Algebra

Dr. Columbus und Prof. Weitze-Schmithüsen
Wintersemester 2019/2020

UNIVERSITÄT
DES
SAARLANDES

Inhaltsverzeichnis

Kapitel I.

Kategorientheorie

1. Grundbegriffe

Definition I.1.1 (Kategorie): Eine *Kategorie* $\mathbf{C}$ besteht aus einer Klasse $\mathrm{Ob}(\mathbf{C})$ von Objekten, Mengen $\mathbf{C}(C, D)$ von Morphismen (manchmal auch Pfeilen) $f\colon C \to D$ für je zwei Objekte $C, D \in \mathrm{Ob}(\mathbf{C})$ und Kompositionen

$$\circ\colon \mathbf{C}(D, E) \times \mathbf{C}(C, D) \longrightarrow \mathbf{C}(C, E), \qquad (f, g) \longmapsto f \circ g$$

für je drei Objekte $C, D, E \in \mathrm{Ob}(\mathbf{C})$, für die gelten:

(i) Für $f\colon E \to F$, $g\colon D \to E$ und $h\colon C \to D$ ist $f \circ (g \circ h) = (f \circ g) \circ h$,

(ii) Für alle $C \in \mathrm{Ob}(\mathbf{C})$ gibt es einen Pfeil $1_C \in \mathbf{C}(C, C)$ mit $1_C \circ f = f$ und $g \circ 1_C = g$ für alle $f\colon B \to C$ und $g\colon C \to D$.

Oft schreiben wir einfach $C \in \mathbf{C}$ statt $C \in \mathrm{Ob}\,\mathbf{C}$.

Beispiel I.1.2 (für Kategorien): (i) Die Klasse der Mengen Set mit Mengenabbildungen als Pfeile,

(ii) Die Klasse der k-Vektorräume k-Vr mit linearen Abbildungen als Pfeile,

(iii) Die Klasse der Gruppen mit Gruppenhomomorphismen als Pfeile,

(iv) Sei $(P, \leqslant)$ eine partiell geordnete Menge. Dann wird $\mathbf{P}$ mit $\mathrm{Ob}(\mathbf{P}) = P$ mit den Mengen von Pfeilen

$$\mathbf{P}(p, q) = \begin{cases} \star, & \text{falls } p \leqslant q, \\ \varnothing, & \text{sonst,} \end{cases}$$

zu einer Kategorie.

(v) Ist G eine Gruppe, dann wird $\mathbf{G}$ mit $\operatorname{Ob}\mathbf{G} = \{\star\}$ und $\mathbf{G}(\star,\star) = G$ zu einer Kategorie.

(vi) Ist $\mathbf{C}$ eine Kateogrie, dann wird $\mathbf{C}^{\mathsf{op}}$ mit $\operatorname{Ob}(\mathbf{C}^{\mathsf{op}}) = \operatorname{Ob}(\mathbf{C})$ und $\mathbf{C}^{\mathsf{op}}(C,D) = \mathbf{C}(D,C)$ eine Kategorie, die sogenannte opposite Kategorie.

Definition I.1.3: Ein Pfeil $f\colon C \to D$ in einer Kategorie $\mathbf{C}$ heißt

(i) *Monomorphismus*, wenn für alle $x, y\colon X \to C$ gilt: „$f\circ x = f\circ y \Rightarrow x = y$“,

(ii) *Epimorphismus*, wenn für alle $x, y\colon D \to X$ gilt: „$x\circ f = y\circ f \Rightarrow x = y$“,

(iii) *Isomorphismus*, wenn es $f^{-1}\colon D \to C$ mit $f^{-1}\circ f = 1_C$ und $f\circ f^{-1} = 1_D$ gibt.

Beispiel I.1.4: (i) In der Kateogrie Set sind injektive Mengenabbildungen genau die Monomorphismen, surjektive Mengenabbildungen genau die Epimorphismen und Isomorphismen genau die bijektiven Mengenabbildungen.

(ii) In einer Kategorie von Räumen und stetigen Abbildungen als Pfeilen ist $\iota\colon \mathbb{Q} \to \mathbb{R}$ ein Epimorphismus und ein Monomorphismus, aber kein Isomorphismus.

(iii) In den Kategorien Gr, k-Vr sind injektive Homomorphismen genau die Monomorphismen, surjektive Homomorphismen genau die Epimorphismen und bijektive Homomorphismen genau die Isomorphismen.

Definition I.1.5 (Funktor): Ein Funktor $F\colon \mathbf{C} \to \mathbf{D}$ zwischen zwei Kategorien $\mathbf{C}$, $\mathbf{D}$ besteht aus einer Zuordnung $F\colon \operatorname{Ob}(\mathbf{C}) \to \operatorname{Ob}(\mathbf{D})$ und Abbildungen $\mathbf{C}(C,D) \xrightarrow{-F\to} \mathbf{D}(FC, FD)$, sodass gelten:

(i) Für alle $C, D, E \in \mathbf{C}$ und $f\colon C \to D$, $g\colon D \to E$ ist $F(gf) = F(g)F(f)$,

(ii) Für alle $C \in \mathbf{C}$ ist $F(1_C) = 1_{FC}$.

Beispiel I.1.6 (für Funktoren): (i) Die Zuordnungen $\mathsf{Grp} \to \mathsf{Set}$, $G \mapsto G$ und k-$\mathsf{Vr} \to \mathsf{Set}$, $V \mapsto V$ sind Funktoren.

(ii) Ist $\mathbf{C} = \star$, so ist ein Funktor $\mathbf{C} \to \mathbf{D}$ nichts anderes als ein Objekt in $\mathbf{D}$.

(iii) Ist $\mathbf{C} = (\bullet \to \bullet)$, so ist ein Funktor $\mathbf{C} \to \mathbf{D}$ nichts anderes als ein Pfeil in $\mathbf{D}$.

(iv) Ein kontravarianter Funktor $\mathbf{C} \to \mathbf{D}$ ist ein Funktor $F\colon \mathbf{C}^{\mathsf{op}} \to \mathbf{D}$.

(v) $(-)^*\colon k\text{-}\mathsf{Vr}^{\mathsf{op}} \to k\text{-}\mathsf{Vr}$, $V \mapsto V^*$ ist ein Funktor.

(vi) $U \otimes (-)\colon k\text{-}\mathsf{Vr} \to k\text{-}\mathsf{Vr}$, $V \mapsto U \otimes_k V$ ist ein Funktor.

(vii) Für Gruppen G und H ist ein Funktor $\mathbf{G} \to \mathbf{H}$ nichts anderes als ein Gruppenhomomorphismus.

(viii) Für partiell geordnete Mengen P und Q ist ein Funktor $\mathbf{P} \to \mathbf{Q}$ eine monotone Abbildung.

(ix) Ist $C \in \mathbf{C}$ und $\mathbf{I}$ eine beliebige Kategorie, so ist

$$\Delta_C \colon \mathbf{I} \longrightarrow \mathbf{C}, \qquad i \longmapsto C, \qquad (i \to j) \longmapsto 1_C$$

ein Funktor.

Definition I.1.7: Ein Funktor $F \colon \mathbf{C} \to \mathbf{D}$ heißt

(i) *voll*, wenn $\mathbf{C}(C, D) \to \mathbf{D}(FC, FD)$ surjektiv für alle $C, D \in \mathbf{C}$ ist,

(ii) *treu*, wenn $\mathbf{C}(C, D) \to \mathbf{D}(FC, FD)$ injektiv für alle $C, D \in \mathbf{C}$ ist,

(iii) *voll treu*, wenn $\mathbf{C}(C, D) \to \mathbf{D}(FC, FD)$ bijektiv für alle $C, D \in \mathbf{C}$ ist,

(iv) *essentiel surjektiv*, wenn es für jedes $D \in \mathbf{D}$ ein $C \in \mathbf{C}$ mit $D \cong F(C)$ gibt.

Definition I.1.8 (Natürliche Transformation):

(i) Eine *natürliche Transformation* $\alpha \colon F \to G$ *zwischen zwei Funktoren* $F, G \colon \mathbf{C} \to \mathbf{D}$ ist eine Familie $\{\alpha_C \colon FC \to GC\}_{C \in \mathbf{C}}$ von Pfeilen in $\mathbf{D}$, sodass für alle $f \colon C \to D$ in $\mathbf{C}$ das Diagram

$$\begin{array}{ccc} FC & \xrightarrow{\alpha_C} & GC \\ {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle Gf} \\ FD & \xrightarrow[\alpha_D]{} & GD \end{array}$$

kommutativ ist. Mit $\mathrm{Nat}(F, G)$ bezeichnen wir die Klasse der natürlichen Transformationen $\alpha \colon F \to G$.

(ii) Hat $\mathbf{C}$ eine Menge von Objekten (solche Kategorien heißen *klein*), dann ist $\mathrm{Nat}(F, G)$ tatsächlich eine Menge. Wir definieren in diesem Fall die Kategorie $\mathrm{Fun}(\mathbf{C}, \mathbf{D})$, wobei die Funktoren $F \colon \mathbf{C} \to \mathbf{D}$ die Objekte dieser Kategorie-, und die natürlichen Transformationen $\alpha \colon F \to G$ die Pfeile dieser Kategorie sind.

Die Komposition in $\mathrm{Fun}(\mathbf{C}, \mathbf{D})$ ist folgendermaßen definiert: Für natürliche Transformationen $\alpha \colon F \to G$ und $\beta \colon G \to H$ ist $(\beta \circ \alpha) \colon F \to H$ mit Komponenten

$$(\beta \circ \alpha)_C \colon FC \xrightarrow{\alpha} GC \xrightarrow{\beta} HC$$

eine natürliche Transformation: Das Diagramm

$$\begin{array}{ccccc} FC & \xrightarrow{\alpha_C} & GC & \xrightarrow{\beta_C} & HC \\ {\scriptstyle Ff}\downarrow & & {\scriptstyle Gf}\downarrow & & {\scriptstyle Hf}\downarrow \\ FD & \xrightarrow[\alpha_D]{} & GC & \xrightarrow[\beta_D]{} & HD \end{array}$$

kommutiert, da die beiden Teilquadrate kommutieren.

Beispiel I.1.9: (i) Es bezeichne $V\colon \mathsf{Grp} \to \mathsf{Set}$, $G \mapsto G$ den Vergissfunktor und

$$\Delta_\star = \star\colon \mathsf{Grp} \longrightarrow \mathsf{Set}, \qquad G \longmapsto \{1\}$$

Es gibt die natürliche Transformation

$$\alpha\colon V \longrightarrow \star$$

mit Komponenten $\alpha_G\colon V(G) \to \star(G)$, $G \to \{\star\}$, $g \mapsto 1$. Das ist natürlich, denn für einen Gruppenhomomorphismus $f\colon G \to H$ ist

$$\begin{array}{ccccccc} G & = & V(G) & \xrightarrow{\alpha_G} & \star(G) & = & \{1\} \\ {\scriptstyle f}\downarrow & & {\scriptstyle V(f)}\downarrow & & \downarrow{\scriptstyle \star(f)} & & \| \\ H & = & V(H) & \xrightarrow[\alpha_H]{} & \star(H) & = & \{1\} \end{array}$$

Umgekehrt gibt es eine natürliche Transformation $\beta\colon \star \to V$ mit Komponenten $\beta_G\colon \star(G) \to V(G)$, $\{1\} \to G$, $1 \mapsto e_G$. Das ist natürlich, denn für alle Gruppenhomomorphismen $f\colon G \to H$ kommutiert das Diagramm

$$\begin{array}{ccccccc} \{1\} & = & \star(G) & \xrightarrow{e_G} & V(G) & = & G \\ \| & & {\scriptstyle \star(f)}\downarrow & & \downarrow{\scriptstyle V(f)} & & \downarrow{\scriptstyle f} \\ \{1\} & = & V(H) & \xrightarrow[e_H]{} & V(H) & = & H \end{array}$$

(ii) Seien $\mathbf{I}$, $\mathbf{C}$ Kategorien. Eine natürliche Transformation $\Delta_C \to \Delta_D$ (mit $C, D \in \mathbf{C}$) ist eine Familie $\{\alpha_i\colon \Delta_C(i) \to \Delta_D(i)\}$ von Pfeilen, sodass für alle $f\colon i \to j$ in $\mathbf{I}$ gilt:

$$\begin{array}{ccccccc} C & = & \Delta_C(i) & \xrightarrow{\alpha_C} & \Delta_D(i) & = & D \\ \downarrow{\scriptstyle 1_C} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle 1_D} \\ C & = & \Delta_C(j) & \xrightarrow[\alpha_D]{} & \Delta_D(j) & = & D \end{array}$$

zum Beispiel $\mathbf{I} = \bullet \leftarrow \bullet \rightarrow \bullet$.

Dann ist eine natürliche Transformation $\Delta_C \to \Delta_D$ dasselbe wie ein Pfeil von C nach D.

(iii) Ist $\mathbf{I}$ wie in (ii), dann ist ein Funktor $F\colon \mathbf{I} \to \mathsf{Set}$ ein Diagramm $A_1 \leftarrow a_1 - A_0 - a_2 \rightarrow A_2$ von Mengen. Eine natürliche Transformation $A \to B$ ist dann ein Diagramm

$$\begin{array}{ccc} A & & \\ {\scriptstyle\gamma}\downarrow & & \\ B & & \end{array} \qquad \begin{array}{ccccc} A_1 & \xleftarrow[a_1]{} & A_0 & \xrightarrow{a_2} & A_2 \\ {\scriptstyle\gamma_1}\downarrow & & \mid{\scriptstyle\gamma_0}\downarrow & & \downarrow{\scriptstyle\gamma_2} \\ B_1 & \xleftarrow[b_1]{} & B_0 & \xrightarrow[b_2]{} & B_2 \end{array}$$

Ist C eine Menge, was ist dann eine natürliche Transformation $\gamma\colon \Delta_C \to B$?

$$\begin{array}{ccccc} & & C & & \\ & {\scriptstyle\gamma_1}\swarrow & \mid{\scriptstyle\gamma_0}\downarrow & \searrow{\scriptstyle\gamma_2} & \\ B_1 & \xleftarrow{} & B_0 & \xrightarrow{} & B_2 \end{array}$$

Satz I.1.10 (Yoneda-Lemma): *Seien* $\mathbf{C}$ *eine Kategorie und* $F\colon \mathbf{C}^{\mathsf{op}} \to \mathsf{Set}$. *Dann gibt es eine Bijektion*

$$\mathrm{Nat}(\mathbf{C}(-, C), F) \cong F(C).$$

Diese Bijektion ist natürlich in C *und* F.

Beweis: Sei $\alpha\colon \mathbf{C}(-, C) \to F$ eine natürliche Transformation, d. h. eine Familie von Pfeilen $\alpha_D\colon \mathbf{C}(D, C) \to F(D)$ sodass für alle $f\colon D \to D'$ das Diagramm

$$\begin{array}{ccc} \mathbf{C}(D', C) & \longrightarrow & F(D') \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathbf{C}(D, C) & \longrightarrow & F(D) \end{array}$$

insbesondere haben wir also für alle $g\colon D \to C$ das kommutative Diagramm

$$\begin{array}{ccccc} 1_C & & \mathbf{C}(C, C) & \xrightarrow{\alpha_C} & F(C) \\ \downarrow & & {\scriptstyle g^*}\downarrow & & \downarrow{\scriptstyle F(g)} \\ g & & \mathbf{C}(D, C) & \xrightarrow[\alpha_D]{} & F(D) \end{array} \qquad \begin{array}{ccc} & \overset{\curvearrowright}{} & \alpha_C(1_C) \\ & & \downarrow \\ & \underset{\curvearrowright}{} & \alpha_D(g) = F(g)(\alpha_C(1_C)) \end{array}$$

Nun definieren wir

$$\Phi\colon \operatorname{Nat}(\mathbf{C}(-,C),F) \longrightarrow F(C), \qquad \alpha \longmapsto \Phi(\alpha) = \alpha_C(1_C),$$

umgekehrt definieren wir $\Psi\colon F(C) \to \operatorname{Nat}(\mathbf{C}(-,C),F)$ durch

$$F(C) \ni x \longmapsto \mathbf{C}(-,C) \xrightarrow{\Psi(x)} F$$

mit den Komponenten

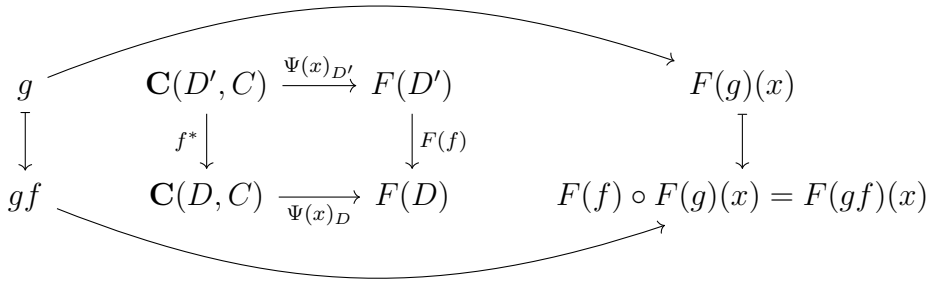
$$\mathbf{C}(D,C) \xrightarrow{\Psi(x)_D} F(D), \qquad g\colon D \xrightarrow{\Psi} C \longmapsto F(g)(x).$$

Dann gilt $\Psi \circ \Phi(\alpha) = \alpha$, denn

$$\Psi(\Phi(\alpha))_D(g) = F(g)(\Phi(\alpha)) = F(g)(\alpha_C(1_C)) = \alpha_D(g),$$

außerdem gilt $\Phi \circ \Psi(x) = \Psi(x)_C(1_C) = F(1_C)(x) = x$.

Sei nun $f\colon D \to D'$ aus $\mathbf{C}$. Wir müssen nachrrechnen, dass das Diagramm



kommutativ ist. □

Korollar I.1.11: *Es sei* $\mathbf{C}$ *eine kleine Kategorie. Dann ist der Funktor*

$$y\colon \mathbf{C} \to \operatorname{Fun}(\mathbf{C}^{\mathsf{op}}, \mathsf{Set}), \qquad C \longmapsto \mathbf{C}(-,C)$$

volltreu. Dabei wird $f\colon C \to D$ *auf* $y(f) = f_*\colon \mathbf{C}(-,C) \to \mathbf{C}(-,D)$ *mit*

$$\mathbf{C}(X,C) \longrightarrow \mathbf{C}(X,D), \qquad g \longmapsto fg$$

abgebildet.

Beweis: Es ist

$$\operatorname{Nat}(\mathbf{C}(-,C),\mathbf{C}(-,D)) \cong \mathbf{C}(-,D)(C) \cong \mathbf{C}(C,D).$$ □

2. Limiten und Kolimiten

Beispiel I.2.1: In der Kategorie Set seien zwei Mengen A, B gegeben. Das Produkt $A \times B := \{(a,b) \mid a \in A, b \in B\}$ kommt mit kanonischen Projektionen

$$\begin{array}{ccccc} A & \xleftarrow{p_A} & A \times B & \xrightarrow{p_B} & B \\ a & \longleftarrow\!\shortmid & (a,b) & \longmapsto & b \end{array}$$

Für jede Menge X mit zwei Abbildungen $A \leftarrow f_A - X - f_B \rightarrow B$ gibt es eine Abbildung $(f_A, f_B)\colon X \to A \times B$, $x \mapsto (f_A(x), f_B(x))$, sodass das Diagramm

$$\begin{array}{ccccc} & & X & & \\ & \swarrow^{f_A} & \downarrow{\scriptstyle \exists!\,(f_A,f_B)} & \searrow^{f_B} & \\ A & \xleftarrow[p_A]{} & A \times B & \xrightarrow[p_B]{} & B \end{array} \tag{I.1}$$

kommutiert. In der Tat ist (f_A, f_B) eindeutig festgelegt dadurch, dass Gl. (I.1) kommutieren soll.

Die beiden Mengen A, B entsprechend einem Funktor $F\colon \{1,2\} \to \mathsf{Set}$, mit $F(1) = A$, $F(2) = B$, und die beiden Projektionen p_A, p_B entsprechen einer natürlichen Transformation $\rho\colon \Delta_{A\times B} \to F$, wobei $\Delta_{A\times B}(1) = \Delta_{A\times B}(2) = A \times B$. Für jede natürliche Transformation $f\colon \Delta_X \to F$ gibt es genau einen Pfeil $\phi\colon X \to A \times B$, der das Diagramm

$$\begin{array}{ccccc} \Delta_X & \xrightarrow{\Delta_\phi} & \Delta_{A\times B} & \xrightarrow{\rho} & F \\ & \searrow & & \nearrow_{f} & \end{array}$$

kommutativ macht.

Das Diagramm Gl. (I.1) legt $A \times B$ hierbei eindeutig (bis auf Isomorphie) fest, denn Elemente von $A \times B$ sind Pfeile $\{\star\} \to A \times B$ und das entspricht nach Gl. (I.1) Paaren von Pfeilen $\{\star\} \to A$, $\{\star\} \to B$. Insgesamt sieht man also, dass Gl. (I.1) das Produkt von Mengen definiert.

Definition I.2.2 (Limes, Kolimes):

(i) Sei $F\colon \mathbf{I} \to \mathbf{C}$ ein Funktor. Ein Objekt L zusammen mit einer natürlichen Transformation $\lambda\colon \Delta_L \to F$ heißt *Limes von* F, wenn

$$\mathbf{C}(X, L) \longrightarrow \mathrm{Nat}(\Delta_X, F), \qquad \phi \longmapsto \lambda \circ \Delta_\phi$$

für alle $X \in \mathbf{C}$ eine Bijektion ist.

(ii) Ein Kolimes von F ist ein Limes in $\mathbf{C}^{\mathsf{op}}$, d. h. ein Objekt C zusammen mit $\gamma\colon F \to \Delta_C$, sodass

$$\mathbf{C}(C, X) \longrightarrow \mathrm{Nat}(F, \Delta_X), \qquad \phi \longmapsto \Delta_\phi \circ \gamma$$

für alle $X \in \mathbf{C}$ eine Bijektion ist.

Bemerkung I.2.3: (i) Die Bijektionen in Definition I.2.2 sind automatisch natürlich in X, d. h. es gibt natürliche Isomorphismen $\mathbf{C}(-, L) \simeq \mathrm{Nat}(\Delta_-, F)$.

(ii) Limiten und Kolimiten sind eindeutig bis auf eindeutige Isomorphie: Für je zwei Limiten L und L' gilt

$$\mathbf{C}(-, L) \simeq \mathrm{Nat}(\Delta_-, F) \simeq \mathbf{C}(-, L'),$$

nach dem Yoneda-Lemma gilt also $L = L'$. Wir schreiben $L = \lim F$ und $C = \operatorname{colim} F$.

Beispiel I.2.4: (i) Für $\mathbf{I} = \{1, 2\}$ ist ein Funktor $F\colon \mathbf{I} \to \mathbf{C}$ ist eine Wahl von zwei Objekten $A = F(1)$, $B = F(2)$. Ist $X \in \mathbf{C}$ ein beliebiges Objekt, so ist eine natürliche Transformation $\gamma\colon F \to \Delta_X$ nichts anderes als zwei Pfeile $\gamma_1\colon F(1) = A \to X$, $\gamma_2\colon F(2) = B \to X$. Ein Kolimes von F ist also ein Objekt $A \coprod B$ mit 2 Pfeilen $i_A\colon F(1) = A \to A \coprod B$, $i_B\colon F(2) = B \to A \coprod B$, sodass

$$\begin{array}{ccccc} A & \xrightarrow{f_A} & X & \xleftarrow{f_B} & B \\ & \searrow^{i_A} & \uparrow{\scriptstyle \exists!} & \swarrow_{i_B} & \\ & & A \coprod B & & \end{array}$$

Dieser spezielle Kolimes heißt Koprodukt. In Set ist $A \coprod B$ die disjunkte Vereinigung von A und B.

In geordneten Mengen ist das Koprodukt zweier Elemente p, q eine kleinste obere Schranke.

In k-Vr ist $V \oplus W$ das Koprodukt.

(ii) Ein Equalizer ist ein Limes von einem Diagramm der Form $\{1 \rightrightarrows 2\} = \mathbf{I}$. Ein Kolimes ist ein Koequalizer. Ein Funktor $F\colon \mathbf{I} \to \mathbf{C}$ entspricht der Wahl zweier Objekte $A, B \in \mathbf{C}$ und zweier paralleler Pfeile $f, g\colon A \to B$.

Ist $X \in \mathbf{C}$, so besteht eine natürliche Transformation $\alpha\colon \Delta_X \to F$ aus zwei Pfeilen $p_A\colon X \to A$, $p_B\colon X \to B$, sodass für alle $h \in \mathbf{I}$ das Diagramm

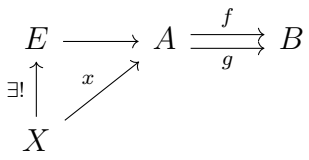
$$\begin{array}{ccc} X = \Delta_X(1) & \xrightarrow[1_X]{\Delta_X(h)} & \Delta_X(2) = X \\ \downarrow & & \downarrow \\ A = F(1) & \xrightarrow[F(h)]{} & F(2) = B \end{array}$$

kommutiert, d. h. die Diagramme

müssen kommutieren. Diese kommutieren genau dann, wenn $f \circ p_A = g \circ p_A = p_B$.

Eine natürliche Transformation $\Delta_X \to F$ ist also nichts anderes als ein Pfeil $p_A \colon X \to A$ mit $f \circ p_A = g \circ p_A$.

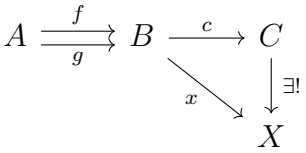
Ein Limes ist also ein Objekt E zusammen mit $e \colon E \to A$, sodass $f \circ e = g \circ e$ und



kommutiert für alle x mit $f \circ x = g \circ x$.

In Set ist $E = \{a \in A \mid f(a) = g(a)\}$ ein Equalizer.

Dual dazu ist ein Koequalizer von $f, g \colon A \to B$ ein Pfeil $c \colon B \to C$ mit $c \circ f = c \circ g$, sodass



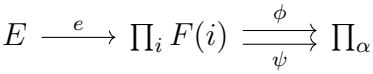
kommutiert für alle x mit $x \circ f = x \circ g$.

In Set ist der Koequalizer $C = B/\!\sim$, wobei „$\sim$“ die Äquivalenzrelation ist, die von $f(a) \sim f(b)$, $a \in A$, erzeugt wird.

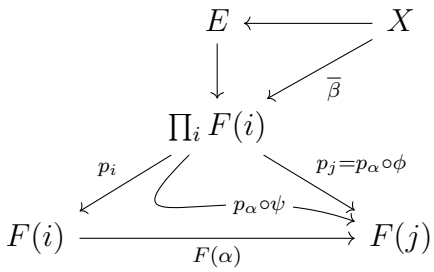
Satz I.2.5: *Hat* $\mathbf{C}$ *kleine Produkte und Equalizer, so hat* $\mathbf{C}$ *alle kleinen Limiten.*

Beweis: Seien $F \colon \mathbf{I} \to \mathbf{C}$ gegeben, wobei $\mathbf{I}$ eine kleine Kategorie sei. Für einen Pfeil $\alpha \colon i \to j$ aus I sei $F_\alpha = F(j)$. Wir bekommen zwei Pfeile $\psi, \phi \colon \prod_{i \in I} F(i) \rightrightarrows \prod_\alpha F_\alpha$ via

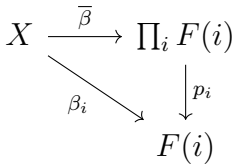
Der Equalizer



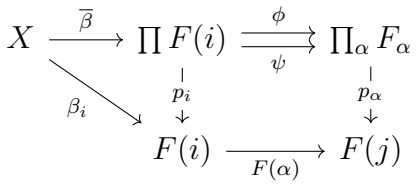
ist ein Limes von F mit Limeskegel



Um nachzurechnen, dass $E \cong \lim F$, wählt man einen Kegel $\beta\colon \Delta_X \to F$ und bekommt einen induzierten Pfeil



Es gilt jetzt $\phi \circ \overline{\beta} = \psi \circ \overline{\beta}$, weil das Diagramm



und $p_\alpha \circ \phi \circ \overline{\beta} = \beta_j$, also $\phi \circ \overline{\beta} = \psi \circ \overline{\beta}$. Das gibt, dass es genau ein $X \to E$ mit ... gibt. □

Korollar I.2.6: *Die Kategorie* Set *hat alle kleinen Limiten und Kolimiten.*

Satz I.2.7: *Hat* $\mathbf{C}$ *alle kleinen Limiten (Kolimiten) und ist* $\mathbf{I}$ *klein, dann hat auch* $\mathrm{Fun}(\mathbf{I}, \mathbf{C})$ *alle kleinen Limiten (Kolimiten) und diese werden punktweise ausgerechnet, d. h. für* $F\colon \mathbf{J} \to \mathrm{Fun}(\mathbf{I}, \mathbf{C})$ *ist*

$$(\lim F)(i) = \lim F_i, \qquad \textit{wobei } F_i(j) = F(j)(i).$$

Zum Beispiel ist $(F \times G)(i) = F(i) \times G(i)$.

Bemerkung I.2.8: Limiten sind funktoriell in dem Sinne, dass für eine natürliche Transformation $\alpha\colon F \to G$ die Komposition

$$\begin{array}{ccc} \mathbf{C}(-, \lim F) & \xrightarrow{\cong} & \mathrm{Nat}(\Delta_-, F) \\ & \swarrow^{\alpha_*} & \\ \mathrm{Nat}(\Delta_-, G) & \xrightarrow{\cong} & C(-, \lim G). \end{array}$$

nach dem Yoneda-Lemma einen Pfeil $\lim F \to \lim G$ induziert.

Insbesondere ist $\lim\colon \mathrm{Fun}(\mathbf{I}, \mathbf{C}) \to \mathbf{C}$ ein Funktor, wenn $\mathbf{C}$ alle Limiten von Form $\mathbf{I}$ besitzt.

3. Adjunktionen

Beispiel I.3.1: (i) Es sei $U\colon k\text{-}\mathsf{Vr} \to \mathsf{Set}$, $V \mapsto V$, $f \mapsto f$ der Vergissfunktor für Vektorräume. Für jede Menge X gibt es einen Vektorraum mit Basis X, nämlich $F(X) = \bigoplus_{x \in X} k$. Eine lineare Abbildung $F(X) \to V$ ist eindeutig bestimmt durch die Bilder der Basisvektoren, d. h. $k\text{-}\mathsf{Vr}(F(X), V) \cong \mathsf{Set}(X, UV)$. Diese Bijektion ist natürlich in beiden Variablen.

(ii) Ist $\mathbf{C}$ eine Kategorie, die alle Limiten von Form $\mathbf{I}$ hat, dann haben wir uns gerade davon überzeugt, dass $\lim\colon \mathrm{Fun}(\mathbf{I}, \mathbf{C}) \to \mathbf{C}$ ein Funktor ist und es gilt

$$\mathrm{Fun}(\mathbf{I}, \mathbf{C})(\Delta_X, F) \cong \mathbf{C}(X, \lim F).$$

Definition I.3.2: Ein Funktor $F\colon \mathbf{C} \to \mathbf{D}$ heißt *linksadjungiert* zu $U\colon \mathbf{D} \to \mathbf{C}$, wenn es eine natürliche Bijektion $\mathbf{D}(FC, D) \simeq \mathbf{C}(C, UD)$ gibt. Die Natürlichkeit bedeutet hier, dass für alle $f\colon C' \to C$ und $g\colon D \to D'$ das Diagramm

$$\begin{array}{ccc} \mathbf{D}(FC, D) & \xrightarrow{\simeq} & \mathbf{C}(C, UD) \\ {\scriptstyle g\circ(-)\circ F_f}\downarrow & & \downarrow{\scriptstyle U_g\circ(-)\circ f} \\ \mathbf{D}(FC', D') & \xrightarrow[\simeq]{} & \mathbf{C}(C', UD') \end{array}$$

kommutiert. U heißt *rechtsadjungiert zu* F und man schreibt $F \dashv U$.

Bemerkung I.3.3: (i) Adjungierte sind eindeutig bis auf eindeutige Isomorphie, denn für zwei rechtsadjungierte $F \dashv U$, $F \dashv U'$ ist

$$\mathbf{C}(-, UD) \simeq \mathbf{D}(F(-), D) \simeq \mathbf{C}(-, U'D).$$

(ii) Adjunktionen komponieren, d. h. für

$$\mathbf{C} \underset{U}{\overset{F}{\rightleftarrows}} \mathbf{D} \underset{V}{\overset{G}{\rightleftarrows}} \mathbf{E}$$

ist $\mathbf{E}(GFC, E) \simeq \mathbf{D}(FC, VE) \cong \mathbf{C}(C, UVE)$, also $GF \dashv UV$.

(iii) Ist $F \dashv U$, so induziert der Isomorphismus $\mathbf{C}(F-,-) \simeq \mathbf{D}(-,U-)$ eine Bijektion zwischen kommutativen Quadraten

$$\begin{array}{ccc} FC & \xrightarrow{\alpha} & D \\ {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle g} \\ FC' & \xrightarrow[\beta]{} & D' \end{array} \qquad\qquad \begin{array}{ccc} C & \xrightarrow{\phi(\alpha)} & UD \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle Ug} \\ C' & \xrightarrow[\phi(\beta)]{} & UD' \end{array}$$

Insbesondere gibt es eine Bijektion $\mathrm{Nat}(F \circ G, H) \cong \mathrm{Nat}(G, U \circ H)$ für alle Funktoren $G\colon \mathbf{I} \to \mathbf{C}$ und $H\colon \mathbf{I} \to \mathbf{D}$.

(iv) Linksadjungierte erhalten alle Kolimiten, Rechtsadjungierte erhalten alle Limiten. Ist nämlich $F\colon \mathbf{C} \to \mathbf{D}$ linksadjungiert zu $U\colon \mathbf{D} \to \mathbf{C}$, und ist $G\colon \mathbf{I} \to \mathbf{C}$ ein Funktor, dann ist

$$\mathbf{D}(F(\operatorname{colim} G), -) \simeq \mathbf{C}(\operatorname{colim} G, U(-)) \simeq \mathrm{Nat}(G, \Delta_{U(-)}) = \mathrm{Nat}(F \circ G, \Delta_-),$$

d. h. $F(\operatorname{colim} G) = \operatorname{colim}(FG)$.

Beispiel I.3.4: (i) Der Funktor $V \otimes_k (-)\colon k\text{-}\mathsf{Vr} \to k\text{-}\mathsf{Vr}$ ist linksadjungiert zum Funktor $\mathrm{Hom}_k(V, -)$, denn

$$k\text{-}\mathsf{Vr}(V \otimes_k X, Y) \simeq k\text{-}\mathsf{Vr}(X, \mathrm{Hom}_k(V, Y)).$$

Daraus folgt sofort, dass $V \otimes_k (A \oplus B) \simeq (V \otimes_k A) \oplus (V \otimes_k B)$, oder für die Sequenz

$$A \xrightarrow{f} B \twoheadrightarrow B/\operatorname{im} f$$

zu der die Sequenz gehört

$$V \otimes_k A \xrightarrow{V \otimes f} V \otimes_k B \twoheadrightarrow V \otimes_k (B/\operatorname{im} f) = V \otimes_k B/\operatorname{im}(V \otimes f)$$

gibt es $V \otimes_k (B/\operatorname{im} f) = V \otimes_k B/\operatorname{im}(V \otimes f)$ gratis.

