1 Splitting Fields

Lemma 1.0.1. If $\alpha \in E$ is transecendental over K then $K(\alpha) \cong K(X) = Q_{K[X]}$

Proof. The map $ev_\alpha : K[X] \mapsto K(\alpha)$ is injective because α is transecendental over K. Thus, because $K(\alpha)$ is a field and $K[X]$ is a domain, ev_α factors into $ev_\alpha = \iota \circ f$ where $\iota : K[X] \to Q_{K[X]}$ is given by $\iota : f \mapsto (f, 1)$ and f is an injective homomorphism.

$$\begin{tikzcd} K[X] \arrow[r, hook, "\iota"] \arrow[dr, hook, "ev_\alpha"'] & K(X) \arrow[d, dashed, "f"] \\ & K(\alpha) \end{tikzcd}$$

Then, f is an embedding of $K(X)$ into $K(\alpha)$ but $K(\alpha)$ is the subfield of E generated by $K[\alpha] = \mathrm{Im}\,(ev_\alpha)$ so $K(X) = K(X)$ ☐

Theorem 1.0.2 (Embedding)**.** Let K be a field and E, E' be extensions with $\alpha \in E$ and $\alpha' \in E'$ with both α and α' algebraic over K. Suppose that $\mathrm{Min}(\alpha; K) = \mathrm{Min}(\alpha'; K)$ then there exists a K-preserving isomorphism $\phi : K(\alpha) \to K(\alpha')$ such that $\phi : \alpha \mapsto \alpha'$.

Proof. There exist K-preserving isomorphisms $\beta : K[X]/(\mathrm{Min}(\alpha; K)) \to K(\alpha)$ and $\gamma : K[X]/(\mathrm{Min}(\alpha'; K)) \to K(\alpha')$ but $\mathrm{Min}(\alpha; K) = \mathrm{Min}(\alpha'; K)$ so let $\phi = \gamma \circ \beta^{-1}$ which is a K-preserving isomorphism. Now,

$$\begin{tikzcd} & K[X]/(\mathrm{Min}(\alpha; K)) \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] & \\ K(\alpha) \arrow[rr, "\phi"] & & K(\alpha') \end{tikzcd}$$

Finally, $\beta(\bar{X}) = ev_\alpha(X) = \alpha$ and $\gamma(\bar{X}) = \alpha'$ so $\phi \circ \beta(\bar{X}) = \gamma(\bar{X})$ thus $\phi(\alpha) = \alpha'$. ☐

Corollary 1.0.3. If E/K and $p \in K[X]$ is irreducible over K with roots $\alpha_1, \alpha_2 \in E$ then there exists a K-isomorphism from $K(\alpha)$ to $K(\alpha')$ which takes α to α'.

Corollary 1.0.4. If $\alpha_1, \alpha_2 \in E$ are algebraic over K with equal minimal polynomials and $E = K(\alpha_1) = K(\alpha_2)$ but $\alpha_1 \neq \alpha_2$ then there exists an automorphism of E which preserves K and sends α_1 to α_2.

Corollary 1.0.5. If $\alpha \in E$ is algebraic over K and E' contains a root of $\mathrm{Min}(\alpha; K)$ then there exists a field embedding $\phi : K(\alpha) \to E'$.

Definition 1.0.6. E/K is an algebraic extension if $\forall \alpha \in E : \alpha$ is algebraic over K.

Proposition 1.0.7. If $[E : K]$ is finite then E/K is algebraic.

Proof. If $[E : K]$ is finite then for any $\alpha \in E$, the identity,

$$[E : K] = [E : K(\alpha)][K(\alpha) : K]$$

gives that $[K(\alpha) : K]$ is finite so α is algebraic over K. ☐

Proposition 1.0.8. $[E : K]$ is finite if and only if $\exists \alpha_1, \dots \alpha_n \in E$ s.t. $E = K(\alpha_1, \dots, \alpha_n)$

Proof. ☐

Definition 1.0.9. Let K be a field and $f \in K[X]$ with L/K a field extension, L is the splitting field of f if,

(a) $f \in L[X]$ is split into linear factors, i.e. $f(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$ with $a \in K$ and $\alpha_i \in L$.

(b) $L = K(\alpha_1, \ldots, \alpha_n)$

Lemma 1.0.10. Let $p \in K[X]$ be irreducible, then there exists a field extension L/K such that $\tilde{p} \in L[X]$ has a root in L.

Proof. Define $L = K[X]/(p)$ which is a field because (p) is a maximal ideal since p is irreducible in a PID. Now, $\iota : K \to K/(p)$ given by $\iota : r \mapsto r + (p)$ is a field homomorphism and thus an injection. Thus, $K \cong \text{Im}(\iota)$ so we have an embedding of K in $K/(p)$. We extend $\iota : K[X] \to L[X]$ by acting on coefficients and $\tilde{p} = \iota(p)$ Consider the map $\pi : K[X] \to K[X]/(p)$ given by $\pi : a \mapsto x + (p)$ is a homomorphism so $\tilde{p}(\pi(X)) = \pi(p(X)) = p(X) + (p) = (p)$ so $\pi(X)$ is a root of $\tilde{p}$ in L. ☐

Corollary 1.0.11. For any $p \in K[X]$, there exists a field extension L/K such that $\tilde{p} \in L[X]$ has a root in L.

Proof. If p is irreducible, we are done. Otherwise, because $K[X]$ is a UFD, take some irreducible $g \mid p$ with $\deg g > 0$ then there exists a field extension in which g has a root and therefore, p has a root. ☐

Theorem 1.0.12. For any nonconstant $f \in K[X]$ there exists a splitting field of f.

Proof. Let $\deg f = n$. Construct $K_1 \supset K$ with $\alpha \in K_1$ s.t. $f(\alpha_1) = 0$ so in $K_1[X]$ we have $f(X) = (X - \alpha_1)g_1(X)$ with $g_1(X) \in K_1[X]$ and $\deg g_n = n - 1$. By Induction, we get a chain $K_n \supset K_{n-1} \supset \cdots \supset K$ such that

$$f(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)g_n(X)$$

with $\deg g = 0$ so $g(X) = c \in K_n[X]$. Then, take $L = K(\alpha_1, \ldots, \alpha_n) \subset K_n$. ☐

Theorem 1.0.13. For nonconstant $f \in K[X]$, if L_1 and L_2 are both splitting fields of f over K then L_1 and L_2 are K-isomorphic.

