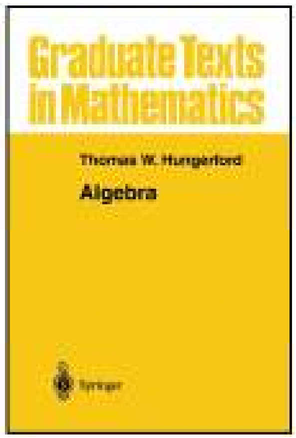
Modern Algebra

Chapter V. Fields and Galois Theory

V.3. Splitting Fields, Algebraic Closure, and Normality (Supplement)—Proofs of Theorems



Theorem V.3.3

Theorem V.3.3. The following conditions on a field F are equivalent:

(i) Every nonconstant polynomial $f \in F[x]$ has a root in F;

(ii) every nonconstant polynomial $f \in F[x]$ splits over F;

(iii) every irreducible polynomial in $F[x]$ has degree one;

(iv) there is no algebraic extension field of F (except F itself);

(v) there exists a subfield K of F such that F is algebraic over K and every polynomial in $K[x]$ splits in $F[x]$.

Proof. Hypothesize (i). If f is a nonconstant polynomial in $F[x]$, then by hypothesis f has a root u_1 in F and so by the Factor Theorem (Theorem III.6.6), $x - u_1$ is a factor of f in $F[x]$. Then $f(x) = (x - u_1)f_1(x)$. Then inductively f can be factored in $F[x]$ into a product of linear terms times a degree 0 polynomial (i.e., a constant). That is, $f(x) = u_0(x - u_1)(x - u_2)\cdots(x - u_n)$. So f splits over F and (ii) follows.

Theorem V.3.3, (i)⇒

Proof (continued). Next, suppose g is an irreducible polynomial in $F[x]$. ASSUME g has degree greater than 1. Then by hypothesis, g has a root u in F and so (again) by the Factor Theorem (Theorem III.6.6), $(x - u)$ is a factor of g in $F[x]$ and so $g(x) = (x - u)g_1(x)$ where $g_1(x)$ is of degree at least 1 (and so g_1 is not a unit in $F[x]$ by Exercise III.6.5, because a field has no nilpotent elements since it has no zero divisors), a CONTRADICTION. So g must be degree 1 and (iii) follows. Next, suppose E is an algebraic extension of F. Then, by definition, every element of E is algebraic over F, so if $e \in E$ then e is a root of some $f \in F[x]$. But by hypothesis, f splits in F (since (i)⇒(ii)) and so all the roots of f are in F and hence $e \in F$. That is, $E = F$ and (iv) follows. For (v), we simply take $K = F$ and then we have trivially that F is algebraic over K. Since (i)⇒(ii) then we have that every polynomial in $K[x] = F[x]$ splits in $F[x]$ (constant polynomials have no zeros and "split" is not defined for them; see page 257). So (v) follows.

Theorem V.3.3, (ii), (iii) ⇒

Proof (continued). Hypothesize (ii). Trivially, (ii)⇒(i) and so from above, (ii) also implies (iii), (iv), and (v).

Hypothesize (iii) and let f be a nonconstant polynomial in $F[x]$. Since F is a field then F is a unique factorization domain (trivially since F contains no nonzero nonunits; see Definition III.3.5) and so by Theorem III.6.14, Fx is a unique factorization domain. So f can be written (uniquely) as a product of irreducible polynomials in $F[x]$. By hypothesis, every irreducible polynomial in $F[x]$ is of degree one and so is of the form $u_0(x - u_1)$ where $u_0, u_1 \in F$ and $u_0 \neq 0$. Then $u_1 \in F$ is a root of an irreducible factor of f and so is a root of f. Therefore (i) follows and, as shown above, (ii), (iv), and (v) follow.

Theorem V.3.3, (iv)⇒

Proof (continued). To show (iv)⇒(i), we consider the contrapositive and hypothesize the negation of (i). That is, suppose there is a nonconstant polynomial $f \in F[x]$ which does not have a root in F. As argued above, $F[x]$ is a unique factorization domain and so f can be (uniquely) written as a product of irreducible polynomials. Consider one of these nonconstant irreducible factors of f, say g where the degree of g is n. Then by Kronecker's Theorem (Theorem V.1.10), there is an extension field $F(u)$ of F where u is a root of g and $[F(u) : F] = n$. By Theorem V.1.11, $F(u)$ is an algebraic extension of F. So there is an algebraic extension of F other than F itself (i.e., the negation of (iv) holds). So "not (i) ⇒ not (iv)" or, equivalently, (iv)⇒(i). As shown above, hypothesizing (iv) then implies (ii), (iii), and (v).