(ii) Zu der Sequenz $\ker(f) \longrightarrow A \xrightarrow{f} B$ gehört die Sequenz

$$\ker(f_*) = \mathrm{Hom}_k(V, \ker(f)) \longrightarrow \mathrm{Hom}_k(V, A) \xrightarrow{f_*} \mathrm{Hom}_k(V, B)$$

und wieder gibt es $\ker(f_*) = \mathrm{Hom}_k(V, \ker(f))$ gratis, wobei

$$f_*\colon \mathrm{Hom}_k(V, A) \longrightarrow \mathrm{Hom}_k(V, B), \qquad \alpha \longmapsto f \circ \alpha.$$

(iii) In Set funktioniert exakt dasselbe Beispiel mit $(X \times -) \dashv \mathrm{Abb}(X, -)$.

(iv) Sei S der Funktor

$$S\colon k\text{-}\mathsf{Vr} \longrightarrow k\text{-}\mathsf{Alg}, \qquad V \longmapsto S(V) = \bigoplus_{n\in\mathbb{N}} T^n(V)/(\text{passendes Ideal}).$$

Dann ist $S \dashv U$ mit $U(V) = V$. In k-Alg ist $A \otimes_k B$ das Koprodukt von A und B. Das heißt $S(V \oplus W) \simeq S(V) \otimes_k S(W)$.

(v) Der Limes-Funktor $\lim\colon \mathrm{Fun}(\mathbf{I}, \mathbf{C}) \to \mathbf{C}$ ist Rechtsadjungierter (falls $\mathbf{C}$ alle Limiten von Form $\mathbf{I}$ hat), d. h. lim bildet Limiten auf Limiten ab. Ist $G\colon \mathbf{J} \times \mathbf{I} \to \mathbf{C}$ ein Funktor, dann ist $\lim_j \lim_i G(i,j) \simeq \lim_i \lim_j G(i,j)$, falls diese Limiten existieren.

Kapitel II.

Gruppen

1. Gruppen und Grundlagen

Definition II.1.1: Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. N heißt *Normalteiler*, falls für alle $x \in G$ gilt $xNx^{-1} = N$. Wir schreiben in diesem Fall $N \triangleleft G$.

N ist ein Normalteiler genau dann, wenn für alle $x \in G$ gilt $xNx^{-1} \subseteq N$, denn für beliebiges $x \in G$ ist $N = xx^{-1}Nxx^{-1} \subseteq xNx^{-1}$.

Beispiel II.1.2: (i) Es sei $f\colon G \to H$ ein Homomorphismus von Gruppen. Dann ist $\ker f$ ein Normalteiler, denn für $x \in \ker f$ und $y \in G$ ist

$$f(yxy^{-1}) = f(y)f(x)f(y)^{-1} = e_H,$$

also $yxy^{-1} \in \ker f$ und damit $y \ker f y^{-1} \subseteq \ker f$.

(ii) In abelschen Gruppen sind alle Untergruppen Normalteiler.

(iii) Die trivialen Untergruppen $\{e_G\}$, G von G sind Normalteiler.

(iv) Die spezielle lineare Gruppe $\mathrm{Sl}_n(k)$ ist ein Normalteiler in $\mathrm{Gl}_n(k)$, denn für $A \in \mathrm{Sl}_n(k)$ und $X \in \mathrm{Gl}_n(k)$ ist wegen der Multiplikativität der Determinante

$$\det(XAX^{-1}) = \det(X)\det(A)\det(X)^{-1} = 1.$$

Dies ist ein Spezialfall von (i), da $\mathrm{Sl}_n(k) = \ker \det$.

(v) In S_n ($n \geq 2$) ist $U = \{(12), \mathrm{id}\}$ eine Untergruppe, die wegen

$$(23)(12)(23) = (13)$$

in S_n für $n \geq 3$ keine normale Untergruppe ist.

Bemerkung II.1.3: (i) Ist N ein Normalteiler in der Gruppe G, dann wird G/N zu einer Gruppe mit der Verknüpfung

$$(xN) \cdot (yN) = xyN.$$

Zur Wohldefiniertheit: Seien $x^{-1}\hat{x} \in N$ und $y^{-1}\hat{y} \in N$. Dann gilt

$$(xy)^{-1}(\hat{x}\hat{y}) = y^{-1}x^{-1}\hat{x}\hat{y} = y^{-1}x^{-1}\hat{x}yy^{-1}\hat{y} \in N,$$

da $x^{-1}\hat{x} \in N$ und somit auch $y^{-1}(x^{-1}\hat{x})y \in N$ und außerdem $y^{-1}\hat{y} \in N$, $y^{-1}x^{-1}\hat{x}yy^{-1}\hat{y} \in N$. Das neutrale Element in G/N ist N.

(ii) Die Abbildung

$$\pi\colon G \longrightarrow G/N, \qquad g \longmapsto gN$$

ist ein surjektiver Gruppenhomorphismus mit $\ker \pi = N$.

Satz II.1.4: *Seien G eine Gruppe, $f\colon G \to H$ ein Homomorphismus von Gruppen und $N \triangleleft G$ mit $\ker(f) \supseteq N$. Dann gibt es genau $f'\colon G/N \to H$, sodass das Diagramm*

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow^{f} & \downarrow{\scriptstyle f'} \\ & & H \end{array}$$

kommutiert. Ist $\ker f = N$, so ist f' injektiv.

Beweis: Setze $f'(gN) = f(g)$. Das ist wohldefiniert, denn für $g, \hat{g} \in G$ mit $g^{-1}\hat{g} \in N$ ist $1 = f(g^{-1}\hat{g}) = f(g)^{-1}f(\hat{g})$, d. h. $f(g) = f(\hat{g})$.

Außerdem ist f' ein Gruppenhomomorphismus, denn

$$f'(gN \cdot hN) = f'(ghN) = f(gh) = f(g)f(h) = f'(gN)f'(hN).$$

Da $\ker f' = \pi(\ker f)$ ist im Fall $N = \ker f$ schon f' injektiv. □

Satz II.1.5: *Seien G eine Gruppe, $N \triangleleft G$ und $U \subseteq G$ eine Untergruppe.*

(i) *Die Menge $NU = \{nu \mid n \in N, u \in U\} \subseteq G$ ist eine Untergruppe,*

(ii) *Es gelten $N \triangleleft NU$, $N \cap U \triangleleft U$ und $NU/N \simeq U/N \cap U$.*

Beweis: (i) Offensichtlich ist $NU \neq \varnothing$. Sind jetzt $nu, \hat{n}\hat{u} \in NU$, dann ist $(nu)^{-1} = u^{-1}n^{-1} = u^{-1}n^{-1}uu^{-1} \in NU$ und $(nu)(\hat{n}\hat{u}) = nu\hat{n}\hat{u} = nu\hat{n}u^{-1}u\hat{u} \in NU$.

(ii) Die Aussagen $N \triangleleft NU$ und $N \cap U \triangleleft U$ sind klar. Zur letzten Aussage: Die Abbildung

$$\phi\colon U \longrightarrow NU, \qquad u \longmapsto u$$

ist ein Gruppenhomomorphismus und die Abbildung

$$\psi\colon U \longrightarrow NU/N, \qquad u \longmapsto uN$$

ist surjektiv, da $nuN = uu^{-1}nuN = uN$. Jetzt ist das Diagramm

$$\begin{array}{ccc} U & \xrightarrow{\phi} & NU \\ {\scriptstyle \pi_1}\downarrow & \searrow^{\psi} & \downarrow{\scriptstyle \pi_2} \\ U/N \cap U & \xrightarrow[\phi']{} & NU/N \end{array}$$

kommutativ mit $\ker(\pi \circ \phi) = N \cap U$, d. h. $U/N \cap U \simeq NU/N$ wie gewünscht. □

Definition II.1.6: Seien G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe. Dann heißt $[G : U] := \#(G/U) = \#(G)/\#(U)$ der *Index von U in G*.

2. Gruppenoperationen und die Sätze von Sylow

Definition II.2.1: Es seien G eine Gruppe und X eine Menge.

(i) Wir schreiben dafür, dass G auf der Menge X operiert, $G \curvearrowright X$.

(ii) Die Bahn eines $x \in X$ ist $Gx = \{gx \mid g \in G\} \subseteq X$.

(iii) Der Stabilisator eines $x \in X$ ist $G_x = \{g \in G \mid gx = x\} \subseteq G$.

Bemerkung II.2.2: (i) Die Abbildung

$$G/G_x \longrightarrow Gx, \qquad gG_x \longmapsto gx$$

ist eine Bijektion.

(ii) Insbesondere für endliche Mengen X erhalten wir die *Bahnenformel*

$$\#(X) = \sum_{i=1}^{r} \#(Gx_i) = \sum_{i=1}^{r} [G : G_{x_i}],$$

wobei $x_1, \ldots, x_r$ ein Repräsentantensystem der Bahnen ist.

Satz II.2.3 (Sylow-Sätze): *Seien G eine endliche Gruppe, $p \in \mathbb{N}$ eine Primzahl und $\#(G) = p^e m$ mit $p \nmid m$.*

(i) *Für jedes $0 \leq d \leq e$ gibt es eine Untergruppe U von G mit $\#(U) = p^d$. Die Untergruppen mit p^e-vielen Elementen heißen* p-Sylowgruppen von G.

(ii) *Ist $S \subseteq G$ eine p-Sylowgruppe und ist $U \subseteq G$ eine Untergruppe mit $\#(U) = p^d$, dann gibt es ein $x \in G$ mit $xUx^{-1} \subseteq S$. Insbesondere sind je zwei p-Sylowgruppen S, T zueinander konjugiert, d. h. es gibt ein $x \in G$, sodass $x^{-1}Sx = T$.*

(iii) *Die Anzahl s_p der p-Sylowgruppen in G erfüllt $s_p \equiv 1 \pmod{p}$ und $s_p \mid m$.*

Beweis: (i) Setze $X := \{M \subseteq G \mid \#(M) = p^d\}$. Ohne Einschränkung sei $d \geq 1$. Wir behaupten, dass $p^{e-d+1} \nmid \#(X)$. Das hätte (i) zur Folge, da G auf X durch Linksmultiplikation operiert und deshalb

$$\#(X) = \sum_{i=1}^{r} [G : G_{M_i}]$$

gilt, wenn $M_1, \ldots, M_r$ ein Repräsentantensystem der Bahnen ist, d. h. es gibt $M \in X$ mit $p^{e-d+1} \nmid [G : G_M] = \#(G)/\#(G_M) = p^e m/\#(G_M)$, also muss gelten $p^d \mid \#(G_M)$. Andererseits ist die Abbildung $G_M \to M$, $g \mapsto gx$ injektiv für ein festes $x \in M$, d. h. $\#(G_M) = p^d$ und G_M ist eine Untergruppe.

Zum Beweis unserer Behauptung: Es gilt

$$\begin{aligned}
\#(X) &= \binom{p^e m}{p^d} \\
&= \frac{(p^e m)!}{(p^d)!(p^e m - p^d)!} \\
&= \frac{(p^e m - 0)(p^e m - 1)\cdots(p^e m - p^d + 1)}{(p^d - 0)(p^d - 1)\cdots(p^d - p^d + 1)} \\
&= p^{e-d} m \prod_{i=1}^{p^d - 1} \frac{p^e m - i}{p^d - i} \\
&= p^{e-d} m \prod_{i=1}^{p^d - 1} \frac{p^e m - p^{f_i} m_i}{p^d - p^{f_i} m_i} && (p \nmid m_i, f_i < d) \\
&= p^{e-d} m \prod_{i=1}^{p^d - 1} \frac{p^{e-f_i} m - m_i}{p^{d-f_i} - m_i},
\end{aligned}$$

das heißt die größte p-Potenz in $\#(X)$ ist p^{e-d}.

(ii) Ohne Einschränkung sei $d \geq 1$. Wir setzen $\mathfrak{S} := \{gSg^{-1} \mid g \in G\}$ und stellen fest, dass G per Konjugation auf $\mathfrak{S}$ operiert – sogar transitiv wegen der Definition von $\mathfrak{S}$. Damit ist $\#(S) = [G : G_S]$, wobei G_S der Stabilisator von $S \in \mathfrak{S}$ ist. Per Definition von G_S ist $S \lhd G_S$, weshalb $p^e \mid G_S$. Insbesondere muss also wegen $\#(\mathfrak{S}) = \#(G)/\#(G_S)$ schon $\#(\mathfrak{S})$ ein Teiler von m sein. Auch U operiert durch Konjugation auf $\mathfrak{S}$ und wir erhalten

$$\#(\mathfrak{S}) = \sum_{i=1}^{r} [U : U_{T_i}]$$

wobei T_i ein Repräsentantensystem der Bahnen durchläuft. Da die linke Seite nicht von p geteilt wird, kann auch die rechte Seite nicht von p geteilt werden; da alle Summanden p-Potenzen sind, muss es also $T \in \mathfrak{S}$ geben mit $[U : U_T] = 1$, d. h. $U = U_T$; insbesondere $U \subseteq G_T$. Jetzt haben wir dass $T \lhd G_T$ und dass $U \subseteq G_T$ eine Untergruppe ist, also ist $UT \subseteq G_T$ eine Untergruppe und $UT/T \simeq U/U \cap T$. Mit dem Satz von Lagrange erhalten wir daraus

$$\#(UT) = \frac{\#(U)\#(T)}{\#(U \cap T)}.$$

Schreiben wir $\#(UT) = p^e n$ mit $p \nmid n$, dann liefert das $p^e n = p^d p^e / x$, also $n = 1$. Dann muss aber schon $UT = T$ gelten, also $U \subseteq T$, d. h. es gibt $g \in G$ mit $U \subseteq gSg^{-1}$.

(iii) Wegen (ii) wissen wir, dass $\mathfrak{S}$ genau die Menge der p-Sylowgruppen ist. Aus (ii) wissen wir, dass $\#(\mathfrak{S})$ ein Teiler von m ist. Im Beweis von Teil (ii) ist außerdem enthalten, dass $\#(\mathfrak{S}) \equiv 1 \pmod{p}$, da

$$\#(\mathfrak{S}) = \sum_{i=1}^{r} [S : S_{T_i}]$$

mit $[S : S_S] = 1$ und $p \mid [S : S_T]$ für $T \neq S$, denn wenn $[S : S_T] = 1$, dann erhalten wir mit dem Argument aus (ii) für diesen Fall, dass $S \subseteq T$, also $S = T$. □

Beispiel II.2.4: (i) Sei G eine nicht-abelsche Gruppe der Ordnung $6 = 2 \cdot 3$. Wegen Satz II.2.3 gibt es x und y in G mit $\mathrm{ord}(x) = 2$, $\mathrm{ord}(y) = 3$. Aber dann kennen wir schon ganz G, denn dann ist $G = \{1, x, y, y^2, xy, xy^2\}$. In G muss yx enthalten sein; es ist $yx \neq xy$, da sonst G abelsch wäre. Durch Fallunterscheidung erkennt man $yx = xy^2$. Damit ist $G \simeq S_3$.

(ii) Sei G eine Gruppe mit $\#(G) = 15$. Dann ist $s_5 = 1$. Genauso ist $s_3 = 1$. Da p-Sylowgruppen konjugiert zueinander sind, sind sowohl die 3-Sylowgruppe als auch die 5-Sylowgruppe normal in G. Insbesondere erhalten wir

$$S_5 \xrightarrow{\triangleleft} G \twoheadrightarrow G/S_5 \simeq C_3 \qquad\qquad S_3 \xrightarrow{\triangleleft} G \twoheadrightarrow G/S_3 \simeq C_5,$$

d. h. es gibt einen Homomorphismus $\phi\colon G \to C_5 \times C_3$ mit $\ker\phi = S_5 \cap S_3 = \{1\}$, also ist ϕ ein Isomorphismus.

(iii) Sei G eine endliche abelsche Gruppe. Dann gibt es zu jedem Primfaktor von $\#(G) = \prod_{i=1}^{r} p_i^{\mu_i}$ genau eine p-Sylowgruppe $S_p \subseteq G$. Wir haben also einen Homomorphismus

$$\prod_{i=1}^{r} S_{p_i} \longrightarrow G, \qquad (x_1, \ldots, x_r) \longmapsto x_1 \cdots x_r$$

und genauer ist das sogar ein Isomorphismus von Gruppen mit den Argumenten aus (ii).

Definition II.2.5 (Konjugationsklasse, Zentralisator, Zentrum):

(i) Sei G eine Gruppe, die auf sich selbst durch Konjugation operiere. Die Bahn eines Elements $x \in G$ heißt *Konjugationsklasse*, geschrieben $GxG^{-1} = \{gxg^{-1} \mid g \in G\}$. Insbesondere bilden die Konjugationsklassen eine Partition von G.

(ii) Der Stabilisator von $x \in G$, geschrieben $C(x) = \{g \in G \mid gxg^{-1} = x\}$, heißt *Zentralisator von x in G*.

(iii) Ist G eine endliche Gruppe, dann liefert die Bahnformel

$$\#(G) = \sum_{x_i} [G : C(g_i)]$$

wobei x_i ein Vertretersystem der Konjugationsklassen durchläuft.

(iv) Die Menge $Z(G) = \{g \in G \mid gx = xg \,\forall\, x \in G\}$ heißt *Zentrum von G*. Das Zentrum ist abelsch und per Definition ein Normalteiler in G.

(v) Offenbar ist $x \in Z(G)$ genau dann, wenn $C(x) = G$. Teil (iii) gibt uns

$$\#(G) = \#(Z(G)) + \sum_{x_i} [G : C(x_i)]$$

wobei x_i ein Vertretersystem der nicht-trivialen Konjugationsklassen durchläuft.

Beispiel II.2.6: (i) Seien e eine natürliche Zahl, p eine Primzahl und G eine endliche Gruppe mit $\#(G) = p^e$. Dann sagt Definition II.2.5 (v), dass $p \mid \#(Z(G))$, insbesondere $Z(G) \neq \{1\}$.

(ii) Ist p eine Primzahl und G eine endliche Gruppe mit $\#(G) = p^2$, dann ist G abelsch. Das sieht man so: $Z(G) = \{1\}$ ist ausgeschlossen nach (i). Ist $\#(Z(G)) = p^2$, dann ist G schon abelsch. Im Fall $\#(Z(G)) = p$ ist $Z(G)$ ein Normalteiler in G mit Index p, d. h.

$$Z(G) \xrightarrow{\triangleleft} G \xrightarrow{\pi} G/Z(G) \simeq C_p.$$

Seien jetzt $g \in C_p$ ein Erzeuger und $\xi \in G$ mit $\pi(\xi) = g$. Für alle $x \in G$ ist also $\pi(x) = g^a$ mit $a \in \mathbb{Z}$, d. h. $x\xi^{-a} \in \ker(\pi) = Z(G)$. Für jedes $x \in G$ gibt es also $a \in \mathbb{Z}$ und $z \in Z(G)$, sodass $x = \xi^a z$. Dann ist aber

$$xy = (\xi^a z)(\xi^b z') = \xi^b z' \xi^a z = yx.$$

3. Einfache- und auflösbare Gruppen

Um endliche Gruppen zu klassifizieren, reicht es Gruppen ohne Normalteiler zu klassifizieren und für gegebenes N und H diejenigen Gruppen G zu finden, sodass $N \triangleleft G$ mit $G/N \simeq H$ gilt.

Definition II.3.1: Eine Gruppe G heißt *einfach*, falls G und $\{1_G\}$ die einzigen Normalteiler von G sind.

Beispiel II.3.2: (i) Die Abbildung $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ ist ein surjektiver Gruppenhomomorphismus mit $\ker \operatorname{sgn} =: A_n$, die sogenannte *alternierende Gruppe*. Da $\#(A_n) = n!/2$ (Homomorphiesatz, Satz von Lagrange), ist A_n ein echter Normalteiler; S_n ist also nicht einfach.

(ii) Ist G eine einfache abelsche Gruppe und $x \in G - \{1_G\}$. Dann ist $\{1_G\} \neq \langle x \rangle \triangleleft G$; d. h. einfache abelsche Gruppen sind zyklisch.

Hat x unendliche Ordnung, dann ist $\langle x^2 \rangle \subseteq G$ ein nicht-trivialer Normalteiler; damit kann G nur endlich sein.

Hat x die Ordnung $\operatorname{ord}(x) = rs$ mit $r, s \neq 1$, dann ist $\langle x^r \rangle \subsetneq G$ eine Gruppe mit s-vielen Elementen, d. h. $x \in G - \{1_G\}$ muss Primzahlordnung haben.

Zusammengefasst: Eine abelsche Gruppe ist genau dann einfach, wenn sie zyklisch und von Primzahlordnung ist.

Definition II.3.3: (i) Eine echt absteigende Kette $G = G_0 \supset G_1 \supset \cdots \supset G_m$ von Untergruppen von G heißt *Subnormalreihe von* G, falls für alle

$0 \leq i < m$ gilt, dass $G_{i+1} \triangleleft G_i$. Die Gruppen G_i/G_{i+1} heißen *Faktoren der Subnormalreihe.*

(ii) Eine *Verfeinerung einer Subnormalreihe von G* ist eine Subnormalreihe, die durch Einfügen von endlich vielen weiteren Untergruppen entsteht.

(iii) Eine Subnormalreihe heißt *Kompositionsreihe*, wenn $G_m = \{1_G\}$ und sie sich nicht weiter verfeinern lässt, d. h. wenn die Faktoren der Subnormalreihe einfache Gruppen sind.

Lässt sich die Subnormalreihe verfeinern, sagen wir $G_{i+1} \subsetneq N \subsetneq G_i$ mit $N \triangleleft G_i$. Dann ist $\pi(N) \subseteq G_i/G_{i+1}$, wobei $\pi\colon G_i \to G_i/G_{i+1}$ die kanonische Projektion bezeichnet, eine nicht-triviale Untergruppe. Sie ist sogar normal, denn für $x \in G_i/G_{i+1}$ gibt es $y \in G_i$ mit $\pi(y) = x$ und dann ist

$$x\pi(N)x^{-1} = \pi(y)\pi(N)\pi(y)^{-1} = \pi(yNy^{-1}) = \pi(N),$$

d. h. G_i/G_{i+1} ist nicht einfach.

Sind umgekehrt die Faktoren einer Subnormalreihe nicht alle einfach, sagen wir $\{1_G\} \neq N \triangleleft G_i/G_{i+1}$, dann ist $\pi^{-1}(N)$ ein nicht-trivialer Normalteiler zwischen G_i und G_{i+1}.

Mit den Argumenten, die wir gerade benutzt haben, haben wir allgemeiner gezeigt: Bilder von Normalteilern unter surjektiven Gruppenhomomorphismen sind Normalteiler, Urbilder von Normalteilern unter Gruppenhomomorphismen sind Normalteiler.

Beispiel II.3.4: (i) Jede endliche Gruppe hat eine Kompositionsreihe.

(ii) Die Gruppe $(\mathbb{Z}, +)$ hat keine Kompositionsreihe, denn jede Subnormalreihe lässt sich verfeinern; für je zwei natürliche Zahlen n und m gilt $n\mathbb{Z} \supseteq mn\mathbb{Z}$.

(iii) Die Subnormalreihe $C_6 = \langle x \rangle \supseteq \langle x^2 \rangle \supseteq \{1_G\}$ ist eine Kompositionsreihe und $C_6 = \langle x \rangle \supseteq \langle x^3 \rangle \supseteq \{1_G\}$ ist eine andere Kompositionsreihe von C_6.

(iv) In S_3 ist A_3 ein Normalteiler; $A_3 = \langle (123) \rangle$, denn $\#(S_3) = 6$, $\#(A_3) = 3$ und

$$\langle (123) \rangle = \{(123), (132), \mathrm{id}\}.$$

Dann ist $S_3 \supseteq A_3 \supseteq \{\mathrm{id}\}$ eine Kompositionsreihe.

(v) In S_4 ist A_4 ein Normalteiler. Die Teilmenge

$$V = \{\sigma \in A_4 \mid \sigma \text{ hat keinen Fixpunkt oder } \sigma = \mathrm{id}\} \subseteq A_4$$

ist eine Untergruppe; außerdem ist V normal, denn hätte $\mathrm{id} \neq f\sigma f^{-1}$ einen Fixpunkt, also $f\sigma f^{-1}(i) = i$ für ein $1 \leq i \leq 4$, dann hätten wir bereits

$\sigma f^{-1}(i) = f^{-1}(i)$ und σ hätte bereits einen Fixpunkt gehabt. Man überlegt sich, dass V die Menge

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

sein muss. Damit haben wir eine Subnormalreihe $S_4 \supset A_4 \supset V \supset \{\mathrm{id}\}$ von S_4. Diese ist allerdings noch keine Kompositionsreihe.

Bemerkung II.3.5: (i) Ist $f\colon G \to H$ ein Gruppenhomomorphismus und $H = H_0 \supset \cdots \supset H_m$ eine Subnormalreihe von H, dann ist $G = G_0 \supset \cdots \supset G_m$ mit $G_i := f^{-1}(H_i)$ eine Subnormalreihe von G (nach eventuellem Entfernen von Wiederholungen). Der Kern von $f|_{G_i}\colon G_i \to H_i \to H_i/H_{i+1}$ ist G_{i+1}, d. h. $G_i/G_{i+1} \hookrightarrow H_i/H_{i+1}$.

(ii) Ist $f\colon G \to H$ ein surjektiver Homomorphismus und $G = G_0 \supset \cdots \supset G_m$ ist eine Subnormalreihe von G, dann ist $H = H_0 \supset \cdots \supset H_m$ mit $H_i = f(G_i)$ (nach eventuellem Entfernen von Duplikaten) eine Subnormalreihe von H.

Wir haben $G \cong H/\ker(f)$, d. h. wir können auch die Subnormalreihe in $G/\ker(f)$ ausrechnen. Es ist

$$\overline{f}(\pi(G_i)) = f(G_i) = H_i = \pi(G_i) = G_i/G_i \cap \ker(f) \cong G_i \ker(f)/\ker(f),$$

also können wir ausrechnen

$$H_i/H_{i+1} \cong [G_i \ker(f)/\ker(f)]/[(G_{i+1} \ker(f)/\ker(f)] \cong G_i \ker(f)/G_{i+1} \ker(f),$$

und wir sind in der Situation

$$\begin{array}{ccc} G_i & \longrightarrow & G_i \ker(f) \\ \downarrow & \overset{\phi}{\searrow} & \downarrow \\ G_i/G_{i+1} & \underset{\exists!}{\cdots\!\!\twoheadrightarrow} & G_i \ker(f)/G_{i+1} \ker(f) \end{array}$$

wobei $G_{i+1} \subseteq \ker(\phi)$ und der Homomorphiesatz gibt die eindeutige surjektive Abbildung $G_i/G_{i+1} \twoheadrightarrow G_i \ker(f)/G_{i+1} \ker(f)$.

Definition II.3.6: Zwei Subnormalreihen $G = G_0 \supset \cdots \supset G_r$, $G = G'_0 \supset \cdots \supset G'_s$ heißen äquivalent, falls $r = s$ und es $\sigma \in S_r$ gibt, sodass für alle $1 \leq i \leq r$ gilt: $G_{i-1}/G_i \cong G'_{\sigma(i)-1}/G'_{\sigma(i)}$.

Satz II.3.7 (Jordan-Hölder-Schreier): *Sind $G = G_0 \supset \cdots \supset G_r = \{1\}$ und $G = H_0 \supset \cdots \supset H_s = \{1\}$ zwei Subnormalreihen von G, dann gibt es äquivalente Verfeinerungen der beiden Subnormalreihen. Insbesondere sind Kompositionsreihen eindeutig bis auf Äquivalenz.*

Beweis: Für jedes i ist $G_i = G_i \cap H_0 \supset \cdots \supset G_i \cap H_s = \{1\}$ eine Subnormalreihe in G_i. Wir wollen zeigen, dass dann auch

$$G_i = (G_i \cap H_0)G_{i+1} \supset \cdots \supset (G_i \cap H_s)G_{i+1} = G_{i+1}$$

eine Subnormalreihe zwischen G_{i+1} und G_i nach Entfernung von Wiederholungen ist; genauso für $H_j = (H_j \cap G_0)H_{j+1} \supset \cdots \supset (H_j \cap G_r)H_{j+1} = H_{j+1}$. Lemma II.3.8 wird das für beide sicherstellen. Damit haben wir also zwei Verfeinerungen und die Behauptung folgt, wenn

$$(G_i \cap H_j)G_{i+1}/(G_i \cap H_{j+1})G_{i+1} \simeq (H_j \cap G_i)H_{j+1}/(H_j \cap G_{i+1})H_{j+1}.$$

Lemma II.3.8 mit $Q = G_i \cap H_j$, $N = G_{i+1}$, $L = G_i \cap H_{j+1}$ liefert uns

$$(G_i \cap H_j)G_{i+1}/(G_i \cap H_{j+1})G_{i+1} \simeq G_i \cap H_j/(G_i \cap H_{j+1})(G_{i+1} \cap H_j);$$

für $Q = H_j \cap G_i$, $N = H_{j+1}$ und $L = H_j \cap G_{i+1}$ liefert uns Lemma II.3.8, dass

$$(H_j \cap G_i)H_{j+1}/(H_j \cap G_{i+1})H_{j+1} \simeq H_j \cap G_i/(H_j \cap G_{i+1})(H_{j+1} \cap G_i),$$

also die Behauptung. Die Isomorphien implizieren im besonderen, dass die Wiederholungen an den selben Stellen auftreten müssen. □

Lemma II.3.8: *Seien Q, N und L Untergruppen der Gruppe G, sodass*

(i) $L \triangleleft Q$,

(ii) *Für alle $q \in Q$ ist $qNq^{-1} = N$.*

Dann sind $LN \triangleleft QN$, $L(Q \cap N) \triangleleft Q$ und $QN/LN \simeq Q/L(Q \cap N)$.

Beweis: Wegen (i) und (ii) haben wir $(LN)(LN) = L(NL)N = LN$ und $(LN)^{-1} = LN$ (wegen $N^{-1}L^{-1} = NL = LN$), für QN genauso. Damit sind QN und LN Gruppen. Weiterhin ist LN normal in QN, denn wegen (i) und (ii) ist $qnLN = qLn'N = qLN = qLNn = LNqn$. Jetzt ist

$$\phi\colon Q \longrightarrow QN/LN, \qquad q \longmapsto qLN$$

surjektiv, da $qLN = qnLN$ und es ist $\ker(\phi) = L(Q \cap N)$. Die Inklusion „$\supseteq$“ ist klar, für „$\subseteq$“ sei $q \in Q$ mit $q = \ell n \in LN$. Dann ist schon $n \in Q \cap N$, also $q \in L(Q \cap N)$. Den Rest erledigt der Homomorphiesatz für uns. □

Definition II.3.9: Eine Gruppe G heißt *auflösbar*, falls es eine Subnormalreihe $G = G_0 \supset \cdots \supset G_m = \{1\}$ mit abelschen Faktoren gibt.

Beispiel II.3.10: (i) Jede abelsche Gruppe ist auflösbar.

(ii) Nach Beispiel II.3.4 sind S_3 und S_4 auflösbar.

(iii) Die symmetrische Gruppe S_n ist nicht auflösbar für $n \geq 5$. Das kann man zum Beispiel so zeigen: Eine Untergruppe $G_i \subseteq S_n$ enthalte alle Dreizykel und G_{i+1} sei ein Normalteiler in G_i, sodass G_i/G_{i+1} abelsch ist. Für alle $\sigma, \tau \in G_i$ ist dann $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+1} = \ker(\pi\colon G_i \to G_i/G_{i+1})$. Ist jetzt (abc) ein Dreizykel, dann finden wir $d, e \in \{1, \ldots, n\}$ sodass $\#(\{a, b, c, d, e\}) = 5$ und es ist

$$(adc)(cbe)(adc)^{-1}(cbe)^{-1} = (adc)(cbe)(acd)(ceb) = (abc),$$

also enthält auch G_{i+1} alle Dreizykel.

Bemerkung II.3.11: Sei $\{1\} \to N \xrightarrow{j} G \xrightarrow{p} H \to \{1\}$ eine kurze exakte Sequenz von Gruppen, d. h. der Homomorphismus $j\colon N \to G$ ist injektiv, der Homomorphismus $p\colon G \to H$ surjektiv und $\ker(p) = \mathrm{im}(j) = N$ (also: $N \cong j(N)$ ist eine normale Untergruppe von G und $H = G/j(N)$). Dann ist G auflösbar genau dann, wenn N und H auflösbar sind.

Beweis: „$\Rightarrow$“: Sei G auflösbar und $G = G_0 \supset \cdots \supset G_m = \{1\}$, sodass G_i/G_{i+1} abelsch ist. Dann ist $N = N_0 \supset \cdots \supset N_m = \{1\}$ mit $N_i = j^{-1}(G_i)$ eine Subnormalreihe mit abelschen Faktoren, siehe Bemerkung II.3.5.

Außerdem ist $H = H_0 \supset \cdots \supset H_m = \{1\}$, wobei $H_i = p(G_i)$, eine Subnormalreihe mit abelschen Faktoren.

„$\Leftarrow$“: Seien $N = N_0 \supset \cdots \supset N_r = \{1\}$ und $H = H_0 \supset \cdots \supset H_s = \{1\}$ Subnormalreihen mit abelschen Faktoren. Dann ist

$$G = G_0 \supset \cdots \supset G_s = N \supset \cdots \supset N_r = \{1\},$$

wobei $G_i = p^{-1}(H_i)$, eine Subnormalreihe mit abelschen Faktoren. □

Beispiel II.3.12: (i) Sei G eine Gruppe der Ordnung p^n, wobei p eine Primzahl sei. Dann haben wir eine kurze exakte Sequenz

$$\{1\} \longrightarrow Z(G) \longrightarrow G \longrightarrow G/Z(G) \longrightarrow \{1\}.$$

Da das Zentrum abelsch ist, ist es auflösbar. Für $n = 1$ ist G zyklisch und somit auflösbar. Ist $n > 1$, dann ist $\#(G/Z(G)) = p^m$ mit einem Exponenten $m < n$ und auflösbar nach Induktionsvoraussetzung, aber damit ist auch G auflösbar nach Bemerkung II.3.11.

(ii) Sei G eine Gruppe mit $\#(G) = p^2q$, wobei p und q verschiedene ungerade Primzahlen seien. Nach den Sylow-Sätzen sind die Anzahlen $s_q \equiv 1 \pmod{q}$ mit $s_q \in \{1, p, p^2\}$, und $s_p \equiv 1 \pmod{p}$ mit $s_p \in \{1, q\}$.

Ist $s_q = 1$, dann ist die einzige q-Sylowgruppe S_q ein Normalteiler in G. Wir haben also eine kurze exakte Sequenz

$$\{1\} \longrightarrow S_q \longrightarrow G \longrightarrow G/S_q \longrightarrow \{1\}$$

und G ist auflösbar.

Ist $s_q \in \{p, p^2\}$, dann muss $q \mid (p-1)(p+1)$, d. h. $q \leq p+1$ und damit $q < p$ nach Voraussetzung. Dann muss aber $s_p = 1$ gelten, wir haben wieder eine kurze exakte Sequenz von Gruppen wie zuvor und G ist auflösbar.

4. Erweiterungen

Im ganzen Abschnitt bezeichne G eine Gruppe und A eine abelsche Gruppe.

Definition II.4.1: Eine *Erweiterung von G durch A* ist eine kurze exakte Sequenz

$$\{0\} \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow \{1\}.$$

Ein Pfeil von Erweiterungen ist ein Diagramm

$$\begin{array}{ccccccccc} \{0\} & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & \{1\} \\ & & \| & & \downarrow & & \| & & \\ \{0\} & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & \{1\} \end{array}$$

Jeder solche Pfeil ist ein Isomorphismus. Zwei solche Erweiterungen heißen äquivalent.

Bemerkung II.4.2: (i) Ist $\{0\} \to A \to E \xrightarrow{\pi} G \to \{1\}$ eine Erweiterung, dann ist π surjektiv; d. h. es existiert ein *mengentheoretischer Schnitt* $s\colon G \to E$ (mit $\pi \circ s = \mathrm{id}_G$).

