x-a)^{m-1}$ for $m \geq 1$.

We are interested in formal derivatives mainly because they can be used to detect higher order zeros:

**Proposition 6.11.** *Let $f \in F[x]$, $\deg f \geq 1$. Then $a \in F$ is a root of multiplicity $m > 1$ if and only if $f(a) = f'(a) = 0$.*

*Proof.* If $a$ is a root of multiplicity $m$, then $f(x) = (x-a)^m g(x)$, so the product rule and Exercise 6.14 now give that $f' = m(x-a)^{m-1}g + (x-a)^m g'$. So if $m \geq 2$, then $f(a) = f'(a) = 0$, as claimed.

Conversely, suppose that $f(a) = f'(a) = 0$. Recall that $g(a) \neq 0$ in the formulae above, by the definition of the multiplicity $m$, so the condition that $f'(a) = 0$ forces $m > 1$, as claimed. □

In the context of field extensions, we will also want to analyze the multiplicity of zeros before they are actually available.

**Definition 6.12.** We say that a polynomial $f \in F[x]$ is *separable* if its zeros in a splitting field $E \supseteq F$ are all simple.

This definition makes sense because we have an $F$-isomorphism between any two splitting fields, which will thus send zeros to zeros again, so a multiple zero in one splitting field will lead to the same situation in any splitting field.

*Exercise* 6.15. Give a more explicit version of this argument please.

**Theorem 6.13.** *An irreducible polynomial $f \in F[x]$, $\deg f \geq 1$, is separable if and only if $f' \neq 0$.*

The condition really is that $f'$ is not the zero polynomial. That is not automatically true in fields of positive characteristic $p$. In this case, $ka_k = 0$ whenever $k$ is a multiple of $p$. In other words, if $\text{char}(F) = p$, then $f' = 0$ precisely if $f$ is of the form

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots + a_{np} x^{np},$$

or, equivalently, if $f(x) = g(x^p)$ for some $g \in F[x]$.

*Proof.* Observe first of all that since $f$ is irreducible and $\deg f' < \deg f$, we have that $(f, f') = 1$, unless $f' = 0$; in that case, $(f, f') = (f, 0) = f$. Recall also that since $F[x]$ is a PID, the gcd may be represented as $(f, f') = hf + kf'$, with $h, k \in F[x]$.

So if $f' \neq 0$, then there are $h, k \in F[x]$ so that $hf + kf' = 1$. Now pass to a splitting field $E \supseteq F$ of $f$. We see that $f, f'$ can't have a common zero $a \in E$ because then the LHS of our identity would vanish at $x = a$.

Conversely, if $f' = 0$, then, trivially, any zero $a$ of $f$ is a zero of $f'$ as well, so $f$ has multiple roots in a splitting field by Proposition 6.11 (in fact, we have seen that *all* roots are multiple). □

*Exercise* 6.16. Show that if $f \in F[x]$ is a general non-constant polynomial, not necessarily irreducible, then $f$ is separable if and only if $(f, f') = 1$.

*Exercise* 6.17. Let $f \in F[x]$ be an irreducible non-constant polynomial. Show that all roots, in a splitting field $E \supseteq F$, have the same multiplicity $m \geq 1$.

Now let $E/F$ be an algebraic field extension. We call an element $a \in E$ *separable* if its minimal polynomial $f_a \in F[x]$ is separable, that is, $f_a$ has only simple zeros in a splitting field. Similarly, we call the (algebraic, by assumption) extension $E/F$ *separable* if all $a \in E$ are separable in this sense. So separable field extensions are those for which we are not plagued by one of the potential problems (namely, multiple zeros) that we identified above. Notice also that separability is a property of *extensions,* relative to a ground field, not just of $E$ itself.

Theorem 6.8 says that Galois extensions are always separable. Moreover, what we did above gives the following:

**Corollary 6.14.** *Let $E/F$ be an algebraic extension. If* $\operatorname{char}(F) = 0$*, then $E/F$ is separable.*

This is immediate from Theorem 6.13 because we always have that $f' \neq 0$ for a non-constant $f \in F[x]$ in characteristic zero.

In positive characteristic, extensions can be inseparable. We observed above, after Theorem 6.13, that if $\operatorname{char}(F) = p > 0$, then $f' = 0$ if and only if $f(x) = g(x^p)$ for some $g \in F[x]$.

**Lemma 6.15.** *Assume that* $\operatorname{char}(F) = p$*. If $a \in F$, $a \notin F^p$, then $f(x) = x^p - a \in F[x]$ is irreducible and inseparable.*

Here I write $F^p := \{b^p : b \in F\}$ for the set of $p$th powers in $F$. Of course, if $a = b^p$ is a $p$th power, then $f = x^p - a$ is reducible because $f(b) = 0$, so $f$ has $x - b$ as a factor.

*Exercise* 6.18. Show (again, you did this earlier, in Exercise 4.16) that in a field of characteristic $p$, we have the formulae

$$(a + b)^p = a^p + b^p, \qquad (a - b)^p = a^p - b^p. \tag{6.6}$$

Then show that $a \mapsto a^p$ is a homomorphism, and thus $F^p$ is in fact a subfield.

This homomorphism $a \mapsto a^p$, in a field of characteristic $p$, is sometimes called the *Frobenius map.*

*Proof.* In a splitting field $E$, the polynomial $f$ has a zero $b \in E$, so $b^p - a = 0$, and then, by (6.6),

$$f(x) = x^p - b^p = (x - b)^p. \tag{6.7}$$

Let me now show that $f$ is irreducible over $F$. Since factors of $f \in F[x]$ from $F[x]$ stay factors in $E[x]$, we see from (6.7) that (after multiplying through by a suitable constant, to make them monic) these can only be of the form $g(x) = (x-b)^k$, and to obtain a *proper* factor, we'd have to have $1 \leq k \leq p - 1$. By multiplying out, we find that the constant term of $g$ is $\pm b^k$, so if $g \in F[x]$, then $b^k \in F$. Since $(p, k) = 1$ under our current assumptions, there are $m, n \in \mathbb{Z}$ so that $mp + nk = 1$. It now follows that $b = b^{mp+nk} = a^m (b^k)^n \in F$, so $a = b^p \in F^p$, contrary to our assumption.

So $f$ is irreducible, and *not* separable since $f' = 0$. In fact, (6.7) shows that $f$ has a single zero, of multiplicity $p > 1$, in a splitting field. □

*Example* 6.3. Let's now try to find a field $F$ to which the Lemma applies. Fix a prime $p$, and consider the field $F = \mathbb{Z}_p(t)$ of rational functions over $\mathbb{Z}_p$; it will become clear in a moment why we need an *infinite* field of positive characteristic to obtain an irreducible inseparable polynomial.

I claim that then $t \notin F^p$, so $a = t$ will work fine in Lemma 6.15. (Perhaps also let the general set-up sink in for a moment: our example of an inseparable polynomial will be $f = x^p - t \in F[x]$. The members of $F[x]$ are polynomials in $x$, with coefficients that are themselves rational functions of a second indeterminate $t$.)

We just check this claim by hand (and it's plausible right away, $t$ doesn't really look like it could be the $p$th power of a rational function). Suppose I had $t = (g(t)/h(t))^p$ for some $g, h \in \mathbb{Z}_p[t]$, $h \neq 0$. Then $g(t)^p = th(t)^p$, but if we now multiply out the $p$th powers with the help of (6.6), we obtain an equation of the form

$$g_0^p + g_1^p t^p + \ldots + g_m^p t^{mp} = t\left(h_0^p + h_1^p t^p + \ldots + h_n^p t^{np}\right).$$

So the exponents are off by 1, and since $p \geq 2$, this forces all coefficients to be equal to zero, but we specifically took $h \neq 0$ a moment ago.

A splitting field $E$ of $f$ is generated by a single zero, so $E = F(b)$, and the extension $E/F$ is not Galois, by Theorem 6.8.

*Exercise* 6.19. Find $[E : F]$ and $|\mathrm{Gal}(E/F)|$ in this example.

To round off our discussion of this topic, we make one more definition: we say that a field $F$ is *perfect* if every irreducible polynomial $f \in F[x]$ is separable. In this new terminology, Theorem 6.13 then implies that every field of characteristic zero is perfect. The positive characteristic case is clarified by:

**Theorem 6.16.** *Suppose that* $\mathrm{char}(F) = p$. *Then* $F$ *is perfect if and only if* $F^p = F$.

**Corollary 6.17.** *Every finite field is perfect.*

To obtain the Corollary from the Theorem, recall that the Frobenius map $F \to F$, $a \mapsto a^p$ is an injective homomorphism (why injective?) whose image is contained in $F^p$. If $F$ is finite, then it follows that $|F^p| \geq |F|$, and since also $F^p \subseteq F$, we conclude that $F^p = F$, as claimed in the Corollary.

*Proof of Theorem 6.16.* If $F^p \neq F$, then, by Lemma 6.15, $f = x^p - a$ with $a \in F$, $a \notin F^p$ is an irreducible, inseparable polynomial, so $F$ is not perfect.

Conversely, suppose now that $F$ is not perfect, and let $f \in F[x]$ be an irreducible, inseparable polynomial. By Theorem 6.13, we then have that $f' = 0$. As we discussed earlier, this means that

$$f = a_0 + a_p x^p + \ldots + a_{np} x^{np}.$$

Now if all coefficients were $p$th powers, say $a_{jp} = b_j^p$, $b_j \in F$, then we could use (6.6) to rewrite this as

$$f = (b_0 + b_1 x + \ldots + b_n x^n)^p = g(x)^p,$$

with $g \in F[x]$, but this contradicts our assumption that $f$ is irreducible. Thus at least one of the coefficients of $f$ is not in $F^p$. □

We now turn to the other (and in fact more obvious) potential problem, namely a lack of conjugates that elements of the extension field could be mapped to under automorphisms. We make one more definition.

**Definition 6.18.** Let $E/F$ be an algebraic field extension. We say that $E$ is *normal* over $F$ if every irreducible polynomial $f \in F[x]$ that has a zero in $E$ splits in $E$.

*Exercise* 6.20. Show that $E$ is normal over $F$ if and only if $E$ contains a splitting field of the minimal polynomial of every element of $E$.

Note that, just as for separability, this is a property of *extensions,* not of individual fields. Theorem 6.8 says that Galois extensions are normal.

**Theorem 6.19.** *Let $E/F$ be a finite field extension. Then $E$ is normal over $F$ if and only if $E$ is a splitting field of some $f \in F[x]$.*

The main point of this is the following: suppose we want a normal extension $E/F$. Then taking a splitting field of a polynomial $f$ is definitely a step in the right direction because it makes sure that at least for this particular polynomial $f$, all its zeros are in $E$. However, if we now take a different irreducible polynomial $g \in F[x]$ with a zero in $E$, will that split, too? That doesn't really seem clear, but the Theorem says it does.

