Kommutative Algebra

N. Perrin

Düsseldorf
Sommersemester 2015

Inhaltsverzeichnis

1 Ringe und Ideale 5
1.1 Ringe . . . 5
1.2 Ideale . . . 6
1.3 Operationen über Ideale . . . 7
1.4 Nullteiler, Nilpotente Elemente invertierbare Elemente . . . 8
1.5 Primideale und maximale Ideale . . . 9
1.6 Lokale Ringe . . . 11
1.7 Radikal . . . 12
1.8 Chinesischer Restsatz . . . 13
1.9 Vermeidungslemma . . . 14
1.10 Konduktor . . . 15

2 Moduln 16
2.1 Definition . . . 16
2.2 Untermoduln . . . 17
2.3 Operationen über Moduln . . . 19
2.4 Direkte Summe und Produkt . . . 20
2.5 Endlich erzeugte Moduln . . . 21
2.6 Exakte Sequenzen II . . . 22
2.7 Lemma von Nakayama . . . 26
2.8 Tensorprodukt . . . 27
2.9 Exakte Sequenzen III . . . 31
2.10 Einschränkung und Erweiterung der Skalare . . . 35
2.11 Algebren . . . 36

3 Lokalisierung 38
3.1 Ringe . . . 38
3.2 Moduln . . . 41
3.3 Lokale vs globale Eingenschaften . . . 43
3.4 Ideale und lokalisierung . . . 46

4 Ganze Elemente 50
4.1 Ganze Elemente . . . 50
4.2 Going-up Theorem . . . 52
4.3 Going-down Theorem . . . 54
4.4 Nullstellensatz . . . 56

5 Dimension I 57
5.1 Transzendenzgrad . . . 57
5.2 Noethersches Lemma . . . 60
5.3 Dimension . . . 61

6 Ketten 64
6.1 Ketten und maximales Element . . . 64
6.2 Einfache Moduln und Länge . . . 67
6.3 Noethersche Ringe . . . 70
6.4 Artinsche Ringe . . . 71

7 Primäre Zerlegung 76
7.1 Primäre Ideale . . . 76
7.2 Primäre Zerlegung . . . 78
7.3 Lokalisierung . . . 80
7.4 Noethersche Ringe . . . 83

8 Dedekinsringe und diskrete Bewertungsringe 85
8.1 Eindimensionale noethersche Integritätsringe . . . 85
8.2 Diskrete Bewertungsringe . . . 86
8.3 Dedekinsringe . . . 89
8.4 Gebrochene Ideale . . . 89

9 Zahlkörper 93
9.1 Spur und Norm . . . 93
9.2 Ein Endlichkeitssatz . . . 97
9.3 Zahlkörper . . . 98

10 Vervollständigung 99
10.1 Topologische Gruppen . . . 99
10.2 Cauchyfolgen . . . 100
10.3 Projektive Limes I . . . 102
10.4 Projektive Limes und Vervollständigung . . . 103
10.5 Projektive Limes II . . . 104
10.6 Beispiele $\mathbb{Z}_p$ und $\mathsf{k}[[X]]$ . . . 106
10.7 Weitere Eigenschaften . . . 108
10.7.1 Noethersche Ringe . . . 108
10.7.2 Lokale noethersche Ringe, Dimension II . . . 108

1 Ringe und Ideale

In diesem Kapitel werden wir die Definitionen von Ringe und Ideale und ihre Haupteigenschaften wiederholen.

1.1 Ringe

Definition 1.1.1 1. **Ein Ring** $(A, +, \times)$ ist eine Menge A mit zwei Verknüpfungen $+ : A \times A \to A, (x, y) \mapsto x + y$ (die Addition) und $\times : A \times A \to A, (x, y) \mapsto xy$ (die Multiplikation) so, dass die folgende Axiome gelten:

1. $(A, +)$ ist eine Abelsche Gruppe mit 0 als neutralem Element.
2. Die Multiplikation ist assoziativ: es gilt $x(yz) = (xy)z$ für alle $x, y, z \in A$.
3. Die Addition ist bilinear (oder distributiv) bezüglich der Multiplikation: es gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$ für alle $x, y, z \in A$.
4. Es gibt eine Eins: es gibt ein Element $1 \in A$ so, dass $x1 = x = 1x$ gilt für alle $x \in A$.

2. Ein Ring $(A, +, \times)$ heißt **kommutativ** falls $xy = yx$ gilt für alle $x, y \in A$.

In dieser Vorlesung sind alle Ringe **kommutativ**.

Bemerkung 1.1.2 1. In jedem Ring gilt $0x = 0 = x0$: es gilt $0x = (0+0)x = 0x+0x$. Daraus folgt $x0 = 0x = 0$.

2. Die Gleichheit $1 = 0$ ist nicht ausgeschlossen. In diesem Fall gilt

$$x = 1x = 0x = 0$$

für alle $x \in A$. Es folgt also, dass A einelementig ist: $A = \{0\}$. Man schreibt in diesem Fall $A = 0$. Dieser Ring heißt **der Nullring**.

3. Die 0 und die 1 sind eindeutig bestimmt.

Definition 1.1.3 Ein Ringhomomorphismus (oder Morphismus in der Kategorie aller Ringe) ist eine Abbildung $f : A \to B$, wobei A und B Ringe sind so, dass

1. $f(x + y) = f(x) + f(y)$ für alle $x, y \in A$

2. $f(xy) = f(x)f(y)$ für alle $x, y \in A$
3. $f(1) = 1$.

Bemerkung 1.1.4 Seien $f : A \to B$ und $g : B \to C$ zwei Ringhomomorphismen. Dann ist $g \circ f$ ein Ring homomorphismus.

Definition 1.1.5 **Ein Unterring** B von A (oder Unterobjekt in der Kategorie aller Ringe) ist eine Teilmenge $B \subset A$ so, dass

1. $x - y \in B$ für alle $x, y \in B$
2. $xy \in B$ für alle $x, y \in B$
3. $1 \in B$.

Bemerkung 1.1.6 Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist $\mathrm{Im} f = f(A)$ ein Unterring von B.

Definition 1.1.7 Sei $(A_i)_{i \in I}$ eine Familie von Ringen. Dann ist das Produkt

$$\prod_{i \in I} A_i = \{(x_i)_{i \in I} \; | x_i \in A_i \text{ für alle } i \in I\}$$

mit $(x_i) + (y_i) = (x_i + y_i)$ und $(x_i)(y_i) = (x_i y_i)$ ein Ring mit $0 = (0_i)$ und $1 = (1_i)$ und heißt **Produktring**.

1.2 Ideale

Definition 1.2.1 Sei A ein Ring. **Ein Ideal** $\mathfrak{a}$ von A ist eine Teilmenge $\mathfrak{a} \subset A$ so, dass

1. $0 \in \mathfrak{a}$
2. $x - y \in \mathfrak{a}$ für alle $x, y \in \mathfrak{a}$
3. $xy \in \mathfrak{a}$ für alle $x \in \mathfrak{a}$ und $y \in A$

Beispiel 1.2.2 Die Menge $\{0\}$ ist ein Ideal: Das Nullideal. Wird werden dieses Ideal mit 0 schreiben.

Bemerkung 1.2.3 Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist $\mathrm{Ker} f$ ein Ideal von A. Die nächste Proposition zeigt, dass alle Ideale dieser Form sind.

Allermeiner, für $\mathfrak{b} \subset B$ ein Ideal, ist $f^{-1}(\mathfrak{b}) \subset A$ ein Ideal.

Ein Ideal $\mathfrak{a}$ ist also eine Untergruppe von $(A, +)$ und wir können das Quotient betrachten. Es ist eine Gruppe: die Quotientgruppe $(A/\mathfrak{a}, +)$. Man überprüft leicht (Übung, Siehe Auch das Skript Algebra Satz 2.1.22 und Korollar 2.1.31), dass die folgende Aussagen wahr sind.

Proposition 1.2.4 Sei A ein Ring und $\mathfrak{a}$ ein Ideal.

1. Die Verknüpfung $[x][y] = [xy]$ ist wohl definiert auf $A/\mathfrak{a}$ und $(A/\mathfrak{a}, +, \times)$ ist ein Ring mit Eins gegeben durch $[1]$.

2. Die kanonische Projektion $\pi : A \to A/\mathfrak{a}, x \mapsto [x]$ ist ein Ringhomomorphismus.

3. Sei $f : A \to B$ ein Ringhomomorphismus. Es gibt genau dann ein Ringhomomorphismus $\bar{f} : A/I \to B$ mit $f = \bar{f} \circ \pi$, wenn $\mathfrak{a} \subset \mathrm{Ker} f$. Die Abbildung $\bar{f}$ ist genau dann injektiv (bzw. surjektiv), wenn $\mathrm{Ker} f = \mathfrak{a}$ gilt (bzw. f surjektiv ist).

4. Es gibt eine Bijektion zwischen die Menge aller Ideale $\mathfrak{b} \subset A$ mit $\mathfrak{a} \subset \mathfrak{b}$ und die Menge aller Ideale $\overline{\mathfrak{b}} \subset A/\mathfrak{a}$:

$$\{\mathfrak{b} \text{ Ideal von } A \text{ mit } \mathfrak{a} \subset \mathfrak{b}\} \to \{\overline{\mathfrak{b}} \text{ Ideal von } A/\mathfrak{a}\},$$

mit $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ und $\overline{\mathfrak{b}} \mapsto \pi^{-1}(\overline{\mathfrak{b}})$.

1.3 Operationen über Ideale

Definition 1.3.1 Sei A ein Ring.

1. Seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale. Dann ist die Summe $\mathfrak{a} + \mathfrak{b} = \{x + y \in A \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$ ein Ideal: **die Summe von $\mathfrak{a}$ und $\mathfrak{b}$**.

2. Allgemeiner, sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie von Ideal. Dann ist die Summe $\sum_i \mathfrak{a}_i = \{\sum_i x_i \in A \mid x_i \in \mathfrak{a}_i, x_i \neq 0$ nur für endlich viele $i \in I\}$ ein Ideal: **die Summe aller** $(\mathfrak{a}_i)_{i \in I}$.

Bemerkung 1.3.2 1. Die Summe $\mathfrak{a} + \mathfrak{b}$ (bzw. $\sum_i \mathfrak{a}_i$) heißt auch, dass von $\mathfrak{a}$ und $\mathfrak{b}$ (bzw. $(\mathfrak{a}_i)_{i \in I}$) erzeugte Ideal. Es ist das kleinste Ideal, das $\mathfrak{a}$ und $\mathfrak{a}$ (bzw. $(\mathfrak{a}_i)_{i \in I}$) enthält.

2. Falls $\mathfrak{a} = (x)$ und $\mathfrak{b} = (y)$ schreibt man $\mathfrak{a} + \mathfrak{b} = (x) + (y) = (x, y)$. Allgemeiner falls $\mathfrak{a}_i = (x_i)$ für alle $i \in I$ schreibt man $\sum_i \mathfrak{a}_i = \sum_i (x_i) = (x_i \, | i \in I)$. Für $I = [1, n]$ schreibt man $(x_i \, | i \in I) = (x_1, \cdots, x_n)$.

Bemerkung 1.3.3 Sei A ein Ring.

1. Seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale. Dann ist der Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ ein Ideal.

2. Allgemeiner, sei $(\mathfrak{a}_i)_{i \in I}$ eine Familie von Ideal. Dann ist die Schnittmenge $\cap_i \mathfrak{a}_i$ ein Ideal.

Beispiel 1.3.4 Für $n, m \in \mathbb{Z}$ gilt $(n) + (m) = (\mathrm{ggT}(n, m))$ und $(n) \cap (m) = (\mathrm{kgV}(n, m))$

Definition 1.3.5 Sei A ein Ring.

1. Seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale. **Das Produktideal** $\mathfrak{ab}$ ist das Ideal

$$\mathfrak{ab} = (xy | x \in \mathfrak{a}, y \in \mathfrak{b})$$

(das von aller Produkte xy mit $x \in \mathfrak{a}$ und $y \in \mathfrak{b}$ erzeugte Ideal).

2. Allgemeiner, sei $(\mathfrak{a}_i)_{i[1,n]}$ eine endliche Familie von Ideal. Dann definiert man das Produktideal per Induktion: $\mathfrak{a}_1 \cdots \mathfrak{a}_n = (\cdots((\mathfrak{a}_1\mathfrak{a}_2)\mathfrak{a}_3)\cdots\mathfrak{a}_n)$. Dieses Ideal ist das von aller Elementen der Form $x_1 \cdots x_n$ mit $x_i \in \mathfrak{a}_i$ für alle $i \in [1, n]$ erzeugte Ideal:

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n = (x_1 \cdots x_n \mid x_i \in \mathfrak{a}_i \text{ für alle } i \in [1, n]).$$

3. Insbesonde für $\mathfrak{a}$ ein Ideal ist $\mathfrak{a}^n$ das von aller Elementen der Form $x_1 \cdots x_n$ mit $x_i \in \mathfrak{a}$ für alle $i \in [1, n]$ erzeugte Ideal:

$$\mathfrak{a}^n = (x_1 \cdots x_n \mid x_i \in \mathfrak{a} \text{ für alle } i \in [1, n]).$$

Bemerkung 1.3.6 Es gilt $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.

Beispiel 1.3.7 Für $\mathfrak{a} = (2) = \mathfrak{b} \subset \mathbb{Z}$ gilt $\mathfrak{ab} \subsetneq \mathfrak{a} \cap \mathfrak{b}$: Es gilt $\mathfrak{ab} = (2)(2) = (4) \subsetneq (2) = (2) \cap (2) = \mathfrak{a} \cap \mathfrak{b}$.

Proposition 1.3.8 Es gilt (distibutiv Gesetz): $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.

Beweis. Übgung. ∎

1.4 Nullteiler, Nilpotente Elemente invertierbare Elemente

Definition 1.4.1 Sei A ein Ring.

1. Ein Element $x \in A$ heißt **Nullteiler** falls es ein $y \in A$ gibt mit $y \neq 0$ so, dass $xy = 0$. Ein Ring $A \neq 0$ ohne Nullteiler (d.h. alle Nullteiler sind Null) heißt **nullteilerfrei oder Integritätsring**.

2. Ein Element $x \in A$ heißt **nilpotent** falls es eine Ganze Zahl $n \geq 1$ mit $x^n = 0$. Ein Ring ohne nilpotente Elemente (d.h. alle nilpotente Elemente sind Null) heißt **reduziert**

3. Ein Element $x \in A$ heißt **invertierbar** falls es ein $y \in A$ gibt mit $xy = 1$. Das Element y ist eindeutig bestimmt und heißt **Inverse** von x und wird x^{-1} bezeichnet. Man schreibt $A^\times$ für die Menge aller invertierbaren Elementen.

Bemerkung 1.4.2 1. Ein nilpotentes Element ist immer ein Nullteiler (außer wenn $A = 0$) aber Nullteiler sind nicht immer nilpotent (z.B. 2 und 3 in $\mathbb{Z}/6\mathbb{Z}$).

2. Die Menge $(A^\times, \times)$ ist eine kommutative Gruppe.

3. Ein Unterring eines Integritätsrings ist auch ein Integritätsring.

Definition 1.4.3 Sei $x \in A$. Die Menge $(x) = \{xy \in A \mid y \in A\}$ ist ein Ideal von A und wird (x) bezeichnet. Ein Ideal dieser Form heißt **Hauptideal**. Ein Ring so, dass alle Ideale Hauptideale sind heißt **Hauptidealring**.

Bemerkung 1.4.4 Sei $x \in A$. Es gilt $x \in A^\times \Leftrightarrow (x) = A$.

Definition 1.4.5 **Ein Körper** ist ein Ring $(A, +, \times)$ mit $1 \neq 0$ und $A^\times = A \setminus \{0\}$.

Proposition 1.4.6 Sei A ein Ring. Die folgende Aussagen sind äquivalent:

1. A ist ein Körper
2. Die einzige Ideale von A sind A und 0.
3. Alle ringhomomorphismen $f : A \to B$ mit $B \neq 0$ sind injektiv.

Beweis. (1. $\Rightarrow$ 2.) Sei $0 \neq \mathfrak{a} \subset A$ ein Ideal. Sei $0 \neq x \in \mathfrak{a}$. Dann ist x invertierbar und es gilt $A = (x) \subset \mathfrak{a} \subset A$ also $\mathfrak{a} = A$.

(2. $\Rightarrow$ 3.) Der Kernel $\mathrm{Ker} f$ ist ein Ideal und es gilt $f(1) = 1 \neq 0$ also $\mathrm{Ker} f \neq A$. Es folgt $\mathrm{Ker} f = 0$ und f injektiv.

(3. $\Rightarrow$ 1.) Sei $x \in A$ nicht invertierbar und $\mathfrak{a} = (x)$. Es gilt $(x) \subsetneq A$ und also $A/\mathfrak{a} \neq 0$. Daraus folgt, dass $\pi : A \to A/\mathfrak{a}$ injektiv ist und also $\mathfrak{a} = \mathrm{Ker}\pi = 0$. Es folgt $x = 0$. ∎

1.5 Primideale und maximale Ideale

Definition 1.5.1 Sei A ein Ring.

1. Ein Ideal $\mathfrak{p} \subset A$ heißt **Primideal** falls $\mathfrak{p} \neq A$ und die Implikation ($xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$) gilt für alle $x, y \in A$.

2. Ein Ideal $\mathfrak{m} \subset A$ heißt **maximales Ideal** falls $\mathfrak{m} \neq A$ und die Implikation ($\mathfrak{m} \subset \mathfrak{a} \subset A \Rightarrow \mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = A$) gilt für alle Ideale $\mathfrak{a} \subset A$.

Man zeigt (Übung, siehe Algebra Lemma 2.1.36)

Proposition 1.5.2 Sei A ein Ring und seien $\mathfrak{p}, \mathfrak{m} \subset A$ Ideale.

1. $\mathfrak{p}$ ist ein Primideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist ein Integritätsring.

2. $\mathfrak{m}$ ist ein maximales Ideal $\Leftrightarrow$ $A/\mathfrak{m}$ ist ein Körper.

Bemerkung 1.5.3 Daraus folgt, dass maximale Ideale Primideale sind. Aber nicht alle Primideale sind maximal (z.B. ist 0 ein Primideal in $\mathbb{Z}$ aber kein maximales Ideal).

Daraus und aus dem Isomorphiesatz folgt:

Korollar 1.5.4 Sei $f : A \to B$ ein Ringhomomorphismus und $\mathfrak{b}$ ein Primideal von B. Dann ist $f^{-1}(\mathfrak{b})$ ein Primideal von A.

Beweis. Sei $g : A \to B/\mathfrak{b}$ mit $g = \pi \circ f$. Es gilt $\mathrm{Ker} g = f^{-1}(\mathfrak{b})$. Daraus folgt, dass es ein injektiver Ringhomomorphismus $\bar{g} : A/f^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$ also ist $A/f^{-1}(\mathfrak{b})$ isomorph zu einem Unterring von $B/\mathfrak{b}$. Da $B/\mathfrak{b}$ ein Integritätsring ist, ist auch $A/f^{-1}(\mathfrak{b})$ ein Integritätsring. ∎

Bemerkung 1.5.5 Die obige Aussage ist für maximale Ideale falsch. Z.B. für $f : \mathbb{Z} \to \mathbb{Q}, x \mapsto x$ ist $f^{-1}(0) = 0$ nicht maximal (aber noch ein Primideal).

Proposition 1.5.6 Sei $f : A \to B$ surjektiv und $\mathfrak{b} \subset B$ maximal. Dann ist $f^{-1}(\mathfrak{b})$ maximal in A.

Beweis. Sei $\mathfrak{a} = \mathrm{Ker} f$. Es gilt $B \simeq A/\mathfrak{a}$. Ohne Einschränkung können wir also f mit der kanonischen Projektion $\pi : A \to A/\mathfrak{a}$ ersetzen. Die Aussage folgt jetzt aus Proposition 1.2.4. ∎

Die folgende Aussage ist äquivalent zum Auswahl-Axiom (dies werden wir nicht beweisen).

Lemma 1.5.7 (Zornslemma) Sei S eine nicht leere Menge mit einer Ordnung $\leq$ (eine Ordnung ist eine Relation R die reflexiv ist *i.e.* xRx für alle $x \in S$, transitiv ist *i.e.* (xRy und $yRz \Rightarrow xRz$) für alle $x, y, z \in S$ und so, dass (xRy und $yRx \Rightarrow x = y$).

Eine Kette T in S ist eine Teilmenge $T \subset S$ so, dass $x \leq y$ oder $y \leq x$ für alle $x, y \in T$.

Falls jede Kette eine obere Grenze hat (*i.e.* es gibt ein $x \in S$ mit $y \leq x$ für alle $y \in T$), dann hat S ein maximales Element. □

Bemerkung 1.5.8 Eine nicht leere geordnete Menge $(S, \leq)$ für die jede Kette eine obere Grenze hat heißt **induktiv**.

Als Korollar gilt

Theorem 1.5.9 Jeder Ring A hat ein maximales Ideal. □

Beweis. Sei S die menge aller echten Ideale in A mit der Ordnung $\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b}$. Dann ist S induktiv: Sei T eine Kette von Ideale. Dann ist

$$\mathfrak{b} = \bigcup_{\mathfrak{a} \in T} \mathfrak{a}$$

ein Ideal: falls $x, y \in \mathfrak{b}$, dann gibt es $\mathfrak{a}, \mathfrak{a}' \in T$ mit $x \in \mathfrak{a}$ und $y \in \mathfrak{a}'$. Es gilt aber $\mathfrak{a} \subset \mathfrak{a}'$ oder $\mathfrak{a}' \subset \mathfrak{a}$ also ohne Einschränkung gilt $\mathfrak{a}' \subset \mathfrak{a}$. Es folgt $x + y, xy \in \mathfrak{a} \subset \mathfrak{b}$. Es gilt auch $\mathfrak{b} \subsetneq A$: sonnst gilt $1 \in \mathfrak{b}$ also gibt es ein $\mathfrak{a} \in T$ mit $1 \in \mathfrak{a}$ und $\mathfrak{a} = A$, ein Widerspruch. Also ist S induktiv und hat ein maximales Element: ein maximales Ideal von A. ∎

Korollar 1.5.10 Sei $\mathfrak{a} \subset A$ ein Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von A mit $\mathfrak{a} \subset \mathfrak{m}$.

Beweis. Setze $\mathfrak{m} = \pi^{-1}(\overline{\mathfrak{m}})$, wobei $\pi : A \to A/\mathfrak{a}$ die kanonische Projektion ist und $\overline{\mathfrak{m}}$ ein maximales Ideal von $A/\mathfrak{a}$ ist. ∎

Korollar 1.5.11 Sei $x \in A$ ein nicht invertierbares Element. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von A mit $x \in \mathfrak{m}$.

Beweis. Sei $\mathfrak{a} = (x)$. Die Aussage folgt aus dem obigen Korollar. ∎

1.6 Lokale Ringe

Definition 1.6.1 Ein Ring A heißt **lokal** falls A nur ein maximales Ideal $\mathfrak{m}$ enthält. Der Körper $A/\mathfrak{m}$ heißt **Restklassenkörper**

Proposition 1.6.2 Sei A ein Ring und $\mathfrak{m} \neq A$ ein Ideal.

1. Falls $A \setminus \mathfrak{m} = A^\times$, dann ist A ein lokaler Ring und $\mathfrak{m}$ sein maximales Ideal.

2. Falls $\mathfrak{m}$ maximal ist und alle Elemente der Form $1 + x$ mit $x \in \mathfrak{m}$ invertierbar sind, dann ist A ein lokaler ring (mit maximalem Ideal $\mathfrak{m}$).

Beweis. 1. Sei $\mathfrak{m}'$ ein maximales Ideal. Es gilt $\mathfrak{m}' \subset A \setminus A^\times = \mathfrak{m}$ und also $\mathfrak{m}' = \mathfrak{m}$.

2. Sei $x \in A \setminus \mathfrak{m}$. Dann gilt $(x) + \mathfrak{m} = A$, wobei $(x) + \mathfrak{m}$ das von $\mathfrak{m}$ und x erzeugte Ideal ist. Es gibt also Elemente $y \in \mathfrak{m}$ und $z \in A$ mit $1 = y + xz$. Es folgt $xz = 1 - y$. Sei $u = (1 - y)^{-1}$ (das Element $1 - y$ ist invertierbar per Annahme). Es gilt $xzu = 1$ und $x \in A^\times$. Daraus folgt $A \setminus \mathfrak{m} \subset A^\times$. Die Ruckenthaltung ist immer wahr (Elemente aus $\mathfrak{m}$ sind nicht invertiebar) also folgt $A \setminus \mathfrak{m} = A^\times$ und die Aussage folgt aus 1. ∎

1.7 Radikal

Lemma 1.7.1 Die Menge $\mathfrak{n}(A) = \sqrt{0} = \{x \in A \mid x \text{ nilpotent}\}$ ist ein Ideal und heißt **Radikalideal oder Nilradikal von** A.

Das quotient $A/\mathfrak{n}(A)$ hat kein nilpotentes Element also ist reduziert. □

Beweis. Übung. ■

Proposition 1.7.2 Das Nilradikal $\mathfrak{n}(A)$ ist die Schnittmenge aller Primideale in A:

$$\mathfrak{n}(A) = \bigcap_{\mathfrak{p} \subset A \text{ Primideal}} \mathfrak{p}.$$

Beweis. Sei $\mathfrak{n}'$ die Schnittmenge aller Primideale in A und sei $x \in \mathfrak{n}(A)$. Es gilt $x^n = 0 \in \mathfrak{p}$ also per Induktion $x \in \mathfrak{p}$ für alle $\mathfrak{p}$ Primideale in A. Es folgt $x \in \mathfrak{n}'$.

Umgekehrt, sei $x \in A \setminus \mathfrak{n}(A)$. Sei S die folgende Menge von Idealen in A:

$$S = \{\mathfrak{a} \mid \mathfrak{a} \subset A \text{ ideal und } x^n \notin \mathfrak{a} \text{ für alle } n \geq 1\}.$$

Sie Menge S mit der Ordnung $\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b}$ ist induktiv: die Menge ist nicht leer, weil $\mathfrak{n}(A) \in S$ und falls T eine Kette in S ist, ist

$$\mathfrak{b} = \bigcup_{\mathfrak{a} \in T} \mathfrak{a}$$

ein Ideal. Falls es ein $n \geq 1$ gibt mit $x^n \in \mathfrak{b}$ dann gibt es ein $\mathfrak{a} \in T$ mit $x^n \in \mathfrak{a}$. Ein Widerspruch zu $\mathfrak{a} \in T \subset S$. Es folgt, dass $\mathfrak{b}$ eine obere Grenze gür T ist und S hat ein maximales Element $\mathfrak{p}$.

Wir zeigen, dass $\mathfrak{p}$ ein Primideal ist. Seien $y, z \in A \setminus \mathfrak{p}$. Dann gilt $\mathfrak{p} \subsetneq (y) + \mathfrak{p}$ und $\mathfrak{p} \subsetneq (z) + \mathfrak{p}$. Es folgt $(y) + \mathfrak{p} \notin S$ und $(z) + \mathfrak{p} \notin S$ und es gibt $n, m \geq 1$ mit $x^n \in (y) + \mathfrak{p}$ und $x^m \in (z) + \mathfrak{p}$. Es folgt $x^{n+m} \in (yz) + \mathfrak{p}$ und $(yz) + \mathfrak{p} \notin S$. Insbesondere gilt $yz \notin \mathfrak{p}$ und $\mathfrak{p}$ ist ein Primideal.

Es folgt, dass $x \notin \mathfrak{p}$, wobei $\mathfrak{p}$ ein Primideal ist also $x \notin \mathfrak{n}'$. Es folgt $A \setminus \mathfrak{n}(A) \subset A \setminus \mathfrak{n}'$ und also $\mathfrak{n}' \subset \mathfrak{n}(A)$. ■

Definition 1.7.3 Sei $\mathfrak{a} \subset A$ ein Ideal, **das Radikal von** $\mathfrak{a}$ is die Menge

$$\sqrt{\mathfrak{a}} = \{x \in A \mid \text{es gibt ein } n \geq 1 \text{ mit } x^n \in \mathfrak{a}\}.$$

Proposition 1.7.4 Sei $\mathfrak{a} \subset A$ ein Ideal.

1. $\sqrt{\mathfrak{a}}$ is ein Ideal.
2. $A/\sqrt{\mathfrak{a}}$ ist reduziert.

3. $\mathfrak{a} = \sqrt{\mathfrak{a}} \Leftrightarrow A/\sqrt{\mathfrak{a}}$ ist reduziert.

4. Das Radikal $\sqrt{\mathfrak{a}}$ ist die Schnittmenge aller Primideale in A die $\mathfrak{a}$ enthalten:

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a}\mathfrak{p}\subset A \text{ Primideal}} \mathfrak{p}.$$

Beweis. 1. Sei $\pi : A \to A/\mathfrak{a}$. Es gilt $\sqrt{\mathfrak{a}} = \pi^{-1}(\mathfrak{n}(A/\mathfrak{a}))$.

2. Es gilt $A/\sqrt{\mathfrak{a}} \simeq (A/\mathfrak{a})/(\sqrt{\mathfrak{a}}/\mathfrak{a}) = (A/\mathfrak{a})/\mathfrak{n}(A/\mathfrak{a})$ und ist also reduziert.

3. Es gilt $A/\mathfrak{a}$ reduziert $\Leftrightarrow \mathfrak{n}(A/\mathfrak{a}) = 0 \Leftrightarrow A/\sqrt{\mathfrak{a}} = A/\mathfrak{a} \Leftrightarrow \sqrt{\mathfrak{a}} = \mathfrak{a}$.

4. Folgt aus der Gleichung $\sqrt{\mathfrak{a}} = \pi^{-1}(\mathfrak{n}(A/\mathfrak{a}))$, wobei $\pi : A \to A/\mathfrak{a}$ die kanonische Projektion ist und aus dem obigen Proposition für $A/\mathfrak{a}$. ∎

Definition 1.7.5 Das Jacobson Radikal $\mathfrak{R}(A)$ ist die Schnittmenge aller maximalen Ideale von A:

$$\mathfrak{R}(A) = \bigcap_{\mathfrak{m}\subset A \text{ maximal}} \mathfrak{m}.$$

Proposition 1.7.6 Sei $x \in A$. Dann gilt

$$x \in \mathfrak{R}(A) \Leftrightarrow 1 - xy \in A^\times \text{ für alle } y \in A.$$

Beweis. ($\Rightarrow$) Sei $x \in \mathfrak{R}(A)$ und $y \in A$. Falls $1 - xy$ nicht invertierbar ist, gibt es ein maximales Ideal $\mathfrak{m}$ mit $1 - xy \in \mathfrak{m}$. Es folgt $1 = 1 - xy + xy \in \mathfrak{m}$. Ein Widerspruch.

($\Leftarrow$) Sei $x \notin \mathfrak{R}(A)$. Es gibt also ein maximales Ideal $\mathfrak{m}$ mit $x \notin \mathfrak{m}$. Daraus folgt $\mathfrak{m} \subsetneq (x) + \mathfrak{m}$ und also $(x) + \mathfrak{m} = A$. Eg gibt also ein $y \in A$ und ein $z \in \mathfrak{m}$ so, dass $1 = xy + z$ *i.e.* $1 - xy = z \in \mathfrak{m}$. Es folgt, dass $1 - xy$ nicht invertierbar ist. ∎

1.8 Chinesischer Restsatz

Definition 1.8.1 Zwei Ideale $\mathfrak{a}, \mathfrak{b} \subset A$ heißer **teilerfremd** falls gilt $\mathfrak{a} + \mathfrak{b} = A$.

Sei A ein Ring und seien $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ Ideale. Man definiert ein Ringhomomorphismus $f : A \to \prod_{i=1}^n A/\mathfrak{a}_i$ durch $f(x) = ([x]_{\mathfrak{a}_1}, \cdots, [x]_{\mathfrak{a}_n})$, wobei $[x]_{\mathfrak{a}_i}$ die Restklasse von x in $A/\mathfrak{a}_i$ ist.

Proposition 1.8.2 (Chinesischer Restsatz) Seien A und $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ wie oben.

1. Falls die Ideale $(\mathfrak{a}_i)_{i\in[1,n]}$ paarweise teilerfremd sind gilt $\prod_i \mathfrak{a}_i = \cap_i \mathfrak{a}_i$.

2. f ist surjektiv $\Leftrightarrow$ die Ideale $(\mathfrak{a}_i)_{i\in[1,n]}$ sind paarweise teilerfremd

3. f ist injektiv $\Leftrightarrow \cap_i \mathfrak{a}_i = 0$.

Beweis. 1. Per Induktion nach n. Für $n = 2$ folgt die Aussage aus dem Übungsblatt 1. Sei also $n > 2$. Sei $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \cap_{i=1}^{n-1} \mathfrak{a}_i$. Es gilt $\mathfrak{a}_i + \mathfrak{a}_n = A$ also gibt es Elemente $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_n$ mit $x_i + y_i = 1$. Es folgt

$$\mathfrak{b} \ni x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) \equiv 1 \pmod{\mathfrak{a}_n}.$$

Es folgt $\mathfrak{b} + \mathfrak{a}_n = A$ und also $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} \cap \mathfrak{a}_n$.

2. ($\Rightarrow$) Wir zeigen, dass $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd sind (analog wird gelten, dass dass $\mathfrak{a}_i$ und $\mathfrak{a}_j$ teilerfremd sind für alle $i \neq j$). Da f surjektiv ist, gibt es ein $x \in A$ mit $f(x) = (1, 0, \cdots, 0)$. Es folgt $x \equiv 1 \pmod{\mathfrak{a}_1}$ also $1 - x \in \mathfrak{a}_1$. Daraus folgt $1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$ und $A = \mathfrak{a}_1 + \mathfrak{a}_2$.

($\Leftarrow$) Es genügt zu zeigen, dass es ein $x \in A$ gibt mit $f(x) = (1, 0, \cdots, 0)$ (analog gilt $(0, \cdots, 0, 1, 0 \cdots, 0) \in \mathrm{Im} f$). Für $i \geq 2$ gibt es Elemente $x_i \in \mathfrak{a}_1$ und $y_i \in \mathfrak{a}_i$ mit $x_i + y_i = 1$. Sei $x = y_2 \cdots y_n$. Dann gilt $x = (1 - x_2) \cdots (1 - x_n) \equiv 1 \pmod{\mathfrak{a}_1}$ und $x \in \mathfrak{a}_i$ für alle $i \geq 2$. Es folgt $f(x) = (1, 0, \cdots, 0)$.

3. Es gilt $\mathrm{Ker} f = \cap_i \mathfrak{a}_i$. ■

1.9 Vermeidungslemma

Proposition 1.9.1 Sei A ein Ring.

1. Seien $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ Primideale und $\mathfrak{a}$ ein Ideal so, dass

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Dann gibt es ein i mit $\mathfrak{a} \subset \mathfrak{p}_i$.

2. Seien $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ Ideale und $\mathfrak{p}$ ein Primideal mit

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subset \mathfrak{p} \text{ (bzw. } \bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}).$$

Dann gibt es ein i mit $\mathfrak{a}_i \subset \mathfrak{p}$ (bzw. $\mathfrak{a}_i = \mathfrak{p}$).

Beweis. 1. Ohne Einschränkung können wir annehmen, dass n minimal ist mit $\mathfrak{a} \subset \cup_{i=1}^{n} \mathfrak{p}_i$. Wir zeigen, dass $n = 1$. Sei also $n \geq 2$. Für alle $j \in [1, n]$ gilt

$$\mathfrak{a} \not\subset \bigcup_{i=1, i \neq j}^{n} \mathfrak{p}_i.$$

Sei also $x_j \in \mathfrak{a} \setminus \cup_{i=1, i \neq j}^{n} \mathfrak{p}_i$. Es folgt $x_j \in \mathfrak{p}_j$ und $x = x_1 + x_2 \cdots x_n \in \mathfrak{a}$. Sei i so, dass $x \in \mathfrak{p}_i$. Falls $i \geq 2$ folgt $x_1 = x - x_2 \cdots x_i \cdots x_k \in \mathfrak{p}_i$ ein Widerspruch. Falls $x \in \mathfrak{p}_1$

gilt $x_2 \cdots x_k = x - x_1 \in \mathfrak{p}_1$. Da $\mathfrak{p}_1$ Prim ist folgt, dass es ein $j \geq 2$ gibt mit $x_j \in \mathfrak{p}_1$ ein Widerspruch.

2. Angenommen $\mathfrak{a}_i \not\subset \mathfrak{p}$ für alle $i \in [1, n]$, sei $x_i \in \mathfrak{a}_i$ mit $x_i \notin \mathfrak{p}$ für alle $i \in [1, n]$ und sei $x = x_1 \cdots x_n$. Es gilt $x \in \mathfrak{a}_i$ für alle i und also $x \in \mathfrak{p}$. Daraus folgt, dass es ein i gibt mit $x_i \in \mathfrak{p}$. Ein Widerspruch. ∎

1.10 Konduktor

Definition 1.10.1 Seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in A. **Der Konduktor von $\mathfrak{b}$ nach $\mathfrak{a}$** ist die Menge

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subset \mathfrak{a}\}.$$

Falls $\mathfrak{a} = 0$ heißt der Konduktor $(0 : \mathfrak{b})$ **der Annihilator von $\mathfrak{b}$**. Man schreibt $\mathrm{Ann}(\mathfrak{b}) = (0 : \mathfrak{b})$. Falls $\mathfrak{b} = (x)$ schreibt man $\mathrm{Ann}(\mathfrak{b}) = \mathrm{Ann}(x)$.

Bemerkung 1.10.2 1. Der Konduktor ist ein Ideal (Übung).

2. Es gilt $\mathrm{Ann}(0) = A$.

3. Die Menge aller Nullteiler ist $\bigcup_{x \neq 0} \mathrm{Ann}(x)$.

2 Moduln

2.1 Definition

Definition 2.1.1 Sei A ein Ring. Ein **A-Modul** ist eine abelsche Gruppe M mit einer linearen Wirkung von A *i.e.* mit einer Abbildung $A \times M \to M$, $(a, m) \mapsto am$ so, dass

1. $a(m + m') = am + am'$ für alle $a \in A$ und $m, m' \in M$,
2. $(a + b)m = am + bm$ für alle $a, b \in A$ und $m \in M$,
3. $a(bm) = (ab)m$ für alle $a, b \in A$ und $m \in M$,
4. $1m = m$ für alle $m \in M$.

Bemerkung 2.1.2 Diese Definition ist äquivalent zu den Eingaben von einer abelschen Gruppe M und einem Ringhomomorphismus $A \to \mathrm{End}(M)$, wobei $\mathrm{End}(M)$ der Ring aller Gruppenhomomorphismen von M nach M ist.

Bemerkung 2.1.3 Die triviale Gruppe $M = \{0\}$ ist ein A-Modul für jeden Ring A mit $a0 = 0$. Dieser Modul heißt **Nullmodul**.

Beispiel 2.1.4 1. Der Ring A ist ein A-Modul mit der Multiplikation $A \times A \to A$, $(a, m) \mapsto am$.

2. Falls $A = \mathsf{k}$ ein Körper ist gilt (A-Modul) $=$ (k-Vektorraum).

3. Falls $A = \mathbb{Z}$, gilt (A-Modul) $=$ (abelsche Gruppe), wobei $nm = \underbrace{m + \cdots + m}_{n\text{-Mal}}$.

4. Für $A = \mathsf{k}[X]$ mit k ein Körper, gilt (A-Modul) $=$ (k-Vektorraum mit einem Endomorphismus f), wobei $Xm = f(m)$.

5. Sei G eine Gruppe und k ein Körper. Sei $A = \mathsf{k}[G]$ die k-Algebra von G. Dann gilt ($\mathsf{k}[G]$-Modul) $=$ (k-Darstellung von G).

Definition 2.1.5 Sei A ein Ring.

1. Ein **A-Modulhomomorphismus** ist eine Abbildung $f : M \to N$, wobei M und N A-Moduln sind mit

   1. $f(m + m') = f(m) + f(m')$ für alle $m, m' \in M$ und

2. $f(am) = af(m)$ für alle $a \in A$ und $m \in M$.

Die Menge aller A-Modulhomomorphismen von M nach N ist $\mathrm{Hom}_A(M, N)$ (oder $\mathrm{Hom}(M, N)$ bezeichnet.

2. Ein A-Modulisomorphismus ist ein A-Modulhomomorphismus $f : M \to N$ so, dass es ein A-Modulhomomorphismus $g : N \to M$ gibt mit $f \circ g = \mathrm{Id}_N$ und $g \circ f = \mathrm{Id}_M$.

Bemerkung 2.1.6 1. Die Komposition von zwei A-Modulhomomorphismen ist ein A-Modulhomomorphismus.

2. Ein A-Modulhomomorphismus f ist genau dann ein Isomorphismus, wenn f bijektiv ist.

3. Die Menge $\mathrm{Hom}(M, N)$ ist ein A-Modul mit $(f + g)(m) = f(m) + g(m)$ und $(af)(m) = af(m)$.

4. Seien $g : M' \to M$ und $h : N \to N'$ zwei A-Modulhomomorphismen. Dann gibt es induzierte A-Modulhomomorphismen

$$\mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N) \text{ und } \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N')$$

definiert durch $f \mapsto f \circ g$ und $f \mapsto h \circ f$.

5. Es gibt ein A-Modulisomorphismus $\mathrm{Hom}(A, M) \simeq M$ gegeben durch $f \mapsto f(1)$ und $m \mapsto (E_m : A \to M)$, wobei $E_m(a) = am$.

2.2 Untermoduln

Definition 2.2.1 Sei M ein A-Modul. Ein **Untermodul** N von M ist eine Untergruppe von N so, dass $an \in N$ für alle $a \in A$ und $n \in N$.

Bemerkung 2.2.2 Die Untermoduln von A betrachtet als A-Modul sind die Ideale.

Lemma 2.2.3 Sei $f : M \to N$ ein Modulhomomorphismus. Dann sind $\mathrm{Ker} f$ und $\mathrm{Im} f$ Untermoduln.

Allgemeiner, seien $M' \subset M$ und $N' \subset N$ Untermoduln. Dann sind $f^{-1}(N')$ und $f(M')$ Untermoduln von M und N. □

Beweis. Übung. ∎

Alle Untermoduln können als Kernel eines Modulhomomorphimus dargestellt werden.

Lemma 2.2.4 Sei $N \subset M$ ein Untermodul. Dann ist der Quotient M/N ein A-Modul mit $a[m] = [am]$, die kanonische Projektion $\pi : M \to M/N$ ist ein Modulhomomorhismus und $\mathrm{Ker}\pi = N$. □

Beweis. Übung. ■

Proposition 2.2.5 Sei $f : M \to N$ ein Modulhomomorphismus und $M' \subset M$ ein Untermodul und $\pi : M \to M/M'$ die kanonische Projektion.

1. Es gibt genau dann ein Modulhomomorphismus $\bar{f} : M/M' \to N$ mit $f = \bar{f} \circ \pi$, wenn $M' \subset \mathrm{Ker}f$.

2. Es gilt $\mathrm{Ker}\bar{f} = \mathrm{Ker}f/M'$.

3. Die Abbildung $\bar{f}$ ist genau dann injektiv (bzw. surjektiv), wenn $\mathrm{Ker}f = M'$ gilt (bzw. f surjektiv ist).

Beweis. Übung. ■

Korollar 2.2.6 Sei $f : M \to N$ ein Homomorphismus. Es gilt $M/\mathrm{Ker}f \simeq \mathrm{Im}f$.

Definition 2.2.7 Sei $f : M \to N$ ein Modulhomomorphismus. **Der Cokernel** $\mathrm{Coker}f$ **von** f ist das Quotient $\mathrm{Coker}f = N/\mathrm{Im}f$.

Definition 2.2.8 **Eine exakte Sequenz von Moduln** ist eine Kette von Modulhomomorphismen

$$\cdots \to M_{i-1} \stackrel{f_{i-1}}{\to} M_i \stackrel{f_i}{\to} M_{i+1} \to \cdot$$

so, dass $\mathrm{Im}f_{i-1} = \mathrm{Ker}f_i$ für alle i.

Bemerkung 2.2.9 1. Eine Kette $0 \to M \stackrel{f}{\to} N$ ist genau dann exakt, wenn f injektiv ist: $\mathrm{Ker}f = \mathrm{Im}0 = 0$.

2. Eine Kette $M \stackrel{f}{\to} N \to 0$ ist genau dann exakt, wenn f sujektiv ist: $N = \mathrm{Ker}0 = \mathrm{Im}f$.

Proposition 2.2.10 Sei $f : M \to N$ ein Homomorphismus. Dann gibt es ein exakte Sequenz

$$0 \to \mathrm{Im}f \to M \to N \to \mathrm{Coker}f \to 0.$$

Beweis. Die Abbildung $\mathrm{Im}f \to M$ ist injektiv und die Abbildung $N \to N/\mathrm{Im}f = \mathrm{Coker}f$ ist surjektiv. Wir zeigen, dass $\mathrm{Ker}(N \to \mathrm{Coker}f) = \mathrm{Im}(\mathrm{Im}f \to M) = \mathrm{Im}f$. Es gilt aber $\mathrm{Ker}(N \to \mathrm{Coker}f) = \mathrm{Ker}(N \to N/\mathrm{Im}f) = \mathrm{Im}f$. Daraus folgt die Aussage. ■

2.3 Operationen über Moduln

Lemma 2.3.1 Sei $(M_i)_{i\in I}$ ein Familie von Untermoduln von M. Dann ist $\cap_{i\in I} M_i$ ein Untermodul.

Sei $E \subset M$ eine Teilmenge. Dann gibt es insbesondere ein minimalen Untermodul das E enthält. □

Beweis. Übung. ■

Definition 2.3.2 Sei M ein Modul und $E \subset M$ eine Teilmenge. Der minimale Untermodul von M, das E enthält heißt **der von E erzeugte Untermodul**.

Bemerkung 2.3.3 1. Falls $E = \cup_{i\in I} M_i$, wobei $(M_i)_{i\in I}$ eine Familie von Untermoduln ist, ist der von E erzeugte Untermodul **die Summe**

$$\sum_{i\in I} M_i = \left\{ \sum_{i\in I} x_i \mid x_i \in M_i \text{ und } x_i \neq 0 \text{ nur für endlich viele } i \in I \right\}.$$

2. Falls $E = \{m_1, \cdots, m_n\}$, ist der von E erzeugte Untermodul der Form

$$Am_1 + \cdots + Am_n = \left\{ \sum_{i=1}^{n} a_i m_i \mid a_i \in A \text{ für alle } i \in I \right\}.$$

Proposition 2.3.4 Sei M ein Modul.

1. Seien $P \subset N \subset M$ Untermoduln. Dann gibt es ein Isomorphismus

$$(M/P)/(N/P) \simeq M/N.$$

2. Seien $P, N \subset M$ Untermoduln. Dann gibt es ein Isomorphismus

$$(N+P)/N \simeq P/(N \cap P).$$

Beweis. 1. Seien $\pi_{M/N} : M \to M/N$ und $\pi_{M/P} : M \to M/P$ die kanonische Projektionen. Da $P \subset N = \mathrm{Ker}\pi_{M/N}$, gibt es ein $\bar{\pi}_{M/N} : M/P \to M/N$ so, dass $\pi_{M/N} = \bar{\pi}_{M/N} \circ \pi_{M/P}$. Diese Abbildung ist surjektiv (weil $\pi_{M/N}$ surjektiv ist) und es gilt $\mathrm{Ker}\bar{\pi}_{M/N} = N/P$. Daraus folgt 1.