Proof. Induction on $\deg f = n$. For $n = 1$, $f(X) = x - r$ with $r \in K$ so $L_1 = L_2 = K$. Suppose the theorem holds for $\deg g < n$. Then, if f is reducible, $f(X) = f_1(X)f_2(X)$ with strictly smaller degrees. ☐

Definition 1.0.14. An algebraic extension E/K is normal if for all $\alpha \in E$, the minimal polynomial splits completely in E.

Lemma 1.0.15. If E/K is normal and $K \subset L \subset E$ then E/L is normal.

Proof. Take $\alpha \in E$ with minimal polynomial over K given by $\text{Min}(\alpha; K)$. Then, $\text{Min}(\alpha; K) \in L[X]$ and has α as a root. Thus, $\text{Min}(\alpha; L) \mid \text{Min}(\alpha; K)$ but $\text{Min}(\alpha; K)$ splits in E so $\text{Min}(\alpha; L)$ splits in E. ☐

Theorem 1.0.16. Let E/K be a finite extension then the following are equivalent:

(a) E/K is normal

(b) E is the splitting field of some $f \in K[X]$

(c) If $K \subset K_1 \subset E \subset E_1$ and $\sigma : K_1 \to E_1$ is a K-homomorphisms then $\mathrm{Im}\,(\sigma) \subset E$

Proof. Since E/K is a finite extension, $E = K(\alpha_1, \dots, \alpha_n)$ for $\alpha_i \in K$. Then take $f = \mathrm{Min}(\alpha_1; K) \dots \mathrm{Min}(\alpha_n;$ By normality, f must split into linear factors in E. Furthermore, $E = K(\alpha_1, \dots, \alpha_n) \subset K(r_1, \dots r_s)$ where there are the roots of f. However, E contains every root by normality so $E = K(r_1, \dots, r_s)$. Thus, E is the splitting field of f.

Take some f with E the splitting field of f. Take $f(X) = a(X - \alpha_1) \dots (X - \alpha_n)$ with $\alpha \in E$ and $E = K(\alpha_1, \dots, \alpha_n)$. Take any $K \subset K_1 \subset E \subset E_1$ and $\sigma : K_1 \to E_1$. Define $K_1' = \sigma(K_1) \subset E_1$ and $E' = K_1'(\alpha_1, \dots, \alpha_n)$.

$$\begin{tikzcd}
 & E_1 & \\
E \arrow[ur, "\iota"] \arrow[rr, dashed, "\tilde{\sigma}"] & & E' \arrow[ul, "\iota"'] \\
K_1 \arrow[u, "\iota"] \arrow[rr, "\sigma"] \arrow[urr, dotted] & & K_1' \arrow[u, "\iota"'] \\
 & K \arrow[ul, "\iota"] \arrow[ur, "\iota"'] &
\end{tikzcd}$$

K is embedded in E and and E' $\iota \circ \sigma$ and both fields contain every root of f so they σ takes f to f and $\tilde{\sigma} : E \to E'$ extends σ because both are the splitting field of f over K. For each $\sigma : \alpha_i \to \alpha_j$ because $\tilde{\sigma}(f(\alpha)) = f(\tilde{\sigma}(\alpha))$ and it maps into a field containing the splitting field. Because $\tilde{\sigma}$ is a K-homomorphism, it fixes K and also preserves the set $\{\alpha_i\}$ so $\sigma(E) = \sigma(K(\alpha_1, \dots, \alpha_n)) = K(\alpha_1, \dots, \alpha_n) = E'$. Thus, $E = E'$ so $K_1' = \mathrm{Im}\,(\sigma) \subset E' = E$.

Let $\alpha \in E$ and let E_1 be the splitting field of $\mathrm{Min}(\alpha; K)$. Then take $K \subset K_1 = K(\alpha) \subset E \subset E_1$. By the embedding theorem, there exits a K-homomorphism $\sigma : K(\alpha) \mapsto E_1$ sending α to any root of $\mathrm{Min}(\alpha; K)$. However by (2), we have $\mathrm{Im}\,(\sigma) \subset E$ so E contains every root of $\mathrm{Min}(\alpha; K)$ so E is normal. ☐

Proposition 1.0.17. If $[E : K] = 2$ then E/K is a normal extension.

Proof. Take $\alpha \in E \backslash K$ then $\{1_K, \alpha\}$ is a basis for E over K because $\alpha \neq k \cdot 1_K$ because $\alpha \notin K$. Thus, $E = K(\alpha)$ so the polynomial $q = \mathrm{Min}(\alpha; K)$ has degree 2. Since $\alpha \in E$ the minimal polynomial has one root in E but $q(X) = (X - \alpha)g(X)$ and $\deg f = 2$ implies that g is a linear factor so q is split. ☐

Proposition 1.0.18. let $f \in K[X]$ and L be the splitting field of f over K then $[L : K] \leq n!$.

Proof. Let $f(X) = c(X - \alpha_1) \cdots (X - \alpha_n) \in L[X]$ and $L = K(\alpha_1, \dots, \alpha_n)$. Now, let $L_i = K(\alpha_1, \dots, \alpha_i)$ such that $L_{i+1} = L_i(\alpha_{i+1})$. Therefore,

$$[L_{i+1} : L_i] = \deg \mathrm{Min}(\alpha_{i+1}; L_i)$$

However $L_i = K(\alpha_1, \dots, \alpha_n)$, so

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_i) g_i(X)$$

with $g_i \in L_i[X]$ but $g_i(\alpha_{i+1}) = 0$ because in $L[X]$,

$$g_i(X) = \frac{f(X)}{(X - \alpha_1) \cdots (X - \alpha_n)} = c(X - \alpha_{i+1}) \cdots (X - \alpha_n)$$

Therefore, $\text{Min}(\alpha_{i+1}; L_i) \mid g_i$ so $[L_{i+1} : L_i] \leq \deg g_i = n - i$. Thus,

$$[L : K] = [L : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_1 : L_0] \leq 1 \cdot 2 \cdots n = n!$$

because $L = L_n$ and $K = L_0$. $\square$

Proposition 1.0.19. If E and K are finite fields then E/K is a normal extension.

