FIELD THEORY

Preliminaries

We call a pair of fields E and F such that $F \subset E$ a field extension and denote it by E/F.

Let S be a subset of E. $F[S]$ (resp. $F(S)$) denotes the smallest subring (resp. subfield) of E containing both F and S. In case $S = \{u_1, \ldots, u_n\}$, a finite subset of E, we write $F[S] = F[u_1, \ldots, u_n]$ and $F(S) = F(u_1, \ldots, u_n)$. Note that $F(S)$ is an extension of F and it is called the extension of F generated by S.

We know how $F[S]$ looks like. It is nothing but the subalgebra of E (over F) generated by S.

Let $u \in E$. If u is a root of a polynomial over F, in which case we say that u is algebraic, then there is a monic polynomial of least degree which assumes u as a root. Such a polynomial is unique and is called the minimal polynomial of u. Let $p(x)$ be the minimal polynomial of u. Then it is easy to see that

$$F(u) = F[u] \cong F[x]/_{(p(x))}.$$

By division algorithm one can easily see that $F[u]$ consists of elements of the form $f(u)$ where $f(x) \in F[x]$ with $\deg(f(x)) < \deg(g(x)) = n$, i.e.,

$F[u] = \{ a_0 + a_1 u + \dots + a_{n-1} u^n : a_0, a_1, \dots, a_{n-1} \in F \}$.
This, in particular, shows that $F(u)$ is spanned, as a vector space over F, by the elements $1, u, \dots, u^{n-1}$. Thus $\dim_F F(u) = n$. This is often expressed as $[F(u):F] = n$ in Field Theory. More generally, for a field extension E/F, the dimension of E, as a vector space, over F is denoted by $[E:F]$. The number $[F(u):F]$ (in case u is algebraic) is also called the degree of u over F. Notice that the degree of u is just the degree of its minimal polynomial.

If $u \in E$ is not algebraic, then we say that u is transcendental over F. In this case, the elements $1, u, u^2, \dots$ of $F(u)$ are linearly independent (which is equivalent to saying that $F[u] \cong F[x]$) and $F(u)$ cannot be finite dimensional over F.

Theorem. Let $F \subset E \subset K$ be a two-storied extension of fields (or, in other words, a tower of fields). Then $[K:F]$ is finite if and only if $[K:E]$ and $[E:F]$ are finite. In this case, we have $[K:F] = [K:E][E:F]$.

A field extension E/F is said to be finitely generated if $E = F(u_1, \dots, u_n)$ for some $u_1, \dots, u_n \in E$. The extension E/F is said to be simple if $E = F(u)$ for a single element $u \in E$.

We say that E is algebraic over F or E/F is an algebraic extension if every element of E is algebraic over F. It can be shown that if $F \subset E \subset K$ is a field tower, then K/F is algebraic if and only if both E/F and K/E are algebraic.

Proposition. Let E/F be a field extension, and let $a_1, \ldots, a_n$ be elements of E which are algebraic over F. Then

$$F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n].$$

Corollary. Let E/F be a field extension and let $a, b \in E$ be algebraic over F. Then $a+b$, ab, a/b are all algebraic over F.

Proposition. Let F be a field. Every extension E of F of finite degree n is algebraic over F, and every element of E is algebraic of degree $\leq n$ over F.

Foundations of Galois theory

Let K/F be a field extension. The Galois group of K over F is the group of all automorphisms of K that leave every element of F fixed (in brief: automorphisms of K/F).

$$K = F \Rightarrow \text{Galois group} = 1$$

$$\left.\begin{array}{ll} F = \mathbb{Q} & K = \mathbb{Q}(\sqrt{2}) \\ F = \mathbb{R} & K = \mathbb{C} \end{array}\right\} \text{ the order of the Galois group is } 2.$$

$$F = \mathbb{Q} \quad K = \mathbb{Q}(\sqrt[3]{2}) \Rightarrow \text{Galois group} = 1$$

Let $F \subset E \subset K$ be a tower of fields and let G be the Galois group K over F. Define

$$E' = \{\sigma \in G : \sigma(x) = x \text{ for all } x \in E\}.$$

Clearly E' in a subgroup of G. Let H be any subgroup of G. We define

$$H' = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in H\},$$

which is clearly a subfield of K containing F.

$$\begin{array}{ccc} K & & 1 \\ \cup & & \cap \\ E & \longrightarrow & E' \\ \cup & & \cap \\ F & & G \end{array} \qquad \begin{array}{ccc} K & & 1 \\ \cup & & \cap \\ H' & \longleftarrow & H \\ \cup & & \cap \\ F & & G \end{array}$$

