CHAPTER VII

FIELD THEORY

1. Fields, Algebraic and Transcendental Elements

We now begin a systematic study of field theory, particularly Galois Theory. Our basic aim is to study the behavior of roots of algebraic equations. In particular, given a polynomial $f(X)$ in an indeterminate X with coefficients in a field F, we want to study the roots of the equation $f(X) = 0$. (More generally, we could consider polynomial equations in several variables $f(X_1, \dots, X_n) = 0$, in which case the set of roots would form a geometric object in "n-space." Such objects are the subject matter of algebraic geometry. For now, we shall concentrate on the case $n = 1$.) Although much of the theory will be valid for arbitrary fields, the prime example will be the field of rational numbers $\mathbf{Q}$.

If F is a field, we know that the intersection F_0 of all subfields of F is again a field—called the *prime* subfield of F. It is the smallest subfield of F. The prime subfield must contain 1 and all its multiples $n \cdot 1$. If we define a ring homomorphism $\mathbf{Z} \to F$ by $n \mapsto n \cdot 1$, its image must be contained in F_0. If the kernel of this homomorphism is $\{0\}$, then F_0 contains a subring isomorphic to $\mathbf{Z}$, and hence it contains a subfield isomorphic to the field of fractions $\mathbf{Q}$ of $\mathbf{Z}$. By minimality, $F_0 \cong \mathbf{Q}$. Otherwise, the kernel is of the form $p\mathbf{Z}$ for some positive integer p. Since $\mathbf{Z}/p\mathbf{Z}$ will be isomorphic to a subring of F, it is a domain so p must be prime and $\mathbf{Z}/p\mathbf{Z}$ is a field. Again, by minimality, $F_0 \cong \mathbf{Z}/p\mathbf{Z}$. In the first case we say that F has *characteristic* 0, and in the second case we say it has *characteristic* p. An alternate notation for $\mathbf{Z}/p\mathbf{Z}$ which is common in field theory is $\mathbf{F}_p$. We shall use this notation below.

In our discussion below, we will often make use of the fact that any nontrivial ring homomorphism of a field into a ring is necessarily a monomorphism since its kernel being an ideal must be trivial.

Let F be a field. Generally speaking, polynomials defined over F may not have roots in F (e. g. $X^2 + 1$ over $\mathbf{Q}$) but they will have roots in fields containing F. Suppose then that E is a field containing F (or even more generally a ring containing F.) We say that $u \in E$ is *algebraic* over F if $f(u) = 0$ for some nonzero polynomial $f(X) \in F[X]$. Elements which are not algebraic are called *transcendental.* For example, $\sqrt{2}$, i, etc. are algebraic over $\mathbf{Q}$ while π and e are transcendental. It is not too difficult to see that the subset of $\mathbf{C}$ of elements algebraic over $\mathbf{Q}$ is denumerable so that practically all elements of $\mathbf{C}$ are transcendental over $\mathbf{Q}$.

Note that if $x \in E$ is algebraic over F, then it is algebraic over any intermediate field L ($E \supseteq L \supseteq F$) since any equation it satisfies over F is also an equation over L.

Given a field E containing F (called hereafter an *extension* of F), and given $u \in E$, we may define a unique ring homomorphism

$$\phi : F[X] \to E$$

by setting $\phi(X) = u$. Its image is the subring $F[u]$ of E.

Proposition. *With the notation as immediately above, u is algebraic if and only if $I = \operatorname{Ker}\phi \neq \{0\}$. If u is algebraic, then I is a maximal ideal of $F[X]$ and $F[u]$ is a field. If u is transcendental, then $F[u] \cong F[X]$ is not a field.*

Proof. $\operatorname{Ker}\phi$ consists of all polynomials $f(X)$ such that $f(u) = 0$ so it is clear that u is algebraic if and only if $\operatorname{Ker}\phi \neq \{0\}$. In any case, by the first isomorphism theorem, $F[X]/I \cong F[u]$ which is a subring of a field so it is a domain. Hence, I is a prime ideal. However, $F[X]$ is a PID so every nonzero prime ideal is maximal. It follows that $F[X]/I \cong F[u]$ is a field if $I \neq \{(0\}$. If $I = \{(0\}$, then $F[X] \cong F[u]$ and we know the former is not a field since in particular X is not invertible. □

Typeset by $\mathcal{AMS}$-TeX

In the transcendental case we can say little more. Denote by $F(X)$ the field of fractions of the domain $F[X]$. It is called the *rational function field* over F, and it consists of quotients of polynomials $f(X)/g(X)$ with coefficients in F, with the denominator not the zero polynomial. Since E is a field, it is not hard to see that the ring monomorphism $\phi : F[X] \to E$ may be extended (in only one way) to a monomorphism of fields $\phi : F(X) \to E$. The image of this monomorphism is the smallest subfield of E containing F and u—denoted $F(u)$. Thus, in the transcendental case $F(u) \cong F(X)$, the field of rational functions over F.

