Im nächsten Resultat, das als Grundlage der Galois Korrespondenz dient, spielt Separabilität eine wichtige Rolle.
Hier nochmals die Definitionen (siehe Def. II. 12)

– ein irreduzibles Polynom ist separabel falls es keine mehrfachen Nullstellen besitzt.
– ein Polynom ist separabel falls jeder seiner irreduzibler Faktoren separabel ist.

Theorem IV. 11 Sei E/k eine endliche Erweiterung mit Galois Gruppe $G = Gal(E/k)$.
Folgende Eigenschaften sind equivalent:
(1) E ist Zerfällungskörper eines separablen Polynoms in $k[x]$.

(2) $k = E^G$

(3) Jedes irreduzible Polynom in $k[X]$ mit einer Nullstelle in E zerfällt in E. (E ist separabel und)

Beweis:

(1) $\Rightarrow$ (2) Aus Thm II.17 (2) folgt $[E:k] = |G|$ und aus Prop. IV.9, $[E:E^G] = |G|$. Folglich:

$$[E^G:k] = \frac{[E:k]}{[E:E^G]} = 1.$$

(2) $\Rightarrow$ (3) Sei $p \in k[X]$ irreduzibel und $\alpha \in E$ mit $p(\alpha) = 0$. Definiere:

$$q(X) := \prod_{\sigma \in G/St(\alpha)} (X - \sigma(\alpha))$$

wobei $St(\alpha) := \{\gamma \in G : \gamma(\alpha) = \alpha\}$ den

Stabilisator von α in G bezeichnet.

Dann folgt:

(1) q ist ein unitäres Polynom

(2) q hat keine mehrfachen Nullstellen

(3) $R(q) \subset R(p)$

(4) $q \in E^G[X]$ (siehe Übung 1)

Aus der Voraussetzung $E^G = k$ folgt

$$q \in k[x].$$

~~Also~~ Da q das Polynom p dividiert folgt aus (1), dass $q = p$. Dies zeigt (3).

(3) $\Rightarrow$ (1): Sei $k \subset E' \subset E$ wobei $[E' : k]$ maximal so, dass E' Zerfällungskörper eines separablen Polynoms $g \in k[x]$ ist.

Annahme: $E' \subsetneq E$: sei $\alpha \in E \setminus E'$.

Dann ist $irr(\alpha, k) \in k[X]$ ein irreduzibles Polynom mit einer Nullstelle in E.

Folglich ist $irr(\alpha, k)$ separabel und zerfällt in E. Dann ist:

$$p = g \cdot irr(\alpha, k) \in k[X]$$

ein separables Polynom dessen Zerfällungskörper E'', $E' \subsetneq F'' \subset E$ erfüllt, also ein Widerspruch. □

Def. IV.12 Eine endliche Erweiterung $E|k$ ist eine Galois Erweiterung von k falls E die equivalenten Eigenschaften von Thm IV-11 erfüllt.

Seien nun $k \subset B \subset E$ wobei E/k Galois ist. Im allgemeinen ist B/k nicht Galois, da eine Galois Erweiterung insbesondere normal ist. Andererseits ist E Zerfällungskörper eines separablen Polynoms $f \in k[x]$; da $f \in B[x]$ betrachtet als Polynom mit Koeffizienten in B immer noch separabel ist folgt

Korollar IV.13 Falls $k \subset B \subset E$ und E/k Galois, dann folgt E/B Galois.

Der nächste Resultat gibt uns ein Kriterium wann in obiger Situation B/k Galois ist.

Prop. IV.14 Sei $k \subset B \subset E$ mit E/k Galois. Dann:

B/k is Galois $\iff \sigma(B) = B \quad \forall \sigma \in Gal(E/k)$.

Beweis:

($\Rightarrow$) Falls B/k Galois ist, ist die insbesondere normal, und die Aussage folgt aus Thm II.26.

($\Leftarrow$) Da $\sigma(B) = B$ $\forall \sigma \in Gal(E/k)$ können wir den Homomorphismus

$$Gal(E/k) \longrightarrow Gal(B/k)$$
$$\sigma \longmapsto \sigma|_B$$

definieren. Sei $H < Gal(B/k)$ dessen Bild. Offensichtlich gilt: $k \subset B^{Gal(B/k)} \subset B^H$.
Nun ist aber auch $B^H \subset E^{Gal(E/k)}$, und da E/k eine Galois Erweiterung ist folgt $E^{Gal(E/k)} = k$. Folglich:

$$k \subset B^{Gal(B/k)} \subset B^H \subset k$$

Woraus $k = B^{Gal(B/k)}$ folgt und somit ist B/k Galois. ∎

Nun wenden wir uns der Galois Korrespondenz zu.