2. Sei $f : P \to (N+P)/N$ definiert durch $f(p) = [p]$. Dann ist f surjektiv: Sei $[n+p] \in (N+P)/N$, wobei $n \in N$ und $p \in P$. Dann gilt $f(p) = [p] = [n+p]$. Außerdem gilt $\mathrm{Ker} f = N \cap P$. Daraus folgt die Aussage. ■

Definition 2.3.5 Sei M ein A-Modul und $\mathfrak{a} \subset A$ ein Ideal. **Das Produkt** $\mathfrak{a}M$ ist die Teilmenge

$$\mathfrak{a}M = \left\{ \sum_{i=1}^{n} a_i m_i \; | n \geq 1, a_i \in \mathfrak{a}, m_i \in M \right\}.$$

Bemerkung 2.3.6 Das Produkt $\mathfrak{a}M$ ist ein Untermodul von M.

Definition 2.3.7 Sei M ein A-Modul und seien $N, P \subset M$ Untermoduln.

1. **Der Konduktor** $(N : P)$ von P nach N ist die Menge

$$(N : P) = \{a \in A \mid aP \subset N\}.$$

Falls $N = 0$ heißt $(0 : M)$ **der Annihilator von** M und ist $\mathrm{Ann}(M)$ bezeichnet.

2. M heißt **treu** falls $\mathrm{Ann}(M) = 0$.

Bemerkung 2.3.8 1. Der Konduktor (und der Annihilator) ist ein Ideal in A.

2. Der Modul M ist genau dann treu, wenn die zugehörige Abbildung $A \to \mathrm{End}(M)$ injektiv ist: der Kernel von $A \to \mathrm{End}(M)$ ist $\mathrm{Ann}(M)$:

$$\mathrm{Ann}(M) = \mathrm{Ker}(A \to \mathrm{End}(M)).$$

Beispiel 2.3.9 1. Sei $A = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$. Dann gilt $\mathrm{Ann}(M) = n\mathbb{Z}$.

2. Sei $A = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Dann gilt $\mathrm{Ann}(M) = n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(n, m)\mathbb{Z}$.

Lemma 2.3.10 Sei M ein A-Modul und sei $\mathfrak{a} \subset \mathrm{Ann}(M) \subset A$ ein Ideal. Dann ist M ein $A/\mathfrak{a}$-Modul, wobei $[a]m = am$. □

Beweis. Zu überprüfen ist nur, dass diese Multiplikation wohl definiert ist. Sei $a' \in \mathfrak{a}$, dann gilt $(a + a')m = am + a'm = am$ weil $a' \in \mathfrak{a} \subset \mathrm{Ann}(M)$. ■

Korollar 2.3.11 Sei M ein A-Modul. Dann ist M ein treues $A/\mathrm{Ann}(M)$-Modul.

Beispiel 2.3.12 Sei $A = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$. Dann ist M ein treues $\mathbb{Z}/n\mathbb{Z}$-Modul.

2.4 Direkte Summe und Produkt

Definition 2.4.1 Sei A ein Ring.

1. Seien M und N zwei A-Moduln. **Die direkte Summe** $M \oplus N$ **von** M **und** N ist die Menge $M \times N$ mit der Addition $(m, n) + (m', n') = (m + m', n + n')$ und Multiplikation $a(m, n) = (am, an)$.

2. Allgemeiner sei $(M_i)_{i\in I}$ eine Familie von A-Moduln. **Die direkte Summe** $\oplus_{i\in I}M_i$ **der Moduln** $(M_i)_{i\in I}$ ist die Menge

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i \text{ und } m_i \neq 0 \text{ nur für endlich viele } i \in I\}$$

mit der Addition $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$ und mit der Multiplikation $a(m_i)_{i\in I} = (am_i)_{i\in I}$.

3. Sei $(M_i)_{i\in I}$ eine Familie von A-Moduln. **Das Produkt** $\prod_{i\in I} M_i$ **der Moduln** $(M_i)_{i\in I}$ ist die Menge

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i \text{ nur für endlich viele } i \in I\}$$

mit der Addition $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$ und mit der Multiplikation $a(m_i)_{i\in I} = (am_i)_{i\in I}$.

Bemerkung 2.4.2 1. Die direkte Summe und das Produkt sind A-Moduln.

2. Falls I endlich ist sind $\oplus_{i\in I}M_i$ und $\prod_{i\in I} M_i$ isomorph. Im allgemein ist $\oplus_{i\in I}M_i$ ein Untermodul von $\prod_{i\in I} M_i$ und es gilt

$$\bigoplus_{i\in I} M_i \subsetneq \prod_{i\in I} M_i.$$

Beispiel 2.4.3 Die Menge A^n mit der komponentweisen Addition und Multiplikation ist ein A-Modul und ist die direkte Summe (und auch das Produkt) der Familie $(M_i)_{i\in I}$, wobei $I = [1, n]$ und $M_i = A$ für alle $i \in [1, n]$.

Allgemeiner, sei I eine Menge. Die Menge

$$A^{(I)} = \{(x_i)_{i\in I} \mid x_i \in A \text{ und } x_i \neq 0 \text{ nur für endlich viele } i \in I\}$$

ist die direkte Summe der Familie $(M_i)_{i\in I}$, wobei $M_i = A$ für alle $i \in [1, n]$.

Definition 2.4.4 Ein Modul heißt **frei**, falls es eine Menge I gibt so, dass M isomorph zu $A^{(I)}$ ist.

Ein Modul heißt **frei endlich erzeugt**, falls es ein n gibt so, dass M isomorph zu A^n ist.

2.5 Endlich erzeugte Moduln

Definition 2.5.1 Ein Modul M heißt **endlich erzeugt** falls es endliche viele Elemente $m_1, \cdots, m_n \in M$ gibt so, dass $M = Am_1 + \cdots + Am_n$.

Proposition 2.5.2 Ein Modul M ist genau dann endlich erzeugt, wenn es ein sujektiver Modulhomomorphismus $f : A^n \to M$ gibt.

Beweis. Sei x_i der i-te Basis Vektor in A^n. Es gilt $A^n = Ax_1 + \cdots + Ax_n$ und daraus folgt $M = f(A) = Af(x_1) + \cdots + Af(x_n)$. Also ist $(f(x_1), \cdots, f(x_n))$ erzeugend für M.

Umgekehrt, sei $(m_1, \cdots, m_n) \in M$ erzeugend in M. Sei $f : A^n \to M$ definiert durch $f(a_1, \cdots, a_n) = a_1m_1 + \cdots a_nm_n$. Dann ist f ein Modulhomomorphismus und surjektiv. ∎

Beispiel 2.5.3 Der A-Modul A ist immer endlich erzeugt.

Bemerkung 2.5.4 Ein Untermodul eines endlichen erzeugten Moduls ist nicht immer endlich erzeugt.

Zum Beispiel, sei $A = \mathsf{k}[X_1, \cdots, X_n, \cdots]$ ein Polynomring mit unendlichen vielen Variablen. Dann ist $M = A$ endlich erzeugt als A-Modul (1 ist ein Erzeuger). Sei aber $N = (X_1, \cdots, X_n, \cdots)$. Dies ist ein Ideal in A also ein Untermodul von $M = A$. Es ist aber nicht endlich erzeugt: wenn es endlich erzeugt wäre würden wir nur endlich viele Variablen benutzen!

2.6 Exakte Sequenzen II

Proposition 2.6.1 Sei N ein A-Modul.

1. Sei $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ eine exakte sequenz. Dann gibt es eine exakte Sequenz $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$.

2. Sei $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine exakte sequenz. Dann gibt es eine exakte Sequenz $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$.

Beweis. 1. Die Abbildungen $\bar{u}$ und $\bar{v}$ sind wie folgt definiert: $\bar{u}(f) = u \circ f$ und $\bar{v}(f) = v \circ f$.

Sei $f' : N \to M'$ mit $f' \in \mathrm{Ker}\bar{u}$. Es gilt $\bar{u}(f') = u \circ f' = 0$ und da u injektiv ist folgt $f' = 0$.

Sei $f' : N \to M'$. Es gilt $\bar{v}(\bar{u}(f')) = v \circ u \circ f' = 0$ (es gilt $v \circ u = 0$, weil $\mathrm{Im}u \subset \mathrm{Ker}v$).

Sei $f : N \to M$ mit $f \in \mathrm{Ker}\bar{v}$. Es gilt $\bar{v}(f) = v \circ f = 0$. Sei $n \in N$, es gilt also $v(f(n)) = 0$ also $f(n) \in \mathrm{Ker}v = \mathrm{Im}u$. Es gibt also ein eindeutiges Element $m' \in M'$ mit $f(n) = u(m')$. Wir definieren $f' : N \to M'$, $n \mapsto m'$. Man überprüft (Übung), dass f' linear ist. Es gilt auch $\bar{u}(f')(n) = u \circ f'(n) = u(m') = f(n)$. Daraus folgt $f = \bar{u}(f') \in \mathrm{Im}\bar{u}$.

2. Die Abbildungen $\bar{u}$ und $\bar{v}$ sind wie folgt definiert: $\bar{u}(f) = f \circ u$ und $\bar{v}(f) = f \circ v$.

Sei $f'' : M'' \to N$ mit $f'' \in \mathrm{Ker}\bar{v}$. Es gilt $\bar{v}(f'') = f'' \circ v = 0$ und da v surjektiv ist folgt $f'' = 0$.

Sei $f'' : M'' \to N$. Es gilt $\bar{u}(\bar{v}(f'')) = f'' \circ u \circ v = 0$ (es gilt $v \circ u = 0$, weil $\mathrm{Im} u \subset \mathrm{Ker} v$).

Sei $f : M \to N$ mit $f \in \mathrm{Ker}\bar{u}$. Es gilt $f(\mathrm{Im} u) = 0$. Sei $m'' \in M''$. Wir wählen ein $m \in M$ mit $v(m) = m''$. Wir zeigen, dass $f(m)$ von dieser Wahl nicht abhängt. Sei $m_1 \in M$ mit $v(m_1) = m''$. Es gilt $v(m_1) = v(m)$ und also $m_1 - m \in \mathrm{Ker} v = \mathrm{Im} u$. Es folgt $f(m_1 - m) = 0$ und also $f(m_1) = f(m)$. Die Abbildung $f'' : M'' \to N$, $m'' \mapsto f(m)$ is also wohl definiert und linear (Übung). Es gilt auch $\bar{v}(f'')(m) = f'' \circ v(m) = f''(m'') = f(m)$. Daraus folgt $f = \bar{v}(f'') \in \mathrm{Im}\bar{v}$. ■

Proposition 2.6.2 (Schlangenlemma) Seien $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ und $0 \to N' \xrightarrow{a} N \xrightarrow{b} N''$ zwei exakte Sequenzen und seien $f' : M' \to N'$, $f : M \to N$ und $f'' : M'' \to N''$ so, dass das die zwei mittlere Zeile des folgenden Diagramm kommutieren:

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \mathrm{Ker}(f') \arrow[r, dotted, "\bar{u}"] \arrow[d] & \mathrm{Ker}(f) \arrow[r, dotted, "\bar{v}"] \arrow[d] & \mathrm{Ker}(f'') \arrow[d] \arrow[dddll, dotted, rounded corners, "\delta"] & \\
 & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "a"] \arrow[d] & N \arrow[r, "b"] \arrow[d] & N'' \arrow[d] & \\
 & \mathrm{Coker}(f') \arrow[r, dotted, "\bar{a}"] \arrow[d] & \mathrm{Coker}(f) \arrow[r, dotted, "\bar{b}"] \arrow[d] & \mathrm{Coker}(f'') \arrow[d] & \\
 & 0 & 0 & 0. &
\end{tikzcd}
$$

1. Dann gibt es ein exakte sequenz

$$\mathrm{Ker}(f') \xrightarrow{\bar{u}} \mathrm{Ker}(f) \xrightarrow{\bar{v}} \mathrm{Ker}(f'') \xrightarrow{\delta} \mathrm{Coker}(f') \xrightarrow{\bar{a}} \mathrm{Coker}(f) \xrightarrow{\bar{b}} \mathrm{Coker}(f'')$$

wie im Diagramm (mit gepunkteten Pfeilen).

2. $\bar{u} : \mathrm{Ker}(f') \to \mathrm{Ker}(f)$ injektiv $\Leftrightarrow$ u injektiv.

3. $\bar{b} : \mathrm{Coker}(f) \to \mathrm{Coker}(f'')$ surjektiv $\Leftrightarrow$ v surjektiv.

Beweis. 1. Sei $m' \in \mathrm{Ker} f'$. Wir setzen $\bar{u}(m') = u(m')$. Es gilt $f(u(m')) = a(f'(m')) = a(0) = 0$. Es folgt $u(m) \in \mathrm{Ker}(f)$ und $\bar{u} : \mathrm{Ker}(f') \to \mathrm{Ker}(f)$ ist wohl definiert. Analog gilt $v(m) \in \mathrm{Ker}(f'')$ für $m \in \mathrm{Ker}(f)$ und $\bar{v} : \mathrm{Ker}(f) \to \mathrm{Ker}(f'')$ ist durch $\bar{v}(m) = v(m)$ wohl definiert.

Seien $\pi' : N' \to \mathrm{Coker}(f')$, $\pi : N \to \mathrm{Coker}(f)$ und $\pi'' : N'' \to \mathrm{Coker}(f'')$ die kanonische Projektionen. Sei $\pi'(n') \in \mathrm{Coker}(f') = N/\mathrm{Im}(f')$. Wir setzen $\bar{a}(\pi'(n')) = \pi(a(n'))$ und zeigen, dass es nur von $\pi'(n')$ (und nicht von n') abhängt. Sei $n'_1 \in N'$ mit $\pi'(n'_1) = \pi'(n')$. Es gilt $n'_1 - n \in \mathrm{Im}(f')$: es gibt ein $m' \in M'$ mit $n'_1 = n' + f'(m')$. Es folgt $\pi(a(n'_1)) = \pi(a(n')) + \pi(a(f'(m'))) = a(n') + \pi(f(u(m')))$. Da $\pi(\mathrm{Im}(f) = 0$, folgt $\pi(a(n'_1)) = \pi(a(n'))$ und $\bar{a} : \mathrm{Coker}(f') \to \mathrm{Coker}(f)$ ist wohl definiert. Analog defniert man $\bar{b} : \mathrm{Coker}(f) \to \mathrm{Coker}(f'')$.

Wir definieren jetzt δ. Sei $m'' \in \mathrm{Ker}(f'')$. Sei $m \in M$ mit $v(m) = m''$. Dann gilt $b(f(m)) = f''(v(m)) = f''(m'') = 0$ und also $f(m) \in \mathrm{Ker} b = \mathrm{Im} a$. Es gibt also ein eindeutig bestimmtes Element $n' \in N'$ mit $a(n') = f(m)$. Wir setzen $\delta(m'') = \pi'(n')$. Wir zeigen, dass $\delta(m'')$ von der Wahl von m nicht abhängt: sei $m_1 \in M$ mit $v(m_1) = m'' = v(m)$. Es gilt $v(m_1 - m) = 0$ und also $m_1 - m \in \mathrm{Ker} v = \mathrm{Im} u$. Es gibt also ein $m' \in M'$ mit $m_1 = m + u(m')$. Es folgt $f(m_1) = f(m) + f(u(m')) = f(m) + a(f'(m'))$. Es gilt also $f(m_1) = a(n') + a(f'(m')) = a(n' + f'(m'))$ und $n' + f'(m'))$ ist das eindeutige Element, das dieser Gleichung erfüllt (weil a injektiv ist). Es folgt $\pi'(n' + f'(m')) = \pi'(n')$ (weil $\pi'(\mathrm{Im} f') = 0$). Daraus folgt, dass $\delta(m'')$ wohl definiert ist.

Man überprüft (Übung), dass alle Abbildungen $\bar{u}$, $\bar{v}$, $\bar{a}$, $\bar{b}$ und δ linear sind.

Wir zeigen jetzt, dass die Sequenz exakt ist.

In $\mathrm{Ker}(f)$**.** Sei $m' \in \mathrm{Ker}(f')$. Es gilt $\bar{v}(\bar{u}(m')) = v(u(m')) = 0$ da $\mathrm{Im} u = \mathrm{Ker} v$. Sei $m \in \mathrm{Ker}(f)$ mit $\bar{v}(m) = 0$. Es gilt also $v(m) = 0$. Daraus folgt, dass es ein $m' \in M'$ gibt mit $u(m') = m$. Es gilt $a(f'(m')) = f(u(m')) = f(m) = 0$. Da a injektiv ist, folgt $f'(m') = 0$ und $m' \in \mathrm{Ker}(f')$. Es folgt $\bar{u}(m') = u(m') = m$.

In $\mathrm{Ker}(f'')$**.** Sei $m \in \mathrm{Ker}(f)$ und $m'' = \bar{v}(m) = v(m) \in \mathrm{Ker}(f'')$. Es gilt $f(m) = 0$ und also gibt es ein eindeutiges $0 = n' \in N'$ mit $a(n') = f(m) = 0$. Es gilt $\delta(m'') = \pi'(n') = \pi'(0) = 0$.

Sei $m'' \in \mathrm{Ker}(f'')$ mit $\delta(m'') = 0$. Sei also $m \in M$ mit $v(m) = m''$. Es gilt $f(m) \in \mathrm{Ker} b$ und es gibt ein $n' \in N'$ mit $a(n') = f(m)$. Per Definition gilt $\delta(m'') = \pi'(n')$. Es folgt $\pi'(n') = 0$ also $n' \in \mathrm{Im}(f')$. Es gibt also $m' \in M'$ mit $f'(m') = n'$. Es gilt also $f(u(m')) = a(f'(m)) = a(n') = f(m)$. Daraus folgt $m - u(m') = m_1 \in \mathrm{Ker}(f)$. Es gilt also $m = u(m') + m_1$ und $m'' = v(u(m')) + v(m_1) = v(m_1) = \bar{v}(m_1)$.

In $\mathrm{Coker}(f')$**.** Sei $m'' \in \mathrm{Ker}(f'')$. Sei also $m \in M$ mit $v(m) = m''$. Es gilt $f(m) \in \mathrm{Ker} b$ und es gibt ein $n' \in N'$ mit $a(n') = f(m)$. Per Definition gilt $\delta(m'') = \pi'(n')$. Per Definition gilt auch $\bar{a}(\delta(m'')) = \bar{a}(\pi'(n')) = \pi(a(n')) = \pi(f(m)) = 0$.

Sei $\pi'(n') \in \mathrm{Ker}\bar{a}$. Es gilt $0 = \bar{a}(\pi'(n')) = \pi(a(n'))$. Daraus folgt $a(n') \in \mathrm{Im}f$. Sei also $m \in M$ mit $f(m) = a(n')$ und sei $m'' = v(m)$. Es gilt $f''(m'') = f''(v(m)) = b(f(m)) = b(a(n')) = 0$. Es folgt $m'' \in \mathrm{Ker}(f'')$ und per Definition von δ gilt $\delta(m'') = \pi'(n')$.

In $\mathrm{Coker}(f)$**.** Sei $\pi'(n') \in \mathrm{Coker}(f')$, wobei $n' \in N'$. Es gilt $\bar{b}(\bar{a}(\pi'(n'))) = \pi''(b(a(n'))) = \pi''(0) = 0$.

Sei $\pi(n) \in \mathrm{Ker}\bar{b}$, wobei $n \in N$. Es gilt $0 = \bar{b}(\pi(n)) = \pi''(b(n))$. Daraus folgt $b(n) \in \mathrm{Im}f''$. Sei also $m'' \in M''$ mit $f''(m'') = b(n)$. Sei jetzt $m \in M$ mit $v(m) = m''$. Es gilt $b(f(m)) = f''(v(m)) = f''(m'') = b(n)$. Daraus folgt $n - f(m) \in \mathrm{Ker}b = \mathrm{Im}a$. Sei also $n' \in N'$ mit $a(n') = n - f(m)$. Es gilt $\bar{a}(\pi'(n')) = \pi(a(n')) = \pi(n - f(m)) = \pi(n) - \pi(f(m)) = \pi(n)$.

2. ($\Leftarrow$) Sei $m' \in \mathrm{Ker}(f')$ mit $\bar{u}(m') = 0$. Es gilt also $u(m') = 0$ und da u injektiv ist folgt $m' = 0$.

($\Rightarrow$) Sei $m' \in M'$ mit $u(m') = 0$. Es gilt $0 = f(u(m') = a(f'(m'))$ und da a injektiv ist folgt $f'(m') = 0$. Es gilt also $m' \in \mathrm{Ker}f'$ und $\bar{u}(m') = u(m') = 0$. Da $\bar{u}$ injektiv ist folgt $m' = 0$.

3. ($\Leftarrow$) Sei $\pi''(n'') \in \mathrm{Coker}(f'')$, wobei $n'' \in N''$. Sei $n \in N$ mit $b(n) = n''$. Es gilt also $\bar{b}(\pi(n)) = \pi''(b(n)) = \pi''(n'')$.

($\Rightarrow$) Sei $n'' \in N''$. Dann gilt $\pi''(n'') \in \mathrm{Coker}(f'')$. Sei $\pi(n) \in \mathrm{Coker}(f)$, wobei $n \in N$ mit $\bar{b}(\pi(n)) = \pi''(n'')$. Es gilt also $\pi''(b(n)) = \bar{b}(\pi(n)) = \pi''(n'')$. Daraus folgt $b(n) - n'' \in \mathrm{Ker}\pi'' = \mathrm{Im}f''$. Sei $m'' \in M''$ mit $f''(m'') = n'' - b(n)$ und sei $m \in M$ mit $v(m) = m''$. Es folgt $b(n + f(m)) = b(n) + b(f(m)) = b(n) + f''(v(m)) = b(n) + f''(m'') = b(n) + n'' - b(n) = n''$. ∎

Definition 2.6.3 Ein Funktion $\ell : \{A\text{-Moduln}\} \to \mathbb{Z}$ heißt **additive Funktion**, falls gilt $\ell(M) = \ell(M') + \ell(M'')$ für jede kurze exakte Sequenz $0 \to M' \to M \to M'' \to 0$.

Beispiel 2.6.4 Sei $A = \mathsf{k}$ ein Körper. Dann ist $\ell(M) = \dim_{\mathsf{k}} M$ eine Additive Funktion: Für eine kurze exakte Sequenz $0 \to M' \to M \to M'' \to 0$ gilt $M'' \simeq M/M'$ also $\dim M'' = \dim M - \dim M'$.

Bemerkung 2.6.5 Es gilt $\ell(0) = 0$: Wir haben eine kurze exakte Sequenz: $0 \to M' = 0 \to M = 0 \to M'' = 0 \to 0$. Daraus folgt $\ell(0) = ell(0) + \ell(0)$ und also $\ell(0) = 0$.

Lemma 2.6.6 Sei

$$0 \xrightarrow{u_{-1}} M_0 \xrightarrow{u_0} M_1 \xrightarrow{u_1} \cdots \xrightarrow{u_{n-1}} M_n \xrightarrow{u_n} 0$$

eine exakte Sequenz. Dann gibt es für jedes $i \in [0, n-1]$ eine kurze exakte Sequenz

$$0 \to \mathrm{Im}u_{i-1} \to M_i \to \mathrm{Ker}u_{i+1} \to 0.$$

Beweis. Da $\mathrm{Im} u_i = \mathrm{Ker} u_{i+1}$, gibt es ein surjektiver Morphismus $M_i \to \mathrm{Ker} u_{i+1}$ definiert durch $m_i \mapsto u_i(m_i)$. Der Kernel ist $\mathrm{Ker} u_i = \mathrm{Im} u_{i-1}$. ■

Korollar 2.6.7 Sei ℓ eine additive Funktion und sei

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

eine exakte Sequenz. Dann gilt

$$\sum_{i=0}^{n}(-1)^i \ell(M_i) = 0.$$

Beweis. Nach dem obigen Lemma gilt $\ell(M_i) = \ell(\mathrm{Im} u_{i-1}) + \ell(\mathrm{Ker} u_{i+1}) = \ell(\mathrm{Ker} u_i) + \ell(\mathrm{Ker}(u_{i+1})$ für alle $i \in [0, n-1]$. Es folgt

$$\sum_{i=0}^{n}(-1)^i \ell(M_i) = \sum_{i=0}^{n-1}(-1)^i \ell(\mathrm{Ker} u_i) + \ell(\mathrm{Ker}(u_{i+1}) + (-1)^n \ell(M_n) = \ell(\mathrm{Ker} u_0).$$

Da u_0 injektiv ist folgt $\mathrm{Ker} u_0 = 0$ und $\ell(\mathrm{Ker} u_0) = 0$. ■

2.7 Lemma von Nakayama

Proposition 2.7.1 Sei M ein endlich erzeugter Modul, sei $\mathfrak{a}$ ein Ideal und sei $f \in \mathrm{End}(M)$ so, dass $f(M) \subset \mathfrak{a} M$.

Dann gibt es Elemente $a_1, \cdots, a_n \in \mathfrak{a}$ so, dass gilt

$$f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0.$$

Beweis. Seien $m_1, \cdots, m_n$ Erzeuger von M. Es gilt $f(m_i) \in \mathfrak{a} M$ also gibt es Elemente $a_{i,j} \in \mathfrak{a}$ so, dass $f(m_i) = \sum_{j=1}^n a_{i,j} m_j$. Daraus folgt $\sum_{j=1}^n \delta_{i,j} f(m_i) - a_{i,j} m_j = 0$ und also

$$\sum_{j=1}^{n}(\delta_{i,j} f - a_{i,j} \mathrm{Id}_M)(m_j).$$

Wir betrachten jetzt die Matrix $P = (P_{i,j})_{i,j \in [1,n]} \in M_n(\mathrm{End}(M))$ definiert durch

$$P_{i,j} = \delta_{i,j} f - a_{i,j} \mathrm{Id}_M.$$

Sei $\mathrm{Com}(P)$ die Comatrix von P. Es gilt $\mathrm{Com}(P)^T P = \det(P) I_n \in \mathrm{End}(M)$. Sei $(m_1, \cdots, m_n) \in M^n$. Es gilt aber $P(m_1, \cdots, m_n)^T = 0$ Daraus folgt

$$\det(P) I_n (m_1, \cdots, m_n)^T = \mathrm{Com}(P)^T P (m_1, \cdots, m_n)^T = 0$$

und also

$$\det(P) m_i = 0 \text{ für alle } i \in [1, n].$$

Da $m_1, \cdots, m_n$ erzeugend ist, folgt $\det(P) = 0$ als Element in $\mathrm{End}(P)$. Die Matrix P ist aber der Form

$$\begin{pmatrix} f - a_{1,1}\mathrm{Id}_M & -a_{1,2}\mathrm{Id}_M & \cdots & -a_{1,n}\mathrm{Id}_M \\ -a_{2,1}\mathrm{Id}_M & f - a_{2,2}\mathrm{Id}_M & \ddots & -a_{2,n}\mathrm{Id}_M \\ \vdots & \ddots & \ddots & \vdots \\ -a_{n,1}\mathrm{Id}_M & \cdots & -a_{n,n-1}\mathrm{Id}_M & f - a_{n,n}\mathrm{Id}_M \end{pmatrix}$$

und also die Gleichung $\det(P) = 0$ ist der Form $f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0$. ∎

Korollar 2.7.2 Sei M ein endlich erzeugter A-Modul und $\mathfrak{a}$ ein Ideal mit $\mathfrak{a}M = M$. Dann gibt es ein $x \in A$ mit $x \equiv 1 \pmod{\mathfrak{a}}$ und $xM = 0$.

Beweis. Sei $f = \mathrm{Id}_M$ und $x = 1 + a_1 + \cdots + a_n$ mit $a_i \in \mathfrak{a}$ wie in dem obigen Proposition. Es gilt $x \equiv 1 \pmod{\mathfrak{a}}$ und auch $x\mathrm{Id}_M = 0$ also $xM = 0$. ∎

Korollar 2.7.3 (Lemma von Nakayama) Sei M ein endlich erzeugter A-Modul und $\mathfrak{a}$ ein Ideal mit $\mathfrak{a} \subset \mathfrak{R}(A)$ und $\mathfrak{a}M = M$. Dann gilt $M = 0$.

Beweis. Aus dem obigen Korollar, gibt es ein $x \equiv 1 \pmod{\mathfrak{a}}$ mit $xM = 0$. Es gilt also $x = 1 - y$ mit $y \in \mathfrak{R}(A)$. Daraus folgt (cf. Lemma 1.7.6), dass x invertierbar ist. Es folgt also $M = x^{-1}xM = x^{-1}0 = 0$. ∎

Korollar 2.7.4 Sei M ein endlich erzeugter A-Modul und N ein Untermodul von M. Sei $\mathfrak{a} \subset \mathfrak{R}(A)$ ein Ideal mit $M = \mathfrak{a}M + N$. Dann gilt $M = N$.

Beweis. Es gilt $\mathfrak{a}(M/N) = M/N$. Aus dem Lemma von Nakayama folgt $M/N = 0$ also $M = N$. ∎

Korollar 2.7.5 Sei A ein lokal Ring mit maximalem Ideal $\mathfrak{m}$ und sei M ein endlich erzeugter A-Modul. Seien $m_1, \cdots, m_n \in M$ so, dass $[m_1], \cdots, [m_n]$ ein EZS (z.B. eine Basis) von $M/\mathfrak{m}M$ ist.

Dann ist $(m_1, \cdots, m_n)$ erzeugend für M.

Beweis. Sei $N = Am_1 + \cdots + Am_n$. Die Abbildung $N \to M \to M/\mathfrak{m}M$ ist surjektiv. Es folgt $N + \mathfrak{m}M = M$. Da $\mathfrak{m} \subset \mathfrak{R}(A)$, folgt aus dem obigen Lemma, dass $M = N$. ∎

2.8 Tensorprodukt

Wir werden hier die Definition vom Tensorprodukt einführen. Für die Konstruktion kann man wie für Verktäume verfahren. Wir werden also die ganze Konstruktion nicht wiederholen und verweisen auf dem Skript LA II für Beweise.

Definition 2.8.1 Seien M, N und P drei A-Moduln. Eine Abbildung $f : M \times N \to P$ heißt **A-bilinear** falls für alle $a, b \in A$ für alle $m, m' \in M$ und alle $n, n' \in N$ gilt:

- $f(am + bm', n) = af(m, n) + bf(m', n)$
- $f(m, an + bn') = af(m, n) + bf(m, n')$.

Lemma 2.8.2 Sei $f : M \times N \to P$ eine bilineare Abbildung und sei $g : P \to Q$ ein Morphismus. Dann ist $g \circ f$ eine bilineare Abbildung. □

Beweis. Übung. ■

Definition 2.8.3 Ein A-Modul E heißt **Tensorprodukt** von M und N falls gilt:

1. Es gibt eine bilineare Abbildung $\pi_E : M \times N \to E$ und
2. für jede bilineare Abbildung $f : M \times N \to P$, es gibt genau eine lineare Abbildung $L^E_f : E \to P$ mit $L^E_f \circ \pi_E = f$.

Satz 2.8.4 Seien E und F zwei Tensorprodukte für M und N. Dann sind E und F isomorph. □

Beweis. Nach dem ersten Punkt der Definition gibt es bilineare Abbildungen $\pi_E : M \times N \to E$ und $\pi_F : M \times N \to F$. Nach dem zweiten Punkt gibt es eindeutig bestimmte Morphismen $L^E_{\pi_F} : E \to F$ und $L^F_{\pi_E} : F \to E$ mit $\pi_F = L^E_{\pi_F} \circ \pi_E$ und $\pi_E = L^F_{\pi_E} \circ \pi_F$. Wir zeigen, dass $L^F_{\pi_E}$ und $L^E_{\pi_F}$ inverse von einander.

Wir haben eine bilineare Abbildung $f = L^F_{\pi_E} \circ L^E_{\pi_F} \circ \pi_E : M \times N \to E$ und es gilt $f = L^F_{\pi_E} \circ L^E_{\pi_F} \circ \pi_E = L^F_{\pi_E} \circ \pi_F = \pi_E$. Nach dem zweiten Punkt gibt es genau eine Abbildung L^E_f mit $L^E_f \circ \pi_E = f = \pi_E$. Aber wir haben $\mathrm{Id}_E \circ \pi_E = \pi_E$ also $L^E_f = \mathrm{Id}_E$. Wir haben auch $f = L^F_{\pi_E} \circ L^E_{\pi_F} \circ \pi_E$ also gilt $L^E_f = L^F_{\pi_E} \circ L^E_{\pi_F}$ und es folgt $L^F_{\pi_E} \circ L^E_{\pi_F} = \mathrm{Id}_E$.

Analog gilt $L^E_{\pi_F} \circ L^F_{\pi_E} = \mathrm{Id}_F$. Es folgt, dass $L^F_{\pi_E}$ und $L^E_{\pi_F}$ inverse von einander sind. ■

Wir zeigen jetzt, dass es ein Tensorprodukt gibt. Wir betrachten

$$A^{(M\times N)} = \{\varphi : M \times N \to A \mid \varphi(m, n) \neq 0 \text{ nur für endlich viele } (m, n) \in M \times N\}.$$

Für $(m, n) \in M \times N$ gibt es eine Abbildung $\varphi_{(m,n)}$ so, dass

$$\varphi_{(m,n)}(m, n') = \begin{cases} 1 & \text{für } (m', n') = (m, n) \\ 0 & \text{sonst.} \end{cases}$$

Lemma 2.8.5 Das System $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ ist eine Basis von $A^{(M\times N)}$. In anderen Worten ist das System $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ linear unabhängig und für $\varphi \in A^{(M\times N)}$ gilt

$$\varphi = \sum_{(m,n)\in M\times N} \varphi(m,n)\varphi_{(m,n)}.$$

In dieser Summe tauchen nur endlich viele $\varphi(m,n)\varphi_{(m,n)}$ auf, die nicht null sind. □

Beweis. Übung. ■

Die Abbildungen

$$\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)} \text{ und } \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}$$

sind in $A^{(M\times N)}$ enthalten. Sei

$$L = \langle \varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}, \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')} \rangle.$$

Definition 2.8.6 Sei $M \otimes_A N = A^{(M\times N)}/L$ und $p : A^{(M\times N)} \to M \otimes_A N$ die kanonische Projektion. Für $(m,n) \in M \times N$, schreiben wir $m \otimes n = p(\varphi_{(m,n)})$ für das Bild von $\varphi_{(m,n)}$ in $M \otimes_A N$.

Lemma 2.8.7 Es gilt

1. $(am + bm') \otimes n = a(m \otimes n) + b(m' \otimes n)$.
2. $m \otimes (an + bn') = a(m \otimes n) + b(m \otimes n')$. □

Beweis. Übung. ■

Lemma 2.8.8 Das System $(m \otimes n)_{(m,n)\in M\times N}$ ist ein EZS von $M \otimes_A N$. □

Beweis. Es ist das Bild der Basis $(\varphi_{(m,n)})_{(m,n)\in M\times N}$. ■

Satz 2.8.9 $(M \otimes_A N, \pi)$ ist ein Tensorprodukt von M und N. □

Beweis. Sei $\pi : M \times N \to M \otimes_A N$ die Abbildung, die durch $\pi(m,n) = m \otimes n$ definiert wird. Nach dem Lemma, ist π bilinear.

Sei jetzt $f : M \times N \to P$ eine bilineare Abbildung. Wir zeigen, dass es eine lineare Abbildung $L_f : M \otimes_A N \to P$ gibt mit $f = L_f \circ \pi$.

Wir definieren zuerst eine lineare Abbildung $g : A^{(M\times N)} \to P$. Da $(\varphi_{(m,n)})_{(m,n)\in M\times N}$ eine Basis ist, genügt es $g(\varphi_{(m,n)})$ zu definieren. Wir setzen $g(\varphi_{(m,n)}) = f(m,n)$. Wir zeigen, dass $g|_L = 0$. Da $(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}, \varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')})$ ein EZS von L ist, genügt es zu zeigen, dass

$$g(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}) = g(\varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}) = 0.$$

Da g linear und f bilinear ist, gilt

$$\begin{aligned} g(\varphi_{(am+bm',n)} - a\varphi_{(m,n)} - b\varphi_{(m',n)}) &= g(\varphi_{(am+bm',n)}) - ag(\varphi_{(m,n)}) - bg(\varphi_{(m',n)})) \\ &= f(am+bm',n) - af(m,n) - bf(m',n) \\ &= 0. \end{aligned}$$

Analog zeigen wir, dass $g(\varphi_{(m,an+bn')} - a\varphi_{(m,n)} - b\varphi_{(m,n')}) = 0$.

Nach dem Homomorphiesatz, gibt es eine lineare Abbildung $L_f : M \otimes_A N \to P$, so dass das Diagramm

$$\begin{tikzcd} A^{(M\times N)} \arrow[r, "g"] \arrow[d, "p"'] & P \\ A^{(M\times N)}/L = M \otimes_A N \arrow[ur, "L_f"'] & \end{tikzcd}$$

kommutiert. Wir zeigen, dass $L_f \circ \pi = f$. Es gilt

$$L_f \circ \pi(m,n) = L_f(m \otimes n) = L_f(p(\varphi_{(m,n)})) = g(\varphi_{(m,n)}) = f(m,n).$$

Es folgt, dass $M \otimes_A N$ ein Tensorprodukt von M und N ist. ∎

Definition 2.8.10 Sei $M_1, \cdots, M_n$ eine Familie von A-Moduln. Eine Abbildung $f : M_1 \times \cdots \times M_n \to P$ heißt ***n*-linear** falls für alle $i \in [1,n]$ und für alle $m_j \in M_j$ mit $j \neq i$, die Abbildung $f_i : M_i \to P$ definiert durch $f_i(m_i) = f(m_1, \cdots, m_n)$ ist linear.

Definition 2.8.11 Ein A-Modul E heißt **Tensorprodukt** von $M_1, \cdots, M_n$ falls gilt:

1. Es gibt eine n-lineare Abbildung $\pi_E : M_1 \times \cdots \times M_n \to P$ und
2. für jede n-lineare Abbildung $f : M_1 \times \cdots \times M_n \to P$, gibt es genau eine lineare Abbildung $L_f^E : E \to P$ mit $L_f^E \circ \pi_E = f$.

Satz 2.8.12 Sei $M_1, \cdots, M_n$ eine Familie von A-Moduln.

1. Seien E und F zwei Tensorprodukte für $M_1, \cdots, M_n$. Dann sind E und F isomorph.

2. Es gibt ein Tensorprodukt $(M_1 \otimes_A \cdots \otimes_A M_n, \pi)$ für $M_1, \cdots, M_n$. □

Beweis. Übung. ∎

Proposition 2.8.13 Seien M, N, P drei Moduln. Dann gibt es eindeutig bestimme Isomorphismen

1. $M \otimes_A N \simeq N \otimes_A M$

2. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A \otimes_A P \simeq M \otimes_A (N \otimes_A P)$

3. $(M \oplus N) \otimes_A P \simeq M \otimes_A N \oplus N \otimes_A P$

4. $A \otimes_A M \simeq M$

so, dass

1. $m \otimes n \mapsto n \otimes m$

2. $(m \otimes n) \otimes p \mapsto m \otimes n \otimes p \mapsto m \otimes (n \otimes p)$

3. $(m, n) \otimes p \mapsto (m \otimes p, n \otimes p)$

4. $a \otimes m \mapsto am$.

Beweis. Übung. ∎

2.9 Exakte Sequenzen III

Proposition 2.9.1 Seien $f : M \to M'$ und $g : N \to N'$ Morphismen. Dann gibt es ein eindeutiger Morphismus $f \otimes g : M \otimes_A N \to M' \otimes_A N'$ mit $f \otimes g(m \otimes n) = f(m) \otimes g(n)$.

Beweis. Übung. ∎

Proposition 2.9.2 Sei $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine exakte Sequenz und N ein A-Modul. Dann ist

$$M' \otimes_A N \overset{u \otimes \mathrm{Id}_N}{\longrightarrow} M \otimes_A N \overset{v \otimes \mathrm{Id}_N}{\longrightarrow} M'' \otimes_A N \to 0$$

eine exakte Sequenz.

Beweis. Sei $\sum_i m_i'' \otimes n_i \in M'' \otimes_A N$, wobei $m_i'' \in M''$ und $n_i \in N$. Sei $m_i \in M$ mit $v(m_i) = m_i''$. Dann gilt $(v \otimes \mathrm{Id}_N)(\sum_i m_i \otimes n_i) = \sum_i v(m_i) \otimes n_i = \sum_i m_i'' \otimes n_i$ und $v \otimes \mathrm{Id}_N$ ist surjektiv.

Sei $m' \otimes n \in M' \otimes_A N$, wobei $m' \in M'$ und $n \in N$. Dann gilt $(u \otimes \mathrm{Id}_N)(m' \otimes n) = u(m') \otimes n$. Es folgt $(v \otimes \mathrm{Id}_N)(u \otimes \mathrm{Id}_N)(m' \otimes n) = v(u(m')) \otimes n = 0 \otimes n = 0$. Da $m' \otimes n$ eine erzeugende Familie von $M' \otimes_A N$ ist folgt $\mathrm{Im}(u \otimes \mathrm{Id}_N) \subset \mathrm{Ker}(v \otimes \mathrm{Id}_N)$.

Sei $P = \mathrm{Im}(u \otimes \mathrm{Id}_N) \subset M \otimes_A N$. Da $P \subset \mathrm{Ker}(v \otimes \mathrm{Id}_N)$ und da $v \otimes \mathrm{Id}_N$ surjektiv ist, gibt es ein surjektiver Morphismus $f : M \otimes_A N/P \to M'' \otimes_A N$ mit $f([m \otimes n]) = v(m) \otimes n$. Wir zeigen, dass dieser Morphismus ein Isomorphismus ist. Sei $G : M'' \times N \to M \otimes_A N/P$ definiert durch $G(m'', n) = [m \otimes n]$, wobei $m \in M$ so, dass $v(m) = m''$. Diese Abbildung ist *a priori* nicht wohl defniert, weil sie von der Wahl von $m \in M$ mit $v(m) = m''$ abhängt. Sei $m_1 \in M$ mit $v(m_1) = m'' = v(m)$. Es gilt $v(m_1 - m) = 0$ also $m_1 - m \in \mathrm{Ker} v = \mathrm{Im} u$. Es folgt $(m_1 - m) \otimes n \in P$ und $[m_1 \otimes n] = [m \otimes n]$. Die Abbildung G is wohl definiert und man überprüft (Übung), dass diese Abbildung bilinear ist. Es folgt, dass es ein Morhismus $g : M'' \otimes_A N \to M \otimes_A N/P$ gibt mit $g(m'' \otimes n) = [m \otimes n]$, wobei $v(m) = m''$. Wir zeigen, dass g und f Inverse von einander sind. Es gilt $f(g(m'' \otimes n)) = f(m \otimes n) = v(m) \otimes n = m'' \otimes n$. Es gilt auch $g(f([m \otimes n])) = g(v(m) \otimes n) = [m \otimes n]$. ∎

Wir werden einen ganz formalen Beweis von der obigen Proposition geben.

Definition 2.9.3 Sei A ein Ring.

1. **Ein kovarianter Funktor F von A-Moduln** ist eine Zuordnung $M \mapsto F(M)$, wobei M und $F(M)$ beide A-Moduln sind und so, dass

   a. Für $f \in \mathrm{Hom}(M, N)$, gibt es ein $F(f) \in \mathrm{Hom}(F(M), F(N))$,

   b. Für jede Morphismen $f : M \to N$ und $g : N \to P$ gilt $F(g) \circ F(f) = F(g \circ f)$.

   c. Es gilt $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$ für jeder Modul M.

2. **Ein kontravarianter Funktor von A-Moduln** ist eine Zuordnung $M \mapsto F(M)$, wobei M und $F(M)$ beide A-Moduln sind und so, dass

   a. Für $f \in \mathrm{Hom}(M, N)$, gibt es ein $F(f) \in \mathrm{Hom}(F(N), F(M))$,

   b. Für jede Morphismen $f : M \to N$ und $g : N \to P$ gilt $F(f) \circ (g) = F(g \circ f)$.

   c. Für jeder Modul M, gilt $F(\mathrm{Id}_M) = \mathrm{Id}_{F(M)}$.

Definition 2.9.4 1. Sei F ein kovarianter Funktor. Der Funktor F heißt **linksexakt** falls die Kette

$$0 \to F(M') \to F(M) \to F(M'')$$

exakt ist für jede exakte Sequenz $0 \to M' \to M \to M''$.

2. Sei F ein kovarianter Funktor. Der Funktor F heißt **rechtsexakt** falls die Kette

$$F(M') \to F(M) \to F(M'') \to 0$$

exakt ist für jede exakte Sequenz $M' \to M \to M'' \to 0$.

3. Sei F ein kontravarianter Funktor. Der Funktor F heißt **linksexakt** falls die Kette

$$0 \to F(M'') \to F(M) \to F(M')$$

exakt ist für jede exakte Sequenz $M' \to M \to M'' \to 0$.

4. Sei F ein kontravarianter Funktor. Der Funktor F heißt **rechtsexakt** falls die Kette

$$F(M') \to F(M) \to F(M'') \to 0$$

exakt ist für jede exakte Sequenz $0 \to M' \to M \to M''$.

Beispiel 2.9.5 Sei A ein Ring und N ein A-Modul.

1. Die Zuordnung $M \mapsto \mathrm{Hom}(N, M)$ ist ein linksexakter kovarianter Funktor. Dieser Funktor beschreibt man mit $\mathrm{Hom}(N, -)$

2. Die Zuordnung $M \mapsto \mathrm{Hom}(M, N)$ ist ein linksexakter kontravarianter Funktor. Dieser Funktor beschreibt man mit $\mathrm{Hom}(-, N)$

3. Die Zuordnung $M \mapsto M \otimes_A N$ ist ein rechtsexakter kovarianter Funktor. Dieser Funktor beschreibt man mit $- \otimes_A N$

Definition 2.9.6 1. Ein Paar (F, G) von kovarianten Funktoren heißt **adjungiertes Funktorpaar** falls es Isomorphismen

$$\Psi_{M,N} : \mathrm{Hom}(M, G(N)) \simeq \mathrm{Hom}(F(M), N)$$

gibt so, dass für jede Morphismen $f : M \to M'$ und $g : N \to N'$ sind die Diagramme

$$\begin{array}{ccc} \mathrm{Hom}(M', G(N)) & \xrightarrow{\bar{f}} & \mathrm{Hom}(M, G(N)) \\ {\scriptstyle \Psi_{M',N}}\downarrow & & \downarrow{\scriptstyle \Psi_{M,N}} \\ \mathrm{Hom}(F(M'), N) & \xrightarrow{\overline{F(f)}} & \mathrm{Hom}(F(M), N) \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}(M, G(N)) & \xrightarrow{\overline{G(g)}} & \mathrm{Hom}(M, G(N')) \\ {\scriptstyle \Psi_{M,N}}\downarrow & & \downarrow{\scriptstyle \Psi_{M,N'}} \\ \mathrm{Hom}(F(M), N) & \xrightarrow{\bar{g}} & \mathrm{Hom}(F(M), N') \end{array}$$

kommutativ.

Der Funktor F heißt **linsadjungiert** zu G und der Funktor G heißt **rechtsadjungiert** zu F.

2. Analog kann man ein adjungiertes Funktorpaar von kontravarianten Funktoren.

Proposition 2.9.7 Das Funktorpaar $(- \otimes_A N, \mathrm{Hom}(N, -))$ ist adjungiert.