In the algebraic case, according to the above proposition, $F(u) = F[u]$, and it does not bear any relation to $F(X)$. Since $F[X]$ is a PID, the ideal $I = \operatorname{Ker}\phi = (g(X))$ is principal. If we choose $g(X)$ monic (i.e. with leading coefficient 1), it is uniquely characterized by the fact that it generates the ideal I. It is also irreducible because I is prime. $g(X)$ is called the *minimal* polynomial of u. Note that it is characterized more directly by the property that if $f(X) \in F[X]$ with $f(u) = 0$ then $g(X) \mid f(X)$.

We may approach the problem from another point of view. Let $g(X) \in F[X]$. If $g(X)$ is not irreducible, we know we can factor it into irreducible factors, and if we know all about the roots of its factors, we know all about the roots of $g(X)$—so assume $g(X)$ is irreducible. In that case $F[X]/(g(X))$ is a field since $I = (g(X))$ is prime and hence maximal. If we put $E = F[X]/I$, then we have constructed a field containing F (after suitable identifications), and if we put $u = X + I$, then clearly $g(u) = 0$. Hence, for any polynomial whatsoever we can always construct an extension of F in which that polynomial has a root.

Proposition. *Suppose $f(X) \in F[X]$ is a nonzero polynomial and E is an extension field of F. Then $f(X)$ has at most $\deg f(X)$ distinct roots in E.*

Proof. Since there is a natural embedding $F[X] \subseteq E[X]$, we may view $f(X)$ as a polynomial in $E[X]$. Since E is a field, $E[X]$ is an Euclidean domain, so the division algorithm applies, and for any $u \in E$, we have

$$f(X) = q(X)(X - u) + r$$

where $q(X) \in E[X]$ and $r \in E$ is a constant. If $f(u) = 0$, it follows that $r = 0$ and $X - u$ divides $f(X)$ in $E[X]$. If $u' \neq u$ is another root of $f(X)$ in E, since $u' - u \neq 0$, it follows that $q(u') = 0$. Continuing by induction on $\deg f(X)$, we conclude that

$$f(X) = (X - u_1)(X - u_2)\dots(X - u_m)f_1(X)$$

where $u_1, u_2, \dots, u_m$ are the distinct roots of $f(X)$ in E and $f_1(X) \in E[X]$ has no roots in E except possibly those already listed.

Clearly, $m \leq \deg f(X)$. □

Corollary. *Let F be a field. Then any finite subgroup G of $U(F) = F^*$ is cyclic. In particular, $\mathbf{F}_p^*$ is cyclic of order $p - 1$.*

Proof. Since G is a finite abelian group, it is a direct product of cyclic groups. If all these cyclic groups have relatively prime orders, then their direct product is cyclic and we are done. Otherwise, the direct product contains two distinct factors $\mathbf{Z}/r\mathbf{Z}$ and $\mathbf{Z}/s\mathbf{Z}$ such that r and s have a prime factor q in common. Since a cyclic group of order divisible by q always contains a subgroup cyclic of order q, it follows that G contains a subgroup isomorphic to $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$, so it contains at least q^2 elements satisfying the equation $x^q = 1$. By the above proposition, there are at most q such elements, so we have a contradiction to the sentence beginning “Otherwise” above. □

A generator of the multiplicative group of $\mathbf{F}_p$ (**i.e.** $\mathbf{Z}/p\mathbf{Z}$) is called in number theory a *primitive* element mod p.

Exercises.

1. Let $E \supseteq F$ be an extension of fields, and let $x \in E$. Define $\lambda_x : E \to E$ by $\lambda_x(y) = xy$. (a) Show that λ_x is F-linear. (b) Assuming $[E : F] < \infty$, show that the minimal polynomial $m(X)$ of x over F (as defined in field theory) is the same as the minimum polynomial of λ_x as defined in linear algebra. (c) Show that the characteristic polynomial of λ_x is $m(X)^{[E:F(x)]}$. **Note:** Use the theory of modules over a PID as developed last quarter and applied to the ring $F[X]$ acting on E by $f(X)y = f(\lambda_x)(y) = f(x)y$.