*Proof.* Assume first that the extension is normal. Since it is also of finite degree, we can obtain $E$ from $F$ by adjoining finitely many elements, say $E = F(a_1, \ldots, a_n)$. We can now take $f = f_1 f_2 \cdots f_n$, where $f_j \in F[x]$ is the minimal polynomial of $a_j$, and then $E$ will be a splitting field of $f$, as desired.

*Exercise* 6.21. Give a more detailed version of this step please.

Conversely, suppose now that $E$ is a splitting field of $f \in F[x]$. So we can write $E = F(a_1, \ldots, a_n)$, and here $f(a_j) = 0$. Let $g \in F[x]$ be irreducible, with $g(b) = 0$ for some $b \in E$. We must show that $g$ splits in $E$. Let $K \supseteq E$ be a splitting field of $g$ over $E$. Notice that then $K$ is also a splitting field of $fg$ over $F$ (just check it against the definition: $K$ is generated over $F$ by the combined zeros of $f, g$, and it contains all these, so $fg$ splits).

I first claim that $\varphi(b) \in E$ for all $\varphi \in \mathrm{Gal}(K/F)$. To check this, it suffices to show that $\varphi(a_j) \in E$ for $j = 1, 2, \ldots, n$ because $E$ is generated by the $a_j$, so this will imply that $\varphi(E) \subseteq E$. This second version of the claim is clear, however, because $f(a_j) = 0$, so, since the coefficients of $f$ are fixed by $\varphi \in \mathrm{Gal}(K/F)$, we also have that $\varphi(f(a_j)) = f(\varphi(a_j)) = 0$, but $E$, being a splitting field of $f$, contains all zeros of $f$, so $\varphi(a_j) \in E$, as desired.

If $c \in K$ is an arbitrary root of $g$, then Lemma 5.14 gives us an $F$-isomorphism $\varphi_0 : F(b) \to F(c)$ that sends $b \mapsto c$. Now observe that $K$ is also a splitting field of $fg$ over both $F(b)$ and $F(c)$. Thus Theorem 5.17 (which, as you perhaps remember, was obtained by repeated application of Lemma 5.14) lets us extend $\varphi_0$ to an $F$-isomorphism $\varphi : K \to K$. In other words, we obtain a $\varphi \in \mathrm{Gal}(K/F)$ with $\varphi(b) = c$. So what we showed in the previous paragraph now implies that $c \in E$ as well. Since $c$ was an arbitrary zero of $g$, this says that $g$ already splits in $E$, as required. □

*Exercise* 6.22. Prove the following generalization of Theorem 6.19: Let $E/F$ be an algebraic extension. Then $E/F$ is normal if and only if $E$ is a splitting field over $F$ of a set of polynomials $\mathcal{P} \subseteq F[x]$.

**Theorem 6.20.** *Let $E/F$ be a finite field extension. Then the following are equivalent:*
*(a) $E$ is Galois over $F$;*
*(b) $|\mathrm{Gal}(E/F)| = [E : F]$;*
*(c) $E/F$ is a normal and separable extension;*
*(d) $E$ is a splitting field of a separable polynomial $f \in F[x]$.*

Note that the polynomial in part (d) does not have to be irreducible. This is crucial because it allows us to combine extensions by zeros of irreducible polynomials by just multiplying those together. We already saw this device in action in the proof of Theorem 6.19 above.

One part of the proof of Theorem 6.20 will be about counting automorphisms, when we deduce (b) from (d). This part will make use of the following Lemma, which is of some independent interest. We'll establish this first and then return to the Theorem.

**Lemma 6.21.** *Let $E$ be a splitting field of $f \in F[x]$, and let $g \in F[x]$ be an irreducible polynomial that splits in $E$. Let $b \in E$ be a fixed root of $g$, and let $K = F(b)$. Write $G = \mathrm{Gal}(E/F)$, $H = \mathrm{Gal}(E/K) \subseteq G$. Then, if $[G : H] = k$, then $g$ has $k$ distinct roots, and these may be obtained as $\varphi_j(b)$, $j = 1, 2, \ldots, k$, where the $\varphi_j \in G$ represent the cosets of $G/H$.*

*Proof.* As above, in the proof of Theorem 6.19, it follows that for any $\varphi \in G$, we have that $\varphi(g(b)) = g(\varphi(b)) = 0$, so $\varphi(b)$ is a root, too. Moreover, and again by the exact same argument as in that proof, we obtain *all* roots of $g$ in this way (if $c$ is another root, we can map $b \mapsto c$ and extend this map to an element $\varphi \in G$).

Now let's look at the natural action of $G$ on this set of roots; this just maps $(\varphi, c) \mapsto \varphi(c)$ for a root $c \in E$ and $\varphi \in G$. We just observed that this action is transitive. The stabilizer of $b$ contains exactly those $\varphi$ with $\varphi(b) = b$, but since $K = F(b)$, this is $\mathrm{Gal}(E/K) = H$. Thus the various claims are now immediate consequences of the natural correspondence between the orbit $Gb$ and the coset space $G/\mathrm{Stab}(b) = G/H$. (Review Theorem 3.16 and its proof perhaps if this isn't clear to you.) □

*Proof of Theorem 6.20.* We already know that (a) and (b) are equivalent. Moreover, and also as discussed earlier, Theorem 6.8 gives that (a) implies (c). To obtain (d) from (c), we argue as in the first part of the proof of Theorem 6.19. More explicitly, since the extension is finite, we have that $E = F(a_1, \ldots, a_n)$ for suitable elements $a_j \in E$. Now again take their minimal polynomials $f_j \in F[x]$, and let $f$ be the product of these, with the extra precaution that identical factors are not repeated (to keep the polynomial separable). Then, as before, $E$ is a splitting field of $f \in F[x]$. Moreover, $f$ is indeed separable: the irreducible factors of $f$ are minimal polynomials of elements of a separable extension, and we made sure (by not repeating irreducible factors) that distinct factors have distinct zeros also.

*Exercise* 6.23. This final step makes use of the following (easy) fact: if $f, g \in F[x]$ are irreducible monic polynomials and $f, g$ have a common zero in some extension $E \supseteq F$, then $f = g$. Prove this please.

Finally, we show that (d) implies (b). So we need to count automorphisms, and we organize the argument as an induction on $[E : F]$, with Lemma 6.21 providing the induction step. Of course, everything becomes trivial if $[E : F] = 1$ (= basis of our induction) because then $E = F$. So assume now (= induction step) that $[E : F] \geq 2$, and that $E'/F'$ satisfies the formula from part (b) whenever $E'$ is a splitting field of a separable polynomial over $F'$ with $[E' : F'] < [E : F]$.

Let $g \in F[x]$ be an irreducible factor of $f$ of degree $k \geq 2$ (what happens if $f$ does not have any such factor?). Let $b \in E$ be a zero of $g$, and put $K = F(b)$, so $K$ is an intermediate field of $E/K/F$. Note that $g$ is separable, so $g$ has exactly $k$ distinct roots. Now Lemma 6.21 shows that $[G : H] = k$, where $G = \mathrm{Gal}(E/F)$, $H = \mathrm{Gal}(E/K)$. We also have that $[K : F] = k$ because this is a simple extension by $b$, an element with a minimal polynomial (namely, $g$, up to a constant factor) of degree $k$. Moreover, $E$ is also a splitting field of $f \in K[x]$ over $K$, and $f$ is still separable (it's the same polynomial as before). Since this extension $E/K$ has smaller degree than $E/F$, the induction hypothesis applies: $E/K$ satisfies $|\mathrm{Gal}(E/K)| = |H| = [E : K]$. By putting things together, we now see that

$$|G| = [G : H]|H| = [K : F][E : K] = [E : F],$$

as desired. □

The next result explains the terminology, to some extent.

**Theorem 6.22.** *Let $E/F$ be a finite Galois extension. Let $L$ be an intermediate field, and write $H = \mathrm{Gal}(E/L)$, $G = \mathrm{Gal}(E/F)$. Then the following are equivalent:*
*(a) $L$ is normal over $F$;*
*(b) $L$ is stable, that is, $\varphi(L) = L$ for all $\varphi \in G$;*
*(c) $H$ is a normal subgroup of $G$.*

*Proof.* Essentially, we did this already. We know that (b) and (c) are equivalent, by combining the last part of the fundamental theorem with Theorem 6.9.

If (a) holds, then we obtain (b) from an argument that we already used in the proof of Theorem 6.19: Let $a \in L$. We want to show that $\varphi(a) \in L$ also for all $\varphi \in G$. Consider the minimal polynomial $f \in F[x]$ of $a$. This splits in $L$, by assumption, and the $\varphi(a)$ are zeros of $f$, so they must all be contained in $L$, as required.

Conversely, assume (b) now and let $f \in F[x]$ be irreducible and monic, with $f(a) = 0$ for some $a \in L$. We must show that $f$ splits in $L$. Again, this follows from an argument we have seen before (see the proof of Theorem 6.8). Let $a_1 = a, a_2, \ldots, a_n$ be the orbit $Ga = \{\varphi(a) : \varphi \in G\}$ of $a$ under $G$, and consider $g = \prod(x - a_j)$. Then $\varphi(g(x)) = g(x)$ for all $\varphi \in G$ because $\varphi$ just permutes the $a_j$. Thus $g \in F[x]$. The $a_j$ are zeros of the irreducible polynomial $f$, and thus cannot be zeros also of a polynomial from $F[x]$ of strictly smaller degree. It follows that $f = g$. The assumption that $L$ is stable gives that $a_j \in L$, so $f$ splits in $L$, as desired. (Alternatively, you could use Theorem 6.9 and the implication (a) $\implies$ (c) of Theorem 6.20, in this order, to deduce that $L/F$ is Galois, hence normal.) □

*Exercise* 6.24. Let $F = \mathbb{Q}$, $E = \mathbb{Q}(2^{1/4})$, $K = \mathbb{Q}(2^{1/2})$, so $E/K/F$ is a field extension. Show that both $E/K$ and $K/F$ are normal, but $E/F$ isn't.

*Exercise* 6.25. Let $K$ be an intermediate field of the normal extension $E/F$. Is it then true that $E/K$ is normal as well? How about $K/F$? Give a proof or counterexample. (If it helps, you can assume that $E/F$ is finite.)

*Exercise* 6.26. Let $f \in F[x]$ be irreducible, and let $E/F$ be Galois. Then $f$ might factor in $E[x]$ into irreducible (in $E[x]$) factors of smaller degree. Show that all of these have the same degree. Also, give an example where this common degree $k$ satisfies $1 < k < \deg f$. *Suggestion:* Let the elements of $\text{Gal}(E/F)$ act on the factorization of $f$ in $E[x]$.

If an algebraic extension $E/F$ fails to be normal, then the reason for this must be that elements are "missing" from $E$. More precisely, there is an $a \in E$ whose minimal polynomial does not split in $E$, but this we can rephrase as follows, if we work in the algebraic closure $\overline{E}$ of $E$. The polynomial $f_a$ has a zero $b \in \overline{E}$, $b \notin E$. A normal extension (that is also a subfield of $\overline{E}$) would be expected to contain all such $b$'s. This problem can be fixed by adjoining these elements, and if we do this in the most economical way possible, then we arrive at what we will call a *normal closure.* More precisely:

**Definition 6.23.** Let $E/F$ be an algebraic extension. We call an extension field $E' \supseteq E$ a *normal closure* if: (1) $E'/F$ is normal; (2) if $E''/F$ is also normal, with $E \subseteq E'' \subseteq E'$, then $E'' = E'$.

