

# Teil I

## Grundlagen

# Kapitel 1

## Grundlagen Kategorientheorie

### 1.1 Kategorien und Morphismen

**Definition 1.1.1** (Kategorie). Eine Kategorie  $\mathcal{C}$  besteht aus den folgenden Daten:

1. Eine Klasse von Objekten  $\text{Ob}(\mathcal{C})$ .
2. Für alle  $x, y \in \text{Ob}(\mathcal{C})$  eine Klasse von Morphismen  $\text{Mor}_{\mathcal{C}}(x, y)$ .
3. Für alle  $x \in \text{Ob}(\mathcal{C})$  einen Identitätsmorphismus  $\text{id}_x \in \text{Mor}_{\mathcal{C}}(x, x)$ .
4. Für alle  $x, y, z \in \text{Ob}(\mathcal{C})$  eine Verkettungsabbildung

$$\text{Mor}_{\mathcal{C}}(y, z) \times \text{Mor}_{\mathcal{C}}(x, y) \rightarrow \text{Mor}_{\mathcal{C}}(x, z), (g, f) \mapsto g \circ f.$$

Dabei fordern wir, dass folgende Bedingungen erfüllt sind:

1. Für alle  $f \in \text{Mor}_{\mathcal{C}}(x, y)$  ist  $f \circ \text{id}_x = f = \text{id}_y \circ f$ .
2. Für alle  $f \in \text{Mor}_{\mathcal{C}}(w, x), g \in \text{Mor}_{\mathcal{C}}(x, y)$  und  $h \in \text{Mor}_{\mathcal{C}}(y, z)$  ist

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Wir nennen eine Kategorie  $\mathcal{C}$  lokal klein, falls für alle  $x, y \in \text{Ob}(\mathcal{C})$  die Klasse  $\text{Mor}_{\mathcal{C}}(x, y)$  eine Menge ist, und klein, falls zusätzlich auch die Klasse  $\text{Ob}(\mathcal{C})$  eine Menge ist.

**Definition 1.1.2** (Mono-,Epi-,Isomorphismus). Sei  $f: x \rightarrow y$  ein Morphismus in einer Kategorie  $\mathcal{C}$ .

1. Wir sagen  $f$  ist ein Monomorphismus, falls für alle  $z \in \mathcal{C}$  die Abbildung

$$f_*: \text{Mor}_{\mathcal{C}}(z, x) \rightarrow \text{Mor}_{\mathcal{C}}(z, y), g \mapsto f \circ g$$

injektiv ist. Dual dazu sagen wir  $f$  ist ein Epimorphismus, falls für alle  $z \in \mathcal{C}$  die Abbildung

$$f^*: \text{Mor}_{\mathcal{C}}(y, z) \rightarrow \text{Mor}_{\mathcal{C}}(x, z), g \mapsto g \circ f$$

injektiv ist.

2. Wir sagen  $f$  ist ein spaltender Monomorphismus, falls es einen Morphismus  $g: y \rightarrow x$  gibt mit  $g \circ f = \text{id}_x$ . Wir nennen dann  $g$  eine Retraktion von  $f$ .  
Dual dazu sagen wir  $f$  ist ein spaltender Epimorphismus falls es einen Morphismus  $g: y \rightarrow x$  mit  $f \circ g = \text{id}_y$ . Wir nennen dann  $g$  einen Schnitt von  $f$ .
3. Wir sagen  $f$  ist ein Isomorphismus falls es einen Morphismus  $f': y \rightarrow x$  gibt der gleichzeitig Retraktion und Schnitt von  $f$  ist. So ein  $f'$  ist dann eindeutig und wir schreiben  $f^{-1} = f'$ .

**Lemma 1.1.3.** Sei  $f: x \rightarrow y$  ein Morphismus in einer Kategorie  $\mathcal{C}$ . Dann sind die folgenden Bedingungen äquivalent:

1.  $f$  ist ein Isomorphismus.

2.  $f$  ist sowohl ein Monomorphismus als auch ein spaltender Epimorphismus.
3.  $f$  ist sowohl ein Epimorphismus als auch ein spaltender Monomorphismus.
4. Für alle  $z \in \mathcal{C}$  ist die Abbildung  $f_*: \text{Mor}_{\mathcal{C}}(z, x) \rightarrow \text{Mor}_{\mathcal{C}}(z, y)$  bijektiv.
5. Für alle  $z \in \mathcal{C}$  ist die Abbildung  $f^*: \text{Mor}_{\mathcal{C}}(y, z) \rightarrow \text{Mor}_{\mathcal{C}}(x, z)$  bijektiv.

*Beweis.* Gelte 1). Dann ist für alle  $z \in \mathcal{C}$ :

$$f_*^{-1} f_* = (f^{-1} f)_* = \text{id}_{\text{Mor}_{\mathcal{C}}(z, x)}$$

also ist  $f_*$  injektiv und damit ist  $f$  ein Monomorphismus. Also gilt 2).

Gelte 2). Dann sei  $g: y \rightarrow x$  ein Schnitt. Es gilt für  $z = x$  dass  $f_*(\text{id}_x) = f = f \circ g \circ f = f_*(g \circ f)$  also ist  $\text{id}_x = g \circ f$ . Damit gilt 1). Gelte 1). Dann ist für Retraction und Schnitt  $g: y \rightarrow x$  und alle  $z \in \mathcal{C}$ :  $\text{id} = (\text{id}_x)_* = (g \circ f)_* = g_* \circ f_*$  und analog  $\text{id} = f_* \circ g_*$ . Also ist  $f_*$  injektiv und surjektiv. Also gilt 4). Gelte 4). Dann ist  $f$  ein Monomorphismus. Zu  $z = y$  gibt es  $g: y \rightarrow x$  mit  $f_*(g) = \text{id}_y$  also  $f \circ g = \text{id}_y$ . Dann ist  $g$  ein Schnitt und es gilt 2). Das zeigt  $1) \iff 2) \iff 4)$ . Analog zeigt man  $1) \iff 3) \iff 5)$ .  $\square$

## 1.2 Funktoren

**Definition 1.2.1** (Funktork). Seien  $\mathcal{C}$  und  $\mathcal{D}$  Kategorien. Ein Funktor  $F: \mathcal{C} \rightarrow \mathcal{D}$  besteht aus folgenden Daten:

1. Eine Abbildung

$$\text{Ob}(\mathcal{C}) \rightarrow \text{Ob}(\mathcal{D}), x \mapsto F(x).$$

2. Für alle Objekte  $x, y \in \mathcal{C}$  eine Abbildung

$$\text{Mor}_{\mathcal{C}}(x, y) \rightarrow \text{Mor}_{\mathcal{D}}(F(x), F(y)), f \mapsto F(f).$$

Dabei fordern wir, dass die folgenden Bedingungen erfüllt sind:

1. Für alle  $x \in \mathcal{C}$  ist  $F(\text{id}_x) = \text{id}_{F(x)}$ .
2. Für alle  $f: x \rightarrow y$  und  $g: y \rightarrow z$  in  $\mathcal{C}$  ist  $F(g \circ f) = F(g) \circ F(f)$ .

Ein Funktor  $F: \mathcal{C} \rightarrow \mathcal{D}$  ist *treu* (bzw. *volltreu*), falls für alle  $x, y \in \mathcal{C}$  die Abbildung

$$F: \text{Mor}_{\mathcal{C}}(x, y) \rightarrow \text{Mor}_{\mathcal{D}}(F(x), F(y))$$

injektiv (bzw. bijektiv) ist.

**Bemerkung 1.2.2.** Sei  $F: \mathcal{C} \rightarrow \mathcal{D}$  ein treuer Funktor. Dann reflektiert  $F$  Mono- und Epimorphismen. Wenn  $F$  volltreu ist, dann reflektiert  $F$  auch spaltende Mono- und Epimorphismen.

**Definition 1.2.3.** Sei  $\text{Cat}$  die Kategorie deren Objekte kleine Kategorien  $\mathcal{C}$  sind mit Morphismen sind die Funktoren.

**Definition 1.2.4.** Sei  $I$  eine partiell geordnete Menge (zB.  $[n] = \text{Set}0, 1, \dots, n$ ). Dann definiere eine Kategorie  $NP$  durch

$$\text{Ob}(NP) = P \text{ und } \text{Mor}_{NP}(p, q) = \begin{cases} \{*\} & \text{falls } p \leq q \\ \emptyset & \text{sonst.} \end{cases}$$

Das gibt einen volltreuen Funktor  $N: \text{CatOrd} \rightarrow \text{Cat}$

### 1.3 Natürliche Transformationen

**Definition 1.3.1.** Seien  $F, G: \mathcal{C} \rightarrow \mathcal{D}$  Funktoren zwischen Kategorien. Eine natürliche Transformation  $\tau: F \rightarrow G$  besteht aus den folgenden Daten:

1. Für alle  $x \in \mathcal{C}$  ein Morphismus  $\tau_x: F(x) \rightarrow G(x)$  in  $\mathcal{D}$ .

Dabei fordern wir, dass folgende Bedingung erfüllt ist:

1. Für alle Morphismen  $f: x \rightarrow y$  in  $\mathcal{C}$  kommutiert das Diagramm
 
$$\begin{array}{ccc} F(x) & \xrightarrow{\tau_x} & G(x) \\ \downarrow F(f) & & \downarrow G(f) \\ F(y) & \xrightarrow{\tau_y} & G(y) \end{array}$$
 Wir

schreiben  $\text{Nat}(F, G)$  für die Klasse der natürlichen Transformationen  $\tau: F \rightarrow G$ .

**Definition 1.3.2** (Funktorkategorie). Seien  $\mathcal{C}$  und  $\mathcal{D}$  Kategorien. Dann definieren wir die Funktorkategorie  $\text{Fun}(\mathcal{C}, \mathcal{D})$  wie folgt

1. Die Objekte sind Funktoren  $F: \mathcal{C} \rightarrow \mathcal{D}$ .
2. Morphismen  $\tau: F \rightarrow G$  sind natürliche Transformationen mit Verkettung  $(\nu \circ \tau)_x = \nu_x \circ \tau_x$  für  $x \in \mathcal{C}$ .

**Lemma 1.3.3.** Sei  $\mathcal{C}$  eine kleine und  $\mathcal{D}$  eine lokal kleine Kategorie. Dann ist  $\text{Fun}(\mathcal{C}, \mathcal{D})$  wieder lokal klein.

*Beweis.* Seien  $F, G: \mathcal{C} \rightarrow \mathcal{D}$  Funktoren. Dann ist

$$\text{Nat}(F, G) \subseteq \prod_{x \in \mathcal{C}} \text{Mor}_{\mathcal{D}}(F(x), G(x))$$

und das letzte ist eine Menge. □

**Lemma 1.3.4.** Eine natürliche Transformation  $\tau: F \rightarrow G$  ist natürlicher Isomorphismus, wenn  $\tau_x$  ein Isomorphismus für alle  $x \in \mathcal{C}$  ist.

*Beweis.* Behauptung:  $(\tau_x^{-1})_x$  ist eine natürliche Transformation. Sei  $f: x \rightarrow y$  ein Morphismus. Dann ist

$$\begin{aligned} \tau_y^{-1} \circ G(f) &= \tau_y^{-1} \circ (G(f) \circ \tau_x) \circ \tau_x^{-1} \\ &= \tau_y^{-1} \circ (\tau_y \circ F(f)) \circ \tau_x^{-1} \\ &= F(f) \circ \tau_x^{-1} \end{aligned}$$

□

**Satz 1.3.5.** Sei  $i: \mathcal{D}' \rightarrow \mathcal{D}$  ein volltreuer Funktor und  $F: \mathcal{C} \rightarrow \mathcal{D}$  ein Funktor mit  $\text{im}(F) \subseteq \text{im}(i)$ . Dann existiert ein Paar  $(F', \kappa)$  bestehend aus einem Funktor  $F': \mathcal{C} \rightarrow \mathcal{D}'$  und einen natürlichen Isomorphismus  $\kappa: i \circ F' \cong F$ . Weiter gibt es für zwei solcher Paare  $(F'_1, \kappa_1)$  und  $(F'_2, \kappa_2)$  einen eindeutigen natürlichen Isomorphismus  $\nu: F'_1 \cong F'_2$  sodass  $\kappa_2 \circ i(\nu) = \kappa_1$ , das heißt das Paar  $(F', \kappa)$  ist eindeutig bis auf eindeutigen Isomorphismus.

**Lemma 1.3.6.** Seien  $\mathcal{C}, \mathcal{D}$  und  $\mathcal{E}$  Kategorien. Dann gibt es einen natürlichen Isomorphismus von Kategorien

$$\text{Fun}(\mathcal{C} \times \mathcal{D}, \mathcal{E}) \cong \text{Fun}(\mathcal{C}, \text{Fun}(\mathcal{D}, \mathcal{E})).$$

*Beweis.* Klar. □

**Definition 1.3.7** (Kategorienäquivalenz). Sei  $F: \mathcal{C} \rightarrow \mathcal{D}$  ein Funktor. Ein Quasiinverses zu  $F$  ist ein Funktor  $G: \mathcal{D} \rightarrow \mathcal{C}$  zusammen mit natürlichen Isomorphismen  $\alpha: G \circ F \cong \text{id}_{\mathcal{C}}$  und  $\beta: F \circ G \cong \text{id}_{\mathcal{D}}$  sodass

$$F(\alpha) = \beta_F: FGF \cong F \text{ und } G(\beta) = \alpha_G: GFG \cong G.$$

Falls ein Quasiinverses existiert dann nennen wir  $F$  eine Kategorienäquivalenz.

**Satz 1.3.8.** Für einen Funktor  $F: \mathcal{C} \rightarrow \mathcal{D}$  sind die folgenden Bedingungen äquivalent:

1.  $F$  ist eine Kategorienäquivalenz.
2. Es existiert ein Funktor  $G: \mathcal{D} \rightarrow \mathcal{C}$  mit natürlichen Isomorphismen  $\alpha: G \circ F \cong \text{id}_{\mathcal{C}}$  und  $\beta: F \circ G \cong \text{id}_{\mathcal{D}}$ .
3.  $F$  ist volltreu und essentiell surjektiv.

Außerdem ist ein Quasiinverses zu  $F$  eindeutig bis auf eindeutigen Isomorphismus.

*Beweis.* 1) nach 2) ist klar. Gelte 2). Für  $y \in \mathcal{D}$  ist  $\beta_y^{-1}: y \cong F(G(y))$  also ist  $F$  essentiell surjektiv. Außerdem sind für  $x, y \in \mathcal{C}$  die Diagramme

$$\begin{array}{ccccc} \text{Mor}_{\mathcal{C}}(x, y) & \xrightarrow{F} & \text{Mor}_{\mathcal{D}}(F(x), F(y)) & \xrightarrow{G} & \text{Mor}_{\mathcal{C}}(GF(x), GF(y)) \\ & & & & \downarrow \alpha_y \circ (-) \circ \alpha_x^{-1} \\ & & & & \text{Mor}_{\mathcal{C}}(x, y) \end{array}$$

□

**Bemerkung 1.3.9.** Sei  $F: \mathcal{C} \rightarrow \mathcal{D}$  ein Funktor. Dann ist äquivalent

1.  $F$  ist Kategorienäquivalenz
2. Für alle Kategorien  $\mathcal{E}$  ist  $F_*: \text{Fun}(\mathcal{E}, \mathcal{C}) \rightarrow \text{Fun}(\mathcal{E}, \mathcal{D})$  eine Kategorienäquivalenz
3. Für alle Kategorien  $\mathcal{E}$  ist  $F^*: \text{Fun}(\mathcal{D}, \mathcal{E}) \rightarrow \text{Fun}(\mathcal{C}, \mathcal{E})$  eine Kategorienäquivalenz

## 1.4 Yoneda Lemma

**Satz 1.4.1** (Yoneda Lemma). Sei  $\mathcal{C}$  eine lokal kleine Kategorie. Sei  $F: \mathcal{C}^{\text{op}} \rightarrow \text{Set}$  ein Funktor und  $x \in \mathcal{C}$ . Dann ist die Abbildung

$$\text{Nat}(\text{Mor}_{\mathcal{C}}(-, x), F) \rightarrow F(x), \tau \mapsto \tau_x(\text{id}_x)$$

bijektiv.

*Beweis.* Für  $s \in F(x)$  definiere  $\tau^{(s)}: \text{Mor}_{\mathcal{C}}(-, x) \rightarrow F$  durch

$$\tau_y^{(s)}: \text{Mor}_{\mathcal{C}}(y, x) \rightarrow F(y), f \mapsto F(f)(s)$$

für  $y \in \mathcal{C}$ .

Es gilt  $\tau_x^{(s)}(\text{id}_x) = s$  und  $\tau_y^{(\tau_x(\text{id}_x))}(f) = \tau_y(f)$ . Also gilt die Aussage. □

**Korollar 1.4.2** (Yoneda-Einbettung). Sei  $\mathcal{C}$  eine lokal kleine Kategorie. Dann ist der Funktor

$$Y_{\mathcal{C}}: \mathcal{C} \rightarrow \text{Fun}(\mathcal{C}^{\text{op}}, \text{Set}), x \mapsto \text{Mor}_{\mathcal{C}}(-, x)$$

volltreu.

*Beweis.* Seien  $x, y \in \mathcal{C}$ . Zeige

$$\text{Mor}_{\mathcal{C}}(x, y) \rightarrow \text{Nat}(\text{Mor}_{\mathcal{C}}(-, x), \text{Mor}_{\mathcal{C}}(-, y)), f \mapsto f_*$$

ist eine Bijektion. Das ist aber genau die Inverse Abbildung aus dem [Yoneda Lemma](#) für den Funktor  $F = \text{Mor}_{\mathcal{C}}(-, y)$ . □

**Bemerkung 1.4.3.** Es gibt eine duale Version vom Yoneda Lemma. Sei  $\mathcal{C}$  eine lokal kleine Kategorie und  $F: \mathcal{C} \rightarrow \text{Set}$  ein Funktor und  $x \in \mathcal{C}$ . Dann ist die Abbildung

$$\text{Nat}(\text{Mor}_{\mathcal{C}}(x, -), F) \rightarrow F(x), \tau \mapsto \tau_x(\text{id}_x)$$

bijektiv. Dann ist die duale Yoneda Einbettung  $Y^{\mathcal{C}}: \mathcal{C}^{\text{op}} \rightarrow \text{Fun}(\mathcal{C}, \text{Set}), x \mapsto \text{Mor}_{\mathcal{C}}(x, -)$  volltreu.

**Definition 1.4.4.** Sei  $\mathcal{C}$  eine lokal kleine Kategorie. Ein Funktor  $F: \mathcal{C}^{\text{op}} \rightarrow \text{Set}$  heißt darstellbar falls er im essentiellen Bild der Yoneda Einbettung liegt. Analog heißt ein Funktor  $F: \mathcal{C} \rightarrow \text{Set}$  kodarstellbar, wenn er im essentiellen Bild von  $Y^{\mathcal{C}}$  liegt.

## 1.5 Adjunktionen

**Definition 1.5.1** (Adjungiertes Objekt). Sei  $G: \mathcal{D} \rightarrow \mathcal{C}$  ein Funktor und  $x \in \mathcal{C}$ . Ein unter  $G$  zu  $x$  linksadjungiertes Objekt ist ein Objekt  $y \in \mathcal{D}$  zusammen mit einem Morphismus  $\eta: x \rightarrow G(y)$  sodass für alle  $y' \in \mathcal{D}$  die Abbildung

$$\text{Mor}_{\mathcal{D}}(y, y') \rightarrow \text{Mor}_{\mathcal{C}}(x, G(y')), f \mapsto G(f) \circ \eta$$

bijektiv ist.

**Bemerkung 1.5.2.** sei  $G: \mathcal{D} \rightarrow \mathcal{C}$  ein Funktor sodass  $\mathcal{C}, \mathcal{D}$  lokal kleine Kategorien sind. Dann ist ein zu  $x$  linksadjungiertes Objekt das gleiche wie ein kodarstellendes Objekt für den Funktor

$$\text{Mor}_{\mathcal{C}}(x, G(-)): \mathcal{D} \rightarrow \text{Set}$$

**Satz 1.5.3** (Adjungierter Funktor). Sei  $G: \mathcal{D} \rightarrow \mathcal{C}$  ein Funktor und sei  $i: \mathcal{C}' \subseteq \mathcal{C}$  eine volle Unterkategorie, sodass alle Objekte in  $\mathcal{C}'$  unter  $G$  ein linksadjungiertes Objekt besitzen. Dann existiert ein Funktor  $F: \mathcal{C}' \rightarrow \mathcal{D}$  und eine natürliche Transformation  $\eta: i \rightarrow G \circ F$  sodass  $(F(x)\eta_x)$  für jedes  $x \in \mathcal{C}$  ein unter  $G$  zu  $x$  linksadjungiertes Objekt ist. Das Paar  $(F, \eta)$  ist eindeutig bis auf eindeutigen Isomorphismus. Wir nennen  $F$ , zusammen mit der natürlichen Transformation, einen partiellen links adjungierten Funktor zu  $G$ . Wenn  $\mathcal{C} = \mathcal{C}'$  dann nennen wir  $F: \mathcal{C} \rightarrow \mathcal{D}$  auch einfach einen linksadjungierten Funktor zu  $G$ .

*Beweis.* Wähle ein linksadjungiertes Objekt  $(F(x), \eta_x)$  für jedes  $x \in \mathcal{C}$ . Für einen Morphismus  $f: x \rightarrow y$  in  $\mathcal{C}$  definiere  $F(f): F(x) \rightarrow F(y)$  als das eindeutige Urbild von  $\eta_y \circ f$  unter der bijektiven Abbildung

$$\text{Mor}_{\mathcal{D}}(F(x), F(y)) \rightarrow \text{Mor}_{\mathcal{C}}(x, G(F(y))), g \mapsto G(g) \circ \eta_x;$$

wir haben also  $G(F(f)) \circ \eta_x = \eta_y \circ f$ . Wir behaupten nun noch, dass diese Daten einen Funktor  $F: \mathcal{C} \rightarrow \mathcal{D}$  definieren; danach ist es dann sofort klar, dass die  $\eta_x$  eine natürliche Transformation  $\eta: i \rightarrow G \circ F$  definieren. Für ein Objekt  $x \in \mathcal{C}'$  ist

$$G(\text{id}_{F(x)}) \circ \eta_x = \eta_x = \eta_x \circ \text{id}_x$$

und somit  $F(\text{id}_x) = \text{id}_{F(x)}$ . Weiter ist für Morphismen  $f: x \rightarrow y$  und  $g: y \rightarrow z$

$$\begin{aligned} G(F(g) \circ F(f)) \circ \eta_x &= G(F(g)) \circ G(F(f)) \circ \eta_x \\ &= G(F(g)) \circ \eta_y \circ f \\ &= \eta_z \circ g \circ f \end{aligned}$$

und somit  $F(g \circ f) = F(g) \circ F(f)$ . Die Eindeutigkeit von  $(F, \eta)$  bis auf eindeutigen Isomorphismus folgt aus der Eindeutigkeit von linksadjungierten Objekten.  $\square$

**Bemerkung 1.5.4.** Sei  $G: \mathcal{D} \rightarrow \mathcal{C}$  ein Funktor und sei  $\mathcal{C}' \subseteq \mathcal{C}$  die volle Unterkategorie der Objekte die unter  $G$  ein linksadjungiertes Objekt besitzen. Wir nehmen außerdem an, dass  $\mathcal{C}$  und  $\mathcal{D}$  lokal klein sind. Dann ist ein partieller Linksadjungierter  $F: \mathcal{C}' \rightarrow \mathcal{D}$  von  $G$  das Gleiche wie eine Faktorisierung des Funktors

$$\mathcal{C}' \rightarrow \text{Fun}(\mathcal{D}, \text{Set})^{\text{op}}, x \mapsto \text{Mor}_{\mathcal{C}}(x, G(-))$$

durch die (volltreue) duale Yoneda-Einbettung

$$Y^{\mathcal{D}, \text{op}}: \mathcal{D} \rightarrow \text{Fun}(\mathcal{D}, \text{Set})^{\text{op}}.$$

In dieser Situation ist also Satz 1.5.3 eine Folgerung aus Satz 1.3.5.

**Definition 1.5.5.** Sei  $\mathcal{C}$  eine Kategorie. Wir definieren die Pfeilkategorie von  $\mathcal{C}$  als

$$\text{Arr}(\mathcal{C}) = \text{Fun}(N[1], \mathcal{C}).$$

**Lemma 1.5.6.** Sei  $\text{codom}: \text{Arr}(\mathcal{C}) \rightarrow \mathcal{C}$  der Funktor, der  $\phi: A \rightarrow B$  auf  $B$  schickt und ein kommutatives Diagramm auf den rechten Morphismus. Dann ist  $\text{codom}$  links-adjungiert zum Funktor  $R: \mathcal{C} \rightarrow \text{Arr}(\mathcal{C}), C \mapsto (\text{id}: C \rightarrow C)$

*Beweis.* Klar  $\square$

## 1.6 Moduln

**Definition 1.6.1.** Sei  $\mathcal{C}$  eine Kategorie mit Pullbacks und sei  $A \in \mathcal{C}$ . Ein Modul ist ein abelsches Gruppenobjekt in der Slice Kategorie  $\mathcal{C}_{/A}$ .

## 1.7 Mengen

**Lemma 1.7.1** (Zornsches Lemma). *Sei  $M$  eine partiell geordnete Menge, sodass jede total geordnete Teilmenge von  $M$  eine obere Schranke in  $M$  hat. Dann hat  $M$  ein maximales Element.*

# Kapitel 2

## Gruppentheorie

### 2.1 Grundlagen und Satz von Lagrange

**Satz 2.1.1** (Gruppenordnung). *Sei  $G$  eine Gruppe und  $H \subseteq G$  eine Untergruppe. Dann ist*

$$|G| = |H| \cdot [G : H]$$

*Beweis.* Es ist  $[G : H] = |G/H| = \{aH \mid a \in G\}$  und

$$G = \bigcup_{aH \in G/H} aH$$

disjunkte Vereinigung, denn wenn  $g \in G$  dann ist  $g \in gH$  und  $aH \cap bH = \emptyset \iff aH = bH$ . Es ist  $|H| \neq |aH|$  für alle  $a \in G$ .  $\square$

**Korollar 2.1.2** (Satz von Lagrange). *Es gilt  $|H| \mid |G|$ .*

**Korollar 2.1.3.** *Für  $a \in G$  ist  $\text{ord}(a) \mid |G|$ . Also  $a^{|G|} = e$ .*

**Korollar 2.1.4.** *Sei  $p$  eine Primzahl und  $a \in \mathbb{Z}$  sodass  $p \nmid a$ . Dann ist  $a^{p-1} \equiv 1 \pmod{p}$ .*

*Beweis.* Sei  $G = \mathbb{F}_p^*$ . Dann ist  $|G| = p - 1$  also gilt  $a^{p-1} = 1$ .  $\square$

### 2.2 Gruppenwirkung

**Definition 2.2.1.** Sei  $G$  eine Gruppe,  $X$  eine Menge und  $G \times X \rightarrow X$  eine Gruppenwirkung.

1. Für  $x \in X$  ist  $Gx = \{ax \mid a \in G\}$  die Bahn von  $x$ .
2. Für  $x \in X$  ist  $\text{Stab}_G(x) = G_x = \{a \in G \mid ax = x\}$  der Stabilisator von  $x$ .
3. Die Wirkung heißt transitiv, wenn  $X = Gx$  für ein  $x \in X$  ist.
4.  $x \in X$  heißt Fixpunkt der Wirkung, wenn  $\text{Stab}_G(x) = G$  ist.
5.  $X^G$  sei die Menge der Fixpunkte von  $G$  auf  $X$ .
6. Die Operation heißt treu, wenn der Homomorphismus  $G \rightarrow S(X)$  injektiv ist.

**Bemerkung 2.2.2.** Sei  $G \times X \rightarrow X$  eine Gruppenwirkung. Dann ist  $X = \bigsqcup_{i \in I} Gx_i$  für  $x_i$  ein Vertretersystem aller Bahnen.

**Lemma 2.2.3.** *Für  $x \in X$  gibt es eine natürliche Bijektion*

$$G/\text{Stab}_G(x) \rightarrow Gx, a\text{Stab}_G(x) \mapsto ax$$

*Beweis.* Man prüft, dass das wohldefiniert ist. Die Abbildung ist surjektiv nach Definition und wenn  $ax = bx$  ist, dann ist  $a^{-1}b \in \text{Stab}_G(x)$  also  $a\text{Stab}_G(x) = b\text{Stab}_G(x)$ .  $\square$



**Korollar 2.2.4.** Sei  $G \times X \rightarrow X$  eine Gruppenwirkung. Dann ist

$$|Gx| = [G : \text{Stab}_G(X)].$$

**Satz 2.2.5** (Bahnengleichung). Sei  $G \times X \rightarrow X$  eine Gruppenwirkung wobei  $X$  eine endliche Menge ist. Seien  $x_1, \dots, x_r$  Vertreter der Bahnen. Dann ist

$$|X| = \sum_{i=1}^r [G : \text{Stab}_G(X_i)].$$

*Beweis.* Da  $X = \coprod_{i=1}^r Gx_i$  eine disjunkte Vereinigung ist, folgt

$$|X| = \sum_{i=1}^r |Gx_i| = \sum_{i=1}^r [G : \text{Stab}_G(x_i)].$$

□

**Definition 2.2.6.** Sei  $G$  eine Gruppe. Dann ist das Zentrum von  $G$  definiert als

$$Z(G) = \{a \in G \mid ab = ba \ \forall b \in G\}.$$

Das ist ein abelscher Normalteiler.  $Z(G)$  sind Fixpunkte der Operation

$$G \times G \rightarrow G, (a, b) \mapsto aba^{-1}.$$

**Definition 2.2.7.** Der Zentralisator von  $a \in G$  ist

$$C_G(a) = \{b \in G \mid ba = ab\}.$$

Das ist eine Untergruppe von  $G$  und  $a \in Z(C_G(a))$ . Es ist  $a \in Z(G)$  genau dann wenn  $C_G(a) = G$ . Es ist  $C_G(a) = \text{Stab}_G(a)$  für die Wirkung  $G \times G \rightarrow G, (a, b) \mapsto aba^{-1}$

**Satz 2.2.8** (Klassengleichung). Sei  $G$  eine endliche Gruppe und  $a_1, \dots, a_r$  Vertreter der Konjugationsklassen von nicht-zentralen Elementen. Dann ist

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(a_i)]$$

*Beweis.* Das ist die [Bahnengleichung](#) für die Wirkung  $G \times G \rightarrow G, (a, b) \mapsto aba^{-1}$ , denn wenn  $x_i$  ein Vertreter einer Bahn mit zentralen Element, dann ist  $\text{Stab}_G(x_i) = C_G(x_i) = G$  □

**Definition 2.2.9.** Sei  $p$  eine Primzahl. Eine  $p$ -Gruppe ist eine Gruppe  $G$  mit  $|G| = p^r$  für  $r \geq 0$ .

**Satz 2.2.10.** Sei  $G \times X \rightarrow X$  eine Wirkung einer  $p$ -Gruppe auf eine endliche Menge  $X$ . Dann ist

$$|X| \equiv |X^G| \pmod{p}.$$

*Beweis.* Nach Satz [2.2.5](#) ist

$$|X| = |X^G| + \sum_{i=1}^r [G : \text{Stab}_G(x_i)]$$

wobei  $x_i$  Vertreter von Bahnen mit mindestens zwei Elementen sind. Da  $G$  eine  $p$ -Gruppe ist, gilt  $p \mid [G : \text{Stab}_G(x_i)] = |X| - |X^G|$ . □

**Satz 2.2.11.** Eine nicht-triviale  $p$ -Gruppe  $G$  hat ein nicht-triviales Zentrum.

*Beweis.* Betrachte Wirkung  $G \times G \rightarrow G, (a, b) \mapsto aba^{-1}$ . Nach Satz [2.2.10](#) gilt  $|G| = |Z(G)| \pmod{p}$ . Also  $|Z(G)| \geq p$ . □

## 2.3 Sylowsätze

Sei  $G$  eine endliche Gruppe und  $p$  eine Primzahl.

**Definition 2.3.1.** Eine  $p$ -Sylowgruppe von  $G$  ist eine  $p$ -Gruppe  $P \subseteq G$  mit  $p \nmid [G : P]$ . Das heißt wenn  $|G| = p^r \cdot m$  mit  $p \nmid m$  dann ist  $P \subseteq G$  eine  $p$ -Sylowgruppe von  $G$  genau dann wenn  $|P| = p^r$ .

**Lemma 2.3.2.** Sei  $G$  eine endliche Gruppe und  $p$  eine Primzahl mit  $p \mid |G|$ . Dann gibt es ein  $a \in G$  mit  $\text{ord}(a) = p$ .

*Beweis.*  $\mathbb{Z}/p\mathbb{Z}$  operiert auf der Menge  $M = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdot g_2 \cdots g_p = e\}$  durch

$$k \cdot (g_1, \dots, g_p) = (g_{1+k \bmod p}, \dots, g_{p+k \bmod p})$$

. Es ist  $|M| = |G|^{p-1}$ . Nach Satz 2.2.10 ist

$$0 \equiv |G|^{p-1} \equiv |M^{\mathbb{Z}/p\mathbb{Z}}| \pmod{p}$$

. Das heißt es gibt Fixpunkt  $(g_1, \dots, g_p)$  wobei  $g_i \neq e$ . Dann ist aber  $g_i = g_j$  für alle  $i, j$  also ist dieses Tupel  $(g, \dots, g)$  für ein  $g \in G$ . Dann ist  $g^p = e$ .  $\square$

**Korollar 2.3.3.** Sei  $G$  eine  $p$ -Gruppe,  $|G| = p^n$ . Dann gibt es für jedes  $k \leq n$  eine normale Untergruppe  $H \subseteq G$  der Ordnung  $p^k$ .

*Beweis.* Da  $|Z(G)| \mid p^n$  und  $Z(G)$  nach Satz 2.2.11 nicht trivial ist, gibt es nach Lemma 2.3.2 ein  $a \in Z(G)$  von der Ordnung  $p$ . Wenn  $k = 1$  dann ist  $N = \langle a \rangle$  die Lösung denn  $N$  ist normal. Wenn  $k > 1$  ist, dann hat  $G/N$  hat Ordnung  $p^{n-1}$ . Nach Induktion hat  $\bar{G} = G/N$  eine normale Untergruppe  $\bar{H}$  der Ordnung  $p^{k-1}$ . Sei  $H = \pi^{-1}\bar{H}$  wobei  $\pi: G \rightarrow G/N$  die Projektion ist. Dann ist  $H/N \cong \bar{H}$  also ist  $H$  normal von Ordnung  $p^k$ .  $\square$

**Satz 2.3.4** (1. Sylowsatz).  $G$  hat eine  $p$ -Sylowgruppe.

*Beweis.* Sei  $|G| = p^r \cdot m$  mit  $p \nmid m$ . Sei ohne Einschränkung  $r \geq 1$ . Angenommen  $p \nmid |Z(G)|$  wobei  $Z(G)$  das Zentrum von  $G$  ist. Wähle  $a \in Z(G)$  mit  $\text{ord}(a) = p$ . Dann ist  $N = \langle a \rangle \subseteq G$  ein Normalteiler, da  $a$  zentral ist. Es ist  $|G/N| = p^{r-1} \cdot m$  und nach Induktion gibt es eine  $p$ -Sylowgruppe  $Q \subseteq G/N$ . Sei  $P = \pi^{-1}(Q)$  wobei  $\pi: G \rightarrow G/N$  die Projektion ist. Dann ist  $P/N \cong Q$  also  $|P| = p^r$ . Somit ist  $P \subseteq G$  eine  $p$ -Sylowgruppe.

Angenommen  $p \mid |Z(G)|$ . Dann gibt es die [Klassengleichung](#)

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(a_i)].$$

Also gibt es ein  $i$  sodass  $p \nmid [G : C_G(a_i)]$ . Da

$$|G| = |C_G(a_i)| \cdot [G : C_G(a_i)]$$

ist  $p^r \mid |C_G(a_i)|$ . Da  $a_i$  nicht zentral ist, ist  $C_G(a_i) \neq G$ . Nach Induktion gibt es eine  $p$ -Sylowgruppe  $P \subseteq C_G(a_i)$ .  $\square$

**Satz 2.3.5** (2. Sylowsatz). Sei  $P \subseteq G$  eine  $p$ -Sylowgruppe und  $H \subseteq G$  eine  $p$ -Gruppe. Dann gibt es ein  $a \in G$  sodass  $aHa^{-1} \subseteq P$ .

*Beweis.*  $H$  operiert auf  $G/P$  durch  $h \cdot (aP) = haP$ . Nach Satz 2.2.10 ist

$$|G/P| \equiv |(G/P)^H| \pmod{p}.$$

Also ist  $p \mid |(G/P)^H|$  und somit gibt es einen Fixpunkt  $aP$ . Das heißt  $HaP = aP$  und somit  $a^{-1}HaP = P$  also  $a^{-1}Ha \subseteq P$ .  $\square$

**Korollar 2.3.6.** Wenn  $H$  eine weitere  $p$ -Sylowgruppe ist, dann folgt  $aHa^{-1} = P$  wegen Anzahl der Elemente. somit sind alle  $p$ -Sylowgruppen konjugiert.

**Bemerkung 2.3.7.** Eine  $p$ -Sylowgruppe  $P \subseteq G$  ist normal  $\iff P$  die einzige  $p$ -Sylowgruppe ist.

**Satz 2.3.8** (3. Sylowsatz). Sei  $G = p^r \cdot m$  mit  $p \nmid m$ . Sei  $s$  die Anzahl der  $p$ -Sylowgruppen von  $G$ . Dann gilt

$$s \equiv 1 \pmod{p} \quad (2.1)$$

$$s \mid m \quad (2.2)$$

*Beweis.* Zeige 1). Sei  $P$  eine  $p$ -Sylowgruppe.  $P$  operiert auf der Menge  $X$  der  $p$ -Sylowgruppen von  $G$  durch Konjugation  $P \times X \rightarrow X, (a, Q) \mapsto aQa^{-1}$ . [Bahnengleichung](#) liefert

$$|X| = \sum_{i=1}^r [P : \text{Stab}_P(P_i)]$$

wobei  $P_i$  Verteter der Bahnen sind. Sei  $P = P_1$ . Dann ist  $[P : \text{Stab}_P(P_1)] = 1$  und für  $i \geq 2$  gilt, dass  $P_i$  normal ist in  $H_i = \{a \in G \mid aP_i a^{-1} = P_i\} = \text{Stab}_G(P_i)$ . Also ist  $P_i$  die einzige  $p$ -Sylowgruppe von  $H_i$ . Also ist  $P \subsetneq H_i$  und damit  $P \neq \text{Stab}_P(P_i)$  also  $p \mid [P : \text{Stab}_P(P_i)]$ . Damit ist

$$s = |X| = 1 + \sum_{i \geq 2}^k [P : \text{Stab}_G(P_i)] \equiv 1 \pmod{p}.$$

Zeige 2). Sei  $X$  wie oben. Wegen [2. Sylowsatz](#) operiert  $G$  transitiv auf  $X$  durch Konjugation. Sei  $H = \text{Stab}_G(P)$  der Normalisator von  $P$ . Es ist  $P \subseteq H$  und somit  $p^r \mid |H|$ . Es ist  $|H| = p^r \cdot \ell$  mit  $p \nmid \ell$ . Nach [2.1.3](#) ist dann  $s = |X| = \text{Bahn}(P) = |G|/|H| = \frac{m}{\ell}$ . Also ist  $s$  ein Teiler von  $m$ .  $\square$

**Satz 2.3.9.** Seien  $p, q$  Primzahlen und  $p < q$  und  $p \nmid q-1$ . Dann ist jede Gruppe der Ordnung  $p \cdot q$  zyklisch.

*Beweis.* Sei  $s$  die Anzahl der  $p$ -Sylowgruppen und  $t$  die Anzahl der  $q$ -Sylowgruppen. Nach [3. Sylowsatz](#) gilt  $s = t = 1$ . Seien also  $P$  eine  $p$ -Sylowgruppe und  $Q$  eine  $q$ -Sylowgruppen. Es ist  $P \cap Q = \{e\}$  denn die Ordnung von  $P \cap Q$  teilt  $p$  und  $q$  nach [2.1.3](#). Also gilt für  $a \in P, b \in Q$  dass  $ab = ba$ , denn  $b^{-1}aba^{-1} \in P \cap Q$  wegen Normalität von  $P$  und  $Q$ . Es sind  $P, Q$  zyklisch. Seien also  $a \in P$  und  $b \in Q$  Erzeuger. Es ist

$$(ab)^n = a^n b^n = e \iff a^n = b^{-n} \iff a^n = e = b^n \iff pq \mid n$$

Also ist  $\text{ord}(ab) = pq = |G|$  und somit  $G = \langle ab \rangle$ .  $\square$

**Lemma 2.3.10.** Jede endliche abelsche Gruppe ist isomorph zum Produkt ihrer Sylowgruppen.

*Beweis.* Sei  $|G| = \prod_{i=1}^r p_i^{e_i}$  wobei  $p_i$  verschiedene Primzahlen sind und  $e_i \geq 1$ . Da  $G$  abelsch ist, sind alle Untergruppen normal somit gibt es genau eine  $p_i$ -Sylowgruppe  $P_i \subseteq G$ . Die Abbildung

$$f: \prod_{i=1}^r P_i \rightarrow G, (a_1, \dots, a_r) \mapsto a_1 \cdots a_r$$

ist Gruppenhomomorphismus. Wegen der Gruppenordnung ist  $f$  bijektiv wenn  $f$  injektiv ist. Angenommen  $a_i \in P_i$  sodass  $a_1 \cdots a_r = e$ . Es ist  $a_1 = (a_2 \cdots a_r)^{-1}$  und  $\text{ord}(a_1) = \text{ord}(a_2 \cdots a_r) \mid \prod_{i=2}^r p_i^{e_i}$ . Somit  $\text{ord}(a_1) \mid \text{ggT}(p_1^{e_1}, \prod_{i=2}^r p_i^{e_i}) = 1$ . Also  $e_1 = e$  und genauso  $a_i = e$  für alle  $i$ . Also ist  $f$  injektiv.  $\square$

## 2.4 Gruppen Strukturen

### 2.4.1 Semidirekte Produkte

**Definition 2.4.1.** Sei  $G$  eine Gruppe und  $N, H \subseteq G$  Untergruppen sodass  $N$  normal ist und  $H \cap N = \{e\}$  und  $G = NH$ . Dann heißt  $G$  das innere semidirekte Produkt von  $N$  und  $H$ .

**Bemerkung 2.4.2.** Wenn  $G$  das semidirekte Produkt von  $N$  und  $H$  ist, dann ist die Abbildung  $N \times H \rightarrow G, (n, h) \mapsto n \cdot h$  bijektiv. Das Verleiht  $N \times H$  mit der Gruppenstruktur  $(n, h) \cdot (n', h') = (n \cdot hn'h^{-1}, h \cdot h')$ . Das heißt wenn

$$\alpha: H \rightarrow \text{Aut}(N), \alpha(h) = (N \rightarrow N, n \mapsto hn'h^{-1})$$

dann ist  $(n, h) \cdot (n', h') = (n \cdot \alpha(h)(n'), hh')$

*Beweis.* Wenn  $nh = n'h'$  dann ist  $n^{-1}n = h'^{-1} \in N \cap H = \{e\}$ .  $\square$

**Definition 2.4.3.** Seien  $N, H$  Gruppen und  $\alpha: H \rightarrow \text{Aut}(N)$  ein Gruppenhomomorphismus. Definiere  $N \rtimes H = N \rtimes_{\alpha} H$  als Menge  $N \times H$  und Gruppenstruktur  $(n, h)(n', h') = (n\alpha(h)(n'), hh')$ . Das ist eine Gruppe. (Z.B. ist  $(n, h)^{-1} = (\alpha(h^{-1})(n^{-1}), h^{-1})$ ).  $N \rtimes_{\alpha} H$  heißt semidirektes Produkt von  $N$  und  $H$  bezüglich  $\alpha$ . Es ist  $N \subseteq N \rtimes H, n \mapsto (n, e)$  und  $H \subseteq N \rtimes H, h \mapsto (e, h)$ .

**Lemma 2.4.4.**  $N \subseteq N \rtimes H = G$  ist normale Untergruppe,  $G = NH$  und  $N \cap H = \{e\}$ .

*Beweis.* Es sei  $\tau = (\star, g) \in G$ . Dann ist  $\tau^{-1} = (\star, g^{-1})$ . Es ist  $\tau(n, e)\tau^{-1} = \tau \cdot (\star, g^{-1}) = (\star, e) \in N$  also ist  $N$  normal. Sei  $\tau = (n, h) \in G$ . Dann ist  $(n, e) \cdot (e, h) = \tau$ .  $\square$

**Definition 2.4.5.** Sei **GroupActions** die Kategorie mit Objekten  $(H, N, \alpha)$  wobei  $H, N$  Gruppen sind und  $\alpha: H \rightarrow \text{Aut}(N)$  ein Gruppenhomomorphismus ist. Morphismen

$$(H, N, \alpha) \rightarrow (H', N', \alpha')$$

in **GroupActions** sind  $(f_H, f_N)$  wobei  $f_H: H \rightarrow H'$  und  $f_N: N \rightarrow N'$   $H$ -equivariante Gruppenhomomorphismen sind. Das heißt  $f_N(\alpha(h)(n)) = \alpha'(f_H(h))(f_N(n))$  für alle  $h \in H$  und  $n \in N$ .

**Lemma 2.4.6.** Sei  $\text{Arr}(\text{Grp})$  die ?? von  $\text{Grp}$ . Der

$$R: \text{Arr}(\text{Grp}) \rightarrow \text{GroupActions}, (\phi: H' \rightarrow N') \mapsto (H', N', \alpha')$$

wobei  $\alpha'$  die Konjugation in  $N'$  ist, das heißt  $\alpha'(h')(n') = \phi(h')n'\phi(h')^{-1}$  für alle  $h' \in H'$  und  $n' \in N'$ .

Der Funktor

$$L: \text{GroupActions} \rightarrow \text{Arr}(\text{Grp}), (H, N, \alpha) \mapsto (H \subseteq N \rtimes_{\alpha} H)$$

ist linksadjungiert zu  $U$ .

*Beweis.* Sei

$$\begin{array}{ccc} & & N \\ & & \downarrow i_N \\ H & \xrightarrow{i_H} & N \rtimes_{\alpha} H \\ \downarrow f_H & & \downarrow f_{N \rtimes H} \\ H' & \xrightarrow{\phi} & N' \end{array}$$

ein kommutatives Diagramm von Gruppen. Definiere  $f_N = i_N \circ f_{N \rtimes H}: N \rightarrow N'$  und sei  $(H', N', \alpha') = R(\phi)$ . Dann ist

$$(f_H, f_{N \rtimes H} \circ i_N): (H, N, \alpha) \rightarrow (H', N', \alpha')$$

ein Morphismus in **GroupActions**, denn

$$\alpha'(f_H(h))(f_{N \rtimes H}(n, e)) = f_{N \rtimes H}((e, h) \cdot (n, e) \cdot (e, h)^{-1})$$

und da

$$(e, h)(n, e)(e, h)^{-1} = (\alpha(h)(n), h)(e, h^{-1}) = (\alpha(h)(n), e)$$

ist

$$\alpha'(f_H(h))(f_N(n)) = f_N(\alpha(h)(n))$$

für alle  $h \in H$  und  $N \in N$ .

Wenn andersrum  $\phi: H' \rightarrow N'$  Gruppenhomomorphismus ist und

$$(f_H, f_N): (H, N, \alpha) \rightarrow R(\phi) = (H', N', \alpha')$$

ein Morphismus in **GroupActions** ist, dann definiere  $f_{N \rtimes H}: N \rtimes_{\alpha} H \rightarrow N'$  durch

$$f_{N \rtimes H}(n, h) = f_N(n)\phi(f_H(h)).$$

Man prüft dass das folgende Diagramm kommutiert, das heißt wir haben einen Morphismus in  $\text{Arr}(\text{Grp})$ :

$$\begin{array}{ccc} H & \xrightarrow{i_H} & N \rtimes_{\alpha} H \\ \downarrow f_H & & \downarrow f_{N \rtimes H} \\ H' & \xrightarrow{\phi} & N' \end{array}$$

Man prüft dass diese Zuordnungen einen natürlichen Isomorphismus der Hom-Funktoren definieren. □

**Lemma 2.4.7.** Sei  $\text{codom}: \text{Arr}(\text{Grp}) \rightarrow \text{Grp}$  der Codomain Funktor aus Lemma 1.5.6 mit Rechtadjungiertem  $R': \text{Grp} \rightarrow \text{Arr}(\text{Grp})$ . Seien  $L, R$  wie in Lemma 2.4.6. Dann ist

$$\text{codom} \circ L: \text{GroupActions} \rightarrow \text{Grp}, (H, N, \alpha) \mapsto N \rtimes_{\alpha} H$$

linksadjungiert zu

$$R \circ R': \text{Grp} \rightarrow \text{GroupActions}, G \mapsto (G, G, \alpha')$$

wobei  $\alpha'(h)(g) = hgh^{-1}$  für alle  $h, g \in G$ .

*Beweis.* Klar. □

## 2.4.2 Auflösbare und Einfache Gruppen

**Definition 2.4.8.**

1. Eine Normalreihe in  $G$  ist eine Folge

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

sodass  $G_i \subseteq G$  eine normale Untergruppe ist.

2. Eine abelsche Normalreihe ist eine Normalreihe sodass  $G_i/G_{i-1}$  abelsch ist für alle  $i$ .
3.  $G$  ist auflösbar, wenn  $G$  eine abelsche Normalreihe hat.

**Beispiel 2.4.9.** Wenn  $G$  abelsch ist, dann ist  $G$  auflösbar denn  $G_0 = \{e\} \subseteq G_1 = G$  ist abelsche Normalreihe.

**Lemma 2.4.10.** Sei  $H \subseteq G$  normal. Es gilt

$$H \text{ auflösbar und } G/H \text{ auflösbar} \implies G \text{ auflösbar}$$

*Beweis.* Sei

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = H$$

eine abelsche Normalreihe und

$$\{e\} = \bar{G}_n \subseteq \bar{G}_{n+1} \subseteq \cdots \subseteq \bar{G}_m = G/H$$

eine abelsche Normalreihe. Sei  $\pi: G \rightarrow G/H$  Projektion und setze  $G_i = H_i$  für  $0 \leq i \leq n$  und  $G_i = \pi^{-1}\bar{G}_i$  für  $n \leq i \leq m$ . Dann bilden die  $G_i$  eine abelsche Normalreihe. □

**Satz 2.4.11.** Seien  $p < q$  Primzahlen. Jede Gruppe der Ordnung  $p \cdot q$  ist auflösbar.

*Beweis.* Sei  $s$  die Anzahl der  $q$ -Sylowgruppen. Dann ist  $s \equiv 1 \pmod{q}$  und  $s \mid p$ . Also ist  $s = 1$  denn  $p < q$ . Somit ist eine  $q$ -Sylowgruppe  $Q \subseteq G$  normal und  $G/Q \cong \mathbb{Z}/p\mathbb{Z}$  und  $Q \cong \mathbb{Z}/q\mathbb{Z}$ . Dann ist  $\{e\} \subseteq Q \subseteq G$  eine abelsche Normalreihe. □

**Satz 2.4.12.** Jede  $p$ -Gruppe  $G$  ist auflösbar

*Beweis.* Wenn  $G \neq \{e\}$  ist, dann ist  $Z(G) \neq \{e\}$ .  $Z(G)$  ist abelscher Normalteiler und somit auflösbar. Nach Induktion ist  $G/Z(G)$  auflösbar. Nach Lemma 2.4.10 folgt die Aussage. □

**Definition 2.4.13.** Sei  $G$  eine Gruppe. Der Kommutator von  $a, b \in G$  ist  $aba^{-1}b^{-1} = [a, b]$ . Die Kommutatorgruppe oder derigierte Gruppe von  $G$  ist  $D(G) = [G, G] = \langle \{[a, b] \mid a, b \in G\} \rangle$ . Die Abelsierung von  $G$  ist  $G^{\text{ab}} = G/D(G)$ .

**Lemma 2.4.14.**  $D(G)$  ist normaler Untergruppe und  $G^{\text{ab}}$  ist abelsch.

*Beweis.* Klar, Rechnung □

**Satz 2.4.15** (Universelle Eigenschaft der Abelsierung). *Abelsierung wird zu einem Funktor  $(-)^{\text{ab}}: \text{Gr} \rightarrow \text{Ab}$  der linksadjungiert ist zum Vergiss-Funktor  $U: \text{Ab} \rightarrow \text{Grp}$*

*Beweis.* Sei  $f: G \rightarrow U(H)$  Gruppenhomomorphismus. Da  $U(H)$  abelsch ist, ist  $D(G)$  im Kern von  $f$ . Das induziert also  $\bar{f}: G/D(G) \rightarrow H$ . □

**Definition 2.4.16.** Sei  $D^n(G) = D(D^{n-1}(G))$  und  $D^0(G) = G$ .

**Bemerkung 2.4.17.** Wenn  $G = G_0 \supseteq G_1 \supseteq \dots$  abelsche Normalreihe ist, dann gilt  $D^n(G) \subseteq G_n$  für alle  $n$ .