In general, we have $K' = 1$, $1' = K$, $F' = G$. But it is <u>not</u> necessarily the case that $G' = F$. G' may be properly larger

than F (for example, when $F=\mathbb{Q}$ and $K=\mathbb{Q}(\sqrt[3]{2})$). We say that K is normal over F if $F=G'$, i.e., for any $x\in K\setminus F$, there exists an automorphism of K leaving every element of F fixed but moving x. If we are given a field K which is not normal over F, we can replace the base field by the larger field G' to obtain a normal extension.

Suppose $F\subset E_1\subset E_2\subset K$ is a field tower and $H_1\subset H_2$ are two subgroups of G. Then we have

$$E_1'\supseteq E_2' \quad \text{and} \quad H_1'\supseteq H_2'.$$

$$E_1\subseteq E_1'' \quad \text{and} \quad H_1\subseteq H_1''$$

The double prime of any object is called its closure. An intermediate field or subgroup is called closed if it is equal to its closure (i.e. double prime).

K is normal over $F \iff F$ is closed.

Theorem. Let K/F be a field extension and G the Galois group of K/F. Then the priming operation sets up a 1-1 correspondence between the closed subgroups of G and the closed fields lying between K and F.

Theorem. Let $F\subset E\subset D\subset K$ be fields with $[D:E]=n<\infty$. Then $[E':D']\leq n$.

Let G be the Galois group of K/F. Let $H\supset J$ be subgroups of G with $[H:J]=n<\infty$. Then $[J':H']\leq n$.

proof. For the first part, we argue by induction on n, the case $n=1$ being trivial. If there is a field E_0 properly between E and D, then we know $[E':E_0'] \leq [E_0:E]$ and $[E_0':D'] \leq [D:E_0]$. By multiplicative property of dimensionalities, we obtain $[E':D'] \leq [D:E]$. We may therefore assume that there are no fields between E and D. Necessarily $D = E(u)$ for some $u \in D$. Let f be the minimal polynomial of u over E. Clearly, $\deg f \leq n$.

Consider a left coset C of D' in E'. It has the form $C = \tau D'$ for some $\tau \in E'$. Since every automorphism in D' leaves u fixed, the entire coset C has the same effect on u, sending u to $\tau(u)$. If $C_0 = \tau_0 D'$ is a second left coset distinct from C, then $\tau_0(u)$ must be different from $\tau(u)$. For if $\tau_0(u) = \tau(u)$, then $\tau_0\tau^{-1}$ leaves u fixed, hence leaves $D = E(u)$ elementwise fixed, hence lies in D'; but then $\tau_0 D' = \tau D'$. Note that each $\tau(u)$ is a root of f, for τ leaves the coefficient of f fixed. Hence the number of left cosets of D' in E' is at most equal to the number of roots of f, which is at most n.

For the second part of the theorem, consider a left coset $C = \tau J$ of J in H. For any $x \in J'$, we may write $Cx = \tau(x)$ and speak of applying C to any

element of J'.

Suppose $[J' : H'] > n$. Pick $u_1, \ldots, u_{n+1}$ in J' linearly independent over H'. Let $C_1, \ldots, C_n$ be the list of all cosets of J in H. Form the equations

$$\begin{aligned}
(C_1 u_1) a_1 + \cdots + (C_1 u_{n+1}) a_{n+1} &= 0 \\
(C_2 u_1) a_1 + \cdots + (C_2 u_{n+1}) a_{n+1} &= 0 \\
\vdots \qquad\qquad\qquad\qquad & \vdots \\
(C_n u_1) a_1 + \cdots + (C_n u_{n+1}) a_{n+1} &= 0
\end{aligned}$$

with $n+1$ unknowns $a_1, \ldots, a_{n+1}$. All the coefficients lie in the field K, and so there exists in K a non-trivial solution. Among all solutions pick one with as many zeros as possible; without loss of generality we may assume that this solution has the form

$$a_1, \ldots, a_r, 0, \ldots, 0$$

where $a_i \neq 0$ for each i. We may also assume $a_1 = 1$. It is not possible that all the a's lie in H'. Suppose $a_2 \notin H'$. Then there exists $\sigma \in H$ such that $\sigma(a_2) \neq a_2$. Apply σ to the equations to get

$$\sum_i \sigma(C_i u_j)\, \sigma(a_j) = 0 \,, \quad j = 1, \ldots, n+1$$

Note that σC_i are simply permutations of $C_1, \ldots, C_n$. Then new equations are the permutations

of the old and $1, \sigma(a_2), \ldots, \sigma(a_r), 0, \ldots, 0$ is also a solution of the system. Substracting the two solutions yield a solution with more zeros, non-trivial since $a_2 - \sigma(a_2) \neq 0$.