Beweis. Sei $F(M) = M \otimes_A M$ und $G(P) = \mathrm{Hom}(N, P)$. Wir zeigen zuerst, dass $\mathrm{Hom}(F(M), P) \simeq \mathrm{Hom}(M, G(P))$ also, dass es ein Isomorphismus

$$\Phi_{M,P} : \mathrm{Hom}(M \otimes_A N, P) \simeq \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

gibt.

Sei $\varphi : M \otimes_A N \to P$. Dann ist $\varphi' : M \times N \to P$ definiert durch $\varphi'(m, n) = \varphi(m \otimes n)$ bilinear. Wir definieren $\Phi_{M,P}(\varphi) : M \to \mathrm{Hom}(N, P)$ wie folgt: $\Phi_{M,P}(\varphi)(m) : N \to P$ ist die Abbildung $\Phi_{M,P}(\varphi)(m)(n) = \varphi'(m, n) = \varphi(m \otimes n)$. Man überprüft (Übung), dass die Abbildungen $\Phi_{M,P}(\varphi)(m)$, $\Phi_{M,P}(\varphi)$ und $\Phi_{M,N}$ linear sind (die Zuordnung $(\varphi, m, n) \mapsto \varphi'(m, n) = \varphi(m \otimes n)$ ist trilinear).

Sei $\psi : M \to \mathrm{Hom}(N, P)$. Die Abbildung $M \times N \to P$, $(m, n) \mapsto \psi(m)(n)$ ist bilinear. Es gibt also eine eindeutige lineare Abbildung $\Psi_{M,P}(\psi) : M \otimes_A N \to P$ so, dass $\Psi_{M,P}(\psi)(m \otimes n) = \psi(m)(n)$.

Wir zeigen, dass $\Psi_{M,P}$ und $\Phi_{M,P}$ Inverse von einander sind. Es gilt $\Phi_{M,P}(\Psi_{M,P}(\psi))(m)(n) = \Psi_{M,P}(\psi)(m \otimes n) = \psi(m)(n)$. Andersrum gilt $\Psi_{M,P}(\Phi_{M,P}(\varphi))(m \otimes n) = \Phi_{M,P}(\varphi)(m)(n) = \varphi(m \otimes n)$.

Jetzt müssen wir überprüfen, dass die obigen Diagramme kommutativ sind. Sei $f : M \to M'$, es gilt $(\Psi_{M',P} \circ \bar{f})(\psi)(m \otimes n) = \psi(f(m))(n)$. Es gilt auch $(\overline{F(f)} \circ \Psi_{M,P})(\psi)(m \otimes n) = \psi(f(m))(n)$. Analog folgt, dass das zweite Diagramm kommutatiiv ist. ∎

Lemma 2.9.8 Sei A ein Ring.

1. Sei $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ eine Kette von Morphismen. Diese Kette ist genau dann eine exakte sequenz, wenn für alle A-Moduln N, die Kette $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$ ein exakte Sequenz ist.

2. Sei $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine Kette von Morphismen. Diese Kette ist genau dann eine exakte sequenz, wenn für alle A-Moduln N, die Kette $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$. ein exakte Sequenz ist. □

Beweis. Wir haben schon bewiesen, dass falls $0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$ (bzw. $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$) eine exakte Sequenz ist, dann ist die Kette $0 \to \mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M) \xrightarrow{\bar{v}} \mathrm{Hom}(N, M'')$ (bzw. $0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$) auch eine exakte Sequenz für alle N.

1. Sei $N = A$. Dann gilt $\mathrm{Hom}(N, M) = \mathrm{Hom}(A, M) \simeq M$ mit $f \mapsto f(1)$ und $m \mapsto (a \mapsto am)$. Modulo dieser Isomorphismus ist die Abbildung $\mathrm{Hom}(N, M') \xrightarrow{\bar{u}} \mathrm{Hom}(N, M)$ genau die Abbildung $u : M' \to M$. Daraus folgt die Aussage.

2. Sei $N = M''/\mathrm{Im}v$ und $\pi \in \mathrm{Hom}(M'', N)$ die kanonische Projektion. Die Abbildung $\bar{v}(\pi) : M \to N = M''/\mathrm{Im}v$ is gegeben durch $\bar{v}(\pi)(m) = \pi(v(m)) = 0$, weil $\mathrm{Im}v = \mathrm{Ker}\pi$. Es gilt also $\bar{v}(\pi) = 0$ und da $\bar{v}$ injektiv ist, folgt $\pi = 0$. Insbesondere gilt $M''/\mathrm{Im}v = 0$ und $\mathrm{Im}v = M''$. Die Abbildung v ist surjektiv.

Sei $N = M''$ und $\mathrm{Id}_{M''} \in \mathrm{Hom}(M'', N)$. Es gilt $v \circ u = \mathrm{Id}_{M''} \circ v \circ u = \bar{v} \circ \bar{u}(\mathrm{Id}_{M''}) = 0$. Es folgt $\mathrm{Im}u \subset \mathrm{Ker}v$.

Sei $N = M/\mathrm{Im}u$ und $\pi \in \mathrm{Hom}(M, N)$ die kanonische Projektion. Es gilt $\bar{u}(\pi)(m') = \pi \circ u(m') = \pi(u(m')) = 0$, weil $\mathrm{Im}u = \mathrm{Ker}\pi$. Es folgt $\bar{u}(\pi) = 0$ und $\pi \in \mathrm{Ker}\bar{u} = \mathrm{Im}\bar{v}$. Es gibt also ein $f \in \mathrm{Hom}(M'', N)$ mit $\pi = \bar{v}(f) = f \circ v$. Sei jetzt $m \in \mathrm{Ker}v$. Es gilt $\pi(m) = f \circ v(m) = 0$. Es folgt $m \in \mathrm{Im}u$. ■

Proposition 2.9.9 Sei (F, G) ein adjungiertes Funktorpaar von kovarianten (bzw. kontravatianten) Funktoren. Dann gilt

$$F \text{ ist rechtsexakt} \Leftrightarrow G \text{ ist linksexakt.}$$

Beweis. ($\Rightarrow$) Sei $0 \to N' \to N \to N''$ eine exakte Sequenz und sei M ein Modul. Dann ist $0 \to \mathrm{Hom}(F(M), N') \to \mathrm{Hom}(F(M), N) \to \mathrm{Hom}(F(M), N'')$ exakt. Daraus folgt, dass $0 \to \mathrm{Hom}(M, G(N')) \to \mathrm{Hom}(M, G(N)) \to \mathrm{Hom}(M, G(N'))$ exakt ist. Dies ist für alle M wahr also nach dem obigen Lemma gilt, dass $0 \to G(N') \to G(N) \to G(N'')$ exakt ist un G ist linksexakt.

($\Rightarrow$) Sei $M' \to M \to M'' \to 0$ eine exakte Sequenz und sei N ein Modul. Dann ist $0 \to \mathrm{Hom}(M'', G(N)) \to \mathrm{Hom}(M, G(N)) \to \mathrm{Hom}(M', G(N))$ exakt. Daraus folgt, dass $0 \to \mathrm{Hom}(F(M''), N) \to \mathrm{Hom}(F(M), N) \to \mathrm{Hom}(F(M'), N)$ exakt ist. Dies ist für alle N wahr also nach dem obigen Lemma gilt, dass $F(M') \to F(M) \to F(M'') \to 0$ exakt ist un F ist linksexakt.

Analog ist die Aussage für ein adjungiertes Funktorpaar von kontravarianten Funktoren wahr. ∎

Korollar 2.9.10 Der Funktor $- \otimes_A N$ ist rechtsexakt.

Beweis. Es ist ein linksadjungiertes Funktor zum Funktor $\mathrm{Hom}(N, -)$ und der Funktor $\mathrm{Hom}(N, -)$ ist linksexakt. ∎

Definition 2.9.11 Ein Funktor F heißt **exakt** falls F links- und rechtsexakt ist.

Definition 2.9.12 Ein A-Modul M heißt **flach** falls der Funktor $- \otimes_A M$ exakt ist.

Proposition 2.9.13 Sei N ein A-Nodul. Die folgende AUssagen sind äquivalent:

1. N ist flach;
2. Für jede exakte Sequenz $0 \to M' \to M \to M'' \to 0$ ist die Sequenz $0 \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$ exakt.
3. Falls $f : M' \to M$ injektiv ist, ist auch $f \otimes \mathrm{Id}_N : M' \otimes_A N \to M \otimes_A N$ injektiv.

Beweis. (1. $\Leftrightarrow$ 2.) gilt nach der Definition von flach.

(2. $\Leftrightarrow$ 3.) gilt weil das Tensorprodukt rechtsexakt ist. ∎

2.10 Einschränkung und Erweiterung der Skalare

Bemerkung 2.10.1 Sei $f : A \to B$ ein Ringhomomorphismus und N ein B-Modul.

1. Dann ist B ein A-Modul mit Skalarmultiplikation $a \cdot b = f(a)b$.

2. Allgemeiner ist N ein A-Modul mit Skalarmultiplikation $a \cdot n = f(a)n$.

Definition 2.10.2 Sei $f : A \to B$ ein Ringhomomorphismus und N ein B-Modul. Die A-Modulstruktur definiert auf N durch $a \cdot n = f(a)n$ heißt die durch **Einschränkung der Skalare definierte A-Modulstruktur**.

Proposition 2.10.3 Sei $f : A \to B$ ein Ringhomomorphismus und N ein B-Modul. Falls N ein endlich erzeugter B-Modul ist und B ein endlich erzeugter A-Modul ist, dann ist auch N ein endlich erzeugter A-Modul.

Beweis. Sei $n_1, \cdots, n_k$ eine erzeugende Familie von N als B-Modul und $b_1, \cdots, b_r$ eine erzeugende Familie von B als A-Modul. Sei $n \in N$. Dann gibt est $\lambda_1, \cdots, \lambda_k \in B$ mit $n = \sum_i \lambda_i n_i$. Für jedes $i \in [1,k]$ gibt es $(a_{i,j})_{j\in[1,r]}$ mit $\lambda_i = \sum_j a_{i,j} b_j$. Es folgt

$$n = \sum_{i=1}^{k} \sum_{j=1}^{r} a_{i,j} b_j n_i$$

und $(b_j n_i)_{i\in[1,k],j\in[1,r]}$ ist eine erzengende Familie von N als A-Modul. ■

Lemma 2.10.4 Sei $f : A \to B$ ein Ringhomomorphismus und sei M ein A-Modul. Dann ist $B \otimes_A M$ ein B-Modul mit Skalarmultiplikation $b(b' \otimes m) = bb' \otimes m$. □

Beweis. Übung. ■

Definition 2.10.5 Sei $f : A \to B$ ein Ringhomomorphismus und M ein A-Modul. Die B-Modulstruktur definiert auf $B \otimes_A M$ durch $b \cdot (b' \otimes m) = bb' \otimes m$ heißt die durch **Erweiterung der Skalare definierte B-Modulstruktur**.

Proposition 2.10.6 Sei $f : A \to B$ ein Ringhomomorphismus und sei M ein endlich erzeugter A-Modul. Dann ist $B \otimes_A M$ ein endlich erzeugter B-Modul.

Beweis. Sei $m_1, \cdots, m_n$ eine erzeugende Familie für M als A-Modul. Sei $b \otimes m \in B \otimes_A M$. Dann gibt es Elemente $a_1, \cdots, a_n \in A$ mit $m = \sum_i a_i m_i$. Es folgt $\sum_i f(a_i) b(1 \otimes m_i) = \sum_i b \otimes a_i m_i = b \otimes m$ und die Familie $(1 \otimes m_i)_{i\in[1,n]}$ ist eine erzeugende Familie für $B \otimes_A M$ als B-Modul. ■

2.11 Algebren

Definition 2.11.1 Sei A ein Ring.

1. **Eine A-Algebra** B ist ein Ring B mit einem Ringhomomorphismus $f : A \to B$.

2. Seien $f : A \to B$ und $g : A \to C$ zwei A-Algebren. **Ein Morphimus von A-Algebren** von B nach C ist ein Ringhomomorphismus $\varphi : B \to C$ so, dass φ auch A-linear ist.

Bemerkung 2.11.2 Eine A-Algebra B ist ein A-Modul mit Skalarmultiplikation $a \cdot b = f(a)b$. Außerdem gelten die übliche Rechnungsregeln:

1. $a(b + b') = ab + ab'$
2. $(a + a')b = ab + a'b$
3. $(aa')b = a(a'b)$
4. $a(bb') = (ab)b' = b(ab')$

5. $a1 = a$ und $1b = b$.

Lemma 2.11.3 Seien $f : A \to B$ und $g : A \to C$ zwei A-Algebren.

1. Dann ist $B \otimes_A C$ eine A-Algebra mit Multiplikation $(b \otimes c)(b' \otimes c') = bb' \otimes cc'$ und Abbildung $A \to B \otimes_A C$, $a \mapsto f(a) \otimes g(a)$.

2. Die Abbildungen $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ und $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$ sind Ringhomomorphismen. $\square$

Beweis. 1. Die Abbildung $B \times C \times B \times C \to B \otimes_A C$ definiert durch $(b, c, b', c') \mapsto bb' \otimes cc'$ ist 4-linear. Es gibt also eine lineare Abbildung $B \otimes_A C \otimes_A B \otimes_A C \to B \otimes C$ definiert durch $b \otimes c \otimes b' \otimes c' \mapsto bb' \otimes cc'$. Daraus folgt, dass dir Abbildung $B \otimes_A C \times B \otimes_A C \to B \otimes_A C$ defniert durch $(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'$ bilinear ist. Man überprüft, dass diese Verknüpfung associativ ist une es gilt $(b \otimes c)(1 \otimes 1) = (1 \otimes 1)(b \otimes c) = b \otimes c$, also ist $B \otimes_A C$ ein Ring. Die Abbildung $A \to B \otimes_A C$ definiert durch $a \mapsto f(a) \otimes g(a)$ ist aber ein Ringhomomorphismus und also ist $B \otimes_A C$ eine A-Algebra.

2. Übung. $\blacksquare$

Bemerkung 2.11.4 Der Ringhomomorphismus $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ ist nicht immer ein Morphismus von A-Algebren.

Zum Beispiel, seien $A = B = C = \mathsf{k}$, wobei k ein Körper ist. Seien $f = g = \mathrm{Id}_{\mathsf{k}}$. Die Abbildung $\varphi : B \to B \otimes_A C$ ist gegeben durch $x \mapsto x \otimes 1 = x(1 \otimes 1)$. Die Abbildung $f \otimes g : A \to B \otimes_A C$ ist gegeben durch $(f \otimes g)(x) = x \otimes x = x(1 \otimes x) = x^2(1 \otimes 1)$. Es gilt also $\varphi(f(x)y) = \varphi(xy) = xy(1 \otimes 1)$ und $(f \otimes g)(x) \cdot \varphi(y) = (x \otimes x)(y \otimes 1) = xy \otimes x = x^2y(1 \otimes 1) \neq xy(1 \otimes 1) = \varphi(f(x)y)$.

Beispiel 2.11.5 Sei B ein Ring und $A = \mathbb{Z}$. Dann ist die Abbildung $f : A \to B$ definiert durch

$$f(n) = nb = \underbrace{1 + \cdots + 1}_{n-\text{Mal}}$$

ein Ringhomomorphismus. Also ist jeder Ring eine $\mathbb{Z}$-Algebra.

Definition 2.11.6 Sei A ein Ring.

1. Ein Ringhomomorphismus $f : A \to B$ heißt **endlich** falls B ein endlich erzeugter A-Modul ist. Man sagt, dass B eine **endliche Algebra** über A ist.

2. Ein Ringhomomorphismus $f : A \to B$ heißt **von endlicher Typ** falls es elemente $x_1, \cdots, x_r \in B$ gibt so, dass jedes Element aus B als Polynom in $x_1, \cdots, x_r$ mit Koeffizieten in $f(A)$ darstellbar ist. Man sagt, dass B eine **endlich erzeugte Algebra** über A ist.

3. Der Ring A heißt **endlich erzeugt**, falls A eine endlich erzeugte $\mathbb{Z}$-Algebra ist.

Bemerkung 2.11.7 Eine A-Algebra B ist genau dann endlich erzeugt, wenn es ein surjektiver Ringhomomorphismus $A[T_1, \cdots, T_r] \to B$ gibt.

3 Lokalisierung

In diesem Kapitel, werden wir die Konstruktion vom Quotientkörper verallgemeinern.

3.1 Ringe

Definition 3.1.1 Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt **multiplikativ** falls $1 \in S$ und es gilt: $(x, y \in S \Rightarrow xy \in S)$.

Beispiel 3.1.2 1. Sei A ein Ring. Dann ist $S = A^\times$ multiplikativ.

2. Sei A ein Ring. Dann ist $S = A \setminus \{\text{Nullteiler}\}$ multiplikativ.

3. Sei A ein Ring und $\mathfrak{p}$ ein Primideal. Dann ist $A \setminus \mathfrak{p}$ multiplikativ.

4. Sei A ein Ring und $f \in A$. Dann ist $\{f^n \mid n \geq 0\}$ multiplikativ.

5. Sei $\mathfrak{a} \subset A$ ein Ideal und sei $1 + \mathfrak{a} = \{1 + x \in A \mid x \in \mathfrak{a}\}$. Dann ist S multiplikativ.

6. Sei A ein Integritätsring. Dann ist $S = A \setminus \{0\}$ multiplikativ.

Definition 3.1.3 Sei A ein Ring und $S \subset A$ eine multiplikative Menge. Wir definieren eine Äquivalenzrelation $\equiv$ die auf $A \times S$ durch

$$(a, s) \equiv (a', s') \Leftrightarrow \exists t \in S,\ t(as' - a's) = 0.$$

Lemma 3.1.4 Die Relation $\equiv$ ist eine Äquivelenzrelation. □

Beweis. Übung. ■

Definition 3.1.5 Wir Schreiben a/s oder $\frac{a}{s}$ für die Äquivalenzklasse von (a, s) für $\equiv$. Wir schreiben $S^{-1}A$ für die Menge aller Äquivalenzklassen.

Beispiel 3.1.6 Sei $A = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$. Dann gilt $S^{-1}A = \mathbb{Q}$.

Proposition 3.1.7 Sei A ein Ring und $S \subset A$ multiplkativ.

1. Dann ist $S^{-1}A$ ein Ring mit $0 = 0/1$, $1 = 1/1$ und

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \text{ und } \frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}.$$

2. Es gilt $s/1 \in (S^{-1}A)^\times$.

3. Die Abbildung $\lambda : A \to S^{-1}A$, $a \mapsto a/1$ ist ein Ringhomomorphismus.

Beweis. 1. Man überprüft (Übung), dass diese Definitionen von der Wahl von Repräsentanten nicht abhängt. Man üperfrüft auch (Übung, Schulwissen), dass diese Verknüpfungen eine Ringstruktur definieren.

2. Es gilt $(s/1)(1/s) = 1/1$.

3. Es gilt $\lambda(1) = 1/1$, $\lambda(a + b) = a + b/1 = a/1 + b/1 = \lambda(a) + \lambda(b)$ und $\lambda(ab) = ab/1 = (a/1)(b/1)$. ∎

Bemerkung 3.1.8 Der Ringhomomorphismus $A \to S^{-1}A$ ist nicht immer injektiv. Zum Beispiel, falls $0 \in S$ gilt $0(a \cdot 1 - s \cdot 0) = 0$ und also $a/s \equiv 0/1$. Es folgt

$$\frac{a}{s} = \frac{0}{1} \text{ für alle } \frac{a}{s} \in S^{-1}A \text{ und es folgt } S^{-1}A = 0$$

und die Abbildung $\lambda : A \to S^{-1}A$ ist die Nullabbildung.

Der Ring $S^{-1}A$ kann auch dank einer universellen Eigenschaft definiert werden.

Proposition 3.1.9 Sei $f : A \to B$ ein Ringhomomorphismus mit $f(s) \in B^\times$ für alle $s \in S$. Dann gibt es ein eindeutiger Ringhomomorphismus $g : S^{-1}A \to B$ mit $f = g \circ \lambda$.

Beweis. Wir definieren $g : S^{-1}A \to B$ durch $g(a/s) = f(a)f(s)^{-1}$. Wir überprüfen, dass dies wohl definiert ist. Sei $a'/s' \in S^{-1}A$ mit $a'/s' = a/s$. Es gibt also ein $t \in S$ mit $t(as' - a's) = 0$. Daraus folgt $f(t)(f(a)f(s') - f(a')f(s)) = 0$; Da $f(t)$ invertierbar ist, folgt $f(a)f(s') - f(a')f(s) = 0$ und also $f(a)f(s)^{-1} = f(a')f(s')^{-1}$. Die Abbildung g ist wohl definiert und man überprüft, dass diese Abbildung ein Ringhomomorphismus ist (Übung).

Wir zeigen, dass $f = g \circ \lambda$. Sei $a/s \in S^{-1}A$. Es gilt $g(\lambda(a) = g(a/1) = f(a)f(1)^{-1} = f(a)$.

Wir zeigen jetzt, dass g eindeutig bestimmt ist. Sei $h : S^{-1}A \to B$ ein weiterer Ringhomomorphismus mit $f = h \circ \lambda$. Es gilt $h(a/s) = h(a/1)h(1/s) = h(a/1)h((s/1)^{-1}) = h(a/1)h(s/1)^{-1}$. Es folgt $h(a/s) = h(\lambda(a))h(\lambda(s))^{-1} = f(a)f(s)^{-1} = g(a/s)$. ∎

Lemma 3.1.10 Sei $S \subset A$ multiplikativ.

1. Für $s \in S$ gilt $\lambda(s) \in S^{-1}A^{\times}$.

2. Sei $a \in A$. Es gilt $(\lambda(a) = 0 \Leftrightarrow$ es gibt ein $s \in S$ mit $sa = 0)$.

3. Jedes Element aus $S^{-1}A$ ist der Form $\lambda(a)\lambda(s)^{-1}$, wobei $a \in A$ und $s \in S$. □

Beweis. 1. Es gilt $\lambda(s) = s/1 \in S^{-1}A^{\times}$.

2. Es gilt $\lambda(a) = 0 \Leftrightarrow a/1 = 0 \Leftrightarrow$ (es gibt ein $s \in S$ mit $sa = s(a - 0) = 0$).

3. Es gilt $a/s = \lambda(a)\lambda(s)^{-1}$. ∎

Diese Eigenschaften bestimmen der Ringhomomorphismus $\lambda : A \to S^{-1}A$.

Proposition 3.1.11 Sei $f : A \to B$ ein Ringhomomorphismus mit

1. Für $s \in S$ gilt $f(s) \in B^{\times}$.
2. Für $a \in A$ gilt, $(\lambda(a) = 0 \Rightarrow$ es gibt ein $s \in S$ mit $sa = 0)$.
3. Jedes Element aus B ist der Form $f(a)f(s)^{-1}$, wobei $a \in A$ und $s \in S$.

Dann gibt es ein Isomorphismus $g : S^{-1}A \to B$ mit $f = g \circ \lambda$.

Beweis. Wir setzen $g(a/s) = f(a)f(s)^{-1}$. Nach Proposition 3.1.9 ist dies wohl definiert, ein Ringhomomorphismus und es gilt $f = g \circ \lambda$. Wir zeigen, dass g ein Isomorphismus ist.

Sei $a/s \in \operatorname{Ker} g$. Es gilt $g(a/s) = f(a)f(s)^{-1} = 0$ und da $f(s)$ invertierbar ist folgt $f(a) = 0$. Es folgt, dass es ein $t \in S$ gibt mit $ta = 0$ und also $t(a \cdots 1 - s \cdot 0) = 0$. Es folgt $a/s = 0$ und g ist injektiv.

Sei $b \in B$. Es gibt ein $a \in A$ und ein $s \in S$ mit $b = f(a)f(s)^{-1}$. Es folgt $b = g(a/1)g(s/1)^{-1} = g(a/1)g(1/s) = g(a/s)$ und g ist surjektiv. ∎

Beispiel 3.1.12 1. Es gilt: $S^{-1}A = 0 \Leftrightarrow 0 \in S \Leftrightarrow S$ enthält nilpotente Elemente.

2. Sei A ein Integritätsring und $S = A \setminus \{0\}$. Dann gilt $S^{-1}A = \operatorname{Frac}(A)$.

3. Sei $S = A \setminus \mathfrak{p}$, wobei $\mathfrak{p}$ ein Primideal ist. In diesem Fall schreibt man $S^{-1}A = A_{\mathfrak{p}}$.

4. Sei $A = \mathbb{Z}$ und $\mathfrak{p} = (p)$, wobei p eine Primzahl ist. Dann gilt

$$A_{\mathfrak{p}} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ mit } \operatorname{ggT}(b, p) = 1 \right\}.$$

5. Sei $f \in A$ und $S = \{f^n \mid n \geq 0\}$. In diesem Fall schreibt man $S^{-1}A = A[f^{-1}]$.

6. Sei $A = \mathbb{Z}$ und $f = p$, wobei p eine Primzahl ist. Dann gilt

$$A_p = \left\{ \frac{a}{p^n} \in \mathbb{Q} \mid a \in \mathbb{Z},\ n \geq 0 \right\}.$$

3.2 Moduln

Definition 3.2.1 Sei A ein Ring, $S \subset A$ eine multiplikative Menge und M ein A-Modul. Wir definieren eine Äquivalenzrelation $\equiv$ die auf $M \times S$ durch

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S,\ t(s'm - sm') = 0.$$

Lemma 3.2.2 Die Relation $\equiv$ ist eine Äquivelenzrelation. □

Beweis. Übung. ■

Definition 3.2.3 Wir Schreiben m/s oder $\frac{m}{s}$ für die Äquivalenzklasse von (m, s) für $\equiv$. Wir schreiben $S^{-1}M$ für die Menge aller Äquivalenzklassen.

Lemma 3.2.4 Die Menge $S^{-1}M$ ist ein $S^{-1}A$-Modul mit Addition und Skalarmultiplikation gegeben durch

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'} \text{ und } \frac{a}{s}\frac{m}{t} = \frac{am}{st}.$$

Insbesondere ist $S^{-1}M$ ein A-Modul mit Skalarmultiplikation $a\dfrac{m}{s} = \dfrac{am}{s}$. □

Beweis. Übung. ■

Beispiel 3.2.5 1. Falls $S = A \setminus \mathfrak{p}$ mit $\mathfrak{p}$ ein Primideal, schreibt man $S^{-1}M = M_{\mathfrak{p}}$.

2. Falls $S = \{f^n \mid n \geq 0\}$, wobei $f \in A$, schreibt man $S^{-1}M = M_f$.

Bemerkung 3.2.6 Es gilt ($m/s = 0 \Leftrightarrow$ es gibt ein $t \in S$ mit $tm = 0$).

Lemma 3.2.7 Die Zuordnung $M \mapsto S^{-1}M$ ist ein Funktor: Für jeder Morphismus von A-Moduln $f : M \to N$, gibt es ein zugehöriger Morphismus von $S^{-1}A$-Moduln $S^{-1}f : S^{-1}M \to S^{-1}N$ definiert durch

$$S^{-1}f\left(\frac{m}{s}\right) = \frac{f(m)}{s}.$$

Beweis. Wir überprüfen, dass dies wohl definiert ist. Sei $m'/s' = m/s$. Es gibt also ein $t \in S$ mit $t(ms' - m's) = 0$. Es folgt $0 = f(t(s'm - sm')) = t(s'f(m) - sf(m'))$ und also

$$\frac{f(m)}{s} = \frac{f(m')}{s'}.$$

Man überprüft (Übung), dass f ein Morphismus ist. ■

Definition 3.2.8 Der Funktor $M \mapsto S^{-1}M$ heißt **Lokalisierung** oder **Lokalisierungsfunktor**.

Proposition 3.2.9 Der Lokalisierungsfunktor ist exakt.

Beweis. Sei $M' \xrightarrow{u} M \xrightarrow{v} M''$ eine exakte Sequenz. Dann gibt es eine Kette $S^{-1}M' \xrightarrow{S^{-1}u} S^{-1}M \xrightarrow{S^{-1}v} S^{-1}M''$, wobei $S^{-1}u(m'/s) = u(m)/s$ und $v(m/s) = v(m)/s$ für $m' \in M'$, $m \in M$ und $s \in S$. Es folgt $S^{-1}v(S^{-1}u(m'/s)) = S^{-1}v(u(m')/s) = v(u(m'))/s = 0/s = 0$. Daraus folgt $\mathrm{Im}S^{-1}u \subset \mathrm{Ker}S^{-1}v$.

Sei $m/s \in \mathrm{Ker}S^{-1}v$. Es gilt $v(m)/s = 0$ also gibt es ein $t \in S$ mit $tv(m) = 0$. Es folgt $v(tm) = 0$ und $tm \in \mathrm{Ker}v = \mathrm{Im}u$. Sei also $m' \in M'$ mit $u(m') = tm$. Es gilt $u(m'/ts) = u(m')/ts = tm/ts = m/s$ also $m/s \in \mathrm{Im}u$. ∎

Korollar 3.2.10 Sei $N \subset M$ ein Untermodul. Dann ist $S^{-1}N \to S^{-1}M$ injektiv und also kann $S^{-1}N$ als Untermodul von $S^{-1}M$ betrachtet werden:

$$S^{-1}N = \left\{\frac{n}{s} \mid n \in N \text{ und } s \in S\right\} \subset S^{-1}M = \left\{\frac{m}{s} \mid m \in M \text{ und } s \in S\right\}.$$

Korollar 3.2.11 Seien $N, P \subset M$ Untermoduln. Dann gilt

1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$;
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;
3. $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ als $S^{-1}A$-Moduln.

Beweis. 1. Übung.

2. Falls $x \in S^{-1}N \cap S^{-1}P$, dann gilt $x = /s = p/s'$, wobei $n \in N$, $p \in P$ und $s, s' \in S$. Daraus folgt, dass es ein $t \in S$ gibt mit $t(s'n - sp) = 0$. Also gilt $N \ni ts'n = tsp \in P$ und $ts'x = tsx \in N \cap P$. Es folgt $x = tsx/ts \in S^{-1}(N \cap P)$. Die Rückenthaltung ist klar.

3. Die Kette $0 \to N \to M \to M/N \to 0$ ist exakt. Es folgt, dass $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ exakt ist. Daraus folgt die Aussage. ∎

Proposition 3.2.12 Es gilt $S^{-1}M \simeq M \otimes_A S^{-1}A$ als $S^{-1}A$-Moduln. Die Isomorphismen sind gegeben durch $m/s \mapsto m \otimes 1/s$ und $m \otimes a/s \mapsto am/s$.

Beweis. Die Abbildung $M \times S^{-1}A \to S^{-1}M$ definiert durch $(m, a/s) \mapsto am/s$ ist A-bilinear. Daraus folgt, dass die Abbildung $M \otimes_A S^{-1}A \to S^{-1}M$, $m \otimes a/s \mapsto am/s$ wohl definiert ist. Man überprüft, dass diese Abbildung $S^{-1}A$-linear ist.

Die Abbildung $m/s \mapsto m \otimes 1/s$ ist wohl definiert: Falls $m'/s' = m/s$, gibt es ein $t \in S$ mit $t(s'm - sm') = 0$. Es folgt $m' \otimes 1/s' = m' \otimes ts/s'ts = tsm' \otimes 1/s'ts = tsm \otimes 1/s'ts = m \otimes ts/s'ts = m \otimes 1/s$. Diese Abbildung ist $S^{-1}A$-linear (Übung).

Diese Abbildung sind inverse von einander: Es gilt $m/s \mapsto m \otimes 1/s \mapsto m/s$ und $m \otimes a/s \mapsto am/s \mapsto am \otimes 1/s = m \otimes a/s$. ∎

Korollar 3.2.13 Der A-Modul $S^{-1}A$ ist flach.

Beweis. Sei $M' \to M \to M''$ eine exakte Sequenz. Dann ist $S^{-1}M' \to S^{-1}M \to S^{-1}M''$ exakt und also ist $M' \otimes_A S^{-1}A \to M \otimes_A S^{-1}A \to M'' \otimes_A S^{-1}A$ exakt. ∎

Proposition 3.2.14 Seien M und N zwei A-Moduln. Dann gibt es einen eindeutigen $S^{-1}A$-Modulisomorphismus $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ mit $f((m/s) \otimes (n/s')) = (m \otimes n)/ss'$.

Beweis. Es gilt $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}N = M \otimes_A N \otimes_A S^{-1}A = S^{-1}(M \otimes_A N)$ (siehe auch Lemma 3.3.7). Das Inverse von f ist gegeben durch $(m \otimes n)/s \mapsto m/s \otimes n = m \otimes n/s$. ∎

Korollar 3.2.15 Für $\mathfrak{p}$ ein Prim ideal gilt

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \simeq (M \otimes_A N)_{\mathfrak{p}}$$

als $A_{\mathfrak{p}}$-Moduln.

3.3 Lokale vs globale Eingenschaften

Definition 3.3.1 Eine Eigenschaft E von einem Ring A (bzw. von einem Modul M) heißt **lokal** falls gilt

$$\text{E gilt für } A \text{ (bzw. } M) \;\Leftrightarrow\; \text{E gilt für } A_{\mathfrak{p}} \text{ (bzw. } M_{\mathfrak{p}}) \text{ für alle Primideale } \mathfrak{p} \subset A.$$

Proposition 3.3.2 Sei A ein Ring und M ein A-Modul. Die folgende Ausagen sind äquivalent:

1. $M = 0$;
2. $M_{\mathfrak{p}} = 0$ für alle $\mathfrak{p} \subset A$ Primideal;
3. $M_{\mathfrak{m}} = 0$ für alle $\mathfrak{m} \subset A$ maximal Ideal.

Insbesondere ist die Eigenschaft (M ist der Nullmodul) lokal.

Beweis. $(1 \Rightarrow 2)$ und $(2 \Rightarrow 3)$ klar.

$(3 \Rightarrow 1)$ Angenommen $M \neq 0$. Sei $m \in M$ mit $m \neq 0$. Sei $\mathfrak{a} = \mathrm{Ann}(m) = \{a \in A \mid am = 0\}$. Es gilt $1m = m \neq 0$ also $\mathfrak{a} \subsetneq A$. Sei $\mathfrak{m}$ ein maximales Ideal mit $\mathfrak{a} \subset \mathfrak{m}$. Es gilt $m/1 \in M_{\mathfrak{m}} = 0$. Also gibt es ein $s \in A \setminus \mathfrak{m}$ mit $sm = 0$ und also $s \in \mathrm{Ann}(m) = \mathfrak{a} \subset \mathfrak{m}$. Ein Widerspruch. ∎

Korollar 3.3.3 Sei A ein Ring und $f : M \to N$ ein A-Modulhomomorphismus. Die folgende Ausagen sind äquivalent:

1. f ist injektiv (bzw. surjektiv);

2. $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ ist injektiv (bzw. surjektiv) für alle $\mathfrak{p} \subset A$ Primideal;

3. $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ ist injektiv (bzw. surjektiv) für alle $\mathfrak{m} \subset A$ maximal Ideal.

Insbesondere sind die Eigenschaft (f ist injektiv), (f ist surjektiv) und (f ist bijektiv) lokal.

Beweis. Die Abbildung f ist genau dann injektiv (bzw. surjektiv), wenn $\mathrm{Ker} f = 0$ (bzw $\mathrm{Coker} f = 0$). Die Kette

$$0 \to \mathrm{Ker} f \to M \xrightarrow{f_{\mathfrak{p}}} N \to \mathrm{Coker} f \to 0$$

ist exakt und da die Lokalisierung exakt ist, ist die Kette

$$0 \to (\mathrm{Ker} f)_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \to (\mathrm{Coker} f)_{\mathfrak{p}} \to 0$$

exakt für alle $\mathfrak{p} \subset A$ Primideal. Daraus folgt $\mathrm{Ker}(f_{\mathfrak{p}}) = (\mathrm{Ker} f)_{\mathfrak{p}}$ und $\mathrm{Coker}(f_{\mathfrak{p}}) = (\mathrm{Coker} f)_{\mathfrak{p}}$. Aus der obigen Proposition sind also ($\mathrm{Ker} f = 0$), ($\mathrm{Ker} f_{\mathfrak{p}} = 0$ für alle $\mathfrak{p}$ Primideal) und ($\mathrm{Ker} f_{\mathfrak{m}} = 0$ für alle $\mathfrak{m}$ maximal) äquivalent. Die Aussage für injektive Abbildungen folgt daraus. Analog gilt die Aussage für f surjektiv. ∎

Korollar 3.3.4 Sei $n \in \mathbb{N}$ und sei $(x_1, \cdots, x_n)$ ein EZS von A^n. Dann ist $(x_1, \cdots, x_n)$ eine Basis *i.e.* die Abbildung $f : A^n \to A^n$ definiert durch $f(a_1, \cdots, a_n) = a_1 x_1 + \cdots + a_n x_n$ ist ein Isomorphismus.

Beweis. Die Abbildung f ist surjektiv. Sei $N = \mathrm{Ker} f$. Wir haben eine exakte Sequenz $0 \to N \to A^n \xrightarrow{f} A^n \to 0$. Wir Zeigen $N = 0$.

Es genügt zu zeigen, dass $N_{\mathfrak{m}} = 0$ für alle $\mathfrak{m}$ maximale Ideale. Durch Ersetzen von A mit $A_{\mathfrak{m}}$ und N mit $N_{\mathfrak{m}}$ können wir annehmen, dass A lokal ist mit maximalem Ideal $\mathfrak{m}$. Der Quotient $\mathsf{k} = A/\mathfrak{m}$ ist ein Körper.

Lemma 3.3.5 Die Kette $0 \to \mathsf{k} \otimes_A N \to \mathsf{k} \otimes_A A^n \to \mathsf{k} \otimes_A A^n \to 0$ ist exakt. □

Beweis. Wir haben eine exakte Sequenz $\mathfrak{m} \otimes_A N \to A \otimes_A N \to \mathsf{k} \otimes_A N \to 0$. Da A flach ist (als A-Modul haben wir eine exakte Sequenz $0 \to \mathfrak{m} \otimes_A A^n \to A \otimes_A A^n \to \mathsf{k} \otimes_A A^n \to 0$.

Daraus folgt, dass wir ein kommutatives Diagramm mit exakten Zeilen haben:

$$
\begin{tikzcd}
 & & 0 \arrow[d] & P \arrow[d] \arrow[dddll, dotted, rounded corners, "\delta"] & \\
 & \mathfrak{m} \otimes_A N \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & \mathsf{k} \otimes_A N \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{m} \otimes_A A^n \arrow[r] \arrow[d] & A^n \arrow[r] \arrow[d] & \mathsf{k} \otimes_A A^n \arrow[r] \arrow[d] & 0 \\
 & \mathfrak{m} \otimes_A A^n & A^n & \mathsf{k} \otimes_A A^n &
\end{tikzcd}
$$

Der Cokernel der Abbildung $N \to A^n$ (bzw. $\mathsf{k} \otimes_A N \to \mathsf{k} \otimes_A A^n$) ist A^n (bzw. $\mathsf{k} \otimes_A A^n$) und die Abbildung zum Cokernel ist f (bzw $\mathrm{Id}_{\mathsf{k}} \otimes f$). Der Kernel der Abbildung $N \to A^n$ ist 0 (diese Abbildung ist injektiv). Sei P der Kernel der Abbildung $\mathsf{k} \otimes_A N \to \mathsf{k} \otimes_A A^n$. Aus dem Schlangenlemma, folgt, dass die Kette $0 \to P \to \mathfrak{m} \otimes_A A^n \to A^n \to \mathsf{k} \otimes_a A^n$ exakt ist. Die Abbildung $\mathfrak{m} \otimes_A A^n \to A^n$ ist aber injektiv (weil A^n flach ist). Daraus folgt $P = 0$. ■

Es gilt aber $\mathsf{k} \otimes_A A^n = (\mathsf{k} \otimes_A A)^n = \mathsf{k}^n$ und also ist die letzte Abbildung ein Isomorphismus von k-Vektorräume. Es folgt $0 = \mathsf{k} \otimes_A N = A/\mathfrak{m} \otimes_A N = N/\mathfrak{m}N$.

Der Untermodul N ist aber endlich erzeugt (cf. Übung 2 Übungsblatt 3) und nach Nakayamaslemma folgt $N = 0$. ■

Proposition 3.3.6 Sei A ein Ring und M ein A-Modul. Die folgende Ausagen sind äquivalent:

1. M ist ein flacher A-Modul;
2. $M_{\mathfrak{p}}$ ist ein flacher $A_{\mathfrak{p}}$-Modul für alle $\mathfrak{p} \subset A$ Primideal;
3. M ist ein flacher $A_{\mathfrak{m}}$-Modul für alle $\mathfrak{m} \subset A$ maximal Ideal.

Insbesondere ist die Eigenschaft (M ist flach) lokal.

Beweis. ($1 \Rightarrow 2$) Wir zeigen ein Lemma.

Lemma 3.3.7 Sei $f : A \to B$ ein Ring homomorphismus und M ein A-Modul.

1. Sei N ein B-Modul. Dann gilt $N \otimes_B (B \otimes_A M) \simeq N \otimes_A M$ als B-Moduln.

2. Falls M ein flacher A-Modul ist, ist $B \otimes_A M$ ein flacher B-Modul. □

Beweis. 1. Die A-Modulstruktur von N ist gegeben durch $a \cdot n = f(a)n$. Die B-Modulstruktur von $N \otimes_B M$ ist gegeben durch $b \cdot (n \otimes m) = bn \otimes m$.

Sei $\varphi : N \times B \times M \to N \otimes_A M$ definiert durch $\varphi(n, b, m) = bn \otimes m$. Diese Abbildung ist A-bilinear in den zwei letzen Variablen und also faktorisiert durch $N \times (B \otimes_A M)$. Die induzierte Abbildung ist gegeben durch $(n, b \otimes m) \mapsto bn \otimes m$ und diese Abbildung ist B-bilinear. Es folgt, dass es ein B-linear Abbildung $\bar{\varphi} : N \otimes_B (B \otimes_A M) \to N \otimes_A M$, $n \otimes (b \otimes m) \mapsto bn \otimes m$ gibt. Analog gibt es eine A-bilineare Abbildung $\psi : N \times M \to N \otimes_B (B \otimes_A M)$ definiert durch $\psi(n, m) = n \otimes (1 \otimes m)$. Daraus folgt, dass es eine A-lineare Abbildung $\bar{\psi} : N \otimes_A M \to N \otimes_B (B \otimes_A M)$, $n \otimes m \mapsto n \otimes (1 \otimes m)$ gibt. Diese Abbildung ist auch B-linear: $\bar{\psi}(b \cdot (n \otimes m)) = \bar{\psi}(bn \otimes m) = bn \otimes (1 \otimes m) = b\bar{\psi}(n \otimes m)$.

Wir zeigen, dass $\bar{\varphi}$ und $\bar{\psi}$ inverse von einander sind. Es gilt $\bar{\varphi}(\bar{\psi}(n \otimes m)) = \bar{\varphi}(n \otimes (1 \otimes m)) = n \otimes m$ und $\bar{\psi}(\bar{\varphi}(n \otimes (b \otimes m))) = \bar{\psi}(bn \otimes m) = bn \otimes (1 \otimes m) = n \otimes (b \cdot (1 \otimes m)) = n \otimes (b \otimes m)$.

2. Sei $N' \to N \to N''$ eine exakte Sequenz von B-Modul. Dann ist die Kette $N' \otimes_B (A \otimes_A M) \to N \otimes_B (A \otimes_A M) \to N'' \otimes_B (A \otimes_A M)$ genau die Kette $N' \otimes_A M \to N \otimes_A M \to N'' \otimes_A M$. Da M flach ist ist diese Kette eine exakte Sequenz. ∎

Es gilt $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \otimes_A M$. Aus dem obigen Lemma folgt, dass $M\mathfrak{p}$ auch flach ist, weil M flach ist.

und $(2 \Rightarrow 3)$ klar.

$(3 \Rightarrow 1)$ Da das Tensorprodukt ein rechtsexakter Funktor ist, genügt es zu zeigen, dass für $0 \to N' \xrightarrow{f} N$ eine exakte Sequenz die Kette $0 \to M \otimes_A N' \xrightarrow{\mathrm{Id}_M \otimes f} M \otimes_A N$ exakt ist. Für alle maximale Ideal $\mathfrak{m} \subset A$ sind aber die folgende Sequenzen exakt (die erste weil lokalisierung exakt ist und die zweite weil $M_{\mathfrak{m}}$ flach ist):

$$0 \to N'_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \text{ und } 0 \to M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N'_{\mathfrak{m}} \xrightarrow{\mathrm{Id}_{M_{\mathfrak{m}}} \otimes f_{\mathfrak{m}}} M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}.$$

Man überprüft aber leicht, dass $(\mathrm{Id}_M \otimes f)_{\mathfrak{m}} = \mathrm{Id}_{M_{\mathfrak{m}}} \otimes f_{\mathfrak{m}}$. Es folgt, dass $(\mathrm{Id}_M \otimes f)_{\mathfrak{m}}$ injektiv für alle maximale Ideale $\mathfrak{m} \subset A$ ist. Daraus folgt, dass $\mathrm{Id}_M \otimes f$ injektiv ist. ∎

3.4 Ideale und lokalisierung

Proposition 3.4.1 Sei A ein Ring und $S \subset A$ eine multiplikative Menge.

1. Sei $\mathfrak{a}$ ein Ideal in A. Dann gilt $(\lambda(\mathfrak{a})) = S^{-1}\mathfrak{a}$.

2. Sei $\mathfrak{b}$ ein Ideal in $S^{-1}A$. Dann ist $\mathfrak{b}$ der Form $S^{-1}\mathfrak{a}$ für $\mathfrak{a}$ ein Ideal in A. Genauer gilt $\mathfrak{b} = S^{-1}(\lambda^{-1}(\mathfrak{b}))$.

3. Sei $\mathfrak{a}$ ein Ideal in A. Es gilt $\lambda^{-1}(S^{-1}\mathfrak{a}) = \lambda^{-1}((\lambda(\mathfrak{a}))) = \cup_{s \in S}(\mathfrak{a} : s)$.

4. Ein Ideal $\mathfrak{a}$ in A ist genau dann der Form $\lambda^{-1}(\mathfrak{b})$ für ein Ideal $\mathfrak{b} \subset S^{-1}A$, wenn kein Element von S zu einem Nullteiler in $A/\mathfrak{a}$ abgebildet ist. In dem Fall gilt $\mathfrak{a} = \lambda^{-1}(S^{-1}(\mathfrak{a}))$.

5. Es gibt eine Bijektion $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ mit Inverse $\mathfrak{q} \mapsto \lambda^{-1}(\mathfrak{q})$ zwischen die Mengen

$$\{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ Primideal mit } \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \{\mathfrak{q} \subset S^{-1}A \mid \mathfrak{q} \text{ Primideal}\}.$$

6. Seien $\mathfrak{a}$ und $\mathfrak{a}'$ Ideale in A. Dann gilt

a. $S^{-1}(\mathfrak{a} + \mathfrak{a}') = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{a}'$

b. $S^{-1}(\mathfrak{a}\mathfrak{a}') = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{a}')$

c. $S^{-1}(\mathfrak{a} \cap \mathfrak{a}') = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{a}'$

d. $\sqrt{S^{-1}\mathfrak{a}} = S^{-1}\sqrt{\mathfrak{a}}$.