(ii) Für $a \in A$ ist $s(g)as(g)^{-1}$ unabhängig von der Wahl des Schnittes s, es gilt nämlich für zwei Schnitte s und t, dass

$$s(g)as(g)^{-1} = t(g)t(g)^{-1}s(g)as(g)^{-1} = t(g)at(g)^{-1}$$

da $t(g)^{-1}s(g) \in A = \ker(\pi)$. Insbesondere definiert $g \bullet a := s(g)as(g)^{-1}$ eine Operation von G auf A via $G \to \mathrm{Aut}(A)$, d. h. $g \bullet (ab) = (g \bullet a)(g \bullet b)$. Diese Operation von G auf A ist dieselbe für zwei äquivalente Erweiterungen.

(iii) Unser Problem der Klassifikation aller Erweiterungen zerfällt also in zwei kleinere Probleme:

(1) Finde alle Operationen $G \to \mathrm{Aut}(A)$,
(2) Finde zu einer gegebenen Operation alle Erweiterungen, die gemäß Bemerkung II.4.2 (ii) diese Operation induzieren.

(iv) Ohne Einschränkung sei $s(1) = 1$. Dann ist die Abbildung

$$\phi_s \colon A \times G \longrightarrow E, \qquad (a, g) \longmapsto a \cdot s(g)$$

eine Bijektion mit $\phi_s^{-1}(e) = (e \cdot (s \circ \pi)(e)^{-1}, \pi(e))$. Also definiert

$$\begin{aligned}(a, g) \star (a', g') &= \phi_s^{-1}(\phi_s(a, g)\phi_s(a', g')) \\ &= \phi_s^{-1}(as(g)a's(g')) = \Big(as(g)a's(g')s(gg')^{-1}, gg'\Big)\end{aligned}$$

eine Gruppenstruktur auf $A \times G$. Das neutrale Element ist $(1_A, 1_G)$. Insbesondere ist

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & A & \longrightarrow & (A \times G, \star) & \longrightarrow & G & \longrightarrow & \{1\} \\ & & \| & & \downarrow{\scriptstyle \phi_s} & & \| & & \\ \{1\} & \longrightarrow & A & \longrightarrow & E & \xrightarrow[\pi]{} & G & \longrightarrow & \{1\} \end{array}$$

eine Äquivalenz von Erweiterungen.

(v) Schreiben wir A additiv und setzen $[g, g'] = s(g)s(g')s(gg')^{-1} \in A$, dann erklärt das eine (wichtige) Funktion $[\cdot, \cdot] \colon G \times G \to A$, die „misst“, wie weit s davon entfernt ist, ein Gruppenhomomorphismus zu sein. Mit dieser Notation können wir schreiben

$$\begin{aligned}(a, g) \star (a', g') &= (as(g)a's(g')s(gg')^{-1}, gg') \\ &= (as(g)a's(g)^{-1}s(g)s(g')s(gg')^{-1}, gg') \\ &= (a \cdot (g \bullet a') \cdot [g, g'], gg') = (a + g \bullet a' + [g, g'], gg').\end{aligned}$$

Insbesondere sind zwei Erweiterungen von G durch A mit derselben (induzierten) Operation und derselben $[\cdot, \cdot]$-Funktion bereits äquivalent.

(vi) Sind $s, t \colon G \to E$ zwei normalisierte Schnitte (d. h. $s(1) = t(1) = 1$), dann gibt es eine Funktion $\alpha \colon G \to A$ mit $\alpha(1) = 1_E = 0_A$, sodass für alle $g \in G$ gilt: $s(g) = \alpha(g)t(g)$ (setze $\alpha := s(g) \cdot t(g)^{-1}$). Dann ist

$$\begin{aligned}[g, g']_s &= \alpha(g)t(g)\alpha(g')t(g')t(gg')^{-1}\alpha(gg')^{-1} \\ &= \alpha(g)t(g)\alpha(g')t(g)^{-1}t(g)t(g')t(gg')^{-1}\alpha(gg')^{-1} \\ &= \alpha(g)g \bullet \alpha(g')[g, g']_t\alpha(gg')^{-1},\end{aligned}$$

d. h., da alle Faktoren in A liegen, dass $[g,g']_s = [g,g']_t + g\bullet\alpha(g') - \alpha(gg') + \alpha(g)$ für eine Funktion $\alpha\colon G \to A$ mit $\alpha(1) = 0$.

Lemma II.4.3: *Für die in Bemerkung II.4.2 konstruierte Abbildung $[\cdot,\cdot]_{E,s}$ gilt:*

(i) $[1,g] = [g,1] = 0$ *für alle* $g \in G$.

(ii) $g_1 \bullet [g_2,g_3] - [g_1g_2,g_3] + [g_1,g_2g_3] - [g_1,g_2] = 0$ *für alle* $g_1,g_2,g_3 \in G$.

Beweis: (i) Offenbar ist $[1,g] = s(1)\cdot s(g)\cdot s(g)^{-1} = 1_E = 0_A$ und die andere Identität lässt sich genauso zeigen.

(ii) Man rechnet

$$\begin{aligned} &g_1 \bullet [g_2,g_3] + [g_1,g_2g_3] \\ &\quad = \Big(s(g_1)s(g_2)s(g_3)s(g_2g_3)^{-1}s(g_1)^{-1}\Big)\cdot\Big(s(g_1)s(g_2g_3)s(g_1g_2g_3)^{-1}\Big) \\ &\quad = s(g_1)s(g_2)s(g_3)s(g_1g_2g_3)^{-1} \end{aligned}$$

sowie

$$\begin{aligned} -[g_1g_2,g_3] - [g_1,g_2] &= \Big(s(g_1g_2)s(g_3)s(g_1g_2g_3)^{-1}\Big)^{-1}\cdot\Big(s(g_1)s(g_2)s(g_1g_2)^{-1}\Big)^{-1} \\ &= s(g_1g_2g_3)s(g_3)^{-1}s(g_2)^{-1}s(g_1)^{-1} \end{aligned}$$

und erhält so das gewünschte Ergebnis. □

Definition II.4.4: Ist $\bullet\colon G \to \mathrm{Aut}(G)$ gegeben, so heißt eine Funktion $[\cdot,\cdot]\colon G\times G \to A$, die (i) und (ii) aus Lemma II.4.3 erfüllt, ein (normalisierter) 2-*Kozykel*.

Die Gruppe der 2-Kozykel (mit punktweiser Addition als Verknüpfung) bezeichnen wir mit $Z^2(G,A)$. Die Untergruppe von $Z^2(G,A)$ von Kozykeln $(g,g') \mapsto g\bullet\alpha(g') - \alpha(gg') + \alpha(g)$ für $\alpha\colon G \to A$ mit $\alpha(1) = 0$ ist die Gruppe $B^2(G,A)$ der 2-Koränder.

Die Quotientengruppe

$$H^2(G,A) = Z^2(G,A)/B^2(G,A)$$

heißt die *zweite Kohomologiegruppe von G mit Koeffizienten in A*, wobei eine Operation $\bullet\colon G \to \mathrm{Aut}(A)$ fixiert ist.

Satz II.4.5: *Sei $G \to \mathrm{Aut}(A)$ eine Operation. Dann steht $H^2(G,A)$ in Bijektion zu den Äquivalenzklassen von Erweiterungen $\{0\} \to A \to E \to G \to \{1\}$ mit der Eigenschaft, dass die induzierte Operation von G auf A mit der gegebenen Operation übereinstimmt. Dabei entspricht $\{0\} \to A \to E \to G \to \{1\}$ dem Kozykel $[g,g'] = s(g)s(g')s(gg')^{-1}$ aus Bemerkung II.4.2 (v).*

Beweis: Wir definieren

$$\mathrm{Ext}(A,G) := \{\text{Erweiterungen}\}/_{\cong} \longrightarrow H^2(G,A), \qquad E \longmapsto [\cdot,\cdot]_E$$

wobei $[\cdot,\cdot]_E$ aus Bemerkung II.4.2 (iv) stammt. Diese Abbildung ist sowohl wohldefiniert, als auch injektiv gemäß Bemerkung II.4.2. Zur Injektivität: Sind E, E' Erweiterungen mit $[\cdot,\cdot]_{E,s} = [\cdot,\cdot]_{E',t}$ in H^2, dann gibt es $\alpha\colon G \to A$ mit $\alpha(1) = 0$, sodass

$$[g,g']_{E,s} = [g,g']_{E',t} + g \bullet \alpha(g') - \alpha(gg') + \alpha(g) = [g,g']_{E',s'}.$$

Damit ist $E \simeq E'$, was wir sehen wollen. Die Surjektivität zeigen wir in Lemma II.4.7. □

Bemerkung II.4.6: Es sind äquivalent:

(i) Die Klasse einer Erweiterung E in $H^2(G,A)$ ist 0.

(ii) Die Erweiterung *spaltet*, d. h. es gibt einen Gruppenhomomorphismus $\sigma\colon G \to E$, sodass $\pi \circ \sigma = \mathrm{id}$, wobei $A \to E \xrightarrow{\pi} G$ die zugehörige Projektion ist. Das kommt von der Definition von $[\cdot,\cdot]_{E,s}$.

Lemma II.4.7: *Seien $G \to \mathrm{Aut}(A)$ eine Operation auf A und $[\cdot,\cdot] \in Z^2(G,A)$.*

(i) *Auf der Menge $A \times G$ definiert*

$$(a,g) \star (a',g') = (a + g \bullet a' + [g,g'], gg')$$

eine Gruppenstruktur.

(ii) *Die kanonische Abbildung $(A \times G, \star) \to G$ ist ein surjektiver Gruppenhomomorphismus, dessen Kern isomorph ist zu A, und die induzierte Operation auf A stimmt mit der gegebenen Operation auf A überein. Insbesondere ist $(\{0\} \to A \to (A \times G, \star) \to G \to \{1\}) \in \mathrm{Ext}(A,G)$.*

(iii) *Der 2-Kozykel $[\cdot,\cdot]_{A\times G,s}$ für den Schnitt $g \mapsto (0,g)$ ist der gegebene 2-Kozykel.*

Beweis: (i) Für die Assoziativität von „$\star$“ rechnen wir

$$\begin{aligned}\Big((a,g) \star (a',g')\Big) \star (a'',g'') &= (a + g \bullet a' + [g,g'], gg') \star (a'',g'') \\ &= (a + g \bullet a' + [g,g'] \\ &\qquad + (gg') \bullet a'' + [gg', g''], gg'g'')\end{aligned}$$

und

$$\begin{aligned}(a,g)\star\Big((a',g')\star(a'',g'')\Big) &= (a,g)\star(a'+g'\bullet a''+[g',g''],g'g'')\\ &= (a+g\bullet a'+g\bullet(g'\bullet a'')\\ &\qquad +g\bullet[g',g'']+[g,g'g''],gg'g'').\end{aligned}$$

Nun ist aber $g\bullet(g'\bullet a'')=(gg')\bullet a''$ und außerdem

$$g\bullet[g',g'']+[g,g'g'']=[gg',g'']+[g,g']$$

wegen der Relationen aus Lemma II.4.3. Ein Vergleich der Komponenten zeigt nun die Assoziativität von „$\star$“.

Außerdem ist $(0,1)$ das neutrale Element für „$\star$“, denn

$$\begin{aligned}&(0,1)\star(a,g)=(0+1\bullet a+[1,g],g)=(a,g)\\ \text{und}\quad &(a,g)\star(0,1)=(a+g\bullet 0+[g,1],g)=(a,g).\end{aligned}$$

Es bleibt lediglich zu zeigen, dass jedes (a,g) ein Inverses besitzt. Man rechnet mit

$$\begin{aligned}(a,g)\star(b,g^{-1})=(0,1) &\iff (a+g\bullet b+[g,g^{-1}],1)=(0,1)\\ &\iff a+g\bullet b+[g,g^{-1}]=0\\ &\iff b=-g^{-1}\bullet a\ -\ g^{-1}\bullet[g,g^{-1}]\end{aligned}$$

und

$$\begin{aligned}(b,g^{-1})\star(a,g)=(0,1) &\iff (b+g^{-1}\bullet a+[g^{-1},g],1)=(0,1)\\ &\iff b=-g^{-1}\bullet a\ -\ [g^{-1},g]\end{aligned}$$

einfach ein Rechts- bzw. Linksinverses von (a,g) aus und schließt mit der Relation

$$g^{-1}\bullet[g,g^{-1}]-[g^{-1}g,g^{-1}]+[g^{-1},gg^{-1}]-[g^{-1},g]=0$$

aus Lemma 1 bzw. mit $g^{-1}\bullet[g,g^{-1}]=[g^{-1},g]$, dass diese tatsächlich dasselbe Element sind.

(ii) Es ist klar, dass $\pi\colon A\times G\to G$ ein Gruppenhomomorphismus ist und der Kern von π ist offenbar $\{(a,1)\mid a\in A\}\subseteq A\times G$. Betrachtet man die Einschränkung von „$\star$“ auf diese Untergruppe, so sieht man, dass

$$(a,1)\star(a',1)=(a+1\bullet a'+[1,1],1)=(a+a',1)$$

und es folgt, dass $\ker\pi\cong A$.

(iii) Wir betrachten den Schnitt $s\colon G \to A \times G$ mit $s(g) = (0, g)$. Die von der Erweiterung

$$\{0\} \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow \{0\}$$

induzierte Operation „$\odot$“ von G auf A ist durch

$$(g \odot a, 1) = (0, g) \star (a, 1) \star (0, g)^{-1}$$

gegeben. Mit der Beschreibung $(0, g)^{-1} = (-g^{-1} \bullet [g, g^{-1}], g^{-1})$ der Inversen aus Teil (i) rechnen wir nun

$$\begin{aligned}(0, g) \star (a, 1) \star (0, g)^{-1} &= (g \bullet a, g) \star (-g^{-1} \bullet [g, g^{-1}], g^{-1}) \\ &= \Big(g \bullet a - g \bullet (g^{-1} \bullet [g, g^{-1}]) + [g, g^{-1}], 1\Big) \\ &= (g \bullet a, 1)\end{aligned}$$

und es folgt $g \odot a = g \bullet a$.

(iv) Um den Kozykel $[\cdot, \cdot]_{A \times G, s}\colon G \times G \to A$, der zu dem Schnitt $s(g) = (0, g)$ gehört, auszurechnen, beobachten wir, dass

$$\Big([g_1, g_2]_{A \times G, s}, 1\Big) = s(g_1) \star s(g_2) \star s(g_1 g_2)^{-1}$$

und rechnen mit Hilfe der Beschreibung der Inversen aus Teil (i) wiederum

$$\begin{aligned}&s(g_1) \star s(g_2) \star s(g_1 g_2)^{-1} \\ &\quad = (0, g_1) \star (0, g_2) \star (0, g_1 g_2)^{-1} \\ &\quad = ([g_1, g_2], g_1 g_2) \star \Big(- (g_1 g_2)^{-1} \bullet [g_1 g_2, (g_1 g_2)^{-1}], (g_1 g_2)^{-1}\Big) \\ &\quad = \Big([g_1, g_2] - (g_1 g_2) \bullet (g_1 g_2)^{-1} \bullet [g_1 g_2, (g_1 g_2)^{-1}] + [g_1 g_2, (g_1 g_2)^{-1}], 1\Big) \\ &\quad = ([g_1, g_2], 1),\end{aligned}$$

was den Beweis beschließt. □

Beispiel II.4.8: (i) Wir betrachten die Erweiterung

$$\{0\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow E \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \{0\}.$$

Operationen von $\mathbb{Z}/3\mathbb{Z}$ auf $\mathbb{Z}/2\mathbb{Z}$ gibt es nur eine, da $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = \{\mathrm{id}\}$, nämlich $g \bullet a = a$. Was ist $H^2(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$?

Zunächst vereinbaren wir $\mathbb{Z}/3\mathbb{Z} = C_3 = \langle\sigma\rangle$. Ist $[\cdot,\cdot] \in Z^2(G)$, dann ist $[1,\sigma] = [1,\sigma^2] = [\sigma,1] = [\sigma^2,1] = 0$; ist $\alpha\colon C_3 \to \mathbb{Z}/2\mathbb{Z}$, dann ist

$$g \bullet \alpha(g) - \alpha(g^2) + \alpha(g) = 2\alpha(g) + \alpha(g^2) = \alpha(g^2),$$

d. h. $[g,g'] \equiv [g,g'] + g \bullet \alpha(g') - \alpha(gg') + \alpha(g)$, insbesondere sind

$$[\sigma,\sigma] \equiv [\sigma,\sigma] + \alpha(\sigma^2), \qquad [\sigma^2,\sigma^2] \equiv [\sigma^2,\sigma^2] + \alpha(\sigma),$$

d. h. jedes Element in H^2 hat einen Vertreter $[\cdot,\cdot]$ mit $[\sigma,\sigma] = [\sigma^2,\sigma^2] = 0$, wegen der Kozykel-Relation ist dann auch $[\sigma,\sigma^2] = 0 = [\sigma^2,\sigma]$. Damit ist $H^2(\mathbb{Z}/3\mathbb{Z},\mathbb{Z}/2\mathbb{Z}) = \{0\}$ und $E \cong \mathbb{Z}/6\mathbb{Z}$.

(ii) Wir betrachten die Erweiterung

$$\{0\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow E \longrightarrow C_2 = \langle\sigma\rangle \longrightarrow \{1\}.$$

Es gibt nur die triviale Operation von C_2 auf $\mathbb{Z}/2\mathbb{Z}$. Kozykel $[\cdot,\cdot]\colon C_2^2 \to \mathbb{Z}/2\mathbb{Z}$ sind eindeutig durch $[\sigma,\sigma]$ festgelegt. Für $\alpha\colon C_2 \to \mathbb{Z}/2\mathbb{Z}$ ist

$$\sigma \bullet \alpha(\sigma) - \alpha(\sigma^2) + \alpha(\sigma) = \alpha(\sigma) - \alpha(\sigma^2) + \alpha(\sigma) = 0,$$

d. h. $H^2(C_2,\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Wir haben die beiden Erweiterungen

$$\{0\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \{0\},$$
$$\{0\} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \{0\},$$

die erste ist die nicht-spaltende Erweiterung, die zweite ist die spaltende Erweiterung.

(iii) Wir betrachten die Erweiterung

$$\{0\} \longrightarrow \mathbb{Z} \longrightarrow E \longrightarrow C_2 = \langle\sigma\rangle \longrightarrow \{1\}.$$

Hier gibt es zwei Operationen $C_2 \to \mathrm{Aut}(\mathbb{Z})$, nämlich $\sigma \bullet a = a$ und $\sigma \bullet a = -a$.

Operiert σ trivial, dann gilt für $\alpha\colon C_2 \to \mathbb{Z}$, dass

$$\sigma \bullet \alpha(\sigma) - \alpha(\sigma^2) + \alpha(\sigma) = 2\alpha(\sigma).$$

Es ist $H^2(C_2,\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ vermöge des Isomorphismus, der zwischen geradem und ungeradem $[\sigma,\sigma]$ unterscheidet. Die spaltende Erweiterung ist, da die Operation trivial ist,

$$\{0\} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \{0\},$$

die nicht-spaltende Erweiterung ist

$$\{0\} \longrightarrow \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \{0\},$$

da es kein Element der Ordnung 2 in $\mathbb{Z}$ gibt, also auch keinen Gruppenhomomorphismus $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$.

Operiert σ per Multiplikation mit -1, dann gibt die Kozykelrelation

$$0 = \sigma \bullet [\sigma, \sigma] - [\sigma^2, \sigma] + [\sigma, \sigma^2] - [\sigma, \sigma] = -[\sigma, \sigma] - [\sigma, \sigma],$$

d. h. ist $[\sigma, \sigma] = 0$ und $H^2(C_2, \mathbb{Z}) = \{0\}$. Die Erweiterung ist

$$\{0\} \longrightarrow \mathbb{Z} \longrightarrow D_\infty \longrightarrow C_2 \longrightarrow \{1\},$$

die Gruppe D_∞ heißt „unendliche Diedergruppe“.

(iv) Gegeben sei eine Gruppe G der Ordnung m und $[\cdot, \cdot] \in Z^2(G, A)$. Die Funktion

$$\alpha \colon G \longrightarrow A, \qquad g \longmapsto \sum_{h \in G} [g, h]$$

erfüllt offenbar $\alpha(1) = 0$. In $H^2(G, A)$ gilt

$$\begin{aligned} 0 = g_1 \bullet \alpha(g_2) - \alpha(g_1 g_2) + \alpha(g_1) &= \sum_{h \in G} g_1 \bullet [g_2, h] - [g_1 g_2, h] + \sum_{h \in G} [g_1, h] \\ &= \sum_{h \in G} g_1 \bullet [g_2, h] - [g_1 g_2, h] + \sum_{h \in G} [g_1, g_2 h] \\ &= \sum_{h \in G} g_1 \bullet [g_2, h] - [g_1 g_2, h] + [g_1, g_2 h] \\ &= m \cdot [g_1, g_2] \end{aligned}$$

Die Multiplikation mit m ist also die Nullabbildung auf $H^2(G, A)$. Ist nun A eine Gruppe der Ordnung n sodass $\mathrm{ggT}(m, n) = 1$, dann ist Multiplikation mit m invertierbar auf A, also ist Multiplikation mit m invertierbar auf $H^2(G, A)$. Es muss also schon $H^2(G, A) = \{0\}$ sein.

Kapitel III.

Ringe

Ringe sind in dieser Vorlesung (soweit nicht explizit anders angegeben) kommutativ und mit Eins.

1. Ideale

Definition III.1.1: Sei R ein Ring.

(i) Sei $I \subseteq R$ eine nichtleere Teilmenge. Gilt für alle $x, y \in I$ und $a \in R$, dass $x + ay \in R$, dann heißt I ein *Ideal*.

(ii) Ist $I \subseteq R$ ein Ideal, dann ist R/I ein Ring mit den repräsentantenweisen Verknüpfungen $(a+I)+(b+I) := a+b+I$ und $(a+I)(b+I) = ab+I$ ein Ring. Die kanonische Projektion $\pi\colon R \to R/I$ ist ein Ringhomomorphismus. Der Quotientenring R/I hat folgende universelle Eigenschaft: Ist $f\colon R \to S$ ein Ringhomomorphismus mit $I \subseteq \ker f$, dann gibt es genau einen Ringhomomorphismus $\bar{f}\colon R/I \to S$, der das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/I \\ & \searrow^{f} & \downarrow{\scriptstyle \bar{f}} \\ & & S \end{array}$$

kommutativ macht.

Bemerkung III.1.2: (i) Jeder Kern eines Ringhomomorphismus ist ein Ideal und umgekehrt ist jedes Ideal der Kern eines Ringhomomorphismus.

(ii) Für $a \in R$ ist $(a) := \{\lambda a \mid \lambda \in R\}$ ein Ideal in R; es heißt das *von a erzeugte Hauptideal*.

(iii) Für eine Familie $(a_i)_{i\in I}$ ist

$$((a_i)_{i\in I}) = \Big\{ \sum_{j=0}^{n} \lambda_j a_{i_j} : n \in \mathbb{N}, \{i_1, \dots, i_n\} \subseteq I, \{\lambda_1, \dots, \lambda_n\} \subseteq R \Big\}.$$

(iv) Ist $(I_j)_{j\in J}$ eine Familie von Idealen in R, dann ist $\bigcap_{j\in J} I_j$ ein Ideal in R.

(v) Ist $(I_j)_{j\in J}$ eine Familie von Idealen, dann ist

$$\sum_{j\in J} I_j := \Big\{ \sum_{j=0}^{n} \lambda_i a_{j_i} : n \in \mathbb{N}, \{j_1, \dots, j_n\} \subseteq J, \{\lambda_1, \dots, \lambda_n\} \subseteq R \Big\}$$

ein Ideal. Dieses ist das kleinste Ideal von R, das die Familie $(I_j)_{j\in J}$ enthält.

(vi) Sind $I_1, \dots, I_k$ Ideale, dann ist

$$I_1 \cdots I_k = \Big\{ \sum_{i=1}^{n} a_1^{(i)} \cdots a_n^{(i)} : a_j^{(i)} \in I_j \Big\}$$

ein Ideal.

(vii) Es gilt $I_1 \cdots I_k \subseteq \bigcap_{i=1}^{k} I_i$.

Beispiel III.1.3: (i) In $\mathbb{Z}$ ist ein Ideal immer von der Form (a) für $a \in \mathbb{Z}$. Zum Beispiel sind $(2) \cap (3) = (6)$, $(2)(3) = (6)$, $(2) \cap (4) = (4)$, $(2)(4) = (8)$, $(2) + (3) = \mathbb{Z}$.

(ii) Es sei $R = C([0,1]) := \{f\colon [0,1] \to \mathbb{R} \mid f \text{ stetig}\}$. Das von den konstanten Funktionen erzeugte Ideal I ist der ganze Ring, weil $f = f \cdot 1 \in I$. Für $x \in [0,1]$ ist $M_x := \{f \in R \mid f(x) = 0\}$ ein nicht-triviales Ideal in R.

(iii) Es sei $R = \mathbb{Z}[2X, 2X^2, \dots] \subseteq \mathbb{Z}[X]$. R ist ein Teilring von $Z[X]$. Der Schnitt der beiden Hauptideale $(2X)$, $(2X^2)$ ist das Ideal $(4X^2, 4X^3, 4X^4, \dots)$.

Definition III.1.4: Es seien R ein Ring und $I \subsetneq R$ ein Ideal.

(i) Gilt für $a, b \in R$ mit $ab \in I$, dass $a \in I$ oder $b \in I$, dann heißt I *Primideal*.

(ii) Ist I maximal bezüglich „$\subseteq$“, dann heißt I *maximales Ideal*.

Bemerkung III.1.5: Ein Ideal $P \subsetneq R$ ist ein Primideal genau dann, wenn R/P nullteilerfrei ist. Ein Ideal $\mathfrak{m} \subsetneq R$ ist maximal genau dann, wenn $R/\mathfrak{m}$ ein Körper ist. Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis: Seien $P \subsetneq R$ ein Ideal, R/P ein nullteilerfreier Ring und $a, b \in R$. Gilt $(a+P)(b+P) = 0$, dann ist $a+P = 0$ oder $b+P = 0$, d. h. $a \in P$ oder $b \in P$.

Ist umgekehrt P prim und ist $(a+P)(b+P) = ab+P = 0+P \in R/P$, dann ist $ab \in P$. Da P prim ist, ist also $a \in P$ oder $b \in P$, d. h. $a+P = 0$ oder $b+P = 0$ und R/P ist nullteilerfrei.

Seien $\mathfrak{m} \subsetneq R$ maximal und $0+\mathfrak{m} \neq a+\mathfrak{m} \in R/\mathfrak{m}$. Dann ist $a \notin \mathfrak{m}$, d. h. $\mathfrak{m} \subsetneq (a, \mathfrak{m}) = R$. Es gibt also $b \in R$ und $m \in \mathfrak{m}$, sodass $1 = ab+m$. Damit ist $1+\mathfrak{m} = (b+\mathfrak{m})(a+\mathfrak{m})$.

Seien umgekehrt $\mathfrak{m} \subsetneq R$ ein Ideal und $R/\mathfrak{m}$ ein Körper. Weiter sei $I \subseteq R$ ein Ideal mit $\mathfrak{m} \subsetneq I$. Wähle $x \in I - \mathfrak{m}$. Da $R/\mathfrak{m}$ ein Körper ist, gibt es $y \in R$ mit $xy+\mathfrak{m} = 1+\mathfrak{m}$. Das heißt aber, es gibt $m \in \mathfrak{m}$, sodass $1 = yx+m \in I$ und damit $I = R$. □

Beispiel III.1.6: (i) Ein Ideal $(a) \subseteq \mathbb{Z}$ ist prim, wenn a prim oder 0 ist und maximal, wenn a prim ist.

(ii) In $\mathbb{R}[X]$ ist (X^2-1) ist nicht prim (und damit erst recht nicht maximal), denn $(X+1)(X-1) \in (X^2-1)$, aber weder $(X+1) \in (X^2-1)$, noch $(X-1) \in (X^2-1)$.

Das Ideal $(X-2)$ ist prim und maximal, denn $(X-2) = \ker(f \mapsto f(2))$ und $\mathbb{R}[X]/(X-2) \cong \mathbb{R}$.

Das Ideal (X^2+1) ist prim und maximal, denn $(X^2+1) = \ker(f \mapsto f(\mathrm{i}))$ und $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Dass $(X^2+1) \subseteq \ker(f \mapsto f(\mathrm{i}))$, ist klar. Ist $f \in \mathbb{R}[X]$ mit $f(\mathrm{i}) = 0$, dann ist $f = q(X^2+1)+r$ mit $\deg(r) \leq 1$. Wir können schreiben $r = aX+b$. Einsetzen von i in r gibt $a = b = 0$.

(iii) Das Ideal $M_x = \{f \in C([0,1]) \mid f(x) = 0\}$ in $C([0,1])$ ist prim, denn $\mathbb{R}$ ist nullteilerfrei. Außerdem ist M_x maximal und $C([0,1])/M_x \cong \mathbb{R}$ via $f \mapsto f(x)$.

(iv) Seien k ein Körper und $R = k[X,Y]$. In R ist (X) prim und nicht maximal, denn $k[X,Y]/(X) \cong k[Y]$.

Definition III.1.7: Seien R ein Ring und $I, J \subseteq R$ Ideale. Gilt $I+J = R$, so heißen I und J *relativ prim* oder auch *koprim*.

Beispiel III.1.8: Für die ganzen Zahlen 2 und 3 ist $(2)+(3) = \mathbb{Z}$.

Bemerkung III.1.9: (i) Sind $I_1, \ldots, I_n$ paarweise koprime Ideale im Ring R, dann finden wir für jedes $i \geq 2$ Elemente $a_i \in I_i$ und $b_i \in I_i$ mit $1 = a_i + b_j$. Für diese Elemente ist $1 = \prod_{i=2}^{n}(a_i+b_i) = (\ldots) + b_2 b_3 \cdots b_n$, d. h. I_1 und $I_2 \cdots I_n$ sind relativ prim.

(ii) Sind $I_1, \ldots, I_n$ relativ prim, dann ist $I_1 \cdots I_n = \bigcap_{i=1}^n I_i$.

Dazu reicht es, den Fall $n = 2$ zu betrachten. Seien $a \in I_1$ und $b \in I_2$ mit $1 = a + b$. Für $c \in I_1 \cap I_2$ ist dann $c = 1c = ac + bc \in I_1 I_2$.

Satz III.1.10 (Chinesischer Restsatz): *Seien $I_1, \ldots, I_n$ paarweise relativ prime Ideale in R.*

(i) *Die Abbildung*

$$\varphi\colon R \longrightarrow \prod_{i=1}^n R/I_i, \qquad r \longmapsto (r + I_1, \ldots, r + I_n)$$

ist surjektiv.

(ii) *Der Kern von ϕ ist $\bigcap_{i=1}^n I_i$ und somit ist $R/\bigcap_{i=1}^n I_i \cong \prod_{i=1}^n R/I_i$.*

Beweis: Wir zeigen nur Teil (i), Teil (ii) ist klar.

Offenbar reicht es zu zeigen, dass $e_i := (\delta_{i,j})_{1 \le j \le n} \in \prod_{i=1}^n R/I_i$ ein Urbild hat beziehungsweise sogar ohne Einschränkung, dass e_1 ein Urbild hat. Wir wissen, dass I_1 und $I_2 \cdots I_n$ relativ prim sind, d. h. es gibt $a \in I_1$ und $b \in I_2 \cdots I_n$ mit $1 = a + b$. Offenbar gilt $\varphi(b) = e_1$. □

Beispiel III.1.11: (i) Ist n eine natürliche Zahl mit Primfaktorzerlegung $n = \prod_{i=1}^r p_i^{e_i}$, dann ist

$$\mathbb{Z}/(n) \cong \prod_{i=1}^r \mathbb{Z}/(p_i^{e_i}).$$

Diese Aussage findet zum Beispiel Anwendung bei der RSA-Verschlüsselung: Seien $N = pq$ eine natürliche Zahl, p und q Primzahlen, φ die eulersche Phi-Funktion und e eine natürliche Zahl mit $\mathrm{ggT}(e, \varphi(N)) = 1$. Vorzugsweise ist e eine relativ große Zahl, um kleine Nachrichten gut zu schützen.

Es ist $\varphi(N) = (p-1)(q-1)$, denn $(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$.

Das RSA-Verfahren basiert auf der Annahme: Ist die Faktorisierung $N = pq$ nicht bekannt, dann kann man $\varphi(N) = (p-1)(q-1)$ nur schwer berechnen. Ist $\varphi(N)$ bekannt, dann kann man $1 = e \cdot d \pmod{\varphi(N)}$ berechnen. Der geheime Schlüssel bei diesem Transfer ist d.

Der öffentliche Schlüssel ist das Tupel (N, e). Das Chiffrat von $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ ist $m^e \pmod N$ und dechiffrieren geht mit $(m^e)^d = m^{ed} = m \pmod N$.

(ii) Das Gleichungssystem von Kongruenzen

$$x \equiv a \pmod 2, \qquad x \equiv b \pmod 3, \qquad x \equiv c \pmod 5$$

hat nach dem chinesischen Restsatz eine Lösung $x \in \mathbb{Z}$, die eindeutig ist modulo $2 \cdot 3 \cdot 5 = 30$. Wir haben die Darstellungen

$$1 = 8 \cdot 2 - 3 \cdot 5, \qquad 1 = -3 \cdot 3 + 2 \cdot 5, \qquad 1 = -1 \cdot 5 + 2 \cdot 3.$$

Eine allgemeine Lösung x des Gleichungssystems ist also

$$x = -15 \cdot a + 10 \cdot b + 6 \cdot c.$$

(iii) In $\mathbb{R}[X]$ sind $(X^2 + 1)$ und (X) koprim, d. h. $\mathbb{R}[X]/(X^3 + X) \cong \mathbb{C} \times \mathbb{R}$.

2. Lokalisierung

Definition III.2.1: Sei R ein Ring. Eine Menge $S \subseteq R$ heißt *multiplikativ abgeschlossen*, falls sowohl $1 \in S$ als auch für alle $s, t \in S$ gilt $st \in S$.

Beispiel III.2.2: Sei R ein Ring

(i) Ist $f \in R$, dann ist $\{f^n \mid n \in \mathbb{N}_0\}$ eine multiplikativ abgeschlossene Menge.

(ii) Ist R nullteilerfrei, dann ist $R - \{0\}$ multiplikativ abgeschlossen.

(iii) Für ein Primideal $P \subseteq R$ ist $R - P$ multiplikativ abgeschlossen.

Definition III.2.3: Sei R ein Ring.

(i) Sei $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann ist

$$(a, s) \sim (a', s') \iff \exists\, t \in S : t(as' - a's) = 0$$

eine Äquivalenzrelation auf $R \times S$. Für die Transitivität der Relation seien $t_1(as' - as') = 0 = t_2(a's'' - a''s')$. Dann ist

$$t_1 t_2 s'(as'' - a''s) = t_2 t_1 as's'' - t_1 t_2 a''s's = t_2 t_1 a'ss'' - t_1 t_2 a's''s = 0,$$

denn nach Voraussetzung sind $t_1 as' = t_1 a's$ und $t_2 a''s' = t_2 a's''$.

(ii) Auf $S^{-1}R = R \times S/\!\sim$ erklären die Verknüpfungen

$$(a, s) + (a', s') = (as' + a's, ss'), \qquad (a, s) \cdot (a', s') = (aa', ss')$$

eine Ringstruktur mit Null $(0, 1)$ und Eins $(1, 1)$. Der Ring $S^{-1}R$ heißt *Lokalisierung von R nach S*. Die Elemente schreibt man als a/s.

