Algebra II
Sommersemester 2007

Prof. Dr. Annette Huber-Klawitter

Fassung vom 13. Juli 2007

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Johannisgasse 26
04109 Leipzig

0341-97 32 185
huber@mathematik.uni-leipzig.de

Kapitel 0

Einleitung

Hauptthema dieser Vorlesung ist die sogenannte *kommutative Algebra*, d.h. die Theorie der kommutativen Ringe. Zunächst sollen zwei wichtige Gebiete vorgestellt werden, die sich auf kommutative Algebra stützen.

Algebraische Varietäten

In diesem Abschnitt ist k stets ein algebraisch abgeschlossener Körper, also zB. $\mathbb{C}$.

Definition 0.1. *Sei $S \subset k[X_1, \ldots, X_n]$ eine Teilmenge. Dann heißt die Nullstellenmenge von S*

$$V(S) = \{(x_1, \ldots, x_n) \in k^n \mid f(x_1, \ldots, x_n) = 0 \text{ für alle } f \in S\}$$

(affine) algebraische Varietät *(definiert durch S) (alternativ:* algebraische Menge*).*

Im Falle $S = \{f\}$ schreiben wir $V(f)$ statt $V(\{f\})$. Die Menge $V(\emptyset) = k^n$ schreiben wir auch $\mathbb{A}^n_k = \mathbb{A}^n$.

Beispiel. (i) $f = X^2 + Y^2 - 1$ hat als Nullstellenmenge

$$V(S) = \{(x, y) \in k^2 \mid x^2 + y^2 = 1\}$$

also die Kreislinie.

(ii) $Y^2 = X(X-1)(X+1)$, $Y^2 = X^2(X+1)$ und $Y^2 = X^3$ sind jeweils symmetrisch zur x-Achse. Für jeden Wert von X gibt es zwei Werte für Y.

(iii) Die algebraischen Teilmengen von $\mathbb{A}^1 = k$ sind $V(\emptyset) = \mathbb{A}^1$, $V(1) =$, sowie jede endliche Teilmenge von k.

Beweis: Sei $S \subset k[X_1, \ldots, X_n]$. Sei $f \in S$ ein nicht-konstantes Polynom. Dann gilt $V(f)$ endlich, genauer hat $V(f)$ genau $\deg f$ Elemente. Durch Hinzufügen weiterer Gleichungen wird diese Menge verkleinert, ist also stets endlich. Andererseits hat für $M = \{a_1, \ldots, a_n\} \subset k$ das Polynom $f = (X - a_1) \ldots (X - a_n)$ die Nullstellenmenge M. □

Wir zeichnen meist *reelle* Bilder der Punktmengen.
Verschiedene Teilmengen von S können dieselbe algebraische Varietät definieren, zB. $V(f) = V(af)$ für $a \in k^*$.

Definition 0.2. *(i) Sei $M \subset \mathbb{A}^n$ eine Teilmenge Dann heißt*

$$I(M) = \{f \in k[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0 \text{ für alle } x = (x_1, \ldots, x_n) \in M\}$$

Verschwindungsideal von M.

(ii) Sei $V \subset \mathbb{A}^n$ eine algebraische Varietät. Eine Funktion $f : V \to k$ heißt regulär*, falls es $P \in k[X_1, \ldots, X_n]$ gibt mit*

$$f(x) = P(x) \text{ für alle } x \in V$$

Der Ring der regulären Funktionen wird mit $k[V]$ bezeichnet.

Offensichtlich ist $k[V]$ wirklich ein Ring, sogar eine k-Algebra.

Lemma 0.3. *$I(M)$ ist ein Ideal. Sei $M = V(S)$ eine algebraische Varietät. Dann gilt*

$$k[V] \cong k[X_1, \ldots, X_n]/I(V)$$

Weiter ist

$$I(S) \subset I(M)$$

wobei $I(S)$ das von S erzeugte Ideal in $k[X_1, \ldots, X_n]$ ist.

Beweis: Man kann die Idealeigenschaft einfach nachrechnen. Besseres Argument: Nach Definition ist $k[X_1, \ldots, X_n] \to k[V]$, die ein Polynom als Abbildung auf V auffasst, eine surjektive Abbildung. Der Kern ist genau $I(V)$, also ein Ideal. Nach dem Homomorphiesatz für Ringe gilt

$$k[X_1, \ldots, X_n]/I(V) \cong k[V] \ .$$

Sei nun $M = V(S)$. Nach Definition gilt $f(x) = 0$ für $f \in S$ und $x \in V(S)$. Daher ist S in $I(M)$ enthalten. Da $I(M)$ ein Ideal ist, ist dann auch $I(S) \subset I(M)$. □

Gilt Gleichheit? Nein! Für $\{0\} = M = V(X^2) \subset \mathbb{A}^1$ liegt $f = X$ im Verschwindungsideal, aber $X \notin (X^2)$. Das ist aber das einzige verbleibende Problem.

Theorem 0.4 (Hilberts Nullstellensatz). *Sei $V(S) \subset \mathbb{A}^n$ eine algebraische Varität definiert durch S. Dann gilt*

$$I(V(S)) = \sqrt{I(S)}$$

Hierbei bezeichnet

$$\sqrt{I} = \{f \in k[X_1, \ldots, X_n] \mid \text{ es gibt } n \in \mathbb{N} \text{ mit } f^n \in I\}$$

das Radikal *von* I.

Die Relation $\sqrt{I(S)} \subset I(V)$ ist offensichtlich, die Umkehrung überhaupt nicht! Dies ist einer der Sätze, die wir im Laufe des Semesters zeigen wollen. Einige einfachere Dinge können wir jedoch direkt beweisen.

Satz 0.5. *Seien J eine Indexmenge, $V_j \subset \mathbb{A}^n$ für $j \in J$ jeweils eine Varietät. Dann ist auch $V = \bigcap_{j \in V} V_j$ eine algebraische Varietät. Mit $V_1, V_2 \subset \mathbb{A}^n$ ist auch $V_1 \cup V_2$ eine Varität.*

Beweis: Sei S_j eine Menge von Gleichungen für V_j.

Behauptung. *$S = \bigcup_j S_j$ hat die Nullstellenmenge V.*

Sei $x \in V_j$ für alle j. Dann erfüllt x für alle j alle Gleichungen in S_j, also alle Gleichungen in S. Sei umgekehrt x ein Nullstelle aller $f \in S$. Dann erfüllt x (für jedes j) alle Gleichungen in S_j, liegt also in jedem V_j.
Seien $V_1 = V(I_1)$, $V_2 = V(I_2)$ für Ideale $I_1, I_2 \subset k[X_1, \ldots, X_n]$.

Behauptung. *$V_1 \cup V_2 = V(I_1 I_2)$ wobei $I_1 I_2$ das Ideal ist, dass von allen $f_1 f_2$ mit $f_1 \in I_1$, $f_2 \in I_2$ erzeugt wird.*

Sei $x \in V_1 \cup V_2$, ohne Einschränkung $x \in V_1$. Dann gilt

$$f_1 f_2(x) = f_1(x) f_2(x) = 0 f_2(x) = 0$$

damit erfüllt x alle Erzeuger von $I_1 I_2$, liegt also in $V(I_1 I_2)$. Sei umgekehrt $x \notin V_1 \cup V_2$, also $x \notin V_1, V_2$. Dann gibt es $f_1 \in I_1$ mit $f_1(x) \neq 0$ und $f_2 \in I_2$ mit $f_2(x) \neq 0$. Dann ist auch $f_1 f_2(x) \neq 0$ da k ein Körper ist. Dies bedeutet $x \notin V(I_1 I_2)$. □

Mit anderen Worten:

Definition 0.6. *Sei V eine algebraische Varietät. Eine Teilmenge $A \subset B$ heißt* abgeschlossen*, falls $A \subset V$ eine algebraische Untervarietät ist. Das Komplement $V \setminus A$ heißt* offen*. Nach dem vorherigen Satz definieren diese offenen Teilmengen eine Topologie auf V, die* Zariski-Toplogie*.*

Zur Erinnerung:
Sei V eine Menge. Ein System $\mathcal{T}$ von Teilmengen von V heißt Topologie, falls $\emptyset, V \in \mathcal{T}$ und $\mathcal{T}$ abgeschlossen ist unter beliebigen Vereinigungen und endlichen Durchschnitten.
Die Zariski-Topologie unterscheidet sich grundlegend von gewöhnlichen Topologie auf $\mathbb{R}^n$ oder $\mathbb{C}^n$. Z.B. sind alle offenen Teilmengen $U \subset \mathbb{A}^n$ dicht, d.h. die kleinste abgeschlossene Teilmenge, die U enthält, ist $\mathbb{A}^n$. Um solche Dinge zeigen zu können, benötigen wir mehr Wissen über die Koordinatenringe $k[V]$, also kommutative Algebra.

Algebraische Zahlentheorie

Definition 0.7. *Sei K ein* Zahlkörper*, d.h. eine endliche Körpererweiterung von $\mathbb{Q}$. Dann heißt*

$$\mathcal{O}_K = \{x \in K \mid \textit{es gibt ein normiertes Polynom } P \in \mathbb{Z}[X] \textit{ mit Nullstelle } x\}$$

Ganzheitsring von K.

Beispiel. Der Ganzheitsring von $\mathbb{Q}$ ist $\mathbb{Z}$ (Gauß-Lemma). Der Ganzheitsring von $\mathbb{Q}(\sqrt{2})$ ist $\mathbb{Z}[\sqrt{2}]$ (Übungsaufgabe).

