4.11 Der Hauptsatz der Galoistheorie[1]

Zunächst machen wir eine kleine Wiederholung:
Es sei eine Körpererweiterung $L : K$ gegeben. Deren Galoisgruppe G besteht bekanntlich aus allen K-Automorphismen von L. Zu dieser Körpererweiterung haben wir zwischen der Menge $\mathcal{F}$ aller Zwischenkörper M und der Menge $\mathcal{G}$ aller Untergruppen H von G die beiden Abbildungen

$$^* : \begin{cases} \mathcal{F} & \to & \mathcal{G} \\ M & \mapsto & M^* \end{cases}$$

und

$$^\dagger : \begin{cases} \mathcal{G} & \to & \mathcal{F} \\ H & \mapsto & H^\dagger \end{cases}$$

gemäß Definition 4.6.5 definiert. Sie erwies sich als ordnungsumkehrend und zeigte die Eigenschaft, dass immer $M \subset M^{*\dagger}$ und $H \subset H^{\dagger *}$ gilt.

Im Folgenden wird u.A. gezeigt, dass unter gewissen Bedingungen an die Körpererweiterung * und † invers zueinander sind.

Dazu wird zunächst eine Definition und ein sehr einfaches Lemma benötigt.

Definition 4.11.1 (separable Elemente, separable Körpererweiterung). Es sei $L : K$ eine Körpererweiterung. Dann heißt ein algebraisches Element $\alpha \in L$ **separabel** über K, wenn α Nullstelle eines separablen Polynoms aus $K[X]$ ist oder, was hierzu äquivalent ist, wenn das Minimalpolynom von α über K separabel ist. Falls jedes Element aus L separabel über K ist, wird $L : K$ **separable Körpererweiterung** genannt.

Lemma 4.11.2. *Es sei $L : K$ eine separable algebraische Körpererweiterung und M ein beliebiger Zwischenkörper. Dann sind $M : K$ und $L : M$ ebenfalls separabel.*

Beweis. Trivialerweise ist $M : K$ separabel. Sei also $\alpha \in L$ und seien m_K und m_M die zugehörigen Minimalpolynome über K bzw. M. Dann ist $m_M | m_K$ in $M[X]$. Nun ist m_K separabel über K, also ist m_M separabel über M und $L : M$ somit eine separable Körpererweiterung. □

Nach diesen Vorbereitungen können wir einen der wichtigen Sätze der Algebra in Angriff nehmen.

Satz 4.11.3 (Hauptsatz der Galoistheorie). *Es sei $L : K$ eine endliche separable normale Körpererweiterung vom Grad n. Weiterhin sei $G := \mathrm{Gal}(L : K)$. Dann gilt:*

1. *Die Galoisgruppe G hat Ordnung n.*

[1] Dieses Kapitel wurde ausgearbeitet, getippt und vorgetragen von Anke Pohl anhand des Kapitels 11 in Ian Stewart: Galois Theory, Chapman & Hall/CRC, Second Edition 1989

2. *Die Abbildungen* * *und* † *sind gegenseitig invers und induzieren eine ordnungsumkehrende* 1–1 *Korrespondenz zwischen* $\mathcal{F}$ *und* $\mathcal{G}$.

3. *Ist* M *ein Zwischenkörper, dann folgt*

$$[L : M] = |M^*|$$

und

$$[M : K] = \frac{|G|}{|M^*|}.$$

4. *Ein Zwischenkörper* M *ist genau dann eine normale Körpererweiterung von* K*, wenn* M^* *ein Normalteiler von* G *ist.*

5. *Ist ein Zwischenkörper* M *eine normale Körpererweiterung von* K*, dann ist die Galoisgruppe* $\mathrm{Gal}(M : K)$ *isomorph zu* G/M^*.

Teil 1 des Beweises. Der erste Teil ist gerade die Aussage von Korollar 4.10.11.

Für 2. ist zu zeigen, dass für jeden Zwischenkörper M

$$M^{*\dagger} = M$$

gilt und ebenso für jede Untergruppe H von G

$$H^{\dagger *} = H$$

folgt.