(iii) Es ist $S^{-1}R$ der Nullring genau dann, wenn $0 \in S$.
Ist nämlich $0 \in S$, dann ist $0(as' - a's) = 0$ für alle $a, a' \in R$ und $s, s' \in S$, d. h. $a/s = a'/s'$ für alle $a, a' \in R$ und $s, s' \in R$.
Ist $S^{-1}R$ der Nullring, dann folgt aus $0/1 = 1/1$ dass $t(1-0) = 0$ für irgendein $t \in S$, d. h. $t = 0$.

(iv) Die Abbildung $\iota\colon R \to S^{-1}R$, $a \mapsto a/1$ ist ein Ringhomomorphismus. Dieser Homomorphismus ist injektiv genau dann, wenn S keine Nullteiler enthält.
Ist nämlich $s \in S$ ein Nullteiler, sagen wir $as = 0$ für $a \in R - \{0\}$, dann ist $\iota(a) = a/1 = as/s = 0/s = 0/1 = \iota(0)$.
Ist umgekehrt $\iota(a) = \iota(b)$, dann gibt es $t \in S$ mit $t(a-b) = 0$. Ist $a \neq b$, dann ist t ein Nullteiler.

(v) Jedes $s \in S$ wird in $S^{-1}R$ invertierbar, denn $s/1 = 1/s = 1/1$.

(vi) Für jeden Ringhomomorphismus $f\colon R \to R'$ mit $f(S) \subseteq R'^{\times}$ gibt es genau einen Ringhomomorphismus $f'\colon S^{-1}R \to R'$, sodass das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\iota} & S^{-1}R \\ & \searrow^{f} & \downarrow{\scriptstyle f'} \\ & & R' \end{array}$$

kommutiert. Setze $f'(a/s) := f(s)^{-1}f(a)$. Dann ist

$$\begin{aligned} f'\Big(\frac{as'+a's}{ss'}\Big) &= f(ss')^{-1} \cdot f(as'+a's) \\ &= f(s)^{-1}f(a) + f(s')^{-1}f(a') = f'\Big(\frac{a}{s}\Big) + f'\Big(\frac{a'}{s'}\Big). \end{aligned}$$

Beispiel III.2.4: Sei R ein Ring.

(i) Ist $S = \mathbb{Z} - \{0\}$, dann ist $S^{-1}\mathbb{Z} = \mathbb{Q}$. Allgemeiner: Ist R ein nullteilerfreier Ring und $S = R - \{0\}$, dann ist $S^{-1}R =: \mathrm{Quot}(R)$ ein Körper, der sogenannte *Quotientenkörper von R*.

(ii) Ist $S = R - P$, wobei $P \subseteq R$ ein Primideal ist, dann schreibt man meist $R_P := S^{-1}R$. Wir kennen schon $\mathbb{Z}_{(0)} = \mathbb{Q}$. Für $P = (2)$ ist

$$\mathbb{Z}_{(2)} = \Big\{\frac{a}{b} : a, b \in \mathbb{Z}, b \notin 2\mathbb{Z}\Big\} \subseteq \mathrm{Quot}(\mathbb{Z}).$$

Allgemeiner ist jede Lokalisierung nach S mit $0 \notin S$ ein Teilring von $\mathrm{Quot}(R)$, falls R nullteilerfrei ist.

(iii) In $\mathbb{Z}/6\mathbb{Z}$ ist $S = \{1, 2, 4\}$ multiplikativ abgeschlossen. Mit der universellen Eigenschaft der Lokalisierung bekommen wir ein kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \xrightarrow{\iota} & S^{-1}(\mathbb{Z}/6\mathbb{Z}) \\ & \searrow^{\pi} & \downarrow \phi \\ & & \mathbb{Z}/3\mathbb{Z} \end{array}$$

Dieses ϕ ist surjektiv, da das Diagramm kommutiert. Außerdem ist ϕ injektiv, denn $\phi(a/s) = \pm a = 0$ genau dann, wenn $a = 0, 3$. Also ist $\ker(\phi) = 0$, denn $3/s = (2 \cdot 3)/(2 \cdot s) = 0/2s = 0$.

Bemerkung III.2.5: (i) Die Abbildung $\iota\colon R \to S^{-1}R$ induziert eine surjektive Abbildung

$$\iota_*\colon \{\text{Ideale } I \text{ in } R\} \longrightarrow \{\text{Ideale } I \text{ in } S^{-1}R\}, \qquad I \longmapsto \left\{\frac{x}{s} : x \in I, s \in S\right\}.$$

Es ist $\langle\{x/s \mid x \in I, s \in S\}\rangle = \langle\iota(I)\rangle$. Ist nämlich $I \subseteq S^{-1}R$ ein Ideal, dann ist $\iota_*(\iota^{-1}(I)) = I$. Die Inklusion „$\subseteq$“ ist klar, für die Inklusion „$\supseteq$“ sei $x/s \in I$. Dann ist $x/1 = s/1 \cdot x/s \in I$, d. h. $x \in \iota^{-1}(I)$ und damit $x/s \in \iota_*(\iota^{-1}(I))$. Die Abbildung ι_* erhält Inklusionen, Schnitte, Summen und Produkte.

(ii) Insbesondere gilt: Ist R ein Hauptidealring und $S \subseteq R - \{0\}$ eine multiplikativ abgeschlossene Menge, so ist auch $S^{-1}R$ ein Hauptidealring.

(iii) Wir haben eine Bijektion

$$\begin{aligned} \{\text{Primideale } P \subseteq R \text{ mit } P \cap S = \varnothing\} &\xrightarrow{\cong} \{\text{Primideale in } S^{-1}R\} \\ P &\longmapsto \iota_*(P) = \{x/s \mid x \in P\} \end{aligned}$$

mit Umkehrabbildug

$$\iota^{-1}(Q) \longmapsfrom Q.$$

Die Abbildung ι_* ist injektiv, denn wenn $\iota_*(P) = \iota_*(Q)$, dann gilt: Für alle $x \in P$ gibt es $q \in Q$ und $s \in S$ mit $x/1 = q/s$, d. h. es gibt $t \in S$ mit $tsx = tq \in Q$; wegen der Voraussetzungen an Q heißt das $x \in Q$ also $Q = P$.

(iv) Für $S = R - P$ hat $S^{-1}R$ genau ein maximales Ideal, nämlich das von $\iota(P)$ erzeugte Ideal. Angenommen, $\iota(P) \subsetneq Q$. Dann können wir $x/s \in Q - \iota(P)$ wählen. Wir haben $x/1 = sx/s \in Q - P$, also ist x eine Einheit in $S^{-1}R$ und es muss $Q = S^{-1}R$ gelten. Solche Ringe heißen *lokale Ringe*.

3. Teilbarkeit und faktorielle Ringe

Definition III.3.1: Sei R ein Ring.

(i) Ist $p \in R - (\{0\} \cup R^\times)$ und (p) ist ein Primideal, dann heißt p *prim*. Das heißt gilt $p \mid ab$, dann gilt $p \mid a$ oder $p \mid b$.

(ii) Ist R nullteilerfrei und $p \in R - (\{0\} \cup R^\times)$, sodass für alle $a, b \in R$ mit $p = ab$ gilt, dass $a \in R^\times$ oder $b \in R^\times$, dann heißt p *irreduzibel*.

Bemerkung III.3.2: (i) Ist R nullteilerfrei und p prim, dann ist p irreduzibel. Ist nämlich $p = ab$, dann ist $ab \in (p)$, d. h. $a \in (p)$ oder $b \in (p)$. Ohne Einschränkung ist $a = px$, d. h. $p = pxb$. Da R nullteilerfrei ist, können wir folgern, dass $1 = xb$, also $b \in R^\times$.

(ii) Die Umkehrung ist im Allgemeinen falsch. Zum Beispiel ist in $\mathbb{Z}[\sqrt{-5}]$ das Element 3 irreduzibel aber $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$ und $3 \nmid (2 \pm \sqrt{-5})$.

(iii) In Hauptidealringen gilt auch die Umkehrung (d. h. irreduzible Elemente sind prim), denn: Ist p irreduzibel und gelten $p \mid ab$ und $p \nmid a$, dann ist $\mathrm{ggT}(p, a) = 1$ und wir finden eine Darstellung $1 = xa + yp$ mit $x, y \in R$. Jetzt ist aber $b = b1 = bxa + byp$, also gilt $p \mid b$.

Definition III.3.3:

(i) Seien R ein nullteilerfreier Ring und $a \in R - \{0\}$. Gibt es eine Einheit ε und irreduzible Elemente $p_i \in R$, $1 \leq i \leq r$, sodass $a = \varepsilon \prod_{i=1}^{r} p_i$ und gilt für jede weitere solche Darstellung $a = \mu \prod_{i=1}^{s} q_i$ bereits $r = s$ und $p_i = \rho_i q_i$ mit $\rho_i \in R^\times$ nach eventueller Umordnung der Indizes, dann hat a eine *eindeutige Zerlegung in irreduzible Faktoren*.

(ii) Ist R ein nullteilerfreier Ring in dem jedes $a \neq 0$ eine eindeutige Zerlegung in irreduzible Faktoren hat, so heißt R ein *faktorieller Ring*.

Bemerkung III.3.4: (i) In faktoriellen Ringen sind irreduzible Elemente bereits prim.

(ii) In faktoriellen Ringen gibt es größte gemeinsame Teiler und kleinste gemeinsame Vielfache (und einfache explizite Formeln für beide).

(iii) Faktorielle Ringe sind stabil unter Lokalisierung.

Satz III.3.5: *Jeder Hauptidealring ist faktoriell.*

Der Beweis kann im Skript zur Linearen Algebra nachgelesen werden.

Beispiel III.3.6: Wir werden zeigen, dass für Körper k der Polynomring in n Variablen, $k[X_1, \ldots, X_n]$, faktoriell ist, oder auch dass $\mathbb{Z}[X]$ faktoriell ist.

4. Endlich erzeugte Moduln über Hauptidealringen

Satz III.4.1: *Seien R ein Hauptidealring und M ein (endlich erzeugter) freier R-Modul. Ist $N \subseteq M$ ein Untermodul, dann ist auch N frei und außerdem gilt* $\operatorname{rank}(N) \leq \operatorname{rank}(M)$.

Bemerkung III.4.2: Der Rang eines freien R-Moduln ist wohldefiniert. Sei dazu $\mathfrak{m} \subseteq R$ ein maximales Ideal. Dann ist $M/\mathfrak{m}M$ ein $R/\mathfrak{m}$-Vektorraum und jede Basis von M induziert eine Basis von $M/\mathfrak{m}M$; und Kardinalitäten von Basen sind eindeutig.

Beweis: Wir zeigen die Aussage nur für endlich erzeugte freie R-Moduln, obwohl die Aussage auch allgemeiner gilt. Wir zeigen die Aussage per Induktion nach $n = \operatorname{rank}(M)$.

Für $n = 1$ ist $M \cong R$, d. h. N ist ein Ideal in R, d. h. $N = (a)$ und damit frei.

Für $n > 1$ sei $\{x_1, \ldots, x_n\}$ eine Basis von M und π sei die Projektion auf die letzte Komponente, d. h.

$$\pi \colon M \longrightarrow R, \qquad \sum_{i=1}^{n} \lambda_i x_i \longmapsto \lambda_n.$$

Nun müssen wir zwei Fälle unterscheiden: Ist $\pi(N) = 0$, dann tuts N bereits nach Induktionsvoraussetzung.

Ist $\pi(N) = (a)$ für irgendein $a \in R$, dann wählen wir $y \in N$ mit $\pi(y) = a$. Jedes $z \in N$ lässt sich schreiben als $z = z - \lambda y + \lambda y$, wo $\pi(z) = \lambda a$, d. h. $z - \lambda y \in \ker \pi$ und $\lambda y \in Ry$. Es gilt $Ry \cap \ker \pi = \{0\}$. Damit ist $N = Ry \oplus \ker \pi$ und wegen $\ker \pi \subseteq \langle x_1, \ldots, x_{n-1} \rangle$ beschließt das den Beweis. □

Korollar III.4.3: *Über Hauptidealringen sind Untermoduln von endlich erzeugten Moduln endlich erzeugt.*

Beweis: Ist M ein endlich erzeugter Modul mit Erzeugendensystem $\{x_1, \ldots, x_n\}$, dann ist

$$p \colon \bigoplus_{i=1}^{n} R \twoheadrightarrow M, \qquad (\lambda_1, \ldots, \lambda_n) \longmapsto \sum_{i=1}^{n} \lambda_i x_i$$

surjektiv und $p^{-1}(N) \twoheadrightarrow N$ ist surjektiv, d. h. N ist frei von endlichem Rang wegen Satz III.4.1. □

Definition III.4.4: Seien R ein Hauptidealring und M ein R-Modul. Gibt es für jedes $x \in M$ ein $r \in R - \{0\}$ mit $rx = 0$, dann heißt M ein *Torsionsmodul*. Jeder R-Modul M enthält einen maximalen Torsionuntermodul, nämlich

$$M_{\text{tor}} := \{x \in M \mid ax = 0 \text{ für ein } a \in R - \{0\}\}.$$

Satz III.4.5: *Seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann ist M/M_{tor} frei und von endlichem Rang und es gibt einen Untermodul $F \subseteq M$, sodass $F \cong M/M_{\text{tor}}$ und $M \cong F \oplus M_{\text{tor}}$.*

Beweis: Um zu zeigen, dass M/M_{tor} ein freier Modul ist, genügt es zu zeigen, dass torsionsfreie endlich erzeugte Moduln frei sind, denn M/M_{tor} ist torsionsfrei (ist nämlich $a \in R - \{0\}$ und $a(x + M_{\text{tor}}) = 0$, dann ist $ax \in M_{\text{tor}}$, d. h. $bax = 0$ für irgendein $b \in R - \{0\}$, also $x \in M_{\text{tor}}$).

Seien $\{y_1, \ldots, y_n\}$ ein Erzeugendensystem des torsionsfreien endlich erzeugten R-Moduln N und $\{v_1, \ldots, v_m\}$ eine maximale linear unabhängige Teilmenge von $\{y_1, \ldots, y_n\}$. Für jedes $1 \leq i \leq n$ haben wir eine Relation

$$a_i y_i + \lambda_{1,i} v_i + \cdots + \lambda_{m,i} v_m = 0$$

mit $a_i \neq 0$. Weiter gilt für $1 \leq i \leq n$, dass $a_i y_i \in \langle v_1, \ldots, v_m \rangle$. Setze jetzt $a := a_1 \cdots a_n \neq 0$. Die Abbildung

$$\mu_a \colon N \longrightarrow \langle v_1, \ldots, v_m \rangle, \qquad n \longmapsto an$$

ist injektiv, d. h. $N \cong \mu_a(N)$ und $\mu_a(N)$ ist frei als Untermodul eines freien Moduln nach Satz III.4.1.

Es bleibt zu zeigen, dass jede kurze exakte Sequenz

$$\{0\} \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow \{0\}$$

wo F ein freier Modul ist, spaltet und liefert, dass $N \cong M \oplus F$. Diese Aussage wird auf einem Übungsblatt zu zeigen sein. □

Definition III.4.6: Seien R ein Hauptidealring und $p \in R$ prim und M ein R-Modul.

(i) Gibt es für alle $x \in M$ einen natürlichen Exponenten n mit $p^n x = 0$, so heißt M ein *p-Torsionsmodul*.

(ii) Für $x \in M$ heißt $c \in R$ mit $cx = 0$ ein *Exponent von x*.

(iii) Für $x \in M$ ist der Kern von $R \to M$, $a \mapsto ax$ von der Gestalt (m); das Element m heißt *Periode*. Ein $c \in R$, das für alle $m \in M$ leistet $cm = 0$, heißt ein *Exponent von M*.

Bemerkung III.4.7: (i) Ist M ein endlich erzeugter Torsionsmodul über R, dann hat M einen Exponenten.

(ii) Summen von p-Torsionsmoduln sind wieder p-Torsionsmoduln. Insbesondere enthält jeder R-Modul M einen maximalen p-Torsionsmodul $M(p)$.

(iii) Ist M ein endlich erzeugter Torsionsmodul über R und c ein Exponent von M mit $c = ab$, dann sind

$$M_a = \{x \in M \mid ax = 0\}, \qquad M_b = \{x \in M \mid bx = 0\}$$

Untermoduln von M. Ist $\mathrm{ggT}(a, b) = 1$, dann ist $1 = \lambda a + \mu b$, d. h. für jedes $x \in M$ gilt $x = \lambda ax + \mu bx \in M_a \oplus M_b$ und damit $M = M_a \oplus M_b$.

Jeder endlich erzeugte Torsionsmodul M über R kann also geschrieben werden als $M = \bigoplus_p M(p)$, wobei wir über ein Vertretersystem der Primelemente von R summiert wird.

Lemma III.4.8: *Seien M ein p-Torsionsmodul über R mit Exponent p^e und $x_0 \in M$ ein Element von Periode p^e. Weiter sei $\pi\colon M \to M/\langle x_0\rangle$ die kanonische Projektion.*

(i) *Ist $y \in M/\langle x_0\rangle$ von Periode p^d, dann gibt es $z \in M$ von Periode p^d mit $\pi(z) = y$.*

(ii) *Sind $y_1, \ldots, y_n \in M/\langle x_0\rangle$ mit Perioden p^{d_i} und sind $z_1, \ldots, z_n \in M$ mit den gleichen Perioden und sodass $\pi(z_i) = y_i$, dann gilt: Ist die Summe $\langle y_1\rangle + \cdots + \langle y_n\rangle \subseteq M/(x_0)$ direkt, dann ist auch $\langle x_0\rangle + \langle z_1\rangle + \cdots + \langle z_n\rangle$ direkt.*

Beweis: (i) Sei z ein beliebiges Urbild von y. Dann ist $p^d z = p^r c x_0$, wobei p^r kein Teiler von c ist, und d ist minimal mit dieser Eigenschaft. Gilt $r = e$, dann hat z Periode p^d.

Ist $r < e$, so hat z Periode p^{d+e-r} und es ist $d + e - r \leq e$, da p^e Exponent für unseren Modul ist; d. h. $d \leq r$. Setze $z' = z - p^{r-d} c x_0 \in \pi^{-1}(\{y\})$; dieses z' hat Periode p^d. Das tut's!

(ii) Ist $ax_0 + b_1 z_1 + \cdots + b_n z_n = 0$, dann ist $b_1 y_1 + \cdots + b_n y_n = 0$. Die die Summe $\langle y_1\rangle + \cdots + \langle y_n\rangle$ direkt ist, folgt für $1 \leq i \leq n$ ist $b_i y_i = 0$; da die Perioden der y_i die p_i sind, muss für $1 \leq i \leq n$ gelten: p^{d_i} teilt b_i. Aber dann ist für $1 \leq i \leq n$ schon $b_i z_i = 0$ und somit erhalten wir $ax_0 = 0$, was wir zeigen wollten. □

Satz III.4.9: *Sei M ein endlich erzeugter p-Torsionsmodul über R. Dann ist*

$$M \cong \bigoplus_{i=1}^{n} R/(p^{e_i}).$$

und die $0 < e_1 \leq e_2 \leq \cdots \leq e_n$ sind eindeutig bestimmt durch den Modul.

Beweis: Sei $x_0 \in M$ ein Element von maximaler Periode p^e. Dann sind $M_p = \{x \in M \mid px = 0\}$ und $(M/\langle x_0\rangle)_p = \{y \in M/\langle x_0\rangle \mid py = 0\}$ endlichdimensionale Vektorräume über $R/(p)$.

Es gilt $\dim M_p > \dim(M/\langle x_0\rangle)_p$, denn für eine Basis $y_1, \ldots, y_n$ von $(M/\langle x_0\rangle)_p$ finden wir ein Element $x \in \langle x_0\rangle$ von Periode p und für $1 \leq i \leq n$ Urbilder $z_i \in \pi^{-1}(\{y_i\})$ von Periode p. Nun liefert Lemma III.4.8 die Behauptung über die Ungleichung.

Jetzt sind wir fertig, denn wir können Induktion über die Dimension von M_p führen und finden so, dass $M/\langle x_0\rangle \cong \bigoplus_{i=1}^n R/(p^{e_i})$ und das Lemma III.4.8 sagt

$$M \cong \langle x_0\rangle \oplus \bigoplus_{i=1}^n R/(p^{e_i}) \cong R/(p^e) \oplus \bigoplus_{i=1}^n R/(p^{e_i}).$$

Die Eindeutigkeit der Exponenten folgt aus dem nächsten Satz. □

Satz III.4.10: *Sei $M \neq \{0\}$ ein endlich erzeugter Torsionsmodul. Dann ist*

$$M \cong \bigoplus_{i=1}^n R/(q_i),$$

wobei für $1 \leq i \leq n$ gilt, dass $q_i \in R - (R^\times \cup \{0\})$ und $q_1 \mid q_2 \mid \cdots \mid q_n$. Die Ideale (q_i) sind eindeutig.

Beweis: Zerlege $M = \bigoplus_{i=1}^s M(p_i)$ und zerlege $M(p_i) = \bigoplus_{j=1}^{r_i} R/(p^{e_{ij}})$ mit $e_{i_1} \leq \cdots \leq e_{i_{r_i}}$. Durch Auffüllen mit Nullen erhalten wir ein Schema

$$\begin{array}{lccccc} p_1 : & e_{1_1} & \leq & e_{1_2} & \leq \ \ldots \ \leq & e_{1_r} \\ p_2 : & e_{2_1} & \leq & e_{2_2} & \leq \ \ldots \ \leq & e_{2_r} \\ \vdots & \vdots & & \vdots & & \vdots \\ p_s : & e_{s_1} & \leq & e_{s_2} & \leq \ \ldots \ \leq & e_{s_r} \end{array}$$

Setze $q_i := p_1^{e_{1_i}} \cdot p_2^{e_{2_i}} \cdots p_s^{e_{s_i}}$. Dann gilt sowohl $q_1 \mid q_2 \mid \cdots \mid q_r$ und nach dem Chinesischen Restsatz erhalten wir die Isomorphie

$$\bigoplus_{i=1}^s R/(p_i^{e_{ij}}) \cong R/(q_j),$$

was die Existenz der Zerlegung beweist.

Für die Eindeutigkeit seien

$$M \cong R/(q_1) \oplus \cdots \oplus R/(q_r), \qquad M \cong R/(t_1) \oplus \cdots \oplus R/(t_s)$$

zwei Zerlegungen von M. Ist p ein Primteiler von q_1 und allen q_i, dann ist $M_p = \{x \in M \mid px = 0\} \cong \{(x_1, \ldots, x_r) \mid px_i = 0\}$ ein $R/(p)$-Vektorraum von Dimension r beziehungsweise $\#t_i$ und $p \mid t_i$. Aus Symmetriegründen ist $r = s$ und alle t_i werden von p geteilt. Schreibe $q_i = pq_i'$, $t_i = pt_i'$; dann ist

$$\begin{aligned} pM &\cong pR/(pq_1') \oplus \cdots \oplus pR/(pq_r') \cong R/(q_1') \oplus \cdots \oplus R/(q_r'), \\ M &\cong pR/(pt_1') \oplus \cdots \oplus pR/(pt_r') \cong R/(t_1') \oplus \cdots \oplus R/(t_r'). \end{aligned}$$

Induktion nach der Anzahl der Primteiler liefert jetzt die Behauptung. □

Beispiel III.4.11: (i) Seien k ein Körper, V ein endlichdimensionaler k-Vektorraum und $\varphi \in \mathrm{End}_k(V)$. Dann induziert φ eine $k[X]$-Modulstruktur auf V via $f \bullet v := f(\varphi)(v)$. Aus Dimensionsgründen ist V ein Torsionsmodul über $k[X]$, d. h.

$$V \cong k[X]/(q_1) \oplus \cdots \oplus k[X]/(q_r)$$

für Polynome $q_1 \mid q_2 \mid \cdots \mid q_r$. Das Polynom q_r ist das Minimalpolynom von φ. Zerfalle $q_r = \prod_i (X_i - a_i)^{e_i}$ in Linearfaktoren. In unserer anderen Klassifikation sehen wir $V \cong \bigoplus_i V_{(X-a_i)}$ und

$$V_{(X-a_i)} = k[X]/(X - a_i)^* \oplus \cdots \oplus k[X]/(X - a_i)^{e_i}.$$

Die Menge $\{(X-a)^0, \ldots, (X-a)^{e-1}\}$ ist k-Basis von $k[X]/(X-a)^e$ und X operiert auf $k[X]/(X-a)^e$ mit der Matrix

$$\begin{pmatrix} a & 0 & \cdots & \cdots & 0 \\ 1 & a & \ddots & & \vdots \\ 0 & 1 & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & a \end{pmatrix}$$

(ii) Seien k ein Körper und $U \subseteq k^\times$ eine endliche Untergruppe. Schreibe $U = \bigoplus_p U(p)$ und betrachte $x \in U(p)$ von maximaler Periode p^r. Dann gilt für alle $y \in U(p)$, dass $y^{p^r} = 1$, d. h. $U(p)$ ist enthalten in der Menge der Nullstellen von $X^{p^r} - 1$; insbesondere ist $\langle x \rangle$ enthalten in der Menge der Nullstellen von $X^{p^r} - 1$ und U ist zyklisch. Insbesondere ist die Einheitengruppe eines endlichen Körpers zyklisch.

5. Polynome über faktoriellen Ringen

Definition III.5.1: Seien R ein faktorieller Ring, $p \in R$ prim und $K = \mathrm{Quot}(R)$.

(i) Für ein $a \in R$ setzen wir

$$v_p(a) := \max\{r \in \mathbb{N}_0 : p^r \mid a\}$$

Wir folgen dabei der Konvention $v_p(0) = \infty$.

(ii) Für $a/b \in \mathrm{Quot}(R)$ setzen wir $v_p(a/b) := v_p(a) - v_p(b)$.

(iii) Für $f \in K[X]$, $f = \sum_{i=0}^{n} a_i X^i$ setzen wir $v_p(f) := \min v_p(a_i)$.

Bemerkung III.5.2: (i) Ist $a \in K$, so liegt a schon in R genau dann, wenn $v_p(a) \geq 0$ für alle Primelemente $p \in R$.

(ii) Genauso gilt für $f \in K[X]$ dass $f \in R[X] \subseteq K[X]$ genau dann, wenn $v_p(f) \geq 0$ für alle Primelemente $p \in R$.

(iii) Für $a, b \in K^\times$ gilt offenbar $v_p(ab) = v_p(a) + v_p(b)$.

Beispiel III.5.3: (i) In $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ sind zum Beispiel $v_2(24) = v_2(3 \cdot 8) = 2$, $v_2(1/13) = 0$, $v_2(1/26) = -1$ und

$$v_2\left(\frac{1}{2}X^3 + 2X + 1\right) = \min\{-1, 0, 1\} = -1.$$

(ii) In $k(T) = \mathrm{Quot}(k[T])$ sind zum Beispiel $v_T(2) = 0$, $v_T(T^2 + 1) = 0$, $v_T(T^3) = 3$, $v_T((T^2 + 1)/T) = 1$ und für $f = ST + S + S^2T^2 \in k(T)[S]$ ist $v_T(f) = \min\{0, 2\} = 2$.

Definition III.5.4: Seien R ein faktorieller Ring, $K = \mathrm{Quot}(R)$ und $f \in K[X]$ ein von Null verschiedenes Polynom. Für ein Vertretersystem P der Primelemente von R heißt

$$\mathrm{inh}(f) = \prod_{p \in P} p^{v_p(f)}$$

der *Inhalt von* f. Der Inhalt von f ist wohldefiniert bis auf Multiplikation mit einer Einheit in R.

Bemerkung III.5.5: (i) Für $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ist

$$\mathrm{inh}(f) = \mathrm{ggT}(a_0, \ldots, a_n).$$

(ii) Für $f \in K[X] - \{0\}$ ist $f \in R[X]$ genau dann, wenn $\mathrm{inh}(f) \in R$.

(iii) Für $f \in K[X] - \{0\}$ und $c \in K^\times$ ist offenbar $\operatorname{inh}(cf) = c \operatorname{inh}(f)$. Somit kann jedes $f \in K[X] - \{0\}$ geschrieben werden als $f = c \cdot g$, wobei $c = \operatorname{inh}(f)$ und $g \in R[X]$ mit $\operatorname{inh}(g) = 1$.

Beispiel III.5.6: Sei $f = \frac{1}{2}X^3 + 2X + 1 \in \mathbb{Q}[X]$. Dann ist $\operatorname{inh}(f) = \frac{1}{2}$ und $f = \frac{1}{2}g$ mit $g = X^3 + 4X + 2 \in \mathbb{Z}[X]$.

Satz III.5.7 (Lemma von Gauß): *Seien R ein faktorieller Ring und K der Quotientenkörper von R. Für $f, g \in K[X]$ gilt* $\operatorname{inh}(fg) = \operatorname{inh}(f) \operatorname{inh}(g)$.

Beweis: Wir schreiben $f = \operatorname{inh}(f) f'$ und $g = \operatorname{inh}(g) g'$ mit $f', g' \in R[X]$ von Inhalt 1 und sehen, dass

$$fg = \operatorname{inh}(f) \operatorname{inh}(g) f' g'.$$

Also reicht es zu zeigen, dass $\operatorname{inh}(f) = \operatorname{inh}(g) = 1$ bereits $\operatorname{inh}(fg) = 1$ impliziert. Dies zeigen wir auf zwei Weisen:

Seien einerseits $f = \sum_{i=0}^{d} a_i X^i$, $g = \sum_{j=0}^{\ell} b_i X^i$, $p \in R$ prim und $r, s \in \mathbb{N}_0$ maximal mit $p \nmid a_r$, $p \nmid b_s$. In fg ist $c = a_r b_s + a_{r-1} b_{s+1} + \cdots + a_{r+1} b_{s-1} + \ldots$ der Koeffizient von X^{r+s}. Offenbar gilt $p \nmid c$ und somit $v_p(fg) = 1$. Das heißt aber genau $\operatorname{inh}(fg) = 1$.

Sei andererseits $p \in R$ prim und $\pi \colon R[X] \to R/(p)[X]$ die kanonische Projektion. Wegen $\operatorname{inh}(f) = \operatorname{inh}(g) = 1$ ist $[f] \neq 0 \neq [g]$. Da aber $R/(p)[X]$ nullteilerfrei ist, ist damit auch $[fg] = [f][g] \neq 0$. Das gilt für alle primen $p \in R$, also muss $\operatorname{inh}(fg) = 1$ gelten. □

Korollar III.5.8: *Hat $f \in R[X]$ eine Faktorisierung $f = gh$ in $K[X]$, dann ist $f = \operatorname{inh}(g) \operatorname{inh}(h) g' h'$ mit $g', h' \in R[X]$ und $\operatorname{inh}(g) \operatorname{inh}(h) \in R$.*

Satz III.5.9: *Seien R ein faktorieller Ring und $K = \operatorname{Quot}(R)$. Dann ist auch $R[X]$ faktoriell und die irreduziblen Elemente in $R[X]$ sind die irreduziblen Elemente in R zusammen mit den Polynomen von Inhalt 1, die in $K[X]$ irreduzibel sind.*

Beweis: Sei f ein Polynom mit Koeffizienten in R. In $K[X]$ schreiben wir $f = c q_1 \cdots q_r$ mit $c = \operatorname{inh}(f) \in R$ und $q_i \in R[X]$, die irreduzibel in $K[X]$ sind und Inhalt 1 haben. Nach dem Lemma von Gauß ist $c \in R$. Das liefert die Existenz der Zerlegung.

Ist $f = c' q_1' \cdots q_r'$ eine weitere Zerlegung, so folgt aus der Eindeutigkeit der Zerlegung in $K[X]$, dass $r = s$ und dass $q_i = a_i q_i'$ mit $a_i \in K^\times$. Nun ist aber $1 = \operatorname{inh}(q_i) = \operatorname{inh}(a_i q_i') = a_i \operatorname{inh}(q_i') = a_i$, d. h. a ist schon eine Einheit in R, was die Eindeutigkeit der Zerlegung zeigt. □

Korollar III.5.10: *Ist R faktoriell, so ist auch $R[X_1, \ldots, X_n]$ faktoriell.*

Satz III.5.11 (Eisenstein-Kriterium): *Seien R ein faktorieller Ring, K der Quotientenkörper von R und $f = \sum_{i=0}^{d} a_i X^i \in R[X]$ ein Polynom vom Grad $d \geq 1$. Ist $p \in R$ prim und gelten*

(i) $a_d \not\equiv 0 \pmod{p}$,

(ii) $a_i \equiv 0 \pmod{p}$ *für* $0 \leq i \leq d-1$,

(iii) $a_0 \not\equiv 0 \pmod{p^2}$,

dann ist f irreduzibel in $K[X]$.

Beweis: Ohne Einschränkung gilt $\mathrm{inh}(f) = 1$. Ist $f = gh$ eine Faktorisierung in $K[X]$, dann ist $f = gh$ ohne Einschränkung eine Faktorisierung in $R[X]$. Seien $g = \sum_{i=0}^{r} b_i X^i$, $h = \sum_{j=0}^{s} c_j X^j$ mit $b_r \neq 0 \neq c_s$. Es gilt $a_0 = b_0 c_0$, ohne Einschränkung $p \mid c_0$ und $p \nmid b_0$. Außerdem gilt $a_d = b_r c_s$, d. h. $p \nmid b_r$ und $p \nmid c_s$. Sei jetzt t maximal mit der Eigenschaft $p \mid c_0, \ldots, c_t$; auf jeden Fall ist $0 \leq t < s < d$. Dann ist

$$a_{t-1} = b_0 c_{t+1} + b_1 c_t + \ldots,$$

wegen $p \mid c_0, \ldots, c_t$ teilt p alle Summanden ab dem zweiten. Der erste Summand wird nicht von p geteilt, da t entsprechend gewählt ist und b_0 nach Voraussetzung nicht von p geteilt wird. Ein Widerspruch! □

Beispiel III.5.12: (i) Das Polynom $3X + 15 \in \mathbb{Z}[X]$ ist irreduzibel über $\mathbb{Q}$, aber nicht über $\mathbb{Z}$, denn in $\mathbb{Z}[X]$ ist $3X^2 - 15 = 3(X^2 - 5)$ die eindeutige Zerlegung in irreduzible Elemente.

Genau so ist $6X^2 - 30$ irreduzibel in $\mathbb{Q}$, aber in $\mathbb{Z}[X]$ hat $6X^2 - 30$ die Zerlegung $6X^2 - 30 = 2 \cdot 3 \cdot (X^2 - 5)$.

(ii) Seien $a \in \mathbb{Z} - \{\pm 1\}$ und n eine natürliche Zahl größergleich Zwei. Dann ist das Polynom $X^n - a$ irreduzibel genau dann, wenn a quadratfrei ist.

(iii) Seien p eine positive Primzahl und $f = X^{p-1} + X^{p-2} + \cdots + X + 1$. Dann ist f irreduzibel über $\mathbb{Q}$, denn $f = (X^p - 1)/(X - 1)$; diese Faktorisierung kann man einsehen über Polynomdivision oder über die geometrische Reihe. Es ist

$$f(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = X^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} X^{i-1} + p,$$

d. h. f ist irreduzibel nach dem Eisensteinkriterium.

Kapitel IV.

Algebraische Körpererweiterungen

Zum Beispiel das Polynom $X^2 - 5 \in \mathbb{Q}[X]$ hat keine Nullstelle über $\mathbb{Q}$. Dieses Problem wollen wir durch „Vergrößerung des Körpers“ lösen; das Ziel ist, einen Körper zu basteln, in dem alle Polynome mit Koeffizienten im ursprünglichen Körper in Linearfaktoren zerfallen.