*Beweis.* Da  $G_n/G_{n+1}$  abelsch ist, ist  $D(G_n) \subseteq G_{n+1}$ . Damit folgt die Aussage per Induktion. □

**Satz 2.4.18.**  $G$  ist auflösbar  $\iff D^n(G) = \{e\}$  für ein  $n \in \mathbb{N}$ .

*Beweis.* Wenn  $G$  auflösbar ist, dann ist  $G = G_0 \supseteq \dots \supseteq G_n = \{e\}$  und somit  $D^n(G) \subseteq \{e\}$ . Wenn  $D^n(G) = \{e\}$ , dann ist  $G \supseteq D(G) \supseteq \dots \supseteq D^n(G)$  eine abelsche Normalreihe. □

**Beispiel 2.4.19.**  $S_3$  ist auflösbar, denn für  $p = \langle (1, 2, 3) \rangle \subseteq S_3$  ist  $G/P \cong \mathbb{Z}/2\mathbb{Z}$  und somit  $\{e\}, P, S_3$  eine abelsche Normalreihe. Es gibt surjektiven Homomorphismus  $\psi: S_4 \rightarrow S_3$  mit  $\ker(\psi) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Das ist abelsch und da  $S_4/\ker(\psi) = S_3$  auflösbar ist, ist  $S_4$  auflösbar.

**Satz 2.4.20.**  $A_n$  ist nicht auflösbar für  $n \geq 5$ .

*Beweis.* Es ist

$$[(1, 2, 3), (3, 4, 5)] = (1, 4, 3).$$

Somit enthält  $D(A_n)$  alle 3-Zykel, also  $D(A_n) = A_n$  und  $D^m(A_n) \neq \{e\}$  für alle  $m$ . □

**Definition 2.4.21.** Eine Gruppe  $G$  heißt einfach, wenn  $G \neq \{e\}$  und  $G$  keine Normalteiler außer  $\{e\}$  und  $G$  hat.

**Bemerkung 2.4.22.** Wenn  $G$  abelsch und einfach ist, dann ist  $G \cong \mathbb{Z}/p\mathbb{Z}$  für eine Primzahl  $p$ .

*Beweis.* Es gibt  $a \in G$  sodass  $\text{ord}(a) = p$  prim ist. Sei  $H = \langle a \rangle \subseteq G$ . Dann ist  $H$  normal und da  $H \neq \{e\}$  ist  $H = G$ . □

**Bemerkung 2.4.23.** Wenn  $G$  einfach ist und nicht abelsch, dann ist  $G$  nicht auflösbar.

**Bemerkung 2.4.24.** In  $A_n$  mit  $n \geq 5$  sind alle 3-Zykel konjugiert. Denn sei  $\tau_1 = (a \ b \ c)$  und  $\tau_2 = (1 \ 2 \ 3)$ . Sei  $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c$  und setze  $\sigma$  fort zu  $\sigma \in A_n$ . Dann ist  $\sigma\tau_2\sigma^{-1} = \tau_1$ .

**Satz 2.4.25.** Für  $n \geq 5$  ist  $A_n$  einfach.

*Beweis.* Sei  $N \subseteq A_n$  normale Untergruppe und  $N \neq \{e\}$ . Sei  $\sigma \in N$  sodass die Anzahl der Fixpunkte von  $\sigma$  maximal ist und  $\sigma \neq e$ . Behauptung: Alle Zykel in der Zykeldarstellung von  $\sigma$  haben die gleiche Länge  $d$ . Denn wenn Längen  $m < d$  vorkommen, dann hat  $\sigma^m$  mehr Fixpunkte und  $\sigma^m \neq e$ . Behauptung:  $\sigma$  ist ein 3-Zykel. Dann enthält  $N$  als normale Untergruppe alle 3-Zykel, somit  $N = A_n$ . Sei  $\sigma = (a \ b \ c \dots)(\dots) \dots$ . Wenn  $d \geq 3$  bilde  $s = (\tau\sigma\tau^{-1})\sigma^{-1}$  für  $\tau = (a \ b)(d \ e)$ . Dann ist  $s = (c \ d \ e)$  ein 3-Zykel. Wegen Maximalität ist dann  $\sigma$  dieser 3-Zykel. Wenn  $d = 2$  dann ist  $\sigma = (a \ b)(c \ d) \dots = \sigma^{-1}$ . Sei  $\tau = (b \ c)(e \ f)$ . Dann ist  $\tau\sigma\tau^{-1}\sigma^{-1} = (a \ d)(b \ c)$ . Wegen der Maximalität von  $\sigma$  ist  $\sigma = (a \ b)(c \ d)$ . Dann ist aber für  $\tau = (d \ e)(a \ b)$  der Folgende 3-Zykel  $\tau\sigma\tau^{-1}\sigma^{-1} = (c \ d \ e)$  was ein Widerspruch zur Maximalität ist. □

**Satz 2.4.26** (Burnside 1911). *Jede endliche Gruppe der Ordnung  $p^a q^b$  wobei  $p, q$  Primzahlen sind ist auflösbar.*

**Satz 2.4.27** (Feit-Thomson 1963). *Jede Gruppe ungerader Ordnung ist auflösbar.*

## 2.5 Endliche Abelsche Gruppen

**Satz 2.5.1** (Struktursatz endlicher abelscher Gruppen). *Jede endliche abelsche Gruppe  $G$  mit  $|G|$  lässt sich schreiben als*

$$|G| \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

mit  $m_1 \mid \cdots \mid m_r$

*Beweis.* Das ist der ?? zusammen mit dem Fakt, dass endliche Gruppen Torsionsmoduln sind.  $\square$

**Lemma 2.5.2** (Chinesischer Restsatz). *Seien  $n, m \in \mathbb{Z}$  und  $d = \text{ggT}(n, m)$  und  $k = \text{kgV}(n, m)$ . Dann ist  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ .*

*Beweis.* Sei  $xn + ym = d$  für  $x, y \in \mathbb{Z}$ . Definiere

$$f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, (a, b) \mapsto (a - b\frac{xn}{d} + n\mathbb{Z}, a + b\frac{ym}{d}) + m\mathbb{Z}.$$

Angenommen  $f(a, b) = (0, 0)$ . Dann ist

$$b\frac{xn}{d} \equiv a \pmod{n}$$

und

$$-b\frac{ym}{d} \equiv a \pmod{m}.$$

Also gilt

$$b\frac{xn}{d} \equiv -b\frac{ym}{d} \pmod{d}$$

und somit

$$b(\frac{xn}{d} + \frac{ym}{d}) \equiv 0 \pmod{d}.$$

Da

$$\frac{xn}{d} + \frac{ym}{d} \equiv 1 \pmod{d}$$

gilt, ist

$$b \equiv 0 \pmod{d}.$$

Sei also  $b = s \cdot d$ . Dann ist

$$a \equiv \frac{xn}{d} \cdot b = xns \equiv 0 \pmod{n}$$

und analog  $a \equiv 0 \pmod{n}$ . Also ist  $a \equiv 0 \pmod{k}$ . Das zeigt  $\ker(f) = k\mathbb{Z} \times d\mathbb{Z}$  und somit ist  $\bar{f}: \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  injektiv und damit surjektiv wegen gleicher Anzahl der Elemente.  $\square$

## Teil II

# Körper und Galois-Theorie



# Kapitel 3

## Körpererweiterungen

### 3.1 Grundlagen

**Definition 3.1.1.** Sei  $K$  ein Körper. Der Primkörper von  $K$  ist der Schnitt aller Teilkörper von  $K$ . Es gibt  $\mathbb{Z}/(p) \subseteq K$  für  $p = \text{char } K$ . Wenn  $p = 0$ , dann ist  $\mathbb{Q} \subseteq K$  und  $\mathbb{Q}$  ist der Primkörper. Wenn  $p \neq 0$ , dann ist  $\mathbb{F}_p \subset K$  der Primkörper.

**Definition 3.1.2.** Seien  $L, K$  Körper sodass  $K \subseteq L$  Teilring ist. Dann heißt  $K$  Teilkörper von  $L$  und  $L$  eine Erweiterung von  $K$ . Wir setzen  $[L : K] = \dim_K(L)$ .

**Satz 3.1.3.** Sei  $L/K$  eine Körpererweiterung und  $V$  ein  $L$ -Vektorraum. Dann ist

$$\dim_K(V) = \dim_L(V) \cdot [L : K].$$

*Beweis.* Wenn  $\dim_L(V) = \infty$  dann ist alles klar. Sonst wähle Isomorphismus  $V = L^n$ . Das ist Isomorphismus von  $K$ -Vektorräumen. Also gilt die Aussage.  $\square$

**Korollar 3.1.4.** Wenn  $M/L/K$  Körpererweiterungen sind, dann ist

$$[M : K] = [M : L] \cdot [L : K]$$

### 3.2 Algebraische und transzendente Erweiterungen

**Definition 3.2.1.** Sei  $L/K$  eine Körpererweiterung und  $a \in L$  und  $\phi: K[X] \rightarrow L$  der Ringhomomorphismus gegeben durch  $\phi(f) = f(a)$ .

1. Das Element  $a$  heißt algebraisch, falls  $\ker(\phi) \neq 0$ . Andererseits nennen wir  $a$  transzendent über  $K$ .
2.  $L/K$  heißt algebraisch, wenn jedes  $a \in L$  algebraisch über  $K$  ist.
3.  $K[X]$  ist Euklidisch, somit Hauptidealring. Also ist  $\ker(\phi) = (f)$  für ein normiertes Polynom  $f$ . Das Polynom  $f$  heißt das Minimalpolynom von  $a$ .

**Definition 3.2.2.** Sei  $L/K$  eine Körpererweiterung und  $a_1, \dots, a_r \in L$ .

1. Die Algebra erzeugt von  $a_1, \dots, a_r$  ist

$$\begin{aligned} K[a_1, \dots, a_r] &= \bigcap_{R \in M} R \\ &= \text{im}(\phi: K[X_1, \dots, X_r] \rightarrow L, X_i \mapsto a_i) \end{aligned}$$

wobei  $M$  die Menge aller Unterringe von  $L$  ist, die  $K$  und die Elemente  $a_1, \dots, a_r$  enthalten.

2. Der Körper erzeugt von  $a_1, \dots, a_r$  ist

$$\begin{aligned} K(a_1, \dots, a_r) &= \bigcap_{K' \in M'} K' \\ &= \text{Quot}(K[a_1, \dots, a_r]) \end{aligned}$$

wobei  $M'$  die Menge aller Teilkörper von  $L$  ist, die  $K$  und die Elemente  $a_1, \dots, a_r$  enthalten.

**Satz 3.2.3.** Sei  $L/K$  Körpererweiterung und  $a \in L$ .

1.  $a$  ist algebraisch über  $K \iff K[a] = K(a) \iff \dim_K(K[a]) < \infty$
2. Wenn  $a$  algebraisch über  $K$  ist, dann ist  $K[a] = K(a) \cong K[X]/(f)$  wobei  $f$  (irreduzibel) das Minimalpolynom von  $a$  ist und
$$\deg(f) = [K(a) : K].$$

*Beweis.* Sei  $a$  algebraisch. Dann ist das Minimalpolynom  $f$  irreduzibel sodass

$$(f) = \text{Ker}(\phi: K[X] \rightarrow L, x \mapsto a).$$

Dann ist  $K[a] \cong K[X]/(f)$  ein Körper, also ist auch  $K[a] = K(a)$ . Wenn  $K[a] \cong K[X]/(f)$  ein Körper ist, dann ist  $f$  irreduzibel also  $f \neq 0$  und  $f(a) = 0$ . Also ist  $a$  algebraisch. In dem Fall ist  $\infty > \deg(f) = [K[a] : K]$ . Wenn  $a$  nicht algebraisch ist, dann ist  $K[a] \cong K[X]$  und  $\dim_K(K[X]) = \infty$ .  $\square$

**Beispiel 3.2.4.**  $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/(X^2 + 1)$

**Satz 3.2.5.** Sei  $L/K$  eine Körpererweiterung.

$$\begin{aligned} L/K \text{ endlich} &\iff L/K \text{ ist algebraisch und } L = K(a_1, \dots, a_n) \\ &\iff L = K(a_1, \dots, a_n) \text{ für } K\text{-algebraische } a_i \in L \end{aligned}$$

In dem Fall gilt  $K(a_1, \dots, a_n) = K[a_1, \dots, a_n]$

*Beweis.* Sei  $L/K$  endlich. Dann ist  $L$  als  $K$ -Vektorraum erzeugt und insbesondere als Körpererweiterung. Für  $a \in L$  gilt  $K[a] \subseteq L$  und

$$\dim_K(K[a]) \leq \dim_K L < \infty$$

also ist  $a$  algebraisch. Sei  $L = K(a_1, \dots, a_n)$  sodass  $a_i$  algebraisch über  $K$  ist. Wenn  $n = 0$  ist, dann ist  $L = K$  also ist  $L/K$  endlich. Sei  $K[a_1] = K'$ . Das ist ein Körper und somit endlich über  $K$  und  $L = K'[a_1, \dots, a_n]$ . Nach Induktion folgt  $K'[a_2, \dots, a_n] = K'(a_2, \dots, a_n)$ .  $\square$

**Korollar 3.2.6.** Sei  $L/K$  eine Körpererweiterung und  $a_1, \dots, a_n \in L$ . Es gilt

$$a_1, \dots, a_n \text{ algebraisch über } K \iff K(a_1, \dots, a_n) = K[a_1, \dots, a_n]$$

*Beweis.* Die eine Richtung folgt aus Satz 3.2.5, die andere aus dem Satz 8.1.1.  $\square$

**Korollar 3.2.7.** Seien  $M/L/K$  Körpererweiterungen. Es gilt

$$M/L \text{ und } L/K \text{ algebraisch} \iff M/K \text{ algebraisch}$$

*Beweis.* Sei  $a \in M$  algebraisch über  $L$  und  $f \in L[X]$  ein Polynom mit  $f(a) = 0$ . Sei

$$f = \sum_{i=0}^n b_i X^i$$

für  $b_i \in L$  und  $b_n = 1$ . Dann ist  $L' = K[b_0, \dots, b_{n-1}]$  ein Körper sodass  $L'/K$  endlich ist. Da  $a$  algebraisch ist über  $L'$ , ist  $L'(a)$  endlich über  $L'$ . Also ist  $L'(a)$  endlich über  $K$  und somit algebraisch.  $\square$

**Satz 3.2.8.** Sei  $K$  Körper und  $f \in K[X]$  irreduzibel. Dann gibt es eine Körpererweiterung  $L/K$  mit  $[L : K] = \deg(f)$  und  $a \in L$  mit  $f(a) = 0$ .

*Beweis.* Klar,  $L = K[X]/(f)$ .  $\square$

**Korollar 3.2.9.** Zu endlich vielen  $f_1, \dots, f_r \in K[X]$  mit  $\deg(f_i) \geq 1$  gibt es eine endliche Erweiterung  $L/K$ , sodass  $f_i \in L[X]$  in Linearfaktoren zerfällt.

*Beweis.* Angenommen es gibt  $L/K$  sodass  $f_1$  in  $L[X]$  zerfällt und  $L_r/L_1$  sodass  $f_2, \dots, f_r$  in  $L_r[X]$  zerfällt. Dann zerfällt  $f_1, \dots, f_r$  in  $L_r/K$ . Also sei nach Induktion  $r = 1$ . Sei  $f = g_1, \dots, g_s$  mit  $g_i$  irreduzibel. Nach letztem Satz gibt es  $L'/K$  endlich und  $a \in L'$  mit  $g_1(a) = 0$ . In  $L'[X]$  gilt  $f = (X - a)f_1$ . Induktion über  $\deg(f)$  gibt die Aussage.  $\square$

**Beispiel 3.2.10.**  $f = X^3 - 2 \in \mathbb{Q}[X]$  ist irreduzibel nach Eisenstein.

$$L_1 = \mathbb{Q}[X]/(f) \cong \mathbb{Q}(\sqrt[3]{2}).$$

In  $L_1[X]$  ist  $f = (X - a) \cdot g$  wobei  $a = \sqrt[3]{2}$  und  $g$  irreduzibel ist (Irreduzibel in  $\mathbb{R}$  also in  $L_1$ ). Wenn  $L = L_1[X]/(g)$  dann hat  $L/\mathbb{Q}$  hat Grad 6 und  $x^3 - 2$  zerfällt in Linearfaktoren in  $L$ .

**Lemma 3.2.11** (Algebraisch Abgeschlossen). Für einen Körper  $K$  ist äquivalent:

1. Jedes nicht-konstante Polynom  $f \in K[X]$  hat eine Nullstelle
2. Jedes irreduzible Polynom  $f \in K[X]$  hat Grad 1
3. Für jede algebraische Erweiterung  $L/K$  gilt  $L = K$

In dem Fall heißt  $K$  algebraisch abgeschlossen.

*Beweis.* 1  $\implies$  2 ist klar.

Gelte 2. Dann sei  $f$  nicht-konstant. Also gibt es ein irreduzibles Polynom  $P$  mit  $P|f$ . Da  $P = aX + b$  für ein  $a \neq 0$ , ist  $P(\frac{-b}{a}) = 0$  also hat  $f$  eine Nullstelle.

Gelte 2 und sei  $a \in L$  algebraisch mit Minimalpolynom  $f \in K[X]$ .  $f$  ist irreduzibel, also ist  $f = X - a$  und somit  $a \in K$ .

Gelte 3. und sei  $f$  irreduzible. Dann ist  $L = K[X]/(f) \cong K$ . Also ist  $\deg(f) = 1$  und  $f$  linear.  $\square$

**Definition 3.2.12.** Sei  $K$  ein Körper. Ein algebraischer Abschluss von  $K$  ist eine algebraische Körpererweiterung  $L/K$  sodass  $L$  algebraisch abgeschlossen ist. Notation  $L = \bar{K}$

### 3.3 Körperhomomorphismen

**Definition 3.3.1.** Ein Körperhomomorphismus ist ein Ringhomomorphismus zwischen Körpern. Seien  $L/K$  und  $M/K$  zwei Körpererweiterungen. Ein  $K$ -Homomorphismus ist ein Homomorphismus von  $K$ -Algebren.  $\text{Aut}_K(L) = \text{Aut}(L/K)$  sei die Menge der invertierbaren  $K$ -Homomorphismen  $f: L \rightarrow L$

**Lemma 3.3.2.** Seien  $L = K(a)/K$  eine Körpererweiterungen und sei  $f$  das Minimalpolynom von  $a$ . Sei  $M$  ein Körper mit einem Homomorphismus  $\sigma: K \rightarrow M$ . Sei

$$\Sigma = \{K\text{-Homomorphismen } \sigma': L \rightarrow M\}.$$

Dann ist die Abbildung

$$\Sigma \rightarrow \{b \in M \mid f(b) = 0\}, \quad \sigma' \mapsto \sigma'(a) = b$$

bijektiv

*Beweis.* Wir haben die Abbildung  $\phi: K[X] \rightarrow M, X \mapsto b$ . Es gilt  $\phi$  lässt sich eindeutig fortsetzen zu  $\sigma': K[X]/(f) \rightarrow M$  genau dann, wenn  $f \in \ker(\phi)$  ist, das heißt wenn  $f(b) = 0$ . Dann ist  $\sigma'(a) = \sigma'(\bar{X}) = b$ .  $\square$

**Beispiel 3.3.3.**  $L = M = \mathbb{C}$  und  $K = \mathbb{R}$ . Dann ist

$$\{\mathbb{R}\text{-Hom } \sigma': \mathbb{C} \rightarrow \mathbb{C}\} \xrightarrow{\sim} \{b \in \mathbb{C} \mid b^2 + 1 = 0\}, \quad \sigma' \mapsto \sigma'(i)$$

also  $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma'\}$  wobei  $\sigma'$  komplexe Konjugation ist.

**Satz 3.3.4.** Sei  $L/K$  eine algebraische Erweiterung und  $M$  ein algebraisch abgeschlossener Körper. Sei weiter  $\sigma: K \rightarrow M$  ein Körperhomomorphismus. Dann existiert eine Fortsetzung von  $\sigma$  zu einem Körperhomomorphismus  $\sigma': L \rightarrow M$  sodass

$$\begin{array}{ccc} L & \xrightarrow{\sigma'} & M \\ & \nwarrow \quad \nearrow \sigma & \\ & K & \end{array}$$

kommutiert

*Beweis.* Fall 1: Sei  $L = K(a) = K[a] = K[X]/(f)$ . Die Menge der  $\sigma'$  ist bijektiv zur Menge der Nullstellen von  $f$  in  $M$ . Also existiert  $\sigma'$ .

Fall 2: Sei  $L/K$  allgemein. Sei  $X$  die Menge der Paare  $(L', \sigma')$  wobei  $L'$  ein Körper ist mit  $K \subseteq L' \subseteq L$  und  $\sigma'$  eine Fortsetzung von  $\sigma$ . Definiere partielle Ordnung  $(L', \sigma') \leq (L'', \sigma'')$  durch  $L' \subseteq L''$  und  $\sigma''|_{L'} = \sigma'$ . Sei  $X' \subseteq X$  total geordnet. Dann ist

$$\tilde{L} = \bigcup_{(L', \sigma') \in X'} L'$$

ein Körper und zusammen mit  $\tilde{\sigma}: \tilde{L} \rightarrow M$  definiert durch  $\tilde{\sigma}(b) = \sigma'(b)$  für  $b \in L'$  eine obere Schranke von  $X'$ . Nach [Zornsches Lemma](#) hat  $X$  ein maximales Element  $(L', \sigma')$ . Angenommen  $L' \neq L$ . Dann wähle  $a \in L \setminus L'$  und setze  $L'' = L'(a)$ . Nach Fall 1 existiert eine Fortsetzung  $\sigma'': L'' \rightarrow M$  was ein Widerspruch ist. Also ist  $L' = L$ .  $\square$

**Korollar 3.3.5.** Seien  $L/K$  und  $M/K$  zwei algebraische Abschlüsse von  $K$ . Dann gibt es einen  $K$ -Isomorphismus  $L \rightarrow M$

*Beweis.* Nach Satz 3.3.4 gibt es  $K$ -Homomorphismus  $\sigma: L \rightarrow M$ . Dadurch wird  $M$  eine algebraische Erweiterung von  $L$ . Also ist  $M/L$  triviale Erweiterung, dh.  $\sigma$  ist bijektiv.  $\square$

### 3.4 Zerfällungskörper und Algebraischer Abschluss

**Satz 3.4.1** (Existenz algebraischer Abschluss). Jeder Körper hat einen algebraischen Abschluss

*Beweis.* Sei  $I$  die Menge aller irreduziblen Polynome  $f \in K[X]$  und sei  $R = K[X_f \mid f \in I]$ . Sei  $J \subseteq R$  das Ideal, das von allen Elementen der Form  $f(X_f)$  mit  $f \in I$  erzeugt wird.

Es gilt die Behauptung  $J \subsetneq R$ . Denn angenommen  $J = R$ , dann ist  $1 \in J$  also gibt es Darstellung

$$1 = \sum_{j=1}^r g_j f_j(X_{f_j}) \quad (3.1)$$

wobei  $g_j \in R$  und  $f_1, \dots, f_r \in I$ . In  $g_1, \dots, g_r$  kommen nur endlich viele  $X_{f_i}$  vor, somit gibt es eine endliche Menge  $I' \subseteq I$ , sodass die Gleichung 3.1 in  $R' = K[X_f \mid f \in I']$  stattfindet. Nach Korollar 3.2.9 gibt es eine endliche Erweiterung  $M/K$ , sodass jedes  $f \in I'$  in  $M$  eine Nullstelle  $a_f$  hat. Betrachte die Abbildung

$$\phi: R' \rightarrow M, \quad \phi(X_f) = a_f.$$

Dann ist  $\phi(f(X_f)) = f(a_f) = 0$  also  $f(X_f) \in \ker(\phi)$ . Die Gleichung 3.1 würde zeigen, dass  $1 \in \ker(\phi)$ , was ein Widerspruch ist zu  $1 \neq 0$  in  $M$ . Also ist gilt die Behauptung  $J \subsetneq R$ .

Also ist  $\bar{R} = R/J \neq 0$  und nach Satz 6.1.4 gibt es maximales Ideal  $\mathfrak{m} \subseteq \bar{R}$ . Für den Quotienten  $L = \bar{R}/\mathfrak{m}$ , ist  $L/K$  eine Körpererweiterung und  $L$  ist erzeugt von  $\bar{X}_f$  für  $f \in I$ . Es ist  $f(X_f) = 0$  in  $\bar{R}$  und somit auch in  $L$ . Also ist  $\bar{X}_f \in L$  algebraisch über  $K$  und damit ist auch  $L/K$  algebraisch und jedes  $f \in I$  hat in  $L$  eine Nullstelle, nämlich  $\bar{X}_f$ . Sei  $L_1 = L$ .  $L_1/K$  ist algebraisch, sodass jedes irreduzible Polynom  $f \in K[X]$  in  $L_1$  eine Nullstelle hat. Konstruiere Analog  $K \subseteq L_1 \subseteq L_2 \subseteq L_3 \dots$  sodass jedes irreduzible Polynom in  $L_i$  in  $L_{i+1}$  eine Nullstelle hat. Sei  $\tilde{L} = \bigcup_{i \geq 1} L_i$ . Das ist ein

Körper und  $\tilde{L}/K$  ist algebraisch. Der Körper  $\tilde{L}$  ist algebraisch abgeschlossen, denn wenn  $f \in \tilde{L}[X]$  irreduzibel dann gibt es  $i \in \mathbb{N}$  sodass  $f \in L_i[X]$  und dann hat  $f$  in  $L_{i+1}$  eine Nullstelle. Also hat  $f$  in  $\tilde{L}$  eine Nullstelle.  $\square$

**Definition 3.4.2.** Sei  $K$  ein Körper und  $\mathcal{F} \subseteq K[X]$  eine Menge von nicht-konstanten Polynomen. Ein Zerfällungskörper ist eine Körpererweiterung  $L/K$  sodass jedes  $f \in \mathcal{F}$  in  $L[X]$  in Linearfaktoren zerfällt und  $L = K(a \in \bar{K} \mid f(a) = 0 \text{ für ein } f \in \mathcal{F})$

**Lemma 3.4.3.** Für eine Menge  $\mathcal{F} \subseteq K[X]$  nicht-konstanter Polynome existiert ein Zerfällungskörper und ein Zerfällungskörper ist eindeutig bis auf  $K$ -Isomorphismus.

*Beweis.* Sei  $L = K(a \in \bar{K} \mid f(a) = 0 \text{ für ein } f \in \mathcal{F}) \subseteq \bar{K}$ . Dann ist  $L$  ein Zerfällungskörper. Sei  $M$  ein weiterer Zerfällungskörper. Dann gibt es nach Satz 3.3.4 einen  $K$ -Homomorphismus  $\sigma: M \rightarrow \bar{K}$ . Seien  $f \in \mathcal{F}$  und  $a_1, \dots, a_n$  die Nullstellen in  $\bar{K}$  von  $f$  und  $b_1, \dots, b_n$  die Bilder der Nullstellen von  $f$  in  $M$  unter  $\sigma$ . Da  $\prod_{i=1}^n (X - a_i) = f = \prod_{i=1}^n (X - b_i)$  in  $\bar{K}[X]$  ist ohne Einschränkung  $a_i = b_i$  für alle  $i$ . Somit ist  $\sigma(M) = L$  und  $\sigma$  ist ein Isomorphismus  $M \rightarrow L$ .  $\square$

**Bemerkung 3.4.4.** Das zeigt: Alle  $K$ -Homomorphismen  $\sigma: M \rightarrow \bar{K}$  haben Bild  $L$ .

**Beispiel 3.4.5.** Sei  $K = \mathbb{Q}$  und  $f = X^3 - 2$ . In  $\bar{\mathbb{Q}}[X]$  gilt  $f = (X - a)(X - \zeta a)(X - \zeta^2 a)$  für  $a = \sqrt[3]{2}$  und  $\zeta = e^{2\pi i/3}$ . Also ist der Zerfällungskörper  $L = \mathbb{Q}(a, \zeta a, \zeta^2 a) = \mathbb{Q}(a, \zeta)$ . Es ist  $\mathbb{Q} \subsetneq \mathbb{Q}(a) \subsetneq \mathbb{Q}(a, \zeta a)$  und  $[\mathbb{Q}(a) : \mathbb{Q}] = 3$  da  $f$  das Minimalpolynom ist. Es ist  $g = (X - \zeta a)(X - \zeta^2 a)$  das Minimalpolynom von  $\zeta a$  über  $\mathbb{Q}(a)$ , also ist  $[\mathbb{Q}(a, \zeta a) : \mathbb{Q}] = 6$

## 3.5 Normale und Separable Erweiterungen

### 3.5.1 Normale Erweiterungen

**Definition 3.5.1.** Eine algebraische Körpererweiterung  $L/K$  ist normal, wenn jedes irreduzible Polynom in  $K[X]$ , das in  $L$  eine Nullstelle hat in  $L[X]$  in Linearfaktoren zerfällt.

**Lemma 3.5.2.** Sei  $L/K$  algebraisch und  $\varphi: L \rightarrow L$  ein  $K$ -Homomorphismus. Dann ist  $\phi$  bijektiv.

*Beweis.* Immer ist  $\phi$  injektiv. Sei  $a \in L$ . Dann gibt es  $f \in K[X]$  sodass  $K(a) = K[X]/(f)$ . Seien  $a = a_1, \dots, a_n$  die Nullstellen von  $f$  in  $L$ .  $\varphi|_{K(a_i)}: K(a_i) \rightarrow L$  gibt  $n$  verschiedene  $K$ -Homomorphismen  $K[X]/(f) \rightarrow L$  da  $\varphi(a_i) \neq \varphi(a_j)$  für  $i \neq j$ . Da diese in Bijektion zu der Menge der  $\{a_1, \dots, a_n\}$  stehen gilt für ein  $i$ :  $\varphi|_{a_i}(a_i) = a_1 = a$ . Also ist  $\varphi$  bijektiv.  $\square$

**Satz 3.5.3.** Sei  $L/K$  algebraisch. Dann ist äquivalent:

1.  $L/K$  ist normal
2.  $L/K$  ist Zerfällungskörper einer Menge  $\mathcal{F} \subseteq K[X]$ .
3. Für jede Körpererweiterung  $M/L$  und jeden  $K$ -Homomorphismus  $\varphi: L \rightarrow M$  gilt  $\phi(L) = L$
4. Für Jeden  $K$ -Homomorphismus  $\varphi: L \rightarrow \bar{L}$  gilt  $\phi(L) = L$ .

*Beweis.* Gelte 1. Dann sei

$$\mathcal{F} = \{f \in K[X] \mid f \text{ ist irreduzibel und hat eine Nullstelle in } L\}.$$

Jedes  $f \in \mathcal{F}$  zerfällt in  $L[X]$  in Linearfaktoren. Sei  $a \in L$  mit Minimalpolynom  $f \in K[X]$ . Dann ist  $f \in \mathcal{F}$  also ist  $L$  von allen Nullstellen erzeugt. Also ist  $L$  Zerfällungskörper. Gelte 2. Sei  $L/K$  Zerfällungskörper von  $\mathcal{F}$  und  $\varphi: L \rightarrow M$  ein  $K$ -Homomorphismus. Für  $f \in \mathcal{F}$  und  $a \in L$  mit  $f(a) = 0$  gilt  $f(\varphi(a)) = 0$  also ist  $\phi(a)$  Nullstelle von  $f$  in  $M$ . Dann ist  $L = K(a \in M \mid f(a) = 0 \text{ für ein } f \in \mathcal{F})$  und somit  $\phi(L) \subseteq L$ . Da  $L/K$  algebraisch ist, ist  $\varphi$  bijektiv und  $\varphi(L) = L$ .

3.  $\implies$  4 ist klar. Gelte 4. Sei  $f \in K[X]$  irreduzibel mit  $f(a) = 0$  für  $a \in L$ . Die Menge der  $K$ -Homomorphismen  $\sigma: K(a) \rightarrow \bar{L}$  ist bijektiv zur Menge  $\{b \in \bar{L} \mid f(b) = 0\}$ . Zu  $b \in \bar{L}$  wähle also  $\sigma: K(a) \rightarrow \bar{L}$ . Nach Satz 3.3.4 gibt es ein  $\varphi: L \rightarrow \bar{L}$ , das  $\sigma$  fortsetzt. Dann ist  $\varphi(L) = L$ . Also ist  $b = \sigma(a) = \varphi(a) \in L$ . Also zerfällt  $f$  in  $L[X]$ .  $\square$

**Lemma 3.5.4** (Normalität in Türmen). Seien  $M/L/K$  Körpererweiterungen. Es gilt

$$M/K \text{ normal} \implies M/L \text{ normal}.$$

*Beweis.* Sei  $M$  ein Zerfällungskörper von  $\mathcal{F} \subseteq K[X]$ . Dann ist  $M/L$  ein Zerfällungskörper von  $\mathcal{F}$  als Teilmenge von  $L[X]$ .  $\square$

**Definition 3.5.5.** Sei  $L/K$  algebraisch. Eine normale Hülle von  $L/K$  ist eine Erweiterung  $M/L$  sodass  $M/K$  normal ist und für jede andere Erweiterung  $M'/L$  mit  $M'/K$  normal gibt es einen  $L$ -Homomorphismus  $M \rightarrow M'$ . Das zeigt: Eine normale Hülle ist eindeutig bis auf Isomorphismus

**Satz 3.5.6.** Die normale Hülle einer algebraischen Erweiterung  $L/K$  existiert

*Beweis.* Sei

$$\mathcal{F} = \{f \in K[X] \text{ irreduzibel sodass } f \text{ eine Nullstelle in } L \text{ hat}\}.$$

Sei  $M/L$  Zerfällungskörper von  $\mathcal{F} \subseteq L[X]$ . Dann ist  $M/K$  Zerfällungskörper der selben Menge und somit  $M/K$  normal. Sei  $M'/L$  mit  $M'/K$  normal. Wähle  $\bar{M}'/M'$  algebraischen Abschluss. Nach Satz 3.3.4 gibt es einen  $L$ -Hom  $\varphi: M \rightarrow \bar{M}'$ . Jedes  $f \in \mathcal{F}$  zerfällt in  $M'[X]$  und da  $M$  von allen Nullstellen erzeugt gilt  $\phi(M) \subseteq M'$ .  $\square$

**Beispiel 3.5.7.** Eine normale Hülle von  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  ist  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ , der Zerfällskörper von  $x^3 - 2$ .

### 3.5.2 Separable Erweiterungen

**Definition 3.5.8.**  $f \in K[X]$  heißt separable, wenn  $f \in \bar{K}[X]$  keine mehrfachen Nullstellen hat.

**Definition 3.5.9.** Die formale Ableitung von  $f \in K[X]$  ist  $f' = \sum_{i=0}^n a_i X^i$  ist  $f' = \sum_{i=0}^n i \cdot a_i X^{i-1}$

**Lemma 3.5.10** (Leibniz-Regel).

$$(fg)' = f'g + fg'$$

*Beweis.* Reduziere auf  $f = X^n$  und  $g = X^m$ . Dann ist alles klar.  $\square$

**Lemma 3.5.11.** Sei  $f \in K[X]$ .

1.  $b \in \bar{K}$  ist mehrfache Nullstelle von  $f \iff f(b) = 0 = f'(b) \iff (X - b) | \text{ggT}(f, f')$
2.  $f$  ist separable  $\iff \text{ggT}(f, f') = 1$

*Beweis.* Der ggT ändert sich nicht bei Übergang zu einer Erweiterung  $L/K$ , also auch nicht bei  $\bar{K}/K$ . 1. ist eine Rechnung und 2. folgt aus 1.  $\square$

**Satz 3.5.12.** Sei  $f \in K[X]$  irreduzibel.

1.  $f$  ist separable  $\iff f' \neq 0$  in  $K[X]$ .
2. Wenn  $K$  Charakteristik 0 hat, ist  $f$  separable.

*Beweis.*

$$f \text{ separable} \iff \text{ggT}(f, f') = 1 \iff f' \neq 0$$

da  $f' \neq f$ . Wenn  $K$  Charakteristik 0 hat, dann ist  $f' \neq 0$  also ist  $f$  separable.  $\square$

**Bemerkung 3.5.13.** Für  $f$  irreduzibel gilt:  $f' = 0 \iff \text{char } K = p > 0$  und  $f = \sum_{i=0}^n b_i X^{p^i}$  für  $b_i \in K$

**Bemerkung 3.5.14.** Sei  $p$  Primzahl und  $K = \text{Quot}(\mathbb{F}_p[Y])$ . Das Polynom  $f = X^p - Y \in K[X]$  ist irreduzibel nach Eisenstein für das Primelement  $Y \in \mathbb{F}_p[X]$  und in-separable.

**Definition 3.5.15.** Sei  $L/K$  eine algebraische Körpererweiterung.

1.  $a \in L$  ist separable über  $K$ , wenn das Minimalpolynom von  $a$  separable ist.
2.  $L/K$  ist separable, wenn jedes  $a \in L$  separable ist.
3. Der Separabilitätsgrad von  $L/K$  ist  $[L : K]_s = |\{K - \text{Hom} . L \rightarrow \bar{K}\}|$

**Lemma 3.5.16.** Sei  $L = K(a)$  algebraisch über  $K$ . Dann gilt

1.  $[L : K]_s \leq [L : K]$
2.  $[L : K]_s = [L : K] \iff a \text{ separable über } K$

*Beweis.* Sei  $f$  Minimalpolynom von  $a$  sodass  $L \cong K[X]/(f)$ . Es gilt

$$|\{K - \text{Hom } L \rightarrow \bar{K}\}| = |\{b \in \bar{K} \mid f(b) = 0\}| \leq \deg(f)$$

und " $=$ " genau dann, wenn  $f$  separable. □

**Lemma 3.5.17.** *Sei  $M/L/K$  endlich. Dann ist  $[M : L]_s \cdot [L : K]_s = [M : K]_s$*

*Beweis.*  $\bar{K}$  kann als algebraischer Abschluss von  $M$  und  $L$  aufgefasst werden. Dann gilt

$$[M : L]_s = |\{\psi : M \rightarrow \bar{K} \mid \psi|_L = \varphi\}|$$

für jeden  $\phi : L \rightarrow \bar{K}$  erfüllt die Abbildung

$$R : \{\psi : M \rightarrow \bar{K} \mid \psi|_K = id\} \rightarrow \{\varphi : L \rightarrow \bar{K} \mid \varphi|_K = id\}, \psi \mapsto \psi|_L$$

$$|R^{-1}\{\varphi\}| = [M : L]_s.$$

Also

$$[M : K]_s = |\{\psi : M \rightarrow \bar{K} \mid \psi|_K = id\}| = [M : L]_s \cdot [L : K]_s$$

□

**Satz 3.5.18.** *Sei  $L/K$  endlich.*

1.  $[L : K]_s \leq [L : K]$
2. *Es ist äquivalent:*
  - (a)  $[L : K]_s = [L : K]$
  - (b)  $L/K$  ist separable
  - (c)  $L/K$  ist von separablen Elementen erzeugt

*Beweis.* 1. Wähle  $a_1, \dots, a_r$  sodass  $L = K(a_1, \dots, a_r)$ . Es gilt

$$[L : K] = [L : K(a_1)] \cdot [K(a_1) : K]$$

und

$$[L : K]_s = [L : K(a_1)]_s \cdot [K(a_1) : K]_s$$

Jetzt folgt 1. mit Induktion.

2.  $b) \implies c)$  ist klar. Gelte c).  $L = K(a_1, \dots, a_r)$  mit  $a_i$  separable. Dann ist

$$[K(a_1) : K]_s = [K(a_1) : K]$$

und nach Induktion  $[L : K(a_1)]_s = [L : K(a_1)]$ . Also gilt a). Gelte a) und sei  $a \in L$ . Dann ist

$$\begin{aligned} [L : K] &= [L : K(a_1)] \cdot [K(a_1) : K] \\ &\geq [L : K(a_1)]_s \cdot [K(a_1) : K]_s \\ &= [L : K]_s = [L : K] \end{aligned}$$

Also ist  $[K(a_1) : K] = [K(a_1) : K]_s$  und somit ist  $a$  separable. Also gilt b). □

**Korollar 3.5.19.** *Seien  $M/L/K$  algebraisch.*

$$M/K \text{ separable} \iff M/L \text{ und } L/K \text{ separable}$$

*Beweis.* Sei  $M/K$  separable und  $a \in M$ . Sei  $f \in K[X]$  das Minimalpolynom über  $K$  und  $g \in L[X]$  das Minimalpolynom über  $L$ . Dann  $g|f$  in  $L[X]$  also ist  $g$  separable und damit auch  $a$  separable über  $L$ .

Seien  $M/L$  und  $L/K$  separable. Sei  $a \in M$  und  $g \in L[X]$  das Minimalpolynom. Wähle  $K \subseteq L' \subseteq L$  sodass  $L'/K$  endlich ist und  $g \in L'[X]$ . Sei  $M' = L'(a)$ . Dann ist  $M'/L'/K$  endlich. Minimalpolynom von  $a$  über  $L'$  ist  $g$  und das ist separable, da  $M/L$  separable. Somit ist  $M'/L'$  separable.  $L'/K$  ist separable das  $L/K$  separable. Somit ist ohne Einschränkung  $M/L/K$  endlich. Dann zeigt eine Rechnung mit den Graden der Erweiterungen, dass  $M/K$  separable ist. □

**Korollar 3.5.20.** *Der Zerfällungskörper einer Menge von separablen Polynomen ist eine separable Erweiterung.*

*Beweis.* Sei  $L/K$  Zerfällungskörper von  $\mathcal{F} \in K[X]$  bestehend aus separablen Polynomen. Zu  $a \in L$  gibt es endliche Teilmenge  $\mathcal{F}' \subseteq \mathcal{F}$  sodass  $a \in L'$  wobei  $L' \subseteq L$  Zerfällungskörper von  $\mathcal{F}'$ .  $L'/K$  ist endlich und von separablen Elementen erzeugt. Somit ist  $L'/K$  separable. Insbesondere ist  $a$  separable über  $K$ .  $\square$

**Korollar 3.5.21.** *Die normale Hülle einer separablen Erweiterung ist ebenfalls separable*

*Beweis.* Folgt aus der Konstruktion der normalen Hülle.  $\square$

## 3.6 Spur und Norm

**Definition 3.6.1.** Sei  $L/K$  eine endliche Körpererweiterung und  $b \in K$ . Dann ist

$$\text{Tr}_{L/K}(b) = \text{Tr}(b \cdot : L \rightarrow L)$$

die Spur und

$$N_{L/K}(b) = \det(b \cdot : L \rightarrow L)$$

die Norm von  $b$ .

**Bemerkung 3.6.2.** Es ist für  $a \in K$

$$\text{Tr}_{L/K}(a) = [L : K]a$$

und

$$N_{L/K}(a) = a^{[L:K]}$$

**Lemma 3.6.3.** *Sei  $L/K$  eine endliche Körpererweiterung und  $b \in L$ . Sei  $P$  das Minimalpolynom von  $b$  über  $K$ ,  $\deg(P) = d$  und  $e = [L : K(b)] = \frac{[L:K]}{d}$ . Dann ist das charakteristische Polynom*

$$\chi_b : L \rightarrow L = P^e.$$

*Beweis.* Wenn  $L = K(b)$  dann ist  $P \mid \chi_b$  und da beide den gleichen Grad haben sind sie gleich. Allgemein ist

$$L = K(b)^e$$

als Vektorraum. Multiplikation mit  $b$  respektiert diese Zerlegung also ist  $\chi_b : L \rightarrow L = \chi_b : K(b) \rightarrow K(b) = P^e$   $\square$

**Korollar 3.6.4.** *Sei  $L/K$  endliche Körpererweiterung und  $P = X^d + a_{d-1}X^{d-1} + \dots + a_0$  das Minimalpolynom von  $b \in L$ . Dann ist*

$$\text{Tr}_{L/K}(b) = -ea_{d-1}$$

und

$$N_{L/K}(b) = (-1)^{[L:K]} a_0$$

wobei  $ed = [L : K]$

*Beweis.* Klar nach Lemma 3.6.3.  $\square$

**Satz 3.6.5.** *Wenn  $L/K$  eine endliche separable Erweiterung ist, dann ist für  $b \in L$  das Minimalpolynom*

$$\mu_b(X) = \prod_{\sigma \in \Sigma} (X - \sigma(b))$$

und das charakteristische Polynom

$$\chi_b(X) = \prod_{\sigma \in \Sigma'} (X - \sigma(b))$$

wobei  $\Sigma = \{\sigma : K(b) \rightarrow \bar{K} \mid \sigma|_K = \text{id}\}$  und  $\Sigma' = \{\sigma : L \rightarrow \bar{K} \mid \sigma|_K = \text{id}\}$ .



*Beweis.* Da  $b$  separabel ist, sind  $\sigma(b)$  die  $\deg(\mu_b)$  vielen verschiedenen Nullstellen für  $\sigma \in \Sigma$ . Somit  $\mu_b = \prod_{\sigma \in \Sigma} (X - \sigma(b))$ . Jedes  $\sigma \in \Sigma$  hat genau  $e = [L : K(b)]$  viele Fortsetzungen zu  $\sigma' \in \Sigma'$ , denn  $L/K(b)$  ist separabel und 3.5.17. Daher ist

$$\prod_{\sigma \in \Sigma'} (X - \sigma(b)) = \prod_{\sigma \in \Sigma} (X - \sigma(b))^e = \mu_b^e = \chi_b$$

nach ??.

□

**Korollar 3.6.6.** Wenn  $L/K$  endlich separabel ist und  $b \in L$ , dann ist

$$\text{Tr}_{L/K}(b) = \sum_{\sigma \in \Sigma} \sigma(b)$$

und

$$N_{L/K}(b) = \prod_{\sigma \in \Sigma} \sigma(b)$$

wobei  $\Sigma = \{\sigma : L \rightarrow \bar{K} \mid \sigma|_K = \text{id}\}$ .

*Beweis.* Klar nach Satz 3.6.5.

□

**Lemma 3.6.7.** Sei  $L$  ein Körper und  $a_1, \dots, a_n$  paarweise verschieden. Wenn  $\lambda_1, \dots, \lambda_n$  nicht alle 0 sind, dann gibt es ein  $e \geq 0$  sodass  $\sum_{i=1}^n \lambda_i a_i^e \neq 0$ .

*Beweis.* Wenn  $n = 1$  dann ist die Aussage klar. Angenommen die Aussage gilt für  $n-1$ . Angenommen die Aussage ist falsch für  $\lambda_1, \dots, \lambda_n$ . Ohne Einschränkung  $\lambda_n = -1$  sodass  $a_n^e = \sum_{i=1}^{n-1} \lambda_i a_i^e$  für alle  $e$ .

$$a_n a_n^e = a_n^{1+e} = \sum_{i=1}^{n-1} \lambda_i a_i^{1+e} = \sum_{i=1}^{n-1} \lambda_i a_i a_i^e$$

. Die erste Gleichung mit  $a_n$  Multiplizieren und beide Gleichungen voneinander abziehen liefert

$$0 = \sum_{i=1}^{n-1} \lambda_i (a_i - a_n)$$

Da nicht alle  $\lambda_i = 0$  ist  $a_i = a_n$  für ein  $i$  nach Induktion für ein  $e$  was ein Widerspruch ist.

**Satz 3.6.8.** Sei  $L/K$  eine endliche Körpererweiterung. Es ist äquivalent:

1.  $L/K$  ist separabel
2.  $\text{Tr}_{L/K} : L \rightarrow K$  ist nicht die Nullabbildung
3. Die Abbildung  $(x, y) \mapsto \text{Tr}_{L/K}(xy)$  ist nicht-ausgeartete Bilinearform  $L \times L \rightarrow K$ .

*Beweis.* Die Äquivalenz von (2) und (3) ist klar. Ohne Einschränkung hat  $K$  die Charakteristik  $p$  denn in Charakteristik 0 Fall sind alle Erweiterungen separabel und  $\text{Tr}_{L/K}(1) = [L : K] \neq 0$ . Es gilt  $\text{Tr} \neq 0$  genau dann wenn  $\text{Tr}$  surjektiv, denn  $\text{Tr}$  ist  $K$ -linear. Wenn  $L/K$  separabel, dann ist  $L = K(\alpha)$  für ein  $\alpha \in L$  nach ???. Wenn  $L/K$  inseparabel, dann gibt es  $\alpha \in L$  inseparabel über  $K$ . Da  $\text{Tr}_{L/K} = \text{Tr}_{K(\alpha)/K} \circ \text{Tr}_{L/K(\alpha)}$  ist ohne Einschränkung  $L = K(\alpha)$ . Sei  $P$  das Minimalpolynom von  $\alpha$  in  $K[X]$ . Dann ist  $P(X) = \tilde{P}(X^{p^m})$  für ein maximales  $m$  sodass  $\tilde{P}$  separabel da irreduzibel und  $P$  ist genau dann separabel, wenn  $m = 0$ . Sei  $n = \deg(P) = p^m d$  with  $d = \deg(\tilde{P})$ . In  $\bar{K}$  gilt  $\tilde{P}(X) = (X - \beta_1) \dots (X - \beta_d)$  für paarweise verschiedene  $\beta_i$ . Dann ist

$$P(X) = \tilde{P}(X^{p^m}) = \prod (X^{p^m} - \beta_i) = \prod (X - \gamma_i)^{p^m}$$

for  $\gamma_i \in \bar{K}$ . Da Körpererweiterungen treuflach sind nach ??? ist  $\text{Tr}_{L/K} : L \rightarrow K$  surjektiv genau dann wenn  $\bar{\text{Tr}} = \text{id}_{\bar{K}} \otimes \text{Tr}_{L/K}$  surjektiv ist. Da  $L = K(\alpha) = K[X]/P$  ist  $\bar{K} \otimes_K L = \prod K[X]/(X^{p^m} - \beta_i)$  und die Spur ist die Summe der Spuren auf  $\bar{K}[X]/(X^{p^m} - \beta_i)$ . Es ist  $\bar{K}[X]/(X^{p^m} - \beta_i) \cong \bar{K}[Y]/(Y^{p^m})$  unter der Substitution  $Y = X - \gamma_i$ . Wenn  $m = 0$  dann ist  $\bar{K}[Y]/(Y^{p^m}) = \bar{K}$  und die Spur ist die Identität. Wenn  $m > 0$  dann ist jedes Element in  $\bar{K}[Y]/(Y^{p^m})$  Summe von etwas Konstantem und etwas nilpotenten. Jede Konstante hat Spur 0 denn  $p^m = 0$  in  $\bar{K}$ . Jedes nilpotente Element hat auch Spur 0. Also hat jedes Element in  $\bar{K}[Y]/(Y^{p^m})$  Spur 0.

□

**Satz 3.6.9.** *Sei  $L/K$  eine endliche Galoiserweiterung und  $A \subseteq K$  normal. Sei  $B$  der ganze Abschluss von  $A$  in  $L$ . Wenn  $b \in B$  dann ist  $\text{Tr}(b) \in A$ .*

*Beweis.* Sei  $\varphi(x) = \prod_{g \in G} (X - g(b))$  mit  $G = \text{Gal}(L/K)$ . Das ist das charakteristische Polynom nach ?? und ??. Alle Koeffizienten von  $\varphi$  sind in  $K$ . Da  $B$  ganz ist über  $A$  ist auch  $g(b)$  ganz. Also sind alle Koeffizienten ganz über  $A$  und damit in  $A$  da  $A$  normal. Also ist  $\text{Tr}(b) \in A$  da  $\text{Tr}(b)$  einer der Koeffizienten ist.  $\square$

# Kapitel 4

## Hauptsatz der Galoistheorie

### 4.1 Galois Erweiterungen

**Definition 4.1.1.** Eine Körpererweiterung  $L/K$  ist eine Galoiserweiterung, wenn  $L/K$  normal und separable ist. In dem Fall ist  $\text{Gal}(L/K) = \text{Aut}_K(L)$

**Satz 4.1.2.** Sei  $L/K$  endlich. Dann ist  $|\text{Aut}_K(L)| \leq [L : K]$  und Gleichheit gilt genau dann, wenn  $L/K$  Galoisch.