Proof. Let $|E| = q$ then E is the splitting field of $X^q - X$ over K so it is a normal extension of K. $\square$

2 Seperable Extensions

Definition 2.0.1. A polynomial $f \in K[X]$ is seperable if f does not have multiple roots in E, the splitting field of f over K.

Lemma 2.0.2. If $f \in K[X]$ is irreducible and $f' \neq 0_{K[X]}$ then f is seperable.

Proof. Because $f' \neq 0$ we have that $\deg f' < \deg f$ so $f \nmid f'$. Now consider the ideal (f, f'). Because $K[X]$ is a PID, we have that $(f, f') = (g)$ so $g \mid f$. However, f is irreducible so $g = uf$ or $g = u$ with $u \in K[X]^\times$. However, $g \mid f'$ and $f \nmid f'$ so $g = u$. Therefore, $(f, f') = K[X]$. In particular, there exist $a, b \in K[X]$ such that $af + bf' = 1$. Take any field extension E/K. If f had a multiple root in E then there would be some $\alpha \in E$ such that $f(\alpha) = f'(\alpha) = 0$. However, then $a(\alpha)f(\alpha) + b(\alpha)f'(\alpha) = 0$ which contraicts the fact that $af + bf' = 1$. Therefore, f has no multiple roots in any field extension of K and, in particular, none in its splitting field. $\square$

Proposition 2.0.3. Let K have characteristic zero, then any irreducible polynomial in $K[X]$ is seperable.

Proof. Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$ be an irreducible polynomial over K. Now,

$$f'(X) = n \cdot a_n X^{n-1} + \cdots a_1$$

If $f' \neq 0$ then f is f is seperable by above. Otherwise, because K has characteristic zero, the unique homomorpihsm $\mathbb{Z} \to K$ given by repeated addition is injective so $f' = 0$ implies that $a_n = \cdots = a_1 = 0$. Therefore, $f(X) = a_0$ which is already split in K and has no roots. Thus, f is vacuously seperable. $\square$

Lemma 2.0.4. Let K have characteristic p and $f \in K[X]$ be irreducible. Then, there exists a seperable polynomial $g \in K[X]$ and some $k \in \mathbb{Z}$ such that $f(X) = g(X^k)$.

Proof. If f is seperable, then let $k = 1$ and $g = f$. Otherwise, because f is inseperable and irreducible, $f' = 0$. Let

$$f(X) = \sum_{k=0}^{n} a_k X^k \quad \text{so} \quad f'(X) = \sum_{k=1}^{n} k \cdot a_k X^{k-1} = 0$$

Therefore, $k \cdot a_k = 0$ for each $k \geq 1$. Therefore, either $a_k = 0$ or $k \in \ker \varphi$ with $\varphi : \mathbb{Z} \to K$. Thus, $p \mid k$. Thus, the only nonzero terms are divisible by k. Therefore,

$$f(X) = \sum_{i=0}^{r} a_{ip} X^{ip} = g_1(X^p) \quad \text{where} \quad g_1(X) = \sum_{i=0}^{n} a_{ip} x^i$$

Now, g_1 is irreducible because $f(X) = g_1(X^p)$ and f is irreducilbe. If g_1 is seperable, we are done. Else, by the same argument, $g_1(X) = g_2(X^p)$ and thus $f(X) = g_2(X^{p^2})$. At each stage, the degree is reduced so either the process terminates because $g_k' \neq 0$ and then g_k is seperable with $f(X) = g_k(X^{p^k})$ or we reach $\deg g_k < p$. However, then $g_k' = 0$ implies that $g = 0$ because no power is an element in the kernel. Thus, $g_k' \neq 0$ which reduces to the earlier case. $\square$

Definition 2.0.5. For a field extension E/K an element $\alpha \in E$ is seperable over K if $\text{Min}(\alpha; K)$ is seperable.

Definition 2.0.6. An extension E/K is seperable if $\forall \alpha \in E : \alpha$ is seperable over K.

Definition 2.0.7. K is perfect is every algebraic extension is seperable.

Proposition 2.0.8. If K has characteristic zero then K is perfect.

Proof. Because K has characteristic zero, every irreducible polynomial over K is seperable including the minimal polynomial of any $\alpha \in E$. $\square$

Definition 2.0.9. Let $\text{char}\, K = p$, the Frobenius map $\sigma_F : K \to K$ is given by $\sigma_F : x \to x^p$.

Lemma 2.0.10. The Frobenius map is a field endomorphism.

Proof. Take $x, y \in K$ then,

$$\sigma_F(x+y) = (x+y)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} x^k y^{p-k}$$

However, if $k < p$ and $p - k < p$ i.e. $0 < k < p$ then $p \mid \frac{p!}{k!(p-k)!}$ so because $\text{char}\, K = p$, the term $\frac{p!}{k!(p-k)!} x^k y^{p-k} = 0$. Therefore, $(x+y)^p = x^p + y^p$. Thus, $\sigma_F(x+y) = \sigma_F(x) + \sigma_F(y)$. Furthermore, $\sigma_F(xy) = (xy)^p = x^p y^p = \sigma_F(x)\sigma_F(y)$ because field multiplication is commutative. $\square$

Theorem 2.0.11. Let $\text{char}\, K = p$, then K is perfect if and only if the Frobenius map is surjective and therefore an isomorphism because field homomorphisms are injective.

Proof. Let σ_F be an isomorphism and suppose that E/K is not seperable. Then, $\exists \alpha \in E$ such that $q = \text{Min}(\alpha; K)$ is not seperable. Therefore, $q(X) = g(X^{p^k})$ for some $k \in \mathbb{Z}$ and some irreducible $g \in K[X]$. Write,

$$q(X) = g(X^p) = \sum_{k=0}^{r} a_k X^{pk}$$

However, because σ is an automorphism, there exists $b_k \in K$ such that $\sigma(b_k) = a_k$. Thus, we have $a_k = (b_k)^p$ and then,

$$q(X) = g(X^p) = \sum_{k=0}^{r} a_k X^{pk} = \sum_{k=0}^{r} (b_k)^p X^{pk} = \sum_{k=0}^{r} \sigma_F(b_k X^k) = \sigma_F\left(\sum_{k=0}^{r} b_k X^k\right) = R(X)^p$$

which contradicts the irreduciblility of q.

