Nun kommen wir zum zentralen Erweiterungssatz:

Thm II.17 (Rotman Thm 3.7)

Mit den Notationen der Prop. II.16:

(1) Sei f separabel. Dann gibt es genau $[E:k]$ Isomorphismen

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E_* \\ \uparrow & & \uparrow \\ k & \xrightarrow{\varphi} & k' \end{array}$$

die φ erweitern.

(2) Sei E/k der Zerfällungskörper eines separablen Polynoms. Dann gilt:

$$|Gal(E/k)| = [E:k].$$

Beweis: (1) Induktion über $[E:k]$.

(a) Falls $[E:k]=1$ zerfällt f in lineare Faktoren in $k[x]$; das selbe gilt für $f^{\varphi(b)}$, somit $[E_*:k']=1$ und $\Phi = \varphi$.

(b) Vorbereitende Bemerkung: die Abbildung

$\varphi_x : k[X] \to k'[X]$, $\varphi_x(a_n X^n + \dots + a_0) =$

$= \varphi(a_n) X^n + \dots + \varphi(a_0)$ ist ein Ring isomorphismus, insb. $\varphi_x(1) = 1$; zudem gilt $\deg(h) = \deg(\varphi_x(h))$ $\forall h \in k[X]$. Daraus folgt $\varphi_x(ggT(h_1, h_2)) = ggT(\varphi_x(h_1), \varphi_x(h_2))$.

Falls h' die Ableitung von h bezeichnet folgt aus der Eigenschaft $\varphi(m\beta) = m\varphi(\beta)$ $\forall m \in \mathbb{Z}$, $\forall \beta \in k$, dass $\varphi_x(h') = \varphi_x(h)'$.

Also $\varphi_x(ggT(h, h')) = ggT(\varphi_x(h), \varphi_x(h)')$

insbesondere hat h keine mehrfachen Nullstellen $\iff$ $\varphi_x(h)$ hat keine mehrfachen Nullstellen.

Falls $f = p_1 \cdot \dots \cdot p_r$ eine Zerlegung in irreduzible Faktoren bezeichnet so gilt dasselbe für $f_x = \varphi_x(f) = \varphi_x(p_1) \cdot \dots \cdot \varphi_x(p_r)$; insbesondere ist f_x separabel falls f separabel.

(c) Sei nun $[E : k] > 1$: dann gibt es $p \in k[X]$ irreduzibel mit $d := \deg(p) > 1$ und p dividiert f: $f = p \cdot g$, $g \in k[X]$.

Dann folgt $f_x = \varphi_x(f) = \underbrace{\varphi_x(p)}_{p_x} \underbrace{\varphi_x(g)}_{g_x}$.

Da f separabel ist folgt aus (2) f_* und somit p_* separabel. Zudem ist p_* irreduzibel mit $\deg(p_*) = \deg(p) = d$. Seien $\alpha_1^*, \ldots, \alpha_d^*$ die Nullstellen von p_*; alle in E_* enthalten.

Sei $\alpha \in R(p) \subset E$. Aus Lemma 2.15 folgt, dass es für jede Nullstelle α_i^* einen Isomorphismus gibt

$$\hat{\varphi}_i : k(\alpha) \longrightarrow k'(\alpha_i^*) \subset E_*$$

mit $\hat{\varphi}_i(\alpha) = \alpha_i^*$, der $\varphi : k \to k'$ erweitert.

Sei $\alpha' = \alpha_i^*$, $\hat{\varphi} = \hat{\varphi}_i$. Dann ist $f \in k(\alpha)[X]$ und E ist offensichtlich ein Zerfällungskörper von $f \in k(\alpha)[X]$; $f_* = (\hat{\varphi})_*(f) \in k'(\alpha^*)[X]$ und E_* ist Zerfällungskörper von $f_* \in k'(\alpha^*)[X]$.

Zudem ist $f \in k(\alpha_1)[x]$ wieder symmetrisch.

Da nun

$$[E : k(\alpha_1)] = [E : k]/_d < [E : k]$$

folgt aus der Induktionshypothese, dass

$$\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha^*)$$

$$[E : k(\alpha_1)] = [E : k]/_d \quad \text{Erweiterungen}$$

$$E \longrightarrow E_*$$

besitzt. Somit besitzt $\varphi : k \to k'$

mindestens $[E : k(\alpha_1)] \cdot d = [E : k]$

Erweiterungen.