A more careful version of the procedure just described proves that normal closures always exist. More specifically, if $E/F$ is finite, say $E = F(a_1, \ldots, a_n)$, and these elements have minimal polynomials $f_j$, then we can take $E'$ as a splitting field of $f = f_1 f_2 \cdots f_n$ over $E$. Then $E' \supseteq E$, and since $E'$ is also a splitting field over $F$ (of the same polynomial $f$), is normal over $F$ by Theorem 6.19. This settles property (1) of the definition. Moreover, (2) is immediate from the definitions (of normal extensions and splitting fields): Any field between $E$ and $E'$ that is normal over $F$ must at least contain all the zeros of $f$, but these generate $E'$, so it must be all of $E'$.

If $E/F$ is only algebraic and not necessarily finite, then a version of this argument still works, if we make use of the result from Exercise 6.22. So indeed any algebraic extension has a normal closure.

**Proposition 6.24.** *The normal closure is essentially unique, in the sense that if $E', E'' \supseteq E$ are normal closures of $E/F$, then there is an $E$-isomorphism $\varphi : E' \to E''$.*

*Exercise* 6.27. Focus on the case of a finite extension $E/F$. Then deduce the Proposition from the uniqueness of splitting fields, as described in Theorem 5.17.

Please keep in mind that normal closures are defined for *extensions,* relative to a ground field. So it does not make sense to ask: what is the normal closure of $E = \mathbb{Q}(2^{1/3})$? This only becomes meaningful if we also provide a ground field, so what we *can* ask is:

*Exercise* 6.28. What is the normal closure of $E/\mathbb{Q}$ and of $E/E$?

Consider again our favorite example $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots in $\mathbb{C}$ are $a_j = 2^{1/3}\zeta^j$, $j = 0, 1, 2$, with $\zeta = e^{2\pi i/3}$, so $\zeta^3 = 1$. To construct a splitting field $E \subseteq \mathbb{C}$, it was not enough to adjoin just one of the roots; rather, we have that $E = \mathbb{Q}(a_j, a_k)$ for any two roots, and $\mathbb{Q}(a_j)$ is a strictly smaller field for any $j$. In other words, $E$ is not obviously a *simple* extension of $\mathbb{Q}$. But maybe we have that $E = \mathbb{Q}(b)$ anyway, for some other element $b \in E$. That is indeed the case here:

*Exercise* 6.29. Show that $E = \mathbb{Q}(b)$ for $b = 2^{1/3} + \zeta$.

We now study this question, when is a field extension $E/F$ simple, that is, when is there an $a \in E$ such that $E = F(a)$, in a general setting. First of all, here's a general criterion:

**Theorem 6.25.** *Let $E/F$ be a finite field extension. Then $E = F(a)$ for some $a \in E$ if and only if there are only finitely many intermediate fields.*

*Proof.* Assume first that the extension is simple, let's say $E = F(a)$ and let's denote the minimal polynomial of $a$ over $F$ by $f \in F[x]$. Let $L$ be an intermediate field, so $E/L/F$, and let $g \in L[x]$ be the minimal polynomial of $a$ over $L$. Then, since $f \in L[x]$ also, we have that $g|f$ in $L[x]$. I claim that $L$ can be recovered from $g$; more precisely, $L$ will turn out to be the field generated by the coefficients of $g$. This will prove that there are only finitely many intermediate fields because $f$ has only finitely many monic factors in $E[x]$.

Let $L'$ be this intermediate field that is generated by ($F$ and) the coefficients of $g$. So the situation is $E/L/L'/F$. Since $g \in L'[x]$, we conclude that $g$ is also the minimal polynomial of $a$ over $L'$. By our assumption, $E = L(a) = L'(a)$, so $[E : L] = [E : L']$ $(= \deg g)$, by Theorem 5.3. Thus also $[L : L'] = 1$, by Theorem 5.4, and this says that $L = L'$, as already announced above.

Conversely, assume now that $E/F$ has only finitely many intermediate fields. We want to show that $E = F(a)$ for some $a \in E$. That is clear if $F$ is a finite field because then $E$ is finite as well, so $(E^\times, \cdot)$ is cyclic by Theorem 4.27. In other words, $E^\times = \langle a \rangle$ for suitable $a \in E$, $a \neq 0$, and then we certainly also have that $E = F(a)$.

So let's now focus on the case when $F$ is infinite. I'll show that if $a, b \in E$ are any two elements, then we can always find a $c \in E$ such that $F(a, b) = F(c)$. Since the extension $E/F$ is finite, repeated application of this step will give the full claim.

*Exercise* 6.30. Give a more detailed version of this argument please.

Since there are only finitely many intermediate fields, the fields $F(a+tb)$, $t \in F$, cannot all be distinct, so we find $s, t \in F$, $s \neq t$, so that $F(a+sb) = F(a+tb) =: L$. We have that $b = (s-t)^{-1}(a+sb-(a+tb)) \in L$ and then also $a = a + sb - sb \in L$, so $F(a, b) = F(a + sb)$, as desired. □

*Exercise* 6.31. Show that a *transcendental* simple extension has infinitely many intermediate fields.

**Corollary 6.26.** *Let $E/F$ be a finite separable extension. Then $E = F(a)$ for some $a \in E$.*

*Proof.* We'll verify the criterion from Theorem 6.25. Consider the normal closure $E'/F$ of $E/F$. Construct this extension $E'$ as discussed above, after Definition 6.23. Recall that we obtain $E'$ as a splitting field of a certain polynomial $f \in F[x]$; more precisely, $f$ is a product of minimal polynomials $f_j$ of certain elements $a_j \in E$. These polynomials $f_j$ are separable, by assumption. Moreover, it is of course not necessary to repeat identical factors when building $f$ as this will not affect the splitting field anyway: $p = \prod g_j$ has the same splitting field as $q = \prod g_j^{k_j}$, $k_j \geq 1$. So we can keep $f$ separable as well (as you proved in Exercise 6.23, irreducible polynomials that are not constant multiples of one another do not have common zeros). This implies that the extension $E'/F$, being a splitting field of a separable polynomial, is Galois.

Moreover, $E'/F$ is also finite, so has a finite Galois group $G$, and the intermediate fields of $E'/F$ are in one-to-one correspondence to the subgroups of $G$, by the fundamental theorem. Since every intermediate field of $E/F$ is an intermediate field of $E'/F$ also, it follows that there are only finitely many of these. □

*Exercise* 6.32. Let $E/F$ be a finite Galois extension. (So $E = F(a)$ by the Corollary.) Let $b \in E$, and let $b_1 = b, b_2, \ldots, b_n$ be the orbit of $b$ under the action of the Galois group $G$.
(a) Show that the minimal polynomial of $b$ is given by $f(x) = \prod(x - b_j)$.
(b) Show that $E = F(b)$ if and only if $n = |G|$ (that is, no two elements of $G$ send $b$ to the same image).

*Exercise* 6.33. Return to the example $E = \mathbb{Q}(2^{1/3}, \zeta)$, $\zeta^3 = 1$, $F = \mathbb{Q}$; so $E$ is a splitting field of $f(x) = x^3 - 2$. Use the criterion from the previous Exercise to confirm one more time that $E = \mathbb{Q}(b)$ with $b = 2^{1/3} + \zeta$ (you did this earlier, in Exercise 6.29, by a direct argument). Then show that $\mathbb{Q}(c) \subsetneqq E$ if we take $c = 2^{1/3}(1 + \zeta)$.

6.4. **Finite and cyclotomic fields.** Usually, it's not easy to determine the Galois group of a given field extension. We now discuss two special types of extensions, where $\mathrm{Gal}(E/F)$ can be found without too much trouble. The fields we will encounter here are of considerable independent interest.

Recall that the cardinality of a finite field can only be a prime power, as we observed in Proposition 5.8; this follows by viewing such a field $F$ as a vector space over its prime field, which must be isomorphic to $\mathbb{Z}_p$, with $p = \mathrm{char}(F)$. Of course, $F$ is not just a vector space but also a field extension of $\mathbb{Z}_p$ (more generally, any field is an extension of its prime field).

**Theorem 6.27.** *Let $q = p^n$, $n \geq 1$, be a prime power. Then there is exactly one field $F$ with $|F| = q$, up to isomorphism. This field $F$ can be obtained as the splitting field of $f(x) = x^q - x \in \mathbb{Z}_p[x]$.*

*We have that $[F : \mathbb{Z}_p] = n$, and $F$ is Galois over $\mathbb{Z}_p$, with $\mathrm{Gal}(F/\mathbb{Z}_p)$ cyclic of order $n$.*

*Proof.* If $F$ is any field with $q$ elements, then the multiplicative group $F^\times$ has order $|F^\times| = q - 1$, so $a^{q-1} = 1$ for all $a \in F^\times$ and thus also $a^q = a$. This last identity obviously also holds for $a = 0$, so $f(a) = 0$ for all $a \in F$, with $f = x^q - x$, as above. So $F$ contains a total of $q = \deg f$ zeros of $f$, thus $f$ splits in $F$, and clearly $F$ is generated by these zeros; in fact, $F$ is equal to the collection of zeros. In other words, $F$ is a splitting field of $f$ over $\mathbb{Z}_p$, as claimed. This also settles uniqueness, by Corollary 5.18.

To actually obtain a field $F$ with $|F| = q$, let's just *define* $F$ as a splitting field of $f = x^q - x \in \mathbb{Z}_p[x]$ and see what happens. We have that $f' = -1$, so Proposition 6.11 shows that all roots of $f$ are simple. In other words, $f$ has $q$ distinct zeros in $F$.

Now if $a, b \in F$ are two such zeros, then also $f(a - b) = 0$, by (6.6), and (if $b \neq 0$) $f(a/b) = 0$. This says that the zeros of $f$ form a subfield of $F$, but $F$, being a splitting field, is generated by these zeros and the elements of $\mathbb{Z}_p$, which are zeros themselves, so $F$ doesn't contain anything else beside the zeros of $f$. (Note that we are in a very special situation here: normally there is of course no reason whatsoever why differences or quotients of zeros of a polynomial would be zeros of that same polynomial again.) So $|F| = q$, exactly as we had hoped.

It is of course clear that $[F : \mathbb{Z}_p] = n$ because a vector space of dimension $n$ over a field with $p$ elements has $p^n$ vectors (just count the linear combinations of basis vectors), so only this degree is consistent with $|F| = p^n$. The extension $F/\mathbb{Z}_p$ is Galois by Theorem 6.20(d); recall that we did establish above that $f$ is separable.