Lemma 0.8. *Sei $d \in \mathbb{Z}$ quadratfrei, d.z. d wird von keiner Quadratzahl geteilt. Sei $K = \mathbb{Q}(\sqrt{d})$. Dann gilt*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d = 2, 3 \mod 4 \\ \{x + y\sqrt{d} \mid 2x, 2y \in \mathbb{Z}, 2x = 2y \mod 2\} & d = 1 \mod 4 \end{cases}$$

Beweis: Sei $a = x + y\sqrt{d} \in \mathcal{O}_K$ Nullstelle des normierten Polynoms $P \in \mathbb{Z}[X]$. Das Minimalpolynom von a ist ein Teiler von P in $\mathbb{Q}[X]$, nach dem Gauß-Lemma liegt dann das Minimalpolynom in $\mathbb{Z}[X]$. Ohne Einschränkung ist dann P gleich dem Minimalpolynom. Ist P linear, so liegt offensichtlich $a \in \mathbb{Z}$. Dieses Element liegt auch auf der rechten Seite. Ist P quadratisch, so gilt

$$P(X) = (X - x - y\sqrt{d})(X - x + y\sqrt{d}) = X^2 - 2xX + x^2 - y^2 d$$

Damit ist a über $\mathbb{Z}$ genau dann, wenn $2x \in \mathbb{Z}$ und $x^2 - y^2 d \in \mathbb{Z}$. Es folgt $4y^2 d \in \mathbb{Z}$. Wir schreiben $y = r/s$ als gekürzten Bruch. Dann gilt

$$s^2 \mid 4r^2 d \Rightarrow s^2 \mid 4d$$

Da d quadratfrei ist, ist nur $s = \pm 1, s = \pm 2$ möglich, d.h. auch $2y$ ist ganz. Wir schreiben $x = x'/2, y = y'/2$ mit $x', y' \in \mathbb{Z}$. Die Bedingung wird nun zu

$$(x'^2 - y'^2 d)/4 \in \mathbb{Z} \Leftrightarrow x'^2 - y'^2 d = 0 \mod 4 \Leftrightarrow x'^2 = y'^2 d \mod 4$$

Ist x' gerade, so gilt $x'^2 = 0 \mod 4$. Ist x' ungerade, so gilt

$$x'^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 1 \mod 4$$

Ebenso kann auch y'^2 nur die Werte $0, 1 \mod 4$ annehmen. Nun gehen wir die Fälle $d \mod 4$ durch.
Für $d = 1 \mod 4$ folgt $x'^2 = y'^2$, also entweder beide gerade oder beide ungerade. Dies ist die Behauptung.
Für $d = 2, 3 \mod 4$ bleibt nur der Fall x', y' gerade, also $x, y \in \mathbb{Z}$. Auch dies ist die Behauptung. □

Warum handelt es sich bei $\mathcal{O}_K$ um einen Ring? Allgemeiner:

Definition 0.9. *Sei $A \to B$ eine Inklusion von Ringen ohne Nullteiler (d.h. $aa' = 0 \Rightarrow a = 0$ oder $a' = 0$). Ein Element $b \in B$ heißt* ganz über A, *falls b Nullstelle eine normierten Polynoms in $A[X]$ ist.*

$$\tilde{A} = \{b \in B \mid \ b \text{ ganz über } A\}$$

heißt ganzer Abschluss von A in B.

Beispiel. (i) Für $Z \subset K$ Zahlkörper ist der ganze Abschluss der Ganzheitsring von K.

(ii) $K \subset L$ eine Körpererweiterung. Dann ist $b \in K$ ganz über K genau dann, wenn es algebraisch ist. Der ganze Abschluss ist dann also der algebraische Abschluss.

Der Beweis, dass der ganze Abschluss ein Ring ist, verallgemeinert also den Satz, dass der algebraische Abschluss ein Körper ist. Wesentliches Hilfsmittel dabei war die Theorie der Vektorräume. Diese müssen wir zunächst auf Ringe verallgemeinern. Man spricht dann von *Moduln*.

Literatur

- S. Lang: Algebra
- Bourbaki: commutative Algebra
- Atiyah, MacDonald: commutative Algebra
- Eisenbud: Commutative Algebra with a view to algebraic geometry
- Samuel: Theory of numbers

Allgemein Bücher über Algebra II (je nach Schwerpunkt) oder zur kommutativen Algebra.

Kapitel 1

Ringe und Moduln

Alle Ringe sind kommutativ mit Eins (insbesondere $1 \neq 0$).

Grundbegriffe

Beispiel. $\mathbb{Z}$, $\mathbb{Z}[i]$ (die ganzen Gaußschen Zahlen), $A[X_1, \ldots, X_n]$ (Polynomringe), $\mathbb{Q}$, $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, (p, b) = 1\}$, $A[[X]]$ (Potenzreihenringe),...

Definition 1.1. *Sei A ein Ring.*

(i) $A^* = \{a \in A \mid$ *es gibt* $b \in A$ *mit* $ab = 1\}$ *heißt* Einheitengruppe.

(ii) $a \in A \setminus \{0\}$ *heißt* Nullteiler*, wenn es ein* $b \in A \setminus \{0\}$ *gibt mit* $ab = 0$.

(iii) Ein Ring ohne Nullteiler heißt Integritätsbereich.

Beispiel. $\mathbb{Z}^* = \{\pm 1\}$, $k[X]^* = k^*$. Der Ring $k[X]/X^2$ hat den Nullteiler X, denn $X \cdot X = 0$. Der Ring A^2 (komponentenweise Multiplikation) hat den Nullteiler $(1, 0)$ wegen $(1, 0)(0, 1) = (0, 0)$.

Definition 1.2. *Sei A ein Ring. Ein A-Modul M ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Skalarmultiplikation*

$$A \times M \to M$$

so dass für alle $a, b \in A$, $x, y \in M$ gilt:

(i) $a(x + y) = ax + ay$,

(ii) $(a + b)x = ax + bx$,

(iii) $a(bx) = (ab)x$,

(iv) $1x = x$.

Beispiel. $A = k$ ein Körper. Dann ist ein A-Modul das Gleiche wie ein k-Vektorraum.

Lemma 1.3. *Ein $\mathbb{Z}$-Modul ist das Gleiche wie eine abelsche Gruppe.*

Beweis: Sei M ein $\mathbb{Z}$-Modul, dann ist nach Definition M eine abelsche Gruppe. Interessant ist also die Gegenrichtung. Sei M eine abelsche Gruppe, $x \in M$, $n \in \mathbb{N}$. Wir definieren $nx = x+(n-1)x$. Für negative n setzen wir $nx = -(-n)x$. Die Modulaxiome gelten alle. Man beweist alles mit Induktion, z.B.

$$n(x+y) = (x+y) + (n-1)(x+y) = x + y + (n-1)x + (n-1)y = nx + ny \ .$$

□

Bemerkung. Man sieht an der Beispielrechung, dass die Kommutativität von M wirklich benötigt wird.

Lemma 1.4. *Sei k ein Körper. Ein $k[X]$-Modul M ist das Gleiche wie ein k-Vektorraum M zusammen mit einem Endomorphismus von M.*

Beweis: Gegeben seien M und $\theta : M \to M$. Wir definieren das Skalarprodukt

$$k[X] \times M \to M \ ; (\sum a_i X^i, v) \mapsto \sum a_i \theta^i(v) \ .$$

Wir zeigen die Assoziativität:

$$(\sum a_i X^i) \left((\sum b_j X^j) v \right) = \sum a_i \theta^i \left(\sum b_j \theta^j(v) \right) = \sum a_i b_j \theta^i(\theta^j(v)) = \sum a_i b_j \theta^{i+j}(v) = (\sum a_i b_j X^{i+j}) v \ .$$

Die anderen Eigenschaften sind noch leichter.
Umgekehrt sei V ein $k[X]$-Modul. Wegen $k \subset k[X]$ ist es dann ein k-Vektorraum. Wir setzen $\theta(v) = Xv$. □

Definition 1.5. *(i) $N \subset M$ heißt* Untermodul*, wenn N abelsche Untergruppe von M ist und abgeschlossen unter Multiplikation mit A.*

(ii) $f : N \to M$ heißt Modulhomomorphismus*, wenn f ein Gruppenhomomorphismus ist und $f(am) = af(m)$. Die Menge der Modulhomomorphismen wird durch* $\mathrm{Hom}_A(M, N)$ *bezeichnet.*

Beispiel. A ist auch ein A-Modul. Die Untermoduln von A sind genau die Ideale. Ist $A \to B$ ein Ringhomomorphismus, so ist B ein A-Modul.

Lemma 1.6. *(i) Kern und Bild eine Modulhomomorphismus sind Untermoduln.*

(ii) Ist $N \subset M$ ein Untermodul, so ist M/N ein Modul mit der induzierten Skalarmultiplikation. Ist speziell $M = A$ der Ring, so ist A/N ein Ring falls $N \neq A$.

(iii) $\mathrm{Hom}_A(M,N)$ *ist ein A-Modul mit* $(f+g)(x) = f(x)+g(x)$ *und* $(af)(x) = a(f(x))$ *für alle* $a \in A$, $x \in M$.