2. (a) Show that $\mathbf{Q}[X]$ as a set is denumerable.

(b) Show that any finite algebraic extension of $\mathbf{Q}$ is denumerable.

(c) Show that any algebraic extension of $\mathbf{Q}$ is denumerable. Hint. You may use the fact that a denumerable union of denumerable sets is denumerable.

2. Degree, Algebraic Extensions

Let F be a field, and let E be an extension field. We may view E as a vector space over F, and so doing we define the *degree* of E over F by $[E : F] = \dim_F E$. The degree of an extension may be finite or infinite. For example, $[\mathbf{C} : \mathbf{R}] = 2$, but $[\mathbf{R} : \mathbf{Q}]$ is the cardinality of $\mathbf{R}$.

Proposition. *Let $F \subseteq L \subseteq E$ be fields. Then*

$$[E : F] = [E : L][L : F].$$

Also, $[E : F] < \infty \Leftrightarrow [E : L] < \infty$ and $[L : F] < \infty$.

Proof. We prove this only in the case of finite degrees although it is true in general.

Suppose first that $[E : L] < \infty$ and $[L : F] < \infty$. Let $\{y_1, \dots, y_n\}$ be a basis for E over L, and let $\{x_1, \dots, x_m\}$ be a basis for L over F. Then $\{x_i y_j \mid i = 1, \dots, m, j = 1, \dots n\}$ is a basis for E over F. For, since any element of E is a linear combination of the y_j with coefficients in L, and any such coefficient is a linear combination of the x_i with coefficients in F, it follows that the elements $x_i y_j$ span E over F. On the other hand, given a relation

$$\sum a_{ij} x_i y_j = \sum \left(\sum a_{ij} x_i \right) y_j = 0,$$

since $\sum a_{ij} x_i \in L$ for each j, we conclude by the independence of the y_j over L that $\sum a_{ij} x_i = 0$ for each j. Since the x_i are linearly independent over F, it follows that $a_{ij} = 0$ for all i and j.

On the other hand, if E has an infinite basis over L or L has an infinite basis over F, it is not hard to see that in either case that basis would be a linearly independent set over F so E would have to be infinite dimensional over F. □

Proposition. *Let E be an extension of F. $x \in E$ is algebraic over F if and only if $[F(x) : F] < \infty$.*

Proof. Clear since $F[x] \cong F[X]/I$ is finite dimensional and equal to $F(x)$ if and only if $I = (g(X))$ is nonzero, i.e. x is algebraic. □

An *extension* $E \supseteq F$ is said to be *algebraic* if every element is algebraic.

Corollary. *If $[E : F] < \infty$ then E is algebraic over F.*

Proof. For any $x \in E$, $[F(x) : F] < [E : F]$ so x is algebraic over F. □

As we shall see shortly, the converse of the corollary is not true.

Let $E \supseteq F$ be a field extension and let $x_1, x_2, \dots, x_k$ be elements of E. We introduce the notation $F(x_1, x_2, \dots, x_k)$ for the smallest subfield of E containing F and $x_1, x_2, \dots, x_k$. Note that if $x_1, x_2, \dots, x_k$ are algebraic over F, then $F[x_1, x_2, \dots, x_k] = F(x_1, x_2, \dots, x_k)$ and it is finite dimensional and hence algebraic over F. For, if $x \in E$ is algebraic over F, then it is algebraic over any intermediate field L with $E \supseteq L \supseteq F$. Hence, we may use induction and the truth of the assertion for $k = 1$.

