Teil I

Grundlagen

Kapitel 1

Grundlagen Kategorientheorie

1.1 Kategorien und Morphismen

Definition 1.1.1 (Kategorie)**.** Eine Kategorie e^x besteht aus den folgenden Daten:

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

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

Dabei fordern wir, dass folgende Bedingungen erfüllt sind:

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

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

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

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

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

$$f_*\colon \mathrm{Mor}_{\mathcal{C}}(z, x) \to \mathrm{Mor}_{\mathcal{C}}(z, y),\ g \mapsto f \circ g$$

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

$$f^*\colon \mathrm{Mor}_{\mathcal{C}}(y, z) \to \mathrm{Mor}_{\mathcal{C}}(x, z),\ g \mapsto g \circ f$$

   injektiv ist.

2. Wir sagen f ist ein spaltender Monomorphismus, falls es einen Morphismus $g\colon y \to x$ gibt mit $g \circ f = \mathrm{id}_x$. Wir nenn dann g eine Retraktion voon f
   Dual dazu sagen wir f ist ein spaltender Epimorphismus falls es einen Morphismus $g\colon y \to x$ mit $f \circ g = \mathrm{id}_y$. Wir nennen dann g einen Schnitt von f.

3. Wir sagen f ist ein Isomorphismus falls es einen Morphismus $f'\colon y \to x$ 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 $f\colon x \to y$ ein Morphismus in einer Kategorie $\mathcal{C}$. Dann sind die folgenden Bedinungen äquivalent:*

1. *f ist ein Isomorphismus.*

2. *f ist sowohl ein Monomorphismus als auch ein spaltender Epimorphismus.*

3. *f ist sowohl ein Epimorphisus als auch ein spaltender Monomorphismus.*

4. *Für alle $z \in \mathcal{C}$ ist die Abbildung $f_*\colon \mathrm{Mor}_{\mathcal{C}}(z,x) \to \mathrm{Mor}_{\mathcal{C}}(z,y)$ bijektiv.*

5. *Für alle $z \in \mathcal{C}$ ist die Abbildung $f^*\colon \mathrm{Mor}_{\mathcal{C}}(y,z) \to \mathrm{Mor}_{\mathcal{C}}(x,z)$ bijektiv.*

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

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

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

1.2 Funktoren

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

1. Eine Abbildung
$$\mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}),\ x \mapsto F(x).$$

2. Für alle Objekte $x, y \in \mathcal{C}$ eine Abbildung
$$\mathrm{Mor}_{\mathcal{C}}(x,y) \to \mathrm{Mor}_{\mathcal{D}}(F(x),F(y)),\ f \mapsto F(f).$$

Dabei fordern wir, dass die folgenden Bedingungen erfüllt sind:

1. Für alle $x \in \mathcal{C}$ ist $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$.

2. Für alle $f\colon x \to y$ und $g\colon y \to z$ in $\mathcal{C}$ ist $F(g \circ f) = F(g) \circ F(f)$.

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

$$F\colon \mathrm{Mor}_{\mathcal{C}}(x,y) \to \mathrm{Mor}\,\mathcal{D}(F(x),F(y))$$

injektiv (bzw. bijektiv ist).

Bemerkung 1.2.2. Sei $F\colon \mathcal{C} \to \mathcal{D}$ 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 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. $[n] = Set0, 1, \ldots n$). Dann definiere eine Kategorie NP durch

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

Das gibt einen volltreuen Funktor $N\colon \mathsf{CatOrd} \to \mathsf{Cat}$

1.3 Natürliche Transformationen

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

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

Dabei fordern wir, dass folgende Bedingung erfüllt ist:

1. Für alle Morphismen $f\colon x \to y$ in $\mathcal{C}$ kommutiert das Diagramm $\begin{array}{ccc} F(x) & \xrightarrow{\tau_x} & G(x) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(y) & \xrightarrow{\tau_y} & G(y) \end{array}$ Wir schreiben $\mathrm{Nat}(F, G)$ für die Klasse der natürlichen Transformationen $\tau\colon F \to G$.

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

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

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

Beweis. Seien $F, G\colon \mathcal{C} \to \mathcal{D}$ Funktoren. Dann ist

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

und das letze ist eine Menge. □

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

Beweis. Behauptung: $(\tau_x^{-1})_x$ ist eine natürliche Transformation. Sei $f\colon x \to y$ 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 $i\colon \mathcal{D}' \to \mathcal{D}$ ein volltreuer Funktor und $F\colon \mathcal{C} \to \mathcal{D}$ ein Funktor mit $\mathrm{im}(F) \subseteq \mathrm{im}(i)$. Dann existiert ein Paar (F', κ) bestehend aus einem Funktor $F'\colon \mathcal{C} \to \mathcal{D}'$ und einen natürlichen Isomorphismus $\kappa\colon i \circ F' \cong F$. Weiter gibt es für zwei solcher Paare (F_1', κ_1) und (F_2', κ_2) einen eindeutigen natürlichen Isomorphismus $\nu\colon F_1' \cong F_2'$ sodass $\kappa_2 \circ i(\nu) = \kappa_1$, das heißt das Paar (F', κ) 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*

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

Beweis. Klar. □

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

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

Falls ein Quasiinverses existiert dann nennen wir F eine Kategorienäquivalenz.

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

1. *F ist eine Kategorienäquivalenz.*
2. *Es existiert ein Funktor $G\colon \mathcal{D} \to \mathcal{C}$ mit natürlichen Isomorphismen $\alpha\colon G \circ F \cong \mathrm{id}_{\mathcal{C}}$ und $\beta\colon F \circ G \cong \mathrm{id}_{\mathcal{D}}$.*
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 $\beta_y^{-1}\colon y \cong F(G(y))$ also ist F essentiell surjektiv. Außerdem sind für $x, y \in \mathcal{C}$ die Diagramme

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

□

Bemerkung 1.3.9. Sei $F\colon \mathcal{C} \to \mathcal{D}$ ein Funktor. Dann ist äquivalent

1. F ist Kategorienäquivalenz
2. Für alle Kategroien $\mathcal{E}$ ist $F_*\colon \mathsf{Fun}(\mathcal{E},\mathcal{C}) \to \mathsf{Fun}(\mathcal{E},\mathcal{D})$ eine Kategorienäquivalenz
3. Für alle Kategroien $\mathcal{E}$ ist $F^*\colon \mathsf{Fun}(\mathcal{D},\mathcal{E}) \to \mathsf{Fun}(\mathcal{C},\mathcal{E})$ eine Kategorienäquivalenz

1.4 Yoneda Lemma

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

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

bijektiv.

Beweis. Für $s \in F(x)$ definiere $\tau^{(s)}\colon \mathrm{Mor}_{\mathcal{C}}(-,x) \to F$ durch

$$\tau_y^{(s)}\colon \mathrm{Mor}_{\mathcal{C}}(y,x) \to F(y),\ f \mapsto F(f)(s)$$

für $y \in \mathcal{C}$.
Es gilt $\tau_x^{(s)}(\mathrm{id}_x) = s$ und $\tau_y^{(\tau_x(\mathrm{id}_x))}(f) = \tau_y(f)$. Also gilt die Aussage. □

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

$$Y_{\mathcal{C}}\colon \mathcal{C} \to \mathsf{Fun}(\mathcal{C}^{\mathrm{op}},\mathsf{Set}),\ x \mapsto \mathrm{Mor}_{\mathcal{C}}(-,x)$$

volltreu.

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

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

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

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

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

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

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

1.5 Adjunktionen

Definition 1.5.1 (Adjungiertes Objekt)**.** Sei $G\colon \mathcal{D} \to \mathcal{C}$ 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 $\eta\colon x \to G(y)$ sodass für alle $y' \in \mathcal{D}$ die Abbildung

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

bijektiv ist.

Bemerkung 1.5.2. sei $G\mathcal{D} \to \mathcal{C}$ 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

$$\mathrm{Mor}_{\mathcal{C}}(x, G(-))\colon \mathcal{D} \to \mathsf{Set}$$

Satz 1.5.3 (Adjungierter Fuktor)**.** *Sei $G\colon \mathcal{D} \to \mathcal{C}$ ein Funktor und sei $i\colon \mathcal{C}' \subseteq \mathcal{C}$ eine volle Unterkategorie, sodass alle Objekte in $\mathcal{C}'$ unter G ein linksadjungiertes Objekt besitzen. Dann existiert ein Funktor $F\colon \mathcal{C}' \to \mathcal{D}$ und eine natürliche Transformation $\eta\colon i \to G \circ F$ sodass $(F(x)\eta_x)$ für jedes $x \in \mathcal{C}$ ein unter G zu x linksadjungiertes Objekt ist. Das Paar (F, η) 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 $F\colon \mathcal{C} \to \mathcal{D}$ auch einfach einen linksadjungierten Funktor zu G.*

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

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

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

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

und somit $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$. Weiter ist für Morphismen $f\colon x \to y$ und $g\colon y \to z$

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

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

Bemerkung 1.5.4. Sei $G\colon \mathcal{D} \to \mathcal{C}$ 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 $F\colon \mathcal{C}' \to \mathcal{D}$ von G das Gleiche wie eine Faktorisierung des Funktors

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

durch die (volltreue) duale Yoneda-Einbettung

$$Y^{\mathcal{D},\mathrm{op}}\colon \mathcal{D} \to \mathsf{Fun}(\mathcal{D}, \mathsf{Set})^{\mathrm{op}}.$$

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

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

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

Beweis. Klar □

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 $aH \cap bH = \Longleftrightarrow\ aH = bH$ Es ist $|H| \neq |aH|$ für alle $a \in G$. □

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

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

Korollar 2.1.4. *Sei p eine Primzahl und $a \in \mathbb{Z}$ sodass $p \not| a$. Dann ist $a^{p-1} \equiv 1 \mod p$.*

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

2.2 Gruppenwirkung

Definition 2.2.1. Sei G eine Gruppe, X eine Meng und $G \times X \to X$ eine Gruppenwirkung.

1. Für $x \in X$ ist $Gx = \{ax \mid a \in G\}$ die Bahn von x.
2. Für ist $x \in X$ ist $\mathrm{Stab}_G(x) = G_x = \{a \in G \mid ax = x\}$ 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 $\mathrm{Stab}_G(X) = G$ ist.
5. X^G sie die Menge der Fixpunkte von G auf X.
6. Die Operation heißt treu, wenn der Homomorphismus $G \to S(X)$ injektiv ist.

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

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

$$G/\operatorname{Stab}_G(X) \to G_x, a \operatorname{Stab}_G(X) \mapsto ax$$

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

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

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

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

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

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

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

□

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

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

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 $C_G(a) = \mathrm{Stab}_G(a)$ für die Wirkung $G \times G \to G,\ (a, b) \mapsto aba^{-1}$

Satz 2.2.8 (Klassengleichung)**.** *Sei G eine endliche Gruppe und $a_1, \ldots, a_r$ Verteter 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 $G \times G \to G,\ (a, b) \mapsto aba^{-1}$, denn wenn x_i ein Vertreter einer Bahn mit zentralen Element, dann ist $\mathrm{Stab}_G(x_i) = C_G(x_i) = G$ □

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 $G \times X \to X$ eine Wirkung einer p-Gruppe auf eine endliche Menge X. Dann ist*

$$|X| \equiv |X^G| \mod p.$$

Beweis. Nach Satz 2.2.5 ist

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

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

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

Beweis. Betrachte Wirkung $G \times G \to G, (a, b) \mapsto aba{-}1.$. Nach Satz 2.2.10 gilt $|G| = |Z(G)| \mod p$. 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 $p \not| [G : P]$. Das heißt wenn $|G| = p^r \cdot m$ mit $p \not| m$ 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 $\operatorname{ord}(a) = p$.*

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

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

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

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

. 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 $g^p = e$. □

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 $\pi \colon G \to N$ die Projektion ist. Dann ist $H/N \cong \bar{H}$ also ist H normal von Ordnung p^{k-1}. □

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

Beweis. Sei $|G| = p^r \cdot m$ mit $p \not| m$. Sei ohne Einschränkung $r \geq 1$. Angenommen $p \mid |Z(G)|$ wobei $Z(G)$ das Zentrum von G ist. Wähle $a \in Z(G)$ mit $\operatorname{ord}(a) = p$. 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 $\pi \colon G \to G/N$ die Projektion ist. Dann ist $P/N \cong Q$ also $|P| = p^r$. Somit ist $P \subseteq G$ eine p-Sylwogruppe.
Angenommen $p \not| |Z(G)|$. Dann gibt es die Klassengleichung

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

Also gibt es ein i sodass $p \not| [G : C_G(a_i)]$. Da

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

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 $P \subseteq C_G(a_i)$. □

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 duch $h \cdot (aP) = haP$. Nach Satz 2.2.10 ist

$$|G/P| \equiv |(G/P)^H| \mod p.$$

Also ist $p \not| |(G/P)^H|$ und somit gibt es einen Fixpunkt aP. Das heißt $HaP = aP$ und somit $a^{-1}HaP = P$ also $a^{-1}Ha \subseteq P$. □

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 $p \not| m$. Sei s die Anzahl der p-Sylowgruppen von G. Dann gilt*

$$s \equiv 1 \mod p \tag{2.1}$$
$$s \mid m \tag{2.2}$$

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

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

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

$$S = |X| = 1 + \sum_{i \geq 2}^{k} [P\colon \mathrm{Stab}_G(P_i)] \equiv 1 \mod p.$$

Zeige 2). Sei X wie oben. Wegen 2. Sylowsatz operiert G transitiv auf X durch Konjugation. Sei $H = \mathrm{Stab}_G(P)$ der Normalisator von P. Es ist $P \subseteq H$ und somit $p^r \mid H$. Es ist $|H| = p^r \cdot \ell$ mit $p \not| \ell$. Nach ist Dann ist $s = |X| = \mathrm{Bahn}(P) = |G|/|H| = \frac{m}{\ell}$. Also ist s ein Teiler von m. □

Satz 2.3.9. *Seien p, q Primzahlen und $p < q$ und $p \not| q - 1$. Dann ist jede Gruppe der Ordnung $p \cdot q$ zyklisch.*

Beweis. Sei s die Anzahl der p-Sylwogruppen 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 Korollar 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 $\mathrm{ord}(ab) = pq = |G|$ und somit $G = \langle ab \rangle$. □

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

$$f\colon \prod_{i=1}^{r} P_i \to G,\ (a_1, \ldots, a_r) \mapsto a_1 \cdot \cdots \cdot a_r$$

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

2.4 Gruppen Stukturen

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 $G = NH$. Dannn 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 $N \times H \to G,\ (n, h) \mapsto n \cdot h$ 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

$$\alpha\colon H \to \mathrm{Aut}(N),\ \alpha(h) = (N \to N, n \mapsto hn'h^{-1})$$

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

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

Definition 2.4.3. Seien N, H Gruppen und $\alpha\colon H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Definiere $N \rtimes H = N \rtimes_\alpha H$ als Menge $N \times H$ und Gruppenstuktur $(n,h)(n',h') = (n\alpha(h)(n'), hh')$. 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 α. Es ist $N \subseteq N \rtimes H, n \mapsto (n,e)$ und $H \subseteq N \times H,\ h \mapsto (e,h)$.

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 $(n,e) \cdot (e,h) = \tau$. □

Definition 2.4.5. Sei GroupActions die Kategorie mit Objekten (H, N, α) wobei H, N Gruppen sind und $\alpha\colon H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus ist. Morphismen

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

in GroupActions sind (f_H, f_N) wobei $f_H\colon H \to H'$ und $f_N\colon N \to N'$ H-equivariante Gruppenhomomorphismen sind. Das heißt $f_N(\alpha(h)(n)) = \alpha'(f_H(h))(f_N(n))$ for all $h \in H$ and $n \in N$.

Lemma 2.4.6. *Sei* Arr(Grp) *die* **??** *von* Grp. *Der*

$$R\colon \mathsf{Arr}(\mathsf{Grp}) \to \mathsf{GroupActions},\ (\phi\colon H' \to N') \mapsto (H', N', \alpha')$$

wobei α' 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

$$L\colon \mathsf{GroupActions} \to \mathsf{Arr}(\mathsf{Grp}), (H, N, \alpha) \mapsto (H \subseteq N \rtimes_\alpha H)$$

ist linksadjungiert zu U.

Beweis. Sei

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

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

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

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 $\phi\colon H' \to N'$ Gruppenhomomorphismus ist und

$$(f_H, f_N)\colon (H, N, \alpha) \to R(\phi) = (H', N', \alpha')$$

ein Morphismus in GroupActions ist, dann definiere $f_{N\rtimes H}\colon N \rtimes_\alpha H \to N'$ 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 $\mathsf{Arr}(Grp)$:

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

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

□

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

$$\mathrm{codom} \circ L\colon \mathsf{GroupActions} \to \mathsf{Grp},\ (H, N, \alpha) \mapsto N \rtimes_\alpha H$$

linksadjungiert zu

$$R \circ R'\colon \mathsf{Grp} \to \mathsf{GroupActions},\ G \mapsto (G, G, \alpha')$$

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 $\pi\colon G \to G/H$ Projektion und setze $G_i = H_i$ für $0 \leq i \leq n$ und $G_i = \pi^{-1}\bar{G}_i$ für $n \leq i \leq n$. 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-Sylowgrupen. Dann ist $s \equiv 1 \mod q$ 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 Kommutatot 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 Abelisierung von G ist $G^{\mathrm{ab}} = G/D(G)$.

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

Beweis. Klar, Rechnung □

Satz 2.4.15 (Universelle Eigenschaft der Abelisierung)**.** *Abelisierung wird zu einem Funktor $(-)^{\mathrm{ab}}\colon \mathrm{Gr} \to \mathsf{Ab}$ der linksadjungiert ist zum Vergiss-Funktor $U\colon \mathsf{Ab} \to \mathsf{Grp}$*

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

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 $\psi\colon S_4 \to S_3$ 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 Normalteler 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 $a \in G$ sodas $\mathrm{ord}(a) = p$ 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 setzte σ 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 σ maximal ist und $\sigma \neq e$. Behauptung: Alle Zykel in der Zykeldarstellung von σ haben die gleiche Länge d. Denn wenn Längen $m < d$ vorkommen, dann hat σ^m mehr Fixpunkte und $\sigma^m \neq e$. Behauptung: σ 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 σ dieser 3-Zykel. Wenn $d = 2$ dann ist $\sigma = (a\ b)(c\ d)\cdots = \sigma^{-1}$. Sei $\tau = (b\ c)(e\ f)$. Dann ist $\tau\sigma\tau^{-1}\sigma^{-1} = (a\ d)(b\ c)$. Wegen der Maximalität von σ 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. □

Lemma 2.5.2 (Chinesischer Restsatz)**.** *Seien $n, m \in \mathbb{Z}$ und $d = \mathrm{ggT}(n, m)$ und $k = \mathrm{kgV}(n, m)$. 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

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

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

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

und

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

Also gilt

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

und somit

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

Da

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

gilt, ist

$$b \equiv 0 \mod d.$$

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

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

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

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 $p = \operatorname{char} K$. 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. □

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 $\phi\colon K[X] \to L$ der Ringhomomorphismus gegeben durch $\phi(f) = f(a)$.

1. Das Element a heißt algebraisch, falls $\ker(\phi) \neq 0$. Andereseits nennen wir a transzendental 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 $a_1, \ldots, a_r \in L$.

