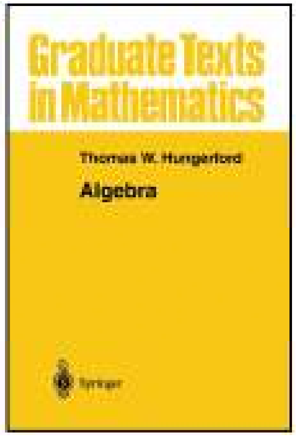
Modern Algebra

Chapter V. Fields and Galois Theory
V.7. Cyclic Extensions—Proofs of Theorems



Theorem V.7.2

Theorem V.7.2. If F is a finite dimensional Galois extension field of K and $\text{Aut}_K(F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ then for any $u \in F$,

$$N_K{}^F(u) = \sigma_1(u)\sigma_2(u)\cdots\sigma_n(u); \text{ and}$$

$$T_K{}^F(u) = \sigma_1(u) + \sigma_2(u) + \cdots + \sigma_n(u).$$

Proof. Let $\overline{K}$ be an algebraic closure of K which contains F. Since F is normal over K by Corollary V.3.15, then by Theorem V.3.14(iii) the K-monomorphisms mapping $F \to \overline{K}$ are precisely the K-automorphisms of F (that is, the elements of $\text{Aut}_K F$). Also by Corollary V.3.15 F is separable over K, so the largest subfield of F which is separable over K is $S = F$ itself and $[F, K]_i = [F, S] = [F, F] = 1$. The result now follows from the definition of norm and trace. □

Theorem V.7.3(i) and (ii)

Theorem V.7.3. Let F be a finite dimensional extension field of K. Then for all $u, v \in F$:

(i) $N_K{}^F(u)N_K{}^F(v) = N_K{}^F(uv)$ and $T_K{}^F(u) + T_K{}^F(v) = T_K{}^F(u+v)$;

(ii) if $u \in K$, then $N_K{}^F(u) = u^{[F:K]}$ and $T_K{}^F(u) = [F:K]u$;

(iii) $N_K{}^F(u)$ and $T_K{}^F(u)$ are elements of K. More precisely, $N_K{}^F = ((-1)^n a_0)^{[F:K(u)]} \in K$ and $T_K{}^F(u) = -[F:K(u)]a_{n-1} \in K$, where a_0 and a_{n-1} are determined by $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ is the irreducible polynomial of u;

(iv) if E is an intermediate field, then $N_K{}^E(N_E{}^F(u)) = N_K{}^F(u)$ and $T_K{}^E(T_E{}^F(u)) = T_K{}^F(u)$.

Theorem V.7.3(i)

Theorem V.7.3. Let F be a finite dimensional extension field of K. Then for all $u, v \in F$:

(i) $N_K{}^F(u)N_K{}^F(v) = N_K{}^F(uv)$ and $T_K{}^F(u) + T_K{}^F(v) = T_K{}^F(u+v)$.

Proof. (i) Since K, F, and $\overline{K}$ are fields and the σ_i are homomorphisms, then

$$\begin{aligned} N_K^F(u)N_K^F(v) &= (\sigma_1(u)\sigma_2(u)\cdots\sigma_r(u))^{[F:K]_i} \times (\sigma_1(v)\sigma_2(v)\cdots\sigma_r(v))^{[F:K]_i} \\ &= (\sigma_1(u)\sigma_1(v)\sigma_2(u)\sigma_2(v)\cdots\sigma_r(u)\sigma_r(v))^{[F:K]_i} \\ &= (\sigma_1(uv)\sigma_2(uv)\cdots\sigma_r(uv))^{[F:K]_i} \\ &= N_K^F(uv). \end{aligned}$$

Theorem V.7.3(i) (continued)

Theorem V.7.3. Let F be a finite dimensional extension field of K. Then for all $u, v \in F$:

(i) ${N_K}^F(u){N_K}^F(v) = {N_K}^F(uv)$ and ${T_K}^F(u) + {T_K}^F(v) = {T_K}^F(u+v)$.

Proof (continued). (i) Also

$$\begin{aligned} T_K^F(u) + T_K^F(v) &= [F:K]_i(\sigma_1(u) + \sigma_2(u) + \cdots + \sigma_r(u)) \\ &\quad +[F:K]_i(\sigma_1(v) + \sigma_2(v) + \cdots + \sigma_r(v)) \\ &= [F:K]_i(\sigma_1(u) + \sigma_1(v) + \sigma_2(u) + \sigma_2(v) + \\ &\quad \cdots + \sigma_r(u) + \sigma_r(v)) \\ &= [F:K]_i(\sigma_1(u+v) + \sigma_2(u+v) + \cdots + \sigma_r(u+v)) \\ &= T_K^F(u+v) \end{aligned}$$

So (i) holds.

