

Chapter 7

Fields

7.1 Field extensions

If F is a field, $E \subseteq F$ is called a *subfield* if it is a subring containing 1_F which is itself a field. It will be convenient to change the point of view: instead, call F an *extension field* of E . If $E \subseteq F$ is a field extension, then F is a vector space over E , so we can consider $\dim_E F$. Denote this by $[F : E]$, the *degree* of the field extension. The field extension is a *finite* or *infinite* extension according to whether $[F : E]$ is finite or infinite.

7.1.1. Lemma. *Given field extensions $E \subseteq F \subseteq K$, $[K : E] = [K : F][F : E]$ (if some of these are ∞ interpret in the usual way!).*

Proof. Pick a basis f_i ($i \in I$) for F as an E -vector space, and k_j ($j \in J$) for K as an F -vector space. We claim that $\{f_i k_j \mid i \in I, j \in J\}$ is a basis for K as an E -vector space, which will prove the lemma.

Take any $k \in K$. We can write $k = \sum_j a_j k_j$ for $a_j \in F$, then $a_j = \sum_i b_{i,j} f_i$ for $b_{i,j} \in E$. Then, $k = \sum_{i,j} b_{i,j} f_i k_j$, so the $f_i k_j$ span K over E . Now suppose we have a linear relation $\sum_{i,j} b_{i,j} f_i k_j = 0$. Since the k_j are linearly independent over F , we deduce that $\sum_i b_{i,j} f_i = 0$, hence since the f_i are linearly independent over E , each $b_{i,j} = 0$. \square

Let $E \subseteq F$ be a field extension and S be a subset of F . Write $E[S]$ for the smallest subring of F containing both E and S , and $E(S)$ for the smallest subfield of F containing both E and S . If $S = \{x_1, \dots, x_n\}$, we write simply $E[x_1, \dots, x_n]$ or $E(x_1, \dots, x_n)$ instead. If in fact $F = E(x_1, \dots, x_n)$ for finitely many elements $x_i \in F$, then F is called a *finitely generated* field extension of E . It is obvious that finite field extensions are finitely generated; the converse is false.

Don't confuse $E[x_1, \dots, x_n]$ with the polynomial ring $E[X_1, \dots, X_n]$ in the case the X_i are indeterminates – for instance all the x_i may in fact be equal!! But there is, by the universal property of the polynomial algebra, a unique E -linear epimorphism $E[X_1, \dots, X_n] \rightarrow E[x_1, \dots, x_n]$, $X_i \mapsto x_i$ (“evaluation”). It follows that $E[x_1, \dots, x_n]$ consists of all elements of F which equal $f(x_1, \dots, x_n)$ for some polynomial $f(X_1, \dots, X_n) \in E[X_1, \dots, X_n]$. Similarly, using now the universal property of fractions, $E(x_1, \dots, x_n)$ consists of all elements of F which equal $f(x_1, \dots, x_n)/g(x_1, \dots, x_n)$ for polynomials $f, g \in E[X_1, \dots, X_n]$ with $g(x_1, \dots, x_n) \neq 0$.

Now let $E \subseteq F$ be a field extension and $u \in F$. Consider the evaluation map

$$E[X] \rightarrow E[u] \subseteq E(u) \subseteq F, \quad f(X) \mapsto f(u)$$

in this case. Let I be its kernel, a prime ideal of $E[X]$ since $E[u] \cong E[X]/I$ is an integral domain. There are two cases:

Case one. $I = (0)$. Then, I is not a maximal ideal, so $E[u]$ is *not* a field, so $E[u] \neq E(u)$. In this case, we call u *transcendental* over E : u is not a zero of any non-zero polynomial over E .

Case two. $I = (m_u(X))$ for some monic polynomial $m_u(X) \in E[X]$, called the *minimal polynomial* of u . This is a non-zero prime ideal of the PID $E[X]$, hence a maximal ideal, and $E[X]/I \cong E[u]$ is a field, and $E[u] = E(u)$. We say that u is *algebraic* over E in this case, of *degree* the degree of the minimal polynomial $m_u(X)$. Obviously, as an E -vector space, $E[X]/(m_u(X))$ has basis $1, X, \dots, X^{n-1}$ where $n = \deg m_u(X)$. So $E[u] = E(u)$ has basis $1, u, \dots, u^{n-1}$ as an E -vector space. Hence,

$$[E(u) : E] = n = \deg m_u(X)$$

in case u is algebraic over E .

We call a field extension $E \subseteq F$ *algebraic* if every $u \in F$ is algebraic over E , and *transcendental* otherwise. Note finite extensions are certainly algebraic, but the converse is false.

7.1.2. Lemma. *If $F = E(S)$ for some $S \subseteq F$, and every $u \in S$ is algebraic over E , then F is algebraic over E . Moreover, if S is finite, then F is finite over E .*

Proof. Take $v \in F$. Then, we can write $v = f/g$ where the f, g are polynomials in the $u \in S$. Now, f, g involve only finitely many $u \in S$, so $v \in E(u_1, \dots, u_n)$ for some $u_i \in S$. It therefore suffices to show that

$$[E(u_1, \dots, u_n) : E] < \infty$$

since finite field extensions are clearly algebraic. Now,

$$[E(u_1, \dots, u_n) : E] = [E(u_1, \dots, u_n) : E(u_1, \dots, u_{n-1})][E(u_1, \dots, u_{n-1}) : E].$$

Hence, by induction on n , it suffices just to show that

$$[E(u) : E] < \infty$$

for u algebraic over E . But in this case we saw above that $[E(u) : E]$ is the degree of the minimal polynomial of u over E . \square

7.1.3. Corollary. *If $E \subseteq F \subseteq K$ are field extensions and both $E \subseteq F$ and $F \subseteq K$ are algebraic, then $E \subseteq K$ is algebraic.*

Proof. Take $u \in K$. Then, u is algebraic over F , so $f(u) = 0$ for some monic polynomial $f \in F[X]$. So in fact, u is algebraic over $E(u_1, \dots, u_n)$ where the u_i are the coefficients of the polynomial f . All of these are algebraic over E by assumption. So,

$$[E(u) : E] \leq [E(u_1, \dots, u_n, u) : E] = [E(u_1, \dots, u_n, u) : E(u_1, \dots, u_n)][E(u_1, \dots, u_n) : E]$$

which is finite, applying the lemma. \square

7.1.4. Corollary. *Let $E \subseteq F$ and let $K = \{u \in F \mid u \text{ is algebraic over } E\}$. Then, K is a subfield of F (and is algebraic over E).*

Proof. Take $u, v \in K$. Then, $E(u, v)$ is an algebraic extension of E by the lemma. So all elements of $E(u, v)$ lie in K . In particular, $u - v$ and uv^{-1} ($v \neq 0$) lie in K . Hence, K is a field. \square

We should mention an important example. Apply the corollary to the field extension $\mathbb{Q} \subseteq \mathbb{C}$. Then,

$$\bar{\mathbb{Q}} = \{\omega \in \mathbb{C} \mid \omega \text{ is algebraic over } \mathbb{Q}\}$$

is a field. It is obviously an algebraic extension of \mathbb{Q} .

It is moreover an *algebraically closed field*. (Recall this means that every polynomial in $\bar{\mathbb{Q}}[X]$ of degree ≥ 1 has a zero in $\bar{\mathbb{Q}}$.) To see this, take $f(X) \in \bar{\mathbb{Q}}[X]$ of degree ≥ 1 . Pick a zero $\lambda \in \mathbb{C}$ of $f(X)$ (using that \mathbb{C} is algebraically closed). then, λ is algebraic over $\bar{\mathbb{Q}}$, and $\bar{\mathbb{Q}}$ is algebraic over \mathbb{Q} , hence λ is algebraic over \mathbb{Q} , hence $\lambda \in \bar{\mathbb{Q}}$.

It is worth pointing out that this algebraically closed field $\bar{\mathbb{Q}}$ of all algebraic numbers is a *countable* algebraically closed field, unlike \mathbb{C} .

7.2 Transcendental extensions

Let us fix throughout the section a field extension $E \subseteq F$. Recall it is a *transcendental extension* if some $u \in F$ is transcendental over E . Then certainly, $[F : E] = \infty$. We'd like some other way of measuring its size!

We will call a subset S of F *algebraically dependent* over E if there exists a polynomial $f(X_1, \dots, X_n)$ in finitely many indeterminates such that $f(s_1, \dots, s_n) = 0$ for some $s_1, \dots, s_n \in S$. Otherwise, we call S *algebraically independent* over E . So if S is algebraically independent over E , then

$$f(s_1, \dots, s_n) = 0 \Rightarrow f(X_1, \dots, X_n) = 0$$

for any polynomial $f(X_1, \dots, X_n)$ and $s_1, \dots, s_n \in S$.