Beweis: Kern und Bild sind Untergruppen. Zu zeigen ist, dass sie von der Skalarmultiplikation respekiert werden. Sei $f : M \to N$ ein Modulhomomorphismus, $x \in \mathrm{Ker}\, f$, $a \in A$. Dann gilt

$$f(ax) = af(x) = a0 = 0 \ .$$

Sei $y = f(x)$ im Bild. Dann gilt

$$ay = af(x) = f(ax) \ .$$

Da M abelsch sit, ist N automatisch ein Normalteiler. Damit ist M/N als abelsche Gruppe definiert. Auch die Modulaxiome sind leicht zu überprüfen. Einzige Frage ist die Wohldefiniertheit der Skalarmultiplikation. Seien also $a \in A$, $x, y \in M$ in der selben Nebenklasse, d.h. $x - y \in N$. Dann gilt

$$a(x+N) = ax + N \ ; a(y+N) = ay + N \ .$$

Da N ein Untermodul ist, gilt $a(x-y) = ax - ay \in N$, also ist die Multiplikation wohldefiniert. Ist speziell $M = A$ der Ring, so ist N ein Ideal. Die Ringaxiome sind leicht zu überprüfen (oder vergleiche Algebra I).
Nun wird $\mathrm{Hom}_A(M,N)$ betrachtet. Die Modulaxiome sind leicht zu überprüfen. Sie gelten, da N ein A-Modul ist. Die eigentliche Frage ist Wohldefiniertheit, nämlich dass $f+g$ und af wieder in $\mathrm{Hom}_A(M,N)$ liegen.

$$(f+g)(ax+by) = f(ax+by)+g(ax+by) = af(x)+bf(y)+ag(x)+bg(y) = a(f+g)(x)+b(f+g)(y) \ .$$

□

Wir führen nun weitere Methoden ein, wie man aus gegebenen Moduln neue definiert.

Definition 1.7. *(i) Seien* N_1, N_2 *Untermoduln von* M. *Die* Summe *ist der Untermodul*

$$N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$$

von M.

(ii) Seien $I_1, I_2 \subset A$ *Ideale. Das* Produkt *ist das Ideal* $I_1 I_2$, *das von den Produkten* $a_1 a_2$ *mit* $a_i \in I_i$ *erzeugt wird.*

(iii) Seien M_i *für* $i \in I$ *A-Moduln. Das* direkte Produkt *ist der A-Modul*

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$$

mit der komponentenweisen Addition und Diagonalmultiplikation.

(iv) Seien M_i für $i \in I$ A-Moduln. Die direkte Summe *ist der A-Modul*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i, m_i = 0 \text{ für fast alle } i \in I\}$$

(v) Ein Modul M heißt frei*, wenn er isomorph zu einem Modul von der Form $\bigoplus_{i\in I} A$ ist. Die Mächtigkeit von I heißt dann* Rang *von M.*

Bemerkung. Seien A_i für $i \in I$ Ringe. Dann ist das direkte Produkt $\prod_{i\in I} A_i$ wieder ein Ring. Für die direkte Summe ist das falsch, falls $|I| = \infty$, denn $1 \notin \bigoplus A_i$.

Lemma 1.8. *Sei $A = k$ ein Körper. Dann sind alle A-Moduln frei. Der Rang, also die Dimension, ist wohldefiniert.*

Beweis: Dies ist der Basisexistenzsatz und die Wohldefiniertheit der Dimension aus der linearen Algebra. Für endlich erzeugte Vektorräume handelt es sich also um Regelstoff aus der linearen Algebra. Der allgemeine Fall folgt mit Hilfe des Zornschen Lemmas. □

Beispiel. Der $\mathbb{Z}$-Modul $\mathbb{Z}/n$ ist nicht frei, denn alle freien $\mathbb{Z}$-Moduln haben unendliche viele Elemente.

Satz 1.9. *Sei $M = A^n$ ein freier A-Modul. Dann ist der Rang wohldefiniert.*

Beweis: Sei $I \subset A$ ein maximales Ideal, d.h. $I \neq A$ und maximal mit dieser Eigenschaft. Solche Ideale existieren nach I Satz 3.13. Sei $N = IA^n$, d.h. der Untermodul, der von den ax mit $a \in I$, $x \in A^n$ erzeugt wird.

Behauptung. $N = I^n$ *(direktes Produkt von Moduln)*

Zunächst $N \supset I^n$. Sei $(x_1, \ldots, x_n) \in I^n$.

$$(x_1, \ldots, x_n) = (x_1, 0, \ldots, 0) + (0, x_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, x_n) = \\ x_1(1, 0, \ldots, 0) + \cdots + x_n(0, \ldots, 0, 1) \in N \ .$$

Für die zweite Inklusion sei $(a_1, \ldots, a_n) \in A^n$ und $x \in I$. Dann folgt $x(a_1, \ldots, a_n) = (xa_1, \ldots, xa_n) \in I^n$. Dann ist

$$M/N = A^n/I^n = (A/I)^n \ .$$

Die Zahl n ist die Dimension des $k = A/I$-Vektoraums M/N, also wohldefiniert. □

Satz 1.10 (Homomorphiesatz, Noethersche Isomorphiesätze). *Sei $f : M \to N$ ein A-Modulhomomorphismus. Dann ist die induzierte Abbildung*

$$\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$$

ein Isomorphismus von A-Moduln. Sind $N, N' \subset M$ Untermoduldn, so ist

$$(N + N')/N \cong N'/(N \cap N')$$

ein kanonischer Isomorphismus. Sind $N' \subset N \subset M$ Untermoduln, so ist

$$(M/N')/(N/N') \cong M/N$$

ein kanonischer Isomorphismus.

Beweis: I Satz 6.16, I Satz 6.17 und I Satz 6.18 liefern diese Ausagen für abelsche Gruppen. Die Verträglichkeit mit der A-Modulstruktur ist leicht zu überprüfen. □

Definition 1.11. *Eine Sequenz $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ von A-Moduln heißt* exakt*, wenn* $\operatorname{Ker} g = \operatorname{Im} f$*. Eine exakte Sequenz der Form*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

heißt kurze exakte Sequenz*.*

Beispiel. $0 \to M_1 \to M_2$ ist genau dann exakt, wenn die Abbildung injektiv ist.
$M_2 \to M_3 \to 0$ ist genau dann exakt, wenn die Abbildung surjektiv ist.

Satz 1.12 (Chinesischer Restsatz). *Seien $I_1, \ldots, I_n$ Ideale von A mit $I_i + I_j = A$ für alle $i \neq j$. Dann ist die Sequenz*

$$0 \to \bigcap_{i=1}^{n} I_i \to A \xrightarrow{\pi} \prod_{i=1}^{n} A/I_i \to 0$$

exakt.

Bemerkung. Für $A = \mathbb{Z}$ ist $I_i = (a_i)$, $I_i + I_j = A$ bedeutet, dass $(a_i, a_j) = 1$. Man erhält genau den chinesischen Restsatz aus Algebra I.

Beweis: Es gilt stets

$$\operatorname{Ker} \pi = \{a \in A \mid a \in I_i \text{ für alle } i\} = \bigcap_{i=1}^{n} I_i \ .$$

Die schwierige Aussage ist also die Surjektivität. Wir argumentieren mit Induktion nach n. Der Fall $n = 1$ ist trivial. Sei nun $n = 2$, $(\overline{a}, \overline{b}) \in A/I_1 \times A/I_2$. Wir wählen ein Urbild a von $\overline{a}$. Es gilt $\pi(a) - (\overline{a}, \overline{b}) = (0, a - \overline{b})$. Die Abbildung

$$I_1 \to A \to A/I_2$$

ist surjektiv, denn das Bild ist

$$I_1/I_1 \cap I_2 \cong I_2 + I_1/I_2 = A/I_2 \ .$$

Sei also $c \in I_1$ mit $c = \overline{b} - a \mod I_2$. Das Element $a + c$ ist das gesuchte Urbild, denn $a + c = a = \overline{a} \mod I_1$ und $a + c = a + \overline{b} - a \mod I_2$.
Sei nun $n > 2$, $J = \bigcap_{i=2}^{n}$. Nach Induktionsvoraussetzung ist

$$A/J \to \prod_{i=2}^{n} /I_i \to 0$$

exakt. Wir wollen den $n = 2$-Fall benutzen, um die Exaktheit von

$$A \to A/I_2 \times A/J \to 0$$

zu zeigen. Dafür brauchen wir nur:

Behauptung. $I_1 + J = A$.

Nach Voraussetzung gibt es $a_i \in I_1$, $b_i \in I_i$ mit $a_i + b_i = 1$. Daraus erhalten wir $1 = \prod(a_i + b_i) = \prod b_i \mod I_1$. Das Produkt $b_1 \dots b_n$ liegt in I_i für alle i, also in J. □

Tensorprodukt

Zu einem Paar von A-Moduln M, N definiert man einen neuen, das Tensorprodukt $M \otimes_A N$. Die Definition ist implizit, das neue Objekt wird durch seine Eigenschaften beschrieben.

Definition 1.13. *Seien M, N A-Moduln, P ein weiterer Modul. Eine Abbildung*

$$f : M \times N \to P$$

heißt A-bilinear*, wenn für alle $m \in M$ und $n \in N$ die Abbildungen $f(\cdot, n) : M \to P$ und $f(m, \cdot) : N \to P$ Modulhomomorphismen sind.*
Das Tensorprodukt *von M und N ist ein A-Modul $T := M \otimes_A N$ zusammen mit einer bilinearen Abbildung*

$$\theta : M \times N \to M \otimes_A N \; ; (m, n) \mapsto m \otimes n$$

so dass

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_{A-\mathrm{bilin.}}(M \times N, P)$$

für alle A-Moduln P.

Man nennt eine solche Definition eine *universelle Eigenschaft*.

Bemerkung. Der Isomorphismus von Homs wird induziert von der Verknüpfung

$$M \times N \xrightarrow{\theta} M \otimes_A N \to P \; .$$

In Worten: Jede bilineare Abbildung $M \times N \to P$ faktorisiert eindeutig über θ.