Theorem V.7.3(ii)

Theorem V.7.3. Let F be a finite dimensional extension field of K. Then for all $u, v \in F$:

(ii) if $u \in K$, then ${N_K}^F(u) = u^{[F:K]}$ and ${T_K}^F(u) = [F:K]u$.

Proof. (ii) By the second Note after Definition V.7.1 in the class notes, we have that $r = [F:K]_s$. From the Remark at the top of page 286, we have that $[F:K]_s[F:K]_i = [F:K]$. Since each σ_i fixes the elements of K, then for $u \in K$ we have $N_K^F(u) = (\sigma_1(u)\sigma_2(u)\cdots\sigma_r(u))^{[F:K]_i} = (u^r)^{[F:K]_i} = u^{[F:K]_s[F:K]_i} = u^{[F:K]}$, and

$$\begin{aligned} T_K^F(u) &= [F:K]_i(\sigma_1(u) + \sigma_2(u) + \cdots + \sigma_r(u)) \\ &= [F:K]_i(u + u + \cdots + u) = [F:K]_i(ru) \\ &= [F:K]_i[F:K]_s u = [F:K]u. \end{aligned}$$

□

Lemma V.7.5

Lemma V.7.5. If S is a set of distinct automorphisms of a field F, then S is linearly independent.

Proof. ASSUME S is not linearly independent. Then there exist nonzero $a_i \in F$ and distinct $\sigma_i \in S$ such that

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0 \text{ for all } u \in F. \quad (1)$$

Among all such dependence relations, choose one with n minimal (notice $n \geq 1$ by the definition of "linearly independent," so such an n exists by the Law of Well Ordering of $\mathbb{N}$ on page 10). Since σ_1 and σ_2 are distinct, there exists $v \in F$ with $\sigma_1(v) \neq \sigma_2(v)$. Applying (1) to the element uv yields (since σ is a homomorphism):

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_2(v) + \cdots + a_n\sigma_n(u)\sigma_n(v) = 0 \quad (2)$$

and multiplying (1) by $\sigma_1(v)$ gives

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_1(v) + \cdots + a_n\sigma_n(u)\sigma_1(v) = 0. \quad (3)$$

Lemma V.7.5 (continued)

Lemma V.7.5. If S is a set of distinct automorphisms of a field F, then S is linearly independent.

Proof (continued). The difference of (2) and (3) is

$$a_2[\sigma_2(v) - \sigma_1(v)]\sigma_2(v) + a_3[\sigma_3(v) - \sigma_3(v)]\sigma_3(v) +$$

$$\cdots + a_n[\sigma_n(v) - \sigma_1(v)]\sigma_n(v) = 0$$

for all $u \in F$. Since $a_2 \neq 0$ (by the choice of relationship (1) with n minimal) and $\sigma_2(v) \neq \sigma_1(v)$ then not all coefficients are zero. But this CONTRADICTS the minimality of n. So the assumption that set S is not linearly independent is incorrect and S is linearly independent. □

Theorem V.7.6

Theorem V.7.6. Let F be a cyclic extension field of degree n, σ a generator of $\mathrm{Aut}_K(F)$ and $u \in F$. Then

(i) ${T_K}^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$;

(ii) (Hilbert's Theorem 90) ${N_K}^F(u) = 1_K$ if and only if $u = v\sigma^{-1}(v)$ for some nonzero $v \in F$.

Proof. By the definition of "cyclic extension," we have that $|\mathrm{Aut}_K F| = [F : K] = n$ and since σ is a generator of $\mathrm{Aut}_K F$, then $\mathrm{Aut}_K F = \{1_F = \sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. By Theorem V.7.2, $T_K^F(u) = T(u) = u\sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u$ and $N_K^F(u) = N(u) = u(\sigma u)(\sigma^2 u)\cdots(\sigma^{n-1}u)$.

(i) If $u = v - \sigma v$, then

$$\begin{aligned} T_K^F(u) &= T(v - \sigma v) \\ &= T(v) - T(\sigma v) \text{ since each } \sigma^j \text{ is a homomorphism of } F \\ &= v + \sigma v + \sigma^2 v + \cdots + \sigma^{n-1}v - \sigma v - \sigma^2 v - \cdots - \sigma^{n-1}v - \sigma^n v \\ &= v - \sigma^n v = v - \sigma^0 v = v - v = 0. \end{aligned}$$

Theorem V.7.6(i)

Theorem V.7.6. Let F be a cyclic extension field of degree n, σ a generator of $\mathrm{Aut}_K(F)$ and $u \in F$. Then

(i) ${T_K}^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$.