For example, if $S = \{s\}$, then S is algebraically dependent over E if and only if s is algebraic over E . In the field $E(X_1, \dots, X_n)$ of rational functions over E , $\{X_1, \dots, X_n\}$ is algebraically independent over E by construction.

7.2.1. Lemma. *Let $S = \{s_1, \dots, s_n\}$ be an algebraically independent subset of F of E . Then*

$$E(s_1, \dots, s_n) \cong E(X_1, \dots, X_n)$$

for indeterminates X_i .

Proof. The map $X_i \mapsto s_i$ induces a homomorphism $\theta : E[X_1, \dots, X_n] \rightarrow E[s_1, \dots, s_n] \subseteq F$ which is injective as the s_i are algebraically independent. Hence, by the universal property of fractions, θ induces a unique monomorphism $\bar{\theta} : E(X_1, \dots, X_n) \rightarrow F$ with image $E(s_1, \dots, s_n)$. \square

A *transcendence base* of $E \subseteq F$ is defined to be a maximal algebraically independent subset of F over E . (Compare: a basis of an E -vector space V is a maximal *linearly* independent subset of V over E .)

7.2.2. Lemma. *Let $S \subseteq F$ be algebraically independent over E and $t \in F$. Then, the following are equivalent:*

- (1) t is algebraic over $E(S)$;
- (2) $f(t) = 0$ for some non-zero polynomial $f \in E[S][X]$.
- (3) $S \cup \{t\}$ is algebraically dependent over E ;

Proof. (1) \Rightarrow (2). Since t is algebraic over $E(S)$, we can find a non-zero polynomial $f(X)$ with coefficients in $E(S)$ such that $f(t) = 0$. Multiplying $f(X)$ up by a common denominator, we may assume that the coefficients of $f(X)$ lie in $E[S]$.

(2) \Rightarrow (1). This is trivial.

(2) \Leftrightarrow (3). A polynomial $f \in E[S][X]$ involves only finitely many elements s_1, \dots, s_n , so that f can be viewed as a polynomial $g(X_1, \dots, X_n, X) \in E[X_1, \dots, X_n, X]$ evaluated at $X_i = s_i$. Now, $f(t) = 0$ for some non-zero $f \in E[S][X]$ if and only if $g(s_1, \dots, s_n, t) = 0$ for some $g \in E[X_1, \dots, X_n, X]$ with $g(s_1, \dots, s_n, X) \neq 0$. The latter condition is equivalent, since s_1, \dots, s_n are algebraically independent over E , to $g(s_1, \dots, s_n, t) = 0$ for some non-zero $g \in E[X_1, \dots, X_n, X]$. \square

7.2.3. Corollary. *$S \subseteq F$ is a transcendence basis for F over E if and only if*

- (1) S is algebraically independent over E ;
- (2) F is an algebraic field extension of $E(S)$.

Proof. By definition, S is a maximal algebraically independent subset of F over E if and only if S is algebraically independent and $S \cup \{t\}$ is algebraically dependent for all $t \in F$. By the lemma, the latter condition is equivalent to all $t \in F$ being algebraic over $E(S)$. \square

Exchange lemma. *Let S be a subset of F that is algebraically independent subset over E . Given $T \subseteq F$ such that F is algebraic over $E(S \cup T)$, there exists a subset T' of T such that $S \cap T' = \emptyset$ and $S \cup T'$ is a transcendence base for F over E .*

Proof. Let A be the poset of all $U \subseteq T$ such that $S \cup U$ is algebraically independent over E and $S \cap U = \emptyset$, partially ordered by inclusion. By Zorn's lemma, A has a maximal element T' . Saying that T' is maximal means that $S \cup T'$ is a transcendence base for $E(S \cup T)$ over E , hence $E(S \cup T)$ is algebraic over $E(S \cup T')$. Since F is algebraic over $E(S \cup T)$, we deduce that F is also algebraic over $E(S \cup T')$. Since $S \cup T'$ is algebraically independent, this implies by Corollary 7.2.3 that it is a transcendence base for F over E . \square

Now we prove the main result:

Transcendence degree is well-defined. *There exists a transcendence base for F over E . Moreover, any two transcendence bases have the same cardinality.*

Proof. Existence follows from the preceding lemma, taking $S = \emptyset, T = F$. For the second statement, I'll only consider the case when F has a *finite* transcendence base $T = \{t_1, \dots, t_n\}$ over E (see Hungerford Theorem VI.1.9 for general case). Let S be another transcendence base. We just need to show that $|S| \leq |T|$. Suppose not, and pick distinct elements s_1, \dots, s_{n+1} out of S . Let $S_i = \{s_1, \dots, s_i\}$ for each $i = 1, \dots, n+1$.

We have that F is algebraic over $E(T)$, hence over $E(S_1 \cup T)$. Hence applying the exchange lemma, there is a $T_1 \subset T$ with $S_1 \cap T_1 = \emptyset$ such that $S_1 \cup T_1$ is a transcendence base. We cannot have $T_1 = T$ since $S_1 \cup T$ is dependent.

Next, F is algebraic over $E(S_1 \cup T_1)$ hence over $E(S_2 \cup T_1)$. The exchange lemma gives a subset $T_2 \subseteq T_1$ such that $S_2 \cap T_2 = \emptyset$ and $S_2 \cup T_2$ is a transcendence base for F over E . We cannot have $T_2 = T_1$ since $S_2 \cup T_1$ is dependent.

Continue to obtain a strictly descending chain $T \supset T_1 \supset \dots \supset T_n = \emptyset$ with each $S_i \cup T_i$ a transcendence base. In particular, S_n is a transcendence base, which contradicts $\{s_1, \dots, s_{n+1}\}$ being algebraically independent. \square

In view of the theorem, we can define the *transcendence degree* of F over E , namely, the cardinality of a transcendence basis. We denote this by $\text{trdeg}_E(F)$. Here is an exercise you should work out for yourself (see Hungerford VI.1.11 if you get stuck) at this point:

Exercise. If $E \subseteq F \subseteq K$ then $\text{trdeg}_E(K) = \text{trdeg}_E(F) + \text{trdeg}_F(K)$.

To summarize: we have shown that given an arbitrary field extension $E \subseteq F$, we can pick $\text{trdeg}_E(F)$ elements S from F so that $E(S)$ is isomorphic to the field of rational functions over E in $|S|$ indeterminates, and F is algebraic over $E(S)$. If in fact $F = E(S)$, then F is called a *purely transcendental* field extension of E . Thus, an arbitrary field extension $E \subseteq F$ can be thought of as a purely transcendental extension $E \subseteq E(S)$ followed by an algebraic extension $E(S) \subseteq F$. From now on, we concentrate on algebraic extensions.

7.3 Splitting fields

Assume from now onwards that E is a field. If we have a field extension $E \subseteq F$ such that $F = E(u)$ for some $u \in E$, we will call F a *simple* extension of E (cyclic might be a better word, but it's not the one used).

Let $f \in E[X]$ be a polynomial. A *splitting field* F of f over E is a field extension $E \subseteq F$ such that

- (S1) $f(X)$ splits as a product of distinct linear factors in $F[X]$;
- (S2) if we have field extensions $E \subseteq K \subseteq F$ such that $f(X)$ splits as a product of linear factors in $K[X]$ then $K = F$.

We remark right away that if a splitting field F of f over E exists, then it is a finite extension of E . Indeed, if $\alpha_1, \dots, \alpha_n \in F$ are the roots of f , then f splits over $E(\alpha_1, \dots, \alpha_n)$ so $F = E(\alpha_1, \dots, \alpha_n)$ by (S2). Hence, $[F : E] < \infty$ by Lemma 7.1.2.

We want to prove that splitting fields exist and are unique. To do this, we need to be able to “adjoin” roots of polynomials to fields:

Adjoining roots lemma. *Let $f \in E[X]$ be a monic irreducible polynomial. Then, there exists a simple field extension $F = E[u]$ of E of degree $\deg f$ over E such that $f(u) = 0$ in F . Moreover, given a field isomorphism $i : E \rightarrow E'$ and a simple field extension $F' = E'[u']$ of E' such that $(i(f))(u') = 0$ in F' , there exists a unique field isomorphism $\bar{i} : F \rightarrow F'$ extending i such that $\bar{i}(u) = u'$.*

Proof. Existence is easy: just take $F = E[X]/(f(X))$. It is a field as $(f(X))$ is a maximal ideal. Then, $F = E[u] = E(u)$ where $u = X + (f(X))$, and certainly $f(u) = 0$ in F .