Theorem V.3.3, (v) ⇒

Proof (continued). Hypothesize (v). Let E be an algebraic extension of F. Since F is hypothesized to be algebraic over K, then by Theorem V.1.13, E is algebraic over K. Let $u \in E$. Then u is algebraic over K so let $k(x)$ be the (monic) irreducible polynomial of u over K. Also, u is algebraic over F so let $f(x)$ be the (monic) irreducible polynomial of u over F. Now $k(x) \in K[x] \subset F[x]$ and $k(u) = 0$, so by Theorem V.1.6(ii), f divides k. But by hypothesis, k splits in $F[x]$, so $k = (x - u_1)(x - u_2)\cdots(x - u_n)$ for some $u_i \in F$. As explained above, $F[x]$ is a unique factorization domain, so since f is a factor of k then f must be a product of some of the $(x - u_i)$'s; in fact, since f is irreducible it must equal one of the $(x - u_i)$ and since u is a root of both k and f then one of the $(x - u_i)$ is $x - u$ and $f(x) = x - u$. Therefore, $u \in F$ and so $E = F$. Therefore, (iv) follows and, as shown above, (v) also implies (i), (ii), and (iii). □

Theorem V.3.4

Theorem V.3.4. If F is an extension field of K, then the following conditions are equivalent:

(i) F is algebraic over K and F is algebraically closed;
(ii) F is a splitting field over K of the set of all (irreducible) polynomials in $K[x]$.

Proof. Hypothesize (i). Let S be the set of all irreducible polynomials in $K[x]$. Since each polynomial in S is also in $F[x]$ and F is algebraically closed, then every polynomial in S splits in $F[x]$ by Theorem V.3.3(ii) and every root of every polynomial in S is in F. Let X be the set of all roots of all polynomials in S. Then $X \subseteq F$. So $K(X) \subseteq F$. Since F is algebraic over K, then every element of F is the root of some polynomial in S and so $F \subseteq K[x]$. Therefore $K(X) = F$ and so F is (by definition) a splitting field over K of the set S of all (irreducible polynomials in $K[x]$. So (i)⇒(ii). Hypothesize (ii). Let sets S and X be as above. Then $F = K(X)$. By Theorem V.1.12, F is algebraic over K. By Theorem V.3.3(v), F is algebraically closed and (i) follows. □

Lemma V.3.5

Lemma V.3.5. If F is an algebraic extension field of K, then $|F| \le \aleph_0 |K|$.

Proof. Let T be the set of monic polynomials of positive degree in $K[x]$. For each $n \in \mathbb{N}$ let T_n be the set of all polynomial in T of degree n. Then $|T_n| = |K^n|$ where $K^n = K \times K \times \cdots \times K$ (n factors), since every polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in T$ is completely determined by its n coefficients $a_0, a_1, \ldots, a_{n-1} \in K$. For each $n \in \mathbb{N}$ let $f_n : T_n \to K^n$ be a bijection. Since the sets T_n for $n \in \mathbb{N}$ are disjoint (as are the sets K^n), the map $f : T = \cup_{n\in\mathbb{N}} T_n \to \cup_{n\in\mathbb{N}} K^n$, given by $f(u) = f_n(u)$ for $u \in T_n$ is a well-defined bijection. Therefore (by the definition of equal cardinality) $|T| = |\cup_{n\in\mathbb{N}} K^n|$. By Theorem 0.8.12(ii), $|\cup_{n\in\mathbb{N}} K^n| = \aleph_0 |K|$. That is, $|T| = \aleph_0 |K|$.

Lemma V.3.5 (continued 1)

Proof (continued). Next we show that $|F| \leq |T|$. Foe each irreducible $f \in T$, choose an ordering of the (distinct) roots of f in F (which can be done by the Well-Ordering Principle). Define a mapping from F to $T \times \mathbb{N}$ as follows. If $a \in F$, then a is algebraic over K by hypothesis, and there exists a unique irreducible monic polynomial $f \in T$ with $f(a) = 0$ by Theorem V.1.6. Assign to $a \in F$ the pair $(f, i) \in T \times \mathbb{N}$ where a is the ith root of f in the previously chosen ordering of the roots of f in F. Since every $f \in T$ is in exactly one T_n and each root a of f is associated with a unique $i \in \mathbb{N}$ (based on the ordering of the unique roots of f). So the mapping is well-defined. Now if a and b in f are mapped to the same (f, i) then a and b are both roots of f and each appears as the ith root of f in the ordering of the roots. But the unique roots of f in the ordering of the roots. But the unique roots of f were ordered, so it must be that $a = b$. So the mapping 0f F to $T \times \mathbb{N}$ is one to one (injective).