Proof (continued). (i) Conversely, suppose $T(u) = 0$. Choose $x \in F$ such that $T(w) = 1_K$ as follows. By Lemma V.7.5, the $1_K, \sigma, \sigma^2, \ldots, \sigma^n$ are linearly independent and so for soem $x \in F$ we have $T(z) = a_F z + \sigma z + \sigma^2 z + \cdots + \sigma^{n-1}z \neq 0$. Since $T(z) \in K$ by the Note after Theorem V.7.2 (in the class notes; see Hungerford page 290), we have that

$$\begin{aligned} \sigma[T(z)^{-1}z] &= \sigma(T(z)^{-1})\sigma(z) \\ &= (\sigma(T(z)))^{-1}\sigma(z) \text{ since } \sigma \text{ is a homomorphism} \\ &= T(z)^{-1}\sigma(z) \text{ since } \sigma \text{ fixes } K \text{ and } T(z)^{-1} \in K \end{aligned}$$

Theorem V.7.6(i) (continued 1)

Proof (continued). (i) Consequently, set $w = T(z)^{-1}z$ and then

$$\begin{aligned} T(w) &= T(T(z)^{-1}z) \\ &= T(z)^{-1}z + \sigma(T(z)^{-1}z) + \sigma^2(T(z)^{-1}z) + \cdots + \sigma^{n-1}(T(z)^{-1}z) \\ &= T(z)^{-1}z + \sigma(T(z)^{-1})\sigma z + \sigma^2(T(z)^{-1})\sigma^2(z) + \cdots \\ &\quad + \sigma^{n-1}(T(z)^{-1})\sigma^{n-1}z \text{ since } \sigma_j \text{ is a homomorphism} \\ &= T(z)^{-1}(z + \sigma z + \sigma^2 z + \cdots + \sigma^{n-1}z) \\ &\quad \text{since } \sigma \text{ fixes } T(z)^{-1} \in K, \text{ as argued above} \\ &= T(z)^{-1}T(z) = 1_K. \end{aligned}$$

Now let $v = uw + (u + \sigma w)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma w) + (u + \sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 w) + \cdots + (u + \sigma u + \cdots + \sigma^{n-2}u)(\sigma^{n-2}w)$.

Theorem V.7.6(i) (continued 2)

Proof (continued). (i) Since we hypothesize that $T(u) = 0$ then $T(u) = u + \sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u = 0$ and so $u = -(\sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u)$. So (since σ is a homomorphism)

$$v - \sigma v = \{uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w)$$
$$+ (u + \sigma u + \sigma^2 u + \sigma^3 u)(\sigma^3 w) + \cdots + (u + \sigma u + \sigma^2 u + \cdots + \sigma^{n-2}u)(\sigma^{n-2}w)\}$$
$$-\{(\sigma u)(\sigma w) + (\sigma u + \sigma^2 u)(\sigma^2 w) + (\sigma u + \sigma^2 + \sigma^3 u)(\sigma^3 w)$$
$$+ (\sigma u + \sigma^2 u + \sigma^3 u + \sigma^4 u)(\sigma^4 w) + \cdots + (\sigma u + \sigma^2 u + \sigma^3 u + \cdots + \sigma^{n-1}u)(\sigma^{n-1}w)\}$$
$$= uw + u\sigma w + u\sigma^2 w + u\sigma^3 w + \cdots + u\sigma^{n-2}w$$
$$-(\sigma u + \sigma^2 u + \sigma^3 u + \cdots + \sigma^{n-1}u)(\sigma^{n-1}w)$$
$$= uw + u\sigma w + u\sigma^2 w + \cdots + u\sigma^{n-2}w + u\sigma^{n-1}w$$
$$\text{since } u = -(\sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u) \text{ by above}$$
$$= uT(w) = u1_K = u.$$

So $u = v - \sigma(v)$ for the value of v given above, and (i) follows.

Theorem V.7.6(ii)

Theorem V.7.6. Let F be a cyclic extension field of degree n, σ a generator of $\text{Aut}_K(F)$ and $u \in F$. Then

(ii) (Hilbert's Theorem 90) $N_K{}^F(u) = 1_K$ if and only if $u = v\sigma^{-1}(v)$ for some nonzero $v \in F$.

Proof. (ii) Suppose $u = v\sigma(v)^{-1}$ for some nonzero $v \in F$. Since σ is an automorphism of order n, then $\sigma^n(v^{-1}) = v^{-1}$, $\sigma(v^{-1}) = \sigma(v)^{-1}$, and for each $1 \le i \le n-1$ we have $\sigma^i(v\sigma(v)^{-1}) = \sigma^i(v)\sigma^i(\sigma(v)^{-1}) = \sigma^i(v)(\sigma^i(\sigma(v)))^{-1} = \sigma^i(v)\sigma^{i+1}(v)^{-1}$. Hence