Theorem. (a) Let $F \subset E \subset D \subset K$ be a field tower. Assume E is closed and that $[D:E]=n < \infty$. Then D is also closed; moreover $[E':D']=n$.
(b) Let $H \subset J$ be subgroups of the Galois group of K/F. Assume that H is closed and that $[J:H]=n < \infty$. Then J is also closed; moreover $[H':J']=n$.

proof. (a) By the previous theorem, we have

$$[E' : D'] \leq n.$$

Using the same theorem together with the fact that E is closed, we have

$$n = [D : E] \leq [D'' : E] = [D'' : E''] \leq [E' : D'] \leq n.$$

This shows that $[E' : D'] = n$ and $D'' = D$.
(b) Similarly as in part (a).

Corollary. Let G be the Galois group of K over F. Then
(a) All finite subgroups of G are closed,
(b) If K is normal over F and E is an intermediate field with $[E:F]$ finite, then K is normal over E.

proof. (a) Let H be a finite subgroup of G. Since $[H:1] = |H| < \infty$ and 1 is closed in G, by the preceding theorem, H is also closed in G.
(b) If K is normal over F, then F is closed. By the preceding theorem, E is also closed, which means that K is normal over E.

Theorem (Fundamental Theorem of Galois Theory) Let K be a normal finite-dimensional extension of F, $G = Gal(K/F)$. Then there is a one-to-one correspondence between the subgroups of G and the fields between F and K, implemented by the priming operation. In this correspondence the relative dimension of two intermediate fields equals the relative index of the corresponding subgroups. In particular, the order of G is equal to $[K:F]$.

Theorem [Artin] Let G be a finite group of automorphisms of a field K and let F be the fixed subfield of K under G. Then K is normal and finite dimensional over F and the full Galois group of K/F is G.

proof. By assumption $G' = F$. Since $|G| = [G:1] \geq [1':G'] = [K:F]$, K/F is finite-dimensional. Let $G_1 = Gal(K/F)$. Then $G \subseteq G_1$ and $F \subseteq G_1' \subseteq G' = F$. This gives that $G_1' = F$ and so K/F is normal $\Rightarrow |G_1|$ is finite $\Rightarrow G$ is closed in G_1. On the other hand, $G = G'' = F' = Gal(K/F) = G_1$, which completes the proof.

D: field, $x_1, \ldots, x_n$: indeterminates,
$K := D(x_1, \ldots, x_n)$: rational function field over D
$G :=$ the group of automorphisms of K obtained by permuting the x's. (Indeed, $G \cong S_n$.)
$F :=$ the fixed subfield of K under G
(Note that F is the field of all symmetric rational functions in the x's with coefficients in D.

$\rightarrow S_n$ is the Galois group of the extension K/F.
Since every finite group is a subgroup of some S_n, we can view any finite group as a Galois group.

Normality and Stability

Definition. Let $F \subset E \subset K$ be a tower of fields. We say that E is stable (relative to F and K) if every automorphism of K/F sends E into itself.

Remark
Let τ be an auto. of K/F and E is stable. Then τ sends E onto itself because τ^{-1} also sends E into itself.

Theorem. Let G be the Galois group of K/F.
(a) If E is a stable intermediate field, then E' is a normal subgroup of G.

(b) If H is a normal subgroup of G, then H' is a stable intermediate field.

proof. (a) Given $\sigma \in G$ and $\tau \in E'$, we must show that $\sigma^{-1}\tau\sigma(x) = x$ for all $x \in E$ or equivalently, $\tau\sigma(x) = \sigma(x)$

for all $x \in E$. But this true since E is stable and so $\sigma(x) \in E$.

(b) The proof is essentially the same. □

Corollary. The closure of a normal subgroup is normal; the closure of a stable intermediate field is stable.

Theorem. If $F \subset E \subset K$ is a field tower, K is normal over F and E is stable (relative to F and K), then E is normal over F.

proof • Take $u \in E \setminus F$.

• Find an automorphis τ of K/F that moves u, i.e. $\tau(u) \neq u$. (use the normality of K/F.)