Now for the second statement, take a simple field extension $F' = E'[u']$ with $(i(f))(u') = 0$ in F' . There is a unique epimorphism $i_1 : E[X] \rightarrow E'[u']$ extending i such that $X \mapsto u'$. The kernel of i_1 is $(m(X))$ for some monic polynomial m . Since $(i(f))(u') = 0$, $f(X)$ lies in the kernel, so $m(X)$ divides $f(X)$. Since $f(X)$ is irreducible, we get that $m(X) = f(X)$. Hence, by the universal property of quotients, i_1 factors through the quotient $F = E[X]/(f(X))$ to induce the required isomorphism $\bar{i} : F \rightarrow F'$. \square

Existence and uniqueness of splitting fields. *Given $f(X) \in E[X]$, there exists a splitting field F for f over E with $[F : E] \leq (\deg f)!$. Moreover, given a field isomorphism $i : E \rightarrow E'$ and a splitting field F' for $i(f)$ over E' , there exists an isomorphism $\bar{i} : F \rightarrow F'$ extending i .*

Proof. For existence, argue by induction on $\deg f$, using the adjoining roots lemma for the induction step.

Now for the uniqueness statement, let $E \subseteq F$, $E' \subseteq F'$ and $i : E \rightarrow E'$ be as described. We proceed by induction on $[E : F]$. If $[E : F] = 1$, then $E = F$, so $i(E)$ is a splitting field for $i(f)$ over E' , hence $i(E) = E' = F'$ and there is nothing to prove.

Otherwise, $[E : F] > 1$ and f has an irreducible factor in $E[X]$, say g , with $\deg g > 1$. Let α be any root of g in F and α' be any root of $i(g)$ in F' . By the adjoining roots lemma, there exists an isomorphism $i_1 : E(\alpha) \rightarrow E'(\alpha')$ extending i .

Now F is the splitting field of $f_1 = f(x)/(x - \alpha)$ over $E(\alpha)$, and F' is the splitting field of $i_1(f_1)$ over $E'(\alpha')$. Now by induction there exists an isomorphism \bar{i} between F and F' extending i_1 . \square

Although the theorem asserts splitting fields of $f(X)$ over E exist and any two are isomorphic, we should avoid talking about *the* splitting field of $f(X)$ over E : the isomorphism in the uniqueness statement in the theorem is not a unique isomorphism (it depends on choice of roots).

Now we apply the existence of splitting fields to discuss the *algebraic closure* of a field. So far we have seen two examples of algebraically closed fields: \mathbb{C} and the field $\bar{\mathbb{Q}}$ of all algebraic numbers over \mathbb{Q} . Actually, we've never *proved* that either of these are algebraically closed (the fact that \mathbb{C} is algebraically closed should always be left to complex analysis; when we showed that $\bar{\mathbb{Q}}$ is algebraically closed we deduced it from the fact that \mathbb{C} is). But there is a direct, algebraic proof that fields like $\bar{\mathbb{Q}}$ exist independent of any results from complex analysis, and this is good enough for our theoretical purposes.

So, define an *algebraic closure* of a field E to be any *algebraic field extension* $E \subseteq F$ such that F is *algebraically closed*. For example, we have seen that $\bar{\mathbb{Q}}$ is algebraic over \mathbb{Q} and is algebraically closed, hence $\bar{\mathbb{Q}}$ is an algebraic closure of \mathbb{Q} .

Existence and uniqueness of algebraic closures. *Every field E possesses an algebraic closure $E \subseteq F$. Moreover given an isomorphism $i : E \rightarrow E'$ and an algebraic closure F' of E' , there exists an isomorphism $\bar{i} : E \rightarrow F'$ extending i .*

Sketch. I am not going to give you a complete proof of this result. But let me give you the idea in the special case that E is *countable*. As you might expect, the general case is the same idea but depends on an unusually technical Zorn's lemma argument which is not very instructive. You can look it up in Hungerford V.3.6.

So suppose E is countable. Then, so is the polynomial ring $E[X]$. Let f_1, f_2, f_3, \dots be a list of all monic polynomials in $E[X]$. Let F_1 be a splitting field for f_1 over E , F_2 be a splitting field for f_2 over F_1 , ..., F_j be a splitting field for f_j over F_{j-1} , Ignoring axiom of choice difficulties, we obtain a chain $E \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots$ of field extensions. Set $F = \bigcup_{j \geq 1} F_j$, easily checked to be another field extension of E .

We claim that F is an algebraic closure of E . Well, F is algebraic over E since any $x \in F$ lies in some F_j and each F_j is algebraic over E (indeed, each F_j is even finite over E). To prove F is algebraically closed, take any irreducible polynomial $f \in F[X]$. Let K be a splitting field for f over F and $\alpha \in K$ be a root of f . We need to show that $\alpha \in F$, so that $F = K$. Well, K is algebraic over F , hence over E , so α is the root of a monic polynomial $g(X) \in E[X]$. Since $f(X)$ is irreducible, it must be the minimal polynomial of α over F , so $f|g$. But F contains a splitting field for g , so must contain a splitting field for f too. This proves the existence statement.

Now for uniqueness, let $i : E \rightarrow E'$ be an isomorphism and F' be an algebraic closure of E' . Recall that F_1 is a splitting field for f_1 over E . Now, $i(f_1)$ splits in F' so F' must contain a splitting field F'_1 for $i(f_1)$ over E' . By uniqueness of splitting fields, there exists an isomorphism $i_1 : F_1 \rightarrow F'_1$ extending i . Repeating the argument, one obtains an isomorphism $i_j : F_j \rightarrow F'_j$ extending i_{j-1} where $F'_j \subseteq F'$ is a splitting field for f_j over F'_{j-1} .

Define $\bar{i} : F \rightarrow F'$ by setting $\bar{i}(x) = i_j(x)$ for any $j \gg 1$ such that $x \in F_j$. You easily check that \bar{i} is injective. Let F'' be the image of \bar{i} , so F'' is an algebraic closure of E' . We just need to see that $F' = F''$. Well, take any $x \in F'$. Then, x is a root of a monic polynomial over F'' , but F'' is algebraically closed, hence $x \in F''$. \square

As with splitting fields, you should avoid talking about *the* algebraic closure of a field E . It is unique up to isomorphism, but not canonical isomorphism (if you like, there is no universal property definition of algebraic closure).

Given the theorem, we can introduce the notion of a splitting field of an arbitrary set $S \subseteq E[X]$ of polynomials over E , which is the obvious generalization of a splitting field of a single polynomial: Let $S \subseteq E[X]$ be a set of polynomials. Then, a field extension $E \subseteq F$ is called a *splitting field* for S over E if:

(S1') every $f \in S$ splits over F ;

(S2') if $E \subseteq K \subseteq F$ and every $f \in S$ splits over K , then $K = F$.

If $E \subseteq F$ is a splitting field for S over E , then $F = E(A)$ where A is the set of all roots of all $f \in S$ over E . In particular, $E \subseteq F$ is algebraic by Lemma 7.1.2.

Existence and uniqueness of splitting fields'. *Given $S \subseteq E[X]$, there exists a splitting field F for S over E . Moreover, given a field isomorphism $i : E \rightarrow E'$ and a splitting field F' for $i(S)$ over E' , there exists an isomorphism $\bar{i} : F \rightarrow F'$ extending i .*

Proof. For the construction, take the intermediate field $E(A)$ in an algebraic closure \bar{E} of E , where $A \subseteq \bar{E}$ is the set of all roots of all $f \in S$. For uniqueness, let $i : E \rightarrow E'$ be an isomorphism and F, F' be splitting fields for S and $i(S)$ over E and E' respectively. Let \bar{F} and \bar{F}' be algebraic closures of F, F' respectively. Note they are also algebraic closures of E, E' , so by uniqueness of algebraic closures, there exists an isomorphism $i_1 : \bar{F} \rightarrow \bar{F}'$ extending i . Now, in \bar{F} we have that $F = E(A)$ where A is the set of all roots of all $f \in S$, and in \bar{F}' we have that $F' = E'(A')$ where $A' = i_1(A)$ is the set of all roots of all $f' \in i(S)$. It follows easily that $i_1(F) = F'$ so taking \bar{i} to be the restriction of i_1 to F gives the required map. \square

7.4 Normal extensions

An algebraic extension $E \subseteq F$ is called *normal* if every irreducible $f \in E[X]$ that has a root in F splits into linear factors over F .