$$\begin{aligned} N_K^F(u) &= N(U) = u(\sigma u)(\sigma^2 u)(\sigma^3 u)\cdots(\sigma^{n-1}u) \\ &= (v\sigma(v)^{-1})(\sigma(v\sigma(v)^{-1}))(\sigma^2(v\sigma(v)^{-1})\cdots(\sigma^{n-1}(v\sigma(v)^{-1})) \\ &= (v\sigma(v)^{-1})(\sigma v\sigma^2(v)^{-1})(\sigma^2 v\sigma^3(v)^{-1})\cdots(\sigma^{n-1}v\sigma^n(v)^{-1}) \\ &\quad \text{since } \sigma^i(v\sigma(v)^{-1}) = \sigma^i(v)\sigma^{i+1}(v)^{-1} \text{ by above} \\ &= v(\sigma(v)^{-1}\sigma v)(\sigma^2(v)^{-1}\sigma^2 v)\cdots(\sigma^{n-1}(v)^{-1}\sigma^{n-1}v)(\sigma^n(v)^{-1}) \\ &= v(\sigma^n(v))^{-1} = vv^{-1} \text{ (since } \sigma^n(v) = \sigma^0(v) = v) = 1_K. \end{aligned}$$

Theorem V.7.6(ii) (continued)

Proof (continued). (ii) Conversely, suppose $N_K^F(u) = N(u) = 1_K$ (and so $u \neq 0$; $N(0) = 0$ since $\sigma(0) = 0$ because σ is a homomorphism). By Lemma V.7.5, $\{1_K, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ are linearly independent and so there is $y \in F$ such that this linear combination of $\sigma^i(y)$'s is nonzero: $v \equiv (u)1_F y + (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + \cdots + (u\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-2}u)\sigma^{n-2}y + (u\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-1}u)\sigma^{n-1}y$. Since we have hypothesized that $N(u) = u\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-1}u = 1_K$, then $v = uy + (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + \cdots + (u\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-2}u)\sigma^{n-2}y + \sigma^{n-1}y$. So $\sigma v = (\sigma u)\sigma y + (\sigma u\sigma^2 u)\sigma^2 y + (\sigma u\sigma^2 u\sigma^3 u)\sigma^3 y + \cdots + (\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-1}u)\sigma^{n-1}y + \sigma^n y$ and $u\sigma v = (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + (u\sigma u\sigma^2 u\sigma^3 u)\sigma^3 y + \cdots + (u\sigma u\sigma^2 u\sigma^3 u\cdots\sigma^{n-1}u)\sigma^{n-1}y + uy$ (since $\sigma^n = \sigma^0 = 1_K$) $= v$. So $u\sigma v = v$ and $u = v\sigma(v)^{-1}$ where v is as defined above (notice that we hypothesizes $v \neq 0$, so $\sigma(v) \neq 0$ since σ is an automorphism and hence is one to one). □

Theorem V.7.7

Proposition V.7.7. Let F be a cyclic extension field of K of degree n and suppose $n = mp^t$ where $0 \neq p = \text{char}(K)$ and $(m,p) = 1$. Then there is a chain of intermediate fields $F \supset E_0 \supset E_1 \supset \cdots \supset E_{t-1} \supset E_t = K$ such that F is a cyclic extension of E_0 of degree m and for each $0 \le i \le t$, E_{i-1} is a cyclic extension of E_i of degree p.

Proof. Since F is a cyclic extension field of K then (by definition) F is Galois over K and $\text{Aut}_K F$ is cyclic (and so abelian). So every subgroup of $\text{Aut}_K F$ is normal. Every subgroup of a cyclic group is cyclic and every homomorphic image of a cyclic group is cyclic by Theorem I.3.5. By Theorem I.5.5, the canonical epimorphism mapping $G \to G/N$ (where $N \triangleleft G$) is a homomorphism from G to G/N, so that q quotient group of cyclic groups is cyclic (and so abelian). Consequently, by the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)) for any intermediate field E (i.e., $K \subset E \subset F$), since the subgroups $\text{Aut}_E F$ and $\text{Aut}_K E$ of $\text{Aut}_K F$ are cyclic (and so abelian and hence normal subgroups of $\text{Aut}_K F$), then F is Galois over E and E is Galois over K.

Theorem V.7.7 (continued 1)

Proof (continued). So F is cyclic over E and E is cyclic over K. Similarly, for any pair L, M of intermediate fields with $L \subset M$, we have that M is a cyclic extension of L; in particular, M is algebraic and Galois over L. By Exercise I.3.6, there is a unique subgroup H of $\text{Aut}_K F$ of order m (and H is cyclic since $\text{Aut}_K F$ is cyclic). Let $E_0 = H'$ be the fixed field of H. Since E_0 is Galois over F then $E_0' = \text{Aut}_{E_o} F$ and $E_0' = H'' = H$. Then F is cyclic over E_0 of degree m and E_0 is cyclic over K of degree p^t (here, $K \subset E_0 \subset F$). Since $\text{Aut}_K E_0$ is cyclic of order p^t it has a chain of subgroups $\{1\} = G_0 < G_1 < G_2 < \cdots < G_{t-1} = \text{Aut}_K E_0$ with $|G_i| = p^i$, $[G_i L G_{i-1} = p$, and G_i/G_{i-1} cyclic of order p (Theorem I.3.4(vii) justifies the existence of these subgroups of cyclic group $\text{Aut}_K E_0$). For each i, let E_i be the fixed field of G_i ("relative to E_0 an d$\text{Aut}_K E_0$"; that is, in the setting where E_0 is treated as the finite dimensional extension of K).

