Modern Algebra

Chapter V. Fields and Galois Theory

V.8. Cyclotomic Extensions—Proofs of Theorems

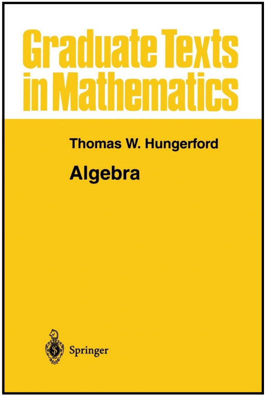

Table of contents

Theorem V.8.1

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that $\text{char}(K)$ does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

(iii) $\text{Aut}_K(F)$ is isomorphic to a subgroup of order d of the multiplicative group of units of $\mathbb{Z}_n$.

Proof. (i) Since $\text{char}(K) \nmid n$ then $nx^{n-1} \neq 0$ (i.e., is not the 0 polynomial in $K[x]$). With $f(x) = x^n - 1_K$ we have the formal derivative $f'(x) = nx^{n-1}$.

Theorem V.8.1

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

(iii) $\text{Aut}_K(F)$ is isomorphic to a subgroup of order d of the multiplicative group of units of $\mathbb{Z}_n$.

Proof. (i) Since char$(K) \nmid n$ then $nx^{n-1} \neq 0$ (i.e., is not the 0 polynomial in $K[x]$). With $f(x) = x^n - 1_K$ we have the formal derivative $f'(x) = nx^{n-1}$. So if $f(c) = 0$ then $f'(x)(c) \neq 0$ (because $f'(x) = 0$ only for $x = 0$). So by Theorem III.6.10(i), $x^n - 1_K$ has only roots of multiplicity one and so $x^n - 1_K$ has n distinct roots in any splitting field of $x^n - 1_K$.

Theorem V.8.1

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

(iii) $\text{Aut}_K(F)$ is isomorphic to a subgroup of order d of the multiplicative group of units of $\mathbb{Z}_n$.

Proof. (i) Since char$(K) \nmid n$ then $nx^{n-1} \neq 0$ (i.e., is not the 0 polynomial in $K[x]$). With $f(x) = x^n - 1_K$ we have the formal derivative $f'(x) = nx^{n-1}$. So if $f(c) = 0$ then $f'(x)(c) \neq 0$ (because $f'(x) = 0$ only for $x = 0$). So by Theorem III.6.10(i), $x^n - 1_K$ has only roots of multiplicity one and so $x^n - 1_K$ has n distinct roots in any splitting field of $x^n - 1_K$.

Theorem V.8.1 (continued 1)

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

Proof (continued). (i) Thus the cyclic group of nth roots of unity in F has order n (and so is isomorphic to $\mathbb{Z}_n$) and contains a generator of this cyclic group, which is (by definition) a primitive nth root of unity, say $\zeta \in F$. So the nth roots of unity are $1_K, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ and these are all in $K(\zeta)$. Therefore $F = K(\zeta)$.

Theorem V.8.1 (continued 1)

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that $\text{char}(K)$ does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

Proof (continued). (i) Thus the cyclic group of nth roots of unity in F has order n (and so is isomorphic to $\mathbb{Z}_n$) and contains a generator of this cyclic group, which is (by definition) a primitive nth root of unity, say $\zeta \in F$. So the nth roots of unity are $1_K, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ and these are all in $K(\zeta)$. Therefore $F = K(\zeta)$.

(ii) and (iii) Since $x^n - 1_K$ has n distinct roots in F, then the irreducible factors of $x^n - 1_K$ are separable. By Exercise V.3.13 (the (iii)⇒(ii) part), $F = K(\zeta)$ is separable and a splitting field of a polynomial in $K[x]$. By Theorem V.3.11 (the (ii)⇒(i) part), $F = K(\zeta)$ is algebraic and Galois over K.

Theorem V.8.1 (continued 1)

Theorem V.8.1. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let F be a cyclotomic extension of K of order n. Then the following hold.

(i) $F = K(\zeta)$ where $\zeta \in F$ is a primitive nth root of unity.

(ii) F is an abelian extension of dimension d where $d \mid \phi(n)$; if n is prime then F is actually a cyclic extension.

