10.3 Galoiserweiterungen, der Hauptsatz

Kehren wir wieder zu der oben beschriebenen Galoisverbindung (Φ, Γ) zurück. Wir bemerken zunächst, daß gilt:

10.3.1 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Körpererweiterung, dann gilt:*

- *Für jedes* $U \leq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *ist*

$$U = \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U),\ |U| = [\mathbb{L} : \mathbb{L}_U].$$

- $\Gamma \circ \Phi = \mathrm{id}_{\mathrm{U}(\mathrm{Gal}(\mathbb{L}:\mathbb{K}))}$, Γ *ist also surjektiv, und* Φ *ist injektiv.*

Beweis:

i) Trivialerweise ist $U \leq \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U)$, 10.1.6 liefert $|\mathrm{Gal}(\mathbb{L} : \mathbb{L}_U)| \leq [\mathbb{L} : \mathbb{L}_U]$, es gilt also $|U| \leq [\mathbb{L} : \mathbb{L}_U]$. Zum Beweis des ersten Punkts genügt demnach der Beweis von

$$|U| \geq [\mathbb{L} : \mathbb{L}_U],$$

bzw. der Nachweis, daß beliebige $|U| + 1$ Elemente

$$\lambda_0, \ldots, \lambda_{|U|} \in \mathbb{L}$$

über $\mathbb{L}_U$ linear abhängig sind. Zu diesem Zweck betrachten wir eine Gleichung $\sum_i \lambda_i x_i = 0$, mit Koeffizienten $x_i \in \mathbb{L}_U$. Wenden wir auf beiden Seiten $\sigma \in U$ an, so erhalten wir, weil σ jedes $x_i \in \mathbb{L}_U$ fest läßt, das lineare Gleichungssystem

$$\sum_{i=0}^{|U|} \sigma^{-1}(\lambda_i) x_i = 0,\ \sigma \in U.$$

Die Anzahl $|U|$ der Gleichungen ist dabei kleiner als die der Unbestimmten, es gibt also nichttriviale Lösungen

$$(x_0, \ldots, x_{|U|}) \neq 0.$$

Ohne Einschränkung können wir $x_0 \neq 0$ annehmen, denn andernfalls können wir die λ_i ja umnumerieren. Weil es sich bei dieser nichttrivialen Lösung um eine Lösung eines homogenen Gleichungssystems handelt, können wir dieses x_0 sogar beliebig vorgeben.
Das Gleichungssystem ist äquivalent zu dem Gleichungssystem

$$\sum_i \lambda_i \sigma(x_i) = 0,\ \sigma \in U,$$

aus dem wir jetzt, durch Aufsummieren der Gleichungen, die Identität

$$\sum_i \left(\sum_{\sigma \in U} \sigma \right) (x_i) \lambda_i = 0$$

bekommen. Nach dem Satz von Dedekind ist $\sum\sigma \neq 0$, es gibt also geeignete $x_0 \in \mathbb{L}_U$, für die $(\sum\sigma)(x_0) \neq 0$ gilt. Die λ_i sind also tatsächlich linear abhängig über $\mathbb{L}_U$. Das beweist den ersten Punkt.

ii) Zum Nachweis der zweiten Behauptung bemerken wir, daß

$$(\Gamma \circ \Phi)(U) = \Gamma(\Phi(U)) = \Gamma(\mathbb{L}_U) = \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U) = U,$$

letzere Gleichung nach i).

□

Wir kommen damit zur Formulierung einer Bedingung, die gewährleistet, daß Φ und Γ (zueinander inverse) Bijektionen sind:

10.3.2 Definition (Galoiserweiterung) Eine Körpererweiterung $\mathbb{L} : \mathbb{K}$ heißt *Galoiserweiterung,* wenn

$$\mathbb{K} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$$

gilt, d.h. wenn $\mathbb{K}$ der Fixkörper der Galoisgruppe ist. •

Beispielsweise ist $\mathbb{R} : \mathbb{Q}$ *keine* Galoiserweiterung, denn $\mathrm{Aut}(\mathbb{R}) = \{1\}$, wie bereits erwähnt. Dagegen ist $\mathbb{C} : \mathbb{R}$ eine Galoiserweiterung.