Conversely, suppose that σ_F is not sujective. Then, there exists $a \in K$ such that $a \notin \mathrm{Im}\,(\sigma_F)$. Therefore, $X^p - a$ has no roots in K. Let α be a root of $X^p - a$ in the splitting field such that $\alpha^p = a$ so $X^p - a = X^p - \alpha^p = (X-\alpha)^p$ because the Frobenius is a homomorphism. However, $\mathrm{Min}(\alpha; K)$ divides $X^p - a = (X-\alpha)^p$ so $\mathrm{Min}(\alpha; K) = (X-\alpha)^k$ by unique factorization. Also, $k > 1$ because $\alpha \notin K$ since α is a root of $X^p - a$ which has no roots in K. Thus, the minimal polynomial of α has multiple roots and therefore, K is not perfect. ☐

3 Classification of Finite Fields

If K is a finite field then $\mathrm{char}\, K = p > 0$ else we would have an injection $\varphi : \mathbb{Z} \to K$ and $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ and $[K : \mathbb{F}_p] = n < \infty \implies |K| = p^n$. Since K is a field and $K^\times$ is a finite group of order $p^n - 1$ so $K^\times$ is cyclic. Thus, $\forall x \in K : x^{p^n} - x = 0$ because 0 satisfies this and for $x \in K^\times = K \setminus \{0\}$ we know that $x^{p^n - 1} = 1$ so $x^{p^n} - x = 0$. Thus, the polynomial $P(X) = X^{p^n} - X$ has exactly p^n roots in K. Thus, K is the splitting field of P over $\mathbb{F}_p$. Therefore, any two extensions of $\mathbb{F}_p$ of equal degree are isomorphic. In particular, a unique K exists by the existence of the splitting field of P over $\mathbb{F}_p$. We must check that $|K| = p^n$. Then $P'(X) = p^n X^{p^n - 1} - 1 = -1$ is always nonzero. Therefore, P cannot have multiple roots in $\mathbb{F}_p$. However, K is the spliting field of a degree p^n polynomial so P splits into p^n factors which are all distict. Thus, $|K| \geq p^n$. However, if α, β are roots of P then

$$(\alpha\beta)^{p^n} - \alpha\beta = (\alpha^{p^n} - \alpha + \alpha)\beta^{p^n} - \alpha\beta = \alpha(\beta^{p^n} - \beta) = 0$$

and likewise,

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - (\alpha + \beta) = 0$$

because K has characteristic p. Thus, the roots of P form a subfield of K but K is the splitting field of P so this subfield cannot be proper. Thus, $|K| = p^n$.

4 Galois Theory

Definition 4.0.1. E/K is Galois if E/K is normal and seperable.

Definition 4.0.2. $\mathrm{Gal}\,(E/K) = H < \mathrm{Aut}\,(E)$ where $\sigma \in H \iff \forall x \in K : \sigma(x) = x$.

Proposition 4.0.3. Let F/K be Galois and $K \subset E \subset F$ then F/E is Galois.

Proof. ☐

Proposition 4.0.4. Let F/K be Galois and $K \subset E \subset F$ then E/K is Galois iff E/K is normal.

Proof. ☐

Proposition 4.0.5. For K'/K and $E, K \subset F'$ and E/K is Galois then EF/KF is Galois.

Proof. ☐

Theorem 4.0.6. A field extension E/K is Galois if and only if $[E : K] = |\mathrm{Gal}\,(E/K)\,|$

Proof. ☐

Definition 4.0.7. For a field extension E/K and $H < \mathrm{Gal}(E/K)$ then,

$$E^H = \mathrm{Fix}_E(H) = \{\alpha \in E \mid \forall \sigma \in H : \sigma(\alpha) = \alpha\}$$

Proposition 4.0.8. Let E/K be fintie Galois and $\alpha \in E$ then by normality,

$$q(X) = \mathrm{Min}(\alpha; K)(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$$

and $\mathrm{Gal}(E/K)$ acts on the set $\{\alpha_1, \ldots, \alpha_n\}$ transitively.

Proof. Let $G = \mathrm{Gal}(E/K)$ and take $\sigma \in G$ then $q(X) = a_0 + a_1 X + \cdots + a_n X^n$ for $a_k \in K$. Now, $q(\alpha_i) = a_0 + a_1\alpha_i + \cdots + a_n \alpha_i^n = 0$. Thus,

$$\sigma(q(\alpha_i)) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha_1) + \cdots + \sigma(a_n)\sigma(\alpha_i)^n = a_0 + a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_i)^n = q(\sigma(\alpha_i))$$

because σ preserves K. Thus, $q(\sigma(\alpha_i)) = \sigma(q(\alpha_i)) = 0$ so $\sigma(\alpha_i)$ is a root of q is is split so $\sigma(\alpha_i) = \alpha_j$ for some j.

By hypothesis, E is normal and thus E is the splittig field of some $f \in K[X]$. Let $s = f \cdot q$ then E is also the splitting field of s over K. Take α, β th (STILL PROVE THIS) $\square$

Proposition 4.0.9. Let E/K be normal and therefore the splitting field of a monic $f \in K[X]$ with $\deg f = n$. Then, there exists an embedding $\phi : \mathrm{Gal}(E/K) \to S_n$ which is a transitive subgroup of S_n if f is irreducible.

Proof. Write $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$. Then, $\mathrm{Gal}(E/K)$ acts on the set of roots $\{\alpha_1, \cdots, \alpha_n\}$ and this action is a homomorphism $\phi : \mathrm{Gal}(E/K) \to S_n$. If $\phi(\sigma) = \mathrm{id}$ then $\sigma(\alpha_i) = \alpha_i$ for every i. However, σ is a K-preserving homomorphism so σ preserves $E = K(\alpha_1, \ldots, \alpha_n)$ and is thus the identitiy element of $\mathrm{Gal}(E/K)$. Suppose f is irreducible and monic, then, $f = \mathrm{Min}(\alpha_i; K)$ and therefore, $\mathrm{Gal}(E/K)$ acts transitivly on $\{\alpha_1, \cdots, \alpha_n\}$ so by definition, its image in S_n is a transitive subgroup. $\square$

Theorem 4.0.10 (Fundamental Theorem of Galois Theory)**.** Let E/K be a finite Galois extension then there is a bijection φ_G (a Galois correspondence) between the subgroups $H < \mathrm{Gal}(E/K)$ and subfields $K \subset F \subset E$ such that:

(a) $\varphi : H \mapsto E^H$

(b) $\varphi^{-1} : F \mapsto \mathrm{Gal}(E/F)$ where E/F is also Galois.