As for finding $G = \mathrm{Gal}(F/\mathbb{Z}_p)$, we can establish a more precise statement: I claim that $G = \langle \varphi \rangle$, where $\varphi(a) = a^p$ is the Frobenius map. We observed earlier that this is a field homomorphism (basically, this depended on (6.6)); also, $\varphi$ fixes $\mathbb{Z}_p$ (why again is that true?), so $\varphi \in G$ (and why is $\varphi$ bijective?). So it now suffices to show that the order of $\varphi$ in $G$ is $n$: this will imply that the cyclic subgroup of $G$ generated by $\varphi$ has $n$ elements, but this is the degree of the field extension, so $|G| = n$ by Theorem 6.20(b), and thus $\langle \varphi \rangle$ is already all of $G$, as claimed.

Now $\varphi^k(a) = a^{p^k}$ (don't get confused by the notation: the exponentiation $\varphi^k$ is done in $G$, so we are asked to apply $\varphi$ $k$ times). If this is the identity map, then $a^{p^k} - a = 0$ for all $a \in F$, but clearly this cannot happen for $k < n$ because the polynomial $g(x) = x^{p^k} - x$ has only $p^k$ zeros and thus cannot vanish for all $p^n$ elements of $F$. So $o(\varphi) \geq n$, and either by checking it directly or referring to the argument from the previous paragraph, it then follows that the order is equal to $n$. □

*Exercise* 6.34. Let $E$ be a finite field. Show that then any field extension $E/F$ is Galois, with cyclic Galois group.

A *cyclotomic* extension of $F$ is an extension by the $n$th roots of unity, or perhaps it's clearer to describe this as a splitting field of $f(x) = x^n - 1 \in F[x]$. The terminology (cyclotomic = circle cutting) refers to the situation when $F = \mathbb{Q}$ and we realize the splitting field as a subfield of $\mathbb{C}$: then the $n$th roots lie on the unit circle and are equally spaced. In fact, I'll only discuss this case ($F = \mathbb{Q}$) here.

If $E$ is such a splitting field of $f = x^n - 1 \in \mathbb{Q}[x]$, let's introduce the notation $W_n = \{a \in E : a^n = 1\}$ for the $n$th roots of unity. Then $|W_n| = n$, as we can see either by considering $f' = nx^{n-1}$ and using

Proposition 6.11, or (more easily, probably) by just pointing out that there are $n$ distinct roots in $\mathbb{C} \supseteq \mathbb{Q}$.

*Exercise* 6.35. For a general field $F$, how can it happen that $|W_n| < n$ in a splitting field?

If $a, b \in W_n$, then also $(ab^{-1})^n = 1$. This says that $W_n$ is a subgroup of $E^\times$. By Theorem 4.27, $W_n$ is a cyclic group. (Again, this is perfectly obvious without the need to appeal to any abstract theory if we just realize the splitting field as a subfield of $\mathbb{C}$.)

**Definition 6.28.** A *primitive* $n$th root of unity is a generator of the cyclic group $W_n$.

For example, if we do realize the splitting field as a subfield of $\mathbb{C}$, so $W_n \subseteq \mathbb{C}$ as well, then for $n = 4$, we have that $W_n = \{1, -1, i, -i\}$, and $\pm i$ are primitive 4th roots of unity, while $\pm 1$ are not primitive. For any $n$, $\zeta = e^{2\pi i/n}$ is always a primitive root; in fact, the situation is easy to clarify completely in the general setting:

**Proposition 6.29.** *Fix a primitive $n$th root of unity $\zeta$, so $W_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. Then $\zeta^k$ is primitive if and only if $(k, n) = 1$.*

*Exercise* 6.36. Prove Proposition 6.29.

By Proposition 6.29, the number of primitive roots equals the number of integers $1 \le k \le n$ that are relatively prime to $n$. This number is called *Euler's $\varphi$ function,* and it is denoted by $\varphi(n)$.

If $\zeta \in W_n$ is any primitive root, then the splitting field may be obtained as the simple extension $E = \mathbb{Q}(\zeta)$. Next, let's factor $f(x) = \prod_{w \in W_n}(x - w)$. The $n$th *cyclotomic polynomial* is obtained by only keeping the primitive roots: we define

$$\Phi_n(x) = \prod_{\zeta \in W_n \text{ primitive}} (x - \zeta).$$

Each $w \in W_n$ has a unique order $d$, and $d|n$; equivalently, if $w^n = 1$, then $w$ is a *primitive* $d$th root of unity for a unique $d|n$. Thus we obtain the factorization

$$f(x) = x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{6.8}$$

We derived this by working in the splitting field $E = \mathbb{Q}(\zeta)$. However, by repeated polynomial division, we in fact obtain from (6.8) that $\Phi_d \in \mathbb{Q}[x]$. More explicitly, we have that $\Phi_1(x) = x - 1$, and then (6.8) for $n = 2$ gives that $x^2 - 1 = \Phi_1\Phi_2$, so $\Phi_2 \in \mathbb{Q}[x]$ as well etc.

*Exercise* 6.37. Establish the following fact (this is an abstract version of what we use here): let $E/F$ be a field extension, let $f, g \in F[x]$, $h \in E[x]$ with $f = gh$. Then $h \in F[x]$ also.

*Exercise* 6.38. Give a Galois theoretic proof that $\Phi_d \in \mathbb{Q}[x]$, along the following lines: (1) Show that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois; (2) investigate the effect of letting a $\varphi \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ act on $\Phi_d \in \mathbb{Q}(\zeta)[x]$.

*Exercise* 6.39. Find $\Phi_n(x)$ for $n = 1, 2, \ldots, 6$.

*Exercise* 6.40. Show that $\Phi_{2^{k+1}}(x) = x^{2^k} + 1$.

Quite a bit more can be said.

**Theorem 6.30** (Gauß). *The cyclotomic polynomials $\Phi_d$ are irreducible, and $\Phi_d \in \mathbb{Z}[x]$.*

*Proof.* I'll discuss the (easier) second claim first. We just showed that $\Phi_d \in \mathbb{Q}[x]$. However, $f(x)$ on the left-hand side of (6.8) is from $\mathbb{Z}[x]$, and now repeated application of Theorem 4.44 (with $D = \mathbb{Z}$, $F = \mathbb{Q}$) shows that the factorization essentially takes place in $\mathbb{Z}[x]$. More precisely, it follows that there are $\alpha_d \in \mathbb{Q}$ with $\prod \alpha_d = 1$ and $\alpha_d \Phi_d \in \mathbb{Z}[x]$. Since both $f$ and the $\Phi_d$ are monic, we must have $\alpha_d = \pm 1$ here, and thus $\Phi_d$ itself is already in $\mathbb{Z}[x]$, as claimed.

To show that $\Phi_n$ is irreducible, fix a primitive $n$th root of unity $\zeta$, and let $f \in \mathbb{Q}[x]$ be its minimal polynomial over $\mathbb{Q}$. Then $f | \Phi_n$, since $\Phi_n(\zeta) = 0$ also, and our goal is to show that $f = \Phi_n$. As above, we obtain right away from Theorem 4.44 and the fact that both $\Phi_n$ and $f$ are monic that $f \in \mathbb{Z}[x]$.

If now $p$ is any prime not dividing $n$, then $\zeta^p$ is again primitive, by Proposition 6.29. Denote its minimal polynomial by $g \in \mathbb{Q}[x]$; in fact, we just showed that the minimal polynomial of a primitive root has integer coefficients, so $g \in \mathbb{Z}[x]$. Moreover, $g(x^p)$ has $\zeta$ as a zero, so we again conclude that

$$g(x^p) = f(x)h(x), \tag{6.9}$$

say, for some $h \in \mathbb{Q}[x]$, and this can again be sharpened to $h \in \mathbb{Z}[x]$ with the help of Theorem 4.44.

I now claim that $f(x), g(x)$ have a common zero in $\mathbb{Q}(\zeta)$ (which is a splitting field for $f, g$). Indeed, if this were not true, then, since $f, g$ both divide $\Phi_n$, which divides $x^n - 1$, in turn, it would follow that

$$x^n - 1 = f(x)g(x)k(x) \tag{6.10}$$

for some $k \in \mathbb{Z}[x]$ (this is becoming repetitive, but why again are the coefficients in $\mathbb{Z}$?). I now want to apply the (ring) homomorphism

$\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $a \mapsto \overline{a}$, $x \mapsto x$ to (6.9), (6.10). By (6.6), in $\mathbb{Z}_p[x]$ we have that $\overline{g}(x^p) = \overline{g}(x)^p$, so from (6.9) we learn that $\overline{g}(x)$ and $\overline{f}(x)$ have a common zero in a splitting field over $\mathbb{Z}_p$; in fact, *all* zeros of $\overline{f}$ are drawn from those of $\overline{g}$. This would give the right-hand side of (6.10) a multiple zero mod$p$, but this contradicts the fact that the derivative $\overline{n}x^{n-1}$ of the left-hand side is relatively prime to $x^n - 1$ itself. Here, we are using the extended version of Theorem 6.13 that was established in Exercise 6.16 and also our earlier assumption that $p \nmid n$ (how does that enter?).

So $f(x), g(x)$ do have a common zero, and since both polynomials are irreducible and monic, they are both equal to the minimal polynomial of this zero. Thus $f = g$.

Let's summarize: if $p \nmid n$, then the minimal polynomial $f$ of the primitive root $\zeta$ satisfies $f(\zeta^p) = 0$, so $f$ is also the minimal polynomial of $\zeta^p$. Now any primitive root is of the form $\zeta^k$, $(k, n) = 1$, so can be reached by exponentiating in this way a number of times. It follows that all primitive roots are zeros of $f$, and thus $f = \Phi_n$. □

It is now easy to clarify the nature of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$:

**Theorem 6.31.** *Let $\zeta$ be a primitive nth root of unity. Then* $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, *the extension is Galois, and* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$.

*Proof.* The first claim, on the degree of the extension, is immediate from Theorem 6.30 because this says that the minimal polynomial of $\zeta$ is $\Phi_n$, and $\deg \Phi_n = \varphi(n)$ (Euler's $\varphi$ function). Also, the extension is certainly Galois because $\mathbb{Q}(\zeta)$ is a splitting field of $\Phi_n$ over $\mathbb{Q}$.

An element of the Galois group is determined by what it does on $\zeta$, and $\zeta$ can be mapped exactly to the other roots of its minimal polynomial $\Phi_n$. These are exactly the primitive $n$th roots, so now Proposition 6.29 gives that for each $1 \le k \le n$ with $(k, n) = 1$, there is exactly one automorphism with $\zeta \mapsto \zeta^k$. Notice that these $k$'s represent the units of (the ring) $\mathbb{Z}_n$ (and each unit once). Thus this correspondence that associates $k \in \mathbb{Z}_n$ with the automorphism that sends $\zeta \mapsto \zeta^k$ provides the desired isomorphism between the Galois group and $U(\mathbb{Z}_n)$. The homomorphism property follows because $(\zeta^j)^k = \zeta^{jk}$. □

*Exercise* 6.41. Give a more explicit version of these final steps please. In fact, is it clear that if you map $U(\mathbb{Z}_n) \to G$ as indicated, then this map is well defined?

