Wir behandeln nun einige mehr oder weniger direkte Konsequenzen der Galois Korrespondenz. Die einfachste ist:

Korollar IV. 18 Eine (endliche) Galois Erweiterung hat nur endlich viele Zwischenkörper.

Beweis: Für eine endliche Galois Erweiterung E/k ist die Menge $\mathrm{Int}(E/k)$ in bijektion mit der Menge $\mathrm{Sub}(\mathrm{Gal}(E/k))$, also endlich. □

Eine weitere interessante Eigenschaft von Körpererweiterungen ist:

Def. IV. 19 Eine Erweiterung $E|k$ ist einfach falls es $u \in E$ gibt mit $E = k(u)$.

Folgendes Resultat impliziert dann unmittelbar, dass Galois Erweiterungen immer einfach sind:

Prop. IV. 20 Eine endliche Erweiterung $E|k$ ist genau dann einfach falls es nur endlich viele Zwischenkörper gibt.

Beweis: ($\Longrightarrow$): Sei $E = k(x)$ und

$$k \subset F \subset E$$

ein Zwischenkörper. Sei

$$f_F(T) := \operatorname{irr}(x, F)(T) \in F[T]$$

$$= T^n + a_{n-1} T^{n-1} + \cdots + a_0$$

das Minimalpolynom von α bez. F.

Sei $F_0 := k(a_{n-1}, \ldots, a_0) \subset F$.

Das Polynom f_F ist irreduzibel über F und daher auch über F_0. Es folgt:

$$[E : F] = [F(\alpha) : F] = n$$

$$[E : F_0] = [F_0(\alpha) : F_0] = n$$

woraus $F_0 = F$ folgt. Nun ist $f_F = \mathrm{irr}(\alpha, F)$ ein Faktor von $\mathrm{irr}(\alpha, k)$, und daraus folgt, dass die Anzahl Zwischenkörper durch die Anzahl von Faktoren von $\mathrm{irr}(\alpha, k) \in E[T]$ beschränkt ist.

($\Leftarrow$) k endlich: $k = \mathbb{F}_q$, $E = \mathbb{F}_{q^n}$ und $E = k(w)$ wobei w ein Erzeugender ist von $\mathbb{F}_{q^n}^{\times}$.

k unendlich: nach Satz 8 Übung 4 gibt es $x \in E$, das nicht in der Vereinigung der echten Zwischenkörper von E/k enthalten ist, woraus $E = k(x)$ folgt. $\square$

In Körpertheorie spielen neben den normalen Erweiterungen, die separablen eine wichtige Rolle. Sei E/k eine Körpererweiterung:

Def. IV.21: (1) $\alpha \in E$ ist separabel (über k) falls entweder α transzendent oder $\mathrm{irr}(\alpha, k)$ separabel ist.

(2) Die Erweiterung E/k ist separabel falls jedes $\alpha \in E$ über k separabel ist.

Bemerkung IV.22: (1) Eine endliche Erweiterung E/k ist genau dann Galois falls sie normal und separabel ist.

(2) Falls $\mathrm{char}\, k = 0$ ist jede Erweiterung E/k separabel.

Korollar IV.23: Eine endliche separable Erweiterung ist einfach.

Beweis: Sei B/k endlich; dann gibt es $u_1, \dots, u_t \in B$ mit $B = k(u_1, \dots, u_t)$. Da jedes $u_1, \dots, u_t$ separabel ist, so ist $f = \prod_{j=1}^{\tilde{}} \mathrm{irr}(u_j, k)$. Dann ist

B im Zerfällungskörper E von f enthalten. Da E/k Galois ist, folgt insbesondere, dass es nur endlich viele Zwischenkörper von B/k gibt und somit ist nach Prop IV.20 B einfach. □

Unser nächstes Ziel ist zu zeigen, dass in Charakteristik null die Umkehrung des Satzes von Galois (Thm 3.14) gilt. Nämlich

Thm IV.24 Sei E/k eine (endliche) Galois Erweiterung wobei $\mathrm{char}\, k = 0$.

Falls $\mathrm{Gal}(E/k)$ auflösbar ist, so ist E in einer radikalen Erweiterung von k enthalten.

Ein wichtiger Zwischenschritt ist:

Lemma IV.25 Sei E/k eine Galois Erweiterung mit $p := [E:k]$ Primzahl. Falls k eine p-te Wurzel w von 1 mit $w \neq 1$ enthält, so gibt es $z \in E$ mit $E = k(z)$ und $z^p \in k$.