Proposition. *(Transitive property of algebraic extensions.) If E is algebraic over L and L is algebraic over F, then E is algebraic over F.*

Proof. Let $x \in E$. Then x is the root of a polynomial $g(X) \in L[X]$ since x is algebraic over L. The *coefficients* $a_1, \dots, a_m \in L$ of this polynomial are algebraic over F. Consider the subfield $L' = F(a_1, \dots, a_m)$ of E. By the above remark, $[L' : F] < \infty$. Since x satisfies a polynomial equation over L', $[L'[x] : L'] < \infty$. By the transitivity of degree, $[L'[x] : F] < \infty$. However, $F[x] \subseteq L'[x]$ so $[F[x] : F] < \infty$ and x is algebraic over F. □

Proposition. *Let $E \supseteq F$ be a field extension. The set of all elements of E which are algebraic over F is a subfield of F.*

Proof. Let $\bar{F}$ denote the set of algebraic elements of E. If u and $v \in \bar{F}$, then $F[u,v] = F(u,v)$ is algebraic over F. Hence, $u+v$, uv and $u^{-1}(u \neq 0)$ are also algebraic over E so it follows that $\bar{F}$ is closed under addition, multiplication, and forming inverses. □

Note that the proof relies on the characterization of algebraic elements in terms of the dimension of $F[x]$ over F. To show *directly* that $u+v$ or uv satisfies an algebraic equation over F would be extremely difficult. Try it!

The subfield $\bar{F}$ of E will often be of infinite degree over F provided E is of infinite degree over F. For example, it is not hard to see that the polynomials $X^n - 2 \in \mathbf{Q}[X]$ are all irreducible. (Try proving it by generalizing the proof that $\sqrt{2}$ is irrational.) Since each of these polynomials has a root in $\mathbf{C}$ (even in $\mathbf{R}$), it follows that $\mathbf{C}$ has subfields of arbitrarily high degree over $\mathbf{Q}$. Hence, $\bar{Q}$ in $\mathbf{C}$ will be infinite dimensional over $\mathbf{Q}$.

$\bar{F}$ can have no proper algebraic extensions L *in* E because of the transitive property of algebraic extensions. However, it could have algebraic extensions partially disjoint from E. In fact, given an irreducible polynomial $f(X)$ in $L[X]$ of degree greater than one, we may construct infinitely many fields isomorphic to $L[X]/(f(x))$ which may be suitable viewed as extensions of E after some identifications. Of course by what we showed above, it would not be possible to make all these extensions subfields of the same extension of L. Often to avoid such complications, one insists that all field extensions be contained in one fixed 'very large' common field. But at this stage we are not ready to specify the properties of such a field, so we shall not make that assumption yet. If you feel more comfortable, then for the rational numbers $\mathbf{Q}$, it would be safe to assume all extensions of $\mathbf{Q}$ are subfields of the complex number field $\mathbf{C}$.

Generally, if an intermediate field L ($E \supseteq L \supseteq F$) has no extensions in E algebraic over F, we say that it is relatively algebraically closed in E. (If it were algebraic over F, it would have to equal $\bar{F}$.) If on the other hand, it has no algebraic extensions whatsoever we say just that it is *algebraically closed*.

Proposition. *A field L is algebraically closed if and only if every irreducible polynomial over L is of degree 1.*

Proof. If $f(X) \in L[X]$ is irreducible, then $L[X]/(f(X))$ is an algebraic extension of L. Hence, if L is algebraically closed, every irreducible polynomial in $L[X]$ is of degree 1. Conversely, if x in some extension is algebraic, then $[L[x] : L] =$ the degree of the minimal polynomial of x, so $[L[x] : L] = 1$ and $x \in L$. □

According to the *fundamental theorem of algebra*, the complex number field $\mathbf{C}$ is algebraically closed. The fundamental theorem was first proved rigorously by Gauss who eventually provided something like eight proofs of the theorem. There are some relatively simple proofs using complex function theory, and there are some neat proofs depending on simple topological properties of plane curves. (The complex function theory relies on Cauchy's theorem which in turn involves some basic geometry in the plane so probably these proofs at heart are the same. Later we shall introduce an almost purely algebraic proof in the exercises.)

For any field F, it is possible to construct by means of Zorn's Lemma an algebraically closed field K containing F. (We shall return to this point later.) In $K[X]$, any polynomial (including polynomials over F) factor completely into linear factors.

Exercises.

1. (a) What is $[\mathbf{Q}[\sqrt{2}, i] : \mathbf{Q}]$? Justify your contentions.
   (b) How about $[\mathbf{Q}[\sqrt{2}, \sqrt{3}] : \mathbf{Q}]$? Find an algebraic equation over $\mathbf{Q}$ satisfied by $\sqrt{2} + \sqrt{3}$.
2. Let p be a prime. Show that $X^n - p$ is irreducible in $\mathbf{Q}[X]$. Hint: Use Gauss's Lemma.