Proof (continued). (i) Thus the cyclic group of nth roots of unity in F has order n (and so is isomorphic to $\mathbb{Z}_n$) and contains a generator of this cyclic group, which is (by definition) a primitive nth root of unity, say $\zeta \in F$. So the nth roots of unity are $1_K, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ and these are all in $K(\zeta)$. Therefore $F = K(\zeta)$.

(ii) and (iii) Since $x^n - 1_K$ has n distinct roots in F, then the irreducible factors of $x^n - 1_K$ are separable. By Exercise V.3.13 (the (iii)$\Rightarrow$(ii) part), $F = K(\zeta)$ is separable and a splitting field of a polynomial in $K[x]$. By Theorem V.3.11 (the (ii)$\Rightarrow$(i) part), $F = K(\zeta)$ is algebraic and Galois over K.

Theorem V.8.1 (continued 2)

Proof (continued). (ii) and (iii) If $\sigma \in \mathrm{Aut}_K F$, then since $F = K(\zeta)$, σ is completely determined by $\sigma(\zeta)$. By Theorem V.2.2, $\sigma(\zeta)$ is also a root of $x^n - 1_K$, so for some i with $1 \leq i \leq n-1$ we have $\sigma(\zeta) = \zeta^i$. Similarly, since $\sigma^{-1} \in \mathrm{Aut}_K F$, then $\sigma^{-1}(\zeta)\zeta^j$ for some j with $1 \leq j \leq n-1$. So $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$.

Theorem V.8.1 (continued 2)

Proof (continued). (ii) and (iii) If $\sigma \in \mathrm{Aut}_K F$, then since $F = K(\zeta)$, σ is completely determined by $\sigma(\zeta)$. By Theorem V.2.2, $\sigma(\zeta)$ is also a root of $x^n - 1_K$, so for some i with $1 \le i \le n-1$ we have $\sigma(\zeta) = \zeta^i$. Similarly, since $\sigma^{-1} \in \mathrm{Aut}_K F$, then $\sigma^{-1}(\zeta)\zeta^j$ for some j with $1 \le j \le n-1$. So $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$. By Theorem I.3.4(v), we have $ij \equiv 1 \pmod{n}$ and hence $\bar{i} \in \mathbb{Z}_n$ as $\theta(\sigma) = \bar{i}$ where $\sigma(\zeta) = \zeta^i$. For $\sigma_1, \sigma_2 \in \mathrm{Aut}_F K$ with $\sigma_1(\zeta) = \zeta^{i_1}$ and $\sigma_2(\zeta) = \zeta^{i_2}$ we have

$$\begin{aligned}\theta(\sigma_1 \circ \sigma_2) &= \overline{i_1 i_2} \text{ since } (\sigma_1 \circ \sigma_2)(\zeta) = \zeta^{i_1 i_2} \\ &= \overline{i_1}\,\overline{i_2} = \theta(\sigma_1)\theta(\sigma_2)\end{aligned}$$

and so θ is a group homomorphism.

Theorem V.8.1 (continued 2)

Proof (continued). (ii) and (iii) If $\sigma \in \mathrm{Aut}_K F$, then since $F = K(\zeta)$, σ is completely determined by $\sigma(\zeta)$. By Theorem V.2.2, $\sigma(\zeta)$ is also a root of $x^n - 1_K$, so for some i with $1 \leq i \leq n-1$ we have $\sigma(\zeta) = \zeta^i$. Similarly, since $\sigma^{-1} \in \mathrm{Aut}_K F$, then $\sigma^{-1}(\zeta)\zeta^j$ for some j with $1 \leq j \leq n-1$. So $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$. By Theorem I.3.4(v), we have $ij \equiv 1 \pmod{n}$ and hence $\bar{i} \in \mathbb{Z}_n$ as $\theta(\sigma) = \bar{i}$ where $\sigma(\zeta) = \zeta^i$. For $\sigma_1, \sigma_2 \in \mathrm{Aut}_F K$ with $\sigma_1(\zeta) = \zeta^{i_1}$ and $\sigma_2(\zeta) = \zeta^{i_2}$ we have

$$\begin{aligned} \theta(\sigma_1 \circ \sigma_2) &= \overline{i_1 i_2} \text{ since } (\sigma_1 \circ \sigma_2)(\zeta) = \zeta^{i_1 i_2} \\ &= \overline{i_1}\,\overline{i_2} = \theta(\sigma_1)\theta(\sigma_2) \end{aligned}$$

and so θ is a group homomorphism. Also, if $\sigma_1 \neq \sigma_2$ (and so $i_1 \neq i_2$ since the σ's are determined based on their values on ζ) then $\theta(\sigma_1) = \overline{i_1} \neq \overline{i_2} = \theta(\sigma_2)$ and θ is one to one. That is, θ is a group monomorphism.