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

$$\begin{aligned} K[a_1, \ldots, a_r] &= \bigcap_{R \in M} R \\ &= \operatorname{im}(\phi\colon K[X_1, \ldots, X_R] \to L,\ X_i \mapsto a_i) \end{aligned}$$

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

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

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

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 Minimalpoylon f irreduzibel sodass

$$(f) = Ker(\phi \colon K[X] \to L, x \mapsto a).$$

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 $\dim_K(K[X]) = \infty$. □

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.*

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

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 $K'[a_2, \dots, a_n] = K'(a_2, \dots, a_n)$. □

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. □

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. □

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, $L = K[X]/(f)$. □

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. □

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. □

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. $\mathrm{Aut}_K(L) = \mathrm{Aut}(L/K)$ sei die Menge der invertierbaren K-Homomorphismen $f\colon L \to L$

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 $\sigma\colon K \to M$. Sei*

$$\Sigma = \{K - \textit{Homomorphismen } \sigma'\colon L \to M\}.$$

Dann ist die Abbildung

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

bijektiv

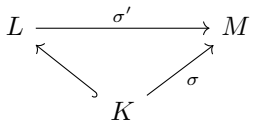
Beweis. Wir haben die Abbildung $\phi\colon K[X] \to M, X \mapsto b$. Es gilt ϕ lässt sich eindeutig fortsetzen zu $\sigma'\colon K[X]/(f) \to M$ genau dann, wenn $f \in \ker(\phi)$ ist, das heißt wenn $f(b) = 0$. Dann ist $\sigma'(a) = \sigma'(\bar{X}) = b$. □

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

$$\{\mathbb{R} - \mathrm{Hom}\, \sigma'\colon \mathbb{C} \to \mathbb{C}\} \xrightarrow{\sim} \{b \in \mathbb{C} \mid b^2 + 1 = 0\},\ \sigma' \mapsto \sigma'(i)$$

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

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



kommutiert

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

Fall 2: Sei L/K allgemein. Sei X die Menge der Paare (L', σ') wobei L' ein Körper ist mit $K \subseteq L' \subseteq L$ und σ' eine Fortsetzung von σ. 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 $\tilde{\sigma}\colon \tilde{L} \to M$ 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', σ'). Angenommen $L' \neq L$. Dann wähle $a \in L \setminus L'$ und setze $L'' = L'(a)$. Nach Fall 1 existiert eine Fortsetzung $\sigma''\colon L'' \to M$ was ein Widerspruch ist. Also ist $L' = L$. □

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

Beweis. Nach Satz 3.3.4 gibt es K-Homomorphismus $\sigma\colon L \to M$. Dadurch wird M eine algebraische Erweiterung von L. Also ist M/L triviale Erweiterung, dh. σ ist bijektiv. □

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

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

wobei $g_j \in R$ und $f_1, \ldots, f_r \in I$. In $g_1, \ldots, g_r$ kommen nur endlich viele X_{f_i} vor, somit gibt es eine endliche Menge $I' \subseteq I$, sodass die Gleichung 3.1 in $R' = K[X_f | f \in I']$ 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

$$\phi\colon R' \to M,\ \phi(X_f) = a_f.$$

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 $L = \bar{R}/m$, 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 $K \subseteq L_1 \subseteq L_2 \subseteq L_3 \ldots$ 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. □

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 bist 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 $\sigma\colon M \to \bar{K}$. 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 σ. 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 σ ist ein Isomorphismus $M \to L$. □

Bemerkung 3.4.4. Das zeigt: Alle K-Homomorphismen $\sigma\colon M \to \bar{K}$ 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 ζa 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 $\varphi\colon L \to L$ ein K-Homomorphismus. Dann ist ϕ bijektiv.*

Beweis. Immer ist ϕ 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. $\varphi|_{K(a_i)}\colon K(a_i) \to L$ gibt n verschiedene K-Homomorphismen $K[X]/(f) \to L$ 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 φ bijektiv. □

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 $\varphi\colon L \to M$ gilt $\phi(L) = L$*
4. *Für Jeden K-Homomorphismus $\varphi\colon L \to \bar{L}$ 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 $\varphi\colon L \to M$ 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 φ 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 $\sigma\colon K(a) \to \bar{L}$ ist bijektiv zur Menge $\{b \in \bar{L} \mid f(b) = 0\}$. Zu $b \in \bar{L}$ wähle also $\sigma\colon K(a) \to \bar{L}$. Nach Satz 3.3.4 gibt es ein $\varphi\colon L \to \bar{L}$, das σ fortsetzt. Dann ist $\varphi(L) = L$. Also ist $b = \sigma(a) = \varphi(a) \in L$. Also zerfällt f in $L[X]$. □

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 $L[X]$. □

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 $M \to M'$. 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'/L normal. Wähle $\bar{M}'/M'$ algebraischen Abschluss. Nach Satz 3.3.4 gibt es einen L-Hom $\varphi\colon M \to \bar{M}'$. Jedes $f \in \mathcal{F}$ zerfällt in $M'[X]$ und da M von allen Nullstellen erzeugt gilt $\phi(M) \subseteq M'$. □

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

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. □

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

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

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. □

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.

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

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

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

Bemerkung 3.5.14. Sei p Primzahl und $K = \operatorname{Quot}(\mathbb{F}_p[Y])$. 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 $[L : K]_s = |\{K - \operatorname{Hom}.\ L \to \bar{K}\}|$

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

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

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

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

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

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

für jeden $\phi \colon L \to \bar{K}$ erfüllt die Abbildung

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

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

Also

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

□

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 $a_1, \ldots, a_r$ sodass $L = K(a_1, \ldots, a_r)$. 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). $L = K(a_1, \ldots, a_r)$ 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. □

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

Beweis. Folgt aus der Konstruktion der normalen Hülle. □

3.6 Spur und Norm

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

$$Tr_{L/K}(b) = Tr(b\cdot \colon L \to L)$$

die Spur und

$$N_{L/K}(b) = \det(b\cdot \colon L \to L)$$

die Norm von b.

Bemerkung 3.6.2. Es ist für $a \in K$

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

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 charackteristische Polynom*

$$\chi_{b\colon L\to L} = P^e.$$

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 $\chi_{b\colon L\to L} = \chi^e_{b\colon K(b)\to K(b)} = P^e$ □

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

$$Tr_{L/K}(b) = -ea_{d-1}$$

und

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

wobei $ed = [L : K]$

Beweis. Klar nach Lemma 3.6.3. □

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 charackteristische Polynom

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

wobei $\Sigma = \{\sigma\colon K(b) \to \bar{K} \mid \sigma|_K = \mathrm{id}\}$ und $\Sigma' = \{\sigma\colon L \to \bar{K} \mid \sigma|_K = \mathrm{id}\}$.

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*

$$Tr_{L/K}(b) = \sum_{\sigma\in\Sigma}\sigma(b)$$

und

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

wobei $\Sigma = \{\sigma\colon L \to \bar{K} \mid \sigma|_K = \mathrm{id}\}$.

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 liefer

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

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 separable*
2. *$Tr_{L/K}\colon L \to K$ ist nicht die Nullabbildung*
3. *Die Abbildung $(x, y) \mapsto Tr_{L/K}(xy)$ ist nicht-ausgeartete Bilinearform $L \times LK$.*

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 $Tr_{L/K}(1) = [L : K] \neq 0$. Es gilt $Tr \neq 0$ genau dann wenn Tr surjektiv, denn Tr ist K-linear. Wenn L/K separabel, dann ist $L = K(\alpha)$ für ein $\alpha \in L$ nach ????. Wenn L/K inseperabel, dann gibt es $\alpha \in L$ inseperabel über K. Da $Tr_{L/K} = Tr_{K(\alpha)/K} \circ Tr_{L/K(\alpha)}$ ist ohne Einschränkung $L = K(\alpha)$. Sei P das Minimalpolynom von α 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 β_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 $Tr_{L/K}\colon L \to K$ surjektiv genau dann wenn $\bar{Tr} = \mathrm{id}_{\bar{K}} \otimes Tr_{L/K}$ surjektiv ist. Da $L = K(\alpha) = K[X]/P$ ist $\bar{K} \otimes_K L = \prod \bar{K}[X]/(X^{p^m} - \beta_i)$ 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 $Tr(b) \in A$.*

Beweis. Sei $\varphi(x) = \prod_{g \in G}(X - g(b))$ mit $G = \mathrm{Gal}(L/K)$. Das ist das Charakterisitsche Polynom nach ?? und ??. Alle Koefffizienten von φ 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 $Tr(b) \in A$ da $Tr(b)$ einer der Koeffienten ist. □

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 $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$

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

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

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

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

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 $\sigma \in \mathrm{Gal}(L/K)$ $\sigma(N) \subseteq N$. Haben also

$$\psi\colon\ \mathrm{Gal}(L/K) \to S(N) \cong S_3,\ \sigma \mapsto \sigma|_N$$

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

4.2 Galois Korrespondenz

Definition 4.2.1. Sei L ein Körper und $G \subseteq \mathrm{Aut}(L)$ 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 $G = \mathrm{Gal}(L/K)$, dann ist $K = L^G$.*

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

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

Somit $[L^G:K] = 1$ und $L^G = K$. □

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

Beweis. Sei $b \in L$ und $N \subset L$ die $G-$Bahn von b, das heißt $N = \{\sigma(b) \mid \sigma \in G\} = \{b_1, \ldots, b_r\}$ 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 $G = \{\sigma_1, \ldots, \sigma_n\}$. 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

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

also $G = \operatorname{Gal}(L/K)$ □

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

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

1. *Folgende Abbildungen sind zueinander inverse Bijektionen:*

$$\{\text{Untergruppen } H \subseteq G\} \underset{\operatorname{Gal}(L/M)\leftarrow M}{\overset{H\mapsto L^H}{\rightleftarrows}} \{\text{Zwischenkörper } K \subseteq M \subseteq L\}$$

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 $M = L^{\operatorname{Gal}(L/M)}$ wegen Lemma 4.2.2. Wenn $H \subseteq G$ eine Untergruppe ist, dann ist $H = \operatorname{Gal}(L/L^H)$ nach Satz 4.2.3.
2. $$[M : K][L : M] = [L : K] = |G| = |H|[G : H]$$
   und $[L : M] = |\operatorname{Gal}(L/M)| = H$
3. Sei $\tau \in G$
$$\begin{aligned}\tau \in \operatorname{Gal}(L/M) &\iff \tau(b) = b,\ \forall b \in M\\ &\iff \sigma\tau\sigma^{-1}\sigma(b) = \sigma(b),\ \forall b \in M\\ &\iff \sigma\tau\sigma^{-1}(c) = c,\ \forall c \in \sigma(M)\\ &\iff \sigma\tau\sigma^{-1} \in \operatorname{Gal}(L/\sigma(M))\end{aligned}$$
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 $\operatorname{Gal}(M/K) \cong G/H$.

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

$$\sigma\colon M \to \bar{L}$$

hat Fortsetzung zu einem K-Homomorphismus

$$\tilde{\sigma}\colon L \to \bar{L}.$$

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

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

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

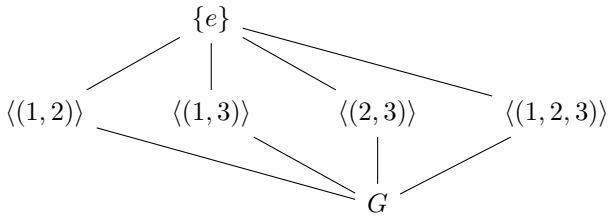
$$\ker(\psi) = \{g \in G \mid g|_M = \mathrm{id}\} = \{g \in \mathrm{Aut}(L) \mid g|_M = \mathrm{id}\} = \mathrm{Gal}(L/M) = H.$$

□

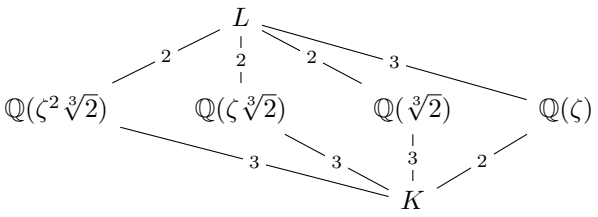
Korollar 4.2.7. *Wenn L/K endlich separable ist, dann hat L/K nur endlich viele Zwischenkörper.*

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 $G = \mathrm{Gal}(\bar{L}/K)$. Die letzte Menge ist endlich. □

Beispiel 4.2.8. Sei L Zerfällungskörper von $X^3 - 2$ über $K = \mathbb{Q}$. Die Abbildung $\psi\colon G \to S_3$ 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_1M_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 $G = \mathrm{Gal}(L/K)$. Wenn M_1, M_2 jeweils zu H_1, H_2 korrespondieren, dann korrespondiert M_1M_2 zu $H_1 \cap H_2$ und $M_1 \cap M_2$ korrepondiert 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. □

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* $\mathrm{Gal}(M'/K') \cong \mathrm{Gal}(M/M \cap K')$. *Insbesondere ist* $[M' : K'] = [M : K' \cap M]$

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

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 $\sigma \in \mathrm{Gal}(M'/K')$ ist $\sigma|_K = id_K$. Da M/K normal ist, folgt $\sigma(M) = M$ das heißt $\sigma|_M \in \mathrm{Gal}(M/K)$. Das gibt Gruppenhomomorphismus

$$\psi\colon \mathrm{Gal}(M'/K') \to \mathrm{Gal}(M/K), \sigma \mapsto \sigma|_M$$

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

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

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

Kapitel 5

Anwendunge der Galoistheorie

5.1 Endliche Körper

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

Beweis. Es ist

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

ϕ ist immer injektiv. Wenn K endlich ist, dann automatisch bijektiv. □

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 $p = \operatorname{char} K$.*

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 $\mathbb{F}_q \to K$ mit $|\mathbb{F}_q| = q = |K|$ also ist $\mathbb{F}_q \cong K$. □

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 $m_1 | m_2 | \ldots | m_r$ 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.

□

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 $\operatorname{ggT}(k, n) = 1$.

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

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

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

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

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

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 Galoisch und für $\sigma \in G = \mathrm{Gal}(L/K)$ gilt

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

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

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

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

wobei wir σ 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 $\mathrm{char}(K) \notin \{2, 3\}$ 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 Diskrimminante. 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 $\mathrm{char}(K) \notin \{2, 3\}$ und $f = X^3 + aX + b \in K[X]$ irreduzibel. Dann ist ein Zerfällungskörper L/K von f Galoisch. Es ist $\mathrm{Gal}(L/K) \subseteq S_3$.*

1. *Δ ist Quadrat in $K \implies G = A_3 \cong \mathbb{Z}/3\mathbb{Z}$*
2. *Δ kein Quadrat in $K \implies G = S_3$*

Beweis. Da f irreduzibel gilt für eine Nullstelle α 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

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

□

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 $\mathrm{Gal}(L/K) = S_3$

Lemma 5.1.16. *Sei R faktoriell und $g, h \in K[X]$ normiert und sei $K = \mathrm{Quot}(R)$. 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 $h, g \in R[X]$. □

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 $\mathrm{Gal}(L/K) = A_3$

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 $\mathrm{char}(K) \not| n$. 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 $ggT(f, f') = 1$ und damit f separabel. □

Definition 5.2.3. Sei $\mathrm{char}(K) \not| n$. Ein $\zeta \in \mu_n(K)$ heißt primitive n-te Einheitswurzel, wenn ζ 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 $\mathrm{End}(G) \cong \mathbb{Z}/n\mathbb{Z}$ als Ring und $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$ als Gruppe.*

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

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

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

Die Funktion φ heißt Eulersche φ-Funktion

Lemma 5.2.6. *Es gilt*

1. $\mathrm{ggT}(n, m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$
2. $\varphi(\mathrm{kgV}(n, m))\varphi(\mathrm{ggT}(n, m)) = \varphi(n)\varphi(m)$
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 Chinsesischem Restzatz 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 $0, p, 2p, \ldots, (p^{e-1} - 1)p$, das sind also p^{e-1} viele. Somit $|(\mathbb{Z}/p^e\mathbb{Z})^*| = p^e - p^{e-1}$ □

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

$$\psi\colon \mathrm{Gal}(L/K) \to \mathrm{Aut}\,\mu_n(\bar{K}),\ \sigma \mapsto \sigma|_{\mu_n(L)}$$

ist ein injektiver Gruppenhomomorphismus.

Beweis. ψ ist injektiv, da L/K von $\mu_n(L)$ erzeugt ist. □

Korollar 5.2.8. *Sei*

$$\phi\colon (\mathbb{Z}/n\mathbb{Z})^* \to Aut(\mu_n(\bar{K})),\ a \mapsto (\mu_n(\bar{K}) \to \mu_n(\bar{K}),\ \zeta \mapsto \zeta^a)$$

der Isomorphismus aus Lemma 5.2.4. Dann ist

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

gegeben durch

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

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

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

Beispiel 5.2.10. $K = \mathbb{R}$ and $n \geq 3$. Dann ist $\mu_n(\mathbb{C}) \subsetneq \mathbb{R}$ und somit $K(\mu_n(\mathbb{C})) = \mathbb{C}$. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ wobei σ 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 $G = \mathrm{Gal}(L/\mathbb{F}_q)$ von ϕ_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 $H = G$. □

Korollar 5.2.12. *Sei $q = p^r$ und $n \in \mathbb{N}$ mit $p \not| n$. Sei $L = \mathbb{F}_q(\zeta_n)$ wobei $\zeta_n \in \bar{\mathbb{F}}_q$ primitive n-te Einheitswurzel. Sei $\chi\colon \mathrm{Gal}(L/\mathbb{F}_q) \to (\mathbb{Z}/n\mathbb{Z})^*, \phi_q \mapsto k = \chi(\phi_q)$ wie in Korollar 5.2.8. Dann ist*

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

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 $[\mathbb{F}_7(\zeta_{12}) : \mathbb{F}_7] = |\mathrm{Gal}(..)| = 2$ und somit $\mathbb{F}_7(\zeta_{12}) = \mathbb{F}_{49}$

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

Beweis. Sei $\zeta_n \in \bar{\mathbb{Q}}$ eine primitive n-te Einheitswurzel und $f \in \mathbb{Q}[x]$ das Minimalpolynom von ζ_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 ζ_n^m eine primitve Einheitswurzel. Ohne Einschärnkung $m = p$ prim. Sei also $p \not| n$ und g Minimalpolynom von ζ_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 ζ_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 $f = g$ □

Korollar 5.2.15. *Für $n, m \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = d$ und $\mathrm{kgV}(n, m) = k$ 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 ζ_n eine primitive n-te Einheitswurzel und ζ_m primitive m-te Einehitswurzel 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 ζ ist eine primitive d-te Einheitswurzel für $d = \operatorname{ord}(\zeta)$ und jede primitive d-te Einheitswurzel für $d \mid n$ 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 ϕ_d ist das Minimalpolynom von ζ_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 $\sigma\colon \mathbb{C} \to \mathbb{C}$. 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 $b = \zeta_9 + \zeta_9^{-1}$

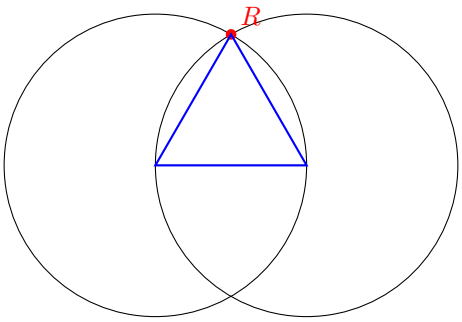
$$b\zeta_9 = \zeta_9^2 + 1$$

also ist $\zeta_9^2 - b\zeta + 1 = 0$ 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

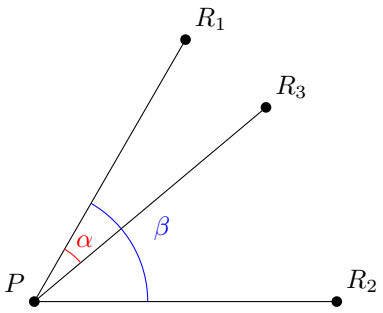
Starte mit einer Menge von Punkten in $\mathbb{R}^2 = \mathbb{C}$ Erlaubte Konstruktionen: Geraden durch 2 Verschiedene Punkte die gegeben sind und Kreise durch 2 Punkte, einer davon der Mittelpunkt, und Schnittpunkte von 2 Objekten dieser Art.

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 wir 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

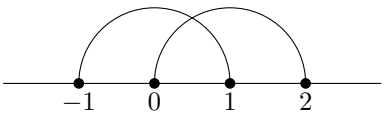
$$\ell(z, w) \cap \ell(z', w') \subseteq K(M)$$
$$\ell(z, w) \cap k(z', w') \subseteq K(M)$$
$$k(z, w) \cap k(z', w') \subseteq K(M)$$

falls die Schnitte jeweils endlich sind.

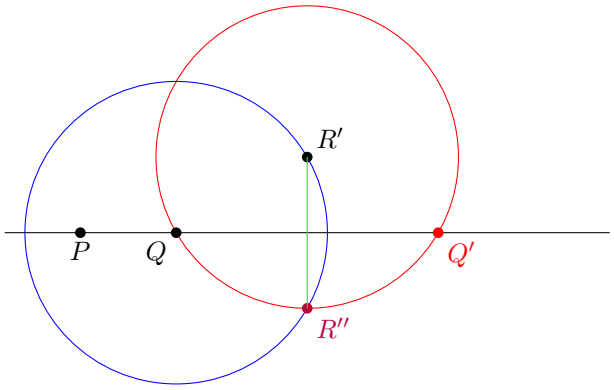
$K(M)$ ist die Menge aller Elemente von $\mathbb{C}$ die durch endlich viele Schnitte in M wie oben gewonnen werde können. Wir nennen $K(M)$ die Menge der aus M konstruierbaren Zahlen.