*Beweis.* Wähle algebraischen Abschluss  $\bar{L}/L$ . Es gilt

$$\text{Aut}_K(L) = \text{Hom}_K(L, L) \subseteq \text{Hom}_K(L, \bar{L})$$

Somit  $|\text{Aut}_K(L)| \leq [L : K]_s \leq [L : K]$ . Gleichheit in 1 ist genau dann, wenn  $L/K$  normal und Gleichheit in 2 genau dann, wenn  $L/K$  separable.  $\square$

**Beispiel 4.1.3.** Sei  $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$  wobei  $\zeta = e^{2\pi i/3}$ . Es ist  $[L : K] = 6$  und  $L/K$  Galoisch. Sei  $N = \{a, \zeta a, \zeta^2 a\}$  und  $\sigma \in \text{Gal}(L/K)$   $\sigma(N) \subseteq N$ . Haben also

$$\psi: \text{Gal}(L/K) \rightarrow S(N) \cong S_3, \sigma \mapsto \sigma|_N$$

$\psi$  ist injektiv denn  $\sigma$  ist Identität auf  $\mathbb{Q}$  also muss es sich auf Erzeugern unterscheiden. Da  $|\text{Gal}(L/K)| = [L : K] = 6 = |S_3|$  ist  $\psi$  bijektiv.

### 4.2 Galois Korrespondenz

**Definition 4.2.1.** Sei  $L$  ein Körper und  $G \subseteq \text{Aut}(L)$  Untergruppe. Der Körper der  $G$ -Invarianten ist  $L^G = \{x \in L \mid \sigma(x) = x \forall \sigma \in G\}$

**Lemma 4.2.2.** Wenn  $L/K$  endlich Galoisch ist mit  $G = \text{Gal}(L/K)$ , dann ist  $K = L^G$ .

*Beweis.* Es gilt  $K \subseteq L^G \subseteq L$  und  $G \subseteq \text{Aut}_{L^G}(L)$ . Es ist  $L/L^G$  Galoisch und deshalb

$$[L : K] \geq [L : L^G] = |\text{Aut}_{L^G}(L)| \geq |G| = [L : K]$$

Somit  $[L^G : K] = 1$  und  $L^G = K$ .  $\square$

**Satz 4.2.3.** Sei  $G \subseteq \text{Aut}(L)$  eine endliche Untergruppe und  $K = L^G$ . Dann ist  $L/K$  Galoisch und  $[L : K] = |G|$  und  $\text{Gal}(L/K) = G$ .

*Beweis.* Sei  $b \in L$  und  $N \subset L$  die  $G$ -Bahn von  $b$ , das heißt  $N = \{\sigma(b) \mid \sigma \in G\} = \{b_1, \dots, b_r\}$  wobei  $r = |N|$ . Sei  $f = \prod_{i=1}^r (X - b_i) \in L[X]$ . Es ist

$$f^\sigma = \prod_i (X - b_i)^\sigma = \prod_i (X - \sigma(b_i)) = \prod_i (X - b_i) = f$$

für alle  $\sigma \in G$ . Also ist  $f \in K[X]$  und  $b$  algebraisch über  $K$  und separable da  $f$  in verschiedene Nullstellen zerfällt. Also ist  $L/K$  Galoisch. Angenommen  $[L : K] > |G|$ . Sei  $G = \{\sigma_1, \dots, \sigma_n\}$ . Wähle

$y_1, \dots, y_m \in L$   $K$ -linear unabhängig und sei  $A$  die Matrix  $A = (\sigma_i(y_j))_{i,j} \in M_{n \times m}(L)$ . Aus  $m > n$  folgt es gibt ein  $b \in L^m \setminus \{0\}$  im Kern von  $A$ . Sei  $b = (b_1, \dots, b_m)$  und  $\sigma(b) = (\sigma(b_1), \dots, \sigma(b_m))$ . Dann ist  $A \cdot \sigma(b) = 0$ . Sei  $\ell(b)$  die Anzahl der  $j$  mit  $b_j \neq 0$ . Wähle also  $b \neq 0$  mit  $Ab = 0$  und  $\ell(b)$  minimal. Ohne Einschränkung  $b_j = 1$  für ein  $j$ . Für  $\sigma \in G$  ist  $\ell(b - \sigma(b)) < \ell(b)$  da  $\sigma(1) = 1$  und  $A(b - \sigma(b)) = 0$ . Da  $\ell(b)$  minimal ist  $b = \sigma(b)$  und somit  $b \in K^m$ . Da  $Ab = 0$  ist  $\sum_{j=1}^m y_j b_j = 0$  und somit sind die  $y_i$  linear abhängig. Was ein Widerspruch darstellt. Also ist  $[L : K] = |G|$  und damit

$$|G| \leq |\text{Gal}(L/K)| = [L : K] = |G|$$

also  $G = \text{Gal}(L/K)$  □

**Beispiel 4.2.4.**  $\mathbb{F}_q$  ist Galoisch über  $\mathbb{F}_p$ . Sei  $\phi: \mathbb{F}_q \rightarrow \mathbb{F}_q, \phi(x) = x^p$  der Frobenius. Es ist  $G = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi \rangle$ , denn  $\phi(x) = x \iff x^p - x = 0$  hat nur  $p$  verschiedene Lösungen. Also ist  $\mathbb{F}_p \subseteq \mathbb{F}_q^{(\phi)}$  eine Gleichheit. Der Satz zeigt, dass  $G$  von  $\phi$  erzeugt ist.

**Satz 4.2.5** (Galoiskorrespondenz). Sei  $L/K$  eine endliche Galoiserweiterung und  $G = \text{Gal}(L/K)$ .

1. Folgende Abbildungen sind zueinander inverse Bijektionen:

$$\begin{array}{ccc} \{\text{Untergruppen } H \subseteq G\} & \xrightarrow{H \mapsto L^H} & \{\text{Zwischenkörper } K \subseteq M \subseteq L\} \\ & \xleftarrow{\text{Gal}(L/M) \mapsto M} & \end{array}$$

2. Wenn  $H$  mit  $M$  korrespondiert, dann ist  $[M : K] = [G : H]$  oder äquivalent  $[L : M] = |H|$

3. Wenn  $\sigma \in G$  ist und  $M$  zu  $H$  korrespondiert, dann korrespondiert  $\sigma(M)$  zu  $\sigma H \sigma^{-1}$

4. wenn  $H_1$  zu  $M_1$  korrespondiert und  $H_2$  zu  $M_2$  korrespondiert, dann ist

$$H_1 \subseteq H_2 \iff M_1 \supseteq M_2$$

5.  $M = K$  korrespondiert zu  $H = G$  und  $M = L$  korrespondiert zu  $H = \{e\}$ .

*Beweis.*

1. Man prüft leicht, dass beide Abbildungen wohldefiniert sind. Wenn  $K \subseteq M \subseteq L$  Zwischenkörper ist, dann ist  $M = L^{\text{Gal}(L/M)}$  wegen Lemma 4.2.2. Wenn  $H \subseteq G$  eine Untergruppe ist, dann ist  $H = \text{Gal}(L/L^H)$  nach Satz 4.2.3.

2.

$$[M : K][L : M] = [L : K] = |G| = |H|[G : H]$$

$$\text{und } [L : M] = |\text{Gal}(L/M)| = |H|$$

3. Sei  $\tau \in G$

$$\begin{aligned} \tau \in \text{Gal}(L/M) &\iff \tau(b) = b, \forall b \in M \\ &\iff \sigma \tau \sigma^{-1} \sigma(b) = \sigma(b), \forall b \in M \\ &\iff \sigma \tau \sigma^{-1}(c) = c, \forall c \in \sigma(M) \\ &\iff \sigma \tau \sigma^{-1} \in \text{Gal}(L/\sigma(M)) \end{aligned}$$

4. Klar

5. klar □

**Satz 4.2.6.** Sei  $L/K$  endlich Galoisch. Korrespondiere  $M$  zu  $H$  in der Galoiskorrespondenz. Es gilt

$$\begin{aligned} M/K \text{ Galoisch} &\iff M/K \text{ normal} \\ &\iff H \subseteq G \text{ ist normale Untergruppe.} \end{aligned}$$

In dem Fall gilt  $\text{Gal}(M/K) \cong G/H$ .

*Beweis.*  $L/K$  separable  $\implies M/K$  separable. Somit gilt die erste Äquivalenz. Jeder  $K$ -Homomorphismus

$$\sigma: M \rightarrow \bar{L}$$

hat Fortsetzung zu einem  $K$ -Homomorphismus

$$\tilde{\sigma}: L \rightarrow \bar{L}.$$

Da  $L/K$  normal ist, gilt  $\tilde{\sigma}(L) = L$  das heißt  $\tilde{\sigma} \in \text{Aut}(L/K) = \text{Gal}(L/K) = G$

$$\begin{aligned} M/K \text{ normal} &\iff \forall \sigma \in \text{Hom}_K(M, \bar{L}) : \sigma(M) = M \\ &\iff \forall \tilde{\sigma} \in G : \tilde{\sigma}(M) = M \\ &\iff \text{Für jedes } \tilde{\sigma} \in G : \tilde{\sigma}H\tilde{\sigma}^{-1} = H \\ &\iff H \subseteq G \text{ normal.} \end{aligned}$$

Sei  $M/K$  normal. Für  $g \in G$  ist  $g(M) = M$ . Somit haben wir einen Homomorphismus von Gruppen  $\psi: \text{Gal}(L/K) \rightarrow \text{Gal}(M/K), \sigma \mapsto \sigma|_M$ . Jedes  $\tau \in \text{Gal}(M/K) = \bar{G}$  hat Fortsetzung zu  $\bar{\tau} \in \text{Gal}(L/K)$ . Somit ist  $\psi$  surjektiv.  $\psi$  induziert  $\text{Gal}(L/K)/\ker(\psi) \xrightarrow{\sim} \text{Gal}(M/K)$  und

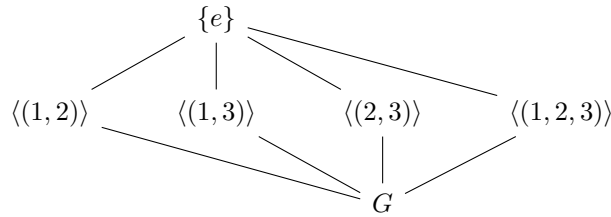
$$\ker(\psi) = \{g \in G \mid g|_M = \text{id}\} = \{g \in \text{Aut}(L) \mid g|_M = \text{id}\} = \text{Gal}(L/M) = H.$$

□

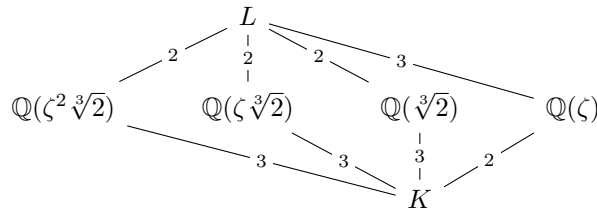
**Korollar 4.2.7.** Wenn  $L/K$  endlich separable ist, dann hat  $L/K$  nur endlich viele Zwischenkörper.

*Beweis.* Sei  $\bar{L}/K$  eine normale Hülle von  $L/K$ .  $\bar{L}/K$  ist Galoisch. Zwischenkörper von  $L/K$  sind Zwischenkörper von  $\bar{L}/K$ . Diese korrespondieren zu Untergruppen von  $G = \text{Gal}(\bar{L}/K)$ . Die letzte Menge ist endlich. □

**Beispiel 4.2.8.** Sei  $L$  Zerfällungskörper von  $X^3 - 2$  über  $K = \mathbb{Q}$ . Die Abbildung  $\psi: G \rightarrow S_3$  sei definiert durch Formel  $\sigma(a_i) = a_{\psi(\sigma)(i)}$  für  $a_1 = \sqrt[3]{2}, a_2 = \zeta a_1, a_3 = \zeta^2 a_1$ . Untergruppen von  $G$  sind



Das entspricht den Teilkörpern



### 4.3 Satz vom Primitiven Element

**Satz 4.3.1** (Satz vom primitiven Element). Sei  $L/K$  eine endliche separable Erweiterung. Dann gibt es ein  $a \in L$  mit  $L = K(a)$ .

*Beweis.* Wenn  $K$  endlich ist, dann ist  $L = \mathbb{F}_q$  endlich.  $L^* = \mathbb{Z}/(q-1)\mathbb{Z}$  ist zyklisch. Sei  $a \in L^*$  Erzeuger als Gruppe. Dann ist  $L = \{0\} \cup \{a^n \mid n \in \mathbb{N}\}$  und somit  $L = K(a)$ . Wenn  $K$  unendlich, wähle  $a \in L$  sodass  $[K(a) : K]$  maximal ist und sei  $b \in L$ . Für  $c \in K$  sei  $M_C = K(a + cb)$ . Da es nach Korollar 4.2.7 nur endlich viele Zwischenkörper gibt, gibt es nur endlich viele Möglichkeiten für  $M_C$ . Somit gibt es  $c_1 \neq c_2$  mit  $M_{c_1} = M_{c_2}$ . Dann ist  $a + c_1 b, a + c_2 b \in K(a + c_1 b) = K(a + c_2 b)$ . Also ist  $(c_1 - c_2)b \in M_{c_1}$  also ist  $b \in M_{c_1}$  und damit  $a \in M_{c_1}$ . Somit  $K(a) \subseteq K(a + c_1 b)$  und wegen Maximalität von  $[K(a) : K]$  ist  $K(a) = M_{c_1}$ . Somit  $b \in K(a)$  also  $L = K(a)$ . □

## 4.4 Kompositum und Translationssatz

**Definition 4.4.1.** Sei  $L/K$  eine Körpererweiterung und  $M_1, M_2$  zwei Zwischenkörper. Die Komposition  $M_1 M_2$  ist der kleinste Teilkörper von  $L$ , der  $M_1$  und  $M_2$  enthält.

**Satz 4.4.2.** Sei  $L/K$  eine endliche Galoiserweiterung und  $G = \text{Gal}(L/K)$ . Wenn  $M_1, M_2$  jeweils zu  $H_1, H_2$  korrespondieren, dann korrespondiert  $M_1 M_2$  zu  $H_1 \cap H_2$  und  $M_1 \cap M_2$  korrespondiert zu  $\langle H_1, H_2 \rangle$ .

*Beweis.* Der kleinste Teilkörper der  $M_1$  und  $M_2$  enthält korrespondiert zu größten Untergruppe von  $G$ , die in  $H_1$  und  $H_2$  liegt. Analog folgt die andere Aussage.  $\square$

**Satz 4.4.3** (Translationssatz). Sei  $L/K$  eine endliche Galoiserweiterung und  $K \subseteq M \subseteq L$  sodass  $M/K$  Galoisch. Sei  $K \subseteq K' \subseteq L$  ein Zwischenkörper und  $M' = MK'$  Kompositum. Dann ist  $M'/K'$  Galoisch und  $\text{Gal}(M'/K') \cong \text{Gal}(M/M \cap K')$ . Insbesondere ist  $[M' : K'] = [M : K' \cap M]$

$$\begin{array}{ccccc} M & \text{---} & MK' & \text{---} & L \\ & | & & | & \\ K & \text{---} & K' \cap M & \text{---} & K' \end{array}$$

*Beweis.*  $M/K$  ist der Zerfällungskörper von separablen Polynomen  $f \in K[X]$ . Dann ist  $M'/K'$  der Zerfällungskörper von den selben Polynomen aufgefasst in  $K'[X]$ . Somit ist  $M'/K'$  Galoisch. Für  $\sigma \in \text{Gal}(M'/K')$  ist  $\sigma|_K = \text{id}_K$ . Da  $M/K$  normal ist, folgt  $\sigma(M) = M$  das heißt  $\sigma|_M \in \text{Gal}(M/K)$ . Das gibt Gruppenhomomorphismus

$$\psi: \text{Gal}(M'/K') \rightarrow \text{Gal}(M/K), \sigma \mapsto \sigma|_M$$

. Angenommen  $\psi(\sigma) = \text{id}$  Dann ist  $\sigma|_{MK'} = \text{id}$  also  $\sigma = \text{id}$ . Also ist  $\psi$  injektiv. Sei  $H \subseteq \text{Gal}(M/K)$  das Bild. Dann ist

$$\begin{aligned} M^H &= M^{\psi(\text{Gal}(M'/K'))} \\ &= \{x \in M \mid \sigma(x) = x \ \forall \sigma \in \text{Gal}(M'/K')\} \\ &= M \cap \{x \in M' \mid \sigma(x) = x \ \forall \sigma \in \text{Gal}(M'/K')\} \\ &= M \cap K' \end{aligned}$$

Also ist  $H = \text{Gal}(M/M \cap K')$   $\square$

## Kapitel 5

# Anwendungen der Galoistheorie

### 5.1 Endliche Körper

**Lemma 5.1.1.** Sei  $K$  ein beliebiger Körper der Charakteristik  $p > 0$ . Die Abbildung  $\phi: K \rightarrow K$ ,  $\phi(x) = x^p$  ist ein Ringhomomorphismus. Wenn  $K$  endlich ist, dann ist  $\phi$  bijektiv.

*Beweis.* Es ist

$$\phi(x + y) = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i} = y^p + x^p = \phi(x) + \phi(y)$$

$\phi$  ist immer injektiv. Wenn  $K$  endlich ist, dann automatisch bijektiv.  $\square$

**Definition 5.1.2.** Sei  $q = p^r$  und  $\mathbb{F}_q$  ein Zerfällungskörper von  $x^q - x$  über  $\mathbb{F}_p$ .

**Satz 5.1.3.** Sei  $q = p^r$  für eine Primzahl  $p$ .  $\mathbb{F}_q$  ist ein endlicher Körper mit  $q$  Elementen und jeder endlich Körper ist isomorph zu  $\mathbb{F}_q$  für ein  $q = p^r$  wobei  $p = \text{char } K$ .

*Beweis.* Sei  $K$  irgendein endlicher Körper der Charakteristik  $p > 0$  und  $b \in K$ . Es ist  $(X^q - X)(b) = 0 \iff \phi^r(b) = b$ . Dann ist  $\{x \in K \mid \phi^r(x) = x\}$  ein Teilkörper von  $K$ . In  $\mathbb{F}_q[X]$  zerfällt  $X^q - X$  in Linearfaktoren. Die Ableitung ist  $(X^q - X)' = -1$  was teilerfremd ist zu  $X^q - X$ . Also ist  $X^q - X$  separable. Also hat  $X^q - X$   $q$ -viele verschiedene Nullstellen, die einen Teilkörper  $L \subseteq \mathbb{F}_q$  bilden. Somit  $\mathbb{F}_q = L$  und  $|\mathbb{F}_q| = q$ . Sei  $K$  ein endlicher Körper der Charakteristik  $p$ . Dann ist  $[K : \mathbb{F}_p] = r < \infty$  und damit  $|K| = p^r = q$ . Für  $a \in K$  gilt  $a^q = a$ . Denn wenn  $a = 0$  dann ist das richtig und wenn  $a \neq 0$  dann ist  $a \in K^*$  und  $|K^*| = q - 1$ . Nach gilt  $a^{q-1} = 1$  also  $a^q = a$  für alle  $a \in K$ . Das heißt  $x^q - x$  zerfällt in  $K[X]$  und somit gibt es Homomorphismus  $\mathbb{F}_q \rightarrow K$  mit  $|\mathbb{F}_q| = q = |K|$  also ist  $\mathbb{F}_q \cong K$ .  $\square$

**Satz 5.1.4.** Sei  $K$  ein beliebiger Körper und  $G \subseteq K^*$  eine endliche Untergruppe. Dann ist  $G$  zyklisch.

*Beweis.* Sei  $n = |G|$ . Der Struktursatz für endlich abelsche Gruppen impliziert

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

mit  $m_1 | m_2 | \dots | m_r$  und  $n = \prod_{i=1}^r m_i$ . Für jedes  $a \in G$  gilt  $a^{m_r} = 1$ . Sei also  $f = X^{m_r} - 1$ . Jedes  $a \in G$  ist Nullstelle von  $f$  und  $f$  hat höchstens  $m_r$  verschiedene Nullstellen. Somit ist  $n = m_r$  und  $G \cong \mathbb{Z}/m_r\mathbb{Z}$  zyklisch.  $\square$

**Korollar 5.1.5.** Wenn  $K$  ein endlicher Körper ist, dann ist  $K^*$  zyklisch mit  $K^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$

**Beispiel 5.1.6.** Sei  $K = \mathbb{C}$  und  $G = \{z \in \mathbb{C} \mid z^n = 1\} = \mu_n(\mathbb{C})$ . Dann ist  $G$  zyklisch.  $x^n - 1$  ist separable da die Ableitung nicht 0 ist. Somit ist  $G \cong \mathbb{Z}/n\mathbb{Z}$   $G = \{e^{2\pi i k/n} \mid 0 \leq k \leq n-1\}$  erzeugt von  $e^{2\pi i/n}$ . Es gilt:  $e^{2\pi i k/n}$  erzeugt  $\mu_n(\mathbb{C})$  genau dann wenn  $\text{ggT}(k, n) = 1$ .

**Definition 5.1.7.** Sei  $f \in K[X]$  ein separables Polynom und  $L/K$  ein Zerfällskörper von  $f$ . Die Galoisgruppe von  $f$  ist  $\text{Gal}(L/K)$

**Bemerkung 5.1.8.** Sei  $N$  die Menge der Nullstellen von  $f$  in  $L$ . Haben injektiven Gruppenhomomorphismus  $\text{Gal}(L/K) \rightarrow S(N) \cong S_n$ ,  $\sigma \mapsto \sigma|_N$  wobei  $n = \deg(f) = |N|$ . Das zeigt

**Satz 5.1.9.** Wenn  $L/K$  Zerfällungskörper eine separablen Polynoms  $f$  von Grad  $n$  ist, dann  $\text{Gal}(L/K) \rightarrow S_n$  injektiv.

**Definition 5.1.10** (Diskriminante). Sei  $f \in K[X]$  ein normiertes Polynom,

$$f = \prod_{i=1}^n (X - \alpha_i)$$

in  $\bar{K}[X]$  und  $n = \deg(f)$ . Sei

$$\delta = \prod_{\substack{i,j \in \{1, \dots, n\} \\ i < j}} (\alpha_i - \alpha_j) \in \bar{K}.$$

Dann ist  $\Delta = \delta^2 \in \bar{K}$  die Diskriminante von  $f$

**Lemma 5.1.11.** Es ist  $\Delta \in K$  und es gilt

$$\Delta \neq 0 \iff f \text{ ist separable.}$$

*Beweis.* Sei  $\Delta \neq 0$  und  $L/K$  Zerfällungskörper von  $f$ . Dann ist  $L/K$  Galois und für  $\sigma \in G = \text{Gal}(L/K)$  gilt

$$\sigma(\alpha_i) - \sigma(\alpha_j) = \alpha_{i'} - \alpha_{j'} = -(\alpha_{j'} - \alpha_{i'})$$

und einer der letzten beiden Terme taucht als Faktor in  $\delta$  auf. Also ist  $\sigma(\delta) = \pm\delta$  und damit  $\sigma(\Delta) = \Delta$ . Also gilt  $\Delta \in L^G = K$ .  $\square$

**Bemerkung 5.1.12.** Wenn  $f$  separabel, dann ist für  $\sigma \in \text{Gal}(L/K)$

$$\sigma(\delta) = \text{sign}(\sigma)\delta$$

wobei wir  $\sigma$  als Element in  $S_n$  auffassen.

**Bemerkung 5.1.13.** sei  $f \in K[X]$  und  $n = \deg(f)$ .

1. Sei  $n = 2$  und  $f = X^2 + pX + q = (X - \alpha_1)(X - \alpha_2) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2$  und

$$\Delta = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q$$

2. Sei  $n = 3$  und  $\text{char}(K) \notin \{2, 3\}$  und  $f = X^3 + a_2X^2 + a_1X + a_0$ . Für  $Y = X + \frac{1}{3}a_2$  erhalten wir können wir  $X$  ersetzen und behalten die gleiche Diskriminante. Wir bekommen

$$\begin{aligned} f &= (Y - \frac{1}{3}a_2)^3 + a_2(Y - \frac{1}{3}a_2)^2 + a_1(Y - \frac{1}{3}a_2) + a_0 \\ &= Y^3 + aY + b \end{aligned}$$

für irgendwelche  $a, b \in K$ . Sei also  $f = X^3 + aX + b$ . Eine ähnliche Rechnung wie für  $n = 2$  ergibt  $\Delta = -4a^3 - 27b^2$

**Satz 5.1.14.** Sei  $\text{char}(K) \notin \{2, 3\}$  und  $f = X^3 + aX + b \in K[X]$  irreduzibel. Dann ist ein Zerfällungskörper  $L/K$  von  $f$  Galois. Es ist  $\text{Gal}(L/K) \subseteq S_3$ .

1.  $\Delta$  ist Quadrat in  $K \implies G = A_3 \cong \mathbb{Z}/3\mathbb{Z}$

2.  $\Delta$  kein Quadrat in  $K \implies G = S_3$

*Beweis.* Da  $f$  irreduzibel gilt für eine Nullstelle  $\alpha$  von  $f$  dass  $[K(\alpha) : K] = 3$  ist. Also ist  $[L : K] \in \{3, 6\}$ . Die einzigen Untergruppen von  $S_3$  mit 3 bzw. 6 Elementen sind  $A_3$  bzw.  $S_3$

$$\begin{aligned} G = A_3 &\iff G = \ker(\text{sign}: S_3 \rightarrow \{\pm 1\}) \\ &\iff \forall \sigma \in G : \text{sign}(\sigma) = 1 \\ &\iff \forall \sigma \in G : \sigma(\delta) = \delta \\ &\iff \delta \in L^G = K \\ &\iff \Delta \text{ ist Quadrat in } K \end{aligned}$$

$\square$



**Beispiel 5.1.15.** Sei  $f = X^3 - a$  wobei  $a$  keine dritte Potenz in  $K = \mathbb{Q}$  ist.  $f$  hat keine Nullstelle also ist  $f$  irreduzibel.  $\Delta = -27a^2$  ist kein Quadrat in  $\mathbb{Q}$ . Also ist  $\text{Gal}(L/K) = S_3$

**Lemma 5.1.16.** Sei  $R$  faktoriell und  $g, h \in K[X]$  normiert und sei  $K = \text{Quot}(R)$ . Wenn  $g \cdot h \in R[X]$  dann ist  $g, h \in R[X]$ .

*Beweis.* Es ist  $g/c(g), h/c(h) \in R[X]$ . Also sind  $1/c(g), 1/c(h) \in R$  da  $g, h$  normiert. Es ist  $1 = c(gh) = c(g)c(h)$  also ist  $1/c(g), 1/c(h) \in R^*$  also ist  $c(g), c(h) \in R^*$  also ist  $h, g \in R[X]$ .  $\square$

**Korollar 5.1.17.** Wenn  $f \in \mathbb{Z}[X]$  normiert ist und  $a \in \mathbb{Q}$  eine Nullstelle von  $f$ , dann ist  $f = (X - a) \cdot g$ , wobei  $g$  normiert ist. Dann ist  $a \in \mathbb{Z}$  und  $g \in \mathbb{Z}$ .

**Beispiel 5.1.18.**  $X^3 - 3x + 1$  mögliche Nullstellen in  $\mathbb{Q}$  sind Teiler von 1 in  $\mathbb{Z}$ . Das sind aber keine Nullstellen, also ist  $f$  irreduzibel in  $\mathbb{Q}[X]$ .  $\Delta = -4(-3)^3 - 27 \cdot 1^2 = 3^4$  ist Quadrat, also  $\text{Gal}(L/K) = A_3$

## 5.2 Kreisteilungskörper

**Definition 5.2.1.** Sei  $K$  ein Körper und  $\mu_n(K) = \{x \in K \mid x^n = 1\}$  Gruppe der  $n$ -ten Einheitswurzeln in  $K$ .

**Satz 5.2.2.** Sei  $\text{char}(K) \nmid n$ . Dann ist  $\mu_n(\bar{K})$  zyklisch von Ordnung  $n$ .

*Beweis.*  $f = X^n - 1$  und  $f' = nX^{n-1} \neq 0$ . Einzige Nullstelle von  $f'$  ist  $x = 0$  aber  $f(0) \neq 0$ . Somit ist  $\text{ggT}(f, f') = 1$  und damit  $f$  separabel.  $\square$

**Definition 5.2.3.** Sei  $\text{char}(K) \nmid n$ . Ein  $\zeta \in \mu_n(K)$  heißt primitive  $n$ -te Einheitswurzel, wenn  $\zeta$  die Gruppe  $\mu_n(\bar{K})$  erzeugt. Sei  $K(\zeta_n) = K(\mu_n(\bar{K}))$  der Zerfällungskörper von  $x^n - 1$ .  $K(\zeta_n)$  heißt der  $n$ -te Kreisteilungskörper über  $K$ .

**Lemma 5.2.4.** Sei  $G$  eine zyklische Gruppe mit  $|G| = n$ . Dann ist  $\text{End}(G) \cong \mathbb{Z}/n\mathbb{Z}$  als Ring und  $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$  als Gruppe.

*Beweis.* Wähle Isomorphismus  $\psi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$  Wenn  $f: G \rightarrow G$  Endomorphismus ist, dann ist  $\psi^{-1}f\psi$  ein Endomorphismus von  $\mathbb{Z}/n\mathbb{Z}$ . somit  $\text{End}(G) \cong \text{End}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$  denn Endomorphismen eindeutig bestimmt durch  $f(1) = a$ .  $\square$

**Definition 5.2.5.** Die Anzahl der zu  $n$  teilerfremden Zahlen in  $\{0, 1, \dots, n-1\}$  ist

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Die Funktion  $\varphi$  heißt Eulersche  $\varphi$ -Funktion

**Lemma 5.2.6.** Es gilt

1.  $\text{ggT}(n, m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$
2.  $\varphi(\text{kgV}(n, m))\varphi(\text{ggT}(n, m)) = \varphi(n)\varphi(m)$
3. Wenn  $n = \prod_{i=1}^r p_i^{e_i}$  wobei  $p_i$  paarweise verschiedene Primzahlen, dann ist

$$\varphi(n) = \prod_{i=1}^n \varphi(p_i^{e_i}) = \prod_{i=1}^n (p_i - 1)p_i^{e_i-1}$$

*Beweis.* Nach Chinesischem Restsatz ist  $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  also gilt die erste Aussage. Die zweite Aussage folgt aus der ersten. Für die dritte reicht  $\varphi(p^e) = p^{e-1}(p-1)$  für eine Primzahl  $p$ . Nicht-Einheiten in  $\mathbb{Z}/p^e\mathbb{Z}$  sind  $0, p, 2p, \dots, (p^{e-1}-1)p$ , das sind also  $p^{e-1}$  viele. Somit  $|(\mathbb{Z}/p^e\mathbb{Z})^*| = p^e - p^{e-1}$   $\square$

**Satz 5.2.7.** Sei  $L = K(\zeta_n)/K$ . Die Abbildung

$$\psi: \text{Gal}(L/K) \rightarrow \text{Aut } \mu_n(\bar{K}), \sigma \mapsto \sigma|_{\mu_n(L)}$$

ist ein injektiver Gruppenhomomorphismus.

*Beweis.*  $\psi$  ist injektiv, da  $L/K$  von  $\mu_n(L)$  erzeugt ist.  $\square$

**Korollar 5.2.8.** *Sei*

$$\phi: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \text{Aut}(\mu_n(\bar{K})), \quad a \mapsto (\mu_n(\bar{K}) \rightarrow \mu_n(\bar{K}), \quad \zeta \mapsto \zeta^a)$$

der Isomorphismus aus Lemma 5.2.4. Dann ist

$$\chi = \phi^{-1}\psi: G \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

gegeben durch

$$\zeta^{\chi(\sigma)} = \zeta^{\phi^{-1}(\sigma|_{\mu_n(\bar{K})})} = \sigma(\zeta).$$

Insbesondere ist  $\chi$  injektiv und  $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$  und dadurch  $\chi(\sigma)$  schon bestimmt.

**Korollar 5.2.9.**  $\text{Gal}(K(\zeta_n)/K)$  ist eine abelsche Gruppe.

**Beispiel 5.2.10.**  $K = \mathbb{R}$  und  $n \geq 3$ . Dann ist  $\mu_n(\mathbb{C}) \subsetneq \mathbb{R}$  und somit  $K(\mu_n(\mathbb{C})) = \mathbb{C}$ .  $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma\}$  wobei  $\sigma$  die komplexe Konjugation ist. Es ist  $\chi(\sigma) = -1$  denn für  $\zeta \in \mu_n(\mathbb{C})$  ist  $\sigma(\zeta) = \bar{\zeta} = \zeta^{-1}$

**Satz 5.2.11.** *Sei  $q = p^r$  für eine Primzahl  $p$  und  $L/\mathbb{F}_q$  eine endliche Galoiserweiterung. Dann ist  $G = \text{Gal}(L/\mathbb{F}_q)$  von  $\phi_q$  erzeugt, wobei  $\phi_q(x) = x^q$ .*

*Beweis.*  $\mathbb{F}_q$  ist Zerfällungskörper von  $x^q - x$  über  $\mathbb{F}_p$  und  $\mathbb{F}_q = \{x \in L \mid \phi_q(x) = x\}$ . Somit ist  $\phi_q \in G$ . Für  $H = \langle \phi_q \rangle \subseteq G$  ist dann  $L^H = \mathbb{F}_q = L^G$  also ist  $H = G$ .  $\square$

**Korollar 5.2.12.** *Sei  $q = p^r$  und  $n \in \mathbb{N}$  mit  $p \nmid n$ . Sei  $L = \mathbb{F}_q(\zeta_n)$  wobei  $\zeta_n \in \bar{\mathbb{F}}_q$  primitive  $n$ -te Einheitswurzel. Sei  $\chi: \text{Gal}(L/\mathbb{F}_q) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*, \phi_q \mapsto k = \chi(\phi_q)$  wie in Korollar 5.2.8. Dann ist*

$$|\text{Gal}(L/\mathbb{F}_q)| = \text{ord}(\phi_q) = \text{ord}(\chi(\phi_q)) = \text{ord}(q \in (\mathbb{Z}/n\mathbb{Z})^*)$$

**Beispiel 5.2.13.** Sei  $n = 12$  und  $p = 7$ . Es ist  $7^2 = 49 = 48 + 1$  also ist die Ordnung von 7 gleich 2. Also  $[\mathbb{F}_7(\zeta_{12}) : \mathbb{F}_7] = |\text{Gal}(\cdot)| = 2$  und somit  $\mathbb{F}_7(\zeta_{12}) = \mathbb{F}_{49}$

**Satz 5.2.14.** *Der Homomorphismus  $\chi: \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  aus Korollar 5.2.8 ist bijektiv, das heißt  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ .*

*Beweis.* Sei  $\zeta_n \in \bar{\mathbb{Q}}$  eine primitive  $n$ -te Einheitswurzel und  $f \in \mathbb{Q}[x]$  das Minimalpolynom von  $\zeta_n$ . Wir zeigen, dass jede andere primitive  $n$ -te Einheitswurzel auch Nullstelle von  $f$  ist. Dann ist  $\deg(f)$  die Anzahl der primitiven  $n$ -ten Einheitswurzeln und somit  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ . Denn wenn  $m$  eine Einheit ist in  $\mathbb{Z}/n\mathbb{Z}$  dann ist  $\zeta_n^m$  eine primitive Einheitswurzel. Ohne Einschränkung  $m = p$  prim. Sei also  $p \nmid n$  und  $g$  Minimalpolynom von  $\zeta_n^p$ . Angenommen  $f \neq g$ . Es ist  $\zeta_n^{pn} - 1 = 0$  also teilt  $f \mid X^n - 1$ ,  $g \mid X^n - 1$  also  $f \cdot g \mid X^n - 1$ . Nach Lemma 5.1.16 folgt  $f, g \in \mathbb{Z}[X]$  und außerdem ist  $\zeta_n$  eine Nullstelle von  $g(X^p)$  also  $f \mid g(X^p)$  und  $g(X^p) = f \cdot h$  für ein  $h \in \mathbb{Z}[X]$ . In  $\mathbb{F}_p[X]$  gilt  $f \mid g(X^p) = g(X)^p$  also sind  $f$  und  $g$  nicht teilerfremd in  $\mathbb{F}_p[X]$ . Da aber  $f \cdot g \mid X^n - 1$  kommt ein irreduzibler Faktor von  $X^n - 1$  doppelt vor, was ein Widerspruch dazu ist, dass  $X^n - 1$  separabel ist über  $\mathbb{F}_p$ . Also ist  $f = g$   $\square$

**Korollar 5.2.15.** *Für  $n, m \in \mathbb{Z}$  mit  $\text{ggT}(n, m) = d$  und  $\text{kgV}(n, m) = k$  gilt*

$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d)$$

und

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_k)$$

*Beweis.* Es ist  $\mathbb{Q}(\zeta_k) \supseteq \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$ . Sei  $\zeta_n$  eine primitive  $n$ -te Einheitswurzel und  $\zeta_m$  primitive  $m$ -te Einheitswurzel und sei  $d = an + bm$  für  $a, b \in \mathbb{Z}$ . Dann ist  $\xi = \zeta_n^b \zeta_m^a$  primitive  $k$ -te Einheitswurzel, denn  $\xi^k = 1$  und wenn  $\xi^s = 1$  ist, dann ist  $\zeta_n^{sb} = \zeta_m^{-sa}$  woraus  $n \mid sbm$  und somit  $n \mid sd$  folgt. Also  $n/d \mid s$ . Analog  $m/d \mid s$  also folgt zusammen  $k \mid s$ . Also gilt

$$\mathbb{Q}(\zeta_k) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m).$$

Außerdem gilt  $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$ . Für  $M = \mathbb{Q}(\zeta_n)$ ,  $K' = \mathbb{Q}(\zeta_n)$ ,  $K = \mathbb{Q}$  und  $M' = MK'$  gilt nach Satz 4.4.3

$$\begin{aligned}\varphi(k)\varphi(d) &= \varphi(n)\varphi(m) \\ &= [M : K] \cdot [K' : K] \\ &= [M' : K][K' \cap M : K] \\ &= \varphi(k)[K' \cap M : K]\end{aligned}$$

Also  $K' \cap M = \mathbb{Q}(\zeta_d)$  □

**Definition 5.2.16.** Sei  $n \in \mathbb{N}$ . Das  $n$ -te Kreisteilungspolynom ist

$$\phi_n = \prod_{\substack{\zeta \in \mu_n(\mathbb{C}) \\ \text{primitiv}}} (X - \zeta) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta_n^k) \in \mathbb{C}[X]$$

für  $\zeta_n = e^{2\pi i/n}$

**Lemma 5.2.17.** Es gilt

$$X^n - 1 = \prod_{d|n} \phi_d$$

*Beweis.* Es ist

$$X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta)$$

und jedes  $\zeta$  ist eine primitive  $d$ -te Einheitswurzel für  $d = \text{ord}(\zeta)$  und jede primitive  $d$ -te Einheitswurzel für  $d | n$  ist ein Element von  $\mu_n(\mathbb{C})$ . Dann impliziert

$$\mu_n(\mathbb{C}) = \coprod_{d|n} \{\zeta_d \text{ primitive } d\text{-te Einheitswurzel}\}$$

die Aussage. □

**Lemma 5.2.18.** Es ist  $\phi_d \in \mathbb{Z}[X]$  und  $\phi_d$  ist das Minimalpolynom von  $\zeta_d$  über  $\mathbb{Q}$ .

*Beweis.* Klar □

**Bemerkung 5.2.19.** Für  $n = p$  prim gilt  $\phi_p = (X^p - 1)/(X - 1) = \sum_{k=0}^{p-1} X^k$

**Beispiel 5.2.20.**  $\mathbb{Q}(\zeta_9)/\mathbb{Q}$  hat Galoisgruppe  $(\mathbb{Z}/9\mathbb{Z})^*$  mit  $\phi(9) = 6$  Elementen. Der ??Satz:StuktEndlAb] liefert

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

und das hat die vier Untergruppen  $\{0\}, \mathbb{Z}/2\mathbb{Z} \times \{0\}, \{0\} \times \mathbb{Z}/3\mathbb{Z}$ . Das entspricht den Untergruppen  $\{1\}, \langle -1 \rangle, \langle 4 \rangle, G$ . Es ist  $\chi(\sigma) = -1$  für die komplexe Konjugation  $\sigma: \mathbb{C} \rightarrow \mathbb{C}$ . Also ist für  $L = \mathbb{Q}(\zeta_9)$

$$L^{\langle -1 \rangle} = L \cap \mathbb{C}^{\langle \sigma \rangle} = L \cap \mathbb{R} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$$

Wobei die letzte Gleichung gilt, da für  $b = \zeta_9 + \zeta_9^{-1}$

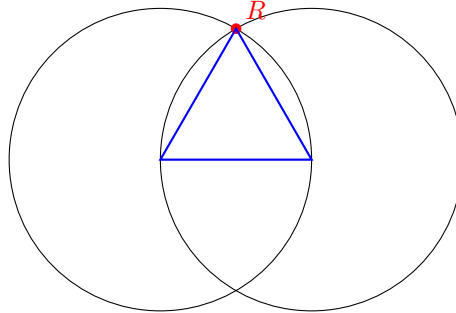
$$b\zeta_9 = \zeta_9^2 + 1$$

also ist  $\zeta_9^2 - b\zeta_9 + 1 = 0$  und somit  $[\mathbb{Q}(\zeta_9) : \mathbb{Q}(b)] \leq 2$ . Da  $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\zeta_9)$  und  $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$  folgt  $L^{\langle 4 \rangle} = \mathbb{Q}(\zeta_3)$ .

### 5.3 Konstruktion mit Zirkel und Lineal

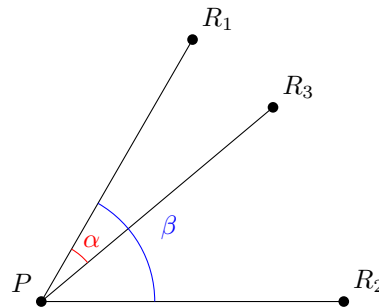
Starte mit einer Menge von Punkten in  $\mathbb{R}^2 = \mathbb{C}$ . Erlaubte Konstruktionen: Geraden durch 2 verschiedene Punkte die gegeben sind und Kreise durch 2 Punkte, einen davon der Mittelpunkt, und Schnittpunkte von 2 Objekten dieser Art.

**Beispiel 5.3.1.** Man kann gleichseitige Dreiecke konstruieren.



**Bemerkung 5.3.2.** Klassische Probleme sind

1. Winkeldreiteilung: Wenn  $P, R_1, R_2, R_3$  gegeben sind, suche  $R_3$  sodass  $3\alpha = \beta$ .



2. Würfeldoppelung: Gegeben  $P, Q$  suche  $Q'$  sodass  $|PQ'|^3 = 2|PQ|^3$ .
3. Quadratur des Kreises: Gegeben  $P, Q$  suche  $Q'$  sodass  $|PQ'|^2 = \pi|PQ|^2$ .
4. Kubatur der Kugel: Suche  $Q'$  sodass Würfel mit Kante  $PQ'$  das gleiche Volumen hat wie Kugel mit Radius  $PQ$ .
5. Konstruktion des regulären  $n$ -Ecks mit 2 gegebenen benachbarten Ecken.

**Definition 5.3.3.** Für  $z, w \in \mathbb{C}$  sei

$$\ell(z, w) = \{z + \lambda(w - z) \mid \lambda \in \mathbb{R}\}$$

die Gerade durch  $z, w$  und

$$k(z, w) = \{w' \in \mathbb{C} \mid |z - w| = |z - w'|\} = \{z + \lambda(w - z) \mid \lambda \in \mathbb{C}, |\lambda| = 1\}$$

der Kreis mit Mittelpunkt  $z$  durch  $w$ .

**Definition 5.3.4.** Für  $M \subseteq \mathbb{C}$  sei  $K(M) \subseteq \mathbb{C}$  die kleinste Menge sodass

1.  $M \subseteq K(M)$
2. Wenn  $z, w, z', w' \in K(M)$  mit  $z \neq w$  und  $z' \neq w'$  dann

$$\ell(z, w) \cap \ell(z', w') \subseteq K(M)$$

$$\ell(z, w) \cap k(z', w') \subseteq K(M)$$

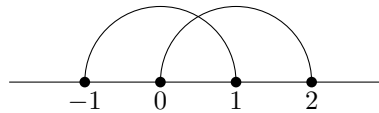
$$k(z, w) \cap k(z', w') \subseteq K(M)$$

falls die Schnitte jeweils endlich sind.

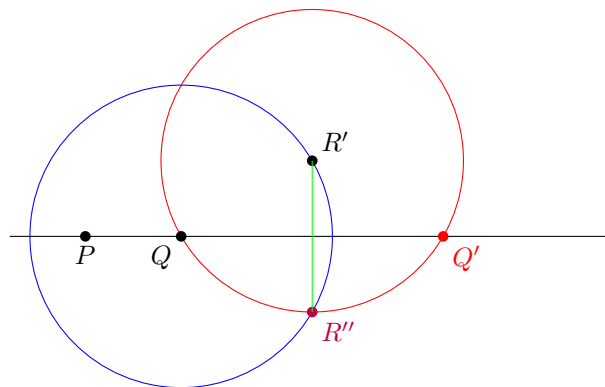
$K(M)$  ist die Menge aller Elemente von  $\mathbb{C}$  die durch endlich viele Schnitte in  $M$  wie oben gewonnen werden können. Wir nennen  $K(M)$  die Menge der aus  $M$  konstruierbaren Zahlen.

**Bemerkung 5.3.5.** Wenn  $M \neq \emptyset$  oder  $|M| = 1$  dann ist  $K(M) = M$ . Sei  $|M| \geq 2$ . Ohne Einschränkung  $0, 1 \in M$ . Es gilt

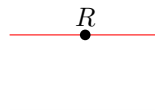
1.  $\mathbb{Z} \subseteq K(0, 1)$



2. Man kann Orthogonalen zu einer Geraden durch einen Punkt konstruieren. Seien  $P, Q$  und  $\overline{PQ}$  gegeben. Sei  $R'$  nicht auf  $\overline{PQ}$ . Bilde den roten Kreis und danach den blauen. Das gibt Schnittpunkt  $R''$ . Die grüne Gerade ist Orthogonale.



3. Parallele zu Geraden durch Punkt R

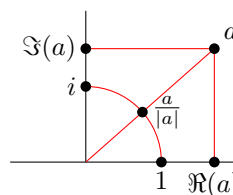


Verfahren: Bestimme Orthogonale durch  $R$ . Dann konstruiere gleichseitiges Dreieck wo  $R$  der Mittelpunkt einer Seite ist. Das gibt Parallele.

4. Verschiebung von Vektoren. Seien  $P, Q, R$  gegeben. Suche  $R + (Q - P)$ . Klar, Konstruiere Parallele, Verbinde Punkte und konstruiere parallele.

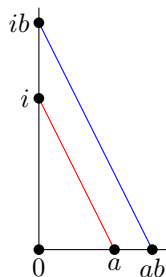
**Lemma 5.3.6.** Sei  $0, 1 \in M$  und  $a \in \mathbb{C}$ . Es ist äquivalent:

1.  $a \in K(M)$
2.  $\bar{a} \in K(M)$
3.  $\Re(a), \Im(a) \in K(M)$
4.  $|a|, \frac{a}{|a|} \in K(M)$

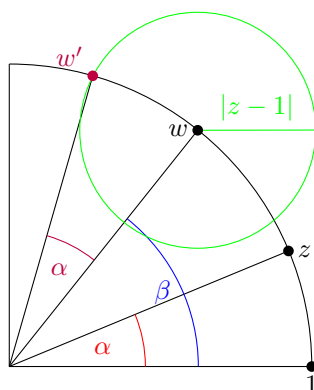


**Lemma 5.3.7.** Sei  $0, 1 \in M$ . Dann ist  $K(M)$  ein Körper. Insbesondere ist  $\mathbb{Q} \subseteq K(M)$ .

*Beweis.* Zeige, dass  $K(M)$  abgeschlossen ist unter Multiplikation und Inverse. Für Multiplikation reicht die Multiplikation von reellen Zahlen und von Zahlen mit Betrag 1 (dh. Addition von Winkeln).



Addition von Winkeln:



□

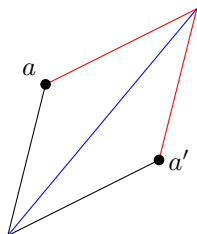
**Bemerkung 5.3.8.** Sei  $0, 1 \in M$ . Dann ist  $\mathbb{Q}(M \cup \bar{M}) \subseteq K(M)$ .

**Satz 5.3.9** (Konstruierbare Zahlen). Sei  $0, 1 \in M$  und  $a \in \mathbb{C}$ . Es gilt

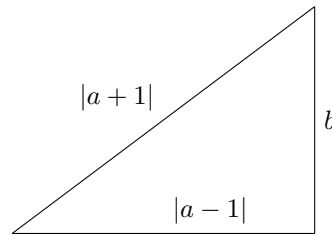
$$a \in K(M) \iff \exists \mathbb{Q}(M \cup \bar{M}) = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r \text{ mit } [K_i : K_{i-1}] = 2 \text{ und } a \in K_r.$$

Insbesondere ist  $[\mathbb{Q}(M \cup \bar{M} \cup \{a\}) : \mathbb{Q}(M \cup \bar{M})]$  eine Zweierpotenz, das heißt  $a$  ist algebraisch über  $\mathbb{Q}(M \cup \bar{M})$ .

*Beweis.* Kurzform: Schnitt von Geraden vergrößert den Körper nicht. Schnitt von Geraden mit Kreisen führt auf quadratische Gleichung. Das heißt  $K_i/K_{i-1}$  hat Grad 2. Das zeigt:  $a \in K(M)$  impliziert, dass eine Kette wie im Satz existiert. Zeige: Wenn  $L/K$  eine quadratische Erweiterung ist mit  $L \subseteq \mathbb{C}$  und  $K \subseteq K(M)$  dann ist auch  $L \subseteq K(M)$ . Sei  $L = K(b)$  wobei  $b$  eine Nullstelle von  $X^2 + cX + d$  ist. Die Substitution  $X = X - \frac{c}{2}$  erreicht  $c = 0$ . Also sei ohne Einschränkung das Polynom  $X^2 + d$  und  $b' = \sqrt{d'}$ . Zeige also: Quadratwurzeln in  $\mathbb{C}$  sind konstruierbar. Es ist  $z = |z| \cdot \frac{z}{|z|}$ . Zeige also: Wurzeln aus reellen Zahlen und Winkelhalbierungen sind konstruierbar.



Sei  $a \in \mathbb{R}$  und  $a \geq 0$ .



$$\begin{aligned} b^2 &= (a+1)^2 - (a-1)^2 \\ &= 4a \end{aligned}$$

also  $b = 2\sqrt{a}$  □

**Lemma 5.3.10.** *Sei  $K$  ein Körper und  $K = K_0 \subseteq K_1 \cdots \subseteq K_n$ ,  $K = L_0 \subseteq L_1 \cdots \subseteq L_m$  Ketten quadratischer Körpererweiterungen. Dann ist  $K = L_0 \subseteq \cdots \subseteq L_m \subseteq K_1 L_m \subseteq \cdots \subseteq K_n L_m$  Kette höchstens quadratischer Körpererweiterungen.*

*Beweis.* Es ist  $[K_i L_m : K_{i-1} L_m] \leq [K_i : K_{i-1}] = 2$  □

**Satz 5.3.11.** *Sei  $K$  ein Körper der Charakteristik  $\neq 2$  und  $a \in \bar{K}$ . Dann sind äquivalent:*

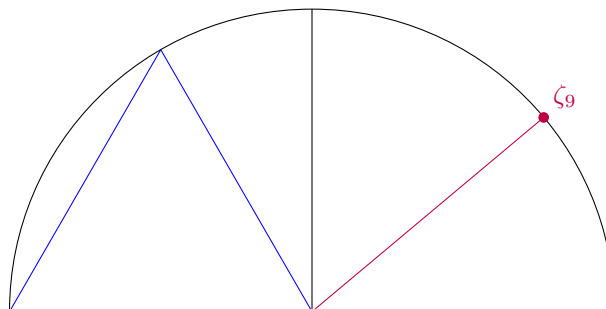
1. *Es gibt Kette quadratischer Erweiterungen  $K = K_0 \subseteq \cdots \subseteq K_n$  and  $a \in K_n$*
2. *Es gibt Galoiserweiterung  $L/K$  mit  $a \in L$  und  $[L : K] = 2^r$ .*

*Beweis.* Gelte 1 und sei  $K_n/K$  gegeben. Dann ist  $K_n/K$  separabel und nach Satz 4.3.1 gilt  $K_n = K(b)$  für ein  $b \in K_n$ . Sei  $L/K$  die normale Hülle von  $K_n/K$ . Nach Konstruktion ist  $L/K$  der Zerfällungskörper vom Minimalpolynom  $f$  von  $b$ . Seien  $b_1, \dots, b_n$  die Nullstellen von  $f$  in  $L$  mit  $b = b_1$ . Es ist  $L = K(b_1) \cdots K(b_n)$  Komposition. Da  $f$  das Minimalpolynom von  $b_i$  ist, ist  $K_n = K(b) = K(b_i)$  für alle  $i$  und somit ist  $K(b_i)/K$  durch Kette quadratischer Erweiterungen erreichbar. Nach Lemma 5.3.10 ist  $L$  als Kompositum durch quadratische Kette erreichbar. Gelte 2. und sei  $L/K$  Galois vom Grad  $2^r$ . Dann ist  $G = \text{Gal}(L/K)$  eine  $p$ -Gruppe für  $p = 2$ .  $G$  ist auflösbar somit gibt es nach Korollar 2.3.3 eine normale Untergruppe  $H \subseteq G$  mit  $[G : H] = 2$ . Sei  $K_r = L$  und  $K_1 = L^H$ . Dann ist  $[K_1 : K_0] = 2$  und  $K_r/K$  Galois von Grad  $2^{r-1}$ . Also folgt die Aussage nach Induktion. □

**Satz 5.3.12.**  $\pi \in \mathbb{R}$  ist transzendent über  $\mathbb{Q}$ .

**Korollar 5.3.13.**  $\pi \notin K(0, 1)$  da  $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ .

**Korollar 5.3.14.** Wäre Winkeldrittung immer möglich, so wäre  $\zeta_9 \in K(0, 1)$ .



Aber  $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = 6$  ist keine Zweierpotenz also Widerspruch und die Aussage ist falsch.