• Restriot τ to E to obtain an auto. of E/F (use stability of E). This restricted auto. fulfills the requirement. □

Theorem. Suppose K is normal over F and f is an irreducible polynomial with coefficients in F having a root u in K. Then f factors over K into distinct linear factors.

proof

$u_1 = u, u_2, \ldots, u_r$: all the distinct images of u under automorphisms of K/F.

$\Rightarrow u_i$ is a root of f $\forall i$. $\Rightarrow r \leq n = \deg(f)$.

Write : $g(x) = (x - u_1) \ldots (x - u_r)$

$\Rightarrow g(x) \in F[x]$ since any auto. of K/F permutes the u's and so coefficients of g are invariant under every auto. of K/F (remember also that K/F is normal).

$\Rightarrow f \mid g$ since f is the minimal poly. of u over F.

$\Rightarrow f = g$ since $\deg(g(x)) \leq \deg(f(x))$. □

Theorem. Let $F \subset E \subset K$ be a field tower, and assume that E is normal over F and algebraic over F. Then E is stable.

proof. $u \in E$ and $\tau \in Gal(K/F) \Rightarrow \tau(u) \in E$ (?)

u algebraic over $F \Rightarrow \exists$ an irreducible f over F s.t. $f(u) = 0 \Rightarrow f$ factors completely in E. Since $\tau(u)$ is a root of f, we must have $\tau(u) \in E$.

□

Theorem. Let G be the Galois group of K/F, and let E be a stable intermediate field. Then G/E' is isomorphic to the group of all automorphisms of E/F that are expandible to K.

proof.

$$\varphi : G \longrightarrow Gal(E/F)$$
$$\tau \longmapsto \tau|_E$$

Clearly $\ker(\varphi) = E'$ and

$Im\,\varphi$ = the set of all automorphisms of E/F that can be extended to K.

□

Suppose:

K/F : finite dimensional and normal

Then stability of an intermediate field E coincides with normality of E/F.

Also $G/E' = Gal(E/F)$ and $[G : E'] = [E : F]$.

This can also be seen using the following more general results.

Theorem. Let $F \subset E \subset K$ be a field tower with $[E:F]=n$. Then there are at most n distinct isomorphisms of E/F into a subfield of K, an isomorphism of E/F being one that leaves F elementwise fixed.

proof We use induction on n. The case $n=1$ is obvious. Let E_0 be an intermediate field properly between F and E. Clearly $[E:E_0] < n$ and $[E_0:F] < n$. By induction, there are at most $[E_0:F]$ isomorphisms of E_0/F into a subfield of K. It is clear that for any two isomorphisms σ and τ of E/F the relation $\sim$ defined by

$$\sigma \sim \tau \iff \sigma|_{E_0} = \tau|_{E_0}$$

is an equivalence relation. Let $[\sigma_1], \ldots, [\sigma_r]$ be the list of all distinct equivalence classes. Clearly, $r \le [E_0:F]$. On the other hand each equivalence class $[\sigma_i]$ contains at most $[E:E_0]$ elements since for any $\tau \in [\sigma_i]$ we have $\tau^{-1}\sigma_i$ is an isomorphism of E/E_0 and, by induction, there are at most $[E:E_0]$ isomorphisms of E/E_0. This gives that there are at most $r \cdot [E:E_0] \le [E_0:F][E:E_0]$ $= [E:F]$ isomorphisms of E/F. Therefore we may assume that there are no intermediate fields properly between F and E. Then $E = F(u)$ for some $u \in E$. Since $[E:F]=n$, u is a root of an irreducible polynomial over F of degree at most n. Since u must go into another root of its irreducible polynomial, the proof is complete. □

Theorem. Let $F \subset E \subset K$ be a field tower with K normal over F and $[E:F] = n < \infty$. Then any isomorphism of

E/F into a subfield of K can be extended to an automorphism of K.

proof. K/F is normal $\Rightarrow F$ is closed $\Rightarrow [G:E'] = n$.
Suppose $G/_{E'} = \{E', \sigma_1 E', \ldots, \sigma_{n-1} E'\}$. Then

$\sigma_1|_E, \ldots, \sigma_{n-1}|_E$ and id_E are all distinct. By above theorem, there are at most n distinct isomorphisms of E/F. This means that if τ is an iso. of E/F which is not identity on E, we must have $\tau = \sigma_i|_E$ for some i. This completes the proof. □

Splitting Fields

Objective: to give a constructive way of exhibiting fields which are normal over a given field K.