Characterization of normal extensions. *An algebraic (resp. finite) extension $E \subseteq F$ is normal if and only if F is a splitting field for some subset $S \subseteq E[X]$ (resp. some element $f \in E[X]$).*

Proof. (\Rightarrow). Let $\{f_i\}_{i \in I}$ be a basis for F over E and m_i be the minimal polynomial of f_i over E . Then, F is a splitting field for $\{m_i\}_{i \in I}$; in case $[F : E]$ is finite, F is a splitting field for the polynomial $f = \prod_{i \in I} m_i$.

(\Leftarrow). Suppose that F is a splitting field for $S \subseteq E[X]$. We need to prove it is normal. Let $R = \{\text{roots of elements of } S \text{ in } F\}$. So, $F = E(R)$. Take any $\alpha \in F$ and let m be its minimal polynomial over E ; we need to prove that m splits into linear factors in F .

Well, $\alpha \in E(R)$ so lies in $E(\alpha_1, \dots, \alpha_n)$ for some finite set of elements $\alpha_i \in R$. Suppose α_i is a root of the polynomial $f_i \in S$ and set $f = f_1 \dots f_n$. Let $A = \{\text{roots of } f \text{ in } F\}$, so $\alpha \in E(A) \subseteq F$. Let M be a splitting field for m over $E(A)$ and pick a root $\beta \in M$ of m different from α . We need to prove $\beta \in E(A)$ (hence $M = E(A) \subseteq F$ giving the theorem).

Since α and β are both roots of the same monic irreducible polynomial m , there is by adjoining roots a unique isomorphism $i : E(\alpha) \rightarrow E(\beta)$ which is the identity on E and maps α to β ; in particular, $[E(\alpha) : E] = [E(\beta) : E]$. Now, $E(A)$ is a splitting field for f over $E(\alpha)$ and $E(A, \beta)$ is a splitting field for f over $E(\beta)$. By uniqueness of splitting fields, there is an isomorphism $\bar{i} : E(A) \rightarrow E(A, \beta)$ extending i . Hence, $[E(A) : E(\alpha)] = [E(A, \beta) : E(\beta)]$. Now,

$$[E(A, \beta) : E(\beta)][E(\beta) : E] = [E(A, \beta) : E(A)][E(A) : E(\alpha)][E(\alpha) : E].$$

Terms cancel to give $[E(A, \beta) : E(A)] = 1$, hence $\beta \in E(A)$ as required. \square

7.4.1. Corollary. *Given algebraic extensions $E \subseteq K \subseteq F$ with $E \subseteq F$ normal, then $K \subseteq F$ is normal.*

Proof. Since $E \subseteq F$ is normal, F is the splitting field for some $S \subseteq E[X]$ over E . Clearly, $S \subseteq K[X]$ and F is also the splitting field for S over K . Hence, $K \subseteq F$ is normal. \square

You should be warned: it is not the case that (under the hypotheses in the corollary) $E \subseteq K$ is necessarily normal.

Let $E \subseteq F$ be a field extension. Its *Galois group* $\Gamma(F/E)$ is defined simply to be the group of all field automorphisms $f : F \rightarrow F$ which are the identity on the subfield E , under operation given by composition. We will call elements of $\Gamma(F/E)$ *E -automorphisms of F* .

Criterion for normality of an intermediate field. *Let $E \subseteq F$ be an algebraic, normal field extension and $E \subseteq K \subseteq F$ be an intermediate field. Then $E \subseteq K$ is normal if and only if every $f \in \Gamma(F/E)$ satisfies $f(K) = K$.*

Proof. (\Rightarrow). Let $f \in \Gamma(F/E)$. So, f is an E -automorphism of F . Take $\alpha \in K$ and let m be its minimum polynomial over E . Then, $m(f(\alpha)) = f(m(\alpha)) = 0$ so $f(\alpha)$ is also a root of m . So since $E \subseteq K$ is normal, $f(\alpha) \in K$. Hence, $f(K) \subseteq K$, but $[f(K) : E] = [K : E]$ so in fact $f(K) = K$.

(\Leftarrow). Since $E \subseteq F$ is normal, it is the splitting field for some subset $S \subseteq E[X]$ over E . To prove $E \subseteq K$ is normal, take any $\alpha \in K$ and let m be its minimal polynomial over E . Let β be any root of m in F . We need to show $\beta \in K$. Well, α and β are roots of the same monic irreducible polynomial m , so by the adjoining roots lemma, there exists a unique E -isomorphism $i : E(\alpha) \rightarrow E(\beta)$ mapping α to β . Now F is a splitting field of S over both $E(\alpha)$ and $E(\beta)$, so by uniqueness of splitting fields, there exists an extension of i to an E -automorphism $f : F \rightarrow F$ such that $f(\alpha) = \beta$. But $f(K) = K$ by assumption, so this shows $\beta \in K$. \square

7.5 Separable extensions

To prepare for the other technical aspect underlying the fundamental theorem of Galois theory, we need to discuss *multiple roots* of polynomials. Let E be a field and $f(X) \in E[X]$ be a monic polynomial of positive degree. Let F be a splitting field for f over E . Write

$$f = (x - r_1)^{k_1} \cdots (x - r_s)^{k_s}$$

for distinct $r_i \in F$ and $k_i \geq 1$. We call k_i the *multiplicity* of r_i as a root of f . If $k_i = 1$, then r_i is a *simple root*, else it is a *multiple root*.

Note if F' is another splitting field, there is an isomorphism $f : F \rightarrow F'$ which is the identity on E , so the roots of f in F' are the $f(r_i)$ with multiplicity k_i , for $i = 1, \dots, s$. This shows that the multiplicities of roots are independent of the choice of splitting field.

In particular, the property that f only has simple roots does not depend on the choice of splitting field. So we can define an irreducible $f(X) \in E[X]$ to be *separable* if $f(X)$ does not have multiple roots, and call an arbitrary $f(X) \in E[X]$ *separable over E* if all of its irreducible factors are separable; otherwise, we call f *inseparable*.

Now consider the E -linear operator $d : E[X] \rightarrow E[X]$ given by formal differentiation with respect to X . Let $f(X) \in E[X]$ be a polynomial and α be a root of $f(X)$ in some splitting field. It should be obvious to you from the product rule that α is a multiple root of $f(X)$ if and only if $(df)(\alpha) = 0$. Using this simple idea, we prove:

Criterion for separability. *Let $f(X) \in E[X]$ be an irreducible polynomial. Then, $f(X)$ is inseparable if and only if $\text{char} E = p > 0$ and*

$$f(X) = a_0 + a_1 X^p + \cdots + a_n X^{np}.$$

Proof. We have that f is inseparable if and only if f and df have a common zero α in some splitting field. In that case, the minimal polynomial of α over E divides both f and df . So, f is inseparable if and only if there is $m \in E[X]$ of positive degree dividing both f and df , which since f is irreducible is equivalent to $f|df$. Since $\deg df < \deg f$, this happens precisely when $df = 0$, i.e. f takes the given form. \square

Let me now give you an example to show how an irreducible polynomial can have multiple roots. Let E be a field of characteristic $p > 0$. Then, the *Frobenius map* $E \rightarrow E, a \mapsto a^p$ is a ring homomorphism. Its image $E^p = \{a^p \mid a \in E\}$ is therefore a subfield of E .

7.5.1. Lemma. *If $\text{char} E = p$ and $a \in E$, then $X^p - a$ is irreducible if and only if $a \notin E^p$.*

Proof. Suppose $X^p - a = g(X)h(X)$ for g monic of degree $1 \leq k < p$. Let E be a splitting field for $X^p - a$ over F and $b \in F$ be a root. Then, $b^p = a$ so $X^p - a = (X - b)^p$ so $g(X) = (X - b)^k$ and $b^k \in E$. Choose integers u, v so that $ku + pv = 1$. Then,

$$b = b^{ku+pv} = (b^k)^u (b^p)^v = (b^k)^u a^v \in E$$

and $a \in E^p$. Conversely, if $a = b^p$ for some $b \in E$, then $X^p - a = (X - b)^p$ is a splitting in $E[X]$. \square

Now for the example. Take $E = \mathbb{Z}_p(t)$, the field of rational functions in an indeterminate t over the field \mathbb{Z}_p . I claim that t is not a p th power in this field, i.e. $t \notin E^p$. Indeed, otherwise,

$$t = f(t)^p / g(t)^p$$

for polynomials $f(t) = a_0 + \cdots + a_n t^n, g(t) = b_0 + \cdots + b_m t^m \in \mathbb{Z}_p[t]$. Then,

$$a_0^p + \cdots + a_n^p t^{np} = b_0^p t + \cdots + b_m^p t^{pm+1}$$

so $a_0 = \cdots = a_n = 0$ which is nonsense. Hence, applying the lemma, $X^p - t \in \mathbb{Z}_p(t)[X]$ is irreducible over $\mathbb{Z}_p(t)$. But in a splitting field, $X^p - t$ (by the lemma again) has p equal roots. So we have exhibited an irreducible polynomial which has multiple roots.