**Korollar 5.3.15** (Würfelverdoppelung). Ist  $\sqrt[3]{2} \in K(0, 1)$ ? Es ist

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

keine Zweierpotenz, also nein.

**Definition 5.3.16.**

1. Ein Körper  $L$  heißt quadratisch abgeschlossen, wenn jedes quadratische Polynom in  $L[X]$  in  $L$  eine Nullstelle hat.
2. Ein quadratischer Abschluss von  $K$  ist eine Erweiterung  $L/K$  sodass  $L$  quadratisch abgeschlossen ist und jede endliche Zwischenerweiterung  $L/L'/K$  lässt sich durch Kette quadratischer Erweiterungen erreichen.

**Bemerkung 5.3.17** (Konstruktion eines quadratische Abschluss). Sei

$$L = \{a \in \bar{K} \mid K(a)/K \text{ ist durch Kette quadratischer Erweiterungen erreichbar}\}.$$

Wir haben gesehen:  $K(M)$  ist der quadratische Abschluss von  $\mathbb{Q}(M \cup \bar{M})$

### 5.3.1 Konstruktion des regulären $n$ -Ecks

Sei  $E$  die Menge der Ecken des regulären  $n$ -Ecks mit  $E \subseteq S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ . Es gilt  $E = \mu_n(\mathbb{C})$ . Sei  $\zeta_n \in \mu_n(\mathbb{C})$  primitiv. Ist  $\zeta_n \in K(0, 1)$ ? Bekannt ist:  $[Q(\zeta_n)/\mathbb{Q}]$  ist Galois mit  $G = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$  und  $|G| = \varphi(n)$ . Antwort:

$$\zeta_n \in K(0, 1) \iff \varphi(n) = 2^r.$$

Wenn  $n = \prod_i p_i^{e_i}$  für verschiedene Primzahlen  $p_i$ , dann ist  $\varphi(n) = \prod (p_i - 1)p_i^{e_i-1}$ . Das ist Zweierpotenz genau dann wenn  $e_i < 2$  für  $p_i \neq 2$  und  $e_i = 1$  nur wenn  $p_i - 1$  eine Zweierpotenz ist.

**Definition 5.3.18** (Fermatsche Primzahl). Eine Fermatsche Primzahl ist eine Primzahl der Form  $p = 2^m + 1$ .

**Bemerkung 5.3.19.** Wenn  $p$  prim dann ist  $\zeta_p$  konstruierbar  $\iff p$  ist Fermatsche Primzahl

**Lemma 5.3.20.**  $2^m + 1$  prim  $\implies m = 2^r$

*Beweis.* Sei  $m = qm'$  wobei  $q$  ungerade. Dann ist nach geometrischer Summe

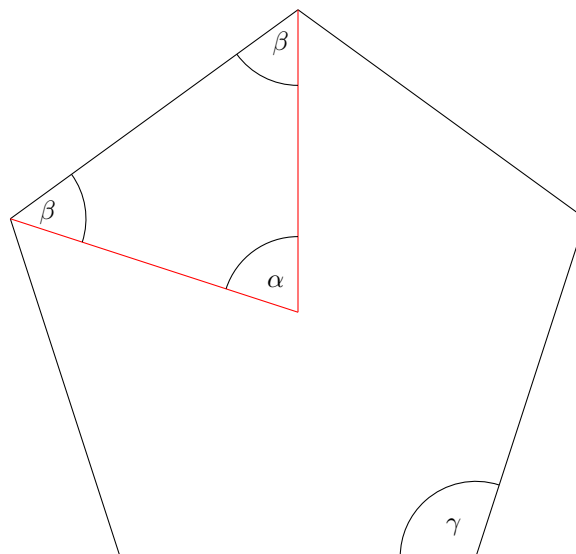
$$\frac{2^m + 1}{2^{m'} + 1} = \frac{1 - (-2^{m'})^q}{1 - (-2^{m'})} = \sum_{k=0}^{q-1} (-2^{m'})^k = \sum_{k=1}^q (-1)^{k+1} 2^{m-km'}$$

also  $2^m + 1$  nicht prim. □

**Bemerkung 5.3.21.**  $2^{2^r} + 1$  ist prim für  $r = 0, 1, 2, 3, 4$  aber für  $2^{2^5} + 1 = 641 \cdot 6700417$

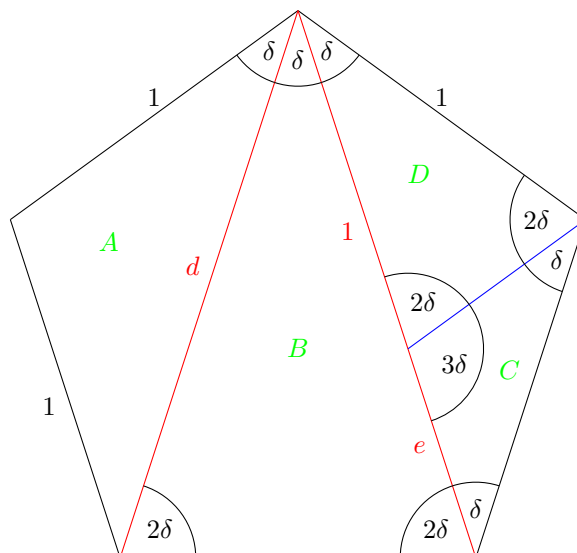
**Bemerkung 5.3.22.** Fazit: Reguläre 3, 5, 17 Eck ist konstruierbar. Reguläre 7, 11, 13, 19-Eck nicht.

**Beispiel 5.3.23.** Sei  $\alpha = \frac{2\pi}{5}$  und  $\beta = \frac{\pi-\alpha}{2} = \frac{3\pi}{16}$  und  $\gamma = 2\beta = \frac{3}{5}\pi$

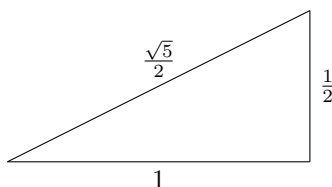


Sei weiter  $\delta = \frac{\pi-\gamma}{2}$ . Dann ist  $\delta = \frac{1}{5}\pi$  und  $\gamma - 2\delta = \frac{1}{5}\pi = \delta$





Die Dreiecke  $A$  und  $C$  sind ähnlich und die Dreiecke  $B$  und  $D$  sind ähnlich, da sie gleiche Winkel haben. Sei  $d$  die Länge der Diagonalen und  $e = d - 1$ . Es gilt also  $\frac{1}{d} = \frac{1}{e} = \frac{1}{d-1}$ . Also ist  $d^2 - d = 1$  was  $d = \frac{\sqrt{5} + 1}{2}$  impliziert. Konstruiere also



und dann konstruiere 5-Eck.

## 5.4 Auflösbarkeit durch Radikale

**Definition 5.4.1.** Sei  $K$  ein Körper der Charakteristik 0.

1. Eine einfache Radikalerweiterung ist eine Körpererweiterung  $L/K$  sodass  $L = K(a)$  für ein  $a$  mit  $a^n \in K$  für ein  $n \in \mathbb{N}_1$
2.  $L/K$  heißt Radikalerweiterung, wenn es eine Kette  $K = K_0 \subseteq \dots \subseteq K_r = L$  gibt sodass  $K_i/K_{i-1}$  eine einfache Radikalerweiterung ist.
3.  $L/K$  ist auflösbar durch Radikale, wenn es für jedes  $a \in L$  eine Radikalerweiterung  $L'/K$  und Einbettung  $K(a) \subseteq L'$  existiert.

**Bemerkung 5.4.2.** Wenn  $L/K$  endlich, dann ist  $L = K(a)$  für ein  $a \in L$ . Dann

$L/K$  ist auflösbar durch Radikale  $\iff L$  ist in einer Radikalerweiterung enthalten

**Bemerkung 5.4.3.** Notation: Wenn  $L/K$  einfache Radikalerweiterung,  $L = K(a)$  und  $a$  Nullstelle von  $X^n - b$  könnte schreiben  $a = \sqrt[n]{b}$  aber das ist ungenau da  $X^n - b$   $n$  verschiedene Nullstellen hat.

**Beispiel 5.4.4.** Sei  $f = X^3 - 2$  und sei  $a = \sqrt[3]{2} \in \mathbb{R}$ . Wenn  $K = \mathbb{Q}(a)$  dann ist  $[K(a) : K] = 3$  aber  $[K(\zeta_3 a) : K] = 2$

**Bemerkung 5.4.5.** Angenommen  $K$  ist ein Körper von Charakteristik  $\neq n$  und  $\mu_n(\bar{K}) \subseteq K$ . Dann sei  $\zeta_n \in \mu_n(\bar{K})$  primitiv. Die Nullstellen von  $f = X^n - b$  sind  $a, \zeta_n a, \zeta_n^2 a, \dots, \zeta_n^{n-1} a$  also  $X^n - b = \prod_{k=0}^{n-1} (X - \zeta_n^k a)$  und  $K(a) = K(\zeta_n^k a)$  für jedes  $k$  da  $K$   $\zeta_n$  enthält. In diesem Fall ist die Bezeichnung  $K(\sqrt[n]{b}) = K(a)$  für irgendein  $a$  mit  $a^n = b$ . Das ist ein Zerfallskörper von  $X^n - b$ .

**Lemma 5.4.6.** Sei  $K$  ein Körper der Charakteristik  $\neq n$  und  $\mu_n(\bar{K}) \subseteq K$ . Dann gibt es einen injektiven Gruppenhomomorphismus  $\text{Gal}(K(\sqrt[n]{a})/K) \rightarrow \mu_n(K) \cong \mathbb{Z}/n\mathbb{Z}$ . Insbesondere ist  $G = \text{Gal}(L/K)$  zyklisch.

*Beweis.* Sei  $\sigma \in G$  und  $b = \sqrt[n]{a}$ . Es ist  $\sigma(b)$  ist eine Nullstelle von  $X^n - a$  also ist  $\sigma(b) = \zeta b$  für ein  $\zeta \in \mu_n(K)$ . Da  $\mu_n(\bar{K}) \subseteq K$  ist für  $\zeta' \in \mu_n(\bar{K})$ :

$$\sigma(\zeta' b) = \zeta' \sigma(b) = \zeta' \zeta b.$$

Sei  $\psi: G \rightarrow \mu_n(\bar{K})$ ,  $\psi(\sigma) = \frac{\sigma(b)}{b}$ . Eine Rechnung zeigt, dass das ein Gruppenhomomorphismus ist. Angenommen  $\psi(\sigma) = 1$ . Dann ist  $\sigma = \text{id}$  auf Menge der Nullstellen und da  $K(\sqrt[n]{a})/K$  Zerfällungskörper ist, ist  $\sigma = \text{id}$ .  $\square$

**Definition 5.4.7.** Sei  $E$  eine Eigenschaft von Gruppen (z.B. zyklisch, auflösbar, abelsch...) Eine Körpererweiterung  $L/K$  hat die Eigenschaft  $E$ , wenn  $L/K$  Galois ist und  $\text{Gal}(L/K)$  diese Eigenschaft  $E$  hat.

**Satz 5.4.8.** Sei  $\text{Char}(K) \neq n$  und  $\mu_n(\bar{K}) \subseteq K$ . Wenn  $L/K$  zyklisch von Grad  $n$ , dann ist  $L = K(\sqrt[n]{a})$  für ein  $a \in K$ .

*Beweis.* Sei  $\sigma \in \text{Gal}(L/K)$  ein Erzeuger. Als Endomorphismus gilt  $\sigma^n - \text{id} = 0$ . Sei  $\mu_\sigma$  Minimalpolynom von  $\sigma$ . Dann gilt  $\mu_\sigma \mid X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$ . Somit ist  $\sigma$  diagonalisierbar und die Eigenwerte sind die Nullstellen von  $\mu_\sigma$ . Sei  $B \subseteq \mu_n$  die Menge dieser Nullstellen. Für  $\zeta \in \mu_n(\bar{K})$  sei  $V_\zeta = \{x \in L \mid \sigma(x) = \zeta x\}$ . Es gilt  $V_\zeta \neq 0 \iff \zeta \in B$  und  $L = \bigoplus_{\zeta \in \mu_n} V_\zeta$ . Sei  $x \in V_\zeta$  mit  $x \neq 0$ . Dann gilt  $x^{-1} \in V_{\zeta^{-1}}$  und somit haben wir inverse Abbildungen

$$V_{\zeta'} \xrightarrow{x} V_{\zeta \zeta'} \xrightarrow{x^{-1}} V_{\zeta'}$$

somit ist  $V_{\zeta'} \cong V_{\zeta \zeta'}$ . Das zeigt:  $B \subseteq \mu_n(\bar{K})$  ist Untergruppe und wenn  $\zeta \in B$  Erzeuger ist, dann ist  $V_1 \cong V_\zeta \cong V_{\zeta^2} \cong \dots$ . Also ist

$$\dim(V_{\zeta^i}) = \dim(V_1)$$

und  $\dim(V_1) = [\mu_n : B]$  denn  $n = \dim(L) = |B| \cdot \dim(V_1)$ . Es ist

$$V_1 = \{x \in L \mid \sigma(x) = x\} = L^{\langle \sigma \rangle} = L^G = K$$

also  $\dim(V_1) = 1$  und somit  $\mu_n = B$  und  $\dim(V_\zeta) = 1$  für alle  $\zeta \in \mu_n$ . Sei  $\zeta_n \in \mu_n$  primitiv. Wähle  $b \in V_{\zeta_n}$  mit  $b \neq 0$ . Es ist  $\langle b^i \rangle = V_{\zeta_n^i}$  somit erzeugen  $1, b, \dots, b^{n-1}$  den  $K$ -Vektorraum  $L$ . Also ist  $L = K(b)$ . Es ist  $\sigma(b) = \zeta_n b$  also  $\sigma(b^n) = b^n$  und somit ist  $a = b^n \in L^G = K$ . Das zeigt:  $b$  ist Nullstelle von  $X^n - a \in K[X]$   $\square$

**Lemma 5.4.9.** Die Komposition von Radikalerweiterungen ist eine Radikalerweiterung.

*Beweis.* Seien  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r$  und  $K = L_0 \subseteq L_2 \subseteq \dots \subseteq L_n$  Ketten von einfachen Radikalerweiterungen. Dann ist  $K = K_0 \subseteq \dots \subseteq K_r = K_r L_0 \subseteq K_r L_1 \subseteq \dots \subseteq K_r L_n$  Kette von einfachen Radikalerweiterungen, denn wenn  $L_i = L_{i-1}(a_i)$  mit  $a_i^n \in L_{i-1}$  dann ist  $K_r L_i = K_r L_{i-1}(a_i)$  und  $a_i^n \in K_r L_{i-1}$   $\square$

**Lemma 5.4.10.** Sei  $L/K$  eine endliche Körpererweiterung in Charakteristik 0.

1.  $L/K$  ist Radikalerweiterung  $\implies$  normale Hülle von  $L/K$  ist Radikalerweiterung.
2.  $L/K$  ist auflösbar durch Radikale  $\iff$  normale Hülle von  $L/K$  ist auflösbar durch Radikale.

*Beweis.* 1): Sei  $L = K(a)$  und seien  $a = a_1, \dots, a_r \in \bar{K}$  die Nullstellen vom Minimalpolynom von  $a$ . Also ist die normale Hülle gegeben durch  $M = K(a_1) \cdots K(a_r)$ . Es ist  $K(a_i) \cong K(a)$  Radikalerweiterung über  $K$ . Nach Section 5.4 ist also  $M/K$  eine Radikalerweiterung.

2): Sei  $L = K(a_1)/K$  auflösbar durch Radikale, dh. es gibt  $L'/L$  sodass  $L'/K$  Radikalerweiterung ist. Sei  $M/K$  bzw  $M'/K$  die normale Hülle von  $L/K$  bzw  $L'/K$ . Dann ist  $M \subseteq M'$ . Nach 1) ist  $M'/K$  Radikalerweiterung also  $M/K$  auflösbar durch Radikale. Sei andersrum  $M/K$  die normale Hülle von  $L/K$  und  $M/K$  auflösbar durch Radikale, dh. Es gibt  $M'/M$  sodass  $M'/K$  Radikalerweiterung. Dann ist  $L/K$  auflösbar durch Radikale nach Definition.  $\square$

**Satz 5.4.11.** *Sei  $L/K$  endliche Körpererweiterung in Charakteristik 0 und  $M/K$  eine normale Hülle. Dann ist  $L/K$  auflösbar durch Radikale  $\iff L/K$  auflösbar.*

*Beweis.* Nach Lemma 5.4.10 ist ohne Einschränkung  $L/K$  Galois. Sei  $n = [L : K]$  und  $K' = K(\mu_n)$  und  $L' = L(\mu_n)$ . Da  $L/K$  Galois ist  $L'/K'$  Galois und  $L'/K$  Galois. Es sind  $\text{Gal}(K'/K)$  und  $\text{Gal}(L'/L)$  abelsch, insbesondere auflösbar. Es ist

$$\text{Gal}(L/K) \cong \text{Gal}(L'/K) / \text{Gal}(L'/L)$$

und  $\text{Gal}(L'/K) / \text{Gal}(L'/K') \cong \text{Gal}(K'/K)$ . Also ist

$$\begin{aligned} \text{Gal}(L/K) \text{ auflösbar} &\iff \text{Gal}(L'/K) \text{ auflösbar} \\ &\iff \text{Gal}(L'/K') \text{ auflösbar} \end{aligned}$$

und  $K'/K$  und  $L'/L$  sind Radikalerweiterungen. Somit ist  $L/K$  auflösbar durch Radikale  $\iff L'/K'$  auflösbar durch Radikale. Somit ist ohne Einschränkung  $L = L'$  und  $K = K'$ . Sei  $L/K$  auflösbar. Wähle Normalreihe in  $\text{Gal}(L/K)$  mit primzyklischen Quotienten. Das entspricht  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = L$  mit  $K_i/K_{i-1}$  Galois und  $\text{Gal}(K_i/K_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$ . Satz 5.4.8 impliziert, dass  $K_i/K_{i-1}$  eine einfache Radikalerweiterung ist. Somit ist  $L/K$  eine Radikalerweiterung. Insbesondere ist  $L/K$  auflösbar durch Radikale.

Sei andersrum  $L/K$  auflösbar durch Radikale. Es gibt  $L'/L$ , sodass  $L'/K$  Radikalerweiterung ist. Ohne Einschränkung ist  $L'/K$  Galois. Es gibt Kette  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = L'$  sodass  $K_i/K_{i-1}$  einfache Radikalerweiterung ist. Behauptung:  $\text{Gal}(L'/K)$  ist auflösbar. Dann ist  $\text{Gal}(L/K)$  als Quotient von  $\text{Gal}(L'/K)$  auch auflösbar. Lemma 5.4.6 impliziert, dass  $K_i/K_{i-1}$  Galois ist mit zyklischer Galoisgruppe. Die Körperkette entspricht Kette von Untergruppen in  $\text{Gal}(L'/K)$ . Das ist eine abelsche Normalreihe.  $\square$

**Korollar 5.4.12.** *Jede Gleichung von Grad  $\leq 4$  in Charakteristik 0 ist durch Radikale auflösbar, dh.  $f \in K[X]$  mit  $\deg(f) \leq 4$  und  $L/K$  Zerfällungskörper von  $f$ , dann ist  $G = \text{Gal}(L/K)$  auflösbar.*

*Beweis.* Haben injektiven Gruppenhomomorphismus  $G \rightarrow S_4$ . Da  $S_4$  auflösbar ist, ist  $G$  auflösbar.  $\square$

**Satz 5.4.13.** *Für jede endliche Gruppe  $G$  gibt es eine Galoiserweiterung  $L/K$  in Charakteristik 0 mit  $G = \text{Gal}(L/K)$ .*

*Beweis.* Wähle  $G \rightarrow S_n$  injektiv mit  $|n| = |G|$ . Wenn  $L/K'$  existiert mit  $\text{Gal}(L/K') = S_n$  dann gilt für  $K = L^G$  dass  $\text{Gal}(L/K) = G$  ist.  $S_n$  operiert auf  $L = \mathbb{Q}(X_1, \dots, X_n)$  durch Permutation der Variablen. Das gibt Homomorphismus  $S_n \rightarrow \text{Aut}(L)$  der injektiv ist. Der Körper  $K = L^{S_n}$  gibt  $\text{Gal}(L/K) = S_n$ .  $\square$

**Bemerkung 5.4.14.**  $S_5$  ist nicht auflösbar.

**Bemerkung 5.4.15.**

1. Es gibt eine Definition von Auflösbar durch Radikale in beliebiger Charakteristik, für die der letzte Satz gilt
2. Frage: Wenn  $K$  gegeben, welche Gruppen  $G$  sind als Galoisgruppen über  $K$  realisierbar, dh. gibt es  $L/K$  Galois mit  $\text{Gal}(L/K) = G$ .
  - (a)  $K = \mathbb{R}$  Dann ist  $G = \{1\}$  und  $G = \mathbb{Z}/2\mathbb{Z}$  möglich.
  - (b) Wenn  $K$  endlich ist: Genau die zyklischen Gruppen sind möglich, denn

$$\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \langle Fr \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

- (c)  $K = \mathbb{Q}$  Frage ist offen.  $G = S_p$  nach Übungsaufgabe?  $G = S_n$  möglich (Hilbert).

**Satz 5.4.16.** *Es gibt Gleichungen vom Grad 5 die nicht auflösbar sind*

*Beweis.*  $S_5$  ist Galoisgruppe von  $M/\mathbb{Q}$  für ein  $M/\mathbb{Q}$  Galois. Es ist  $H = S_4 = \text{Stab}(1) \subseteq S_5$  also  $[G : H] = 5$  und somit  $[M^H : K] = 5$ . Es ist  $M = K(a)$  für ein  $a$ . Die normale Hülle von  $M^H/K$  entspricht nach Galois-Korrespondenz  $\bigcap_{g \in S_5} gHg^{-1} = \{e\}$ , also ist  $M/K$  die normale Hülle von  $M^H = \mathbb{Q}(a) = \mathbb{Q}[X]/(f)$  wobei  $f$  das Minimalpolynom von  $a$  ist. Damit ist  $S_5$  Galoisgruppe von  $f$  und  $S_5$  ist nicht auflösbar. Es ist  $\deg(f) = [\mathbb{Q}(a) : \mathbb{Q}] = 5$   $\square$

Teil III

Commutative Algebra

# Kapitel 6

## Ringe und Ideale

### 6.1 Grundlagen

**Definition 6.1.1.** Ein Ring  $R$  heißt Integritätsbereich (oder nullteilerfrei), wenn  $R \neq 0$  und  $ab = 0 \implies a = 0$  oder  $b = 0 \forall a, b \in R$ .

**Lemma 6.1.2.** Sei  $R$  ein kommutativer Ring.

1. Ein Ideal  $I \subseteq R$  ist ein Primideal  $\iff R/I$  ist Integritätsbereich.
2.  $R$  ist ein Körper  $\iff R$  hat genau zwei Ideale  $\{0\}$  und  $R$ .
3. Ein Ideal  $I \subseteq R$  ist maximal  $\iff R/I$  ist ein Körper.

*Beweis.* 1) ist klar. Zeige 2). Wenn  $R$  ein Körper ist und  $I \subsetneq \{0\}$  ein Ideal, dann gibt es  $x \in I$  mit  $x \neq 0$ . Dann ist  $1 = x^{-1}x \in I$ , also ist  $I = R$ . Andersrum zeige, dass  $x \neq 0$  invertierbar ist. Es ist  $R = (x)$  also gibt es Inverses. Zeige 3).  $I \subseteq R$  ist maximal  $\iff R/I$  hat genau zwei Ideale  $\{0\}, R/I \iff R/I$  ist Körper.  $\square$

**Lemma 6.1.3.** Seien  $R_1, R_2$  Ringe und  $R = R_1 \times R_2$ . Jedes Ideal von  $R$  hat die Form  $I = I_1 \times I_2$  wobei  $I_1 \subseteq R_1$  und  $I_2 \subseteq R_2$  Ideale sind.  $I$  ist genau dann prim wenn entweder  $I_1$  prim und  $I_2 = R_2$  oder  $I_1 = R_1$  und  $I_2$  prim ist. Folglich ist  $\text{Spec}(R) = \text{Spec}(R_1) \amalg \text{Spec}(R_2)$ .

*Beweis.* Die erste Behauptung ist klar. Es ist  $R/I \cong R_1/I_1 \times R_2/I_2$  und  $I$  ist prim, genau dann wenn  $R/I$  nullteilerfrei ist. Da  $(a, 0) \cdot (0, b) = (0, 0)$  ist, ist das genau dann der Fall, wenn eines der  $I_j = R_j$  ist und das andere prim.  $\square$

**Satz 6.1.4.** Sei  $R$  ein kommutativer Ring,  $R \neq 0$ . Dann hat  $R$  ein maximales Ideal.

*Beweis.* Sei  $M$  die Menge aller Ideale  $I \subseteq R$  mit  $I \neq R$  und sei  $M' \subseteq M$  eine totale geordnete Teilmenge. Ohne Einschränkung ist  $(0) \in M'$ . Sei

$$J = \bigcup_{I \in M'} I.$$

Dann ist  $J$  ein Ideal mit  $1 \notin J$  also  $J \in M$ . Das ist eine obere Schranke für  $M'$ . Also hat  $M$  ein maximales Element nach Lemma von Zorn.  $\square$

**Definition 6.1.5.** Sei  $R$  ein kommutativer Ring. Sei  $n \in \mathbb{N}$  gegeben sodass  $(n) = \ker(\mathbb{Z} \rightarrow R)$ . Dann heißt  $n$  die Charakteristik von  $R$ . Wenn  $R$  nullteilerfrei ist, dann ist  $n = 0$  oder  $n$  eine Primzahl.

**Definition 6.1.6.** Ein Ring  $R$  heißt lokal, wenn es genau ein maximales Ideal gibt.

**Satz 6.1.7.** Sei  $\mathfrak{m} \subsetneq R$  ein Ideal. Es ist äquivalent:

1.  $R$  ist lokal mit maximalem Ideal  $\mathfrak{m}$
2.  $\forall a \in R \setminus \mathfrak{m} : a \in R^*$
3.  $\mathfrak{m}$  ist maximales Ideal und jedes Element  $a = 1 + m$  mit  $m \in \mathfrak{m}$  ist eine Einheit.

*Beweis.* Gelte 1. Wenn  $a$  keine Einheit, dann ist  $a$  in einem maximalen Ideal enthalten. Also in  $\mathfrak{m}$ . Gelte 3. Sei  $a \notin \mathfrak{m}$  das heißt  $a + \mathfrak{m}$  ist Einheit in  $R/\mathfrak{m}$ . Also gibt es  $x$  sodass  $ax + \mathfrak{m} = 1 + \mathfrak{m}$  also ist  $1 = ax + m$  für ein  $m \in \mathfrak{m}$ . Dann ist  $ax \in R^*$  also auch  $a$ .  $\square$

**Lemma 6.1.8.**  $\mathbb{Z}/n\mathbb{Z}$  ist lokal genau dann wenn  $n = p^r$  für eine Primzahl  $p$  und  $r > 1$ .

*Beweis.* Sei  $n = p^r$ . Primideale in  $\mathbb{Z}/n\mathbb{Z}$  sind Primideale in  $\mathbb{Z}$  die  $n\mathbb{Z}$  enthalten. Das ist nur  $(p)$ . Also ist der Ring lokal. Andersrum wenn  $n = p_1^{e_1} \cdots p_s^{e_s}$  die Primfaktorzerlegung von  $n$  ist mit  $p_i \neq p_j$  für  $i \neq j$  dann korrespondiert mit selber Begründung jedes  $(p_i)$  zu einem maximalen Ideal in  $\mathbb{Z}/n\mathbb{Z}$ .  $\square$

**Lemma 6.1.9** (Primvermeidung). Sei  $\mathfrak{a} \subseteq R$  ein Ideal. Wenn  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  Primideale sind mit  $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$  dann ist  $\mathfrak{a} \subseteq \mathfrak{p}_i$  für ein  $i$ .

*Beweis.* Induktion:  $n = 1$  ist klar. Gelte die Behauptung für  $n - 1$ . Angenommen  $\mathfrak{a} \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$  für alle  $i$ . Das heißt es gibt  $f_i \in \mathfrak{a}$  mit  $f_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$  und  $f_i \in \mathfrak{p}_i$ . Es ist  $f_1 + f_2 \cdots f_n \in \mathfrak{a}$  aber  $f_1 + f_2 \cdots f_n \notin \mathfrak{p}_1$  und  $f_1 + f_2 \cdots f_n \notin \mathfrak{p}_i$  für  $i \geq 2$ . Das ist ein Widerspruch. Also ist  $\mathfrak{a} \subseteq \bigcup_{j \neq i} \mathfrak{p}_j$  für ein  $i$ . Also folgt die Aussagen mit Induktion.  $\square$

## 6.2 Euklidische Ringe, Hauptidealringe und faktorielle Ringe

**Definition 6.2.1.** Sei  $R$  ein Ring.  $R$  ist Euklidisch wenn  $R$  ein Integritätsbereich ist und es eine Abbildung  $\delta: R \setminus \{0\} \rightarrow \mathbb{N}$  gibt sodass für  $a, q \in R$  mit  $q \neq 0$  es  $b, c \in R$  gibt mit  $a = bq + c$  und  $\delta(x) < \delta(q)$  oder  $c = 0$ .

**Definition 6.2.2.** Ein Ring  $R$  ist ein Hauptidealring, wenn  $R$  ein Integritätsbereich ist und jedes Ideal ein Hauptideal ist.

**Satz 6.2.3.** Jeder Euklidische Ring ist ein Hauptidealring.

*Beweis.* Sei  $I \subseteq R$  ein Ideal,  $I \neq \{0\}$ . wähle  $q \in I$  sodass  $\delta(q)$  minimal ist. Dann ist  $I = (q)$ .  $\square$

**Beispiel 6.2.4.**  $R = \mathbb{Z}[X]$  ist kein Hauptidealring, also auch nicht Euklidisch. Denn  $(2, X)$  ist kein Hauptideal.

**Definition 6.2.5.** Sei  $R$  nullteilerfrei und  $a \in R$ . Wir nennen  $a \in R$  Primelement, wenn  $\{0\} \subsetneq (a) \subsetneq R$  ist und wenn für alle  $b, c \in R$  mit  $a \mid bc$  folgt, dass  $a \mid b$  oder  $a \mid c$ . Wir nenne  $a \in R$  irreduzibel, wenn  $\{0\} \subsetneq (a) \subsetneq R$  und für alle  $b, c \in R$  folgt, dass  $b \in R^*$  oder  $c \in R^*$ .

**Bemerkung 6.2.6.** Es gilt  $a \in R$  prim  $\implies a \in R$  irreduzibel und wenn  $\{0\} \subsetneq (a)$  ist, dann ist  $a$  prim  $\iff (a)$  Primideal ist.

*Beweis.* Sei  $a \in R$  prim und  $a = bc$  für  $b, c \in R$ . Dann ist  $a \mid b$  oder  $a \mid c$ . Wenn  $a \mid b$  dann ist  $b = ad = bcd$ . Da  $b \neq 0$  und  $R$  nullteilerfrei ist, ist  $1 = cd$  und  $c \in R^*$ .  $\square$

**Lemma 6.2.7.** Sei  $R$  nullteilerfrei und  $a \in R$  mit  $a \neq 0$ . Es gilt

$$a \text{ ist irreduzibel} \iff (a) \text{ ist maximal unter Hauptidealen} \neq R.$$

*Beweis.* Das ist eine direkte Übersetzung der Eigenschaft irreduzibel zu sein.  $\square$

**Definition 6.2.8.** Ein faktorieller Ring  $R$  ist ein Integritätsbereich  $R$ , sodass jedes  $a \in R$  mit  $\{0\} \subsetneq (a) \subsetneq R$  eine Darstellung  $a = p_1 \cdots p_r$  hat mit  $r \in \mathbb{N}$  und  $p_i$  Primelementen. Die Darstellung ist automatisch eindeutig bis auf Reihenfolge und Assoziiertheit.

**Lemma 6.2.9.** Sei  $R$  ein Integritätsbereich.

$$\begin{aligned} R \text{ ist faktoriell} &\iff \text{Jedes irreduzible Element von } R \text{ ist prim und} \\ &\text{Jedes } a \in R \text{ mit } \{0\} \subsetneq (a) \subsetneq R \text{ ist Produkt von} \\ &\text{irreduziblen Elementen} \end{aligned}$$

*Beweis.* Sei  $R$  faktoriell und  $a \in R$  irreduzibel. Sei  $a = p_1 \cdots p_r$  mit Primelementen  $p_i$ . Da  $a$  irreduzibel ist, ist  $p_1 \in R^*$  oder  $p_2 \cdots p_r \in R^*$ . Da beides nicht der Fall ist, muss  $a = p_1$  prim sein.  $\square$

**Satz 6.2.10.** *Jeder Hauptidealring  $R$  ist faktoriell. Für  $a \in R$  prim ist  $R/(a)$  ein Körper.*

*Beweis.* Zeige: Jedes irreduzible  $a \in R$  ist prim. Es gilt

$$\begin{aligned} a \text{ ist irreduzibel} &\iff (a) \text{ ist maximal unter echten Hauptidealen} \\ &\stackrel{R \text{ HIR}}{\iff} (a) \text{ ist maximales Ideal} \\ &\iff R/(a) \text{ ist Körper} \\ &\implies a \text{ ist Primelement.} \end{aligned}$$

Sei  $n = p_1^{e_1} \cdots p_s^{e_s}$  die Primfaktorzerlegung in paarweise verschiedene Primzahlen. Dann ist nach ??  $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{e_i}\mathbb{Z}$  und nach Lemma 6.1.3 haben maximale Ideale die Form  $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathfrak{m}_i \times \cdots \times \mathbb{Z}/p_s^{e_s}\mathbb{Z}$  für ein maximales Ideal  $\mathfrak{m}_i \subseteq \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ . Da Primideale von  $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$  den Primidealen in  $\mathbb{Z}$  entsprechen, die  $(p_i^{e_i})$  enthalten, folgt, dass der Ring lokal ist. also folgt die Aussage.  $\square$

**Lemma 6.2.11.** *Es sei  $R$  ein Ring und  $I, J \subseteq R$  beliebige Ideale und  $\mathfrak{p} \subseteq R$  ein Primideal. Dann gilt  $IJ \subseteq \mathfrak{p} \implies I \subseteq \mathfrak{p}$  oder  $J \subseteq \mathfrak{p}$*

*Beweis.* Wenn  $I \not\subseteq \mathfrak{p}$  dann gibt es  $x \in I \setminus \mathfrak{p}$ . Für  $y \in J$  gilt dann  $xy \in \mathfrak{p}$  also  $y \in \mathfrak{p}$   $\square$

**Korollar 6.2.12.** *Für ein maximales Ideal  $\mathfrak{m} \subseteq R$  hat der Ring  $R/\mathfrak{m}^n$  genau ein Primideal und ist insbesondere lokal.*

*Beweis.* Primideale in  $R/\mathfrak{m}$  entsprechen den Primidealen  $\mathfrak{m}'$  in  $R$  mit  $\mathfrak{m}^n \subseteq \mathfrak{m}'$ . Nach Lemma 6.2.11 folgt  $\mathfrak{m} \subseteq \mathfrak{m}'$  also  $\mathfrak{m} = \mathfrak{m}'$ .  $\square$

**Beispiel 6.2.13.** Es sei  $R$  der Ring der stetigen Funktionen  $f : \mathbb{R} \rightarrow \mathbb{R}$ . Für jedes  $x \in \mathbb{R}$  ist  $\mathfrak{m}_x = \{f \in R \mid f(x) = 0\}$  ein maximales Ideal von  $R$ , denn betrachte Abbildung  $eval_x : R \rightarrow \mathbb{R}, f \mapsto f(x)$ . Das ist surjektiv mit  $\ker(eval_x) = \mathfrak{m}_x$ . da  $\mathbb{R}$  ein Körper ist, ist folgt die Behauptung. Weiter ist die Menge  $I$  aller  $f \in R$  mit kompaktem Träger ein echtes Ideal von  $R$ , das in keinem  $\mathfrak{m}_x$  enthalten ist, denn definiere

$$f_x : \mathbb{R} \rightarrow \mathbb{R}, y \mapsto \begin{cases} y - (x - 1), & y \in [x - 1, x] \\ -y + x + 1, & y \in [x, x + 1] \\ 0, & \text{sonst} \end{cases}$$

. Dann ist  $f_x$  stetig mit kompaktem Träger  $K = [x - 1, x + 1]$  also ist  $f_x \in I$ . Da aber  $f_x(x) = 1$  folgt  $I \not\subseteq \mathfrak{m}_x$ . Also hat  $R$  maximale Ideale die nicht von der Form  $\mathfrak{m}_x$  sind.

## 6.3 Jacobson und Nilradikal

**Definition 6.3.1.** Sei  $R$  ein Ring und  $j(R) = \bigcap_{\mathfrak{m} \in \text{Specm}(R)} \mathfrak{m}$  das Jacobson Radikal von  $R$ . Wenn  $R = \{0\}$  dann setze  $j(R) = \{0\}$ . Es ist  $j(R)$  maximal genau dann wenn  $R$  lokal ist

**Bemerkung 6.3.2.** Für  $a \in R$  ist äquivalent:

1.  $a \in j(R)$
2.  $1 - ab \in R^*$  für alle  $b \in R$

*Beweis.* Angenommen  $1 - ab \in R^*$  für alle  $b$ . Sei  $\mathfrak{m}$  ein maximales Ideal. Setze  $\mathfrak{n} = (a, \mathfrak{m})$ . Wenn  $a \notin \mathfrak{m}$  dann ist  $\mathfrak{n} = R$  und es gibt  $b \in R$  und  $m \in \mathfrak{m}$  sodass  $1 = ab + m$ . Aber dann ist  $m$  eine Einheit. Also muss  $a \in \mathfrak{m}$  sein für alle maximalen Ideal  $\mathfrak{m}$ . Also ist  $a \in j(R)$ .  $\square$

**Definition 6.3.3.** Sei  $\text{rad}(R) = \bigcap_{\mathfrak{p} \in \text{Spec } R} \mathfrak{p}$  das Nilradikal.  $R$  heißt reduziert, wenn  $\text{rad}(R) = 0$ .

**Satz 6.3.4.**  $\text{rad}(R) = \{a \in R \mid a \text{ nilpotent}\}$

*Beweis.* Sei  $a$  nicht nilpotent. Dann ist  $0 \notin S = 1, a, a^2, \dots$  also  $S^{-1}R \neq 0$ . Das heißt es gibt ein maximales Ideal in  $S^{-1}R$  das zu Primideal  $\mathfrak{p} \subseteq R$  korrespondiert mit  $\mathfrak{p} \cap S = \emptyset$ . Das heißt  $a \notin \mathfrak{p}$  und  $a \notin \text{rad}(R)$ . Die andere Inklusion ist klar.  $\square$

**Lemma 6.3.5.** *Es ist äquivalent:*

1.  $R$  hat genau ein Primideal
2.  $a \in R \implies a \in R^*$  oder  $a$  ist nilpotent
3.  $R/\text{rad}(R)$  ist ein Körper

*Beweis.* klar.  $\square$

**Definition 6.3.6.** Sei  $\mathfrak{a} \subseteq R$  ein Ideal.  $j(\mathfrak{a}) := \pi^{-1}(j(R/\mathfrak{a}))$  und  $\text{rad}(\mathfrak{a}) = \pi^{-1}(\text{rad}(R/\mathfrak{a}))$  wobei  $\pi : R \rightarrow R/\mathfrak{a}$  kanonische Abbildung.

**Satz 6.3.7.** sei  $K$  Körper.  $j(K[X_1, \dots, X_n]) = 0$

*Beweis.* sei  $\bar{K}$  der algebraische Abschluss von  $K$ . Sei

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \bar{K}^n$$

. Betrachte

$$\mathfrak{m}_x = \{f \in K[X_1, \dots, X_n] \mid f(x) = 0\} = \ker(K[X_1, \dots, X_n] \rightarrow \bar{K}, g \mapsto g(x))$$

Die letzte Abbildung ist surjektiv auf den Körper  $K(x_1, \dots, x_n)$  (Betrachte Minimalpolynom und dann modifiziere um Element zu erhalten). Also ist  $K[X_1, \dots, X_n]/\mathfrak{m}_x \cong K(x_1, \dots, x_n)$  Körper und somit  $\mathfrak{m}_x$  maximales Ideal in  $K[X_1, \dots, X_n]$ .  $f \in j(K[X_1, \dots, X_n])$  impliziert dass  $f \in \mathfrak{m}_x$  ist also  $f(x) = 0$  für alle  $x \in \bar{K}^n$ . Also ist  $f$  das Nullpolynom nach Induktion.  $\square$

## 6.4 Lokalisierung

**Definition 6.4.1.** Sei  $R$  ein Ring und  $S \subseteq R$  eine multiplikative Menge, das heißt  $1 \in S$  und  $s, s' \in S$  impliziert  $ss' \in S$ . Definiere Äquivalenzrelation auf  $R \times S$  durch

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

. Notation:  $R_S = S^{-1}R = (R \times S)/\sim$  und schreibe  $\frac{a}{s}$  für die Äquivalenzklasse  $[(a, s)]$ .  $S^{-1}R$  wird Ring durch

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st} \end{aligned}$$

$S^{-1}R$  heißt Lokalisierung von  $R$  mit  $S$ . Es gibt Ringhomomorphismus  $\tau : R \rightarrow S^{-1}R, a \mapsto \frac{a}{1}$ . Es ist  $\ker(\tau) = \{a \in R \mid \exists s \in S: as = 0\}$  und  $S^{-1}R \neq 0 \iff 0 \notin S$  und  $\tau$  ist bijektiv wenn  $S \subseteq R^*$ . Wenn  $R$  ein Integritätsbereich ist, dann ist  $S = R \setminus \{0\}$  multiplikativ und wir definieren  $\text{Quot}(R) = S^{-1}R$ . Das ist ein Körper. Wenn  $\mathfrak{p} \subseteq R$  ein primideal ist, dann ist  $S = R \setminus \mathfrak{p}$  multiplikativ. Definiere  $R_{\mathfrak{p}} = S^{-1}R$ .

**Satz 6.4.2.** Sei  $R$  ein Ring und  $S \subseteq R$  multiplikativ. Dann existiert ein kommutatives Diagramm:

$$\begin{array}{ccc} \{\mathfrak{a} \mid \mathfrak{a} \subseteq R \text{ Ideal}, S \cap \mathfrak{a} = \emptyset\} & \xrightarrow{\mathfrak{a} \mapsto \mathfrak{a}S^{-1}R} & \{\mathfrak{b} \mid \mathfrak{b} \subseteq S^{-1}R \text{ Ideal}\} \\ \uparrow & & \uparrow \\ \{\mathfrak{p} \mid \mathfrak{p} \subseteq R \text{ Primideal}, S \cap \mathfrak{p} = \emptyset\} & \xrightarrow{\sim} & \{\mathfrak{q} \mid \mathfrak{q} \subseteq S^{-1}R \text{ Primideal}\} \end{array}$$



*Beweis.* Angenommen  $\frac{a}{s} = 1$  für  $a \in \mathfrak{a}$  und  $s \in S$ . Das heißt  $\exists t \in S$  sodass  $(a - s)t = 0$  also  $at = ts \in S$ . Dann ist aber  $at \in \mathfrak{a} \cap S$ . wenn  $\mathfrak{b} \subsetneq S^{-1}R$  ein Ideal ist, definiere  $\mathfrak{a} = \tau^{-1}(\mathfrak{b})$ . Dann ist  $\mathfrak{a}S^{-1}R = \mathfrak{b}$  und  $S \cap \mathfrak{a} = \emptyset$ . Wenn  $\mathfrak{p} \subseteq R$  prim ist mit  $S \cap \mathfrak{p} = \emptyset$  dann ist  $\mathfrak{q} = \mathfrak{p}S^{-1}R$  prim, denn wenn  $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}R$  mit  $\frac{aa'}{ss'} = \frac{b}{t} \in \mathfrak{q}$  mit  $b \in \mathfrak{p}$  dann ist

$$(aa't - ss'b)r = 0$$

für ein  $r \in S$  also  $aa't \in \mathfrak{p}$ . Dann ist  $a \in \mathfrak{p}$  oder  $a' \in \mathfrak{p}'$  also  $\frac{a}{s} \in \mathfrak{q}$  oder  $\frac{a'}{s'} \in \mathfrak{q}$ . Wenn  $\mathfrak{p}$  prim ist, dann ist  $\mathfrak{p} = \tau^{-1}(\mathfrak{p}S^{-1}R)$  denn wenn  $x \in \mathfrak{p}$  sodass  $\frac{x}{1} = \frac{a}{s}$  für ein  $a \in \mathfrak{p}$  dann folgt wie oben dass  $x \in \mathfrak{p}$ . Wenn  $\mathfrak{q} \subseteq S^{-1}R$  prim ist, dann ist  $\tau^{-1}(\mathfrak{q})$  prim. Somit ist untere Abbildung Bijektion.  $\square$

**Beispiel 6.4.3.** Sei  $R = \mathbb{Z}$  und  $\mathfrak{a} = (2)$  sowie  $\mathfrak{a}' = (6)$  und  $S = \{1, 3, 3^2, 3^3, \dots\}$ . Dann ist  $\mathfrak{a}S^{-1}\mathbb{Z} = \{\frac{2x}{3^n} \mid x \in \mathbb{Z}, n \in \mathbb{N}\}$  und  $\mathfrak{a}'S^{-1}\mathbb{Z} = \{\frac{6y}{3^m} \mid y \in \mathbb{Z}, m \in \mathbb{N}\} = \mathfrak{a}S^{-1}\mathbb{Z}$ .

**Korollar 6.4.4.**  $\tau: R \rightarrow S^{-1}R$  induziert Isomorphismus

$$\text{Spec}(S^{-1}R) \rightarrow \{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \cap S \neq \emptyset\}. \mathfrak{q} \mapsto \tau^{-1}(\mathfrak{q})$$

**Korollar 6.4.5.** Für alle  $\mathfrak{p} \subseteq R$  prim ist  $R_{\mathfrak{p}}$  ein lokaler Ring mit maximalem Ideal  $\mathfrak{p}R_{\mathfrak{p}}$

*Beweis.*  $R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$  besteht aus Einheiten.  $\square$

**Satz 6.4.6** (Universelle Eigenschaft der Lokalisierung). *Es ist  $\tau(S) \subseteq (S^{-1}R)^*$ . Wenn  $\varphi: R \rightarrow R'$  Ringhomomorphismus ist, dann gilt  $\varphi(S) \subseteq (R')^*$  genau dann, wenn es einen eindeutigen Ringhomomorphismus  $\varphi': S^{-1}R \rightarrow R'$  gibt sodass  $\varphi = \varphi' \circ \tau$ .*

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ \tau \downarrow & \nearrow \varphi' & \\ S^{-1}R & & \end{array}$$

Wenn  $\varphi: R \rightarrow R'$  dieselbe Eigenschaft erfüllt wie  $\tau$ , dann ist  $\varphi'$  Isomorphismus.

*Beweis.* Definiere  $\varphi'(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$ . Prüfe dass das wohldefiniert und eindeutig ist. Angenommen  $\tau, \varphi$  sind beide universell, das heißt es existiert  $\varphi': S^{-1}R \rightarrow R'$  mit  $\varphi = \varphi' \circ \tau$  und  $\tau': R' \rightarrow S^{-1}R$  mit  $\tau = \tau' \circ \varphi$ . Dann ist

$$\text{id}_{R'} \circ \varphi = \varphi' \circ \tau = (\varphi' \circ \tau') \circ \varphi$$

also  $\text{id}_{R'} = \varphi' \circ \tau'$  wegen Eindeutigkeit. Analog ist  $\text{id}_{S^{-1}R} = \tau' \circ \varphi'$   $\square$

**Lemma 6.4.7.** Sei  $R$  ein Ring und  $F = (f_i)_{i \in I}$  eine Familie in  $R$  und  $S \subseteq R$  eine multiplikative Menge von  $F$  erzeugt. Seien Variablen  $T = (t_i)_{i \in I}$  gegeben. Dann existiert ein Isomorphismus

$$R_S \rightarrow R[T]/(1 - f_i t_i \mid i \in I)$$

Insbesondere ist  $R_f \cong R[X]/(1 - fX)$

*Beweis.* Sei  $\varphi: R \rightarrow R'$  Ringhomomorphismus sodass  $\varphi(S) \subseteq (R')^*$ . Definiere  $\tilde{\varphi}: R[T] \rightarrow R'$  durch  $\varphi$  und  $t_i \mapsto \varphi(f_i)^{-1}$ . Dann ist  $\ker(\tilde{\varphi}) = (1 - f_i t_i \mid i \in I)$  was  $\varphi': R[T]/(1 - f_i t_i \mid i \in I) \rightarrow R'$  induziert sodass  $\varphi = \varphi' \circ \tau$  wobei  $\tau: R \rightarrow R[T]/(1 - f_i t_i \mid i \in I)$ .  $\varphi'$  ist eindeutig da  $1 = \varphi'(f_i t_i) = \varphi(f_i)\tilde{\varphi}(t_i)$  ist. Also gibt es Isomorphismus nach Satz 6.4.6  $\square$

**Satz 6.4.8.** Seien  $f, g \in R$  und  $d, e \in \mathbb{N}$  mit  $d \geq 1$ . Dann kommutiert

$$\begin{array}{ccc} R & \longrightarrow & R_f \\ \downarrow & & \downarrow \\ R_{fg} & \xrightarrow{\sim} & (R_f)_{f^{-e}g^d} \end{array}$$

*Beweis.* Die Abbildung  $R \rightarrow R_f \rightarrow (R_f)_{f^{-e}g^d}$  schickt  $f, g$  und somit  $fg$  auf Einheiten. Das gibt  $R_{fg} \rightarrow (R_f)_{f^{-e}g^d}$   $R \rightarrow R_{fg}$  schickt  $f$  auf Einheit, das gibt also  $R_f \rightarrow R_{fg}$  und der schickt  $f^{-e}g^d$  auf eine Einheit. Das gibt  $(R_f)_{f^{-e}g^d} \rightarrow R_{fg}$  invers zu oben.  $\square$

**Satz 6.4.9.** Sei  $\mathfrak{p}$  Primideal,  $f \in R \setminus \mathfrak{p}$ . Dann kommutiert

$$\begin{array}{ccc} R & \longrightarrow & R_f \\ \downarrow & & \downarrow \\ R_{\mathfrak{p}} & \xrightarrow{\sim} & (R_f)_{\mathfrak{p}R_f} \end{array}$$

*Beweis.* Analog wie in Satz 6.4.8 □

**Beispiel 6.4.10.** Es gibt Isomorphismus  $(\mathbb{Z}/12\mathbb{Z})[3^{-1}] \rightarrow \mathbb{Z}/4\mathbb{Z}$  und jeder Zwischenring  $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$  ist eine Lokalisierung von  $\mathbb{Z}$ .

*Beweis.* Sei  $\varphi: \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ . Einheiten von  $\mathbb{Z}/12\mathbb{Z}$  sind 1, 5, 5, 11 und diese gehen auf Einheiten in  $\mathbb{Z}/4\mathbb{Z}$ . Sei  $\tau': \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}[-3]$ ,  $x + 4\mathbb{Z} \mapsto \frac{x+12\mathbb{Z}}{1}$ . Das ist wohldefiniert wie man prüft und  $\tau'$  ist eindeutig sodass  $\tau' \circ \varphi = \tau$ . also ist beides Isomorph. Sei  $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$  Zwischenring und  $S$  die multiplikative Menge erzeugt von allen Primzahlen  $p$  sodass  $\frac{1}{p} \in R$ . Dann ist  $S^{-1}\mathbb{Z} \subseteq R$ . Sei  $\frac{a}{b} \in R$  mit  $a, b$  teilerfremd. sei  $p$  eine Primzahl mit  $p \mid b$ . Dann ist  $\frac{a}{p} \in R$  und da  $a, p$  teilerfremd, gibt es  $m, n \in \mathbb{Z}$  sodass  $1 = ma + np$  ist. Also ist

$$\frac{1}{p} + n = \frac{ma}{p} \in R$$

also ist  $\frac{1}{p} \in R$ . Dann ist  $\frac{1}{b} \in S^{-1}R$  und somit  $\frac{a}{b} \in S^{-1}\mathbb{Z}$ . □

**Lemma 6.4.11.** Eine Lokalisierung von noetherschen Ringen ist noethersch.

*Beweis.* Klar, betrachte aufsteigende Kette die zu aufsteigender Kette im Ring korrespondiert □

## Kapitel 7

# Ganze Ringerweiterungen und Dimensionstheorie

### 7.1 Ganze Ringerweiterungen

**Definition 7.1.1.** Sei  $\varphi: R \rightarrow R'$  ein Ringhomomorphismus.  $x \in R'$  heißt ganz über  $R$ , wenn es eine Ganzheitsgleichung  $x^n + a_1x^{n-1} + \dots + a_n = 0$  erfüllt für  $a_1, \dots, a_n \in R$ .  $R'$  heißt ganz über  $R$ , falls jedes  $x \in R'$  ganz ist.  $\varphi$  heißt endlich, wenn es  $R'$  mit einer endlichen  $R$ -Modulstruktur versieht.