Wir definieren, für eine Gruppe G:

$$Sub(G) := \{ H \subset G : H \text{ ist eine Untergruppe von } G \}$$

und für eine Körpererweiterung E/k,

$$Int(E/k) := \{ B \subset E : B \text{ ist ein Unterkörper von } E \text{ mit } B \supset k \},$$

die Menge aller Zwischenkörper von E/k.

Beide Menge $Sub(G)$ und $Int(E/k)$ sind durch Inklusion geordnet.

Thm IV.16. Sei E/k eine (endliche) Galoiserweiterung.

(1) Die Abbildung $\gamma : Sub(Gal(E/k)) \to Int(E/k)$

$$H \longmapsto E^H$$

die einer Untergruppe von $Gal(E|k)$ ihren Fixkörper zuordnet ist eine inklusionsumkehrende Bijektion deren Inverse gegeben ist durch:

$$\delta : Int(E|k) \longrightarrow Gal(E|k)$$
$$B \longmapsto Gal(E|B).$$

(2) $B \in Int(E|k)$ ist genau dann eine Galois Erweiterung von k, falls $Gal(E|B)$ eine normale Untergruppe von $Gal(E|k)$ ist.

In diesem Fall sind $Gal(E|k)/Gal(E|B)$ und $Gal(B|k)$ isomorph.

Beweis:

(1)

γ ist injektiv: Seien H_1, H_2 Untergruppen von $Gal(E/k)$, insbesondere sind es endliche Untergruppen von $Aut(E)$ und dann folgt aus $E^{H_1} = E^{H_2}$ mit Kor. IV-10, dass $H_1 = H_2$.

$\gamma\delta = Id_{Int(E/k)}$:

Sei $B < Int(E/k)$, dann ist $\gamma\delta(B) = \gamma(Gal(E/B)) = E^{Gal(E/B)}$

Aus Kor IV.13 folgt, dass E/B eine Galois-Erweiterung ist und (Thm IV.11) folglich gilt: $E^{Gal(E/B)} = B$.

Dies zeigt, dass γ surjektiv und somit

bijektiv ist.

(2)

Annahme: B/k ist eine Galois Erweiterung.

Dann folgt schon aus Thm II.21, dass $\sigma(B) = B \quad \forall \sigma \in Gal(E/k)$, $Gal(E/B)$ ist der Kern des Restriktionshomomorphismus

$$Gal(E/k) \longrightarrow Gal(B/k)$$
$$\sigma \longmapsto \sigma|_B$$

insbesondere eine normale Untergruppe von $Gal(E/k)$; Jedem induziert dieser Homomorphismus nach Thm II.20 einen Isomorphismus:

$$Gal(E/k) / Gal(E/B) \xrightarrow{\sim} Gal(B/k).$$

Annahme $Gal(E/B) \lhd Gal(E/k)$.

Wir zeigen jetzt, dass $\sigma(B) = B \quad \forall \sigma \in Gal(E/B)$,

und somit (Prop. IV. 14) ist $B|k$ eine Galois Erweiterung.

Seien also $\sigma \in Gal(E|k)$ und $\xi \in B = E^{Gal(E|B)}$.

Dann folgt $\forall h \in Gal(E|B)$:

$$h(\sigma(\xi)) = \sigma(\underbrace{\sigma^{-1} h \sigma}_{\in Gal(E|B)}(\xi)) = \sigma(\xi)$$

folglich $\sigma(\xi) \in E^{Gal(E|B)} = B$.

∎

Beispiel IV.17

Sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und

$\mathbb{C} \supset E \supset \mathbb{Q}$ Zerfällungskörper von f.

Das Polynom $f \in \mathbb{Q}[x]$ ist irreduzibel:

angenommen würde f eine Nullstelle

$\frac{p}{q} \in \mathbb{Q}$ besitzen, mit p und q Teiler-

fremd. Dann folgt $p^3 = 2q^3$ woraus

$2 \mid p$, $8 \mid p^3$ und $4 \mid q^3$ und somit

$2 \mid q$ folgt, ein Widerspruch.

Seien $\beta = \sqrt[3]{2} \in \mathbb{R}$, $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$.

Die Nullstellen von f sind dann:

$$\alpha_1 = \beta, \quad \alpha_2 = \beta\omega, \quad \alpha_3 = \beta\omega^2.$$

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\beta)] \underbrace{[\mathbb{Q}(\beta) : \mathbb{Q}]}_{= 3 \ (f \text{ irreduzibel})}$$