Beweis. 1. Es gilt $\lambda(\mathfrak{a}) \subset S^{-1}\mathfrak{a}$ und also $(\lambda(\mathfrak{a})) \subset S^{-1}\mathfrak{a}$. Sei $a/s \in S^{-1}\mathfrak{a}$ mit $a \in \mathfrak{a}$ und $s \in S$. Dann gilt $a/s = 1/s \cdot a/1 = 1/s \cdot \lambda(a) \in (\lambda(\mathfrak{a}))$.

2. Es gilt $S^{-1}(\lambda^{-1}(\mathfrak{b})) = ((\lambda(\lambda^{-1}(\mathfrak{b})))) = ((\mathfrak{b})) = \mathfrak{b}$.

3. Sei $a \in \lambda^{-1}(S^{-1}(\mathfrak{a}))$. Es gilt $\lambda(a) = a'/s$, wobei $a' \in \mathfrak{a}$ und $s \in S$. Es folgt, dass es ein $t \in S$ gibt mit $t(as - a') = 0$ also $tsa = ta' \in \mathfrak{a}$. Es folgt $a \in (\mathfrak{a}, ts)$. Umgekehrt, sei $a \in (\mathfrak{a} : s)$. Dann gilt $sa = a' \in \mathfrak{a}$. Es folgt $\lambda(a) = a/1 = sa/s = a'/s \in S^{-1}\mathfrak{a}$.

4. Sei $\mathfrak{a}$ der Form $\mathfrak{a} = \lambda^{-1}(\mathfrak{b})$. Es gilt also $S^{-1}(\mathfrak{a}) = \mathfrak{b}$. Sei $s \in S$ und $\bar{s}$ die Klasse von s in $A/\mathfrak{a}$. Angenommen $\bar{s}$ sei Nullteiler. Dann gibt es ein $a \in A$ mit $\bar{a} \neq 0$ und $\bar{a}\bar{s} = 0$. Es folgt $sa \in \mathfrak{a}$ und also $a \in (\mathfrak{a} : s)$. Aus 3. folgt $a \in \lambda^{-1}(S^{-1}(\mathfrak{a})) = \lambda^{-1}(\mathfrak{b}) = \mathfrak{a}$ *i.e.* $\bar{a} = 0$ ein Widerspruch.

Umgekehrt,angenommen, dass kein Element von S zu einem Nullteiler in $A/\mathfrak{a}$ abgebildet ist. Wir zeigen $\mathfrak{a}\lambda^{-1}(S^{-1}(\mathfrak{a}))$. Es gilt immer $\mathfrak{a} \subset \lambda^{-1}(S^{-1}(\mathfrak{a}))$. Sei also $a \in \lambda^{-1}(S^{-1}(\mathfrak{a}))$. Nach 3. gibt es ein $s \in S$ mit $sa \in \mathfrak{a}$. Es folgt $\bar{s}\bar{a} = 0$ in $A/\mathfrak{a}$. Da $\bar{a}$ kein Nullteiler ist folgt $\bar{a} = 0$ und $a \in \mathfrak{a}$.

5. Sei $\mathfrak{p}$ prim mit $\mathfrak{p} \cap S = \emptyset$. Wir zeigen zuerst, dass $S^{-1}\mathfrak{p}$ prim ist. Seien a/s und a'/s' in $S^{-1}A$ mit $(a/s)(a'/s') \in S^{-1}\mathfrak{p}$. Es gibt also ein $b \in \mathfrak{p}$ und $t \in S$ mit $aa'/ss' = b/t$. Es folgt, dass es ein $t \in S$ gibt mit $t'(aa't - bss') = 0$. Es folgt $tt'aa' = tbss' \in \mathfrak{p}$. Da $t, t' \in S$ gilt $t, t' \notin \mathfrak{p}$. Es folgt $a \in \mathfrak{p}$ oder $a' \in \mathfrak{p}$ und also $a/s \in S^{-1}\mathfrak{p}$ oder $a'/s' \in S^{-1}\mathfrak{p}$.

Für $\mathfrak{p}$ prim mit $\mathfrak{p} \cap S = \emptyset$ gilt $0 \neq \bar{s} \in A/\mathfrak{p}$ und da $A/\mathfrak{p}$ Nullteilerfrei ist folgt, dass $\bar{s}$ kein Nullteiler ist. Es folgt also $\mathfrak{p} = \lambda^{-1}(S^{-1}(\mathfrak{p}))$.

Umgekehrt gilt nach 2: $S^{-1}(\lambda^{-1}(\mathfrak{q})) = \mathfrak{q}$.

6. Übung. ∎

Proposition 3.4.2 Es gilt $\mathfrak{n}(S^{-1}A) = S^{-1}\mathfrak{n}(A)$.

Beweis. Sei $a \in \mathfrak{n}(A)$ mit $a^n = 0$. Dann gilt $(a/s)^n = a^n/s^n = 0$ und $a/s \in \mathfrak{n}(S^{-1}A)$ für alle $s \in S$. Umgekehrt, sei $a/s \in \mathfrak{n}(S^{-1}A)$. Es gilt $a^n/s^n = (a/s)^n = 0$. Es gilt also ein $t \in S$ mit $ta^n = 0$ und also $(ta)^n = 0$. Es folgt $a/s = ta/ts \in S^{-1}\mathfrak{n}(A)$. ∎

Proposition 3.4.3 Sei $\mathfrak{p}$ ein Primideal. Es gibt eine Bijektion $\mathfrak{q} \mapsto \mathfrak{q}_\mathfrak{p}$ und $\mathfrak{r} \mapsto \lambda^{-1}(\mathfrak{r})$ zwischen

$$\{\mathfrak{q} \subset A \mid \mathfrak{q} \subset \mathfrak{p} \text{ Primideal}\} \longleftrightarrow \{\mathfrak{r} \subset A_\mathfrak{p} \mid \mathfrak{r} \text{ Primideal}\}.$$

Beweis. Sei $S = A \setminus \mathfrak{p}$. Es gilt $\mathfrak{q} \cap S = \emptyset \Leftrightarrow \mathfrak{q} \subset \mathfrak{p}$. Die Aussage folgt aus Proposition 3.4.1.5. ∎

Proposition 3.4.4 Sei M ein endlich erzeugter A-Modul. Dann gilt $S^{-1}\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$.

Beweis. Sei $a \in \mathrm{Ann}(M)$, sei $s \in S$ und sei $m/t \in S^{-1}M$, wobei $m \in M$ und $t \in S$. Es gilt $am = 0$. Daraus folgt $a/s \cdot m/t = am/st = 0$ und $a/s \in \mathrm{Ann}(S^{-1}M)$.

Umgekehrt, sei $a/s \in \mathrm{Ann}(S^{-1}M)$ und seien $m_1, \cdots, m_n$ eine erzeugende Familie für M. Für jedes $i \in [1, n]$ gilt $am_i/s = a/s \cdot m_i/1 = 0$. Es gibt also ein $t_i \in S$ mit $tam_i = 0$ für alle $i \in [1, m]$. Also gilt $t_1 \cdots t_n am_i = 0$ für alle $i \in [1, n]$. Es folgt $t_1 \cdots t_n a \in \mathrm{Ann}(M)$. Also gilt $a/s = t_1 \cdots t_n a/t_1 \cdots t_n s \in S^{-1}\mathrm{Ann}(M)$. ∎

Korollar 3.4.5 Seien $N, P \subset M$ Untermoduln mit P endlich erzeugt. Dann gilt $S^{-1}(N : P) = (S^{-1}N, S^{-1}P)$.

Beweis. Wir haben ein Morphismus $P \to P + N/N$ definiert durch $p \mapsto [p]$. Dieser Morphismus ist surjektiv: es gilt $[p + n] = [p]$ also ist $P + N/N$ endlich erzeugt. Wir zeigen $(N : P) = \mathrm{Ann}(P+N/N)$. Sei $a \in (N : P)$. Dann gilt $a(P+N) = aP+N \subset N$ also $a(P + N/N) = 0$ und $a \in \mathrm{Ann}(P + N/N)$. Umgekehrt, sei $a \in \mathrm{Ann}(P + N/N)$. Dann gilt $a(P + N) \subset N$ und also $aP \subset N$ und $a \in (N : P)$. Es folgt

$$S^{-1}(N : P) = S^{-1}\mathrm{Ann}(P+N/N) = \mathrm{Ann}(S^{-1}(P+N/N)) = \mathrm{Ann}(S^{-1}P+S^{-1}N/S^{-1}N) = (S^{-1}N : S$$

Proposition 3.4.6 Sei $f : A \to B$ ein Ringhomomorphismus und sei $\mathfrak{p} \subset A$ ein Primideal.

Es gibt genau dann ein Primideal $\mathfrak{q} \subset B$ mit $f^{-1}(\mathfrak{q}) = \mathfrak{p}$, wenn $\mathfrak{p} = f^{-1}((f(\mathfrak{p})))$.

Beweis. Sei $\mathfrak{q} \subset B$ prim mit $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Es gilt $f(\mathfrak{p}) \subset \mathfrak{q}$ und $f^{-1}(f(\mathfrak{p})) \subset f^{-1}(\mathfrak{q}) = \mathfrak{p}$. Es folgt $\mathfrak{p} = f^{-1}((f(\mathfrak{p})))$.

Umgekehrt, sei $\mathfrak{p}$ prim mit $\mathfrak{p} = f^{-1}((f(\mathfrak{p})))$. Sei $S = f(A \setminus \mathfrak{p}) \subset B$. Dann ist S multiplikativ: für $x, x' \in S$ gibt es $a, a' \in A \setminus \mathfrak{p}$ mit $f(a) = x$ und $f(a') = x'$. Es gilt aber $aa' \in A \setminus \mathfrak{p}$ also $xx' = f(a)f(a') = f(aa') \in S$. Es gilt $(f(\mathfrak{p})) \cap S = \emptyset$: falls

$x \in (f(\mathfrak{p})) \cap S$ gibt es ein $a \in A \setminus \mathfrak{p}$ mit $f(a) = x$ also $a \in f^{-1}((f(\mathfrak{p}))) = \mathfrak{p}$. Ein Widerspruch. Es folgt, dass $S^{-1}(f(\mathfrak{p}))$ ein echtes Ideal in $S^{-1}B$ ist: wenn $S^{-1}(f(\mathfrak{p})) = B$ gilt $1 \in S^{-1}(f(\mathfrak{p}))$ also gibt es ein $s \in S$ mit $s = s \cdot 1 \in (f(\mathfrak{p}))$. Ein Widerspruch. Sei jetzt $\mathfrak{m}$ ein maximales Ideal in $S^{-1}B$ mit $(f(\mathfrak{p})) \subset \mathfrak{m}$ und sei $\lambda : B \to S^{-1}B$. Wir setzen $\mathfrak{q} = \lambda^{-1}(\mathfrak{m})$. Dann ist $\mathfrak{q}$ ein Primideal in B.

Wir zeigen $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. Sei $a \in \mathfrak{p}$. Es gilt $\lambda(f(a)) \in \lambda(f(\mathfrak{p})) \subset S^{-1}(f(\mathfrak{p})) \subset \mathfrak{m}$. Es folgt $f(a) \in \mathfrak{q}$. Umgekehrt, sei $a \in f^{-1}(\mathfrak{q})$. Falls $a \notin \mathfrak{p}$, gilt $f(a) \in S$. Es gilt aber $f(a) \in \mathfrak{q}$ und also $S \cap \mathfrak{q} \not\emptyset$. Daraus folgt $\lambda\mathfrak{q} = S^{-1}\mathfrak{q} = S^{-1}B$. Ein Widerspruch. ∎

4 Ganze Elemente

4.1 Ganze Elemente

Definition 4.1.1 Sei B ein Ring und A ein Unterring von B. Ein Element $x \in B$ heißt **ganz** falls es ein Polynom $P \in A[X]$ mit Leitkoeffizient 1 so, dass $P(x) = 0$:

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

wobei $a_i \in A$ für alle $i \in [1, n]$.

Bemerkung 4.1.2 Elemente aus A sind ganz über A.

Beispiel 4.1.3 Sei $A = \mathbb{Z}$ und $B = \mathbb{Q}$. Ein Element $x \in \mathbb{Q}$ is genau dann ganz, wenn $x \in \mathbb{Z}$ (Übung).

Proposition 4.1.4 Sei $A \subset B$ ein Unterring und $x \in B$. Die folgende Aussagen sind äquivalent:

1. x in ganz über A;
2. $A[x]$ ist ein endlich erzeuger A-Modul;
3. $A[x] \subset C$, wobei C ein Unterring von B und auch ein endlich erzeugter A-modul ist.
4. Es gibt ein treuer $A[x]$-Modul M, der als A-Modul endlich erzeugt ist.

Beweis. (1. $\Rightarrow$ 2.) Es gilt $x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r)$ für alle $r \geq 0$. Daraus folgt, dass $A[x]$ von der Familie $(1, \cdots, x^{n-1})$ erzugt ist.

(2. $\Rightarrow$ 3.) Setze $C = A[x]$.

(3. $\Rightarrow$ 4.) Setze $M = C$. Sei $P \in A[x]$ mit $P \in \mathrm{Ann}(M)$ *i.e* $P \cdot M = 0$. Da $1 \in C = M$, folgt $P = P \cdot 1 = 0$ also $\mathrm{Ann}(M) = 0$ und M ist treu.

(4. $\Rightarrow$ 1.) Sei M ein treuer $A[x]$-Modul so, dass M auch endlich erzeugt als A-Modul ist. Sei $f : M \to M$ die A-lineare Abbildung definiert durch $f(m) = xm$. Sei $\mathfrak{a} = A$. Nach Proposition 2.7.1 gibt es Elemente $a_1, \cdots, a_n \in \mathfrak{a} = A$ so, dass $f^n + a_1 f^{n-1} + \cdots + a_n \mathrm{Id}_M = 0$. Für alle $m \in M$ gilt also $(x^n + a_1 x^{n-1} + \cdots + a_n)m = 0$. Da M treu ist folgt $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. ∎

Korollar 4.1.5 Seien $x_1, \cdots, x_n$ ganze Elemente über A. Dann ist $A[x_1, \cdots, x_n]$ endlich erzeugt als A-Modul.

Beweis. Aus der Proposition ist $A[x_1]$ endlich erzeugt. Per Induktion ist $A[x_1, \cdots, x_{n-1}]$ endlich erzeugt über A. Aber x_n ist ganz über A also auch über $A[x_1, \cdots, x_{n-1}]$. Der Modul $A[x_1, \cdots, x_n]$ ist endlich erzeugt über $A[x_1, \cdots, x_{n-1}]$ und $A[x_1, \cdots, x_{n-1}]$ ist endlich erzeugt über A. Die Aussage folgt aus Proposition 2.10.3. ■

Korollar 4.1.6 Sei $A \subset B$ ein Unterring. Die Menge aller genzen Elemente in B ist ein Unterring von B, der A enthält.

Beweis. Wir wissen schon, dass alle Elemente in A ganz sind. Seien $x, y \in B$ ganz über A. Dann ist $A[x, y]$ endlich erzeugt über A und enthält $A[x + y]$ und $A[xy]$. Daraus folgt, dass $x + y$ und xy ganz über A sind. ■

Definition 4.1.7 Sei $A \subset B$ ein Unterring.

1. Der Ring aller Elemente die ganz über A sind heißt **ganzer Abschluss** von A in B.

2. Wenn A der ganze Abschluss von A in B ist heißt A **ganz abgechlossen** in B.

3. Wenn B der ganze Abschluss von A in B ist (*i.e.* alle Elemente aus B sind ganz über A) heißt B **ganz über** A.

Definition 4.1.8 Sei $f : A \to B$ ein Ringhomomorphismus also B ist eine A-Algebra. Die A-Algebra heißt B **ganz** falls B ganz über $f(A)$ ist.

Lemma 4.1.9 Sei $f : A \to B$ eine A-Algebra. Es gilt

$$B \text{ ist als } A\text{-Modul endlich erzeugt} \Leftrightarrow B \text{ ist eine endlich erzeugte } A\text{-Algebra und ist ganz über } A.$$

Beweis. ($\Rightarrow$) Klar aus was wir bewiesen haben.

($\Leftarrow$) Sei $(x_1, \cdots, x_n)$ eine erzeugende Familie von B als A-Algebra. Es gilt also $f(A)[x_1, \cdots, x_n] = B$. Da B ganz über A ist sind alle x_i ganz und dieser Modul ist endlich erzeugt. ■

Proposition 4.1.10 Seien $A \subset B \subset C$ Unterringe. Falls B ganz über A ist und C ganz über B ist, ist C ganz über A.

Beweis. Sei $x \in C$. Es gibt Elemente $b_1, \cdots, b_n \in B$ mit $x^n + b_1 x^{n-1} + \cdots + b_n = 0$. Sei $B' = A[b_1, \cdots, b_n]$. Da alle b_i ganz über A sind, ist B' endlich erzeugt als A-Modul. Aber x ist ganz über B' also ist $B'[x]$ endlich erzeugt über B'. Es folgt, dass $B'[x]$ endlich erzeugt über A ist. Da dieser Modul $A[x]$ enthält ist x ganz über A. ■

Korollar 4.1.11 Sei $A \subset B$ ein Unterring und C der ganze Abschluss von A in B. Dann ist C ganz abgeschlossen in B.

Beweis. Sei $\overline{C}$ der ganze Abschluss von C in B. Dann ist $\overline{C}$ ganz über A und also $\overline{C} \subset C$. Da $C \subset \overline{C}$ folgt die Aussage. ■

Proposition 4.1.12 Sei $A \subset B$ mit B ganz über A.

1. Sei $\mathfrak{b} \subset B$ ein Ideal und $\mathfrak{a} = A \cap \mathfrak{b}$. Dann ist $B/\mathfrak{b}$ ganz über $A/\mathfrak{a}$.

2. Sei $S \subset A$ multiplikativ. Dann ist $S^{-1}B$ ganz über $S^{-1}A$.

Beweis. 1. Sei $x \in B$. Dann gibt es $a_1, \cdots, a_n \in A$ mit $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Es folgt $[x]^n + [a_1][x]^{n-1} + \cdots + [a_n] = 0$.

2. Sei $x/s \in S^{-1}B$ mit $x \in B$ und $s \in S$. Dann gibt es $a_1, \cdots, a_n \in A$ mit $x^n + a_1x^{n-1} + \cdots + x_n = 0$. Es folgt $(x/s)^n + (a_1/s)(x/s)^{n-1} + \cdots + (a_n/s^n) = 0$. ■

4.2 Going-up Theorem

Proposition 4.2.1 Sei $A \subset B$ zwei Integritätsringe mit B ganz über A. Dann gilt

$$A \text{ ist ein Körper} \Leftrightarrow B \text{ ist ein Körper.}$$

Beweis. ($\Rightarrow$) Sei $b \in B$ mit $b \neq 0$. Dann gibt es Elemente $a_1, \cdots, a_n \in A$ mit $b^n + a_1b^{n-1} + \cdots + a_n = 0$. Sei n minimal so, dass es eine solche Gleichung gibt. Falls $a_n = 0$ gilt $b(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1}) = 0$ also $b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1} = 0$ ein Widerspruch zur minimalität. Es gibt also ein $a_n^{-1} \in A$ und $-b(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1})a_n^{-1} = 1$. Daraus folgt, dass b invertierbar in B ist.

($\Leftarrow$) Sei $a \in A$ mit $a \neq 0$. Dann gibt es ein $a^{-1} \in B$. Wir zeigen $a^{-1} \in A$. Da B ganz über A ist gibt es Elemente $a_1, \cdots, a_n \in A$ mit $a^{-n} + a_1a^{-n+1} + \cdots + a_n = 0$. Nach Multiplikation mit a^{n-1} folgt $a^{-1} + a_1 + \cdots + a_na^{n-1}$ und also $a^{-1} = -(a_1 + \cdots + a_na^{n-1}) \in A$. ■

Korollar 4.2.2 Seien $A \subset B$ Ringe mit B ganz über A. Sei $\mathfrak{q}$ ein Primideal in B und sei $\mathfrak{p} = A \cap \mathfrak{q}$. Dann gilt

$$\mathfrak{q} \text{ maximal} \Leftrightarrow \mathfrak{p} \text{ maximal.}$$

Beweis. Der Ring $B/\mathfrak{q}$ is ganz über $A/\mathfrak{p}$ und beide sind Integritätsringe. Die Aussage folgt aus der obigen Proposition. ■

Korollar 4.2.3 Seien $A \subset B$ Ringe mit B ganz über A. Seien $\mathfrak{q}$ und $\mathfrak{q}'$ Primideale mit $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Falls gilt $\mathfrak{q} \subset \mathfrak{q}'$ folgt $\mathfrak{q} = \mathfrak{q}'$.

Beweis. Sei $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Der Ring $B_\mathfrak{p}$ ist ganz über $A_\mathfrak{p}$. Sei $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$ das von $\mathfrak{p}$ erzeugte Ideal in $A_\mathfrak{p}$. Dann ist $\mathfrak{m}$ maximal in $A_\mathfrak{p}$. Seien $\mathfrak{n}$ und $\mathfrak{n}'$ die von $\mathfrak{q}$ und $\mathfrak{q}'$ erzeugte Ideale in $B_\mathfrak{p}$. Es gilt $\mathfrak{n} \subset \mathfrak{n}'$ und $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{m} = \mathfrak{n}' \cap A_\mathfrak{p}$. Da $\mathfrak{m}$ maximal ist sind auch $\mathfrak{n}$ und $\mathfrak{n}'$ maximal. Es folgt $\mathfrak{n} = \mathfrak{n}'$. Es gibt aber eine Bijektion zwischen Primideale in B die $S = A \setminus \mathfrak{p}$ nicht treffen und Primideale in $S^{-1}B = B_\mathfrak{p}$. Da $A \cap \mathfrak{q} = \mathfrak{p} = A \cap \mathfrak{q}'$, gilt $\mathfrak{q} \cap S = \emptyset = \mathfrak{q}' \cap S$. Es folgt $\mathfrak{q} = \mathfrak{q}'$. ■

Satz 4.2.4 Seien $A \subset B$ Ringe mit B ganz über A. Sei $\mathfrak{p}$ ein Primideal in A. Dann gibt es ein Primideal $\mathfrak{q}$ in B mit $\mathfrak{q} = A \cap \mathfrak{q}$. □

Beweis. Wir haben ein kommutatives Diagramm

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle \lambda_A}\downarrow & & \downarrow{\scriptstyle \lambda_B} \\ A_\mathfrak{p} & \longrightarrow & B_\mathfrak{p}. \end{array}$$

Sei $\mathfrak{n}$ maximal in $B_\mathfrak{p}$. Dann ist $\mathfrak{m} = \mathfrak{n} \cap A_\mathfrak{p}$ maximal in $A_\mathfrak{p}$. Dieser Ring ist aber lokal mit maximalem Ideal $\mathfrak{p}A_\mathfrak{p}$. Es folgt $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$. Sei $\mathfrak{q} = \lambda_B^{-1}(\mathfrak{n})$. Dies ist ein Primideal in B und es gilt $\mathfrak{q} \cap A = \lambda_A^{-1}(\mathfrak{m}) = \lambda^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$. ■

Bemerkung 4.2.5 Sei $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ Primideal}\}$. Für ein Ringhomomorphismus $f : A \to B$ haben wir eine Abbildung $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ definiert durch $\mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$. Der obige Satz bedeudet, dass diese Abbildung surjektiv ist, wenn $A \subset B$ und B ganz über A ist.

Satz 4.2.6 (Going-up Theorem) Seien $A \subset B$ Ringe mit B ganz über A. Sei $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ eine Kette von Primidealen in A und sei $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ mit $m < n$ eine Kette von Primidealen in B mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $i \in [1, m]$.

Dann kann mann die Kette $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ ergänzen in einer Kette von Primidealen $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ so, dass $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $i \in [1, n]$. □

Beweis. Per Induktion nach n genügt es die Aussage für $m = 1$ und $n = 2$ zu zeigen. Wir haben ein kommutatives Diagramm

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A/\mathfrak{p}_1 & \longrightarrow & B/\mathfrak{q}_1, \end{array}$$

wobei π_A und π_B die kanonische Projektionen sind. Sei $\mathfrak{p} = \pi_A(\mathfrak{p}_2)$. Da $\mathfrak{p}_1 \subset \mathfrak{p}_2$ gilt, ist $\mathfrak{p}$ prim in $A/\mathfrak{p}_1$. Der Ring $B/\mathfrak{q}_1$ ist aber ganz über $A/\mathfrak{p}_1$ also gibt es, nach dem obigen Satz, ein Primideal $\mathfrak{q} \subset B/\mathfrak{q}_1$ mit $\mathfrak{q} \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$. Sei $\mathfrak{q}_2 = \pi_B^{-1}(\mathfrak{q})$. Dann ist $\mathfrak{q}_2$ prim und es gilt $\mathfrak{q}_2 \cap A = \pi_A^{-1}(\mathfrak{q} \cap (A/\mathfrak{p}_1) = \pi_A^{-1}(\mathfrak{p}) = \mathfrak{p}_2$. ■

4.3 Going-down Theorem

Proposition 4.3.1 Seien $A \subset B$ Ringe und sei C der ganze Abschluss von A in B. Sei $S \subset A$ multiplikativ, dann ist $S^{-1}C$ der ganze Abschluss von $S^{-1}A$ in $S^{-1}B$.

Beweis. Wir wissen schon, dass $S^{-1}C$ ganz über $S^{-1}A$ ist (weil C ganz über A ist). Sei jetzt $b/s \in S^{-1}B$ ganz über $S^{-1}A$. Dann gibt es $a_1, \cdots, a_n \in A$ und $s_1, \cdots, s_n \in S$ so, dass

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \cdots + (a_n/s_n) = 0.$$

Sei $t = s_1 \cdots s_n \in S$. Dank Multiplikation mit $(ts)^n$, gilt $(tb)^n + a_1 s s_2 \cdots s_n (tb)^{n-1} + \cdots + s^n t^{n-1} s_1 \cdots s_{n-1} a_n = 0$. Es folgt, dass tb ganz über A ist also $tb \in C$. Daraus folgt $b/s = bt/ts \in S^{-1}C$. ∎

Definition 4.3.2 Ein Integritätsring A heißt **ganz abgeschlossen** falls A ganz abgeschlossen in seinem Quotientkörper $\mathrm{Frac}(A)$ ist.

Beispiel 4.3.3 Der Ring $\mathbb{Z}$ ist ganz abgeschlossen. Jeder faktorieller Ring A ist ganz abgeschlossen. Z.B. ist $\mathsf{k}[X_1, \cdots, Xn]$ ganz abgeschlossen sobald k ein Körper ist.

Proposition 4.3.4 Sei A ein Integritätsring. Die folgende Aussagen sind äquivalent:

1. A ist ganz abgeschlossen;
2. $A_\mathfrak{p}$ ist ganz abgeschlossen für alle Primideale $\mathfrak{p}$;
3. $A_\mathfrak{m}$ ist ganz abgeschlossen für alle maximale Ideale $\mathfrak{m}$.

Beweis. Es gilt $\mathrm{Frac}(A) = \mathrm{Frac}(A_\mathfrak{p}) = \mathrm{Frac}(A_\mathfrak{m})$ also sind alle Ringe A, $A\mathfrak{p}$ und $A_\mathfrak{m}$ in $\mathrm{Frac}(A)$ enthalten. Sei C der ganze Abschluss von A in $\mathrm{Frac}(A)$. Dann ist $C_\mathfrak{p}$ (bzw. $C_\mathfrak{m}$) der ganze Abschluss von $A_\mathfrak{p}$ (bzw. $AA\mathfrak{m}$) in $\mathrm{Frac}(A)$. Es gilt also

$$A \text{ ganz abgeschlossen} \Leftrightarrow A \to C \text{ surjektiv;}$$

$$A_\mathfrak{p} \text{ ganz abgeschlossen} \Leftrightarrow A_\mathfrak{p} \to C_\mathfrak{p} \text{ surjektiv;}$$

$$A_\mathfrak{m} \text{ ganz abgeschlossen} \Leftrightarrow A_\mathfrak{m} \to C_\mathfrak{m} \text{ surjektiv.}$$

Die Aussage folgt jetzt aus Korolar 3.3.3. ∎

Definition 4.3.5 Seien $A \subset B$ Ringe und sei $\mathfrak{a} \subset A$ ein Ideal.

1. Ein Element $x \in B$ heißt **ganz über** $\mathfrak{a}$ falls es Elemente $a_1, \cdots, a_n \in \mathfrak{a}$ gibt mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

2. Die Menge $\overline{\mathfrak{a}}^B$ aller Elemente in B die ganz über $\mathfrak{a}$ sind heißt **ganzer Abschluss von** $\mathfrak{a}$

Lemma 4.3.6 Seien $A \subset B$ Ringe und sei $\mathfrak{a} \subset A$ ein Ideal. Sei C der ganze Abschluss von A in B. Sei $(\mathfrak{a})_C$ das von $\mathfrak{a}$ erzeugte Ideal in C und sei $\sqrt{(\mathfrak{a})_C}$ sein Radikal. Dann gilt

$$\overline{\mathfrak{a}}^B = \sqrt{(\mathfrak{a})_C}.$$

Insbesondere ist $\overline{\mathfrak{a}}^B$ abgeschlossen für $+$ und $\cdot$. $\square$

Beweis. Sei $x \in \overline{\mathfrak{a}}^B$. Dann gibt es Elemente $a_1, \cdots, a_n \in \mathfrak{a}$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Es folgt $x \in C$ und $x^n = -(a_1 x^{n-1} + \cdots + a_n) \in (\mathfrak{a})_C$. Daraus folgt $x \in \sqrt{(\mathfrak{a})_C}$.

Sei $x \in \sqrt{(\mathfrak{a})_C}$. Dann gilt $x^n \in (\mathfrak{a})_C$ also gibt es Elemente $y_1, \cdots, y_n \in C$ und $x_1, \cdots, x_n \in \mathfrak{a}$ mit $x^n = x_1 y_1 + \cdots + x_n y_n$. Sei $M = A[y_1, \cdots, y_n]$. Dann sind alle y_i ganz über A also ist M ganz über A und also endlich erzeugt als A-Modul. Sei $f : M \to M$ definiert durch $f(m) = x^n m$. Da $x^n = x_1 y_1 + \cdots + x_n y_n$, folgt $x^n M \subset \mathfrak{a} M$. Daraus folgt, dass es Elemente $a_1, \cdots, a_m \in \mathfrak{a}$ gibt mit $f^m + a_1 f^{m-1} + \cdots + a_m = 0$. Es folgt $x^{nm} + a_1 x^{n(m-1)} + \cdots + a_m = 0$ und x ist ganz über $\mathfrak{a}$. $\blacksquare$

Proposition 4.3.7 Seien $A \subset B$ Integritätsringe mit A ganz abgeschlossen. Sei $K = \mathrm{Frac}(A)$, sei $\mathfrak{a}$ ein Ideal in A und sei $x \in B$ ganz über $\mathfrak{a}$.

Dann ist x algebraisch über K und sein Minimalpolynom über K ist der Form $X^n + a_1 X^{n-1} + \cdots a_n$ mit $a_1, \cdots, a_n \in \sqrt{\mathfrak{a}}$.

Beweis. Da x ganz über $\mathfrak{a}$ ist, ist x algebraisch über K und es gibt $a_1, \cdots, a_n \in \mathfrak{a}$ mit $x^n + a_1 x^{n-1} + \cdots a_n = 0$. Sei $P = X^n + a_1 X^{n-1} + \cdots + a_n$ und χ das Minimalpolynom von x über K. Es gilt $\chi | P$. Sei $L = D_K(\chi)$ ein Zerfallungskörper. Seien $x_1, \cdots, x_n$ die Nullstellen von χ in L. Dann sind alle x_i Nullstellen von P also ganz über $\mathfrak{a}$. Die Koeffizienten von χ sind in K und Polynome in den $x_1, \cdots, x_n$ also ganz über $\mathfrak{a}$. Da A ganz abgeschlossen ist sind diese Koeffizienten in A und ganz über $\mathfrak{a}$. Nach dem obigen Lemma folgt, dass diese Koeffizienten in $\sqrt{\mathfrak{a}}$ sind. $\blacksquare$

Satz 4.3.8 (Going-down Theorem) Seien $A \subset B$ Integritätsringe mit A ganz abgeschlossen und B ganz über A. Sei $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ eine Kette von Primidealen in A und sei $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ mit $m < n$ eine Kette von Primidealen in B mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $i \in [1, m]$.

Dann kann mann die Kette $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ ergänzen in einer Kette von Primidealen $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$ so, dass $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für alle $i \in [1, n]$. $\square$

Beweis. Per Induktion kann man ohne Einschräkung annehmen, dass $m = 1$ und $n = 2$. Wir haben ein kommutatives Diagramm:

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\lambda_A"'] & B \arrow[d, "\lambda_B"] \\ A_{\mathfrak{p}_1} \arrow[r] & B_{\mathfrak{q}_1}, \end{tikzcd}$$

wobei alle Abbildungen injektiv sind. Dank der Bijektion zwischen Primideale in $B_{\mathfrak{q}_1}$ und Primideale in B, die in $\mathfrak{q}_1$ enthalten sind, müssen wir nur zeigen, dass es ein Primideal $\mathfrak{q} \subset B_{\mathfrak{q}_1}$ gibt mit $\lambda_A^{-1}(\mathfrak{q} \cap A_{\mathfrak{p}_1}) = \mathfrak{p}_2$. Sei $f : A \to B_{\mathfrak{q}_1}$ die Komposition, dies ist äquivalent zu $f^{-1}(\mathfrak{q}) = \mathfrak{p}_2$. Nach Proposition 3.4.6 ist dies äquivalent zu: $\mathfrak{p}_2 = f^{-1}(f(\mathfrak{p}_2)) = \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$.

Es gilt $\mathfrak{p}_2 \subset \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$. Sei also $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$. Dann ist x der Form y/s mit $y \in \mathfrak{p}_2 B$ und $s \in B \setminus \mathfrak{q}_1$. Nach Lemma 4.3.6 mit $B = C$ sind Elemente in $\mathfrak{p}_2 B$ ganz über $\mathfrak{p}_2$. Nach der obigen Proposition sind die Koeffizienten des Minimalpolynoms χ_y von y über $K = \mathrm{Frac}(A)$ in $\sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$ (weil $\mathfrak{p}_2$ prim ist). Es gilt also

$$y^k + a_1 y^{k-1} + \cdots + a_k = 0,$$

wobei $a_i \in \mathfrak{p}_2$.

Da $x \in A$ folgt $s = yx^{-1}$ in K. Es gilt

$$s^k + a_1/x s^{k-1} + \cdots + a_k/x^k = 0.$$

Die ist das Minimalpolynom von s über K: wenn es eine weitere Gleichung $s^r + a'_1 s^{r-1} + \cdots + a'_r = 0$ gibt mit $r < s$ $a'_i \in K$ folgt $y^r + x a'_1 y^{r-1} + \cdots + x^r a'_r = 0$ ein Widerspruch zur Minimalität von k. Wir schreiben $u_i = a_i/x^i$ also ist

$$s^k + u_1 s^{k-1} + \cdots + u_k = 0$$

ein Minimalpolynom von s über K. Da $s \in B$ ganz über A ist, folgt aus der obigen Proposition folgt, dass $u_i \in A$.

Angenommen $x \notin \mathfrak{p}_2$. Dann gilt $x^i u_i = a_i \in \mathfrak{p}_2$ und also $u_i \in \mathfrak{p}_2$ für alle i. Daraus folgt $s^k = -(u_1 s^{k-1} + \cdots + u_1) \in \mathfrak{p}_2 B \subset \mathfrak{p}_1 B \subset \mathfrak{q}_1$. Es folgt $s \in \mathfrak{q}_1$ ein Widerspruch und also $x \in \mathfrak{p}_2$. ■

4.4 Nullstellensatz

Dank ganzen Ringen haben wir in der Vorlesung Einführung in die algebraische Geometrie den folgenden Satz bewiesen (Satz 3.2.1, Nullstellensatz 1).

Satz 4.4.1 (Nullstellensatz – algebraische Version) Sei k ein Körper und B eine endlich erzeugte k-Algebra. Falls B ein Körper ist ist $\mathsf{k} \subset B$ eine endliche Erweiterung. □

5 Dimension I

5.1 Transzendenzgrad

Definition 5.1.1 Sei $\mathsf{k} \subset K$ eine Körpererweiterung.

Eine Familie $x_1, \cdots, x_n$ von Elementen aus K heißt **algebraisch unabhängig** oder **transzendent** über k falls gilt

$$(P \in \mathsf{k}[T_1, \cdots, T_n], P(x_1, \cdots, x_n) = 0 \Rightarrow P = 0).$$

Proposition 5.1.2 Sei $K \subset L$ eine Körpererweiterung und seien $S, T \subset K$ Teilmengen. Die folgende Aussagen sind äquivalent:

1. $S \cup T$ ist algebraisch unabhängig über k und $S \cap T = \emptyset$;
2. S ist algebraisch unabhängig über k und T ist algebraisch unabhängig über $\mathsf{k}(S)$;
3. T ist algebraisch unabhängig über k und S ist algebraisch unabhängig über $\mathsf{k}(T)$.

Beweis. Es genügt zu zeigen, dass 1. und 2. äquivalent sind.

(1. $\Rightarrow$ 2.) Da $S \cup T$ algebraisch unabhängig über k ist, ist auch S algebraisch unabhängig über k. Angenommen T sei algebraisch abhängig über $\mathsf{k}(S)$, gibt es Elemente $t_1, \cdots, t_n \in T$ und ein Polynom $P \in \mathsf{k}(S)[T_1, \cdots, T_n]$ so, dass $P(t_1, \cdots, t_n) = 0$. Dank multiplikation mit einem Element aus $\mathsf{k}[S]$ können wir annehmen, dass P seine Koeffizienten in $\mathsf{k}[S]$ hat. Das Element P kann also als ein Polynom Q in S und $T_1, \cdots, T_n$ betrachten werden mit $Q(S, t_1, \cdots, t_n) = 0$. Daraus folgt, dass $P = Q = 0$.

(2. $\Rightarrow$ 1.) Da T algebraisch unabhängig über $\mathsf{k}(S)$ ist muss $S \cap T = \emptyset$ gelten. Seien $x_1, \cdots, x_n \in S$, $t_1, \cdots, t_m \in T$ und $P \in k[X_1, \cdots, X_n, T_1, \cdots, T_m]$ ein Polynom mit $P(x_1, \cdots, x_n, t_1, \cdots, t_m) = 0$. Wir betrachten P als Polynom Q in $T_1, \cdots, T_m$ mit Koeffizienten in $\mathsf{k}[x_1, \cdots, x_n] \subset \mathsf{k}(S)$. Es gilt $Q(t_1, \cdots, t_m) = 0$ also $Q = 0$. Es folgt, dass alle Koeffizienten von Q null sind. Diese Koeffizieten sind Polynome in $\mathsf{k}[S]$ und also alle Koeffizienten von diesen Polynomen sind auch Null. Diese Koeffizienten sind die Koeffizienten von P. Es folgt $P = 0$. ∎

Korollar 5.1.3 Sei $\mathsf{k} \subset K$ ein Körpererweiterung und sei $S \subset K$. Die Menge S ist genau dann algebraisch unabhängig über k, wenn alle $x \in S$ transzendent über $\mathsf{k}(S \setminus \{x\})$ ist.

Beweis. Nach der obigen Proposition, falls S algebraisch unabhängig ist, ist x transzendent über $\mathsf{k}(S \setminus \{x\})$.

Umbekehrt, seien $x_1, \cdots, x_n \in S$. Dann ist x_n transzendent über $\mathsf{k}(x_1, \cdots, x_{n-1})$ und per Induktion und nach der obigen Proposition folgt, dass $(x_1, \cdots, x_n)$ algebraisch unabhängig über k ist, also ist S algebraisch unabhängig über k. ■

Proposition 5.1.4 Sei $\mathsf{k} \subset K$ eine Körpererweiterung und sei $\mathsf{k} \subset \mathsf{k}'$ eine algebraische Erweiterung. Sei S algebraisch unabhängig über k, dann ist auch S algebraisch unabhängig über k'.

Beweis. Angenommen S sei algebraisch abhängig über k'. Dann gibt es ein $x \in S$ so, dass x algebraisch über $\mathsf{k}'(S \setminus \{x\})$ ist. Da aber k' algebraisch über k ist, ist auch $\mathsf{k}'(S \setminus \{x\})$ algebraisch über $\mathsf{k}(S \setminus \{x\})$ und also x ist algebraisch über $\mathsf{k}(S \setminus \{x\})$. Daraus folgt S algebraisch abhängig. Ein Widerspruch. ■

Definition 5.1.5 Sei $\mathsf{k} \subset K$ eine Körpererweiterung. Eine **Transzendenzbasis** von K über k ist eine Teilmenge $B \subset K$ so, dass B algebraisch unabhängig über k ist und K akgebraisch über $\mathsf{k}(B)$ ist.

Beispiel 5.1.6 Sei $K = \mathsf{k}(X)$.

1. Dann ist $B = \{X\}$ eine Transzendenzbasis von K über k.

2. Dann ist $B = \{X^2\}$ eine Transzendenzbasis von K über k.

Proposition 5.1.7 Sei $\mathsf{k} \subset K$ eine Körpererweiterung. Eine Teilmenge $B \subset K$ ist genau dann eine Transzendenzbasis, wenn B eine maximale algebraisch unabhängige Familie ist.

Beweis. Falls B eine Transzendenzbasis ist und $x \in K \setminus B$. Dann ist x algebraisch über $\mathsf{k}(B)$ und also ist $B \cup \{x\}$ algebraisch abhängig.

Umgekehrt, falls B eine maximale algebraisch unabhängige Familie ist, ist B algebraisch unabhängig über k und jedes Element von K ist algebraisch über $\mathsf{k}(B)$ (sonst wäre $B \cup \{x\}$ algebraisch unabhängig). ■

Satz 5.1.8 (Satz von Steinitz) Sei $\mathsf{k} \subset K$ eine Körpererweiterung. Seien $S, T \subset K$ so, dass S algebraisch unabhängig über k ist und K algebraisch über $\mathsf{k}(T)$ ist.

Dann gibt es eine Transzendenzbasis B mit $S \subset B \subset T$. □

Beweis. Sei Σ die Menge aller Teilmenge $B \subset T$ so, dass $S \subset B$ und B algebraisch unabhängig über k ist. Diese Menge ist induktiv (die Vereinigung von Elementen in einer Kette ist ein Maximum) also gibt es eine maximale solche Teilmenge B. Diese Teilmenge B ist algebraisch unabhängig. Falls alle Elemente von T algebraisch über $\mathsf{k}(B)$ sind, ist $\mathsf{k}(T)$ algebraisch über $\mathsf{k}(B)$. Es folgt, dass K auch algebraisch über $\mathsf{k}(B)$ ist und B ist eine Transzendenzbasis. Wenn es ein $t \in T$ gibt so, dass t transzendent über $\mathsf{k}(B)$ ist, ist $B \cup \{t\}$ in Σ. Ein Widerspruch. ∎

Satz 5.1.9 Sei $\mathsf{k} \subset K$ eine Körpererweiterung. Dann haben alle Transzendenzbasen die selbe Anzahl von Elementen. □

Beweis. Wir zeigen dies Falls es eine Transzendenzbasis B gibt mit $|B| = n < \infty$.

Sei B' eine weitere Transzendenzbasis. Es genügt zu zeigen $|B'| \leq |B|$ (Analog wird also gelten $|B| \leq |B'|$).

Wir verfahren per Induktion nach n. Für $n = 0$ ist K algebraisch über k und jede Transzendenzbasis ist die leere Menge.

Sei also $n \geq 1$ und sei $x \in B'$. Dann gibt es (Satz von Steinitz) eine Teilmenge $C \subset B$ so, dass $x \notin C$ und $\{x\} \cup C$ eine Transzendenzbasis von K über k ist. Es gilt $C \subsetneq B$: falls $x \in B$ gilt $C = B \setminus \{x\}$. Für $x \notin B$, falls $C = B$ gilt $C \cup \{x\} \supsetneq B$ und $C \cup \{x\}$ ist nich algebraisch unabhängig (maximalität von Transzendenzbasen). Ein Widerspruch. Es folgt also $|C| < n$. Sei $\mathsf{k}' = \mathsf{k}(x)$ und $C' = B' \setminus \{x\}$. Dann sind C und C' linear unabhängig über k' und K ist algebraisch über $\mathsf{k}'(C) = \mathsf{k}(C \cup \{x\})$ und $\mathsf{k}'(C') = \mathsf{k}(B')$. Es folgt, dass C und C' Transzendenzbasen von K über k' sind und also $|C| = |C'|$. Daraus folgt $|B'| = |C'| + 1 = |C| + 1 \leq n$. ∎

Definition 5.1.10 Sei $\mathsf{k} \subset K$ eine Körpererweiterung.

Der Transzendenzgrad $\mathrm{Trdeg}_{\mathsf{k}}(K)$ **von** K **über** k ist die maximale Anzahl von Elementen in einer algebraischen unabhängigen Familie. Dies ist auch die Anzahl von Elementen in einer Transzendenzbasis.

Ein paar Korollare vom obigen Satz.

Korollar 5.1.11 Sei $\mathsf{k} \subset K$ eine Körpererweiterung mit $n = \mathrm{Trdeg}_{\mathsf{k}}(K)$ und $S \subset K$.

Falls K algebraisch über $\mathsf{k}(S)$ ist gilt $|S| \geq n$. Falls $|S| = n$ ist S algebraisch unabhängig.

Beweis. Nach dem Satz von Steinitz gibt es eine Transzendenzbasis $B \subset S$. ∎

Korollar 5.1.12 Sei $\mathsf{k} \subset K$ eine Körpererweiterung mit $n = \mathrm{Trdeg}_{\mathsf{k}}(K)$ und seien $x_1, \cdots, x_m \in K$ mit $K = \mathsf{k}(x_1, \cdots, x_m)$.

Dann gilt $m \geq n$. Falls $m = n$ ist $(x_1, \cdots, x_n)$ eine Transzendenzbasis. Eine solche Erweiterung heißt **rein transzendent**.

Beweis. Nach dem Satz von Steinitz gibt es eine Transzendenzbasis $B \subset \{x_1, \cdots, x_m\}$. ■

Korollar 5.1.13 Sei $\mathsf{k} \subset K$ eine Körpererweiterung mit $n = \mathrm{Trdeg}_{\mathsf{k}}(K)$. Für eine algebraisch unabhängige Familie $S \subset K$ gilt $|S| \leq n$. Außerdem, falls $|S| = n$ ist S algebraisch unabhängig also eine Transzendenzbasis.

Proposition 5.1.14 Seien $\mathsf{k} \subset K \subset L$ Körpererweiterungen und seien S und T Transzendenzbasen von K über k und von L über K.

Dann gilt $S \cap T = \emptyset$ und $S \cup T$ ist eine Transzendenzbasis von L über k.

Beweis. Der Körper L ist algebraisch über $K(T)$ und $K(T)$ ist algebraisch über $\mathsf{k}(S \cup T) = \mathsf{k}(S)(T)$. Daraus folgt, dass L algebraisch über $\mathsf{k}(S \cup T)$ ist.

Außerdem ist T algebraisch unabhängig über K also auch über $\mathsf{k}(S)$. Es folgt $S \cap T = \emptyset$ und $S \cup T$ ist algebraisch unabhängig über k. ■

Korollar 5.1.15 Seien $\mathsf{k} \subset K \subset L$ Körpererweiterungen. Es gilt

$$\mathrm{Trdeg}_{\mathsf{k}}(L) = \mathrm{Trdeg}_{\mathsf{k}}(K) + \mathrm{Trdeg}_K(L).$$

5.2 Noethersches Lemma

Satz 5.2.1 (Noethersches Lemma) Sei k ein Körper und A eine endlich erzeugte k-Algebra so, dass A ein Integritätsring ist. Sei $K = \mathrm{Frac}(A)$.