3. Splitting fields and Normality

Let F be a field and let $f(X) \in F[X]$. An extension $M \supseteq F$ is called a *splitting* field for $f(X)$ if and only if $M = F(x_1, \dots, x_n)$ and $f(X)$ *splits completely* in $M[X]$, that is

$$f(X) = c(X - x_1)(X - x_2) \dots (X - x_n) \text{ in } M[X]$$

(where $c \in M$ is a nonzero constant). $x_1, \dots, x_n$ are "all" the roots of $f(X)$ in the sense that there are not any other distinct roots in any extension M' of M. (If there were such a root y, $X - y$ would have to divide $f(X)$ in $M'[X]$ which contradicts unique factorization). Of course, $f(X)$ could have other roots in some other field not containing M.

Proposition. *Let $f(X) \in F[X]$ be a non-constant polynomial over a field F. Then there exists a splitting field for $f(X)$.*

Proof. Let $g(X)$ be an irreducible factor of $f(X)$. As mentioned previously, we may construct an extension $F_1 = F[X]/(g(X)) = F[x_1]$ in which $g(X)$ has a root x_1. In $F_1[X]$, we may factor

$$f(X) = (X - x_1)f_1(X)$$

and then we may iterate the argument for $f_1(X)$ over F_1. □

Often it is convenient to choose some algebraically closed field containing F and then take all splitting fields of polynomials within that field.

It is a remarkable fact that if K is a splitting field of a polynomial $f(X) \in F[X]$, then not only does that polynomial split completely in $K[X]$, but *any* irreducible polynomial $g(X) \in F[X]$ which has a root in K also splits completely in $K[X]$. An extension $K \supseteq F$ with the latter property is called *normal*.

Before proving this assertion about splitting fields, we need an auxiliary fact about extending field isomorphisms. Let $\sigma : F \to F'$ be an isomorphism of fields. We may extend this to an isomorphism of rings (also denoted σ) from $F[X] \to F'[X]$ by defining

$$\sigma(a_0 + a_1X + \cdots + a_kX^k) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_k)X^k.$$

Lemma. *Let $\sigma : F \to F'$ be a field isomorphism, and suppose $g(X) \in F[X]$ is irreducible. let x and x' be elements in appropriate extensions of these fields where x is a root of $g(X)$ and x' is a root of $\sigma(g(X))$. Then σ extends uniquely to a field isomorphism $\phi : F[x] \to F'[x']$ such that $\phi(x) = x'$.*

$$\begin{tikzcd}
F[x] \arrow[r, "\phi"] & F'[x'] \\
F \arrow[u] \arrow[r, "\sigma"'] & F' \arrow[u]
\end{tikzcd}$$

Proof. Certainly, such an extension, if it exists, is unique since it is given on F and takes x to x'.

To construct such an isomorphism, proceed as follows. Let $g'(X) = \sigma(g(X))$. Then,the natural epimorphism $F[X] \to F[x]$ has kernel $I = (g(X))$ and the natural epimorphism $F'[X] \to F'[x']$ has kernel $I' = (g'(X))$. Since $\sigma(I) = I'$, it follows that the function $\phi : F[x] \to F'[x']$ defined by $\phi(\sum a_i x^i) = \sum \sigma(a_i)(x')^i$ is well defined and is an isomorphism of fields.

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d] & F[X] \arrow[r] \arrow[d, "\sigma"'] & F[x] \arrow[r] \arrow[d, "\phi"'] & 0 \\
0 \arrow[r] & I' \arrow[r] & F'[X] \arrow[r] & F'[x'] \arrow[r] & 0
\end{tikzcd}$$

Also, it is clear that ϕ extends σ □

Note that even in the case $\sigma = id_F$ (so $F = F'$), ϕ need not be the identity if $x \neq x'$.

Proposition. *Let K be a splitting field for $f(X) \in F[X]$. Then K is normal over F. Conversely, any finite normal extension K of F is a splitting field of some nonconstant polynomial in $F[X]$.*