Satz 1.14. *Das Tensorprodukt existiert und ist eindeutig.*

Beweis: Eindeutigkeit: Seien (T, θ) und (T', θ') zwei Tensorprodukte. Die Abbildung $\theta' : M \times N \to T'$ ist bilinear. Nach der universellen Eigenschaft von (T, θ) gibt es dann eine Faktorisierung

$$\theta' : M \times N \xrightarrow{\theta} T \xrightarrow{f} T' \ .$$

Ebenso gibt es

$$\theta : M \times N \xrightarrow{\theta'} T \xrightarrow{g} T' \ .$$

Behauptung. $f \circ g = \mathrm{id}$.

Es gilt

$$f \circ g \circ \theta' = f \circ \theta = \theta' = \mathrm{id} \circ \theta' \ .$$

Wegen der Eindeutigkeit in der universellen Eigenschaft von θ' folgt $f \circ g = \mathrm{id}$.
Existenz: Sei $\tilde{T}$ der freie A-Modul

$$\bigoplus_{i \in M \times N} A = \{\sum_{j=1}^{n} a_j(m_j, n_j) \mid n \geq 0, a_j \in A, m_j \in M, n_j 1 N\} \ .$$

Wir definieren $\tilde{\theta} M \times N \to \tilde{T}$ durch $(m, n) \mapsto 1(m, n)$. Hieraus wollen wir eine bilineare Abbildung machen. Dies erzwingt Relationen. Sei $R \subset \tilde{T}$ der Untermodul, der erzeugt wird von

$$\begin{gathered}(m + m', n) - (m, n) - (m', n) \\ (m, n + n') - (m, n) - (m, n') \\ (am, n) - a(m, n) \\ (m, an) - a(m, n)\end{gathered}$$

für alle $m, m' \in M$, $n, n' \in N$, $a \in A$. Sei $T = \tilde{T}/R$. Wir schreiben $m \otimes n$ für $(m, n) + R$. Sei $\theta(m, n) = m \otimes n$. Es gilt

$$\begin{gathered}(m + m') \otimes n = m \otimes n + m' \otimes n, m \otimes (n + n') = m \otimes n + m \otimes n' \\ (am) \otimes n = a(m \otimes n) = m \otimes (an)\end{gathered}$$

insbesondere ist θ eine bilineare Abbildung.

Behauptung. (T, θ) *erfüllt die universelle Eigenschaft.*

Sei $f : M \times N \to P$ bilinear. Wir definieren

$$\tilde{f} : \tilde{T} \to P \ ; \sum a_j(m_j, n_j) \mapsto \sum a_j f(m_j, n_j) \ .$$

Dies ist ein Modulhomomorphismus. R liegt im Kern von $\tilde{f}$, z.B. gilt

$$\tilde{f}((m + m', n) - (m, n) - (m', n)) = \tilde{f}(m + m', n) - \tilde{f}(m, n) - \tilde{f}(m', n) = 0$$

Daher faktorisiert $\tilde{f}$ über $T = \tilde{T}/R$. Dies ist die einzige Möglichkeit, denn es muss $f(m, n) = \tilde{f}(m \otimes n)$ gelten. □

Elemente der Form $m \otimes n$ heißen *Elementartensoren*. Im allgemeinen ist *nicht* jeder Tensor elementar.

Satz 1.15. *Seien V, W K-Vektorräume mit Basen $\{e_i \mid i \in I\}$ und $\{f_j \mid j \in J\}$. Dann ist $\{e_i \otimes f_j \mid i \in I, j \in J\}$ eine Basis von $V \otimes_K W$. Insbesondere ist* $\dim(V \otimes_K W) = \dim V \cdot \dim W$.

Beweis: Wir zeigen, dass die angegebene Menge ein lineare unabhängiges Erzeugendensystem ist. Aus dem Beweis der Existenz kennen wir eine Beschreibung von $V \otimes W$. Sei $\sum \lambda_k v_k \otimes w_k$ ein beliebiges Element. Es gilt

$$v_k = \sum a_{ki} e_i \ ; w_k = \sum b_{kj} f_j$$

mit $a_{ki}, b_{kj} \in K$. Es folgt

$$\sum \lambda_k v_k \otimes w_k = \sum \lambda_k (\sum a_{ki} e_i) \otimes (\sum b_{kj} f_j) = \sum \lambda_k a_{ki} b_{kj} e_i \otimes f_j \ .$$

Die $e_i \otimes f_j$ sind ein Erzeugendensystem. Sei

$$\sum a_{ij} e_i \otimes f_j = 0 \ .$$

Sei $f : V \times W \to P$ ein bilineare Abbildung. Nach Voraussetzung gilt dann $\sum a_{ij} f(e_i, f_j) = 0$. Wir wählten speziell $P = K$ und

$$f_{kl} : V \times W \to K \ ; (\sum b_i e_i, \sum c_j f_j) \mapsto b_k c_l \ .$$

Also gilt

$$0 = \sum a_{ij} f_{kl}(e_i, f_j) = a_{kl} \ .$$

Demnach sind die Vektoren linear unabhängig. □

Fasst man K^n als Spaltenvektoren auf, so entsprechen die Elemente von $K^n \otimes K^m$ den $n \times m$-Matrizen.

Bemerkung. In der Physik ist oft die Rede von Tensoren, entwar dem Trägheitstensor. Sei dafür M eine Mannigfaltigkeit (die Raumzeit oder ein Phasenraum), $V = TM_x$ der Tangentialraum in einem Punkt. Dann ist

$$T^p_q = V \otimes \ldots V \otimes V^* \otimes \ldots \otimes V^* \quad q \text{ bzw. } p \text{ Faktoren})$$

($V^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ der Dualvektorraum) der Raum der p-fach kontravarianten und q-fach kovarianten Vektoren. Sie bilden ein Vektorraumbündel auf M.

Beispiel. $\mathbb{Z}/3 \otimes_{\mathbb{Z}} \mathbb{Z}/2$ hat als Erzeuger $m \otimes n$ mit $m \in \mathbb{Z}/3$ und $n \in \mathbb{Z}/2$. Es folgt

$$m \otimes n = (4m) \otimes n = 4(m \otimes n) = m \otimes (4n) = m \otimes 0 = 0(m \otimes 0) = 0$$

Also verschwinden alle Erzeuger von $\mathbb{Z}/3 \otimes_{\mathbb{Z}} \mathbb{Z}/2$. Das Tensorprodukt ist der Nullmodul.

Satz 1.16 (Rechenregeln). *Seien M, N, P Moduln für den Ring A. Dann gibt es kanonische Isomorphismen*

(i) $M \otimes N \cong N \otimes M$

(ii) $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$

(iii) $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$

(iv) $A \otimes M \cong M$.

(v) Für $i \in I$ sei M_i ein Modul. $\left(\bigoplus_{i\in I} M_i\right) \otimes N \cong \bigoplus_{i\in I} (M_i \otimes N)$.

Beweis: Alle Beweise verlaufen nach dem gleichen Muster. Z.B. (iv):

Behauptung. *M erfüllt die universelle Eigenschaft für $A \otimes M$.*

Sei $\theta : A \times M \to M$ definiert durch $(a, m) \mapsto am$. Gegeben sei eine bilineare Abbildung $f : A \times M \to P$. Man definiert $\tilde{f} : M \to P$ durch $\tilde{f}(m) = f(1, m)$. (Dies ist die einzige Möglichkeit). Dann gilt $f = \tilde{f} \circ \theta$.
Interessant noch (iv): Sei

$$f : \bigoplus M_i \times N \to P$$

eine bilineare Abbildung. Dann ist jede der Abbildungen

$$f_j : M_j \times N \to \bigoplus M_i \times N \to P$$

bilinear, faktorisiert also eindeutig über eine lineare Abbildung

$$f'_j : M_j \otimes N \to P.$$

Dann ist

$$f' = \sum f'_j : \bigoplus (M_j \otimes N) \to P$$

die gesuchte lineare Abbildung. Sie ist eindeutig durch f bestimmt. □

Bemerkung. Wendet man dies auf freie Moduln an, so erhält man das Analogogn von Satz 1.15 für Moduln über beliebigen Ringen.

Satz 1.17. *Sei $f : A \to B$ ein Ringhomomorphismus. Dann gibt es Funktoren*

$$\{A\text{-}Moduln\} \underset{f^*}{\overset{f_*}{\rightleftarrows}} \{B\text{-}Moduln\}$$

indem jedem A-Modul M der B-Modul $B \otimes_A M$ zugeordnet wird (Skalarenerweiterung), bzw. ein B-Modul N als A-Modul aufgefasst wird (Skalareneinschränkung).

Beweis: Jeder B-Modul ist auch ein A-Modul. Ist M ein A-Modul, so wird $B \otimes_A M$ ein B-Modul via

$$B \times B \otimes_A M \to B \otimes_A M \; ; (b, b' \otimes m) \mapsto (bb') \otimes m \; .$$

□

Lokalisierung

Definition 1.18. *Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt* multiplikativ, *wenn $1 \in S$, $0 \notin S$ und $s, t \in S \Rightarrow st \in S$. Wir setzen dann*

$$S^{-1}A = S \times A/\sim = \{\frac{a}{s} \mid a \in A, s \in S\}/\sim$$

wobei $\frac{a}{s} \sim \frac{a'}{s'}$ genau dann, wenn es ein $t \in S$ gibt mit $(as' - as)t = 0$. Wir definieren

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

$S^{-1}A$ heißt Lokalisierung von A an S.

Wir werden gleich überprüfen, dass dies einen Ring definiert.