*Exercise* 6.42. Show that the (abelian) group $U(\mathbb{Z}_n)$ may or may not be cyclic, depending on the value of $n$. (Give concrete examples for both cases please.)

*Exercise* 6.43. Let $E \supseteq F$ be a splitting field of $f(x) = x^6 + 1 \in F[x]$. Find $[E : F]$ for $F = \mathbb{Z}_2$ and $F = \mathbb{Q}$.

Here's a spectacular application of cyclotomic polynomials:

**Theorem 6.32** (Wedderburn). *A finite division ring is a field.*

*Proof.* Call the division ring $D$, and let

$$C := \{a \in D : ad = da \text{ for all } d \in D\}$$

be its *center.* It's easy to check that $C$ is a field.

*Exercise* 6.44. Provide the details please.

So $|C| = q = p^k$ for some prime $p$ (in fact, we know that $p = \text{char}(D)$), and since we can view $D$ as a vector over $C$, we have that $|D| = q^n$ for some $n \geq 1$; the fact that at this point $D$ is not known to be commutative plays no role here since we actually ignore multiplication of elements of $D$ among themselves when we view $D$ as a $C$-vector space.

We now consider the group $(D^\times, \cdot)$ and let $D^\times = D \setminus 0$ act on itself by conjugation $(d, x) \mapsto dxd^{-1}$. (We secretly know that this will turn out to be the trivial action where each $d$ acts as the identity map, if we already assume the theorem.) Clearly, the center of the group $D^\times$ is $C^\times = C \setminus 0$, so the class equation for this action reads

$$|D^\times| = |C^\times| + \sum [D^\times : C(x_j)], \tag{6.11}$$

where the $x_j$ represent the conjugacy classes with more than one element, and $C(x_j) = \{a \in D^\times : ax_j = x_j a\}$; see Theorem 3.19. It's again straightforward to show that $F = C(x_j) \cup 0$ is a division subring (that is, a subring that is a division ring itself) of $D$; you can argue exactly as you did in Exercise 6.44 above. As usual, by viewing $F$ as a vector space over (the field) $C$, we see that $|F| = q^d$, with $d = \dim_C F$. I now want to apply an analog of Theorem 5.4 to conclude that $d|n$, $n = \dim_C D$, but here we definitely need to tread carefully because $F$ and $D$ haven't been shown to be commutative yet. Fortunately, that turns out not to be a problem: we still have analogs of the notions of linear independence and a basis. More specifically, call $d_1, \ldots, d_m$ linearly independent over $F$ if $\sum f_j d_j = 0$, with $f_j \in F$, implies that $f_1 = \ldots = f_m = 0$. Then, if $d_1, \ldots, d_m$ is a linearly independent set, any two linear combinations $\sum f_j d_j$ are distinct unless they have identical coefficients. This implies that $m$ cannot get arbitrarily large; more precisely, we must have that $|F|^m \leq |D|$. It follows that there is a maximal linearly independent set, in the sense that if any element is added to the set, then it will become linearly dependent. Such a set spans $D$ because otherwise it would not be maximal.

*Exercise* 6.45. Give a more explicit version of these steps please; notice that the assumption that $D$ is a division ring is used here.

By counting linear combinations for such a spanning set, we then obtain that $|D| = q^n = |F|^m = q^{dm}$, so $dm = n$ and thus indeed $d|n$, as claimed.

So we can now rewrite (6.11) as follows:

$$q^n - 1 = q - 1 + \sum_j \frac{q^n - 1}{q^{d_j} - 1}, \tag{6.12}$$

and here $d_j|n$ and in fact we also know that $d_j < n$ because otherwise $x_j$ would be in the center and the corresponding conjugacy class consists of a single point and would have been counted by the first term on the right-hand side of (6.12).

If $d|n$, then $x^d - 1|x^n - 1$ in $\mathbb{Z}[x]$ because $t - 1|t^k - 1$ (check this directly or just observe that $t = 1$ is a zero of $t^k - 1$) and then we can substitute $t = x^d$. Now recall that $x^n - 1 = \Phi_n(x)f(x)$, with $f \in \mathbb{Z}[x]$, and $x^d - 1$ does not have any zeros in common with $\Phi_n$ if $d < n$ because if $\zeta^d = 1$, then $\zeta$ certainly isn't a *primitive* $n$th root of unity. So $\Phi_n$ divides the polynomial $(x^n - 1)/(x^d - 1)$ (in $\mathbb{Z}[x]$) for any divisor $d$ of $n$ with $d < n$. Thus (6.12) implies that (the integer) $N = \Phi_n(q)$ divides $q - 1$ (in $\mathbb{Z}$).

However, $N = \prod(q - \zeta)$, where $\zeta \in \mathbb{C}$ ranges over the primitive $n$th roots of 1, and if $\zeta \neq 1$, then $|q - \zeta| > q - 1 \geq 1$. Hence if $n > 1$, then $N > q - 1$ and $N$ cannot divide $q - 1$. It follows that $n = 1$, but this says that $D = C$ is commutative, as desired. □

6.5. **Galois theory of equations.** In this final section, we discuss the famous classical results of Abel, Ruffini, Galois on the solvability by radicals (we'll make this notion precise in a moment) of polynomial equations $f(x) = 0$. Throughout this section, we make the following

> *basic assumption:* all fields have characteristic zero.

This will avoid some technical complications later on. As an immediate pay-off, we obtain that for any polynomial $f \in F[x]$, its splitting field $E$ is Galois over $F$.

*Exercise* 6.46. Prove this in more detail please.

In this sense, we can meaningfully speak of the Galois group $G = \mathrm{Gal}(E/F)$ of a polynomial $f \in F[x]$. Moreover, as we have observed (and used) a number of times already, $G$ acts on the zeros $a_1, \ldots, a_n \in E$ of $f$. Since $E = F(a_1, \ldots, a_n)$, a $\varphi \in G$ that acts as the identity map on $\{a_1, \ldots, a_n\}$ actually is the identity automorphism $1 \in G$. So the associated homomorphism $G \to S_n = S(a_1, \ldots, a_n)$ is injective; one usually expresses this fact by saying that the action is *faithful.*

Let's summarize: the Galois group $G$ of a polynomial $f \in F[x]$ is defined as $G = \mathrm{Gal}(E/F)$, where $E$ is a splitting field of $f$. If $f$ has $n$ distinct zeros, then $G$ can be naturally viewed as a subgroup of $S_n$. An element of $G$ corresponds to the permutation on these zeros it induces.

**Proposition 6.33.** *Let $f \in F[x]$ be a separable polynomial. Then $f$ is irreducible if and only if its Galois group acts transitively on the zeros.*

Recall that an action is called transitive if there is only one orbit, or, equivalently, if for any two points of the space acted on (here: for any two zeros of $f$), there is a group element that sends one to the other.

*Proof.* If $f$ is irreducible and $f(a) = f(b) = 0$, then there is a $\varphi \in G$ with $\varphi(a) = b$ by an argument we have already used a number of times, for example in the proof of Theorem 6.19: first of all, there is an $F$-isomorphism $F(a) \to F(b)$ that sends $a \mapsto b$, and this map can then be extended to an $F$-automorphism of the splitting field. Here, we make use of Lemma 5.14 and Theorem 5.17. Alternatively, Lemma 6.21, with $g = f$, gives the claim at once.

Conversely, suppose now that $G$ acts transitively on the zeros of $f$, and let $g \in F[x]$ be an irreducible factor of $f$. Let $a \in E$ be a zero of $g$, and let $b \in E$ be an arbitrary zero of $f$. By assumption, $b = \varphi(a)$ for some $\varphi \in G$. Since the coefficients of $g$ are fixed by $\varphi$, this implies that $g(b) = 0$ also. In other words, $f$ doesn't have any zeros that are not also zeros of $g$. So $g$ is the only irreducible factor of $f$, and thus $f = cg^k$ for some $k \geq 1$. Since $f$ is separable, we must have $k = 1$ here, and $f$ turns out to be irreducible, as claimed. □

Now consider a (monic) quadratic polynomial $f(x) = x^2 + px + q$, $p, q \in F$, and the associated equation $f(x) = 0$. Its solutions are given by the familiar formula

$$x = -p/2 \pm \sqrt{p^2/4 - q}. \tag{6.13}$$

Here, as usual, $2 := 1 + 1 \in F$, $4 := 1 + 1 + 1 + 1$; note that $2, 4 \neq 0$ because $\mathrm{char}(F) = 0$.

Of course, (6.13) needs to be interpreted suitably in an abstract setting because the square root is not a field operation. We can work in the algebraic closure $\overline{F}$ of $F$, and then define $\sqrt{a}$ as a zero of $x^2 - a$; there will be exactly two such zeros if $a \neq 0$ (here we use that $\text{char}(F) \neq 2$), and it doesn't matter which one we take because of the $\pm$ in (6.13).

There are really two aspects here that are interesting. First of all (and quite obviously), (6.13) produces the solutions of $f = 0$ in a systematic way from the coefficients of $f$, or it would be more precise to say that the formula reduces the task of solving $f = 0$ to the (simpler looking) equation $x^2 = a$, for $a = p^2/4 - q$. In addition to this, (6.13) also shows that a splitting field of $f$ can be constructed in a particular way, by adjoining a root of $x^2 - a$ for a suitable $a \in F$. We now make a precise definition that formalizes this second aspect.

**Definition 6.34.** A *simple radical extension* is a field extension $E/F$ of the form $E = F(a)$, with $a^k \in F$ for some $k \geq 1$. We call $E/F$ an *extension by radicals* if there is a sequence of intermediate fields $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$ such that each $K_j$ is a simple radical extension of $K_{j-1}$, for $j = 1, 2, \ldots, n$.

We say that a polynomial $f \in F[x]$ is *solvable by radicals* if there is an extension by radicals of $F$ that contains a splitting field of $f$.

So any quadratic polynomial is solvable by radicals. More precisely, the simple radical extension $E = F(a)$ by an $a \in \overline{F}$ with $a^2 = p^2/4 - q \in F$ is a splitting field, and here $[E : F] = 1$ or $= 2$, depending on whether or not $a \in F$.

We are now ready for the following spectacular achievement of Galois theory:

**Theorem 6.35** (Galois)**.** *Let $f \in F[x]$. Then $f$ is solvable by radicals if and only if the Galois group of $f$ is solvable.*

(Please review Section 3.6 now if you don't remember this material clearly.) Now that we have made this connection, the statement actually sounds quite plausible. The simple radical extensions $K_j/K_{j-1}$ from Definition 6.34 will somehow correspond to the abelian quotients $H_j/H_{j-1}$ from a normal series of the Galois group. Before we prove Theorem 6.35 in detail, let us enjoy some of its consequences.

**Corollary 6.36.** *Any $f \in F[x]$ with $\deg f \leq 4$ is solvable by radicals.*

*Proof.* As we discussed at the beginning of this section, the Galois group of $f$ can be viewed as a subgroup of $S_k$, where $k$ is the number of (distinct) zeros of $f$ in a splitting field. So $k \leq 4$ here, and thus these groups, together with their subgroups, are solvable. □

We knew this already for $\deg f = 2$, from (6.13), and the degree $3, 4$ cases can be handled directly, in the same way: there are explicit formulae that display the zeros of $f$ in terms of the coefficients, using field operations and roots. These formulae are not nearly as easy to find as in the degree 2 case, though.