Andererseits: Falls $\tilde{\varphi} : E \longrightarrow E_*$

den Isomorphismus $\varphi : k \to k'$

Erweitert und $\alpha \in R(p)$ dann ist

$\tilde{\varphi}(\alpha) \in R(p_*)$ d.h. $\tilde{\varphi}(\alpha_i) = \alpha_i^*$

für ein i und somit ist

$$\tilde{\varphi}\big|_{k(\alpha)} : k(\alpha) \longrightarrow k'(\alpha_i^*)$$

eine der Erweiterungen φ_i'; somit hat φ höchstens d. $[E:k(\alpha_1)] = [E:k]$ Erweiterungen.

(2) $k = k'$, $\varphi = id_k$. Dann ist $Gal(E/k)$ genau die Menge der Erweiterungen von $id: k \to k$ auf $E \to E$ und somit $|Gal(E|k)| = [E:k]$.

□

Bemerkung: Die grössen $[E:k]$ und $|Gal(E|k)|$ sind in der Praxis aus verschiedenen Gründen schwer zu berechnen. Die Beziehung $[E:k] = |Gal(E|k)|$ gibt darum nicht triviale Information wie folgendes Korollar zeigt.

Korollar II.18 (siehe Rotman 3.9)

Sei E/k der Zerfällungskörper eines separablen Polynom $f \in k[X]$ vom Grad $n = \deg(f)$. Falls f irreduzibel so folgt

$$n \mid |Gal(E(k)|.$$

Beweis: Sei $\alpha \in R(f) \subset E$. Da f irreduzibel folgt $[k(\alpha):k] = n$ woraus mit Satz II.17:

$$|Gal(E|k)| = [E:k] = [E:k(\alpha)][k(\alpha):k]$$

und $n \mid |Gal(E/k)|$ folgt.

∎

Wir werden später sehen wie man die Information $n \mid |Gal(E|k)|$ in Verbindung mit Gruppentheorie dazu benützen kann um $Gal(E|k)$ in spezifischen Fällen zu bestimmen.

Hier ist eine Anwendung von §II.17 auf endliche Körper:

Thm 2.19 (Rotman Thm 3.13)

Sei p eine Primzahl und $n \in \mathbb{N}$, $n \geq 1$. Dann ist

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

und ein erzeugendes Element ist der Frobenius automorphismus

$$\mathrm{Fr}: \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$
$$x \longmapsto x^p.$$

Hier bezeichnet $\mathbb{Z}/n\mathbb{Z}$ die zyklische Gruppe der Ordnung n.

Beweis:

(1) $\mathbb{F}_{p^n}$ ist ein Zerfällungskörper von $X^{p^n-1}-1 \in \mathbb{F}_p[X]$: Die multiplikative Gruppe $\mathbb{F}_{p^n}^\times$ hat Ordnung p^n-1, insbesondere

$$\xi^{p^n-1} = 1 \qquad \forall \xi \in \mathbb{F}_{p^n}^\times$$

also ist $\mathbb{F}_{p^n}^\times$ die Menge der Nullstellen von $X^{p^n-1}-1$.

(2) $\dim(\mathbb{F}_{p^n} / \mathbb{F}_p) = n$ und $X^{p^n-1}-1$ ist separabel, somit folgt aus Thm 3.8:

$$|Gal(\mathbb{F}_{p^n} | \mathbb{F}_p)| = n.$$

(3) Offensichtlich gilt $Fr \in Gal(\mathbb{F}_{p^n} | \mathbb{F}_p)$.

Wir zeigen, dass Fr Ordnung n besitzt.

$Fr^k = id \Leftrightarrow k$ ist die Ordnung von Fr.

bezeichnet, dann gilt

$$Fr^k = Id_{\mathbb{F}_{p^n}}$$

Aber $Fr^k(x) = x^{p^k}$ und somit

ist jedes $x \in \mathbb{F}_{p^n}$ Nullstelle von $X^{p^k} - X$

Woraus $p^n \leq p^k$ und somit $k = n$ folgt.

□

Nun wenden wir uns einer Familie von Polynomen zu deren Galois Gruppe so gross wie möglich ist.

Thm 2.20 Sei p eine Primzahl und $f \in \mathbb{Q}[X]$ ein Polynom mit $deg(f) = p$ und Zerfällungskörper E. Annahme:

(1) f ist irreduzibel.

(2) f hat genau $p-2$ reelle Nullstellen.

Dann folgt $Gal(E/\mathbb{Q}) \cong S_p$.

Aus Korollar 2.18 folgt $p \mid |\mathrm{Gal}(E/\mathbb{Q})|$.