**Beispiel 7.1.2.** Wenn  $R = K, R' = K'$  Körper sind, dann ist  $K'/K$  algebraisch wenn es ganz ist über  $K$ .

**Lemma 7.1.3.** Sei  $\varphi: R \rightarrow R'$  injektive und  $R, R'$  Integritätsbereiche und  $R'$  ganz über  $R$ . Dann ist  $R$  ein Körper genau dann wenn  $R'$  ein Körper ist.

**Beispiel 7.1.4.** Sei  $K/\mathbb{Q}$  eine endliche Körpererweiterung und  $a \in K$ . Für einen Körperhomomorphismus  $\sigma: K \rightarrow \bar{K}$  gilt  $a$  ist ganz über  $\mathbb{Z}$  genau dann wenn  $\sigma(a)$  ganz ist über  $\mathbb{Z}$  und  $a$  ist ganz über  $\mathbb{Z}$  genau dann wenn das Minimalpolynom von  $a$  in  $\mathbb{Z}[X]$  ist. Wenn  $K = \mathbb{Q}(\sqrt{n})$  wobei  $n > 1$  quadratfrei ist, dann ist  $a + b\sqrt{n}$  mit  $a, b \in \mathbb{Q}$  ganz über  $\mathbb{Z}$  genau dann, wenn  $a, b \in \mathbb{Z}$  oder  $a, b \in \frac{1}{2} + \mathbb{Z}$  und  $n \equiv 1 \pmod{4}$ .

*Beweis.* Wenn  $a^n + b_1a^{n-1} + \dots + b_n = 0$  mit  $b_i \in \mathbb{Z}$  dann ist auch  $\sigma(a)^n + b_1\sigma(a)^{n-1} + \dots + b_n = 0$  also ist  $\sigma(a)$  ganz. Die Rückrichtung geht genauso unter Verwendung dass  $\sigma$  injektiv ist. Wenn  $a$  ganz ist, Sei  $F \in \mathbb{Z}[X]$  Ganzheitsgleichung. Sei  $\mu$  das Minimalpolynom von  $a$ . Dann ist  $F = \mu g$  Nach Lemma von Gauß ??? ist  $\mu \in \mathbb{Z}[X]$ . Andere Richtung ist klar. Mipol von  $a + b\sqrt{n}$  ist  $(X - (a - b\sqrt{n}))(X - (a + b\sqrt{n})) = X^2 - 2aX + a^2 - b^2n$ . Also ist  $a \in \mathbb{Z}$  oder  $a \in \frac{1}{2} + \mathbb{Z}$ . Wenn  $a \in \mathbb{Z}$  dann ist  $b^2n \in \mathbb{Z}$  und da  $n$  quadratfrei ist, ist  $b \in \mathbb{Z}$ . Wenn  $a \in \frac{1}{2} + \mathbb{Z}$  Dann ist  $a = \frac{1}{2} + x$  für ein  $x \in \mathbb{Z}$ . also ist  $a^2 = \frac{1}{4} + x + x^2$  und somit  $b^2n \in \frac{1}{4} + \mathbb{Z}$  also  $b \in \frac{1}{2} + \mathbb{Z}$  und außerdem  $b^2n \in \frac{1}{4} + \mathbb{Z} \implies n \equiv 1 \pmod{4}$ .  $\square$

*Beweis.* Sei  $R'$  ein Körper und  $x \in R \setminus \{0\}$  Es ist  $x^{-1} = x \in R'$  und es gibt  $a_1, \dots, a_n \in R$  sodass

$$y^n + a_1y^{n-1} + \dots + a_n = 0$$

ist. Also ist

$$y^n = -a_1y^{n-1} - \dots - a_n$$

und somit

$$y = x^{n-1}y^n = -a_1y^{n-1}x^{n-1} - \dots - a_nx^{n-1} \in R$$

. also ist  $R$  Körper. Sei andersrum  $R$  ein Körper und  $x \in R'$  mit  $x \neq 0$ . Dann gibt es  $x^n + a_1x^{n-1} + \dots + a_n = 0$  mit  $a_i \in R$ . Da  $R'$  Integritätsbereich ist ohne Einschränkung  $a_n \neq 0$ . Im Quotientenkörper gilt

$$-x^{-1}a_n = x^{n-1} + a_1x^{n-2} + \dots + a_{n-1} \in R'$$

. Also ist

$$x^{-1} = -a_n^{-1}(x^{n-1} + \dots + a_{n-1}) \in R'$$

also ist  $R'$  ein Körper.  $\square$

**Lemma 7.1.5.** Sei  $\varphi: R \rightarrow R'$  ein ganzer (bzw. endlicher) Ringhomomorphismus.

1. Seien  $I \subseteq R, J \subseteq R'$  Ideale mit  $\varphi(I) \subseteq J$ . Dann ist  $R/I \rightarrow R'/J$  ganz (bzw. endlich)
2. Sei  $S \subseteq R$  eine multiplikative Menge. dann ist  $R_S \rightarrow R'_S$  ganz (bzw. endlich)

Beweis. Klar  $\square$

**Lemma 7.1.6.** Sei  $\varphi: R \rightarrow R'$  ein Ringhom und  $x \in R'$ . Es ist äquivalent

1.  $x$  ist integral über  $R$ .
2. Der Unterring  $R[x] \subseteq R'$  ist endlich erzeugt als  $R$ -Modul.
3. Es gibt endlich-erzeugten  $R$ -Untermodule  $M \subseteq R'$  sodass  $1 \in M$  und  $xM \subseteq M$ .
4. Es gibt eine  $R[x]$ -Modul  $M$  sodass  $M$  ein endlicher  $R$ -Modul ist und  $aM = 0 \implies a = 0$  für alle  $a \in R[x]$ .

Beweis. Gelte 1. Die Ganzheitsgleichung  $x^n + a_1x^{n-1} + \dots + a_n = 0$  zeigt, dass  $x^n$  Element ist von  $M = \sum_{i=0}^{n-1} Rx^i$  und per Induktion ist  $x^m \in M$  für alle  $m$ . Also ist  $M = R[x]$  und  $R[x]$  ist endlich erzeugt. Die Richtung von 2 nach 3 und von 3 nach 4 ist klar. Gelte 4. Sei  $M$  ein  $R[x]$ -Modul mit  $y_1, \dots, y_n \in M$  Erzeuger über  $R$ . Es ist  $xM \subseteq M$  also gibt es Gleichungen

$$xy_i = a_{i1}y_1 + \dots + a_{in}y_n$$

für alle  $i$  mit  $a_{ji} \in R$ . Sei also  $\Delta$  die Matrix über  $R[x]$  sodass

$$\Delta \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0$$

Es ist  $\Delta^{adj} \Delta = \det(\Delta)E_n$  und somit

$$\det(\Delta) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \Delta^{adj} \Delta \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0$$

also ist  $\det(\Delta)y_i = 0$  für alle  $i$ . Also ist  $\det(\Delta)M = 0$  und somit  $\det(\Delta) = 0$ . Also ist  $\det(\delta_{ij}X - a_{ij})$  Polynom über  $R$  das bei  $x$  verschwindet.  $\square$

**Korollar 7.1.7.** Jeder endliche Ringhomomorphismus  $R \rightarrow R'$  ist ganz

Beweis. sei  $M = R'$  Dann ist  $M$  endlich erzeugt. Nach Teil 3 von ?? ist  $R \rightarrow R'$  ganz.  $\square$

**Korollar 7.1.8.** sei  $\varphi: R \rightarrow R'$  Ringhomomorphismus und  $y_1, \dots, y_r \in R'$  ganz über  $R$  sodass  $R' = R[y_1, \dots, y_n]$ . dann ist  $\varphi$  endlich und insbesondere ganz.

Beweis. Es ist  $\varphi(R) \subseteq \varphi(R)[y_1] \subseteq \dots \subseteq \varphi(R)[y_1, \dots, y_r] = R'$  und alle Inklusionen sind endlich nach Lemma ?? . Also ist  $\varphi$  endlich.  $\square$

**Korollar 7.1.9.** Seien  $\varphi: R \rightarrow R'$  und  $\varphi': R' \rightarrow R''$  endlich (bzw ganz). dann ist die Komposition  $\varphi'\varphi$  auch endlich (bzw ganz)

Beweis. Endlich ist klar wie zuvor. Seien beide ganz.  $z \in R''$  erfüllt Ganzheitsgleichung  $z^n + b_1z^{n-1} + \dots + b_n = 0$  mit  $b_i \in R'$ . also ist  $z$  ganz über  $R[b_1, \dots, b_n]$  und  $R[b_1, \dots, b_n, z]$  ist endlich über  $R[b_1, \dots, b_n]$  was endlich ist über  $R$  da alle  $b_i$  ganz über  $R$ . Also ist  $R \rightarrow R[b_1, \dots, b_n, z]$  endlich und damit ganz. Also ist  $R \rightarrow R''$  ganz.  $\square$

**Lemma 7.1.10.** Sei  $R \rightarrow R'$  injektiv und  $\bar{R} = \{x \in R' \mid x \text{ ganz}\}$  Dann ist  $R \subseteq \bar{R} \subseteq R'$  Unterring, genannt der ganze Abschluss von  $R$  in  $R'$ .  $\bar{R}$  ist ganzabgeschlossen in  $R'$

Beweis. Seien  $x, y \in R'$  ganz. Dann ist  $R[x, y]$  ganz über  $R$  also sind  $x + y, x \cdot y \in \bar{R}$ . Es ist  $R \rightarrow \bar{R} \rightarrow \bar{R}$  ganz also  $\bar{R} = \bar{\bar{R}}$ .  $\square$

## 7.2 Normale Ringerweiterungen

**Definition 7.2.1.** Ein Integritätsbereich  $R$  heißt normal, falls  $R$  ganz-abgeschlossen ist in seinem Quotientenkörper.

**Bemerkung 7.2.2.** Ein faktorieller Ring ist normal. Denn sei  $q = \frac{a}{b}$  ganz mit  $b$  keine Einheit und ohne Einschränkung  $a, b$  teilerfremd. Dann führt eine Ganzheitsgleichung für  $q$  zu  $a^n = bx$  also sind  $a$  und  $b$  nicht teilerfremd. Also ist  $q \in R$ .

**Lemma 7.2.3.** Sei  $S \subseteq R \setminus \{0\}$  eine multiplikative Menge und  $R$  normal. Dann ist  $R_S$  normal.

*Beweis.* Es ist  $R \subseteq R_S \subseteq \text{Quot}(R)$  und  $\text{Quot}(R_S) = Q(R)$ . Sei  $x \in \text{Quot}(R)$  ganz über  $R_S$  und

$$x^n + \frac{a_1}{s_1}x^{n-1} + \dots + \frac{a_n}{s_n} = 0$$

Ganzheitsgleichung. Sei  $s = s_1 \cdots s_n$ . Dann ist  $sx$  ganz über  $R$  also  $sx \in R$  und somit  $x = \frac{1}{s}sx \in R_S$  und somit  $R_S$  normal.  $\square$

**Lemma 7.2.4.** Sei  $A$  nullteilerfrei und  $K = \text{Quot}(A)$  und  $L/K$  eine Körpererweiterung. Sei  $B \subseteq L$  der ganze Abschluss von  $A$  in  $L$  und  $S \subseteq A$  eine multiplikative Menge. Dann ist  $S^{-1}B$  der ganze Abschluss von  $S^{-1}A$  in  $L$ .

*Beweis.* Sei  $x = \frac{b}{s} \in S^{-1}B$  dann ist  $sx = b$  ganz über  $A$  also gibt es

$$b^n + a_1b^{n-1} + \dots + a_0 = 0$$

dann ist

$$x^n + \frac{a_1}{s}x^{n-1} + \dots + \frac{a_0}{s^n} = 0$$

und somit  $x$  ganz über  $S^{-1}A$ . Sei  $x \in L$  ganz über  $S^{-1}A$

$$x^n + \frac{a_1}{s_1}x^{n-1} + \dots + \frac{a_0}{s_0} = 0$$

sei  $s = s_1 \cdots s_n$  dann ist  $sx$  ganz über  $A$  also  $sx \in B$  und  $x \in S^{-1}B$ .  $\square$

**Satz 7.2.5.** Für einen Integritätsbereich  $R$  ist äquivalent:

1.  $R$  ist normal
2.  $R_{\mathfrak{p}}$  ist normal für alle primideale  $\mathfrak{p} \subseteq R$ .
3.  $R_{\mathfrak{m}}$  ist normal für alle  $\mathfrak{m} \subseteq R$  maximal.

*Beweis.* 1 impliziert 2 nach Lemma ?? 2 nach 3 ist klar. Gelte 3. und Sei  $x \in \text{Quot}(R)$  ganz über  $R$ . Da  $R_{\mathfrak{m}}$  normal ist, ist  $x \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ . Zeige also  $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$ . Sei  $x \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ . Wähle  $a_{\mathfrak{m}} \in R$  und  $b_{\mathfrak{m}} \in R \setminus \mathfrak{m}$  sodass  $x = \frac{a_{\mathfrak{m}}}{b_{\mathfrak{m}}}$ . Es ist  $\sum (b_{\mathfrak{m}}) = R$  da es in keinem maximalen Ideal enthalten ist. Also gibt es Gleichung  $\sum c_{\mathfrak{m}}b_{\mathfrak{m}} = 1$  mit  $c_{\mathfrak{m}} \in R$  und  $c_{\mathfrak{m}} = 0$  fast immer 0. Also ist

$$x = \left( \sum_{\mathfrak{m}} c_{\mathfrak{m}}b_{\mathfrak{m}} \right) x = \sum_{\mathfrak{m}} c_{\mathfrak{m}}a_{\mathfrak{m}} \in R.$$

Also ist  $R$  normal.  $\square$

**Lemma 7.2.6.** Sei  $A$  normaler Integritätsbereich und  $K = \text{Quot}(A)$ . Sei  $L/K$  eine endliche Körpererweiterung und  $B$  der ganze Abschluss von  $A$  in  $L$ . Dann ist  $B$  normal und für alle  $x \in L$  gilt  $x = \frac{b}{a}$  für ein  $b \in B$  und  $a \in A$ .

*Beweis.* Sei  $a_nx^n + \dots + a_1x + a_0 = 0$  mit  $a_i \in A$  und  $a_n \neq 0$ . Sowas findet man immer, wähle zum Beispiel Minimalpolynom über  $K$  und Multipliziere mit allen Nennern. Dann ist  $(a_nx)^n + \dots + a'_1(a_nx) + a'_0 = 0$  mit  $a'_i \in A$ . Also ist  $a_nx$  ganz über  $A$  und damit in  $B$ . Also ist  $x = \frac{b}{a}$  wie oben. Somit ist  $\text{Quot}(B) = L$  und  $B$  normal.  $\square$

**Satz 7.2.7.** Sei  $A$  noethersch und normal und  $K = \text{Quot}(A)$ . Sei  $L/K$  eine endliche, separable Körpererweiterung und  $B \subseteq L$  der ganze Abschluss von  $A$  in  $L$ . Dann ist  $B$  ein endlicher  $A$ -Modul und insbesondere noethersch.

*Beweis.* Zeige dass  $B$  ein Untermodul ist von  $\sum_{i=1}^n Ax_i \subseteq L$ . Dann ist  $B$  als Untermodul von endlichem Modul endlich, da  $A$  noethersch ist. Ohne Einschränkung ist  $L/K$  Galois, denn sonst sei  $L_1/K$  Galois-Hülle von  $L/K$  und  $B_1$  der ganze Abschluss von  $A$  in  $L_1$ . Wenn  $B_1$  endlicher  $A$ -Modul dann ist auch  $B$ . Sei also  $G = \text{Gal}(L/K)$ . Für  $x \in L$  ist  $\text{Tr}(x) = \sum_{g \in G} g(x)$ . Sei  $\frac{y_1}{x_1}, \dots, \frac{y_n}{x_n}$  Basis von  $L$  über  $K$  mit  $x_i \in A$  und  $y_i \in B$  wie in ????. Dann ist auch  $y_1, \dots, y_n$  eine Basis von  $L$ . Da  $\text{Tr}$  nicht-ausgeartet ist nach ??? definiert  $y \mapsto (x \mapsto \text{Tr}(xy))$  eine injektive Abbildung  $L \rightarrow L^\vee = \text{Hom}(L, K)$ , die somit ein Isomorphismus ist. Wähle also  $x_i$  in  $L$  sodass die Bilder von  $y_i$  genau die duale Basis sind von  $y_i$ , das heißt  $\text{Tr}(x_i y_j) = \delta_{ij}$ . Jedes  $b \in B$  kann geschrieben werden als  $b = \sum c_i x_i$  mit  $c_i \in K$  also dann  $c_j = \text{Tr}(b y_j) \in A$ . Also ist  $B \subseteq \sum Ax_i$ .  $\square$

### 7.3 Going Up

**Satz 7.3.1.** Sei  $\varphi: R \rightarrow R'$  ganzer Ringhomomorphismus.

1. Ein Primideal  $\mathfrak{p} \subseteq R'$  ist maximal genau dann, wenn  $\mathfrak{q} = \mathfrak{p} \cap R$  maximal ist.
2. Seien  $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq R'$  Primideale sodass  $\mathfrak{p}_1 \cap R = \mathfrak{p}_2 \cap R$ . Dann gilt

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \implies \mathfrak{p}_1 = \mathfrak{p}_2.$$

*Beweis.* Es ist  $R/\mathfrak{q} \rightarrow R'/\mathfrak{p}$  ganz und injektiv nach ????. Dann ist

$$R/\mathfrak{q} \text{ Körper} \iff R'/\mathfrak{p} \text{ Körper}$$

nach Lemma 7.1.3. Sei nun  $\mathfrak{p} = \mathfrak{p}_1 \cap R = \mathfrak{p}_2 \cap R$  wie im Satz sodass  $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ . Dann ist für  $S = R \setminus \mathfrak{p}$  die Abbildung  $R_S \rightarrow R'_{\varphi(S)}$  ganz und  $S^{-1}\mathfrak{p}$  ist maximal in  $R_S$ . Es ist  $S^{-1}\mathfrak{p}_i$  prim in  $R'_{\varphi(S)}$  da  $\varphi(S) \cap \mathfrak{p}_i = \emptyset$ . Also ist  $\mathfrak{q}_i = S^{-1} \cap R_S$  Primideal in  $R_S$  die  $S^{-1}\mathfrak{p}$  enthalten. Da  $S^{-1}\mathfrak{p}$  maximal ist, ist  $S^{-1}\mathfrak{p} = \mathfrak{q}_i$  maximal und somit nach 1  $S^{-1}\mathfrak{p}_i$  maximal in  $R'_{\varphi(S)}$ . Da  $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$  ist  $S^{-1}\mathfrak{p}_1 = S^{-1}\mathfrak{p}_2$  und weil  $\mathfrak{p}_i = S^{-1}\mathfrak{p}_i \cap R$  ist  $\mathfrak{p}_1 = \mathfrak{p}_2$ .  $\square$

**Satz 7.3.2** (Living Over). Sei  $\varphi: R \rightarrow R'$  ein ganzer Ringhomomorphismus und  $\mathfrak{p} \subseteq R$  ein Primideal sodass  $\ker(\varphi) \subseteq \mathfrak{p}$ . dann gibt es ein Primideal  $\mathfrak{q} \subseteq R'$  sodass  $\mathfrak{q} \cap R = \mathfrak{p}$ .

*Beweis.* Sei  $S = R \setminus \mathfrak{p}$ . Dann ist  $R_S \rightarrow R'_{\varphi(S)}$  ganz. Da  $\ker(\varphi) \subseteq \mathfrak{p}$  gilt, ist  $0 \notin \varphi(S)$  also  $R'_{\varphi(S)} \neq 0$ . Nach ?? gibt es ein maximales Ideal  $\bar{\mathfrak{q}}$  in  $R'_{\varphi(S)}$ . Nach ??? ist  $\bar{\mathfrak{q}} \cap R_S = S^{-1}\mathfrak{p}$  und somit ist  $\mathfrak{q} = R'_{\varphi(S)} \cap R'$  Primideal mit  $\mathfrak{q} \cap R = \mathfrak{p}$ .  $\square$

**Satz 7.3.3** (Going Up). Sei  $\varphi: R \rightarrow R'$  ganzer injektiver Ringhomomorphismus und

$$\mathfrak{p}_0 \subseteq \dots \subseteq \mathfrak{p}_n$$

Kette von Primidealen in  $R$ . Sei  $\mathfrak{q}_0$  ein Primideal in  $R'$  sodass  $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$ . Dann existiert eine Kette von Primidealen

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \dots \subseteq \mathfrak{q}_n$$

in  $R'$  mit  $\mathfrak{q}_i \cap R = \mathfrak{p}_i$

*Beweis.* Es reicht der Fall  $n = 1$ . Es ist  $R/\mathfrak{p}_0 \rightarrow R'/\mathfrak{q}_0$  ganz und injektiv. Nach [Living Over](#) existiert  $\mathfrak{q} \subseteq R'/\mathfrak{q}_0$  über  $\mathfrak{p}_0$ . Sei  $\mathfrak{q}_1$  Urbild von  $\mathfrak{q}$  unter  $R' \rightarrow R'/\mathfrak{q}_0$ . Dann ist  $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$ .  $\square$

### 7.4 Going Down

**Lemma 7.4.1.** Sei  $R \rightarrow R'$  endlicher Ringhomomorphismus.. Sei  $I \subseteq R$  ein Ideal und  $x \in IR'$ . Dann existiert Ganzheitsgleichung  $h$  mit Koeffizienten in  $I$

*Beweis.* Sei  $R'$  erzeugt von  $y_1, \dots, y_n$ . Es ist  $y_i x \in IR'$  also gibt es Darstellung

$$y_i x = \sum_{j=1}^n r_{ij} y_j$$

mit  $r_{ij} \in I$ . Also ist für  $A = (R_{ij})$

$$(x \cdot E_n - A) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0.$$

Also ist wie in ???

$$\det(x \cdot E_n - A) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0$$

also  $\det(xE_n - A)R' = 0$  und somit  $\det(xE_n - A) = 0$ . Das ist Ganzheitsgleichung mit Koeffizienten in  $I$ .  $\square$

**Lemma 7.4.2.** Sei  $\varphi: R \rightarrow R'$  injektiv und  $s \in R'$  ganz. Seien  $R, R'$  Integritätsringe und  $R$  normal. Es gilt

1. Das Minimalpolynom  $f \in \text{Quot}(R)[X]$  von  $s$  ist in  $R[X]$ .
2. Wenn  $R'$  endlich erzeugter  $R$ -Modul und  $s \in \mathfrak{p}R'$  für ein Primideal  $\mathfrak{p} \subseteq R$  Dann sind alle Koeffizienten von  $f$  in  $\mathfrak{p}$ .

*Beweis.* Sei  $K = \text{Quot}(R)$  und  $L = \text{Quot}(R')$  und  $h$  Ganzheitsgleichung von  $s$ . Es ist

$$f = \prod_{i=1}^n (X - S_i) \in \bar{K}[X].$$

Da  $f \mid h$  folgt dass  $h(s_i) = 0$  und somit  $s_i$  ganz über  $R$  ist. Die Koeffizienten von  $f$  sind in  $K \cap R[S_1, \dots, S_n]$  also sind die Koeffizienten ganz. Da  $R$  normal ist sind die Koeffizienten in  $R$ . Für den zweiten Teil wähle nach Lemma ???  $h$  so, dass Koeffizienten in  $\mathfrak{p}$  liegen. Dann ist wie oben  $h(s_i) = 0$  also  $s_i^n \in \mathfrak{p}R'$  für alle  $i$ . nach [Living Over](#) gibt es Primideal  $\mathfrak{P} \subseteq R'$  sodass  $\mathfrak{P} \cap R = \mathfrak{p}$ . Also ist  $\mathfrak{p}R' \subseteq \mathfrak{P}$  und  $s_i \in \mathfrak{P}$ . Damit sind auch alle Koeffizienten von  $f$  in  $\mathfrak{P} \cap R = \mathfrak{p}$ .  $\square$

**Satz 7.4.3 (Going Down).** Sei  $\varphi: R \rightarrow R'$  ganz und injektiv und  $R$  und  $R'$  Integritätsringe sodass  $R$  normal ist. Für eine Kette von Primidealen

$$R \supseteq \mathfrak{p}_0 \supseteq \dots \supseteq \mathfrak{p}_n$$

und einem Primideal  $\mathfrak{q}_0 \subseteq R'$  mit  $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$  gibt es Kette von Primidealen

$$R' \supseteq \mathfrak{q}_0 \supseteq \dots \supseteq \mathfrak{q}_n$$

sodass  $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ .

*Beweis.* Es reicht der Fall  $n = 1$ . Sei  $S = R \setminus \mathfrak{p}_1$  und  $S' = R' \setminus \mathfrak{q}_0$ . Sei  $T = S \cdot S'$ . Dann ist  $\mathfrak{p}_1 \cdot R' \cap T = \emptyset$ . Sei nämlich  $x \in \mathfrak{p}_1 R' \cap T$ ,  $x = u \cdot v$  mit  $u \in S, v \in S'$  und  $x = \sum_{i=1}^k a_i s_i$  mit  $a_i \in \mathfrak{p}_1, s_i \in R'$ . Ersetze  $R', \mathfrak{q}_0, R' \setminus \mathfrak{q}_0$  durch  $R[v, s_1, \dots, s_k], \mathfrak{q}_0 \cap R[v, s_1, \dots, s_k]$  und deren Komplement. Also ist  $R'$  ohne Einschränkung von endlichem Typ und da  $R'$  ganz ist, ist  $R'$  endlich erzeugt als  $R$ -Modul. Sei  $f$  das Minimalpolynom von  $v$  über  $K = \text{Quot}(R)$ . Nach ??? ist  $f = Z^d + r_{d-1}Z^{d-1} + \dots + r_0 \in R[X]$  da  $R$  normal ist. Sei  $g = Z^d + u \cdot r_{d-1}Z^{d-1} + \dots + u^d \cdot r_0$ . Dann ist  $g(uv) = u^d \cdot f(v) = 0$ . Da  $u \in R \setminus \{0\} \subseteq K^*$ , ist

$$K[uv] = K[v]$$

und somit ist der Grad der Erweiterung  $d = \deg(f)$ . Also ist  $g$  das Minimalpolynom von  $uv$ . Nach Lemma ??? ist wegen  $x \in \mathfrak{p}_1 R'$  alle Koeffizienten von  $g$  in  $\mathfrak{p}_1$ . Also ist auch  $r_{d-i} \in \mathfrak{p}_1$  und somit  $v^d$  und auch  $v \in \mathfrak{p}_1$ . Dann ist aber  $v \in \mathfrak{p}_0 \subseteq \mathfrak{q}_0$  was nicht sein kann. Also ist  $\mathfrak{p}_1 R' \cap T = \emptyset$  Wähle also  $\mathfrak{p}_1 R' \subseteq \mathfrak{q}_1$  mit  $\mathfrak{q}_1 \subseteq R'$  prim und  $\mathfrak{q}_1 \cap T = \emptyset$ . ( Betrachte  $R'_T$  ). Dann ist  $\mathfrak{p}_1 \subseteq \mathfrak{p}_1 R' \cap R \subseteq \mathfrak{q}_1 \cap R$ . Wenn  $a \in \mathfrak{q}_1 \cap R$  aber  $a \notin \mathfrak{p}_1$  dann wäre  $a \in \mathfrak{P} \cap T = \emptyset$  Also ist  $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$  und  $\mathfrak{q}_1 \subseteq \mathfrak{q}_0$  denn  $S' = R' \setminus \mathfrak{q}_0$ .  $\square$

## 7.5 Noether Normalisierung

**Definition 7.5.1.** Sei  $K$  ein Körper und  $R$  eine  $K$ -Algebra.  $y_1, \dots, y_n \in R$  heißen algebraisch unabhängig über  $K$ , falls die Surjektion

$$K[Y_1, \dots, Y_n] \rightarrow K[y_1, \dots, y_n]$$

ein Isomorphismus ist. Wenn  $R = L$  ein Körper ist, so heißt eine maximal algebraisch unabhängige Teilmenge Transzendenzbasis der Körpererweiterung  $L/K$ .

**Lemma 7.5.2** (Horrible Lemma). Sei  $I$  eine endliche Menge von Tupeln  $m = (m_1, \dots, m_n) \in \mathbb{N}^n$ . Es gibt  $r_1, \dots, r_{n-1} \in \mathbb{N}$  und  $r_n = 1$  sodass  $m \neq m' \in I \implies \sum_{i=1}^n r_i m_i \neq \sum_{i=1}^n r_i m'_i$

*Beweis.* Wenn  $n = 1$  dann ist das klar. Sei  $\bar{I} = \{\bar{m} = (m_2, \dots, m_n) \mid \exists m_1: (m_1, m_2, \dots, m_n) \in I\}$ . Nach Induktion gibt es  $r_2, \dots, r_n$  mit  $r_n = 1$  sodass

$$(m_2, \dots, m_n) \neq (m'_2, \dots, m'_n) \implies \sum_{i=2}^n r_i m_i \neq \sum_{i=2}^n r_i m'_i$$

Wähle  $r_1 > \max\{\sum_{i=2}^n r_i m_i \mid \bar{m} = (m_2, \dots, m_n) \in \bar{I}\}$ . Dann ist für  $m \neq m'$  entweder  $m_1 \neq m'_1$  oder  $\bar{m} = (m_2, \dots, m_n) \neq \bar{m}' = (m'_2, \dots, m'_n)$ . In beiden Fällen ist  $\sum_{i=1}^n r_i m_i \neq \sum_{i=1}^n r_i m'_i$ .  $\square$

**Lemma 7.5.3.** Sei  $K$  ein Körper und  $A$  eine  $K$ -Algebra vom endlichen Typ,  $A = K[x_1, \dots, x_n]$  und sei  $\varphi: K[X_1, \dots, X_n] \rightarrow A$  die natürliche Abbildung und  $y = \varphi(F)$  für ein  $F \neq 0$ . Dann gibt es Elemente  $y_1, \dots, y_{n-1} \in A$  sodass  $K[y_1, \dots, y_{n-1}, y] \rightarrow A$  endlich ist und  $A = K[y_1, \dots, y_{n-1}, y, x_n]$

*Beweis.* Setze  $y_i = x_i - x_n^{r_i}$  für  $i = 1, \dots, n-1$  wobei  $r_i \in \mathbb{Z}$  später bestimmt werden und setze  $r_n = 1$ . Definiere Relation  $G$  über  $K[y_1, \dots, y_{n-1}]$  durch

$$G(y_1, \dots, y_{n-1}, x_n) = F(y_1 + x_n^{r_1}, \dots, y_{n-1} + x_n^{r_{n-1}}, x_n) = F(x_1, \dots, x_n) = y$$

Schreibe  $F = \sum_{m=(m_1, \dots, m_n) \in I} a_m X^m = \sum_m a_m \prod X_i^{m_i}$ . Dann ist

$$\begin{aligned} G &= \sum_m a_m x_n^{m_n} \prod_{i \neq n} (y_i + x_n^{r_i}) \\ &= \sum_m a_m (x_n^{\sum_{i=1}^n r_i m_i} + \text{Rest}_m) \end{aligned}$$

wobei der Rest ein Polynom in  $x_n$  ist von Grad echt kleiner als  $\sum_{i=1}^n r_i m_i$ . Nach Lemma ??? kann man  $r_i$  so wählen, dass  $m \neq m' \implies \sum_{i=1}^n r_i m_i \neq \sum_{i=1}^n r_i m'_i$ . Dann wird  $\max\{\sum r_i m_i \mid a_m \neq 0\}$  genau in einem Summanden angenommen, sodass sich nicht alle Terme wegheben. Da  $a_m \neq 0$  wo das Maximum angenommen wird, ist  $x_n$  ganz über  $K[y_1, \dots, y_{n-1}, y]$ .  $\square$

**Bemerkung 7.5.4.** Wenn in ??  $y = 0$ , das heißt

$$x_1, \dots, x_n$$

algebraisch abhängig sind, dann gibt es  $y_1, \dots, y_{n-1}$  sodass  $K[y_1, \dots, y_{n-1}] \rightarrow K[x_1, \dots, x_n]$  endlich ist.

**Satz 7.5.5** (Noether Normalisierung). Sei  $K$  ein Körper und  $A$  eine  $K$ -Algebra von endlichem Typ. Dann gibt es  $z_1, \dots, z_m \in A$  sodass

1.  $z_1, \dots, z_m$  algebraisch unabhängig über  $K$  sind und
2.  $A$  ist endlich über  $K[z_1, \dots, z_m] \subseteq A$

*Beweis.* Es ist  $A = K[y_1, \dots, y_n]$ . Wenn  $n = 0$  ist, ist nichts zu zeigen. Sei  $n > 0$ . Wenn  $y_1, \dots, y_n$  algebraisch unabhängig sind über  $K$ , dann ist nichts zu zeigen. Seien  $y_1, \dots, y_n$  also algebraisch abhängig. Das heißt

$$K[Y_1, \dots, Y_n] \rightarrow K[y_1, \dots, y_n]$$

hat nicht triviale Kern. Nach Lemma ?? gibt es also  $y_1^*, \dots, y_{n-1}^* \in A$  sodass  $y_n$  ganz über  $A^* = K[y_1^*, \dots, y_{n-1}^*]$  und  $A = A^*[y_n]$ . Nach Induktion gibt es  $z_1, \dots, z_m \in A^*$  algebraisch unabhängig sodass  $A^*$  endlich ist über  $B = K[z_1, \dots, z_m]$  da  $y_n$  ganz über  $A^*$  ist ist  $A^*[y_n]$  endlich über  $A$  sodass  $A$  endlich über  $B$  ist.  $\square$



## 7.6 Krull-Dimension und Höhe

**Definition 7.6.1.** Die Krull-Dimension eines Rings  $R$  ist das Supremum aller Längen  $d$  von Ketten von Primidealen  $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$  in  $R$ .

**Beispiel 7.6.2.** Körper haben die Dimension 0. Es ist  $\dim(\mathbb{Z}) = 1$  und  $\dim(K[X]) = 1$ . Ein artinscher Ring ist ein noetherscher Ring mit Krull-Dimension 0

**Lemma 7.6.3.** Für einen Körper  $K$  gilt

$$\dim(K[X_1, \dots, X_n]) = n.$$

*Beweis.* Primideale  $\mathfrak{p}_i = (X_1, \dots, X_i)$  bilden Kette der Länge  $n$ . Der Fall  $n = 0$  ist klar. Sei  $R = K[X_1, \dots, X_n]$  und  $d = \dim(R)$ . Wenn  $n \geq 1$  dann ist  $d \geq 1$  und sei  $\mathfrak{p}_0 \subsetneq \mathfrak{p}_d$  eine Kette von Primidealen. Sei  $\mathfrak{q} = \mathfrak{p}_{d-1}$  und  $R_i = K[X_i] \subseteq R$  und  $\mathfrak{q}_i = \mathfrak{q} \cap R_i$ . Angenommen  $\mathfrak{q}_i \neq 0$  für alle  $i$ . Dann enthält  $\mathfrak{q}_i$  ein Polynom  $g_i(X_i)$  mit  $g_i \neq 0$  für alle  $i$ . Sei  $J = (g_1, \dots, g_n)$ . Es ist  $R/J$  ein endlich-dimensionaler  $K$ -Vektorraum, also ist  $R/J$  artinscher Ring also null-dimensional. Wir haben aber eine Kette

$$\mathfrak{p}_{d-1}/J \subsetneq \mathfrak{p}_d/J$$

in  $R/J$ . Also muss es in  $i$  gegeben sodass  $\mathfrak{q}_i = 0$ . Nach Umordnen ist das ohne Einschränkung  $\mathfrak{q}_n$ . Sei  $S = R_n \setminus \{0\}$  multiplikative Menge. Dann ist  $S \cap \mathfrak{p}_{d-1} = \emptyset$ . Also gibt es Kette  $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-1}$  von Primidealen der Länge  $d-1$  in Lokalisierung

$$S^{-1}R = (S^{-1}K[X_n])[X_1, \dots, X_{n-1}] = K(X_n)[X_1, \dots, X_{n-1}].$$

Das ist Polynomring in  $n-1$  Variablen über Körper. Nach Induktion ist also  $d-1 \leq n-1$  also  $d \leq n$ . □

**Lemma 7.6.4.**

1. Ein Hauptidealring, der kein Körper ist hat Dimension 1.
2.  $R = K[X_1, X_s, \dots]$  hat Dimension  $\infty$ .

**Definition 7.6.5.** Sei  $I$  ein Ideal von  $R$ . Definiere  $\text{ht}(I)$  als das Supremum von Längen von Ketten von Primidealen in  $I$  und  $\text{coht}$  als das Supremum von Längen von Ketten von Primidealen in  $R$  die  $I$  enthalten.

**Lemma 7.6.6.** Sei  $R$  ein faktorieller Ring.

1. Die Primideale der Höhe 1 sind genau die Ideale  $p$  für Primideale von  $R$ .
2. In  $K = \text{Quot}(R)$  ist  $R = \bigcap_{\text{coht } \mathfrak{p}=1} R_{\mathfrak{p}}$ .

*Beweis.* Es ist  $(0) \subseteq (p)$  also  $\text{ht}(p) \geq 1$ . Wenn  $\mathfrak{p} \subseteq (p)$  ein Primideal ungleich 0 dann gibt es Primzahl  $q \in \mathfrak{p}$  also  $q = xp$  und somit  $\mathfrak{p} = (p)$ . Also  $\text{ht}(p) = 1$ . Genauso zeigt man, dass jedes Primideal der Höhe 1 von dieser Form ist. Klar ist, dass  $R \subseteq \bigcap R_{\mathfrak{p}}$ . Sei also  $x \in \bigcap R_{\mathfrak{p}}$  mit  $x = \frac{a}{b}$  vollständig gekürzt. Wenn  $b \neq 1$  dann ist  $b = p_1 \cdots p_r$  und somit  $b \in p_1$ . Also ist  $\frac{a}{b}$  nicht in  $R_{p_1}$ . Also muss  $b = 1$  sein und somit  $x \in R$ . □

**Lemma 7.6.7.** Sei  $I \subseteq R$  ein Ideal. Es gilt

1.  $\text{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$  für ein Primideal  $\mathfrak{p}$  von  $R$  und  $\text{coht}(I) = \dim(R/I)$
2.  $\text{ht}(I) = \min_{I \subseteq \mathfrak{p} \in \text{Spec}(R)} \text{ht}(\mathfrak{p})$
3.  $\dim(R) = \sup_{\mathfrak{p} \in \text{Spec } R} \dim(R_{\mathfrak{p}}) = \sup_{\mathfrak{p} \in \text{Spec } R} \dim(R_{\mathfrak{p}})$

*Beweis.* 1. und 2. sind klar. Ohne Einschränkung sei  $\dim(R) < \infty$  und  $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$  maximale Kette. Dann ist  $\dim(R) = d$  und

$$\sup \dim(R_{\mathfrak{p}}) = \sup \text{ht}(\mathfrak{p}) = \text{ht}(\mathfrak{p}_d) = d$$

□

**Satz 7.6.8.** Sei  $R \rightarrow R'$  ganz und injektiv. Sei  $I' \subseteq R'$  ein Ideal und  $I = I' \cap R$ . Dann gilt

1.  $\dim(R') = \dim(R)$
2.  $\text{ht}(I) \leq \text{ht}(I')$  und  $\text{ht}(I) = \text{ht}(I')$  wenn  $R, R'$  Integritätsbereiche und  $R$  normal ist.
3.  $\text{coht}(I) = \text{coht}(I')$ .

*Beweis.* Nach [Going Up](#) kann jede aufsteigende Kette in  $R$  zu einer in  $R'$  erweitert werden. Jede Kette in  $R'$  schränkt sich nach Satz ??? zu einer Kette ein. Also gilt 1. und dann folgt 3. direkt. Wenn  $I'$  Primideal ist, dann lässt sich genauso eine zu  $I'$  aufsteigende Kette einschränken und gibt eine zu  $I$  aufsteigende Kette. Also ist  $\text{ht}(I') \leq \text{ht}(I)$ . Wenn  $I'$  nicht prim ist, wähle  $\mathfrak{p}$  minimal mit  $I \subseteq \mathfrak{p}$ . Nach ?? zu  $R/I \rightarrow R'/I'$  gibt es minimales  $I' \subseteq \mathfrak{q}$  prim das über  $\mathfrak{p}$  liegt. also ist  $\text{ht}(\mathfrak{q}) \leq \text{ht}(\mathfrak{p})$  und somit  $\text{ht}(I') \leq \text{ht}(I)$ . Wenn  $R, R'$  Integritätsbereiche mit  $R$  normal, dann lässt sich auch jede Kette mit [Going Up](#) heben, sodass die Höhen gleich sind.  $\square$

**Satz 7.6.9.** Sei  $A$  eine  $K$ -Algebra von endlichem Typ und  $A$  ein Integritätsbereich. Dann ist

$$\dim(A) = \text{transdeg}_K(\text{Quot}(A))$$

*Beweis.* Nach [Noether Normalisierung](#) gibt es injektiven endlichen Morphismus  $K[X_1, \dots, X_d] \rightarrow A$ . Nach Satz 7.6.8 ist  $\dim(A) = \dim(K[X_1, \dots, X_d]) = d$ . Außerdem ist

$$\begin{aligned} d &= \text{transdeg}_K(\text{Quot}(K[X_1, \dots, X_d])) \\ &= \text{transdeg}_K(\text{Quot}(A)) \end{aligned}$$

da  $\text{Quot}(A)/\text{Quot}(K[X_1, \dots, X_d])$  algebraisch ist.  $\square$

**Satz 7.6.10.** Sei  $A$  eine  $K$ -Algebra von endlichem Typ,  $A$  ein Integritätsbereich. Dann ist

1.  $\text{ht}(\mathfrak{p}) + \text{coht}(\mathfrak{p}) = \dim(A)$  für alle primideale  $\mathfrak{p} \subseteq A$
2.  $\text{htm} = \dim(A)$  für alle maximalen Ideale.

*Beweis.* 2 folgt aus 1. Nach ??? gibt es endlichen Monomorphismus  $K[x_1, \dots, x_d] \rightarrow A$  mit  $\dim(A) = d$  und  $x_1, \dots, x_d$  algebraisch unabhängig. Wenn  $d = 0$  dann ist  $A$  ganz über  $K$  also Körper, da stimmt die Aussage. Wenn  $\mathfrak{p} = 0$  dann stimmt die Aussage auch. Sei also  $d \geq 1$  und  $\mathfrak{p} \neq 0$ . Wähle  $y \in \mathfrak{p} \cap K[x_1, \dots, x_d]$  mit  $y \neq 0$ . Das existiert da  $\mathfrak{p} \neq 0 \implies \mathfrak{p} \cap K[x_1, \dots, x_d] \neq 0$  nach Satz ??? . Nach Lemma ??? gibt es  $y_1, \dots, y_{d-1} \in K[x_1, \dots, x_d]$  such that  $K[y_1, \dots, y_{d-1}, y] \rightarrow K[x_1, \dots, x_d]$  ist endlich und injektiv und  $y_1, \dots, y_{d-1}, y$  algebraisch unabhängig. Dann ist  $K[y_1, \dots, y_{d-1}, y] \rightarrow A$  endlich und da  $K[y_1, \dots, y_{d-1}, y]$  normal nach ??? (faktoriell impliziert normal). Nach [Going Down](#) gibt es Ideal  $\mathfrak{p}_0 \subseteq \mathfrak{p} \subseteq A$  mit  $\mathfrak{p}_0 \cap K[y_1, \dots, y_{d-1}, y] = (y_d)$ . Betrachte Monomorphismus  $K[Y_1, \dots, Y_{d-1}] \rightarrow A/\mathfrak{p}_0$  und Ideal  $\mathfrak{p}/\mathfrak{p}_0$ . Nach Induktion ist

$$\text{ht}(\mathfrak{p}/\mathfrak{p}_0) + \text{coht}(\mathfrak{p}/\mathfrak{p}_0) = d - 1$$

Da  $\text{ht}(\mathfrak{p}) \geq \text{ht}(\mathfrak{p}/\mathfrak{p}_0) + 1$  und  $\text{coht}(\mathfrak{p}) = \text{coht}(\mathfrak{p}/\mathfrak{p}_0)$  ist

$$\text{ht}(\mathfrak{p}) + \text{coht}(\mathfrak{p}) \geq d$$

und somit  $= d$ .  $\square$

**Bemerkung 7.6.11.** Es gilt

$$\text{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}) = \text{transdeg}_K(\text{Quot}(R_{\mathfrak{p}})) = \text{transdeg}_K(\text{Quot}(A))$$

Nach Satz ??? und  $\text{coht}(\mathfrak{p}) = \text{transdeg}_K(\text{Quot}(A/\mathfrak{p}))$  Also haben wir

$$\text{ht}(\mathfrak{p}) = \text{transdeg}_K(\text{Quot}(A)) - \text{transdeg}_K(k(\mathfrak{p}))$$

mit  $k(\mathfrak{p}) = \text{Quot}(A/\mathfrak{p})$ .

**Satz 7.6.12.** Jede maximale Kette von Primidealen  $\mathfrak{q}\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_d = \mathfrak{p}$  hat Länge

$$d = \text{transdeg}_K(k(\mathfrak{q})) - \text{transdeg}_K(k(\mathfrak{p}))$$

*Beweis.* Sei  $n = \text{transdeg}_K(k(\mathfrak{q}))$ ,  $m = \text{transdeg}_K(k(\mathfrak{p}))$ . Da  $\dim(A/\mathfrak{p}) = n$  nach Satz ?? gibt es  $\mathfrak{p} = \mathfrak{p}_d \subsetneq \dots \subsetneq \mathfrak{p}_{d+n}$  in  $A$ . Da  $\dim(A/\mathfrak{q}) = m$  folgt, dass  $d + n \leq m$  also  $d \leq m - n$ . Sei  $\mathfrak{q} = \mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_m$  aufsteigende Kette. Da  $\text{ht}(\mathfrak{p}/\mathfrak{q}) + \text{coht}(\mathfrak{p}/\mathfrak{q}) = \dim(A/\mathfrak{q})$  nach ??? gibt es maximale Kette, die  $\mathfrak{p}$  beinhaltet. Der Teil hinter  $\mathfrak{p}$  hat Länge  $\leq n$  der Teil Zwischen  $\mathfrak{p}$  und  $\mathfrak{q}$  hat Länge  $\geq mn$ . Also ist  $= m - n$ .  $\square$

## Kapitel 8

# Schritte zur Algebraischen Geometrie

### 8.1 Nullstellensatz

**Satz 8.1.1** (Schwacher Nullstellensatz). *Sei  $K$  ein Körper,  $L$  eine  $K$ -Algebra von endlichem Typ die ein Körper ist. Dann ist  $L/K$  endlich.*

*Beweis.* Nach [Noether Normalisierung](#) gibt es  $z_1, \dots, z_m \in L$  algebraisch unabhängig sodass  $L$  endlich ist über  $A = K[z_1, \dots, z_m]$ . Dann ist  $A \subseteq L$  ganz und da  $L$  ein Körper ist, ist  $A$  ein Körper. Da  $z_1, \dots, z_m$  algebraisch unabhängig sind, ist  $A$  ein Polynomring in  $m$  Variablen. Also ist  $m = 0$  und  $L$  ist endlich über  $K$ .  $\square$

**Korollar 8.1.2.** *Sei  $K$  ein Körper und  $f: A \rightarrow B$  ein Homomorphismus von  $K$ -algebren sodass  $B$  eine  $K$ -Algebra vom endlichen Typ ist. sei  $\mathfrak{m} \subseteq B$  ein maximales Ideal. Dann ist  $f^{-1}(\mathfrak{m})$  maximal.*

*Beweis.* Es ist  $K \rightarrow A/f^{-1}(\mathfrak{m}) \rightarrow B/\mathfrak{m}$  injektiv, da  $B/\mathfrak{m}$  eine endliche Körpererweiterung nach Schwachen NstSatz. Dann sind  $K \rightarrow A/f^{-1}(\mathfrak{m}) \rightarrow B/\mathfrak{m}$  alle ganz und damit  $A/f^{-1}(\mathfrak{m})$   $\square$

**Beispiel 8.1.3.** Sei  $K$  ein Körper und  $R = K[X_1, \dots, X_n]$  und  $\mathfrak{m} \subseteq R$  ein maximales Ideal und  $L = R/\mathfrak{m}$ . Nach Schwachem Nullstellensatz ist  $L/K$  endliche, algebraische Erweiterung.

**Korollar 8.1.4.** *Sei  $K$  algebraisch abgeschlossen und  $\mathfrak{m} \subseteq R = K[X_1, \dots, X_n]$  ein maximales Ideal. Dann ist  $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$  für  $a_1, \dots, a_n$  in  $K$  und die Projektion  $\pi: R \rightarrow R/\mathfrak{m}$  ist  $f \mapsto f(a_1, \dots, a_n)$ . Das heißt es gibt Bijektion  $K^n \rightarrow \text{Specm}(R)$ ,  $(a_1, \dots, a_n) \mapsto (X - a_1, \dots, X_n - a_n)$ .*

*Beweis.* Sei  $L = K[X_1, \dots, X_n]/\mathfrak{m}$ . Dann ist nach ???  $L/K$  algebraisch also  $L = K$ . Das heißt  $\pi: K[X_1, \dots, X_n] \rightarrow K$  und sei  $a_i = \pi(X_i)$ . Dann ist  $\pi(X_i - a_i) = 0$  also  $X_i - a_i \in \mathfrak{m}$  für alle  $i$ . Also ist  $\mathfrak{m} \supseteq (X_1 - a_1, \dots, X_n - a_n)$  und letzteres ist maximal denn die Abbildung  $K[X_1, \dots, X_n] \rightarrow K, f \mapsto f(a_1, \dots, a_n)$  hat dieses Ideal als Kern.  $\square$

**Definition 8.1.5.** Sei  $K$  ein Körper. Eine Varietät  $V \subseteq K^n$  ist eine Teilmenge

$$V = V(J) = \{p = (a_1, \dots, a_n) \in K^n \mid f(p) = 0 \forall f \in J\}$$

für ein Ideal  $J \subseteq K[X_1, \dots, X_n]$  ein Ideal. Da  $J = (f_1, \dots, f_m)$  endlich erzeugt ist, ist  $V$  definiert durch  $f_1(p) = \dots = f_m(p) = 0$ .

**Satz 8.1.6.** *Sei  $K$  algebraisch abgeschlossen und  $A = K[X_1, \dots, X_n]/J$  für ein Ideal  $J \subseteq K[X_1, \dots, X_n]$ . Dann hat jedes maximale Ideal von  $A$  die Form*

$$(X - a_1, \dots, X_n - a_n)$$

für ein  $(a_1, \dots, a_n) \in V(J)$ . Das heißt es gibt Bijektion von  $V(J)$  und  $\text{Specm} A$  gegeben durch  $(a_1, \dots, a_n) \leftrightarrow (X_1 - a_1, \dots, X_n - a_n)$ .

*Beweis.* Ideal von  $A$  sind Ideale in  $K[X_1, \dots, X_n]$  die  $J$  enthalten. Also haben alle maximalen Ideale von  $A$  die Form  $(X_1 - a_1, \dots, X_n - a_n)$  für  $a_1, \dots, a_n$  sodass  $J \subseteq (X_1 - a_1, \dots, X_n - a_n)$ . Da jedoch

$$(X_1 - a_1, \dots, X_n - a_n) = \ker(f \mapsto f(a_1, \dots, a_n))$$

ist, ist  $J \subseteq (X_1 - a_1, \dots, X_n - a_n) \iff f(a_1, \dots, a_n) = 0 \forall f \in J$  also ist  $(a_1, \dots, a_n) \in V(J)$ .  $\square$

**Bemerkung 8.1.7.** Es gibt zwei Abbildungen

$$\{J \subseteq K[X_1, \dots, X_n] \text{ Ideal}\} \begin{array}{c} \xrightarrow{V} \\ \xleftarrow{I} \end{array} \{X \subseteq K^n \text{ Teilmenge}\}$$

wobei  $I(X) = \{f \in K[X_1, \dots, X_n] \mid f(p) = 0 \forall p \in X\}$  ein Ideal ist. Es gilt

1.  $J \subseteq J' \implies V(J) \supseteq V(J')$
2.  $X \subseteq Y \implies I(X) \supseteq I(Y)$
3.  $X \subseteq V(I(X))$
4.  $X \text{ ist Varietät} \iff X = V(I(X))$
5.  $J \subseteq I(V(J))$ .