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

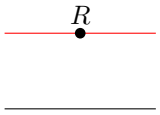
1. $\mathbb{Z} \subseteq K(0, 1)$



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



3. Parallele zu Geraden durch Punkt R

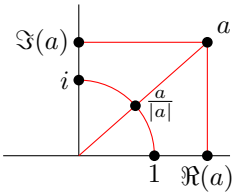


Verfahren: Bestimme Orthogonale durch R. Dann konstruire gleichseitiges Dreieck wo R der Mittelpunkt einer Seite ist. Das gibt Parallele.

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

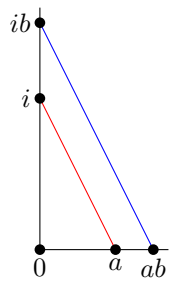
Lemma 5.3.6. *Sei $0, 1 \in M$ und $a \in \mathbb{C}$. Es ist äquivalent:*

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

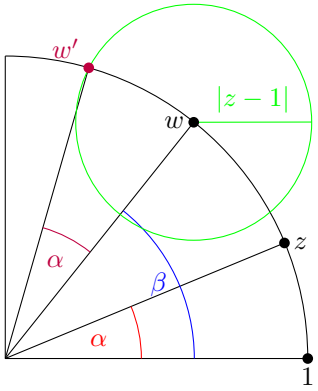


Lemma 5.3.7. *Sei $0, 1 \in M$. Dann ist $K(M)$ ein Körper. Insbesondere ist $\mathbb{Q} \subseteq K(M)$.*

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:



□

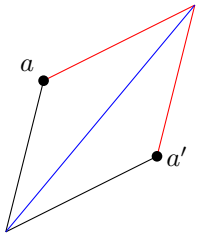
Bemerkung 5.3.8. Sei $0, 1 \in M$. Dann ist $\mathbb{Q}(M \cup \bar{M}) \subseteq K(M)$.

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

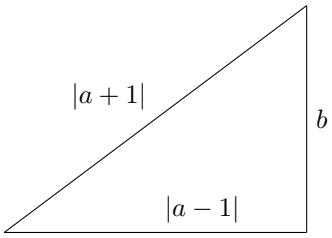
$$a \in K(M) \iff \exists\, \mathbb{Q}(M \cup \bar{M}) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r \text{ mit } [K_i : K_{i-1}] = 2 \text{ und } a \in K_r.$$

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 ohen 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 $K = L_0 \subseteq \cdots \subseteq L_m \subseteq K_1L_m \subseteq \cdots \subseteq K_nL_m$ Kette höchstens quadratischer Körpererweiterungen.*

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

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

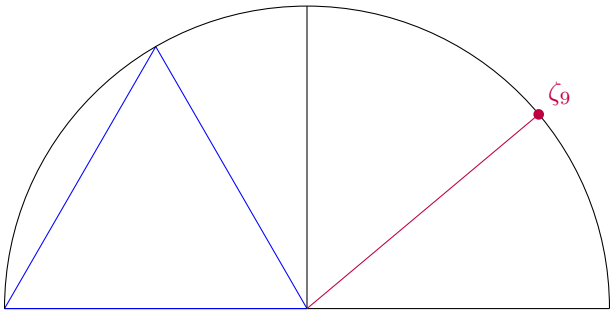
1. *Es gibt Kette quadratischer Erweiterungen $K = K_0 \subseteq \cdots \subseteq K_n$ and $a \in K_n$*
2. *Es gibt Galoiserweiterung L/K mit $a \in L$ und $[L : K] = 2^r$.*

Beweis. Gelte 1 und sei K_n/K gegeben. Dann ist K_n/K ist 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 $b_1, \ldots, b_n$ 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 Galoisch vom Grad 2^r. Dann ist $G = \mathrm{Gal}(L/K)$ 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 Galoisch 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 Winkeldrittelung 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 quadratische 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 Galoisch mit $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ 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 ζ_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

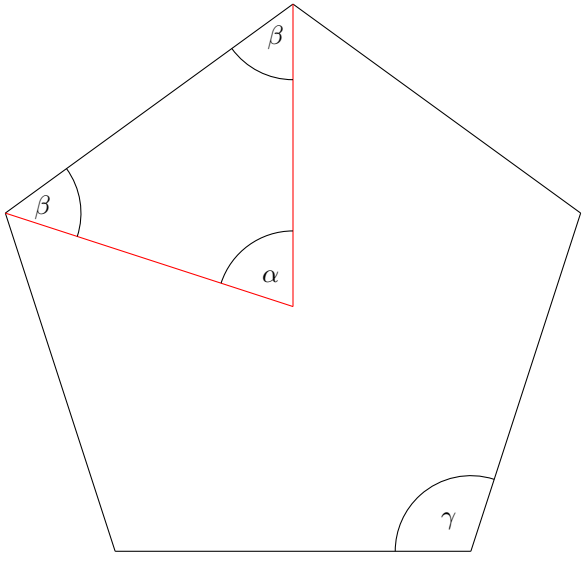
$$\frac{2^m + 1}{2^{m'} + 1} = \frac{1 - (-2^{m'})^q}{1 - (-2^{m'})} = \sum_{k=0}^{q-1} (-2^{m'})^k = \sum_{k=1}^{q} (-1)^{k+1} 2^{m - km'}$$

also $2^m + 1$ nicht prim. □

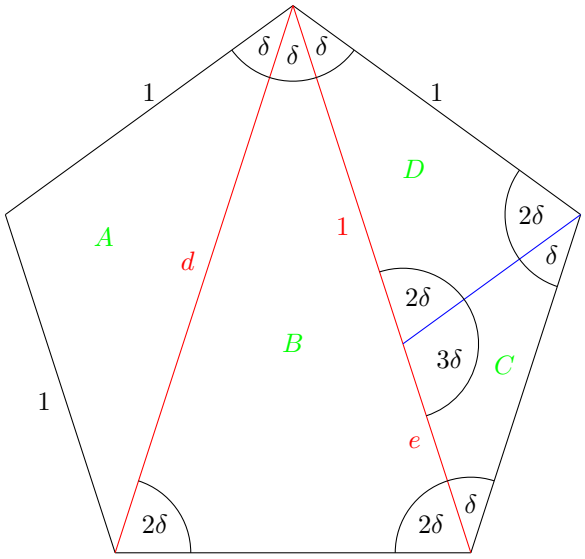
Bemerkung 5.3.21. $2^{2^r} + 1$ ist prim für $r = 0, 1, 2, 3, 4$ aber für $2^{2^5} + 1 = 641 \cdot 6700417$

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

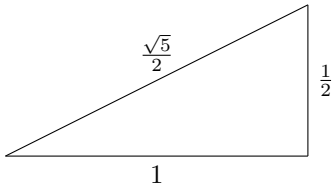
Beispiel 5.3.23. Sei $\alpha = \frac{2\pi}{5}$ und $\beta = \frac{\pi - \alpha}{2} = \frac{3\pi}{16}$ und $\gamma = 2\beta = \frac{3}{5}\pi$



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 $d = \dfrac{\sqrt{5}+1}{2}$ 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 $K = K_0 \subseteq \cdots \subseteq K_r = L$ 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

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

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 $[K(a) : K] = 1$ 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 $a, \zeta_n a, \zeta_n^2 a, \ldots, \zeta_n^{n-1} a$ 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 ζ_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 $\mathrm{Gal}(K(\sqrt[n]{a})/K) \to \mu_n(K) \cong \mathbb{Z}/n\mathbb{Z}$. Insbesondere ist $G = \mathrm{Gal}(L/K)$ 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 $\psi \colon G \to \mu_n(\bar{K}),\ \psi(\sigma) = \frac{\sigma(b)}{b}$. Eine Rechnung zeigt, dass das ein Gruppenhomomorphismus ist. Angenommen $\psi(\sigma) = 1$. Dann ist $\sigma = \mathrm{id}$ auf Menge der Nullstellen und da $K(\sqrt[n]{a})/K$ Zerfällungskörper ist, ist $\sigma = \mathrm{id}$. □

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 Galoisch ist und $\mathrm{Gal}(L/K)$ diese Eigenschaft E hat.

Satz 5.4.8. *Sei $Char(K) \neq n$ 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 $\sigma \in \mathrm{Gal}(L/K)$ ein Erzeuger. Als Endormorphismus gilt $\sigma^n - \mathrm{id} = 0$. Sei μ_σ Minimalpolynom von σ. Dann gilt $\mu_\sigma \mid X^n - 1 = \prod_{\zeta \in \mu_n}(X - \zeta)$. Somit ist σ diagonalisierbar und die Eigenwerte sind die Nullstellen von μ_σ. 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 $L = \oplus_{\zeta \in \mu_n} V_\zeta$. 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 $V_1 \cong V_\zeta \cong V_{\zeta^2} \cong \ldots$. 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 $1, b, \ldots, b^{n-1}$ 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 $X^n - a \in K[X]$ □

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

Beweis. Seien $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ und $K = L_0 \subseteq L_2 \subseteq \cdots \subseteq L_n$ Ketten von einfachen Radikalerweiterungen. Dann ist $K = K_0 \subseteq \ldots K_r = K_r L_0 \subseteq K_r L_1 \subseteq \cdots \subseteq K_r L_n$ 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 $a_i^n \in K_r L_{i-1}$ □

Lemma 5.4.10. *Sei L/K eine endliche Körpererweiterung in Charakterisitk 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 $a = a_1, \ldots, a_r \in \bar{K}$ 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. □

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 Galoisch. Sei $n = [L : K]$ und $K' = K(\mu_n)$ und $L' = L(\mu_n)$. Da L/K Galoisch ist L'/K' Galoisch und L'/K Galoisch. Es sind $\mathrm{Gal}(K'/K)$ und $\mathrm{Gal}(L'/L)$ abelsch, insbesondere auflösbar. Es ist

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

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

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

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 $\mathrm{Gal}(L/K)$ mit primzyklischen Quotienten. Das entsprich $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$ mit K_i/K_{i-1} Galoisch und $\mathrm{Gal}(K_i/K_{i-1}) \cong \mathbb{Z}/p_i\mathbb{Z}$. 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 Galoisch. Es gibt Kette $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L'$ sodass K_i/K_{i-1} einfache Radikalerweiterung ist. Behauptung: $\mathrm{Gal}(L'/K)$ ist auflösbar. Dann ist $\mathrm{Gal}(L/K)$ als Quotient von $\mathrm{Gal}(L'/K)$ auch auflösbar. Lemma 5.4.6 impliziert, dass K_i/K_{i-1} Galoisch ist mit zyklischer Galoisgruppe. DIe Körperkette entspricht Kette von Untergruppen in $\mathrm{Gal}(L'/K)$. Das ist eine abelsche Normalreihe. □

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

Beweis. Haben injektiven Gruppenhomomorphismus $G \to S_4$. Da S_4 auflösbar ist, ist G auflösbar. □

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

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

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 Galoisch mit $\mathrm{Gal}(L/K) = G$.
   (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
   $$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \langle Fr \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$
   (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 $M/\mathbb{Q}$ Galoisch. Es ist $H = S_4 = \mathrm{Stab}(1) \subseteq S_5$ 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 Galoiskorrespondenz $\bigcap_{g \in S_5} gHg^{-1} = \{e\}$, 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 $\deg(f) = [\mathbb{Q}(a) : \mathbb{Q}] = 5$ □

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 Idea $I \subseteq R$ 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. □

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* $\operatorname{Spec}(R) = \operatorname{Spec}(R_1) \coprod \operatorname{Spec}(R_2)$.

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. □

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. □

Definition 6.1.5. Sei R ein kommutativer Ring. Sei $n \in \mathbb{N}$ gegeben sodass $(n) = \ker(\mathbb{Z} \to R)$.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. □

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 korrespondier mit selber Begründung jedes (p_i) zu einem maximalen Ideal in $\mathbb{Z}/n\mathbb{Z}$. □

Lemma 6.1.9 (Primvermeidung)**.** *Sei $\mathfrak{a} \subseteq R$ ein Ideal. Wenn $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ 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. □

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 $\delta \colon R \setminus \{0\} \to \mathbb{N}$ 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 $I = (q)$. □

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 $c \in R^*$. □

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. □

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 Assoziertheit.

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. □

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

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

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, das der Ring lokal ist. also folgt die Aussage. □

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 $I \subsetneq \mathfrak{p}$ dann gibt es $x \in I \setminus \mathfrak{p}$. Für $y \in J$ gilt dann $xy \in \mathfrak{p}$ also $y \in \mathfrak{p}$ □

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 $\mathfrak{m} = \mathfrak{m}'$. □

Beispiel 6.2.13. Es sei R der Ring der stetigen Funktionen $f : \mathbb{R} \to \mathbb{R}$. 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 $eval_x \colon R \to \mathbb{R}, f \mapsto f(x)$. 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

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

. 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 $I \subsetneq \mathfrak{m}_x$. Also hat R maximale Ideale die nicht von der Form $\mathfrak{m}_x$ sind.

6.3 Jacobson und Nilradical

Definition 6.3.1. Sei R ein Ring und $j(R) = \cap_{\mathfrak{m} \in \operatorname{Specm}(R)} \mathfrak{m}$ das Jacobson Radikal von R. Wenn $R = \{0\}$ dann setzte $j(R) = \{0\}$. 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 $a \in j(R)$. □

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

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

Beweis. Sei a nicht nilpotent. Dann ist $0 \notin S = 1, a, a^2, \ldots$ 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 $a \notin \operatorname{rad}(R)$. Die andere Inklusion ist klar. □

Lemma 6.3.5. *Es ist äquivalent:*

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

Beweis. klar. □

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

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

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

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

Die letzte Abbildung ist surjektiv auf den Körper $K(x_1, \ldots, x_n)$ (Betrachte Minimalpolynom und dann modifiziere um Element zu erhalten). Also ist $K[X_1, \ldots, X_m]/\mathfrak{m}_x \cong K(x_1, \ldots, x_n)$ Körper und somit $\mathfrak{m}_x$ maximales Ideal in $K[X_1, \ldots, X_n]$. $f \in j(K[X_1, \ldots, X_n])$ 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. □

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

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

. 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

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

$S^{-1}R$ heißt Lokalisierung von R mit S. Es gibt Ringhomomorphismus $\tau : R \to S^{-1}R, a \mapsto \frac{a}{1}$. Es ist $\ker(\tau) = \{a \in R \mid \exists s \in S \colon as = 0\}$ und $S^{-1}R \neq 0 \iff 0 \notin S$ and τ ist bijektiv wenn $S \subseteq R^*$. Wenn R ein Integritätsbereich ist, dann ist $S = R \setminus \{0\}$ multiplikativ und wir definieren $\operatorname{Quot}(R) = S^{-1}R$. 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:*

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

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 $S \cap \mathfrak{a} =$. Wenn $\mathfrak{p} \subseteq R$ prim ist mit $S \cap \mathfrak{p} = \emptyset$ dann ist $q = \mathfrak{p}S^{-1}R$ prim, denn wenn $\frac{a}{s}, \frac{a'}{a} \in S^{-1}R$ 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 $x \in b$ 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. □

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 $\mathfrak{a}'S^{-1}\mathbb{Z} = \{\frac{6y}{3^m} \mid y \in \mathbb{Z}, m \in \mathbb{N}\} = \mathfrak{a}S^{-1}\mathbb{Z}$.

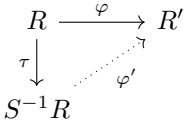
Korollar 6.4.4. *$\tau\colon R \to S^{-1}R$ induziert Isomorphismus*

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

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. □

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



Wenn $\varphi\colon R \to R'$ dieselbe Eigenschaft erfüllt wie τ, dann ist φ' Isomorphismus.

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

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

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

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 Isomoprhismus*

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

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

Beweis. Sei $\varphi : R \to R'$ Ringhomomorphismus sodass $\varphi(S) \subseteq (R')^*$. Definiere $\tilde{\varphi}\colon R[T] \to R'$ durch φ und $t_i \mapsto \varphi(f_i)^{-1}$. Dann ist $\ker(\tilde{\varphi}) = (1 - f_i t_i \mid i \in I)$ was $\varphi' : R[T]/(1 - f_i t_i \mid i \in I) \to R'$ induziert sodass $\varphi = \varphi' \circ \tau$ wobei $\tau : R \to R[T]/(1 - f_i t_i \mid i \in I)$. φ' 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 □

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

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 $(\mathbb{Z}/12\mathbb{Z})[3^{-1}] \to \mathbb{Z}/4\mathbb{Z}$ und jeder Zwischenring $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ ist eine Lokalisierung von $\mathbb{Z}$.

Beweis. Sei $\varphi\colon \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Einheiten von $\mathbb{Z}/12\mathbb{Z}$ sind $1, 5, 5, 11$ und diese gehen auf Einheiten in $\mathbb{Z}/4\mathbb{Z}$. Sei $\tau'\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}[-3]$, $x + 4\mathbb{Z} \mapsto \frac{x+12\mathbb{Z}}{1}$. Das ist wohldefiniert wie man prüft und τ' 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 Primzaheln p sodas $\frac{1}{p} \in R$. 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 $\varphi\colon R \to R'$ ein Ringhomomorphismus. $x \in R'$ heißt ganz über R, wenn es eine Ganzheitsgleichung $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ erfüllt für $a_1, \ldots, a_n \in R$. R' heißt ganz über R, falls jedes $x \in R'$ ganz ist. φ 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 $\varphi\colon R \to R'$ 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 $\sigma\colon K \to K$ 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 $n = 1 \mod 4$.

Beweis. Wenn $a^n + b_1 a^{n-1} + \cdots + b_n = 0$ mit $b_i \in \mathbb{Z}$ dann ist auch $\sigma(a)^n + b_1\sigma(a)^{n-1} + \cdots + b_n = 0$ also ist $\sigma(a)$ ganz. Die Rückrichtung geht genauso unter Verwendung dass σ injektiv ist. Wenn a ganz ist, Sei $F \in \mathbb{Z}[X]$ Ganzheitsgleichung. Sei μ 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 $(X - (a - b\sqrt{n}))(X - (a + b\sqrt{n})) = X^2 - 2aX + a^2 - b^2 n$. Also ist $a \in \mathbb{Z}$ oder $a \in \frac{1}{2} + \mathbb{Z}$. Wenn $a \in \mathbb{Z}$ dann ist $b^2 n \in \mathbb{Z}$ 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 $b^2 n \in \frac{1}{4} + \mathbb{Z}$ also $b \in \frac{1}{2} + \mathbb{Z}$ und außerdem $b^2 n \in \frac{1}{4} + \mathbb{Z} \implies n = 1 \mod 4$. □

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

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$

ist. Also ist

$$y^n = -a_1 y^{n-1} - \cdots - a_n$$

und somit

$$y = x^{n-1} y^n = -a_1 y^{n-1} x^{n-1} - \cdots - a_n x^{n-1} \in R$$

. also ist R Körper. Sei andersrum R ein Körper und $x \in R'$ mit $x \neq 0$. Dann gibt es $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit $a_i \in R$. Da R' Integritätsbereich ist ohne Einschränkung $a_n \neq 0$. Im Quotientenkörper gilt

$$-x^{-1} a_n = x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} \in R'$$

. Also ist

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

also ist R' ein Körper. □

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

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

Beweis. Klar □

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

1. *x ist integralt über R.*
2. *Der Unterring $R[x] \subseteq R'$ ist endlich erzeugt als R-Modul.*
3. *Es gibt endlich-erzeugten R-Untermodul $M \subseteq R'$ sodass $1 \in M$ und $xM \subseteq M$.*
4. *Es gibt eine $R[x]$-Modul M sodss 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 Δ 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 $\det(\delta_{ij}X - a_{ij})$ Poylon über R das bei x verschwindet.

