## 10.1 Galoisgruppen

Unser Ziel ist der Beweis des Hauptsatzes der Galoistheorie, der einen Ordnungsisomorphismus zwischen dem Untergruppenverband der sogenannten Galoisgruppe beschreibt und dem Verband der Zwischenkörper des Zerfällungskörpers. Definieren wir deshalb zunächst *die Galoisgruppe, die aus den Körperautomorphismen von* $\mathbb{L}$ *besteht, die Wurzeln von Polynomen* $f \in \mathbb{K}[x]$ *wieder in Wurzeln überführen*:

**10.1.1 Definition (Galoisgruppe)** Als *Galoisgruppe* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ der Körpererweiterung $\mathbb{L}:\mathbb{K}$ bezeichnet man den punktweisen Stabilisator von $\mathbb{K}$ in der Automorphismengruppe von $\mathbb{L}$:

$$\mathrm{Gal}(\mathbb{L}:\mathbb{K}) := \{\sigma \in \mathrm{Aut}(\mathbb{L}) \mid \forall\, \kappa \in \mathbb{K}\colon \sigma(\kappa) = \kappa\} = \mathrm{Aut}(\mathbb{L})_{\mathbb{K}}.$$

•

Man kan dies auch noch anders formulieren, denn wir wissen ja, daß $\mathbb{L}$ ein $\mathbb{K}-$Vektorraum ist:

**10.1.2 Hilfssatz** $\sigma \in \mathrm{Aut}(\mathbb{L})$ *liegt genau dann in* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$, *wenn* $\sigma$ *eine lineare Abbildung auf dem* $\mathbb{K}-$*Vektorraum* $\mathbb{L}$ *induziert.*

Beweis: Ist $\sigma$ $\mathbb{K}$-linear, dann gilt

$$\sigma(\kappa) = \sigma(\kappa \cdot 1_{\mathbb{L}}) = \kappa\sigma(1_{\mathbb{L}}) = \kappa.$$

Ist umgekehrt $\sigma \in \mathrm{Gal}(\mathbb{L}:\mathbb{K})$, dann haben wir, für jedes $x \in \mathbb{L}$,

$$\sigma(\kappa x) = \sigma(\kappa)\sigma(x) = \kappa\sigma(x),$$

$\sigma$ ist also $\mathbb{K}$-linear. □

**10.1.3 Folgerung**

$$\mathrm{Gal}(\mathbb{L}:\mathbb{K}) = \mathrm{Aut}(\mathbb{L})_{\mathbb{K}} = \mathrm{End}_{\mathbb{K}}(\mathbb{L}) \cap \mathrm{Aut}(\mathbb{L}).$$

Wir können ein Element $\sigma$ der Galoisgruppe also auch als *lineare Abbildung* — und nicht nur als *Körperautomorphismus* — betrachten. Eine dritte Interpretationsmöglichkeit kommt hinzu: $\sigma \in \mathbb{L}^{\mathbb{L}}$ zeigt, daß $\sigma$ auch als *Vektor* verstanden werden kann, denn $\mathbb{L}^{\mathbb{L}}$ ist ja ein $\mathbb{L}-$Vektorraum! Tatsächlich werden wir gleich sehen, daß $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ sich als linear unabhängige Menge erweist, so daß an wichtigen Stellen dieser Theorie *Dimensionsargumente* benutzt werden können. Dies wird mit dem folgenden ganz allgemeinen Satz fundiert:

**10.1.4 Der Satz von Dedekind** *Sei* $\mathbb{L}$ *ein Körper,* $H$ *eine nicht leere, multiplikativ geschriebene Halbgruppe. Dann ist die Menge* $\mathrm{Hom}(H,\mathbb{L})^*$ *der Homomorphismen* $\neq 0$ *von* $H$ *in* $\mathbb{L}$ *als Teilmenge des* $\mathbb{L}$*-Vektorraums* $\mathbb{L}^H$ *linear unabhängig.*

Beweis: Sei $\{\sigma_0, \ldots, \sigma_{n-1}\}_{\neq} \subseteq \mathrm{Hom}(H, \mathbb{L})^*$. Wir zeigen, per Induktion nach $n$, daß jede Linearkombination der Nullabbildung aus diesen $\sigma_i$ trivial sein muß.

i) $n = 1$ : Wegen $\sigma_0 \neq 0$ erzwingt $\lambda \cdot \sigma_0 = 0$, daß $\lambda = 0$.