Theorem V.7.7 (continued 2)

Proposition V.7.7. Let F be a cyclic extension field of K of degree n and suppose $n = mp^t$ where $0 \neq p = \text{char}(K)$ and $(m, p) = 1$. Then there is a chain of intermediate fields $F \supset E_0 \supset E_1 \supset \cdots \supset E_{t-1} \supset E_t = K$ such that F is a cyclic extension of E_0 of degree m and for each $0 \leq i \leq t$, E_{i-1} is a cyclic extension of E_i of degree p.

Proof. The Fundamental Theorem of Galois Theory (Theorem V.2.5) implies:

(i) $E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_{t-1} \supset E_t = K$ (by the "one to one correspondence" claim in Theorem V.2.5),

(ii) $[E_{i-1} : E_i] = [G_i : G_{i-1}] = p$ (by part (i) f Theorem V.2.5), and

(iii) $\text{Aut}_{E_i} E_{i-1} \cong G_i / G_{i-1}$ (by part (ii) of Theorem V.2.5; since all Galois groups are cyclic, they are abelian and so normal subgroups of larger Galois groups).

Therefore, E_{i-1} is a cyclic extension of E_i of degree $[E_{i-1} : E_i] = p$. □

Theorem V.7.8

Proposition V.7.8. Let K be a field of characteristic $p \neq 0$. F is a cyclic extension field of K of degree p if and only if F is a splitting field over K of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case $F = K(u)$ where u is any root of $x^p - x - a$.

Proof. (1) Suppose F is a cyclic extension field of K of degree p. If σ is a generator of the cyclic group $\text{Aut}_K F$ then by Theorem V.7.3(ii), $F_K^F(1_K) = [F : K]1_K = p1_K = 0$ since K is of characteristic p. Whence, by Theorem V.7.6(i), $1_K = v - \sigma(v)$ for some $v \in F$. With $u = -v$ we have $\sigma(u) = \sigma(-v) = -\sigma(v) = 1_K - v = 1_K + u \neq u$, whence $u \notin K$ (because $\sigma \in \text{Aut}_K F$ and so σ fixes the elements of K). Since $[F : K] = p$ prime, there are no intermediate fields (by Theorem V.1.2) and we must have $F = K(u)$ (that is, we know $K \subset K(u) \subset F$ by $K \neq K(u)$ and $K(u)$ cannot be a "proper" intermediate field, so $F = K(u)$).

Theorem V.7.8 (continued 1)

Proof (continued). Since $\sigma(u) = u + 1_K$ and σ is a homomorphism then $\sigma(u^p) = \sigma(u)^p = (u + 1_K)^p$ and since K is of characteristic p then $p1_K = 0$ and so by the Binomial Theorem (Theorem III.1.6), $(u + 1_K)^p = u^p + 1_K^p = u^p + 1_K$ (we do not necessarily know that $F = K(u)$ is of characteristic p and so we cannot use the Freshman's Cream [Exercise III.1.11] here). These combine to give $\sigma(u^p - u) = \sigma(u^p) - \sigma(u) = (u^p + 1_K) - (u + 1_K) = u^p - u$; that is, $u^p - u$ is fixed by σ. Since F is a cyclic extension of K then (by the definition of "cyclic extension") F is Galois over K and so (by the definition of "Galois extension") the fixed field of $\text{Aut}_K F$ is precisely K, so $a = u^p - u \in K$. Therefore, u is a root of $x^p - x - a \in K[x]$. Since the degree of u over K is (Definition V.1.7) $[K(u) : K] = [F : K] = p$, then $x^p - x - a$ must be the irreducible polynomial of u over K (see Theorem V.1.6).