□

Korollar 7.1.7. *Jeder endliche Ringhomomorphismus $R \to R'$ ist ganz*

Beweis. sei $M = R'$ Dann ist M endlich erzeugt. Nach Teil 3 von ?? ist $R \to R'$ ganz. □

Korollar 7.1.8. *sei $\varphi\colon R \to R'$ Ringhomomorphismus und $y_1, \dots, y_r \in R'$ ganz über R sodass $R' = R[y_1, \dots, y_n]$. dann ist φ 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 inst R' endlich. □

Korollar 7.1.9. *Seien $\varphi\colon R \to R'$ und $\varphi'\colon R' \to R''$ 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 $R \to R[b_1, \dots, b_n, z]$ endlich und damit ganz. Also ist $R \to R''$ ganz. □

Lemma 7.1.10. *Sei $R \to R'$ injektiv und $\bar{R} = \{x \in R' \mid x \text{ ganz}\}$ Dann ist $R \subseteq \bar{R} \subseteq R'$ Unterring, gennant 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 $R \to \bar{R} \to \bar{\bar{R}}$ ganz also $\bar{R} = \bar{\bar{R}}$. □

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 ohen 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 $R \subseteq R_S \subseteq \mathrm{Quot}(R)$ und $\mathrm{Quot}(R_S) = Q(R)$. Sei $x \in \mathrm{Quot}(R)$ ganz über R_S und

$$x^n + \frac{a_1}{s_1}x^{n-1} + \ldots \frac{a_n}{s_n} = 0$$

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. □

Lemma 7.2.4. *Sei A nullteilerfrei und $K = \mathrm{Quot}(A)$ 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

$$b^n + a_1 b^{n-1} + \cdots + a_0 = 0$$

dann ist

$$x^n + \frac{a_1}{s}x^{n-1} + \cdots + \frac{a_n}{s^n} = 0$$

und somit x ganz über $S^{-1}A$. Sei $x \in L$ ganz über $S^{-1}A$

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

sei $s = s_1 \cdots s_n$ dann ist sx ganz über A also $sx \in B$ und $x \in S^{-1}B$. □

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 noraml für alle $\mathfrak{m} \subseteq R$ maximal.*

Beweis. 1 impliziert 2 nach Lemma ?? 2 nach 3 ist klar. Gelte 3. und Sei $x \in \mathrm{Quot}(R)$ 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 $x \in \bigcap R_\mathfrak{m}$. 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 $\sum_\mathfrak{m} c_\mathfrak{m} b_\mathfrak{m} = 1$ mit $c_\mathfrak{m} \in R$ und $c_\mathfrak{m} = 0$ fast immer 0. Also ist

$$x = (\sum_\mathfrak{m} c_\mathfrak{m} b_\mathfrak{m})x = \sum_\mathfrak{m} c_\mathfrak{m} a_\mathfrak{m} \in R.$$

Also ist R normal. □

Lemma 7.2.6. *Sei A normaler Integritätsbereich und $K = \mathrm{Quot}(A)$. 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 $a_n x^n + \cdots + a_1 x + a_0 = 0$ mit $a_i \in A$ und $a_n = 0$. Sowas findet man immer, wähle zum Beispiel Minimalpolynom über K und Multipliziere mit allen Nennern. Dann ist $(a_n x)^n + \cdots + a_1'(a_n x) + a_0' = 0$ mit $a_i' \in A$. Also ist $a_n x$ ganz über A und damit in B. Also ist $x = \frac{b}{a}$ wie oben. Somit ist $\mathrm{Quot}(B) = L$ und B normal. □

Satz 7.2.7. *Sei A noethersch und normal und $K = \mathrm{Quot}(A)$. 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 $G = \mathrm{Gal}(L/K)$. Für $x \in L$ ist $Tr(x) = \sum_{g\in G} g(x)$. Sei $\frac{y_1}{x_1}, \ldots, \frac{y_n}{x_n}$ Basis von L über K mit $x_i \in A$ und $y_i \in B$ wie in ????. Dann ist auch $y_1, \ldots, y_n$ eine Basis von L. Da Tr nicht-ausgeartet ist nach ??? definiert $y \mapsto (x \mapsto Tr(xy))$ eine injektive Abbildung $L \to L^\vee = \mathrm{Hom}(L, K)$, 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 $Tr(x_i y_j) = \delta_{ij}$. Jedes ¸$b \in B$ kann geschrieben werden als $b = \sum c_i x_i$ mit $c_i \in K$ also dann $c_j = Tr(by_j) \in A$ Also ist $B \subseteq \sum Ax_i$. □

7.3 Going Up

Satz 7.3.1. *Sei $\varphi\colon R \to R'$ 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 $R/\mathfrak{q} \to R'/\mathfrak{p}$ ganz und injektiv nach ???. Dann ist

$$R/\mathfrak{q} \text{ Körper} \iff R'/\mathfrak{p} \text{ Körper}$$

nach Lemma 7.1.3. Sei nun $\mathfrak{p} = \mathfrak{p}_1 \cap R = \mathfrak{p}_2 \cap$ wie im Satz sodass $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$. Dann ist für $S = R \setminus \mathfrak{p}$ die Abbildung $R_S \to R'_{\varphi(S)}$ 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 $\mathfrak{p}_1 = \mathfrak{p}_2$ □

Satz 7.3.2 (Living Over)**.** *Sei $\varphi\colon R \to R'$ ein ganzer Ringhomomorphismus und $\mathfrak{p} \subseteq R$ ein Primideal sodass $\ker(\varphi) \subseteq \mathfrak{p}$. dann gibt es ein Primdieal $\mathfrak{q} \subseteq R'$ sodass $\mathfrak{q} \cap R = \mathfrak{p}$.*

Beweis. Sei $S = R \setminus \mathfrak{p}$. Dann ist $R_S \to R'_{\varphi(S)}$ 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 $\mathfrak{q} \cap R = \mathfrak{p}$. □

Satz 7.3.3 (Going Up)**.** *Sei $\varphi\colon R \to R'$ ganzer injektiver Ringhomomorphismus und*

$$\mathfrak{p}_0 \subseteq \ldots \mathfrak{p}_n$$

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

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$$

in R' mit $\mathfrak{q}_i \cap R = \mathfrak{p}_i$

Beweis. Es reicht der Fall $n = 1$. Es ist $R/\mathfrak{p}_0 \to R'/\mathfrak{q}_0$ ganz und injektiv. Nach Living Over existiert $\mathfrak{q} \subseteq R'/\mathfrak{q}_0$ über $\bar{\mathfrak{p}_0}$. Sei $\mathfrak{q}_1$ Urbild von $\mathfrak{q}$ unter $R' \to R'/\mathfrak{q}_0$. Dann ist $\mathfrak{q}_n \cap R = \mathfrak{p}_n$. □

7.4 Going Down

Lemma 7.4.1. *Sei $R \to R'$ 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 $y_1, \ldots, y_n$. 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 Koeffizeinten in I. □

Lemma 7.4.2. *Sei $\varphi\colon R \to R'$ injektiv und $s \in R'$ ganz. Seien R, R' Integritätsrings und R normal. Es gilt*

1. *Das Minimalpolynom $f \in \mathrm{Quot}(R)[X]$ 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 $K = \mathrm{Quot}(R)$ und $L = \mathrm{Quot}(R')$ 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 $K \cap R[S_1, \ldots, s_n]$ also sind die Koeffizienten ganz. Da R normal ist sind die Koeffienten in R. Für den zweiten Teil wähle nach Lemma ??? h so, dass Koeffizeinten 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 Primdieal $\mathfrak{P} \subseteq R'$ 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 $\mathfrak{P} \cap R = \mathfrak{p}$.

□

Satz 7.4.3 (Going Down)**.** *Sei $\varphi\colon R \to R'$ ganz und injektiv und R und R' Integritätsringe sodass R normal ist. Für eine Kette von Primidealen*

$$R \supseteq \mathfrak{p}_o \supseteq \cdots \supseteq \mathfrak{p}_n$$

und einem Primideal $\mathfrak{q}_0 \subseteq R'$ mit $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$ gibt es Kette von Primidealen

$$R' \supseteq \mathfrak{q}_0 \supseteq \cdots \supseteq \mathfrak{q}_n$$

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 $x \in \mathfrak{p}_1 R' \cap R$, $x = u \cdot v$ 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 $R[v, s_1, \ldots, s_k], \mathfrak{q}_0 \cap R[v, s_1, \ldots, s_k]$ 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 $K = \mathrm{Quot}(R)$. Nach ??? ist $f = Z^d + r_{d-1}Z^{d-1} + \cdots + r_0 \in R[X]$ da R normal ist. Sei $g = Z^d + u \cdot r_{d-1}Z^{d-1} + \cdots + u^d \cdot r_0$. 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 $v \in \mathfrak{p}_0 \subseteq \mathfrak{q}_o$ 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 $S' = R' \setminus \mathfrak{q}0$. □

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

$$K[Y_1, \dots, Y_n] \to K[y_1, \dots, y_n]$$

ein Isomorphismus ist. Wenn $R = L$ ein Körper ist, so heißt eine maximal algebraisch unabhängige Teilmege 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 $\bar{I} = \{\bar{m} = (m_2, \dots, m_n) \mid \exists m_1 \colon (m_1, m_2, \dots, m_n) \in I\}$ 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 $\sum_{i=1}^n r_i m_i \neq \sum_{i=1}^n r_i m_i'$. □

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 $\varphi \colon K[X_1, \dots, X_n] \to A$ 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 $K[y_1, \dots, y_{n-1}, y] \to A$ 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 bestimmtwerden und setze $r_n = 1$. Definiere Relation G über $K[y_1, \dots, y_{n-1}]$ durch

$$G(y_1, \dots, y_{n-1}, x_n) = F(y_1 + x_n^{r_i}, \dots, y_{n-1} + x_n^{r_{n-1}}, x_n) = F(x_1, \dots, x_n) = y$$

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 nciht alle Terme wegheben. Da $a_m \neq 0$ wo das Maximum angenommen wird, ist x_n ganz über $K[y_1, \dots, y_{n-1}, y]$. □

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 $K[y_1, \dots, y_{n-1}] \to K[x_1, \dots, x_n]$ 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

$$K[Y_1, \dots, Y_n] \to K[y_1, \dots, y_n]$$

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. □

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*

$$\dim(K[X_1, \ldots, X_n]) = n.$$

Beweis. Primideale $\mathfrak{p}_i = (X_1, \ldots, X_i)$ bilden Kette der Länge n. Der Fall $n = 0$ ist klar. Sei $R = K[X_1, \ldots, X_n]$ 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 $J = (g_1, \ldots, g_n)$. 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

$$S^{-1}R = (S^{-1}K[X_n])[X_1, \ldots, X_{n-1}] = K(X_n)[X_1, \ldots, X_{n-1}].$$

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. *$R = K[X_1, X_s, \ldots]$ hat Dimension ∞.*

Definition 7.6.5. Sei I ein Ideal von R. Definiere $\mathrm{ht}(I)$ als das Supremum von Längen von Ketten von Primidealen in I und coht als das Supremum von Lägen 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 $K = \mathrm{Quot}(R)$ ist $R = \bigcap_{\mathrm{coht}\mathfrak{p}=1 \ prim} R_\mathfrak{p}$.*

Beweis. Es ist $(0) \subseteq (p)$ also $oht(p) \geq 1$. 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 $\mathrm{ht}(p) = 1$. Genauso zeigt man, dass jedes Primideal der Höhe 1 von dieser Form ist. Klar ist, dass $R \subseteq \bigcap R_\mathfrak{p}$. Sei also $x \in \bigcap R_p$ 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. $\mathrm{ht}(\mathfrak{p}) = \dim(R_\mathfrak{p})$ *für ein Primideal* $\mathfrak{p}$ *von R und* $\mathrm{coht}(I) = \dim(R/I)$
2. $\mathrm{ht}(I) = \min_{I \subset \mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{ht}(\mathfrak{p})$
3. $\dim(R) = \sup_{\mathfrak{p} \in \mathrm{Spec}\, R}(R_\mathfrak{p}) = \sup_{\mathfrak{p} \in \mathrm{Specm}}(R_\mathfrak{p}))$

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

$$\sup \dim(R_\mathfrak{p}) = \sup \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}_d) = d$$

□

Satz 7.6.8. *Sei $R \to R'$ ganz und injektiv. Sei $I' \subseteq R'$ ein Ideal und $I = I' \cap R$. Dann gilt*

1. $\dim(R') = \dim(R)$
2. $\mathrm{ht}(I) \leq \mathrm{ht}(I)$ *und* $\mathrm{ht}(I) = \mathrm{ht}(I)$ *wenn R, R' Integritätsbereiche und R normal ist.*
3. $\mathrm{coht}(I) = \mathrm{coht}(I')$.

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 $\mathrm{ht}(I') \leq \mathrm{ht}(I)$. Wenn I' nicht prim ist, wähle $\mathfrak{p}$ minimal mit $I \subseteq \mathfrak{p}$. Nach **??** zu $R/I \to R'/I'$ gibt es minimales $I' \subseteq \mathfrak{q}$ prim das über $\mathfrak{p}$ liegt. also ist $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p}$ und somit $\mathrm{ht}(I') \leq \mathrm{ht}(I)$. Wenn R, R' Integritätsbereiche mit R normal, dann lässt sich auch jede Kette mit Going Up heben, sodass die Höhen gleich sind. □

Satz 7.6.9. *Sei A eine K- Algebra von endlichem Typ und A ein Integritätsbereich. Dann ist*

$$\dim(A) = \mathrm{transdeg}_K(\mathrm{Quot}(A)$$

Beweis. Nach Noether Normalisierung gibt es injektiven endlichen Morphismus $K[X_1, \ldots, X_d] \to A$. Nach Satz 7.6.8 ist $\dim(A) = \dim(K[x_1, \ldots, X_d]) = d$. Außerdem ist

$$\begin{aligned} d &= \mathrm{transdeg}_K(\mathrm{Quot}(K[X_1, \ldots, X_d])) \\ &= \mathrm{transdeg}_K(\mathrm{Quot}(A)) \end{aligned}$$

da $\mathrm{Quot}(A)/\mathrm{Quot}(K[X_1, \ldots, X_d])$ algebraisch ist. □

Satz 7.6.10. *Sei A eine K - Algebra von endlichem Typ, A ein Integritätsbereich. Dann ist*

1. $\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) = \dim(A)$ *für alle primdieale $\mathfrak{p} \subseteq A$*
2. $\mathrm{ht}\mathfrak{m} = \dim(A)$ *für alle maximalen Ideale.*

Beweis. 2 folgt aus 1. Nach ??? gibt es endlichen Monomorphismus $K[x_1, \ldots, x_d] \to A$ mit $\dim(A) = d$ und $x_1, \ldots, x_d$ 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 $y \in \mathfrak{p} \cap K[x_1, \ldots, x_d]$ mit $y \neq 0$. Das existiert da $\mathfrak{p} \neq 0 \implies \mathfrak{p} \cap K[x_1, \ldots, x_d] \neq 0$ nach Satz ???. Nach Lemma ??? gibt es $y_1, \ldots, y_{d-1} \in K[x_1, \ldots, x_d$ such that $K[y_1, \ldots, y_{d-1}, y] \to K[x_1, \ldots, x_d]$ ist endlich und injektiv und $y_1, \ldots, y_{d-1}, y$ algebraisch unabhängig. Dann ist $K[y_1, \ldots, y_{d-1}, y] \to A$ endlich und da $K[y_1, \ldots, y_{d-1}, y]$ normal nach ??? (faktoriell impliziert normal). Nach Going Down gibt es Ideal $\mathfrak{p}_0 \subseteq \mathfrak{p} \subseteq A$ mit $\mathfrak{p}_0 \cap K[y_1, \ldots, y_{d-1}, y] = (y_d)$. Betrachte Monomorphismus $K[Y_1, \ldots, Y_{d-1} \to A/\mathfrak{p}_0$ und Ideal $\mathfrak{p}/\mathfrak{p}_0$. Nach Induktion ist

$$\mathrm{ht}(\mathfrak{p}/\mathfrak{p}_0) + \mathrm{coht}(\mathfrak{p}/\mathfrak{p}_0) = d - 1$$

Da $\mathrm{ht}\mathfrak{p} \geq \mathrm{ht}(\mathfrak{p}/\mathfrak{p}_0) + 1$ und $\mathrm{coht}(\mathfrak{p}) = \mathrm{coht}(\mathfrak{p}/\mathfrak{p}_0)$ ist

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \geq d$$

und somit $= d$. □

Bemerkung 7.6.11. Es gilt

$$\mathrm{ht}(\mathfrak{p}) = \dim(R_\mathfrak{p}) = \mathrm{transdeg}_K(\mathrm{Quot}(R_\mathfrak{p})) = \mathrm{transdeg}_K(\mathrm{Quot}(A))$$

Nach Satz ??? und $\mathrm{coht}(\mathfrak{p}) = \mathrm{transdeg}_K(\mathrm{Quot}(A/\mathfrak{p})$ Also haben wir

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{transdeg}_K(\mathrm{Quot}(A)) - \mathrm{transdeg}_K(k(\mathfrak{p}))$$

mit $k(\mathfrak{p}) = \mathrm{Quot}(A)$.

Satz 7.6.12. *Jede maximale Kette von Primidealen $\mathfrak{q}\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}$ hat Länge*

$$d = \mathrm{transdeg}_K(k(\mathfrak{q})) - \mathrm{transdeg}_K(k(\mathfrak{p}))$$

Beweis. Sei $n = \mathrm{transdeg}_K(k(\mathfrak{q}))$, $m\,\mathrm{transdeg}_K(k(\mathfrak{p}))$. Da $\dim(A/\mathfrak{p}) = n$ nach Satz ?? gibt es $\mathfrak{p} = \mathfrak{p}_d \subsetneq \cdots \subsetneq \mathfrak{p}_{d+n}$ in A. Da $\dim(A/\mathfrak{q} = m$ folgt, dass $d + n \leq m$ also $d \leq m - n$. Sei $\mathfrak{q} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ aufsteigende Kette. Da $\mathrm{ht}(\mathfrak{p}/\mathfrak{q}) + \mathrm{coht}(\mathfrak{p}/\mathfrak{q}) = \dim(A/\mathfrak{q})$ 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 $= m - n$. □

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. □

Korollar 8.1.2. *Sei K ein Körper und $f\colon A \to B$ 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 $K \to A/f^{-1}(\mathfrak{m}) \to B/\mathfrak{m}$ injektiv, da $B\mathfrak{m}$ eine endliche Körpererweiterung nach Schwachen NstSatz. Dann sind $K \to A/f^{-1}(\mathfrak{m}) \to B/\mathfrak{m}$ alle ganz und damit $A/f^{-1}(\mathfrak{m})$ □

Beispiel 8.1.3. Sei K ein Körper und $R = K[X_1, \dots, X_m]$ 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 $\mathfrak{m} \subseteq R = K[X_1, \dots, X_m]$ 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 $\pi\colon R \to R/\mathfrak{m}$ ist $f \mapsto f(a_1, \dots, a_n)$. Das heißt es gibt Bijektion $K^n \to \operatorname{Specm}(R)$, $(a_1, \dots, a_n) \mapsto (X - a_1, \dots, X_n - a_n)$.*

Beweis. Sei $L = K[X_1, \dots, X_n]/\mathfrak{m}$. Dann ist nach ??? L/K algebraisch also $L = K$. Das heißt $\pi\colon K[X_1, \dots, X_n] \to K$ 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 $K[X_1, \dots, X_n] \to K, f \mapsto f(a_1, \dots, a_n)$ hat dieses Ideal als Kern. □

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 $f_1(p) = \cdots = f_m(p) = 0$.

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 $\operatorname{Specm} A$ 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 $(a_1, \dots, a_n) \in V(J)$. □

Bemerkung 8.1.7. Es gibt zwei Abbildungen

$$\{J \subseteq K[X_1, \ldots, X_n] \text{ Ideal}\} \underset{I}{\overset{V}{\rightleftarrows}} \{X \subseteq K^n \text{ Teilmenge}\}$$

wobei $I(X) = \{f \in K[X_1, \ldots, X_n] \mid f(p) = 0 \, \forall p \in X\}$ 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 ist Varietät $\iff X = V(I(X))$
5. $J \subseteq I(V(J))$.

Bemerkung 8.1.8. Sei K algebraisch abgeschlossen und $R = K[X_1, \ldots, X_n]$ und $Y \subseteq R$ eine Teilmenge. Dann gilt

1. $V(Y) = V((Y))$
2. $V(f) = V(f^n)$
3. $I \subseteq R$ Ideal $\implies V(\sqrt{J}) = V(J)$
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 abgeschlossenere Körper.*

1. *wenn $J \subsetneq K[X_1, \ldots, X_n]$ dann ist $V(J) \neq \emptyset$.*
2. *$I(V(J)) = \operatorname{rad}(J)$*

Das heißt I und V induzieren inverse Bijektionen

$$\{\text{Radikale } J = \sqrt{J} \subseteq K[X_1, \ldots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{ \text{ Varietäten } V \subseteq K^n\}$$

Beweis. Sei $J \subseteq \mathfrak{m}$ für ein maximales Ideal $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$.
Dann ist $P = (a_1, \ldots, a_n) \in V(J)$ Angenommen $f \in K[X_1, \ldots, X_n]$ sodass $f(p) = 0$ für alle $p \in V(J)$. Sei $J' = (J, fY - 1) \subseteq K[X_1, \ldots, X_n, Y]$. Ein Punkt $p \in V(J')$ ist $(n+1)$-Tupel $(a_1, \ldots, a_n, b) \in K^{n+1}$. Angenommen $V(J') \neq \emptyset$. Dann gibt es so einen Punkt p und $p' = (a_1, \ldots, a_n)$ ist dann in $V(J)$. Da aber $bf(a_1, \ldots, a_n) = 1$ ist, ist das ein Widerspruch. Also ist $V(J') = \emptyset$ und somit $J' = K[X_1, \ldots, X_n, Y]$ Also gibt es Gleichung

$$1 = \sum g_i h_i + g_0(fY - 1)$$

mit $g_i \in K[X_1, \ldots, X_n, Y]$ und $h_1 \in J$. Multipliziere die Gleichung mit f^m sodass Y nur in Kombination mit f auftritt und erhalte

$$f^m = \sum G_i(X_1, \ldots, X_n, fY)h_1 + G_0(X_1, \ldots, X_n, fY)(fY - 1)$$

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 $\operatorname{rad}(J) \subseteq I(V(J))$ 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 $f \in I(V(J))$. □

Bemerkung 8.1.10. 1. Der Satz hat den Namen wegen 1. Sei M eine Menge von Poylonomen in $K[X_1, \ldots, X_n]$ 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 $\operatorname{rad} J = \bigcap_{J \subset \mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$ 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 $\varphi\colon X \to Y$ heißt polynomiell, wenn es $f_1, \ldots, f_m \in K[X_1, \ldots, X_m]$ gibt sodas $\varphi(x) = (f_1(x), \ldots, f_m(x))$ 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 $A(X) = K[X_1, \ldots, X_n]/I(X)$.