A *perfect field* is a field E over which every polynomial is separable. The criterion for separability gives at once that all fields of characteristic 0 are perfect. Moreover, we have:

Criterion for perfect fields. *A field E of characteristic $p > 0$ is perfect if and only if $E^p = E$.*

Proof. If $E^p \neq E$, then we can pick $a \in E - E^p$ and $X^p - a$ is irreducible by Lemma 7.5.1 and inseparable by the criterion for separability. Conversely, given $a_0 + a_1X^p + \cdots + a_nX^{np}$ irreducible and inseparable, we cannot have that all of the a_i are p th powers, for in that case the polynomial would be a p th power so not irreducible. So there exists some $a_i \in E - E^p$. \square

Corollary. *All finite fields are perfect.*

Proof. Let E be a finite field of characteristic p . The map $F : E \rightarrow E^p, x \mapsto x^p$ is injective, so $|E^p| \geq |E|$. Hence, since $E^p \subseteq E$, we have that $E^p = E$ and E is perfect by the criterion for perfect fields. \square

In particular, this explains why we had to look to such a complicated field as $\mathbb{Z}_p(X)$ to find an example of a field that is not perfect.

The main importance of separability is the following result:

Counting monomorphisms theorem. *Suppose that $E \subseteq F$ is a finite extension of degree d and that $i : E \rightarrow K$ is a monomorphism. If for every $\alpha \in F$, its minimal polynomial m_α over E is separable and $i(m_\alpha)$ splits in K , then there exist exactly $[F : E]$ ways of extending i to a monomorphism $\bar{i} : F \rightarrow K$; otherwise, there are strictly fewer such extensions.*

Proof. For $\alpha \in F$, let $h(\alpha)$ be the number of distinct roots of $i(m_\alpha)$ in K . Choose $\alpha \in F - E$ so that $\deg m_\alpha - h_\alpha$ is maximal. If the conditions hold, then $\deg m_\alpha = h(\alpha)$, otherwise $\deg m_\alpha > h(\alpha)$.

Now, for each root β_j of $i(m_\alpha)$ in K , we obtain from the adjoining roots lemma a unique extension of i to a monomorphism $\bar{i} : E(\alpha) \rightarrow K$ such that $\bar{i}(\alpha) = \beta_j$. So there are exactly $h(\alpha)$ extensions of i to a monomorphism $E(\alpha) \rightarrow K$.

Now, take $\beta \in F - E(\alpha)$. Let n_β be its minimal polynomial over $E(\alpha)$. Note that if $i(m_\beta)$ splits in K and m_β is separable over E , then $i(n_\beta)$ also splits in K and n_β is separable over $E(\alpha)$ (since $n_\beta | m_\beta$). So we can simply apply induction, using that $[F : E] = [F : E(\alpha)] \deg m_\alpha$. \square

In view of the result, let us call an algebraic extension $E \subseteq F$ *separable* if the minimal polynomial m_α of every $\alpha \in F$ is separable over E . Finally, define a *Galois extension* to be an algebraic extension which is both *normal* and *separable*. Recall that for any extension $E \subseteq F$, $\Gamma(F/E)$ denotes its Galois group, the group of all E -automorphisms of F .

Counting automorphisms theorem. *Suppose that $E \subseteq F$ is a finite extension. Then $\Gamma(F/E)$ is a finite group of order at most $[F : E]$. Moreover, $\Gamma(F/E)$ has order exactly $[F : E]$ if and only if $E \subseteq F$ is a Galois extension.*

Proof. Apply the counting monomorphisms theorem to the identity map $i : E \rightarrow E$ to get that there are $\leq [F : E]$ E -automorphisms of F , with equality if and only if every m_α is separable and splits into linear factors over F . The last condition is equivalent to $E \subseteq F$ being both separable and normal, i.e. a Galois extension. \square

Finally in this section, we want to explain how Galois extensions arise naturally. Of course, normal extensions are just splitting fields, so Galois extensions should be splitting fields of separable polynomials!

7.5.2. Lemma. *Suppose we have a chain $E = E_0 \subseteq E_1 \subseteq \dots$ of field extensions where $E_i = E_{i-1}(\alpha_i)$ for $\alpha_i \in E_i$ that is algebraic over E_{i-1} and whose minimal polynomial over E_{i-1} is separable. Then $E \subseteq E_i$ is separable for all i .*

Proof. Proceed by induction on i , the case $i = 0$ being trivial. Consider $E \subseteq E_i$ assuming inductively that $E \subseteq E_{i-1}$ is separable. Let $\alpha = \alpha_i$ and m_α be its minimal polynomial over E_{i-1} . Also let n_{α_j} be the minimal polynomial of α_j over E for each j and let F be a splitting field for $\{\alpha_1, \dots, \alpha_i\}$ over E .

By the induction hypothesis and counting monomorphisms, there are exactly $[E_{i-1} : E]$ monomorphisms $E_{i-1} \rightarrow F$ extending the identity on E . Take any one of these, j say. Noting $m_\alpha | n_{\alpha_i}$, which splits in F , we get that $j(m_\alpha)$ splits in F . So by counting monomorphisms and the assumption that m_α is separable over E_{i-1} , there are exactly $[E_i : E_{i-1}] = \deg m_\alpha$ extensions of j to a monomorphism $E_i \rightarrow K$.

Hence, there are in total $[E_i : E] = [E_i : E_{i-1}][E_{i-1} : E]$ extensions of the identity on E to monomorphisms $E_i \rightarrow K$. This implies by counting monomorphisms again that $E \subseteq E_i$ is separable. \square

A very special case of this result gives that the splitting field of a separable polynomial is a Galois extension. See Hungerford V.3.11 for the generalization to infinitely many polynomials.

Transitivity of separable extensions. *Let $E \subseteq F$ be a finite extension and K be an intermediate field. Then, $E \subseteq F$ is separable if and only if both $E \subseteq K$ and $K \subseteq F$ are separable.*

Proof. (\Rightarrow). Obviously, $E \subseteq K$ is separable. Now suppose $\alpha \in F$ and let m_α be its minimal polynomial over E , n_α be its minimal polynomial over K . Then, $n_\alpha | m_\alpha$ and m_α has simple roots in a splitting field. So n_α does too, hence is separable.

(\Leftarrow). Write $K = E(\alpha_1, \dots, \alpha_s)$ and $F = K(\alpha_{s+1}, \dots, \alpha_t)$. Set $E_i = E(\alpha_1, \dots, \alpha_i)$. Then, each $E_{i-1} \subseteq E_i$ is separable by the case \Rightarrow just proved. So we can apply Lemma 7.5.2 to deduce each $E \subseteq E_i$ is separable. \square

Combining this with Corollary 7.4.1, we see that if $E \subseteq K \subseteq F$ is a finite extension and $E \subseteq F$ is Galois, then $K \subseteq F$ is Galois. But recall $E \subseteq K$ may not be Galois (it is only separable for sure).

7.6 The fundamental theorem of Galois theory

Now we are ready to state and prove the fundamental theorem of Galois theory. Let $E \subseteq F$ be an algebraic extension and set $G = \Gamma(F/E)$, its Galois group. So the elements of G are the E -automorphisms of F . Given any intermediate field $E \subseteq K \subseteq F$, the group $\Gamma(F/K)$ consists of K -automorphisms of F , which are certainly E -automorphisms of F . So:

$$\Gamma(F/K) \leq \Gamma(F/E).$$

On the other hand, given any subgroup $H \leq G$, we obtain an intermediate field

$$\text{Inv}H = \{x \in F \mid hx = x \text{ for all } h \in H\},$$

where $E \subseteq \text{Inv}H \subseteq F$. We therefore have two maps, one $\Gamma(F/?)$ from intermediate fields of $E \subseteq F$ to subgroups of G , the other Inv from subgroups of G to intermediate fields of $E \subseteq F$. These maps are *inclusion reversing*, i.e. given intermediate fields K_1, K_2 and subgroups H_1, H_2 ,

- (1) $K_1 \subseteq K_2 \Rightarrow \Gamma(F/K_1) \supseteq \Gamma(F/K_2)$,
- (2) $H_1 \subseteq H_2 \Rightarrow \text{Inv}H_1 \supseteq \text{Inv}H_2$.