Beispiel. (i) Wenn A ein Integritätsbereich ist, dann vereinfacht sich die Äquivalenzrelation zu $\frac{a}{s} \sim \frac{a'}{s'}$ genau dann, wenn $as' = a's$. Speziell für $S = A \setminus \{0\}$ erhalten wir den *Qutientenkörper von A*.

(ii) $A = \mathbb{Z}$, $S = 1, 3, 9, \ldots$. Dann ist $S^{-1}A$ die Menge der Brüche, deren Nenner eine Potenz von 3 ist.

(iii) $A = \mathbb{Z}$, p eine Primzahl, $S = \{n \in \mathbb{Z} \mid (p, n) = 1$. Dann ist $S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$, die Menge der Brüche, deren Nenner nicht durch p teilbar ist.

(iv) Sei A ein Ring, $f \in A$ ein Element. Dann ist $S = \{f^i \mid i \in \mathbb{N}_0\}$ multiplikativ. Man schreibt für $S^{-1}A$ auch A_f, die *Lokalisierung von A an f*.

(v) Sei A ein Ring, $\mathfrak{m} \subset A$ ein maximales (allgemeiner: Primideal, s.u.). Dann ist $S = A \setminus \mathfrak{m}$ eine multiplikative Menge. ($f \neq 0 \mod \mathfrak{m}, g \neq 0 \mod \mathfrak{m} \Rightarrow fg \neq 0 \mod \mathfrak{m}$, denn $A/\mathfrak{m}$ ist ein Körper.) Man schreibt für $S^{-1}A$ auch $A_{\mathfrak{m}}$, die Lokalisierung von A an $\mathfrak{m}$.

Lemma 1.19. *Die Lokalisierung ist ein Ring.*

Beweis:

Behauptung. *$\sim$ ist eine Äquivalenzrelation.*
Die Relation ist symmetrisch und reflexiv. Zur Transitivität:

$$\frac{a}{s} \sim \frac{a'}{s'} \sim \frac{a''}{s''} \Rightarrow (as' - a's)t = 0, (a's'' - a''s')u = 0$$

Die erste Gleichung wird mit us'' multipliziert, die zweite mit ts.

$$\Rightarrow 0 = ut(ass'' - a'ss'') + ut(a's''s - a''s's) = uts'(as'' - a''s) \Rightarrow \frac{a}{s} \sim \frac{a''}{s''} \; .$$

Behauptung. *$+$ ist wohldefiniert.*

Sei $\frac{a}{s} \sim \frac{a'}{s'}$, d.h. es gibt $t \in S$ mit $t(as' - a's)) = 0$. Dann gilt

$$\frac{a}{s} + \frac{b}{u} = \frac{au + bs}{su} \; ; \frac{a'}{s'} + \frac{b}{u} = \frac{a'u + bs'}{s'u}$$

Zu untersuchen ist die Differenz

$$(au + bs)(s'u) - (a'u + bs')(su) = au^2s' + buss' - a'u^2s - bss'u = u^2(as' - a's) \; .$$

Sie wird von t annuliert. Wegen $u^2t \in S$ ist dies die gesuchte Relation.
Die übrigen Behauptungen und Axiome werden ebenso überprüft. □

Lemma 1.20. *Die Abbildung $A \to S^{-1}A$ via $a \mapsto \frac{a}{1}$ ist ein Ringhomomorphismus. Sie ist genau dann injektiv, wenn S nullteilerfrei ist.*

Beweis:

$$a + b \mapsto \frac{a}{1} + \frac{b}{1} = \frac{a1 + b1}{1 \cdot 1} = \frac{a + b}{1}$$
$$ab \mapsto \frac{a}{1}\frac{b}{1} = \frac{ab}{1}$$

Der Kern ist

$$\left\{ a \in A \mid \frac{a}{1} \sim \frac{0}{1} \right\} = \{ a \in A \mid \text{ es gibt } s \in S \mid s(a1 - 01) = 0 \} \; .$$

□

Im Falle eines Integritätsbereichs können alle Lokalisierungen als Unterringe des Quotientenkörpers aufgefasst werden.

Definition 1.21. *Sei M ein A-Modul, $S \subset M$ eine muliplikative Teilmenge. Wir setzen*

$$S^{-1}M = \{ \frac{m}{s} \mid m \in M, s \in S \} / \sim$$

wobei $\frac{m}{s} \sim \frac{m'}{s'}$ genau dann, wenn $t(sm' - s'm)$ für ein $t \in S$.

Lemma 1.22. *$S^{-1}M$ ist ein $S^{-1}A$-Modul. Es gilt*

$$S^{-1}A \otimes_A M \cong S^{-1}M \; .$$

Beweis: Die Modulstruktur wird durch

$$(\frac{a}{s}, \frac{m}{t}) \mapsto \frac{am}{st}$$

gegeben. Wohldefiniertheit und alle Axiome sind leicht zu überprüfen. Diese Skalarmultiplikation

$$S^{-1}A \times M \to S^{-1}A \times S^{-1}M \to S^{-1}M$$

ist A-bilinear, also gibt es eine eindeutige A-lineare Abbildung

$$\phi : S^{-1}A \otimes_A M \to S^{-1}M \; .$$

Behauptung. *Dies ist ein $S^{-1}A$-Modulhomomorphismus.*

$$\frac{a}{s}\phi(\frac{b}{t}\otimes m) = \frac{a}{s}\frac{bm}{t} = \frac{abm}{st} = \phi(\frac{ab}{st}\otimes m)$$

Behauptung. *ϕ ist surjektiv.*

$\frac{m}{s} = \phi(\frac{1}{s}\otimes m)$.

Behauptung. *ϕ ist injektiv.*

Ein beliebiges Element von $S^{-1}A\otimes_A M$ kann geschrieben werden als

$$\begin{aligned}\sum a_i\frac{b_i}{s_i}\otimes m_i = \sum\frac{1}{s_i}\otimes a_ib_im_i &= \sum\frac{1}{s_1\dots s_n}\otimes s_1\dots\hat{s}_i\dots s_na_ib_im_i\\ &= \frac{1}{s_1\dots s_n}\otimes\sum s_1\dots\hat{s}_i\dots s_na_ib_im_i = \frac{1}{s}\otimes m\end{aligned}$$

($\hat{s}_i$ bedeutet, dass dieser Faktor weggelassen wird.) Ein solches Element liegt im Kern von ϕ, wenn $\frac{m}{s} = \frac{0}{1}$, also wenn es $t\in S$ gibt mit $tm = 0$ in M. Dann gilt aber auch

$$\frac{1}{s}\otimes m = \frac{1}{st}\otimes tm = 0\ .$$

□

Bemerkung. Ist $0\to M_1\to M_2\to M_3\to 0$ exakt, so ist auch $0\to S^{-1}M_1\to S^{-1}M_2\to S^{-1}M_3\to 0$ exakt. Für beliebige Tensorprodukte ist das falsch. Im allgemeinen ist nur $N\otimes M_1\to N\otimes M_2\to N\otimes M_3\to 0$ exakt.

Geometrische Interpretation

Sei in diesem Abschnitt k ein algebraisch abgeschlossener Körper.

Satz 1.23. *Sei $V\subset\mathbb{A}^n$ eine affine Varietät über k.*

(i) Die offenen Mengen $U_f = V\setminus V(f)$ für $f\in k[V]$ sind eine Basis der Zariski-Topologie, d.h. jede offene Menge ist Vereinigung von solchen.

(ii) U_f ist isomorph zu einer affinen Varietät $\tilde{U}_f\subset\mathbb{A}^{n+1}$ mit Ring der regulären Funktionen

$$k[\tilde{U}_j]\cong k[V]_f$$

Wir sagen: Jede Zariski-offene Teilemenge einer affinen Varietät kann durch affine Varietäten überdeckt werden.

Beweis: Sei $U = V\smallsetminus V(S)$ Zariski-offen. Nach Definition ist

$$V(S) = \bigcap_{f\in S}V(f)\Rightarrow V\smallsetminus V(S) = V\smallsetminus\bigcap_{f\in S}V(f) = \bigcup_{f\in S}U_f$$

Sei nun $V = V(T)$ für eine Teilmenge $T \subset k[X_1, \ldots, X_n]$. Das Element $f \in k[V]$ wird repräsentiert durch $\tilde{f} \in k[X_1, \ldots, X_n]$. Sei nun

$$\tilde{T} = T \cup \{\tilde{f}X_{n+1} - 1\} \subset k[X_1, \ldots, X_{n+1}] \qquad \tilde{U}_f = V(\tilde{T})$$

Damit gilt

$$\tilde{U}_f = \{(x_1, \ldots, x_n, x_{n+1}) \in k^{n+1} \mid (x_1, \ldots, x_n) \in V \text{ und } \tilde{f}(x_1, \ldots, x_n)x_{n+1} = 1\}$$

Die Koordiante x_{n+1} ist also eindeutig durch $x_1, \ldots, x_n$ bestimmt, die Projektionsabbildung $\tilde{U}_f \to V$ ist injektiv. Die Gleichung ist genau dann lösbar, wenn

$$\tilde{f}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \neq 0,$$

also der Bildpunkt in U_f liegt. Dies ist die gesuchte Bijektion

$$\pi : \tilde{U}_f \to U_f$$

Dasselbe Argument zeigt, dass auch die offenen Teilmengen von U_f und $\tilde{U}_f$ übereinstimmen, d.h. die Abbildung ist ein Homöomorphismus.