Dann gibt es algebraisch unabhängige Elemente $x_1, \cdots, x_n \in A$ so, dass A ganz über $\mathsf{k}[x_1, \cdots, x_n]$ ist und $n = \mathrm{Trdeg}_{\mathsf{k}}(K)$. □

Beweis. Sei $y_1, \cdots, y_m$ eine erzeugende Familie von A als k-Algebra. Ohne Einschränkung können wir annehmen, dass $y_1, \cdots, y_r$ algebraisch unabhängig sind und dass $y_{r+1}, \cdots, y_m$ algebraisch über $k[y_1, \cdots, y_r]$ sind. Wir verfahren per Induktion nach m.

Für $m = r$ ist die Aussage klar. Wir nehmen also an, dass die Aussage für k-Algebren mit $m-1$ Erzeugern gilt. Das Element y_m ist ganz über $\mathsf{k}[y_1, \cdots, y_{m-1}]$. Daraus folgt, dass es ein Polynom $P \in \mathsf{k}[y_1, \cdots, y_{m-1}][T]$ gibt so, dass $P(y_1, \cdots, y_m) = 0$.

Seien $r_1, \cdots, r_{m-1}$ naturlische Zahlen. Wir setzen $z_i = y_i - y_m^{r_i}$ und $A' = \mathsf{k}[z_1, \cdots, z_{m-1}]$. Dann gilt $A = A'[y_m]$. Es gilt $P(z_1 + y_m^{r_1}, \cdots z_{m-1} + y_m^{r_{m-1}}, y_m) = 0$. Wir schreiben P als Polynom in $z_1, \cdots, z_{m-1}, y_m$. Für jedes Monom $y_1^{k_1} \cdots y_m^{k_m}$ gibt es ein Monom der Form $y_m^{k_m + r_1 k_1 + \cdots + r_{m-1} k_{m-1}}$. Wenn die r_i gut gewählt sind z.B. mit $r_1 \gg r_2 \gg \cdots \gg r_{m-1} \gg 0$ ist dieser Term der Term mit höherem Grad in $y_1^{k_1} \cdots y_m^{k_m}$. Es folgt, dass $P(z_1 + y_m^{r_1}, \cdots z_{m-1} + y_m^{r_{m-1}}, y_m) = \lambda y_m^N +$Terme von Grad $< N$ mit $0 \neq \lambda \in \mathsf{k}$. Es folgt, dass y_m ganz über $A' = \mathsf{k}[z_1, \cdots, z_{m-1}]$ ist also $A = A'[y_m]$ ist ganz über A'. Nach Induktion gibt es algebraische unabhängige Elemente $x_1, \cdots, x_n \in A' = \mathsf{k}[z_1, \cdots, z_{m-1}]$

so, dass A' ganz über $\mathsf{k}[x_1, \cdots, x_n]$ ist. Daraus folgt, dass A ganz über $\mathsf{k}[x_1, \cdots, x_n]$ ist.

Wir zeigen jetzt, dass $n = \mathrm{Trdeg}_{\mathsf{k}}(K)$. Per Definition gilt $n \leq \mathrm{Trdeg}_{\mathsf{k}}(K)$. Alle Elemente aus A sind ganz über $\mathsf{k}[x_1, \cdots, x_n]$. Sei $a/b \in K$ mit $a, b \in A$ und $b \neq 0$. Seien $b_1, \cdots, b_k \in \mathsf{k}[x_1, \cdots, x_n]$ mit $b^k + b_1 b^{k-1} + \cdots + b_k = 0$ und k minimal so, dass es eine solche Gleichung gibt. Es folgt, dass $b_k \neq 0$ und also

$$b(b^{k-1} + b_1 b^{k-2} + \cdots + b_{k-1}) b_k^{-1} = 1.$$

Daraus folgt

$$b^{-1} = (b^{k-1} + b_1 b^{k-2} + \cdots + b_{k-1}) b_k^{-1}.$$

Da b ganz über $\mathsf{k}[x_1, \cdots, x_n]$ ist und da $b_k^{-1} \in \mathsf{k}(x_1, \cdots, x_n)$ folgt, dass b^{-1} algebraisch über $\mathsf{k}(x_1, \cdots, x_n)$ ist und also auch a/b. Es folgt, dass K algebraisch über $\mathsf{k}(x_1, \cdots, x_n)$ ist und also $\mathrm{Trdeg}_{\mathsf{k}}(K) \leq n$. ∎

5.3 Dimension

Definition 5.3.1 Sei A ein Ring.

1. **Die krullsche Dimension** $\mathrm{Kdim}(A)$ **von** A ist die maximale Zahl n so, dass es eine Kette $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq A$ gibt mit $\mathfrak{p}_i$ prim für alle $i \in [0, n]$. Falls es unendliche Ketten gibt, ist $\mathrm{Kdim}(A) = \infty$.

2. Sei $\mathfrak{p}$ ein Primideal in A. 1. **Die lokale Dimension** $\mathrm{Kdim}_{\mathfrak{p}}(A)$ **von** A **bei** $\mathfrak{p}$ ist die krullsche Dimension vom lokalen Ring $A_{\mathfrak{p}}$.

Bemerkung 5.3.2 Für $A \neq 0$ gilt $\mathrm{Kdim}(A) \geq 0$ (es gilt $\infty \geq 0$).

Beispiel 5.3.3 1. Für $A = \mathsf{k}$ ein Körper, gilt $\mathrm{Kdim}(A) = 0$.

2. Für $A = \mathbb{Z}$, gilt $\mathrm{Kdim}(A) = 1$.

3. Für $A = \mathbb{Z}$ und $\mathfrak{p} = (p)$, wobei p eine Primzahl ist, gilt $\mathrm{Kdim}\mathfrak{p}(A) = 1$. Für $\mathfrak{p} = (0)$, gilt $\mathrm{Kdim}\mathfrak{p}(A) = 0$.

Lemma 5.3.4 Es gilt $\mathrm{Kdim}(A) = \sup\limits_{\mathfrak{m}\text{ maximal}} \mathrm{Kdim}_{\mathfrak{m}}(A)$. □

Beweis. Die Aussage folgt aus der Bijektion $\{\mathfrak{p} \subset \mathfrak{m} \mid \mathfrak{p} \text{ prim}\} \leftrightarrow \{\mathfrak{q} \subset A_{\mathfrak{m}} \mid \mathfrak{q} \text{ prim}\}$: Sei $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ eine Kette von maximalen Idealen in A. Falls $\mathfrak{p}_n$ nicht maximal ist können wir diese Kette mit einem maximalen Ideal $\mathfrak{m}$ ergänzen: $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq \mathfrak{m}$. Insbesondere ist eine maximale Kette immer in einem maximalen Ideal enthalten. ∎

Proposition 5.3.5 Seien $A \subset B$ Integritätsringe mit B ganz über A und A ganz abgeschlossen.

1. Sei $\mathfrak{n} \subset B$ maximal und $\mathfrak{m} = \mathfrak{n} \cap A$. Dann ist $\mathfrak{m}$ maximal und es gilt

$$\mathrm{Kdim}(A_{\mathfrak{m}}) = \mathrm{Kdim}(B_{\mathfrak{n}}).$$

2. Es gilt $\mathrm{Kdim}(A) = \mathrm{Kdim}(B)$.

Beweis. 1. Aus Korollar 4.2.2 folgt, dass $\mathfrak{m}$ maximal ist. Sei $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n \subsetneq \mathfrak{n}$ eine Kette in B (zu dieser Kette gehörte genau eine Kette in $B_{\mathfrak{n}}$). Sei $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. Dank Korollar 4.2.3 gilt $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq \mathfrak{m}$ und also $\mathrm{Kdim} A_{\mathfrak{m}} \geq \mathrm{Kdim} B_{\mathfrak{n}}$.

Umgekehrt, für eine Kette $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq \mathfrak{m}$ gibt es (dank Going-down) eine Kette $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n \subsetneq \mathfrak{n}$ und also $\mathrm{Kdim} A_{\mathfrak{m}} \leq \mathrm{Kdim} B_{\mathfrak{n}}$.

2. Aus 1. folgt, dass es für jedes $\mathfrak{n} \subset B$ maximal ein $\mathfrak{m} = \mathfrak{n} \cap A \subset A$ maximal gibt mit $\mathrm{Kdim}_{\mathfrak{m}}(A) = \mathrm{Kdim}_{\mathfrak{n}}(B)$.

Andersrum, dank dem Satz 4.2.4, gibt es für jedes $\mathfrak{m} \subset A$ maximal ein $\mathfrak{q} \subset B$ prim mit $\mathfrak{q} \cap A = \mathfrak{m}$. Sei $\mathfrak{n} \subset B$ maximal mit $\mathfrak{q} \subset \mathfrak{n}$. Es gilt $\mathfrak{m} = \mathfrak{q} \cap A \subset \mathfrak{n} \cap A$ und das letzte Ideal ist maximal. Da $\mathfrak{m}$ auch maximal ist gilt $\mathfrak{m} = \mathfrak{n} \cap A$ und nach dem Korollar 4.2.3 folgt $\mathfrak{n} = \mathfrak{q}$ also ist $\mathfrak{q} = \mathfrak{n}$ maximal. Es folgt, dass es für jedes $\mathfrak{m} \subset A$ maximal ein $\mathfrak{n} \subset B$ maximal gibt mit $\mathrm{Kdim}_{\mathfrak{n}}(B) = \mathrm{Kdim}_{\mathfrak{m}}(A)$. Die Aussage folgt daraus und aus dem obigen Lemma. ∎

Satz 5.3.6 Es gilt $\mathrm{Kdim}(\mathsf{k}[X_1, \cdots, X_n]) = n$. □

Beweis. Sei $A = \mathsf{k}[X_1, \cdots, X_n]$. Es gilt $(0) \subsetneq (X_1) \subsetneq (X_1, \cdots, X_n)$ also gilt $\mathrm{Kdim}(A) \geq n$. Wir zeigen die Gleichheit per Induktion nach n.

Sei $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ eine Kette von Primidealen. Falls $\mathfrak{p}_0 \neq (0)$ können wir diese Kette ergänzen in $(0) \subsetneq \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$. Wir können also annehmen, dass $\mathfrak{p}_0 = (0)$. Sei $Q \in \mathfrak{p}_1$ mit $Q \neq 0$. Falls Q invertierbar ist gilt $\mathfrak{p}_1 = A$ und wir setzen $P = X_1$. Sonst betrachten wir die Primzerlegung $Q = P_1 \cdots P_r$ von Q. Da $\mathfrak{p}_1$ prim ist gibt es ein i so, dass $P = P_i \in \mathfrak{p}_1$. Da A faktoriel ist, ist (P) prim und es gilt $(P) \subset \mathfrak{p}_1$. Ohne Einschränkung durfen wir also annehmen, dass $\mathfrak{p}_1 = (P)$ mit P irreduzibel.

Wir setzen $Y_1 = P$ und $Y_i = X_i - X_1^{r_i}$ für $i \in [2, n]$. Sei $B = \mathsf{k}[Y_1, \cdots, Y_n]$. Wir zeigen, dass A ganz über B ist. Es genügt zu zeigen, dass X_1 ganz über B ist. Es gilt $P(X_1, Y_2 + X_1^{r_2}, \cdots Y_n + X_1^{r_n}) = Y_1$. Wir schreiben P als Polynom in $X_1, Y_2, \cdots, Y_n$. Für jedes Monom $X_1^{k_1} \cdots X_n^{k_m}$ gibt es ein Monom der Form $X_1^{k_1 + r_2 k_2 + \cdots + r_n k_n}$. Wenn die r_i gut gewählt sind z.B. mit $r_n \gg \cdots \gg r_1 \gg 0$ ist dieser Term der Term mit höherem Grad in $X_1^{k_1} \cdots X_n^{k_n}$. Es folgt, dass $P(X_1, Y_2 + X_1^{r_1}, \cdots Y_n + X_n^{r_n}) = \lambda X_1^N + \text{Terme von Grad} < N$ mit $0 \neq \lambda \in \mathsf{k}$. Es folgt, dass X_1 ganz über B ist. Der Ring A ist also ganz über B. Es folgt, dass $\mathrm{Frac}(A) = \mathsf{k}(X_1, \cdots, X_n)$ algebraisch über $\mathrm{Frac}(B) = \mathsf{k}(Y_1, \cdots, Y_n)$ ist. Daraus folgt, dass $\mathrm{Trdeg}_{\mathsf{k}}(\mathrm{Frac}(B)) = \mathrm{Trdeg}_{\mathsf{k}}(A) = n$

und dass die Familie $(Y_1, \cdots, Y_n)$ algebraisch unabhängig ist. Es folgt, dass $B = \mathsf{k}[Y_1, \cdots, Y_n]$ ein Polynomring ist und also dass B faktoriel. Daraus folgt auch, dass B ganz abgeschlossen ist. Es folgt $\mathrm{Kdim}(A) = \mathrm{Kdim}(B)$ und eine Kette $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ in A induziert eine Kette $\mathfrak{p}_0 \cap B \subsetneq \cdots \subsetneq \mathfrak{p}_m \cap B$ in B. Wir können also A mit B erzetzen und $(0) = \mathfrak{p}_0 \subsetneq (P) = \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ mit $\mathfrak{q}_0 = (0) = \mathfrak{p}_0 \subsetneq \mathfrak{q}_1 = (P) \cap B = \mathfrak{p}_1 \cap B \subsetneq \cdots \subsetneq \mathfrak{q}_m = \mathfrak{p}_m \cap B$ ersetzen.

Es gilt aber $\mathfrak{p}_1 \cap B = (P) \cap B = (Y_1) \cap B$. Wir zeigen $(Y_1)_B = (Y_1) \cap B$, wobei $(Y_1)_B$ das von Y_1 erzeugte Ideal in B. Da $Y_1 \in B$ gilt $(Y_1)_B \subset (Y_1) \cap B$. Sei $Q \in (Y_1) \cap B$. Dann gibt es $R \in A$ mit $Q = Y_1 R$. Es gilt $R = Q/Y_1 \in \mathrm{Frac}(B)$ und da $R \in A$ ist R ganz über B. Da B ganz abgeschlossen ist, folgt $R \in B$ und also $Q \in (Y_1)_B$. Wir haben also $B = \mathsf{k}[Y_1, \cdots, Y_n]$ und die Kette $(0) = \mathfrak{q}_0 \subsetneq (Y_1) = \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$. Diese Kette induzierte ein Kette $(0) \subsetneq \mathfrak{q}_2/(Y_1) \subsetneq \cdots \subsetneq \mathfrak{q}_m/(Y_1) \subsetneq B/(Y_1) \simeq \mathsf{k}[Y_2, \cdots, Y_n]$. Per Induktion folgt $m - 1 \leq n - 1$ und also $m \leq n$. ∎

Satz 5.3.7 Sei k ein Körper und A eine k-Algebra so, dass A ein Integritätsring ist. Sei $K = \mathrm{Frac}(A)$. Es gilt

$$\mathrm{Kdim}(A) = \mathrm{Trdeg}_{\mathsf{k}}(K).$$

Beweis. Nach dem notherschen Lemma gibt es algebraisch unabhängige Elemente $x_1, \cdots, x_n \in A$ so, dass A ganz über $\mathsf{k}[x_1, \cdots, x_n]$ ist. Der Ring $\mathsf{k}[x_1, \cdots, x_n]$ ist ein Polynomring also faktoriel und also auch ganz abgeschlossen. Es folgt $\mathrm{Kdim}(A) = \mathrm{Kdim}(\mathsf{k}[x_1, \cdots, x_n]) = n$. ∎

6 Ketten

6.1 Ketten und maximales Element

Proposition 6.1.1 Sei $(\Sigma, \leq)$ eine geordnete Menge (*i.e.* eine Menge mit einer Ordnung). Die folgende Aussagen sind äquivalent:

1. Jede Aufsteigende Kette $x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$ ist stationär.
2. Jede nicht leere Teilmenge von Σ hat ein maximalies Element.

Beweis. (1. $\Rightarrow$ 2.) Falls 2. falsch ist gibt es eine nicht leere Menge $X \subset \Sigma$ ohne maximales Element. Dann kann man per Induktion eine aufsteigende und nicht stationäre Kette konstruieren: man wählt $x_1 \in \Sigma$ beliebig. Falls x_n konstuirt ist, wähl man $x_{n+1} > x_n$ (dies ist möglich, weil X kein maximales Element hat).

(2. $\Rightarrow$ 1.) Sei $(x_n)_{n\in\mathbb{N}}$ eine Aufsteigende Kette. Dann hat $X = \{x_n \mid n \in \mathbb{N}\}$ ein maximales Element x_m. Es gilt also für $n \geq m$: $x_m \geq x_n$ aber auch per Konstruktion $x_m \leq x_n$ also $x_n = x_m$ für alle $m \geq n$. ∎

Definition 6.1.2 Sei M ein A-Modul und sei Σ die Menge aller Untermoduln von M.

1. Sei $\leq$ die Ordnung über Σ definiert durch $N \leq P \Leftrightarrow N \subset P$. Falls $(\Sigma, \leq)$ eine der beiden äquivalenten Aussagen von der obigen Proposition erfüllt, hat M die **aufsteigende Kettenbedingung oder acc (ascending chain condition)**. Ein solcher Modul heißt **noethersch**

2. Sei $\leq$ die Ordnung über Σ definiert durch $N \leq P \Leftrightarrow N \supset P$. Falls $(\Sigma, \leq)$ eine der beiden äquivalenten Aussagen von der obigen Proposition erfüllt, hat M die **absteigende Kettenbedingung oder dcc (descending chain condition)**. Ein solcher Modul heißt **artinsch**

Beispiel 6.1.3 1. Eine endliche abelsche Gruppe (und also auch ein endlicher $\mathbb{Z}$-Modul) ist noethersch und artinsch.

2. Der Ring $A = \mathbb{Z}$ als A-Modul ist noethersch: alle Ideal sind Hauptideale und $(a) \subset (b)$ gilt genau dann, wenn $b|a$. Da a nur endlich viele teiler hat, erfüllt $\mathbb{Z}$ (acc).

Es ist aber kein artinscher Modul: wir haben eine unendliche absteigende Kette $(p) \supsetneq (p^2) \supsetneq \cdots \supsetneq (p^n) \supsetneq \cdots$

3. Sei p eine Primzahl und sei G die Untergruppe von $\mathbb{Q}/\mathbb{Z}$ aller Elemente deren Ordnung eine Potenze von p ist:

$$G = \left\{ \left[\frac{a}{p^k}\right] \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Sei G_n die Menge aller Elemente in G der Ordnung ein Teiler von p^n *i.e.*

$$G_n = \left\{ \left[\frac{a}{p^n}\right] \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z} \right\}.$$

Dies ist die einzige Untergruppe von G mit p^n Elemente. Es gilt

$$G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n \subsetneq \cdots$$

also G (als $\mathbb{Z}$-Modul) ist nicht noethersch.

Andersrum sind die G_n die einzigen Untergruppen von G und also ist G artinsch.

4. Die Untergruppe H von $\mathbb{Q}$ der Form

$$H = \left\{ \frac{a}{p^k} \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Es gilt $\mathbb{Z} \subset H$ und eine exacte Sequenz $0 \to \mathbb{Z} \to H \to G \to 0$. Insbesondere ist H nicht noethersch und auch nicht artinsch.

5. Der Ring $A = \mathsf{k}[X]$ ist noethersch aber nicht artinsch als A-Modul (Kette $\mathsf{k}[X] \supsetneq (X) \supsetneq \cdots \supsetneq (X^n) \supsetneq \cdots$.

6. Der Ring $A = \mathsf{k}[X_1, \cdots, X_n, \ldots]$ ist als A-Modul nicht noethersch (Kette $(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n) \subsetneq \cdots$ und nicht artinsch (Kette $\mathsf{k}[X_1] \supsetneq (X_1) \supsetneq \cdots \supsetneq (X_1^n) \supsetneq \cdots$).

Bemerkung 6.1.4 Für Ringe ist (dcc) also artinsch viel stärker als (acc) also noethersch. Wir werden sehen, dass (artinsch = noethersch + Dimension Null).

Proposition 6.1.5 Sei M ein A-Modul. Es gilt

$$M \text{ ist noethersch } \Leftrightarrow \text{jeder Untermodul von } M \text{ ist endlich erzeugt.}$$

Beweis. ($\Rightarrow$) Sei $N \subset M$ ein Untermodul. Sei Σ die Menge aller endlich erzeugten Untermoduln von N. Dies ist eine nicht leere Menge (der Nullmodul ist in Σ). Da M (acc) hat gibt es ein maximales Element N' in Σ. Wir zeigen $N' = N$. Falls $N' \subsetneq N$, sei $n \in N \setminus N'$. Dann ist $N' + An$ endlich erzeugt mit $N' \subsetneq N' + An$. Ein Widerspruch.

($\Leftarrow$) Sei $N_0 \subset \cdots \subset N_n \subset \cdots$ eine Kette von Untermoduln. Sei $N = \cup_n N_n$. Dann ist N ein Untermodul von M und also endlich erzeugt. Seien $n_1, \cdots, n_k$ Erzeuger von N. Es gibt ein n groß genug mit $n_i \in N_n$ für alle i. Daraus folgt $N = N_n$ und die Kette ist stationär. ∎

Proposition 6.1.6 Sei $0 \to M' \overset{u}{\to} M \overset{u}{\to} M'' \to 0$ eine exakte Sequenz. Es gilt

1. M noethersch $\Leftrightarrow$ M' und M'' noethersch.

2. M artinsch $\Leftrightarrow$ M' und M'' artinsch.

Beweis. Wir zeigen 1. Die zweite Aussage kann man analog beweisen.

($\Rightarrow$) Eine Kette in M' oder M'' induziiert eine Kette in M via u oder v^{-1}. Beide induzierte Ketten sind stationär und es folgt das die Anfangsketten auch stationär waren.

($\Leftarrow$) Sei $M_0 \subset \cdots \subset M_n \subset \cdots$ eine Kette in M. Dann ist $(v(M_n))_n$ eine Kette in M'' und also gibt es ein N'' mit $v(M_n) = v(M_{N''})$ für $n \geq N''$. Die Kette $(u^{-1}(M_n))_n$ it auch stationär: es gibt ein N' mit $u^{-1}(N_n) = u^{-1}(N_{N'})$ für $n \geq N'$. Sei $N = \max(N', N'')$, $n \geq N$ und $m \in M_n$. Es gilt $v(m) \in v(M_n) = v(M_N)$ also gibt es ein $m_1 \in M_N$ mit $v(m_1) = v(m)$ *i.e.* $m - m_1 \in M_n \cap \mathrm{Ker}(v) = M_n \cap \mathrm{Im} u$. Sei $m' \in M'$ mit $u(m') = m - m_1$. Es gilt $m' \in u^{-1}(M_n) = u^{-1}(M_N)$ also $m - m_1 = u(m') \in M_N$. Da $M_1 \in M_N$ folgt $m \in M_N$. ■

Korollar 6.1.7 Seien $M_1, \cdots, M_n$ eine Familie von noetherschen (bzw. artinschen) A-Moduln. Dann ist $\oplus_{k=1}^{n} M_k$ noethersch (bzw. artinsch).

Beweis. Folgt aus der obigen Proposition per Induktion nach n dank der exaten Sequenz $0 \to M_n \to \oplus_{k=1}^{n} M_k \to \oplus_{k=1}^{n-1} M_k \to 0$. ■

Definition 6.1.8 Ein Ring A heißt **noethersch** (bzw. **artinsch**) falls A noethersch (bzw. artinsch) als A-Modul ist.

Beispiel 6.1.9 1. Ein Körper ist noethersch und artinsch als Ring.

2. Ein Hauptideal ist noethersch. Z.B. $\mathbb{Z}$ oder $\mathsf{k}[X]$. Die Beide sind aber nicht artinsch.

3. Der Ring $\mathsf{k}[X_1, \cdots, X_n, \cdots]$ ist nicht noethersch und nicht artinsch.

Proposition 6.1.10 Sei M ein endlich erzeugter Modul. Es gilt

1. A noethersch $\Rightarrow$ M noethersch,

2. A artinsch $\Rightarrow$ M artinsch.

Beweis. Es gibt ein surjektiver Morphismus $A^n \to M$. Da A noethersch (bzw. artinsch) ist ist auch A^n noethersch (bzw. artinsch) und also auch M. ■

Korollar 6.1.11 Sei A ein noetherscher Ring. Es gilt

$$M \text{ noethersch } \Leftrightarrow M \text{ endlich erzeugt.}$$

Beweis. ($\Rightarrow$) Folgt aus der Definition von noethersch.

($\Leftarrow$) Folgt aus der obigen Proposition. ∎

Proposition 6.1.12 Sei A ein noetherscher (bzw. artinscher) Ring und $\mathfrak{a}$ ein Ideal. Dann ist $A/\mathfrak{a}$ ein noetherscher (bzw. artinscher) Ring.

Beweis. Es gibt ein surjektiver Morphismus $\pi : A \to A/\mathfrak{a}$. Ein Ideal $\bar{\mathfrak{b}}$ in $A/\mathfrak{a}$ ist das Bild $\pi(\mathfrak{b})$ von einem Ideal $\mathfrak{a} \subset \mathfrak{b} \subset A$. Aber $\mathfrak{b}$ ist endlich erzeugt als A-Modul also muss $\bar{\mathfrak{b}} = \pi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a}$ endlich erzeugt als $A/\mathfrak{a}$-Modul sein. ∎

6.2 Einfache Moduln und Länge

Definition 6.2.1 Ein Modul M heißt **einfach** falls der Nullmodul und M selber die einzige Untermoduln von M sind.

Definition 6.2.2 Sei M ein A-Modul.

1. Eine **Kette** von Untermoduln von M ist eine Folge $(M_i)_{i\in[0,n]}$ von Untermoduln mit

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0.$$

Die Zahl n ist die **Länge der Kette**.

2. Eine **vollständige Kette** von Untermoduln von M ist eine maximale Kette.

Lemma 6.2.3 Eine Kette $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ is genau dann maximal, wenn M_i/M_{i+1} einfach ist für alle i. □

Beweis. Übung. ∎

Proposition 6.2.4 Falls M eine maximale Kette der Länge n besitzt, dann sind alle maximale Ketten der Länge n. Außerdem kann jede Kette in eine maximale Kette ergänzt werden.

Beweis. Sei $\ell(M)$ die minimale Länge einer maximalen Kette.

Sei $N \subset M$ ein echter Untermodul. Wir zeigen $\ell(N) < \ell(M)$. Sei $M = M_n \supsetneq \cdots \supsetneq M_0 = 0$ eine maximale Kette. Dann ist $(N_i)_i$ mit $N_i = M_i \cap N$ eine Kette in N. Außerdem gilt $N_i/N_{i+1} \subset M_i/M_{i+1}$. Da M_i/M_{i+1} einfach ist gilt $N_i/N_{i+1} = 0$ oder $N_i/N_{i+1} = M_i/M_{i+1}$. Im ersten Fall gilt $N_{i+1} = N_i$. Im zweiten Fall ist N_i/N_{i+1} einfach. Wenn wir die N_{i+1} mit $N_{i+1} = N_i$ weglassen ist $(N_i)_i$ eine maximale Kette der Länge kleiner (oder gleich) die Länge von M. Es folgt $\ell(N) \leq \ell(M)$. Falls die beide übereinstimmen gilt, für $n = \ell(M)$ die Gleichung $N_i/N_{i+1} = M_i/M_{i+1}$ für alle i. Es folgt also $N_n = 0 = M_n$ und $N_{n-1} = N_{n-1}/N_n = M_{n-1}/M_n = M_{n-1}$. Per

Induktion zeigen wir $N_i = M_i$: es gibt ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd} 0 \arrow[r] & N_{i+1} \arrow[r] \arrow[d, equal] & N_i \arrow[r] \arrow[d] & N_i/N_{i+1} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & M_{i+1} \arrow[r] & N_i \arrow[r] & N_i/N_{i+1} \arrow[r] & 0 \end{tikzcd}$$

Es folgt aus dem schlangen Lemma, dass die Enthaltung $N_i \subset M_i$ ein Isomorphismus ist also $N_i = M_i$. Daraus folgt $N = M$ ein Widerspruch.

Sei n die Länge einer Kette. Wir zeigen jetzt, dass $n \leq \ell(M)$. Sei $M_0 = M \supsetneq \cdots \supsetneq M_n = 0$ eine Kette. Es gilt $\ell(M) > \ell(M_1) > \cdots > \ell(M_n) = 0$. Per Induktion folgt $\ell(M) \geq n$.

Es folgt, dass jede maximale Kette der Länge $\ell(M)$ ist.

Sei $M = M_n \supsetneq \cdots \supsetneq M_0 = 0$ eine Kette. Falls $n = \ell(M)$ ist die Kette schon maximal. Sonst können wir diese Kette erweitern. Per Induktion folgt, dass jede Kette zu einer maximalen Kette ergänzen werden kann. ∎

Proposition 6.2.5 Ein A-Modul hat genau dann eine vollständige Kette, wenn M beide Bedingungen (acc) und (dcc) erfüllt.

Beweis. ($\Rightarrow$) Alle Ketten sind endlich also erfüllt M (acc) und (dcc).

($\Leftarrow$) Wir konstruieren per Induktion eine vollständige Kette. Wegen (acc) gibt es einen maximalen Untermodul M_1 von M. Seien $M_1 \supsetneq \cdots \supsetneq M_n$ mit M_{i+1} maximal in M_i. Dann erfüllt M_n (acc) und damit hat ein maximalen Untermodul M_{n+1}. Damit haben eine Kette konstruirt und da M auch (dcc) erfüllt muss diese Kette endlich sein ($i.e.$ es gibt ein n mit $M_n = 0$. Damit haben wie eine vollständige Kette. ∎

Definition 6.2.6 Ein M Modul, der (acc) und (dcc) erfüllt heißt von **endlicher Länge**. Die Länge $\ell(M)$ einer vollständigen Kette heißt **Länge von** M.

Proposition 6.2.7 Sei M von endlicher Länge und seien $0 = M_n \subsetneq \cdots \subsetneq M_1 = M$ und $0 = M'_m \subsetneq \cdots \subsetneq M'_1 = M$ zwei vollständige Kette. Dann gilt $n = m$ und $M_i/M_{i+1} \simeq M'_i/M'_{i+1}$, modulo Vertauchen.

Beweis. Wir wissen schon, dass vollständige Kette die selbe Länge haben also $n = m$.

Sei $j = \max\{i \mid M_{n-1} \subset M'_i\}$. Dann gilt $M_{n-1} \cap M'_{j+1} \subsetneq M_1$ (sonst gilt $M_{n-1} \subset M'_{j+1}$ ein Widerspruch). Es folgt (die Ketten vollständig) $M'_{j+1} \cap M_{n-1} = 0$. Es gilt also $M'_{j+1} \subsetneq M'_{j+1} \oplus M_{n-1} \subset M'_j$. Daraus folgt (die Ketten vollständig) $M'_{j+1} \oplus M_{n-1} = M_j$. Es folgt $M_j/M_{j+1} \simeq M_{n-1}$.

Setze $N = M/M_{n-1}$, $N_i = M_i/M_{n-1}$ und $N'_i = (M'_i + M_{n-1})/M_{n-1} \simeq M'_i/(M'_i \cap M_{n-1})$. Es gilt $M_i/M_{i+1} \simeq (M_i/M_{n-1})/(M_{i+1}/M_{n-1}) = N_i/N_{i+1}$. Für $j \leq i$ gilt

$N'_i = M'_i/M_{n-1}$. Für $j > i$ gilt $N'_i \simeq M'_i/0 = M'_i$ und $N'_{j+1} = M'_{j+1} + M_{n-1}/M_{n-1} = M'_j/Mn - 1$.

Es gilt also $N'_i/N'_{i+1} = (M'_i/M_{n-1})/(M'_{i+1}/M_{n-1}) = M'_i/M'_{i+1}$ für $i \leq j-1$. Es gilt $N'_i/N'_{i+1} \simeq M'_i/M'_{i+1}$ für $i > j$ und $N'_j/N'_{j+1} = (M'_j/M_{n-1})/(M'_j/M_{n-1}) = 0$. Die Aussage folgt per Induktionsannahme für N. ■

Proposition 6.2.8 Die Länge ist eine addidive Funktion: Falls $0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ eine exakte Sequenz ist, gilt $\ell(M) = \ell(M') + \ell(M'')$.

Beweis. Seien $M' = M'_0 \supsetneq \cdots \supsetneq M'_n = 0$ und $M'' = M''_0 \supsetneq \cdots \supsetneq M''_m = 0$ vollständige Ketten. Dann ist

$$M = v^{-1}(M''_0) \supsetneq \cdots \supsetneq v^{-1}(M''_m) = \mathrm{Ker} v = \mathrm{Im} u = u(M') = u(M'_0) \supsetneq \cdots \supsetneq u(M'_n) = 0$$

eine Kette. Wir zeigen, dass diese Kette vollständig ist. Daraus folgt $\ell(M) = n+m = \ell(M') + \ell(M'')$.

Falls es ein Untermodul N mit $v^{-1}(M''_i) \supset N \supset v^{-1}(M''_{i+1})$ gibt, folgt $M''_i \supset v(N) \supset M''_{i+1}$ und also (vollständigkeit) $v(N) = M''_i$ oder $v(N) = M''_{i+1}$. Da $\mathrm{Ker} v \subset v^{-1}(M''_i) \subset N$ folgt $N = v^{-1}(M''_{i+1})$ oder $N = v^{-1}(M''_{i+1})$. Falls es ein Untermodul N mit $u(M'_i) \supset N \supset u(M'_{i+1})$ gibt, folgt (vollständigkeit) $N = u(M'_i)$ oder $N = u(M'_{i+1})$. ■

Proposition 6.2.9 Sei k ein Körper und V ein Vektorraum. Die folgende Eigenschaften sind äquivalent

a. $\dim_{\mathsf{k}}(V) < \infty$;

b. $\ell(V) < \infty$;

c. V hat (acc);

d. V hat (dcc).

Beweis. Übung. ■

Korollar 6.2.10 Sei A ein Ring so, dass es maximale Ideale $\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ gibt mit $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Dann gilt

$$A \text{ noethersch} \Leftrightarrow A \text{ artinsch}.$$

Beweis. Setze $I_k = \mathfrak{m}_1 \cdots \mathfrak{m}_k$ und betrachte die Kette $A \supset I_1 = \mathfrak{m}_1 \supset I_2 = \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset I_n = \mathfrak{m}_1 \cdots \mathfrak{m}_n = (0)$. Es gilt $I_k/I_{k+1} \simeq I_k/\mathfrak{m}_{k+1}I_k = I_k \otimes_A A/\mathfrak{m}_k$. Also ist I_k/I_{k+1} ist ein $A/\mathfrak{m}_{k+1}$-Vektorraum. Es folgt (acc) $\Leftrightarrow$ (dcc) für alle I_k/I_{k+1}. Daraus folgt (acc) $\Leftrightarrow$ (dcc) für A dank Proposition 6.1.6. ■

6.3 Noethersche Ringe

Proposition 6.3.1 Sei A ein Ring. Die folgende Aussagen sind äquivalent:

1. A ist noethersch.
2. Jede aufsteigende Kette von Idealen ist stationär.
3. Jede nicht leere Menge von Idealen hat ein maximales Element.
4. Jedes Ideal ist endlich erzeugt.

Beweis. Folgt aus der Definition von noethersch, aus Proposition 6.1.1 und Proposition 6.1.5. ∎

Lemma 6.3.2 Sei $f : A \to B$ ein surjektiver Ringhomomorphimus. Falls A noethersch ist, ist B auch noethersch. □

Beweis. Folgt direkt da $B \simeq A/\mathfrak{a}$ mit $\mathfrak{a} = \mathrm{Ker}(f)$. ∎

Proposition 6.3.3 Sei $A \subset B$ ein Unterring so, dass B endlich erzeugt als A-Modul ist. Falls A ein noetherscher Ring ist, ist auch B ein noetherscher Ring.

Beweis. B ist noethersch als A-Modul also auch als B-Modul. ∎

Proposition 6.3.4 Sei A ein noetherscher Ring und $S \subset A$ multiplikativ. Dann ist $S^{-1}A$ noethersch.

Beweis. Sei $\mathfrak{b}$ ein Ideal in $S^{-1}A$. Dann ist $\mathfrak{b}$ der Form $\mathfrak{b} = S^{-1}\mathfrak{a}$ mit $\mathfrak{a} = \lambda^{-1}\mathfrak{b}$, wobei $\lambda : A \to S^{-1}A$ die kanonische Abbildung ist. Es gibt Elemente $x_1, \cdots, x_n \in \mathfrak{a}$ so, dass $\mathfrak{a} = (x_1, \cdots, x_n)$. Wir zeigen, dass $\mathfrak{b} = (x_1/1, \cdots, x_n/1)$. Sei $a/s \in \mathfrak{b} = S^{-1}\mathfrak{a}$ mit $a \in \mathfrak{a}$ und $s \in S$. Es gibt $a_1, \cdots, a_n \in A$ mit $a = a_1x_1 + \cdots + a_nx_n$. Es folgt $as = a_1/sx_1/1 + \cdots + a_n/sx_n/1$. ∎

Korollar 6.3.5 Sei A noethersch und $\mathfrak{p}$ ein Primideal. Dann ist $A_\mathfrak{p}$ noethesch.

Satz 6.3.6 (Hilbertssatz) Sei A noethersch. Dann ist $A[X]$ noethersch. □

Beweis. Siehe Einführung in die algebraische Geometrie, Theorem 1.2.5. ∎

Korollar 6.3.7 Sei A noethersch. Dann ist $A[X_1, \cdots, X_n]$ noethersch.

Korollar 6.3.8 Sei B eine endlich erzeugte A-algebra mit A noethersch. Dann ist B noethersch.

Beweis. B ist der Form $A[X_1, \cdots, X_n]/I$, wobei I ein Ideal ist. ∎

Korollar 6.3.9 Sei B eine endlich erzeugter Ring oder eine endlich erzeugte k-Algebra mit k ein Körper. Dann ist B noethersch.

Proposition 6.3.10 Sei A ein noetherscher Ring und $\mathfrak{a} \subset A$ ein Ideal. Dann gibt es ein n mit $(\sqrt{\mathfrak{a}})^n \subset \mathfrak{a}$.

Beweis. Seien $x_1, \cdots, x_r$ so, dass $\sqrt{\mathfrak{a}} = (x_1, \cdots, x_r)$. Es gibt $k_1, \cdots, k_r$ mit $x_i^{k_i} \in \mathfrak{a}$. Sei $n = \sum_i (k_i - 1) + 1$. Das Ideal $(\sqrt{\mathfrak{a}})^n$ ist von alle Produkte $x_1^{i_1} \cdots x_r^{i_r}$ erzeugt, wobei $\sum_j i_j = n$. Es gibt aber ein j mit $i_j \geq k_j$ und also $x_1^{i_1} \cdots x_r^{i_r} \in \mathfrak{a}$. ■

Korollar 6.3.11 Sei A noethersch. Dann gibt es ein n mit $\mathfrak{n}(A)^n = 0$.

Beweis. Es gilt $\mathfrak{n}(A) = \sqrt{(0)}$. Die Aussage folgt aus der obigen Proposition. ■

6.4 Artinsche Ringe

Proposition 6.4.1 Sei A ein artinscher Ring und sei $\mathfrak{p}$ prim. Dann ist $\mathfrak{p}$ maximal.

Beweis. Sei $\mathfrak{p}$ prim. Dann ist $A/\mathfrak{p}$ ein artinscher Integritätsring. Sei $x \in A/\mathfrak{p}$ mit $x \neq 0$. Dann ist die Kette $A \supset (x) \supset \cdots \supset (x^n) \supset \cdots$ stationär. Es gibt also ein n mit $(x^n) = (x^{n+1})$. Es gilt also $x^n \in (x^{n+1})$ *i.e.* es gibt ein $y \in A$ mit $x^n = yx^{n+1}$. Es folgt $x^n(1 - xy) = 0$. Da $x \neq 0$ und $A/\mathfrak{p}$ Integritätsring folgt $1 - xy = 0$ und x ist invertierbar. Es folgt, dass $A/\mathfrak{p}$ ein Körper ist und also ist $\mathfrak{p}$ maximal. ■

Korollar 6.4.2 Sei A ein artinscher Ring. Dann gilt $\mathfrak{n}(A) = \mathfrak{R}(A)$ (wobei $\mathfrak{n}(A)$ das Nilradikal ist und $\mathfrak{R}(A)$ das Jacobson-Radikal ist).

Beweis. Folgt aus $\mathfrak{n}(A) = \cap_{\mathfrak{p} \text{ prim}} \mathfrak{p} = \cap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \mathfrak{R}(A)$. ■

Proposition 6.4.3 Ein artinscher Ring hat nur endlich viele maximale Ideale.

Beweis. Sei Σ die Menge aller endlichen Durchschnitte $\mathfrak{m}_1 \cap \cdots \mathfrak{m}_r$ mit $\mathfrak{m}_i$ maximal. Diese Menge hat ein minimales Element, weil A artinsch ist. Sei $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ ein minimales Element und sei $\mathfrak{m}$ ein maximales Ideal. Dann gilt $\mathfrak{m} \cap \mathfrak{m}_1 \cdots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$. Es folgt $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \subset \mathfrak{m}$. Aus dem Vermeidungslemma folgt, dass es ein i mit $\mathfrak{m}_i \subset \mathfrak{m}$. Da $\mathfrak{m}_i$ maximal ist folgt $\mathfrak{m}_i = \mathfrak{m}$ also sind $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ alle maximale Ideal von A. ■

Proposition 6.4.4 Sei A ein artinscher Ring. Dann gibt es ein n mit $\mathfrak{n}(A)^n = 0$.

Beweis. Die Kette $\mathfrak{n}(A) \supset \mathfrak{n}(A)^2 \supset \cdots \supset \mathfrak{n}(A)^n \supset \cdots$ ist stationär also gibt es ein n mit $\mathfrak{n}(A)^m = \mathfrak{n}(A)^n$ für alle $m \geq n$.

Angenommen $\mathfrak{n}(A)^n \neq 0$, sei $\Sigma = \{\mathfrak{a} \subset A \mid \mathfrak{a} \text{ Ideal und } \mathfrak{a}\mathfrak{n}(A)^n \neq 0\}$. Die Menge Σ ist nicht leer (z.B gilt $\mathfrak{a} = A \in \Sigma$). Da A artinsch ist gibt es ein $\mathfrak{b} \in \Sigma$ minimal. Es gibt also ein $x \in \mathfrak{b}$ mit $x\mathfrak{n}(A)^n \neq 0$ also $(x) \in \Sigma$. Es gilt aber $(x) \subset \mathfrak{b}$. Aus der Minimalität folgt $\mathfrak{b} = (x)$. Es gilt $(x\mathfrak{n}(A)^n)\mathfrak{n}(A)^n = x(\mathfrak{n}(A)^n\mathfrak{n}(A)^n) = x\mathfrak{n}(A)^{2n} = x\mathfrak{n}(A)^n \neq 0$ also $x\mathfrak{n}(A)^n \in \Sigma$. Es gilt aber $x\mathfrak{n}(A)^n \subset (x)$. Es folgt $(x) = x\mathfrak{n}(A)^n$. Es gibt also ein $y \in \mathfrak{n}(A)^n$ mit $x = xy$. Es folgt $x = xy^k$ für alle k. Da y nilpotent ist folgt $y^k = 0$ für ein k und $x = 0$. Ein Widerspruch. ∎

Satz 6.4.5 Sei A ein Ring. Es gilt

$$A \text{ artinsch} \Leftrightarrow A \text{ noethersch und } \operatorname{Kdim}(A) = 0.$$

Beweis. ($\Rightarrow$) Sei $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq A$ eine Kette von Primidealen. Da A artinsch ist, ist $\mathfrak{p}_0$ maximal. Es folgt $n = 0$ und $\operatorname{Kdim}(A) = 0$. Seien $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ die maximale Ideale von A (es sind nur endlich viele maximale Ideale). Dann gilt $\mathfrak{n}(A) = \mathfrak{R}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$. Es gibt aber ein n mit $\mathfrak{n}(A)^n = 0$ also gilt $\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n \subset (\mathfrak{m}_1 \cdots \mathfrak{m}_r)^n \subset (\mathfrak{m}_1 \cap \cdots \mathfrak{m}_r)^n = \mathfrak{n}(A)^n = 0$. Aus dem Korollar 6.2.10 folgt, dass A genau dann noethersch ist, wenn A artinsch ist. Daraus folgt die Aussage.

($\Leftarrow$) Wir setzen, dass (0) als Produkt von Primideal darstellbar ist. Sei

$$\Sigma = \{I \subset A \mid I \text{ ist ein Ideal und enthält kein endliches Produkt von Primidealen}\}.$$

Falls $\Sigma \neq \emptyset$, hat Σ ein maximales Element I. Dann ist I kein Primideal also es gibt $x, y \in A$ mit $xy \in I$ und $x, y \notin I$. Seien $J = I + (x)$ und $K = I + (y)$. Es gilt $I \subsetneq J$ und $I \subsetneq K$ also sind J und K nicht in Σ. Es gibt also Primideale $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ und $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ so, dass $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J$ und $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset K$. Aber es gilt $JK \subset I^2 + xI + yI + (xy) \subset I$. Es folgt $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I$ und $I \notin \Sigma$. Ein Widerspruch. Es folgt, dass jedes Ideal ein endliches Produkt von Primidealen enthält. Insbesondere gibt es Primideale $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ so, dass $\mathfrak{m}_1 \cdots \mathfrak{m}_r \subset (0)$. Es folgt $\mathfrak{m}_1 \cdots \mathfrak{m}_r = (0)$. Aber da $\operatorname{Kdim}(A) = 0$ sind alle Primideale maximal: für $\mathfrak{p}$ prim gibt es $\mathfrak{m}$ maximal mit $\mathfrak{p} \subset \mathfrak{m}$ und dank $\operatorname{Kdim}(A) = 0$ folgt $\mathfrak{p} = \mathfrak{m}$ maximal. Also sind die Ideale $\mathfrak{m}_1 \cdots, \mathfrak{m}_r$ maximal. Aus dem Korollar 6.2.10 folgt, dass A genau dann artinsch ist, wenn A noethersch ist. Daraus folgt die Aussage. ∎

Lemma 6.4.6 Sei A ein lokaler artinscher Ring mit maximalem Ideal $\mathfrak{m}$. Dann gilt

1. $\mathfrak{m}$ ist das einzige Primideal.

2. $\mathfrak{m} = \mathfrak{n}(A) = \mathfrak{R}(A)$.

3. Jedes Element in A ist entweder nilpotent oder invertierbar. □

Beweis. 1. Da A artinsch ist sind alle Primideale maximal. Da es nur ein maximales Ideal gibt, folgt die Aussage.

2. Wir wissen schon, dass $\mathfrak{n}(A) = \mathfrak{R}(A)$. Aus 1. folgt $\mathfrak{n}(A) = \cap_{\mathfrak{p}\text{ prim}}\mathfrak{p} = \mathfrak{m}$.

3. Sei x nicht invertierbar. Dann gilt $x \in \mathfrak{m} = \mathfrak{n}(A)$ also ist x nilpotent. ∎

Beispiel 6.4.7 Der Ring $\mathbb{Z}/p^n\mathbb{Z}$ ist artinsch und lokal.