1. Algebraische Körpererweiterungen

Wir kennen bereits die Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}(\sqrt{5})$, Quotientenkörper von Integritätsringen und Quotientenringe von maximalen Idealen in Ringen, zum Beispiel $K[X]/(f)$ mit einem irreduziblen $f \in K[X]$.

Definition IV.1.1 (Körpererweiterung): (i) Seien K und L Körper. Gilt $K \subseteq L$, dann heißt L eine *Körpererweiterung von K*. Man schreibt dafür auch „L/K“, „$L|K$“ oder „Sei $K \subseteq L$ eine Körpererweiterung“. Wir können in diesem Fall L als einen K-Vektorraum auffassen.

(ii) Die Zahl $[L : K] := \dim_K(L)$ heißt *Grad* der Körpererweiterung $K \subseteq L$.

(iii) Ist $[L : K] < \infty$, so heißt die Körpererweiterung $K \subseteq L$ *endlich*.

(iv) Sind K_1, K_2 und K_3 Körper mit $K_1 \subseteq K_2 \subseteq K_3$, dann heißt K_2 *Zwischenkörper* der Körpererweiterung $K_1 \subseteq K_3$.

Proposition IV.1.2: *Für zwei endliche Körpererweiterungen $K_1 \subseteq K_2$ und $K_2 \subseteq K_3$ gilt*

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1].$$

Beweis: Ist $\{b_1, \ldots, b_n\}$ eine K_2-Basis von K_3 und $\{c_1, \ldots, c_k\}$ eine K_1-Basis von K_2, dann ist $\{b_i c_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, k\}\}$ eine K_1-Basis von K_3.□

Definition IV.1.3 (Algebraische Körpererweiterungen): Sei $K \subseteq L$ eine Körpererweiterung.

(i) Sei $\alpha \in L$. Gibt es $f \in K[X]$ mit $f(\alpha) = 0$, dann heißt α *algebraisch* (über K).

(ii) Sind alle Elemente von L algebraisch über K, dann heißt die Körpererweiterung $K \subseteq L$ *algebraisch*.

Definition IV.1.4 (Minimalpolynom): Seien $K \subseteq L$ eine Körpererweiterung und $\alpha \in L$ algebraisch.

(i) Die Menge $I_\alpha := \{f \in K[X] \mid f(\alpha) = 0\} \subseteq K[X]$ ist ein Ideal in $K[X]$, und damit ein Hauptideal. Sei f_α das eindeutige normierte Polynom, das I_α erzeugt. Dann heißt f_α das *Minimalpolynom von* α.

(ii) Der Kern des Einsetzungshomomorphismus $\varphi_\alpha \colon K[X] \to L$, $f \mapsto f(\alpha)$ ist genau I_α.

Definition IV.1.5 (Erzeugnisse): Seien $K \subseteq L$ eine Körpererweiterung und $\alpha_1, \ldots, \alpha_n \in L$.

(i) Die Menge

$$K[\alpha_1, \ldots, \alpha_n] := \bigcap \{A \mid K \subseteq A \subseteq L \text{ ist } K\text{-Algebra}, \{\alpha_1, \ldots, \alpha_n\} \subseteq A\}$$

heißt die von $\alpha_1, \ldots, \alpha_n$ *erzeugte K-Algebra* und ist in der Tat eine K-Algebra.

(ii) Die Menge $K(\alpha_1, \ldots, \alpha_n)$ ist die von $\alpha_1, \ldots, \alpha_n$ erzeugte Körperalgebra von K in L.

(iii) Gibt es $\alpha \in L$ mit $L = K(\alpha)$, dann heißt die Körpererweiterung einfach.

Bemerkung IV.1.6: Ist $K \subseteq L$ eine Körpererweiterung und sind $\alpha_1, \ldots, \alpha_n \in L$ Elemente, dann können wir $K[\alpha_1, \ldots, \alpha_n]$ und $K(\alpha_1, \ldots, \alpha_n)$ folgendermaßen charakterisieren: Es ist $K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}$ und $K(\alpha_1, \ldots, \alpha_n) = \mathrm{Quot}(K[\alpha_1, \ldots, \alpha_n])$.

Beispiel IV.1.7: Seien $K \subseteq L$ eine Körpererweiterung und $\alpha \in L$.

(i) Ist α algebraisch und f_α das Minimalpolynom von α mit $d := \deg(f_\alpha)$, dann ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ eine K-Basis von $K(\alpha)$ und $[K(\alpha) : K] = d$. Wir erhalten die kurze exakte Sequenz

$$\{0\} \longrightarrow (f_\alpha) = I_\alpha \longrightarrow K[X] \xrightarrow{\varphi_\alpha} K(\alpha) \longrightarrow \{0\}$$

d. h. es gilt $K(\alpha) = K[X]/(f_\alpha)$.

(ii) Ist α nicht algebraisch, dann ist $[L : K] = \infty$.

Bemerkung IV.1.8: Sei $K \subseteq L$ eine Körpererweiterung.

(i) Die Körpererweiterung ist endlich genau dann, wenn es endlich viele algebraische $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$ gibt.

(ii) Die Körpererweiterung ist algebraisch genau dann, wenn L als Körpererweiterung von K von algebraischen Elementen erzeugt wird.

(iii) Sind $K_1 \subseteq K_2$ und $K_2 \subseteq K_3$ algebraische Körpererweiterungen, dann ist auch $K_1 \subseteq K_3$ eine algebraische Körpererweiterung.

Beweis: (i) „⇒“: Klar mit Beispiel IV.1.7.
„⇐“: Das ist eine Konsequenz von Beispiel IV.1.7. zusammen mit Proposition IV.1.2.

(ii) „⇒“: Klar.
„⇐“: Seien $\alpha_1, \alpha_2 \in L$ algebraisch über K. Nach Beispiel IV.1.7. sind die Körpererweiterung $K \subseteq K(\alpha_1)$ und $K(\alpha_1) \subseteq K(\alpha_1, \alpha_2)$ endliche Körpererweiterungen. Nach Proposition IV.1.2 ist dann auch $K \subseteq K(\alpha_1, \alpha_2)$ eine endliche Körpererweiterung. Nach (i) ist dann $K \subseteq K(\alpha_1, \alpha_2)$ eine algebraische Körpererweiterung, d. h. $\alpha_1 + \alpha_2$, $\alpha_1\alpha_2$ und α_1/α_2 (falls $\alpha_2 \neq 0$) sind ebenfalls algebraisch über K.

(iii) Sei $\alpha \in K_3$. Dann gibt es $f = \sum_{k=0}^{d} c_k X^k \in K_2[X]$ mit $f(\alpha) = 0$. Die Körpererweiterungen $K_1 \subseteq K_1(c_0, \ldots, c_d) \subseteq K_1(c_0, \ldots, c_d, \alpha)$ sind jeweils algebraisch (nach Voraussetzung) und damit (nach (i)) endlich. Jetzt gibt Proposition IV.1.2, dass $K_1 \subseteq K_1(c_0, \ldots, c_d, \alpha)$ endlich über K_1 ist. Nach (i) ist deshalb α algebraisch über K_1. □

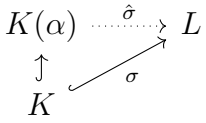
Proposition IV.1.9 (Konstruktion von Kronecker): *Es seien K ein Körper und $f \in K[X]$ ein Polynom mit $\deg(f) \geq 1$. Dann gibt es eine Körpererweiterung $K \subseteq L$, sodass f eine Nullstelle in L hat.*

Beweis: Sei $f = \sum_{i=0}^{d} c_i X^i$ mit $c_i \in K$. Ist f irreduzibel, dann ist $(f) \subseteq K[X]$ ein maximales Ideal, d. h. $L := K[X]/(f)$ ist ein Körper. Die Komposition $K \hookrightarrow K[X] \xrightarrow{\pi} L$ ist ein Körperhomomorphismus, damit insbesondere injektiv und wir können L als Körpererweiterung von K auffassen. Bleibt zu zeigen, dass f eine Nullstelle in L hat. Für $\alpha := \pi(X)$ gilt

$$f(\alpha) = \sum_{i=0}^{d} c_i \alpha^i = \sum_{i=0}^{d} c_i \pi(X)^i = \pi\Big(\sum_{i=0}^{d} c_i X^i\Big) = \pi(f) = 0.$$

Ist f nicht irreduzibel, dann können wir f zerlegen in irreduzible Faktoren und erhalten so jedenfalls eine Nullstelle eines irreduziblen Faktors, also von f. □

Vorüberlegung IV.1.10: Seien K ein Körper, $K \subseteq H$ eine Körpererweiterung, $\alpha \in H$ und $K \subseteq L$ eine weitere Körpererweiterung. Dann sind wir in der Situation



Für $f = \sum_{k=0}^{d} c_k X^k \in K[X]$ mit $f(\alpha) = 0$ schreiben wir $f^\sigma := \sum_{k=0}^{d} \sigma(c_k) X^k$. Dann ist

$$f^\sigma(\hat{\sigma}(\alpha)) = \sum_{k=0}^{d} \sigma(c_k) \cdot (\hat{\sigma}(\alpha))^k = \hat{\sigma}\Big(\sum_{k=0}^{d} c_k \alpha^k \Big) = \hat{\sigma}(0) = 0.$$

Satz IV.1.11 (Fortsetzungssatz I): *Es seien $K \subseteq K(\alpha)$ eine algebraische Körpererweiterung, $f = f_\alpha$ das Minimalpolynom von α und $\sigma\colon K \to L$ ein Körperhomomorphismus.*

(i) *Für jede Fortsetzung $\hat{\sigma}\colon K(\alpha) \to L$ von $\sigma\colon K \to L$ ist $\hat{\sigma}(\alpha)$ eine Nullstelle von f_α^σ (siehe Vorüberlegung IV.1.10).*

(ii) *Sei $\mathrm{Hom}_\sigma(K(\alpha), L) := \{\hat{\sigma}\colon K(\alpha) \to L \mid \hat{\sigma}|_K = \sigma\}$. Dann ist die Abbildung*

$$\mathrm{Hom}_\sigma(K(\alpha), L) \longrightarrow \mathrm{Nst}_L(f_\alpha^\sigma) := \{\beta \in L \mid f_\alpha^\sigma(\beta) = 0\}, \qquad \hat{\sigma} \longmapsto \hat{\sigma}(\alpha)$$

eine Bijektion.

Beweis: (i) ist eine Konsequenz von Vorüberlegung IV.1.10.

Zu (ii): Die Abbildung ist injektiv, da $K(\alpha)$ von α erzeugt wird. Die Abbildung ist außerdem surjektiv, denn: Ist β eine Nullstelle von f_α^σ, definiere $\bar{\sigma}\colon K[X] \to L$, durch $X \mapsto \beta$ mit $\bar{\sigma}|_K = \sigma$. Dann ist

$$\bar{\sigma}(f) = \bar{\sigma}(\sum_{k=0}^{d} c_k X^k) = \sum_{k=0}^{d} \sigma(c_k)\beta^k = f^\sigma(\beta) = 0,$$

d. h. $\bar{\sigma}$ steigt ab zu einem Körperhomomorphismus $\hat{\sigma}\colon K(\alpha) \cong K[X]/(f_\alpha) \to L$ mit $\bar{\sigma}|_K = \sigma$ und $\bar{\sigma}(\alpha) = \hat{\sigma}(X) = \beta$. □

Proposition IV.1.12 (Iteriertes Kroneckerverfahren): *Sei $f \in K[X]$ ein Polynom des Grades d. Dann gibt es eine Körpererweiterung $K \subseteq L$ mit den Eigenschaften:*

(i) *Das Polynom f zerfällt über L in Linearfaktoren, d. h. es gibt $\alpha_1, \ldots, \alpha_d \in L$ mit $f = \prod_{i=0}^{n}(X - \alpha_i) \in L[X]$,*

(ii) *Die Körpererweiterung L wird von den Nullstellen von f erzeugt, d. h. $L = K(\alpha_1, \ldots, \alpha_d)$.*

Beweis: Wir zeigen die Aussage via Induktion über den Grad d von f. Für $d = 1$ ist alles klar.

Ist $d \geq 1$, dann gibt es eine Körpererweiterung $K \subseteq L_1$ wie in Proposition IV.1.9. In L_1 hat f also eine Nullstelle α_1 und wir können zerlegen $f = (X - \alpha_1)g$ in $L[X]$. Nach Induktionsvoraussetzung gibt es eine Körpererweiterung $L_1 \subseteq L$ und Elemente $\alpha_2, \ldots, \alpha_d \in L$, sodass $g = \prod_{i=2}^{d}(X-\alpha_i) \in L[X]$ und $L = L_1(\alpha_2, \ldots, \alpha_d)$. Damit ist aber $L = K(\alpha_1, \ldots, \alpha_d)$ und $f = \prod_{i=1}^{d}(X - \alpha_i) \in L[X]$. □

Definition IV.1.13 (Zerfällungskörper): Sei $f \in K[X]$. Eine Körpererweiterung $K \subseteq L$ heißt *Zerfällungskörper von f*, falls f über L in Linearfaktoren zerfällt und L von den Nullstellen von f erzeugt wird.

Proposition IV.1.14 (Eindeutigkeit des Zerfällungskörpers): *Zu jedem Polynom $f \in K[X]$ gibt es einen Zerfällungskörper $Z(f)$ von f. Dieser ist bis auf Isomorphie über K eindeutig, d. h. sind L_1 und L_2 Zerfällungskörper von f, dann gibt es einen Isomorphismus $\varphi\colon L_1 \to L_2$ mit $\varphi|_K = \mathrm{id}_K$, d. h. das Diagramm*

$$\begin{array}{ccc} L_1 & \xrightarrow{\varphi} & L_2 \\ \uparrow & \nearrow & \\ K & & \end{array}$$

kommutiert

Beweis: Die Existenz ist sichergestellt durch Proposition IV.1.12. Zur Eindeutigkeit: Sind $K(\alpha_1, \ldots, \alpha_d)$ und $K(\beta_1, \ldots, \beta_d)$ zwei Zerfällungskörper von f, dann ist wegen Satz IV.1.11 durch $\alpha_i \mapsto \beta_i$ ein Homomorphismus erklärt. Durch $\beta_i \mapsto \alpha_i$ wird der Umkehrhomomorphismus geklärt, was die Surjektivität zeigt. □

Bemerkung IV.1.15: Ist $f \in K[X]$ ein Polynom vom Grad d, dann lesen wir aus dem Beweis von Proposition IV.1.12 und Proposition IV.1.14 ab, dass $[Z(f) : K] \leq d!$.

2. Der algebraische Abschluss

In diesem Abschnitt sei K stets ein Körper. Zu K suchen wir eine algebraische Körpererweiterung $\bar{K}$ von K, die alle algebraischen Körpererweiterungen von

K enthält. Für eine solche Körpererweiterung gälte: Jedes Polynom in $\bar{K}[X]$ zerfällt in Linearfaktoren.

Definition IV.2.1 (Algebraisch abgeschlossen): Der Körper K heißt *algebraisch abgeschlossen*, falls jedes Polynom $f \in K[X]$ mit $\deg(f) \geq 1$ eine Nullstelle in K hat.

Beispiel IV.2.2: Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen. Diese Aussage zeigen wir später.

Proposition IV.2.3: *Die folgenden Aussagen sind äquivalent:*

(i) *K ist algebraisch abgeschlossen.*

(ii) *Jedes Polynom $f \in K[X]$ zerfällt über K in Linearfaktoren.*

(iii) *Jedes irreduzible Polynom f aus $K[X]$ ist linear.*

(iv) *Es gibt keine echten algebraischen Körpererweiterungen von $K \subseteq L$, d. h. ist $K \subseteq L$ eine algebraische Körpererweiterung, dann ist $K = L$.*

(v) *Jede echte Körpererweiterung $K \subseteq L$ hat unendlichen Grad, d. h. es gilt $[L : K] = \infty$.*

Beweis: „(i) $\Rightarrow$ (ii)“ und „(ii) $\Rightarrow$ (iii)“ sind klar.

Zu „(iii) $\Rightarrow$ (iv)“: Sei $K \subseteq L$ eine algebraische Körpererweiterung und $\alpha \in L$. Das Minimalpolynom $f_\alpha \in K[X]$ von α über K ist nach Voraussetzung linear, d. h. es ist bereits $\alpha \in K$.

„(iv) $\Rightarrow$ (v)“: Endliche Körpererweiterungen sind stets algebraisch.

„(v) $\Rightarrow$ (i)“: Das ist garantiert durch Proposition IV.1.9. $\square$

Definition IV.2.4: Eine Körpererweiterung $K \subseteq L$ heißt *algebraischer Abschluss von K*, falls die Körpererweiterung algebraisch ist und L algebraisch abgeschlossen ist.

Bemerkung IV.2.5: Ist $K \subseteq L$ eine Körpererweiterung, wobei L algebraisch abgeschlossen ist, dann ist

$$A(L/K) := \{\alpha \in L \mid \alpha \text{ ist algebraisch über } L\}$$

ein algebraischer Abschluss von K.

Beweis: Die Menge $A(L/K)$ ist ein Körper, denn sind $\alpha, \beta \in A(L/K)$, dann gilt nach Bemerkung IV.1.8 schon $K(\alpha, \beta) \subseteq A(L/K)$, d. h. $\alpha + \beta, \alpha\beta$ und α/β (sofern definiert) sind ebenfalls in $A(L/K)$ enthalten.

Per Definition ist die Körpererweiterung $K \subseteq A(L/K)$ algebraisch. Bleibt zu zeigen, dass $A(L/K)$ algebraisch abgeschlossen ist. Ist $f \in A(L/K)[X]$, dann ist $f \in L[X]$. Da L algebraisch abgeschlossen ist, hat f eine Nullstelle $\alpha \in L$. Dieses α ist algebraisch über $A(L/K)$ und $A(L/K)$ ist algebraisch über K, d. h. α ist algebraisch über K und damit schon $\alpha \in A(L/K)$. □

Beispiel IV.2.6: Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{C}$ ist nicht algebraisch, denn $\mathbb{C}$ ist überabzählbar. Wir schreiben $\bar{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ ist algebraisch über } \mathbb{Q}\}$ für den algebraischen Abschluss von $\mathbb{Q}$.

Satz IV.2.7 (über den algebraischen Abschluss):

(i) *Jeder Körper K hat einen algebraischen Abschluss $\bar{K}$.*

(ii) *Ein algebraischer Abschluss $\bar{K}$ ist eindeutig bis auf Isomorphie über K.*

(iii) *Die Körpererweiterung $K \subseteq \bar{K}$ ist die maximale algebraische Körpererweiterung in dem folgenden Sinn: Ist $K \subseteq L$ eine algebraische Körpererweiterung, dann gibt es eine Einbettung $\sigma\colon L \hookrightarrow \bar{K}$ mit $\sigma|_K = \mathrm{id}_K$.*

Proposition IV.2.8 („halbe Existenz“): *Es gibt eine algebraische Körpererweiterung $K \subseteq \bar{K}$, sodass für jedes nicht-konstante Polynom $f \in K[X]$ in $\bar{K}$ eine Nullstelle hat.*

Beweis: Für jedes $f \in K[X] - K$ sei X_f ein Symbol und

$$\mathfrak{X} := \{X_f \mid f \in K[X] - K\}.$$

Setze $R := K[\mathfrak{X}]$ und $I := (\{f(X_f) \mid X_f \in \mathfrak{X}\})$ das von allen $f(X_f)$ erzeugte Ideal. Ist $I \neq R$, dann gibt es ein maximales Ideal $\mathfrak{m} \subseteq R$ mit $I \subseteq \mathfrak{m}$. Angenommen, $I = R$. Dann wäre insbesondere $1 \in I$. Wir hätten also eine Darstellung $1 = \sum_{i=1}^{n} g_i f_i(X_{f_i}) =: h$ mit $g_i \in R$ und $f_i \in K[X] - K$. Sei $K \subseteq L$ eine Körpererweiterung, in der jedes f_i eine Nullstelle α_i hat (z. B. $Z(f_1 \cdots f_n)$). Setze in $h \in R = K[\mathfrak{X}]$ für X_f jeweils ein: α_i, falls $f = f_i$, 42 sonst. In L gilt dann

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, \alpha_2, \ldots, \alpha_n, 42, 42, \ldots) \cdot f_i(\alpha_i) = 0,$$

ein Widerspruch.

Wir setzen $K' := R/\mathfrak{m}$. Dieses K' ist ein Körper und wir haben eine Einbettung $K \hookrightarrow K'$; außerdem ist für alle $f \in K[X] - K$ schon $f([X_f]) = [f(X_f)] = 0$, d. h. K' leistet das Gewünschte. □

Beweis (von Satz IV.2.7): Definiere rekursiv $K_0 := K$ und $K_{i+1} := (K_i)'$ mit K_i' wie in Proposition IV.2.8. Das liefert eine Körperkette $K_0 \subseteq K_1 \ldots$ Setze $L := \bigcup_{i \geq 1} K_i$. Dann gelten:

(i) L ist ein Körper, denn für $\alpha \in K_i$ und $\beta \in K_j$, wobei $i \leq j$, ist auch $\alpha \in K_j$, d. h. es sind auch $\alpha + \beta$, $\alpha\beta$ und α/β (sofern $\beta \neq 0$) in K_j.

(ii) L ist algebraisch über K, ist nämlich $\alpha \in L$, dann gibt es $i \in \mathbb{N} - \{0, 1\}$ sodass $\alpha \in K_i$. Nach Bemerkung II.4.2 ist $K \subseteq K_i$ algebraisch, also ist α algebraisch über K.

(iii) L ist algebraisch abgeschlossen. Ist nämlich $f = \sum_{i=0}^{d} c_n X^n \in L[X]$, dann sind $c_0, \ldots, c_d \in K_i$ für irgendein ausreichend großes i. Nach Konstruktion hat also f eine Nullstelle in $K_{i+1} \subseteq L$.

Die Teile (ii) und (iii) sind direkte Konsequenzen aus dem nachfolgenden Satz. □

Satz IV.2.9 (Fortsetzungssatz II): *Es seien $K \subseteq K'$ und $K \subseteq L$ algebraische Körpererweiterungen und L sei algebraisch abgeschlossen.*

(i) *Jeder Homomorphismus $\sigma\colon K \hookrightarrow L$ besitzt eine Fortsetzung $\sigma'\colon K' \hookrightarrow L$, also $\sigma'|_K = \sigma$.*

(ii) *Ist außerdem K' algebraisch abgeschlossen und $L(\sigma(K))$ algebraisch, dann ist σ' ein Isomorphismus.*

Beweis: (i) Wir wollen das Lemma von Zorn und Satz IV.1.11 verwenden. Setze

$$\mathfrak{X} := \{(F, \tau) \mid F \text{ ist ein Zwischenkörper von } K \subseteq K' \text{ und } \tau\colon F \hookrightarrow L \text{ mit } \tau|_K = \sigma\}.$$

Dann gelten:

(1) $\mathfrak{X}$ ist partiell geordnet durch $(F_1, \tau_1) \leqslant (F_2, \tau_2)$ genau dann, wenn $F_1 \subseteq F_2$ und $\tau_2|_{F_1} = \tau_1$.

(2) (K, σ) ist ein Element von $\mathfrak{X}$, d. h. $\mathfrak{X} \neq \varnothing$.

(3) $(\mathfrak{X}, \leqslant)$ ist induktiv geordnet, denn für eine Kette $\mathfrak{K}$ in $\mathfrak{X}$ erhalten wir eine Schranke $(F_{\mathfrak{K}}, \tau_{\mathfrak{K}})$ durch $F_{\mathfrak{K}} := \bigcup_{F \in \mathfrak{K}} F$ und $\tau_{\mathfrak{K}}\colon F_{\mathfrak{K}} \to L$, $\alpha \mapsto \tau_F(a)$, wobei F ein Körper in $\mathfrak{K}$ ist, der a enthält.

Nach dem Lemma von Zorn gibt es ein maximales Element $(\hat{F}, \hat{\sigma})$ in $\mathfrak{X}$. Bleibt zu zeigen, dass $\hat{F} = K'$. Wäre $\hat{F} \subsetneq K'$, dann könnte man $a \in K' - \hat{F}$ wählen. Nach Satz IV.1.11 gäbe es eine Fortsetzung $\hat{\sigma}' \colon \hat{F}(\alpha) \to L$, die $\hat{\sigma}'|_{\hat{F}} = \hat{\sigma}$. Dies steht im Widerspruch zur Maximalität von $\hat{F}$. Insgesamt erhalten wir also $\hat{\sigma} \colon \hat{F} = K' \to L$ mit $\hat{\sigma}|_K = \mathrm{id}_K$.

(ii) Sei nun K' algebraisch abgeschlossen. Dann ist auch $\hat{\sigma}(K') \subseteq L$ algebraisch abgeschlossen und die Erweiterung $\sigma(K') \subseteq L$ ist algebraisch. Nach Proposition IV.2.3 ist dann $L' = \sigma(\hat{K})$, d. h. $\hat{\sigma}$ ist surjektiv und als Körperhomomorphismus damit bijektiv. □

3. Normale Körpererweiterungen

In diesem Abschnitt sei K stets ein Körper.

Definition IV.3.1 (Normale Körpererweiterungen): Es sei $F \subseteq K[X]$ eine Menge nicht-konstanter Polynome. L heißt *Zerfällungskörper von* F, falls die folgenden beiden Bedingungen gelten:

(i) Jedes $f \in F$ zerfällt über L in Linearfaktoren, d. h. wir können schreiben $f = c \cdot \prod_{i=1}^{n}(X - \alpha_i)$, wobei $c \in K$, $\alpha_i \in L$, $1 \leq i \leq n$ und n der Grad von f ist.

(ii) Die Körpererweiterung $K \subseteq L$ wird erzeugt von den Nullstellen der $f \in F$.

Wir schreiben in diesem Fall $L = Z(F)$.

Eine Körpererweiterung $K \subseteq L$ heißt *normal*, falls L ein Zerfällungskörper für eine Teilmenge F in $K[X]$ ist.

Bemerkung IV.3.2 (Bilder von Zerfällungskörpern): Seien $F \subseteq K[X]$ und $L_1 = Z(F)$ eine normale Körpererweiterung. Für einen Körperhomomorphismus $\sigma \colon L_1 \to L_2$ in einen beliebigen Körper L_2 gilt $\sigma(L_1) = Z(F^\sigma)$, wobei wir ${}^\sigma F := \{\sigma(f) \mid f \in K[X]\}$ schreiben und wir für $f = \sum_{i=0}^{n} a_i X^i \in F$ setzen $\sigma(f) := \sum_{i=0}^{n} \sigma(a_i) X^i$.

Bemerkung IV.3.3 (Zerfällungskörper in algebraischem Abschluss): Es seien $F \subseteq K[X] - K$ und $\bar{K}$ ein algebraischer Abschluss. Definiere $L := K(A)$, wobei $A := \{\alpha \in \bar{K} \mid \text{Es gibt } f \in F \text{ mit } f(\alpha) = 0\}$. Dann ist L Zerfällungskörper von F mit $K \subseteq L \subseteq \bar{K}$ und L ist eindeutig mit dieser Eigenschaft.

Definition IV.3.4: Seien $K \subseteq L_1$ und $K \subseteq L_2$ Körpererweiterungen. Ein Körperhomomorphismus $\Phi\colon L_1 \to L_2$ heißt *K-Homomorphismus*, falls $\Phi|_K = \mathrm{id}_K$.

Wir schreiben $\mathrm{Hom}_K(L_1, L_2) := \{\Phi\colon L_1 \to L_2 \mid \Phi \text{ ist } K\text{-Homomorphismus}\}$ und $\mathrm{Aut}_K(L_1) := \mathrm{Hom}_K(L_1, L_1)$.

Proposition IV.3.5 (Normaler Abstieg): *Es seien $F \subseteq K[X]$, L_1 und L_2 zwei Zerfällungskörper von F und $\bar{L}_2$ ein algebraischer Abschluss von L_2.*

(i) *Für jeden K-Homomorphismus $\hat{\sigma}\colon L_1 \hookrightarrow \bar{L}_2$ gilt $\hat{\sigma}(L_1) = L_2$, $\hat{\sigma}$ schränkt sich also ein zu einem K-Homomorphismus $\sigma\colon L_1 \to L_2$.*

(ii) *L_1 und L_2 sind K-isomorph.*

Beweis: Aussage (i) folgt aus Bemerkung IV.3.2 und Bemerkung IV.3.3, Aussage (ii) folgt aus (i) und Satz IV.2.7. □

Satz IV.3.6 (Charakterisierung normaler Körpererweiterungen): *Es seien K ein Körper mit algebraischem Abschluss $\bar{K}$ und L ein Zwischenkörper von $K \subseteq \bar{K}$. Dann sind äquivalent:*

(i) *Die Erweiterung $K \subseteq L$ ist normal.*

(ii) *Für alle $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ gilt $\sigma(L) = L$.*

(iii) *Jedes irreduzible Polynom $f \in K[X]$, welches in L eine Nullstelle hat, zerfällt über L in Linearfaktoren.*

Beweis: „(i) ⇒ (ii)“: Das folgt aus Proposition IV.3.5, Bemerkung IV.3.2 und Bemerkung IV.3.3.

„(ii) ⇒ (iii)“: Schreibe $f = c \cdot \prod_{i=1}^{d}(X - \alpha_i)$ mit $\alpha_i \in \bar{K}$ und $c \in K$. Wir zeigen für $i \geq 2$, dass $\alpha_i \in L$. Nach Satz IV.1.11 gibt es einen Körperhomomorphismus $\sigma\colon K(\alpha_1) \hookrightarrow \bar{K}$ mit $\sigma(\alpha_1) = \alpha_i$ und nach Satz IV.2.9 hat dieses σ eine Fortsetzung $\hat{\sigma}\colon L \hookrightarrow \bar{K}$. Nach Voraussetzung ist aber $\hat{\sigma}(L) = L$, d. h. es gilt $\sigma(\alpha_1) = \alpha_i \in L$.

„(iii) ⇒ (i)“: Sei $\{\alpha_i \mid i \in I\} \subseteq L$ eine Menge von Erzeugern der Körpererweiterung $K \subseteq L$, ferner bezeichne jeweils f_i das Minimalpolynom von α_i. Nach (iii) zerfällt jedes dieser f_i über L in Linearfaktoren, d. h. L ist Zerfällungskörper von $\{f_i \mid i \in I\}$. □

Bemerkung IV.3.7: Für eine normale Körpererweiterung $K \subseteq L$ erhalten wir also die Abbildung $\mathrm{Hom}_K(L, \bar{K}) \to \mathrm{Aut}_K(L)$, $\sigma \mapsto \sigma$, die das Bild auf L einschränkt.

Definition IV.3.8 (Normale Hülle): Seien $K \subseteq L$ eine algebraische Körpererweiterung. Eine algebraische Körpererweiterung $L \subseteq L'$ heißt *normale Hülle von* $K \subseteq L$, falls die beiden folgenden Bedingungen gelten:

(i) $K \subseteq L'$ ist eine normale Körpererweiterung und

(ii) L' ist minimal mit dieser Eigenschaft, d. h. es gibt keinen echten Zwischenkörper von $L \subseteq L'$, der (i) erfüllt.

Proposition IV.3.9 (Existenz und Eindeutigkeit der normalen Hülle): *Es sei $K \subseteq L$ eine normale Körpererweiterung. Dann gelten:*

(i) *Es gibt eine normale Hülle L' von $K \subseteq L$. Diese ist bis auf L-Isomorphie eindeutig,*

(ii) *Ist $K \subseteq L$ eine endliche Körpererweiterung, dann ist $K \subseteq L'$ auch eine endliche Körpererweiterung.*

Proposition IV.3.10 (Normale Hülle in M): *Sei $K \subseteq L$ eine algebraische Körpererweiterung und $L \subseteq M$ eine algebraische Körpererweiterung, sodass $K \subseteq M$ normal ist. Dann enthält M genau eine normale Hülle L' von $K \subseteq L$ und es gilt:*

(i) $L' = \bigcap \{F \mid L \subseteq F \subseteq M \text{ und } K \subseteq F \text{ ist normal}\}$.

(ii) *Für jedes Erzeugendensystem A von $K \subseteq L$ gilt: L' ist Zerfällungskörper von $\mathfrak{F} := \{f_\alpha \mid f_\alpha \text{ ist Minimalpolynom von } \alpha \in A\}$.*

(iii) $L' = K(\bigcup \{\sigma(L) \mid \sigma \in \mathrm{Hom}_K(L, M)\}) =: E$.

Der Körper L' heißt dann Normale Hülle von $K \subseteq L$ in M.

Beweis: (i) Für die Existenz der normalen Hülle: Definiere L' wie in (i). Dann ist L' normal (da $K \subseteq M$ normal ist) und nach Konstruktion eine normale Hülle.

Zur Eindeutigkeit: Da L' aus (i) enthalten ist in allen normalen Körpererweiterungen in M, die L enthalten, ist L' eindeutig.

(ii) Es ist $Z(\mathfrak{F}) \subseteq L'$, denn die Körpererweiterung $K \subseteq L'$ ist normal. Außerdem ist $L' \subseteq Z(\mathfrak{F})$, da die Körpererweiterung $K \subseteq Z(\mathfrak{K})$ normal ist und L enthalten ist in $Z(\mathfrak{F})$.

(iii) „$\supseteq$“ folgt, da die Körpererweiterung $K \subseteq L'$ normal ist und L enthalten ist in L'. Die Inklusion „$\subseteq$“ folgt, da $E \subseteq K$ normal ist – für alle $h \in \mathrm{Hom}(E, \bar{E})$ gilt nämlich, dass für alle $\alpha \in L$ und $\sigma \in \mathrm{Hom}_K(L, M)$ schon $h(\sigma(\alpha)) \in E$. $\square$

Beweis (von Proposition IV.3.9): Die Existenz und Teil (ii) folgen aus Proposition IV.3.10. Die Eindeutigkeit folgt aus Proposition IV.3.10(ii) und der Eindeutigkeit des Zerfällungskörpers (Proposition IV.1.14). Wir fassen dazu $\mathfrak{F}$ aus Proposition IV.3.10(ii) als Teilmenge von $L[X]$ auf. □

4. Separable Körpererweiterungen

Sei α algebraisch über K. Wie viele Homomorphismen von $K(\alpha)$ in den algebraischen Abschluss $\bar{K}$ gibt es? Wegen des Fortsetzungsatzes (Satz IV.1.11) stehen die Homomorphismen von $K(\alpha)$ in den algebraischen Abschluss $\bar{K}$ in Eins-zu-eins-Korrespondenz zu den Nullstellen des Minimalpolynoms f_α. Hat f_α keine mehrfachen Nullstellen, dann ist

$$\#\operatorname{Hom}_K(K(\alpha), \bar{K}) = d = \deg(f_\alpha) = [K(\alpha) : K].$$

Im Folgenden wollen wir uns Gedanken darüber machen, was bei doppelten Nullstellen passiert.

In diesem Abschnitt seien stets K ein Körper, $K \subseteq L$ eine algebraische Körpererweiterung und $\bar{K}$ ein algebraischer Abschluss von K.

Definition IV.4.1 (Separabel):

(i) Ein Polynom $f \in K[X]$ heißt *separabel*, falls f in $\overline{K}$ keine mehrfachen Nullstellen hat, d. h. f zerfällt über $\overline{K}$ in verschiedene Linearfaktoren.

(ii) Ein Element $\alpha \in L$ heißt *separabel*, falls das Minimalpolynom f_α separabel ist.

(iii) Die Körpererweiterung $K \subseteq L$ heißt *separabel*, falls jedes $\alpha \in L$ separabel ist.

Bemerkung IV.4.2: Definition IV.4.1 hängt nach der Eindeutigkeit des algebraischen Abschlusses nicht vom gewählten Abschluss $\bar{K}$ ab.