Behauptung. *Für $g : V \to k$ regulär ist auch die Restriktion $\pi^* g : \tilde{U}_f \to k$ regulär.*

g ist repräsentiert durch ein Polynom $g' \in k[X_1, \ldots, X_n] \subset k[X_1, \ldots, X_{n+1}]$. Dann ist g' auch ein Repräsentant von $\pi^* g$.
Damit haben wir einen Ringhomomorphismus $\pi^* : k[V] \to k[\tilde{U}_f]$.

Behauptung. *π^* faktorisiert durch $k[V]_f$.*

Wir müssen überprüfen, dass $\pi^* f$ invertierbar ist. Das Inverse ist die Funktion X_{n+1}, denn in $k[\tilde{U}_f]$ gilt $fX_{n+1} = 1 \mod I(\tilde{T})$.
Wir haben es mit dem folgenden kommutativen Diagramm zu tun:

$$\begin{array}{ccc}
k[X_1, \ldots, X_n] & \xrightarrow{\subset} & k[X_1, \ldots, X_{n+1}] \\
\downarrow & & \downarrow \\
k[X_1, \ldots, X_n]/I(T)_{\tilde{f}} & \longrightarrow & k[X_1, \ldots, X_{n+1}/I(\tilde{T}) \\
\downarrow & & \downarrow p \\
k[V]_f & \xrightarrow{\pi^*} & k[\tilde{U}_f]
\end{array}$$

Behauptung. *$k[V]_f \to k[\tilde{U}_f]$ ist surjektiv.*

Wegen $I(\tilde{T}) \subset I(\tilde{U}_f)$ ist p surjektiv. Es genügt daher zu zeigen, dass

$$k[X_1, \ldots, X_n]/I(T)_{\tilde{f}} \to k[X_1, \ldots, X_{n+1}/I(\tilde{T})$$

surjektiv. Die Erzeuger $X_1, \ldots, X_n$ liegen offensichtlich im Bild. Der Erzeuger $X_{n+1} = \tilde{f}^{-1} \mod I(\tilde{T})$ ist das Bild von $1/\tilde{f}$.

Behauptung. $k[V]_f \to k[\tilde{U}_f]$ *ist injektiv.*

Sei $g/f^i \in k[V]_f$, so dass $\pi^*(g/f^i) = 0$. Diese Funktion wird nach unseren bisherigen Überlegungenrepräsentiert durch $\tilde{g}X_{n+1}$. Da X_{n+1} keine Nullstellen auf $\tilde{U}_f$ hat, folgt hieraus $\tilde{g} \in I(\tilde{U}_f)$, d.h. g verschwindet auf ganz U_f. Hieraus folgt $gf = 0$ auf ganz V. Nach Definition der Lokalisierung ist dann $g/f^i = 0$ in $k[V]_f$. □

Kapitel 2

Moduln über Hauptidealringen

Ziel ist der Beweis des Elementarteilersatzes: Ist A eine endliche abelsche Gruppe, so gilt

$$A \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k \ .$$

Eine abelsche Gruppe ist nichts als ein $\mathbb{Z}$-Modul. Der Beweis des Satzes funktioniert gleichermaßen für alle Hauptidealringe.
In diesem Kapitel sind alle Ringe nullteilerfrei.

Hauptidealringe und Primfaktorzerlegung

Definition 2.1. *$I \subset A$ heißt* Hauptideal*, wenn $I = (f) = Af$ für ein $f \in A$. Ein Integritätsring heißt* Hauptidealring*, wenn jedes Ideal ein Hauptideal ist.*

Beispiel. $\mathbb{Z}$, $k[X]$ (I Satz 2.2), $\mathbb{Z}[i]$ (Übungsaufgabe), alle Körper (trivial). Keine Hauptidealringe sind $\mathbb{Z}[\sqrt{-5}]$, $k[X, Y]$ (betrachte $I = (X, Y)$).

Lemma 2.2. *Sei k ein Körper. Dann ist der Potenzreihenring $k[[X]]$ ein Hauptidealring.*

Beweis: Es gilt $k[[X]]^* = k^*$, denn

$$1 = \sum_i a_i X^i \sum_j b_j X^j = \sum (\sum_{i+j=k} a_i b_k X^k$$

impliziert $a_0 b_0 = 1$ und rekursiv ist jedes b_j eindeutig aus den a_i für $i \leq j$ zu bestimmen.
Jedes $f \in k[[X]]$ kann also als $X^{v(f)} g$ geschrieben werden, wobei $g \in k[[X]]^*$. Sei $I \subset k[[X]]$ ein Ideal. Es wird erzeugt von X^v wobei v das Minimum der $v(f)$ für $f \in I$. □

Dieses Beispiel läßt sich verallgemeinern:

Definition 2.3. *Sei K ein Körper. Eine* diskrete Bewertung *von K ist eine surjektive Abbildung*

$$v : K^* \to \mathbb{Z}$$

so dass

(i) $v(xy) = v(x) + v(y)$,

(ii) $v(x + y) \geq \min(v(x), v(y))$.

$A = \{0\} \cup \{x \in K^* \mid v(x) \geq 0$ *heißt* Bewertungsring *von K. Ein Ring, der isomorph zu einem solchen A ist, heißt* diskreter Bewertungsring.

Das Wort diskret bezieht sich auf die diskrete Gruppe $\mathbb{Z}$, im Unterschied zu Bewertungen mit Werten in $\mathbb{R}$ oder $\mathbb{Z}^2$. Man kann zwanglos v auf ganz K fortsetzen, wenn man $v(0) = \infty$ setzt.

Beispiel. (i) $A = k[[X]] \subset K = \{\sum_{i=n}^{\infty} a_i X^i \mid n \in \mathbb{Z}, a_i \in k\}$ für einen Körper k. Die Bewertung ist wie im letzten Beweis definiert, d.h. $f = X^{v(f)}g$ mit $g \in k[[X]]^*$. Der Bewertungsring ist der Ring der Potenzreihen.

(ii) Speziell $k = \mathbb{C}$, A der Ring der in einer Umgebung von 0 konvergierenden Potenzreihen, d.h. der Ring der Potenzreihenentwicklungen von holomorphen Funktionen. Die Bewertung ist die gleiche wie im vorherigen Beispiel.

(iii) Sei p eine Primzahl, $K = \mathbb{Q}$, $v_p : \mathbb{Q} \to \mathbb{Z}$ bildet $p^i a$ mit $a \in \mathbb{Z}^*_{(p)}$ auf i ab. Der Bewertungsring ist gerade $\mathbb{Z}_{(p)}$.

Bemerkung. Sei $v : K^* \to \mathbb{Z}$ eine diskrete Bewertung, $a \in \mathbb{R}$ eine feste positive reelle Zahl. Die Abbildung

$$|\cdot| : K \to \mathbb{R} \ ; \ 0 \mapsto 0 \ ; \ x \neq 0 \mapsto a^{-v(x)}$$

hat alle Eigenschaften eines Absolutbetrages. Dieser Betrag macht dann K zu einem metrischen Raum. Im Fall $K = \mathbb{Q}$ und $v = v_p$ erhält man die p-adische Metrik auf $\mathbb{Q}$. Die Komplettierung von $\mathbb{Q}$ bezüglich dieser Metrik heißt *Körper der p-adischen Zahlen.*

Satz 2.4. *Jeder diskrete Bewertungsring A ist ein Hauptidealring. Er hat ein eindeutig bestimmtes maximales Ideal, nämlich*

$$I = \{x \in A \mid v(x) > 0\}$$

Es gilt $A^* = \{x \in A \mid v(x) = 0\}$.

Beweis: Zunächst bestimmen wir A^*. Es gilt $v(1) = v(1 \cdot 1) = v(1) + v(1)$, also $v(1) = 0$. (Damit haben wir auch $1 \in A$ überprüft). Sei $xy = 1$ in A. Dann folgt

$$0 = v(1) = v(xy) = v(x) + v(y) \ .$$

Da $x, y \in A$ ist $v(x), v(y) \geq 0$. Es folgt $v(x) = v(y) = 0$. Ist umgekehrt $v(x) = 0$, so ist $x \neq 0$ und hat demnach ein Inverses y in K. Dieses Inverse hat die Bewertung 0, liegt also auch in A.
Sei nun I wie im Lemma angegeben.

Behauptung. *Dies ist ein Ideal, das jedes echte Ideal enthält.*

Seien $x, y \in I$, d.h. $v(x), v(y) > 0$. Dann folgt $v(x+y) = \min(v(x), v(y) > 0$. Für $a \in I$ und $x \in I$ folgt $v(ax) = v(a) + v(x) > 0$, also $ax \in I$. Damit ist I ein Ideal. Sei $J \subset A$ ein Ideal ungleich A, d.h. J enthält keine Einheiten. Sei $x \in J$. Dann ist einerseits $v(x) \geq 0$, andererseits $v(x) \neq 0$. Also liegt x in I.

Behauptung. *Alle Ideale sind Hauptideale.*

Sei J ein Ideal, $\pi \in J$ ein Element mit minimaler Bewertung. (Wegen $v(J) \subset \mathbb{N}_0$ gibt es ein solches Element.) Sei $x \in J$ beliebig. Dann gilt

$$v\left(\frac{x}{\pi}\right) = v(x) - v(\pi) \geq 0$$

nach Wahl von π. Also liegt $y = \frac{x}{\pi}$ im Bewertungsring und $x = y\pi \in (\pi)$. □

Bemerkung. Sei $I = (\pi)$. Dann ist jedes andere Ideal von der Form (π^n) mit $n \in \mathbb{N}_0$.