ii) $n > 1$ : Wegen $\sigma_0 \neq \sigma_{n-1}$ gibt es $h' \in H$ mit $\sigma_0(h') \neq \sigma_{n-1}(h')$. Der Ansatz $\sum_i \lambda_i \sigma_i = 0$ ergibt, für jedes $h \in H$, die beiden Gleichungen

$$\sum_{i=0}^{n-1} \lambda_i \sigma_i(h'h) = 0 = \sigma_{n-1}(h') \sum_{i=0}^{n-1} \lambda_i \sigma_i(h).$$

Subtraktion der rechten von der linken Seite liefert — unter Verwendung der Homomorphieeigenschaft von $\sigma_i$ — die Identität

$$\sum_{i=0}^{n-2} \lambda_i (\sigma_i(h') - \sigma_{n-1}(h'))\sigma_i(h) = 0.$$

Die Induktionsannahme impliziert die lineare Unabhängigkeit von $\{\sigma_0, \ldots, \sigma_{n-2}\}$, und damit

$$\lambda_i(\sigma_i(h') - \sigma_{n-1}(h')) = 0, 0 \leq i \leq n-2,$$

woraus, wegen $\sigma_0(h') \neq \sigma_{n-1}(h')$, die Identität $\lambda_0 = 0$ folgt.
Aus $\lambda_0 = 0$ folgt aber $\sum_{i=1}^{n-1} \lambda_i \sigma_i = 0$, so daß sich mit der Induktionsannahme auch $\lambda_1 = \ldots = \lambda_{n-1} = 0$, und damit die lineare Unabhängigkeit der $\sigma_i$, insgesamt also die Behauptung ergibt. □

**10.1.5 Folgerung** $\mathrm{Aut}(\mathbb{L})$ *ist, als Teilmenge des* $\mathbb{L}$*-Vektorraums* $\mathbb{L}^{\mathbb{L}}$*, linear unabhängig, ebenso natürlich auch die Teilmenge* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$*. Beide Mengen sind auch* $\mathbb{K}-$*linear unabhängig, als Teilmengen von* $\mathbb{L}^{\mathbb{L}}$*, als* $\mathbb{K}-$*Vektorraum.*

Dies ermöglicht den Beweis von

**10.1.6 Satz** *Ist* $[\mathbb{L} : \mathbb{K}]$ *endlich, dann gilt*

$$dim_{\mathbb{L}}(\mathrm{End}_{\mathbb{K}}(\mathbb{L})) = [\mathbb{L} : \mathbb{K}] \geq |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|.$$

*Ist* $[\mathbb{L} : \mathbb{K}]$ *endlich und* $\mathbb{L} : \mathbb{K}$ *normal und separabel, dann gilt sogar*

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

Beweis:

i) Ist $\{\beta_0, \ldots, \beta_{n-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann bilden die $f_i \in \mathrm{End}_{\mathbb{K}}(\mathbb{L}), i \in n$, definiert durch $f_i(\beta_k) := \delta_{ik}$ eine $\mathbb{K}$-Basis von $\mathrm{End}_{\mathbb{K}}(\mathbb{L})$. Daraus folgt die Behauptung, denn die Galoisgruppe liegt in $\mathrm{End}_{\mathbb{K}}(\mathbb{L})$, und sie besteht aus linear unabhängigen Elementen.

ii) Ist $\mathbb{L} : \mathbb{K}$ darüberhinaus normal und separabel, dann gibt es $\beta_i$ mit

$$\mathbb{L} = \mathbb{K}(\beta_0, \ldots, \beta_{n-1}).$$

Wegen der Separabilität sind die $\beta_i$ separabel, also auch algebraisch. Nach dem Satz vom primitiven Element folgt die Existenz eines $\lambda \in \mathbb{L}$ mit

$$\mathbb{L} = \mathbb{K}(\lambda).$$

Das Minimalpolynom $f_{\mathbb{K},\lambda}$ von $\lambda$ ist separabel, die Wurzeln $\lambda = \lambda_1, \ldots, \lambda_n$ also alle verschieden, und sie liegen in $\mathbb{L}$, wegen der Normalität. Für die Erweiterungen gibt es also $\sigma_i \in \mathrm{Aut}(\mathbb{L})$ mit $\sigma_i(\lambda) = \lambda_i$, die $\mathbb{K}$ elementweise fest lassen. Die $\sigma_i$ liegen also in der Galoisgruppe, und es folgt $n \leq |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$. Zusammen mit der Abschätzung der Ordnung der Galoisgruppe nach oben in i) folgt damit die Behauptung. □