Bemerkung IV.4.3 (Ableitung): Für ein Polynom $f = \sum_{i=0}^n a_i X^i$ aus $K[X]$ heißt $f' := \sum_{i=1}^n i a_i X^{i-1}$ die Ableitung von f. Die Ableitung $f \mapsto f'$ ist eine Derivation, d. h. $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.

Lemma IV.4.4 (Separabel vs Ableitung): *Sei $f \in K[X]$ ein Polynom mit Grad größergleich eins.*

(i) *Ein Element $\alpha \in \bar{K}$ ist eine mehrfache Nullstelle genau dann, wenn $f(\alpha) = 0 = f'(\alpha)$. Dies gilt genau dann, wenn α eine Nullstelle von $\operatorname{ggT}(f, f')$.*

(ii) *Ist f irreduzibel, dann gilt die folgende Äquivalenz: f ist genau dann nicht separabel, wenn $f' = 0$.*

Beweis: (i) Diese Aussage ist in Teilen bereits auf Blatt 9 bewiesen worden, der verbleibende Teil wird auf Blatt 11 zu beweisen sein.

(ii) Ohne Einschränkung sei f normiert und α eine Nullstelle von f in $\bar{K}$. Dann ist f das Minimalpolynom von α. Ist f nicht separabel, dann ist α wegen (i) eine Nullstelle von f und f', d. h. es muss gelten $f' = 0$.

Ist andererseits $f' = 0$, dann ist f nach (i) nicht separabel. □

Beispiel IV.4.5 (Nicht-separables Element): Sei $K = \mathbb{F}_p(t) = \mathrm{Quot}(\mathbb{F}_p[t])$. Dann ist $f = X^p - t$ irreduzibel nach dem Eisenstein-Kriterium. Weiter ist $f' = pX^{p-1} = 0$. Nach dem vorhergehenden Lemma ist f nicht separabel, d. h. $t^{1/p}$ ist ein nicht-separables Element von $\bar{K}$.

Proposition IV.4.6 (Kriterium für Separabilität): *Sei $f \in K[X]$ ein irreduzibles Polynom vom Grad mindestens eins.*

(i) *Ist $\mathrm{char}(K) = 0$, dann ist f separabel.*

(ii) *Ist $\mathrm{char}(K) = p > 0$, wähle r maximal sodass f Polynom in X^{p^r} ist, d. h. $f = g(X^{p^r})$ mit $g \in K[X]$. Dann hat jede Nullstelle von f die Vielfachheit p^r.*

Beweis: (i) Das ist eine Konsequenz von Lemma IV.4.4.

(ii) Für $f = \sum_{i=0}^{n} a_i X^i$ gilt $f' = 0$ genau dann, wenn für $0 \leq i \leq n$ gilt: $ia_i = 0$. Das ist genau dann der Fall, wenn für $0 \leq i \leq n$ der Koeffizient a_i Null ist, oder i von p geteilt werden, was genau dann der Fall ist, wenn es $h \in K[X]$ mit $f = h(X^p)$ gibt.

Wir bemerken: Ist f irreduzibel, dann ist auch g irreduzibel. Außerdem gilt nach Definition von g und unserer Vorüberlegung, dass g separabel ist, wenn $g' \neq 0$ gilt, da es mindestens einen nicht durch p teilbaren Exponenten von g gibt, dessen Koeffizient ungleich Null ist.

Wir können schreiben $g = \prod_{i=1}^{k}(X - \beta_i) \in \bar{K}[X]$, wobei $\beta_1, \ldots, \beta_k$ paarweise verschieden sind. Wähle eine Nullstelle $\alpha_i \in X^{p^r} - \beta_i$. Dann ist

$$X^{p^r} - \beta_i = X^{p^r} - \alpha_i^{p^r} = (X - \alpha_i)^{p^r},$$

d. h. $X^{p^r} = \beta_i$ hat genau die Lösung α_i in $\bar{K}[X]$. Wir erhalten deshalb die Darstellung $f = \prod_{i=1}^{k}(X^{p^r} - \alpha_i^{p^r}) = \prod_{i=1}^{k}(X - \alpha_i)^{p^r}$ und lesen ab, dass alle Nullstellen die Vielfachheit p^r haben. □

Den Zusammenhang zwischen Separabilität und der Anzahl der Einbettungen einer einfachen Körpererweiterung in den algebraischen Abschluss des Grundkörpers ist der Folgende:

Korollar IV.4.7: *Es seien $K \subseteq K(\alpha)$ eine einfache Körpererweiterung und f das Minimalpolynom von α über K. Dann gilt:*

(i) *Es ist α separabel genau dann, wenn f separabel ist und das ist genau dann der Fall, wenn*

$$[K(\alpha) : K] = \# \operatorname{Hom}_K(K(\alpha), \bar{K}).$$

(ii) *Ist* $\operatorname{char}(K) = p > 0$*, sei p^r die Vielfachheit der Nullstelle α von f. Dann ist*

$$[K(\alpha) : K] = p^r \# \operatorname{Hom}_K(K(\alpha), \bar{K}).$$

Beweis: (i) Diese Aussage folgt aus Satz IV.1.11.

(ii) Ist eine Konsequenz von Proposition IV.4.6 und Satz IV.1.11. □

Proposition IV.4.8 (Multiplikativität von Hom): *Seien $K \subseteq L \subseteq M \subseteq \bar{K}$ algebraische Körpererweiterungen.*

(i) *Es gibt eine Bijektion*

$$\operatorname{Hom}_K(M, \bar{K}) \longleftrightarrow \operatorname{Hom}_K(L, \bar{K}) \times \operatorname{Hom}_L(M, \bar{K}).$$

(ii) *Ist $K \subseteq M$ eine endliche Körpererweiterungen, dann gilt insbesondere:*

$$\# \operatorname{Hom}_K(M, \bar{K}) = \# \operatorname{Hom}_K(L, \bar{K}) \cdot \# \operatorname{Hom}_L(M, \bar{K}).$$

Beweis: Wir wollen für jedes $\sigma \in \operatorname{Hom}_K(L, \bar{K})$ eine Fortsetzung $\hat{\sigma} \in \operatorname{Hom}_K(\bar{K}, \bar{K})$ wählen – das dürfen wir nach Satz IV.2.9.

Definiere

$$\begin{aligned} \phi\colon \operatorname{Hom}_K(M, \bar{K}) &\longrightarrow \operatorname{Hom}_K(L, \bar{K}) \times \operatorname{Hom}_L(M, \bar{K}), \\ h &\longmapsto (\sigma := h|_L, \tau := (\hat{\sigma}^{-1} \circ h)), \end{aligned}$$

wir sind also in der Situation

$$\begin{array}{ccccc} M & \xhookrightarrow{h} & \bar{K} & \xhookleftarrow{\hat{\sigma}} & \bar{K} \\ \uparrow & & \uparrow & & \uparrow \\ L & \xhookrightarrow[\sigma]{} & h(L) & \xhookleftarrow[\sigma]{} & L \end{array}$$

Es gilt $\hat{\sigma}^{-1} \circ h|_L = \mathrm{id}$, denn für alle $\ell \in L$ gilt

$$\hat{\sigma}^{-1} \circ h(l) = \hat{\sigma}^{-1} \circ \sigma(\ell) = \hat{\sigma}^{-1}\hat{\sigma}(\ell) = \ell.$$

Definiere

$$\psi\colon \mathrm{Hom}_K(L, \bar{K}) \times \mathrm{Hom}_L(M, \bar{K}) \longrightarrow \mathrm{Hom}_K(M, \bar{K}),$$
$$(\sigma, \tau) \longmapsto \hat{\sigma} \circ \tau =: h.$$

Per Definition sind ϕ und ψ invers zueinander und (ii) ist eine direkte Konsequenz von (i). □

Proposition IV.4.9 (Grad vs $\#\,\mathrm{Hom}_K(L, \bar{K})$): *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann gilt:*

(i) *Ist* $\mathrm{char}(K) = 0$, *dann ist* $[L : K] = \#\,\mathrm{Hom}_K(L, \bar{K})$,

(ii) *Ist* $\mathrm{char}(K) = p > 0$, *dann gibt es* $r \in \mathbb{N}_0$ *mit* $[L : K] = p^r\,\mathrm{Hom}_K(L, \bar{K})$.

Beweis: Man zeigt die Proposition per Induktion unter Verwendung von Korollar IV.4.7, Proposition IV.4.8 und Proposition IV.1.2. □

Satz IV.4.10 (über Separabilität): *Für eine endliche Körpererweiterung $K \subseteq L$ ist äquivalent:*

(i) *Die Körpererweiterung $K \subseteq L$ ist separabel.*

(ii) *Es ist $L = K(\alpha_1, \ldots, \alpha_n)$ mit über K separablen $\alpha_1, \ldots, \alpha_n \in L$.*

(iii) *Es gilt $[L : K] = \#\,\mathrm{Hom}_K(L, \bar{K})$.*

Beweis: „(i) ⇒ (ii)“ ist klar, die Implikation „(ii) ⇒ (iii)“ zeigt man wie bei Proposition IV.4.9. Zu „(iii) ⇒ (i)“: Betrachte die Körpererweiterung $K \subseteq K(\alpha)$. Dann gilt wegen Proposition IV.4.8, dass

$$\begin{aligned}[L : K(\alpha)] \cdot [K(\alpha) : K] &= [L : K] \\ &= \#\,\mathrm{Hom}_K(L, \bar{K}) \\ &= \#\,\mathrm{Hom}_{K(\alpha)}(L, \bar{K}) \cdot \#\,\mathrm{Hom}_K(K(\alpha), \bar{K}). \qquad \text{(IV.1)}\end{aligned}$$

Aus Proposition IV.4.9 folgt, dass $\#\,\mathrm{Hom}_{K(\alpha)}(L, \bar{K})$ Teiler von $[L : K(\alpha)]$ und $\#\,\mathrm{Hom}_K(K(\alpha), K)$ ein Teiler von $[K(\alpha) : K]$ ist. Somit folgt jeweils Gleichheit für die Faktoren, also gilt insbesondere $[K(\alpha) : K] = \#\,\mathrm{Hom}_K(K(\alpha), \overline{K})$, weshalb α nach Korollar IV.4.7 separabel sein muss. □

Definition IV.4.11 (Separabilitätsgrad): Für eine algebraische Körpererweiterung $K \subseteq L$ heißt $[L : K]_S := \#\operatorname{Hom}_K(L, \bar{K})$ der *Separabilitätsgrad von L über K*.

Bemerkung IV.4.12: (i) Sind $K \subseteq L \subseteq M$ algebraische Körpererweiterungen, dann gilt nach Proposition IV.4.8

$$[M : L]_S[L : K]_S = [M : K]_S.$$

(ii) Der Separabilitätsgrad $[L : K]_S$ ist ein Teiler von $[L : K]$, genauer gilt $[L : K]_S = [L : K]$ genau dann, wenn $K \subseteq L$ separabel ist; sonst ist $\operatorname{char}(K) = p > 0$ und $[L : K] = p^r[L : K]_S$ mit $r \geq 1$ nach Satz IV.4.10 und Proposition IV.4.9.

Satz IV.4.13 (vom primitiven Element): *Sei $K \subseteq L$ eine endliche separable Körpererweiterung. Dann gibt es $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis: Wir unterscheiden zwei Fälle. Ist K ein endlicher Körper, dann ist insbesondere L endlich. Die multiplikative Gruppe $L^\times$ ist in diesem Fall zyklisch, d. h. es gibt $\alpha \in L$ mit $\langle\alpha\rangle = L$ und damit ist $L = K(\alpha)$.

Ist K ein unendlicher Körper, schreibe $L = K(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_i \in L$, $1 \leq i \leq n$. Nun zeigen wir die Behauptung durch vollständige Induktion über die Anzahl der Erzeuger. Für $n = 0$ und $n = 1$ ist alles klar. Gilt die Aussage nun für ein festes n, dann ist $K \subseteq L' := K(\alpha_1, \ldots, \alpha_{n-1}) \subseteq L = L'(\alpha_n)$. Nach Aufgabe 3 von Übungsblatt 11 sind die Erweiterungen $K \subseteq L'$ und $L' \subseteq L$ separabel und nach Induktionsvoraussetzung gibt es $\alpha \in L'$ mit $L' = K(\alpha)$. Schreibe $\beta := \alpha_n$. Es reicht zu zeigen, dass es $\gamma \in L$ mit $K(\alpha, \beta) = K(\gamma)$ gibt.

Sei $d := [L : K]$. Wir versuchen jetzt $\gamma \in L$ zu finden, dessen Minimalpolynom f_γ mindestens Grad d hat. Dieses γ würde unsere Wünsche erfüllen. Beachte nun:

(i) $\deg(f_\gamma) = \#\{\text{Nullstellen von } f_\gamma\}$, da γ separabel ist;

(ii) $\{\text{Nullstellen von } f_\gamma\} \leftrightarrow \operatorname{Hom}_K(K(\gamma), K)$ nach Satz IV.1.11;

(iii) $\operatorname{Hom}(L, \bar{K}) \to \operatorname{Hom}(K(\gamma), \overline{K})$, $\sigma \mapsto \sigma|_{K(\gamma)}$ ist surjektiv nach Satz IV.2.9 und deshalb haben wir die Eins-zu-eins-Entsprechung

$$\operatorname{Hom}(K(\gamma), \bar{K}) \longleftrightarrow \{\sigma(\gamma) \mid \sigma \in \operatorname{Hom}(L, \bar{K})\};$$

(iv) $\#\operatorname{Hom}(L, \bar{K}) = [L : K]$.

Aus den obigen Punkten folgt, dass $\deg(f_\gamma) = d$ genau dann gilt, wenn die Bilder $\sigma(\gamma)$ von γ für unterschiedliche σ verschieden sind.

Schreibe $\mathrm{Hom}(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_d\}$. Wir müssen also jetzt $\gamma \in L$ finden, sodass $\sigma_i(\gamma) \neq \sigma_j(\gamma)$ für $i \neq j$ gilt. Wir setzen γ an als $\gamma = \alpha + c\beta$ mit $c \in K$ und hoffen, dass für $i \neq j$ schon gilt $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$. Jetzt ist aber

$$\begin{aligned}
&\forall\, i \neq j : \sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta) \\
&\quad\iff \forall\, i \neq j : \sigma_i(\alpha) - \sigma_j(\alpha) + c(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0 \\
&\quad\iff \prod_{i \neq j} \sigma_i(\alpha) - \sigma_j(\alpha) + c(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0.
\end{aligned}$$

Definiere das Polynom $P = \prod_{i \neq j}(\sigma_i(\alpha) - \sigma_j(\alpha)) + X(\sigma_i(\beta) - \sigma_j(\beta))$. Dieses P ist nicht das Nullpolynom, da für $\sigma_i \neq \sigma_j$ stets gilt, dass $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ oder $\sigma_i(\beta) \neq \sigma_j(\beta)$. Insbesondere hat P nur endlich viele Nullstellen; da K unendlich ist, gibt es $c \in K$ mit $P(c) \neq 0$ und $\gamma = \alpha + c\beta$ leistet das Gewünschte. □

Definition IV.4.14 (Perfekter Körper): Ein Körper K heißt *perfekt* (gelegentlich auch *vollkommen*), falls jede algebraische Körpererweiterung von K separabel ist.

Bemerkung IV.4.15: (i) Ist K ein Körper mit $\mathrm{char}(K) = 0$, so ist K perfekt.

(ii) Ist K ein endlicher Körper, so ist K perfekt (diese Aussage ist als Übungsaufgabe auf Blatt 11 zu zeigen).

(iii) Ist K ein perfekter Körper, dann ist jede endliche Körpererweiterung von K primitiv.

Definition IV.4.16 (Total inseparabel): Eine Körpererweiterung $K \subseteq L$ heißt *total inseparabel*, falls $[L : K]_S = 1$.

Kapitel V.

Galois-Theorie

1. Hauptsatz der Galoistheorie

In diesem Abschnitt seien $K \subseteq L$ eine algebraische Körpererweiterung und $\bar{K}$ ein algebraischer Abschluss von K.

Bemerkung V.1.1: (i) Sei $K \subseteq L$ eine normale Körpererweiterung. Wähle eine Einbettung $L \subseteq \bar{K}$. Dann haben wir die kurze exakte Sequenz

$$\{1\} \longrightarrow \mathrm{Aut}_L(\bar{K}) \longrightarrow \mathrm{Aut}_K(\bar{K}) \longrightarrow \mathrm{Aut}_K(L) \longrightarrow \{1\}$$

(ii) Die Körpererweiterung $K \subseteq L$ ist normal und separabel genau dann, wenn $\#(\mathrm{Aut}_K(L)) = [L : K]$.

Beweis: (i) Folgt aus Satz IV.3.6 und dem zweiten Fortsetzungssatz.

(ii) Wir haben $\#\,\mathrm{Aut}_K(L) \leq \#\,\mathrm{Hom}_K(L, \bar{K}) = [L : K]_S \leq [L : K]$, wobei das erste Ungleichheitszeichen nach dem Satz über den algebraischen Abschluss (Satz IV.2.7)— und das zweite Ungleichheitszeichen nach Bemerkung IV.4.12 gilt. Dabei sit das erste Ungleichheitszeichen eine Gleichheit genau dann, wenn $L|K$ normal ist und das zweite ist eine Gleichheit genau dann, wenn $K \subseteq L$ separabel ist. □

Definition V.1.2: Eine Körpererweiterung $K \subseteq L$ heißt *galoissch*, falls sie normal und separabel ist. In diesem Fall heißt $\mathrm{Gal}(L|K) := \mathrm{Aut}_K(L)$ auch *Galois-Gruppe* von $K \subseteq L$.

Proposition V.1.3 (Fixkörper): *Seien L ein Körper und $G \subseteq \mathrm{Aut}(L)$ eine Untergruppe. Für den* Fixkörper

$$L^G := \{\alpha \in L \mid \forall\, \sigma \in G : \sigma(\alpha) = \alpha\}$$

gilt:

(i) *L^G ist ein Körper.*

(ii) *Ist G eine endliche Gruppe, dann ist $L^G \subseteq L$ eine galoissche Körpererweiterung und es gilt* $\mathrm{Gal}(L|L^G) = G$.

(iii) *Ist $L^G \subseteq L$ eine algebraische Körpererweiterung, dann ist $L^G \subseteq L$ galoissch und $G \subseteq \mathrm{Gal}(L|L^G)$.*

(iv) *Es gilt $G_1 \subseteq G_2$ genau dann, wenn $L^{G_1} \supseteq L^{G_2}$.*

Beweis: (i) Klar, denn die Elemente aus G sind Körperhomomorphismen.

(ii) Die Körpererweiterung $L^G \subseteq L$ ist algebraisch; sind nämlich $\alpha \in G$ und G endlich, dann ist die Bahn $G\alpha = \{\alpha = \alpha_1, \ldots, \alpha_r\}$ endlich und wir erhalten das Polynom $f = \prod_{i=1}^{r}(X - \alpha_i) \in L^G[X]$ – der Beweis dieser Tatsache funktioniert wie in (iii). Da $f(\alpha) = 0$ ist, folgt dass α algebraisch über L^G ist. Nach (iii) ist die Körpererweiterung $L^G \subseteq L$ galoissch und $G \subseteq \mathrm{Gal}(L|L^G)$. Für $G = \mathrm{Gal}(L|L^G)$ bleibt zu zeigen, dass $[L : L^G] \leq \#(G)$. Da $L^G \subseteq L$ separabel ist, ist jeder endliche Zwischenkörper $L^G \subseteq E \subseteq L$ primitiv nach Satz IV.4.13. Ist außerdem $E = L^G(\alpha)$ mit $\alpha \in L$, dann ist $[E : L^G] = [L^G(\alpha) : L^G] = \deg(f_\alpha) \leq \#(G)$, d. h. $[L : L^G] \leq \#(G)$.

(iii) Wir haben, dass $G \subseteq \mathrm{Aut}_{L^G}(L)$, denn für alle $\sigma \in G$ und alle $\alpha \in L^G$ ist $\sigma(\alpha) = \alpha$. Die Körpererweiterung $L^G \subseteq L$ ist separabel; seien nämlich $\alpha \in L$ und $f_\alpha \in L^G[X]$ das Minimalpolynom von α über L^G. Nach dem ersten Fortsetzungssatz (Satz IV.1.11) permutiert G die Nullstellen von f_α. Die Bahn von α unter der Wirkung von G ist $G\alpha = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r\} \subseteq L$.

Setze $f = \prod_{i=1}^{n}(X - \alpha_i) \in L[X]$. Für alle $\sigma \in G$ ist ${}^\sigma f = \prod_{i=1}^{r}(X - \sigma(\alpha_i)) = f$, da f_α ein Teiler des obigen Polynoms f ist, d. h. in Wahrheit ist $f \in L^G[X]$. Außerdem ist f separabel, da die α_i paarweise verschieden sind und damit ist α separabel.

Die Körpererweiterung $L^G \subseteq L$ ist außerdem normal. Seien nämlich $\alpha \in L$ und $\tilde{\alpha}$ eine weitere Nullstelle des Minimalpolynoms $f_\alpha \in L^G[X]$. Da f_α ein Teiler von f ist, gilt $\tilde{\alpha} \in G\alpha$. Es gibt also ein $\sigma \in G$ mit $\sigma(\alpha) = \tilde{\alpha}$, d. h. $\tilde{\alpha} \in L$.

Insgesamt ist also $L^G \subseteq G$ galoissch und $G \subseteq \mathrm{Gal}(L|L^G)$.

(iv) Das ist klar. □

Proposition V.1.4 (Fixkörper der Galois-Gruppe): *Sei $K \subseteq L$ eine galoissche Körpererweiterung. Dann ist $L^{\mathrm{Gal}(L|K)} = K$.*

Beweis: Wähle eine Einbettung von L in $\bar{K}$ und erhalte den Körperturm $K \subseteq L \subseteq \bar{K}$. Weiter sei $G := \mathrm{Gal}(L|K)$. Offenbar gilt $K \subseteq L^G \subseteq L$. Insbesondere sind die Körpererweiterungen $L^G \subseteq L$ und $K \subseteq L^G$ algebraisch.

(i) Es gilt $[L^G : K]_S = 1$, ist nämlich $\sigma \in \mathrm{Hom}_K(L^G, \bar{K})$, dann hat σ nach dem zweiten Fortsetzungssatz (Satz IV.2.9) und (Satz IV.3.6) eine Fortsetzung $\hat{\sigma} \in \mathrm{Gal}(L|K)$ und für alle $\alpha \in L^G$ ist $\sigma(\alpha) = \hat{\sigma}(\alpha) = \alpha$.

(ii) Da die Körpererweiterung $K \subseteq L$ separabel ist, ist auch $K \subseteq L^G$ separabel, d. h. $L^G = K$ nach (i). □

Satz V.1.5 (Hauptsatz der Galoistheorie): *Sei $K \subseteq L$ eine endliche galoissche Körpererweiterung mit $G := \mathrm{Gal}(L|K)$.*

(i) *Die beiden folgenden Abbildungen ϕ und ψ sind invers zueinander:*

$$\{H \subseteq G \text{ Untergruppe}\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{E \subseteq L \text{ Zwischenkörper von } K \subseteq L\}$$

mit

$$H \overset{\phi}{\longmapsto} L^H, \qquad \mathrm{Gal}(L|E) \overset{\psi}{\longmapsto} E.$$

(ii) *Die Untergruppe $\mathrm{Gal}(L|E)$ ist normal in G genau dann, wenn $K \subseteq E$ normal ist. In diesem Fall ist $\mathrm{Gal}(E|K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$.*

Beweis: (i) Zur Wohldefiniertheit: Ist $H \subseteq \mathrm{Gal}(L|K)$ eine Untergruppe, dann ist $K \subseteq L^H$ und damit ist L^H ein Zwischenkörper der Erweiterung $K \subseteq L$. Ist $K \subseteq L$ galoissch, dann ist auch $E \subseteq L$ galoissch und damit ist $\mathrm{Gal}(L|E)$ definiert.

Für einen Zwischenkörper E der Körpererweiterung $K \subseteq L$ gilt

$$\phi(\psi(E)) = \phi(\mathrm{Gal}(L|E)) = L^{\mathrm{Gal}(L|E)} = E$$

wegen Proposition V.1.4.

Ist H eine Untergruppe von $\mathrm{Gal}(L|K)$, dann ist

$$\psi(\phi(H)) = \psi(L^H) = \mathrm{Gal}(L|L^H) = H$$

nach Proposition V.1.3.

(ii) „⇐“: Ist $K \subseteq E$ eine normale Körpererweiterung, dann erhalten wir wie in Bemerkung V.1.1 die kurze exakte Sequenz

$$\{1\} \longrightarrow \mathrm{Gal}(L|E) \longrightarrow \mathrm{Gal}(L|K) \longrightarrow \mathrm{Gal}(E|K) \longrightarrow \{1\},$$

d. h. $\mathrm{Gal}(L|E)$ ist ein Normalteiler in $\mathrm{Gal}(L|K)$ und es gilt die behauptete Isomorphie von Gruppen.

„⇒“: Sei $H := \mathrm{Gal}(L|E)$. Wegen (i) ist $E = L^H$. Nach Satz IV.3.6 ist zu zeigen, dass für alle $\sigma \in \mathrm{Hom}(E, \bar{K})$ schon $\sigma(E) \subseteq E$ gilt. Da $K \subseteq L$ normal ist, erhalten wir wegen Satz IV.2.9 und Satz IV.3.6 eine Fortsetzung $\hat{\sigma} \in \mathrm{Gal}(L|K)$. Sei nun $\alpha \in E$. Wir wollen zeigen, dass $\sigma(\alpha) \in E = L^H$. Für alle $\tau \in H = \mathrm{Gal}(L|E)$ ist $\hat{\sigma}^{-1}\tau\hat{\sigma} =: \tau' \in H$, da H normal in G ist. Damit ist

$$\tau\sigma(\alpha) = \tau\hat{\sigma}(\alpha) = \hat{\sigma}\tau'(\alpha) = \hat{\sigma}(\alpha) = \sigma(\alpha).$$

Somit ist $\sigma(\alpha) \in E = L^H$. □

Im Beweis des Hauptsatzes der Galoistheorie wurde nur für $\psi \circ \phi = \mathrm{id}$ verwendet, dass die Körpererweiterung $K \subseteq L$ endlich ist.

Bemerkung V.1.6: Sei $K \subseteq L$ eine unendliche galoissche Körpererweiterung, $G := \mathrm{Gal}(L|K)$ und ϕ, ψ wie in Satz V.1.5. Dann ist weiterhin $\phi \circ \psi = \mathrm{id}$ und somit ist ψ injektiv und ϕ surjektiv und man erhält eine Bijektion

$$\{H \subseteq G \text{ Untergruppe mit } \mathrm{Gal}(L|L^H) = H\} \longleftrightarrow \{E \text{ Zwischenkörper von } K \subseteq L\}.$$

Definition V.1.7 (Kompositum): Seien E_1, E_2 Teilkörper von L. Dann heißt

$$E_1 \cdot E_2 := \bigcap \{E \mid E \subseteq L \text{ Teilkörper mit } E_1, E_2 \subseteq E\}$$

das *Kompositum von E_1 und E_2*.

Bemerkung V.1.8 (Eigenschaften des Kompositium):

(i) $E_1 \cdot E_2$ ist der kleinste Teilkörper von L, der E_1 und E_2 enthält.

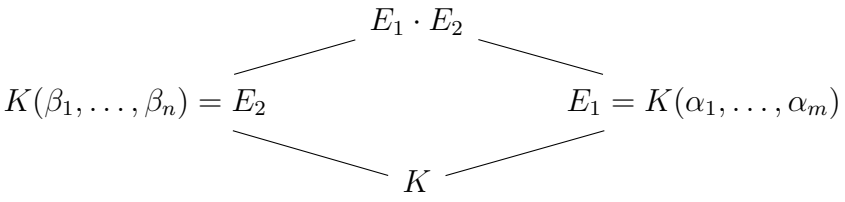
(ii) $E_1 \cdot E_2 = E_1(E_2) = E_2(E_1)$, d. h. wir erhalten das Kompositum durch Adjunktion von E_2 an E_1 oder umgekehrt.

(iii) Es gilt also $E_1E_2 = E_2E_1$.

(iv) Sind E_1 und E_2 endliche Körpererweiterungen von K, dann ist

$$[E_1 \cdot E_2 : E_2] \leq [E_1 : K] \quad \text{und} \quad [E_1 \cdot E_2 : K] \leq [E_1 : K][E_2 : K].$$

Beweis: Die Punkte (i), (ii) und (iii) sind klar. Zu (iv): Wir sind in der Situation



und sehen damit, dass $E_1E_2 = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$. □

Proposition V.1.9 (Galois-Gruppe unter Körperaktionen): *Seien $K \subseteq L$ eine endliche galoissche Körpererweiterung, $E_1, E_2 \subseteq L$ Zwischenkörper von $K \subseteq L$ und $G_1 := \mathrm{Gal}(L|E_1)$, $G_2 := \mathrm{Gal}(L|E_2)$. Dann gelten:*

(i) *Es ist $E_1 \subseteq E_2$ genau dann, wenn $G_1 \supseteq G_2$,*

(ii) *$E_1 \cdot E_2 = L^{G_1 \cap G_2}$ beziehungsweise $\mathrm{Gal}(L|E_1 \cdot E_2) = G_1 \cap G_2$.*

(iii) *$E_1 \cap E_2 = L^{\langle G_1 \cup G_2 \rangle}$ – wobei $\langle G_1 \cup G_2 \rangle$ das Erzeugnis als Untergruppe von G ist – beziehungsweise $\mathrm{Gal}(L|E_1 \cap E_2) = \langle G_1 \cup G_2 \rangle$.*

Der Beweis dieser Proposition findet sich als Übungsaufgabe auf Blatt 12.

Proposition V.1.10 (Galois-Gruppe für Kompositum): *Seien E und E' Zwischenkörper der Körpererweiterung $K \subseteq L$ sodass $E|K$ und $E'|K$ endliche Galois-Erweiterungen sind. Dann gilt:*

(i) *Die Körpererweiterung $K \subseteq E \cdot E'$ ist endlich und galoissch und für ihre Galois-Gruppe gilt $\mathrm{Gal}(E \cdot E'|E) \cong \mathrm{Gal}(E'|E \cap E')$.*

(ii) *Der Homomorphismus*

$$\psi\colon \mathrm{Gal}(E \cdot E'|K) \longrightarrow \mathrm{Gal}(E|K) \times \mathrm{Gal}(E'|K), \qquad \sigma \longmapsto (\sigma|_E, \sigma|_{E'})$$

ist injektiv. Gilt sogar $E \cap E' = K$, dann ist ψ bijektiv.

Beweis: (i) Dass die Erweiterung endlich und galoissch ist, folgt aus Bemerkung V.1.8, Aufgabe 3 von Übungsblatt 10 und Aufgabe 10 auf Übungsblatt 11. Betrachte die Abbildung

$$\varphi\colon \mathrm{Gal}(E' \cdot E|E) \longrightarrow \mathrm{Gal}(E'|E \cap E'), \qquad \sigma \longmapsto \sigma|_{E'}.$$

Diese ist injektiv; sei nämlich $\sigma \in \mathrm{Gal}(E' \cdot E|E)$ mit $\sigma \in \ker(\varphi)$. Dann ist $\sigma|_{E'} = \mathrm{id}_{E'}$ und $\sigma|_E = \mathrm{id}_E$, d. h. $\sigma = \mathrm{id}_{E' \cdot E}$. Außerdem ist φ surjektiv, denn

$$(E')^{\mathrm{im}(\varphi)} = (E \cdot E')^{\mathrm{Gal}(E \cdot E'|E)} \cap E' = E \cap E'$$

nach dem Hauptsatz der Galois-Theorie (Satz V.1.5). Wieder nach dem Hauptsatz der Galois-Theorie ist damit $\mathrm{im}(\varphi) = \mathrm{Gal}(E'|E \cap E')$.

(ii) Die Injektivität von ψ ist klar (gleiche Argumente wie in (i)). Angenommen $K = E \cap E'$ und sei $(\sigma, \sigma') \in \mathrm{Gal}(E|K) \times \mathrm{Gal}(E'|K)$. Wegen (i) und $E \cap E' = K$ erhalten wir Fortsetzungen $\hat{\sigma} \in \mathrm{Gal}(E \cdot E'|E')$ von $\sigma \in \mathrm{Gal}(E|K)$ und $\hat{\sigma}' \in \mathrm{Gal}(E \cdot E'|E)$ von $\sigma' \in \mathrm{Gal}(E'|K)$. Das heißt die Komposition $\hat{\sigma} \circ \hat{\sigma}' \in \mathrm{Gal}(E \cdot E'|K)$ erfüllt, dass

$$(\hat{\sigma} \circ \hat{\sigma}')|_E = \hat{\sigma} \circ (\hat{\sigma}'|_E) = \hat{\sigma}|_E = \sigma,$$
$$(\hat{\sigma} \circ \hat{\sigma}')|_{E'} = \hat{\sigma}|_{E'} \circ (\hat{\sigma}'|_{E'}) = \mathrm{id}\,|_{E'} \circ \hat{\sigma}'|_{E'} = \sigma'. \qquad \square$$

2. Einheitswurzeln

Das Ziel dieses Abschnitts soll die Bestimmung der Galois-Gruppe $\mathrm{Gal}(K(\xi_n)|K)$ für eine primitive n-te Einheitswurzel ζ_n sein. Über $\mathbb{Q}$ kennen wir schon den Grad dieser Körpererweiterung, dieser ist nämlich $\varphi(n)$.

In diesem Abschnitt seien K ein Körper und $\bar{K}$ ein algebraischer Abschluss von K.

Definition V.2.1 (Einheitswurzeln):

(i) Ein Element $\zeta \in \bar{K}$ heißt *n-te Einheitswurzel*, falls $\zeta^n = 1$.

(ii) Die Menge $\mu_n := U_n := \{\zeta \in \bar{K} \mid \zeta^n = 1\} \subseteq \bar{K}^\times$ heißt *Gruppe der n-ten Einheitswurzeln* und ist es auch.

Bemerkung V.2.2: (i) Die Gruppe U_n ist zyklisch.

(ii) Ist n kein Vielfaches von $\mathrm{char}(K)$, dann ist $\#(U_n) = n$, d. h. $U_n \cong \mathbb{Z}/n\mathbb{Z}$.

(iii) Ist $\mathrm{char}(K) = p > 0$, schreibe $n = p^r \cdot n'$ mit $\mathrm{ggT}(p, n') = 1$. Dann ist $U_n = U_{n'}$.

Beweis: (i) Nach Satz III.4.10 sind endliche Untergruppen von $\bar{K}^\times$ zyklisch.

(ii) Das Polynom $f = X^n - 1$ hat die Ableitung $f' = nX^{n-1}$, d. h. f und f' haben keine gemeinsamen Nullstellen. Nach Lemma IV.4.4 ist f damit separabel, d. h. f hat n Nullstellen.

(iii) Wegen $f = X^{p^r \cdot n'} - 1 = (X^{n'} - 1)^{p^r}$ folgt die Behauptung.

Insbesondere folgt aus Bemerkung V.2.2, dass wir $\mathrm{char}(K) \nmid n$ annehmen können. □

Definition V.2.3 (Primitive Einheitswurzeln):

(i) Ein $\zeta \in U_n$ heißt *primitive n-te Einheitswurzel*, falls $\langle\zeta\rangle = U_n$.

(ii) Ist $K = \mathbb{Q}$ und ζ eine primitive Einheitswurzel, dann heißt $\mathbb{Q}(\zeta)$ auch *Kreisteilungskörper*.