Proposition 6.4.8 Sei A ein lokaler noetherscher Ring und $\mathfrak{m}$ sein maximales Ideal. Dann gilt genau genau eine der folgenden Aussagen:

1. $\mathfrak{m}^n \supsetneq \mathfrak{m}^{n+1}$ für alle $n \geq 0$.
2. Es gibt ein n mit $\mathfrak{m}^n = 0$ und A ist artinsch.

Beweis. Falls $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ gilt $M = \mathfrak{m}M$ mit $M = \mathfrak{m}^n$. Da M endlich erzeugt ist (A ist noethersch) folgt aus Nakayama, dass $\mathfrak{m}^n = M = 0$. Wir zeigen jetzt, dass A artinsch ist. Sei $\mathfrak{p}$ ein Primideal. Es gilt $\mathfrak{m}^n = (0) \subset \mathfrak{p}$ also $\mathfrak{m} = \sqrt{\mathfrak{m}} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$ und $\mathfrak{p}$ ist maximal. Es folgt $\mathrm{Kdim}(A) = 0$ und A ist noethersch. ∎

Bemerkung 6.4.9 In der obigen Proposition, im zweiten Fall, für n minimal mit $\mathfrak{m}^n = (0)$ gilt $\mathfrak{m}^k \supsetneq \mathfrak{m}^{k+1}$ für alle $k < n$.

Satz 6.4.10 (Struktursatz der artinschen Ringe) Sei A ei artinscher Ring. Dann gibt es eindeutig bestimmte (modulo Vertauschen) lokale artinsche Ringe $A_1, \cdots, A_r$ so, dass

$$A = A_1 \times \cdots \times A_r.$$

Beweis. Seien $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ die maximale Ideale in A. Es gilt $\mathfrak{m}_1 \cdots \mathfrak{m}_r \subset \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathfrak{n}(A)$. Also gibt es ein n mit $\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n = (\mathfrak{m}_1 \cdots \mathfrak{m}_r)^n \subset \mathfrak{n}(A)^n = 0$.

Es gilt $\sqrt{\mathfrak{m}_i^n} + \sqrt{\mathfrak{m}_j^n} = \mathfrak{m}_i + \mathfrak{m}_j = A$ für $i \neq j$. Aus Übungsblatt 2 Aufgabe 1.5 folgt $\mathfrak{m}_i^n + \mathfrak{m}_j^n = A$ also sind diese Ideale Teilerfremd. Aus dem chinesischem Restsatz folgt $\mathfrak{m}_1^n \cdots \mathfrak{m}_r^n = \mathfrak{m}_1^n \cap \cdots \cap \mathfrak{m}_r^n$ und

$$A \simeq A/\mathfrak{m}_1^n \times \cdots \times A/\mathfrak{m}_r^n.$$

Wir zeigen, dass $A/\mathfrak{m}_i^n$ lokal und artinsch ist. Da dieser Ring ein Quotient von einem artinschen Ring ist, ist der Ring artinsch. Sei $\bar{\mathfrak{m}}$ maximal in $A/\mathfrak{m}_i^n$. Dann ist $\mathfrak{m} = \pi^{-1}(\bar{\mathfrak{m}})$ maximal mit $\mathfrak{m}_i^n \subset \mathfrak{m}$, wobei $\pi : A \to A/\mathfrak{m}_i^n$ die kanonische Projektion ist. Es folgt $\mathfrak{m} = \sqrt{\mathfrak{m}} \supset \sqrt{\mathfrak{m}_i^n} = \mathfrak{m}_i$ und also $\mathfrak{m} = \mathfrak{m}_i$. Daraus folgt $\bar{\mathfrak{m}} = \pi(\mathfrak{m}_i)$ und $A/\mathfrak{m}_i^n$ hat nur ein maximales Ideal und also ist lokal.

Umgekehrt, seien $A_1, \cdots, A_r$ lokale artinsche Ringe mit $A \simeq A_1 \times \cdots \times A_r$. Es gilt $A = \oplus_i A_i$ als A-Modul und alle A_i sind als A-Modul artinsch also ist A artinsch. Wir zeigen, dass die A_i durch A eindeutig bestimmt sind.

Sei $\varphi_i : A \to A_i$ die kanonische Projektion, sei $\mathfrak{a}_i = \mathrm{Ker}\varphi_i$, sei $\bar{\mathfrak{m}}_i$ das maximale Ideal in A_i und sei $\mathfrak{m}_i = \varphi_i^{-1}(\bar{\mathfrak{m}}_i)$. Da φ_i surjektiv ist, ist $\mathfrak{m}_i$ maximal. Nach dem chinesischem Restsatz gilt: $\mathfrak{a}_i$ und $\mathfrak{a}_j$ sind teilerfremd für alle $i \neq j$ also $A = \mathfrak{a}_i + \mathfrak{a}_j \subset \mathfrak{m}_i + \mathfrak{m}_j$ und $\mathfrak{m}_i \neq \mathfrak{m}_j$. Nach dem chinesischen Restsatz gilt auch $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = (0)$. Sei $\mathfrak{m}$ maximal. Es gilt $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r = (0) \subset \mathfrak{m}$ also gibt es ein i mit $\mathfrak{a}_i \subset \mathfrak{m}$ (Vermeidungslemma) und $\varphi_i(\mathfrak{m}) = \mathfrak{m}/\mathfrak{a}_i$ ist maximal also $\varphi_i(\mathfrak{m}) = \bar{\mathfrak{m}}_i$ und $\mathfrak{m} \subset \mathfrak{m}_i$. Es folgt $\mathfrak{m} = \mathfrak{m}_i$. Die Ideale $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ sind also die maximale Ideale von A.

Wir zeigen jetzt, dass es für jedes i ein $n_i \in \mathbb{N}$ gibt mit $\mathfrak{m}_i^k \supsetneq \mathfrak{m}_i^{k+1}$ für $k < n_i$ und $\mathfrak{m}_i^k = \mathfrak{m}_i^{n_i}$ für alle $k \geq n_i$ und auch, dass $\mathfrak{a}_i = \mathfrak{m}_i^{n_i}$. Daraus folgt $A_i \simeq A/\mathfrak{a}_i = A/\mathfrak{m}_i^{n_i}$ und die A_i sind eindeutig durch A bestimmt.

Es gilt $\varphi_i(\mathfrak{m}_i) = \bar{\mathfrak{m}}_i$ und nach dem obigen Proposition gibt es ein n_i mit $\bar{\mathfrak{m}}_i^k \supsetneq \bar{\mathfrak{m}}_i^{k+1}$ für $k < n_i$ und $\bar{\mathfrak{m}}_i^k = \bar{\mathfrak{m}}_i^{n_i} = (0)$ für alle $k \geq n_i$. Es folgt $\mathfrak{m}_i^k \supsetneq \mathfrak{m}_i^{k+1}$ für $k < n_i$ und $\varphi_i(\mathfrak{m}_i^k) \subset \bar{\mathfrak{m}}_i^k = (0)$ für alle $k \geq n_i$: Es folgt $\mathfrak{m}_i^k \subset \mathfrak{a}_i$ für alle $k \geq n_i$. Sei $x_i = (1, \cdots, 1, 0, 1, \cdots, 1)$, wobei die 0 an der i-te Stelle ist. Es gilt $(x_i) = \mathfrak{a}_i$ und also $x_i \in \mathfrak{m}_i$. Es folgt $\mathfrak{a}_i = (x_i) = (x_i^k) \subset \mathfrak{m}_i^k$ also $\mathfrak{a}_i \subset \mathfrak{m}_i^k$ für alle k. Daraus folgt $\mathfrak{m}_i^k = \mathfrak{m}_i^{n_i} = \mathfrak{a}_i$ für alle $k \geq n_i$ und die Aussage. ∎

Lemma 6.4.11 Sei A ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{m}$ und sei $\mathsf{k} = A/\mathfrak{m}$ der Restklassenkörper. Dann ist $\mathfrak{m}/\mathfrak{m}^2$ ein endlich dimensionaler Vektorraum. □

Beweis. Es gilt $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{m} \otimes_A A/\mathfrak{m} = \mathfrak{m} \otimes_A \mathsf{k}$. Da $\mathfrak{m}$ ein endlich erzeugter Modul ist, ist auch $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{m} \otimes_A \mathsf{k}$ ein endlich erzeugter k-Modul also ein endlich dimensionaler k-Vektorraum. ∎

Proposition 6.4.12 Sei A ein artinscher lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und $\mathsf{k} = A/\mathfrak{m}$ der Restklassenkörper. Die folgende Aussagen sind äquivalent:

1. A ist ein Hauptidealring.
2. $\mathfrak{m}$ ist ein Hauptideal.
3. $\dim_{\mathsf{k}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

Beweis. (1. $\Rightarrow$ 2.) Klar.

(2. $\Rightarrow$ 3.) Sei $x \in A$ mit $(x) = \mathfrak{m}$. Dann ist $[x] \in \mathfrak{m}/\mathfrak{m}^2$ ein Erzeuger von $\mathfrak{m}/\mathfrak{m}^2$ als k-Vektorraum.

(3. $\Rightarrow$ 1.) Da $\dim_{\mathsf{k}}(\mathfrak{a}/\mathfrak{m}) \leq 1$, gibt es ein $x \in \mathfrak{m}$ so, dass $[x]$ erzeugend in $\mathfrak{m}/\mathfrak{m}^2$ ist. Nach Korollar 2.7.5 ist x erzeugend für $\mathfrak{m}$ als A-Modul also $\mathfrak{m} = (x)$.

Wir zeigen, dass jedes Ideal $\mathfrak{a}$ der Form $\mathfrak{a} = (x^n)$ ist oder $\mathfrak{a} = (0)$. Für $\mathfrak{a} = A$ gilt $\mathfrak{a} = (1) = (x^0)$. Sei $\mathfrak{a} \neq (0)$.

Es gilt $\mathfrak{a} \subset \mathfrak{m}$. Das Ideal $\mathfrak{m}$ ist aber nilpotent also gibt es ein k mit $\mathfrak{m}^k = 0 \subset \mathfrak{a}$. Sei n minimal mit $\mathfrak{a} \subset \mathfrak{m}^n$ aber $\mathfrak{m}^n \not\subset \mathfrak{a}$. Dies ist möglich, weil $\mathfrak{a} \neq (0)$. Sei $y \in \mathfrak{a} \setminus \mathfrak{m}^{n+1}$.

Da $\mathfrak{m} = (x)$ gilt $\mathfrak{m}^n = (x^n)$. Es gilt also $y = ax^n$ für ein $a \in A$ und $y \notin (x^{n+1})$. Daraus folgt $a \notin (x) = \mathfrak{m}$ und also a ist invertierbar. Es folgt $x^n = a^{-1}y \in \mathfrak{a}$ und $\mathfrak{a} = (x^n) = \mathfrak{m}^n$. ■

Bemerkung 6.4.13 In der obigen Proposition, für $\dim_{\mathsf{k}}(\mathfrak{m}/\mathfrak{m}^2) = 0$ gilt $\mathfrak{m} = \mathfrak{m}^2$ und also $\mathfrak{m} = 0$ nach Nakayama. Es folgt, dass A ein Körper ist.

7 Primäre Zerlegung

In einem Ring gibt es eine Primzahzerlegung sobald der Ring faktoriel ist. Es gibt aber sehr einfache nicht faktoriele Ringe. Zum Beispiel ist der Ring $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ nicth faktoriel: es gibt zwei Primzahlzerlegungen von 9:

$$3 \times 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5}).$$

Wir werden aber sehen, dass es eine solche Zerlegung für Ideale gibt sobald der Ring noethersch ist.

7.1 Primäre Ideale

Definition 7.1.1 Ein Ideal $\mathfrak{a} \subset A$ heißt **primär** falls $\mathfrak{a} \subsetneq A$ und gilt $(xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a}$ oder $\exists\ n$ mit $y^n\mathfrak{a})$ für alle $x, y \in A$.

Bemerkung 7.1.2 1. Primideale sond primär.

2. Ein Ideal $\mathfrak{a}$ ist genau dann primär, wenn $A/\mathfrak{a} \neq 0$ und jeder Nullteiler in $A/\mathfrak{a}$ ist nilpotent.

Lemma 7.1.3 Sei $f : A \to B$ ein Ringhomomorphismus mit $\mathfrak{b} \subset B$ primär. Dann ist $f^{-1}(\mathfrak{b})$ primär. □

Beweis. Der Ring $A/f^{-1}(\mathfrak{b})$ ist ein Unterring von $B/\mathfrak{b}$. Daraus folgt die Aussage. ■

Proposition 7.1.4 Sei $\mathfrak{a} \subset A$ primär. Dann ist $\sqrt{\mathfrak{a}}$ ein Primideal und dieses Ideal ist das kleineste Primideal, das $\mathfrak{a}$ umfast.

Beweis. Seien $x, y \in A$ mit $xy \in \sqrt{\mathfrak{a}}$ und $x \notin \mathfrak{a}$. Dann gibt es ein n mit $x^n y^n = (xy)^n \in \mathfrak{a}$. Dann gilt $x^n \in \mathfrak{a}$ oder es gibt ein m mit $y^{nm} \in \mathfrak{a}$. Es folgt $x \in \sqrt{\mathfrak{a}}$ oder $y \in \sqrt{\mathfrak{a}}$.

Sei jetzt $\mathfrak{p}$ ein Primideal mit $\mathfrak{a} \subset \mathfrak{p}$ und sei $x \in \sqrt{\mathfrak{a}}$. Dann gibt es ein n mit $x^n \in \mathfrak{a} \subset \mathfrak{p}$ also $x \in \mathfrak{p}$. ■

Definition 7.1.5 Sei $\mathfrak{a}$ primär und $\mathfrak{p} = \sqrt{\mathfrak{a}}$ sein Radikal (ein ist ein Primideal). In diesem Fall heißt $\mathfrak{a}$ **$\mathfrak{p}$-primär**.

Beispiel 7.1.6 1. Die primäre Ideale von $\mathbb{Z}$ sind (0) und (p^n) für p eine Primzahl.

2. Sei $\mathfrak{a} = (X, Y^3) \subset \mathsf{k}[X, Y]$. Dann gilt $\mathsf{k}[X, Y]/\mathfrak{a} \simeq \mathsf{k}[Y]/(Y^3)$ und die Nullteiler sind nilpotent. Also ist $\mathfrak{a}$ primär. Es gilt $\mathfrak{p} = \sqrt{\mathfrak{a}} = (X, Y)$ und $\mathfrak{p}^3 \subsetneq \mathfrak{a} \subsetneq \mathfrak{p}$. Es gilt auch $\mathfrak{a} \neq \mathfrak{p}^2$ also sind primäre Idale nicht immer Potenze von Primidealen.

3. Eine Potenze von einem Primideal ist auch nicht immer primär. Z.B. $\mathfrak{p} = (XY - Z^2)$ ist ein Primideal in $\mathsf{k}[X, Y, Z]$. Sei $A = \mathsf{k}[X, Y, Z]/(XY - Z^2)$ und sei $\mathfrak{p} = ([X], [Z]) \subset A$. Es gilt $A/\mathfrak{p} \simeq \mathsf{k}[Y]$ also ist $\mathfrak{p}$ prim. Es gilt aber $[X][Y] = [Z^2] \in \mathfrak{p}^2$ aber $[X] \notin \mathfrak{p}^2$ und $[Y]^n \not\in \mathfrak{p}^2$ für alle n: sonst gilt $[Y] \in \sqrt{\mathfrak{p}^2} = \mathfrak{p}$ Widerspruch.

Proposition 7.1.7 Falls $\sqrt{\mathfrak{a}}$ maximal ist, ist $\mathfrak{a}$ primär. Insbesondere, die Potenze von einem maximalen Ideal $\mathfrak{m}$ sind $\mathfrak{m}$-primär.

Beweis. Sei $\mathfrak{m} = \sqrt{\mathfrak{a}}$ maximal. Es gilt $\sqrt{\mathfrak{a}}/\mathfrak{a} = \mathfrak{n}(A/\mathfrak{a})$. Es folgt $\mathfrak{m}/\mathfrak{a} = \cap_{\mathfrak{p} \text{ prim} \subset A/\mathfrak{a}} \mathfrak{p}$. Da $\mathfrak{m}/\mathfrak{a}$ ein maximales Ideal also auch Primideal von $A/\mathfrak{a}$ ist, folgt $\mathfrak{m}/\mathfrak{a} \subset \mathfrak{p}$ für alle Primideale $\mathfrak{p}$ von $A/\mathfrak{a}$. Da $\mathfrak{m}/\mathfrak{a}$ maximal ist gilt $\mathfrak{p} = \mathfrak{m}/\mathfrak{a}$ und $A/\mathfrak{a}$ hat nur ein maximales Ideal: $\mathfrak{m}/\mathfrak{a}$. Dieser Ring ist also lokal und $\mathfrak{m}/\mathfrak{a} = \mathfrak{n}(A/\mathfrak{a})$. Ein Element in $A/\mathfrak{a}$ ist also entweder invertierbar (in $A/\mathfrak{a} \setminus \mathfrak{m}/\mathfrak{a}$) oder nilpotent (in $\mathfrak{m}/\mathfrak{a}$).

Für $\mathfrak{m}$ maximal gilt $\sqrt{\mathfrak{m}^n} = \mathfrak{m}$. Daraus folgt die letzte Aussage. ∎

Lemma 7.1.8 Sei $\mathfrak{p}$ ein Primideal und seien $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ $\mathfrak{p}$-primäre Ideale. Dann ist $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ $\sqrt{\mathfrak{p}}$-primär. □

Beweis. Es gilt $\sqrt{\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n} = \sqrt{\mathfrak{a}_1} \cap \cdots \cap \sqrt{\mathfrak{a}_n} = \mathfrak{p} \cap \cdots \cap \mathfrak{p} = \mathfrak{p}$. Seien $x, y \in A$ mit $xy \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ und $x \notin \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Dann gibt es ein i mit $xy \in \mathfrak{a}_i$ und $x \notin \mathfrak{a}_i$. Es folgt, dass es ein k gibt mit $y^k \in \mathfrak{a}_i \subset \mathfrak{p} = \sqrt{\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n}$. Es gibt also ein m mit $y^{km} \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. ∎

Lemma 7.1.9 Sei $\mathfrak{a}$ ein $\mathfrak{p}$-primäres Ideal und $x \in A$. Dann gilt

1. $x \in \mathfrak{a} \Rightarrow (\mathfrak{a} : x) = A$.

2. $x \notin \mathfrak{a} \Rightarrow (\mathfrak{a} : x)$ ist $\mathfrak{p}$-primär und $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}$.

3. $x \notin \mathfrak{p} \Rightarrow (\mathfrak{a} : x) = \mathfrak{a}$. □

Beweis. 1. Folgt aus der Definition von $(\mathfrak{a} : x) = \{a \in A \mid ax \in \mathfrak{a}\}$.

2. Seien $a, b \in A$ mit $ab \in (\mathfrak{a} : x)$ also $abx \in \mathfrak{a}$. Falls $a \notin (\mathfrak{a} : x)$, gilt $ax \notin \mathfrak{a}$ und also gibt es ein n mit $b^n \in \mathfrak{a}$. Es folgt $b^n \in (\mathfrak{a} : x)$ und $(\mathfrak{a} : x)$ ist primär.

Wir zeigen $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}$. Sei $a \in \sqrt{(\mathfrak{a} : x)}$. Dann gibt es ein n mit $a^n \in (\mathfrak{a} : x)$ also mit $a^n x \in \mathfrak{a}$. Da $x \notin \mathfrak{a}$ folgt, dass es ein m gibt mit $a^{nm} \in \mathfrak{a}$ also $a \in \sqrt{\mathfrak{a}} = \mathfrak{p}$. Sei $a \in \mathfrak{p}$. Dann gibt es ein n mit $a^n \in \mathfrak{a}$ und also $a^n x \in \mathfrak{a}$. Es folgt $a^n \in (\mathfrak{a} : x)$ und die Aussage.

3. Die Enthaltung $\mathfrak{a} \subset (\mathfrak{a} : x)$ ist immer wahr. Sei $a \in (\mathfrak{a} : x)$ also $ax \in \mathfrak{a}$. Da $x^n \notin \mathfrak{p}$ für alle n folgt $y \in \mathfrak{a}$. ∎

7.2 Primäre Zerlegung

Definition 7.2.1 Sei $\mathfrak{a}$ ein Ideal.

1. Eine **primäre Zerlegung** von $\mathfrak{a}$ ist ein Darstellung von $\mathfrak{a}$ als endlichen Durchschnitt von primären Idealen:

$$\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$$

mit $\mathfrak{a}_i$ primär für alle i. Wenn $\mathfrak{a}$ eine primäre Zerlegung hat heißt $\mathfrak{a}$ **zerlegbar**.

2. Wenn die Ideale $\sqrt{\mathfrak{a}_i}$ paarweise verschieden sind und es gilt

$$\bigcap_{j \neq i} \mathfrak{a}_j \not\subset \mathfrak{a}_i \text{ für alle } i, j$$

heißt die obige Zerlegung **minimal**.

Bemerkung 7.2.2 Dank dem Lemma 7.1.8, kann man die Ideale $\mathfrak{a}_{i_1}, \cdots, \mathfrak{a}_{i_k}$ durch $\mathfrak{a}_{i_1} \cap \cdots \cap \mathfrak{a}_{i_k}$ ersetzen und die erste Bedingung von minimalen Zerlegungen ist erfüllt.

Satz 7.2.3 (Eindeutigkeit 1) Sei $\mathfrak{a}$ zerlegbar und sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ eine minimale primäre Zerlegung von $\mathfrak{a}$. Let $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Dann sind die Ideale $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ genau die Primideale, die in der Familie $(\sqrt{(\mathfrak{a} : x)})_{x \in A}$ auftauchen. Insbesondere hängt diese Menge nur von A ab und nicht von der Wahl der Zerlegung. □

Beweis. Sei $x \in A$. Es gilt $(\mathfrak{a} : x) = (\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n : x) = (\mathfrak{a}_1 : x) \cap \cdots \cap (\mathfrak{a}_n : x)$ und also $\sqrt{(\mathfrak{a} : x)} = \sqrt{(\mathfrak{a}_1 : x)} \cap \cdots \cap \sqrt{(\mathfrak{a}_n : x)}$. Es gilt aber $\sqrt{(\mathfrak{a}_i : x)} = \mathfrak{p}_i$ für $x \notin \mathfrak{a}_i$ und $\sqrt{(\mathfrak{a}_i : x)} = A$ für $x \in \mathfrak{a}_i$. Es folgt

$$\sqrt{(\mathfrak{a} : x)} = \bigcap_{x \notin \mathfrak{a}_i} \mathfrak{p}_i.$$

Falls $\sqrt{(\mathfrak{a} : x)}$ prim ist, folgt aus dem Vermeidungslemma, dass es ein i gibt mit $\mathfrak{p}_i = \sqrt{(\mathfrak{a} : x)}$.

Umgekehrt, da die Zerlegung minimal ist gibt es für jedes i ein $x \in \cap_{j \neq i} \mathfrak{a}_j$ mit $x \notin \mathfrak{a}_i$. Es gilt also $\sqrt{(\mathfrak{a}_i : x)} = \mathfrak{p}_i$ und $\sqrt{(\mathfrak{a}_j : x)} = A$ für $j \neq i$. Daraus folgt $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_i$. Das Ideal $\sqrt{(\mathfrak{a} : x)}$ is sogar $\mathfrak{p}_i$-primär. ■

Beispiel 7.2.4 1. Sei $\mathfrak{a} = (X(X-1), XY) \subset A = \mathsf{k}[X, Y]$. Es gilt $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2$, wobei $\mathfrak{p}_1 = (X)$ ist prim und $\mathfrak{p}_2 = (X-1, Y)$ ist maximal.

Es gilt $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}_1 \cap \mathfrak{p}_2} = \sqrt{\mathfrak{p}_1} \cap \sqrt{\mathfrak{p}_2} = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{a}$.

2. Sei $\mathfrak{a} = (X(X-t), XY) \subset A = \mathsf{k}[X, Y]$ mit $t \neq 0$. Es gilt $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2$, wobei $\mathfrak{p}_1 = (X)$ ist prim und $\mathfrak{p}_2 = (X-t, Y)$ ist maximal.

Es gilt $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}_1 \cap \mathfrak{p}_2} = \sqrt{\mathfrak{p}_1} \cap \sqrt{\mathfrak{p}_2} = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{a}$.

3. Sei $\mathfrak{a} = (X^2, XY) \subset A = \mathsf{k}[X,Y]$. Es gilt $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$, wobei $\mathfrak{p}_1 = (X)$ ist prim und $\mathfrak{p}_2 = (X, Y)$ ist maximal.

In diesem Fall gilt $\mathfrak{p}_1 \subset \mathfrak{p}_2$ und $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}_1 \cap \mathfrak{p}_2^2} = \sqrt{\mathfrak{p}_1} \cap \sqrt{\mathfrak{p}_2^2} = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$. Das Ideal $\mathfrak{a}$ ist nicht $\mathfrak{p}_1$-primär: es gilt $XY \in \mathfrak{a}$ aber $X \notin \mathfrak{a}$ und $Y^k \notin \mathfrak{a}$ für alle k.

Definition 7.2.5 Sei $\mathfrak{a}$ zerlegbar.

1. Die Primideale, die in der Familie $(\sqrt{(\mathfrak{a} : x)})_{x \in A}$ auftauchen heißen **die assoziierte Primideale von $\mathfrak{a}$**. Diese Menge ist $\mathrm{Ass}(\mathfrak{a})$ oder $\mathrm{Ass}(A/\mathfrak{a})$ bezeichnet.

2. Falls $\mathfrak{p}$ ein minimales assoziiertes Primideal von $\mathfrak{a}$ ist, heißt $\mathfrak{p}$ **minimales assoziiertes Primideal von $\mathfrak{a}$**.

2. Falls $\mathfrak{p}$ ein nicht minimales assoziiertes Primideal von $\mathfrak{a}$ ist, heißt $\mathfrak{p}$ **eingebettetes assoziiertes Primideal von $\mathfrak{a}$**.

Bemerkung 7.2.6 Wenn man $A/\mathfrak{a}$ als A-Modul betrachtet sind die assoziierte Primideale von $\mathfrak{a}$ genau die Primideale der Form $\sqrt{\mathrm{Ann}(x)}$, wobei $x \in A/\mathfrak{a}$.

Definition 7.2.7 Sei M ein A-Modul.

1. Die Primideale, die in der Familie $(\sqrt{(\mathrm{Ann}(x))})_{x \in M}$ auftauchen heißen **die assoziierte Primideale von M**. Diese Menge ist $\mathrm{Ass}(M)$ bezeichnet.

2. Falls $\mathfrak{p}$ ein minimales assoziiertes Primideal von M ist, heißt $\mathfrak{p}$ **minimales assoziiertes Primideal von M**.

2. Falls $\mathfrak{p}$ ein nicht minimales assoziiertes Primideal von M ist, heißt $\mathfrak{p}$ **eingebettetes assoziiertes Primideal von M**.

Proposition 7.2.8 Sei $\mathfrak{a}$ zerlegbar und sei $\mathfrak{p}$ prim mit $\mathfrak{a} \subset \mathfrak{p}$. Dann enthält $\mathfrak{p}$ ein minimales assoziiertes Ideal von $\mathfrak{a}$.

Insbesondere sind die minimale assoziierte Ideale von $\mathfrak{a}$ die minimale Primideale die $\mathfrak{a}$ enthalten.

Beweis. Sei $\mathfrak{p} \supset \mathfrak{a}$ prim und sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Dann gilt $\cap_i \mathfrak{p}_i = \cap_i \sqrt{\mathfrak{a}_i} = \sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$. Nach dem Vermeidungslemma gilbt es ein i mit $\mathfrak{p}_i \subset \mathfrak{p}$. ∎

Beispiel 7.2.9 Sei $\mathfrak{a} = (X^2, XY) \subset \mathsf{k}[X,Y]$. Dann sind $\mathfrak{a} = (X) \cap (X,Y)^2 = (X) \cap (X^2, Y)$ zwei verschiedene primäre Zerlegungen. Die Zerlegung ist also nicht eindeutig. Nur die assozzierte Primideale sind eindeutig bestimmt. In dem Fall (X) und (X, Y).

Beispiel 7.2.10 In $\mathbb{Z}[i\sqrt{5}]$ hat das Ideal $\mathfrak{a} = (9)$ die primäre Zerlegung (übung):

$$(9) = (3, 2 + i\sqrt{5}) \cap (3, 2 - i\sqrt{5}).$$

Proposition 7.2.11 Sei $\mathfrak{a}$ zerlegbar und sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ für alle i. Dann gilt

$$\bigcup_{i=1}^{r} \mathfrak{p}_i = \{x \in A \mid (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

Insbesondere, falls das Nullideal (0) zerlegbar ist, ist die Menge N aller Nullteiler die Vereinigung aller assoziierten Primideale von (0) (verg. mit Übungsblatt 1 Aufgabe 4.2).

Beweis. Für jedes i gibt es ein $x_i \in A$ mit $\mathfrak{p}_i = \sqrt{(\mathfrak{a} : x_i)}$. Sei $x \in \mathfrak{p}_i$. Es gilt immer $\mathfrak{a} \subset (\mathfrak{a} : x)$. Wir zeigen, dass $(\mathfrak{a} : x) \supsetneq \mathfrak{a}$. Es gibt ein n mit $x^n \in (\mathfrak{a} : x_i)$ also $x^n x_i \in \mathfrak{a}$. Insbesondere gilt $x^{n-1}x_i \in (\mathfrak{a} : x)$. Falls $x^{n-1}x_i \notin \mathfrak{a}$ sind wir fertig. Sonst gilt $x^{n-1}x_i \in \mathfrak{a}$ und $x^{n-2}x_i \in (\mathfrak{a} : x)$. Per Induktion folgt $\mathfrak{a} \subsetneq (\mathfrak{a} : x)$ oder $x_i \in \mathfrak{a}$. In disem Fall folgt $(\mathfrak{a} : x_i) = A$ und $\mathfrak{p}_i = \sqrt{(\mathfrak{a} : x_i)} = A$. Ein Widerspruch, weil $\mathfrak{p}_i$ prim ist.

Umgekehrt, sei $x \in A$ mit $(\mathfrak{a} : x) \supsetneq \mathfrak{a}$. Dann gibt es ein $y \in A \setminus \mathfrak{a}$ mit $xy \in \mathfrak{a}$. Es folgt $x \in (\mathfrak{a} : y)$. Es gilt $(\mathfrak{a} : y) = (\cap_i \mathfrak{a}_i : y) = \cap_i (\mathfrak{a}_i : y)$. Es folgt $\sqrt{(\mathfrak{a} : y)} = \cap_i \sqrt{(\mathfrak{a}_i : y)} = \cap_{i,\ y \notin \mathfrak{a}_i} \mathfrak{p}_i$. Da $y \notin \mathfrak{a}$, gibt es ein i mit $y \notin \mathfrak{a}_i \subset \mathfrak{p}_i$ und also $x \in \sqrt{(\mathfrak{a} : y)} \subset \mathfrak{p}_i$.

Sobald die erste Aussage war ist, gilt für $\mathfrak{a} = (0)$: $\cup_i \mathfrak{p}_i = \{x \mid \mathrm{Ann}(x) \neq 0\} = D$. ∎

Korollar 7.2.12 Sei A ein Ring so, dass (0) zerlegbar ist. Sei D die Menge aller Nulteiler. Es gilt

$$D = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p} \text{ und } \mathfrak{n}(A) = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(A)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(A),\text{ minimal}} \mathfrak{p}.$$

7.3 Lokalisierung

Proposition 7.3.1 Sei $S \subset A$ multiplikativ und $\lambda : A \to S^{-1}A$ die kanonische Abbildung. Sei $\mathfrak{a}$ ein $\mathfrak{p}$-primäres Ideal.

1. Falls $S \cap \mathfrak{p} \neq \emptyset$ gilt $S^{-1}\mathfrak{a} = S^{-1}A$.

2. Falls $S \cap \mathfrak{p} = \emptyset$, ist $S^{-1}\mathfrak{a}$ ein $S^{-1}\mathfrak{p}$-primäres Ideal und es gilt $\mathfrak{a} = \lambda^{-1}(S^{-1}\mathfrak{a})$.

Beweis. 1. Sei $s \in S \cap \mathfrak{p}$. Es gibt ein n mit $s^n \in \mathfrak{a}$ und $s^n \in S$. Es folgt $1 = s^n/s^n \in S^{-1}\mathfrak{a}$ und $S^{-1}\mathfrak{a} = S^{-1}A$. Umgekehrt, gilt $1 \in S^{-1}\mathfrak{a}$ also gibt es ein $a \in \mathfrak{a}$ und $s \in S$ mit $a/s = 1$. Daraus folgt, dass es ein $t \in S$ gibt mit $ta = s$. Da $s = at \in \mathfrak{a} \subset \sqrt{\mathfrak{a}} = \mathfrak{p}$ und $s \in S$, folgt die Aussage.

2. Seien $a/s, b/t \in S^{-1}A$ mit $ab/st \in S^{-1}\mathfrak{a}$. Dann gibt es $x \in \mathfrak{a}$ und $s' \in S$ mit $ab/st = x/s'$. Daraus folgt, dass es ein $t' \in S$ gibt mit $t'(abs' - xst) = 0$. Es folgt $abs't' \in \mathfrak{a}$. Da $S \cap \mathfrak{p} = \emptyset$, folgt $s't' \notin \mathfrak{a}$. Es gibt also ein n mit $(xy)^n \in \mathfrak{a}$ und also $x^n \in \mathfrak{a}$ oder gibt es ein m mit $y^{nm} \in \mathfrak{a}$. Daraus folt, dass $S^{-1}\mathfrak{a}$ primär ist. Außerdem gilt $\sqrt{S^{-1}\mathfrak{a}} = S^{-1}\sqrt{\mathfrak{a}} = S^{-1}\mathfrak{p}$.

Wir zeigen jetzt $\mathfrak{a} = \lambda^{-1}(S^{-1}\mathfrak{a})$. Nach Proposition 3.4.1.3 gilt $\lambda^{-1}(S^{-1}\mathfrak{a}) = \cup_{s\in S}(\mathfrak{a} : s)$. Es gilt aber $(\mathfrak{a} : s) = \mathrm{Ann}_{A/\mathfrak{a}}([s])$ und also $((\mathfrak{a} : s) = \mathfrak{a} \Leftrightarrow [s]$ ist kein Nullteiler in $A/\mathfrak{a})$. Da $\mathfrak{a}$ primär ist gilt $((\mathfrak{a} : s) = \mathfrak{a} \Leftrightarrow [s]$ ist nicht nilpotent in $A/\mathfrak{a})$. Aber wenn $[s]$ nilpotent ist gibt es ein n mit $[s]^n = 0$ also $s^n \in \mathfrak{a}$ und $s \in \mathfrak{p}$. Aber $s^n \in S$ und $S \cap \mathfrak{p} \neq \emptyset$. Ein Widerspruch. Also gilt für alle $s \in S$: $[s]$ nicht nilpotent und $(\mathfrak{a} : s) = \mathfrak{a}$. Es folgt $\mathfrak{a} = \lambda^{-1}(S^{-1}\mathfrak{a})$. ∎

Definition 7.3.2 Sei S multiplikativ $\lambda : A \to S^{-1}A$ und $\mathfrak{a} \subset A$ ein Ideal. Dann setzen wir $S(\mathfrak{a}) = \lambda^{-1}(S^{-1}\mathfrak{a})$.

Bemerkung 7.3.3 Es gilt $\mathfrak{a} \subset S(\mathfrak{a}) \subset A$.

Proposition 7.3.4 Sei S multiplkativ und $\mathfrak{a}$ zerlegbar. Sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ für alle i. Durch umnummerierung dürfen wir annehmen, dass es ein m gibt so, dass S die Ideale $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ nicht trifft aber S trifft $\mathfrak{p}_{m+1}, \cdots, \mathfrak{p}_r$.

Dann sind
$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{a}_i \text{ und } S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{a}_i$$
minimale primäre Zerlegungen.

Beweis. Es gilt $S^{-1}\mathfrak{a} = \cap_{i=1}^{r} S^{-1}\mathfrak{a}_i = \cap_{i=1}^{m} S^{-1}\mathfrak{a}_i$. Außerdem sind die $S^{-1}\mathfrak{a}_i$ $S^{-1}\mathfrak{p}_i$-primär. Da die Ideale $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ prim und paarweise verschieden sind und da alle diese Ideal S nicht treffen, sind $S^{-1}\mathfrak{p}_1, \cdots, S^{-1}\mathfrak{p}_m$ auch paarweise verschieden. Falls $\cap_{j\neq i, j=1}^{m} S^{-1}\mathfrak{a}_j \subset S^{-1}\mathfrak{a}_i$ folgt $\cap_{j\neq i, j=1}^{m} S(\mathfrak{a}_j) = \lambda^{-1}(\cap_{j\neq i, j=1}^{m} S^{-1}\mathfrak{a}_j) \subset \lambda^{-1}(S^{-1}\mathfrak{a}_i)$. Da $S(\mathfrak{a}_j) = \mathfrak{a}_j$ für alle $j \leq m$, folgt $\cap_{j\neq j}\mathfrak{a}_j \subset \cap_{j\neq i, j=1}^{m}\mathfrak{a}_j \subset \mathfrak{a}_i$. Ein Widerspruch.

Wir setzen diese Zerlegung in λ^{-1} ein. Es gilt $S(\mathfrak{a}) = \cap_{i=1}^{m}\mathfrak{a}_i$. Falls $\cap_{j\neq i, j=1}^{m}\mathfrak{a}_j \subset \mathfrak{a}_i$ folgt $\cap_{j\neq j}\mathfrak{a}_j \subset \cap_{j\neq i, j=1}^{m}\mathfrak{a}_j \subset \mathfrak{a}_i$. Ein Widerspruch und die Zerlegung ist minimal. ∎

Definition 7.3.5 Sei $\mathfrak{a}$ ein Ideal und sei Σ eine Teilmenge der Menge aller assoziierten Primideale von $\mathfrak{a}$. Die Menge Σ heißt **isoliert** falls gilt: für jedes $\mathfrak{p} \in \Sigma$ und jedes $\mathfrak{p}'$ assoziiertes Primideal von $\mathfrak{a}$ mit $\mathfrak{p}' \subset \mathfrak{p}$ gilt $\mathfrak{p}' \in \Sigma$.

Beispiel 7.3.6 Sei $\mathfrak{p}$ ein minimales assoziiertes Primideal. Dann ist $\Sigma = \{\mathfrak{p}\}$ assoziiert.

Lemma 7.3.7 Sei Σ isoliert.

1. Dann ist $S = A \setminus \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ multiplikativ.

2. Sei $\mathfrak{p}'$ ein assoziiertes Primideal von $\mathfrak{a}$, dann gilt
   (a) $\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \emptyset$.
   (b) $\mathfrak{p}' \notin \Sigma \Rightarrow \mathfrak{p}' \not\subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \Rightarrow \mathfrak{p}' \cap S \neq \emptyset$. □

Beweis. 1. Seien $s, t \in S$. Fall $st \notin S$, gibt es ein $\mathfrak{p} \in \Sigma$ mit $st \in \mathfrak{p}$ und also $s \in \mathfrak{p}$ oder $t \in \mathfrak{p}$. Daraus folgt die Aussage.

2.a. Klar.

2.b. Falls $\mathfrak{p}' \subset \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ folgt $\mathfrak{p}' \subset \mathfrak{p}$ (Vermeidungslemma). Da Σ isoliert ist folgt $\mathfrak{p}' \in \Sigma$. Ein Widerspruch. Die zweite Implikation ist klar. ■

Satz 7.3.8 (Eindeutigket 2) Sei $\mathfrak{a}$ zerlegbar und sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ und sei $\Sigma = \{\mathfrak{p}_{i_1}, \cdots, \mathfrak{p}_{i_m}\}$ isoliert. Dann ist der Durchschnitt

$$\mathfrak{a}_{i_1} \cap \cdots \cap \mathfrak{a}_{i_m}$$

unabhängig von der Zerlegung. □

Beweis. Sei Σ isoliert. Dann ist $S = A\setminus\cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ multiplikativ und $S(\mathfrak{a}) = \mathfrak{a}_{i_1} \cap \cdots \cap \mathfrak{a}_{i_m}$ ist eine primäre Zerlegung von $S(\mathfrak{a})$. Insbesondere gilt $\mathfrak{a}_{i_1} \cap \cdots \cap \mathfrak{a}_{i_m} = S(\mathfrak{a})$ und hängt nur von $\mathfrak{a}$ und Σ ab. ■

Definition 7.3.9 Sei $\mathfrak{a}$ zerlegbar und $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Die **minimale Komponente der Zerlegung** sind die Ideale $\mathfrak{a}_i$ so, dass $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ ein minimales assoziiertes Primideal ist.

Korollar 7.3.10 Sei $\mathfrak{a}$ zerlegbar. Dann sind die minimale Komponente einer Zerlegung unabhängig von der Zerlegung.

Beweis. Folgt aus dem obigen Satz mit $\Sigma = \{\mathfrak{p}\}$, wobei $\mathfrak{p}$ ein minimales assoziiertes Primideal von $\mathfrak{a}$ ist. ■

Beispiel 7.3.11 Sei $\mathfrak{a} = (X^3, X^2Y)$. Dann haben wir die folgende zwei minimales primäre Zerlegungen:

$$\mathfrak{a} = (X, Y)^3 \cap (X^2) \text{ und } \mathfrak{a} = (X^3, Y) \cap (X^2).$$

Die assoziierte Primideale sind $\mathfrak{p}_1 = (X) \subset \mathfrak{p}_2 = (X, Y)$. Das Ideal $\mathfrak{p}_1$ ist minimal und $\mathfrak{p}_2$ ist eingebettet. Man sieht, dass die beide Zerlegungen das Ideal (X^2) (mit $\sqrt{(X^2)} = (X)$) als minimale Komponente haben aber, dass die weitere Komponente von der Zerlegung abhängt.

7.4 Noethersche Ringe

In diesem Abschnitt zeigen wir, dass in einem noetherschen Ring, jedes Ideal $\mathfrak{a} \subsetneq A$ zerlegbar ist.

Definition 7.4.1 Ein Ideal $\mathfrak{a}$ heißt **irreduzibel** falls die Implikation

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ oder } \mathfrak{a} = \mathfrak{c})$$

gilt für alle Ideale $\mathfrak{b}$ und $\mathfrak{c}$.

Beispiel 7.4.2 Ein Primideal $\mathfrak{p}$ ist irreduzibel: falls $\mathfrak{p} = \mathfrak{b} \cap \mathfrak{c}$ dann gilt nach dem Vermeidungslemma $\mathfrak{b} = \mathfrak{p}$ oder $\mathfrak{c} = \mathfrak{p}$.

Bemerkung 7.4.3 Sei $\mathfrak{a} \subset A$ ein Ideal.

1. $\mathfrak{a}$ ist genau dann irreduzibel, wenn $(0) \subset A/\mathfrak{a}$ irreduzibel ist.

2. Analog ist $\mathfrak{a}$ genau dann primär, wenn $(0) \subset A/\mathfrak{a}$ primär ist.

Lemma 7.4.4 Sei A noethersch. Ein irreduzibles Ideal ist primär. □

Beweis. Wir können in $A/\mathfrak{a}$ arbeiten und zeigen, dass wenn (0) irreduzibel ist, dann ist (0) primär.

Seien $x, y \in A$ mit $xy = 0$. Wir betrachten die Kette $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots \subset \mathrm{Ann}(x^n) \subset \cdots$. Da A noethersch ist ist diese Kette stationär. Sei n so, dass $\mathrm{Ann}(x^m) = \mathrm{Ann}(x^n)$ für alle $m \geq n$.

Wir zeigen $(0) = (x^n) \cap (y)$. Sei $ay \in (y) \cap (x^n)$. Dann gilt $ayx = 0$. Es gilt auch $ay = bx^n$ also $bx^{n+1} = ayx = 0$. Es gilt also $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$ also $ay = bx^n = 0$. Da (0) irreduzibel ist, gilt $(x^n) = (0)$ oder $(y) = (0)$ also $x^n = 0$ oder $y = 0$. ■

Lemma 7.4.5 Sei A noethersch. Jedes Ideal kann als endlichen Durchschnitt von irreduziblen Idealen dargestellt werden. □

Beweis. Sei Σ die Menge aller Ideal die keine solche Darstellun haben. Falls Σ nicht leer ist hat Σ ein maximales Element. Sei $\mathfrak{a}$ ein solches Element. Dann ist $\mathfrak{a}$ nicht irreduzibel. Insbesondere gibt es eine Zerlegung $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ mit $\mathfrak{a} \subsetneq \mathfrak{b}$ und $\mathfrak{a} \subsetneq \mathfrak{c}$. Da maximal war gibt es irreduzible Ideale $\mathfrak{b}_1, \cdots, \mathfrak{b}_r$ und $\mathfrak{c}_1, \cdots, \mathfrak{c}_s$ mit $\mathfrak{b} = \mathfrak{b}_1 \cap \cdot \cap \mathfrak{b}_r$ und $\mathfrak{c} = \mathfrak{c}_1 \cap \cdots \cap \mathfrak{c}_s$. Es folgt $\mathfrak{a} = \mathfrak{b}_1 \cap \cdots \cap \mathfrak{b}_r \cap \mathfrak{c}_1 \cap \cdots \cap \mathfrak{c}_s$ und $\mathfrak{a}$ hat eine Darstellung. Ein Widerspruch. ■

Satz 7.4.6 Sei A noethersch. Jedes echtes Ideal hat eine primäre Zerlegung. □

Beweis. Folgt aus den zwei obigen Lemmas. ■

Proposition 7.4.7 Sei A ein noetherscher Ring, sei $\mathfrak{m}$ ein maximales Ideal und $\mathfrak{a}$ ein Ideal. Die folgenden Aussagen sind äquivalent:

1. $\mathfrak{a}$ ist $\mathfrak{m}$-primär.
2. $\sqrt{\mathfrak{a}} = \mathfrak{m}$.
3. Es gibt ein n mit $\mathfrak{m}^n \subset \mathfrak{a} \subset \mathfrak{m}$.

Beweis. (1. $\Rightarrow$ 2.) Klar.

(2. $\Rightarrow$ 3.) Folgt aus Proposition 6.3.10: es gibt ein n mit $\mathfrak{m}^n = (\sqrt{\mathfrak{a}})^n \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}} = \mathfrak{m}$.

(3. $\Rightarrow$ 1.) Es gilt $\mathfrak{m} = \sqrt{\mathfrak{m}^n} \subset \sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{m}} = \mathfrak{m}$. Es folgt $\sqrt{\mathfrak{a}} = \mathfrak{m}$. Aus der Proposition 7.1.7 folgt, dass $\mathfrak{a}$ primär ist. ∎

Satz 7.4.8 Sei A noethersch und $\mathfrak{a}$ ein Ideal. Die assoziierte Primideale von $\mathfrak{a}$ sind genau die Primideal in der Familie $(\mathfrak{a} : x)_{x \in A}$. □

Beweis. Sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Sei jetzt $\mathfrak{b}_i = \cap_{j \neq i} \mathfrak{a}_i$. Es gilt $\mathfrak{a} \subsetneq \mathfrak{b}_i$. Außerdem gilt für alle $x \in \mathfrak{b}_i \setminus \mathfrak{a}$: $\sqrt{(\mathfrak{a} : x)} = \cap_{\mathfrak{a}_j \ni x} \mathfrak{p}_j = \mathfrak{p}_i$.