For $n \geq 5$, $S_n$ is not solvable, and this means that there could be polynomials of degree $\geq 5$ that are not solvable by radicals; of course, it doesn't follow just yet because the Galois group is a *subgroup* of $S_n$, which could be solvable anyway. Let us now try to find such examples.

We'll do this for $F = \mathbb{Q}$. We can then conveniently construct our splitting fields as subfields of $\mathbb{C}$.

**Theorem 6.37.** *Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $p$, with $p \geq 5$ prime. Suppose that $f$ has exactly two non-real zeros (in $\mathbb{C}$). Then the Galois group of $f$ is $S_p$.*

*Proof.* Since $f$ is irreducible, it has exactly $p$ zeros $a_1, \ldots, a_p \in \mathbb{C}$, and the two non-real zeros are complex conjugates of each other because the coefficients of $f$ are real. Since $f$ is the minimal polynomial of each of the $a_j$'s, the splitting field $E = \mathbb{Q}(a_1, \ldots, a_p)$ has degree

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(a_1)][\mathbb{Q}(a_1) : \mathbb{Q}] = p[E : \mathbb{Q}(a_1)],$$

which is a multiple of $p$. This degree is also the order of the Galois group $G$, so Sylow's first theorem now shows that $G$ contains an element of order $p$.

Moreover, the complex conjugation automorphism $a \mapsto \overline{a}$ of $\mathbb{C}/\mathbb{Q}$ yields another element of the Galois group by restriction to $E \subseteq \mathbb{C}$. Here, we use that $\{a_1, \ldots, a_p\}$ is mapped back to itself: indeed, complex conjugation exchanges the two non-real roots and doesn't move the other (real) $a_j$'s at all. This description also clarifies the nature of this element of the Galois group when (again) viewed as a permutation on $\{a_1, \ldots, a_p\}$: it is a transposition.

Now the proof is finished by referring to Lemma 6.38 below. □

**Lemma 6.38.** *Suppose that $p \geq 2$ is a prime. Let $H \subseteq S_p$ be a subgroup that contains a transposition and a $p$ cycle. Then $H = S_p$.*

Recall that the order of a permutation is the lcm of its cycle lengths in its cycle decomposition, so the elements of order $p$ are exactly the $p$ cycles.

*Proof.* (Warning: There is one small point in the first part of this proof that I won't discuss very explicitly; I'll let you clarify in an Exercise.) Let's say the transposition is (12). If we keep applying the $p$ cycle $\alpha$, then 1 will move around and will eventually (or maybe quite soon) visit 2. So a suitable power of $\alpha$ will have the form $\alpha^k = (12\ldots)$, and by relabeling the remaining points $3, 4, \dots, p$ if necessary, we may now also assume that $\alpha^k = (1234 \dots p)$.

Now I'll just repeat what you did (much) earlier in Exercise 2.63(a), (b): we obtain that $(23) = (123 \dots p)(12)(123 \dots p)^{-1} \in H$, but then also $(13) = (23)(12)(23) \in H$. By repeating this procedure, we see that $(1j) \in H$ for all $j$. Then it follows that all transpositions $(jk) = (1k)(1j)(1k)$ are in $H$, and $S_p$ is generated by these. □

*Exercise* 6.47. Show that $S_4$ is *not* generated by (12), (1324). So I must have used the assumption that $p$ is a prime somewhere in the proof of Lemma 6.38 if the argument was correct. Where exactly?

*Example* 6.4. Now, with the help of Theorem 6.37, it's easy to produce examples of polynomials with non-solvable Galois group. Let's take a look at $f(x) = x^5 - 4x + 2$. First of all, this polynomial is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion, Theorem 4.45, with $p = 2$. We verify the condition that $f$ has exactly two non-real zeros by basic calculus: $f(0) = 2 > 0$, $f(1) = -1$, and $f(x) \to \pm\infty$ as $x \to \pm\infty$, so there are at least three real zeros by the mean value theorem. Then an investigation of the derivative $f'(x) = 5x^4 - 4$ shows that there are exactly three real zeros. Indeed, $f'$ has only two real zeros, at $\pm(4/5)^{1/4}$, but Rolle's Theorem says that there is a zero of $f'$ between any two zeros of $f$, so $f$ can't have more than three (real) zeros.

So the Galois group of $f$ is $S_5$, by Theorem 6.37, which is not solvable. Thus Theorem 6.35 implies that $f$ is not solvable by radicals: it is not possible to reach the zeros by combinations of field operations and extraction of roots, applied to rational numbers, and that's true whether these rational numbers are related to the coefficients of $f$ or not!

*Exercise* 6.48. Let $f \in \mathbb{Q}[x]$ be as in Theorem 6.37, with zeros $a_1, \dots, a_p$. Recall from Exercise 5.16 that the splitting field is always obtained by adjoining any $p - 1$ zeros: $E = \mathbb{Q}(a_1, \dots, a_{p-1})$. Show that in the case at hand, $E$ *not* generated by $p - 2$ of the zeros.

Let's now prove Theorem 6.35. In outline, we already know what we want to do (see the paragraph following the theorem), but there are some technical issues we'll have to address. We prepare for the proof with a number of auxiliary statements.

**Lemma 6.39.** *Let $E_1, E_2$ be intermediate fields of $L/F$, and suppose that $E_j/F$, $j = 1, 2$, are extensions by radicals. Then $F(E_1 \cup E_2)$, the field generated by $E_1$ and $E_2$, also is an extension by radicals.*

*Proof.* Let's say we reach $E_1$, starting from $F$, by successively adjoining the radicals $a_1, \dots, a_m$ (so $a_j^{n_j}$ is in the previous field for suitable $n_j \geq$

1), and, similarly, $E_2$ is obtained by adjoining $b_1, \ldots, b_n$. Then we get to $F(E_1 \cup E_2) = F(a_1, \ldots, a_m, b_1, \ldots, b_n)$ by adjoining, say, first the $a_j$'s and then the $b_j$'s, and each individual step is still a simple radical extension (possibly of smaller degree than before in the case of the $b_j$). □

This has the following important consequence:

**Lemma 6.40.** *If $E/F$ is an extension by radicals, then so is its normal closure.*

*Proof.* Denote a normal closure by $E'$, and recall our construction of $E'$ from Definition 6.23 and the discussion following the definition: if $a_1, \ldots, a_n$ are the radicals that are adjoined to get from $F$ to $E$, then $E'$ may be obtained as a splitting field of $f = f_1 f_2 \cdots f_n$, where $f_j \in F[x]$ is the minimal polynomial of $a_j$ over $F$. So $E'$ is generated over $F$ by the zeros of $f$. The $a_j$ are among these zeros, and by Proposition 6.33 (or Lemma 6.21), applied to the individual factors $f_j$, we can obtain the other zeros by letting $G = \text{Gal}(E'/F)$ act on the $a_j$. Recall in this context that in characteristic zero, irreducible polynomials are automatically separable.

If we apply a fixed automorphism $\varphi \in G$ to a simple radical extension $K(b)/K$, then we obtain another such simple radical extension $\varphi(K(b))/\varphi(K)$. This much is obvious because $\varphi(K(b)) = \varphi(K)(\varphi(b))$ (prove this more explicitly please if you are not sure), and if $b^n \in K$, then also $\varphi(b)^n = \varphi(b^n) \in \varphi(K)$. It then follows that if $K/L$ is an extension by radicals, then so is $\varphi(K)/\varphi(L)$, by just applying this observation to the sequence of *simple* radical extensions that get us from $L$ to $K$.

Now the Lemma follows because $E'$ is generated by the fields $\varphi(E)$, $\varphi \in G$; this follows from our observations made at the beginning of the proof because, taken together, these fields contain all zeros of $f$. Moreover, the field $E'$ that they generate is an extension by radicals by Lemma 6.39 and what we just discussed. □

An obvious question that we certainly want to look at here at some point is: what is the Galois group of a simple radical extension? In fact, we already know from the example $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ that we discussed long ago that a simple radical extension need not be Galois; see Example 6.2. We will avoid this problem here by adjoining suitable roots of unity to our fields, and then the situation becomes very pleasant:

**Lemma 6.41.** *Assume that $F$ contains a primitive $n$th root of unity, and let $a \in F$. Let $b \in E$ be a root of $f(x) = x^n - a \in F[x]$ in an* *extension $E/F$. Then $F(b)$ is a splitting field of $f$, and the Galois group* $\mathrm{Gal}(F(b)/F)$ *of $f$ is cyclic.*

*Proof.* This is very similar to what we did in the previous section in analogous situations; see for example the proof of Theorem 6.31. Let $\zeta \in F$ be a primitive $n$th root of unity. Then $\zeta^j b$ is a zero of $f$ also for arbitrary $j = 0, 1, \ldots, n-1$, and these are $n$ distinct zeros (unless $b = 0$, but then $a = 0$ also and everything becomes trivial), so $f$ splits in $E = F(b)$, as claimed.

An element of $G = \mathrm{Gal}(E/F)$ must send $b$ to another root of $f$, so $b \mapsto \zeta^j b$ for some $j$. We obtain a map $G \to \mathbb{Z}_n$ that sends a $\varphi \in G$ to the $j \in \mathbb{Z}_n$ with $\varphi(b) = \zeta^j b$ (note that since $\zeta^n = 1$, we are free to add multiples of $n$ in the exponent, so it is natural to view this as a map to $\mathbb{Z}_n$). This map is a (group) homomorphism because if $\varphi, \psi \in G$ correspond in this way to $j$ and $k$, respectively, then, since $\zeta \in F$ is fixed by elements of the Galois group, we have that $\varphi\psi(b) = \varphi(\zeta^k b) = \zeta^k \varphi(b) = \zeta^{j+k} b$. This homomorphism $G \to \mathbb{Z}_n$ is injective because $E = F(b)$, so if $\varphi(b) = b$, then $\varphi \in G$ is the identity automorphism.

So $G$ is isomorphic to a subgroup of the cyclic group $\mathbb{Z}_n$ and thus cyclic itself. □

Of course, $G$ need not be isomorphic to the full group $\mathbb{Z}_n$ here. For example, we could have $a = b^n$ for some $b \in F$, and then $E = F$ and $G = 1$.

*Exercise* 6.49. Give a (less trivial) example of an $a \in F$ (take $F = \mathbb{Q}(\zeta)$ perhaps, $\zeta$ a primitive $n$th root of unity) for which the Galois group $G$ of $x^n - a$ is isomorphic to a proper subgroup of $\mathbb{Z}_n$ (but $G \neq 1$). Can you in fact characterize, in terms of a condition on $f = x^n - a$, when $G \cong \mathbb{Z}_n$ happens?