Theorem V.8.1 (continued 2)

Proof (continued). (ii) and (iii) If $\sigma \in \text{Aut}_K F$, then since $F = K(\zeta)$, σ is completely determined by $\sigma(\zeta)$. By Theorem V.2.2, $\sigma(\zeta)$ is also a root of $x^n - 1_K$, so for some i with $1 \le i \le n-1$ we have $\sigma(\zeta) = \zeta^i$. Similarly, since $\sigma^{-1} \in \text{Aut}_K F$, then $\sigma^{-1}(\zeta)\zeta^j$ for some j with $1 \le j \le n-1$. So $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$. By Theorem I.3.4(v), we have $ij \equiv 1 \pmod{n}$ and hence $\bar{i} \in \mathbb{Z}_n$ as $\theta(\sigma) = \bar{i}$ where $\sigma(\zeta) = \zeta^i$. For $\sigma_1, \sigma_2 \in \text{Aut}_F K$ with $\sigma_1(\zeta) = \zeta^{i_1}$ and $\sigma_2(\zeta) = \zeta^{i_2}$ we have

$$\begin{aligned} \theta(\sigma_1 \circ \sigma_2) &= \overline{i_1 i_2} \text{ since } (\sigma_1 \circ \sigma_2)(\zeta) = \zeta^{i_1 i_2} \\ &= \overline{i_1}\,\overline{i_2} = \theta(\sigma_1)\theta(\sigma_2) \end{aligned}$$

and so θ is a group homomorphism. Also, if $\sigma_1 \ne \sigma_2$ (and so $i_1 \ne i_2$ since the σ's are determined based on their values on ζ) then $\theta(\sigma_1) = \overline{i_1} \ne \overline{i_2} = \theta(\sigma_2)$ and θ is one to one. That is, θ is a group monomorphism. As commented above, if $\sigma(\zeta) = \zeta^i$ then $\bar{i}$ is a unit in $\mathbb{Z}_n$, so $\text{Im}(\theta)$ is a subgroup of the group of units in $\mathbb{Z}_n$.

Theorem V.8.1 (continued 2)

Proof (continued). (ii) and (iii) If $\sigma \in \mathrm{Aut}_K F$, then since $F = K(\zeta)$, σ is completely determined by $\sigma(\zeta)$. By Theorem V.2.2, $\sigma(\zeta)$ is also a root of $x^n - 1_K$, so for some i with $1 \le i \le n-1$ we have $\sigma(\zeta) = \zeta^i$. Similarly, since $\sigma^{-1} \in \mathrm{Aut}_K F$, then $\sigma^{-1}(\zeta)\zeta^j$ for some j with $1 \le j \le n-1$. So $\zeta = \sigma^{-1}(\sigma(\zeta)) = \zeta^{ij}$. By Theorem I.3.4(v), we have $ij \equiv 1 \pmod{n}$ and hence $\bar{i} \in \mathbb{Z}_n$ as $\theta(\sigma) = \bar{i}$ where $\sigma(\zeta) = \zeta^i$. For $\sigma_1, \sigma_2 \in \mathrm{Aut}_F K$ with $\sigma_1(\zeta) = \zeta^{i_1}$ and $\sigma_2(\zeta) = \zeta^{i_2}$ we have

$$\begin{aligned} \theta(\sigma_1 \circ \sigma_2) &= \overline{i_1 i_2} \text{ since } (\sigma_1 \circ \sigma_2)(\zeta) = \zeta^{i_1 i_2} \\ &= \overline{i_1}\,\overline{i_2} = \theta(\sigma_1)\theta(\sigma_2) \end{aligned}$$

and so θ is a group homomorphism. Also, if $\sigma_1 \ne \sigma_2$ (and so $i_1 \ne i_2$ since the σ's are determined based on their values on ζ) then $\theta(\sigma_1) = \overline{i_1} \ne \overline{i_2} = \theta(\sigma_2)$ and θ is one to one. That is, θ is a group monomorphism. As commented above, if $\sigma(\zeta) = \zeta^i$ then $\bar{i}$ is a unit in $\mathbb{Z}_n$, so $\mathrm{Im}(\theta)$ is a subgroup of the group of units in $\mathbb{Z}_n$.