(c) $\varphi^{-1} \circ \varphi : H \mapsto \mathrm{Gal}\left(E/E^H\right) = H$

(d) $\varphi \circ \varphi^{-1} : F \mapsto E^{\mathrm{Gal}(E/F)} = F$

(e) $H_1 < H_2 \iff E^{H_1} \supset E^{H_2}$

(f) $|H| = [E : E^H]$ and $[\mathrm{Gal}(E/K) : H] = [E^H : K]$

(g) $H \triangleleft \mathrm{Gal}(E/K) \iff E^H/K$ is Galois and then $\mathrm{Gal}\left(E^H/K\right) \cong \mathrm{Gal}(E/K)/H$

Proof. (a)

(b)

(c)

(d)

(e)

(f)

(g) For $\sigma \in G$, $\varphi(\sigma H \sigma^{-1}) = \sigma(E^H)$ so if H is normal iff $\sigma(E^H)$ for every $\sigma \in G$.

$\square$

Proposition 4.0.11. Let E/K be a finite Galois extension with $G = \mathrm{Gal}\,(E/K)$ and let $H \subset G$ with $F = E^H$. Then F/K is Galois iff $H \triangleleft G$ and then $\mathrm{Gal}\,(F/K) \cong G/H$.

Proof. Since E/K is seperable, so is F/K. Now, $g(F) = E^{gHg^{-1}}$ because for $g \in G$,

$$x \in g(F) \iff \exists y \in F = E^H : g(y) = x \iff \forall \sigma \in H : \sigma(y) = y \text{ and } g(y) = x$$

if and only if for any $\sigma \in H$, $g\sigma g^{-1}(x) = g\sigma(y) = g(y) = x$ i.e. $x \in E^{gHg^{-1}}$. Suppose that H is normal then $gHg^{-1} = H$ so $g(F) = F$ and thus F contains all the roots of any minimal polynomial of its elements because the set of g acts transitivly on the roots but $g(F) = F$ so F contains all the images. Explicitly, for any $\alpha \in F$ we have $g(\alpha) \in g(F) = F$ so F contains all the conjuates of α. Therefore, F/E is normal. Now, let F/K be normal and therefore the splitting field of some polynomial $f \in K[X]$. Therefore,

$$f(X) = a(X - \beta_1) \cdots (X - \beta_n)$$

and $F = K(\beta_1, \ldots, \beta_n)$. However, $g \in \mathrm{Gal}\,(E/K)$ so g acts on the set of roots of f. However, g preserves K so $g(F) = F$ because $g(\beta_i) = \beta_j$ and $F = K(\beta_1, \ldots, \beta_n)$. Therefore, $E^H = E^{gHg^{-1}}$ so $H = gHg^{-1}$ thus $H \triangleleft G$. In this case, define the homomorphism $\eta : G \to \mathrm{Gal}\,(F/K)$ by $\eta : \sigma \to \sigma|_F = \sigma \circ \iota_F$. Now,

$$\sigma \in \ker \eta \iff \sigma|_F = \mathrm{id}_F \iff \sigma \in \mathrm{Gal}\,(E/F) \iff \sigma \in H$$

Thus, $\ker \eta = H$ so $G/H \cong \mathrm{Im}\,(\eta)$. However, $[F : K] = |G/H| = |\mathrm{Gal}\,(F/K)\,|$ so $|\mathrm{Im}\,(\eta)\,| = |\mathrm{Gal}\,(F/K)\,|$ and thus $\mathrm{Im}\,(\eta) = \mathrm{Gal}\,(F/K)$. Finally, $\mathrm{Gal}\,(F/K) \cong G/H$. $\square$

Definition 4.0.12. In $\mathbb{Q}(Y_1, \cdots, Y_n)$, the fraction field of $\mathbb{Q}[Y_1, \cdots, Y_n]$, the elementary symmetric polynomials are,

$$u_i = \sum_{k_1 < k_1 < \cdots < k_i} Y_{k_1} Y_{k_2} \cdots Y_{k_i}$$

Proposition 4.0.13. Let $K_0 = \mathbb{Q}(u_1, \cdots, u_n) \subset \mathbb{Q}(Y_1, \cdots, Y_n) = E_0$ then let $f_0 \in K_0[X]$ be the polynomial $x^n - u_1 X^{n-1} + u_2 X^{n-2} + \cdots + (-1)^n u_n$. Then E_0 is the splitting field of f_0 and $\mathrm{Gal}\,(E_0/K_0) \cong S_n$.

Proof. By Vieta, $f_0(X) = (X - Y_1) \cdots (X - Y_n)$ so because $E_0 = \mathbb{Q}(Y_1, \cdots Y_n)$ we have that E_0 is the splitting field of f_0 over K_0. Therefore, E_0/K_0 is a normal extension and also a seperable extension because $\mathbb{Q}$ is perfect and $\mathbb{Q} \subset K_0 \subset E_0$. Therefore, E_0/K_0 is Galois. Futhermore, consider $G = S(\{Y_1, \cdots, Y_n\}) \cong S_n$. Any $\sigma \in G$ satisfies $\sigma(u_i) = u_i$ because they are unique with respect to reordering. We extend $\sigma : E_0 \to E_0$ by fixing it on $\mathbb{Q}$. Then $\sigma|_{K_0} = \mathrm{id}_{K_0}$ because $K_0 = \mathbb{Q}(u_1, \cdots u_n)$. Then $G \hookrightarrow \mathrm{Gal}\,(E_0/K_0) \hookrightarrow S_n \cong G$. Therefore, $G \cong \mathrm{Gal}\,(E_0/K_0)$. $\square$

Corollary 4.0.14. Any symmetric polynomial is generated by elementary symmetric polynomials.