Moreover,

$$(3) \quad \Gamma(F/InvH) \supseteq H,$$

$$(4) \quad Inv(\Gamma(F/K)) \supseteq K.$$

These four facts follow from the definitions (exercise!). Of course, we would like to know in fact that the maps $\Gamma(F/?)$ and Inv are *mutually inverse*, i.e. that equality holds in both (3) and (4).

Artin's lemma. *Let F be a field, H be a finite group of automorphisms of F and set $K = InvH = \{x \in F \mid hx = x \text{ for all } h \in H\}$. Then, $|H| \geq [F : K]$.*

Proof. Let $n = |H|$. It suffices to prove that any $m > n$ elements of F are linearly dependent over K . Say $H = \{1 = h_1, h_2, \dots, h_n\}$. Take $u_1, \dots, u_m \in F$. Then, the system of equations

$$\sum_{i=1}^m h_j(u_i)X_i = 0 \quad j = 1, \dots, n$$

has a non-trivial solution (because there are m unknowns and n equations). Let (a_1, \dots, a_m) be a non-zero solution with a minimal number of non-zero a_i 's, and assume without loss of generality that $a_1 = 1$. Then,

$$\sum_{i=1}^m h_j(u_i)a_i = 0.$$

Applying h_k permutes the equations,

$$\sum_{i=1}^m h_k h_j(u_i)h_k(a_i) = 0$$

Hence, $(h_k a_1, h_k a_2, \dots, h_k a_m)$ is also a solution, and $h_k a_1 = 1 = a_1$ by assumption. The difference is $(0, a_2 - h_k a_2, \dots, a_m - h_k a_m)$ is therefore a solution with fewer non-zero entries, so is actually zero. Hence, $a_i = h_k a_i$ for all i and all k , so $a_i \in K$ for each i . Now the first equation gives

$$\sum_{i=1}^m a_i u_i = 0$$

so the u_i are dependent over K . \square

The fundamental theorem of Galois theory for *finite extensions* goes as follows (see Hungerford V.3.12 for the algebraic but not necessarily finite case).

Fundamental theorem of Galois theory. *Let $E \subseteq F$ be a Galois extension and $G = \Gamma(F/E)$. Then, the maps $\Gamma(F/?)$ and Inv are mutually inverse bijections between the set of intermediate fields of $E \subseteq F$ and the set of subgroups of G , i.e.*

$$\Gamma(F/InvH) = H \quad \text{for} \quad H \leq G$$

and

$$Inv\Gamma(F/K) = K \quad \text{for} \quad E \subseteq K \subseteq F.$$

Moreover,

- (i) $[G : H] = [InvH : E]$ and $|H| = [F : InvH]$;
- (ii) $H \trianglelefteq G$ if and only if $E \subseteq InvH$ is normal, in which case $\Gamma(InvH/E) \cong G/H$.

Proof. Applying (4), we have that

$$\Gamma(F/\text{Inv}(\Gamma(F/K))) \subseteq \Gamma(F/K).$$

Applying (3), we have that

$$\Gamma(F/\text{Inv}(\Gamma(F/K))) \supseteq \Gamma(F/K).$$

Hence, we have equality.

Now, since $E \subseteq F$ is Galois, so are $K \subseteq F$ and $\text{Inv}(\Gamma(F/K)) \subseteq F$, so by counting automorphisms,

$$[F : \text{Inv}(\Gamma(F/K))] = |\Gamma(F/\text{Inv}(\Gamma(F/K)))| = |\Gamma(F/K)| = [F : K].$$

As $\text{Inv}(\Gamma(F/K)) \supseteq K$ by (4), we therefore get by comparing degrees that

$$\text{Inv}(\Gamma(F/K)) = K.$$

Next, $|\Gamma(F/\text{Inv}H)| = [F : \text{Inv}H]$ by counting automorphisms. Moreover, $[F : \text{Inv}H] \leq |H|$ by Artin's lemma. Hence, $|\Gamma(F/\text{Inv}H)| \leq |H|$. But $\Gamma(F/\text{Inv}H) \supseteq H$ by (3), so we deduce that

$$\Gamma(F/\text{Inv}H) = H.$$

In particular, $|H| = |\Gamma(F/\text{Inv}H)| = [F : \text{Inv}H]$ and $[G : H] = [F : E]/[F : \text{Inv}H] = [\text{Inv}H : E]$ which proves (i).

That just leaves (ii). Recall that $E \subseteq K$ is normal if and only if $g(K) = K$ for all $g \in G$. So if $E \subseteq \text{Inv}H$ is normal, then $g(\text{Inv}H) \subseteq \text{Inv}H$ for all $g \in G$. Hence, $hgx = gx$ for all $g \in G, x \in \text{Inv}H, h \in H$, so $g^{-1}hg \in \Gamma(G/\text{Inv}H) = H$. This shows that $H \trianglelefteq G$. Conversely, if $H \trianglelefteq G$, then for any $x \in \text{Inv}H$, we have that $hgx = gh'x$ for some $h' \in H$, so $hgx = gx$ so $gx \in \text{Inv}H$, i.e. G leaves $\text{Inv}H$ invariant and $E \subseteq \text{Inv}H$ is normal. \square

7.7 Radical extensions

Let $f(X) \in E[X]$ be a monic polynomial of positive degree. We say the equation $f(X) = 0$ is *solvable by radicals over E* if there exists an extension field $E \subseteq F$ and a chain of field extensions

$$E = E_1 \subseteq E_2 \subseteq \cdots \subseteq E_{r+1} = F$$

such that

- (1) $E_{i+1} = E_i(d_i)$ and $d_i^{n_i} \in E_i$ for some n_i ;
- (2) F contains a splitting field for $f(X)$.

We will refer to such a chain of extensions as a *root tower*. Intuitively, “ $f(X) = 0$ is solvable by radicals” means all of its roots can be built up from the basic field operations together with the operation of extracting n th roots.

Now assume that $f(X)$ has distinct roots $\alpha_1, \dots, \alpha_n$ in some splitting field $E \subseteq F$ (which is the case for instance if $f(X)$ is irreducible and separable). Consider $G = \Gamma(F/E)$. Now, G acts on $\alpha_1, \dots, \alpha_n$, so we obtain a homomorphism

$$\rho : G \rightarrow S_n$$

where S_n is the symmetric group on $\alpha_1, \dots, \alpha_n$. Since $F = E(\alpha_1, \dots, \alpha_n)$, ρ is injective so $G \cong \text{im } \rho$. Let us denote $\text{im } \rho$ by G_f and call it the *Galois group* of the polynomial $f(X)$. So by definition, G_f is a certain group of permutations of the roots of f . For example if $G_f = S_n$, we say that the Galois group of f is S_n .

Example. Suppose that $f(X) \in \mathbb{Q}[X]$ is irreducible of degree p and has $p - 2$ real roots and 2 complex roots. Then, the Galois group G_f of f is S_p .

Proof. Let $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ be a splitting field for f . Since f is irreducible, G_f acts transitively on the roots. For otherwise, we can partition the roots into two disjoint G_f -stable subsets $\{\alpha_i\}$ and $\{\beta_i\}$, and then $f(X) = g(X)h(X)$ where

$$g(X) = \prod (X - \alpha_i), \quad h(X) = \prod (X - \beta_i).$$

But then G_f leaves $g(X)$ and $h(X)$ invariant, so that their coefficients are in the fixed field of G_f , namely, \mathbb{Q} . Therefore, G_f has an orbit of size p , so $p \mid |G_f|$, so since p is prime, G_f contains a p -cycle. Now complex conjugation $z \mapsto \bar{z}$ fixes the real roots and interchanges the complex ones. Hence, G_f contains a transposition. But S_p is generated by a p -cycle and a transposition, so $G_f = S_p$. \square

Now take $f(X) = X^5 - 4X + 2$. It is irreducible by Eisenstein's criterion. Moreover, $f'(X) = 5X^4 - 4$ has exactly 2 real roots. So by Rolle's theorem, $f(X)$ has at most 3 real roots. Since $f(-2) = -22, f(0) = 2, f(1) = -1, f(2) = 26$, $f(X)$ has at least 3 real roots by the Intermediate Value Theorem. So $f(X)$ satisfies the above condition, and its Galois group is S_5 .

Galois' celebrated criterion for solvability of polynomials by radicals is the following:

Galois' theorem. *The equation $f(X) = 0$ is solvable by radicals over a field E of characteristic 0 if and only if the Galois group G_f is solvable.*

Thus for example, the equation $X^5 - 4X + 2$ is not solvable by radicals over the field \mathbb{Q} , since the group S_5 is not solvable. The proof will take the remainder of the section. We assume from now on that we have a given field E of characteristic 0.