Theorem V.8.1 (continued 3)

Proof (continued). (ii) and (iii) By Exercise V.8.1, the order of the group of units in $\mathbb{Z}_n$ is $\varphi(n)$, so be Lagrange's Theorem (Corollary I.4.6), with d as the order of $\text{Im}(\theta)$, $d \mid \varphi(n)$. Also $\text{Aut}_K F \cong \text{Im}(\theta)$, so $\text{Aut}_K F$ is an abelian group with order d where $d \mid \varphi(n)$. So (iii) follows. As commented above, F is Galois over K and since $\text{Aut}_K F$ is abelian, then F is an abelian extension of K. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)), $[F : K] = |\text{Aut}_K F| = d$. If n is prime then $\mathbb{Z}_n$ is a field and all nonzero elements of $\mathbb{Z}_n$ are units and by Theorem V.5.3 form a cyclic group. So $\text{Aut}_K F \cong \text{Im}(\theta)$ is a cyclic group and so F is a cyclic extension of K and (ii) follows. □

Theorem V.8.1 (continued 3)

Proof (continued). (ii) and (iii) By Exercise V.8.1, the order of the group of units in $\mathbb{Z}_n$ is $\varphi(n)$, so be Lagrange's Theorem (Corollary I.4.6), with d as the order of $\text{Im}(\theta)$, $d \mid \varphi(n)$. Also $\text{Aut}_K F \cong \text{Im}(\theta)$, so $\text{Aut}_K F$ is an abelian group with order d where $d \mid \varphi(n)$. So (iii) follows. As commented above, F is Galois over K and since $\text{Aut}_K F$ is abelian, then F is an abelian extension of K. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(ii)), $[F : K] = |\text{Aut}_K F| = d$. If n is prime then $\mathbb{Z}_n$ is a field and all nonzero elements of $\mathbb{Z}_n$ are units and by Theorem V.5.3 form a cyclic group. So $\text{Aut}_K F \cong \text{Im}(\theta)$ is a cyclic group and so F is a cyclic extension of K and (ii) follows. □

Theorem V.8.2

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char(K) $= 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

(iii) $\text{Deg}(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Proof. (i) Let F be the splitting field of $x^n - 1_K$. Then F is a cyclotomic extension of K or order n. Let $\zeta \in F$ be a primitive nth root of unity.

Theorem V.8.2

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

(iii) Deg$(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Proof. (i) Let F be the splitting field of $x^n - 1_K$. Then F is a cyclotomic extension of K or order n. Let $\zeta \in F$ be a primitive nth root of unity. By Lemma V.7.10(i) applied to F, the cyclic group $G = \langle \zeta \rangle$ of all nth roots of unity contains all dth roots of unity for every divisor d of n. Now $\eta \in G$ is a primitive dth root of unity (where $d \mid n$) if and only if the order of η satisfies $|\eta| = d$.

Theorem V.8.2

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

(iii) $\mathrm{Deg}(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Proof. (i) Let F be the splitting field of $x^n - 1_K$. Then F is a cyclotomic extension of K or order n. Let $\zeta \in F$ be a primitive nth root of unity. By Lemma V.7.10(i) applied to F, the cyclic group $G = \langle \zeta \rangle$ of all nth roots of unity contains all dth roots of unity for every divisor d of n. Now $\eta \in G$ is a primitive dth root of unity (where $d \mid n$) if and only if the order of η satisfies $|\eta| = d$.