We are now ready for the

*Proof of Theorem 6.35, first part.* In this part, I will show that if $f$ is solvable by radicals, then $f$ has a solvable Galois group. So let $K_0 = F, K_1, \ldots, K_N$ be a sequence of simple radical extensions, such that $L = K_N$ contains a splitting field $E$ of $f$. By Lemma 6.40, the normal closure of $L/F$ will then also be an extension by radicals, so we can right away assume that $L$ is normal over $F$, and thus also Galois, by Theorem 6.20(c), because extensions in characteristic zero are always separable. Moreover, $E$, being a splitting field, is also Galois over $F$. Thus, by the fundamental theorem, $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/F)$ and $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(L/F)/\mathrm{Gal}(L/E)$. We want to show that $\mathrm{Gal}(E/F)$

is solvable, but since quotients of solvable groups are solvable, it now suffices to show that $\mathrm{Gal}(L/F)$ is solvable.

Let $n_1, n_2, \ldots, n_N$ be the exponents of the individual simple radical extensions: so if $K_j = K_{j-1}(a_j)$, then $a_j^{n_j} \in K_{j-1}$ (it's natural to take $n_j \geq 1$ as the smallest such integer, but we actually don't need this). Let $n = n_1 n_2 \cdots n_N$, and adjoin a primitive $n$th root $\zeta$ of unity to $F$ ($F$ might already contain such a $\zeta$, of course, and then we do nothing). As we just discussed, $L$ is Galois over $F$. By Theorem 6.20(d), this means that $L$ is the splitting field of a (separable) polynomial $g \in F[x]$. It then follows that $L(\zeta)$ is also Galois over both $L$ and $F$ because this field is still a splitting field, of $x^n - 1$ and $(x^n - 1)g(x)$, respectively. This latter polynomial may or may not be separable, but this is not really an issue here because a polynomial can only fail to be separable in characteristic zero if some of its (automatically separable) irreducible factors are repeated, and then we can just drop these extra factors and the polynomial becomes separable and still has the same zeros as before.

Moreover, $L(\zeta)/F$ is still an extension by radicals: everything is as before, and there is one extra simple radical extension, by $\zeta$ (if $\zeta \notin L$). So, by the same argument as above, it now suffices to show that $\mathrm{Gal}(L(\zeta)/F)$ is solvable.

To do this, we actually adjoin $\zeta$ (if necessary) in the very first step. So the situation is as follows now: we have a sequence of simple radical extensions

$$F = K_0 \subseteq K_1 = F(\zeta) \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_{N+1} = L(\zeta);$$

for $j \geq 2$, we have that $K_j = K_{j-1}(a_j)$, $a_j^{n_j} \in K_{j-1}$ and also $\zeta \in K_{j-1}$. We now consider the corresponding Galois groups $G_j = \mathrm{Gal}(L(\zeta)/K_j)$. Each extension $K_j/K_{j-1}$ is Galois: this follows form Lemma 6.41 for $j \geq 2$, and $K_1 = F(\zeta)$ is a splitting field of $x^n - 1$ over $F$. Note that Lemma 6.41 does apply here because $K_{j-1}$ for $j \geq 1$ also contains an $n_j$th primitive root of unity. Indeed, $n_j | n$, so $n = n_j k_j$, and then $\zeta^{k_j}$ is such an $n_j$th primitive root.

Since $K_j$ is Galois over $K_{j-1}$, the fundamental theorem shows that $G_j \trianglelefteq G_{j-1}$, and $G_{j-1}/G_j \cong \mathrm{Gal}(K_j/K_{j-1})$. These groups are abelian, by Lemma 6.41 for $j \geq 2$, and by a generalized version of results from the previous section for the extension $K_1/K_0 = F(\zeta)/F$.

*Exercise* 6.50. Give more details concerning this last claim please. More specifically, show that for any field $F$ of characteristic zero, $\mathrm{Gal}(F(\zeta)/F)$ is isomorphic to a subgroup of $U(\mathbb{Z}_n)$. *Suggestion:* Proceed exactly as in the proof of Theorem 6.31. (Note that we are making a weaker claim here than in the more specific situation when $F = \mathbb{Q}$, which should be relatively easy to establish.)

Putting things together, we now see that

$$\mathrm{Gal}(L(\zeta)/F) = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{N+1} = 1$$

is a normal series for the Galois group with abelian (in fact, cyclic, except possibly for $j = 1$) quotients $G_{j-1}/G_j$, so this group is solvable, as desired. □

For the proof of the other direction, we will need a partial converse of Lemma 6.41. In the proof of this statement, we will make use of the following formula, valid for any $n$th root $w \neq 1$ of unity in any field:

$$1 + w + w^2 + \ldots + w^{n-1} = 0 \tag{6.14}$$

Of course, if $w = 1$, then the sum equals $n1$.

*Exercise* 6.51. Prove (6.14).

**Lemma 6.42.** *Let $E/F$ be a Galois extension with $[E : F] = p$, $p$ a prime. Assume that $F$ contains a primitive $p$th root of unity. Then $E = F(a)$ is a simple radical extension of $F$ by a $p$th root (so $a^p \in F$).*

Note that under these assumptions, $|\mathrm{Gal}(E/F)| = p$, so the Galois group is automatically cyclic, of order $p$.

*Proof.* Fix a generator $\varphi \in \mathrm{Gal}(E/F)$ of the cyclic Galois group, and let $b \in E$, $b \notin F$. Let $w \in F$ be a $p$th root of unity (not necessarily primitive; in other words, $w = 1$ is possible), and introduce the *Lagrange resolvent*

$$L(w, b) = b + w\varphi(b) + w^2\varphi^2(b) + \ldots + w^{p-1}\varphi^{p-1}(b);$$

here $\varphi^j(b)$ means $\varphi$ applied $j$ times to $b$. Then $\varphi(L(w, b)) = w^{-1}L(w, b)$, since $w \in F$ is fixed by $\varphi$. Thus $\varphi(L^p) = L^p$. Since $\varphi$ generates the whole Galois group and the extension is Galois, this means that $L(w, b)^p \in F$.

Now let $\zeta \in F$ be a *primitive* $p$th root of unity. I claim that then $L(\zeta^k, b) \notin F$ for at least one value of $k = 0, 1, \ldots, p - 1$. To see this, consider

$$\sum_{k=0}^{p-1} L(\zeta^k, b) = \sum_{j=0}^{p-1} \varphi^j(b) \sum_{k=0}^{p-1} \zeta^{jk} = pb.$$

We evaluated this last sum over $k$ with the help of (6.14), with $w = \zeta^j$. This is a $p$th root of unity, and it is equal to 1 precisely if $j = 0$. Since $pb \notin F$ (this step uses that $\mathrm{char}(F) = 0$), it cannot be the case that $L(\zeta^k, b) \in F$ for all $k$, exactly as claimed.

Now we can take $a = L(\zeta^k, b)$, where $k$ is chosen such that $a \notin F$. Then, as we saw above, $a^p \in F$, and $F(a)$ is an intermediate field $\supsetneqq F$ of $E/F$. However, this extension had prime degree $p$, so does not have proper intermediate fields, and thus it follows that $F(a) = E$. □

As a final preparation, we again take a look at the effect of adjoining extra elements to a given extension:

**Lemma 6.43.** *Let $G$ be the Galois group of $f \in F[x]$ over $F$, and let $E$ be an extension field of $F$. Then the Galois group $H$ of $f$ over $E$ is isomorphic to a subgroup of $G$.*

*Proof.* Let's spell out the set-up more explicitly: we have that $H = \mathrm{Gal}(L/E)$, where $L$ is a splitting field of $f$ over $E$. So $L = E(a_1, \ldots, a_n)$, where the $a_j$ form the complete list of zeros of $f$ (we don't really need all of them here, to generate the splitting field, but this agreement will come in handy in a moment). Then $K = F(a_1, \ldots, a_n)$ is a splitting field of $f$ over $F$ because $f$ splits in $K$ because this field contains all zeros of $f$, and $K$ as an extension of $F$ is generated by these zeros; also note that everything takes place in the larger field $L$, so it does make sense to adjoin the $a_j \in L$ to $F \subseteq L$. With these notations, we then have that $G = \mathrm{Gal}(K/F)$.

Now $K \subseteq L$ is mapped back to itself by any $\varphi \in H$ because such an automorphism permutes the $a_j$ and fixes $F \subseteq E$ pointwise. Thus restriction of $\varphi \in H$ to $K$ produces an element of $G = \mathrm{Gal}(K/F)$. Moreover, this restriction map respects composition of automorphism, so is a homomorphism $H \to G$ between the Galois groups. This homomorphism is injective because if $\varphi \in H$ is the identity map after restricting to $K$, then, since $a_1, \ldots, a_n \in K$, it must act as the identity permutation on the $a_j$, but then it also was the identity on $L = E(a_1, \ldots, a_n)$. So it follows that $H$ is isomorphic to a subgroup of $G$, as claimed. □

*Proof of Theorem 6.35, second part.* So now we assume that $f \in F[x]$ has a solvable Galois group, and I want to show that then $f$ is solvable by radicals. I will again adjoin a primitive $n$th root $\zeta$ to $F$, where $n = [E : F]$, and $E$ is a splitting field of $f$. Then $E(\zeta)$ is a splitting field of $f$ over $F(\zeta)$, and the Galois group $G = \mathrm{Gal}(E(\zeta)/F(\zeta))$ of $f$ over $F(\zeta)$ is still solvable, by Lemma 6.43 and the fact that subgroups of solvable groups are solvable.

By Theorem 3.41, this group has a composition series $G \rhd G_2 \rhd \ldots \rhd G_N = 1$ with cyclic quotients $G_j/G_{j+1}$ of prime orders. By the fundamental theorem, the subgroups $G_j$ correspond to intermediate fields $K_j$, such that $G_j = \mathrm{Gal}(E(\zeta)/K_j)$. In particular, $K_1 = F(\zeta)$ and $K_N = E(\zeta)$. By the fundamental theorem (or, more explicitly, Corollary 6.6(b)), $E(\zeta)$ is Galois over each $K_j$, and since $G_{j+1} = \text{Gal}(E(\zeta)/K_{j+1}) \trianglelefteq G_j$, we also conclude that $K_{j+1}/K_j$ is Galois, with Galois group $G_j/G_{j+1} \cong \mathbb{Z}_{p_j}$ for some prime $p_j$. Now Lemma 6.42 clarifies the nature of the extension $K_{j+1}/K_j$: it is a simple radical extension. Recall that we adjoined $\zeta \in F(\zeta) \subseteq K_j$, and $\zeta$ was a primitive $n$th root of unity. Moreover, $|G|$ divides $n$ ($G$ is isomorphic to a subgroup of $\text{Gal}(E/F)$, which has order $n$), and $|G| = p_1 p_2 \cdots p_{N-1}$. Thus a suitable power of $\zeta$ is a primitive $p_j$th root of unity, and Lemma 6.42 does apply.