Definition 2.5. *Sei A ein Integritätsring. $a \in A$ heißt* irreduzibel*, wenn a keine Einheit ist und aus $a = bc$ in A folgt b Einheit oder a Einheit. a heißt* Primelement*, wenn $a \neq 0$ und a keine Einheit und aus $a \mid bc$ folgt $a \mid b$ oder $a \mid c$.*

Beispiel. In $\mathbb{Z}$ sind die irreduziblen Elemente die Primzahlen, in $k[X]$ die irreduziblen Polynome.

Lemma 2.6. *Primelemente sind stets irreduzibel. Ist A ein Hauptidealring, so sind irreduzible Elemente prim.*

Beweis: Sei a Primelement, $a = bc$. Dann folgt ohne Einschränkung $b = ab'$, also $a = abb'c \Rightarrow a(1 - b'c) =$. Da $a \neq 0$ und A ein Integritätsring, muss $1 = bc'$ gelten, dh. c ist Einheit. Der Umkehrschluss wurde in I Lemma 2.10 gezeigt. Dort ging es um Polynomringe, aber das Argument war allgemein. □

Definition 2.7. *Ein Integritätsring heißt* faktoriell*, wenn jedes Element ungleiche Null eine Zerlegung in Primfaktoren hat, d.h. zu $0 \neq x \in A$ gibt es irreduzible $p_i \in A$ mit*

$$a = p_1 \dots p_n \ .$$

Hat man zwei solche Darstellungen $p_1 \dots p_n = q_1 \dots q_m$, sow ist $n = m$ und nach geeigneter Umnummerierung gilt $p_i = u_i q_i$ mit $u_i \in A^*$.

Beispiel. $\mathbb{Z}$, $k[X]$, aber auch $k[X_1, \dots, X_n]$ (kein Beweis).

Satz 2.8. *Hauptidealringe sind faktoriell.*

Beweis: Man vergleiche den Beweis von I Theorem 2.11, den Fall von Polynomringen. Tatsächlich wurde nur verwendet, dass in einem Hauptidealring gerechnet wird. □

Elementarteilersatz

Theorem 2.9 (Elementarteilersatz). *Sei A ein Hauptidealring, N ein endlich erzeugter A-Modul. Dann gilt*

$$N \cong A^r \times A/(q_1) \times A/(q_2) \times \dots A/(q_n)$$

mit $0 \neq q_i \in A$ und $q_i \mid q_{i-1}$. Die Zahl r und die Folge der Ideale

$$(q_1) \supset (q_2) \supset \dots \supset (q_n)$$

ist eindeutig bestimmt.

Die q_i heißen *Elementarteiler von M*. Für $A = \mathbb{Z}$ erhalten wir den mehrfach genannten Elementarteilersatz.

Theorem 2.10 (2. Version des Elementarteilersatzes). *Sei A ein Hauptidealring, F ein freier A-Modul von endlichem Rang, $M \subset F$ ein Untermodul. Dann gibt es eine Basis $e_1, \dots, e_m$ von F und Elemente $q_1, \dots, q_n \in A \setminus \{0\}$ mit $q_i \mid q_{i+1}$, so dass*

$$\{q_i e_i \mid i = 1, \dots, n\}$$

eine Basis von M ist. Die Folge der Ideale $(q_1), \dots, (q_n)$ ist eindeutig bestimmt.

Bemerkung. In 2.10 sei $N = F/M$. In der Basis des Theorems gilt dann

$$N \cong A/(q_1) \times \dots A/(q_n) \times A^r$$

mit $r = m - n$. Dies ist ein endlich erzeugter Modul. Die Eindeutigkeit in 2.9 impliziert also die Eindeutigkeit in 2.10. Sei umgekehrt N ein A-Modul mit Erzeugenden $x_1, \dots, x_m$. Sei F ein freier A-Modul mit Basis $b_1, \dots, b_m$. Dann gibt es eine surjektive Abbildung

$$F \to N \ ; \ b_i \mapsto x_i \ .$$

Sei M der Kern. Die Existenz der Elementarteiler in 2.10 impliziert also die Existenz der Zerlegung in 2.10
Der Beweis ist aufwendiger, wir holen aus.

Definition 2.11. *Sei A ein Ring, M ein A-Modul. $x \in M$ heißt* Torsionselement*, falls es $0 \neq a \in A$ gibt mit $ax = 0$. M heißt* Torsionsmodul*, wenn jedes Element ein Torsionselement ist. M heißt* torsionsfrei*, wenn 0 das einzige Torsionselement ist.*

Beispiel. Für $A = \mathbb{Z}$ sind $\mathbb{Z}/5$ und $\mathbb{Q}/\mathbb{Z}$ Torsionsmoduln.

Satz 2.12. *Sei M ein endlich erzeugter torsionsfreier Modul über einem Hauptidealring. Dann ist M frei.*

Wir arbeiten vor:

Lemma 2.13. *Sei A ein Ring,*

$$0 \to N \to M \to F \xrightarrow{\pi} 0$$

eine kurze exakte Sequenz von A-Moduln.

(i) Wenn es eine Abbildung $\psi : F \to M$ gibt mit $\pi \circ \psi = \mathrm{id}$, dann ist $M \cong N \oplus F$.

(ii) F sei freier A-Modul. Dann gilt $M \cong N \oplus F$.

Beweis: Wegen $\pi \circ \psi = \mathrm{id}$ ist ψ injektiv. Sei $\tilde{F} = \mathrm{Im}(\psi)$.

Behauptung. $\tilde{F} \cap N = 0$.

Sei $x \in \tilde{F} \cap N$. Nach Voraussetzung ist $N = \mathrm{Ker}\,\pi$, also $0 = \pi(x)$. Wegen $x \in \tilde{F}$ gilt $x = \psi(y)$, zusammen also $y = \pi\psi(y) = 0$.

Behauptung. *Die natürliche Abbildung $N \oplus \tilde{F} \to M$ ist ein Isomorphismus.*

Der Kern sind Paare (f, n) mit $f + n = 0$, also $f = -n \in N \cap \tilde{F} = 0$. Damit ist die Abbildung injektiv. Sei $x \in M$ beliebig, $n = x - \psi\pi(x)$. Es gilt $\pi(n) = \pi(x) - \pi\psi\pi(x) = \pi(x) - \mathrm{id}\,\pi(x) = 0$, also $n \in N$. Es gilt $\psi\pi(x) \in \tilde{F} = \mathrm{Im}\,\psi$. Es folgt $x = n + \psi\pi(x)$, d.h. x ist Bild des Paares $(n, \psi\pi(x))$.
Sei nun F freier A-Modul. Sei $B = \{b_i \mid i \in I\}$ eine Basis von F, d.h. jedes Element von F ist eindeutige (endliche) Linearkombination von Elemente aus B. Wähle Urbilder $\tilde{b_i} \in M$ der b_i. Wir definieren

$$\psi : F \to M \ ; \ \sum_{i \in I} a_i b_i \mapsto \sum_{i \in I} a_i \tilde{b_i} \ .$$

Offensichtlich ist $\pi \circ \psi = \mathrm{id}$. □

Bemerkung. ψ heißt *Schnitt* von π. Die Abbildung $p = \psi\pi$ ist ein Projektor, d.h. $p^2 = \psi\pi\psi\pi = \psi\,\mathrm{id}\,\pi = p$. Projektoren erzeugen stets eine Zerlegung in direkte Summen (Übungsaufgabe).

Lemma 2.14. *Sei A ein Hauptidealring, $M \subset A^n$ ein Untermodul. Dann ist M frei von Rang höchstens n.*

Beweis: Induktion nach n. Für $n = 1$ ist M ein Ideal. Da A ein Hauptidealring ist, gilt $M = (f) = Af$ für ein $f \in M$. Dieses Element ist Basis, da Hauptidealringe nullteilerfrei sind.
Sei nun $n > 1$ beliebig, $1 \leq m < n$. Wir betrachten

$$p : A^n \to A^m$$

die Projektion auf die ersten m Koordinaten. Der Kern ist $0^m \times A^{m-n}$, also frei. Sei $\pi = p|_M$. Der Kern von π ist enthalten im Kern von p, also frei nach Induktionsvoraussetzung. Das Bild von π ist enthalten in A^m, also ebenfalls frei nach Induktionsvoraussetzung. Die Sequenz

$$0 \to \mathrm{Ker}\,\pi \to M \to \mathrm{Im}\,\pi \to 0$$

ist exakt. Nach dem letzten Lemma folgt $M \cong \operatorname{Ker}\pi \oplus \operatorname{Im}\pi$. Als direkte Summe von freien Moduln ist M frei. Der Rang von M ist die Summe der Ränge von $\operatorname{Ker}\pi$ und $\operatorname{Im}\pi$, nach Induktionsvoraussetzung also höchstens $m+n-m$. □

Beweis von Satz 2.12. Sei A der Hauptidealring, M ein endlich erzeugter torsionsfreier A-Modul. Seien $x_1, \ldots, x_N$ Erzeuger von M. Darin sei $\{x_1, \ldots, x_n\}$ eine maximale linear unabhängige Teilmenge. Für $i > n$ gilt

$$a_i x_i + a_{i1} x_1 + \cdots + a_{in} x_n = 0$$

mit $a_i \neq 0$, denn sonst wäre $\{x_1, \ldots, x_n, x_i\}$ linear unabhängig. Mit anderen Worten: $a_i x_i \in < x_1, \ldots, x_n >$. Sei $b = \prod_{i=n+1}^{N} a_i$. Dann ist $bx_i \in < x_1, \ldots, x_n >$ für $i = 1, \ldots, N$. Wir definieren

$$\phi : M \to M \ ; \ x \mapsto bx \ .$$

M ist torsionsfrei, daher ist $\operatorname{Ker}\phi = \{x \in M \mid bx = 0\} = 0$. Damit ist $M \cong \phi(M)$: Das Bild von ϕ liegt in $< x_1, \ldots, x_n > \cong A^n$. Der Untermodul $\phi(M)$ ist dann frei. □

Bemerkung. Das letzte Lemma folgt umgekehrt sofort aus dem Satz: Ein Untermodul eines torsionsfreien Moduls ist torsionsfrei. Für Hauptidealringe sind Untermoduln von endlich erzeugten Moduln endlich erzeugt (siehe später: Theorie der noetherschen Ringe). Sind torsionsfreie endliche erzeugte Moduln frei, so überträgt sich das auf Untermoduln.