Theorem V.7.8 (continued 2)

Proof (continued). As shown in the proof of Theorem V.5.1, the prime subfield $\mathbb{Z}_p$ of K consists of the p distinct elements $\mathbb{Z}_p = \{0, 1_K, 2 \cdot 1_K, 3 \cdot 1_K, \ldots, (p-1) \cdot 1_K\}$. Treating $\mathbb{Z}_p$ as a multiplicative group of order $p - 1$ (see Exercise I.1.7) we have that for all $i \in \mathbb{Z}_p$, $i^{p-1} = 1_K$ or $i^p = i$ (this is also argued in the first paragraph of the proof of Theorem V.5.6). Since u is a root of $x^p - x - a$ we have for each $i \in \mathbb{Z}_p$ that

$$\begin{aligned}(u+i)^p - (u+i) - 1 &= u^p + i^p - u - 1 - a \text{ (as argued above, based on} \\ &= (u^p - u - a)(i - i) = 0.\end{aligned}$$

Thus $u + i \in K(u) = F$ is a root of $x^p - x - a$ for each $i \in \mathbb{Z}_p$, whence F contains p distinct roots of $x^p - x - a$. Therefore $F = K(u)$ is a splitting field over K of $x^p - x - a$. Finally, if $u + i$ is any root of $x^p - x - a$, then "clearly" $K(u + i) = K(u) = F$ (since the other roots $(u_i) + j$ for $j \in \mathbb{Z}_p$ are still in $K(u + i)$).

Theorem V.7.8 (continued 3)

Proposition V.7.8. Let K be a field of characteristic $p \neq 0$. F is a cyclic extension field of K of degree p if and only if F is a splitting field over K of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case $F = K(u)$ where u is any root of $x^p - x - a$.

Proof (continued). (2) Suppose F is a splitting field over K of $x^p - x - a \in K[x]$. "We shall not assume that $x^p - x - a$ is irreducible and shall prove somewhat more than is stated in the theorem." If u is a root of $x^p - x - a$, then as shown above (based on the Binomial Theorem, not based on the specific value of a used above) $K(u)$ contains p distinct roots of $x^p - x - a$, namely $u, t + 1_k, u + 2 \cdot 1_K, \ldots, u + (p-1) \cdot 1_K \in K(u)$. But $x^p - x - a$ has at most p roots in F and these roots generate F over K (since we have hypothesized that F is a splitting field over K of $x^p - x - a$). Therefore $F = K(u)$ and the irreducible factors of $x^p - x - a$ are separable (since $x^p - x - a$ has p distinct roots).

Theorem V.7.8 (continued 4)

Proof (continued). By Exercise V.3.13 (the (iii)⇒(ii) part), F is separable and a spitting field of a polynomial in $K[x]$, and by Theorem V.3.11 (the (ii)⇒(i) part) F is algebraic and Galois over K. Every $\tau \in \mathrm{Aut}_K F = \mathrm{Aut}_K K(u)$ is completely determined by $\tau(u)$. Theorem V.2.2 implies that τ maps roots of $x^p - x - a$ to roots of $x^p - x - a$, so $\tau(u) = u + i$ for some $i \in \mathbb{Z}_p$. For such $\tau \in \mathrm{Aut}_K F$ and $i \in \mathbb{Z}_p$ define $\theta : \mathrm{Aut}_K F \to \mathbb{Z}_p$ as $\theta(\tau) = i$. Then for $\tau_1, \tau_2 \in \mathrm{Aut}_K F$ where $\tau_1(u) = u + i_1$ and $\tau_2(u) = u + i_2$ we have $\theta(\tau_1 \circ \tau_2)(u) = \tau_1(\tau_2(u)) = \tau_1(u + i_2) = u + (i_1 + i_2)$. So θ is a homomorphism. Also, if $\tau_1 \neq \tau_2$ then $\tau_1(u) \neq \tau_2(u)$ (since the τ's are determined by their values on u) or $i_1 \neq i_2$, and $\theta(\tau_1) = i_1 \neq i_2 = \theta(\tau_2)$. So τ is one to one. That is, τ is a monomorphism. So $\mathrm{Aut}_K F \cong \mathrm{Im}(\theta)$ and $\mathrm{Im}(\theta)$ is a subgroup of $\mathbb{Z}_p$ so (by Lagrange's Theorem) $\mathrm{Im}(\theta)$ is either $\{1\}$ or $\mathbb{Z}_p$.

Theorem V.7.8 (continued 5)

Proposition V.7.8. Let K be a field of characteristic $p \neq 0$. F is a cyclic extension field of K of degree p if and only if F is a splitting field over K of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case $F = K(u)$ where u is any root of $x^p - x - a$.

Proof (continued). If $\mathrm{Aut}_K F = \{1\}$ then $[F : K] = 1$ by Theorem V.2.5(i) (Fundamental Theorem of Galois Theory), whence $u \in K$ and $x^p - x - a$ splits in $K[x]$. However, we have hypothesized that $x^p - x - a$ is irreducible cover K, so we must have $\mathrm{aut}_K F \cong \mathbb{Z}_p$. In this case, F is cyclic over K of degree p. □

Corollary V.7.9

Corollary V.7.9. If K is a field of characteristic $p \neq 0$ and $x^p - x - a \in K[x]$, then $x^p - x - a$ is either irreducible of splits in $K[x]$.