We begin by studying roots of unity. Call a splitting field of $x^n - 1$ over E a *cyclotomic field* of order n over E .

7.7.1. Lemma. *The Galois group of a cyclotomic field of order n over E is Abelian.*

Proof. Since $d(X^n - 1) = nX^{n-1}$ is coprime to $X^n - 1$, $X^n - 1$ has n distinct roots $\omega_1, \dots, \omega_n$ in a splitting field F . These constitute a multiplicative group U contained in the cyclotomic field. Moreover, U is cyclic (since for each $d \mid n$ U contains exactly d solutions to the equation $x^d - 1 = 0$). Of course if you work in \mathbb{C} , then $\omega_i = e^{2\pi i/n}$ and it is immediate that U is cyclic!

Now, the map $g \mapsto g|_U$ is a monomorphism (because U generates F) of the Galois group into the group of automorphisms of the group U . But $\text{Aut}(U) \cong \text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$ which is Abelian. (Note we do not claim the Galois group is *isomorphic* to U : for instance E may contain all the ω_i in which case the Galois group is trivial.) \square

7.7.2. Lemma. *If E contains n distinct roots of unity, then the Galois group of $x^n - a$ over E is cyclic of order a divisor of n , for each $a \in E$.*

Proof. Let U be the set of n th roots of 1 contained in E , let F be a splitting field over E of $x^n - a$. If r is one of the roots of $x^n = a$ in F , then this equation has the n roots $\{r\omega \mid \omega \in U\}$. Hence, $F = E(r)$. If $g, h \in G = \Gamma(F/E)$, then $gr = \omega r, hr = \omega' r$ some $\omega, \omega' \in U$. Hence, $(hg)r = \omega\omega' r$. Thus, the map $g \mapsto \omega$ is a homomorphism of G into U which is an injection. So, G is isomorphic to its image, which is contained in U which is cyclic. Hence, G is cyclic. \square

The lemma has a partial converse:

7.7.3. Lemma. *Let p be a prime and suppose E contains p distinct p th roots of 1. Suppose $E \subseteq F$ is a Galois extension and that its Galois group has order p . Then, $F = E(d)$ for some $d \in F$ with $d^p \in E$.*

Proof. Choose $c \in F - E$. Then, $F = E(c)$ since $[E(c) : E] > 1$ and $[F : E]$ is prime. Let $U = \{\omega_1, \dots, \omega_p\}$ be the set of p th roots of 1 in E . Let $g \in G = \Gamma(F/E)$ be a generator (G has order p so is cyclic!). Set $c_i = g^{i-1}(c)$ for $1 \leq i \leq p$, so that $c_1 = c$. Then, g induces the p -cycle $(c_1 c_2 \dots c_p)$ on the c_i . Introduce the *Lagrange resolvent*

$$(5) \quad (\omega_i, c) = c_1 + c_2 \omega_i + c_3 \omega_i^2 + \dots + c_p \omega_i^{p-1}.$$

Then,

$$g((\omega_i, c)) = c_2 + c_3 \omega_i + \dots + c_1 c_i^{p-1} = \omega_i^{-1}(\omega_i, c).$$

So, $(\omega_i, c)^p$ is fixed by g , hence by G hence $(\omega_i, c)^p \in E$ for each $\omega_i \in U$.

Now we can express c_1, c_2, \dots, c_p as a linear combination of the (ω_i, c) . To see this, view (5) as a system of linear equations in unknowns c_1, c_2, \dots, c_p . Then, the matrix of coefficients is a Vandermonde determinant, whose value is

$$\prod_{i>j} (\omega_i - \omega_j)$$

which is non-zero.

Hence, since $F = E(c)$, $F = E(d_1, \dots, d_p)$ where $d_i = (\omega_i, c)$. So there must be some i such that $d_i \notin F$, let d denote this d_i . Then, $F = E(d)$ and $d^p \in E$. \square

7.7.4. Lemma. *Let $f(X) \in E[X]$ and let F be an extension field of E . Then, the Galois group of $f(X)$ over F is isomorphic to a subgroup of the Galois group of $f(X)$ over E .*

Proof. Let F' be a splitting field over F of $f(X)$. Since $E \subseteq F$, F' contains a splitting field E' of $f(X)$ over E . In fact, if

$$f(X) = \prod_{i=1}^n (X - r_i)$$

in $F'[X]$, then $F' = F(r_1, \dots, r_n)$ and $E' = E(r_1, \dots, r_n)$. Let $R = \{r_1, \dots, r_n\}$.

Now, take $g \in \Gamma(F'/F)$. It maps R into itself and fixes E , hence it maps E' into itself. So restriction from F' to E' gives a homomorphism $\Gamma(F'/F) \rightarrow \Gamma(E'/E)$. It is clearly injective since r_1, \dots, r_n generate F' and lie in E' . \square

7.7.5. Lemma. *Let $E \subseteq F$ have a root tower, say*

$$E = E_0 \subseteq E_1 \subseteq \dots \subseteq E_{r+1} = F$$

with $E_{i+1} = E_i(d_i)$, $d_i^{n_i} \in E_i$. Assume moreover that F is generated over E by a finite set of elements whose minimal polynomials are separable. Then, there exists a normal extension $E \subseteq K$ also having a root tower for which the set of integers n_i appearing are the same as in the given tower (ignoring multiplicities).

Proof. Say F is generated over E by $\alpha_1, \dots, \alpha_m$ which all have separable minimal polynomials m_{α_i} over E . Let K be a splitting field for $m = m_{\alpha_1} \dots m_{\alpha_m}$ over F . Then, K is also a splitting field for m over E , hence K is normal over E , and m is separable so $E \subseteq K$ is a Galois extension. (Remark: K is called a *normal closure* for $E \subseteq F$.)

We claim that K is generated by all $g(F)$ for all $g \in \Gamma(K/E)$. Indeed, let K' be the subfield of K generated by all $g(F)$ for all $g \in \Gamma(K/E)$. Then, $E \subseteq K'$ is normal by the criterion for normality of an intermediate field. Now each m_{α_i} has a root in F hence in K' , so splits in K' by normality. So m splits over K' , hence $K = K'$ as K was a splitting field for m .

Now applying $g \in \Gamma(K/E)$ to the given root tower for F yields an analogous root tower for $g(F)$. Then,

$$K = E(g_1(d_1), \dots, g_1(d_r); g_2(d_1), \dots, g_2(d_r); \dots; g_n(d_1), \dots, g_n(d_r))$$

where $\Gamma(K/E) = \{g_1, \dots, g_n\}$. Now you can obviously glue all the root towers for all $g_i(F)$ together to build a root tower for $E \subseteq K$ with the integers n_i appearing being the same as before. \square

Now finally we are ready to prove Galois' criterion. Assume from now on that E has characteristic 0.

Suppose first that $f(X) = 0$ is solvable by radicals over E . Then, we have an extension field $E \subseteq F$ containing a splitting field for $f(X)$ and having a root tower. Applying Lemma 7.7.5, we can even assume that $E \subseteq F$ is normal, hence Galois since we are in characteristic 0.

Let n be the least common multiple of the n_i occurring in the root tower. Then, we can extend F to $F(\omega)$ where ω is a primitive n th root of 1. Since F is normal over E , it is a splitting field for some set S of polynomials over E . Then $F(\omega)$ is a splitting field for $S \cup \{X^n - 1\}$ so is also normal over E ; hence $E \subseteq F(\omega)$ is Galois. Finally, let $K \subseteq F$ be the splitting field for $f(X)$ over E . So we have:

$$E \subseteq K \subseteq F \subseteq F(\omega)$$

Let $G = \Gamma(F(\omega)/E)$. Choose a root tower for $E \subseteq F(\omega)$:

$$E = E_0 \subseteq E_1 = E(\omega) \subseteq E_2 \subseteq \dots \subseteq E_m \subseteq E_{m+1} = F(\omega)$$

with $E_{i+1} = E_i(d_i)$, $d_i^{n_i} \in E_i$. Each E_{i+1} is in fact normal over E_i since the n th roots of 1 are there so all n_i th roots of d_i are there so it is a splitting field of $X^{n_i} - d_i$ over E_i . The group $\Gamma(E_{i+1}/E_i)$ is Abelian (by Lemma 7.7.1 in case $i = 0$, Lemma 7.7.2 otherwise).