Lemma 8.1.12. *Für abgeschlossene $X \subseteq K^n$ und $Y \subseteq K^m$ gibt es Bijektion*

$$\{\varphi\colon X \to Y \text{ polynomiell } \} \to \operatorname{Hom}_{K-\mathsf{Alg}}(A(Y), A(X))$$

Beweis. Angenommen $g \in \operatorname{Hom}_{K-\mathsf{Alg}}(A(Y), A(X))$ gegeben. Betrachte

$$\begin{array}{ccc} K[X_1, \ldots, X_m] & \dashrightarrow & K[X_1, \ldots, X_m] \\ \downarrow & & \downarrow \\ A(Y) & \xrightarrow{\quad g \quad} & A(X) \end{array}$$

Sei $f_i \in K[X_1, \ldots, X_n]$ ein Urbild von $g(\bar{X}_i)$. Dann definieren $f_1, \ldots, f_m$ eine polynomielle Abbildung $\varphi\colon X \to Y, x \mapsto (f_1(x), \ldots, f_m(x))$. Wenn andersrum φ gegeben ist, dann ist $\varphi^*\colon A(Y) \to A(X), \varphi^*(f) = f \circ \varphi$ eine Abbildung von K -Algebren. □

Bemerkung 8.1.13. Sei K ein Körper und $R = K[X_1, \ldots, X_n]$. 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 $V(J) = V(I(V(J)) = \cdots = V(J')$

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 $f, g \in A = K[X_1, \ldots, X_n] \setminus I$ 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 $I(X)$ primist 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 $X = V(J_2)$. □

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 $(X - a, X - b)$ 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*

$$\begin{array}{ccc} \left\{ \text{ Radikale } J = \sqrt{J} \subseteq K[X_1, \ldots, X_n] \right\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{ \text{ Varietäten } X \subseteq K^n \} \\ \uparrow & & \uparrow \\ \{ \text{ Primideale } \mathfrak{p} \subseteq K[X_1, \ldots, X_n] \} & \rightleftarrows & \{ \text{ irreduzible Varietäten } X \subseteq K^n \} \end{array}$$

Also ist $\operatorname{Spec} K[X_1, \ldots, X_n] = \{$ *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*

$$\operatorname{Spec} A \leftrightarrow \{ \textit{ irreduzible Varietäten } X \subseteq V(J)\}$$

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 heir der Co-endlichen Topologie. Die Zariski-Topologie ist nicht Hausdorf, 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. □

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 $X_i \subsetneq \bigcup_{i \neq j} X_j$.

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 Untervaritäten von X. Da X noethersch ist, muss diese abbrechen. □

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 $I(V(J)) = \sqrt{J} = J$ □

Definition 8.1.25. Sei A ein Ring. Die Zariski-Topologie auf $\operatorname{Spec} A$ ist gegeben durch die abgeschlossenen Mengen $V(J) = \{\mathfrak{p} \in \operatorname{Spec} A \mid J \subseteq \mathfrak{p}\}$ 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 $A \to A/\mathfrak{p}$.

Lemma 8.1.27. *Sei R ein Ring und $\mathfrak{p} \in \operatorname{Spec}(R)$. Es gilt*

1. *$V(\mathfrak{p})$ ist der Abschluss von $\{\mathfrak{p}\}$.*
2. *$\{\mathfrak{p}\} \subseteq \operatorname{Spec}(R)$ 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. □

Bemerkung 8.1.28. Sei $X \subseteq \operatorname{Spec} A$ und $I(X) \coloneqq \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$. 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

$$\begin{array}{ccc} \left\{ \text{ Radikale } J = \sqrt{J} \subseteq A \right\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{ \text{ abgeschlossene } X \subseteq \operatorname{Spec} A \} \\ \uparrow & & \uparrow \\ \{ \text{ Primideale } \mathfrak{p} \subseteq A \} & \rightleftarrows & \{ X \subseteq \operatorname{Spec} A \text{ irreduzibel } \} \end{array}$$

und analog impliziert A noethersch, dass $\operatorname{Spec} A$ noethersch ist und in dem Fall jede abgeschlossene Menge von $\operatorname{Spec} A$ 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. *$\operatorname{rad} J$ ist Schnitt endlich vieler Primideale.*
3. *Wenn A Nullteiler hat, dann hat A entweder nicht-triviale nilpotente Elemente oder endliche Anzahl ≥ 2 von minimalen Primidealen*

Beweis. 1 und 2 sind klar. Angenommen $\operatorname{rad} A = 0$. Es ist $\operatorname{rad} A = \bigcap \mathfrak{p}_i$ 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. □

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 $V_1, \ldots, V_k$ 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

$$V_{k+1} = (\bigcup_{i=1}^{k+1} U_{i_k})^c \subsetneq V_k$$

. Das ist abgeschlossen und gibt absteigende Kette abgeschlossener Mengen $V_1 \supsetneq V_2 \supsetneq \ldots$ was stationär wird. Also ist U quasi-kompakt. Wenn andersrum jede offene Menge quasi-kompakt ist und $V_1 \supsetneq \ldots$ Kette von abgeschlossenen Mengen ist, dann setze $U_i = V_i^c$. Dann hat $\bigcup U_i$ endliche Teilüberdeckung und die Kette wird stationär. □

Lemma 8.1.31. *Sei R ein Ring. Dann ist $\operatorname{Spec} R$ quasi-kompakt.*

Beweis. Sei $\operatorname{Spec} R = \bigcup U_i$ offene Überdeckung. Dann ist

$$\begin{aligned} \emptyset &= \bigcap U_i^c \\ &= \bigcap V(J_i) \\ &= \bigcap (\sum J_i) \end{aligned}$$

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

$$\emptyset = V(\sum_{i=1}^{n} J_{i_k})$$

und somit $\operatorname{Spec} R = \bigcup_{i=1}^{n} U_{i_k}$ □

Beispiel 8.1.32. Sei $R = K[X_1, X_2, \dots]/J^2$ mit $J = (X_1, X_2, \dots$. Es ist

$$\mathrm{Spec}(R) = \{J/J^2\}$$

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 $V_0 \subsetneq \cdots \subsetneq V_d \subseteq X$.
2. Die Krull-Dimension eines Ringes R ist das Supremun aller Längen d von Ketten von Primidealen $P_0 \subsetneq \cdots \subsetneq P_d$ in R.

Kapitel 9

Bewertungsringe und Dedekindringe

9.1 Bewertungsringe

Definition 9.1.1. Sei A Integritätsbereich und $K = \mathrm{Quot}(A)$. 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 Γ eine total geordnete abelsche Gruppe. Eine Bewertung von K ist eine surjektive Abbildung $\nu\colon K^* \to \Gamma$ sodass $\nu(xy) = \nu(x)+\nu(y)$ und $\nu(x+y) \geq |\ \{\nu(x), \nu(y)\}$ ist für alle $x, y \in K^*$. Es gilt die Konvention $\nu(0) = \infty$. ν heißt diskrete Bewertung falls $\Gamma \cong \mathbb{Z}$ ist.

Satz 9.1.3. *Sei A ein Integritätsbereich und $K = \mathrm{Quot}(A)$. Dann ist äquivalent:*

1. $\forall x \in K^*\colon x \in A$ *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 Γ (Bewertungsgruppe genannt) und eine Bewertung $\nu\colon K^* \to \Gamma$ 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 Γ und Bewertung ν. Ist ν 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 $nu\colon K^* \to \Gamma$ 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 $nu(x) = 0$ 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 $x_1, \ldots, x_n$ Erzeuger sodass $\nu(x_1) < \cdots < \nu(x_n)$. Da ν 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 $x_k = tux_1$ 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 $x^{-1} \in A$. □

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 $x = tx_1 = t^2x_2 = \cdots = t^nx_n = \ldots$ und somit $(x) \subsetneq (x_1) \subsetneq \ldots$. Da A noethersch ist, muss die Kette stoppen. □

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 $x = t^nu$ 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 $x = t^nu$ für eine Einheit u. Somit ist $\mathfrak{m} = (t)$. Wenn $x = t^nu$ 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 $n = \min\{k \mid t^n \in I\}$. Dann ist $I = (t^n)$. □

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 Bedingen 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. □

Satz 9.1.8. *Sei A Integritätsbereich. A ist diskreter Bewertungsring genau dann, wenn A noethersch, normal und* $\mathrm{Spec}(A) = \{0, \mathfrak{m}\}$ *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 $\mathrm{Spec}(0, \mathfrak{m})$ 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 $\mathrm{Ass}(M) \neq 0$ nach Satz 10.6.8. Das heißt es gibt esin $0 \neq y \in \mathfrak{m} \setminus (x)$ sodass $my \subseteq (x)$. Dann ist $\mathfrak{y}y \in A$ also $\frac{y}{x} \notin A$ aber $\frac{y}{x}\mathfrak{m} \subseteq A$ ein Ideal. Angenommen $\frac{y}{x}\mathfrak{m}A = A$. 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 $\frac{y}{x}\mathfrak{m} \subseteq \mathfrak{m}$. Multiplikation mit $\mathfrak{y}y$ ist Lineare Abbildung $\varphi\colon \mathfrak{m} \to \mathfrak{m}$ zwischen endlichen A-Moduln. Wähle also Surjektion $\pi\colon R^n \to M, e_i \mapsto x_i$ und sei $B = (b_{ij})$ die Matrix mit $\varphi(x_i) = \sum b_{ij}x_j$. Nach Cayley Hamilton ??? gibt es Polynom $P = X^n + a_{n-1}X^n + \cdots + a_0$ mit $P(B) = 0$ also ist $P(\varphi) = 0$. Für $0 \neq z \in \mathfrak{m}$ ist also

$$((\frac{x}{y})^n + \cdots + a_0)z = 0$$

Also ist $\frac{x}{y}$ integral. Da A normal ist, ist $\frac{x}{y} \in A$ was Ein Widerspruch ist. Also ist $\mathfrak{m} = (x)$. □

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. □

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 $R \to R/\mathfrak{m}$ 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 $\mathrm{Quot}(R) = \mathrm{Quot}(R')$. Sei $x \in \mathrm{Quot}(R')$ 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 $x^{-1} \in R'$. □

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 $g = b_0 + b_1 X + \ldots$ sodass $1 = gf = a_0 b_0$ also ist a_0 eine Einheit. Wenn a_0 Einheit ist, dann ist $a_o^{-1} f = 1 + \ldots$ also ohne Einschränkung $a_0 = 1$. Setze $b_0 = 1$ und rekursiv $b_n = -\sum_{i=1}^{n} a_i b_{n-1}$. 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 $\frac{f}{g} \in \mathrm{Quot}(K[[X]])$ setze $\nu(\frac{f}{g}) = \nu(f) - \nu(g)$. dann ist ν eine diskrete Bewertung und $K[[X]] = \{y \mid \nu(y) \geq 0\}$. □

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, neotherscher Integritätsring der Dimension $leq1$.

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 $(0) \neq I \subseteq I$ kann geschrieben werden als Produkt $I = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ 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 Rank 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 $J = (y)$. □

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 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. □

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 $b_\mathfrak{m} \in J$ sodas $\nu_\mathfrak{m}(a) \geq \nu_\mathfrak{m}(b)$. Also ist $a \in J_\mathfrak{m}$ für alle 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

$$\nu_\mathfrak{m}(\prod_\mathfrak{n} \mathfrak{n}^{\nu_\mathfrak{n}(I)} = \sum \nu_\mathfrak{m}(frakn^{\nu_\mathfrak{n}(I)}) = \sum_\mathfrak{n} \nu_\mathfrak{n}(I)\nu_\mathfrak{m}(\mathfrak{n}) = \nu_\mathfrak{n}(I)$$

Also $I = \prod_\mathfrak{n} \mathfrak{n}^{\nu_\mathfrak{n}(I)}$. □

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 $IJ = (x)$. □

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 $I/r_0 A \subseteq A/r_0 A$. □

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. □

9.3 Idealklassengruppe

Definition 9.3.1. Ein gebrochenes Ideal von einem Dedekindring R ist ein endlich erzeugter R-Untermodul von $K = \mathrm{Quot}(R)$. 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 $\mathfrak{a} = \mathfrak{p}_2 \dots \mathfrak{p}_r$. 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. □

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 $-5 \equiv 3 \mod 4$ 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 $R = \mathbb{Z}[X]/(\mu)$ woibe i $X \leftrightarrow 1 + \sqrt{-5}$ 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 $dR \subseteq R$ ein Ideal ist. Dann ist $dI = (x)$ und $I = \frac{x}{d}R$ gebrochenes Hauptideal. Rest ist einfach. □

Satz 9.3.6. *Sei R ein Dedekindring und M ein endlich erzeugter R-Modul der Torsionsmodul ist. Dann ist* $\mathrm{Supp}(M)$ *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 $\varphi\colon M \to \bigoplus_{\mathfrak{p} \in \mathrm{Supp}(M)} M_\mathfrak{p}$. Für $\mathfrak{q} \in \mathrm{Spec}(R)$ 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 φ ein Isomorphismus. Da $R_\mathfrak{p}$ Hauptidealring ist folgt mit Struktursatz, dass jeder Torsionsmodul von der Form $\bigoplus_{n \in J} R_p/(\mathfrak{p}R_\mathfrak{p})^n R_\mathfrak{p} = \bigoplus (R/\mathfrak{p}^n)_\mathfrak{p}$ ist. Da $R/\mathfrak{p}^n$ lokal ist, ist $R/\mathfrak{p}^n)_\mathfrak{p} \cong R/\mathfrak{p}^n$. Also gilt die Aussage. □

Kapitel 10

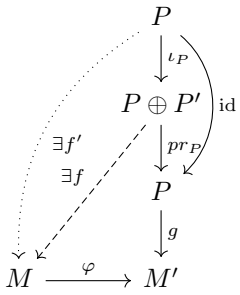
Moduln

10.1 Ext und Tor

Definition 10.1.1. Ein R-Modul P heißt projektiv, falls für jeden Epimorphismus $\varphi\colon M \to M''$ die Abbildung $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M')$ 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 $g\colon P \to M'$ und Epimorphismus $\varphi\colon M \to M'$ gegeben. Die Projektion $P \oplus P' \to P$ gibt



Also ist P projektiv. Andersrum sei P projektiv und F frei sodass $\varphi\colon F \to P$ 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 $M_0 \to P$ surjektiv. Setze Konstruktion fort mit $\ker(M_0 \to P$. □

Lemma 10.1.4. *Projektive Moduln sind flach.*

Beweis. Freie Moduln sind flach und da sich Flachheit auf direkte Summanend 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 $x_1, \ldots, x_n$ in P die auf eine Basis Abbilden in $P/\mathfrak{m}P$. Sei $f\colon R^n \to P$, $e_i \mapsto x_i$. 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 $M_* \to M$.

Beispiel 10.1.7. Seien $n, m \geq 1$. Haben freie Auflösung

$$\ldots \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

Mit $\mathbb{Z}/m\mathbb{Z}$ tensorieren gibt

$$\ldots \longrightarrow 0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}\otimes\mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

also ist für $d = \mathrm{ggT}(n,m)$:

$$Tor_0^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}\otimes\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/d\mathbb{Z}$$

$$Tor_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \frac{m}{d} = \mathbb{Z}/d\mathbb{Z}$$

$$Tor_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = 0\, i \geq 2$$

Beispiel 10.1.8. Sei $R = K[X,Y]$ für einen Körper K und $M = R/(X,Y) = K$ als R-Modul. Sei $f\colon R^2 \to R, f(\varphi,\psi) = X\varphi + Y\psi)$ und $g\colon R \to R^2$, $g(\varphi) = (Y\varphi, -X\varphi)$. 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 Ableitun von $M\otimes_R -$ aufgefasst werden.*

Beweis. Seien $M_* \to M$ und $E_* \to E$ 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 $Tot(C^{**}) \to B^*$ und $Tot(C^{**}) \to A^*$. Wenn beide Abbildungen quasi Isomorphismen sind, dann ist $H^i(B^*) = H^i(A^*)$ was die Aussage ist. In Zeile j ist $C^{**} \to B^*$ aber nichts anderes als

$$\ldots \longrightarrow M_1 \otimes E_j \longrightarrow M_0 \otimes E_j \longrightarrow M \otimes E_j \longrightarrow 0$$

was exakt ist da E_j projektiv und somit flach ist. Nach ??? ist also $Tot(C^{**} \to B^*$ 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 α endlich erzeugt ist, ist $Tor_1 = 0$. Die lange exakte Tor Sequenz liefert

$$\ldots \longrightarrow 0 = Tor_1^R(M,R) \longrightarrow Tor_1^R(M, R/\alpha) \longrightarrow M\otimes_R \alpha \longrightarrow M\otimes_R R = M \longrightarrow \ldots$$

wobei links 0 steht da R frei ist. Also ist $Tor_1^R(M, R/\alpha) \cong \ker(M \otimes_R \alpha \to M$. Für jedes endlich erzeugte Ideal $\alpha' \subseteq \alpha$ ist

$$M \otimes_R \alpha' \to M \otimes \alpha \to M$$

injektiv da $Tor_1^R(M, R/\alpha') = 0$. Wenn $z = \sum_{i=1}^n m_i \otimes a_i \in \ker(M \otimes alpha \to M)$ sei $\alpha' = (a_1, \ldots, a_r$. dann ist $z \in \ker(M \otimes alpha' \to M) = 0$. Also ist $M \otimes_R \alpha \to M$ 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 $0 \to N' \to N \to N'' \to 0$ 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 $0 \to N' \to N \to N'' \to N$ exakt. Wenn$N$ endlich erzeugt ist, dann auch N'' und somit ist $0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$ exakt. Wenn N nicht endlich, sei $z = \sum_{i=1}^r m_i \otimes n_i \in \ker(M \otimes N' \to M \otimes M \to N)$. Ersetze N' durch Modul erzeugt durch die n_i. Dann ist

$$z \in \ker(M \otimes N' \to M \otimes \Im(N')) = 0$$

somit ist M flach. □

Korollar 10.1.11. *Ein R-Modul M ist flach genau dann wenn für jedes endlich erzeugte Ideal $\alpha \subseteq R$ die Abbildung $\alpha \otimes M \to M$ injektiv ist.*

Beweis. Wenn M flach ist gilt die Behauptung da $\alpha \to R$ injektiv ist. Andererseits gibt die exakte Sequenz $0 \to \alpha \to R \to R/\alpha \to 0$ die exakte Sequenz

$$0 = Tor_1^R(M, R) \to Tor_1^R(M, R/\alpha) \to \alpha \otimes_R M \to M \to M/\alpha M \to 0$$

Da $\alpha \otimes M \to M$ injektiv ist ist $Tor_1^R(M, R/\alpha) = 0$ also M flach. □

Satz 10.1.12. *Sei M'' ein R-Modul. Dann ist äquivalent:*

1. *M'' flach*
2. *Für alle exakte Sequenzen*
$$0 \to M' \to M \to M'' \to 0$$
und für alle R-Moduln N ist
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
exakt.

Beweis. (1) nach (2) ist klar. Sei M frei und N beliebig. Dann ist

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

exakt. Also ist $Tor_1^R(M, N) = 0$ also $Tor_1^R(M'', N) = 0$ also M'' flach. □

Satz 10.1.13. *Sei*

$$0 \to M' \to M \to M'' \to 0$$

exakt und M'' flach. Dan ist M' flach genau dann wenn M flach ist.