Lemma V.3.5 (continued 2)

Lemma V.3.5. If F is an algebraic extension field of K, then $|F| \leq \aleph_0 |K|$.

Proof (continued). Whence, $|F| \leq |T \times \mathbb{N}|$ (see Definition 0.8.4). By Definition 0.8.3 (and the definition of $\aleph_0$), $|T \times \mathbb{N}| = |T||\mathbb{N}| = |T|\aleph_0$. Since T is infinite, by Theorem 0.8.11 implies $|T|\aleph_0 = |T|$. By the first paragraph, $|T| = \aleph_0 |T|$. Therefore
$|F| \leq |T \times \mathbb{N}| = |T||\mathbb{N}| = |T|\aleph_0 = |T| = \aleph_0 |K|$. □

Theorem V.3.6

Theorem V.3.6. Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.

Proof. Choose a set S such that $\aleph_0 |K| < |S|$ (which can be done because $|\mathcal{P}(A)| > |A|$ for any set A; this is Theorem 0.8.5). Since $|K| \leq \aleph_0 |K|$ by Theorem 0.8.11, there is by Definition 0.8.4 an injection θ mapping $K \to S$. Since S was chosen only for its cardinality, we could redefine the image of K to be K itself (so θ maps $k \in K$ to itself) and replace $\mathrm{Im}(\theta)$ with K to get $K \subset S$.
(I) Let $\mathcal{S}$ be the class of all fields E such that E is a subset of S and E is an algebraic extension field of K. So we are using set S as a set of symbols on which extension fields of K are defined. We now argue that $\mathcal{S}$ is a set. Now a field E in $\mathcal{S}$ is completely determined by the subset E of S and the binary operations of addition and multiplication in E. Now addition and multiplication (by the definition of binary operation, see page 24) are functions φ and ψ, say, mapping $E \times E$ to E.

Theorem V.3.6(I)

Proof (continued). So we identify φ and ψ with their "graphs" (see page 4), which are subsets of $E \times E \times E \subset S \times S \times S$. Consequently, there is a one to one (injective) map τ from $\mathcal{S}$ into the set
$P = \mathcal{P}(S \times (S \times S \times S) \times (S \times S \times S))$ (which is a set by the Power Axiom, see page 3) given by the mapping $E \mapsto (E, \varphi, \psi)$ (technically, mapping to $(E, \text{graph of } \varphi, \text{graph of } \psi)$). The one to one property of τ follows from the fact that φ and ψ are binary operations and for two different fields E_1 and E_2 in $\mathcal{S}$, either the corresponding φ;s or ψ's must differ, and so the graphs of the corresponding φ's or ψ's must differ. Therefore, $\tau(E_1) \neq \tau(E_2)$. Now $\mathrm{Im}(\tau)$ is a set by the "Axiom of Class Formation," namely $\mathrm{Im}(\tau) = \{X \in P \mid X = \tau(E) \text{ for some } E \in \mathcal{S}\}$. Since $\tau : \mathcal{S} \to P$ is one to one, so τ^{-1} is a function and $\tau^{-1}(\mathrm{Im}(\tau)) = \mathcal{S}$. That is, $\mathcal{S}$ is the image of a set under a function. Hungerford states that "the axioms of set theory guarantee $\mathcal{S}$ is in fact a set."

Theorem V.3.6(II)

Theorem V.3.6. Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.

Proof (continued). (II) Note that $\mathcal{S} \neq \varnothing$ since $K \in \mathcal{S}$. Partially oder the set $\mathcal{S}$ by defining $E_1 \leq E_2$ if and only if E_2 is an extension field of E_1 (and so $E_1 \subset E_2$). Then every chain under $\leq$ has an upper bound, namely the union of all the fields in the chain. Therefore, by Zorn's Lemma there is a maximal element F of $\mathcal{S}$.