Now let G_i be the subgroup of G corresponding to the subfield E_i , i.e. $G_i = \Gamma(F(\omega)/E_i)$. Since E_{i+1} is normal over E_i , we have that $H_{i+1} \trianglelefteq H_i$, and $H_i/H_{i+1} \cong \Gamma(E_{i+1}/E_i)$ is Abelian. This constructs a subnormal series of G with Abelian factor groups, so G is solvable. Finally, $\Gamma(K/E)$ is a quotient of $\Gamma(F(\omega)/E)$ so is also solvable.

For the converse, suppose that the Galois group G of $f(X) = 0$ over E is solvable. Let $n = |G|$. Let $E_0 = E$, $E_1 = E(\omega)$ where ω is a primitive n th root of unity. Let F be a splitting field for f over E_0 and K be a splitting field for f over E_1 . By Lemma 7.7.4, $H = \Gamma(K/E_1)$ is isomorphic to a subgroup of $G = \Gamma(F/E_0)$, so solvable. So, there is a subnormal series

$$H = H_1 \geq \dots \geq H_{r+1} = \{1\}$$

with successive quotients being of prime order p_i . Correspondingly, we obtain an increasing chain of subfields

$$E_1 \subseteq E_2 \subseteq \dots \subseteq E_{r+1} = K,$$

each E_{i+1} being normal over E_i and $\Gamma(E_{i+1}/E_i)$ of order $p_i|n$. Since E_i contains a primitive n th root of 1, it contains a primitive p_i th root of 1 so Lemma 7.7.3 implies $E_{i+1} = E_i(d_i)$ where $d_i^{p_i} \in E_i$. Hence, we have constructed K containing the splitting field F and having a root tower over E . So $f(X) = 0$ is solvable by radicals.

Exercises. I include here some longer exercises exploring some further topics on Galois groups of polynomials.

1. Suppose that $f(X)$ is a polynomial in $E[X]$ having distinct roots $\alpha_1, \dots, \alpha_n$ in a splitting field F . Let G_f be its Galois group, acting naturally on $\alpha_1, \dots, \alpha_n$. Set

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i),$$

and let $\Delta = \delta^2$, the *discriminant* of $f(X)$. Of course, δ is defined only up to a sign (since it depends on the ordering of the roots). But Δ is defined uniquely.

(i) Show that for $g \in G_f$,

$$g(\delta) = \text{sgn}(g)\delta,$$

where sgn denotes the sign of the permutation $g \in G_f \leq S_n$.

(ii) Explain why Δ is an element of the ground field E .

(iii) Now prove that $G_f \leq A_n$ (the alternating group) if and only if Δ has a square root in E (i.e. $\delta \in E$).

2. The following question explains how to calculate the discriminant. Using the same notation as exercise 1, the discriminant δ is by definition equal to the Vandermonde determinant:

$$\delta = \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{bmatrix}.$$

(i) Multiply this matrix by its transpose to show:

$$\Delta = \det \begin{bmatrix} n & \lambda_1 & \dots & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & \dots & \lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & \dots & \lambda_{2n-2} \end{bmatrix}$$

where $\lambda_i = \alpha_1^i + \alpha_2^i + \dots + \alpha_n^i$.

(ii) The quantities λ_i in (i) can be expressed in terms of the coefficients of the original polynomial $f(X)$ in a way you should be familiar with! Indeed, if $f(X) = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n$, then

$$\begin{aligned} \lambda_1 &= -a_1 \\ \lambda_2 &= a_1^2 - 2a_2. \end{aligned}$$

Give similar expressions for λ_3 and λ_4 in terms of the a_i . (This problem is the starting point for the study of *symmetric functions*.)

3. Finally consider the polynomial

$$f(X) = X^5 + 20X + 16.$$

(i) Calculate its discriminant over \mathbb{Q} .

(ii) Given that this polynomial is not solvable by radicals over \mathbb{Q} , what is its Galois group?

7.8 Finite fields

Suppose that F is a finite field. Then, $\text{char} F = p$ for some prime $p > 0$. The subring of F generated by 1 is therefore isomorphic to \mathbb{Z}_p , so that we can view F as a field extension of \mathbb{Z}_p . If $[F : \mathbb{Z}_p] = n$, then we get that $|F| = p^n$.

Classification of finite fields. For each prime power p^n , there exists a field F with $|F| = p^n$. If F' is another field of order p^n , then $F' \cong F$.

Proof. Let $\mathbb{Z}_p \subseteq F$ be a splitting field for the polynomial $f(X) = X^{p^n} - X$ over \mathbb{Z}_p . Since $df(X) = -1$, $f(X)$ has p^n distinct roots in F . Let $R \subseteq F$ denote the set of all of these roots, so $|R| = p^n$. Let $\sigma : F \rightarrow F, x \mapsto x^p$ be the Frobenius morphism, and observe that

$$R = \{x \in F \mid \sigma^n(x) = x\}.$$

But $\{x \in F \mid \sigma^n(x) = x\}$ is a subfield of F . Hence, R is already a field and $f(X)$ splits in $R[X]$, so $R = F$ and $|F| = p^n$.

Now let K be another finite field of order p^n , and view K as a field extension of \mathbb{Z}_p as explained at the start of the section. Then, K^* is a multiplicative group of order $p^n - 1$. Hence, $x^{p^n-1} = 1$ for all $x \in K^*$. Hence, $x^{p^n} = x$ for all $x \in K$ (even $x = 0$!). Thus the polynomial $f(X) = X^{p^n} - X$ has p^n distinct roots in K , so K is a splitting field for $f(X)$ over \mathbb{Z}_p . So by uniqueness of splitting fields, $K \cong F$. \square

Exercise. The goal in this exercise is to prove that the multiplicative group of units of a finite field is cyclic.

(i) Let p be a prime and A be a non-trivial cyclic group of p -power order, written additively. Prove that the equation $pX = 0$ has p solutions in A . More generally, prove that if A is the direct sum of s non-trivial cyclic groups of p -power order then the equation $pX = 0$ has p^s solutions.

(ii) Now let F be a finite field of order p^n and $A = F^*$ be its multiplicative group of units, a finitely generated Abelian group. We know that

$$A = \bigoplus_q A_q$$

where the product is over all primes q , and A_q is the “ q -primary component” of A , i.e. the set of all elements of A of q -power order. Prove using (i) and the primary decomposition theorem for finitely generated Abelian groups that each A_q is cyclic.

(iii) Deduce using the Chinese Remainder Theorem that F^* is a cyclic group of order $p^n - 1$.

(iv) Letting $\omega \in F^*$ be a generator, deduce that $F = \mathbb{Z}_p(\omega)$, so that F is a simple field extension of its prime subfield.

We note that if F is a finite field, then $\mathbb{Z}_p \subseteq F$ is a Galois extension. Indeed, the proof of the theorem shows that F is a splitting field of a polynomial over \mathbb{Z}_p so it is normal, and it is separable since all finite fields are perfect. Let us now determine $G = \Gamma(F/\mathbb{Z}_p)$.

As $\mathbb{Z}_p \subseteq F$ is a Galois extension, we have that $|G| = [F : \mathbb{Z}_p] = n$. Consider $\sigma : F \rightarrow F, x \mapsto x^p$, the Frobenius morphism. It is certainly an element of G . Let d denote its order,

$$x^{p^d} = x$$

for all $x \in F$. Hence, the equation $X^{p^d} - X$ has exactly p^n different roots on F , which implies that $p^d \geq p^n$, i.e. $d \geq n$. But $\sigma \in G$ generates a subgroup of order exactly d , so we must have in fact that $d = n$ and σ generates G . We have shown:

The Galois group of a finite field. Let $\mathbb{Z}_p \subseteq F$ with $|F| = p^n$. Then, $\Gamma(F/\mathbb{Z}_p)$ is cyclic of order n and is generated by the Frobenius morphism.

So now we understand $G = \Gamma(F/\mathbb{Z}_p)$, we can describe precisely the lattice of subfields of our finite field F of order p^n . Well, $G \cong C_n$, so for each divisor d of n , G has a unique subgroup of index d . It follows from the fundamental theorem of Galois theory that F has a unique subfield of degree d over \mathbb{Z}_p , i.e. a unique subfield of order p^d . The lattice of subfields of F is therefore isomorphic to the lattice of divisors of n .

Take F of order p^n and $d|n$. We can describe the unique subfield of F of order p^d explicitly using the Frobenius morphism $\sigma : F \rightarrow F$: since $G = \langle \sigma \rangle$, the cyclic subgroup of G generated by $\langle \sigma^d \rangle$ has index d . The corresponding fixed field of F , namely,

$$E = \{x \in F \mid \sigma^d(x) = x\} = \{x \in F \mid x^{p^d} = x\}$$

is therefore, by the fundamental theorem, exactly the unique subfield of F of order p^d .