Für endliche Erweiterungen $\mathbb{L} : \mathbb{K}$ läßt sich die Bedingung Galoiserweiterung zu sein auch anders formulieren bzw. nachweisen:

10.3.3 Satz *Ist* $[\mathbb{L} : \mathbb{K}] \in \mathbb{N}$, *dann sind äquivalent:*

i) $\mathbb{L} : \mathbb{K}$ *ist Galoiserweiterung,*

ii) $[\mathbb{L} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$,

iii) $\mathbb{L} : \mathbb{K}$ *ist normal und separabel,*

iv) $\mathbb{L}$ *ist Zerfällungskörper eines über* $\mathbb{K}$ *separablen Polynoms.*

Beweis:

i)$\Rightarrow$ ii):

$$[\mathbb{L} : \mathbb{K}] \in \mathbb{N} \Rightarrow_{10.3.1} |\mathrm{Gal}(\mathbb{L} : \mathbb{K})| = [\mathbb{L} : \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}] =_{i)} [\mathbb{L} : \mathbb{K}].$$

ii)$\Rightarrow$ i):

$$[\mathbb{L} : \mathbb{K}] =_{ii)} |\mathrm{Gal}(\mathbb{L} : \mathbb{K})| =_{10.3.1} [\mathbb{L} : \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}] \Rightarrow_{\mathbb{K}\subseteq\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}} \mathbb{K} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}.$$

i)$\Rightarrow$ iii): Sei $\lambda \in \mathbb{L}$. Wir betrachten die Bahn dieses Elements unter der Galoisgruppe:

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K})(\lambda) = \{\lambda = \lambda_0, \ldots, \lambda_{n-1}\},$$

und das normierte Polynom mit diesen Wurzeln:

$$f_\lambda := \prod_{i\in n}(x - \lambda_i) = \sum_{j\in n}\mu_j x^j,\ \mu_j \in \mathbb{L}.$$

Für die Fortsetzung $\tilde{\sigma}$ von σ auf $\mathbb{L}[x]$ gilt

$$\tilde{\sigma}(f_\lambda) = \sum \sigma(\mu_j)x^j = \prod(x - \sigma(\lambda_i)) = f_\lambda,$$

es gilt also $\mu_j = \sigma(\mu_j)$, für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, also, wegen i), $\mu_j \in \mathbb{K}$ und damit $f_\lambda \in \mathbb{K}[x]$. Weil f_λ separabel ist, gilt das auch für λ, die Erweiterung $\mathbb{L} : \mathbb{K}$ ist demnach separabel. Sie ist auch normal: Ist $\{b_0, \ldots, b_{[\mathbb{L}:\mathbb{K}]-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann können wir — analog zu f_λ — die Polynome f_{b_i} betrachten, $\mathbb{L}$ ist Zerfällungskörper von deren Produkt $f = \prod_i f_{b_i}$, die Erweiterung also normal.

iii)$\Rightarrow$ iv) ist klar.

iv)$\Rightarrow$ i): Sei $\mathbb{L}$ Zerfällungskörper von $f \in \mathbb{K}[x]$, f separabel. Die Implikation $\mathbb{K} \subseteq \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$ ist klar, es gilt, die Umkehrung zu beweisen. Wir induzieren nach der Anzahl r der nicht in $\mathbb{K}$ liegenden Wurzeln von f.

I $r = 0$: $\mathbb{K} = \mathbb{L}$ ergibt die Behauptung.

II $r > 0$: Sei $\lambda \notin \mathbb{K}$, aber Wurzel von f. Dann ist $f = f_{\mathbb{K},\lambda} \cdot h$. Wir betrachten $\mathbb{M} := \mathbb{K}(\lambda)$. $\mathbb{L}$ ist Zerfällungskörper von f über $\mathbb{K}$, also auch über $\mathbb{M}$. Die Induktionsannahme liefert, daß $\mathbb{L} : \mathbb{M}$ eine Galoiserweiterung ist, es gilt demnach $\mathbb{M} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})}$ und damit

$$\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})} \subseteq \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})} = \mathbb{M} = \mathbb{K}(\lambda).$$

Ist $s := [\mathbb{K}(\lambda) : \mathbb{K}] = \mathrm{Grad}(f_{\mathbb{K},\lambda})$, dann gibt es, zu jedem $x \in \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$, Elemente κ_i von $\mathbb{K}$ mit

$$x = \kappa_0 + \kappa_1\lambda^1 + \ldots + \kappa_{s-1}\lambda^{s-1}.$$

Wir wollen zeigen, daß $x = \kappa_0 \in \mathbb{K}$.
f ist separabel, also auch $f_{\mathbb{K},\lambda}$, die (verschiedenen) Wurzeln dieses Minimalpolynoms seien $\lambda = \lambda_0, \ldots, \lambda_{s-1}$. Wir wissen, daß es Isomorphismen $\varphi_i\colon \mathbb{K}(\lambda) \simeq \mathbb{K}(\lambda_i)$ gibt mit $\varphi_i(\lambda) = \lambda_i$, und die auf $\mathbb{K}$ die identische Abbildung induzieren. ϕ_i sei die Fortsetzung von φ_i auf $\mathbb{L}$. Wegen $\phi_i \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ und $\phi_i(\lambda) = \lambda_i$ gilt

$$\forall\, x \in \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}\colon\ x = \phi_i(x) = \kappa_0 + \kappa_1\lambda_i^1 + \ldots + \kappa_{s-1}\lambda_i^{s-1}.$$