Proposition V.2.4 (Ordnungen von Einheitswurzeln): *Seien n und m natürliche Zahlen mit $\mathrm{ggT}(n, m) = 1$ und $\mathrm{char}(K) \nmid m, n$. Für $\zeta \in U_n$ und $\eta \in U : m$ betrachte $\zeta\eta \in U_{n,m}$. Dann gilt:*

(i) $\mathrm{ord}_{U_{nm}}(\zeta\eta) = \mathrm{ord}_{U_n}(\zeta)\,\mathrm{ord}_{U_m}(\eta)$.

(ii) *Sind ζ und η primitive Einheitswurzeln in U_n respektive U_m, dann ist $\zeta\eta$ eine primitive Einheitswurzel in U_{nm}.*

(iii) *Die Abbildung*

$$h\colon U_n \times U_m \longrightarrow U_{nm}, \qquad (\zeta, \eta) \longmapsto \zeta\eta$$

ist ein Gruppenisomorphismus.

Beweis: (i) Seien $k := \mathrm{ord}_{U_{nm}}(\zeta\eta)$, $r := \mathrm{ord}_{U_n}(\zeta)$ und $s := \mathrm{ord}_{U_m}(\eta)$. Offensichtlich ist $(\zeta\eta)^{rs} = 1$, d. h. k teilt rs. Da außerdem $\mathrm{ggT}(n, m) = 1$, gibt es $a, b \in \mathbb{Z}$ mit $1 = na + mb$. Deshalb ist

$$1 = \Big((\zeta\eta)^k\Big)^{(1-an)} = \zeta^{k(1-an)}\eta^{kmb} = \zeta^k,$$

d. h. r teilt k. Analog erhalten wir, dass auch $s \mid k$, d. h. rs teilt k, da $r \mid n$ und $s \mid m$.

(ii) Folgt aus (i).

(iii) Wir rechnen nach, dass

$$h\Big((\zeta_1, \eta_1) \cdot (\zeta_2, \eta_2)\Big) = h(\zeta_1\zeta_2, \eta_1\eta_2) = \zeta_1\zeta_2\eta_1\eta_2 = h(\zeta_1, \eta_1)h(\zeta_2, \eta_2),$$

d. h. h ist ein Gruppenhomomorphismus. Wegen (ii) ist h surjektiv und da $\#U_n \times U_m = \#U_{nm}$ ist h auch injektiv. □

Bemerkung V.2.5 (primitive Einheitswurzeln): Es gelte wieder $\mathrm{char}(K) \nmid n$.

(i) Ist $\zeta \in U_n$ eine primtive n-te Einheitswurzel, dann ist ζ^a genau dann primitiv, wenn $\mathrm{ggT}(a, n) = 1$.

(ii) Es gibt $\varphi(n)$-viele primitive n-te Einheitswurzeln, wpbei φ die Euler'sche φ-Funktion ist.

Beweis: (i) Verwende, dass $\mathbb{Z}/n\mathbb{Z} \cong U_n$ vermöge $a \mapsto \zeta^a$. Aus Lineare Algebra I wissen wir für $a \in \mathbb{Z}/n\mathbb{Z}$, dass $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ genau dann, wenn $\mathrm{ggT}(a, n) = 1$.

(ii) Folgt aus der Definition der Euler'schen φ-Funktion. □

Erinnerung V.2.6 (Euler'sche φ-Funktion): (i) Für eine natürliche Zahl n ist $\varphi(n)$ definiert durch

$$\varphi(n) := \#\{t \in \mathbb{N} \mid 1 \leq t \leq n \text{ und } \mathrm{ggT}(t, n) = 1\}.$$

(ii) Für eine Primzahl p und eine natürliche Zahl r gilt $\varphi(p^r) = p^r - p^{r-1}$.

(iii) Für teilerfremde natürliche Zahlen n und m gilt $\varphi(nm) = \varphi(n)\varphi(m)$, denn in diesem Fall ist $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ und damit

$$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \oplus (\mathbb{Z}/m\mathbb{Z})^\times.$$

Proposition V.2.7 (Automorphismengruppe von U_n): *Wir haben die Isomorphie*

$$\mathrm{Aut}(U_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Beweis: Wir wollen verwenden, dass $U_n \cong \mathbb{Z}/n\mathbb{Z}$. Definiere

$$\Phi\colon\ \mathrm{Aut}(U_n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \gamma \longmapsto \gamma(1).$$

Dieses Φ ist ein Gruppenhomomorphismus, denn es ist

$$\Phi(\gamma_1 \circ \gamma_2) = \gamma_1(\gamma_2(1)) = \gamma_1\Big(\sum_{i=1}^{\gamma_2(1)} 1\Big) = \sum_{i=1}^{\gamma_2(1)} \gamma_1(1) = \gamma_1(1)\gamma_2(1) = \Phi(\gamma_1)\Phi(\gamma_2).$$

Offensichtlich ist Φ injektiv. Außerdem ist Φ surjektiv, denn ist $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, dann ist $\gamma\colon x \mapsto ax$ ein Automorphismus mit $\Phi(\gamma) = a$. □

Bemerkung V.2.8 (Galois-Gruppe operiert auf U_n): Ist $\sigma \in \mathrm{Gal}(K(\zeta_n)|K)$, dann ist die Einschränkung $\sigma|_{U_n}\colon \eta \mapsto \sigma(\eta)$ ein Automorphismus von U_n.

Proposition V.2.9 (Die Körpererweiterung $K(\zeta_n)|K$): *Sei $\zeta_n \in U_n$ eine primitive n-te Einheitswurzel und es gelte* $\mathrm{char}(K) \nmid n$.

(i) *Der Körper $K(\zeta_n)$ ist der Zerfällungskörper $Z(X^n - 1)$ und $K \subseteq K(\zeta_n)$ is galoissch.*

(ii) *Für den Grad der Körpererweiterung $K \subseteq K(\zeta_n)$ haben wir die Abschätzung $[K(\zeta_n) : K] \leq \varphi(n)$.*

(iii) *Falls K der Körper der rationalen Zahlen ist, dann ist $[K : K(\zeta_n)] = \varphi(n)$.*

Beweis: (i) Es ist $K(\zeta_n) = Z(X^n - 1)$, denn $\langle\zeta_n\rangle = U$, damit ist die Körpererweiterung $K \subseteq K(\zeta_n)$ normal. Außerdem ist die Körpererweiterung separabel nach Bemerkung IV.3.2.

(ii) Nach Bemerkung V.2.8 erhalten wir einen Gruppenhomomorphismus

$$\iota\colon\ \mathrm{Gal}(K(\zeta_n)|K) \longrightarrow \mathrm{Aut}(U_n), \qquad \sigma \longmapsto \sigma|_{U_n}.$$

Offensichtlich ist ι injektiv. Wegen $\#\,\mathrm{Aut}(U_n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ beschließt das den Beweis.

(iii) Das haben Sie bereits in Aufgabe 4 auf dem achten Übungsblatt gezeigt. □

Satz V.2.10 (Die Galois-Gruppe von $K(\zeta_n)|K$): *Es sei* $\mathrm{char}(K)$ *kein Teiler von* n*.*

(i) *Die Körpererweiterung* $K \subseteq K(\zeta_n)$ *ist eine abelsche Galois-Erweiterung von Grad höchstens* $\varphi(n)$*. Genauer gilt:* $\mathrm{Gal}(K(\zeta_n)|K)$ *ist Untergruppe von* $(\mathbb{Z}/n\mathbb{Z})^\times$*.*

(ii) *Ist* $K = \mathbb{Q}$*, dann ist* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$*.*

Beweis: (i) Wir definieren den Gruppenhomomorphismus

$$\nu\colon \mathrm{Gal}(K(\zeta_n)|K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad \sigma \longmapsto \nu_\sigma,$$

wobei ν_σ definiert ist durch $\sigma(\zeta_n) = \zeta_n^{\nu_\sigma}$.

Dies ist die Verknüpfung der Abbildung ι aus Proposition V.2.9 und dem Isomorphismus aus Proposition V.2.7. Da ι injektiv ist, ist auch ν injektiv und die Behauptung ist gezeigt.

(ii) Nach Proposition V.2.9 wissen wir

$$\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times \qquad \square$$

Proposition V.2.11: *Ist* $K = \mathbb{F}_p$*, dann ist* $\mathrm{Gal}(\mathbb{F}_p(\zeta_n)|\mathbb{F}_p) \cong ?$*.*

3. Intermezzo I - Darstellungen und Charaktere

In diesem Abschnitt seien G eine Gruppe und K ein Körper.

Definition V.3.1 (Darstellugen und Charaktere):

(i) Eine *Darstellung von* G ist ein Gruppenhomomorphismus

$$\begin{aligned}\rho\colon G &\longrightarrow \mathrm{Gl}(V) = \mathrm{Aut}(V)\\ &= \{\varphi\colon V \to V \mid \varphi \text{ ist Isomorphismus von } K\text{-Vektorräumen}\},\end{aligned}$$

wobei V ein K-Vektorraum ist. Die Dimension $d = \dim V$ heißt auch *Dimension der Darstellung* oder *Grad der Darstellung.*

(ii) Ein *Charakter von* G ist eine eindimensionale Darstellung von G, d. h. ein Gruppenhomomorphismus $\chi\colon G \to \mathrm{Gl}(K) \cong K^\times$.

Beispiel V.3.2: (i) Die Abbildung $\chi_0 \colon G \to K^\times$, $g \mapsto 1$ heißt *trivialer Charakter.*

(ii) Ist G eine endliche Gruppe, also $G = \{g_1, \ldots, g_d\}$, wobei d eine natürliche Zahl ist, dann setze $V = K^d$ mit Basis $e_{g_1}, \ldots, e_{g_d}$ und definiere

$$\rho \colon G \longrightarrow \mathrm{Gl}(V), \qquad g \longmapsto \rho(g),$$

wobei $\rho(g)(e_{g_i}) = e_{gg_i}$. Dieses ρ ist eine Darstellung von G.

(iii) Jedes Element $a \in K^\times$ definiert einen Charakter von $\mathbb{Z}$ durch

$$\chi_a \colon \mathbb{Z} \longrightarrow K^\times, \qquad z \longmapsto a^z.$$

Bemerkung V.3.3 (Gruppe der Charaktere): Sei

$$\chi_G := \{\chi \colon G \to K^\times \mid \chi \ K\text{-wertiger Charakter}\}.$$

(i) Die Menge χ_G ist eine Gruppe mit den punktweisen Verknüpfungen, d. h. für $\chi_1, \chi_2 \in \chi_G$ und $g \in G$ gilt $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$.

(ii) Für $G = K^\times$ erhalten wir die Inklusion von Gruppen

$$\mathrm{Aut}(K) \hookrightarrow \chi_G, \qquad \sigma \longmapsto \sigma|_{K^\times}.$$

Der folgende Satz geht zurück auf Emil Artin

Satz V.3.4 (über Unabhängigkeit der Charaktere): *Fasse χ_G als Teilmenge des K-Vektorraums* $\mathrm{Abb}(G, K)$ *auf. Dann ist χ_G linear unabhängig.*

Beweis: Angenommen, χ_G wäre linear abhängig. Diese Annahme wollen wir führen zu einem Widerspruch führen.

Sei n minimal mit der Eigenschaft, dass es $\chi_1, \ldots, \chi_n \in \chi_G$ gibt, sodass $\{\chi_1, \ldots, \chi_n\}$ linear abhängig ist. Da wir über einem Körper arbeiten, wäre n mindestens 2. Es gäbe also $a_1, \ldots, a_n \in K^\times$, sodass $a_1\chi_1 + \cdots + a_n\chi_n = 0$ und für alle $g \in G$ gälte

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0. \tag{V.1}$$

Wir könnten $h \in G$ finden, sodass $\chi_1(h) \neq \chi_2(h)$. Einsetzen in Gl. (V.1) lieferte, dass für alle $g \in G$ schon

$$a_1\chi_1(hg) + a_2\chi_2(hg) + \cdots + a_n\chi_n(hg) = 0 \tag{V.2}$$

gälte. Subtraktion des $\chi_1(h)$-fachen von Gl. (V.1) von Gl. (V.2) lieferte, dass für alle $g \in G$ gälte, dass

$$a_2(\chi_2(h) - \chi_1(h)) \cdot \chi_2(g) + \cdots + a_n(\chi_n(h) - \chi_1(h))\chi_1(g) = 0.$$

Wegen der Minimalität von n müssten $\chi_2, \ldots, \chi_n$ linear unabhängig sein, d. h. $a_2(\chi_2(h) - \chi_1(h)) = \cdots = a_n(\chi_n(h) - \chi_1(h)) = 0$. Insbesondere $\chi_2(h) = \chi_1(h)$ im Widerspruch zur Wahl von h. □

Korollar V.3.5: *Sei L ein Körper.*

(i) *Zur Erinnerung: Wir haben die Inklusionen* $\mathrm{Aut}(L) \subseteq \chi_G \subseteq \mathrm{Abb}(L^\times, L)$, *d. h.* $\mathrm{Aut}(L)$ *ist als Teilmenge von* $\mathrm{Aut}(L^\times, L)$ *linear unabhängig.*

(ii) *Seien $G = \mathbb{Z}$, $a_1, \ldots, a_n \in K^\times$ und $\chi_{a_i} \colon \mathbb{Z} \to K^\times$, $z \mapsto a_i^z$ aus 5.3.2. Dann sind die Charaktere $\chi_{a_1}, \ldots, \chi_{a_n}$ linear unabhängig, d. h. für $c_1, \ldots, c_n \in K$, die für alle $z \in \mathbb{Z}$ leisten, dass*

$$c_1 a_1^z + \ldots c_n a_n^z = 0,$$

gilt schon $c_1 = \cdots = c_n = 0$.

4. Intermezzo II - Norm und Spur

In diesem Abschnitt seien $K \subseteq L$ eine Körpererweiterung vom Grad n und $\bar{K}$ ein algebraischer Abschluss von K.

Definition V.4.1 (Norm und Spur): Für $\alpha \in L$ sei φ_α die K-lineare Abbildung $\varphi_\alpha \colon L \to L$, $x \mapsto \alpha x$.

(i) Die Zahl $\mathrm{Sp}_{L|K}(\alpha) := \mathrm{Spur}(\varphi_\alpha)$ heißt *Spur von α bezüglich $K \subseteq L$.*

(ii) Die Zahl $N_{L|K}(\alpha) := \det(\varphi_a)$ heißt *Norm von α bezüglich $K \subseteq L$.*

Bemerkung V.4.2 (Bezug zu charakteristischen Polynomen): Sei

$$\chi_{\varphi_a} = \sum_{i=0}^{n} c_i X^i$$

das charakteristische Polynom von φ_a. Aus Bemekerung IX.8.5 im Lineare Algebra Skript wissen wir, dass $c_n = (-1)^n$, $c_{n-1} = (-1)^{n-1}\,\mathrm{Sp}(\varphi_a)$ und $c_0 = \det(\varphi_a)$.

Bemerkung V.4.3 (Spur- und Normabbildung): Für die Abbildungen

$$\mathrm{Sp}_{L|K}\colon L \longrightarrow K, \qquad \alpha \longmapsto \mathrm{Sp}(\varphi_a),$$
$$N_{L|K}\colon L^\times \longrightarrow K^\times, \qquad \alpha \longmapsto \det(\varphi_a)$$

gilt:

(i) $\mathrm{Sp}_{L|K}$ ist ein K-Vektorraumhomomorphismus und damit eine Linearform,

(ii) $N_{L|K}$ ist ein Gruppenhomomorphismus und damit ein Charakter.

Beispiel V.4.4 (Die Körpererweiterung $\mathbb{C}|\mathbb{R}$): Es seien $L = \mathbb{C}$ und $K = \mathbb{R}$. Wähle die Basis $B = \{1, \mathrm{i}\}$ in $\mathbb{C}$. Für $z = x + \mathrm{i}y$ gilt für φ_z: $\varphi_z(1) = z = x + \mathrm{i}y$, $\varphi_z(\mathrm{i}) = z\mathrm{i} = y + \mathrm{i}x$, d. h. die Darstellungsmatrix von φ_z bezüglich der Basis B ist

$$D_{B,B}(\varphi_z) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

Jetzt sind $\mathrm{Sp}_{\mathbb{C}|\mathbb{R}}\colon \mathbb{C} \to \mathbb{R}$, $z \longmapsto 2\Re(z)$, $N_{\mathbb{C}|\mathbb{R}}\colon \mathbb{C}^\times \to \mathbb{R}^2$, $z \mapsto |z|$.

Bemerkung V.4.5 (Rechenregeln für φ_a):

(i) Die Abbildung $\varphi\colon L \to \mathrm{End}_K(L)$, $\alpha \mapsto \varphi_\alpha$ ist ein K-Algebrenhomomorphismus,

(ii) Für $f \in K[X]$ gilt $f(\varphi_\alpha) = \varphi_{f(\alpha)}$.

Beweis: Rechenregel (i) ist klar. Für (ii): Schreibe $f = \sum_{i=0}^n c_i X^i$. Dann ist $f(\varphi_\alpha) = \sum_{i=0}^n c_i \varphi_\alpha^i$ und mit (i) sehen wir $f(\varphi_\alpha) = \sum_{i=0}^n c_i \varphi_{\alpha^i} = \varphi_{f(\alpha)}$. □

Proposition V.4.6 (Rechenregeln für Norm und Spur in Spezialfällen):

(i) *Ist $\alpha \in K$, dann ist $\mathrm{Sp}_{L|K}(\alpha) = n\alpha$ und $N_{L|K}(\alpha) = \alpha^n$.*

(ii) *Ist $\alpha \in L$, wobei $L = K(\alpha)$, mit Minimalpolynom $f = \sum_{i=0}^{n-1} c_i X^i + X^n$ von α über K. Dann ist $f = (-1)^n \chi_{\varphi_\alpha}$ und insbesondere sind*

$$\mathrm{Sp}_{L|K}(\alpha) = (-1)c_{n-1} \quad \textit{und} \quad N_{L|K}(\alpha) = (-1)^n c_0.$$

Beweis: (i) Ist B eine beliebige Basis von $K \subseteq L$, dann ist $D_{B,B}(\varphi) = \alpha I_n$, was die Behauptung liefert.

(ii) Wegen Bemerkung V.4.5 ist $f(\varphi_\alpha) = \varphi_{f_\alpha}$ und $\varphi_{f(\alpha)} = 0$, da $f(\alpha) = 0$. Wir wissen also, dass f den Endomorphismus φ_α annuliert und dass f irreduzibel ist über K, f ist also das Minimalpolynom von φ_α. Wegen $\deg(f) = n = \dim_K L$ ist f bis auf einen konstanten Faktor das charakteristische Polynom von φ_α. □

Proposition V.4.7 (Rechenregeln für Spur und Norm): *Für $\alpha \in L$ betrachte die Kette $K \subseteq K(\alpha) \subseteq L$. Sei $t := [L : K(\alpha)]$. Dann gilt:*

(i) $\mathrm{Sp}_{L|K}(\alpha) = t\,\mathrm{Sp}_{K(\alpha)|K}(\alpha)$,

(ii) $N_{L|K}(\alpha) = N_{K(\alpha)|K}(\alpha)^t$.

Beweis: Wir wählen die K-Basis $B_1 = \{x_1, \ldots, x_r\}$ von $K \subseteq K(\alpha)$ und die $K(\alpha)$-Basis $B_2 = \{y_1, \ldots, y_t\}$ von $K(\alpha) \subseteq L$. Dann ist

$$B = (x_1y_1, x_2y_1, \ldots, x_ry_1, x_1y_2, \ldots, x_1y_t, \ldots, x_ry_1, \ldots, x_ry_t)$$

eine geordnete Basis von L. Sei $A := D_{B_1,B_1}(\varphi_\alpha) = (a_{i,j})$ und verwende $\alpha x_i = \sum_{k=1}^r a_{k,i}x_k$. Dann ist $\alpha x_i y_j = \sum_{k=1}^r a_{k,i}x_k y_j$, d. h. wir haben

$$D_{B,B}(\varphi_\alpha) = \begin{pmatrix} \boxed{A} & & & \\ & \boxed{A} & & \\ & & \ddots & \\ & & & \boxed{A} \end{pmatrix},$$

was die Behauptung zeigt. □

Korollar V.4.8: *Für alle $\alpha \in L$ gilt:*

(i) $\mathrm{Sp}_{L|K}(\alpha) = \mathrm{Sp}_{K(\alpha)|K}(\mathrm{Sp}_{L|K(\alpha)}(\alpha))$,

(ii) $N_{L|K}(\alpha) = N_{K(\alpha)|K}(N_{L|K(\alpha)}(\alpha))$.

Beweis: Wir zeigen die Behauptung nur für die Spur, für die Norm funktioniert der Beweis analog. Nach Proposition V.4.7 und Proposition V.4.6 gilt

$$\begin{aligned} \mathrm{Sp}_{L|K}(\alpha) &= [L : K(\alpha)]\,\mathrm{Sp}_{K(\alpha)|K}(\alpha) \\ &= \mathrm{Sp}_{K(\alpha)|K}([L : K(\alpha)]\alpha) = \mathrm{Sp}_{K(\alpha)|K}(\mathrm{Sp}_{L|K(\alpha)}(\alpha)). \end{aligned}$$ □

Satz V.4.9: *Schreibe $[L : K] = [L : K]_S \cdot q$ und $\mathrm{Hom}(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_r\}$ mit $r = [L : K]_s$. Dann gilt*

$$\mathrm{Sp}_{L|K}(\alpha) = q\sum_{i=1}^r \sigma_i(\alpha) \quad \textit{und} \quad N_{L|K}(\alpha) = \Big(\prod_{i=1}^r \sigma_i(\alpha)\Big)^q.$$

Beweis: Wir zeigen die Aussage zunächst für $\alpha \in K$. In diesem Fall haben wir, dass $\sigma_1(\alpha) = \cdots = \sigma_r(\alpha) = \alpha$, d. h. nach Proposition V.4.6 gilt

$$\mathrm{Sp}_{L|K}(\alpha) = [L:K]\alpha = qr\alpha = q\sum_{i=1}^{r}\sigma_i(\alpha), \qquad N_{L|K}(\alpha) = \alpha^{qr} = \Big(\prod_{i=1}^{r}\sigma_i(\alpha)\Big)^q.$$

Ist $L = K(\alpha)$, dann gilt für das Minimalpolynom f_α von α über K, dass $f_\alpha = \sum_{k=0}^{n} c_k X^k = \prod_{i=1}^{r}(X - \sigma_i(\alpha))^q$. Mit Proposition V.4.6 also

$$\mathrm{Sp}_{L|K}(\alpha) = (-1)c_{n-1} = q\sum_{i=1}^{r}\sigma_i(\alpha), \qquad N_{L|K}(\alpha) = (-1)^n c_n = \prod_{i=1}^{r}\sigma_i(\alpha)^q.$$

Ist α beliebig in $K \subseteq L$, dann betrachten wir die Körperkette $K \subseteq K(\alpha) \subseteq L$, schreiben $\mathrm{Hom}_K(K(\alpha), \bar{K}) = \{\sigma_1, \ldots, \sigma_r\}$, $[K(\alpha) : K] = q_1 r$ und außerdem schreiben wir $\mathrm{Hom}_{K(\alpha)}(L, \bar{K}) = \{\tau_1, \ldots, \tau_{r_2}\}$ sowie $[L : K(\alpha)] = q_2 r_2$. Wir wählen Fortsetzungen $\hat{\sigma}_i \colon \bar{K} \to \bar{K}$.

Nach Proposition IV.4.8 ist $\mathrm{Hom}_K(L, \bar{K}) = \{\hat{\sigma}_i \circ \tau_j \mid 1 \le i \le r_1, 1 \le j \le r_2\}$. Beachte, dass $[L : K] = r_1 q_1 r_2 q_2 = q[L : K]_s$ mit $q = q_1 q_2$. Nach Korollar V.4.8 gilt jetzt

$$\begin{aligned}\mathrm{Sp}_{L|K}(\alpha) &= \mathrm{Sp}_{K(\alpha)|K}(\mathrm{Sp}_{L|K(\alpha)}(\alpha)) \\ &= \mathrm{Sp}_{K(\alpha)|K}\Big(\sum_{j=1}^{r_2}\tau_j(\alpha)\Big) = q_1 q_2 \sum_{i=1}^{r_1}\sigma_i\Big(\sum_{j=1}^{r_2}\tau_j(\alpha)\Big) = q\sum_{i=1}^{r_1}\sum_{j=1}^{r_2}\hat{\sigma}_i\tau_j(\alpha).\end{aligned}$$

Die Behauptung über die Norm zeigt man auf die gleiche Art und Weise. □

Korollar V.4.10 (Verknüpfung von Spur und Norm): *Sei $K \subseteq L \subseteq M$ eine Kette von endlichen Körpererweiterungen. Dann gilt:*

(i) $\mathrm{Sp}_{M|K} = \mathrm{Sp}_{L|K} \circ \mathrm{Sp}_{M|L}$.

(ii) $N_{M|K} = N_{L|K} \circ N_{L|M}$.

Beweis: Schreibe $[M : L] = q_2 r_2$ mit $r_2 = [M : L]$ und $[L : K] = q_1 r_1$ mit $r_1 = [L : K]_s$. Dann ist $[M : K] = qr$ mit $q = q_1 q_2$ und $r = [M : K]_s$. Ferner seien $\mathrm{Hom}_L(M, \bar{K}) = \{\tau_1, \ldots, \tau_{r_2}\}$ und $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_{r_1}\}$ und $\hat{\sigma}_i \colon \bar{K} \to \bar{K}$ eine Fortsetzung von σ. Nach Proposition IV.4.8 ist $\mathrm{Hom}_K(M, \bar{K}) = \{\hat{\sigma}_i \circ \tau_j \mid 1 \le i \le r_1, 1 \le j \le r_2\}$.

Für $\alpha \in M$ gilt nach Satz V.4.9, dass

$$\begin{aligned}\mathrm{Sp}_{L|K}(\mathrm{Sp}_{M|L}(\alpha)) &= q_1\sum_{i=1}^{r_1}\sigma_i\Big(\mathrm{Sp}_{M|L}(\alpha)\Big) \\ &= q_1 q_2 \sum_{i=1}^{r}\sigma_i\Big(\sum_{j=1}^{r_2}\tau_j(\alpha)\Big) = q\sum_{i=1}^{r_1}\sum_{j=1}^{r_2}\hat{\sigma}_i \circ \tau_j(\alpha) = \mathrm{Sp}_{M|K}(\alpha).\end{aligned}$$

Die Aussage über die Norm zeigt man analog. □

Korollar V.4.11 (Invarianz unter Galois-Gruppe): *Sei $K \subseteq L$ eine galoissche Körpererweiterung. Dann sind $\mathrm{Sp}_{L|K}$ und $N_{L|K}$ invariant unter Galois-Automorphismen im folgenden Sinne: Für alle $\alpha \in L$ und $\sigma \in \mathrm{Gal}(L|K)$ gilt $\mathrm{Sp}_{L|K}(\sigma(\alpha)) = \mathrm{Sp}_{L|K}(\alpha)$ und $N_{L|K}(\sigma(\alpha)) = N_{L|K}(\alpha)$.*

Beweis: Folgt direkt aus Satz V.4.9. □

Korollar V.4.12 (Spur für inseparable Körpererweiterungen): *Die Körpererweiterung $K \subseteq L$ ist inseparabel genau dann, wenn $\mathrm{Sp}_{L|K} \equiv 0$.*

Beweis: Die Implikation „⇒“ folgt aus Satz V.4.9 und der Tatsache $q = p^k$ für eine natürliche Zahl k und $p = \mathrm{char}(K)$ nach (Proposition IV.4.6).

„⇐“: Angenommen, $K \subseteq L$ ist separabel und sei $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_r\}$. Wir fassen σ_i via $\sigma_i|_{L^\times} \colon L^\times \to \bar{K}^\times$ als $\bar{K}$-wertigen Charakter auf. Nach Satz V.4.9 ist $\mathrm{Sp}_{L|K} = \sum_{i=1}^{r} \sigma_i$. Wäre $\mathrm{Sp}_{L|K} \equiv 0$, dann wäre $\{\sigma_1, \ldots, \sigma_r\}$ linear abhängig im Widerspruch zu Satz V.3.4. □

Für eine separable Körpererweiterung $K \subseteq L$ ist die Abbildung

$$\mathrm{Sp} \colon L \times L \longrightarrow K, \qquad (x, y) \longmapsto \mathrm{Sp}_{L|K}(xy)$$

eine symmetrische Bilinearform. Außerdem ist Sp nicht ausgeartet, d. h. für all $x \in L^\times$ gibt es $y \in L$ sodass $\mathrm{Sp}(xy) \neq 0$. Wäre nämlich $x \in L^\times$ mit der Eigenschaft, dass für alle $y \in L$ schon $\mathrm{Sp}(xy) = 0$, dann wäre für alle $\alpha \in L$ auch $\mathrm{Sp}_{L|K}(\alpha) = 0$, was nicht sein kann, denn $K \subseteq L$ ist separabel.

Korollar V.4.13 (Spur induziert Isomorphismus $L \cong \hat{L}$): *Ist $K \subseteq L$ eine separable Körpererweiterung, dann ist*

$$\mathrm{Sp} \colon L \times L \longrightarrow K, \qquad (x, y) \longmapsto \mathrm{Sp}_{L|K}(xy)$$

eine nicht-ausgeartete symmetrische Bilinearform und definiert den folgenden Isomorphismus von K-Vektorräumen:

$$\Phi \colon L \longrightarrow \hat{L}, \qquad x \longmapsto \mathrm{Sp}(x-),$$

wobei $\hat{L}$ den Dualraum von L bezeichnet.

Korollar V.4.14: *Ist $K \subseteq L$ eine separable Körpererweiterung und $\{x_1, \ldots, x_n\}$ eine K-Basis von L, dann gibt es eine eindeutig bestimmte K-Basis $\{y_1, \ldots, y_n\}$ von L, sodass für $1 \leq i, j \leq n$ gilt, dass $\mathrm{Sp}_{L|K}(x_i y_j) = \delta_{i,j}$.*

Beweis: Sei $\{\beta_1, \ldots, \beta_n\}$ die Dualbasis von $\{x_1, \ldots, x_n\}$, d. h. $\beta_i(x_j) = \delta_{i,j}$. Wählen wir $y_i := \Phi^{-1}(\beta_i)$, dann gilt $\mathrm{Sp}_{L|K}(x_i y_j) = \Phi(y_j)(x_i) = \beta_j(x_i) = \delta_{i,j}$, wie gewünscht. □

5. Zyklische Körpererweiterungen

In diesem Abschnitt seien K ein Körper, n eine natürliche Zahl, die kein Vielfaches der Charakteristik von K sei und K enthalte eine n-te Einheitswurzel ζ_n.

Proposition V.5.1 (Galois-Gruppe $\mathrm{Gal}(K(\sqrt[n]{c})|K)$): *Seien $c \in K$ und $L = K(\sqrt[n]{c})$, d. h. $L = K(\alpha)$ mit $\alpha^n = c$. Dann gilt:*

(i) *Die Erweiterung $K \subseteq L$ ist eine galoissche Körpererweiterung.*

(ii) *Die Galoisgruppe $\mathrm{Gal}(L|K)$ ist zyklisch.*

(iii) *Der Grad $d := [L : K]$ teilt n, es gilt $\alpha^d \in K$ und $X^d - \alpha^d$ ist das Minimalpolynom von α.*

Beweis: (i) Ohne Einschränkung sei $c \in K^\times$. Dann sind α, $\alpha\zeta_n$, $\ldots$, $\alpha\zeta_n^{n-1}$ die n verschiedenen Nullstellen von $X^n - c$, die alle in L liegen und L ist der Zerfällungskörper der Polynoms $X^n - c$, d. h. $K \subseteq L$ ist normal.

Für $f = X^n - c$ ist $f' = nX^{n-1}$, d. h. f ist separabel, da f und f' keine gemeinsamen Nullstellen haben. Insbesondere ist $K \subseteq L$ separabel.

(ii) Sei $\sigma \in \mathrm{Gal}(L|K)$. Dann ist $\sigma(\alpha)\eta_\sigma$ mit $\eta_\sigma \in U_n$. Wir erhalten also einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(L|K) \hookrightarrow U_n$ via $\sigma \mapsto \eta_\sigma$. Da U_n zyklisch ist, ist auch $\mathrm{Gal}(L|K)$ zyklisch und $d = \#\,\mathrm{Gal}(L|K)$ teilt n.

(iii) Für ein $\sigma \in \mathrm{Gal}(L|K)$ ist

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (\alpha\eta_\sigma)^d = \alpha^d\eta_\sigma = \alpha^d,$$

also ist $\alpha^d = L^{\mathrm{Gal}(L|K)} = K$. Weiter annuliert $X^d - \alpha^d \in K[X]$ unser α und hat den richtigen Grad. □

Im Folgenden wollen wir uns davon überzeugen, dass das das einzige Beispiel mit $\mathrm{Gal}(L|K) \cong \mathbb{Z}/n\mathbb{Z}$, wobei die Charakteristik von K unser n nicht teilt.

Satz V.5.2 (Hilbert '90): *Es sei $K \subseteq L$ eine endliche zyklische Galois-Erweiterung mit $\mathrm{Gal}(L|K) = \langle\sigma\rangle$. Für $\beta \in L$ ist $N_{L|K}(\beta) = 1$ genau dann, wenn es $\alpha \in L^\times$ mit $\beta = \alpha\sigma(\alpha)^{-1}$ gibt.*

Satz V.5.3 (über zyklische Körpererweiterungen): *Sei $K \subseteq L$ eine Körpererweiterung von Grad n. Die Körpererweiterung $K \subseteq L$ ist zyklisch genau dann, wenn $L = K(\alpha)$ für ein $\alpha \in L$ mit Minimalpolynom $f_\alpha = X^n - c$, wobei $c \in K$.*

Beweis: „⇐“ ist Proposition V.5.1.

„⇒“: Sei $\mathrm{Gal}(L|K) = \langle\sigma\rangle$. Wegen $\zeta_n \in K$ ist $N_{L|K}(\zeta_n) = \zeta_n^n = 1$ nach Proposition 5.4.6. Genauso ist $N_{L|K}(\zeta_n^{-1}) = 1$.

Wegen Satz V.5.2 gibt es $\alpha \in L^\times$ mit $\zeta_n^{-1} = \alpha\sigma(\alpha)^{-1}$, d. h. $\sigma(\alpha) = \zeta_n\alpha$. Wir erhalten, dass α, $\sigma(\alpha) = \zeta_n\alpha$, $\sigma^2(\alpha) = \zeta_n^2\alpha$, …, $\sigma^{n-1}(\alpha) = \zeta_n^{n-1}\alpha$ allesamt Nullstellen von f_α sind, d. h. $[K(\alpha : K] \geq n$. Da aber $[L : K] = n$, muss $L = K(\alpha)$ gelten.

Bleibt zu zeigen, dass $f_\alpha = X^n - c$, wobei $c \in K$. Wir zeigen dazu, dass $\alpha^n \in K$ gilt. Es ist

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta_n\alpha)^n = \alpha^n,$$

d. h. $\alpha^n \in K$. Aus $[L : K] = n$ folgt, dass $X^n - c$ irreduzibel ist. □

Beweis (von V.1.5): „⇐“ folgt aus (Korollar 5.4.11).