Dies impliziert im allgemeinen folgendes:

Lemma 2.21. (Cauchy) *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Dann enthält G ein Element der Ordnung p.*

Beweis:

Wir betrachten $\Gamma_p = \{(g_1, \dots, g_p) \in G^p : g_1 \cdot \dots \cdot g_p = e\}$.

Die symmetrische Gruppe S_p wirkt auf G^p via:

$$\eta_\sigma(g_1, \dots, g_p) = (g_{\sigma(1)}, \dots, g_{\sigma(p)})$$

Sei $\sigma = (1, 2, \dots, p)$ der p-Zyklus:

$$\begin{matrix} 1 & 2 & \cdots & p \\ 2 & 3 & \cdots & 1 \end{matrix}$$

und $C_p = \{\mathrm{id} = \sigma^0, \sigma, \sigma^2, \dots, \sigma^{p-1}\}$

die durch σ erzeugte zyklische Gruppe:

sie hat Ordnung p. Wir behaupten, dass die Wirkung von C_p auf G^p die Teilmenge Γ_p erhält: in der Tat aus

$$g_1 \cdot g_2 \cdot g_3 \cdots \cdot g_p = e$$

folgt

$$\underbrace{g_1^{-1}(g_1 \cdots g_p) g_1}_{g_2 \cdot g_3 \cdots \cdot g_p \cdot g_1} = e$$

und somit

$$\tau_*(g_1, \ldots, g_p) \in \Gamma_p$$

falls $(g_1, \ldots, g_p) \in \Gamma_p$.

Daraus folgt, dass Γ_p disjunkte Vereinigung der C_p-Bahnen in Γ_p ist; da p Primzahl ist die Kardinalität einer solchen Bahn 1 oder p. ∎

$$\Gamma_p = \bigcup_{i \in I} \quad \bigcup_{j \in J_i}$$

Sei jetzt I die Menge der Bahnen der ~~Ordnung~~ Kardinalität 1 und J die der Kardinalität p. Dann ist:

$$\Gamma_p = \bigsqcup_{i \in I} \mathcal{O}_i \quad \bigsqcup \bigsqcup_{j \in J} \mathcal{O}_j.$$

wobei $\bigsqcup$ angibt, dass die Vereinigung disjunkt ist. Somit:

$$|\Gamma_p| = |I| + |J| \cdot p \quad . \quad (*)$$

Nun bemerken wir:

(1) $|\Gamma_p| = |G|^{p-1}$, folglich teilt p die Kardinalität $|\Gamma_p|$ von Γ_p.

(2) $|I| \geq 1$ denn $(e, \dots, e) \in \Gamma_p$ ist eine Bahn mit Kardinalität 1.

Aus $(*)$ folgt dann p teilt $|I|$ insbesondere $|I| \geq 2$.

Es gibt also $h \neq e$ mit $(h, \dots, h) \in T_p$
d.h. $h^p = e$. Folglich hat h Ordnung p.

□

Beweis von Thm 2.20.

Sei $\mathbb{Q} \subset E \subset \mathbb{C}$ ein in $\mathbb{C}$ enthaltener Zerfällungskörper von f und

$$R(f) = \{\alpha_1, \dots, \alpha_n\}$$

die Nullstellen von f geordnet so dass $\{\alpha_3, \alpha_4, \dots, \alpha_p\} \subset \mathbb{R}$.

Da f reelle Koeffizienten in $\mathbb{Q} \subset \mathbb{R}$ hat folgt

$$\alpha_2 = \overline{\alpha_1}$$

wobei $\varepsilon : z \mapsto \overline{z}$ komplexe Konjugation von $\mathbb{C}$ bezeichnet.

Mithilfe Lemma II.7 können wir

Gal(E/ℚ) mit einer Untergruppe von

$$S_{\mathcal{R}(f)} = S_p$$

identifizieren.

Beachte, dass $\varepsilon(\alpha_i) = \alpha_i \quad 3 \leq i \leq p$

$$\varepsilon(\alpha_1) = \alpha_2$$

$$\varepsilon(\alpha_2) = \alpha_1$$

und da $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$

folgt $\varepsilon(E) = E$.

Folglich ist $\varepsilon|_E \in Gal(E/\mathbb{Q})$ und

entspricht der Transposition (12).

Andererseits folgt aus Korollar 2.18, dass

$$p \mid |Gal(E/\mathbb{Q})|$$

und folglich (Lemma II.2.1) enthält

Gal(E/ℚ) ein Element η der Ordnung p.

Dann ist η ein p-Cykel und da

p Primzahl folgt daß ein p-Cykel und

eine Transposition σ_p ergeben. ∎