Sei jetzt n mit $\mathfrak{p}_i^n = (\sqrt{\mathfrak{a}_i})^n \subset \mathfrak{a}_i$. Es gilt $\mathfrak{p}_i^n \mathfrak{b}_i \subset \mathfrak{a}_i \mathfrak{b}_i \subset \mathfrak{a}_i \cap \mathfrak{b}_i = \mathfrak{a}$. Sei m minimal mit $\mathfrak{p}_i^n \mathfrak{b}_i \subset \mathfrak{a}$. Dann gibt es ein $x \in \mathfrak{p}_i^{m-1} \mathfrak{b}_i$ mit $x \notin \mathfrak{a}$. Es gilt $x\mathfrak{p}_i \subset \mathfrak{p}_i^m \mathfrak{b}_i \subset \mathfrak{a}$ also $\mathfrak{p}_i \subset (\mathfrak{a} : x)$. Aber da $x \in \mathfrak{b}_i$ gilt auch $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_i$. Es folgt $(\mathfrak{a} : x) = \mathfrak{p}_i$.

Andersrum, sei $x \in A$ so, dass $(\mathfrak{a} : x)$ prim ist. Dann gilt $\sqrt{(\mathfrak{a} : x)} = (\mathfrak{a} : x)$ und ist auch prim und also ein assoziiertes Primideal. ∎

8 Dedekinsringe und diskrete Bewertungsringe

In diesem Kapitel wollen wir die noethersche ganz abgeschlossene Integritätsringe der Dimension 1 betrachten.

8.1 Eindimensionale noethersche Integritätsringe

Proposition 8.1.1 Sei A eine noetherscher Integritätsring mit $\mathrm{Kdim}(A) = 1$ und sei $\mathfrak{a}$ ein Ideal mit $\mathfrak{a} \neq 0$. Dann gibt es primäre Ideale $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ mit

$$\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_r$$

so, dass die Primideale $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ paarweise verschieden sind.

Beweis. Sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung und sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Da A ein Integritätsring ist, ist (0) prim und für $\mathfrak{p}$ prim mit $\mathfrak{p} \supsetneq (0)$, ist $\mathfrak{p}$ maximal (weil $\mathrm{Kdim}(A) = 1$). Da $\mathfrak{a} \neq 0$, gilt $0 \subsetneq \mathfrak{a} \subset \mathfrak{a}_i \subset \mathfrak{p}_i$ und also sind alle $\mathfrak{p}_i$ maximal. Es folgt, dass $\mathfrak{p}_i + \mathfrak{p}_j = A$ für $i \neq j$ und also sind diese Ideale teilerfremd. Es folgt, dass $\mathfrak{a}_i$ und $\mathfrak{a}_j$ paarweise teilerfremd sind und also gilt $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r = \mathfrak{a}_1 \cdots \mathfrak{a}_r$.

Sei $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_r$ so eine Darstellung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Es gilt $\mathfrak{a} \subset \mathfrak{a}_i \subset \mathfrak{p}_i$ also ist $\mathfrak{p}_i$ maximal. Es folgt, dass die $\mathfrak{p}_i$ paarweise teilerfremd sind und also $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r = \mathfrak{a}_1 \cdots \mathfrak{a}_r$. Es folgt, dass dies eine primäre Zerlegung ist. Außerdem sind alle Primideale $\mathfrak{p}_i$ maximal und also auch minimale assoziierte Primideale. Daraus folgt, dass die Zerlegung eindeutig bestimmt ist. ∎

Korollar 8.1.2 Sei A ein noetherscher Integritätsring der Dimension 1 so, dass alle primäre Ideal der Form $\mathfrak{p}^n$ mit $\mathfrak{p}$ prim sind.

Dann hat jedes Ideal $\mathfrak{a}$ in A eine eindeutige Zerlegung der Form:

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}.$$

Beweis. Nach dem obigen Satz, gibt es eine eindeutige Zerlegung $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_r$, wobei $\mathfrak{a}_i$ $\mathfrak{p}_i$-primär ist und die Ideale $\mathfrak{p}_i$ paarweise verschieden sind. Nach voraussetzung, gibt es ein α_i mit $\mathfrak{a}_i = \mathfrak{p}_i^{\alpha_i}$. Daraus folgt die Aussage. ∎

Beispiel 8.1.3 Der Ring $\mathbb{Z}$ ist ein solcher Ring.

8.2 Diskrete Bewertungsringe

Definition 8.2.1 Sei K ein Körper.

1. Eine **diskete Bewertung** von K ist ein Gruppenhomomorphismus $v : K^\times \to \mathbb{Z}$ so, dass $v(x+y) \geq \min(v(x), v(y))$.

2. **Der Bewertungsring** der Berwertung v ist die Menge $A = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.

3. Ein Ring A heißt **diskret Bewertungsring**, wenn es eine diskrete Bewertung $v : \mathrm{Frac}(A) \to \mathbb{Z}$ gibt so, dass $A = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.

Bemerkung 8.2.2 Die Menge $A = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ ist ein Unterring von K und $K = \mathrm{Frac}(A)$.

Beispiel 8.2.3 1. Sei $K = \mathbb{Q}$ und p eine Primzahl. Wir schreiben $\frac{x}{y} \in \mathbb{Q}^\times$ mit $x, y \in \mathbb{Z} \setminus \{0\}$. Dann gibt es n, m und $a, b \in \mathbb{Z}$ mit $x = p^n a$, $y = p^m b$ und $p \not| a, b$. Wir setzen

$$v\left(\frac{x}{y}\right) = v\left(\frac{p^n a}{p^m b}\right) = n - m.$$

Dann ist v eine Bewertung. Diese Bewertung heißt **p-adische Bewertung**

2. Sei $K = \mathsf{k}(X)$ und $P \in \mathsf{k}[X]$ irreduzibel. Wir schreiben $\frac{Q}{R} \in \mathsf{k}(X)$ mit $Q, R \in \mathbb{Z} \setminus \{0\}$. Dann gibt es n, m und $a, b \in \mathbb{Z}$ mit $Q = P^n A$, $R = P^m B$ und $P \not| A, B$. Wir setzen

$$v\left(\frac{Q}{R}\right) = v\left(\frac{P^n A}{P^m B}\right) = n - m.$$

Dann ist v eine Bewertung. Diese Bewertung heißt **P-adische Bewertung**.

Bemerkung 8.2.4 Sei $v : K \to \mathbb{Z}$ eine dirkrete Bewertung. Dann gilt $v(1) = 0$: es gilt $v(1) = v(1 \times 1) = v(1) + v(1)$. Es gilt auch $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$ also $v(x^{-1}) = -v(x)$ für alle $x \in K^\times$.

Bemerkung 8.2.5 Sei $v : K^\times \to \mathbb{Z}$ eine nicht triviale Bewertung (*i.e.* es gibt ein x mit $v(x) \neq 0$). Dann gibt es ein y mit $v(y) > 0$: Falls $v(x) > 0$ sind wir fertig. Sonst gilt $v(x^{-1}) = -v(x) > 0$. Das Bild von v ist eine Untergruppe von $\mathbb{Z}$ und also der Form $n\mathbb{Z}$. Wir können eine neue Bewertung $v' = \frac{1}{n} v$ definieren und dann ist v' surjektiv.

Dank der Bemerkung kann man also immer annehmen, dass v surjektiv ist. Ab jetzt sind alle Bewertungen surjektiv.

Lemma 8.2.6 Sei $A = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$ ein diskreter Bewertungsring. Dann gilt

1. A ist lokal mit maximalem Ideal $\mathfrak{m} = \{x \in K^\times \mid v(x) > 0\} \cup \{0\}$.

2. Für $x, y \in A$ mit $v(x) = v(y)$, gilt $(x) = (y)$.

3. Die einzige nicht triviale Ideale von A sind der Form $\mathfrak{m}_k = \{x \in A \mid v(x) \geq k\} \cup \{0\}$.

4. Der Ring $\mathfrak{a}$ ist noethersch.

5. Alle nicht triviale Ideale sind der Form (x^n) für ein x mit $v(x) = 1$.

6. $\mathrm{Kdim}(A) = 1$ und $\mathfrak{m}$ ist das einzige nicht triviale Primideal.

7. Alle nicht triviale Ideale sind der Form $\mathfrak{m}^k$. □

Beweis. 1. Es ist klar (Übung), dass $\mathfrak{m}$ ein Ideal ist. Sei $x \in A \setminus \mathfrak{m}$. Dann gilt $v(x) = 0$ und also $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$. Es folgt $v(x^{-1}) = 0$ und $x^{-1} \in A$.

2. Es gilt $v(xy^{-1}) = v(x) - v(y) = 0$ und also $xy^{-1} \in A^\times$. Daraus folgt die Aussage.

3. $\mathfrak{m}_k$ ist ein Ideal (Übung). Sei $\mathfrak{a}$ ein Ideal und $k = \min\{v(x) \mid x \in \mathfrak{a}\}$. Es gilt $\mathfrak{a} \subset \mathfrak{m}_k$. Sei $x \in \mathfrak{a}$ mit $v(x) = k$ und sei jetzt $y \in \mathfrak{m}_k$. Dann gilt $v(yx^{-1}) = v(y) - v(x) \geq 0$ also $yx^{-1} \in A$ und $y \in (x) \subset \mathfrak{a}$.

4. Die einzige Ideale bilden eine absteigende Kette $A = \mathfrak{m}_0 \supset \mathfrak{m} = \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_k \supset \cdots$. Daraus folgt, dass jede Aufsteigende Kette stationär ist.

5. Sei $x \in A$ mit $v(x) = 1$ (dies ist möglich, weil v surjektiv ist). Sei $y \in \mathfrak{m}_k$, dann gilt $v(yx^{-k}) = v(y) - k \geq 0$ also $yx^{-k} \in A$ und $y \in (x^k)$. Es folgt $\mathfrak{m}_k \subset (x^k)$. Da $v(x) = k$ folgt $(x^k) \subset \mathfrak{m}_k$ und also $\mathfrak{m}_k = (x^k)$.

6. Das Ideal (x^k) ist genau dann prim wenn $k = 1$. Also gibt es nur ein nicht triviales Primideal: das maximale Ideal $\mathfrak{m}$.

7. Folgt aus 5. ■

Proposition 8.2.7 Sei A ein noetherscher lokaler Integritätsring mit $\mathrm{Kdim}(A) = 1$ und sei $\mathfrak{m}$ sein maximales Ideal und $\mathsf{k} = A/\mathfrak{m}$ der Restklassenkörper. Die folgende Aussagen sind äquivalent:

1. A ist ein diskreter Bewertungsring.
2. A ist ganz abgeschlossen
3. $\mathfrak{m}$ ist ein Hauptideal.
4. $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$
5. Jedes Ideal ist der Form $\mathfrak{m}^k$ für ein k.
6. Es gibt ein $x \in A$ so, dass jedes Ideal der Form (x^k) ist, für ein k.

Beweis. Sei $\mathfrak{a}$ ein Ideal mit $\mathfrak{a} \neq 0$ und sei $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ eine minimale primäre Zerlegung. Sei $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$. Dann sind die Ideale $\mathfrak{p}_i$ prim und paarweise verschieden. Es gilt aber $0 \neq \mathfrak{a} \subset \mathfrak{p}_i$ und also ist $\mathfrak{p}_i$ prim und nicht Null. Da $\mathrm{Kdim}(A) = 1$ folgt, dass $\mathfrak{p}_i$ maximal ist und also $\mathfrak{p}_i = \mathfrak{m}$. Es gilt also $r = 1$ und $\mathfrak{a}$ ist $\mathfrak{m}$-primär. Es gibt also ein n mit $\mathfrak{m}^n \subset \mathfrak{a}$.

Es gilt auch $\mathfrak{m}^n \supsetneq \mathfrak{m}^{n+1}$ für alle n (sonst ist A artinsch und also der Dimension 0).

(1. $\Rightarrow$ 2.) Siehe Übungsblatt 8.

(2. $\Rightarrow$ 3.) Sei $a \in \mathfrak{m}$ und n mit $\mathfrak{m}^n \subset (a)$ aber $\mathfrak{m}^{n-1} \not\subset (a)$. Sei $b \in \mathfrak{m}^{n-1} \setminus \mathfrak{a}$ und $x = a/b$. Es gilt $x^{-1} \notin A$ (sonst gilt $a|b$ also $b \in (a)$, Widerspruch). Es folgt, dass x^{-1} nicht ganz über A ist.

Wir zeigen, dass $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$. Sonst gilt $x^{-1}\mathfrak{m} \subset \mathfrak{m}$ also ist $\mathfrak{m}$ ein $A[x^{-1}]$-Modul und endlich erzeugt als A-Modul also auch als $A[x^{-1}]$-Modul. Aber dieser Modul ist treu: Sei $E_y : \mathfrak{m} \to \mathfrak{m}$ die Multiplikation mit $y \in A[x^{-1}]$. Falls $E_y = E_z$ dann gilt $ym = zm$ für alle $m \in \mathfrak{m}$ und also $(y-z)m = 0$. Da es ein $m \in \mathfrak{m}$ mit $m \neq 0$ gibt folgt $y-z = 0$ und also dieser Modul ist treu. Es folgt, dass x^{-1} ganz über A ist. Ein Widerspruch.

Es gilt aber $x^{-1}\mathfrak{m} = (b/a)\mathfrak{m} \subset (1/a)\mathfrak{m}^{n-1}\mathfrak{m} = (1/a)\mathfrak{m}^n \subset 1/a(a) = A$. Also ist $x^{-1}\mathfrak{m}$ ein Ideal in A mit $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ also $x^{-1}\mathfrak{m} = A$. Es folgt $\mathfrak{m} = (x)$.

(3. $\Rightarrow$ 4.) Sei x mit $\mathfrak{m} = (x)$. Es folgt $\mathfrak{m}/\mathfrak{m}^2 = \langle x \rangle$ und $\dim(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. Da $\mathfrak{m} \neq 0$ folgt $\mathfrak{m} \neq \mathfrak{m}^2$ nach Nakayama.

(4. $\Rightarrow$ 5.) Es gibt ein n mit $\mathfrak{m}^n \subset \mathfrak{a}$. Wir betrachten den Ring $A/\mathfrak{m}^n$. Sei $\bar{\mathfrak{p}}$ prim in $A/\mathfrak{m}^n$. Dann gibt es ein Primideal $\mathfrak{p} \supset \mathfrak{m}^n$ mit $\mathfrak{p}/\mathfrak{m}^n = \bar{\mathfrak{p}}$. Es gilt also $\mathfrak{p} = \mathfrak{m}$ und $\bar{\mathfrak{p}} = \mathfrak{m}/\mathfrak{m}^n$. Also hat $A/\mathfrak{m}^n$ nur ein Primideal und also $\mathrm{Kdim}(A/\mathfrak{m}^n) = 0$. Dieser Ring ist artinsch und lokal mit maximalem Ideal $\bar{\mathfrak{m}} = \mathfrak{m}/\mathfrak{m}^n$. Es gilt also $\dim(\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2) = 1$ und nach dem Beweis von Proposition 6.4.12 sind alle Ideal in $A/\mathfrak{m}^n$ der Form $\bar{\mathfrak{m}}^k$. Es folgt $\mathfrak{a}/\mathfrak{m}^n = \bar{\mathfrak{m}}^k$ und also $\mathfrak{a} = \mathfrak{m}^k$.

(5. $\Rightarrow$ 6.) Es gilt $\mathfrak{m} \supsetneq \mathfrak{m}^2$. Sei $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Es gibt ein r mit $(x) = \mathfrak{m}^r$ und also $(x) = \mathfrak{m}$. Sei $\mathfrak{a}$ ein Ideal, es gibt ein n mit $\mathfrak{a} = \mathfrak{m}^n$. Es folgt $\mathfrak{a} = (x^n)$.

(6. $\Rightarrow$ 1.) Es gilt $\mathfrak{m} = (x)$ und $(x^k) \supsetneq (x^{k+1})$. Sei $a \in A$ mit $a \neq 0$. Dann gibt es ein k mit $(a) = (x^k)$. Falls es ein n gibt mit $(a) = (x^n)$ folgt $(x^k) = (x^n)$ und also $n = k$. Wir setzen $v(a) = k$ und $v(a/b) = v(a) - v(b)$ für alle Elemente aus $K^\times$. Es gibt: v ist ein Gruppenhompomorphismus. Seien $a, b \in A$ mit $(a) = (x^n)$ und $(b) = (x^m)$. Ohne Einschränkung können wir annehmen $n \leq m$. Es gilt $(a+b) \subset (x^n) + (x^m) = (x^n)$ also $(a+b) = (x^k)$ mit $k \geq n$. Es folgt $v(a+b) \geq \min(v(a), v(b))$. ∎

8.3 Dedekinsringe

Satz 8.3.1 Sei A ein noetherscher Integritätsring mit $\mathrm{Kdim}(A) = 1$. Die folgende Aussagen sind äquivalent:

1. A ist ganz abgeschlossen.
2. Jedes primäres Ideal ist der Form $\mathfrak{p}^k$ für ein k und $\mathfrak{p}$ prim.
3. Jeder lokal Ring $A_\mathfrak{p}$ mit $\mathfrak{p} \neq 0$ prim ist ein diskreter Bewertungsring. □

Beweis. (1. $\Leftrightarrow$ 3.) Nach Proposition 4.3.4 ist A genau dann ganz abgeschlossen, wenn alle $A_\mathfrak{p}$ ganz abgeschlossen sind. Aber $A_\mathfrak{p}$ ist lokal noethersch mit krullscher Dimension 1. Aus dem obigen Satz folgt, dass $A_\mathfrak{p}$ genau dann ganz abgeschlossen ist, wenn $A_\mathfrak{p}$ ein diskreter Bewertungsring ist.

(2. $\Rightarrow$ 3.) Sei $\mathfrak{p}$ ein Primideal und sei $\mathfrak{b}$ ein Ideal in $A_\mathfrak{p}$. Sei $\lambda : A \to A_\mathfrak{p}$ die kanonische Abbildung und $\mathfrak{a} = \lambda^{-1}(\mathfrak{b})$. Wie im Beweis der vorherigen Proposition, ist $\mathfrak{b}$ $\mathfrak{p}A_\mathfrak{p}$-primär und $\mathfrak{a}$ ist auch primär. Also gibt es ein Primideal $\mathfrak{q}$ und ein n mit $\mathfrak{a} = \mathfrak{q}^n$. Falls $\mathfrak{q} \neq \mathfrak{p}$ gilt $\mathfrak{b} = \mathfrak{a}_\mathfrak{p} = (\mathfrak{q}^n)_\mathfrak{p} = A_\mathfrak{p}$. Ein Widerspruch. Es folgt $\mathfrak{q} = \mathfrak{p}$ und $\mathfrak{b} = (\mathfrak{p}^n)_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$ und also ist $\mathfrak{b}$ eine Potenz vom maximalen Ideal von $A_\mathfrak{p}$ und aus der obigen Proposition folgt $A_\mathfrak{p}$ ist ganz abgeschlossen.

(3. $\Rightarrow$ 2.) Sei $\mathfrak{a}$ $\mathfrak{p}$-primär. Dann gibt es ein n mit $\mathfrak{a}_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$. Sei $\mathfrak{q}$ ein Primideal, wir zeigen $\mathfrak{a}_\mathfrak{q} = (\mathfrak{p}^n)_\mathfrak{q}$. Falls $\mathfrak{q} \neq \mathfrak{p}$, gilt $\mathfrak{a} \not\subset \mathfrak{q}$ (sonst gibt es ein k mit $\mathfrak{p}^k \subset \mathfrak{a} \subset \mathfrak{q}$ und also $\mathfrak{p} \subset \mathfrak{q}$. Da alle nicht triviale Primideal maximal sind folgt $\mathfrak{p} = \mathfrak{q}$). Es folgt $\mathfrak{a}_\mathfrak{q} = A_\mathfrak{q} = (\mathfrak{p}^n)_\mathfrak{q}$. Es gilt auch $\mathfrak{a}_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n = (\mathfrak{p}^n)_\mathfrak{p}$. Daraus folgt $\mathfrak{a} = \mathfrak{p}^n$. ■

Definition 8.3.2 Ein Integritätsring, der die Aussagen des obigen Satz erfüllt heißt **Dedekinsring**.

Korollar 8.3.3 In einem Dedekinsgring hat jedes Ideal eine eindeutige Zerlegung als Produkt von Primidealen.

Beweis. Folgt aus dem obigen Satz und Korollar 8.1.2 ■

8.4 Gebrochene Ideale

Definition 8.4.1 Sei A ein Integritätsring und $K = \mathrm{Frac}(A)$. Ein A-Untermodul von K heißt **gebrochenes Ideal** falls es ein $x \in A \setminus \{0\}$ gibt mit $xM \subset A$.

Für M ein gebrochenes Ideal setzt man $(A : M) = \{x \in K \mid xM \subset A\}$.

Beispiel 8.4.2 1. Alle Ideale $\mathfrak{a} \subset A$ sind auch gebrochene Ideale: $1\mathfrak{a} = \mathfrak{a} \subset A$.

2. Sei $u = \frac{a}{b} \in K$, wobei $a, b \in A$. Dann ist $M = Au \subset K$ ein gebrochenes Ideal: es gilt $bM = Aa = (a) \subset A$. Dieser Modul M oder dieses gebrochenes Ideal beschreibt man mit (u). Ein solches gebrochenes Ideal heißt **gebrochenes Hauptideal**.

Lemma 8.4.3 Sei A ein Integritätsring und $K = \mathrm{Frac}(A)$.

1. Sei $M \subset K$ ein endlich erzeugter A-Modul. Dann ist M ein gebrochenes Ideal.

2. Falls A nothersch ist sind alle gebrochene Ideale endlich erzeugte A-Moduln. □

Beweis. 1. Sei $(u_1, \cdots, u_n)$ eine erzeugende Familie von M als A-Modul. Es gibt $x_1, \cdots, x_n \in A \setminus \{0\}$ so, dass $x_i u_i \in A$. Sei $x = x_1 \cdots x_n$. Dann gilt $xu_i \in A$ und $xM = x(Au_1 + \cdots + Au_n) \subset A$.

2. Sei M ein gebrochenes Ideal und $x \in A$ mit $x \neq 0$ und $xM \subset A$. Dann ist $\mathfrak{a} = xM$ ein A-Untermodul von A also ein Ideal. Da A noethersch ist, ist $\mathfrak{a}$ endlich erzeugt: $\mathfrak{a} = Aa_1 + \cdots + Aa_n$ und es folgt, dass $M = A\frac{a_1}{x} + \cdots + A\frac{a_n}{x}$. ■

Definition 8.4.4 Sei A ein Integritätsring und $K = \mathrm{Frac}(A)$. Ein A-Untermodul $M \subset K$ heißt **invertierbar** falls es ein Untermodul $N \subset K$ gibt mit $MN = A$.

Lemma 8.4.5 Sei A ein Integritätsring und $K = \mathrm{Frac}(A)$. Sei $M \subset K$ ein A-Untermodul.

1. Falls M invertierbar ist, ist der Modul N mit $MN = A$ eindeutig bestimmt: es gilt $N = (A : M)$.

2. Falls M invertiebar ist, ist M endlich erzeugt und also ein gebrochenes Ideal.

3. Falls $M = (u)$ ein gebrochenes Hauptideal ist, ist M invertierbar. □

Beweis. 1. Es gilt $N \subset (A : M) = (A : M)MN \subset AN = N$. Daraus folgt $N = (A : M)$.

2. Sei N mit $MN = A$. Dann gibt es Elemente $x_1, \cdots, x_n \in M$ und $y_1, \cdots, y_n \in N$ mit $\sum_i x_i y_i = 1$. Sei $x \in M$. Es gilt $x = \sum_i x_i(xy_i)$. Aber $x \in M$ und $y_i \in N$ also $xy_i \in MN = A$. Es folgt $M \subset Ax_1 + \cdots + Ax_n$.

3. Sei $N = (u^{-1})$. Es gilt $MN = A$. ■

Bemerkung 8.4.6 Für $M, N, P \subset K$ Untermoduln, gilt $MN = NM$, $AM = M$ und $(MN)P = M(NP)$. Also ist die Menge $\mathrm{Inv}(A)$ aller invertierbare Moduln eine Gruppe mit Inverse $M^{-1} = (A : M)$ und A ist die Einheit.

Proposition 8.4.7 Sei M ein gebrochenes Ideal. Die folgende Aussagen sind äquivalent:

1. M ist invertierbar.

2. M ist endlich erzeugt und $M_{\mathfrak{p}}$ ist invertierbar für jedes Primideal $\mathfrak{p}$

3. M ist endlich erzeugt und $M_{\mathfrak{m}}$ ist invertierbar für jedes maximales Ideal $\mathfrak{m}$.

Beweis. (1. $\Rightarrow$ 2.) Da M endlich erzeugt ist (M ist invertierbar) folgt aus Korollar 3.4.5 $(A : M)_{\mathfrak{p}} = (A_{\mathfrak{p}} : M_{\mathfrak{p}})$ und also $M_{\mathfrak{p}}(A_{\mathfrak{p}} : M_{\mathfrak{p}}) = A_{\mathfrak{p}}(A : M)_{\mathfrak{p}} = (M(A : M))_{\mathfrak{p}} = A_{\mathfrak{p}}$.

(2. $\Rightarrow$ 3.) Klar

(3. $\Rightarrow$ 1.) Sei $\mathfrak{a} = M(A : M)$. Dann ist $\mathfrak{a}$ ein Ideal von A. Für $\mathfrak{m}$ maximal gilt $\mathfrak{a}_{\mathfrak{m}} = M_{\mathfrak{m}}(A_{\mathfrak{m}} : M_{\mathfrak{m}}) = A_{\mathfrak{m}}$. Es folgt $\mathfrak{a} = A$. ∎

Proposition 8.4.8 Sei A ein lokaler Intergritätsing mit maximalem Ideal $\mathfrak{m}$. Es gilt

$$A \text{ ist ein diskreter Bewertungsring} \Leftrightarrow \text{jedes gebrochenes Ideal } M \neq 0 \text{ ist invertierbar.}$$

Beweis. ($\Rightarrow$). Sei x mit $\mathfrak{m} = (x)$. Sei M ein gebrochenes Ideal und sei $y \in A$ mit $yM \subset A$. Dann ist yM ein Ideal in A also der Form $yM = (x^r)$. Sei $k = v(y)$, wobei v die Bewertung ist. Es gilt $y = ux^k$ mit $u \in A^\times$. Es folgt $M = y^{-1}(x^r) = (x^{r-s})$ und M ist invertierbar.

($\Leftarrow$). Wir zeigen, dass A noethersch ist. Sei $\mathfrak{a} \subset A$ ein Ideal. Dann ist $\mathfrak{a}$ ein gebrochenes Ideal und also invertierbar. Es folgt, dass $\mathfrak{a}$ endlich erzeugt ist und A ist noethersch.

Wir zeigen, dass jedes nicht triviales Ideal der Form $\mathfrak{m}^n$ ist. Sei Σ die Menge aller Ideale, die nicht dieser Form sind. Wir zeigen, dass $\Sigma = \{0\}$. Die Menge Σ hat Σ ein maximales Element $\mathfrak{a}$. Es gilt $\mathfrak{a} \neq \mathfrak{m}$ also $\mathfrak{a} \subsetneq \mathfrak{m}$. Es folgt $(A : \mathfrak{m})\mathfrak{a} \subset (A : \mathfrak{m})\mathfrak{m} = A$. Falls $(A : \mathfrak{m})\mathfrak{a} = A$ folgt $\mathfrak{a} = \mathfrak{m}(A : \mathfrak{m})\mathfrak{a} = \mathfrak{m}A = \mathfrak{m}$ ein Widerspruch also gilt $(A : \mathfrak{m})\mathfrak{a} \subsetneq A$. Es gilt $\mathfrak{a} \subset (A : \mathfrak{m})\mathfrak{a}$. Falls $\mathfrak{a} \subsetneq (A : \mathfrak{m})\mathfrak{a}$, folgt $(A : \mathfrak{m})\mathfrak{a} \notin \Sigma$ also gibt es ein n mit $(A : \mathfrak{m})\mathfrak{a} = \mathfrak{m}^n$. Es folgt $\mathfrak{a} = \mathfrak{m}(A : \mathfrak{m})\mathfrak{a} = \mathfrak{m}^{n+1}$. Ein Widerspruch. Daraus folgt $\mathfrak{a} = (A : \mathfrak{m})\mathfrak{a}$ und also $\mathfrak{m}\mathfrak{a} = \mathfrak{m}(A : \mathfrak{m})\mathfrak{a} = \mathfrak{a}$. Nach Nakayama folgt $\mathfrak{a} = 0$. ∎

Satz 8.4.9 Sei A ein Intergritätsing. Es gilt

$$A \text{ ist ein Dedekinsring} \Leftrightarrow \text{jedes gebrochenes Ideal } M \neq 0 \text{ ist invertierbar.}$$

Beweis. ($\Rightarrow$). Sei $M \neq 0$ ein gebrochenes Ideal und $\mathfrak{p}$ ein Primideal. Dann ist $M_{\mathfrak{p}}$ ein gebrochenes Ideal und $A_{\mathfrak{p}}$ ein diskreter Bewertungsring. Also is $M_{\mathfrak{p}}$ invertierbar. Da A noethersch ist, ist M endlich erzeugt. Es folgt, dass M invertierbar ist.

($\Leftarrow$). Sei $\mathfrak{a} \subset A$ ein Ideal. Dann ist $\mathfrak{a}$ ein gebrochenes Ideal und also invertierbar. Es folgt, dass $\mathfrak{a}$ endlich erzeugt ist und A ist noethersch. Es genügt zu zeigen, dass für jedes Primideal $\mathfrak{p}$, der Ring $A_{\mathfrak{p}}$ ein diskreter Bewertungsring ist. Dafür genügt es zu zeigen, dass jedes gebrochenes Ideal von $A_{\mathfrak{p}}$ invertierbar ist. Sei also M ein begrochenes Ideal in $A_{\mathfrak{p}}$. Dann ist $\mathfrak{b} = (A_{\mathfrak{p}} : M)M \subset A_{\mathfrak{p}}$ ein Ideal in $A_{\mathfrak{p}}$. Falls

$\mathfrak{b}$ invertierbar in $A_{\mathfrak{p}}$ ist, gilt $A = (A : \mathfrak{b})\mathfrak{b} = (A : \mathfrak{b})(A : M)M$ und also ist M invertierbar. Es genügt also zu zeigen, dass jedes Ideal $\mathfrak{b} \subset A_{\mathfrak{p}}$ invertierbar ist. Ein silches Ideal ist der Form $\mathfrak{b} = \mathfrak{a}_{\mathfrak{p}}$ mit $\mathfrak{a} \subset A$ ein Ideal in A. Da $\mathfrak{a}$ ein gebrochenes Ideal ist, ist $\mathfrak{a}$ invertierbar und also ist $\mathfrak{b} = \mathfrak{a}_{\mathfrak{p}}$ invertierbar. ■

Korollar 8.4.10 Sei A ein Dedekinsring. Dann hat die Menge aller gebrochenen Ideale eine Gruppenstruktur für die Multiplikation.

Die Menge alle gebrochene Hauptideale ist eine Untergruppe von dieser Gruppe.

Beweis. Diese Menge ist eine Teilmenge aller invertierbare Moduln. Außerdem, falls M, N gebrochene Ideale sind, ist MN en gebrochenes Ideal: es gibt $x, y \in A$ mit $xM \subset A$ und $yN \subset A$. Es folgt $xyMN \subset A$.

Falls $M = (u)$ und $N = (v)$ gilt $MN = (uv)$ und $M^{-1} = (u^{-1})$ also ist die Teilmenge aller gebrochenen Hauptideale eine Untergruppe. ■

Definition 8.4.11 Sei A ein Dedekinsring.

1. Die Gruppe aller gebrochenen Ideale heißt **Idealgruppe von** A und ist mit J_A bezeichnet.

2. Die Untergruppe aller gebrochenen Hauptideale heißt **Hauptidealgruppe von** A und ist mit P_A bezeichnet.

3. Die Faktorgruppe $\mathrm{Pic}(A) = J_A/P_A$ heißt **Idealfaktorgruppe**.

Proposition 8.4.12 Es gibt eine exakte Sequenz von Gruppen

$$1 \to A^\times \to K^\times \to J_A \to \mathrm{Pic}(A) \to 1.$$

Beweis. Wir haben eiine Abbildung $K^\times \to J_A$ definiert durch $u \mapsto (u)$. Das Bild ist P_A also ist diese Sequenz exakt in $\mathrm{Pic}(A)$ und J_A. Es genügt zu zeigen, dass $N = \mathrm{Ker}(K^\times \to J_A) = A^\times$. Falls $u \in A^\times$, gilt $(u) = Au = A$ also $u \in N$. Umgekehrt, sei $u \in K^\times$ mit $(u) = A$. Es gilt $u \in A^\times$. ■

9 Zahlkörper

9.1 Spur und Norm

In diesem Abschnitt brauchen wir zuerst Resultate aus der Galoistheorie.

Definition 9.1.1 Sei $\mathsf{k} \subset K$ eine endliche Erweiterung und sei $x \in K$. Dann ist $L_x : K \to K, y \mapsto xy$ ein k-Endomorphismus.

1. **Die Spur** $\mathrm{Tr}_{K/\mathsf{k}}(x)$ **von** x ist $\mathrm{Tr}_{K/\mathsf{k}}(x) = \mathrm{Tr}(L_x)$.

2. **Die Norm** $N_{K/\mathsf{k}}(x)$ **von** x ist $N_{K/\mathsf{k}}(x) = \det(L_x)$.

In diesem Abschnitt wollen wir die Spur und die Norm von Elementen bestimmen.

Beispiel 9.1.2 Sei $\mathsf{k} = \mathbb{R}$ und $K = \mathbb{C}$. Sei $x = i = \sqrt{-1}$. In der Basis $(1, i)$ ist die Matrix von L_x der Form

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Es folgt $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(i) = 0 = (i + \bar{\imath})$ und $N_{\mathbb{C}/\mathbb{R}}(i) = 1 = i\bar{\imath}$.

Lemma 9.1.3 Sei $\mathsf{k} \subset K$ eine endliche Erweiterung mit $n = [K : \mathsf{k}]$ und sei $x \in K$. Sei $\chi_x = X^d + a_1 X^{d-1} + \cdots + a_d$ das Minimalpolynom von x über k. Dann gilt $r = \frac{n}{d} \in \mathbb{Z}$ und

$$\mathrm{Tr}_{K/\mathsf{k}}(x) = -ra_1 \text{ und } N_{K/\mathsf{k}}(x) = (-1)^r a_d^r.$$

Beweis. Wir zeigen, dass der k-Vektorraum K eine Basis der Form $(x^i y_j)_{i \in [0,d-1], j \in [1,r]}$ hat mit $y_1 = 1$. Da χ_x das Minimalpolynom von x ist, ist die Familie $(1, x, \cdots, x^{d-1})$ linear unabhängig. Sei $(x^i y_j)_{i \in [0,d-1], j \in [1,r]}$ eine linear unabhängige Familie. Es existiert eine solche Familie (mit $k = 1$ und $y_1 = 1$ zum Beispiel). Falls diese Familie erzeugend ist, sind wir fertig. Sonst gibt es ein $y_{r+1} \notin \langle x^i y_j \mid i \in [0, d-1], j \in [1, r] \rangle$. Wir zeigen, dass $(x^i y_j)_{i \in [0,d-1], j \in [1,r+1]}$ linear unabhängig ist. Seien $\lambda_{i,j} \in \mathsf{k}$ mit

$$\sum_{i=0}^{d-1} \sum_{j=1}^{r+1} \lambda_{i,j} x^i y_j = 0 \text{ also } y_{d+1} z = -\sum_{i=0}^{d-1} \sum_{j=1}^{r} \lambda_{i,j} x^i y_j,$$

wobei $z = \sum_{i=0}^{d-1} \lambda_{i,r+1} x^i$. Falls $z \neq 0$ gilt $z^{-1} \in \langle 1, x, \cdots, x^{d-1} \rangle$ und also $y_{d+1} \in \langle x^i y_j \mid i \in [0, d-1], j \in [1, r] \rangle$. Ein Widerspruch. Also gilt $z = 0$ und $\lambda_{i,r+1} = 0$ für alle i. Es folgt

$$\sum_{i=0}^{d-1} \sum_{j=1}^{r} \lambda_{i,j} x^i y_j = 0$$

und per Induktion $\lambda_{i,j} = 0$ für alle i und j.

Sei also $(x^i y_j)_{i \in [0,d-1], j \in [1,r]}$ eine Basis von K über k und sei $A \in M_d(\mathsf{k})$ die Matrix

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_d \\ 1 & 0 & \cdots & 0 & \vdots \\ 0 & 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & -a_2 \\ 0 & \cdots & 0 & 1 & -a_1 \end{pmatrix}$$

Dann ist in der obigen Basis die Matrix von L_x eine $r \times r$-Blockmatrix der Form

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A \end{pmatrix}.$$

Daraus folgt $\mathrm{Tr}_{K/\mathsf{k}}(x) = r\mathrm{Tr}(A) = -ra_1$ und $N_{K/\mathsf{k}}(x) = \det(A)^r = (-1)^r a_d^r$. ∎

Lemma 9.1.4 Sei $\mathsf{k} \subset K$ eine endliche separable Erweiterung mit $n = [K : \mathsf{k}]$. Dann gibt es eine endliche Erweiterung $\mathsf{k} \subset L$ so, dass $K \otimes_{\mathsf{k}} L \simeq L^n$ als L-Algebren. □

Beweis. Da die Erweiterung $\mathsf{k} \subset K$ separabel ist gibt es ein separables Element $x \in K$ so, dass $K = \mathsf{k}(x)$ (Satz vom primitiven Element). Sei χ_x das Minimalpolynom von x über k. Es gilt $n = [K : \mathsf{k}] = \deg(\chi_x)$. Sei $L = D_{\mathsf{k}}(\chi_x)$ der Zerfalungskörper von χ_x über k. Da x separabel ist sind die Nullstellen $x_1, \cdots, x_n$ von χ_x paarweise verschieden. In $L[X]$ gilt also $\chi_x(X) = \prod_{i=1}^n (X - x_i)$. Es folgt

$$K \otimes_{\mathsf{k}} L = \mathsf{k}(x) \otimes_{\mathsf{k}} L \simeq \mathsf{k}[X]/(\chi_x) \otimes_{\mathsf{k}} L \simeq L[X]/(\chi_x) = L[X]/(\prod_{i=1}^n (X - x_i)).$$

Es gilt aber $(\prod_{i=1}^n (X - x_i)) = (X - x_1) \cdots (X - x_n)$. Da die Ideale $(X - x_i)$ maximale Ideale sind, sind diese Ideale paarweise teilerfremd und also $(X - x_1) \cdots (X - x_n) = (X - x_1) \cap \cdots \cap (X - x_n)$. Es folgt nach dem Chinesischen Restsatz, dass wir einen Isomorphismus

$$K \otimes_{\mathsf{k}} L \simeq L[X]/(\prod_{i=1}^n (X - x_i)) \simeq \prod_{i=1}^n L[X]/(X - x_i) \simeq L^n$$

haben. ∎

Lemma 9.1.5 Seien $\mathsf{k} \subset K$ und $\mathsf{k} \subset L$ Erweiterungen. Dann ist die Menge aller k-Algebrahomomorphismen von K nach L eine L-linear unabhängige Familie von $\mathrm{Hom}_{\mathsf{k}}(K, L)$ (der Vektorraum aller k-linearen Abbildungen von mit K nach L. □

Beweis. Wir zeigen per Induktion über die Anzahl von Elementen, dass jede endliche Familie von k-Algebrahomomorphismen L-linear unabhängig ist. Für $n = 0$ ist die Aussage klar. Wir nehmen an, dass die Aussage für alle Familien mit weniger als $n-1$ Elementen gilt. Sei $(u_1, \cdots, u_n)$ eine Familie von nicht trivialen paarweise verschiedenen k-Algebrahomomorphismen und seien $a_1, \cdots, a_n \in L$ mit $\sum_i a_i u_i = 0$. Für alle $x, y \in K$ gilt

$$\sum_{i=1}^{n} a_i(u_i(x) - u_n(x))u_i(y) = \sum_{i=1}^{n} a_i u_i(xy) - u_n(x) \sum_{i=1}^{n} a_i u_i(y) = 0.$$

Damit haben wir

$$\sum_{i=1}^{n-1} a_i(u_i(x) - u_n(x))u_i = 0$$

und per Induktion $a_i(u_i(x) - u_n(x)) = 0$ für alle $x \in K$ und alle $i \leq n-1$. Da $u_i \neq u_n$ gibt es ein x mit $u_i(x) \neq u_n(x)$ und es folgt $a_i = 0$ für alle $i \leq n-1$. Es folgt auch $a_n = 0$, weil $u_n \neq 0$. ■

Korollar 9.1.6 Sei $\mathsf{k} \subset K$ eine endliche separable Erweiterung mit $n = [K : \mathsf{k}]$. Dann gibt es eine endliche Erweiterung $\mathsf{k} \subset L$ und n k-Algebrahomomorphismen $u_1, \cdots, u_n : K \to L$ so, dass gilt

1. $\{u_1, \cdots, u_n\}$ ist die Menge aller k-Algebrahomomorphimen von K nach L;
2. $v_1 \times \cdots \times v_n : K \otimes_{\mathsf{k}} L \simeq L^n$ als L-Algebren, wobei $v_i(x \otimes y) = u_i(x)y$.

Beweis. Sei L so, dass $\varphi : K \otimes_{\mathsf{k}} L \simeq L^n$. Sei $p_i : L^n \to L$ die i-te Projektion und sei $u_i : K \to L$ definiert durch $u_i(x) = p_i(\varphi(x \otimes 1))$. Man überprüft leicht, dass u_i ein k-Algebrahomomorphismus ist und, dass $u_1, \cdots, u_n$ paarweise verschieden sind also ist $(u_1, \cdots, u_n)$ eine L-linear unabhängige Familie in $\mathrm{Hom}_{\mathsf{k}}(K, L)$. Es gilt aber $\mathrm{Hom}_{\mathsf{k}}(K, L) = K^\vee \otimes_{\mathsf{k}} L \simeq \mathsf{k}^n \otimes_{\mathsf{k}} L \simeq L^n$ also gilt $\dim_L \mathrm{Hom}_{\mathsf{k}}(K, L) = n$ und $(u_1, \cdots, u_n)$ ist eine Basis. Aus dem obigen Lemma folgt, dass $\{u_1, \cdots, u_n\}$ die Menge aller k-Algebrahomomorphimen von K nach L ist.

Außerdem ist $v_i : K \otimes_{\mathsf{k}} L \to L, x \otimes y \mapsto u_i(x)y$ wohl definiert und es gilt (da p_i und φ beide L-linear sind): $v_i(x \otimes y) = u_i(x)y = p_i(\varphi(x \otimes 1))y = p_i(\varphi(x \otimes y))$ also $v_i = p_i \circ \varphi$ und $v_1 \times \cdots \times v_n = \varphi$ ist ein Isomorphismus. ■

Korollar 9.1.7 Sei $\mathsf{k} \subset K$ eine endliche separable Erweiterung mit $n = [K : \mathsf{k}]$ und seien $\mathsf{k} \subset L$ und $u_1, \cdots, u_n : K \to L$ wie im obigen Korollar.

Sei $x \in K$, dann gilt

$$\mathrm{Tr}_{K/\mathsf{k}}(x) = \sum_{i=1}^{n} u_i(x) \text{ und } N_{K/\mathsf{k}}(x) = \prod_{i=1}^{n} u_i(x).$$

Beweis. Sei $L_{x,L} : K \otimes_{\mathsf{k}} L \to K \otimes_{\mathsf{k}} L, y \otimes a \mapsto xy \otimes a$. Es gilt $L_{x,L} = L_x \otimes \mathrm{Id}_L$ und $\mathrm{Tr}(L_{x,L}) = \mathrm{Tr}_{K/\mathsf{k}}(x) \otimes 1$ und $\det(L_{x,L}) = N_{K/\mathsf{k}}(x) \otimes 1$. Aber $K \otimes_{\mathsf{k}} L \simeq L^n, y \otimes a \mapsto (u_1(y)a, \cdots, u_n(y)a)$. Dank dieser Identifizierung ist $L_{x,L}$ der Form $L_{x,L}(u_1(y)a, \cdots, u_n(y)a) = (u_1(xy)a, \cdots, u_n(xy)a) = (u_1(x)u_1(y)a, \cdots, u_n(x)u_n(y)a)$. die Matrix von $L_{x,L}$ der Form

$$\begin{pmatrix} u_1(x) & 0 & \cdots & 0 \\ 0 & u_2(x) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & u_n(x) \end{pmatrix}.$$

Daraus folgt $\mathrm{Tr}(L_{x,L}) = \sum_{i=1}^n u_i(x)$ und $\det(L_{x,L}) = \prod_{i=1}^n u_i(x)$ und die Aussage. ■

Beispiel 9.1.8 Sei $\mathsf{k} = \mathbb{R}$ und $K = \mathbb{C}$. Sei $L = \mathbb{C}$ und $u_1, u_2 : \mathbb{C} \to \mathbb{C}$ definiert durch $u_1(x) = x$ und $u_2(x) = \bar{x}$. Dann sind u_1 und u_2 $\mathbb{R}$-Algebrahomomorphismen und da $[\mathbb{C} : \mathbb{R}] = 2$ sind es die einzige $\mathbb{R}$-Algebrahomomorphismen. Es gilt also $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(x) = u_1(x) + u_2(x) = x + \bar{x}$ und $N_{\mathbb{C}/\mathbb{R}}(x) = u_1(x)u_2(x) = x\bar{x} = |x|^2$.

Definition 9.1.9 Sei $\mathsf{k} \subset K$ eine Erweiterung und sei $(x_1, \cdots, x_n)$ eine Familie von Elementen aus K. Die Determinante $D_{K/\mathsf{k}}(x_1, \cdots, x_n)$ der Matrix $(\mathrm{Tr}_{K/\mathsf{k}}(x_i x_j))_{i,j \in [1,n]}$ heißt **Diskriminante von** $(x_1, \cdots, x_n)$:

$$D_{K/\mathsf{k}}(x_1, \cdots, x_n) = \det((\mathrm{Tr}_{K/\mathsf{k}}(x_i x_j))_{i,j \in [1,n]}).$$

Korollar 9.1.10 Sei $\mathsf{k} \subset K$ eine endliche separable Erweiterung mit $n = [K : \mathsf{k}]$ und seien $\mathsf{k} \subset L$ und $u_1, \cdots, u_n : K \to L$ wie im obigen Korollar.

Sei $(x_1, \cdots, x_n) \in K$ eine Familie, dann gilt

$$D_{K/\mathsf{k}}(x_1, \cdots, x_n) = \det((u_i(x_j))_{i,j \in [1,n]})^2.$$

Beweis. Sei $U = (u_i(x_j))$ und $T = U^T U = (t_i i, j)$ mit $t_{i,j} = \sum_k u_k(x_i) u_k(x_j)$. Es gilt

$$\mathrm{Tr}_{K/\mathsf{k}}(x_i x_j) = \sum_k u_k(x_i x_j) = \sum_k u_k(x_i u_k(x_j) = t_{i,j}.$$

Es folgt $D_{K/\mathsf{k}}(x_1, \cdots, x_n) = \det(T) = \det(U^T U) = \det(U)^2 = \det((u_i(x_j))_{i,j \in [1,n]})^2$. ■

Korollar 9.1.11 Sei $\mathsf{k} \subset K$ eine endliche separable Erweiterung. Dann ist die Bilinearform $B : K \times K \to \mathsf{k}$ definiert durch $B(x, y) = \mathrm{Tr}_{K/\mathsf{k}}(xy)$ nicht ausgeartet.