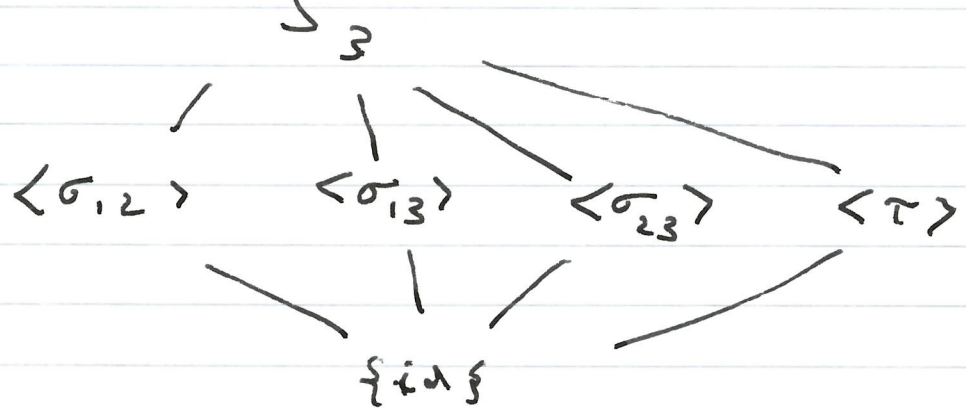
und da $E \not\subset \mathbb{R}$ folgt $[E : \mathbb{Q}(\beta)] \geq 2$

und somit $[E:\mathbb{Q}] \geq 6$. Andererseits geht $Gal(E/\mathbb{Q})$ injektiv nach S_3 woraus $Gal(E/\mathbb{Q}) = S_3$ folgt.

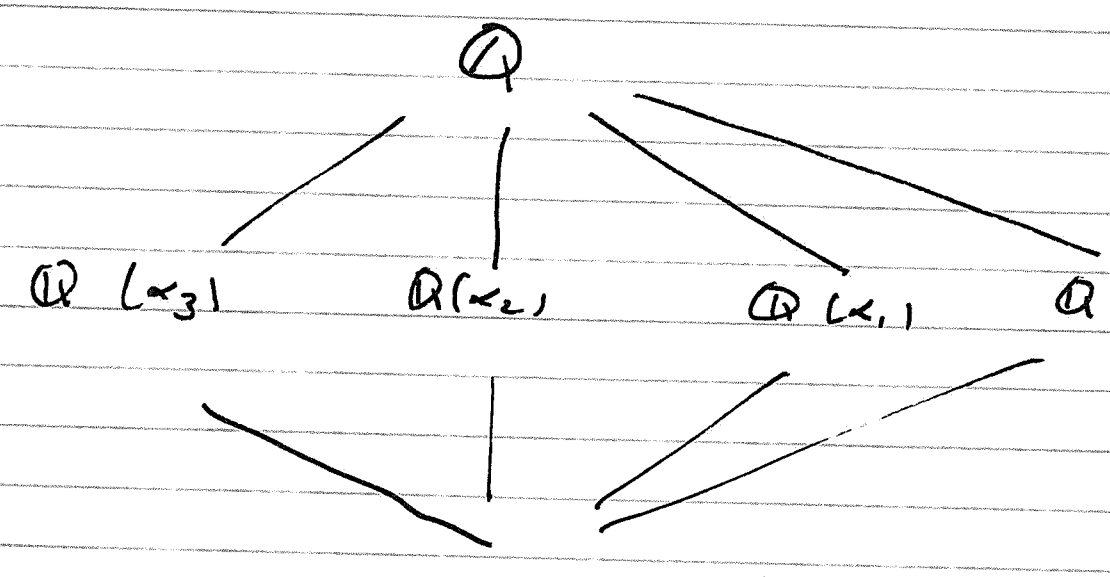
D.h. jede Permutation von $\{\alpha_1, \alpha_2, \alpha_3\}$ wird von einem (eindeutig bestimmten) Element von $Gal(E/\mathbb{Q})$ induziert.

Sei σ_{ij} $(i \neq j)$ die Transposition die α_i und α_j vertauscht, sowie τ die zyklische Permutation $\alpha_1 \to \alpha_2 \to \alpha_3 \to \alpha_1$.

Die Untergruppenstruktur von S_3 ist:



Die Struktur der Zwischenerweiterungen entsprechenden ist dann:



Z.B: $\sigma_{12}(\alpha_3) = \alpha_3$, also $E^{\langle \sigma_{12} \rangle} \supset Q(\alpha_3)$.

Nun ist $[E : E^{\langle \sigma_{12} \rangle}] = 2$ und $[Q(\alpha_3) : Q] = 3$

woraus $E^{\langle \sigma_{12} \rangle} = Q(\alpha_3)$ folgt.

Ein analoges Argument funktioniert für α_2, α_3.

Wir berechnen $\tau(\omega) = \tau\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_2}$

$$= \frac{\beta\omega^2}{\beta\omega} = \omega$$

IV - 28

Also $E \supset \Phi(w) \supset \Phi$. Aus

$[E : E^{\langle\tau\rangle}] = 3$ folgt dann $E^{\langle\tau\rangle} = \Phi(w)$.

□