Proof. Let K be a splitting field for $f(X) \in F[X]$ with roots $x_1, \dots, x_n$ in K. Let $g(X) \in F[X]$ be irreducible, and suppose it has a root $y \in K$. If $g(X)$ does not split completely in $K[X]$, we may certainly construct a splitting field M for $g(X)$ *over* K. Pick some other root $z \in M$ with z possibly not in K. Since y and z are both roots of the same irreducible polynomial $g(X)$ over F, we may extend the identity on F to a field isomorphism $\sigma : F[y] \to F[z]$ by the above lemma. Now view $f(x)$ as a polynomial over each of these fields. Since the coefficients of $f(X)$ are in F, we have $\sigma(f(X)) = f(X)$. It is clear that $K = F[x_1, \dots, x_n] = F[y, x_1, \dots, x_n]$ is a splitting field for $f(X)$ over $F[y]$ and $K' = F[z, x_1, \dots, x_n]$ is a splitting field for $f(X)$ over $F[z]$. If we consider inductively each element x_i and its minimal polynomial over $F[y, x_1, \dots, x_{i-1}]$, we may apply the lemma to obtain a root x_i' of $f(X)$ in M and an isomorphism $\phi_i : F[y, x_1, \dots, x_i] \to F[z, x_1', \dots, x_i']$ extending σ and such that $\phi(x_i) = x_i', i = 1, \dots, n$. However, since $f(X)$ can have at most n roots in M, it follows that $\{x_1', \dots, x_n'\} = \{x_1, \dots, x_n\}$. Hence, we have an isomorphism $K = F[y, x_1, \dots, x_n] \to F[z, x_1, \dots, x_n] = K[z]$. But since $K \subseteq K[z]$, this is not possible by degree considerations unless $z \in K$. Thus, $M = K$ and $g(X)$ splits completely in K.

Conversely, let K be a finite normal extension. Since it is finite, it can be written $F[z_1, \dots, z_n]$. Each element z_i is a root of an irreducible polynomial $g_i(X) \in F[X]$ which splits completely in K by normality. If we take $f(X)$ to be the product of the $g_i(X)$, then $f(X)$ certainly splits completely in K, and since K is generated by a subset of its roots, it is also generated by all its roots. □

Exercises.

1. Determine the degrees of the splitting fields of each of the following polynomials over the indicated fields. (a) $X^2 + 10X + 1$ over $\mathbf{Q}$. (b) $X^2 + 10X + 1$ over $\mathbf{F}_5$. (c) $X^3 - 1$ over $\mathbf{Q}$. (d) $X^3 - 2$ over $\mathbf{Q}$.

2. Prove that every extension of degree 2 is normal.

4. Extension of morphisms

In the previous section, we showed that a splitting field is always a normal extension. For the proof we introduced a fact about extending isomorphisms of fields. We shall now investigate such questions in greater detail.

Proposition. *Assume $\sigma : F \to F'$ is a field isomorphism, let $f(X) \in F[X]$ be any non-constant polynomial, and let $f'(X) = \sigma(f(X))$. Let $K \supseteq F$ be a splitting field for $f(X)$, and let $K' \supseteq F'$ be a splitting field for $f'(X)$. Then σ may be extended to an isomorphism $\Sigma : K \to K'$.*

$$\begin{tikzcd}
K \arrow[r, "\Sigma"] & K' \\
F \arrow[u] \arrow[r, "\sigma"] & F' \arrow[u]
\end{tikzcd}$$

Proof. Choose a subfield E with $K \supseteq E \supseteq F$ and such that σ can be extended to a monomorphism $\tau : E \to K'$ and such that $[E : F]$ is maximal with respect to these properties. Let x be any root of $f(X)$ in K. If x is not in E, then τ can be extended to $\tau' : E[x] \to K'$. For if $g(X)$ is the minimal polynomial of x over E, then $g'(X) = \sigma(g(X))$ is a factor in $\tau(E)[X]$ of $f'(X)$, so $g'(X)$ splits completely in K'. Thus, by the above extension result, we can extend τ to $\tau' : E[x] \to \tau(E)[x'] \subseteq K'$ where x' is any root of $g'(X)$ in K'. By maximality, it follows that E contains all roots of $f(X)$ in K so $E = K$.