Beweis: $Gal(E/k)$ ist zyklisch der Ordnung p; sei $\sigma \in Gal(E/k)$ ein Erzeugender. Wir betrachten $\sigma : E \to E$ als k-lineare Abbildung und bemerken $\sigma^p = Id$; ausserdem gibt es kein Polynom $P \in k[X]$ mit $\operatorname{grad} P \leq p-1$ und $P \neq 0$ mit $P(\sigma) = 0$ da dies die lineare Unabhängigkeit von

$$1, \sigma, \dots, \sigma^{p-1} \in \operatorname{Hom}(E^\times, E^\times)$$

widersprechen würde (Prop. IV-5).

Folglich ist $X^p - 1$ das Minimal-

polynom der k-linearen Abbildung

$\sigma : E \to E$, da zudem $[E:k] = p$

ist also $X^p - 1$ das charakteristische

Polynom von σ. Also ist ω ein

Eigenwert von σ, und es gibt $z \in E$

mit $\sigma(z) = \omega \cdot z$.

Da $\omega \neq 1$, folgt $z \in E \setminus k$ und

somit $E = k(z)$. Zudem:

$$\sigma(z^p) = \sigma(z)^p = \omega^p z^p = z^p$$

also ist $z^p \in E^{\mathrm{Gal}(E|k)} = k$.

□

Beweis (Thm IV.24)

Der Beweis ist via Induktion über $[E:k]$. Falls $[E:k]=1$ gibt es nichts zu zeigen. Sei also $[E:k]>1$ und somit $G:=\mathrm{Gal}(E/k)$, $|G|>1$. Da G auflösbar ist gibt es $N \lhd G$ mit Primzahl Index p. Sei k^*/k ein Zerfällungskörper von $X^p-1 \in k[X]$ und $\omega \in k^*$ eine primitive p-te Wurzel von 1, d.h. eine erzeugende der Gruppe $\{\zeta \in k^* : \zeta^p = 1\}$.

Da $\mathrm{char}\, k = 0$ gilt insbesondere $\omega \neq 1$. Wir unterscheiden zwei Fälle:

Fall 1: $\omega \in k$. Dann ist nach Lemma IV.25 E^N eine rane Erweiterung von k von Typ p; E/E^N ist eine Galois Erweiterung mit Galois Gruppe N, daher auflösbar und $[E : E^N] < [E : k]$.

Es gibt also, nach Induktionshypothese, einen Turm

$$K_1 = E^N \subset K_2 \subset \cdots \subset K_t$$

von ranen Erweiterungen mit $K_t \supset E$.

Also ist

$$k \subset K_1 = E^N \subset K_2 \subset \cdots \subset K_t$$

ein Turm von ranen Erweiterungen, K_t ist daher eine radikale Erweiterung von k und $E \subset K_t$.

Fall 2: Sei $E^* = E(w)$; da E/k Zerfällungskörper eines separablen Polynoms $f \in k[x]$ ist, ist E^* Zerfällungskörper von $f(x^{p-1})$ also ist E^*/k Galois.

Betrachte:

$$\begin{array}{ccc} E^* & \supset & k^* \\ \cup & & \cup \\ E & \supset & k. \end{array}$$

Da E/k Galois ist, haben wir einen Restriktions-~~Abbildung~~ Homomorphismus

$$\begin{aligned} Gal(E^*/k^*) &\longrightarrow Gal(E/k) \\ \sigma &\longmapsto \sigma|_E \end{aligned}$$

und da $E^* = E(w)$ ist dieser Homomorphismus injektiv. Also ist $Gal(E^*/k^*)$ auflösbar.

Falls $E^* = k^*$ folgt $E \subset k^*$

und somit ist E in einer reinen, insbesondere radikalen, Erweiterung von k enthalten.

Falls $[E^* : k^*] > 1$, also $|Gal(E^*/k^*)| > 1$ produziert das obige Argument eine Zwischenerweiterung

$$k^* \subset (E^*)^N \subset E^*$$

wobei $(E^*)^N / k^*$ rein vom Primzahltyp.

Aus der Induktionshypothese folgt die Existenz eines Turms:

$$K_1 = (E^*)^N \subset \cdots \subset K_t$$

von reinen Erweiterungen mit $E^* \subset K_t$.

Dann ist:

$$k \subset k^* = k(\omega) \subset (E^*)^N = K_1 \subset \cdots \subset K_t$$

ein Turm von reinen Erweiterungen

mit $K_t \supset E^* \supset E$. ∎