Theorem. Let f be an irreducible polynomial with coefficients in a field F. Then there exists a field containing F and a root of f.

Theorem. Let F, F_0 be fields and σ an isomorphism of F onto F_0. Let f be an irreducible polynomial with coefficients in F, f_0 the corresponding polynomial with coefficients in F_0. Let $K = F(u)$, $K_0 = F_0(u_0)$, where u and u_0 are roots of f and f_0, respectively. Then there exists an isomorphism of K onto K_0 which coincides with σ on F and sends u into u_0.

Definition. Let f be a polynomial with coefficients in F. We say that K is a splitting field of f over F if f factors completely in K and $K = F(u_1, \dots, u_r)$ where u's are all the roots of f. When there is no need to call attention to the polynomial f, we shall simply say that K is a splitting field over F.

Later, we shall give a criterion for splitting fields that is independent

of the choice of any polynomial.

Theorem. Let f be any polynomial with coefficients in F. Then there exists a field K which is a splitting field of f over F.

proof. We argue by induction on the degree of f. If f is linear, then $K=F$ will do; more generally if f factors completely in F, $K=F$. Let g be an irreducible factor of f of degree >1. Construct $F(u)$ with u a root of g. Then $f=(x-u)h$, h a polynomial with coefficients in $F(u)$. It suffices to take K to be a splitting field of h over $F(u)$.

Theorem. Let F, F_0 be fields and σ an isomorphism of F onto F_0. Let $f \in F[x]$, $f_0 \in F_0[x]$ the corresponding polynomial. Let K be a splitting field of f over F, K_0 a splitting field of f_0 over F_0. Then σ can be extended to an isomorphism of K onto K_0.

proof. We make an induction on $[K:F]$. If $K=F$, then f factors completely in F, whence f_0 factors completely in F_0, and $K_0=F_0$. We may assume that f has an irreducible factor g of degree >1; let g_0 be the corresponding irreducible factor of f_0 over F_0. Let u (resp. u_0) be a root of g (resp. g_0) in K (resp. K_0). Then we may extend the isomorphism σ to an iso. of $F(u)$ onto $F_0(u_0)$; we continue to write σ for the extended map. Now K is a splitting field of f over $F(u)$ and K_0 is a splitting field of f_0 over $F_0(u_0)$. Since $[K:F(u)]<[K:F]$

our inductive assumption shows that σ can be extended to an isomorphism of K onto K_0.

If $f = \sum a_i x^i$ is a polynomial with coefficients in F, we define $f' = \sum i a_i x^{i-1}$, the derivative of f. By routine computation, we can verify that the usual rules for derivatives hold: $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$, $(cf)' = cf'$ for $c \in K$.

Theorem. Let $f \in F[x]$, a an element of F. Then $(x-a)^2$ divides f if and only if $x-a$ divides both f and f'.

proof. If $f = (x-a)^2 g$, then $f' = (x-a)^2 g' + 2(x-a)g$ is divisible by $x-a$. Suppose $f = (x-a)h$ and $f' = h + (x-a)h'$ is divisible by $x-a$. Then $x-a \mid h$, and hence $(x-a)^2 \mid f$.

Theorem. Let $f \in F[x]$ be irreducible. The following three statements are equivalent:

(1) In every splitting field of f over F, f factors into distinct linear factors.

(2) In some splitting field of f over F, f factors into distict linear factors.

(3) $f' \neq 0$.

proof. (1) implies (2) is obvious.

(2) $\Rightarrow$ (3): Suppose on the contrary that f has a repeated factor $(x-a)^2$ in the splitting field, then $x-a$ divides both f and f'. But f is irreducible over F and f' is a genuine polynomial of lower degree.

Hence $(f, f') = 1$, and so $rf + sf' = 1$ for suitable polynomials $r, s \in F[x]$. On setting $x = a$ we get a contradiction.

Remark. $f' = 0 \iff$ the characteristic is $p \neq 0$ and f is a polynomial in x^p.

Definition. Let f be an irreducible polynomial over F. We say that f is separable over F if any (hence all) of the statements in the above theorem hold. An element u which is algebraic over F is said to be separable over F if its minimal polynomial is separable over F.
A field K which is algebraic over F is separable over F if every element is separable over F.

We remark that separability is automatic in the case of characteristic 0.

Theorem. Let K be a finite-dimensional extension of F. The following statements are equivalent:
(1) K is normal over F,
(2) K is separable over F and K is a splitting field over F,
(3) K is a splitting field over F of a polynomial whose irreducible factors are separable.

proof.