Thus, we at least have a monomorphism $\Sigma : K \to K'$ extending σ. In fact, it is an epimorphism also. For, since $f(X)$ splits completely into linear factors in K, it follows that $f'(X)$ does the same in $\Sigma(K) \subseteq K'$. Hence, $\Sigma(K)$ contains a splitting field for $f'(X)$, so $\Sigma(K) = K'$. □

Corollary. *Any two splitting fields of the same polynomial $f(X) \in F[X]$ are isomorphic by an isomorphism which is the identity on F.*

Corollary. *Let K be a finite normal extension of F. Let $\sigma : E \to E'$ be an isomorphism of one intermediate field onto another which fixes F. Then σ may be extended to an automorphism of K which fixes F.*

Proof. Since K is finite and normal over F, it is a splitting field for some polynomial over F. Clearly, it is a splitting field for the same polynomial over E and E' respectively. Now apply the proposition. □

Let $E \supseteq F$ be a finite extension. Then certainly $E = F(y_1, \dots, y_m)$ for appropriate $y_1, \dots, y_m \in E$. Let $g_i(X) \in F[X]$ be the minimal polynomial of y_i. Let $g(X) = \prod g_i(X)$. Viewing $g(X)$ as a polynomial in $E[X]$, we may construct a splitting field $N = E(x_1, \dots, x_n)$ where $x_1, \dots, x_n$ are the roots of $g(X)$. However,

$$N = F(y_1, \dots, y_m)(x_1, \dots, x_n) = F(x_1, \dots, x_n)$$

since $\{y_1, \dots, y_m\}$ is a subset of $\{x_1, \dots, x_n\}$. Hence, N is a splitting field over F and so it is normal over F. If we let K be the smallest subfield of N normal over F and containing E, then it is possible to show that K is unique up to an isomorphism fixing E. That is, if we picked another $N' \supseteq E$ normal over F and we formed the corresponding K', there would be an isomorphism $K \cong K'$ fixing E. K is called a *normal closure* of E, and it is unique in the above sense..

Proposition. *(Characterization of normality) Let $K \supseteq F$ be a finite field extension. K is normal over F if and only if for every finite extension $N \supseteq K \supseteq F$ which is normal over F and for every automorphism $\sigma : N \to N$ fixing F, we have $\sigma(K) = K$.*

Proof. Suppose K is normal over F. Then it is a splitting field of a polynomial $f(X) \in F[X]$. Hence, $\sigma(K)$ is a splitting field for $\sigma(f(X)) = f(X)$ since σ fixes F. However, since a splitting field is generated by "all" the roots of $f(X)$, there is at most one splitting field of $f(X)$ in any one field N. Hence, $\sigma(K) = K$.

Suppose conversely that K is fixed under all appropriate σ. Let $g(X) \in F[X]$ be irreducible and suppose it has at least one root $x \in K$. Since $N \supseteq F$ is normal, it splits completely over N. Let $y \in N$ be any other root. We shall show that $y \in K$ so it will follow that $g(X)$ splits completely over K. To see that $y \in K$, consider the two subfields $F[x]$ and $F[y]$ of N. Since x and y are roots of the same irreducible polynomial, there is an isomorphism $\sigma : F[x] \cong F[y]$ fixing F, and by our basic result on extending isomorphisms, σ may be extended to an automorphism σ of N. Since $\sigma(K) = K$, $y = \sigma(x) \in K$ as claimed. □

Example. In $\mathbf{C}$, let $\omega = e^{(2\pi i/3)}$. ω is a root of the irreducible quadratic polynomial $X^2 + X + 1 \in \mathbf{Q}[X]$. Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2.

$$\begin{tikzcd}
 & \mathbf{C} \arrow[d, dash] & \\
 & K = \mathbf{Q}[\alpha, \omega] & \\
\mathbf{Q}[\alpha] & & \mathbf{Q}[\omega] \\
 & \mathbf{Q} &
\end{tikzcd}$$

The roots in $\mathbf{C}$ of $X^3 - 2$ are α, $\alpha\omega$, and $\alpha\omega^2$. (Note that $\omega^3 = 1$.) Hence, it is easy to see that K is its splitting field. Thus, K is normal over $\mathbf{Q}$. $\mathbf{Q}[\omega]$ is also normal over $\mathbf{Q}$ since it is a splitting field for $X^2 + X + 1$. $\mathbf{Q}[\alpha]$ is not normal over $\mathbf{Q}$. (Why not?)

Exercises.

1. In the example, show that $\mathbf{Q}[\alpha]$ is not normal over $\mathbf{Q}$.

2. Let α be the real fourth root of two and let $\zeta = e^{2\pi/4}$. Show that $\mathbf{Q}(\alpha, \zeta)$ is the splitting field in $\mathbf{C}$ of $X^4 - 2$ over $\mathbf{Q}$. Show that $\mathbf{Q}(\alpha^2)$ and $\mathbf{Q}(\zeta)$ are normal extensions of $\mathbf{Q}$ but $\mathbf{Q}(\alpha)$ is not.