**Bemerkung 8.1.8.** Sei  $K$  algebraisch abgeschlossen und  $R = K[X_1, \dots, X_n]$  und  $Y \subseteq R$  eine Teilmenge. Dann gilt

1.  $V(Y) = V((Y))$
2.  $V(f) = V(f^n)$
3.  $I \subseteq R \text{ Ideal} \implies V(\sqrt{I}) = V(I)$
4.  $Y \subseteq Y' \subseteq R \implies V(Y') \subseteq V(Y)$
5.  $Y_i \subseteq R \implies V(\bigcup_i Y_i) = \bigcap_i V(Y_i)$

**Satz 8.1.9** (Nullstellensatz). *Sei  $K$  ein algebraisch abgeschlossener Körper.*

1. wenn  $J \subsetneq K[X_1, \dots, X_n]$  dann ist  $V(J) \neq \emptyset$ .
2.  $I(V(J)) = \text{rad}(J)$

Das heißt  $I$  und  $V$  induzieren inverse Bijektionen

$$\{\text{Radikale } J = \sqrt{J} \subseteq K[X_1, \dots, X_n]\} \begin{array}{c} \xrightarrow{V} \\ \xleftarrow{I} \end{array} \{\text{Varietäten } V \subseteq K^n\}$$

*Beweis.* Sei  $J \subseteq \mathfrak{m}$  für ein maximales Ideal  $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ .

Dann ist  $P = (a_1, \dots, a_n) \in V(J)$ . Angenommen  $f \in K[X_1, \dots, X_n]$  sodass  $f(p) = 0$  für alle  $p \in V(J)$ . Sei  $J' = (J, fY - 1) \subseteq K[X_1, \dots, X_n, Y]$ . Ein Punkt  $p \in V(J')$  ist  $(n+1)$ -Tupel  $(a_1, \dots, a_n, b) \in K^{n+1}$ . Angenommen  $V(J') \neq \emptyset$ . Dann gibt es so einen Punkt  $p$  und  $p' = (a_1, \dots, a_n)$  ist dann in  $V(J)$ . Da aber  $bf(a_1, \dots, a_n) = 1$  ist, ist das ein Widerspruch. Also ist  $V(J') = \emptyset$  und somit  $J' = K[X_1, \dots, X_n, Y]$ . Also gibt es Gleichung

$$1 = \sum g_i h_i + g_0(fY - 1)$$

mit  $g_i \in K[X_1, \dots, X_n, Y]$  und  $h_i \in J$ . Multipliziere die Gleichung mit  $f^m$  sodass  $Y$  nur in Kombination mit  $f$  auftritt und erhalte

$$f^m = \sum G_i(X_1, \dots, X_n, fY) h_i + G_0(X_1, \dots, X_n, fY)(fY - 1)$$

Gleichung gilt auch mod  $(fY - 1)$  was zeigt, dass  $f^m \in J$ . Wenn  $f^n(a) = 0$  ist dann ist  $f(a) = 0$  also  $\text{rad}(J) \subseteq I(V(J))$ . Denn wenn  $f^n \in J$  dann ist  $f^n \in I(V(J))$  also  $f^n(p) = 0$  für alle  $p \in V(J)$ . also  $f(p) = 0$  also  $f \in I(V(J))$ .  $\square$

**Bemerkung 8.1.10.** 1. Der Satz hat den Namen wegen 1. Sei  $M$  eine Menge von Polynomen in  $K[X_1, \dots, X_n]$  gegeben. Dann gibt es eine gemeinsame Nullstelle. Der Satz ist falsch, wenn  $K$  nicht algebraisch abgeschlossen ist, denn wenn  $f$  ein Polynom  $K[X]$  ohne Nullstelle ist, dann ist  $(f) \neq K[X]$  aber  $V(f) = \emptyset$  und  $I(V(f)) = K[X]$ .

2. Es ist  $\text{rad } J = \bigcap_{J \subseteq \mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$  aber der Nullstellensatz ist stärker, denn 2. sagt es reichen die maximalen Ideale, die  $J$  enthalten.

**Definition 8.1.11.** Seien  $X \subseteq K^n$  und  $Y \subseteq K^m$  abgeschlossene Teilmengen. Eine Abbildung  $\varphi: X \rightarrow Y$  heißt polynomiell, wenn es  $f_1, \dots, f_m \in K[X_1, \dots, X_m]$  gibt sodass  $\varphi(x) = (f_1(x), \dots, f_m(x))$  für alle  $x \in X$ . Die Polynome  $f_i$  sind nicht eindeutig, denn sie können um ein Element von  $I(X)$  verändert werden. Für eine Teilmenge  $X \subseteq K^n$  definiere  $A(X) = K[X_1, \dots, X_n]/I(X)$ .

**Lemma 8.1.12.** Für abgeschlossene  $X \subseteq K^n$  und  $Y \subseteq K^m$  gibt es Bijektion

$$\{\varphi: X \rightarrow Y \text{ polynomiell}\} \rightarrow \text{Hom}_{K\text{-Alg}}(A(Y), A(X))$$

*Beweis.* Angenommen  $g \in \text{Hom}_{K\text{-Alg}}(A(Y), A(X))$  gegeben. Betrachte

$$\begin{array}{ccc} K[X_1, \dots, X_m] & \xrightarrow{\quad} & K[X_1, \dots, X_m] \\ \downarrow & & \downarrow \\ A(Y) & \xrightarrow{\quad g \quad} & A(X) \end{array}$$

Sei  $f_i \in K[X_1, \dots, X_n]$  ein Urbild von  $g(\bar{X}_i)$ . Dann definieren  $f_1, \dots, f_m$  eine polynomielle Abbildung  $\varphi: X \rightarrow Y, x \mapsto (f_1(x), \dots, f_m(x))$ . Wenn andersrum  $\varphi$  gegeben ist, dann ist  $\varphi^*: A(Y) \rightarrow A(X), \varphi^*(f) = f \circ \varphi$  eine Abbildung von  $K$ -Algebren.  $\square$

**Bemerkung 8.1.13.** Sei  $K$  ein Körper und  $R = K[X_1, \dots, X_n]$ . Dann ist für  $J, J'$  Ideale von  $R$

$$V(J) = V(J') \iff \sqrt{J} = \sqrt{J'}$$

Denn  $V(J) = V(J') \implies I(V(J)) = I(V(J'))$  und wenn  $\sqrt{J} = \sqrt{J'}$  dann ist  $I(V(J)) = I(V(J'))$  also  $V(J) = V(I(V(J))) = \dots = V(J')$

**Definition 8.1.14.** Sei  $K$  algebraisch abgeschlossener Körper. Eine Varietät  $X \subseteq K^n$  ist irreduzibel, falls  $X \neq \emptyset$  und nicht die Vereinigung zweier echter Untervarietäten ist.

**Satz 8.1.15.** Eine Varietät  $X$  ist irreduzibel genau dann wenn  $I(X)$  prim ist.

*Beweis.* Sei  $I = I(X)$ . Angenommen es gibt  $f, g \in A = K[X_1, \dots, X_n] \setminus I$  sodass  $fg \in I$ . Sei  $J_1 = (I, f)$  und  $J_2 = (I, g)$ . Es ist  $V(J_1) = X \cap V(f)$  und da  $f \notin I(X)$  ist  $V(J_1) \subsetneq X$  und analog  $V(J_2) \subsetneq X$ . Es ist also

$$X = V(J_1) \cup V(J_2)$$

reduzibel. Wenn  $I(X)$  prim ist und

$$X = V(J_1) \cup V(J_2) = V(J_1 J_2)$$

ist, dann ist  $J_1 J_2 \subseteq I(X)$ . Also ist  $J_1 \subseteq I(X)$  oder  $J_2 \subseteq I(X)$ , d.h.  $X = V(J_1)$  oder  $X = V(J_2)$ .  $\square$

**Beispiel 8.1.16.**

1. Primideale in  $K[X]$  sind  $(0)$  und  $(X - a)$  für  $a \in K$ . Die Zugehörigen irreduziblen Varietäten sind  $K$  bzw.  $\{0\}$ .
2. Primideale in  $K[X, Y]$  sind  $(0)$ ,  $f$  für irreduzible Polynome  $f$  und  $(X - a, Y - b)$  für  $a, b \in K$ . Zugehörige irreduzible Varietäten sind  $K^2$ , die durch  $f = 0$  definierte Kurve und die Einpunktmenge  $(a, b)$ .

**Korollar 8.1.17.** Sei  $K$  algebraisch abgeschlossen. Dann gibt es mit  $V, I$  bijektive Korrespondenz

$$\begin{array}{ccc} \left\{ \text{Radikale } J = \sqrt{J} \subseteq K[X_1, \dots, X_n] \right\} & \xrightleftharpoons[I]{V} & \{ \text{Varietäten } X \subseteq K^n \} \\ \uparrow & & \uparrow \\ \{ \text{Primideale } \mathfrak{p} \subseteq K[X_1, \dots, X_n] \} & \xrightleftharpoons{\quad} & \{ \text{irreduzible Varietäten } X \subseteq K^n \} \end{array}$$

Also ist  $\text{Spec } K[X_1, \dots, X_n] = \{ \text{irreduzible Varietäten } X \subseteq K^n \}$ .

**Satz 8.1.18.** Sei  $K$  algebraisch abgeschlossen und  $A = K[X_1, \dots, X_n]/J$  für ein Ideal  $J \subseteq K[X_1, \dots, X_n]$ . Dann gibt es Bijektive Korrespondenz

$$\text{Spec } A \leftrightarrow \{ \text{irreduzible Varietäten } X \subseteq V(J) \}$$

**Definition 8.1.19** ( Zariski Topologie ). Die Varietäten  $X \subseteq K^n$  bilden abgeschlossene Mengen einer Topologie auf  $K^n$ .

**Bemerkung 8.1.20.** Auf  $\mathbb{R}^n$  oder  $\mathbb{C}^n$  ist das nicht die Standardtopologie. Zwar sind Varietäten in der Standardtopologie abgeschlossen, da Polynome stetig sind, aber  $B_\epsilon(o)$  ist nicht Zariski-offen.

**Beispiel 8.1.21.** Ideale  $\neq 0$  in  $K[X]$  sind von der Form  $(f)$  und  $V(f)$  ist endlich. Die Zariski Topologie entspricht hier der Co-endlichen Topologie. Die Zariski-Topologie ist nicht Hausdorff, für  $X = V(J)$  irreduzibel ist  $X$  nicht die Vereinigung von zwei echten abgeschlossenen Teilmengen. Also haben zwei nicht-leere offene Teilmengen von  $X$  nicht-leeren Schnitt. Somit  $X$  nicht Hausdorff und damit auch nicht  $K^n$ .

**Satz 8.1.22** ( Zariski Topologie ist noethersch ).

1. Jede absteigende Kette  $V_1 \supseteq V_2 \supseteq \dots$  von Varietäten von  $K^n$  wird stationär.
2. Eine nicht-leere Menge von Varietäten von  $K^n$  hat minimales Element.

*Beweis.* 1 und 2 sind äquivalent. Zeige also 1. Die absteigende Kette der Varietäten korrespondiert zu absteigender Kette von Idealen in  $K[X_1, \dots, X_n]$  und das ist noethersch, wird also stationär.  $\square$

**Satz 8.1.23.** Sei  $X \subseteq K^n$  Varietät. Dann hat  $X$  Zerlegung

$$X = X_1 \cup X_2 \cup \dots \cup X_k$$

wobei jedes  $X_i$  irreduzibel ist und  $X_i \not\subseteq \bigcup_{i \neq j} X_j$ .

*Beweis.* Wenn  $X$  nicht irreduzibel ist, dann ist  $X = X_1 \cup X_2$  mit  $X_1, X_2 \subsetneq X$ . Fahre so fort mit  $X_1$  und  $X_2$  und erhalte absteigende Kette von Untervarietäten von  $X$ . Da  $X$  noethersch ist, muss diese abbrechen.  $\square$

**Korollar 8.1.24.** Ein Radikal Ideal  $J$  von  $K[X_1, \dots, X_n]$  ist Schnitt von endlich vielen Primidealen.

*Beweis.* Irreduzible Zerlegung von  $V(J)$  entspricht Schnitt von Primidealen da  $I(V(J)) = \sqrt{J} = J$   $\square$

**Definition 8.1.25.** Sei  $A$  ein Ring. Die Zariski-Topologie auf  $\text{Spec } A$  ist gegeben durch die abgeschlossenen Mengen  $V(J) = \{ \mathfrak{p} \in \text{Spec } A \mid J \subseteq \mathfrak{p} \}$  wobei  $J \subseteq A$  ein Ideal ist.

**Bemerkung 8.1.26.**  $J \subseteq \mathfrak{p}$  bedeutet, dass  $f \in J$  auf 0 geschickt wird durch  $A \rightarrow A/\mathfrak{p}$ .

**Lemma 8.1.27.** Sei  $R$  ein Ring und  $\mathfrak{p} \in \text{Spec}(R)$ . Es gilt

1.  $V(\mathfrak{p})$  ist der Abschluss von  $\{ \mathfrak{p} \}$ .
2.  $\{ \mathfrak{p} \} \subseteq \text{Spec}(R)$  ist abgeschlossen genau dann wenn  $\mathfrak{p}$  maximal ist.

*Beweis.* Sei  $V = V(J)$  abgeschlossen mit  $\{ \mathfrak{p} \} \subseteq V$ , d.h.  $J \subseteq \mathfrak{p}$ . Dann ist  $V(\mathfrak{p}) \subseteq V(J)$  und somit  $V(\mathfrak{p})$  der Abschluss. Die zweite Aussage folgt aus der ersten.  $\square$

**Bemerkung 8.1.28.** Sei  $X \subseteq \text{Spec } A$  und  $I(X) := \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$ . Es gilt

$$\sqrt{J} = \bigcap_{J \subseteq \mathfrak{p} \text{ prim}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in V(J)} \mathfrak{p} = I(V(J))$$

Wenn  $J, J'$  Radikale Ideale, dann

$$V(I) = V(J') \implies J = \sqrt{J} = \sqrt{J'} = J'$$

. Das gibt Bijektionen

$$\begin{array}{ccc}
\left\{ \text{Radikale } J = \sqrt{J} \subseteq A \right\} & \begin{array}{c} \xrightarrow{V} \\ \xleftarrow{I} \end{array} & \left\{ \text{abgeschlossene } X \subseteq \text{Spec } A \right\} \\
\uparrow & & \uparrow \\
\left\{ \text{Primideale } \mathfrak{p} \subseteq A \right\} & \begin{array}{c} \xrightarrow{\quad} \\ \xleftarrow{\quad} \end{array} & \left\{ X \subseteq \text{Spec } A \text{ irreduzibel} \right\}
\end{array}$$

und analog impliziert  $A$  noethersch, dass  $\text{Spec } A$  noethersch ist und in dem Fall jede abgeschlossene Menge von  $\text{Spec } A$  Vereinigung endlich vieler irreduziblen Mengen ist.

**Korollar 8.1.29.** *Sei  $A$  noethersch.*

1.  $J \subseteq A$  Ideal dann hat  $V(J)$  endliche Anzahl minimaler Elemente.
2.  $\text{rad } J$  ist Schnitt endlich vieler Primideale.
3. Wenn  $A$  Nullteiler hat, dann hat  $A$  entweder nicht-triviale nilpotente Elemente oder endliche Anzahl  $\geq 2$  von minimalen Primidealen

*Beweis.* 1 und 2 sind klar. Angenommen  $\text{rad } A = 0$ . Es ist  $\text{rad } A = \bigcap \mathfrak{p}_i$  wobei  $\mathfrak{p}_i$  die minimalen Primideale von  $A$  sind. Fall es nur ein  $\mathfrak{p}$  gibt, dann ist  $\mathfrak{p} = 0$  also  $A$  nullteilerfrei.  $\square$

**Lemma 8.1.30.** *Ein Topologischer Raum  $X$  ist noethersch genau dann, wenn jede offene Menge quasi-kompakt ist.*

*Beweis.* Sei  $X$  noethersch und  $U \subseteq X$  offen mit  $U = \bigcup_i U_i$ . Sei  $V_1 = U_{i_1}^c$ . Angenommen  $V_1, \dots, V_k$  gegeben. Wenn  $U = \bigcup_{i=1}^k U_{i_k}$  dann ist man fertig. Sonst wähle  $U_{i_{k+1}}$  mit

$$\bigcup_{i=1}^k U_{i_k} \subsetneq \bigcup_{i=1}^{k+1} U_{i_k}$$

und setze

$$V_{k+1} = \left( \bigcup_{i=1}^{k+1} U_{i_k} \right)^c \subsetneq V_k$$

. Das ist abgeschlossen und gibt absteigende Kette abgeschlossener Mengen  $V_1 \supsetneq V_2 \supsetneq \dots$  was stationär wird. Also ist  $U$  quasi-kompakt. Wenn andersrum jede offene Menge quasi-kompakt ist und  $V_1 \supsetneq \dots$  Kette von abgeschlossenen Mengen ist, dann setze  $U_i = V_i^c$ . Dann hat  $\bigcup U_i$  endliche Teilüberdeckung und die Kette wird stationär.  $\square$

**Lemma 8.1.31.** *Sei  $R$  ein Ring. Dann ist  $\text{Spec } R$  quasi-kompakt.*

*Beweis.* Sei  $\text{Spec } R = \bigcup U_i$  offene Überdeckung. Dann ist

$$\begin{aligned}
\emptyset &= \bigcap U_i^c \\
&= \bigcap V(J_i) \\
&= \bigcap \left( \sum J_i \right)
\end{aligned}$$

Dann gibt es also Darstellung

$$1 = \sum_{k=1}^n f_{i_k} x_{i_k}$$

mit  $f_{i_k} \in R$  und  $x_{i_k} \in J_{i_k}$ . Also ist schon

$$\emptyset = V\left(\sum_{i=1}^n J_{i_k}\right)$$

und somit  $\text{Spec } R = \bigcup_{i=1}^n U_{i_k}$   $\square$

**Beispiel 8.1.32.** Sei  $R = K[X_1, X_2, \dots]/J^2$  mit  $J = (X_1, X_2, \dots)$ . Es ist

$$\operatorname{Spec}(R) = \{J/J^2\}$$

noethersch aber  $R$  ist nicht noethersch da  $(X_1) \subsetneq (X_1, X_2) \subsetneq \dots$  aufsteigende Kette ist, die nicht stationär wird.

**Definition 8.1.33** (Dimension).

1. Die Dimension einer Varietät  $X \subseteq K^n$  ist das Supremum aller Längen von Ketten von irreduziblen Varietäten  $V_0 \subsetneq \dots \subsetneq V_d \subseteq X$ .
2. Die Krull-Dimension eines Ringes  $R$  ist das Supremum aller Längen  $d$  von Ketten von Primidealen  $P_0 \subsetneq \dots \subsetneq P_d$  in  $R$ .



# Kapitel 9

## Bewertungsringe und Dedekindringe

### 9.1 Bewertungsringe

**Definition 9.1.1.** Sei  $A$  Integritätsbereich und  $K = \text{Quot}(A)$ .  $A$  heißt Bewertungsring, falls für alle  $x \in K^*$  gilt dass  $x \in A$  oder  $x^{-1} \in A$ . Sei  $\Gamma = K^*/A^*$ . Das ist abelsche Gruppe mit  $[a] + [b] = [a + b]$ . Definiere partielle Ordnung durch  $p \geq 0 \iff p = [a]$  für ein  $a \in A$ , also  $[b] \geq [a] \iff \frac{b}{a} \in A$ .

**Definition 9.1.2.** Sei  $K$  ein Körper und  $\Gamma$  eine total geordnete abelsche Gruppe. Eine Bewertung von  $K$  ist eine surjektive Abbildung  $\nu: K^* \rightarrow \Gamma$  sodass  $\nu(xy) = \nu(x) + \nu(y)$  und  $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$  ist für alle  $x, y \in K^*$ . Es gilt die Konvention  $\nu(0) = \infty$ .  $\nu$  heißt diskrete Bewertung falls  $\Gamma \cong \mathbb{Z}$  ist.

**Satz 9.1.3.** Sei  $A$  ein Integritätsbereich und  $K = \text{Quot}(A)$ . Dann ist äquivalent:

1.  $\forall x \in K^*: x \in A \text{ or } x^{-1} \in A$ .
2. Für zwei Ideale  $I, J \subseteq A$  gilt  $I \subseteq J$  oder  $J \subseteq I$ .
3. Das gleiche wie 2. nur für Hauptideale.
4. Es gibt eine total geordnete abelsche Gruppe  $\Gamma$  (Bewertungsgruppe genannt) und eine Bewertung  $\nu: K^* \rightarrow \Gamma$  sodass  $A = \{x \in K^* \mid \nu(x) \geq 0\} \cup \{0\}$ .
5.  $A$  ist ein lokaler Bézout Ring.

In diesem Fall heißt  $A$  diskreter Bewertungsring mit Bewertungsgruppe  $\Gamma$  und Bewertung  $\nu$ . Ist  $\nu$  zusätzlich eine diskrete Bewertung, so heißt  $A$  diskreter Bewertungsring.

*Beweis.* Zeige 1 nach 2: Sei  $x \in I$  mit  $x \notin J$  und sei  $y \in J$ . Sei ohne Einschränkung  $y \neq 0$ . Aus  $\frac{x}{y} \in A$  folgt  $x \in J$ , also ist  $\frac{y}{x} \in A$  und damit  $y \in I$ . Also ist  $J \subseteq I$ .

2. nach 3. ist klar. Gelte 3. Sei  $\Gamma = K^*/A^*$  mit  $[a] + [b] = [ab]$ . Das ist abelsche Gruppe. Definiere partielle Ordnung durch

$$[b] \geq [a] \iff \frac{b}{a} \in A$$

und sei  $\text{nu}: K^* \rightarrow \Gamma$  die Projektion. Seien  $x = \frac{a}{b}, y = \frac{c}{d} \in K^*$  mit  $a, b, c, d \in A \setminus \{0\}$ . Dann ist  $(ad) \subseteq (bc)$  oder  $(bc) \subseteq (ad)$ . das heißt  $\frac{x}{y} \in A$  oder  $\frac{y}{x} \in A$  also ist die Ordnung total. Wenn 3. gilt dann ist  $x \in K^*$  eine Einheit von  $A$  genau dann wenn  $\text{nu}(x) = 0$  ist da  $\nu(x^{-1}) = -\nu(x)$ . Also ist  $\mathfrak{m} = \{x \in A \mid \nu(x) > 0\}$  das maximale Ideal von  $A$ . Sei  $I \subseteq A$  ein endlich erzeugtes Ideal und seien  $x_1, \dots, x_n$  Erzeuger sodass  $\nu(x_1) < \dots < \nu(x_n)$ . Da  $\nu$  surjektiv ist, gibt es zu  $k > 1$  ein  $t \in K^*$  sodass  $\nu(t) = \nu(x_k) - \nu(x_1) > 0$ . Dann ist  $t \in A$  und  $\nu(tx_1) = \nu(x_k)$  woraus folgt dass  $x_k = tx_1$  ist für eine Einheit  $u \in A$ . Also ist  $I = (x_1)$  und somit  $A$  ein Bézout Ring. Gelte 4 und sei  $x = \frac{a}{b} \in K^*$  mit  $a, b \in A^*$ . Es ist  $a, b) = (c)$  nach 4 und somit  $c = ua + vb$  und  $a = wc$  und  $b = zc$ . Dann ist  $c(1 - uw - vz) = 0$ . Da  $A$  lokal ist, ist  $1 - uw - vz$  im maximalen Ideal denn sonst wäre es Einheit und damit  $c = 0$ . Also ist  $w$  oder  $z$  eine Einheit und  $a, b) = (a)$  oder  $a, b) = (b)$  und somit  $x \in A$  oder  $x^{-1} \in A$ .  $\square$

**Bemerkung 9.1.4.** Ein Bewertungsring  $A$  ist lokal mit maximalem Ideal  $\mathfrak{m} = \{x \in K \mid \nu(x) > 0\}$ .

**Lemma 9.1.5.** *Sei  $A$  ein noetherscher Integritätsbereich und  $t \in A$  keine Einheit. Dann ist*

$$\bigcap_{n=1}^{\infty} (t^n) = 0.$$

*Beweis.* Angenommen  $0 \neq x \in \bigcap_{n=1}^{\infty} (t^n) = 0$ . Dann ist  $x = tx_1 = t^2x_2 = \dots = t^nx_n = \dots$  und somit  $(x) \subsetneq (x_1) \subsetneq \dots$ . Da  $A$  noethersch ist, muss die Kette stoppen.  $\square$

**Satz 9.1.6.** *Sei  $A$  ein Integritätsbereich. Es ist äquivalent:*

1.  $A$  ist ein diskreter Bewertungsbereich.
2.  $A$  ist lokal mit maximalem Ideal  $\mathfrak{m} = (t)$  für  $t \neq 0$  und  $\bigcap_{n=1}^{\infty} (t^n) = 0$

*In dem Fall hat jedes Element  $0 \neq x \in A$  die Darstellung  $x = t^n u$  mit  $n \geq 0$  und  $u$  eine Einheit in  $A$  und jedes Ideal  $I \neq 0$  ist von der Form  $I = (t^n)$ . Insbesondere ist  $A$  noethersch.*

*Beweis.* Gelte 1. Es gibt  $t \in A$  mit  $\nu(t) = 1$ . Wenn also  $x \in \mathfrak{m}$  dann ist  $\nu(x) \geq \nu(t^n) \geq 1$  und also  $x = t^n u$  für eine Einheit  $u$ . Somit ist  $\mathfrak{m} = (t)$ . Wenn  $x = t^n u$  ist für eine Einheit  $u$  dann ist  $\nu(x) = n$  also ist  $\bigcap_{n=1}^{\infty} (t^n) = 0$ . Gelte 2. Dann gibt es für jedes  $x \in A$  ein  $n$  sodass  $x \in (t^n) \setminus (t^{n+1})$ . Also hat  $x$  Darstellung  $x = t^n \cdot u$ . Definiere  $\nu(x) = n$  und  $\nu(\frac{x}{y}) = \nu(x) - \nu(y)$ . Das ist eine diskrete Bewertung sodass  $A$  diskreter Bewertungsring ist. Sei  $I$  ein Ideal und  $n = \min\{k \mid t^k \in I\}$ . Dann ist  $I = (t^n)$ .  $\square$

**Satz 9.1.7.** *Sei  $A$  ein Bewertungsring. Dann ist äquivalent:*

1.  $A$  ist noethersch
2.  $A$  ist Hauptidealring.

*Wenn zusätzlich  $A$  kein Körper ist, ist auch äquivalent:*

- (3)  $A$  ist diskreter Bewertungsring.

*Beweis.* Da Jedes Ideal in einem noetherschen Ring endlich erzeugt ist, ist jedes Ideal ein Hauptideal. Ein Hauptidealring ist auch noethersch. Zeige also das 3. aus den Bedingungen folgt. Wenn  $A$  noethersch ist, dann folgt mit Lemma 9.1.5 dass  $\bigcap_{n=1}^{\infty} (t^n) = 0$  für  $(t) = \mathfrak{m}$ . Der Rest ist Satz Satz 9.1.6.  $\square$

**Satz 9.1.8.** *Sei  $A$  Integritätsbereich.  $A$  ist diskreter Bewertungsring genau dann, wenn  $A$  noethersch, normal und  $\text{Spec}(A) = \{0, \mathfrak{m}\}$  ist wobei  $\mathfrak{m} \neq 0$ .*

*Beweis.* Nach Satz 9.1.6 sind diskrete Bewertungsringe noethersch und faktoriell, also normal (Bemerkung 7.2.2) und  $\text{Spec}(0, \mathfrak{m})$  klar. Sei also  $A$  gegeben wie im Satz. Wir zeigen dass  $\mathfrak{m}$  ein Hauptideal ist. Der Rest folgt dann aus Lemma 9.1.5 und Satz 9.1.6. Sei  $I \subseteq A$  ein Ideal. Das ist endlich erzeugter  $A$ -Modul. Nach Nakayama gilt  $\mathfrak{m}I = I \implies I = 0$ . Also ist  $\mathfrak{m}^2 \neq \mathfrak{m}$ . Sei also  $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ . Sei  $M = \mathfrak{m}/(x)$ . Wenn  $M \neq 0$  dann ist  $\text{Ass}(M) \neq 0$  nach Satz 10.6.8. Das heißt es gibt esin  $0 \neq y \in \mathfrak{m} \setminus (x)$  sodass  $my \subseteq (x)$ . Dann ist  $xy \in A$  also  $\frac{y}{x} \notin A$  aber  $\frac{y}{x}\mathfrak{m} \subseteq A$  ein Ideal. Angenommen  $\frac{y}{x}\mathfrak{m} = A$ . Dann ist  $\frac{yy'}{x} = 1$  für ein  $y' \in \mathfrak{m}$  also wäre  $x \in \mathfrak{m}^2$  was ein Widerspruch ist. Also ist  $\frac{y}{x}\mathfrak{m} \subsetneq \mathfrak{m}$ . Multiplikation mit  $xy$  ist Lineare Abbildung  $\varphi: \mathfrak{m} \rightarrow \mathfrak{m}$  zwischen endlichen  $A$ -Moduln. Wähle also Surjektion  $\pi: R^n \rightarrow M, e_i \mapsto x_i$  und sei  $B = (b_{ij})$  die Matrix mit  $\varphi(x_i) = \sum b_{ij}x_j$ . Nach Cayley Hamilton ??? gibt es Polynom  $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$  mit  $P(B) = 0$  also ist  $P(\varphi) = 0$ . Für  $0 \neq z \in \mathfrak{m}$  ist also

$$\left(\left(\frac{x}{y}\right)^n + \dots + a_0\right)z = 0$$

Also ist  $\frac{x}{y}$  integral. Da  $A$  normal ist, ist  $\frac{x}{y} \in A$  was Ein Widerspruch ist. Also ist  $\mathfrak{m} = (x)$ .  $\square$

**Lemma 9.1.9.** *Lokalisierungen von Bewertungsringen sind wieder Bewertungsringe. Quotienten mit Primidealen von Bewertungsringen sind wieder Bewertungsringe.*

*Beweis.* Klar wegen Beschreibung durch Ordnung der Ideale.  $\square$

**Lemma 9.1.10.** Sei  $R$  ein Bewertungsring mit maximalem Ideal  $\mathfrak{m}$  und sei  $A \subseteq R/\mathfrak{m}$  ein Bewertungsring mit Quotientenkörper  $R/\mathfrak{m}$ . Sei  $R \rightarrow R/\mathfrak{m}$  die Projektion. Dann ist  $\pi^{-1}(A)$  Bewertungsring.

*Beweis.* Wenn  $R$  Körper ist, ist alles klar. Sei  $R$  kein Körper. Wähle  $t \in \mathfrak{m}$  ungleich 0. Dann ist für alle  $a \in R$

$$a = \frac{ta}{t}$$

und  $ta \in R' = \pi^{-1}(A)$ . Also ist  $\text{Quot}(R) = \text{Quot}(R')$ . Sei  $x \in \text{Quot}(R')$  nicht 0. Es ist  $x \in R$  oder  $x^{-1} \in R$ . Wenn einer der beiden in  $\mathfrak{m}$  dann ist einer der beiden in  $R'$ . Sei also  $x$  in  $R$  aber nicht in  $\mathfrak{m}$ . Dann  $\pi(x) \in A$  oder  $\pi(x)^{-1} \in A$ . Also  $x \in R'$  oder  $x^{-1} \in R'$ .  $\square$

**Beispiel 9.1.11.** Sei  $R$  ein Ring und  $R[[X]]$  der Ring der formalen Potenzreihen. Ein Element  $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$  ist eine Einheit, genau dann wenn  $a_0$  eine Einheit ist. Wenn  $R = K$  ein Körper ist, dann ist  $K[[x]]$  ein Bewertungsring.

*Beweis.* Wenn  $f$  Einheit, dann gibt es  $g = b_0 + b_1 X + \dots$  sodass  $1 = gf = a_0 b_0$  also ist  $a_0$  eine Einheit. Wenn  $a_0$  Einheit ist, dann ist  $a_0^{-1} f = 1 + \dots$  also ohne Einschränkung  $a_0 = 1$ . Setze  $b_0 = 1$  und rekursiv  $b_n = -\sum_{i=1}^n a_i b_{n-i}$ . Dann ist

$$f \cdot \sum_{i=0}^{\infty} b_i X^i = 1$$

. Definiere  $\nu(f) = \min\{n \in \mathbb{N} \mid a_n \neq 0\}$  für  $f \neq 0$ . und für  $\frac{f}{g} \in \text{Quot}(K[[X]])$  setze  $\nu(\frac{f}{g}) = \nu(f) - \nu(g)$ . dann ist  $\nu$  eine diskrete Bewertung und  $K[[X]] = \{y \mid \nu(y) \geq 0\}$ .  $\square$

**Beispiel 9.1.12.** Das letzte Lemma ist erfüllt für  $R = \mathbb{Q}[[x]]$  und  $\mathfrak{m} = (x)$  und  $A = \mathbb{Z}_p$ . In dem Fall ist  $\pi^{-1}A = \{\sum_{i=0}^{\infty} a_i X^i \mid a_0 \in \mathbb{Z}_p\}$ .

## 9.2 Dedekindringe

**Definition 9.2.1.** Ein Dedekindring ist ein normaler, noetherscher Integritätsring der Dimension  $\leq 1$ .

**Beispiel 9.2.2.** Jeder Hauptidealring ist Dedekindring.

**Satz 9.2.3.** Sei  $R$  ein Ring- es ist äquivalent:

1.  $R$  ist Dedekindring
2. Jedes Ideal  $(0) \neq I \subseteq R$  kann geschrieben werden als Produkt  $I = \mathfrak{p}_1 \dots \mathfrak{p}_r$  von bis auf Reihenfolge eindeutigen Primidealen  $\mathfrak{p}_i \neq 0$ .
3.  $R$  ist noethersch und für jedes maximale Ideal  $\mathfrak{m} \neq 0$  ist  $R_{\mathfrak{m}}$  ein diskreter Bewertungsring.

**Lemma 9.2.4.** Sei  $R$  ein Ring und  $I, J$  Ideale ungleich 0 sodass  $IJ = (f)$  für ein Nichtnullteiler  $f \in A$ . Dann sind  $I$  und  $J$  endlich erzeugt und endlich lokal frei vom Rang 1 als  $A$ -Modul.

*Beweis.* Endlich lokal frei impliziert endlich erzeugt nach ??? . Sei also  $f = \sum_{i=1}^n x_i y_i$  mit  $x_i \in I$  und  $y_i \in J$  und  $x_i y_i = a_i f$  für ein  $a_i \in A$ . Da  $f$  Nichtnulleiler ist  $\sum a_i = 1$ . Es reicht also, dass  $I_{a_i}, J_{a_i}$  frei von Rang 1 über  $A_{a_i}$ . Ersetze also  $A$  durch  $A_{a_i}$ . Dann ist  $f = xy$  für  $x \in I$  und  $y \in J$ . Wenn  $x' \in I$  dann ist  $x'y = af = axy$  für  $a \in A$ . Da  $y$  Nichtnullteiler ist  $x' = ax$  und  $I = (x)$ . Analog ist  $J = (y)$ .  $\square$

**Lemma 9.2.5.** Sei  $R$  ein Ring.

1. Jedes Ideal  $I \subseteq R$  mit der Eigenschaft maximal unter nicht-endlich erzeugten Idealen ist ein Primideal.
2. Wenn jedes Primideal von  $R$  endlich erzeugt ist, dann ist jedes Ideal endlich erzeugt.

*Beweis.* Sei  $I$  maximal mit der Eigenschaft. Angenommen  $ab \in I$  aber  $a \notin I$  und  $b \notin I$ . Dann ist  $(I, a) \neq I$  und  $b \in (I : a)$  sodass  $I \neq (I : a)$ . Also enthalten  $I, a$  und  $I : a$  beide echt  $I$  und sind damit endlich erzeugt. Wenn aber  $I : a$  erzeugt ist von  $a_i$  und  $(I, a)$  erzeugt ist von  $a$  und  $b_i$  dann ist  $I$  erzeugt von  $aa_i$  und  $b_i$ . Also ist  $I$  prim. Angenommen es gibt ein Ideal  $I$  das nicht endlich erzeugt ist. Die Vereinigung einer total geordneten Familie nicht-endlich erzeugter Ideale ist nicht endlich erzeugt. Also gibt es nach Lemma von Zorn?? ein Ideal maximal mit der Eigenschaft nicht endlich erzeugt zu sein. Nach Teil 1 ist das dann prim, was ein Widerspruch ist.  $\square$

*Beweis.* Die Äquivalenz von 1 und 3 ist Satz 7.2.5 zusammen mit Satz 9.1.8. Gelte also 2. Wegen Eindeutigkeit der Primzerlegung ist  $\mathfrak{p} \neq \mathfrak{p}^2$  für jedes Primideal  $\mathfrak{p} \subseteq R$ . Sei  $x \in \mathfrak{p} \setminus \mathfrak{p}^2$  und  $y \in \mathfrak{p}$ . Dann ist  $(x, y) = \mathfrak{p}_1 \dots \mathfrak{p}_r$  und da  $(x, y) \subseteq \mathfrak{p}$  muss  $\mathfrak{p}_i \subseteq \mathfrak{p}$  für ein  $i$ . Da aber  $x \notin \mathfrak{p}^2$  kann das höchstens für ein  $i$  geschehen. OE ist also  $\mathfrak{p}_1 \subseteq \mathfrak{p}$ . Also ist  $(x, y)R_{\mathfrak{p}} = \mathfrak{p}_1 R_{\mathfrak{p}}$  prim für jede Wahl von  $y$ , also auch für  $y^2$ . Also ist  $x, y^2 R_{\mathfrak{p}}$  prim und somit  $y \in (x, y^2)R_{\mathfrak{p}}$ . Dann gibt es Darstellung  $y = ax + by^2$  in  $R_{\mathfrak{p}}$  und somit ist

$$(1 - by)y = ax \in (x)R_{\mathfrak{p}}$$

Also ist  $y \in (x)R_{\mathfrak{p}}$  und  $(x)R_{\mathfrak{p}} = \mathfrak{p}_1 R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ . Nach Lemma ?? ist jedes primideal also endlich erzeugt und damit ist  $R$  noethersch. Also ist jede lokalisierung ein diskreter Bewertungsring. Gelten jetzt 1 und 3. Definiere für ein Ideal  $I \neq 0$

$$\nu_{\mathfrak{m}}(I) = \min\{\nu_{\mathfrak{m}}(I) \mid a \in I\}$$

wobei  $\nu_{\mathfrak{m}}$  diskrete Bewertung von  $A_{\mathfrak{m}}$  ist. Es gilt  $I \subseteq J \iff \nu_{\mathfrak{m}}(I) \geq \nu_{\mathfrak{m}}(J)$ . Denn wenn  $a \in I$  dann gibt es  $b_{\mathfrak{m}} \in J$  sodass  $\nu_{\mathfrak{m}}(a) \geq \nu_{\mathfrak{m}}(b)$ . Also ist  $a \in J_{\mathfrak{m}}$  für alle  $\mathfrak{m}$  also  $a \in J$  nach ????. Eine Rechnung zeigt, dass  $\nu(IJ) = \nu(I) + \nu(J)$ . Es ist  $\nu_{\mathfrak{m}}(I) > 0 \iff \mathfrak{m} \supseteq I$  und da  $\mathfrak{m}/I$  minimales Primideal in  $A/a$  und da Ring noethersch ist folgt, dass das nur für endlich viele maximale Ideale  $\mathfrak{m}$  passieren kann. Es ist

$$\nu_{\mathfrak{m}}\left(\prod_{\mathfrak{n}} \mathfrak{n}^{\nu_{\mathfrak{n}}(I)}\right) = \sum \nu_{\mathfrak{m}}(\text{frakn}^{\nu_{\mathfrak{n}}(I)}) = \sum_{\mathfrak{n}} \nu_{\mathfrak{n}}(I) \nu_{\mathfrak{m}}(\mathfrak{n}) = \nu_{\mathfrak{n}}(I)$$

Also  $I = \prod_{\mathfrak{n}} \mathfrak{n}^{\nu_{\mathfrak{n}}(I)}$ .  $\square$

**Lemma 9.2.6.** Sei  $A$  Dedekindring. Zu jedem Ideal  $I$  gib es ein Ideal  $J$  sodass  $IJ$  ein Hauptideal ist.

*Beweis.* OE  $I \neq 0$  und  $(0) \neq (x) \subseteq I$ . Sei  $I = \prod \mathfrak{m}_i^{e_i}$  und  $(x) = \prod \mathfrak{m}_i^{f_i}$ . Dann ist  $r_i - n_i \geq 0$  nach obigem. Definiere also  $J = \prod \mathfrak{m}_i^{f_i - e_i}$ . Dann ist  $IJ = (x)$ .  $\square$

**Lemma 9.2.7.** Sei  $R$  noetherscher Integritätsbereich der Dimension 1 mit Quotientenkörper  $K$  und sei  $L/K$  eine endliche Erweiterung. Dann ist jeder Ring  $R \subseteq A \subseteq L$  noethersch.

*Beweis.* Sei  $I \subseteq A$  ein Ideal ungleich  $(0)$  und  $x \in I \setminus \{0\}$ . Wähle  $r_n x^n + \dots + r_0 = 0$  mit  $r_i \in R$ . und  $r_0, r_n \neq 0$ . Dann ist  $r_0 \in R \cap I$ . Also ist  $I/r_0 A \subseteq A/r_0 A$ .  $\square$

**Satz 9.2.8** (Krull-Akizuki). Sei  $A$  noetherscher Integritätsbereich der Dimension 1 mit Quotientenkörper  $K$  und sei  $L/K$  eine endliche Erweiterung. Sei  $B$  der ganze Abschluss of von  $A$  in  $L$ . Dann ist  $B$  ein Dedekindring.

*Beweis.*  $\square$

## 9.3 Idealklassengruppe

**Definition 9.3.1.** Ein gebrochenes Ideal von einem Dedekindring  $R$  ist ein endlich erzeugter  $R$ -Untermodul von  $K = \text{Quot}(R)$ . Für zwei gebrochene Ideale  $I, J$  ist  $IJ$  der  $R$ -Modul der erzeugt ist von allen  $xy$ .

**Satz 9.3.2.** Die Menge der gebrochenen Ideale ungleich Null ist mit diesem Produkt eine abelsche Gruppe  $J_R$ .

*Beweis.* Sei  $I$  gebrochenes Ideal erzeugt durch  $\frac{1}{x_1}, \dots, \frac{1}{x_n}$ . Sei  $x = \prod x_i$  das heißt  $xI \subseteq R$  Ideal. Sei  $xI = \mathfrak{p}_1 \dots \mathfrak{p}_r$  Primzerlegung. Sei  $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ . Dann ist  $\mathfrak{p}\mathfrak{a} = (x)$  und  $\mathfrak{p}(\frac{1}{x})\mathfrak{a} = (1)$  Also ist  $\mathfrak{p}_i$  invertierbar für alle  $i$ . Dann ist

$$x\mathfrak{p}_i^{-1} \dots \mathfrak{p}_r^{-1}I = (1)$$

und somit  $I$  invertierbar.  $\square$

**Definition 9.3.3.** sei  $a \in K^*$ . Dann ist  $aR$  gebrochenes Ideal. Gebrochene Ideale von der Form nennt man gebrochene Hauptideale. Wir haben exakte Sequenz

$$0 \longrightarrow R^* \longrightarrow K^* \xrightarrow{a \mapsto aR} J_R \longrightarrow Cl(R) \longrightarrow 0$$

und der Quotient  $Cl(R)$  heißt Idealklassengruppe.

**Beispiel 9.3.4.** sei  $R = \mathbb{Z}[\sqrt{-5}]$ . Es ist  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$  Also ist  $R$  nicht faktoriell. Da  $-5 \equiv 3 \pmod{4}$  ist, ist  $R = \mathbb{O}_K$  Ring der ganzen Zahlen in  $K = \mathbb{Q}[\sqrt{-5}]$ . Also ein Dedekindring, der kein Hauptidealring ist. Es gibt unter anderen die maximalen Ideale  $\mathfrak{p}_1 = (2, 1 + \sqrt{-5})$ ,  $\mathfrak{p}_2 = (3, 1 + \sqrt{-5})$  und  $\mathfrak{p}_3 = (3, 1 - \sqrt{-5})$ . Das Minimalpolynom von  $1 + \sqrt{-5}$  ist nämlich  $\mu = (X - 1)^2 + 5 = X^2 - 2X + 6$  was irreduzibel ist nach Eisenstein. ??? also ist  $R = \mathbb{Z}[X]/(\mu)$  wobei  $X \leftrightarrow 1 + \sqrt{-5}$  und  $R/\mathfrak{p}_1 \cong \mathbb{F}_2$  Körper. Genauso ist  $R/\mathfrak{p}_i = \mathbb{F}_3$  Körper für  $i = 2, 3$ . Es gilt  $(2) = \mathfrak{p}_1^2$  und  $(1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2$  und  $(3) = \mathfrak{p}_2\mathfrak{p}_3$  und  $(1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$ . Also ist  $(6) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$  die Eindeutige Zerlegung.

**Lemma 9.3.5.** Sei  $R$  ein Dedekindring. Es ist äquivalent

1.  $R$  ist ein Hauptidealring
2. Jedes Primideal ist ein Hauptideal
3.  $Cl(R)$  hat nur ein Element.
4.  $R$  ist faktoriell

*Beweis.* 1 nach 2 ist klar. Gelte 1. Sei  $I$  gebrochenes Ideal. Es gibt  $d \in R$  sodass  $dR \subseteq I$  ein Ideal ist. Dann ist  $dI = (x)$  und  $I = \frac{x}{d}R$  gebrochenes Hauptideal. Rest ist einfach.  $\square$

**Satz 9.3.6.** Sei  $R$  ein Dedekindring und  $M$  ein endlich erzeugter  $R$ -Modul der Torsionsmodul ist. Dann ist  $\text{Supp}(M)$  endlich und  $M \cong \bigoplus_{i \in I} R/\mathfrak{m}_i^{n_i}$  wobei  $I$  endlich und  $\mathfrak{m}_i$  maximal.

*Beweis.* Da  $R$  noethersch ist ist der Support endlich nach ?? Betrachte  $\varphi: M \rightarrow \bigoplus_{\mathfrak{p} \in \text{Supp}(M)} M_{\mathfrak{p}}$ . Für  $\mathfrak{q} \in \text{Spec}(R)$  ist

$$M_{\mathfrak{p}} \otimes R_{\mathfrak{q}} = M \otimes (R_{\mathfrak{p}})_{\mathfrak{q}} = \begin{cases} 0 & \mathfrak{p} \neq \mathfrak{q} \\ M_{\mathfrak{p}} & \mathfrak{p} = \mathfrak{q} \end{cases}$$

wobei oberes gilt da  $M$  ein Torsionsmodul ist und  $\mathfrak{p} \cap \mathfrak{q} = (0)$ . Somit ist  $\varphi$  ein Isomorphismus. Da  $R_{\mathfrak{p}}$  Hauptidealring ist folgt mit Struktursatz, dass jeder Torsionsmodul von der Form  $\bigoplus_{n \in J} R_{\mathfrak{p}}/(\mathfrak{p}R_{\mathfrak{p}})^n R_{\mathfrak{p}} = \bigoplus (R/\mathfrak{p}^n)_{\mathfrak{p}}$  ist. Da  $R/\mathfrak{p}^n$  lokal ist, ist  $R/\mathfrak{p}^n \cong R/\mathfrak{p}^n$ . Also gilt die Aussage.  $\square$

# Kapitel 10

## Moduln

### 10.1 Ext und Tor

**Definition 10.1.1.** Ein  $R$ -Modul  $P$  heißt projektiv, falls für jeden Epimorphismus  $\varphi: M \rightarrow M'$  die Abbildung  $\text{Hom}_R(P, M) \rightarrow \text{Hom}_R(P, M')$  surjektiv ist.

**Satz 10.1.2.** Ein  $R$ -Modul  $P$  ist projektiv genau dann wenn  $P$  ein direkter Summand eines freien Modules ist. Insbesondere sind freie Moduln projektiv.

*Beweis.* Klar: freie Moduln sind projektiv. Wenn  $P$  ein Modul ist sodass  $P \oplus P'$  frei ist, dann ist  $P \oplus P'$  projektiv. Sei  $g: P \rightarrow M'$  und Epimorphismus  $\varphi: M \rightarrow M'$  gegeben. Die Projektion  $P \oplus P' \rightarrow P$  gibt

$$\begin{array}{ccc}
 & P & \\
 & \downarrow \iota_P & \\
 & P \oplus P' & \\
 & \downarrow pr_P & \swarrow \text{id} \\
 & P & \\
 & \downarrow g & \\
 M & \xrightarrow{\varphi} & M'
 \end{array}$$

$\exists f'$  (dotted arrow from  $P$  to  $M$ )  
 $\exists f$  (dashed arrow from  $P \oplus P'$  to  $M$ )

Also ist  $P$  projektiv. Andersrum sei  $P$  projektiv und  $F$  frei sodass  $\varphi: F \rightarrow P$  surjektiv ist. Das gibt split exakte Sequenz

$$0 \longrightarrow \ker(\varphi) \longrightarrow F \xrightarrow{\varphi} P \longrightarrow 0$$

sodass  $F = \ker(\varphi) \oplus P$

□

**Satz 10.1.3.** Jeder  $R$ -Modul hat eine freie und somit projektive homologische Auflösung.

*Beweis.* Wähle Erzeugendensystem  $(x_i)_{i \in I}$  und setze  $M_0 = R^{(I)}$ . Dann ist  $M_0 \rightarrow P$  surjektiv. Setze Konstruktion fort mit  $\ker(M_0 \rightarrow P)$ . □

**Lemma 10.1.4.** Projektive Moduln sind flach.

*Beweis.* Freie Moduln sind flach und da sich Flachheit auf direkte Summanden überträgt gilt die Aussage. □

**Satz 10.1.5.** Sei  $R$  lokal. Dann ist jeder endliche projektive Modul frei.

*Beweis.* Sei  $\mathfrak{m}$  das maximale Ideal von  $R$ . Dann ist  $R/\mathfrak{m}$  ein Körper also  $P \otimes R/\mathfrak{m} = P/\mathfrak{m}P$  frei. Wähle  $x_1, \dots, x_n$  in  $P$  die auf eine Basis Abbilden in  $P/\mathfrak{m}P$ . Sei  $f: R^n \rightarrow P, e_i \mapsto x_i$ . Nach Lemma 10.1.18 ist  $f$  surjektiv. Es ist weil  $P$  projektiv ist  $R^n \cong \ker(f) \oplus P$  und somit  $\ker(f)$  endlich erzeugt. Da  $f$  ein Isomorphismus ist über  $R/\mathfrak{m}R$  ist  $\ker(f) \otimes R/\mathfrak{m}R = 0$ . Also ist  $\ker(f) = 0$  nach Lemma 10.1.18. Somit ist  $f$  ein Isomorphismus. □

**Definition 10.1.6.** Der  $n$ -te Ableitungsfunktor von  $- \otimes_R E$  wird mit  $Tor_n^R(-, E)$  bezeichnet. Das heißt  $Tor_n^R(M, E) = H_n(M_* \otimes_R E)$  für eine projektive Auflösung  $M_* \rightarrow M$ .