Proof. We use the notation from the proof of Proposition V.7.8. In view of the last paragraph of that proof (where Hungerford says that he "shall prove somewhat more than is stated in the theorem") it suffices to prove that if $\mathrm{Aut}_K F = \mathrm{Im}(0) = \mathbb{Z}_p$, then $x^p - x - a$ is irreducible. By Theorem V.3.6, $x^p - x - a$ has p roots in the algebraic closure of K. If $\mathrm{Im}(\theta) = \mathbb{Z}_p$ (and so $\mathrm{Im}(\theta) \neq \{1\}$) then there are roots u an dv of $x^p - x - a$ in $\overline{K}$. As argued above, $v = u + i$ for some $i \in \mathbb{Z}_p$, so there is $\tau \in \mathrm{Aut}_K F$ such that $\tau(u) = v$ and so $\tau : K(u) \to K(v)$ is an isomorphism (choose τ with $\theta(\tau) = i$). By Corollary V.1.9, u and v are roots of the same irreducible polynomial in $K[x]$. Since u and v were *any* roots of $x^p - x - a$, then $x^p - x - a$ is the irreducible polynomial in $K[x]$ of which u an dv are roots. □

Lemma V.7.10

Lemma V.7.10. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ.

(i) If $d \mid n$, then $\zeta^{n/d} = \eta$ is a primitive dth root of unity in K.

(ii) If $d \mid n$ and u is a nonzero root of $x^d - a \in K[x]$, then $x^d - a$ had d distinct roots, namely $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$, where $\eta \in K$ is a primitive dth root of unity. Furthermore $K(u)$ is a splitting field of $x^d - a$ over K and is Galois over K.

Proof. (i) Since ζ is a primitive nth root of unity, it generates a multiplicative cyclic group of order n. By Theorem 1.3.4(iv), if $d \mid n$ then $\eta = \zeta^{n/d}$ has order d, whence η is a primitive dth root of unity in K.

(ii) Let u be a root of $x^d - 1$. Then $\eta^i u = \zeta^{ni/d} u$ satisfies $(\eta^i u)^d = \zeta^{ni} u^d = 1_K u^d = a$ and so $\eta^i u$ is also a root of $x^d - a$. Since η is a primitive dth root of unity by (i), then $\eta^0 = 1_K, \eta, \eta^2, \ldots, \eta^{d-1}$ are distinct (the text quotes Theorem I.3.4(vi) here).

Lemma V.7.10 (continued)

Lemma V.7.10. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ.

(ii) If $d \mid n$ and u is a nonzero root of $x^d - a \in K[x]$, then $x^d - a$ had d distinct roots, namely $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$, where $\eta \in K$ is a primitive dth root of unity. Furthermore $K(u)$ is a splitting field of $x^d - a$ over K and is Galois over K.

Proof (continued). (ii) Consequently, since $\eta \in K$, the roots $u, \eta u, \eta^2 u, \ldots, \eta^{d-1} u$ of $x^d - a$ are distinct elements of $K(u)$. Thus $K(u)$ is a splitting field of $x^d - a$ over K. The irreducible factors of $x^d - a$ are separable since all the roots are distinct. By Exercise V.3.13 (the (iii)⇒(ii) part), $K(u)$ is separable and a splitting field of a polynomial in $K[x]$. By Theorem V.3.11 (the (ii)⇒(i) part), $K(u)$ is algebraic and Galois over K. □

Theorem V.7.11

Theorem V.7.11. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ. Then the following conditions on an extension field F of K are equivalent.

(i) F is cyclic of degree d, where $d \mid n$;

(ii) F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$ (in which case $F = K(u)$, for any root u of $x^n - a$);

(iii) F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$, where $d \mid n$ (in which case $F = K(v)$, for any root v of $x^d - b$).

Proof. (ii)⇒(i) Suppose F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$. By Lemma V.7.10(ii), $F = K(u)$ and F is Galois over K for any root of $x^n - a$. If $\sigma \in \mathrm{Aut}_K F = \mathrm{Aut}_K K(u)$ then σ is completely determined by $\sigma(u)$, which is a root of $x^n - a$ by Theorem V.2.2.