Das Polynom

$$g := (\kappa_0 - x) + \kappa_1\mu^1 + \ldots + \kappa_{s-1}\mu^{s-1}$$

hat dann die $\lambda_i, i \in s$, als Wurzeln, obwohl es nur den Grad $s - 1$ hat, es muß also das Nullpolynom sein, d.h. es gilt $x = \kappa_0 \in \mathbb{K}$ und damit $\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})} \subseteq \mathbb{K}$, was noch zu zeigen war. □

Endliche Galoiserweiterungen $\mathbb{L} : \mathbb{K}$ sind also genau die endlichen Körpererweiterungen $\mathbb{L} : \mathbb{K}$, die normal und separabel sind. Hieraus folgt, daß endliche Galoiserweiterungen auch Galoiserweiterungen ihrer Zwischenkörper sind, denn endliche, normale und separable Erweiterungen sind natürlich auch endliche, normale und separable Erweiterungen ihrer Zwischenkörper $\mathbb{M}$. Es gilt demnach

$$\mathbb{M} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})} = (\Phi\Gamma)(\mathbb{M}),$$

und wir erhalten die

10.3.4 Folgerung *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung und* $\mathbb{M}$ *ein Zwischenkörper, dann ist* $\mathbb{L} : \mathbb{M}$ *ebenfalls Galoiserweiterung. Die Komposition* $\Phi \circ \Gamma$ *induziert die Identität auf ZwK*$(\mathbb{L} : \mathbb{K})$, $\Phi: U \mapsto \mathbb{L}_U$ *ist also ebenfalls surjektiv. Die Abbildungen* Φ *und* Γ *sind zueinander inverse Ordnungsantiisomorphismen zwischen* $\mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K}))$ *und ZwK*$(\mathbb{L} : \mathbb{K})$.

Es bleibt zu untersuchen, wann $\mathbb{M} : \mathbb{K}$ Galoiserweiterung ist.

10.3.5 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung,* $\mathbb{M}$ *ein Zwischenkörper, dann sind äquivalent:*

- $\mathbb{M} : \mathbb{K}$ *ist normal,*
- $\sigma(\mathbb{M}) = \mathbb{M}$, *für alle* $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$,
- $\mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$.

Beweis: $\mathbb{M}$ ist einfache Erweiterung, etwa $\mathbb{M} = \mathbb{K}(\lambda)$.

i)$\Rightarrow$ ii): Ist $\mathbb{M} = \mathbb{K}(\lambda)$ normal, dann liegen alle Wurzeln von $f_{\mathbb{K},\lambda}$ in $\mathbb{M}$. Das Bild $\sigma(\lambda)$ von λ unter der Operation eines Elements σ der Galoisgruppe ist Wurzel, liegt demnach für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ in $\mathbb{M}$ und damit auch $\sigma(m = \sum_i \kappa_i \lambda^i)$. Es folgt $\sigma(\mathbb{M}) = \mathbb{M}$.

ii) $\Rightarrow$ i): Ist $\sigma(\mathbb{M}) = \mathbb{M}$, dann gilt $\sigma(\lambda) \in \mathbb{M}$. Das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}:\mathbb{K})} (x - \sigma(\lambda)) = \sum_j \mu_j x^j$$

hat λ als Wurzel und zerfällt in Linearfaktoren. Ist jetzt $\tau \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, dann gilt für die Fortsetzung $\tilde{\tau}$:

$$\tilde{\tau} f = \prod_{\sigma} (x - \tau\sigma(\lambda)) = f,$$

also $\tau\mu_j = \mu_j \in \mathbb{K}$. Der Zwischenkörper $\mathbb{M} = \mathbb{K}(\lambda)$ ist demnach Zerfällungskörper von f über $\mathbb{K}$, $\mathbb{M} : \mathbb{K}$ ist also normale Erweiterung.