Beweis. Klar, Lange exakte Tor Sequenz. □

Definition 10.1.14. Seien M, N R-Moduln und $M_* \to M$ projektive Auflösung. Sei $Ext_R^n(M, N)$ die n-te homologische Ableitung von $Hom_R(-, N)$. Sei $N \to N^*$ injektive Auflösung. Sei $\tilde{Ext}_R^n(M, N)$ die cohomologische Ableitung von $Hom_R(M, -)$.

Satz 10.1.15. $\tilde{Ext}_R^n(M, N) \cong Ext_R^n(M, N)$

Beweis. Wie in ?? sei $C^{**} = \mathrm{Hom}_R(M_*, M^*)$ und $A^* = Hom(M_*, N)$ und $B^* = \mathrm{Hom}(M, N^*)$. Das gibt Abbildungen $B^* \to Tot(C^{**})$ und $A^* \to Tot(C^{**})$. Das sind quasi-Isomorphismen, denn zum Beispiel in Zeile j ist $B^* \to C^{**}$ einfach nur

$$\cdots \to \mathrm{Hom}(M_1, N^j) \to \mathrm{Hom}(M_0, N^j) \to \mathrm{Hom}(M, N^j)$$

was exakt ist da N^j injektiv ist. □

Satz 10.1.16. *Für ein R-Modul P ist äquivalent:*

1. *P projektiv.*
2. $Ext^n_R(P,N) = 0$ *für alle* $n > 0$ *und alle Moduln* N.
3. $Ext^1_R(P,N) = 0$ *für alle* n.

Beweis. wie bei Tor □

Satz 10.1.17. *Für einen R Modul I ist äquivalent*

1. *I ist injektiv*
2. $Ext^n_R(M,I) = 0$ *für alle n und alle Moduln M*
3. $Ext^1_R(M,I) = 0$ *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* $N \to M$ *eine Abbildung sodass* $N/IN \to M/IM$ *surjektiv ist dann ist* $N \to M$ *surjektiv.*
4. *Wenn* $x_1, \ldots, x_n \in M$ M/IM *erzeugen dann erzeugen* $x_1, \ldots, x_n$ *schon* M.

Beweis. Angenommen $M \neq 0$. Da M endlich erzeugt ist, betrachte minimales Erzeugendensystem $x_1, \ldots, x_n \in M$. Da $\mathfrak{a}M = M$ gilt, ist $x_n = a_1x_1 + \cdots + a_nx_n$ für $a_i \in \mathfrak{a}$. Dann ist $(1 - a_n)x_n = a_1x_1 + \cdots + a_nx_n$ und da $(1 - a_n)$ eine Einheit ist, folgt x_n ist im Erzeugnis von $(x_1, \ldots, x_{n-1})$ 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 $M = \mathrm{im}(N \to M) + IM$ und nach 2. folgt, dass $M = \mathrm{im}(N \to M)$. Sei $R^n \to M, (a_1, \ldots, a_n) \mapsto a_1x_1 + \ldots a_nx_n$. 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 Σ hat die aufsteigende Kettenbedingung, falls jede Kette $S_1 \leq S_2 \leq \cdots \leq S_k \leq \ldots$ irgendwann stationär wird.

Lemma 10.2.2. *Sei* Σ *partiell geordnet.* Σ *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* Σ *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 $I_1 \subseteq I_2 \subseteq \ldots$ Kette von Idealen. Dann ist $I = \bigcup_k I_k$ endlich erzeugt, $I = (f_1, \ldots, f_n)$ dann ist $f_1, \ldots, f_n \in I_k$ 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 Σ 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 Σ 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 $\bigcap_{j=1}^{k} M_{i_j} \neq \bigcap_{i\in I} M_i$. Sei $I_0 = \{i_1, \dots, i_k\}$. □

Lemma 10.2.7. *Sei $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ 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 $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ 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 □

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 $\varphi\colon A \to B$ 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 $A^r \to M$ surjektiv mit

$$(a_1, \dots, a_n) \mapsto a_1 f_1 + \dots + a_n f_n.$$

Sei N der Kern. Das gibt exakte Sequenz $0 \to N \to A^r \to M \to 0$ und nach 1 ist A^r noethersche also auch M. □

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

$$J_n = \{a \in A \mid \exists f \in I\colon f = aX^n + b_{n-1}X^{n-1} + \dots + b_0\}.$$

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 $0 \to K \to A[X] \to R \to 0$ exakt, wobei K der Kern ist von $X \mapsto 0$. Also ist A noethersch. □

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 noehtersch. 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. □

Lemma 10.2.12. *Sei M noetherscher R-Modul. Zeigen Sie, dass jeder surjektive Endomorphismus $f\colon M \to M$ 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 $Ker(f) = 0$ □

10.3 Localization

Satz 10.3.1. *Sei $S \subseteq R$ multiplikative Menge, M R-Modul. $\tau\colon M \to S^{-1}M, m \mapsto \frac{m}{1}$. Dann gilt*

1. $\ker(\tau) = \{m \in M \mid \exists u \in S\colon um = 0\}$
2. *Wenn M endlich erzeugt ist, dann ist $S^{-1}M = 0 \iff M$ wird annuliert von einem $M \in S$.*

Beweis. Wähle Erzeuger und multipliziere deren Annihilatoren. □

Lemma 10.3.2. *$S^{-1}R \otimes_R M \to S^{-1}M$, $\frac{r}{u} \otimes m \mapsto \frac{rm}{u}$ ist ein Isomorphismus.*

Satz 10.3.3 (Lokalisierung ist flach)**.** *Sei $\varphi\colon M \to N$ 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 $0 \to \bigcap_i M_i \to M \to \bigoplus_i M/M_i \to 0$ also auch

$$0 \to S^{-1}\bigcap_i M_i \to S^{-1}M \to \bigoplus_i S^{-1}M/S^{-1}M_i \to 0$$

und somit gilt die Aussage. □

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 □

Korollar 10.3.6. *$\varphi\colon M \to N$ Homomorphism von R-Moduln. φ ist injektiv (surjektiv, bijektiv) $\iff \forall \mathfrak{m} \subseteq R$ maximal ist $\varphi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ injektiv (surjektiv, bijektiv)*

Beweis. φ 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. □

10.4 Structursatz endlicher Moduln über Hauptidealringe

Lemma 10.4.1. *Sei M ein R-Modul. Dann ist äquivalent:*

1. *$M \oplus M' = \bigoplus_{i \in I} R/f_iR$ für $f_i \in R$ und ein R-Modul M'.*
2. *Für jede kurze exakte Sequenz*

$$0 \to A \to B \to C \to 0$$

von R-Moduln sodass $fA = A \cap fB$ ist für alle $f \in R$ ist die Abbildung

$$\mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$$

surjektiv.

Beweis. Gelte 1 und sei eine exakte Sequenz wie im Satz gegebgen. Es reicht der Fall $M = R/fR$. Sei $\psi\colon R/fR \to C$ 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 $\varphi\colon R/fR \to B, 1 \mapsto b - a$ das ψ liftet. Wenn andersrum 2 gilt, sie I die Menge der Paare (f, φ) wobei $f \in R$ ist und $\varphi\colon R/fR \to M$. Für $i \in I$ sei (f_i, φ_i) das entsprechende Paar. Betrachte $B = \bigoplus_{i\in I} R/f_iR \to M$ induziert durch φ_i. Sei $A = \ker(B \to M)$. Wenn die Sequenz $0 \to A \to B \to M \to 0$ 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 geordnetet durch Inklusion*

Das ist insebsondere 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 $0 \to M_1 \to M_2 \to M_3 \to 0$ 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.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^n & \longrightarrow & R^{n+m} & \longrightarrow & R^m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

Snake Lemma liefert exakte Sequenz $0 \to \ker(R^n \to M_1) \to \ker(R^{n+m} \to M_2) \to \ker(R^m \to M_3) \to 0$. Nach (5) sind die beiden äußeren endlich erzeugt also der innere auch. Nach (4) ist dann M_2 endlich präsentiert.
Zeige 5. Wähle Auflösung $R^m \to R^n \to M_3 \to 0$. Da R^n projektiv ist nach ??? gibt es eine Abbildung $R^n \to M$ sodass das solide Diagramm kommutiert:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^m & \longrightarrow & R^n & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \vdots & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

Das gibt dann gestrichelten Pfeil. Nach Schlangenlemma ist $\operatorname{coker}(R^m \to M_1) \cong \operatorname{coker}(R^n \to M_2)$. Also ist $\operatorname{coker}(R^m \to M_1)$ endlich erzeugt. Nach (3) ist $\operatorname{im}(R^m \to M_1)$ endlich erzeugt also ist M_1 endlich nach (1). Zeige 4. Wähle Auflösung $R^m \to R^n \to M_2 \to 0$ und Surjektion $R^k \to M_1$. Dann gibt es nach ?? $R^k \to R^n$ und $R^{k+m} \to R^n \to M_3 \to 0$ ist eine Auflösung. □

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 Bedinungen 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 κ-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

$$0 \to A \to M \to M/A \to 0$$

. 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.

□

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 $0 \to A \to B \to C \to 0$ 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 $\operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C)$ surjektiv ist. Es reicht, dass es surjektiv ist nach lokalisieren an maximalen Idealen $\mathfrak{m}$ nach Korollar 10.3.6. Da Lokalisierungnach Satz 10.3.3 exakt ist $0 \to A_\mathfrak{m} \to B_\mathfrak{m} \to C_\mathfrak{m} \to 0$ exakt und $fA_\mathfrak{m} = A_\mathfrak{m} \cap fB_\mathfrak{m}$. Da M endlich präsentiert ist, gilt $\operatorname{Hom}_R(M, B)_\mathfrak{m} = \operatorname{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, B_\mathfrak{m})$ und $\operatorname{Hom}_R(M, C)_\mathfrak{m} = \operatorname{Hom}_{R_\mathfrak{m}}(M_\mathfrak{m}, C_\mathfrak{m})$ nach ???. $M_\mathfrak{m}$ ist enldich 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 ist Abbildung der Lokalisierung surjektiv. Also ist M direkter Summand von $\bigoplus_{i \in I'} R/f_iR$. Betrachte $M \to \bigoplus_{i \in I'} R/f_iR$. Da M endlich erzeugt ist, ist das Bild von M in $\bigoplus_{i \in I} R/f_iR$ für eine endliche Teilmenge $I \subseteq I'$. □

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 $V = (g_{ij}) \in \mathrm{GL}_2(R)$ 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 $\bigoplus_{i=1,\dots,n} R/f_iR$ wobei f_i nicht-null sind.*

Beweis. Sei $M \subseteq F$ endich 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 $pr_n \colon R^n \to R$ und $I = \mathrm{im}(pr_n|_M \colon M \to R)$. 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 $M \cong R \oplus \ker(M \to I)$ 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

$$R^r \oplus \bigoplus_{i=1,\dots,n} R/f_iR$$

wobei $f_i \neq 0$. Dann ist M_{tors} ein Summand von $\bigoplus_{i=1,\dots,n} R/f_iR$ 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*

$$R^n \oplus \bigoplus_{i=1,\dots,n} R/f_iR$$

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 $fM = 0$. Dannist 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 $R/fR \to R_j$ gibt dass $R_j = R/f_jR$ für ein f_j. Dann erfüllt R_j die Bedinugnen von Lemma 10.4.2. Schreibe $M = \prod M_j$ mit $M_j = e_jM$ wobei $e_j \in R/fR$ das idempotente Element ist dass zu $1 \in R_j$ correspondiert. Nach Lemma Lemma 10.4.4 ist $M_j = \bigoplus_{i=1,\dots,n_j} R_j/\bar{f}_{ij}R_j$ für $\bar{f}_{ij} \in R_j$. 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 $M = N_0 \supsetneq \cdots \supsetneq N_n = 0$ 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 Komositionsreihe bzw als ∞ falls das nicht exisitert.

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 $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ 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 $M' \supseteq M' \cap M_1 \supseteq \cdots \supseteq M' \cap M_n = 0$ 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* $M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_k$ *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 $M \supsetneq M_1 \supsetneq M_2 \ldots$ 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 abteigende 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 $m \subseteq R$.*

Beweis. Gelte *a.* sei $x \in M$ mit $x \neq 0$. $x \cdot R \neq 0 \implies xR = M$ also ist

$$0 \to \mathfrak{m} \to R \xrightarrow{x} M \to 0$$

exakt mit $\mathfrak{m} = \ker(x)$. Da $M \cong R/\mathfrak{m}$ keine echten Ideale hat, ist $\mathfrak{m}$ maximal. □

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 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 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 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 $\alpha\colon M \to \bigoplus M_\mathfrak{p}$ Summe der Lokalisierungsabbildugen. Sei $Q \subseteq R$ maximales Ideal. Es ist $\alpha_\mathfrak{q}\colon M_\mathfrak{q} \to (\bigoplus M_\mathfrak{q})_\mathfrak{q}$ die Identität für alle Q. □

Satz 10.5.11. *Sei* length$(M) < \infty$. *Dann gilt*

$$M = M_\mathfrak{p} \iff M \text{ wird von einer Potenz von } \mathfrak{p} \text{ annuliert}$$

Beweis. Sei $\mathfrak{q} \neq \mathfrak{p}$ maximales Ideal, $x \in \mathfrak{p} \backslash \mathfrak{q}$. 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 $\mathfrak{p}^n M \subseteq M_n = 0$. □

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 git, 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

$$0 \to R/(I : a) \to R/I \to R/(I + (a)) \to 0$$

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 damiit 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 $IJ \subseteq I$. Wegene 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. □

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

$$0 \to n\mathbb{Z} \to \mathbb{Z} \xrightarrow{\cdot m} m\mathbb{Z} \to 0$$

exakt ist für ein $n \in \mathbb{Z}$. Wenn $n = 0$ dan 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 torionsmodul.

3. Sei M ein Untermodul. Dann ist $\frac{a}{p^n} \in M$ für ein $p \not| a$. 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 ∞ oder $m \in \mathbb{N}$. Falls ∞ 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 mist $\mathfrak{m}^n \subseteq p \subseteq R$. 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 $0 \to M' \to M \to M'' \to 0$ 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

$$M[a] \cong R^d \oplus \bigoplus R/a_iR$$

und da $M[a]$ Torsionsmodul ist, ist $d = 0$. Nach 1. ist $\text{length}(R/a_iR) < \infty$ 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot a} & & \downarrow{\scriptstyle \cdot a} & & \downarrow{\scriptstyle \cdot a} & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Nach Schlangenlemma gibt das eine exakte Sequenz

$$0 \to M'[a] \to M[a] \to M''[a] \to M'/aM' \to M/aM \to M''/aM'' \to 0$$

Es gilt

$$0 = \text{length}(M'[a]) - \text{length}(M[a]) + \text{length}(M''[a]) - \text{length}(M'/aM') + \text{length}(M/aM) - \text{length}(M''/aM'') \to 0$$

Also gilt die Aussage.

4. Nach 3. reich 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

$$0 \to M[a] \to M \xrightarrow{\cdot a} M \to M/aM \to 0$$

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 Assozierte 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 $\text{Ann}(m) \coloneqq \{f \in A \mid fm = 0\}$. 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 $\text{Supp}(M) = (\text{Spec}(\mathbb{Z}) \backslash \{0\}$.

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 $\text{Supp}(M) = \bigcup_{i \in J} \text{Supp}\, M_j$*
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
$$\frac{x}{1} = 0 \in M_\mathfrak{p} \iff sx = 0 \text{ für ein } s \in R \setminus \mathfrak{p}$$
$$\iff (A \setminus \mathfrak{p}) \cap \operatorname{Ann}(x) \neq \emptyset$$
Also $\frac{x}{1} \neq 0 \iff \operatorname{Ann}(x) \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\operatorname{Ann}(x))$
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 assoziertes 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 $\mathfrak{p} = Ann(x)$ Primideal ist. Sei $\operatorname{Ass}(M)$ die Menge der assoziierten Primideale.

Beispiel 10.6.5.

1. Wenn $R = \mathbb{Z}$ und $M = \mathbb{Q}$ dann ist $\operatorname{Ass}(M) = 0$ 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 $p = \operatorname{Ann}(x)$. Somit $Ass(M) = \operatorname{Spec}(\mathbb{Z}) \setminus \{0\} = \operatorname{Supp}(M)$.
3. Wenn $R = k[X, Y]$ und $M = R/(X^2, XY)$ dann sei $a \in M$ sodass $\operatorname{Ann}(a)$ prim ist. Wenn $a \in (x)$ dann ist $\operatorname{Ann}(a) = (X, Y)$ und wenn $a \notin (x)$ dann ist $\operatorname{Ann}(a) = (x)$. Also ist $\operatorname{Ass}(M) = \{(X), (X, Y)\}$.

Bemerkung 10.6.6. Wenn $\mathfrak{p} \in \operatorname{Ass}(M)$ dann $\operatorname{Ann}(M) = \bigcap_{x \in M} \operatorname{Ann}(x) \subseteq \mathfrak{p}$

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 $\operatorname{Ass}(\mathbb{Z}/n\mathbb{Z}) = \{(p), [q]\}$, denn $m)p^{\alpha-1}q^\beta + n\mathbb{Z}$ hat $Ann(m) = \mathfrak{p}$ und ähnlich fpr q.

Satz 10.6.8. *Sei M ein R-Modul.*

1. *Sei $\mathfrak{p} = Annx$ prim für $x \in M$. Dann gilt*
$$0 \neq y \in Rx \implies \operatorname{Ann}(y) = \mathfrak{p}$$
2. *Jedes maximale Element der Menge $\{\operatorname{Ann} x \mid 0 \neq x \in M\}$ ist Primideal, also in $\operatorname{Ass}(M)$.*
3. *Wenn R noethersch ist, dann ist $\operatorname{Ass}(M) \neq \emptyset$ falls $M \neq 0$.*
4. *Wenn $L \subseteq M, N = M/L$ dann ist $\operatorname{Ass}(M) \subseteq \operatorname{Ass}(L) \cup \operatorname{Ass}(N)$.*

Beweis. Es ist $Rx \cong R/\mathfrak{p}$ Integritätsbereich. Wenn also $y \neq o \in R/\mathfrak{p}$ Dann ist $\operatorname{Ann}(y) = \mathfrak{p}$.

1. Angenommen $\mathfrak{p} = \operatorname{Ann}(x)$ maximal und $f \cdot g \in \operatorname{Ann}(x)$. Dann ist $fgx = 0$. Wenn $gx = 0$ dann ist $g \in \mathfrak{p}$. wenn $0 \neq gx$, dann ist $Ann(x) \subseteq Ann(gx)$ also $\operatorname{Ann}(gx) = \operatorname{Ann}(x)$ und dan $f \in \operatorname{Ann}(gx) = \operatorname{Ann}(x)$.
2. folgt mit 2.
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 $\mathfrak{p} \in Ass(N)$. Andernfalls gilt für alle $x \neq 0 \in (R/\mathfrak{p}) \cap L$: $\operatorname{Ann}(x) = \mathfrak{p}$ nach 1. Also ist $\mathfrak{p} \in \operatorname{Ass}(L)$.

□

Korollar 10.6.9. *wenn R noethersch ist, dann ist*

$$\{ \textit{ Nullteiler von } M\} = \bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)} \mathfrak{p}$$

Beweis. Sei $0 \neq m \in M$. Jedes $a \in \mathrm{Ann}(m)$ ist in einem Ideal $Ann(x)$ enthalten wobei $\mathrm{Ann}(x)$ maximal unter Annihilatoren. Also in $\mathrm{Ass}(M)$ nach Satz 10.6.8. □

Beispiel 10.6.10. $N = M/L$ kann assozierte Primideale haben, die nicht in $\mathrm{Ass}(M)$ liegen, zum Beispiel ist $\mathrm{Ass}(\mathbb{Z}/2\mathbb{Z}) = \{(2)\}$ aber $(2) \notin \mathrm{Ass}(\mathbb{Z})$.