Proof. Let $f \in \mathbb{Q}(Y_1, \cdots, Y_n)$ be symmetric. For any automorphism $\sigma \in \operatorname{Gal}(E_0/K_0)$, $\sigma(f) = f$ because the variables are symmetric under exchange. Therefore, f is fixed by every Galois automorphism so $f \in E_0^{\operatorname{Gal}(E_0/K_0)} = K_0 = \mathbb{Q}(u_1, \cdots, u_n)$ by the Galois correspondence. Thus, f is a fraction of elements of $\mathbb{Q}[u_1, \ldots, u_n]$ but since $f \in \mathbb{Q}[Y_1, \ldots, Y_n]$ then it mut lie in $\mathbb{Q}[u_1, \ldots, u_n]$. □

Corollary 4.0.15. Let K be a field and $f \in K[X]$ with splitting field E such that $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ then any symmetric polynomial in the roots is given by a universal polynomial in the coefficients of f.

Definition 4.0.16. $\operatorname{Disc}(f) = \Delta = \prod\limits_{i<j}(\alpha_i - \alpha_j)^2$ is a symmetric polynomial in the roots of f and therefore expressible as a polynomial of the coefficients of f.

Proposition 4.0.17. $f \in K[X]$ is seperable if and only if $\operatorname{Disc}(f) \neq 0$

Proof. $\operatorname{Disc}(f) = \prod\limits_{i<j}(\alpha_i - \alpha_j)^2 = 0$ if and only if one of the factors is zero i.e. for $i < j$ we must have $\alpha_i - \alpha_j = 0$ so $\alpha_i = \alpha_j$. Thus, f has multiple roots in its splitting field and is thus non-seperable if and only if $\operatorname{Disc}(f) = 0$. □

Corollary 4.0.18. Let $\operatorname{char} K = 0$, if $\operatorname{Disc}(f) = 0$ then f is not irreducible.

Proof. Suppose that $\operatorname{Disc}(f) = 0$ then f must be non-seperable but because $\operatorname{char} K = 0$ every irreducible polynomial over K is seperable so f is not irreducible. □

Definition 4.0.19. For $\sigma \in \operatorname{Gal}(E/K)$ embdded in S_n, define $\operatorname{sgn} : \operatorname{Gal}(E/K) \to \{\pm 1\}$ where $\operatorname{sgn}(\sigma)$ is the sign of the permutation defined by σ acting on the n roots.

Lemma 4.0.20. Let $\sigma \in \operatorname{Gal}(E/K)$ then $\sigma(d) = d \cdot \operatorname{sgn}(\sigma)$ where $d = \prod\limits_{i<j}(\alpha_i - \alpha_j)$

Theorem 4.0.21. Let $f \in K[X]$ with $\deg f = n$ and $\operatorname{char} K = 0$ and $\Delta = \operatorname{Disc}(f) \neq 0$. Suppose that E is the splitting field of f over K. Now, $\operatorname{Gal}(E/K)$ is embedded in A_n if and only if Δ is a square in K.

Proof. $\pm d \in E$ are the only square roots of Δ (since $X^2 - \Delta$ has exactly two solutions) therefore if Δ is a square in K then $d \in K$. However, K is fixed by every Galois automorphism so $\sigma(d) = d$. Since $d \neq 0$, $\operatorname{sgn}(\sigma) = 1$ because $\sigma(d) = d \cdot \operatorname{sgn}(\sigma)$. Therefore, $\sigma \in A_n$. Conversely, if $\operatorname{Gal}(E/K) \hookrightarrow A_n$ then every $\sigma \in \operatorname{Gal}(E/K)$ satisfies $\operatorname{sgn}(\sigma) = 1$. □

4.1 Candano's Formula

Theorem 4.1.1. Let K have characteristic 0 then if $f \in K[X]$ is $f(X) = X^3 + px + q$ then

Proof. □

4.2 Cyclic Extensions

Definition 4.2.1. Let K be a field, then $\mu_n(K) = \{\alpha \in K \mid \alpha^n = 1\}$.

Proposition 4.2.2. Let $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ which is coprime with n then if $f(X) = X^n - 1$ splits in K then $|\mu_n(K)| = n$.

Proof. In this case, $f'(X) = nX^{n-1} \neq 0$ because $n \notin (p)$. Thus, f has no double roots in K but f splits in K so it has exactly n roots. Therefore, $|\mu_n(K)| = n$. $\square$

Proposition 4.2.3. $\mu_n(K)$ is a cyclic group under multiplication. Its generators are the *primitive* n^{th} roots of unity.

Proof. Take $\alpha, \beta \in \mu_n(K)$ then $(\alpha\beta)^n = \alpha^n\beta^n = 1$ thus $\alpha\beta \in \mu_n(K)$. Futhermore, since $\alpha^n = 1$ then $\alpha \neq 0$ therefore $\alpha^{-1} \in K$ and $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1$ so $\alpha^{-1} \in \mu_n(K)$. Lastly, $1^n = 1$ so $1 \in \mu_n(K)$. Therefore, $\mu_n(K)$ is a finite subgroup of $K^\times$ so $\mu_(K)$ is cyclic. $\square$

Proposition 4.2.4. If $|\mu_n(K)| = n$ and $m \mid n$ then $|\mu_m(K)| = m$.

Proof. Since $\mu_n(K)$ is cyclic and $m \mid n$ there is a unique subgroup $H < \mu_n(K)$ of order m. By Lagrange, $\forall h \in H : h^m = 1$ so $H \subset \mu_m(K)$. Therefore, $|\mu_m(K)| \geq m$ however, by the maximum number of roots of a polynomial, $|\mu_m(K)| \leq m$ so $|\mu_m(K)| = m$. $\square$

Definition 4.2.5. E/K is a cyclic extension if it is Galois and $\operatorname{Gal}(E/K)$ is a cyclic group.

Lemma 4.2.6. Let G be a group and K a field. Let $\phi_1, \dots, \phi_n : G \to K^\times$ be distinct homomorphisms then $\forall \lambda_1, \dots, \lambda_n \in K$ not all zero, the map $\lambda_1\phi_1 + \cdots + \lambda_n\phi_n : G \to K$ is not identically zero.