We have shown that we get from $F(\zeta)$ to $E(\zeta)$, which contains a splitting field of $f$ over $F$, by a sequence of simple radical extensions. Since $F(\zeta)/F$ also is a simple radical extension ($F(\zeta)$ is a splitting field of $x^n - 1$ over $F$), it follows that $f \in F[x]$ is solvable by radicals, as claimed. □

While this was interesting, it addresses the most obvious question about polynomial equations only in a somewhat roundabout way: Is there a general formula, in the style of (6.13), that produces the roots of a *general* polynomial of degree $n$ in terms of its coefficients, by using field operations and radicals? In other words, I want a "formula" (and I don't want to worry right now about what exactly that means) that works for *all* polynomials of a given degree, not just for particular examples.

We can formalize this as follows. Let $F$ be the field (of characteristic zero, as always in this section) that I want to work in. Then consider $F(t_1, t_2, \ldots, t_n)$, the field of rational functions in $n$ indeterminates $t_1, \ldots, t_n$. Strictly speaking, we haven't formally defined this field yet, but it is of course clear how we want to proceed. First of all, the polynomial ring $F[t_1, \ldots, t_n]$ in several indeterminates $t_1, \ldots, t_n$ could be defined inductively as $F[t_1, t_2] = (F[t_1])[t_2]$, $F[t_1, t_2, t_3] = (F[t_1, t_2])[t_3]$, and so on, but it's better to think of $F[t_1, \ldots, t_n]$ as formal polynomials $\sum a_{k_1 \ldots k_n} t_1^{k_1} \cdots t_n^{k_n}$, and these are added and multiplied in the obvious way.

*Exercise* 6.52. Show that the following (natural) generalization of Theorem 4.15 holds: If $\psi : F \to S$ is a (ring) homomorphism, and $u_1, \ldots, u_n \in S$, then there is a unique homomorphism $\varphi : F[t_1, \ldots, t_n] \to S$ that extends $\psi$ and sends $\varphi(t_j) = u_j$.

The field of rational functions $F(t_1, \ldots, t_n)$ is then defined as the field of fractions of $F[t_1, \ldots, t_n]$; in more concrete terms, the elements of this field are represented by formal rational functions in $t_1, \ldots, t_n$, and again it's clear how to add and multiply these.

With these preliminaries out of the way, consider now the polynomial $f \in F(t_1, \ldots, t_n)[x]$

$$f(x) = x^n + t_1 x^{n-1} + t_2 x^{n-2} + \ldots + t_n.$$

Since the coefficients are indeterminates, this deserves to be called the *general* (monic) *polynomial* of degree $n$. I would then like to know: is $f$ solvable by radicals? This seems to be the proper formalization of the question I asked earlier: a positive answer to this question would mean that the zeros of $f$ can be produced from elements of $F(t_1, \ldots, t_n)$, or, equivalently, from the elements of $F$ and the coefficients $t_j$, using field operations and extraction of roots. This would be the "formula" I was hoping for.

By Theorem 6.35, we can attack this question by computing the Galois group of $f$. This becomes much easier if we start over and approach things slightly differently. More specifically, let again $x_1, \ldots, x_n$ be indeterminates, and consider $g \in F(x_1, \ldots, x_n)[x]$,

$$g(x) = \prod_{j=1}^{n} (x - x_j). \tag{6.15}$$

Instead of general *coefficients,* this polynomial has general *zeros.* If we multiply out, then we find that

$$g(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + \ldots + (-1)^n s_n,$$

where the $s_j$ are the *elementary symmetric polynomials* in $x_1, \ldots, x_n$. More precisely, these are given by

$$s_1 = \sum_{j=1}^{n} x_j, \quad s_2 = \sum_{1 \le j_1 < j_2 \le n} x_{j_1} x_{j_2}, \quad \ldots \quad , s_n = x_1 x_2 \cdots x_n. \tag{6.16}$$

The $s_k$ are indeed symmetric in the sense that

$$s_k(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = s_k(x_1, x_2, \ldots, x_n)$$

for any permutation $\pi \in S_n$. This can be checked from the definition (6.16), but it's even easier to observe that $g$ from (6.15) is obviously invariant under a permutation of the $x_j$, and thus so are its coefficients $s_k$.

We have seen that in fact $g$ has coefficients from $F(s_1, \ldots, s_n)$, and this is a proper subfield of $F(x_1, \ldots, x_n)$ (if $n > 1$) because its members are symmetric rational functions (more precisely: rational functions that have a symmetric representation), and clearly $F(x_1, \ldots, x_n)$ contains rational functions that are not symmetric, such as $f = x_1$. Moreover, $F(x_1, \ldots, x_n)$ is a splitting field of $g \in F(s_1, \ldots, s_n)[x]$.

It seems plausible that the Galois group of $g \in F(s_1, \ldots, s_n)[x]$ is isomorphic to the Galois group of $f \in F(t_1, \ldots, t_n)[x]$ because we would probably expect a polynomial with general coefficients to have general zeros also, so there should be no essential difference between $f$ and $g$. I'll give a formal proof of this claim about the Galois groups below, which will then not look very quick, but this is so mainly because setting up notations will be mildly tedious.

*Exercise* 6.53. Show that $g$ is irreducible over $F(s_1, \ldots, s_n)$.

**Theorem 6.44.** *The general polynomial of degree $n$ has Galois group $G \cong S_n$.*

If we combine this with Theorem 6.35, then we obtain as an immediate consequence:

**Corollary 6.45** (Abel-Ruffini)**.** *The general polynomial of degree $n$ is solvable by radicals if and only if $n \leq 4$.*

In more intuitive terms: there is a general formula that delivers the roots of a polynomial in terms of its coefficients, using field operations and extraction of roots, if and only if the degree is at most 4.

*Proof of Theorem 6.44.* As already announced, I'll discuss the Galois group of $g$ over $F(s_1, \ldots, s_n)$, and I assume (for now) the fact that this is the same as the Galois group of $f$ over $F(t_1, \ldots, t_n)$.

We already observed that $F(x_1, \ldots, x_n)$ is a splitting field, and we also know that we may identify elements of the Galois group with the permutations of the roots $x_1, \ldots, x_n$ that they induce.

For any $\pi \in S_n$, we have an isomorphism $\varphi_0$ of the polynomial ring $F[x_1, \ldots, x_n]$ that sends $a \mapsto a$, $a \in F$, and $x_j \mapsto x_{\pi(j)}$; see Exercise 6.52. This extends to an isomorphism $\varphi$ of the field of fractions $F(x_1, \ldots, x_n)$, by mapping $\varphi(f/g) = \varphi_0(f)/\varphi_0(g)$ (in more formal style, you can also deduce this from Theorem 4.14 with $F = F(R) = F(x_1, \ldots, x_n)$). (Really all I'm saying in this paragraph is that given $\pi \in S_n$, if you now send a rational function to the same rational function, but with the variables reshuffled according to $\pi$, then this map is an automorphism of $F(x_1, \ldots, x_n)$, and this you can check directly, if you prefer.)

Since each $s_k$ is clearly invariant under $\varphi$, the whole field $F(s_1, \ldots, s_n)$ is fixed by $\varphi$, and thus $\varphi \in G = \mathrm{Gal}(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n))$. So, to summarize, an arbitrary permutation $\pi \in S_n$ corresponds to an element of the Galois group that permutes the roots $x_j$ according to $\pi$. Thus $G \cong S_n$, as claimed. □

*Exercise* 6.54. Show that a *symmetric* (that is, invariant under arbitrary permutations of the indeterminates) rational function $f/g \in F(x_1, \ldots, x_n)$ lies in $F(s_1, \ldots, s_n)$. (This is almost, but not quite, the *fundamental theorem of symmetric polynomials,* which says that a symmetric *polynomial* is a *polynomial* of the elementary symmetric polynomials.)

Finally, and as promised, let me show how to identify the field extensions $E/F(t_1, \ldots, t_n)$ and $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$; here, $E$ denotes a splitting field of $f$ over $F(t_1, \ldots, t_n)$. Let's make this more concrete and denote the zeros of $f$ in $E$ by $b_1, b_2, \ldots, b_n$; here, I repeat multiple zeros according to their multiplicity (if we already assume what we are about to show, then it follows that there are no such multiple zeros, by Exercise 6.53). Then $E = F(t_1, \ldots, t_n, b_1, \ldots, b_n)$. In fact, by multiplying out the factorization $f = \prod(x - b_j)$ of $f$ in $E[x]$, we again see that the $t_j = (-1)^j s_j(b_1, \ldots, b_n)$ are (elementary symmetric) polynomials in the $b_j$, so we also have that $E = F(b_1, \ldots, b_n)$.

I would now like define a homomorphism

$$\begin{aligned} &\varphi : F(t_1, \ldots, t_n) \to F(s_1, \ldots, s_n), \\ &\varphi(a) = a,\ a \in F, \quad \varphi(t_j) = (-1)^j s_j. \end{aligned} \tag{6.17}$$

To confirm that this can be done, we start out by mapping the polynomial ring, which is possible by Exercise 6.52 (the $t_j$ are indeterminates). I then want to extend this map $\varphi_0 : F[t_1, \ldots, t_n] \to F[s_1, \ldots, s_n]$ to the field of fractions $F(t_1, \ldots, t_n)$ of $F[t_1, \ldots, t_n]$; this extension will take values in the field $F(s_1, \ldots, s_n)$. I will be able to do this if (and only if) $\varphi_0$ is injective. To verify this property of $\varphi_0$, consider the similarly defined map $\psi : F[x_1, \ldots, x_n] \to E$ that sends $a \mapsto a$, $a \in F$, and $\psi(x_j) = b_j$. Since the range of $\varphi_0$ is contained in the domain of $\psi$, we can compose these maps. Moreover, $\psi\varphi_0(t_j) = \psi((-1)^j s_j) = (-1)^j s_j(b_1, \ldots, b_n) = t_j$ and of course $\psi\varphi_0(a) = a$ for $a \in F$, so $\psi\varphi_0$ is the identity on $F[t_1, \ldots, t_n]$. In particular, it follows that $\varphi_0$ is injective, as desired. So we do have a well defined map $\varphi$ as in (6.17)

Since $\varphi$ is clearly surjective also ($F$ and the $s_j$ are in the image), we have an isomorphism of the ground fields $F(t_1, \ldots, t_n) \cong F(s_1, \ldots, s_n)$. By Theorem 5.17, this may be extended to an isomorphism of the splitting fields $E \cong F(x_1, \ldots, x_n)$. Here, we make use of the fact that $f$ gets mapped to $g$ by our map, if we also send the extra indeterminate to itself: $x \mapsto x$. This follows because $t_j \mapsto (-1)^j s_j$, and these are the coefficients of $f$ and $g$, respectively. So we have isomorphic field extensions, and thus the Galois groups will be isomorphic, too.

*Exercise* 6.55. Give a more formal argument please for this (intuitively obvious) fact. More precisely, suppose that $E_j/F_j$, $j = 1, 2$, are field extensions, with Galois groups $G_j = \mathrm{Gal}(E_j/F_j)$, and suppose that $\varphi : E_1 \to E_2$ is an isomorphism that also maps $F_1$ onto $F_2$. Show that then $G_1 \cong G_2$.