**10.1.7 Beispiele** Wir fassen zunächst die *allgemeine Methode zur Bestimmung von Galoisgruppen endlicher normaler und separabler Erweiterungen* zusammen, die sich aus obigen Beweisen ergibt:

i) Ist $\mathbb{L} : \mathbb{K}$ endlich, normal und separabel, dann kann man wie folgt vorgehen:

a) Man ermittelt zunächst ein primitives Element $\lambda$, wie im Beweis vom Satz vom primitiven Element vorgeschlagen.

b) Danach bestimmt man das Minimalpolynom von $\lambda$, indem man das minimale $s$ ermittelt, für welches $\{1, \lambda, \ldots, \lambda^s\}$ linear abhängig ist (vgl. 8.2.6). Gilt hierfür
$$\lambda^s = \kappa_{s-1}\lambda^{s-1} + \ldots + \kappa_0,$$
dann ist
$$f_{\mathbb{K},\lambda} = x^s - \kappa_{s-1}x^{s-1} - \ldots - \kappa_0.$$

c) Dann folgt die Berechnung der Wurzeln dieses Minimalpolynoms, hierfür sind allerdings nur wenige Methoden bekannt und sie ist nur in günstigen Fällen durchführbar.

d) Die abschließende Beschreibung der Elemente $\sigma_i\colon \lambda \mapsto \lambda_i$ der Galoisgruppe ist einfach, denn ganz offensichtlich gilt
$$\sigma_i\colon (x = \sum_{j=0}^{s-1} \kappa_j \lambda^j) \mapsto \sum_{j=0}^{s-1} \kappa_j \lambda_i^j.$$

e) Zusammenfassend ist also
$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) = \{\sigma_1 = \mathrm{id}_{\mathbb{K}}, \sigma_2, \ldots, \sigma_n\}.$$

ii) Ein konkretes und ganz einfaches Beispiel illustriert die gerade beschriebene Methode:

a) Wegen $\mathbb{C} = \{r + is \mid r, s \in \mathbb{R}\}$ ist $\mathbb{C} : \mathbb{R}$ endlich, $[\mathbb{C} : \mathbb{R}] = 2$.

b) $\mathbb{C} : \mathbb{R}$ ist auch normal, denn $\mathbb{C}$ ist algebraisch und Zerfällungskörper von $1 + x^2$.

c) Als Körper der Charakteristik 0 ist $\mathbb{C} : \mathbb{R}$ zudem separabel.

d) Ein primitives Element ist $i$, $\mathbb{C} = \mathbb{R}(i)$.

e) Die Menge $\{1, i, i^2\}$ ist linear abhängig, und es gilt

$$i^2 = -1 + 0 \cdot i \in \mathbb{C},$$

also

$$f_{\mathbb{R},i} = x^2 + 1$$

das Minimalpolynom von $i$.

f) Dieses Minimalpolynom zerfällt wie folgt in Linearfaktoren:

$$x^2 + 1 = (x - i)(x + i).$$

Die Galoisgruppe besteht demnach aus den beiden Elementen

$$\sigma_1 : i \mapsto i \text{und } \sigma_2 : i \mapsto -i.$$

Offensichtlich ist $\sigma_1 = \mathrm{id}_{\mathbb{C}}$ und $\sigma_2$ die Konjugation $r + is \mapsto r - is$.

iii) Die Kreisteilungskörper $\mathbb{Q}(\zeta)$ : Hier ist $\zeta$ eine primitive $n$-te Einheitswurzel. Wir wissen bereits, daß folgendes gilt:

a) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, der Kreisteilungskörper ist also eine endliche Erweiterung. Er ist algebraisch, also normal, denn er ist Zerfällungskörper von $\Phi_n$. Als Erweiterung von $\mathbb{Q}$ ist er separabel.

b) Das Minimalpolynom von $\zeta$ zerfällt wie folgt:

$$f_{\mathbb{Q},\zeta} = \Phi_n = \prod_{k \in n : \mathrm{ggT}\,(k,n) \ni 1} (x - \zeta^k).$$

c) Für die Galoisgruppe über $\mathbb{Q}$ gilt also

$$G(\mathbb{Q}(\zeta) : \mathbb{Q}) = \{\sigma_k \mid \zeta \mapsto \zeta^k \mid \mathrm{ggT}\,(k, n) \ni 1\}.$$

Diese Galoisgruppe ist also isomorph zur Einheitengruppe des Rings $\mathbb{Z}_n$, also zur *primen Restklassengruppe* modulo $n$.