Theorem V.8.2 (continued 1)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

Proof (continued). (i) Therefore for each divisor d of n (by the definition of $g_d(x)$), $g_d(x) = \prod_{\eta \in G, |\eta|=d}(x - \eta)$ and

$$x^n - 1_K = \prod_{\eta \in G}(x - \eta) = \prod_{d|n}\left(\prod_{\eta \in G, |\eta|=d}(x - \eta)\right) = \prod_{d|n} g_d(x).$$

(ii) We prove the first statement by (the Strong Principle of) Induction. Clearly $q_1(x) \in x - 1_K \in P[x]$.

Theorem V.8.2 (continued 1)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(i) $x^n - 1_K = \prod_{d|n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

Proof (continued). (i) Therefore for each divisor d of n (by the definition of $g_d(x)$), $g_d(x) = \prod_{\eta \in G, |\eta| = d}(x - \eta)$ and

$$x^n - 1_K = \prod_{\eta \in G}(x - \eta) = \prod_{d|n}\left(\prod_{\eta \in G, |\eta| = d}(x - \eta)\right) = \prod_{d|n} g_d(x).$$

(ii) We prove the first statement by (the Strong Principle of) Induction. Clearly $q_1(x) \in x - 1_K \in P[x]$.

Theorem V.8.2 (continued 2)

Proof (continued). (ii) Assume that (ii) is true for *all* $k < n$ and let $f(x) = \prod_{d|n, d<n} g_d(x)$. Then $f \in P[x]$ by the induction hypothesis. In $F[x]$ (F a cyclotomic extension of K of order n, as in the proof of (i))

$$x^n - 1_K = \prod_{d|n, d \le n} g_d(x) = g_n(x) \prod_{d|n, d<n} g_d(x) = g_n(x) f(x).$$

On the other hand, $x^n - 1_K \in P[x]$ and f is monic (since each $g_d(x)$ is monic).

Theorem V.8.2 (continued 2)

Proof (continued). (ii) Assume that (ii) is true for *all* $k < n$ and let $f(x) = \prod_{d|n, d<n} g_d(x)$. Then $f \in P[x]$ by the induction hypothesis. In $F[x]$ (F a cyclotomic extension of K of order n, as in the proof of (i))

$$x^n - 1_K = \prod_{d|n, d\leq n} g_d(x) = g_n(x) \prod_{d|n, d<n} g_d(x) = g_n(x) f(x).$$

On the other hand, $x^n - 1_K \in P[x]$ and f is monic (since each $g_d(x)$ is monic). Consequently, by the Division Algorithm in $P[x]$ (Theorem III.6.2) we have that $x^n - 1_K - fh + r$ for unique $h, r \in P[x] \subset F[x]$ where $\deg(r) < \deg(f)$. Since $x^n - 1_K = fg_n$ from above, the uniqueness of h and r implies that $r = 0$ and $h = g_n$.

Theorem V.8.2 (continued 2)

Proof (continued). (ii) Assume that (ii) is true for *all* $k < n$ and let $f(x) = \prod_{d|n,d<n} g_d(x)$. Then $f \in P[x]$ by the induction hypothesis. In $F[x]$ (F a cyclotomic extension of K of order n, as in the proof of (i))

$$x^n - 1_K = \prod_{d|n,d\leq n} g_d(x) = g_n(x) \prod_{d|n,d<n} g_d(x) = g_n(x)f(x).$$

On the other hand, $x^n - 1_K \in P[x]$ and f is monic (since each $g_d(x)$ is monic). Consequently, by the Division Algorithm in $P[x]$ (Theorem III.6.2) we have that $x^n - 1_K - fh + r$ for unique $h, r \in P[x] \subset F[x]$ where $\deg(r) < \deg(f)$. Since $x^n - 1_K = fg_n$ from above, the uniqueness of h and r implies that $r = 0$ and $h = g_n$. Since $h(x) \in P[x]$ then $g_n(x) = h(x) \in P[x]$. So the first statement in (ii) is true for n and so holds for all $n \in \mathbb{N}$.