**Beispiel 10.1.7.** Seien  $n, m \geq 1$ . Haben freie Auflösung

$$\dots \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

Mit  $\mathbb{Z}/m\mathbb{Z}$  tensorieren gibt

$$\dots \longrightarrow 0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

also ist für  $d = \text{ggT}(n, m)$ :

$$Tor_0^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/d\mathbb{Z}$$

$$Tor_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \frac{m}{d} = \mathbb{Z}/d\mathbb{Z}$$

$$Tor_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = 0 \quad i \geq 2$$

**Beispiel 10.1.8.** Sei  $R = K[X, Y]$  für einen Körper  $K$  und  $M = R/(X, Y) = K$  als  $R$ -Modul. Sei  $f: R^2 R, f(\varphi, \psi) = X\varphi + Y\psi$  und  $g: R \rightarrow R^2, g(\varphi) = (Y\varphi, -X\varphi)$ . Dann ist

$$0 \longrightarrow R \xrightarrow{g} R \xrightarrow{f} R \xrightarrow{\pi} K \longrightarrow 0$$

eine Auflösung. Somit ist

$$Tor_i^R(R, M) = \begin{cases} K & i = 0 \\ K^2 & i = 1 \\ K & i = 2 \\ 0 & i \geq 3 \end{cases}$$

**Satz 10.1.9.** *Tor kann als Ableitung von  $- \otimes_R E$  oder als Ableitung von  $M \otimes_R -$  aufgefasst werden.*

*Beweis.* Seien  $M_* \rightarrow M$  und  $E_* \rightarrow E$  homologische Auflösungen von zwei  $R$ -Moduln  $M, E$ . Sei  $C^{i,j} = M_i \otimes E_j$  und  $A^i = M_i \otimes_R E$  und  $B^j = M \otimes_R E_j$ . Das gibt Abbildung von Komplexen  $Tot(C^{**}) \rightarrow B^*$  und  $Tot(C^{**}) \rightarrow A^*$ . Wenn beide Abbildungen quasi Isomorphismen sind, dann ist  $H^i(B^*) = H^i(A^*)$  was die Aussage ist. In Zeile  $j$  ist  $C^{**} \rightarrow B^*$  aber nichts anderes als

$$\dots \longrightarrow M_1 \otimes E_j \longrightarrow M_0 \otimes E_j \longrightarrow M \otimes E_j \longrightarrow 0$$

was exakt ist da  $E_j$  projektiv und somit flach ist. Nach ??? ist also  $Tot(C^{**} \rightarrow B^*)$  quasi isomorphismus. Analog geht das für  $A^*$  statt  $B^*$ . □

**Satz 10.1.10.** *Für einen  $R$ -Modul  $M$  ist äquivalent:*

1.  $M$  ist flach
2.  $Tor_n^R(M, N) = 0$  für alle  $n \geq 1$  und alle  $R$ -Moduln  $N$ .
3.  $Tor_1^R(M, N) = 0$  für alle endlichen  $R$ -Moduln.
4.  $Tor_1^R(M, R/\alpha) = 0$  für alle endlich erzeugten Ideale  $\alpha \subseteq R$ .

*Beweis.* (1)  $\iff$  (2) ist klar und (2)  $\implies$  (3)  $\implies$  (4) auch. Gelte (4) und zeige (3). Sei  $s$  die Anzahl von Erzeugern von  $N$ . Wenn  $s = 1$  dann ist  $N = R \cdot x$  und somit  $N \cong R/\alpha$  für  $\alpha = \ker(\cdot x)$ . Wenn  $\alpha$  endlich erzeugt ist, ist  $Tor_1 = 0$ . Die lange exakte Tor Sequenz liefert

$$\dots \longrightarrow 0 = Tor_1^R(M, R) \longrightarrow Tor_1^R(M, R/\alpha) \longrightarrow M \otimes_R \alpha \longrightarrow M \otimes_R R = M \longrightarrow \dots$$

wobei links 0 steht da  $R$  frei ist. Also ist  $Tor_1^R(M, R/\alpha) \cong \ker(M \otimes_R \alpha \rightarrow M)$ . Für jedes endlich erzeugte Ideal  $\alpha' \subseteq \alpha$  ist

$$M \otimes_R \alpha' \rightarrow M \otimes_R \alpha \rightarrow M$$

injektiv da  $Tor_1^R(M, R/\alpha') = 0$ . Wenn  $z = \sum_{i=1}^n m_i \otimes a_i \in \ker(M \otimes_R \alpha' \rightarrow M)$  sei  $\alpha' = (a_1, \dots, a_r)$ . dann ist  $z \in \ker(M \otimes_R \alpha' \rightarrow M) = 0$ . Also ist  $M \otimes_R \alpha \rightarrow M$  injektiv und somit  $Tor_1^R(M, N) = 0$ . Wenn  $s \geq 1$  dann ist  $N = \sum_{i=1}^s Rx_i$  und sei  $N' = \sum_{i=1}^{s-1} Rx_i$ . Dann ist  $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$  exakt und  $N''$  erzeugt durch ein Element. Nach Induktion ist  $Tor_1^R(M, N') = 0$  und  $Tor_1^R(M, N'') = 0$ . Dann auch  $Tor_1^R(M, N) = 0$  nach langer exakter Tor Sequenz. Gelte (3) und sei  $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$  exakt. Wenn  $N$  endlich erzeugt ist, dann auch  $N''$  und somit ist  $0 \rightarrow M \otimes N' \rightarrow M \otimes N \rightarrow M \otimes N'' \rightarrow 0$  exakt. Wenn  $N$  nicht endlich, sei  $z = \sum_{i=1}^r m_i \otimes n_i \in \ker(M \otimes N' \rightarrow M \otimes N \rightarrow N)$ . Ersetze  $N'$  durch Modul erzeugt durch die  $n_i$ . Dann ist

$$z \in \ker(M \otimes N' \rightarrow M \otimes \mathfrak{G}(N')) = 0$$

somit ist  $M$  flach.  $\square$

**Korollar 10.1.11.** *Ein  $R$ -Modul  $M$  ist flach genau dann wenn für jedes endlich erzeugte Ideal  $\alpha \subseteq R$  die Abbildung  $\alpha \otimes M \rightarrow M$  injektiv ist.*

*Beweis.* Wenn  $M$  flach ist gilt die Behauptung da  $\alpha \rightarrow R$  injektiv ist. Andererseits gibt die exakte Sequenz  $0 \rightarrow \alpha \rightarrow R \rightarrow R/\alpha \rightarrow 0$  die exakte Sequenz

$$0 = Tor_1^R(M, R) \rightarrow Tor_1^R(M, R/\alpha) \rightarrow \alpha \otimes_R M \rightarrow M \rightarrow M/\alpha M \rightarrow 0$$

Da  $\alpha \otimes M \rightarrow M$  injektiv ist ist  $Tor_1^R(M, R/\alpha) = 0$  also  $M$  flach.  $\square$

**Satz 10.1.12.** *Sei  $M''$  ein  $R$ -Modul. Dann ist äquivalent:*

1.  $M''$  flach
2. Für alle exakte Sequenzen

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

und für alle  $R$ -Moduln  $N$  ist

$$0 \rightarrow M' \otimes N \rightarrow M \otimes N \rightarrow M'' \otimes N \rightarrow 0$$

exakt.

*Beweis.* (1) nach (2) ist klar. Sei  $M$  frei und  $N$  beliebig. Dann ist

$$0 \rightarrow M' \otimes N \rightarrow M \otimes N \rightarrow M'' \otimes N \rightarrow 0$$

exakt. Also ist  $Tor_1^R(M, N) = 0$  also  $Tor_1^R(M'', N) = 0$  also  $M''$  flach.  $\square$

**Satz 10.1.13.** *Sei*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*exakt und  $M''$  flach. Dann ist  $M'$  flach genau dann wenn  $M$  flach ist.*

*Beweis.* Klar, Lange exakte Tor Sequenz.  $\square$

**Definition 10.1.14.** Seien  $M, N$   $R$ -Moduln und  $M_* \rightarrow M$  projektive Auflösung. Sei  $Ext_R^n(M, N)$  die  $n$ -te homologische Ableitung von  $Hom_R(-, N)$ . Sei  $N \rightarrow N^*$  injektive Auflösung. Sei  $Ext_R^{n'}(M, N)$  die cohomologische Ableitung von  $Hom_R(M, -)$ .

**Satz 10.1.15.**  $Ext_R^{n'}(M, N) \cong Ext_R^n(M, N)$

*Beweis.* Wie in ?? sei  $C^{**} = Hom_R(M_*, M^*)$  und  $A^* = Hom(M_*, N)$  und  $B^* = Hom(M, N^*)$ . Das gibt Abbildungen  $B^* \rightarrow Tot(C^{**})$  und  $A^* \rightarrow Tot(C^{**})$ . Das sind quasi-Isomorphismen, denn zum Beispiel in Zeile  $j$  ist  $B^* \rightarrow C^{**}$  einfach nur

$$\cdots \rightarrow Hom(M_1, N^j) \rightarrow Hom(M_0, N^j) \rightarrow Hom(M, N^j)$$

was exakt ist da  $N^j$  injektiv ist.  $\square$



**Satz 10.1.16.** Für ein  $R$ -Modul  $P$  ist äquivalent:

1.  $P$  projektiv.
2.  ${}^n_R(P, N) = 0$  für alle  $n > 0$  und alle Moduln  $N$ .
3.  $\text{Ext}^1_R(P, N) = 0$  für alle  $n$ .

*Beweis.* wie bei Tor □

**Satz 10.1.17.** Für einen  $R$  Modul  $I$  ist äquivalent

1.  $I$  ist injektiv
2.  $\text{Ext}^n_R(M, I) = 0$  für alle  $n$  und alle Moduln  $M$
3.  $\text{Ext}^1_R(M, I) = 0$  für alle  $n$  und alle Moduln  $M$

*Beweis.* Genau wie vorher. □

### 10.1.1 Nakayama

**Lemma 10.1.18** (Nakayama). Sei  $I \subseteq R$  ein Ideal mit  $I \subseteq j(R)$ . Sei  $M$  ein endlich erzeugter  $R$ -Modul. Es gilt:

1. Wenn  $IM = M$  ist dann ist  $M = 0$ .
2. Wenn  $N, N' \subseteq M$  und  $M = N + IN'$  wobei  $N'$  endlich erzeugt dann ist  $M = N$ .
3. Wenn  $N \rightarrow M$  eine Abbildung sodass  $N/IN \rightarrow M/IM$  surjektiv ist dann ist  $N \rightarrow M$  surjektiv.
4. Wenn  $x_1, \dots, x_n \in M$   $M/IM$  erzeugen dann erzeugen  $x_1, \dots, x_n$  schon  $M$ .

*Beweis.* Angenommen  $M \neq 0$ . Da  $M$  endlich erzeugt ist, betrachte minimales Erzeugendensystem  $x_1, \dots, x_n \in M$ . Da  $\mathfrak{a}M = M$  gilt, ist  $x_n = a_1x_1 + \dots + a_nx_n$  für  $a_i \in \mathfrak{a}$ . Dann ist  $(1 - a_n)x_n = a_1x_1 + \dots + a_nx_n$  und da  $(1 - a_n)$  eine Einheit ist, folgt  $x_n$  ist im Erzeugnis von  $(x_1, \dots, x_{n-1})$  was ein Widerspruch ist. Das zeigt 1. Wenn  $N'$  endlich erzeugt ist, dann auch  $M/N$ . Anwenden von 1 auf  $M/N$  liefert die Aussage. Es ist  $M = \text{im}(N \rightarrow M) + IM$  und nach 2. folgt, dass  $M = \text{im}(N \rightarrow M)$ . Sei  $R^n \rightarrow M, (a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n$ . Nach 3. folgt, dass die Abbildung surjektiv ist also gilt 4. □

## 10.2 Noethersche und Artinsche Moduln

**Definition 10.2.1.** Eine partiell geordnete Menge  $\Sigma$  hat die aufsteigende Kettenbedingung, falls jede Kette  $S_1 \leq S_2 \leq \dots \leq S_k \leq \dots$  irgendwann stationär wird.

**Lemma 10.2.2.** Sei  $\Sigma$  partiell geordnet.  $\Sigma$  hat die aufsteigende Ketten-Bedingung genau dann wenn für alle  $S \subseteq \Sigma$  mit  $S \neq \emptyset$  gilt, dass  $S$  ein maximales Element hat.

**Beispiel 10.2.3.** Unterräume eines endlich-dimensionalen Vektorraums oder Ideale in  $\mathbb{Z}$  erfüllen aufsteigende Kettenbedingung.

**Satz 10.2.4.** Sei  $A$  ein Ring. Es ist äquivalent:

1. Die Menge  $\Sigma$  der Ideale von  $A$  hat die aufsteigende Ketten-Bedingung.
2. Jede nicht-leere Menge  $S \subseteq \Sigma$  hat ein maximales Element
3. Jedes Ideal  $I \in \Sigma$  ist endlich erzeugt.

In dem Fall heißt  $A$  noethersch.

*Beweis.* Zeige 3 nach 1. Sei  $I_1 \subseteq I_2 \subseteq \dots$  Kette von Idealen. Dann ist  $I = \bigcup_k I_k$  endlich erzeugt,  $I = (f_1, \dots, f_n)$  dann ist  $f_1, \dots, f_n \in I_k$  für ein  $k$  und somit wird Kette stationär nach  $k$ . □

**Satz 10.2.5.** Sei  $M$  ein  $A$ -Modul. Es ist äquivalent:

1. Die Menge  $\Sigma$  der Untermoduln von  $M$  hat die aufsteigende Ketten-Bedingung.
2. Jede nicht-leere Menge  $S \subseteq \Sigma$  hat ein maximales Element
3. Jeder Untermodul  $N \in \Sigma$  ist endlich erzeugt.

In dem Fall heißt  $M$  *noethersch*.

**Satz 10.2.6.** Sei  $M$  ein  $A$ -Modul. Es ist äquivalent:

1. Die Menge  $\Sigma$  der Untermoduln von  $M$  hat die absteigende Ketten-Bedingung.
2. Jede nicht-leere Menge  $S \subseteq \Sigma$  hat ein minimales Element
3. Für Jede Familie  $\{M_i\}_{i \in I}$  von Untermoduln gibt es  $I_0 \subseteq I$  endlich sodass

$$\bigcap_{i \in I} M_i = \bigcap_{i \in I_0} M_i$$

In dem Fall heißt  $M$  *artinsch*.

*Beweis.* Zeige 1 nach 3. Wähle  $i_1 \in I$  sodass  $M_{i_1} \neq \bigcap_{i \in I} M_i$  (falls möglich). Für  $M_{i_1}, \dots, M_{i_k}$  gegeben wähle  $M_{i_{k+1}}$  so, dass  $\bigcap_{j=1}^{k+1} M_{i_j} \neq \bigcap_{j=1}^k M_{i_j}$ . Das gibt  $M_{i_1} \supsetneq M_{i_1} \cap M_{i_2} \supsetneq \dots$ . Also gibt es ein  $k$  sodass  $\bigcap_{j=1}^k M_{i_j} = \bigcap_{i \in I} M_i$ . Sei  $I_0 = \{i_1, \dots, i_k\}$ .  $\square$

**Lemma 10.2.7.** Sei  $0 \rightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \rightarrow 0$  eine exakte Sequenz von  $A$ -Moduln und  $M_1 \subseteq M_2 \subseteq M$  Untermoduln. Es gilt

$$L \cap M_1 = L \cap M_2 \text{ und } \beta(M_1) = \beta(M_2) \implies M_1 = M_2$$

**Satz 10.2.8.** Sei  $0 \rightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \rightarrow 0$  eine exakte Sequenz von  $A$ -Moduln. Dann ist

$$M \text{ noethersch} \iff M \text{ und } L \text{ noethersch}$$

*Beweis.* Angenommen  $M_1 \subseteq M_2 \subseteq \dots$  ist aufsteigende Kette von Untermoduln von  $M$ . Das gibt aufsteigende Ketten  $L \cap M_1 \subseteq L \cap M_2 \subseteq \dots$  und  $\beta(M_1) \subseteq \beta(M_2) \subseteq \dots$  in  $L$  und  $N$ . Beide Ketten werden stationär. Nach Lemma 10.2.7 wird also die ursprüngliche Kette stationär  $\square$

**Korollar 10.2.9.** 1.  $M_i$  noethersch impliziert  $\bigoplus_{i=1}^r M_i$  noethersch.

2. Wenn  $A$  noetherscher Ring dann ist  $A$ -Module  $M$  noethersch genau dann wenn  $M$  endlich ist über  $A$ .
3. sei  $A$  noetherscher Ring und  $\varphi: A \rightarrow B$  Ringhomomorphismus sodass  $B$  endlicher  $A$ -Modul ist. Dann ist  $B$  noetherscher Ring.

*Beweis.* Zeige 2. sei  $M$  endlich erzeugt von  $f_1, \dots, f_r$  und  $A^r \rightarrow M$  surjektiv mit

$$(a_1, \dots, a_r) \mapsto a_1 f_1 + \dots + a_r f_r.$$

Sei  $N$  der Kern. Das gibt exakte Sequenz  $0 \rightarrow N \rightarrow A^r \rightarrow M \rightarrow 0$  und nach 1 ist  $A^r$  noethersch also auch  $M$ .  $\square$

**Satz 10.2.10** (Hilbert Basis Theorem). Sei  $A$  Ring. Dann ist  $A[X]$  noethersch genau dann wenn  $A$  noethersch ist.

*Beweis.* Sei  $A$  noethersch. Sei  $I \subseteq A[X]$ . Definiere

$$J_n = \{a \in A \mid \exists f \in I: f = aX^n + b_{n-1}X^{n-1} + \dots + b_0\}.$$

$J_n$  ist Ideal da  $I$  Ideal ist. Es ist  $J_n \subseteq J_{n+1}$  und da  $A$  noethersch ist, ist  $J_n = J_{n+1} = \dots$  für ein  $n$ . Für  $m \leq n$  ist  $J_m \subseteq A$  endlich erzeugt,  $J_m = (a_{m,1}, \dots, a_{m,r_m})$ . Sei  $f_{m,j} \in I$  mit Leitkoeffizient  $a_{m,j}$ . Dann erzeugt  $\{f_{m,j}\}_{\substack{m \leq n \\ 1 \leq j \leq r_m}}$  das Ideal  $I$ . Sei nämlich  $f \in I$  vom Grad  $m$  und  $a$  der Leitkoeffizient von  $f$ ,  $a \in J_m$ . Wenn  $m \geq n$  dann ist  $a \in J_n$  sodass  $a = \sum b_i a_{n,i}$  für  $b_i \in A$  und  $f - \sum b_i X^{m-n} f_{n,i}$  hat Grad  $< n$ . Wenn  $m \leq n$  dann ist  $a \in J_m$  sodass  $a = \sum b_i a_{m,i}$  für  $b_i \in A$  und  $f - \sum b_i f_{m,i}$  hat Grad  $< m$ . Mit Induktion folgt die Behauptung. Sei  $A[X]$  noethersch. Dann ist  $0 \rightarrow K \rightarrow A[X] \rightarrow R \rightarrow 0$  exakt, wobei  $K$  der Kern ist von  $X \mapsto 0$ . Also ist  $A$  noethersch.  $\square$

**Lemma 10.2.11.** Wenn  $I \subseteq R$  ein endlich erzeugtes Ideal ist mit  $I^2 = 0$  und wenn  $R/I$  noethersch ist, dann ist  $R$  noethersch.

*Beweis.*  $I$  ist  $R/I$  Modul und da endlich erzeugt, ist  $I$  als  $R/I$  Modul noethersch. Das heißt jeder  $R/I$ -Untermodule  $J \subseteq I$  ist endlich erzeugt und dann auch endlich erzeugt als  $R$ -Modul. Also ist  $I$  noetherscher  $R$ -Modul. Exakte Sequenz liefert, dass  $R$  noethersch ist da  $R/I$  endlicher  $R$ -Modul.  $\square$

**Lemma 10.2.12.** Sei  $M$  noetherscher  $R$ -Modul. Zeigen Sie, dass jeder surjektive Endomorphismus  $f: M \rightarrow M$  bijektiv ist.

*Beweis.* Sei  $I_i = \ker(f^{(i)})$ . Es ist  $I_i \subseteq I_{i+1}$  also gibt es  $k$  sodass  $I_k = I_{k+1}$ . Da  $f$  jedoch surjektiv ist, folgt  $\ker(f) = 0$   $\square$

### 10.3 Localization

**Satz 10.3.1.** Sei  $S \subseteq R$  multiplikative Menge,  $M$   $R$ -Modul.  $\tau: M \rightarrow S^{-1}M, m \mapsto \frac{m}{1}$ . Dann gilt

1.  $\ker(\tau) = \{m \in M \mid \exists u \in S: um = 0\}$
2. Wenn  $M$  endlich erzeugt ist, dann ist  $S^{-1}M = 0 \iff M$  wird annulliert von einem  $M \in S$ .

*Beweis.* Wähle Erzeuger und multipliziere deren Annihilatoren.  $\square$

**Lemma 10.3.2.**  $S^{-1}R \otimes_R M \rightarrow S^{-1}M, \frac{r}{u} \otimes m \mapsto \frac{rm}{u}$  ist ein Isomorphismus.

**Satz 10.3.3** (Lokalisierung ist flach). Sei  $\varphi: M \rightarrow N$  injektiv.  $\frac{\varphi(x)}{s} = 0$  Dann gibt es  $t \in S$  sodass  $t\varphi(x) = \varphi(tx) = 0$  also ist  $tx = 0$  und somit  $\frac{x}{s} = 0$

**Korollar 10.3.4** (Lokalisierung erhält endliche Schnitte). Seien  $M_1, \dots, M_t \subseteq M$  Untermoduln. Dann ist  $S^{-1}(\bigcap_i M_i) = \bigcap_i S^{-1}M_i$ .

*Beweis.* Es ist exakt  $0 \rightarrow \bigcap_i M_i \rightarrow M \rightarrow \bigoplus_i M/M_i \rightarrow 0$  also auch

$$0 \rightarrow S^{-1}\bigcap_i M_i \rightarrow S^{-1}M \rightarrow \bigoplus_i S^{-1}M/S^{-1}M_i \rightarrow 0$$

und somit gilt die Aussage.  $\square$

**Lemma 10.3.5.** Sei  $R$  ein Ring  $M$  ein  $R$ -Modul.

1. Für  $m \in M$  ist  $m = 0 \iff \frac{m}{1} = 0 \in M_{\mathfrak{m}}$  für alle maximalen Ideale  $\mathfrak{m} \subseteq R$
2.  $M = 0 \iff M_{\mathfrak{m}} = 0$  für alle maximalen Ideale  $\mathfrak{m}$  von  $R$ .

*Beweis.* Sei  $I$  der Annihilator von  $M$ .  $m = 0 \iff I = R \iff I \not\subseteq \mathfrak{m}$  für alle maximalen Ideal  $\mathfrak{m}$ .  
2. folgt direkt aus 1  $\square$

**Korollar 10.3.6.**  $\varphi: M \rightarrow N$  Homomorphism von  $R$ -Moduln.  $\varphi$  ist injektiv (surjektiv, bijektiv)  $\iff \forall \mathfrak{m} \subseteq R$  maximal ist  $\varphi_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  injektiv (surjektiv, bijektiv)

*Beweis.*  $\varphi$  injektiv  $\iff \ker(\varphi) = 0 \iff \ker(\varphi)_{\mathfrak{m}} = \ker(\varphi_{\mathfrak{m}}) = 0 \forall \mathfrak{m}$ . Surjektiv geht analog mit Cokern statt kern.  $\square$

## 10.4 Structursatz endlicher Moduln über Hauptidealringe

**Lemma 10.4.1.** *Sei  $M$  ein  $R$ -Modul. Dann ist äquivalent:*

1.  $M \oplus M' = \bigoplus_{i \in I} R/f_i R$  für  $f_i \in R$  und ein  $R$ -Modul  $M'$ .

2. Für jede kurze exakte Sequenz

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

von  $R$ -Moduln sodass  $fA = A \cap fB$  ist für alle  $f \in R$  ist die Abbildung

$$\mathrm{Hom}_R(P, B) \rightarrow \mathrm{Hom}_R(P, C)$$

surjektiv.

*Beweis.* Gelte 1 und sei eine exakte Sequenz wie im Satz gegeben. Es reicht der Fall  $M = R/fR$ . Sei  $\psi: R/fR \rightarrow C$  eine Abbildung und sei  $b \in B$  mit  $b \mapsto \psi(1)$  in  $C$ . Dann ist  $fb \in A$  und es gibt  $a \in A$  sodass  $fa = fb$  also  $f(b - a) = 0$ . Das gibt  $\varphi: R/fR \rightarrow B, 1 \mapsto b - a$  das  $\psi$  liftet. Wenn andersrum 2 gilt, sei  $I$  die Menge der Paare  $(f, \varphi)$  wobei  $f \in R$  ist und  $\varphi: R/fR \rightarrow M$ . Für  $i \in I$  sei  $(f_i, \varphi_i)$  das entsprechende Paar. Betrachte  $B = \bigoplus_{i \in I} R/f_i R \rightarrow M$  induziert durch  $\varphi_i$ . Sei  $A = \ker(B \rightarrow M)$ . Wenn die Sequenz  $0 \rightarrow A \rightarrow B \rightarrow M \rightarrow 0$  exakt ist wie in 2. dann spaltet sie also folgt (1). Sei also  $f \in R$  und  $a \in A$  mit  $a \mapsto fb$ . Sei  $b = (r_i)_{i \in I}$  wobei  $r_i = 0$  für fast alle  $i$ . dann ist  $f \sum \varphi_i(r_i) = 0$  in  $M$ . Also gibt es  $i_0 \in I$  sodass  $f_{i_0} = f$  und  $\varphi_{i_0}(1) = \sum \varphi_i(r_i)$ . sei  $x_{i_0} \in R/f_{i_0}R$  die Klasse von 1. Dann ist

$$a' = (r_i)_{i \in I} - (0, \dots, 0, x_{i_0}, 0, \dots)$$

ein Element von  $A$  und  $f'a = a$ . □

**Lemma 10.4.2.** *Sei  $R \neq 0$  ein Ring. Dann ist äquivalent:*

1. Für  $a, b \in R$  gilt  $a \mid b$  oder  $b \mid a$

2. Jedes endlich erzeugte Ideal ist ein Hauptideal und  $R$  ist lokal

3. Die Menge der Ideale ist linear geordnet durch Inklusion

Das ist insbesondere erfüllt durch einen Bewertungsring

*Beweis.* Angenommen 2. gilt und  $a, b \in R$ . Dann ist  $(a, b) = (c)$ . Wenn  $c = 0$  ist, dann ist  $a = b = 0$  und  $a$  teilt  $b$ . Wenn  $c \neq 0$  sei  $c = ua + vb$  und  $a = wc$  und  $b = zc$ . Dann ist  $c(1 - uw - vz) = 0$ . Da  $R$  lokal ist, ist  $1 - uw - vz \in \mathfrak{m}$  denn sonst wäre es Einheit und  $c = 0$ . Also ist entweder  $w$  oder  $z$  eine Einheit. Also gilt 1. Wenn 1. gilt und  $R$  hat zwei maximale Ideal  $\mathfrak{m}, \mathfrak{n}$  Dann wähle  $a \in \mathfrak{m} \setminus \mathfrak{n}$  und  $b \in \mathfrak{n} \setminus \mathfrak{m}$ . Dann teilen  $a$  und  $b$  einander nicht. Also hat  $R$  nur ein maximales Ideal und ist lokal. Sei  $I = (f_1, \dots, f_n)$  und  $I' = (f_2, \dots, f_n)$ . Es ist nach Induktion  $I' = (c)$  und somit  $I = (f_1, c) = (c')$ . Es ist klar dass 1 und 3 äquivalent sind.

Die letzte Behauptung gilt in einem Bewertungsring, da im Quotientenkörper für  $a, b \neq 0$  gilt, dass  $\frac{a}{b} = x$  ist und  $x \in R$  oder  $x^{-1} \in R$ . Das heißt  $a = bx$  oder  $b = ax$  für ein  $x \in R$ . □

**Lemma 10.4.3.** *Sei  $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$  eine kurze exakte Sequenz von  $R$ -Moduln. Dann gilt*

1.  $M_1, M_3$  endlich erzeugt  $\implies M_2$  endlich erzeugt.

2.  $M_1, M_3$  endlich präsentiert  $\implies M_2$  endlich präsentiert.

3.  $M_2$  endlich erzeugt  $\implies M_3$  endlich erzeugt.

4.  $M_2$  endlich präsentiert und  $M_1$  endlich erzeugt  $\implies M_3$  ist endlich präsentiert.

5.  $M_3$  endlich präsentiert und  $M_2$  endlich erzeugt  $\implies M_1$  endlich erzeugt.

*Beweis.* 1 und 3 klar. Zeige 2.

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^n & \longrightarrow & R^{n+m} & \longrightarrow & R^m \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \end{array}$$

Snake Lemma liefert exakte Sequenz  $0 \rightarrow \ker(R^n \rightarrow M_1) \rightarrow \ker(R^{n+m} \rightarrow M_2) \rightarrow \ker(R^m \rightarrow M_3) \rightarrow 0$ . Nach (5) sind die beiden äußeren endlich erzeugt also der innere auch. Nach (4) ist dann  $M_2$  endlich präsentiert.

Zeige 5. Wähle Auflösung  $R^m \rightarrow R^n \rightarrow M_3 \rightarrow 0$ . Da  $R^n$  projektiv ist nach ??? gibt es eine Abbildung  $R^n \rightarrow M$  sodass das solide Diagramm kommutiert:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^m & \longrightarrow & R^n & \longrightarrow & M_3 \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \text{id} \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \end{array}$$

Das gibt dann gestrichelten Pfeil. Nach Schlangenlemma ist  $\text{coker}(R^m \rightarrow M_1) \cong \text{coker}(R^n \rightarrow M_2)$ . Also ist  $\text{coker}(R^m \rightarrow M_1)$  endlich erzeugt. Nach (3) ist  $\text{im}(R^m \rightarrow M_1)$  endlich erzeugt also ist  $M_1$  endlich nach (1). Zeige 4. Wähle Auflösung  $R^m \rightarrow R^n \rightarrow M_2 \rightarrow 0$  und Surjektion  $R^k \rightarrow M_1$ . Dann gibt es nach ??  $R^k \rightarrow R^n$  und  $R^{k+m} \rightarrow R^n \rightarrow M_3 \rightarrow 0$  ist eine Auflösung.  $\square$

**Lemma 10.4.4.** *Sei  $R$  ein Ring sodass die Menge der Ideale linear geordnet ist durch Inklusion. Dann ist jeder endlich-präsentierte  $R$ -Modul isomorph zu einer endlichen direkten Summe von Moduln der Form  $R/fR$ .*

*Beweis.* Es werden die Äquivalenten Bedingungen in Lemma 10.4.2 Benutzt. Sei  $M$  ein endlich präsentierter  $R$ -Modul. Sei  $\mathfrak{m} \subseteq R$  das maximale Ideal und  $\kappa = R/\mathfrak{m}$  der Restklassenkörper. Sei  $I = \{r \in R \mid rM = 0\}$ . Wähle Basis  $y_1, \dots, y_n$  des endlich-dimensionalen  $\kappa$ -Vektorraum  $M/\mathfrak{m}M$ . Nach Lemma 10.1.18 erzeugen Lifts  $x_1, \dots, x_n$  von  $y_1, \dots, y_n$  schon  $M$ . Es gibt  $i$  sodass für alle Wahlen von  $x_i$  gilt  $I = \{r \in R \mid rx = 0\} =: I_i$ . Denn angenommen nicht. Dann gibt es Wahlen von  $x_1, \dots, x_n$  sodass  $I_i \neq I$  für alle  $i$ . Aber da  $I \subseteq I_i$  gilt  $I \subsetneq I_i$  für alle  $i$ . Da Ideale total geordnet sind, wäre auch  $I = I_1 \cap I_2 \cap \dots \cap I_n$  größer als  $I$ , was ein Widerspruch ist. Nach Umordnen ist  $i = 1$  und jeder Lift  $x_i$  von  $y_i$  erfüllt  $I_1 = I$ . Sei  $A = RX_1 \subseteq M$  und betrachte die exakte Sequenz

$$0 \rightarrow A \rightarrow M \rightarrow M/A \rightarrow 0$$

. Da  $A$  endlich erzeugt ist, ist  $M/A$  endlich präsentiert nach Lemma 10.4.3 mit weniger Erzeugern. Nach Induktion ist also  $M/A \cong \bigoplus_{j=1, \dots, m} R/f_jR$ . Es gilt das wenn  $f \in R$  dann ist  $fA = A \cap fM$ . Sei also  $x \in A \cap fM$ . dann ist  $x = gx_1 = fy$  für ein  $g \in R$  und  $y \in M$ . wenn  $f \mid g$  dann ist  $x \in fA$ . Wenn nicht, dann ist  $f = hg$  für  $h \in \mathfrak{m}$ . Dann ist  $x'_1 = x_1 - hy$  ein Lift von  $y_1$  also ist  $g \in I$  und  $x = 0$ . Nach Lemma Lemma 10.4.1 spaltet die exakte Sequenz von oben und  $M \cong A \oplus \bigoplus_{j=1, \dots, m} R/f_jR$ . Dann ist  $A = R/I$  endlich präsentiert als Summand von  $M$  und deswegen ist  $I$  endlich generiert nach beides nach Lemma 10.4.3 und also  $I$  ein Hauptideal. Das zeigt den Satz.  $\square$

**Lemma 10.4.5.** *Sei  $R$  ein Ring sodass alle Ideale von  $R_{\mathfrak{m}}$  total geordnet sind für jedes maximale Ideal  $\mathfrak{m} \subseteq R$ . Dann ist jeder endlich präsentierte  $R$ -Modul direkter Summand von  $\bigoplus_{i \in I} R/f_iR$  wobei  $I$  endlich.*

*Beweis.* Sei  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  eine kurze exakte Sequenz von  $R$ -Moduln sodass  $fA = A \cap fB$  für alle  $f \in R$ . Nach Lemma Lemma 10.4.1 reicht es, zu zeigen dass  $\text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$  surjektiv ist. Es reicht, dass es surjektiv ist nach lokalisieren an maximalen Idealen  $\mathfrak{m}$  nach Korollar 10.3.6. Da Lokalisierung nach Satz 10.3.3 exakt ist  $0 \rightarrow A_{\mathfrak{m}} \rightarrow B_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}} \rightarrow 0$  exakt und  $fA_{\mathfrak{m}} = A_{\mathfrak{m}} \cap fB_{\mathfrak{m}}$ . Da  $M$  endlich präsentiert ist, gilt  $\text{Hom}_R(M, B)_{\mathfrak{m}} = \text{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, B_{\mathfrak{m}})$  und  $\text{Hom}_R(M, C)_{\mathfrak{m}} = \text{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}})$  nach ??? .  $M_{\mathfrak{m}}$  ist endlich präsentierter  $R_{\mathfrak{m}}$  Modul und nach Lemma 10.4.4 gilt dass  $M_{\mathfrak{m}}$  direkte Summe von Moduln der Form  $R_{\mathfrak{m}}/fR_{\mathfrak{m}}$  ist. Nach Lemma 10.4.1 ist Abbildung der Lokalisierung surjektiv. Also ist  $M$  direkter Summand von  $\bigoplus_{i \in I'} R/f_iR$ . Betrachte  $M \rightarrow \bigoplus_{i \in I'} R/f_iR$ . Da  $M$  endlich erzeugt ist, ist das Bild von  $M$  in  $\bigoplus_{i \in I'} R/f_iR$  für eine endliche Teilmenge  $I \subseteq I'$ .  $\square$

**Definition 10.4.6.** Sei  $R$  nullteilerfrei.

1.  $R$  ist ein Bézout Ring, wenn jedes endlich erzeugte Ideal ein Hauptideal ist.
2.  $R$  ist ein Elementarteiler Ring, falls für alle  $n, m \geq 1$  und jede  $n \times m$  matrix  $A$  es invertierbare Matrizen  $U, V$  der Größe  $n \times n$  bzw.  $m \times m$  gibt sodass

$$UAV = \begin{pmatrix} f_1 & 0 & 0 & \dots \\ 0 & f_2 & 0 & \dots \\ 0 & 0 & f_3 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

mit  $f_1, \dots, f_{\min(n,m)} \in R$  und  $f_1 \mid f_2 \mid \dots$ .

**Lemma 10.4.7.** Ein Elementarteilerring ist Bézout Ring.

*Beweis.* Seien  $a, b \in R$  nicht-null. Betrachte  $A = (ab)$ . Dann gibt es  $u \in R^*$  und  $V = (g_{ij}) \in \text{GL}_2(R)$  sodass  $u(a, b)V = (f, 0)$ . Dann ist  $f = uag_{11} + ubg_{21}$ . Es ist auch

$$\begin{pmatrix} a & b \end{pmatrix} = u^{-1} \begin{pmatrix} f & 0 \end{pmatrix} V^{-1}$$

Also ist  $(a, b) = (f)$ . Induktion zeigt das Ergebnis. □

**Satz 10.4.8.** Die Lokalisierung eines Bezout-Rings ist Bezout. Ein lokaler Integritätsbereich ist Bezout genau dann wenn es ein Bezout ring ist.

*Beweis.* Erste Aussage ist klar und zweite gilt nach ??? was genau die Aussage ist. □

**Lemma 10.4.9.** Sei  $R$  Bézout ring. Dann gilt

1. Jeder endliche Untermodul eines freien Moduls ist frei
2. Jeder endlich präsentierte  $R$ -Modul  $M$  ist direkte Summe eines endlich freien Moduls und einem torsions Modul  $M_{tors}$  der Summan ist einer direkten Summe  $\bigoplus_{i=1, \dots, n} R/f_i R$  wobei  $f_i$  nicht-null sind.

*Beweis.* Sei  $M \subseteq F$  endlich erzeugter Untermodul,  $F$  frei. Da  $M$  endlich ist, ist ohne Einschränkung  $F$  auch endlich,  $F = R^n$ . Wenn  $n = 1$  dann ist  $M$  ein endlich erzeugtes Ideal, also ein Hauptideal. Wenn  $n > 1$  betrachte  $pr_n: R^n \rightarrow R$  und  $I = \text{im}(pr_n|_M: M \rightarrow R)$ . Wenn  $I = (0)$  dann ist  $M \subseteq R^{n-1}$  und man ist fertig nach Induktion. Wenn  $I \neq 0$  dann ist  $I = (f) \cong R$ . also  $M \cong R \oplus \ker(M \rightarrow I)$  und Induktion.

Sei  $M$  also endlich präsentiert. Nach ??? sind lokalisierungen von  $R$  an maximalen Idealen Bewertungsringe, also können wir mit Lemma 10.4.5 folgern, dass  $M$  direkter Summand ist von

$$R^r \oplus \bigoplus_{i=1, \dots, n} R/f_i R$$

wobei  $f_i \neq 0$ . Dann ist  $M_{tors}$  ein Summand von  $\bigoplus_{i=1, \dots, n} R/f_i R$  und  $M/M_{tors}$  ist ein Summand von  $R^r$ . Nach erstem Teil ist  $M/M_{tors}$  endlich frei und also  $M \cong M_{tors} \oplus M/M_{tors}$ . □

**Satz 10.4.10** (Struktursatz endlicher Moduln über Hauptidealrings). Sei  $R$  ein Hauptidealring. Dann ist jeder endliche  $R$ -Modul  $M$  isomorph zu einem Modul der Form

$$R^n \oplus \bigoplus_{i=1, \dots, n} R/f_i R$$

für  $r, n \geq 0$  und  $f_i$  nicht-null mit  $f_1 \mid f_2 \mid \dots$

*Beweis.* Ein Hauptidealring ist ein noetherscher Bézout Ring. Nach Lemma 10.4.9 reicht der Fall wo  $M$  torsion ist. Da  $M$  endlich erzeugt, gibt es  $f \in R \setminus \{0\}$  sodass  $fM = 0$ . Dann ist  $M$  ein  $R/fR$  Modul und  $R/fR$  ist noethersch und jedes Primideal ist maximal. Also ist nach Korollar 10.5.13

$$R/fR = \prod R_j$$

endliches Produkt wobei  $R_j$  lokal artinsch. Die Projektion  $R/fR \rightarrow R_j$  gibt dass  $R_j = R/f_jR$  für ein  $f_j$ . Dann erfüllt  $R_j$  die Bedingungen von Lemma 10.4.2. Schreibe  $M = \prod M_j$  mit  $M_j = e_j M$  wobei  $e_j \in R/fR$  das idempotente Element ist dass zu  $1 \in R_j$  correspondiert. Nach Lemma 10.4.4 ist  $M_j = \bigoplus_{i=1, \dots, n_j} R_j/f_{ij}R_j$  für  $f_{ij} \in R_j$ . wähle Lifts  $f_{ij} \in R$  und  $g_{ji} \in R$  mit  $(g_{ji}) = (f_j, f_{ji})$ . Dann ist

$$M \cong \bigoplus R/g_{ji}R$$

als  $R$ -Modul. □

## 10.5 Moduln endlicher Länge

**Definition 10.5.1.** Eine Kompositionsreihe ist Kette  $M = N_0 \supsetneq \dots \supsetneq N_n = 0$  sodass  $N_i/N_{i+1}$  keine echten Untermodule ungleich 0 hat.

**Definition 10.5.2.** Sei  $M$  ein  $R$ -Modul. Definiere  $\text{length}(M)$  als das Minimum aller Längen einer Kompositionsreihe bzw als  $\infty$  falls das nicht existiert.

**Beispiel 10.5.3.** Sei  $V$  ein endlich-dimensionaler Vektorraum der Dimension  $n$ . Dann ist  $n = \text{length}(V)$ .

**Lemma 10.5.4.** Sei  $M' \subsetneq M$  ein echter Untermodul,  $\text{length}(M) = n < \infty$ . Dann ist  $\text{length}(M') < \text{length}(M)$

*Beweis.* Sei  $M = M_0 \supsetneq \dots \supsetneq M_n = 0$  eine Kompositionsreihe. Es ist

$$(M' \cap M_i)/(M' \cap M_{i+1}) \cong (M' \cap M_i + M_{i+1})/M_{i+1} \subseteq M_i/M_{i+1}.$$

Also ist  $(M' \cap M_i)/(M' \cap M_{i+1}) = 0$  oder  $(M' \cap M_i)/(M' \cap M_{i+1})$  hat keine echten Untermoduln und  $M' \cap M_i + M_{i+1} = M_i$ . Letzteres gilt nicht für alle  $i$ , denn angenommen doch. Es ist  $M_n = 0 \subseteq M'$  und angenommen  $M_{i+1} \subseteq M'$ . Dann ist  $M' \cap M_i = M' \cap M_i + M_{i+1} = M_i$  also  $M_i \subseteq M'$  und mit Induktion  $M \subseteq M'$ . Also kann  $M' \supseteq M' \cap M_1 \supseteq \dots \supseteq M' \cap M_n = 0$  kann verändert werden durch Weglassen der Terme  $M' \cap M_i$  sodass  $M' \cap M_i = M' \cap M_{i+1}$ . Das gibt  $\text{length}(M') < \text{length}(M)$  □

**Lemma 10.5.5.** sei  $\text{length}(M) = n < \infty$  und  $M = N_0 \supsetneq N_1 \supsetneq \dots \supsetneq N_k$  Kette von Untermoduln. Dann ist  $k \leq \text{length}(M)$ .

*Beweis.* Induktion:  $\text{length}(M) = 0 \implies M = 0 \implies k = 0$ . Allgemein ist

$$\text{length}(N_1) < \text{length}(M)$$

also ist  $k - 1 \leq \text{length}(N_1)$  und damit  $k \leq \text{length}(M)$ . □

**Korollar 10.5.6.**  $\text{length}(M)$  ist das maximal aller Längen einer Kette in  $M$ .

**Korollar 10.5.7.** Alle Kompositionsreihen haben die gleiche Länge

**Satz 10.5.8.** Sei  $M$  ein  $R$ -Modul.

$$\text{length}(M) < \infty \iff M \text{ ist artinsch und noethersch}$$

*Beweis.* Sei  $M$  artinsch und noethersch. Wähle maximalen Untermodul  $M_1 \subsetneq M$  und maximalen Untermodul  $M_2 \subsetneq M_1$  usw. Das gibt  $M \supsetneq M_1 \supsetneq M_2 \dots$ . Da  $M$  artinsch wird das stationär also  $M_n = 0$  für ein  $n$ . Dann ist das Kompositionsreihe. Angenommen  $M$  hat endliche Länge  $n$ . Das heißt jede aufsteigende oder absteigende Kette bricht ab also ist  $M$  artinsch und noethersch. □

**Satz 10.5.9.** Sei  $M$  ein  $R$ -Modul. Es ist äquivalent:

1.  $M$  hat keine echten Untermoduln  $\neq 0$
2.  $\text{length}(M) = 1$
3.  $M \cong R/\mathfrak{m}$  für ein maximales Ideal  $\mathfrak{m} \subseteq R$ .

*Beweis.* Gelte a. sei  $x \in M$  mit  $x \neq 0$ .  $x \cdot R \neq 0 \implies xR = M$  also ist

$$0 \rightarrow \mathfrak{m} \rightarrow R \xrightarrow{x} M \rightarrow 0$$

exakt mit  $\mathfrak{m} = \ker(x)$ . Da  $M \cong R/\mathfrak{m}$  keine echten Ideale hat, ist  $\mathfrak{m}$  maximal.  $\square$

**Satz 10.5.10.** Sei  $\text{length}(M) < \infty$  und  $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$  Kompositionsreihe. Es ist  $M \cong \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}}$  wobei die Summe über alle maximalen Ideale  $\mathfrak{p} \subseteq R$  geht sodass  $M_i/M_{i+1} \cong R/\mathfrak{p}$ . Die Anzahl der  $M_i/M_{i+1}$  isomorph zu  $R/\mathfrak{p}$  ist  $\text{length}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}})$ .

*Beweis.* Angenommen  $\text{length}(M) = 1$ . Dann ist  $M \cong R/\mathfrak{p}$  für ein maximales Ideal  $\mathfrak{p}$ . Sei  $\mathfrak{q}$  ein maximales Ideal. Wenn  $\mathfrak{p} = \mathfrak{q}$  dann ist  $M_{\mathfrak{q}} = (R/\mathfrak{p})_{\mathfrak{q}} = R/\mathfrak{p} = M$ . Wenn  $\mathfrak{p} \neq \mathfrak{q}$  dann ist  $(R/\mathfrak{p})_{\mathfrak{q}} = 0$ . Somit ist  $(M_{\mathfrak{q}})_{\mathfrak{q}'} = 0$  für zwei verschiedene maximalen Ideale  $\mathfrak{q}, \mathfrak{q}'$ . Allgemein für  $\text{length}(M) = n$  gilt dass die Kompositionsreihe  $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$  gibt  $M_{\mathfrak{q}} = (M_0)_{\mathfrak{q}} \supsetneq \cdots \supsetneq (M_n)_{\mathfrak{q}} = 0$  und  $\text{length}(M_i/M_{i+1}) = 1$ . Also ist

$$(M_i/M_{i+1})_{\mathfrak{q}} = \begin{cases} M_i/M_{i+1}, & M_i/M_{i+1} \cong R/\mathfrak{q} \\ 0, & \text{sonst} \end{cases}$$

Behalte in Reihe nur die  $(M_i)_{\mathfrak{q}}$  aus oberen Fall, das gibt Kompositionsreihe von  $M_{\mathfrak{q}}$ . Sei  $\alpha: M \rightarrow \bigoplus M_{\mathfrak{p}}$  Summe der Lokalisierungsabbildungen. Sei  $Q \subseteq R$  maximales Ideal. Es ist  $\alpha_Q: M_Q \rightarrow (\bigoplus M_{\mathfrak{p}})_Q$  die Identität für alle  $Q$ .  $\square$

**Satz 10.5.11.** Sei  $\text{length}(M) < \infty$ . Dann gilt

$$M = M_{\mathfrak{p}} \iff M \text{ wird von einer Potenz von } \mathfrak{p} \text{ annulliert}$$

*Beweis.* Sei  $\mathfrak{q} \neq \mathfrak{p}$  maximales Ideal,  $x \in \mathfrak{p} \setminus \mathfrak{q}$ . Dann ist  $\frac{x}{1} M_{\mathfrak{q}} = M_{\mathfrak{q}}$  aber  $x^n = 0$  für ein  $n$ , also  $M_{\mathfrak{q}} = 0$ . Nach Satz 10.5.10 folgt  $M = M_{\mathfrak{p}}$ . Sei andererseits  $M \cong M_{\mathfrak{p}}$  und  $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n$  Kompositionsreihe,  $M_i/M_{i+1} \cong R/\mathfrak{p}$ . Es ist  $\mathfrak{p}M = M = M_0$  und wenn  $\mathfrak{p}^i M \subseteq M_i$  dann ist  $\mathfrak{p}^{i+1} M \subseteq \mathfrak{p}M_i \subseteq M_{i+1}$ . Nach Induktion ist also  $\mathfrak{p}^n M \subseteq M_n = 0$ .  $\square$

**Satz 10.5.12.** Sei  $R$  ein Ring. Es ist äquivalent:

1.  $R$  ist noethersch und alle Primideale in  $R$  sind maximal
2.  $R$  ist als  $R$ -Modul von endlicher Länge
3.  $R$  ist artinsch.

Wenn das gilt, dann hat  $R$  nur endlich viele maximale Ideale.

*Beweis.* Gelte 1. Sei  $I \subseteq R$  ein Ideal maximal mit der Eigenschaft dass  $R/I$  keine endliche Länge hat. Dann ist  $I$  prim, denn seien  $a \cdot b \in I$  und  $a \notin I$ . Haben exakte Sequenz

$$0 \rightarrow R/(I : a) \rightarrow R/I \rightarrow R/(I + (a)) \rightarrow 0$$

wobei  $(I : a) = \{x \in R \mid ax \in I\}$ . Da  $I \subsetneq I + (a)$  hat  $R/(I + (a))$  endliche Länge. Falls  $b \notin I$  dann  $I \subsetneq (I : a)$  also hat  $R/(I : a)$  endliche Länge und damit auch  $R/I$  was nicht sein kann. Also ist  $I$  prim. Damit ist  $I$  maximal und somit  $R/I$  ein Körper. Ein Körper hat Länge = 1 was ein Widerspruch ist. Also hat  $R$  endliche Länge. Gelte 2. 3. Folgt mit Satz Satz 10.5.8. gelte 3. Sei also  $R$  artinsch. Zeige: 0 ist Produkt maximaler Ideal von  $R$ . sei  $J \subseteq R$  minimal sodass  $J$  Produkt maximaler Ideale ist. Zeige  $J = 0$ . Sei  $\mathfrak{m}$  maximales Ideal in  $R$ . Dann ist  $\mathfrak{m}J = J$  wegen Minimalität von  $J$  also  $J \subseteq \mathfrak{m}$ . Es ist  $J^2 = J$ . Falls  $J \neq 0$  wähle  $I$  minimal unter Idealen, die  $J$  nicht annihilieren. Es gilt  $(IJ)J = IJ^2 = IJ \neq 0$  und  $IJ \subseteq I$ . Wegen Minimalität von  $I$  ist  $IJ = I$ . Das heißt es gibt  $f \in I$  mit  $fJ \neq 0$ . Da  $I$  minimal ist, ist  $(f) = I$ . Es gibt ein  $g \in J$  mit  $f = fg$  und somit  $(1 - g)f = 0$ .  $g$  ist in allen maximalen Idealen enthalten also ist  $1 - g$  eine Einheit. Also ist  $f = 0$  und damit  $I = 0$ . Also ist  $J = 0$ . Somit ist  $0 = \mathfrak{m}_1 \cdots \mathfrak{m}_t$  für maximale Ideale  $\mathfrak{m}_i \subseteq R$ . Der Quotient  $V_S = \mathfrak{m}_1 \cdots \mathfrak{m}_s / \mathfrak{m}_1 \cdots \mathfrak{m}_{s+1}$  ist Vektorraum über  $R/\mathfrak{m}_{s+1}$ . Untermodule von  $V_s$  sind Ideale in  $R$ , die  $\mathfrak{m}_1 \cdots \mathfrak{m}_{s+1}$  enthalten. Absteigende Kette von Untermoduln sind absteigende Kette in  $R$ . Da  $R$  artinsch ist, muss Kette endlich sein. Also ist  $V_s$  endlich-dimensional über  $R/\mathfrak{m}_{s+1}$  und hat also endliche Kompositionsreihe. Alle Ketten Vereinigen gibt endliche Kompositionsreihe von  $R$ . Also hat  $R$  endliche Länge und ist noethersch. Sei  $\mathfrak{p} \subseteq R$  Primideal. Da  $\mathfrak{m}_1 \cdots \mathfrak{m}_t = 0 \subseteq \mathfrak{p}$  ist  $\mathfrak{m}_i = \mathfrak{p}$  für ein  $i$ . Also ist jedes Primideal maximal.  $\square$



**Korollar 10.5.13.** *Jeder Artinsche Ring ist Produkt allseiner Lokalisierungen an maximalen Idealen.*

**Lemma 10.5.14.** *Sei  $R$  ein Ring.*

1. *Jeder Untermodul eines Artinschen  $R$ -Modules ist artinsch*
2. *Jeder artinsche  $\mathbb{Z}$ -Modul ist torsionsmodul*
3. *Sei  $p$  eine Primzahl. Die echten Untermoduln des Moduls  $\mathbb{Z}[1/p]/\mathbb{Z}$  sind  $K_n$  wobei  $K_n$  erzeugt ist von  $\frac{1}{p^n}$  und  $\mathbb{Z}[1/p]/\mathbb{Z}$  ist artinsch.*

*Beweis.* 1. Klar

2. Sei  $M$  artinscher  $\mathbb{Z}$ -Modul. Es gibt absteigende Kette  $m\mathbb{Z} \supseteq 2m\mathbb{Z} \supseteq 4m\mathbb{Z} \supseteq 8m\mathbb{Z} \supseteq \dots$  von Untermoduln für  $m \in M$ . Da  $M$  artinsch ist, ist  $2^k m\mathbb{Z} = 2^{k+1} m\mathbb{Z}$  für ein  $k$ . Das heißt  $2^k m = 2^{k+1} xm$  für ein  $x \in \mathbb{Z}$ . das heißt  $m2^k(1 - 2x) = 0$ . Alternativ kann man sehen dass

$$0 \rightarrow n\mathbb{Z} \rightarrow \mathbb{Z} \xrightarrow{\cdot m} m\mathbb{Z} \rightarrow 0$$

exakt ist für ein  $n \in \mathbb{Z}$ . Wenn  $n = 0$  dann ist  $m\mathbb{Z} = \mathbb{Z}$  artinsch nach 1 was ein Widerspruch ist. also ist  $n \neq 0$  und  $m\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ . Dann ist  $n \cdot m = 0$  also  $M$  torsionsmodul.