◇

Neben dieser systematischen Vorgehensweise gibt es in vielen Fällen erfolgreiche *ad hoc* Methoden.

### 10.1.8 Beispiele

i) $\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}$ ist *keine* normale Erweiterung, da $\sqrt[3]{2}$ die einzige Wurzel von $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2}\,)$ ist. Liegt $\sigma$ in der Galoisgruppe, dann ist $\sigma(\sqrt[3]{2}\,)$ eine Wurzel des Minimalpolynoms von $\sqrt[3]{2}$, die in $\mathbb{Q}(\sqrt[3]{2}\,)$ liegt. Dort liegt aber nur diese eine Wurzel, so daß sich $\sigma = \mathrm{id}$ ergibt und damit

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}) = \{1\}.$$

ii) Die Körpererweiterung $\mathbb{R} : \mathbb{Q}$ ist nicht algebraisch, also nicht normal.

a) Jedes $\sigma \in \mathrm{Aut}(\mathbb{R})$ läßt jedes Element von $\mathbb{Q}$ fest: Ist $z \in \mathbb{Z}^*$, so gilt, weil $\sigma(z) = z\sigma(1) = z$,

$$1 = \sigma\left(\frac{z}{z}\right) = z \cdot \sigma\left(\frac{1}{z}\right),$$

also

$$\sigma\left(\frac{1}{z}\right) = \frac{1}{z}.$$

Das ergibt natürlich auch, für $z' \in \mathbb{Z}$,

$$\sigma\left(\frac{z'}{z}\right) = \frac{z'}{z}.$$

b) Ist $\sigma$ eine Automorphismus von $\mathbb{R}$, $x \in \mathbb{R}_{>0}$, dan gibt es $y \in \mathbb{R}$ mit $y^2 = x$, also

$$\sigma(x) = \sigma(y^2) = \sigma(y)^2 \geq 0,$$

d.h. $0 \leq x$ ergibt $\sigma(0) \leq \sigma(x)$. Daraus folgt, wegen der Homomorphie bzgl. Addition, daß $x \leq y$ die Ungleichung $\sigma(x) \leq \sigma(y)$ impliziert, $\sigma$ respektiert demnach die Anordnung auf $\mathbb{R}$.

c) Jede reelle Zahl ist rational approximierbar. Sei $(x_n)_{n\in\mathbb{N}}$ eine gegen $x \in \mathbb{R}$ strebende Folge rationaler Zahlen. Für alle $n \in \mathbb{N}$ gibt es dann $N_n \in \mathbb{N}$ mit

$$\forall\ k \geq N_n\colon\ x - \frac{1}{n} \leq x_k \leq x + \frac{1}{n}.$$

Dies impliziert

$$\sigma(x) - \frac{1}{n} \leq x_k \leq \sigma(x) + \frac{1}{n}.$$

Hieraus folgt die Konvergenz von $(x_k)_{k\in\mathbb{N}}$ gegen $\sigma(x)$ und daraus $\sigma(x) = x$. $\sigma$ läßt also auch die reellen Zahlen fest, es gilt

$$\mathrm{Gal}(\mathbb{R} : \mathbb{Q}) = \{1\}.$$

iii) Wichtig ist die Galoisgruppe eines Galoisfelds über einem endlichen Primkörper. Hierzu wissen wir folgendes:

a) Der Körpergrad ist $[GF(p^n) : GF(p)] = n$.

b) Der Erweiterungskörper $GF(p^n)$ ist Zerfällungskörper von $x^{(p^n)} - x$.

c) Die Erweiterung ist normal und separabel, die Ordnung der Galoisgruppe also gleich dem Körpergrad $n$.

d) Wir wissen bereits, daß der Frobeniusautomorphismus $\sigma\colon \kappa \mapsto \kappa^p$ in der Galoisgruppe liegt, denn er läßt den Primkörper elementweise fest.

e) Dieser Automorphismus hat die Ordnung $n$. Setzen wir nämlich $m := |\langle\sigma\rangle|$, so gilt

$$\forall\ \kappa \in GF(p^n)\colon \kappa^{(p^m)} = \kappa,$$

was $GF(p^n) \subseteq GF(p^m)$ und damit $n \leq m$ ergibt. Andererseits gilt aber $m \leq |\mathrm{Gal}(GF(p^n) : GF(p)| = n$, insgesamt also $m = n$. $\sigma$ erzeugt demnach die Galoisgruppe:

$$\mathrm{Gal}(GF(p^n) : GF(p)) = \langle\sigma\rangle \simeq C_n.$$

$\diamond$