Beweis. Sei $(x_1, \cdots, x_n)$ eine Basis von K als k-Vektorraum. Die Matrix von B ist die Matrix $(\mathrm{Tr}_{K/\mathsf{k}}(x_i x_j))_{i,j \in [1,n]}$ und ihre Determinant ist $D_{K/\mathsf{k}}(x_1, \cdots, x_n) = \det((u_i(x_j))_{i,j \in [1,n]})^2$. Aber $\varphi : K \otimes_{\mathsf{k}} L \to L^n, x \otimes y \mapsto (u_1(x)y, \cdots, u_n(x)y)$ ist ein Isomorphismus also ist $(\varphi(x_1), \cdots, \varphi(x_n))$ eine Basis von L_n. Es gilt aber $\varphi(x_i) = (u_1(x_i), \cdots, u_n(x_i)$ also ist die Matrix $(u_i(x_j))_{i,j \in [1,n]}$ invertierbar. Daraus folgt die Aussage. ■

9.2 Ein Endlichkeitssatz

Proposition 9.2.1 Sei A ein ganz abgeschlossener Integritätsring und $K = \mathrm{Frac}(A)$. Sei $K \subset K'$ eine endliche separable Erweiterung und sei B der algebraische Abschluss von A in K'.

Dann gibt es eine K-Basis $v_1, \cdots, v_n \in K'$ so, dass $B \subset Av_1 + \cdots + Av_n$.

Beweis. Sei $w \in K'$. Dann ist w algebraisch über K also gibt es $x_0, \cdots, x_r \in K$ mit $x_0 w^r + \cdots + x_r = 0$. Dank Multiplikation mit den Nennern gibt es $a_0, \cdots, a_r \in A$ mit $a_0 w^r + \cdots a_n = 0$. Dank Multiplikation mit a_0^{r-1} erhält man, dass $u = a_0 w$ ganz über A ist. Daraus folgt, das modulo Muliplikation mit Elementen aus A kann man eine Basis $(w_1, \cdots, w_n)$ von K' über K ersetzen durch einer Basis $(u_1, \cdots, u_n)$ von K' über K so, dass u_i ganz über A ist für alle i. Also gilt $u_i \in B$ für alle i.

Sei $B : K' \times K' \to K$ die Bilinearfrom $B(x, y) = \mathrm{Tr}_{K'/K}(xy)$. Diese Bilinearform ist nicht ausgeartet also gibt es eine Basis $(v_1, \cdots, v_n)$ von K' über K so, dass $B(u_i, v_j) = \delta_{i,j}$. Wir zeigen, dass $B \subset Av_1 + \cdots + Av_n$.

Sei $x \in B$. Es gibt Elemente $x_i \in K$ mit $x = \sum_i x_i v_i$. Wir zeigen $x_i \in A$. Es gilt $u_i \in B$ und $x \in B$ also $xu_i \in B$. Das Minimalpolynom von xu_i hat also Koeffizienten in A nach Proposition 4.3.7. Es folgt aus Lemma 9.1.3, dass $\mathrm{Tr}_{K/\mathsf{k}}(xu_i) \in A$. Daraus folgt $x_i = \sum_j x_j \mathrm{Tr}_{K/\mathsf{k}}(v_j u_i) = \mathrm{Tr}_{K/\mathsf{k}}(\sum_j x_j v_j u_i) = \mathrm{Tr}_{K/\mathsf{k}}(xu_i) \in A$. Es folgt $x \in Av_1 + \cdots + Av_n$ und also $B \subset Av_1 + \cdots + Av_n$. ∎

Korollar 9.2.2 Sei k ein Körper mit $\mathrm{char}(\mathsf{k}) = 0$ und A eine endlich ezeugte k-Algebra so, dass A ein Integritätsring ist. Sei K der Quotientkörper von A und $\bar{A}$ der ganze Abschluss von A.

Dann ist $\bar{A}$ ein endlich erzeugter A-Modul und insbesondere eine endlich erzeugte k-Algebra.

Beweis. Nach Noetherschem Lemma gibt es eine Transzendenzbasis $x_1, \cdots, x_n \in A$ von K über k so, dass A ganz über $A' = \mathsf{k}[x_1, \cdots, x_n]$ ist. Sei $K' = \mathsf{k}(x_1, \cdots, x_n)$. Dann ist die Erweiterung $K' \subset K$ endlich. Der ganze Abschluss von A' in K ist $\bar{A}$. Nach der obigen Proposition gibt es Elemente $v_1, \cdots, v_n \in K$ so, dass $\bar{A} \subset A'v_1 + \cdots + A'v_n$. Der A'-Modul $M = A'v_1 + \cdots + A'v_n$ ist endlich erzeugt und A' ist noethersch also ist M noethersch. Es folgt, dass $\bar{A}$ endlich erzeugt als A'-Modul ist alsi ist $\bar{A}$ endlich erzeugt als A-Modul. Es folgt, dass $\bar{A}$ endlich erzeugt als A-Algebra ist und also auch als k-Algebra. ∎

Die Aussage ist ohne Charakteristik-Annahme auch wahr (Siehe Serre local algera Proposition 16 Seite 46):

Theorem 9.2.3 Sei k ein Körper und A eine endlich ezeugte k-Algebra so, dass A ein Integritätsring ist. Sei K der Quotientkörper von A und $\bar{A}$ der ganze Abschluss von A.

Dann ist $\bar{A}$ ein endlich erzeugter A-Modul und insbesondere eine endlich erzeugte k-Algebra. □

Bemerkung 9.2.4 Diese Aussage ist für beliebige Integritätsringe nicht mehr wahr. Ringe für die, diese Aussage gilt heißen **japanische Ringe**.

9.3 Zahlkörper

Definition 9.3.1 1. Eine endliche Erweiterung von $\mathbb{Q}$ heißt **Zahlkörper**.

2. Sei K ein Zahlkörper. Der ganze Abschluss von $\mathbb{Z}$ in K heißt **Ring der ganzen Zahlen in** K.

Satz 9.3.2 Der Ring der ganzen Zahlen eines Zahlkörpers ist ein Dedekinsring. □

Beweis. Sei K ein Zahlkörper und sei A der Ring der ganzen Zahlen in K. Die Erweiterung $\mathbb{Q} \subset K$ is separabel, weil $\mathrm{char}(\mathbb{Q}) = 0$. Es gibt also Elemente $v_1, \cdots, v_n \in A$ so, dass $A \subset \mathbb{Z}v_1 + \cdots + \ v_n$. Der Ring A ist also ein $\mathbb{Z}$-Untermodul von einem endlich erzeugten $\mathbb{Z}$-Modul. Da $\mathbb{Z}$-noethersch ist, ist A endlich als $\mathbb{Z}$-Modul also eine endlich erzeugte $\mathbb{Z}$-Algebra und somit ein noetherscher Ring.

Wir zeigen $K = \mathrm{Frac}(A)$. Da $A \subset K$, gilt $\mathrm{Frac}(A) \subset K$. Sei $x \in K$. Dann ist x algebraisch über $\mathbb{Q}$ und also gibt es Elemente $a_0, \cdots, a_n \in \mathbb{Q}$ mit $a_n x^n + \cdots + a_0 = 0$. Dank Multiplikation mit einem Element aus $\mathbb{Z}$ können wir annehmen, dass $a_0, \cdots, a_n \in \mathbb{Z}$. Dank Multiplikation mit a_n^{n-1} gilt für $y = a_n x$: $y^n + b_1 y^{n-1} + \cdots + b_{n-1} = 0$ mit $b_i \in \mathbb{Z}$. Es folgt, dass y ganz über $\mathbb{Z}$ ist und also $y \in A$. Es folgt $x = y/a_n \in \mathrm{Frac}(A)$.

Da A der ganze Abschluss von $\mathbb{Z}$ in K ist, ist A ganz abgeschlossen in K und ist A ganz abgeschlossen.

Aus der Proposition 5.3.5 folgt, dass $\mathrm{Kdim}(A) = \mathrm{Kdim}(\mathbb{Z}) = 1$. ■

Bemerkung 9.3.3 Für K ein Zahlkörper und A der Ring der ganzen Zahlen, kann man zeigen, dass $\mathrm{Pic}(A)$ endlich ist.

10 Vervollständigung

10.1 Topologische Gruppen

Definition 10.1.1 Eine topologische abelsche Gruppe ist eine Gruppe G, die auch ein topologischer Raum ist so, dass die Abbildungen $G \times G \to G$, $(x, y) \mapsto x + y$ und $G \to G$, $x \mapsto -x$ stetig sind (in $G \times G$ benutzen wir die Produkttopologie).

Bemerkung 10.1.2 1. Eine abelsche topologische Gruppe ist nicht immer Hausdorff. Falls $\{0\}$ abgeschlossen ist, ist $\Delta_G = \{(x, x) \mid x \in G\}$ abegschlossen: es gilt

$$\Delta_G = \mu^{-1}(0), \text{ wobei } \mu : G \times G \to G, \; \mu(x, y) = x - y.$$

Dies ist äquivalent zu: G ist Hausdorff. Andersrum, falls G Hausdorff ist, ist $\{0\}$ abgeschlossen: sei $x \neq 0$ und seien U, V Umgebungen von 0 und x mit $U \cap V = \emptyset$. Es folgt $x \notin V^c$ aber V^c ist abgeschlossen mit $0 \in V^c$ also $\overline{\{0\}} \subset V^c \not\ni x$.

Eine abelsche topologische Gruppe ist genau dann Haudorff, wenn $\{0\}$ abgeschlossen ist.

2. Sei $a \in G$. Die Translation $T_a : G \to G$, $T_a(x) = a + x$ ist ein Homöomorphismus (T_a ist stetig mit inverse T_{-a}). Wenn man die Umbebungen von 0 kennt, kennt man die Umbegungen von a für alle $a \in G$. Um die Topologie zu bestimmen genügt es also alle Umgebungen von 0 zu kennen.

Lemma 10.1.3 Sei G eine abelsche topologische Gruppe und sei H der Durchschnitt aller Umbegungen von 0 in G:

$$H = \bigcap_{U \text{ Umgebung von } 0} U.$$

1. Dann ist H eine Untergruppe von G.

2. $H = \overline{\{0\}}$.

3. G/H ist Hausdorff.

4. G Hausdorff $\Leftrightarrow H = \{0\}$. $\square$

Beweis. 1. Seien $x, y \in H$ und sei U eine Umbegung von 0. Sei $\varphi : G \times G \to G$. Dann ist $\varphi^{-1}(U)$ eine Umgebung von $(0,0)$ und also gibt es Umbegungen V und W von 0 mit $V \times W \subset \varphi^{-1}(U)$. Es folgt $(x,y) \in V \times W \subset \varphi^{-1}(U)$ und also $x-y = \varphi(x,y) \in U$.

2. Sei $x \in G$. Es gilt

$$\begin{aligned} x \in H \quad & \Leftrightarrow -x \in H \\ & \Leftrightarrow -x \in U \text{ für alle } U \text{ Umgebung von } 0 \\ & \Leftrightarrow 0 \in U + x \text{ für alle } U \text{ Umgebung von } 0 \\ & \Leftrightarrow 0 \in V \text{ für alle } V \text{ Umgebung von } x \\ & \Leftrightarrow x \in \overline{\{0\}}. \end{aligned}$$

3. Die Gruppe G/H ist eine abelsche topologische Gruppe für die Quotienttopologie. Es gilt ($\{[0]\}$ abgeschlossen $\Leftrightarrow$ H abgeschlossen). Also ist $\{[0]\}$ abgeschlossen und G/H Hausdorff.

4. Folgt aus der obigen Bemerkung. ∎

10.2 Cauchyfolgen

Definition 10.2.1 1. Sei $(x_n)_{n \in \mathbb{N}}$ eine Folge von Elementen aus G. Diese Folge heißt **Cauchy**, falls gilt: für alle U Umgebung von 0 gibt es ein $s(U) \in \mathbb{N}$ so, dass $x_n - x_m \in U$ gilt für alle $n, m \geq s(U)$.

2. Zwei Cauchyfolgen (x_n) und (y_n) heißen **äquivalent** falls gilt: für alle U Umgebung von 0 gibt es ein $s(U) \in \mathbb{N}$ so, dass $x_n - y_n \in U$ gilt für alle $n \geq s(U)$ (*i.e.* $\lim_\infty (x_n - y_n) = 0$).

Lemma 10.2.2 1. Falls (x_n) und (y_n) Cauchyfolgen sind, ist auch $(x_n - y_n)$ eine Cauchyfolge.

2. Die Relation $(x_n) \sim (y_n) \Leftrightarrow x_n - y_n \to 0$ ist eine Äquivalenzrelation.

Sei $[x_n]$ die Klasse von (x_n) für $\sim$.

3. Seien (x_n) und (y_n) Cauchyfolgen. Dann hängt die Klasse $[x_n - y_n]$ nur von $[x_n]$ und $[y_n]$ ab. Insbesondere ist die Menge aller Äquivalenzklassen eine Gruppe für $+$. □

Beweis. Übung. ∎

Definition 10.2.3 Sei G eine abelsche topologische Gruppe. Die Menge aller Äquivalenzklassen von Cauchyfolgen heißt **Vervollständigung von** G und ist mit $\widehat{G}$ bezeichnet.

Bemerkung 10.2.4 Sei $x \in G$ und (x_n) die Folge mit $x_n = x$ für alle $n \in \mathbb{N}$. Dann ist (x_n) eine Cauchyfolge und es gibt eine Abbildung

$$\varphi : G \to \widehat{G}$$

definiert durch $\varphi(x) = [x_n]$, wobei $x_n = x$ für alle n.

Lemma 10.2.5 Die Abbildung $\varphi : G \to \widehat{G}$ ist ein Gruppenhomomorphismus. □

Beweis. Übung. ■

Lemma 10.2.6 Es gilt

$$\mathrm{Ker}\varphi = H = \bigcap_{U \text{ Umgebung von } 0} U.$$

Beweis. Es gilt $x \in \mathrm{Ker}\varphi \Leftrightarrow \varphi(x) = [0] \Leftrightarrow (x_n) \to 0$ mit $x_n = x$ für alle $n \Leftrightarrow$ für jede Umgebung U gibt es ein $s(U)$ mit $x_n \in U$ für $n \geq s(U) \Leftrightarrow$ für jede Umgebung U gilt $x \in U \Leftrightarrow x \in H$. ■

Korollar 10.2.7 G Hausdorff $\Leftrightarrow$ φ ist injektiv.

Lemma 10.2.8 Seien G und G' zwei abelsche topologische Gruppen und sei $f : G \to G'$ ein stetiger Gruppenhomomorphismus.

1. Sei (x_n) eine Cauchyfolge in G, dann ist $(f(x_n))$ eine Cauchyfolge in G'.

2. Dies definiert eine Abbildung $\widehat{f} : \widehat{G} \to \widehat{G'}$ durch $[x_n] \mapsto [f(x_n)]$. Diese Abbilung ist ein Gruppenhomomorphismus und das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\varphi_G} & \widehat{G} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \widehat{f}} \\ G' & \xrightarrow{\varphi_H} & \widehat{G'} \end{array}$$

ist kommutativ.

3. Seien $f : G \to G'$ und $f' : G' \to G''$ zwei stetige Gruppenhomomorphismen. Dann gilt $\widehat{f' \circ f} = \widehat{f'} \circ \widehat{f}$. □

Beweis. Übung. ■

10.3 Projektive Limes I

Definition 10.3.1 1. Eine Familie $(A_n)_{n\in\mathbb{N}}$ von Mengen und Abbildungen $f_{j,i} : A_j \to A_i$ für alle $i \leq j$ so, dass $f_{i,i} = \mathrm{Id}_{A_i}$ und $f_{k,i} = f_{k,j} \circ f_{j,i}$ für alle $i \leq j \leq k$ heißt **projektives System oder inverses System**

2. Sei $(A_i, f_{i,j})$ ein projektives System. **Der projektive Limes oder der inverse Limes von** $(A_i, f_{i,j})$ ist die Menge

$$\varprojlim A_n = \left\{ (a_n) \in \prod_{n=0}^{\infty} A_n \mid f_{n,m}(a_n) = a_m \text{ für alle } n \geq m \right\}.$$

Beispiel 10.3.2 Sei A eine Menge und $(A_n)_{n\in\mathbb{N}}$ eine Familie von Teilmengen so, dass $A_{n+1} \subset A_n$ für alle $n \in \mathbb{N}$. Für alle $j \geq i$, sei $f_{j,i} : A_j \to A_i$ die Enthaltung. Dann ist die Abbildung

$$\bigcap_{n=0}^{\infty} A_n \to \varprojlim A_n$$

definiert durch $a \mapsto (a)_{n\in\mathbb{N}}$ eine Bijektion, wobei $(a)_{n\in\mathbb{N}}$ die konstante Folge ist.

Lemma 10.3.3 Falls alle A_n Ringe (bzw. Gruppen, bzw. Körper, bzw. A-Moduln...) sind und alle Abbildungen $f_{j,i}$ Ringhomomorphismen (bzw. Gruppenhomomorphismen, bzw. Körperhomomorphismen bzw. A-Modulhomomorphisen...) sind, ist auch $\varprojlim A_n$ ein Ring (bzw. eine Gruppe, bzw. ein Körper bzw. ein A-Moduln...). □

Beweis. Übung. ■

Beispiel 10.3.4 1. Sei p eine Primzahl und $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Dann gibt es eine (surjektive) Abbildung $f_{n,m} : A_n = \mathbb{Z}/p^n\mathbb{Z} \to A_m = \mathbb{Z}/p^m\mathbb{Z}$ für alle $n \geq m$. Der inverse Limes

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

heißt **Ring der p-adischen Zahlen**.

2. Sei k ein Körper, $A = \mathsf{k}[X]$ und $\mathfrak{m} = (X)$. Sei $A_n = A/\mathfrak{m}^n = \mathsf{k}[X]/(X^n)$. Dann gibt es eine (surjektive) Abbildung $f_{n,m} : A_n \to A_m$ für alle $n \geq m$. Der inverse Limes

$$\mathsf{k}[[X]] = \varprojlim A_n$$

heißt **Ring der formalen Potenzreihen**. Es gibt ein Isomorphismus

$$\mathsf{k}[[X]] \to \left\{ \sum_{n=0}^{\infty} a_n X^n \mid a_n \in \mathsf{k} \right\}.$$

Die Abbildung is gegeben durch $\sum_{k=0}^{\infty} a_k X^k \mapsto ([\sum_{k=0}^{n-1} a_k X^k])_{n\in\mathbb{N}}$.

Analog definiert man $\mathsf{k}[[X_1, \cdots, X_n]]$.

10.4 Projektive Limes und Vervollständigung

Ab jetzt betrachten wir spezielle topologische abelsche Gruppen: wir nehmen an, dass G eine Basis aller Umgebungen von 0 der Form

$$G = G_0 \supset G_1 \supset \cdots \supset G_n \supset \cdots$$

hat, wobei G_n eine Untergruppe ist. Mit anderen Wörter ist eine Teilmenge $U \subset G$ genau dann eine Umgebung von 0, wenn es ein n gibt mit $G_n \subset U$.

Beispiel 10.4.1 Sei p eine Primzahl. Die p-adische Topologie von $\mathbb{Z}$ ist dank der Basis $(p^n\mathbb{Z})_{n\in\mathbb{N}}$ von Umgebungen von 0 definiert.

Allgemeiner, sei A ein Ring und $\mathfrak{a} \subset A$ eine Ideal. Die $\mathfrak{a}$-adische Topologie von A ist die Topologie definiert dank der Basis $(\mathfrak{a}^n)_{n\in\mathbb{N}}$.

Lemma 10.4.2 Die Untergruppen G_n sind offen und abgeschlossen. □

Beweis. Sei $x \in G_n$. Dann ist $x + G_n$ eine Umgebung von x_n aber da G_n eine Gruppe ist folgt $x_n + G_n \subset G_n$ also ist G_n offen. Es folgt, dass $x + G_n$ offen ist für alle $x \in G$. Insbesondere ist $\cup_{x\notin G_n}(x + G_n)$ offen. Es ist aber das Komplement von G_n und also ist G_n abgeschlossen. ■

Satz 10.4.3 Es gibt ein Isomorphismus $\widehat{G} \simeq \varprojlim(G/G_n)$. □

Beweis. Sei $\varphi_n : G \to G/G_n$ die kanonische Projektion und $\varphi_{n,m} : G/G_n \to G/G_m = (G/G_n)/(G_m/G_n)$ die kanonische Projektion. Es gilt $\varphi_{n,m} \circ \varphi_n = \varphi_m$.

Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in G. Für jede Zahl n gibt es ein $s(n) \in \mathbb{N}$ mit $x_k - x_l \in G_n$ für alle $k, l \geq s(n)$. Die Folge $(\varphi_n(x_k))_{k\in\mathbb{N}}$ ist also stationär. Sei $\xi_n = \varphi_n(x_k)$ für $k \gg 0$. Es gilt $\varphi_{n,m}(\xi_n) = \varphi_{n,m}(\varphi_n(x_k)) = \varphi_m(x_k) = \xi_m$ für alle $k \gg 0$. Es folgt, dass $(\xi_n)_{n\in\mathbb{N}} \in \varprojlim(G/G_n)$.

Dies definiert eine Abbildung $\varphi : \widehat{G} \to \varprojlim(G/G_n)$ und man überprüft (Übung), dass es ein Gruppenhomomorphismus ist.

Sei $(x_n)_{n\in\mathbb{N}} \in \mathrm{Ker}\varphi$. Es gilt $\xi_n = 0$ für alle n. Also gilt $\varphi_n(x_k) = \xi_n = 0$ für alle $k \gg 0$ *i.e.* $x_k \in G_n$ für alle $k \gg 0$. Es folgt $\lim_\infty x_n = 0$ und also $[(x_n)_{n\in\mathbb{N}}] = 0$.

Sei $(\xi_n)_{n\in\mathbb{N}} \in \varprojlim(G/G_n)$. Sei $x_n \in G$ mit $\varphi_n(x_n) = \xi_n$. Wir zeigen, dass $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist und dass $\varphi_n(x_k) = \xi_n$ für $k \gg 0$.

Für $k \geq n$, gilt $\varphi_n(x_k) = \xi_n = \varphi_{k,n}(\xi_k) = \varphi_{k,n}(\varphi_k(x_k)) = \varphi_n(x_k)$ also $x_k - x_n \in G_n$. Insbesondere ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge. Außerdem gilt $\varphi_n(x_k) = \xi_n$ für alle $k \gg 0$. Es folgt $\varphi((x_n)_{n\in\mathbb{N}}) = (\xi_n)_{n\in\mathbb{N}}$. ■

10.5 Projektive Limes II

Definition 10.5.1 Seien $(A_i, f_{i,j})$ und $(B_i, g_{i,j})$ zwei projektive Systeme. **Ein Morphismus** $\varphi : (A_i, f_{i,j}) \to (B_i, g_{i,j})$ **von projektiven Systemen** ist eine Familie von Abbildungen $\varphi_i : A_i \to B_i$ so, dass $\varphi_i \circ f_{j,i} = g_{j,i} \circ \varphi_j$.

Dann ist die Abbildung $\varprojlim \varphi_n : \varprojlim A_n \to \varprojlim B_n$, $(a_n)_{n\in\mathbb{N}} \to (\varphi_n(a_n))_{n\in\mathbb{N}}$ wohl definiert.

Definition 10.5.2 Ein projektives System $(A_i, f_{i,j})$ heißt **surjektiv** falls alle Abbildungen $f_{j,i} : A_j \to A_i$ für $j \geq i$ surjektiv sind.

Proposition 10.5.3 Seien $(A_i, f_{i,j})$, $(A'_i, f'_{i,j})$ und $(A''_i, f''_{i,j})$ drei projektive Systeme von A-Moduln. Seien $u : (A'_i, f'_{i,j}) \to (A_i, f_{i,j})$ und $v : (A_i, f_{i,j}) \to (A''_i, f''_{i,j})$ zwei Morphismen von projektiven Systemen so, dass alle Abbildungen A-linear sind und

$$0 \to A'_n \stackrel{u}{\to} A_n \stackrel{v}{\to} A''_n \to 0$$

eine exakte Sequenz ist, für alle $n \in \mathbb{N}$. Ein solches Datum heißt **exakte Sequenz von projektiven Systemen** und ist mit

$$0 \to (A'_i, f'_{i,j}) \stackrel{u}{\to} (A_i, f_{i,j}) \stackrel{v}{\to} (A''_i, f''_{i,j}) \to 0$$

dargestellt.

1. Dann ist die Sequenz

$$0 \to \varprojlim A'_n \stackrel{\varprojlim u}{\to} \varprojlim A_n \stackrel{\varprojlim v}{\to} \varprojlim A''_n$$

exakt.

2. Falls $(A'_i, f'_{i,j})$ surjektiv ist, ist die Sequenz

$$0 \to \varprojlim A'_n \stackrel{\varprojlim u}{\to} \varprojlim A_n \stackrel{\varprojlim v}{\to} \varprojlim A''_n \to 0$$

exakt.

Beweis. 1. Sei $(a'_n)_{n\in N} \in \mathrm{Ker}(\varprojlim u)$. Dann gilt $u_n(a'_n) = 0$ für alle n und also $a'_n = 0$ für alle n.

Sei $(a'_n)_{n\in N} \in \varprojlim A'_n$. Dann gilt $\varprojlim v(\varprojlim u(a'_n)) = (v(u(a'_n))_{n\in\mathbb{N}} = 0$.

Sei $(a'_n)_{n\in N} \in \mathrm{Ker}(\varprojlim v)$. Es gilt $v_n(a_n) = 0$ also gibt es ein $a'_n \in A'_n$ mit $u(a'_n) = a_n$. Es gilt auch $u_m(f'_{n,m}(a'_n)) = f_{n,m}(u(a_n)) = f_{n,m}(a_n) = a_m = u_m(a'_m)$. Da u'_m injektiv ist, folgt $f'_{n,m}(a'_n) = a'_m$ und $(a'_n) \in \varprojlim A'_n$ mit $\varprojlim u(a'_n) = (a_n)$.

2. Sei $(a''_n)_{n\in N} \in \varprojlim A''_n$. Wir zeigen, per Induktion nach n, dass es eine Familie $(a_m)_{m\in[0,n]}$ gibt mit $a_m \in A_m$ und $f_{j,i}(a_j) = a_i$ für alle $i, j \in [0, n]$ mit $j \geq i$.

Für $n = 0$ ist die Aussage klar. v_0 ist surjektiv. Sei $(a_m)_{m\in[0,n-1]}$ eine solche Familie. Es genügt zu zeigen, dass es ein $a_n \in A_n$ gibt mit $f_{n,n-1}(a_n) = a_{n-1}$ und $v_n(a_n) = a''_n$.

Da v_n surjektiv ist gibt es ein b_n mit $v_n(b_n) = a''_n$. Es folgt $v_{n-1}(f_{n,n-1}(b_n)) = f''_{n,n-1}(v(b_n)) = f''_{n,n-1}(a''_n) = a''_{n-1}$. Also gilt $f_{n,n-1}(b_n) - a_{n-1} \in \mathrm{Ker}(v_{n-1}) = \mathrm{Im}(u_{n-1})$. Sei also $a'_{n-1} \in A'_{n-1}$ mit $u_{n-1}(a'_{n-1}) = f_{n,n-1}(b_n) - a_{n-1}$. Da alle $f'_{n,m}$ surjektiv sind gibt es ein $a'_n \in A'_n$ mit $f'_{n,n-1}(a'_n) = a'_{n-1}$. Sei $a_n = b_n - u_n(a'_n)$. Es gilt $v_n(a_n) = v_n(b_n) - v_n(u_n(a'_n)) = a''_n$. Es gilt auch $f_{n,n-1}(a_n) = f_{n,n-1}(b_n) - f_{n,n-1}(u_n(a'_n)) = f_{n,n-1}(b_n) - u_{n-1}(f'_{n,n-1}(a'_n)) = f_{n,n-1}(b_n) - u_{n-1}(a'_{n-1}) = f_{n,n-1}(b_n) - f_{n,n-1}(b_n) + a_{n-1} = a_{n-1}$. ∎

Korollar 10.5.4 Sei $0 \to G' \xrightarrow{u} G \xrightarrow{v} G'' \to 0$ eine exakte Sequenz von abelschen Gruppen und sei $(G_n)_{n\in\mathbb{N}}$ eine absteigende Familie von Untergruppen die eine Topologie über G definieren.

Seien $G'_n = G_n \cap G'$ und $G''_n = v(G_n)$. Diese Untergruppen von G' bzw. G'' definieren eine Topologie über G' bzw. G'' und es gibt eine exakte Sequenz

$$0 \to \widehat{G'} \xrightarrow{\widehat{u}} \widehat{G} \xrightarrow{\widehat{v}} \widehat{G''} \to 0.$$

Beweis. Wir haben eine exakte Sequenz $0 \to G'/(G' \cap G_n) = G'G_n/G_n \to G/G_n \to G''/v(G_n) \to 0$. Außerdem ist das System $(G''/G''_n)_{n\in\mathbb{N}}$ surjektiv. Die Aussage folge aus der Proposition. ∎

Korollar 10.5.5 Sei G eine abelsche Gruppe mit Untergruppen $(G_n)_{n\in\mathbb{N}}$, die ein Topologie definieren. Dann gilt $\widehat{G}/\widehat{G_n} \simeq G/G_n$.

Beweis. Sei $\pi : G \to G/G_n$ die kanonische Projektion. Die Topologie in G/G'' ist gegeben durch die Familie $(\pi(G_k))_{k\in\mathbb{N}}$. Aber für $k \geq n$ gilt $\pi(G_k) = 0$. Sei (x_m) eine Cauchyfolge für $l, m \gg 0$ gilt $x_l - x_m \in \pi(G_n) = 0$ also ist (x_m) stationär. Sei $x = x_m$ für $m \gg 0$. Dann sind die Folgen (x_m) und (x) (die konstante Folge) äquivalent. Es folgt $\widehat{G/G_n} \simeq G/G_n$.

Die Aussage folgt jetzt aus dem obigen Korollar mit $G' = G_n$ und $G'' = G/G_n$. ∎

Korollar 10.5.6 Es gilt $\widehat{\widehat{G}} \simeq \widehat{G}$: die Vervollständigung ist vollständig.

Beweis. Es gilt $\widehat{\widehat{G}} \simeq \varprojlim(\widehat{G}/\widehat{G_n}) \simeq \varprojlim(G/G_n) \simeq \widehat{G}$ ∎

Definition 10.5.7 Eine abelsche topologische Gruppe G heißt **vollständig** falls $\varphi : G \to \widehat{G}$ ein Isomorphismus ist.

Bemerkung 10.5.8 1. Die Vervollständigung ist vollständig.

2. Eine vollständige Gruppe ist Hausdorff.

Beispiel 10.5.9 1. Die p-adische Zahlen $\mathbb{Z}_p$ sind die Vervollständigung von $\mathbb{Z}$ mit der Topologie $(p^n\mathbb{Z})_{n\in\mathbb{N}}$.

2. Die formale Reihen $\mathsf{k}[[X]]$ sind die Vervollständigung von $\mathsf{k}[X]$ mit der Topologie $(\mathfrak{m}^n)_{n\in\mathbb{N}}$, wobei $\mathfrak{m} = (X)$.

10.6 Beispiele $\mathbb{Z}_p$ und $\mathsf{k}[[X]]$

Proposition 10.6.1 Seien $(p^n\mathbb{Z})$ bzw. (X^n) eine Basis der Umgebungen von 0 in $\mathbb{Z}$ bzw. $\mathsf{k}[X]$.

1. Die topologische Gruppen $\mathbb{Z}$ und $\mathsf{k}[X]$ $\mathbb{Z}$ sind Hausdorff. Insbesondere gilt $\mathbb{Z} \subset \mathbb{Z}_p$ und $\mathsf{k}[X] \subset \mathsf{k}[[X]]$.

2. Ein Element x in $\mathbb{Z}_p$ bzw. in $\mathsf{k}[[X]]$ ist genau dann invertierbar, wenn x nicht durch p bzw. X teilbar ist.

3. Ein Element in $\mathbb{Z}_p$ bzw. $\mathsf{k}[[X]]$ ist der Form up^n bzw. uX^n, wobei $u \in \mathbb{Z}_p^\times$ bzw. $u \in \mathsf{k}[[X]]^\times$.

4. Die Ringe $\mathbb{Z}_p$ und $\mathsf{k}[[X]]$ sind lokale Integritätsringe.

Beweis. 1. Sei $x \in \mathrm{Ker}(\mathbb{Z} \to \widehat{Z})$ bzw. $x \in \mathrm{Ker}(\mathbb{Z} \to \widehat{\mathsf{k}[X]})$. Dann ist x durch p^n bzw. x^n für alle n teilbar. Es folgt $x = 0$.

2. Sei (x_n) invertierbar und sei $(y_n) = (x_n)^{-1}$. Dann gilt $(x_n y_n) = (1)$ und also $x_1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Falls $p = (p)$ ein Teiler von (x_n) ist, gilt $p|x_n$ für alle n also $x_1 = 0$. Ein Widerspruch.

Andersrum, falls p kein Teiler von (x_n) ist, gibt es ein n so, dass p kein Teiler von x_n in $\mathbb{Z}/p^n\mathbb{Z}$ ist. Es folgt, dass p kein Teiler von x_n ist für alle n (weil $x_n \equiv x_m \pmod{p^n}$ für $n \leq m$ und $x_n \equiv x_m \pmod{p^m}$ für $n \geq m$). Daraus folgt, dass x_m in $\mathbb{Z}/p^m\mathbb{Z}$ invertierbar ist für alle m. Sei $z_n = x_n^{-1}$ in $\mathbb{Z}/p^n\mathbb{Z}$. Es gilt $(x_n)(z_n) = (x_n z_n) = (1) = 1$.

Analog folgt die Aussage für $\mathsf{k}[[X]]$.

3. Sei $x \in \mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})$. Dann ist x der Form $x = (x_n)_{n\in\mathbb{N}}$ mit $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ so, dass $f_{n,m}(x_n) = x_m$ für $f_{n,m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. Sei $k = \min\{n \mid x_n \neq 0\}$. Dann gilt $x_{k-1} = 0 \in \mathbb{Z}/p^{k-1}\mathbb{Z}$. Sei $f_{n,m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ dann teilt p^{k-1} das Element $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ für alle $n \geq k$ also gibt es ein $y_n \in \mathbb{Z}/p^n\mathbb{Z}$ mit $x_n = p^{k-1}y_n$ und $p \nmid y_n$ für alle $n \geq k$. Insbesondere ist y_n invertierbar in $\mathbb{Z}/p^n\mathbb{Z}$ für alle $n \geq k$. Seien

$$y_n = \begin{cases} 1 & \text{für } n < k \\ y_n & \text{für } n \geq k. \end{cases} \quad \text{und } z_n = \begin{cases} 1 & \text{für } n < k \\ y_n^{-1} & \text{für } n \geq k. \end{cases}$$

Es gilt $(y_n)(z_n) = (y_n z_n) = (1)$ also ist (y_n) invertierbar. Es gilt auch $(x_n) = (p)^{k-1}(y_n)$.

Analog folgt die Aussage für $\mathsf{k}[[X]]$.

4. Sei $\mathfrak{m}$ das von p erzeugte Ideal in $\mathbb{Z}_p$. Ein Element $x \in \mathbb{Z}_p$ ist genau dann invertierbar, wenn $x \notin \mathfrak{m}$ ist. Es folgt, dass $\mathbb{Z}_p$ lokal mit maximalem ideal $\mathfrak{m}$ ist.

Seien $x, y \in \mathbb{Z}_p$ mit $xy = 0$. Es gibt $u \in \mathbb{Z}_p^\times$ und $n \in \mathbb{N}$ mit $y = up^n$. Es folgt $uxp^n = 0$ und also $xp^n = 0$. Es genügt also die Implikation $px = 0 \Rightarrow x = 0$ zu zeigen. Sei

$x = (x_n)$, es gilt $px_n = 0$ für alle n. Es folgt $x_n \equiv p^{n-1} \pmod{p^n}$ für alle n. Es gilt aber $x_{n-1} \equiv x_n \pmod{p^{n-1}}$ für alle n. Es folgt $x_{n-1} = 0$ für alle n und $x = 0$.

Analog folgt die Aussage für $\mathsf{k}[[X]]$. ■

Beispiel 10.6.2 In $\mathbb{Z}_2$ gilt $1 + 2 + \cdots + 2^n + \cdots = -1$.

In $\mathbb{Z}_p$ gilt $1 + p + \cdots + p^n + \cdots = \frac{1}{1-p}$.

In $\mathsf{k}[[X]]$ gilt $1 + X + \cdots + X^n + \cdots = \frac{1}{1-X}$.

Definition 10.6.3 Der Quotientkörper von $\mathbb{Z}_p$ ist $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$. Der Quotientkörper von $\mathsf{k}[[X]]$ ist $\mathsf{k}((X)) = \mathrm{Frac}(\mathsf{k}[[X]])$.

Wir schreiben Elemente aus $\mathbb{Z}_p$ in der folgenden Form

$$(x_n) = \sum_{n=0}^{\infty} a_n p^n$$

wobei $x_n = \sum_{k=0}^{n-1} a_k p^k$.

Proposition 10.6.4 Es gilt

$$\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right] \text{ und } \mathsf{k}((X)) = \mathsf{k}[[X]][X^{-1}].$$

Für jedes Element x in $\mathbb{Q}_p$ bzw. $\mathsf{k}((X))$ gibt es also ein n so, dass

$$x = \sum_{k=-n}^{\infty} a_k p^k \text{ bzw. } x = \sum_{k=-n}^{\infty} a_k X^k,$$

wobei $a_k \in \mathbb{Z}/p^n\mathbb{Z}$ bzw. $a_k \in \mathsf{k}$.

Beweis. Da $\mathbb{Z}_p$ lokal mit maximalem Ideal $\mathfrak{m} = (p)$ ist, gilt $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$. Ein Element $x \in \mathbb{Q}_p$ ist also der Form $x = y/p^n$ mit $y \in \mathbb{Z}_p$. Wir schreiben $y = \sum_{k=0}^{\infty} a_k p^k$. Es folgt $x = \sum_{k=-n}^{\infty} a_{k+n} p^k$.

Analog folgt die Aussage für $\mathsf{k}[[X]]$. ■

10.7 Weitere Eigenschaften

10.7.1 Noethersche Ringe

Definition 10.7.1 Sei M ein A-Modul und $\mathfrak{a} \subset A$ ein Ideal. Dann definiert $(\mathfrak{a}^n M)_{n\in\mathbb{N}}$ eine Topologie und $\widehat{M}$ eine Vervollständigung.

Lemma 10.7.2 Sei M ein A-Modul.

1. Dann ist $\widehat{M}$ ein $\widehat{A}$-Modul.

2. Falls $f : M \to N$ ein Modulhomomorphismus ist, ist f stetig ($\mathfrak{a}^n M \subset f^{-1}(\mathfrak{a}^n N)$ ist eine Umbegung von 0) und $\widehat{f} : \widehat{M} \to \widehat{N}$ ist auch stetig. □

Satz 10.7.3 Sei A ein noetherscher Ring, sei $\mathfrak{a} \subset A$ ein Ideal und $\widehat{A}$ die $\mathfrak{a}$-adische Vervollständigung. Dann ist der A-Modul $\widehat{A}$ flach. □

Proposition 10.7.4 Sei A ein noetherscher Ring, sei M ein endlich erzeugter A-Modul, $\mathfrak{a} \subset A$ ein Ideal und $\widehat{A}, \widehat{M}$ die $\mathfrak{a}$-adischen Vervollständigungen. Es gilt $\widehat{M} \simeq M \otimes_A \widehat{A}$.

Korollar 10.7.5 Sei A ein noetherscher Ring und $0 \to M' \to M \to M'' \to 0$ eine exakte Sequenz von endlich erzeugten A-Moduln. Dann gibt es eine exakte Sequenz $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$.

Satz 10.7.6 Sei A ein noetherscher Ring und $\mathfrak{a} \subset A$ ein Ideal. Sei $\widehat{A}$ die $\mathfrak{a}$-adische Vervollständigung. Dann ist $\widehat{A}$ noethersch. □

Korollar 10.7.7 Die Ringe $\mathbb{Z}_p$ und $\mathsf{k}[[X_1, \cdots, X_n]]$ sind noethersch.

10.7.2 Lokale noethersche Ringe, Dimension II

Proposition 10.7.8 Sei A ein noetherscher lokal Ring und $\mathfrak{m}$ sein maximales Ideal. Sei $\widehat{A}$ die $\mathfrak{m}$-adische Vervollständigung von A. Dann ist $\widehat{A}$ lokal mit maximalem Ideal $\widehat{\mathfrak{m}}$.

Außerdem ist $\widehat{A}$ Hausdorff und für M ein endlich erzeugter A-Modul ist $\widehat{M}$ auch Hausdorff.

Definition 10.7.9 Sei A ein noetherscher lokaler Ring und sei $\mathfrak{m}$ das maximale Ideal. Wir schreiben $d(A)$ für die minimale Anzahl von Erzeugern in $\mathfrak{m}$.

Satz 10.7.10 Es gilt $d(A) = \mathrm{Kdim}(A)$. □

Dank Nakayama haben wir:

Korollar 10.7.11 Sei A ein noetherscher lokaler Ring und sei $\mathfrak{m}$ das maximale Ideal und $\mathsf{k} = A/\mathfrak{m}$ der Restklassenkörper. Es gilt $\mathrm{Kdim}(A) \leq \dim_{\mathsf{k}} \mathfrak{m}/\mathfrak{m}^2$.

Satz 10.7.12 Es gilt $\mathrm{Kdim}(A) = \mathrm{Kdim}(\widehat{A})$. $\square$

Definition 10.7.13 Sei A ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{m}$ und $\mathsf{k} = A/\mathfrak{m}$ der Restklassenkörper. Der Ring A heißt **regulär** falls gilt $\mathrm{Kdim}(A) = \dim_{\mathsf{k}} \mathfrak{m}/\mathfrak{m}^2$.

Proposition 10.7.14 Sei A ein noetherscher Ring A mit $\mathrm{Kdim}(A) = 1$. Dann gilt

$$A \text{ regulär} \Leftrightarrow A \text{ Dedekin.}$$

Satz 10.7.15 Sei A ein lokaler noetherscher regulärer Ring. Dann ist A faktoriell. Insbesonder ist A ein Integritätsring und ist ganz abgeschlossen. $\square$

Satz 10.7.16 Sei A ein lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{m}$. Sei $\widehat{A}$ die $\mathfrak{m}$-adische Vervollständigung von A. Dann gilt

$$A \text{ regulär} \Leftrightarrow \widehat{A} \text{ regulär.}$$

Satz 10.7.17 (Cohen Struktursatz) Sei A ein lokaler vollständiger regulärer Ring mit $\mathrm{Kdim}(A) = n$ so, dass A einen Ring enthält. Dann gilt

$$A \simeq \mathsf{k}[[X_1, \cdots, X_n]],$$

wobei k der Restklassenkörper ist. $\square$

Index

A-bilinear, 28
n-linear, 30
Äquivalenz von Cauchyfolgen, 100

additive Funktion, 25
Algebra, 36
    endlich, 37
    endlicher Typ, 37
    Morphismus, 36

Bewertung
    p-adische, 86
    diskrete Bewertung, 86

Cauchyfolge, 100

Dimension
    krullsche Dimension, 61
    lokale Dimension, 61

exakte Sequenz von projektiven Systemen, 104

Funktor
    $- \otimes_A N$, 32
    $\mathrm{Hom}(-, N)$, 32
    $\mathrm{Hom}(N, -)$, 32
    ajungiertes Paar, 33
    exakt, 35
    kontravariant, 32
    kovariant, 32
    linksadjungiert, 33
    rechtsadjungiert, 33

ganz
    ganz über ein Ideal, 54
    ganz über einem Ring, 50
    ganz abgeschlossen, 54
    ganz abgschlossen in einem Ring, 51
    ganzer Abschluss, 51
    ganzer Abschluss eines Ideals, 54
    ganzer Ring über einen Ring, 51
    ganzer Ringhomomorphismus, 51

Hauptidealgruppe, 92

Ideal, 6
    $\mathfrak{p}$-primär, 76
    Annihilator, 15
    assoziiertes Primideal, 79
    eingebettetes assoziiertes Primideal, 79
    gebrochenes Hauptideal, 90
    gebrochenes Ideal, 89
    Hauptideal, 9
    irreduzibel, 83
    isoliert, 81
    Jacobson Radikal, 13
    Konduktor, 15
    maximal, 9
    minimales assoziiertes Primideal, 79
    Nilradikal, 12
    primär, 76
    Primideal, 9
    Produktideal, 8
    Radikal, 12
    Radikalideal, 12
    Summe, 7
    teilerfremd, 13
    zerlegbar, 78
Idealfaktorgruppe, 92
Idealgruppe, 92
inverser Limes, 102
inverses System, 102

Körper, 9
 Diskriminante, 96
 Norm von einem Element, 93
 Restklassenkörper, 11
 Spur von einem Element, 93
 Zahlkörper, 98

lokale Eingenschaft, 43
Lokalisierung, 41
Lokalisierungsfunktor, 41

Modul, 16
 absteigende Kettenbedingung, 64
 acc, 64
 Annihilator, 20
 artinsch, 64
 assoziiertes Primideal, 79
 aufsteigende Kettenbedingung, 64
 Coker, 18
 dcc, 64
 direkte Summe, 20, 21
 einfach, 67
 eingebettetes assoziiertes Primideal, 79
 Einschränkung der Skalare, 35
 endlich erzeugt, 21
 endlicher Länge, 68
 Erweiterung der Skalare, 36
 erzeugtes Untermodul, 19
 exakte Sequenz, 18
 flach, 35
 frei, 21
 invertierbar, 90
 Kette, 67
 Konduktor, 20
 Länge, 68
 minimales assoziiertes Primideal, 79
 Modulhomomorphismus, 16
 noethersch, 64
 Nullmodul, 16
 Produkt, 20, 21
 Summe, 19
 treu, 20
 Untermodul, 17
 vollständige Kette, 67
Morphismus von projrktiven Systemen, 104

primäre Zerlegung, 78
projektiver Limes, 102
projektives System, 102
 surjektiv, 104

rein transzendent, 59
Ring, 5
 artinsch, 66
 Dedekinsring, 89
 endlich erzeugt, 37
 ganze Zahlen eines Zahlkörpers, 98
 Hauptidealring, 9
 Integritätsring, 8
 Inverse, 8
 invertierbar, 8
 japanischer Ring, 98
 kommutativ, 5
 lokal, 11
 nilpotent, 8
 noethersch, 66
 Nullring, 5
 Nullteiler, 8
 nullteilerfrei, 8
 Produktring, 6
 reduziert, 8
 regulär, 109
 Ringhomomorphismus, 5
 Unterring, 6

Tensorprodukt, 28, 30
transczendent, 57
transzendent
 Transzendenzbasis, 58
transzendenz
 Transzendenzgrad, 59

Vervollständigung, 100
vollständig, 105