Theorem V.3.6(III)

Proof (continued). (III) We now show that F is algebraically closed. ASSUME that F is not algebraically closed. Then there is some $f \in F[x]$ which does not split over F by Theorem V.3.3(ii). By Kronecker's Theorem (Theorem V.1.10), there is a proper algebraic extension $F_0 = F(u)$ of F where u is a root of f which does not lie in F. Since F is algebraic over K (by construction) and $F(u)$ is algebraic over F (by Theorem V.1.12), then $F + 0 = F(u)$ is an algebraic extension of K by Theorem V.1.13. Notice that we cannot get a contradiction based on F_0 since we do not have $F_0 \in \mathcal{S}$. Therefore $|F_0 \setminus F| \leq |F_0|$ since $F_0 \setminus F \subset F_0$ and $|F_0| \leq \aleph_0 |K|$ by Lemma V.3.5. So, by the argument in the first paragraph $|F_0 \setminus F| \leq |F_0| \leq \aleph_0 |K| < |S|$. Since $|F| \leq |F_0| < |S|$ and $|S| = |(S \setminus F) \cup F| = |S \setminus F| + |F|$ by Definition 0.8.3. So, by Theorem 0.8.10, we have $|S| = |S \setminus F|$. Thus $|F_0 \setminus F| < |S| = |S \setminus F|$ and there is an injective (one to one) map $\zeta : F_0 \setminus F \to X \setminus F$ by Definition 0.8.4. Extend ζ to all of F_0 by defining ζ as the identity on F and the letting ζ map F_0 into S; the extended ζ is still injective.

Theorem V.3.6(III)

Theorem V.3.6. Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.

Proof (continued). Denote the image of ζ as $\mathrm{Im}(\zeta) = F_1$. Define in F_1 the sum $\zeta(a) + \zeta(b)$ as $\zeta(a+b)$ and define the product $\zeta(a)\zeta(b)$ as $\zeta(ab)$. Then F_1 is a field isomorphic to F_0 and $\zeta : F_0 \to F_1$ is an F-isomorphism. Since $F \subset F_1$, then F_1 is an extension field of F. Consequently, since F_0 is a proper algebraic extension of F (and hence of K), then so is F_1. Also, by construction, $F_1 \in \mathcal{S}$. So under the partial ordering on $\mathcal{S}$ we have $F < F_1$, but this is a CONTRADICTION to the maximality of F in $\mathcal{S}$. So the assumption that F is not algebraically closed is false, and so F is algebraically closed. Since F_0 is algebraic over K and F_1 is F-isomorphic to F_0, then F_1 is algebraic over K. Therefore (by Theorem V.3.4(i)) F is an algebraic closure of K.

The claim that any two algebraic closures of K are K-isomorphic will be shown in Corollary V.3.9 below (independently of this theorem). □

Corollary V.3.7

Corollary V.3.7. If K is a field and S a set of polynomials (of positive degree) in $K[x]$, then there exists a splitting field of S over K.

Proof. Let F be an algebraic closure of K. Let $f \in S$. As argued above in the proof of Theorem V.3.3, $F[x]$ is a unique factorization domain. So f can be (uniquely) written as a product of irreducible polynomials in $K[x]$, say $f = f-1 f_2 \cdots f_n$. By Theorem V.3.4(ii), each f_i splits in f and so f itself splits in F. Therefore, F is a splitting field of S over K. □

Theorem V.3.8

Theorem V.3.8. (For S infinite.) Let $\sigma : K \to L$ be an isomorphism of fields, $S = \{f_i\}$ a set of polynomials (of positive degree) in $K[x]$, and $S' = \{\sigma f_i\}$ the corresponding set of polynomials in $L[x]$. If F is a splitting field of S over K and M is a splitting field of S' over L, then σ is extendible to an isomorphism $F \cong M$.

Proof. Let S be an arbitrary (infinite) set. Let $\mathcal{S}$ consist of all triples (E, N, τ), where E is an intermediate field of F and K, N is an intermediate field of M and L, and $\tau : E \to N$ is an isomorphism that extends σ (i.e., $K \subset E \subset F$, $L \subset N \subset M$, and $E \cong N$ under τ). Define $(E_1, N_1, \tau_1) \le (E_2, N_2, \tau_2)$ if $E_1 \subset E_2$, $N_1 \subset N_2$, and $\tau_2|_{E_1} = \tau_1$. Then $\le$ is a partial ordering on $\mathcal{S}$ and for any chain in $\mathcal{S}$ (that is, for any subset of $\mathcal{S}$ which is totally ordered under $\le$), say $C = \{(E_i, N_i, \tau_i)\}_{i \in I}$, has a maximal element, namely $(\sup_{i\in I} E_i, \cup_{i\in I} N_i, \tau)$ where τ is defined on E_i as τ_i (and so $\tau|_{E_i} = \tau_i$). So by Zorn's Lemma, $\mathcal{S}$ has a maximal element as $(F_0, M_0, \tau_0) \in \mathcal{S}$.