(1) $\Rightarrow$ (2): Let $u \in K$ and f the minimal polynomial of of u over F. Since M/K is normal, f factors completely over F into distinct linear factors. Hence u is separable over F. This shows that K is separable over F since $u \in K$ is arbitrary.

Let $v_1, v_2, \ldots, v_r$ be a basis of K over F, let f_i be the minimal polynomial of v_i over F and write $g = f_1 \cdots f_r$. Normality of M/K implies that each f_i factors completely in F and hence so does g. Clearly K is a splitting field of g over F.

(2) $\Rightarrow$ (3): Say K is a splitting field of f over F, and $f = f_1 \cdots f_r$ is the factorization of f into irreducible factors over F. Each f_i is the minimal polynomial of an element in K which by hypothesis is seperable over F. Hence each f_i is separable over K.

(3) $\Rightarrow$ (1): Assume that K is a splitting field of f over F where the irreducible factors of f are separable. Let $G = Gal(K/F)$. To see that K/F is normal, it is enough to see that $|G| = [K:F]$. (Because if $u \in K \setminus F$, then $|E'| \leq [K:E] \leq [K:F] = |G|$ where $E = F(u)$, which shows that not every element of G leaves u fixed.) If f factors completely in F, then $K = F$ and there is nothing to prove. Let g be an irreducible factor f with degree > 1; say $\deg(g) = r$. Let u be the root of g and write $E = K(u)$, $H = E'$. We have $[G:H]$ = number of images of u in automorphisms of K/F. (For, given two left casets $C_1 = \tau_1 H$ and $C_2 = \tau_2 H$ of H in G, $C_1 = C_2 \Leftrightarrow \tau_1(u) = \tau_2(u)$.)

But every one of the r distinct roots of g is such an image, for if v is another root there is an isomorphism $\sigma : K(u) \longrightarrow K(v)$ leaving K elementwise fixed, and then σ can be extended to an automorphism of K. Hence $[G:H] = r = [E:F]$. Since K is also the splitting field of f over E and the irreducible factors of f over E are separable (they divide the irreducible factors of f over F), $|H| = [K:E]$ by induction. Multiplying, we get that $|G| = [K:F]$ and hence K is normal over F.

Theorem. Let K be a finite-dimensional extension of F. The following statements are equivalent:

(1) K is a splitting field over F.

(2) Whenever an irreducible polynomial over F has a root in K it factors completely in K.

proof.

(1) $\Rightarrow$ (2) : Assume that K is a splitting field of f over F, and let g be an irreducible polynomial over F with root u in K. We must show that g factors completely in K. Suppose on the contrary that over K, g has an irreducible factor h of degree greater than one. Adjoin to K a root v of h. Then there is an isomorphism $\sigma : F(u) \longrightarrow F(v)$ which is identity on F. Now K is a splitting field of f over $F(u)$ and $K(v)$ is a splitting field of f over $F(v)$. It follows that σ can be extended to an isomorphism of K onto $K(v)$. But this is impossible since

$[K(v) : F] \gneq [K : F]$.

(2) $\Rightarrow$ (1): Let $v_1, \ldots, v_r$ be a basis for K over F, let f_i be the minimal polynomial of v_i over F, and write $f = f_1 \cdots f_r$. Then f factors completely in K by hypothesis and K is a splitting field of f over F.

Theorem. Let E/F be an extension of fields, $[E:F]$ finite. There exists a field K containing E such that K is a splitting field over F and no field other than K between E and K is a splitting field over F. If K_0 is a second such field, then there is an isomorphism of K onto K_0 which is the identity on E. If E is separable, then K is normal over F.

proof. Take a basis $v_1, \ldots, v_r$ for E over F, $f = f_1 \cdots f_r$ where f_i is the minimal polynomial of v_i over F, and take K to be a splitting field of f over E. Then K is also a splitting field of f over F and it is normal over F if E is separable over F (for then each f_i is separable over F). Any splitting field over F which contains E must split each f_i since they each possesses a root in E. This shows that K has the property asserted in the theorem. Any second such field K_0 must also be a splitting field of f over F or E, and the uniqueness follows.

We shall call a field having the properties of K in the above theorem a split closure of E over F; if E is separable over F we call K a normal closure of E over F.

Remark. For characteristic 0, normal is the same as splitting field; for characteristic p, normal is splitting field plus separability.