Satz 10.6.11. *Es ist* $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ *Insbesondere* $\mathfrak{p} \in \mathrm{Ass}(M) \implies V(\mathfrak{p} \subseteq \mathrm{Supp}(M)$ *Wenn außerdem R noch noethersch, dann ist minimales Element* $\mathfrak{p} \in \mathrm{Supp}(M)$ *in* $\mathrm{Ass}(M)$*. Insbesondere wenn* $V(\mathfrak{p}) \subseteq \mathrm{Supp}\, M$ *irreduzible Komponente ist, dann ist* $\mathfrak{p} \in \mathrm{Ass}(M)$*.*

Beweis. Es ist

$$(R/\mathfrak{p})_\mathfrak{p} \cong \mathrm{Quot}(R/\mathfrak{p}) =: k(\mathfrak{p})$$

Da $R/\mathfrak{p} \subseteq M$ folgt $0 \neq k(\mathfrak{p}) = (Rfrakp)_\mathfrak{p} \subseteq M_\mathfrak{p}$. Somit ist $\mathfrak{p} \in \mathrm{Supp}(M)$. Sei nun R noethersch. $M_\mathfrak{p}$ ist $R_\mathfrak{p}$-Modul, $M_\mathfrak{p} \neq 0$. Also ist $\mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \neq \emptyset$. 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 $\mathrm{Supp}_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$ und dann

$$0 \neq \mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \subseteq \mathrm{Supp}_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$$

und also $\mathrm{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$. Das heißt es gibt $0 \neq \frac{m}{s} \in M_\mathfrak{p}$ sodass $\mathrm{Ann}(\frac{m}{s}) = \mathfrak{p}R_\mathfrak{p}$. 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 $\mathfrak{p} = (f_1, \ldots, f_n)$ 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 $\mathfrak{p} \subseteq \mathrm{Ann}(tm)$. 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 $\mathrm{Ann}(tm) \subseteq \mathfrak{p}$ und damit $\mathfrak{p} = \mathrm{Ann}(tm)$. □

Korollar 10.6.12. *Wenn R noethersch und M endlicher R-Modul ist, dann ist*

$$\mathrm{Supp}(M) = \bigcup_{i=1}^{n} V(\mathfrak{p}_i)$$

wobei die $\mathfrak{p}_i$ *endlich viele minimale Primideale sind, die* $\mathrm{Ann}(M)$ *enthalten. Jedes* $\mathfrak{p}_i$ *ist assoziertes Primideal.*

Beweis. $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$ und $V(\mathrm{Ann}(M)$ hat endlich viele minimale Elemente $\{\mathfrak{p}_i, \ldots, \mathfrak{p}_k\}$ und $V(\mathrm{Ann}(M)) = \bigcup V(\mathfrak{p}_i)$ Nach letztem Satz ?? sind diese in $Ass(M)$. □

Satz 10.6.13. *Sei R noethersch und M endlicher A-Modul. Es gibt Kette*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

Untermodul sodass $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ *mit* $\mathfrak{p}_i \in \mathrm{Spec}(A)$*. Dann ist* $Ass(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$*.*

Beweis. Es ist $\mathrm{Ass}(M) \neq 0$ 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 von den enstehenden Moduln. Kette muss abrechen, 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 $\mathrm{Ass}(M) = 0$. Wenn $a = 0$ dann ist $M = R$ und dann $\mathrm{Ass}(M) = \{0\}$. Wenn a weder 0 noch Einheit ist, ist $a = p_1 \ldots p_r$ für Primelemente p_i. sei $M_i = p_1 \cdots p_i \cdot R/aR$. Diese bilden absteigende Kette mit

$$M_{i-1}/M_i \cong R/p_i R.$$

Also ist $\mathrm{Ass}(M) = \{p_1, \ldots, p_r\} = \mathrm{Supp}(M)$.

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

$$\{a \in \mathbb{Z}/n \mid \ell \dot{a} = 0\} = \{k \cdot b \mid b \in \mathbb{Z}/n\mathbb{Z}\}$$

denn für $x \in \mathbb{Z}$ ist $n \mid \ell \dot{x} \iff k \mid x$.

Bemerkung 11.1.2. Es ist $(\mathbb{F}_p^*, \cdot) \cong (\mathbb{Z}/(p-1), +)$, $1 \mapsto 0$ nach Satz ???. Wenn also $p-1 = n = k\dot{\ell}$ 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

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \not\mid a \text{ und } a \text{ Quadratzahl in} \mathbb{F}_p \\ -1 & p \not\mid a \text{ und } a \text{ keine Quadratzahl in} \mathbb{F}_p \end{cases}$$

Lemma 11.1.4.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

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. □

Lemma 11.1.5.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & 4 \mid p-1 \iff p \equiv 1 \mod 4 \\ -1 & 4 \not\mid p-1 \iff p \equiv 3 \mod 4 \end{cases}$$

Lemma 11.1.6. *Wenn $p \equiv 1 \mod 4$ dann ist $-1 \in \mathbb{F}_p$ eine Quadratzahl.*

Beweis. □

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 $p \equiv 1 \mod 4$.*

Beweis. Für alle $x \in \mathbb{N}$ gilt $x^2 \equiv 0 \mod 4$ oder $x^2 \equiv 1 \mod 4$. wenn also $p = x^2 + y^2$ ist, dann ist $p \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases} \mod 4$. Also ist eine Richtung gezeigt. Sei andererseits $p \equiv 1 \mod 4$. Wähle x sodass $x^2 \equiv -1 \mod p$ nach ?? Das heißt $p \mid x^2 + 1 = (x+i)(x-i)$ in $\mathbb{Z}[i]$. Aber $p \not| x \pm i$ 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 $p = N(z) = a^2 + b^2$. □

Satz 11.2.3. *Primelemnte in $\mathbb{Z}[i]$ sind*

1. *Primzahlen $p \in \mathbb{Z}$ mit $p \equiv 3 \mod 4$*
2. *$a + bi \in \mathbb{Z}[i]$ mit $a^2 + b^2 = p$ und $p = 2$ oder $p \equiv 1 \mod 4$.*

Beweis. Ähnliche Rechnung. □

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

$$\mathcal{O}_K = \{z \in K \mid z \text{ ganz über } \mathbb{Z}\}$$

Also $\mathcal{O}_K$ 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 ZZ genau dann wenn $a \in \mathbb{Z}$. Wennn $b \neq 0$ 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 $d \equiv 1 \mod 4$. Das heißt

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv \mod 4 \\ \mathbb{Z}[\frac{\sqrt{d}+1}{2}] & d \equiv 1 \mod 4 \end{cases}$$

Bemerkung 11.3.3. Aus ??? folgt, dass $\mathcal{O}_K$ ein endlicher $\mathbb{Z}$-Modul ist. Da $\mathcal{O}_K$ torsionsfrei ist folgt mit ??? $_K = \mathbb{Z}^n$ als $\mathbb{Z}$-Modul.

Definition 11.3.4. Eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$ heißt Ganzheitsbasis von K.

Lemma 11.3.5. *Jede Ganzheitsbasis ist eine Q-Basis von K und $\mathcal{O}_K \cong \mathbb{Z}^n$ mit $n = [L : K]$.*

Beweis. Seien $a_1, \ldots, a_n \in \mathcal{O}_K$ eine Ganzheitsbasis. Dann sind sie auch
Q-linear unabhängig. Sei $y \in K$ mit $f \in \mathbb{Q}[X]$ Minimalpolynom. Sei b der gemeinsame Nenner aller Koeffienten von f. Dann ist by ganz also in $\mathcal{O}_K$. somit ist $y \in \mathbb{Q} \cdot \mathcal{O}_K$. □

Beispiel 11.3.6. Wenn $K = \mathbb{Q}(\sqrt{d})$ mit d quadratfrei, dann ist falls $d \equiv 1 \mod 4$ eine Ganzheitsbasis gegeben durch $1, \frac{\sqrt{d}+1}{2}$ und falls $d \not\equiv \mod 4$ gegeben durch $1, \sqrt{d}$.

Definition 11.3.7. Sei L/K eine Körpererweiterung. Definiere die Spur von $b \in L$ durch

$$Tr_{L/K}(b) = Tr(b\colon L \to L)$$

und die Norm von $b \in L$ durch

$$N_{L/K}(b) = \det(b\colon L \to L)$$

Lemma 11.3.8. *Wenn L/K separabel, dann ist für $b \in L$ und $\Sigma = \{\sigma\colon L \to \bar{K} \mid \sigma|_K = \mathrm{id}\}$:*

$$Tr_{L/K}(b) = \sum_{\sigma \in \Sigma} \sigma(b)$$

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

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 Gerade haben sind sie gleich und Aussage folgt. Wenn L allgemein, sei $M = K(b)$. Jedes $\sigma'\colon M \to \bar{K}$ hat genau $r = [L : M]$ Fortsetzungen zu $\sigma\colon L \to \bar{K}$ nach ????. Also ist $\prod_{\sigma\in\Sigma}(X - \sigma(b)) = \prod_{\sigma'\in\Sigma'}(X - \sigma'(b))^r$ mit $\Sigma' = \{\sigma'\colon M \to \bar{K}$. Es ist $L = M^r$ als M Vektorraum und $b \in M$ respektiert die Summenzerlegung. Also ist $\chi_{b\colon LL} = (\chi_{b\colon M\to M})^r$.
□

Korollar 11.3.9. *Seien $M//L/K$ separable Körpererweiterungen und $b \in M$. Dann*

$$Tr_{M/K}(b) = Tr_{L/K}(Tr_{M/L}(b))$$

$$N_{M/K}(b) = N_{L/K}(N_{M/L}(b))$$

Beweis. Genau wie in ??? □

Definition 11.3.10. Sei L/K endliche separable Körpererweiterung und $a_1, \ldots, a_n$ eine K-Basis. Die Diskrimminante von $a_1, \ldots, a_n$ sei

$$d(a_1, \ldots, a_n) = \det(Tr_{L/K}(a_i a_j)_{ij})$$

das heißt die Determinante der Darstellenden Matrix bzgl der Bilinearform $L \times L \to K, (a, b) \mapsto Tr_{L/K}(ab)$.

Bemerkung 11.3.11 (Basiswechsel)**.** Wenn $a_1, \ldots, a_n$ und $b_1, \ldots, b_n$ zwei K-Basen und S die Übergangsmatrix ist, dann ist

$$d(b_1, \ldots, b_n) = det(S^T Tr(a_i a_j)_{ij} S) = \det(S)^2 d(a_1, \ldots, a_n)$$

Lemma 11.3.12. *Wenn $A = Tr(a_i a_j)_{ij})$ Dann ist $A = B^t B$ für $B = \sigma_i(a_j)_{i,j} \in M_n(\bar{K})$ mit wobei σ_i die verscchiedenen K-Homomorphismen $L \to \bar{K}$.*

Beweis. Nach ?? ist

$$(B^t B)_{ik} = \sum_{j=1}^{n} \sigma_j(a_i)\sigma_j(a_k) = \sum_{j=1}^{n} \sigma_j(a_i a_k) = Tr_{L/K}(a_i a_k) = A_{ik}$$

□

Korollar 11.3.13. $d(a_1, \ldots, a_n) = det(A) = \det(B)^2$

Satz 11.3.14. $d(a_1, \ldots, a_n) \neq 0$ *also ist* $(a, b) \to Tr_{L/K}(ab)$ *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 $B = \begin{pmatrix} 1 & \dots & 1 \\ \sigma_1(b) & & \\ \vdots & & \vdots \\ \sigma_1(b)^{n-1} & & \sigma_n(b)^{n-1} \end{pmatrix}$ Nach ??? ist $\det(B) = \prod_{i<j}(\sigma_i(b) - \sigma_j(b)) \neq 0$. □

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 Diskrimminante $d(a_1, \dots, a_n$ ganz über A.

Definition 11.3.16. Sei $K/\mathbb{Q}$ endlich und $a_1, \dots, a_n \in \mathcal{O}_K$ Ganzheitsbasis. Diskrimminante von K ist $d_K = d(a_1, \dots, a_n) = \det(Tr_{K/\mathbb{Q}}(a_i a_j))$. Eine Basiswechselmatrix S zu einer anderen Ganzheitsbasis ist über $\mathbb{Z}$ also ist hat Determinante ± 1 also ist nach ??? d_K wohldefiniert.

Beispiel 11.3.17. Sei $K = \mathbb{Q}(\sqrt{d})$ und d quadratfrei. Wenn $d \not\equiv 1 \mod 4$, 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 $d \equiv 1 \mod 4$, 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 K ein Zahlkörper und r die Anzahl der Homomorphismen $K \to RR$ und sei $[K : \mathbb{Q}] = n = r + 2s$. Dann ist d_K positiv genau dann wenn S gerade ist.*

Beweis. Es ist nach ??? $d_K = \det(B)^2$ für $B = (\sigma_i(x_j))_{ij}$ wobei $x_1, \dots, x_n$ eine Ganzheitsbasis ist und $\sigma_i \colon K \to \mathbb{C}$ $\mathbb{Q}$-Homomorphismen. Sei $\tau \colon \mathbb{C} \to \mathbb{C}$ die Komplexe Konjugation. Dann ist

$$(\bar{B})_{ij} = \tau(\sigma_i(x_j)) = \sigma_{i'}(x_j)$$

wobei $\sigma_{i'} = \tau\sigma_i$. Wenn $\sigma \colon K \to \mathbb{C}$ Bild in $\mathbb{R}$ hat, dann ist $\tau\sigma = \sigma$ und wenn nicht, dann ist $\tau\sigma \neq \sigma$. Also entsteht $\bar{B}$ aus B durch s Vertauschungen der Zeilen. Also ist

$$\overline{\det}(B) = \det(\bar{B}) = (-1)^s \det(B)$$

Also gilt

$$s \text{ gerade} \iff \overline{\det}(B) = \det(B) \iff \det(B) \in \mathbb{R} \iff d_K = \det(B)^2 > 0$$
$$s \text{ ungerade} \iff \overline{\det}(B) = -\det(B) \iff \det(B) \in i \cdot \mathbb{R} \iff d_K = \det(B)^2 < 0$$

□

Lemma 11.3.19. *sei $(0) \neq I \subseteq \mathcal{O}_K$ 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 $a\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$. Da $a\mathcal{O}_K \cong \mathbb{Z}^n$ ist $I \cong \mathbb{Z}^n$. □

Definition 11.3.20. 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 11.3.21.

$$| \det(S) | =| \mathcal{O}_K / I |$$

und somit $d(I) =| {}_K/I |^2 d_K$.

Beispiel 11.3.22. Sei $K = \mathbb{Q}(\zeta_p)$ für eine primitive p-te Einheitswurzel ζ_p. Es ist $\Sigma = \{\sigma \colon K \to \bar{\mathbb{Q}}\} = \{\sigma_i \mid \sigma_i(\zeta_p) = \zeta_p^i, i$
Also ist

$$Tr_{K/\mathbb{Q}}(\zeta_p) = \sum_{i=1}^{n-1} b^i = -1 + \sum_{i=0}^{n-1} b^i = -1 + \frac{\zeta_p^p - 1}{\zeta_p - 1} = -1$$

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 χ_{ζ_p}. Es ist $f(0) = -p$. Somit ist $N_{L/K}(1 - \zeta_p) = p$.

Beispiel 11.3.23. 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 $b\colon K \to K$ ist dargestellt durch

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Also ist $Tr(b) = 0$. $b^2\colon K \to K$ ist dargestellt durch

$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

hat also auch $Tr(b^2) = 0$. Es ist $Tr(1) = 3$ und $Tr(2) = 2\dot{3}$. 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 11.3.24. 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 $f(X) = \left((X^3 - 1)^4 - 2\right)^2 - 7 \in \mathbb{Z}[X]$ und $f(a) = 0$ also ist a ganz über $\mathbb{Z}$. Angenommen b wäre ganz über $\mathbb{Z}$). Dann auch $\left((b^3 - 1)^4 - 2\right)^2 = \frac{7}{4}$ 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 11.3.25. *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*

$$\mathbb{R}^n/H \text{ kompakt} \iff \exists B \subseteq \mathbb{R}^n \text{ beschränkte Menge sd.} B + H = \mathbb{R}^n$$

Beweis. 1. Klar.

2. Die Abbildung $H \to H/K$ wobei H/K Unterraumtopologie hat ist stetig. Wenn also U offen in Unterraumtopologie dann auch in Quotiententopologie. Sei U offen in Quotiententopologie, $\pi_H\colon H \to H/K$, $\pi_G\colon G \to G/K$ 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, $\pi\colon G \to G/H$. 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 $G \times G \to G/H \times G/H$. Das ist offen da π 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 $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/H$ die Projektion. Angenommen R/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 $\pi(B) = R^n/H$ ist ist auch R^n/H kompakt.

□

Lemma 11.3.26. *Sei Γ in vollständiges Gitter in einem Euklidischen Vektorraum der Dimension n.*

1. *Der Gitterpunktsatz ist optimal, das heißt es gibt in V eine konvexe, zentralsymmetrische Menge X mit dem Volumen*
$$2^n \operatorname{Vol}(\Gamma)$$
sodass $X \cap \Gamma = \{0\}$

2. *Wenn X eine kompakte konvexe zentralsymmetrische Menge mit dem Volumen $\geq 2^n \operatorname{Vol}(\Lambda)$ ist, dann ist $X \cap \Gamma \neq \{0\}$.*

Beweis. 1. Sei $v_1, \ldots, v_n$ eine Basis von Γ über $\mathbb{Z}$. Sei $X = \{\lambda_1 v_1 + \cdots + \lambda_n v_n \mid |\lambda_i| < 1\}$ Dann ist $\operatorname{Vol}(X) = 2^n \operatorname{Vol}(\Gamma)$ Aber wenn $\gamma \in X \cap \Gamma$ dann ist
$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \gamma = \alpha_1 v_1 + \cdots + \alpha_n v_n$$
für $\alpha_i \in \mathbb{Z}, |\lambda_i| < 1$. Also ist $\alpha_i = \lambda_i = 0$ für alle i. Somit ist $\gamma = 0$.

2. Sei $X_{\frac{1}{n}} = (1 + \frac{1}{n})X$. Dann gibt es nach Satz 12.1.1 ein $\gamma_{\frac{1}{n}} \in X_{\frac{1}{n}} \cap \Gamma \setminus \{0\}$. Es ist $X = \bigcap_n X_{\frac{1}{n}}$ und da Γ diskret gibt es ein $\gamma_{\frac{1}{n}}$ mit minimaler Länge. Also ist $\gamma_{\frac{1}{n}} \in X$.

□

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 Λ in V $\mathbb{R}$-linear unabhängig ist.

2. Ein Gitter $\Lambda \subseteq V$ ist vollständig, wenn Λ 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 $\alpha\colon \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \to V, (x, v) \mapsto xv$. Es ist Λ ein Gitter $\iff$ α injektiv ist. *Lambda* ist vollständiges Gitter $\iff$ α. bijektiv.

Wenn $\Lambda \subseteq V$ vollständiges Gitter ist, dann gibt eine Wahl von Basis von Λ und

$$\begin{array}{ccc} \Lambda & \hookrightarrow & V \\ \| \wr & & \| \wr \\ \mathbb{Z}^n & \hookrightarrow & \mathbb{R}^n \end{array}$$

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 $RR{\cdot}\Lambda$ und wähle RR-Basis $v_1, \ldots, v_n \in \Lambda$. Sei $Lambda_0 = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$. Dann ist Λ_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 $\Lambda_0 \subseteq$ vollständiges Gitter ist, ist V/Λ_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 Λ/Λ_0 kompakt und diskret also endlich. Also ist Λ endlich erzeugte abelsche Gruppe. Nach ??? Strukturtsatz ist $\Lambda \cong ZZ^r$. Da $v_1, \ldots, v_n$ linear unabhängig sind, ist $\Lambda_0 = \Lambda$ und somit Λ Gitter.

2. Wenn Λ vollständig, dann ist $\mathbb{R}^n/\mathbb{Z}^n = (S^1)^n$ kompakt. Wenn $\Lambda \subseteq V$ Gitter sodass V/Λ 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 $V/\Lambda \cong V_0/\Lambda \oplus V_1 =$ kompakt $\times \mathbb{R}^m$ kompakt. Also ist $m = 0$ und damit $V_0 = V$.

□

Definition 12.0.5. Sei $\Lambda \subseteq \mathbb{R}^n$ ein Gitter. Eine Grundmasche ist eine Teilmenge $F \subseteq \mathbb{R}^n$ sodass jedes $x \in \mathbb{R}^n$ genau eine Darstellung $x = \lambda + \gamma$ hat mit $\lambda \in \Lambda$ und $\gamma \in F$.

Lemma 12.0.6. *Ein Gitter Λ ist vollständig genau dann wenn eine beschränkte Grundmasche existiert.*

Beweis. Sei Λ vollständig. Wähle $\mathbb{Z}$-Basis $v_1, \dots, v_n$ von Λ und setze $F = \{\sum_{i=1}^n a_i v_i \mid 0 \leq a_i < 1\}$. Dann ist F eine Fundamentalmasche. Wenn es F beschränkte Fundamentalmasche gibt, dann ist $\mathbb{R}^n/\Lambda$ kompakt nach ??? da Λ diskret. Nach ??? ist Λ vollständig.

□

Lemma 12.0.7. *Seien F_1, F_2 zwei Fundamentalmaschen in $\mathbb{R}^n$ für ein vollständiges Gitter $\Lambda \subseteq \mathbb{R}^n$. Dann gilt* $\mathrm{Vol}(F_1) = \mathrm{Vol}(F_2)$.