Theorem V.7.11 (continued 1)

Proof (continued). (ii)⇒(i) Therefore, $\sigma(u) = \zeta^i u$ for some i (where $0 \le i \le n-1$) by Lemma V.7.10(ii) where ζ is the given primitive root of unity. Define $\theta : \mathrm{Aut}_K F \to \{n\text{th roots of unity}\}$ as $\theta(\sigma) = \zeta^i$ where $\sigma(u) = \zeta^i u$. Then for $\sigma_1, \sigma_2 \in \mathrm{Aut}_K F$ where $\sigma_1(u) = \zeta^{i_1} u$ and $\sigma_2(u) = \zeta^{i_2} u$ we have (since $\sigma_1(\sigma_2(u)) = \zeta^{i_1}(\zeta^{i_2} u)$) that $\theta(\sigma_1 \circ \sigma_2) = \zeta^{i_1 + i_2} = \zeta^{i-1}\zeta^{i_2} = \theta(\sigma_1)\theta(\sigma_2)$, so θ is a homomorphism. If $\sigma_1 \ne \sigma_2$ then $\sigma_1(u) \ne \sigma_2(u)$ (since elements of $\mathrm{Aut}_K F = \mathrm{Aut}_K K(u)$ are determined by their values on u) and so $\sigma_1(u) = \zeta^{i_1} u \ne \zeta^{i_2} u = \sigma_2(u)$ where $0 \le i_1 \le n-1$, $0 \le i_2 \le n-2$. $i_1 \ne i_2$ and $\theta(\sigma_1) = i_1 \ne i_2 = \theta(\sigma_2)$. So θ is one to one and so is a monomorphism. So $\mathrm{Aut}_K F$ is isomorphic to a subgroup of $\mathbb{Z}_n$ (since the multiplicative nth roots of unity form a group isomorphic to the cyclic group $\mathbb{Z}_n$) then $\mathrm{Aut}_K F$ is cyclic of some order d where $d \mid n$ (Hungerford quotes Theorem I.3.5 and Corollary I.4.6 here). Hence F is cyclic of degree d over K and (i) follows.

Theorem V.7.11 (continued 2)

Theorem V.7.11. Let $n \in \mathbb{N}$ and K a field which contains a primitive nth root of unity ζ. Then the following conditions on an extension field F of K are equivalent.

(i) F is cyclic of degree d, where $d \mid n$;

(ii) F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$ (in which case $F = K(u)$, for any root u of $x^n - a$).

Proof. (i)⇒(ii) Suppose F is cyclic of degree d over K where $d \mid n$. Then $d = [F : K]$. Say a generator of $\mathrm{Aut}_K F$ is σ. Let $\eta = \zeta^{n/d} \in K$ be a primitive dth root of unity. By Theorem V.7.3(ii), $N_K^F(\eta) = \eta^{[F:K]} = \eta^d = 1_K$, so by Theorem V.7.6 (Hilbert's Theorem 90) we have $\eta = w\sigma(w)^{-1}$ for some $w \in F$. With $v = w^{-1}$ we have $\sigma(v) = \eta w^{-1} = \eta v$ and $\sigma(v^d) = \sigma(v)^d = (\eta v)^d = \eta^d v^d = v^d$. Since F is Galois over K (by hypothesis) and v^d is fixed by σ, then $v^d = b$ must lie in K so that v is a root of $x^d - b \in K[x]$.

Theorem V.7.11 (continued 3)

Proof (continued). (i)⇒(ii) By Lemma V.7.10(ii), $K(v) \subset F$ and $K(v)$ is a splitting field over K of $x^d - b$ (whose distinct roots are $v, \eta v, \eta^2 v, \ldots, \eta^{d-1} v$). Furthermore for each i, where $0 \le i \le d-1$, $\sigma^i(v) = \eta^i v$ since $\sigma(v) = \eta v$ so that σ^i is an isomorphism between $K(v)$ and $K(\eta^i v)$. By Corollary I.1.9 (since σ^i fixes K) v and $\eta^i v$ are roots of the same irreducible polynomial over K. Since this holds for all i where $0 \le i \le d-1$, the irreducible polynomial of which these all are a root must be $x^d - b$ and so $x^d - b$ is irreducible in $K[x]$. By Theorem V.1.6 (parts (ii) and (iii)), $[F(v) : K] = d$. We now have that $d = [K(v) : K] = [F : K]$ where $K(v) \subseteq F$, so $[K(v) : F] = 1$ by Theorem V.1.2 and hence $K(v) = F$. So F is a splitting field of $x^d - b$ over K and (iii) follows.

Theorem V.7.11 (continued 4)

Proof. (iii)⇒(ii) Suppose F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$ where $d \mid n$. If $v \in F$ is a root of $x^d - b \in K[x]$ then $F = K(v)$ by Lemma V.7.10(ii). Now $(\zeta v)^n = \zeta^n v^n = 1_K v^{d(n/d)} = b^{n/d} \in K$ where ζ is the primitive nth root of unity hypothesized to be in K. So ζv is a root of $x^n - a \in K[x]$ where $z = b^{n/d}$. By Lemma V.7.10(ii), $K(\zeta v)$ is a splitting field of $x^n - a$ over K. But since $\zeta \in K$ then $K(\zeta v) = K(v) = F$ and so F is a splitting field of $x^n - a$ and (ii) follows. □