Theorem V.3.8 (continued)

Proof (continued). We claim that $F_0 = F$ and $M_0 = M$, so that τ_0 is an isomorphism and $F \cong M$. τ_0 is then the desired extension of σ. ASSUME $F_0 \ne F$. Then there is some $f \in S$ which does not split over F_0 (because F_0 is an intermediate field of F and K). Since all the roots of f lie in F (by hypothesis), F contains a splitting field F_1 of f over F_0. Similarly, M contains a splitting field M_1 of $\tau_0 f = \sigma f$ over M_0. The part of the proof of thsi theorem where S is a finite set of polynomials (see the regular class notes for this section; we are using $S = \{f\}$ here) shows that τ_0 can be extended to an isomorphism τ_1 mapping $F_1 \to M_1$ and yielding $F_1 \cong M_1$. But this means that $(F_1, M_1, \tau) \in \mathcal{S}$ and (since $F_0 \subset F_1$ and $M_0 \subset M_1$) $(F_0, M_0, \tau_0) < (F_1, M_1, \tau_1)$. But this CONTRADICTS the maximality of (F_0, M_0, τ_0). So the assumption that $F_0 \ne F$ is false and we have $F_0 = F$. If we assume $M_0 \ne M$ then we get a similar contradiction (this time defining F_1 as $\tau_0^{-1}(M_1)$). Whence $(F, M, \tau_0) \in \mathcal{S}$ and τ_0 is the desired extension of σ is an isomorphism of F with M. □

Theorem V.3.12

Theorem V.3.12. (Generalized Fundamental Theorem of Galois Theory) If F is an algebraic Galois extension field of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all closed subgroups of the Galois group $\mathrm{Aut}_K F$ (given by $E \mapsto E' = \mathrm{Aut}_E F$) such that:

(ii)′ F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup E' is normal in $G = \mathrm{Aut}_K F$; in this case G/E' is (isomorphic to) the Galois group $\mathrm{Aut}_K E$ of E over K.

Proof. We will show that every intermediate field E is closed (i.e., $E = E''$) and then the one-to-one correspondence is given by Theorem V.2.7.

Since F is algebraic and Galois over K by hypothesis, then by Theorem V.3.11 (the (i)⇒(iii) part), F is the splitting field over K of a set T of separable polynomials.

Theorem V.3.12 (continued 1)

Proof. By Exercise V.3.2, F is also a splitting field of T over intermediate field E. Hence by Theorem V.3.11 (the (iii)⇒(i) part) F is Galois over E; that is, E is closed (recall that F is Galois over E if and only if E is closed—see page 247). The one-to-one correspondence now follows.

Now for (ii″). Since F is algebraic over K, then every intermediate field E is algebraic over K. So the first paragraph of the proof of Theorem V.2.5(i) (which only uses Lemma V.2.11 and Lemma V.2.13, neither of which requires finite dimensional extensions) carries over to show that E is Galois over K if and only if E' is normal in $\mathrm{Aut}_K F$.

If $E = E''$ is Galois over K so that E' is normal in $G = \mathrm{Aut}_K F$ as shown above, then $E'' = E$ is a stable intermediate field by Lemma V.2.11(ii) (with $H = E$ and $H' = E'' = E$). Therefore, Lemma V.2.14 implies that $G/E' = \mathrm{Aut}_K F/\mathrm{Aut}_E F$ is isomorphic to the subgroup of $\mathrm{Aut}_K E$ consisting of those automorphisms that are extendible to F.

Theorem V.3.12 (continued 2)

Theorem V.3.12. (Generalized Fundamental Theorem of Galois Theory) If F is an algebraic Galois extension field of K, then there is a one-to-one correspondence between the set of all intermediate fields of the extension and the set of all closed subgroups of the Galois group $\text{Aut}_K F$ (given by $E \mapsto E' = \text{Aut}_E F$) such that:

(ii)′ F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup E' is normal in $G = \text{Aut}_K F$; in this case G/E' is (isomorphic to) the Galois group $\text{Aut}_K E$ of E over K.

Proof. Since F is a splitting field over the set of polynomials T as shown above, then by Exercise V.3.2, F is also a splitting field over E. Therefore every K-automorphism in $\text{Aut}_K E$ extends to F by Theorem V.3.8 (where $L = K$, $T = S = S'$, and $M = F$ so that the extended σ is in fact an automorphism of F). So all of $\text{Aut}_K E$ is extendible to F and (by Lemma V.2.14, mentioned above), $\text{Aut}_K E \cong G/E'$. □