Beweis. Sei $\mathbb{1}_{F_1}$ die charakteristische Funktion von F_1. Es ist

$$\begin{aligned}
\mathrm{Vol}(F_1) &= \int_{\mathbb{R}^n} \mathbb{1}_{F_1}(x)\mathrm{d}x \\
&= \sum_{g\in\Lambda} \int_{F_2+g} \mathbb{1}_{F_1}(x)\mathrm{d}x \\
&= \sum_{g\in\Lambda} \int_{F_2} \mathbb{1}_{F_1}(x+g)\mathrm{d}x \\
&= \int_{F_2} \sum_{g\in\Lambda} \mathbb{1}_{F_1}(x+g)\mathrm{d}x \\
&= \int_{F_2} 1\mathrm{d}x \\
&= \mathrm{Vol}(F_2)
\end{aligned}$$

wobei man Summe und Integral nach Fubini-Tonelli ??? vertauschen darf. □

Sei ab jetzt V ein endlich-dimensionaler eukldischer Vektorraum. Wähle Isometrie $\varphi\colon (V, \langle,\rangle) \to (\mathbb{R}^n, \cdot)$ und definiere ein Maß μ auf V durch $\mu(A) = \lambda(\phi(A))$ für Messbare Mengen A wobei λ das Lebesgueq Maß auf $\mathbb{R}^n$ ist. Das ist wohldefiniert denn für eine andere Isometrie sind die Orthonormalbasen verbunden durch eine orthonormale Matrix und das Lebesgue Maß ist invariant unter diesen Transformationen nach ???.

Lemma 12.0.8. *Sei V ein Euklidischer Vektorraum und $v_1, \dots, v_n \in V$ und sei Γ das Parallelopid das aufgespannt wird von $v_1, \dots, v_n$. Dann ist $\mu(\Gamma) = |\det(A)|$ wobei A die Darstellungsmatrix ist der v_1 bezüglich einer Orthonormalbasis.*

Beweis. Eine Orthonormalbasis gibt Isometrie zu $\mathbb{R}^n$ mit Standardskalarprodukt. Somit ist ohne Einschränkung $V = \mathbb{R}^n$ und die Orthonormalbasis die Standardbasis. Sei A die Abbildungsmatrix. Nach QR-Zerlegung ??? ist $A = QR$ wobei Q Orthogonal ist und R obere Dreiecksmatrix. Wegen Invarianz des Lebesgue Maß von Orthogonalen Transformationen ist ohne Einschränkung A obere Dreiecksmatrix. Dann ist sowohl das Volumen als auch der Betrag der Determinante gleich dem Produkt der Diagoaleinträge. □

Lemma 12.0.9. *Seien $M \subseteq N$ zwei vollständige Gitter in $\mathbb{R}^n$ und sei $A \in M_n(\mathbb{Z})$ die Übergangsmatrix von einer Basis von N zu einer Basis von M. Es gilt*

1. $\mathrm{Vol}(M) = |\det(A)|\,\mathrm{Vol}(N)$
2. $N/M = |det(A)|$

Beweis. Sei $v_1, \dots, v_n$ eine Basis von N und $w_1, \dots, w_n$ eine Basis von M und A die Übergangsmatrix. Dann ist $(w_1, \dots, w_n) = (v_1, \dots, v_n)\cdot A$ und somit $\mathrm{Vol}(M) = |\det(w_1, \dots, w_n)| = |\det(A)|\cdot|\det(v_1, \dots, v_n)| = |\det($
Die zweite Aussage kann man rein algebraisch Zeigen. Oder aber so: Sei $x \in N$. Es gibt Darstellung $x = \sum_i \beta_i w_i$ mit $\beta_i \in \mathbb{R}$. Sei $y = \sum_i \lfloor\beta_i\rfloor w_i \in M$. Dann ist $x - y \in \Gamma_M \cap N$. Wenn $x_1 - y_1 = x_2 - y_2 \in \Gamma_M \cap N$ für $x_1, x_2 \in N$ und $y_1, y_2 \in M$ dann ist sind die Koeffizienten von $x_1 - x_2$ ganze Zahlen aber auch im Betrag < 1 also 0. Das heißt es gibt Bijektion $N/M \to N \cap \Gamma_M$. Sei $\Gamma_M \cap N = \{s_1, \dots, s_k\}$. Es ist $s_i + \Gamma_N$ disjunkt für verschiedene i Es ist $\Gamma_M = \bigcup_i s_i + \Gamma_N$

□

Definition 12.0.10. Das Volumen $\mathrm{Vol}(\Lambda)$ von Gitter Λ ist definiert als $\mu(\Gamma)$ wobei Γ 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 geschiet durch Betrag der Determinante.

Bemerkung 12.0.11. Es ist $A^t \cdot A = \langle v_i, v_j \rangle_{i,j} = B$ und somit $\det(B) = \det(A)^2$. Also ist $\mathrm{Vol}(A) = \sqrt{\det(B)}$

12.1 Miskowskysche Gitterpunktsatz

Satz 12.1.1 (Gitterpunktsatz)**.** *Sei V ein Euklidischer Vektorraum und $\Lambda \subseteq V$ ein vollständiges Gitter und $X \subseteq V$ eine konvexe, zentralsymmetrische (dh. $x \in X \implies -x \in X$) Menge. Wenn*

$$\mu(X) > 2^n \,\mathrm{Vol}(\Lambda)$$

dann ist $X \cap \Lambda \neq \{0\}$

Beweis. Es reicht zu zeigen, dass es $\gamma_1, \gamma_2 \in \Lambda$ gibt mit $\gamma_1 \neq \gamma_2$ sodass

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$$

denn wenn

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$$

mit $x_1, x_2 \in X$ dann ist

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X \cap \Lambda$$

Also angenommen $\frac{1}{2}X + \gamma$ für $\gamma \in \Lambda$ sind paarweise disjunkt. Dann sind auch $\Gamma \cap (\frac{1}{2}X + \gamma)$ paarweise disjunkt wobei Γ eine Grundmasche ist von Λ Dann ist

$$\begin{aligned}
\mathrm{Vol}(\Lambda) &\geq \sum_{\gamma \in \Lambda} \mathrm{Vol}(\Gamma \cap ()\frac{1}{2} + \gamma)) \\
&= \sum_{\gamma \in \Lambda} \mathrm{Vol}((\Gamma - \gamma) \cap \frac{1}{2}X) \\
&= \mathrm{Vol}(\frac{1}{2}X) \\
&= \frac{1}{2^n}\,\mathrm{Vol}(X)
\end{aligned}$$

was ein Widerspruch ist. □

Korollar 12.1.2. *Jede natürliche Zahl lässt sich schreiben als Summe von vier Quadraten.*

Beweis. Es ist

$$\begin{aligned}
(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 \\
+ (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2
\end{aligned}$$

Also reicht es die Aussage für eine Primzahl p zu zeigen. Es ist $2 = 1^2 + 1^2 + 0^2 + 0^2$ also ist ohne Einschränkung $p \geq 3$. Es ist

$$|\{m^2 \mod p \mid m = 0, \ldots p-1\}| = \frac{p+1}{2}$$

und

$$|\{-1 - n^2 \mod p \mid n = 0, \ldots p-1\}| = \frac{p+1}{2}$$

Also gibt es $m, n \in \mathbb{Z}$ sodass $m^2 + n^2 + 1 \equiv 0 \mod p$. Sei

$$\Lambda = \{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv ma + nb,\ d \equiv mb - na \mod p\}$$

Gitter. Dann ist $p\mathbb{Z}^4 \subseteq \Lambda \subseteq ZZ^4$ und $\Lambda / p\mathbb{Z}^4 \subseteq \mathbb{F}_p^4$ Unterraum der Dimension 2. Also ist der Index $[\mathbb{Z}^4 \colon \Lambda] = p^2$ und somit ist $\mathrm{Vol}(\Lambda) = p^2$. Sei $T = \bar{B_r}(0)$ und r so gewählt, dass $2p > r^2 > \frac{4\sqrt{2}}{\pi}p$. Dann ist

$$\mathrm{Vol}(T) = \frac{\pi^2 r^4}{2} > 16p^2 = \mathrm{Vol}(\Lambda)$$

Nach Gitterpunktsatz gibt es $(a, b, c, d) \in \Lambda \backslash \{0\} \cap T$ das heißt $a^2+b^2+c^2+d^2 \equiv a^2(1+m^2+n^2)+b^2(1+n^2+m^2) \equiv 0 \mod p$. Da $(a, b, c, d) \in T$ ist $a^2 + b^2 + c^2 + d^2 < 2p$. Also ist $a^2 + b^2 + c^2 + d^2 = p$. □

Bemerkung 12.1.3. Sei K ein Zahlkörper. $\mathcal{O}_K \cong \mathbb{Z}^n$ soll ein Gitter werden in einem passenden $\mathbb{R}$-Vektorraum. Da jede $\mathbb{Z}$-Basis von $\mathcal{O}_K$ eine $\mathbb{Q}$-Basis ist, ist die natürliche Abbildung $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \to K$ bijektiv. Betrachte Diagramm

$$\begin{array}{ccccccc} \mathbb{Z} & \hookrightarrow & \mathbb{Q} & \hookrightarrow & \mathbb{R} & \hookrightarrow & \mathbb{C} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{O}_K & \hookrightarrow & \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} & \hookrightarrow & \mathcal{O}_K \otimes_{\mathbb{Z}} \otimes \mathbb{R} & \hookrightarrow & \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C} \end{array}$$

Sei $K_{\mathbb{R}} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} \cong (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$ der Minkowski Raum. Es sei $K_{\mathbb{C}} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C}$. Es ist $\mathcal{O}_K$ ein vollständiges Gitter in $K_{\mathbb{R}}$ denn die Abbildung $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} \to K_{\mathbb{R}}, (x, a) \mapsto a \cdot x = (1 \otimes a)(x \otimes 1) = x \otimes a$ ist bijektiv.

Lemma 12.1.4. *Die Komplexe Konjugation $\tau \colon \mathbb{C} \to \mathbb{C}$ induziert einen Homomorphismus*

$$\tilde{\tau} = \mathrm{id} \otimes \tau \colon K \otimes_{\mathbb{Q}} \mathbb{C} \to K \otimes_{\mathbb{Q}} \mathbb{C}$$

. Die Invarianten davon sind

$$(K \otimes_{\mathbb{Q}} \mathbb{C})^{\tilde{\tau}} = \{x \in K \otimes \mathbb{C} \mid \tilde{\tau}(x) = x\} = K_{\mathbb{R}}$$

Beweis. Wähle eine $\mathbb{Q}$-Basis von $K \cong \mathbb{Q}^n$. Dann ist $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ und $K_{\mathbb{C}} \cong \mathbb{C}^n$. Also ist $(K_{\mathbb{C}})^{\tilde{\tau}} \cong (\mathbb{C}^n)^{\tilde{\tau}} = \mathbb{R}^n \cong K \otimes_{\mathbb{Q}} \mathbb{R}$. □

Lemma 12.1.5. *Es gibt Isomorphismus von $\mathbb{C}$-Algebren $\psi \colon K_{\mathbb{C}} \to \prod_\tau \mathbb{C}, \psi(a \otimes b) = (\tau(a) \cdot b)_\tau$ wobei τ alle Körperhomomorphismen $\tau \colon K \to \mathbb{C}$ durchläuft.*

Beweis. $K_{\mathbb{C}}$ ist endlich-dimensionale $\mathbb{C}$-algebra, also ein Modul endlicher Länge und damit Artinscher Ring. Nach 10.5.13 ist $K_{\mathbb{C}} \cong \prod R_i$ mit $(R_i, \mathfrak{m}_i)$ lokale artinsche Ringe. Es gilt dass $R_i/\mathfrak{m}_i = \mathbb{C}$ da $\mathbb{C}$ algebraisch abgeschlossen ist. Seien $\tau_1, \ldots, \tau_n$ die Homomorphismen $K \to \mathbb{C}$. Es ist $n = [K : \mathbb{Q}]_S = [K : \mathbb{Q}]$. Also sind auch $\tilde{\tau}_1, \ldots, \tilde{\tau}_n$ verschiedene Abbildungen $K_{\mathbb{C}} \to \mathbb{C}$. Jeder Homomorphismus von $\mathbb{C}$-Algebren $\prod R_i \to \mathbb{C}$ hat die Form $\prod R_i \to R_i \to R_i/\mathfrak{m}_i \cong \mathbb{C}$ siehe ???. Also ist Anzahl r der Homomorphismen $K_{\mathbb{C}} \to \mathbb{C}$ gleich Anzahl der Faktoren. Da jede Algebra R_i als Vektorraum mindestens Dimension 1 hat, muss $n \geq r$ sein. Aber oben haben wir gesehen, dass $r \geq n$. Also ist $r = n$ und $\dim_{\mathbb{C}}(R_i) = 1$. Somit ist $R_i \cong \mathbb{C}$.
Alternativ kann man auch wie folgt argumentieren: Sei $b \in K$ sodass $K = \mathbb{Q}[b] \cong \mathbb{Q}[X]/(f)$. Dann ist $K_{\mathbb{C}} \cong \mathbb{C}[X]/(f)$. Wenn $f = \prod_{i=0}^{r}(X - b_i)$ mit paarweisen verschiedenen Nullstellen in $\mathbb{C}$ dann ist

$$K_{\mathbb{C}} \cong \prod_{i=1}^{r} \mathbb{C}[X]/(X - b_i) \cong \prod \mathbb{C}_i$$

Es ist $\{b_1, \ldots, b_n\} = \{\tau(b) \colon \tau \colon K \to \mathbb{C}\}$. Sei $\tau_i \colon K \to \mathbb{C}$ sodass $\tau(b) = b_i$. dann ist die Abbildung gegeben durch

$$K_{\mathbb{C}} \xrightarrow{\sim} \prod_{i=1}^{n} \mathbb{C} \xrightarrow{pr_i} \mathbb{C}$$

$$b \otimes 1 \longmapsto (b_i)_{1,\ldots,n} \longmapsto b_i = \tau_i(b)$$

folglich ist die Abbildung wie im Satz auch für alle Elemente in $K_{\mathbb{C}}$. □

Beispiel 12.1.6. Sei $d > 1$ quadratfrei und $K = \mathbb{Q}[\sqrt{d}] \cong \mathbb{Q}[X]/(X^2 - d)$ Dann ist $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(X - \sqrt{d}) \times \mathbb{R}[X]/(X +$ wobei $1 \otimes a$ auf a, a geschickt wird und $\sqrt{d}$ auf $\sqrt{d}, -\sqrt{d}$. Wenn $d \not\equiv 1 \mod 4$ dann ist $d_K = d$ und $1, \sqrt{d}$ eine Ganzheitsbasis. Es ist $\mathrm{Vol}(\mathcal{O}_K) = |\det(\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix})| = \sqrt{d} = \sqrt{d_K}$ Analog wenn $d \equiv 1 \mod 4$ dann $\mathrm{Vol}(\mathcal{O}_K) = \sqrt{(d_K)}$

Teil V

Applied Mathematics

Kapitel 13

Cryptography

Book recommendations: Buchmann Einführung in die Kryptografie
Bernstein/Buchmann/Dahmen Post Quantum Cryptography
Hoffstein/Pipher/Silverman An introduction to mathematical Cryptography
Werner Elliptische Kurven in der Kryptografie
Criteria for passing: 50 percent of the points, 75 percent useful answers to questions, present twice per semester

13.1 Basics and historical examples

13.1.1 Ceasar-Chiffre

It was used during (100-44 bc)

Beispiel 13.1.1. WKDRO SCD CMRYOX Procedure: We choose a number of $i \in \{1, \dots, 26\}$ and move every letter of the plaintext by the fixed number i. For example $i = 5$ and the plaintext **TODAY**. This becomes **YTIFD**. The encyphered plaintext is called cipher text. The set of Keys is in this example $\mathbb{Z}/26\mathbb{Z}$.

Definition 13.1.2 (Cryptosystem)**.** A Cryptosystem consists of

1. a set $\mathcal{P}$ of plaintext
2. a set $\mathcal{C}$ of cipher text
3. a set $\mathcal{K}$ of Keys
4. an encyphering function $e\colon \mathcal{P} \times \mathcal{K} \to \mathcal{C}$
5. a decyphering function $d\colon \mathcal{C} \times \mathcal{K} \to \mathcal{P}$

Such that for each $k \in K$ there is a $h \in K$ such that

$$d(e(m,k),h) = m$$

for all $m \in \mathcal{P}$. Write for $e(m,k)$ also $e_k(m)$ and for $d(c,k) =$ also $d_k(m)$.

13.1.2 Kerkhoff's principle(Jean Guillaume Hubert Victoir François Alexandre August Kerkhoff von Nieuwenhof 1883)

The security of a crypto system should not be based on the knowledge of the used system. The security should only be based on the secrecy of the Key

13.2 Alphabet and Words

Definition 13.2.1. An Alphabet is a non-empty finite set. The elements of the Alphabet are called Letters.

Beispiel 13.2.2. Typical alphabets:

1. $\mathcal{A} = \{a, \ldots, z\}$
2. $\mathcal{A} = \{0, 1\}$
3. $\mathcal{A} =$ ASCII-Code} (American standard Code for information interchange)
4. $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$

Definition 13.2.3. Let $calA$ be an alphabet. A finite sequence of elements from $\mathcal{A}$ is called a Word over $\mathcal{A}$. The length of a Word ω over $\mathcal{A}$ is the length of the corresponding sequence. $\mathcal{A}^n$ is the set of Words of length n and $A^\infty = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$ the set of all Words.

Bemerkung 13.2.4.

1. The Word of length 0 is {} the empty Word.
2. Let $w_1 = \sigma_1 \ldots \sigma_r$ and $w_2 = \tilde{\sigma}_1 \ldots \tilde{\sigma}_s$ be Words over $\mathcal{A}$. Then

   $$w_1 \cdot w_2 := \sigma_1 \ldots \sigma_r \tilde{\sigma}_1 \ldots \tilde{\sigma}_s$$

   is again a Word. This makes $(\mathcal{A}^\infty, \cdot)$ a Monoid (Muliplication is associative with a neutral element {}.

Beispiel 13.2.5. In Caesar chiffre we have $\mathcal{P} = \mathcal{C} = \mathcal{A}^\infty$ with $\mathcal{A} = \mathbb{Z}/26$. $\mathcal{K} = \mathcal{A}$ and $e_k(w) = e_k(\sigma_1 \ldots \sigma_r) = \sigma_1 + k \ldots \sigma_r + k$ And $d_k(w) = d_k(\sigma_1 \ldots \sigma_r) = \sigma_1 - k \ldots \sigma_r - k$

Generalization

Beispiel 13.2.6 (Permutation Chiffre)**.** $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}\, \mathcal{P} = \mathcal{C} = \mathcal{A}^\infty, \mathcal{K} = S_n$ For $\pi \in S_n$ we set

$$e_\pi(w) = \pi(\sigma_1) \ldots \pi(\sigma_r) \in \mathcal{C}$$

$$d_\pi(w) = \pi^{-1}(\sigma_1) \ldots \pi^{-1}(\sigma_r) \in \mathcal{C}$$

13.2.1 Statistical analysis

In German and in English the five most often used letters are **E,N,I,R,S** with percentages 18, 11 , 8, 7, 7 in German and **E,T,A,I,N** with percentages 12,9,8,7,7 in English respectively. In our Crypto Systems we have to take care that the frequency of a letter has no importance.

Definition 13.2.7. A block Cipher is a crypto system in which all the plaintexts have the same length, as well as every cipher text. I.E. $\mathcal{P} = \mathcal{A}^n = \mathcal{C}$ for some $m \in \mathbb{N}$. Then for each $k \in K$ we have $e_k \colon \mathcal{A}^n \to \mathcal{A}^n$

Bemerkung 13.2.8. We can split any text in blocks of equal size.

Beispiel 13.2.9. The Vignère cipher is based on such a splitting.

13.2.2 Types of Attacks

1.
2. **Attack with the ciphertext(ciphertext only attack)** The attacker Eve has only the cipher text.
3. **Knowing plaintext attack** Eve has plain and Chiffre text for certain parts of the message.
4. **Chosen plaintext attack** Eve can produce to a given plaintext the cipher text

Beispiel 13.2.10 (Ceasar Cipher)**.** 1. Eve can try all the 26 Keys to decipher

2. Eve only needs to know the cipher text of one letter
3. Eve only needs to ask for the cipher text of one letter

Beispiel 13.2.11 (Permutation Cipher)**.** 1. Eve can use the statistical analysis
2. Eve knows the encyphering for some letters and can use first point for the remaining
3. She can ask to Encipher the Alphabet