Proof. Suppose that n is the least positive $n \in \mathbb{Z}^+$ such that $\exists \lambda_1, \dots, \lambda_n \in K$ not all zero such that the map $\lambda_1\phi_1 + \cdots + \lambda_n\phi_n : G \to K$ is identically zero. However, because n is minimal, every $\lambda_i \neq 0$ since if $\lambda_1\phi_1 + \cdots + \lambda_n\phi_n = 0$ then $\lambda_1\phi_1 + \cdots + \lambda_{i-1}\phi_{i-1} + \lambda_{i+1}\phi_{i+1} + \cdots + \lambda_n\phi_n = 0$ so we have a smaller counterexample. Since $\phi_1 \neq \phi_2$ then $\exists g \in G : \phi_1(g) \neq \phi_2(g)$. Then, $\forall x \in G$,

$$\lambda_1\phi_1(gx) + \cdots + \lambda_n\phi_(gx) = \lambda_1\phi_1(g)\phi_1(x) + \cdots + \lambda_n\phi_n(g)\phi_n(x) = 0$$

but also,

$$\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x) = 0 \implies \phi_1(g)(\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x)) = 0$$

Therefore, subtracting the expressions,

$$\lambda_1(\phi_1(g) - \phi_1(g))\phi_1(x) + \lambda_2(\phi_2(g) - \phi_1(g))\phi_2(x) + \cdots + \lambda_n(\phi_n(g) - \phi_2(g))\phi_1(x) = 0$$

so define $\mu_i = \lambda_i(\phi_i(g) - \phi_1(g))$ then $\mu_1 = 0$ but $\mu_2 \neq 0$ because $\lambda_2 \neq 0$ and $\phi_1(g) \neq \phi_2(g)$. Thus, for any $x \in G$,

$$\mu_2\phi_2(x) + \cdots + \mu_n\phi_n(x) = 0$$

where not all μ_i are zero. Thus, we have found a counterexample of size $n - 1$ contradicting the minimality of n. $\square$

Theorem 4.2.7. If $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ is coprime to n and $|\mu_n(K)| = n$ then,

(a) If E/K is cyclic of degree n then $\exists \alpha \in E$ such that $E = K(\alpha)$ and $\alpha^n \in K$.

(b) If $E = K(\alpha)$ where $\alpha \in E$ such that $\alpha^n \in K$, where m is the least positive integer such that this holds, then E/K is cyclic of degree m.

Proof. Suppose that E/K is cyclic then let $\sigma \in \mathrm{Gal}\,(E/K)$ be a generator. Let $\omega \in \mu_n(K)$ be a primitive n^{th} root of unity. Applying Dedekind's Lemma to the set of homomorphisms,

$$\phi_1 = \sigma, \phi_2 = \sigma^2, \dots, \phi_{n-1} = \sigma^{n-1}, \phi_n = \sigma^n = \mathrm{id} : E^\times \to E^\times$$

Also, take the element,

$$\lambda_1 = \omega, \lambda_2 = \omega^2, \dots, \lambda^n = \omega^n = 1$$

Then, the map $\phi = \sum\limits_{i=1}^{n} \lambda_i \phi_i = \sum\limits_{i=1}^{n} \omega^i \sigma^i : E^\times \to E$ is not the zero map. Therefore, $\exists \beta \in E^\times$ such that $\alpha = \phi(\beta) = \omega\sigma(\beta) + \omega^2\sigma^2(\beta) + \cdots + \omega^n\sigma^n(\beta) \neq 0$. Now, consider,

$$\sigma(\alpha) = \omega\sigma^2(\beta) + \omega\sigma^3(\beta) + \cdots + \omega^n\sigma^{n+1}(\beta) = \sigma(\beta) + \omega\sigma^2(\beta) + \cdots + \omega^{n-1}\sigma^n(\beta) = \omega^{-1}\alpha$$

Therefore, $\sigma(\alpha^n) = \sigma(\alpha)^n = \omega^{-n}\alpha^n = \alpha^n$. Because σ generates $\mathrm{Gal}\,(E/K)$ we have that α^n is fixed under every Galois automorphism so $\alpha^n \in K$. Futhermore, $\sigma^i(\alpha) = \omega^{-i}\alpha$ which are all distinct because ω is primitive and $\alpha \neq 0$ so if $\omega^i\alpha = \omega^j\alpha$ then $\omega^{i-j} = 1$ which means $n \mid i - j$ so $i = j$ because both are reduced modulo n. Therefore, $\mathrm{Min}(\alpha; K)$ has n distinct roots in E so $\deg \alpha \geq n$ but

$$[E : K] = [E : K(\alpha)][K(\alpha) : K] \geq n[E : K(\alpha)]$$

which implies that $[E : K(\alpha)] = 1$ since $[E : K] = n$. Therefore, $E = K(\alpha)$.

Suppose that $E = K(\alpha)$ and m is the least positive integer such that $\alpha^m \in K$. Then $m \mid n$ and take $b = \alpha^n \in K$. Then, α is a root of the polynomial $f(X) = X^m - b \in K[X]$. Let $\zeta = \omega^{n/m}$ which is a primitve m^{th} root of unity in K and then $f(X) = (X - \alpha)(X - \zeta\alpha) \cdots (X - \zeta^{m-1}\alpha)$ so $E = K(\alpha)$ is the splitting field of f which is therefore seperable because ζ is primitive. Therefore, E/K is a Galois extension. Consider the map $\phi : \mathrm{Gal}\,(E/K) \to \langle \zeta \rangle \subset K^\times$ given by $\phi : \sigma \mapsto \sigma(\alpha)\alpha^{-1}$ which is a power of ζ because σ maps α to a root of f which is of the form $\zeta^i\alpha$. Also,

$$\phi(\sigma\tau) = \sigma \circ \tau(\alpha)\alpha^{-1} = \sigma(\alpha\tau(\alpha)\alpha^{-1})\alpha^{-1} = \sigma(\alpha\phi(\tau))\alpha^{-1} = \sigma(\alpha)\alpha^{-1}\sigma(\phi(\tau)) = \phi(\sigma)\phi(\tau)$$

because $\phi(\tau) \in K$ and is thus fixed by the Galois group. Furthermore, if $\phi(\sigma) = 1$ then $\sigma(\alpha) = \alpha$ so $\sigma(\zeta^i\alpha) = \zeta^i\alpha$ so σ acts trivially on the roots of f. Therefore, $\sigma = \mathrm{id}$ because E is the splitting field of f. Thus, ϕ is injective so the Galois group is embedded in $\langle \zeta \rangle \cong C_m$. ☐

Definition 4.2.8. A finite extension E/K is solvable if $E = K(\alpha_1, \dots, \alpha_n)$ such that $\forall i$, $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$. E/K is N-solvable if $n_i \mid N$ for each i.