Sei also M ein beliebiger Zwischenkörper. Nach Lemma 4.11.2 gilt dann, dass $L : M$ separabel ist und Satz 4.7.10 weist $L : M$ als normal nach. Somit ist M nach Satz 4.10.12 der Fixkörper von M^*, was auch schon

$$M^{*\dagger} = M \tag{4.1}$$

zeigt.
Der andere Teil ist etwas komplizierter. Für eine beliebige Untergruppe H von G haben wir schon festgestellt, dass immer $H \subset H^{\dagger *}$ gilt. Die Feststellung (4.1) liefert

$$H^{\dagger *\dagger} = (H^\dagger)^{*\dagger} = H^\dagger.$$

Nach Satz 4.9.2 gilt

$$|H| = [L : H^\dagger],$$

also

$$|H| = [L : H^{\dagger *\dagger}]$$

und wiederum nach Satz 4.9.2

$$|H^{\dagger *}| = [L : H^{\dagger *\dagger}].$$

Insgesamt haben wir somit

$$|H| = |H^{\dagger *}|$$

erreicht, was wegen der Endlichkeit der Gruppen zu

$$H = H^{\dagger *}$$

führt.
Die 1–1 Korrespondenz zwischen $\mathcal{F}$ und $\mathcal{G}$ ist also

$$F \leftrightarrow \mathrm{Gal}(L : F).$$

Nach früheren Ergebnissen ist sie ordnungsumkehrend.

Der dritte Punkt ist eine einfache Konsequenz des Turmgesetzes: Oben haben wir schon gesehen, dass $L : M$ separabel und normal ist. Nach Korollar 4.10.11 gilt

$$[L : M] = |M^*|.$$

Mit dem Turmgesetz 4.5.4 folgt wegen der Endlichkeit der Grade

$$[M : K] = \frac{[L : K]}{[L : M]} = \frac{|G|}{|M^*|}.$$

□

Für den Beweis der letzten beiden Punkte des Hauptsatzes beweisen wir zunächst ein hilfreiches Lemma.

Lemma 4.11.4. *Sei $L : K$ eine Körpererweiterung, M ein Zwischenkörper und τ ein K-Automorphismus von L. Dann gilt*

$$(\tau(M))^* = \tau M^* \tau^{-1}.$$

Beweis. Wir setzen $N := \tau(M)$. Dann ist zu zeigen

1. $\tau M^* \tau^{-1} \subset N^*$
2. $\tau^{-1} N^* \tau \subset M^*$.

Sei $y \in N$. Also existiert ein $x \in M$ mit $\tau(x) = y$. Dann gilt für jedes $\gamma \in M^*$

$$\tau\gamma\tau^{-1}(y) = \tau\gamma\tau^{-1}\tau(x) = \tau\gamma(x) = \tau(x) = y,$$

also gilt 1. Umgekehrt seien $x \in M$ und $\eta \in N^*$ beliebig. Dann setzen wir

$$\tau^{-1}\eta\tau(x) = \tau^{-1}\tau(x) = x,$$

somit folgt 2. □

Damit können wir jetzt den Rest vom Hauptsatz beweisen.

Teil 2 des Beweises von Satz 4.11.3. Für den vierten Teil sei zunächst $M : K$ normal und $\tau \in G$ beliebig. Dann ist $\tau|_M : M \to L$ ein K-Monomorphismus. Nach Satz 4.10.9 ist $\tau|_M$ ein K-Automorphismus von M. Also gilt

$$\tau(M) = M.$$

Nach obigem Lemma 4.11.4 folgt

$$\tau M^* \tau^{-1} = M^*,$$

was bedeutet, dass M^* ein Normalteil von G ist.

Sei umgekehrt M^* ein Normalteiler von G. Weiterhin sei $\sigma : M \to L$ ein K-Monomorphismus. Nach Satz 4.10.3 existiert ein K-Automorphismus τ von L mit $\tau|_M = \sigma$.
Weil $M^* \lhd G$ ist, haben wir $\tau M^* \tau^{-1} = M^*$ und somit nach Lemma 4.11.4 $(\tau(M))^* = M^*$. Nach 2. heißt dieses aber $\tau(M) = M$, also $\sigma(M) = M$, was zeigt, dass σ ein K-Automorphismus von M ist. Nach Satz 4.10.9 ist $M : K$ normal.

Jetzt fehlt nur noch der fünfte Teil: Mit H sei die Galoisgruppe $\mathrm{Gal}(M : K)$ bezeichnet. Wir betrachten die Abbildung

$$\varphi : \left\{ \begin{array}{ccc} G & \to & H \\ \tau & \mapsto & \tau|_M. \end{array} \right.$$

Nach Satz 4.10.9 ist $\tau|_M$ ein K-Automorphismus von M, also bildet φ überhaupt in H ab. Weiterhin ist φ offensichtlich ein Gruppenhomomorphismus. Nach Satz 4.10.3 ist φ surjektiv. Nun ist $\ker \varphi = M^*$ und der Homomorphiesatz 1.8.7 für Gruppen liefert

$$H = \mathrm{Im}\, \varphi \cong G/\ker \varphi = G/M^*.$$

□