3. Sei  $M$  ein Untermodul. Dann ist  $\frac{a}{p^n} \in M$  für ein  $p \nmid a$ . Damit gibt es  $1 = p^n x + ay$  nach Lemma von Bezout ??? für  $x, y \in \mathbb{Z}$ . Also ist

$$\frac{ay}{p^n} = \frac{1 - p^n x}{p^n} = \frac{1}{p^n} \in M$$

Es gilt  $\max\{n \in \mathbb{N} \mid \frac{1}{p^n} \in M\}$  ist  $\infty$  oder  $m \in \mathbb{N}$ . Falls  $\infty$  dann ist  $M = \mathbb{Z}[1/p]/\mathbb{Z}$ . Wenn das maximum  $m$  ist dann ist  $M = K_m$ . Also sind die einzigen Untermoduln  $K_0 \subseteq K_1 \subseteq \dots$  also muss jede absteigende Kette stationär werden und  $\mathbb{Z}[1/p]/\mathbb{Z}$  ist artinsch. □

**Lemma 10.5.15.** *Sei  $\mathfrak{m} \subseteq R$  ein maximales Ideal und  $n \in \mathbb{N}$ .*

1. *Wenn  $R$  noethersch ist, dann ist  $R/\mathfrak{m}^n$  artinsch.*
2. *Wenn  $\mathfrak{m}$  endlich erzeugt ist, dann ist  $R/\mathfrak{m}^n$  artinsch*

*Beweis.* 1. Es ist  $R/\mathfrak{m}^n$  noethersch. sei  $\mathfrak{p}$  ein Primideal von  $R$  mit  $\mathfrak{m}^n \subseteq \mathfrak{p} \subseteq R$ . Dann ist  $\mathfrak{m} \subseteq \mathfrak{p}$  also  $\mathfrak{m} = \mathfrak{p}$  und alle Primideale in  $R/\mathfrak{m}^n$  sind maximal. Also ist  $R/\mathfrak{m}^n$  artinsch.

2. Sei  $\mathfrak{m}$  endlich erzeugt. Dann ist  $\mathfrak{m}^k/\mathfrak{m}^{k+1}$  endlich erzeugt über  $R/\mathfrak{m}$ , das heißt ein endlich-dimensionaler Vektorraum. Damit hat es endliche Kompositionsreihe nach ???. all diese Kompositionsreihen Vereinigen ergibt Kompositionsreihe von  $R/\mathfrak{m}^n$ . Also hat  $R/\mathfrak{m}^n$  endliche Länge und ist artinsch. □

*Beweis.* Nach Satz Satz 10.5.12  $R$  ein  $R$ -Modul von endlicher Länge. Nach Satz Satz 10.5.10 ist  $R \cong \prod R_{\mathfrak{p}}$  wobei  $\mathfrak{p}$  maximal ist. □

**Lemma 10.5.16.** *Sei  $R$  ein Hauptidealring und  $a \in R \setminus \{0\}$ .*

1. *Es ist  $\text{length}(R/aR)$  gleich der Anzahl der Primfaktoren in der Primfaktorzerlegung von  $a$ .*
2. *Wenn  $M$  endlich erzeugter  $R$ -Modul ist und  $M[a] = \{m \in M \mid am = 0\}$  dann sei*

$$h_a(M) = \text{length}(M/aM) - \text{length}(M[a]).$$

*Alle Zahlen in der Gleichung sind endlich.*

3. *Wenn  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  exakt ist von endlichen  $R$ -Moduln, dann ist  $h_a(M) = h_a(M') + h_a(M'')$ .*
4. *Sei  $K = \text{Quot}(R)$  und  $M$  ein endlich-erzeugter  $R$ -Modul. Dann ist*

$$h_a(M) = \dim_K(M \otimes_R K) \cdot \text{length}(R/aR)$$

*Beweis.* 1. Sei  $a = p_1 \cdots p_r$  die Primfaktorzerlegung. Dann ist

$$(p_1) \supseteq (p_1 p_2) \supseteq \cdots \supseteq (p_1 \cdots p_r) = (a)$$

und

$$(p_1 \cdots p_k)/(p_1 \cdots p_{k+1}) \cong R/p_{k+1}R$$

ein Körper, hat also keine echten Untermoduln ungleich 0. Somit ist

$$(\bar{p}_1) \supseteq (\bar{p}_1 \bar{p}_2) \supseteq \cdots \supseteq (\bar{p}_1 \cdots \bar{p}_r) = 0$$

Kompositionsreihe in  $R/aR$ . Also ist  $\text{length}(R/aR) = r$ .

2. Da  $M$  endlich erzeugt ist, ist  $M$  noethersch. Also ist  $M[a]$  auch endlich erzeugt. Es ist

$$M[a] \cong R^d \oplus \bigoplus R/a_i R$$

und da  $M[a]$  Torsionsmodul ist, ist  $d = 0$ . Nach 1. ist  $\text{length}(R/a_i R) < \infty$  also auch die  $\text{length}(M[a]) < \infty$ .  $M/aM$  ist auch endlich erzeugt und Torsionsmodul. Also ist analog die Länge auch endlich.

3. Betrachte kommutatives Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow \cdot a & & \downarrow \cdot a & & \downarrow \cdot a & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Nach Schlangenlemma gibt das eine exakte Sequenz

$$0 \rightarrow M'[a] \rightarrow M[a] \rightarrow M''[a] \rightarrow M'/aM' \rightarrow M/aM \rightarrow M''/aM'' \rightarrow 0$$

Es gilt

$$0 = \text{length}(M'[a]) - \text{length}(M[a]) + \text{length}(M''[a]) - \text{length}(M'/aM') + \text{length}(M/aM) - \text{length}(M''/aM'') \rightarrow 0$$

Also gilt die Aussage.

4. Nach 3. reicht es, die Aussage für  $M = R$  und  $M$  Torsionsmodul zu zeigen wegen Struktursatz ????. Es ist  $\dim(R \otimes_R K) = 1$  und  $R[a] = 0$  also ist  $h_a(R) = \text{length}(R/aR) = \dim(R \otimes_R K) \cdot \text{length}(R/aR)$ . Wenn  $M$  Torsionsmodul ist, dann hat  $M$  endliche Länge nach Struktursatz und somit ergibt die exakte Sequenz

$$0 \rightarrow M[a] \rightarrow M \xrightarrow{\cdot a} M \rightarrow M/aM \rightarrow 0$$

dass

$$0 = \text{length}(M[a]) - \text{length}(M) + \text{length}(M) - \text{length}(M/aM) = h_a(M)$$

. und

$$\dim(M \otimes_R K) = 0$$

□

## 10.6 Support und Assoziierte Primideale

**Definition 10.6.1.** Sei  $M$  ein  $A$ -Modul. Der Träger von  $M$  ist die Teilmenge

$$\text{Supp}(M) = \{\mathfrak{p} \in \text{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\} \subseteq \text{Spec}(A).$$

Für  $m \in M$  ist der Annihilator das Ideal  $\text{Ann}(m) := \{f \in A \mid fm = 0\}$ . Es ist  $\text{Ann}(M) = \{f \in A \mid fM = 0\}$ .  $f \in A$  heißt Nullteiler von  $M$  falls  $fm = 0$  für ein  $m \neq 0$  in  $M$ .

**Beispiel 10.6.2.** 1. Wenn  $R = \mathbb{Z}$  ist und  $M = \mathbb{Q}$  dann ist  $\mathbb{Q}_{\mathfrak{p}} = \mathbb{Q}$  also ist  $\text{Supp}(M) = \text{Spec}(\mathbb{Z})$ .

2. Wenn  $M = \mathbb{Q}/\mathbb{Z}$  ist dann ist  $(\mathbb{Q}/\mathbb{Z})_p = \mathbb{Q}_p/\mathbb{Z}_p = \begin{cases} 0 & p = 0 \\ \neq 0 & p \neq 0 \end{cases}$  Also ist  $\text{Supp}(M) = (\text{Spec}(\mathbb{Z}) \setminus \{0\})$ .

**Satz 10.6.3.** Sei  $M$  ein  $R$ -Modul.

1. Wenn  $M = Rx$  für ein  $x \in M$  dann ist  $\text{Supp}(M) = V(\text{Ann}(x))$ .
2. Wenn  $M = \sum_{i \in J} M_i$ , dann ist  $\text{Supp}(M) = \bigcup_{i \in J} \text{Supp}(M_i)$
3. Wenn  $L \subseteq M$  und  $N = M/L$  dann ist  $\text{Supp}(M) = \text{Supp}(L) \cup \text{Supp}(N)$
4. wenn  $M$  endlich erzeugt ist, dann ist  $\text{Supp}(M) = V(\text{Ann}(M))$  eine abgeschlossene Menge.
5. Wenn  $\mathfrak{p} \in \text{Supp}(M)$ , dann ist  $V(\mathfrak{p}) \subseteq \text{Supp}(M)$ .

*Beweis.*

1. Es ist

$$\begin{aligned} \frac{x}{1} = 0 \in M_{\mathfrak{p}} &\iff sx = 0 \text{ für ein } s \in R \setminus \mathfrak{p} \\ &\iff (R \setminus \mathfrak{p}) \cap \text{Ann}(x) \neq \emptyset \end{aligned}$$

$$\text{Also } \frac{x}{1} \neq 0 \iff \text{Ann}(x) \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\text{Ann}(x))$$

2. Klar, da  $M_i \subseteq M \implies (M_i)_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$
3. Folgt, da Lokalisierung exakt ist.
4. Folgt aus 1 und 2
5. Sei  $\mathfrak{p} \subseteq \mathfrak{q}$  Primideal. Es ist  $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}}$ . Also ist  $M_{\mathfrak{q}} \neq 0$ .

□

**Definition 10.6.4.** Sei  $M$  ein  $R$ -Modul. Ein assoziiertes Primideal von  $M$  ist ein Primideal  $\mathfrak{p} \subseteq R$  sodass es Untermodul  $N \subseteq M$  gibt sodass  $N \cong R/\mathfrak{p}$ . Äquivalent ist, dass es  $x \in M$  gibt sodass  $\mathfrak{p} = \text{Ann}(x)$  Primideal ist. Sei  $\text{Ass}(M)$  die Menge der assoziierten Primideale.

**Beispiel 10.6.5.**

1. Wenn  $R = \mathbb{Z}$  und  $M = \mathbb{Q}$  dann ist  $\text{Ass}(M) = \emptyset$  da es keine Inklusion  $\mathbb{F}_p \subseteq \mathbb{Q}$  gibt.
2. Wenn  $M = \mathbb{Q}/\mathbb{Z}$  ist, dann ist für  $p \neq 0$

$$p \cdot \frac{1}{p} = 0$$

sodass  $p = \text{Ann}(x)$ . Somit  $\text{Ass}(M) = \text{Spec}(\mathbb{Z}) \setminus \{0\} = \text{Supp}(M)$ .

3. Wenn  $R = k[X, Y]$  und  $M = R/(X^2, XY)$  dann sei  $a \in M$  sodass  $\text{Ann}(a)$  prim ist. Wenn  $a \in (x)$  dann ist  $\text{Ann}(a) = (X, Y)$  und wenn  $a \notin (x)$  dann ist  $\text{Ann}(a) = (x)$ . Also ist  $\text{Ass}(M) = \{(X), (X, Y)\}$ .

**Bemerkung 10.6.6.** Wenn  $\mathfrak{p} \in \text{Ass}(M)$  dann  $\text{Ann}(M) = \bigcap_{x \in M} \text{Ann}(x) \subseteq \mathfrak{p}$

**Beispiel 10.6.7.** Sei  $n = p^\alpha q^\beta \in \mathbb{Z}$  mit zwei verschiedenen Primzahlen  $p, q$  und  $\alpha, \beta \geq 1$ . Dann ist  $\text{Ass}(\mathbb{Z}/n\mathbb{Z}) = \{(p), [q]\}$ , denn  $m)p^{\alpha-1}q^\beta + n\mathbb{Z}$  hat  $\text{Ann}(m) = \mathfrak{p}$  und ähnlich für  $q$ .

**Satz 10.6.8.** Sei  $M$  ein  $R$ -Modul.

1. Sei  $\mathfrak{p} = \text{Ann}(x)$  prim für  $x \in M$ . Dann gilt

$$0 \neq y \in Rx \implies \text{Ann}(y) = \mathfrak{p}$$

2. Jedes maximale Element der Menge  $\{\text{Ann}(x) \mid 0 \neq x \in M\}$  ist Primideal, also in  $\text{Ass}(M)$ .
3. Wenn  $R$  noethersch ist, dann ist  $\text{Ass}(M) \neq \emptyset$  falls  $M \neq 0$ .
4. Wenn  $L \subseteq M, N = M/L$  dann ist  $\text{Ass}(M) \subseteq \text{Ass}(L) \cup \text{Ass}(N)$ .

*Beweis.* Es ist  $R/\mathfrak{p}$  Integritätsbereich. Wenn also  $y \neq 0 \in R/\mathfrak{p}$  Dann ist  $\text{Ann}(y) = \mathfrak{p}$ .

1. Angenommen  $\mathfrak{p} = \text{Ann}(x)$  maximal und  $f \cdot g \in \text{Ann}(x)$ . Dann ist  $fgx = 0$ . Wenn  $gx = 0$  dann ist  $g \in \mathfrak{p}$ . wenn  $0 \neq gx$ , dann ist  $\text{Ann}(x) \subseteq \text{Ann}(gx)$  also  $\text{Ann}(gx) = \text{Ann}(x)$  und dann  $f \in \text{Ann}(gx) = \text{Ann}(x)$ .
2. folgt mit 1.
3. Angenommen  $R/\mathfrak{p} \subseteq M$  Untermodul. Wenn  $R/\mathfrak{p} \cap L = 0$ , dann ist  $R/\mathfrak{p} + N$  Untermodul von  $N$  also  $\mathfrak{p} \in \text{Ass}(N)$ . Andernfalls gilt für alle  $x \neq 0 \in (R/\mathfrak{p}) \cap L$ :  $\text{Ann}(x) = \mathfrak{p}$  nach 1. Also ist  $\mathfrak{p} \in \text{Ass}(L)$ .

□

**Korollar 10.6.9.** wenn  $R$  noethersch ist, dann ist

$$\{\text{Nullteiler von } M\} = \bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p}$$

*Beweis.* Sei  $0 \neq m \in M$ . Jedes  $a \in \text{Ann}(m)$  ist in einem Ideal  $\text{Ann}(x)$  enthalten wobei  $\text{Ann}(x)$  maximal unter Annihilatoren. Also in  $\text{Ass}(M)$  nach Satz 10.6.8. □

**Beispiel 10.6.10.**  $N = M/L$  kann assoziierte Primideale haben, die nicht in  $\text{Ass}(M)$  liegen, zum Beispiel ist  $\text{Ass}(\mathbb{Z}/2\mathbb{Z}) = \{(2)\}$  aber  $(2) \notin \text{Ass}(\mathbb{Z})$ .

**Satz 10.6.11.** Es ist  $\text{Ass}(M) \subseteq \text{Supp}(M)$  Insbesondere  $\mathfrak{p} \in \text{Ass}(M) \implies V(\mathfrak{p}) \subseteq \text{Supp}(M)$  Wenn außerdem  $R$  noch noethersch, dann ist minimales Element  $\mathfrak{p} \in \text{Supp}(M)$  in  $\text{Ass}(M)$ . Insbesondere wenn  $V(\mathfrak{p}) \subseteq \text{Supp } M$  irreduzible Komponente ist, dann ist  $\mathfrak{p} \in \text{Ass}(M)$ .

*Beweis.* Es ist

$$(R/\mathfrak{p})_{\mathfrak{p}} \cong \text{Quot}(R/\mathfrak{p}) =: k(\mathfrak{p})$$

Da  $R/\mathfrak{p} \subseteq M$  folgt  $0 \neq k(\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$ . Somit ist  $\mathfrak{p} \in \text{Supp}(M)$ . Sei nun  $R$  noethersch.  $M_{\mathfrak{p}}$  ist  $R_{\mathfrak{p}}$ -Modul,  $M_{\mathfrak{p}} \neq 0$ . Also ist  $\text{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \neq \emptyset$ . Sei  $\mathfrak{q}' \subseteq R_{\mathfrak{p}}$  ein Primideal ungleich  $\mathfrak{p}R_{\mathfrak{p}}$ . Dann ist  $\mathfrak{q}' = \mathfrak{q}R_{\mathfrak{p}}$  für Primideal  $\mathfrak{q} \subseteq \mathfrak{p}$ . Also ist  $M_{\mathfrak{p}}_{\mathfrak{q}'} = M_{\mathfrak{q}} = 0$  für  $\mathfrak{q} \neq \mathfrak{p}$  da  $\mathfrak{p}$  minimal. Also ist  $\text{Supp}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = \{\mathfrak{p}R_{\mathfrak{p}}\}$  und dann

$$0 \neq \text{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \subseteq \text{Supp}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = \{\mathfrak{p}R_{\mathfrak{p}}\}$$

und also  $\text{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = \{\mathfrak{p}R_{\mathfrak{p}}\}$ . Das heißt es gibt  $0 \neq \frac{m}{s} \in M_{\mathfrak{p}}$  sodass  $\text{Ann}(\frac{m}{s}) = \mathfrak{p}R_{\mathfrak{p}}$ . Das heißt für alle  $f \in \mathfrak{p}$  gilt  $\frac{f}{1} \cdot \frac{m}{s} = 0$ . Also gibt es ein  $t \in R \setminus \mathfrak{p}$  sodass  $ftm = tfm = 0$ . Da  $\mathfrak{p} = (f_1, \dots, f_n)$  endlich erzeugt ist, gibt es  $t_i \in R \setminus \mathfrak{p}$  sodass  $f_i t_i m = 0$ . Dann ist  $t = \prod t_i$  ein Element in  $R \setminus \mathfrak{p}$  sodass  $ftm = 0$ . Also ist  $\mathfrak{p} \subseteq \text{Ann}(tm)$ . Andersrum wenn  $u \in R \setminus \mathfrak{p}$  mit  $utm = 0$  dann ist  $\frac{u}{1} \cdot \frac{t}{1} \frac{m}{1} = 0$  und da erstere beide eine Einheit sind, ist das ein Widerspruch. Also ist  $\text{Ann}(tm) \subseteq \mathfrak{p}$  und damit  $\mathfrak{p} = \text{Ann}(tm)$ . □

**Korollar 10.6.12.** Wenn  $R$  noethersch und  $M$  endlicher  $R$ -Modul ist, dann ist

$$\text{Supp}(M) = \bigcup_{i=1}^n V(\mathfrak{p}_i)$$

wobei die  $\mathfrak{p}_i$  endlich viele minimale Primideale sind, die  $\text{Ann}(M)$  enthalten. Jedes  $\mathfrak{p}_i$  ist assoziiertes Primideal.

*Beweis.*  $\text{Supp}(M) = V(\text{Ann}(M))$  und  $V(\text{Ann}(M))$  hat endlich viele minimale Elemente  $\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$  und  $V(\text{Ann}(M)) = \bigcup V(\mathfrak{p}_i)$  Nach letztem Satz ?? sind diese in  $\text{Ass}(M)$ . □

**Satz 10.6.13.** Sei  $R$  noethersch und  $M$  endlicher  $A$ -Modul. Es gibt Kette

$$0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_n = M$$

Untermodul sodass  $M_i/M_{i-1} \cong R/\mathfrak{p}_i$  mit  $\mathfrak{p}_i \in \text{Spec}(A)$ . Dann ist  $\text{Ass}(M) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ .

*Beweis.* Es ist  $\text{Ass}(M) \neq \emptyset$  also gibt es  $M_1 \subseteq M$  sodass  $M_1 = R/\mathfrak{p}_1$ . Fahre so fort mit  $M/M_i$ . Bekomme Kette in  $M$  durch Urbild nehmen von den entstehenden Moduln. Kette muss abbrechen, da  $A$  noethersch. □

**Beispiel 10.6.14.** Wenn  $R$  faktoriell ist und  $M = R/aR$  für ein  $a \in R$  dann gibt es drei Fälle. Wenn  $a$  eine Einheit ist, dann ist  $M = 0$  und also  $\text{Ass}(M) = \emptyset$ . Wenn  $a = 0$  dann ist  $M = R$  und dann  $\text{Ass}(M) = \{0\}$ . Wenn  $a$  weder 0 noch Einheit ist, ist  $a = p_1 \dots p_r$  für Primelemente  $p_i$ . sei  $M_i = p_1 \dots p_i \cdot R/aR$ . Diese bilden absteigende Kette mit

$$M_{i-1}/M_i \cong R/p_iR.$$

Also ist  $\text{Ass}(M) = \{p_1, \dots, p_r\} = \text{Supp}(M)$ .

## Teil IV

# Algebraische Zahlentheorie

# Kapitel 11

## Grundlagen

### 11.1 Quadratzahlen mod $p$

**Bemerkung 11.1.1.** Sei  $n = k \cdot \ell$  natürliche Zahlen. Dann ist

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot k} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot \ell} \mathbb{Z}/n\mathbb{Z}$$

exakt, das heißt

$$\{a \in \mathbb{Z}/n\mathbb{Z} \mid \ell a = 0\} = \{k \cdot b \mid b \in \mathbb{Z}/n\mathbb{Z}\}$$

denn für  $x \in \mathbb{Z}$  ist  $n \mid \ell x \iff k \mid x$ .

**Bemerkung 11.1.2.** Es ist  $(\mathbb{F}_p^*, \cdot) \cong (\mathbb{Z}/(p-1), +)$ ,  $1 \mapsto 0$  nach Satz ???. Wenn also  $p-1 = n = k\ell$  dann ist  $\{a \in \mathbb{F}_p^* \mid a^k = 1\} = \{b^\ell \mid b \in \mathbb{F}_p^*\}$ . Wenn also  $p \geq 3$  dann ist  $p-1 = 2 \cdot \frac{p-1}{2}$ . Also ist

$$\{b^2 \mid b \in \mathbb{F}_p^*\} = \{a \in \mathbb{F}_p^* \mid a^{\frac{p-1}{2}} = 1\}.$$

**Definition 11.1.3** (Legendre Symbol). Sei  $p$  prim und  $a \in \mathbb{Z}$ . Dann ist das Legendre Symbol gegeben durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ und } a \text{ Quadratzahl in } \mathbb{F}_p \\ -1 & p \nmid a \text{ und } a \text{ keine Quadratzahl in } \mathbb{F}_p \end{cases}$$

**Lemma 11.1.4.**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

*Beweis.* Wenn  $\left(\frac{a}{p}\right) = -1$  dann ist  $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1$  in  $\mathbb{F}_p$ . also  $a^{\frac{p-1}{2}} \in \{\pm 1\}$  aber  $a^{\frac{p-1}{2}} \neq 1$  da sonst  $a$  ein Quadrat.  $\square$

**Lemma 11.1.5.**

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & 4 \mid p-1 \iff p \equiv 1 \pmod{4} \\ -1 & 4 \nmid p-1 \iff p \equiv 3 \pmod{4} \end{cases}$$

**Lemma 11.1.6.** Wenn  $p \equiv 1 \pmod{4}$  dann ist  $-1 \in \mathbb{F}_p$  eine Quadratzahl.

*Beweis.*  $\square$

### 11.2 Primzahlen in $\mathbb{Z}[i]$

**Bemerkung 11.2.1.** Für  $z \in \mathbb{Z}[i]$  definiere  $N(z) = z \cdot \bar{z}$ . Damit wird  $\mathbb{Z}[i]$  ein Euklidischer Ring bzgl  $N$ . Es ist  $N(zw) = N(z)N(w)$  und  $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$ .

**Satz 11.2.2.** Eine Primzahl  $p \in \mathbb{N}$  hat eine Darstellung  $p = a^2 + b^2$  mit  $a, b \in \mathbb{N}$  genau dann wenn  $p = 2$  oder  $p \equiv 1 \pmod{4}$ .

*Beweis.* Für alle  $x \in \mathbb{N}$  gilt  $x^2 \equiv 0 \pmod{4}$  oder  $x^2 \equiv 1 \pmod{4}$ . wenn also  $p = x^2 + y^2$  ist, dann ist  $p \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases} \pmod{4}$ . Also ist eine Richtung gezeigt. Sei andererseits  $p \equiv 1 \pmod{4}$ . Wähle  $x$  sodass  $x^2 \equiv -1 \pmod{p}$  nach ?? Das heißt  $p \mid x^2 + 1 = (x+i)(x-i)$  in  $\mathbb{Z}[i]$ . Aber  $p \nmid x \pm i$  da  $\frac{x \pm i}{p} = \frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$ . Somit ist  $p$  nicht prim in  $\mathbb{Z}[i]$ . Da  $\mathbb{Z}[i]$  Euklidisch, ist es faktoriell nach ?? somit ist  $p$  nicht irreduzibel. das heißt  $p = z \cdot w$  für  $z, w \in \mathbb{Z}[i]$  keine Einheiten. Dann ist  $p^2 = N(p) = N(z)N(w)$  und  $N(z), N(w) \neq 1$  also  $p = N(z) = N(w)$ . Wenn  $z = a + bi$  dann ist  $p = N(z) = a^2 + b^2$ .  $\square$

**Satz 11.2.3.** Primelemente in  $\mathbb{Z}[i]$  sind

1. Primzahlen  $p \in \mathbb{Z}$  mit  $p \equiv 3 \pmod{4}$
2.  $a + bi \in \mathbb{Z}[i]$  mit  $a^2 + b^2 = p$  und  $p = 2$  oder  $p \equiv 1 \pmod{4}$ .

*Beweis.* Ähnliche Rechnung.  $\square$

**Beispiel 11.2.4** (Pellsche Gleichung). Fixiere  $N \in \mathbb{N}$  und  $N$  sei keine Quadratzahl. Suche  $a, b \in \mathbb{N}$  sodass  $a^2 - Nb^2 = 1$ .

**Lemma 11.2.5.** Sei  $R = \mathbb{Z}[\sqrt{N}] = \{a + b\sqrt{N} \mid a, b \in \mathbb{Z}\}$ .  $z = a + b\sqrt{N} \in R^* \iff a^2 - Nb^2 = \pm 1$

**Beispiel 11.2.6.** Sei  $R = \mathbb{Z}[\sqrt{2}]$ . Die Norm von  $x = a + b\sqrt{2}$  ist definiert als  $N(x) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ . Es ist  $x \in R$  eine Einheit genau dann wenn  $N(x) = \pm 1$ . Denn wenn  $x \cdot \bar{x} = N(x) = \pm 1$  dann ist  $\pm \bar{x}$  das Inverse zu  $x$ , wobei  $\bar{x} = a - b\sqrt{2}$  ist. Es ist jede Einheit  $u = a + b\sqrt{2}$  von  $R$  von der Form  $\pm(1 + \sqrt{2})^n$  für  $n \in \mathbb{Z}$ .

Induktion über  $n = |a + b|$ . Wenn  $n = 0$  dann ist  $a = -b$  sodass  $u = b(-1 + \sqrt{2})$ . Da  $-1 + \sqrt{2} = (1 + \sqrt{2})^{-1}$  ist muss  $b = \pm 1$  sein also hat es die gewünschte Form. Sei  $n = |a + b| > 0$ . Wenn  $a, b$  verschiedene Vorzeichen haben sei  $u' = \frac{a - b\sqrt{2}}{N(u)} = \pm(a - b\sqrt{2})$  und  $uu' = \pm 1$  und ersetze  $u$  durch  $u'$ . Wenn  $a, b$  beide negativ sind, ersetze  $u$  durch  $-u$ . Also ohne Einschränkung  $a, b > 0$ . Dann ist  $u' = u(-1 + \sqrt{2}) = (-a + 2b) + (a - b)\sqrt{2}$  eine Einheit, da  $-1 + \sqrt{2} = (1 + \sqrt{2})^{-1}$ . Sei  $c = -a + 2b$  und  $d = a - b$ . Dann ist  $|c + d| = |b| < |a + b|$ . Nach Induktion hat  $u'$  die gewünschte Form und damit auch  $u$ . Das zeigt, dass  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \cong R^*$ ,  $(n + 2\mathbb{Z}, m) \mapsto (-1)^n(1 + \sqrt{2})^m$ .

## 11.3 Zahlkörper

**Definition 11.3.1.** Ein Zahlkörper ist eine endliche Erweiterung  $K/\mathbb{Q}$ . Wenn  $K$  ein Zahlkörper ist, dann ist der Ring der ganzen Zahlen von  $K$  gegeben durch

$$\mathbb{O}_K = \{z \in K \mid z \text{ ganz über } \mathbb{Z}\}$$

Also  $\mathbb{O}_K$  ist der ganze Abschluss von  $\mathbb{Z}$  in  $K$ .

**Beispiel 11.3.2.** Sei  $K$  ein quadratischer Zahlkörper,  $K = \mathbb{Q}(\sqrt{d})$  für ein quadratfreies  $d \in \mathbb{Z}$ . Sei  $x = a + b\sqrt{d} \in K$  mit  $a, b \in \mathbb{Q}$ . Wenn  $b = 0$  dann ist  $x$  ganz über  $\mathbb{Z}$  genau dann wenn  $a \in \mathbb{Z}$ . Wenn  $b \neq 0$  dann ist das Minimalpolynom von  $x$  gegeben durch  $X^2 - 2aX + (a^2 - db^2)$ .  $x$  ist nach ??? ganz über  $\mathbb{Z}$  genau dann wenn  $-2a, a^2 - db^2 \in \mathbb{Z}$  also genau dann wenn  $a, b \in \mathbb{Z}$  oder  $a, b \in \frac{1}{2} + \mathbb{Z}$  und  $d \equiv 1 \pmod{4}$ . Das heißt

$$\mathbb{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod{4} \\ \mathbb{Z}[\frac{\sqrt{d+1}}{2}] & d \equiv 1 \pmod{4} \end{cases}$$

**Bemerkung 11.3.3.** Aus ??? folgt, dass  $\mathbb{O}_K$  ein endlicher  $\mathbb{Z}$ -Modul ist. Da  $\mathbb{O}_K$  torsionsfrei ist folgt mit ???  $\mathbb{O}_K \cong \mathbb{Z}^n$  als  $\mathbb{Z}$ -Modul.

**Definition 11.3.4.** Eine  $\mathbb{Z}$ -Basis von  $\mathbb{O}_K$  heißt Ganzheitsbasis von  $K$ .

**Lemma 11.3.5.** Jede Ganzheitsbasis ist eine  $\mathbb{Q}$ -Basis von  $K$  und  $\mathbb{O}_K \cong \mathbb{Z}^n$  mit  $n = [K : \mathbb{Q}]$ .



*Beweis.* Seien  $a_1, \dots, a_n \in \mathbb{O}_K$  eine Ganzheitsbasis. Dann sind sie auch  $\mathbb{Q}$ -linear unabhängig. Sei  $y \in K$  mit  $f \in \mathbb{Q}[X]$  Minimalpolynom. Sei  $b$  der gemeinsame Nenner aller Koeffizienten von  $f$ . Dann ist  $by$  ganz also in  $\mathbb{O}_K$ . somit ist  $y \in \mathbb{Q} \cdot \mathbb{O}_K$ .  $\square$

**Beispiel 11.3.6.** Wenn  $K = \mathbb{Q}(\sqrt{d})$  mit  $d$  quadratfrei, dann ist falls  $d \equiv 1 \pmod{4}$  eine Ganzheitsbasis gegeben durch  $1, \frac{\sqrt{d}+1}{2}$  und falls  $d \not\equiv 1 \pmod{4}$  gegeben durch  $1, \sqrt{d}$ .

**Definition 11.3.7.** Sei  $L/K$  eine Körpererweiterung. Definiere die Spur von  $b \in L$  durch

$$\text{Tr}_{L/K}(b) = \text{Tr}(b: L \rightarrow L)$$

und die Norm von  $b \in L$  durch

$$N_{L/K}(b) = \det(b: L \rightarrow L)$$

**Lemma 11.3.8.** Wenn  $L/K$  separabel, dann ist für  $b \in L$  und  $\Sigma = \{\sigma: L \rightarrow \bar{K} \mid \sigma|_K = \text{id}\}$ :

$$\text{Tr}_{L/K}(b) = \sum_{\sigma \in \Sigma} \sigma(b)$$

$$N_{L/K}(b) = \prod_{\sigma \in \Sigma} \sigma(b)$$

*Beweis.* Wenn  $L = K(b)$  und  $f$  das Minimalpolynom von  $b$  ist, dann ist  $f = \mu_b \mid \chi_b$  und  $n = [L : K] = \deg(f) = \deg(\chi_b)$  also ist  $\chi_b = f$ . Die  $\sigma(b)$  sind paarweise verschiedene Nullstellen von  $f$  da  $b$  separabel. Da Separabilitätsgrad gleich Körpergrad, ist  $|\Sigma| = n$ . Somit teilt  $\prod_{\sigma \in \Sigma} (X - \sigma(b)) \mid f$  und weil beide gleiche Grade haben sind sie gleich und Aussage folgt. Wenn  $L$  allgemein, sei  $M = K(b)$ . Jedes  $\sigma': M \rightarrow \bar{K}$  hat genau  $r = [L : M]$  Fortsetzungen zu  $\sigma: L \rightarrow \bar{K}$  nach ????. Also ist  $\prod_{\sigma \in \Sigma} (X - \sigma(b)) = \prod_{\sigma' \in \Sigma'} (X - \sigma'(b))^r$  mit  $\Sigma' = \{\sigma': M \rightarrow \bar{K}\}$ . Es ist  $L = M^r$  als  $M$  Vektorraum und  $b \in M$  respektiert die Summenzerlegung. Also ist  $\chi_b: L \rightarrow L = (\chi_b: M \rightarrow M)^r$ .  $\square$

**Korollar 11.3.9.** Seien  $M/L/K$  separable Körpererweiterungen und  $b \in M$ . Dann

$$\text{Tr}_{M/K}(b) = \text{Tr}_{L/K}(\text{Tr}_{M/L}(b))$$

$$N_{M/K}(b) = N_{L/K}(N_{M/L}(b))$$

*Beweis.* Genau wie in ???  $\square$

**Definition 11.3.10.** Sei  $L/K$  endliche separable Körpererweiterung und  $a_1, \dots, a_n$  eine  $K$ -Basis. Die Diskriminante von  $a_1, \dots, a_n$  sei

$$d(a_1, \dots, a_n) = \det(\text{Tr}_{L/K}(a_i a_j)_{ij})$$

das heißt die Determinante der Darstellenden Matrix bzgl der Bilinearform  $L \times L \rightarrow K, (a, b) \mapsto \text{Tr}_{L/K}(ab)$ .

**Bemerkung 11.3.11** (Basiswechsel). Wenn  $a_1, \dots, a_n$  und  $b_1, \dots, b_n$  zwei  $K$ -Basen und  $S$  die Übergangsmatrix ist, dann ist

$$d(b_1, \dots, b_n) = \det(S^T \text{Tr}(a_i a_j)_{ij} S) = \det(S)^2 d(a_1, \dots, a_n)$$

**Lemma 11.3.12.** Wenn  $A = \text{Tr}(a_i a_j)_{ij}$  Dann ist  $A = B^t B$  für  $B = \sigma_i(a_j)_{i,j} \in M_n(\bar{K})$  mit wobei  $\sigma_i$  die verschiedenen  $K$ -Homomorphismen  $L \rightarrow \bar{K}$ .

*Beweis.* Nach ?? ist

$$(B^t B)_{ik} = \sum_{j=1}^n \sigma_j(a_i) \sigma_j(a_k) = \sum_{j=1}^n \sigma_j(a_i a_k) = \text{Tr}_{L/K}(a_i a_k) = A_{ik}$$

$\square$

**Korollar 11.3.13.**  $d(a_1, \dots, a_n) = \det(A) = \det(B)^2$

**Satz 11.3.14.**  $d(a_1, \dots, a_n) \neq 0$  also ist  $(a, b) \mapsto \text{Tr}_{L/K}(ab)$  nicht ausgeartet.

*Beweis.* Das folgt eigentlich schon direkt aus ??? Alternativ: Nach [Satz vom primitiven Element](#) ist  $L = K(b)$ . Das heißt eine  $K$  basis von  $L$  ist  $1, b, b^2, \dots, b^{n-1}$  mit  $n = [L : K]$ . Sei

$$B = \begin{pmatrix} 1 & \dots & 1 \\ \sigma_1(b) & & \vdots \\ \vdots & & \vdots \\ \sigma_1(b)^{n-1} & & \sigma_n(b)^{n-1} \end{pmatrix} \quad \text{Nach ??? ist } \det(B) = \prod_{i < j} (\sigma_i(b) - \sigma_j(b)) \neq 0. \quad \square$$

**Bemerkung 11.3.15.** Angenommen  $A \subset K$  Teilring und  $a_1, \dots, a_n \in L$  ganz über  $A$ . Dann ist  $\sigma_i(a_j)$  ganz über  $A$  und damit  $\det(B)$  ganz über  $A$ . Also ist Diskriminante  $d(a_1, \dots, a_n)$  ganz über  $A$ .

**Definition 11.3.16.** Sei  $K/\mathbb{Q}$  endlich und  $a_1, \dots, a_n \in \mathbb{O}_K$  Ganzheitsbasis. Diskriminante von  $K$  ist  $d_K = d(a_1, \dots, a_n) = \det(\text{Tr}_{K/\mathbb{Q}}(a_i a_j))$ . Eine Basiswechselmatrix  $S$  zu einer anderen Ganzheitsbasis ist über  $\mathbb{Z}$  also ist hat Determinante  $\pm 1$  also ist nach ???  $d_K$  wohldefiniert.

**Beispiel 11.3.17.** Sei  $K = \mathbb{Q}(\sqrt{d})$  und  $d$  quadratfrei. Wenn  $d \not\equiv 1 \pmod{4}$ , dann ist  $1, \sqrt{d}$  eine Ganzheitsbasis nach ??? Also ist  $B = (\sigma_i(a_j))_{ij} = \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}$  und  $d_K = \det(B)^2 = 4d$ . Wenn  $d \equiv 1 \pmod{4}$ , dann ist  $1, \frac{\sqrt{d+1}}{2}$  eine Ganzheitsbasis nach ??? Also ist  $B = (\sigma_i(a_j))_{ij} = \begin{pmatrix} 1 & 1 \\ \frac{\sqrt{d+1}}{2} & -\frac{\sqrt{d+1}}{2} \end{pmatrix}$  und  $d_K = \det(B)^2 = d$ .

**Lemma 11.3.18.** sei  $(0) \neq I \subseteq \mathbb{O}_K$  ein Ideal. Dann ist  $I \cong \mathbb{Z}^n$  als  $\mathbb{Z}$ -Modul und  $n = [L : K]$ .

*Beweis.* Wähle  $a \in I$  mit  $a \neq 0$ . Dann ist  $a\mathbb{O}_K \subseteq I \subseteq \mathbb{O}_K$ . Da  $a\mathbb{O}_K \cong \mathbb{Z}^n$  ist  $I \cong \mathbb{Z}^n$ .  $\square$

**Definition 11.3.19.** Definiere  $d(I) = d(b_1, \dots, b_n)$  für eine  $\mathbb{Z}$ -Basis  $b_1, \dots, b_n$  von  $I$ . Wenn  $a_1, \dots, a_n$  Ganzheitsbasis und  $S$  Übergangsmatrix, dann ist  $d(I) = \det(S)^2 d_K$  mit  $\det(S) \neq 0$  über  $\mathbb{Q}$  invertierbar.

**Lemma 11.3.20.**

$$|\det(S)| = |\mathbb{O}_K/I|$$

und somit  $d(I) = |\mathbb{O}_K/I|^2 d_K$ .

**Beispiel 11.3.21.** Sei  $K = \mathbb{Q}(\zeta_p)$  für eine primitive  $p$ -te Einheitswurzel  $\zeta_p$ . Es ist  $\Sigma = \{\sigma : K \rightarrow \bar{\mathbb{Q}}\} = \{\sigma_i \mid \sigma_i(\zeta_p) = \zeta_p^i\}$ . Also ist

$$\text{Tr}_{K/\mathbb{Q}}(\zeta_p) = \sum_{i=1}^{n-1} b^i = -1 + \sum_{i=0}^{n-1} b^i = -1 + \frac{\zeta_p^p - 1}{\zeta_p - 1} = -1$$

und Es ist  $K = \mathbb{Q}(1 - \zeta_p)$  daher hat das Minimalpolynom von  $1 - \zeta_p$  Grad  $p - 1$ . Dann ist  $f(X) = \frac{(1-X)^p - 1}{X} = -\frac{(1-X)^p - 1}{(1-X) - 1} = -(1 + (1-X)^1 + \dots + (1-X)^{p-1}) \in \mathbb{Q}[X]$  das Minimalpolynom denn  $f(1 - \zeta_p) = 0$  und  $f$  hat Grad  $p - 1$  und ist normiert. Somit ist  $f$  auch das Charakteristische Polynom  $\chi_{\zeta_p}$ . Es ist  $f(0) = -p$ . Somit ist  $N_{L/K}(1 - \zeta_p) = p$ .

**Beispiel 11.3.22.** Sei  $K = \mathbb{Q}(\sqrt[3]{2})$  mit Ganzheitsbasis  $1, \sqrt[3]{2}, \sqrt[3]{4}$ . Es ist  $\Sigma = \{\sigma_k \mid b \mapsto b \cdot e^{\frac{2\pi i k}{3}}, k = 0, 1, 2\}$  Dann ist

$$B = (\sigma_i(b^j))_{ij} = \begin{pmatrix} 1 & 1 & 1 \\ \sqrt[3]{2} & \sqrt[3]{2}e^{\frac{2\pi i 1}{3}} & \sqrt[3]{2}e^{\frac{2\pi i 2}{3}} \\ \sqrt[3]{4} & \sqrt[3]{4}e^{\frac{2\pi i 1}{3}} & \sqrt[3]{4}e^{\frac{2\pi i 2}{3}} \end{pmatrix}$$

und  $d_K = \det(B)^2 = (-3i2\sqrt{3})^2 = -3^3 \cdot 2^2$ . Alternativ: Wenn  $a_1 = 1, a_2 = b, a_3 = b^2$  Ganzheitsbasis ist, Dann ist  $\{a_i a_j \mid i, j = 1, 2, 3\} = \{1, b, b^2, 2\}$ . Es ist  $b : K \rightarrow K$  ist dargestellt durch

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Also ist  $\text{Tr}(b) = 0$ .  $b^2 : K \rightarrow K$  ist dargestellt durch

$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

hat also auch  $\text{Tr}(b^2) = 0$ . Es ist  $\text{Tr}(1) = 3$  und  $\text{Tr}(2) = 2\bar{3}$ . Also ist

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix}$$

und somit  $d_K = \det(A) = -3^3 \cdot 2^2$ .

**Beispiel 11.3.23.** Seien

$$a = \sqrt[3]{1 + \sqrt[4]{2 + \sqrt{7}}}, b = \sqrt[3]{1 + \sqrt[4]{2 + \frac{1}{2}\sqrt{7}}}, c = \frac{3 + 2\sqrt{6}}{1 - \sqrt{6}}$$

Es ist  $f(X) = ((X^3 - 1)^4 - 2)^2 - 7 \in \mathbb{Z}[X]$  und  $f(a) = 0$  also ist  $a$  ganz über  $\mathbb{Z}$ . Angenommen  $b$  wäre ganz über  $\mathbb{Z}$ . Dann auch  $((b^3 - 1)^4 - 2)^2 = \frac{7}{4}$  was nicht richtig ist da  $\mathbb{Z}$  ganzabgeschlossen in  $\mathbb{Q}$ . Es ist  $c = -(\sqrt{6} + 3)$  und  $\sqrt{6}$  ist ganz da  $\sqrt{6}^2 - 6 = 0$  und 3 ist ganz. Also ist auch  $c$  ganz.

**Lemma 11.3.24.** Sei  $G$  eine topologische Gruppe. Dann gilt:

1. Für eine normale Untergruppe  $H \subseteq G$  ist  $G/H$  eine topologische Gruppe.
2. Wenn  $K \subseteq H \subseteq G$  normale Untergruppen sind, dann ist die Teilraumtopologie  $H/K \subseteq G/K$  die gleiche wie die Quotiententopologie.
3. Sei  $G$  Hausdorff. Dann

$$G/H \text{ Hausdorff} \iff H \subseteq G \text{ abgeschlossen}$$

4. Sei  $H \subseteq \mathbb{R}^n$  abgeschlossen. Es gilt

$$\mathbb{R}^n/H \text{ kompakt} \iff B \subseteq \mathbb{R}^n \text{ beschränkte Menge s.d. } B + H = \mathbb{R}^n$$

*Beweis.* 1. Klar.

2. Die Abbildung  $H \rightarrow H/K$  wobei  $H/K$  Unterraumtopologie hat ist stetig. Wenn also  $U$  offen in Unterraumtopologie dann auch in Quotiententopologie. Sei  $U$  offen in Quotiententopologie,  $\pi_H: H \rightarrow H/K$ ,  $\pi_G: G \rightarrow G/K$  Projektion. Das heißt es gibt ein  $V \subseteq G$  offen sodass  $V \cap H = \pi_H^{-1}(U)$ . Es ist

$$\pi_G^{-1}(V/K) = V \cdot K = \bigcup_{k \in K} V \cdot k$$

offen, also  $V/K \subseteq G/K$  offen. Es ist  $V/K \cap H/K = (V \cap H)/K = U$ . Also ist  $U$  offen in Unterraumtopologie.

3. Sei  $G/H$  Hausdorff,  $\pi: G \rightarrow G/H$ . Es ist  $eH$  abgeschlossen in  $G/H$  da Einpunktmengen immer abgeschlossen sind in Hausdorff. Also ist  $H = \pi^{-1}(eH) = H$  abgeschlossen. Sei andererseits  $H$  abgeschlossen. Betrachte  $G \times G \rightarrow G/H \times G/H$ . Das ist offen da  $\pi$  offen ist (Topologische Gruppen). Sei  $W = \{(x, y) \in G \times G \mid x^{-1}y \in G \setminus H\}$ . Das ist offen da  $G$  topologische Gruppe. Es ist  $(\pi \times \pi)(W) = G/H \times G/H \setminus \{\text{Diagonale}\}$ . Also ist die Diagonale abgeschlossen in  $G/H \times G/H$  also  $G/H$  Hausdorff.
4. Sei  $H \subseteq \mathbb{R}^n$  abgeschlossen und  $\pi: \mathbb{R}^n \rightarrow \mathbb{R}^n/H$  die Projektion. Angenommen  $\mathbb{R}^n/H$  kompakt das heißt  $\mathbb{R}^n \setminus H = \bigcup_{i=1}^m \pi(B_k(0))$  für ein  $m$ . Dann ist  $\mathbb{R}^n = \bigcup_{k=1}^m B_k(0) + H$ . wenn andererseits  $\mathbb{R}^n = B + H$  wobei  $B$  beschränkt, dann ist ohne Einschränkung  $B$  abgeschlossen also kompakt. Da  $\pi(B) = \mathbb{R}^n/H$  ist ist auch  $\mathbb{R}^n/H$  kompakt.

□

# Kapitel 12

## Minkowski Theorie

**Definition 12.0.1.** Sei  $V$  ein endlich-dimensionaler  $\mathbb{R}$ -Vektorraum.

1. Eine Untergruppe  $\Lambda \subseteq V$  ist ein Gitter, wenn jede  $\mathbb{Z}$ -lineare unabhängige Menge in  $\Lambda$  in  $V$   $\mathbb{R}$ -linear unabhängig ist.
2. Ein Gitter  $\Lambda \subseteq V$  ist vollständig, wenn  $\Lambda$   $V$  als  $\mathbb{R}$ -Vektorraum erzeugt.

**Beispiel 12.0.2.**  $\mathbb{Z}^n \subseteq \mathbb{R}^n$  ist vollständiges Gitter.  $\mathbb{Z}[i] \subseteq \mathbb{C}$  ist vollständiges Gitter mit Basis  $1, i$ . Aber  $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$  ist kein Gitter.

**Bemerkung 12.0.3.** Sei  $\Lambda \subseteq V$  und  $\alpha: \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \rightarrow V, (x, v) \mapsto xv$ . Es ist  $\Lambda$  ein Gitter  $\iff \alpha$  injektiv ist.  $\Lambda$  ist vollständiges Gitter  $\iff \alpha$  bijektiv.

Wenn  $\Lambda \subseteq V$  vollständiges Gitter ist, dann gibt eine Wahl von Basis von  $\Lambda$  und

$$\begin{array}{ccc} \Lambda & \hookrightarrow & V \\ \parallel & & \parallel \\ \mathbb{Z}^n & \hookrightarrow & \mathbb{R}^n \end{array}$$

**Satz 12.0.4.** Sei  $V$  ein  $\mathbb{R}$ -Vektorraum.

1. Eine Untergruppe  $\Lambda \subseteq V$  ist Gitter iff  $\Lambda$  ist diskret in  $V$ .
2. Ein Gitter  $\Lambda \subseteq V$  ist vollständig iff  $V/\Lambda$  ist kompakt.

*Beweis.* 1. Wenn  $\Lambda$  Gitter dann ist es diskret da  $\mathbb{Z}^n \subseteq \mathbb{R}^n$  diskret ist. Sei also  $\Lambda \subseteq V$  diskret. Ersetze  $V$  durch  $\mathbb{R} \cdot \Lambda$  und wähle  $\mathbb{R}$ -Basis  $v_1, \dots, v_n \in \Lambda$ . Sei  $\Lambda_0 = \langle v_1, \dots, v_n \rangle_{\mathbb{Z}}$ . Dann ist  $\Lambda_0$  Gitter in  $V$ . Es ist  $\Lambda/\Lambda_0 \subseteq V/\Lambda_0$  wobei die Quotiententopologie gleich der Teilraumtopologie ist nach ???. Da  $\Lambda \subseteq V$  diskret, ist  $\Lambda/\Lambda_0 \subseteq V/\Lambda_0$  diskret. Da  $\Lambda_0 \subseteq V$  vollständiges Gitter ist, ist  $V/\Lambda_0$  kompakt nach (2). Also ist  $\Lambda/\Lambda_0$  auch kompakt da  $\Lambda/\Lambda_0 \subseteq V/\Lambda_0$  abgeschlossen denn  $\Lambda \subseteq V$  ist diskrete Untergruppe einer Hausdorff Gruppe. Also ist zusammen  $\Lambda/\Lambda_0$  kompakt und diskret also endlich. Also ist  $\Lambda$  endlich erzeugte abelsche Gruppe. Nach ??? Struktursatz ist  $\Lambda \cong \mathbb{Z}^r$ . Da  $v_1, \dots, v_n$  linear unabhängig sind, ist  $\Lambda_0 = \Lambda$  und somit  $\Lambda$  Gitter.

2. Wenn  $\Lambda$  vollständig, dann ist  $\mathbb{R}^n/\mathbb{Z}^n = (S^1)^n$  kompakt. Wenn  $\Lambda \subseteq V$  Gitter sodass  $V/\Lambda$  kompakt ist, dann sei  $V_0 = \mathbb{R}\Lambda$ . Es ist  $V = V_0 \oplus V_1$  nach ergänzen einer Basis von  $V_0$ . Also ist  $V/\Lambda \cong V_0/\Lambda \oplus V_1 = \text{kompakt} \times \mathbb{R}^m$  kompakt. Also ist  $m = 0$  und damit  $V_0 = V$ . □

**Definition 12.0.5.** Sei  $\Lambda \subseteq V$  ein Gitter. Eine Grundmasche ist eine Menge der Form  $\{\sum_{i=1}^n a_i v_i \mid a_i \in [0, 1]\}$  für eine Basis  $v_1, \dots, v_n$  von  $\Lambda$ .

Sei ab jetzt  $V$  ein euklidischer Vektorraum, dh.  $V$  hat ein Skalarprodukt. Dann trägt  $V$  ein Maß  $\mu$ .

**Definition 12.0.6.** Das Volumen  $\text{Vol}(\Lambda)$  von Gitter  $\Lambda$  ist definiert als  $\mu(\Gamma)$  wobei  $\Gamma$  eine Grundmasche ist. Das ist wohldefiniert, denn zwei Basen von  $\Lambda$  unterscheiden sich um ein Element von  $GL_n(\mathbb{Z})$  und das hat Determinante

pm1. Wirkung auf Volumen geschieht durch Betrag der Determinante.