Definition 4.2.9. The normal closure E' of E/K is the splitting field of α_i for all i.

Proposition 4.2.10. If E/K is solvable then its normal closure is also solvable.

Proposition 4.2.11. If $K \subset K' \subset E$ and E/K is solvable then E/K' is also solvable.

Definition 4.2.12. A polynomial $f \in K[X]$ is solvable if its splitting field over K is contained in a solvable extension of K.

Definition 4.2.13. A finite group G is solvable if there is a tower $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{e\}$ such that for each i the factor group G_i/G_{i+1} is abelian.

Lemma 4.2.14. A finite group G is solvable if and only if there is a tower $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = \{e\}$ such that for each i the factor group G_i/G_{i+1} is cyclic.

Theorem 4.2.15 (Galois)**.** $f \in K[X]$ is solvable if and only if $\mathrm{Gal}\,(E/K)$ is solvable where E is the splitting field of f and $\mathrm{char}\, K = 0$.

Proof. Let $f \in K[X]$ be solvable and let E be the splitting field of f over K. Then, there exists a solvable extension F of K such that $K \subset E \subset F$. Let N be the lcm of the degrees of the extensions from K to F so F is N-solvable over K. Now let ω be a primitive n^{th} root of unity. Because $\omega^N = 1 \in E$ then the extension $F(\omega)$ is N-solvable over K. Finally, let L be the normal closure of $F(\omega)$ which is still solvable over K. Futhermore because $K \subset K(\omega) \subset L$ then L is solvable over $K(\omega)$.

$$\begin{tikzcd}
L \arrow[d, dash] & \\
F(\omega) \arrow[d, dash] \arrow[ddr, dash] & \\
F \arrow[d, dash] & \\
E \arrow[d, dash] & K(\omega) \arrow[dl, dash] \\
K &
\end{tikzcd}$$

Because $L/K(\omega)$ is solvable, there exists $K \subset K(\omega) = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_k = L$ such that $L_{i+1} = L_i(\alpha_i)$ such that $\alpha_i^N \in L_i$. Because $\omega \in L_i$ and $\mathrm{char}\, L_i = 0$, by the main theorem on cyclic extensons, L_{i+1}/L_i is a cyclic extension. This holds because ω is a primitive root so $|\mu_N(L_i)| = N$. Futhermore, $K(\omega)/K$ is a cyclotomic extension and thus abelian. Now, by the Galois correspondence, the chain,

$$K \subset K(\omega) \subset L_1 \subset L_2 \subset \cdots \subset L_k = L$$

corresponds to the subgroups,

$$\mathrm{Gal}\,(L/K) \supset \mathrm{Gal}\,(L/K(\omega)) \supset \mathrm{Gal}\,(L/L_1) \supset \cdots \supset \mathrm{Gal}\,(L/L_{k-1}) \supset \mathrm{Gal}\,(L/L_k) = \{e\}$$

however, each extension is Galois and therefore, each group is a normal subgroup of the previous. Furthermore, $\mathrm{Gal}\,(L_{i+1}/L_i) \cong \mathrm{Gal}\,(L/L_i)\,/\mathrm{Gal}\,(L/L_{i+1})$ but L_{i+1}/L_i is a cyclic extension so these quotient groups are cyclic. Likewise, $K(\omega)/K$ is an abelian extension and thus Galois so $\mathrm{Gal}\,(K(\omega)/K) \cong \mathrm{Gal}\,(L/K)\,/\mathrm{Gal}\,(L/K(\omega))$ but $\mathrm{Gal}\,(K(\omega)/K)$ is abelian so the quotient is also abelian. Therefore, this is a solvable series for $\mathrm{Gal}\,(L/K)$. Therefore, because E/K is Galois, then,

$$\mathrm{Gal}\,(E/K) \cong \mathrm{Gal}\,(L/K)\,/\mathrm{Gal}\,(L/E)$$

which is a quotient group of a solvable group and therefore solvable.

Conversely, let E be the splitting field of $f \in K[X]$ and suppose that $\mathrm{Gal}\,(E/K)$ is solvable. Let L be the normal closure of $E(\omega)$ where ω is a primitve N^{th} root of unity. Consider $L/K(\omega)$ and define the map,

$$\psi : \mathrm{Gal}\,(L/K(\omega)) \subset \mathrm{Gal}\,(L/K) \to \mathrm{Gal}\,(E/K) = G$$
$$\psi : \sigma \mapsto \sigma|_E$$

Now, L is the splitting field of f over $K(\omega)$ so if $\sigma \in \mathrm{Gal}\,(L/K(\omega))$ then σ is determined by its action on the roots of f. However, all the roots of f are contained in E so σ is determined by its action of E. Therfore, ψ is an injective map. Thus, $\mathrm{Gal}\,(L/K(\omega))$ is embedded in $\mathrm{Gal}\,(E/K) = G$ a solvable group. Therefore, $\mathrm{Gal}\,(L/K(\omega))$ is also solvable. By the lemma, $\mathrm{Gal}\,(L/K(\omega))$ admits a normal series with cyclic factors,

$$G = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_0 = \{e\}$$

By the Galois correspondence, we obtain a tower of subextensions,

$$K(\omega) = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_k = L$$

such that each extension is cyclic. Because $K(\omega) \subset L_i$ then $\omega \in L_i$ and $[L_{i+1}/L_i] = n$ where $n \mid N$ so $|\mu_n(L_i)| = n$. Therefore, by the main theorem on cyclic extensions, $L_{i+1} = L_i(\alpha_i)$ such that $\alpha_i^n \in L_i$. Therefore, L is solvable over $K(\omega)$ and thus solvable over K because $\omega^N = 1 \in K$. Therefore, f is solvable because $E \subset L$ where L/K is a solvable extension. $\square$

Corollary 4.2.16.