iii) $\Leftrightarrow$ ii): Die Normalteilereigenschaft

$$\Gamma(\mathbb{M}) = \mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$$

ist äquivalent zu $\sigma\Gamma(\mathbb{M})\sigma^{-1} = \Gamma(\mathbb{M})$, für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, und das wiederum ist, wegen

$$\sigma\Gamma(\mathbb{M})\sigma^{-1} = \sigma\mathrm{Gal}(\mathbb{L} : \mathbb{M})\sigma^{-1} = \sigma\mathrm{Aut}(\mathbb{L})_{\mathbb{M}}\sigma^{-1} = \mathrm{Aut}(\mathbb{L})_{\sigma(\mathbb{M})} = \Gamma(\sigma(\mathbb{M}))$$

äquivalent zu $\Gamma(\sigma(\mathbb{M})) = \Gamma(\mathbb{M})$, für alle σ. Wegen der Injektivität von Γ ist das äquivalent zu $\sigma(\mathbb{M}) = \mathbb{M}$, für alle σ aus der Galoisgruppe.

□

Fassen wir zusammen, so ergibt sich der

10.3.6 Hauptsatz der Galoistheorie *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung, dann gilt*

- *Die Abbildungen* $\Phi: U \mapsto \mathbb{L}_U$ *und* $\Gamma: \mathbb{M} \mapsto \mathrm{Gal}(\mathbb{L} : \mathbb{M})$ *sind zueinander inverse Ordnungsantiisomorphismen zwischen dem Untergruppenverband* $\mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K}))$ *und dem Zwischenkörperverband ZwK*$(\mathbb{L} : \mathbb{K})$.
- *Für alle Zwischenkörper* $\mathbb{M}$ *ist* $\mathbb{L} : \mathbb{M}$ *ebenfalls Galoiserweiterung.*
- *Für jede Untergruppe* U *der Galoisgruppe und für jeden Zwischenkörper* $\mathbb{M}$ *von* $\mathbb{L} : \mathbb{K}$ *gilt*

$$[\mathbb{M} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L} : \mathbb{K})/\mathrm{Gal}(\mathbb{L} : \mathbb{M})|, \ |U| = [\mathbb{L} : \mathbb{L}_U].$$

- $\mathbb{M} : \mathbb{K}$ *ist genau dann eine Galoiserweiterung, wenn* $\mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *ist, in welchem Fall gilt*

$$\mathrm{Gal}(\mathbb{M} : \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L} : \mathbb{K})/\mathrm{Gal}(\mathbb{L} : \mathbb{M}).$$

□

(Die letzte Behauptung ergibt sich durch den Nachweis, daß die Einschränkung der σ auf $\mathbb{M}$ einen Epimorphismus von $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ auf $\mathrm{Gal}(\mathbb{M} : \mathbb{K})$ ergibt mit $\mathrm{Gal}(\mathbb{L} : \mathbb{M})$ als Kern!)

Als Anwendung können wir jetzt beispielsweise die noch fehlende Hälfte des Satzes über die Konstruierbarkeit regelmäßiger $n-$Ecke beweisen:

10.3.7 Satz *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn*

$$n = 2^k p_1 \cdots p_r,$$

mit verschiedenen Fermatschen Primfaktoren $p_1, \ldots, p_r$.

Beweis:

i) Wir wissen bereits, daß diese Form von n notwendig ist (vgl. 9.2.12) für die Konstruierbarkei.

ii) Zum Beweis der Umkehrung betrachten wir den Kreisteilungskörper $\mathbb{Q}(\zeta)$, mit einer primitiven n-ten Einheitswurzel ζ.

a) Wegen
$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = 2^m,$$
m geeignet, ist $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ eine 2-Gruppe der Ordnung 2^m.

b) Da, nach dem Satz von Sylow, jede Gruppe der Ordnung 2^r eine Untergruppe der Ordnung 2^{r-1} besitzt, also einen Normalteiler vom Index 2, gibt es eine Kette
$$\{1\} = U_0 \triangleleft U_1 \triangleleft \ldots \triangleleft U_m = \mathrm{Gal}\mathbb{Q}(\zeta) : \mathbb{Q}),$$
bei der $|U_i/U_{i-1}| = 2$ gilt.

c) Nach dem Hauptsatz gibt es deshalb eine Kette von Zwischenkörpern

$$\mathbb{Q}(\zeta) = \mathbb{M}_0 \supset \mathbb{M}_1 \supset \ldots \supset \mathbb{M}_m = \mathbb{Q},$$

mit $[\mathbb{M}_i : \mathbb{M}_{i+1}] = 2$. Damit ist jedes Element von $\mathbb{Q}(\zeta)$ konstruierbar, insbesondere also ζ und damit das regelmäßige n-Eck.

□