„⇒“: Es sei $n = [L : K]$. Dann ist $\mathrm{Gal}(L|K) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. Wir betrachten wiederum die zugehörigen Charaktere $\chi_i := \sigma^i|_{L^\times} : L^\times \to L^\times$. Nach Satz V.3.4 ist $\{\chi_0, \ldots, \chi_{n-1}\}$ linear unabhängig über L. Setzen wir

$$f := \chi_0 + \beta\chi_1 + \beta\sigma(\beta)\chi_2 + \cdots + \beta\sigma(\beta)\sigma^2(\beta)\ldots\sigma^{n-2}(\beta)\chi_{n-1},$$

dann ist $f \neq 0$, d. h. es gibt $\gamma \in L^\times$, sodass $\alpha = f(\gamma) \neq 0$. Es ist also

$$\alpha = \gamma + \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\gamma) + \cdots + \beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\gamma).$$

Damit ist

$$\begin{aligned}\beta\sigma(\alpha) &= \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\gamma) \\ &\quad + \cdots + \beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}(\beta)\sigma^n(\gamma) \\ &= \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\gamma) \\ &\quad + \cdots + N_{L|K}(\beta)\gamma \\ &= \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(\gamma) \\ &\quad + \cdots + \gamma\end{aligned}$$

d. h. $\beta\sigma(\alpha) = \alpha$, was die Behauptung zeigt. □

Satz V.5.4 (Hilbert ’90 additiv): *Seien $K \subseteq L$ eine endliche zyklische Galois-Erweiterung mit $\mathrm{Gal}(L|K) = \langle\sigma\rangle$ und sei $\beta \in L$. Dann gilt für $\beta \in L$ dass $\mathrm{Sp}_{L|K}(\beta) = 0$ genau dann, wenn es $\alpha \in L$ mit $\beta = \alpha - \sigma(\alpha)$ gibt.*

Beweis (ähnlich aber nicht analog): „⇐“: Das ist (Korollar 5.4.11).

„⇒“: Es seien wiederum $n = [L : K]$ und $\mathrm{Gal}(L|K) = \{\mathrm{id}, \sigma, \dots, \sigma^{n-1}\}$. Da die Körperweiterung $K \subseteq L$ separabel ist, gibt es $\gamma \in L$ mit $\mathrm{Sp}_{L|K}(\gamma) \neq 0$. Definiere $\alpha \in L$ durch

$$\mathrm{Sp}_{L|K}(\gamma)\alpha = \beta\sigma(\gamma) + (\beta + \sigma(\beta))\sigma^2(\gamma) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta)).$$

Eine einfache (aber vermutlich längliche) Rechnung liefert, dass

$$(\alpha - \sigma(\alpha))\,\mathrm{Sp}_{L|K}(\gamma) = \beta\,\mathrm{Sp}_{L|K}(\gamma),$$

d. h. $\alpha\sigma(\alpha) = \beta$. □

Als Ausblick, wozu das eben bewiesene nützlich ist: Seien $(G, \cdot)$ eine Gruppe, $(M, +)$ eine abelsche Gruppe und $G \to \mathrm{Aut}(M)$ eine Gruppenaktion von G auf M. Wir definieren $C^n(G, M) := \mathrm{Abb}(G^n, M)$ und

$$d^n \colon C^n(G, M) \longrightarrow C^{n+1}(G, M), \qquad f \longmapsto d^n(f),$$

wobei

$$\begin{aligned} d^n(f)(g_1, \dots, g_{n+1}) &:= g_1 \cdot f(g_2, \dots, g_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^j f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+1}, \dots, g_n) \\ &\quad + (-1)^{n+1} f(g_1, \dots, g_n). \end{aligned}$$

Dadurch erhalten wir eine Kette von Homomorphismen von abelschen Gruppen

$$M \cong C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \xrightarrow{d^2} C^3(G, M) \dots$$

Es gilt $d^n \circ d^{n-1} = 0$, d. h. $\mathrm{im}(d^{n-1}) \subseteq \ker(d^n)$. Der Quotient

$$H^n(G, M) := \ker(d^n)/\,\mathrm{im}(d^{n-1})$$

heißen *n-te Gruppenkohomologie mit Werten in M*. Beachte:

(0) Ist $a \in M = C^0(G, M)$, dann ist $d^0(a) \in C^1(G, M) = \mathrm{Abb}(G, M)$ und

$$d^0(a) \colon G \longrightarrow M, \qquad g \longmapsto ga - a$$

(1) Ist $f \in C^1(G, M)$, dann ist $d^1(f) \in C^2(G, M)$ mit

$$d^1(f) \colon G^2 \longrightarrow M, \qquad (g_1, g_2) \longmapsto g_1 f(g_2) - f(g_1, g_2) + f(g_1).$$

(2) Ist $h \in C^2(G,M) = \mathrm{Abb}(G^2, M)$, dann ist

$$d^2(h)\colon G^3 \longrightarrow M,$$
$$(g_1,g_2,g_3) \longmapsto g_1 h(g_2,g_3) - h(g_1g_2,g_3) + h(g_1,g_2g_3) - h(g_1,g_2).$$

Beispiel: Ist $G = \mathrm{Gal}(L|K)$ und $M = L^\times$, dann ist $H^1(\mathrm{Gal}(L|K), L^\times) = \ker(d^1)/\operatorname{im}(d^0)$. Es sind

$$\ker(d^1) = \{f \in \mathrm{Abb}(G, L^\times) \mid \forall\, \sigma_1,\sigma_2 \in G : \sigma_1(f(\sigma_2)) \cdot (f(\sigma_1 \circ \sigma_2))^{-1} \cdot f(\sigma_1) = 1\}$$
$$\operatorname{im}(d^0) = \{f \in \mathrm{Abb}(G, L^\times) \mid \exists\, a \in L^\times : f(\sigma) = \sigma(a)a^{-1}\}$$

Ist G eine zyklische Gruppe mit Erzeuger σ, d. h. falls $K \subseteq L$ eine zyklische Erweiterung ist, dann ist $H^1(G; L^\times) = \{0\}$, d. h. $\ker(d^1) = \operatorname{im}(d^0)$.

Seien nämlich $f \in \ker(d^1)$ und $b = f(\sigma)$. Wegen $f \in \ker(d^1)$ ist $f(\sigma^2) = \sigma(f(\sigma))f(\sigma) = \sigma(b)b$. Analog ist $f(\sigma^3) = \sigma^2(b)\sigma(b)b$ und so weiter und $f(\sigma^n) = \sigma^{n-1}(b)\sigma^{n-2}(b)\cdots\sigma(b)b$. Daraus folgt, dass $N_{L|K}(b) = f(\sigma^n) = f(\mathrm{id})$. Wegen der obigen Mengenbeschreibung (für $\sigma_1 = \mathrm{id} = \sigma_2$) können wir ablesen, dass $f(\mathrm{id}) = 1$, also $N_{L|K}(f) = 1$. Jetzt liefert Satz V.5.2 die Behauptung.

Proposition V.5.5 (Artin-Schreier-Beispiel): *Seien K ein Körper der Charakteristik $p > 0$ und $L = K(\alpha)$, wobei α eine Nullstelle von $f = X^p - X - c \in K[X]$ ist. Dann ist $L = K$ und $X^p - X - c$ zerfällt über K in Linearfaktoren oder $K \subseteq L$ ist eine zyklische Galois-Erweiterung und $X^p - X - c$ ist irreduzibel.*

Beweis: Beachte, dass $f(\alpha+1) = (\alpha+1)^+ - (\alpha+1) - c = \alpha^p - \alpha - c = f(\alpha)$. Deshalb sind α, $\alpha+1$, …, $\alpha+p-1$ schon p verschiedene Nullstellen von f in L, d. h. $K \subseteq L$ ist eine normale Körpererweiterung. Wegen $f' = pX^{p-1} - 1 = -1$ haben f und f' haben keine gemeinsamen Nullstellen, also ist f separabel und $K \subseteq L$ ist in der Tat galoissch.

Ist $\alpha \in K$, dann liegen auch alle anderen Nullstellen von f schon in K. Sei jetzt $\alpha \in L - K$. Wir wollen zeigen, dass $f = X^p - X - c$ irreduzibel ist. Angenommen, g wäre ein Teiler von f, d. h. g wäre von der Form

$$g = (X - \alpha - i_1)\cdots(X - \alpha - i_d) \in K[X],$$

wobei $i_1, \ldots, i_d \in \{0, \ldots, p-1\}$. Der Koeffizient von X^{d-1} ist von der Form $-d\alpha + j$ mit $j \in \mathbb{F}_p \subseteq K$, wir erhielten also $\alpha \in K$ im Widerspruch zur Annahme. f ist also das Minimalpolynom von α.

Wir finden deshalb $\sigma \in \mathrm{Gal}(L|K)$ mit $\sigma(\alpha) = \alpha + 1$. Die Potenzen id, σ, σ^2, …, σ^{d-1} sind damit verschieden und $\mathrm{Gal}(L|K) = \langle\sigma\rangle$. □

Satz V.5.6 (von Artin-Schreier): *Sei $K \subseteq L$ eine Körpererweiterung der Charakteristik $\mathrm{char}(K) = \mathrm{char}(L) = p > 0$. Dann gilt: Die Körpererweiterung $K \subseteq L$ ist eine zyklische Galois-Erweiterung von Grad p genau dann, wenn es $c \in K$ gibt, sodass $L = K(\alpha)$, wobei $\alpha \in L - K$ eine Nullstelle von $X^d - X - c$ ist.*

Beweis: „$\Leftarrow$“ haben wir in Proposition V.5.5 gesehen.

„$\Rightarrow$“: Sei $\mathrm{Gal}(L|K) = \langle\sigma\rangle$. Dann ist $\mathrm{Sp}_{L|K}(-1) = p \cdot (-1) = 0$. Nach der additiven Variante von Hilbert '90 (Satz V.5.4) gibt es $\alpha \in L$ mit $\sigma(\alpha) = \alpha + 1$. Weiter ist $\sigma^i(\alpha) = \alpha + i$, d. h. die Körperelemente α, $\sigma(\alpha)$, $\ldots$, $\sigma^{p-1}(\alpha)$ sind alle verschieden. Wegen $[K(\alpha) : K] \geq p$ ist $L = K(\alpha)$, denn $[L : K] = p$.

Außerdem ist

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha,$$

wir sollten also $c := \alpha^p - \alpha \in L^{\mathrm{Gal}(L|K)} = K$ wählen. Also ist α eine Nullstelle von $X^p - X - c \in K[X]$. □

6. Auflösbarkeit von Gleichungen

Beispiel V.6.1 (quadratische Gleichungen): Die Lösungen von $X^2 + pX + q$ sind $X_{1,2} = -p/2 \pm (p^2/4 - q)^{1/2}$.

Beispiel V.6.2 (kubische Gleichungen): (i) Gleichungen $X^3 + 3pX + 2q = 0$: Ist ζ_3 eine primitive Einheitswurzel und schreiben wir $u = (-q + (q^2 + p^3)^{1/2})^{1/3}$ und $v = (-q - (q^2 + p^3)^{1/2})^{1/3}$, wobei wir die dritten Wurzeln so wählen, dass $uv = -p$ gilt, dann haben wir die drei Lösungen

$$X_1 = u + v, \qquad X_2 = u\zeta_3 + v\zeta_3^2, \qquad X_3 = u\zeta_3^2 + v\zeta_3,$$

Diese Formeln sind bekannt als die Cardanischen Formeln, stammen aber tatsächlich von Ferro.

Um diese Formeln zu erhalten, wählt man den Ansatz, dass man eine Lösung X schreiben kann als Summe $X = u + v$. Einsetzen gibt

$$\begin{aligned} X^3 = (u + v)^3 &= u^3 + 3u^2v + 3uv^2 + v^3 \\ &= 3uv(u + v) + u^3 + v^3 = 3uvX + u^3 + v^3 = -3pX - 2q, \end{aligned}$$

wobei das letzte Gleichheitszeichen daher kommt, dass X eine Lösung der Ausgangsgleichung ist. Wir suchen also u und v, sodass $uv = -p$, $u^3 + v^3 = -2q$. Einfacher ist aber, u^3 und v^3 zu suchen, die $u^3v^3 = -p^3$ und $u^3 + v^3 = -2q$ leisten. Nach dem Satz von Vieta erfüllen das die Lösungen der Gleichung $T^2 + 2qT - p^3$. Diese sind $-q \pm (q^2 + p^3)^{1/3}$.

(ii) Gleichungen der Form $X^3+aX^2+bX+c=0$: Ersetzt man $X=Y-\frac{1}{3}a$, dann ist $-(3/3)a+a=0$ der Koeffizient von Y^2 und wir erhalten eine Gleichung vom Typ (i). Genauer ist unsere neue Gleichung $Y^3+3pY+2q=0$, wobei $p=(1/3)a^2+b$ und $q=(3/27)a^3-(ba/3)+c$.

Definition V.6.3 (durch Radikale auflösbare Körpererweiterungen): Eine endliche Körpererweiterung $K \subseteq L$ heißt *durch Radikale auflösbar*, falls es eine Körperkette $K =: E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m$ mit $L \subseteq E_m$ und $E_{i+1} = E_i(\alpha_{i+1})$, wobei

(i) α_{i+1} ist Einheitswurzel,

(ii) α_{i+1} ist Nullstelle von $X^n - c \in E_i[X]$ für ein $c \in E_i$ und eine natürliche Zahl n, die kein Vielfaches der Charakteristik von K ist,

(iii) α_{i+1} ist Nullstelle von $X^p - X - c \in E_i[X]$ mit $p = \mathrm{char}(K) > 0$ und $c \in E_i$.

Bemerkung V.6.4: Ist $K \subseteq L$ durch Radikale auflösbar, dann ist $K \subseteq L$ separabel.

Definition V.6.5 (Auflösbare Körpererweiterung): Eine endliche Körpererweiterung $K \subseteq L$ heißt *auflösbar*, falls es eine Körpererweiterung $L \subseteq E$ gibt, sodass $K \subseteq E$ galoissch und $\mathrm{Gal}(E|K)$ auflösbar ist.

Bemerkung V.6.6: Ist $K \subseteq L$ eine endliche galoissche Körpererweiterung, dann ist $K \subseteq L$ auflösbar genau dann, wenn $\mathrm{Gal}(L|K)$ auflösbar ist.

Beweis: „$\Leftarrow$“ ist klar. Für „$\Rightarrow$“: Sei E wie in Definition V.6.5. Dann ist $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(E|K)/\mathrm{Gal}(E|L)$, d. h. $\mathrm{Gal}(L|K)$ ist auch auflösbar nach (Bemerkung II.3.11). □

Proposition V.6.7 (Vererbung von Auflösbarkeit): *Für algebraische Körpererweiterungen $K \subseteq L, E \subseteq M$ gilt:*

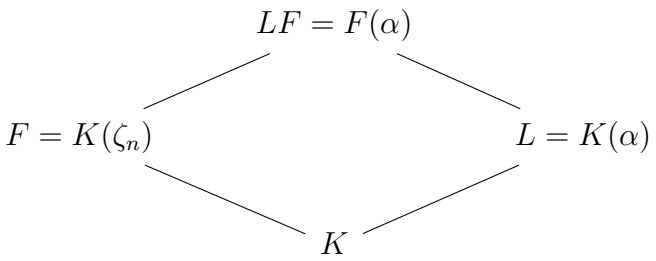
(i) *Sind $K \subseteq L$ und $K \subseteq M$ auflösbar, dann auch $K \subseteq LE$ und $K \subseteq L \cap E$,*

(ii) *Es ist $K \subseteq M$ auflösbar genau dann, wenn $L \subseteq M$ und $K \subseteq L$ auflösbar sind.*

Der Beweis dieser Aussage wird Ihnen als Übungsaufgabe 3 auf Blatt 13 überlassen.

Proposition V.6.8 (Auflösbarkeit der elementeren Körpererweiterungen): *Die Körpererweiterungen vom Typ (i), (ii) und (iii) aus Definition V.6.3 sind auflösbar.*

Beweis: Für Typ (i) und Typ (iii) folgt die Behauptung aus (Satz V.2.10) und (Satz V.5.5). Sei $K \subseteq L$ eine Körpererweiterung vom Typ (ii) und $n := [L : K]$. Das heißt $L = K(\alpha)$, wobei α Nullstelle von $X^n - c \in K[X]$. Sei weiter ζ_n eine primitive n-te Einheitswurzel und $F := K(\zeta_n)$. Wir sind also in der Situation



Es ist also $LF = F(\alpha)$. Nach (Satz 5.5.3) ist $F \subseteq LF$ eine zyklische Galois-Erweiterung und damit auflösbar. Nach (Satz 5.2.10) ist $K \subseteq L$ auflösbar, nach (Proposition 5.6.8) ist $K \subseteq LF$ aufösbar und schließlich ist wegen (Proposition 5.6.8) auch $K \subseteq L$ auflösbar. □

Satz V.6.9 (über Auflösbarkeit von Körpererweiterungen): *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann gilt: $K \subseteq L$ ist auflösbar genau dann, wenn $K \subseteq L$ durch Radikale auflösbar ist.*

Beweis: „⇐“ folgt aus Proposition 5.6.8 und Proposition 5.6.7.
„⇒“: Wir zeigen die Aussage in drei Schritten:

(1) Die Behauptung stimmt, wenn $K \subseteq L$ galoissch ist und K alle n-ten Einheitswurzeln enthält, wobei $n = [L : K]$,

(2) Die Behauptung stimmt, wenn $K \subseteq L$ galoissch ist,

(3) Die Behauptung stimmt für allgemeine endliche Körpererweiterungen.

Zu (1): Es sei $G = \mathrm{Gal}(L|K)$ die auflösbare Galois-Gruppe unserer Körpererweiterung, d. h. es gibt eine Kompositionsreihe

$$\mathrm{Gal}(L|K) = G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_k = \{1\}$$

mit zyklischen Quotienten von Primzahlordnung. Nach dem Hauptsatz der Galois-Theorie erhalten wir einen Körperturm $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_k = L$,

wobei, für $1 \leq i \leq k$, die Körpererweiterung $E_i \subseteq E_{i+1}$ zyklisch ist mit primem Grad $p_i = [E_{i+1} : E_i]$, der n teilt.

Satz 5.5.3 liefert im $\mathrm{char}(K) \neq p_i$, dann ist $E_i \subseteq E_{i+1}$ vom Typ (ii) und Satz 5.5.5 liefert im Fall $\mathrm{char}(K) = p_i$, dass $E_i \subseteq E_{i+1}$ vom Typ (iii) ist.

Zu (2): Wie verwenden den gleichen Trick wie in Proposition V.6.8. Seien $n = [L : K]$, ζ_n eine primitive n-te Einheitswurzel und $F := K(\zeta_n)$. Wähle für L und F in einem algebraischen Abschluss das Kompositum LF. Nach Satz V.2.10 ist $K \subseteq F$ auflösbar und $K \subseteq L$ ist auflösbar nach Voraussetzung. Nach Proposition V.6.8 ist also auch $K \subseteq LF$ auflösbar.

Außerdem ist nach Proposition V.1.10 auch $K \subseteq LF$ galoissch. Nach (1) ist $F \subseteq LF$ durch Radikale auflösbar und $K \subseteq F$ ist eine elementare Erweiterung, d. h. nach Proposition V.6.8 ist auch $K \subseteq LF$ durch Radikale auflösbar. Aber dann ist erst Recht auch $K \subseteq L$ durch Radikale auflösbar.

Zu (3): Ist $K \subseteq L$ auflösbar, so gibt es eine endliche Körpererweiterung $L \subseteq E$, wobei die Erweiterung $K \subseteq E$ galoissch und auflösbar ist. Nach (2) ist $K \subseteq E$ durch Radikale auflösbar, damit erst Recht $K \subseteq L$. □

Korollar V.6.10:

(i) *Ist $K \subseteq L$ eine separable Körpererweiterung mit $[L : K] \leq 4$, dann ist $K \subseteq L$ auflösbar.*

(ii) *Ist $K \subseteq L$ eine galoissche Körpererweiterung mit $\mathrm{Gal}(L|K) \cong S_n$ und $n \geq 5$, dann ist $K \subseteq L$ nicht durch Radikale auflösbar.*

Insbesondere: Ist $f \in K[X]$ ein separables Polynom sodass $\mathrm{Gal}(Z(f)|K) \cong S_n$ mit $n \geq 5$, dann lassen sich die Nullstellen von f nicht durch Wurzelausdrücke angeben.

Satz V.6.11: *Seien $p \geq 5$ eine Primzahl und $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit $\deg(f) = p$. Hat f mindestens zwei reelle Nullstellen und mindestens eine nicht-reelle Nullstelle, dann ist $\mathbb{Q} \subseteq Z(f)$ nicht auflösbar.*

Korollar V.6.12: *Für jede Primzahl $p \geq 5$ gibt es für Gleichungen von Grad p keine Lösungsformel.*

Beweis: Satz V.6.11 oder auch Übungsaufgabe 4 von Blatt 13. □

Bemerkung V.6.13: Die Aussage aus Korollar V.6.12 gilt auch allgemeiner für natürliche Zahlen $n \geq 5$, vergleiche Bosch, Korollar 7 in Kapitel 6.1.

Lemma V.6.14 (Gruppentheorie in S_n): *Seien p eine Primzahl und $G \subseteq S_p$ eine Untergruppe, die transitiv auf $\{1, \ldots, p\}$ operiert.*

(i) *Die Gruppe G hat eine Untergruppe H mit* $\operatorname{ord}(H) = p$,

(ii) *Ist G auflösbar, dann ist die Untergruppe H aus (i) eindeutig bestimmt und ein Normalteiler in G.*

(iii) *Ist G auflösbar, dann hat jedes $\sigma \in G$ mit $\sigma \neq \{\mathrm{id}\}$ höchstens einen Fixpunkt.*

Beweis: (i) Nach der Bahnformel haben wir $\#(G) = \#\operatorname{Stab}(\{1\})p$, d. h. die Behauptung folgt aus den Sylow-Sätzen.

(ii) Da G auflösbar ist, gibt es eine Kompositionsreihe

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{k-1} \triangleright \{1\} = G_k$$

sodass, für $1 \leq i \leq n$, G_i/G_{i+1} zyklisch und von primer Ordnung ist.

Zunächst halten wir fest, dass für alle $0 \leq i \leq k-1$ die Gruppe G_i transitiv auf $\{1, \ldots, p\}$ operiert. Das zeigt man per Induktion: Seien $B_1 = G_i g_1, \ldots, B_r = G_i g_r$ die Bahnen von G_i. Dann operiert G_{i-1} auf $\{B_1, \ldots, B_r\}$ durch

$$gB_k = gG_i g_k = G_i g g_k.$$

Dies ist wohldefiniert, da G_i ein Normalteiler in G_{i-1} ist. Diese Aktion ist transitiv nach Induktionsvoraussetzung, insbesondere sind alle Bahnen gleichmächtig. Es ist also $p = \#\{1, \ldots, p\} = r\#(B_1)$ für ein $r \in \mathbb{N}$. Wäre $r = p$, so wäre $\#(B_k) = 1$ für alle $k \in \mathbb{N}$ und damit $G_i = \{1\}$; andernfalls wäre $\#B_1 = p$ und damit die Operation transitiv.

Weiter ist $H = G_{n-1}$. Das sieht man so: Da G_{n-1} transitiv auf $\{1, \ldots, p\}$ operiert wissen wir aus (i) dass $p \mid \#(G_{n-1})$, also $\#(G_{k-1}) = p$. Außerdem gilt

$$\#(G) = \#(G_0/G_1) \cdot \#(G_1/G_2) \cdots \#(G_{k-2}/G_{k-1}) \cdot \#(G_{k-1}).$$

Wegen $G \subseteq S_p$ teilt p^2 nicht die Gruppenordnung von G, d. h. $\#(G_{i-1}/G_i)$ ist nicht durch p teilbar für $i \leq k-1$.

Schließlich zeigen wir durch vollständige Induktion über i, dass $H \subseteq G_{k-1}$. Für $i = 0$ ist alles klar. Die Behauptung gelte nun für ein $i-1$. Wir betrachten das Diagramm

$$\mathbb{Z}/p\mathbb{Z} \cong H \hookrightarrow G_{i-1} \twoheadrightarrow G_{i-1}/G_i$$

Da p die Ordnung von G_{i-1}/G_i nicht teilt, ist das Bild von H unter der kanonischen Projektion trivial, d. h. $H \subseteq G_i$. Wegen $\#(H) = p'\#(G_{k-1})$ folgt dann $G_{k-1} = H$. Damit ist H eindeutig bestimmt und muss unter Konjugation auf sich selbst abgebildet werden.

(iii) Sei $\sigma \in G$ ein Element mit zwei Fixpunkten. Wir fassen S_p auf als Symmetriegruppe $\mathrm{Sym}(\mathbb{Z}/p\mathbb{Z})$. Ohne Einschränkung gelte $\sigma(0) = 0$. Sei H der Normalteiler aus (ii) mit $\mathrm{ord}(H) = p$. Ohne Einschränkung sei $H = \langle\pi\rangle$ mit $\pi = (01 \dots p-1)$. Da H ein Normalteiler ist, gilt $\sigma\pi\sigma^{-1} \in H$, d. h. es gibt $r \in \mathbb{N}$ mit $\sigma\pi\sigma^{-1} = \pi^r$. Wir haben also

$$(\sigma(0) = 0\sigma(1) \dots \sigma(p-1)) = \sigma\pi\sigma^{-1} = \pi^r = (0, r, 2r, \dots, (p-1)r).$$

Sei $i \neq 0$ ein weiterer Fixpunkt von σ. also $i = \sigma(i) = ir$. Damit ist $i(r-1) = 0$ in $\mathbb{Z}/p\mathbb{Z}$, also $r \equiv 1 \pmod{p}$ was ergibt, dass $\sigma(j) = j$ für alle $j \in \mathbb{Z}/p\mathbb{Z}$ und $\sigma = \mathrm{id}$. □

Proposition V.6.15 („Zwei sind genug"): *Seien p eine Primzahl, K ein Körper, $f \in K[X]$ ein irreduzibles separables Polynom mit $\deg(f) = p$ und $L = Z(f)$.*

Ist $K \subseteq L$ auflösbar, dann gilt für zwei beliebige verschiedene Nullstellen α, β von f, dass $L = K(\alpha, \beta)$.

Beweis: Betrachte die Einbettung der Galois-Gruppe $\mathrm{Gal}(L|K)$ in die symmetrische Gruppe $S_p = \mathrm{Sym}(\mathrm{Nst}(f))$. Das Bild von $\mathrm{Gal}(L|K)$ unter dieser Einbettung ist transitiv, da f irreduzibel ist. Sei jetzt $\sigma \in \mathrm{Gal}(L|K(\alpha, \beta))$. Dann gilt $\sigma(\alpha) = \alpha$ und $\sigma(\beta) = \beta$. Dann muss aber schon $\sigma = \mathrm{id}$ gelten, d. h. $\mathrm{Gal}(L|K(\alpha, \beta)) = \{\mathrm{id}\}$ und nach dem Hauptsatz der Galoistheorie ist deshalb $L = K(\alpha, \beta)$. □

Beweis (von Satz V.6.11): Sei $L = Z(f)$. Angenommen, die Körpererweiterung $\mathbb{Q} \subseteq L$ wäre auflösbar. Dann wäre auch die Galois-Gruppe $\mathrm{Gal}(L|K)$ auflösbar. Seien α und β die beiden reellen Nullstellen von f. Nach Proposition V.6.15 wäre dann $L(\alpha, \beta) = \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{R}$ im Widerspruch zur Existenz einer nicht-reellen Nullstelle. □

7. Fundamentalsatz der Algebra

Satz V.7.1 (Fundamentalsatz der Algebra): *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Im weiteren Verlauf verwenden wir die folgenden Eigenschaften der reellen Zahlen:

(A) Jedes Polynom $f \in \mathbb{R}[X]$ mit $\deg(f) \in 2\mathbb{N} + 1$ hat eine reelle Nullstelle,

(B) Jede nichtnegative reelle Zahl a hat eine nichtnegative reelle Quadratwurzel q.

Bemerkung V.7.2: (i) Jede komplexe Zahl $z = x + \mathrm{i}y$ besitzt eine Quadratwurzel in den komplexen Zahlen.

(ii) Ein Polynom $f \in \mathbb{C}[X]$ vom Grad 2 zerfällt über den komplexen Zahlen.

(iii) Die komplexen Zahlen haben keine echten Körpererweiterungen vom Grad 2.

Beweis: (i) Sei $z = x + \mathrm{i}y$ eine komplexe Zahl. Es gilt

$$z = (a + \mathrm{i}b)^2 = (a^2 - b^2) + \mathrm{i}2ab$$

mit reellen Zahlen a, b, x, y genau dann, wenn $a^2 - b^2 = x$ und $2ab = y$. Ist $y = 0$, dann folgt die Behauptung aus (ii). Sonst gilt $a^2 - b^2 = x$ und $2ab = y$ genau dann, wenn $a = y/(2b)$ und $x = y^2/(4b^2) - b^2$. Das ist äquivalent dazu, dass $a = y/(2b)$ und $b^4 = b^2x - (1/4)y^2 = 0$. Lösen der quadratischen Gleichung liefert, da $b^2 > 0$, dass

$$b^2 = -\frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2}, \quad \text{und} \quad a^2 = x + b^2 = \frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2}.$$

Wähle a und b als Wurzeln mit $a, b \geq 0$ falls $y \geq 0$ und $a \geq 0$, $b < 0$ falls $y < 0$. Dann erfüllen a und b die Gleichungen.

(ii) Folgt aus (i) und der p-q-Formel.

(iii) Ist klar. □

Erinnerung V.7.3: Seien p eine Primzahl und G eine Gruppe mit $\#(G) = p^k$. Dann gibt es für jedes $\ell \in \{0, \ldots, k\}$ eine Untergruppe $H \subseteq G$ mit $\#(H) = p^\ell$.

Beweis (von Satz V.7.1): Sei $\mathbb{C} \subseteq L$ eine endliche Körpererweiterung. Wir wollen zeigen, dass $L = \mathbb{C}$. Wir betrachten den Körperturm $\mathbb{R} \subseteq \mathbb{C} \subseteq L \subseteq \hat{L}$, wobei $\hat{L}$ die normale Hülle vpn L über $\mathbb{R}$ bezeichne.

Sei $G = \mathrm{Gal}(\hat{L}|\mathbb{R})$. Beachte, dass $\#(G) = [\hat{L} : \mathbb{R}]$ eine grade Zahl ist.

Im ersten Schritt wollen wir zeigen, dass G eine 2-Gruppe ist, d. h. es gibt eine natürliche Zahl k, sodass $\#(G) = 2^k$. Da $\#(G)$ eine gerade Zahl ist, gibt es eine ungerade natürliche Zahl m und eine natürliche Zahl k, sodass $\#(G) = 2^k m$. Weiter sei H die 2-Sylow-Gruppe in G, d. h. $\#(H) = 2^k$. Nach dem Hauptsatz der Galois-Theorie gilt für den Fixkörper $\hat{L}^H$, dass $\mathrm{Gal}(L|\hat{L}^H) = H$. Wir haben also den Körperturm $\mathbb{R} \subseteq \hat{L}^H \subseteq \hat{L}$, wobei $[\hat{L}^H : \mathbb{R}] = m$ und $[L : \hat{L}^H] = 2^k$.

Wegen des Satzes vom primitiven Element ist $\hat{L}^H = \mathbb{R}(\alpha)$ mit $\alpha \in \hat{L}^H$. Das Minimalpolynom f_α hat dann Grad m, nach Eigenschaft (A) der rellen Zahlen ist $m = 1$.

Im zweiten Schritt zeigen wir, dass tatsächlich schon $k = 1$ gelten muss. Angenommen, es wäre $k \geq 2$. Sei $G' := \mathrm{Gal}(\hat{L}|\mathbb{C})$. Nach Schritt 1 wäre $\#(G') = 2^{k-1}$. Aus Erinnerung V.7.3 wüssten wir, dass G' eine Untergruppe H' mit $\#(H') = 2^{k-2}$ hätte. Wir erhielten also die Körperkette $\mathbb{C} \subseteq \hat{L}^{H'} \subseteq \hat{L}$ mit $[\hat{L}^{H'} : \mathbb{C}] = 2$ und $[\hat{L} : \hat{L}^{H'}] = 2^{k-2}$. Aber das stünde im Widerspruch zu Bemerkung V.7.2(iii). □

Kapitel VI.

Ausblick

1. Inverses Galois-Problem

Welche endlichen Gruppen lassen sich als Galois-Gruppe von einer Körpererweiterung $\mathbb{Q} \subseteq L$ auftreten?

Proposition VI.1.1 (zyklische Gruppen): *Jede endliche zyklische Gruppe lässt sich als Galois-Gruppe einer Körpererweiterung von $\mathbb{Q}$ realisieren.*

Beweis: Sei n eine natürliche Zahl. Wähle eine Primzahl p mit $p \equiv 1 \pmod{n}$.[1] Weiter seien ζ_p eine primitive p-te Einheitswurzel und $L = \mathbb{Q}(\zeta_p)$. Die Galois-Gruppe G der Erweiterung $\mathbb{Q} \subseteq L$ ist isomorph zu $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Da $p-1$ von n geteilt wird, finden wir in der Galois-Gruppe eine Untergruppe H der Ordnung $(p-1)/n$ und wir erhalten die Körperkette

$$\mathbb{Q} \overset{n}{\hookrightarrow} E := L^H \overset{(p-1)/n}{\hookrightarrow} L$$

Da H normal in G ist, ist $\mathbb{Q} \subseteq E$ eine normale Körpererweiterung mit Galois-Gruppe $\mathrm{Gal}(E|\mathbb{Q}) \cong G/H$. Diese ist deshalb zyklisch und von Ordnung n. $\square$

Ähnlich wie in Proposition IV.6.1 lässt sich jede endliche abelsche Gruppe als Galois-Gruppe einer Körpererweiterung von $\mathbb{Q}$ realisieren.

Hilberts Irreduzibelitäts-Theorem von 1892 liefert, dass sich Galois-Gruppen von endlichen Körpererweiterungen von $\mathbb{Q}(T)$ auch als Galois-Gruppen von Körpererweiterungen von $\mathbb{Q}$ realisieren lassen. Als Spezialfall fällt aus dieser

[1] Das geht nach dem Dirichlet'schen Satz, zum Beispiel enthalten im Stoff der Anschlussveranstaltung „Algebraische Zahlentheorie“. Allgemeiner sagt der Dirichletsche Satz: Sind a, d natürliche Zahlen mit $\mathrm{ggT}(a,d) = 1$, dann enthält $\{a + kd \mid k \in \mathbb{N}\}$ unendliche viele Primzahlen.

Aussage heraus, dass sich für jede natürliche Zahl n die Gruppen S_n und A_n als Galois-Gruppen von Körpererweiterungen von $\mathbb{Q}$ realisieren lassen.

Schulz und Rechhardt haben 1937 gezeigt, dass alle p-Gruppen, p eine ungerade Primzahl, als Galois-Gruppen von Körpererweiterungen von $\mathbb{Q}$ auftreten.

Verbessert wurde dieses Resultat 1989 von Shafarevich, der gezeigt hat, dass jede auflösbare Gruppe als Galois-Gruppe einer Körpererweiterung von $\mathbb{Q}$ auftritt.

Es ist ein offenes Problem, ob jede endliche Gruppe als Galois-Gruppe einer Körpererweiterung von $\mathbb{Q}$ realisiert wird. Man kennt konkrete Gruppen, von denen man nicht weiß, ob sie als eine solche Galois-Gruppe auftreten, so zum Beispiel die sporadische Gruppe M_{23} (die Matthieu-Gruppe). Die Ordnung der Matthieu-Gruppe ist 10 200 960.

$$s = (1\,2)(3\,4)(5\,6)\cdots(21\,22)(23\,34), \qquad t = (2\,23\,3)(4\,5\,7)(9\,8\,24)\ldots$$

Dann sind $M_{24} = \langle s, t\rangle \subseteq S_{24}$ und M_{23} ist der Stabilisator eines Elementes der Menge $\{1, \ldots, 24\}$ unter der Operation von M_{24} auf dieser.