Theorem V.8.2 (continued 2)

Proof (continued). (ii) Assume that (ii) is true for *all* $k < n$ and let $f(x) = \prod_{d|n,d<n} g_d(x)$. Then $f \in P[x]$ by the induction hypothesis. In $F[x]$ (F a cyclotomic extension of K of order n, as in the proof of (i))

$$x^n - 1_K = \prod_{d|n,d\leq n} g_d(x) = g_n(x) \prod_{d|n,d<n} g_d(x) = g_n(x) f(x).$$

On the other hand, $x^n - 1_K \in P[x]$ and f is monic (since each $g_d(x)$ is monic). Consequently, by the Division Algorithm in $P[x]$ (Theorem III.6.2) we have that $x^n - 1_K - fh + r$ for unique $h, r \in P[x] \subset F[x]$ where $\deg(r) < \deg(f)$. Since $x^n - 1_K = fg_n$ from above, the uniqueness of h and r implies that $r = 0$ and $h = g_n$. Since $h(x) \in P[x]$ then $g_n(x) = h(x) \in P[x]$. So the first statement in (ii) is true for n and so holds for all $n \in \mathbb{N}$.

Theorem V.8.2 (continued 3)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If char$(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

Proof (continued). (ii) If char$(K) = 0$ then the prime field $P \cong \mathbb{Q}$ by Theorem V.5.1. As argued above, $g_1(x) = x - 1 \in \mathbb{Z}[x]$ and by (i), $x^n - 1 = f(x)g_n(x)$ in $\mathbb{Q}[x]$ (with the above notation). By the Division Algorithm in $\mathbb{Z}[x]$, $x^n - 1 = fh + r$ were $\deg(r) < \deg(f)$, and $r, h \in \mathbb{Z}[x]$. But (as above) this implies $r(x) = 0$ and $h(x) = g_n(x)$. Since $h(x) \in \mathbb{Z}[x]$ then $g_n(x) \in \mathbb{Z}[x]$ and the second statement in (ii) is true for all $n \in \mathbb{N}$.

Theorem V.8.2 (continued 3)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that $\text{char}(K)$ does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If $\text{char}(K) = 0$ and P is identified with the field $\mathbb{Q}$ of rationals, then the coefficients are actually integers.

Proof (continued). (ii) If $\text{char}(K) = 0$ then the prime field $P \cong \mathbb{Q}$ by Theorem V.5.1. As argued above, $g_1(x) = x - 1 \in \mathbb{Z}[x]$ and by (i), $x^n - 1 = f(x)g_n(x)$ in $\mathbb{Q}[x]$ (with the above notation). By the Division Algorithm in $\mathbb{Z}[x]$, $x^n - 1 = fh + r$ were $\deg(r) < \deg(f)$, and $r, h \in \mathbb{Z}[x]$. But (as above) this implies $r(x) = 0$ and $h(x) = g_n(x)$. Since $h(x) \in \mathbb{Z}[x]$ then $g_n(x) \in \mathbb{Z}[x]$ and the second statement in (ii) is true for all $n \in \mathbb{N}$.

Theorem V.8.2 (continued 4)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(iii) $\mathrm{Deg}(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Proof (continued). (iii) By the definition of $g_n(x)$, $\deg(g_n)$ is the number of primitive nth roots of unity. Let ζ be such a primitive root so that every other primitive root is a power of ζ (since ζ generates *all* nth roots of unity). By Theorem I.3.6, ζ^i where $1 \leq i \leq n$ is a primitive nth root of unity (i.e., a generator of G) if and only if $\gcd(i, n) = (i, n) = 1$. But the number of such i is by definition precisely $\varphi(n)$. □

Theorem V.8.2 (continued 4)

Theorem V.8.2. Let $n \in \mathbb{N}$, let K be a field such that char(K) does not divide n, and let $g_n(x)$ be the nth cyclotomic polynomial over K. Then the following hold.

(iii) $\text{Deg}(g_n(x)) = \varphi(n)$ where φ is the Euler phi function.

Proof (continued). (iii) By the definition of $g_n(x)$, $\deg(g_n)$ is the number of primitive nth roots of unity. Let ζ be such a primitive root so that every other primitive root is a power of ζ (since ζ generates *all* nth roots of unity). By Theorem I.3.6, ζ^i where $1 \leq i \leq n$ is a primitive nth root of unity (i.e., a generator of G) if and only if $\gcd(i, n) = (i, n) = 1$. But the number of such i is by definition precisely $\varphi(n)$. □