Beispiel. Sei p eine Primzahl, $\mathbb{Q}$ ist eine torsionsfreie abelsche Gruppe, aber nicht frei, denn je zwei Brüche sind linear abhängig.

Korollar 2.15. *Sei A ein Hauptidealring, M endlich erzeugter A-Modul. Sei*

$$T = \{x \in M \mid x \text{ ist Torsionselement}\}$$

Der Torsionsuntermodul. Dann ist $F = M/T$ frei, und es gilt

$$M \cong T \oplus F \ .$$

Beweis: Offensichtlich ist F endlich erzeugt. Sei $x \in F$ ein Torsionselement, d.h. es gibt $a \in A$ mit $ax = 0$. Sei $\tilde{x}$ ein Urbild von x in M. Dann gilt $a\tilde{x} \in T$, d.h es gibt $b \in A$ mit $ba\tilde{x} = 0$. Nach Definition liegt dann $\tilde{x}$ im Torsionsuntermodul T, d.h. aber $x = 0$ in M/T. Damit ist F torsionsfrei, nach Satz 2.12 also frei. Die Sequenz

$$0 \to T \to M \to F \to 0$$

ist exakt. Nach Lemma 2.13 (ii) folgt $M \cong T \oplus F$. □

Beweis der Eindeutigkeit in Theorem 2.9. Sei

$$M \cong A^r \times A/(q_1) \times A/(q_2) \times \ldots A/(q_n) \ .$$

Dann ist $F = M/T \cong A^r$. Nach dem Korollar ist r der Rang von M/T, also eindeutig nach Lemma 1.9. Wir betrachten nur noch Moduln der Form

$$A/(q_1) \times A/(q_2) \times \dots A/(q_n)$$

mit $q_i \neq 0$ und $q_i \mid q_{i+1}$. Seien $p_1, \dots, p_k$ teilerfremde Primteiler von q_n (und damit aller q_i). Sei $q_i = u_i p_1^{e_{1i}} \dots p_k^{e_{ki}}$ die Primfaktorzerlegung. Die Teilerfremdheit bedeutet, dass das Hauptideal $(p_l^{e_{li}}) + (p_j^{e_{ji}})$ für $l \neq j$ der ganze Ring ist. Damit sind die Voraussetzungen des chinesischen Restsatzes erfüllt. Wir können $A/(q_i)$ zerlegen in Faktoren der Form $A/(p_j^{e_{ji}})$. Zu zeigen ist nun die Eindeutigkeit der Folge der Exponenten e_{ji} in

$$M \cong \prod_{i=1}^{k} A/(p_i^{e_{i1}}) \times \dots \times A/(p_i^{e_{in}}) \ .$$

Sei $k_i = A/(p_i)$ der Restklassenkörper.
Wir betrachten $T_1 = \{x \in M \mid p_1 x = 0\}$. Für $i \neq 1$ hat $A/(p_i^e)$ keine solchen Elemente, für $i = 1$ sind es in $A/(p_1^e)$ die Vielfachen von p_1^{e-1}. M/T_1 ist ein k_1-Modul, also ein Vekorraum. Seine Dimension d ist die Anzahl der Elemente von $\{e_{ij} > 0 \mid j = 1, \dots, n\}$. Weiterhin ist

$$M/T_1 \cong \prod_{i=1}^{k} A/(p_i^{f_{i1}}) \times \dots \times A/(p_i^{f_{in}})$$

mit $f_{1j} = e_{1j} - 1$ und $f_{ij} = e_{ij}$ für $i \neq j$. Nach Induktionsvoraussetzung sind die f_{ij} eindeutig bestimmt. Man beachte, dass Faktoren mit $e_{1j} = 1$ nicht aus M/T_1 abgelesen werden können. Ihre Anzahl ist jedoch aus d abzulesen. □

Beweis der Existenz in Theorem 2.10. Sei F freier A-Modul vom Rang m, $M \subset F$ ein Untermodul. Nach Lemma 2.14 ist M ebenfalls frei vom Rang höchstens m. Wir betrachten einen beliebigen Modulhomomorphismus

$$\lambda : F \to A \ .$$

Dann ist $\lambda(M)$ ein Untermodul von A, also ein Ideal J_λ. Ein Ideal ist umso größer, je weniger Primfaktoren sein Erzeuger hat. Sei λ_1 ein Funktional, so dass J_{λ_1} maximal in der Menge der J_λ ist und $(q_1) = J_{\lambda_1}$. Sei $x_1 \in M$ mit $\lambda_1(x_1) = a_1$.

Behauptung. *Für jedes λ gilt $\lambda(x_1) \in (a_1)$.*

Sei $\lambda : F \to A$ mit $b\lambda(x_1) \notin (a_1)$. Wir betrachten das Ideal $(c) = (a_1, b) \supset (a_1)$. Es gibt also $\alpha, \beta \in A$ mit $c = \alpha a_1 + \beta b$. Nun betrachten wir das Funktional $\lambda' = \alpha\lambda_1 + \beta\lambda$. Wegen $\lambda'(x_1) = c$ gilt $J_{\lambda'} \supset (c) \supset (a_1)$. Dies ist ein Widerspruch zur Maximalität von J_{λ_1}.
Sei $f_1, \dots, f_m$ eine beliebige Basis von F,

$$x_1 = c_1 f_1 + \dots c_m f_m \ .$$

Die Projektion auf auf den Koeffizienten von f_i ist ein Funktional, also gilt $c_i \in (a_1)$. Alle Koeffizienten von x_1 sind durch a_1 teilbar. Damit gilt

$$x_1 = a_1 e_1 \text{ für ein } e_1 \in F \ .$$

Behauptung. $F = Ae_1 \oplus \operatorname{Ker} \lambda_1$.

Nach Konstruktion gilt $\lambda(e_1) = 1$, also ist $Ae_1 \cap \lambda_1 = 0$. Sei $x \in F$, dann liegt $y = x - \lambda_1(x)e_1$ im Kern von λ_1. Damit ist x das Bild von $(\lambda_1(x)e_1, y)$.
Sei $F_1 = \operatorname{Ker} \lambda_1$. Dies ist ein freier Modul, dessen Rang echt kleiner ist als m. Sei $M_1 = M \cap F_1$.

Behauptung. $M = Ax_1 \oplus M_1$.

Wir zerlegen $x \in M$ in seine Komponenten, nämlich

$$x = (\lambda_1(x)e_1, x - \lambda_1(x)e_1) \ .$$

Wegen $\lambda_1(x) \in J_{\lambda_1} = (a_1)$, kann der Koeffizient durch a_1 geteilt werden. $\lambda_1(x) = \alpha a_1$ impliziert $\lambda_1(x)e_1 = \alpha a_1 e_1 = \alpha x_1 \in M$. Dann liegt aber auch die zweite Komponente in M. Das Element hat die angegebene Form.
Nach Induktionsvoraussetzung gibt es eine Basis $e_2, \ldots, e_m$ von F_1 und Elemente $a_2, \ldots a_m$ von A, so dass die $a_i e_i$ eine Basis von M_1 sind. Insgesamt haben wir dann eine Basis von F und M gefunden. Ebenfalls nach Induktionsvoraussetzung gilt $a_i \mid a_{i+1}$. für $i \geq 2$.

Behauptung. $a_1 \mid a_2$.

Sei $(c) = (a_1, a_2)$, also gibt es γ_1, γ_2 mit $c = \gamma_1 a_1 + \gamma_2 a_2$. Sei $p_2 : M \to A$ die Projektion auf den Koeffizienten von e_2. Wir betrachten das Funktional $\lambda = \gamma_1 \lambda_1 + \gamma_2 p_2$. Es folgt

$$\lambda(x_1 + a_2 e_2) = \gamma_1 \lambda_1(x_1 + a_2 e_2) + \gamma_2(x_1 + a_2 e_2) = \gamma_1 a_1 + \gamma_2 a_2 = c \ .$$

Wegen der Maximalität von λ_1 und $J_\lambda \subset (c) \subset (a_1)$ folgt $a_1 \mid c$. Dann gilt auch $a_1 \mid a_2$. Damit ist der Beweis abgeschlossen. □

Jordansche Normalform

Wir spezialisieren den Normalteilersatz im Fall $A = k[X]$, wobei k ein Körper ist. Wir haben gesehen (Lemma 1.4), dass ein $k[X]$-Modul das Gleiche ist wie ein Vektorraum zusammen mit einem Endomorphismus.

Lemma 2.16. *Ein endlich erzeuter $k[X]$-Torsionsmodul ist das Gleiche wie ein endlich dimensionaler k-Vektorraum zusammen mit einer linearen Abbildung $\theta : V \to V$.*

Beweis: Sei M ein endlich erzeugter $k[X]$-Torsionsmodul. Nach dem Elementarteilersatz gilt dann

$$M \cong k[X]/(q_1) \times \cdots \times k[X]/(q_n)$$

wobei die q_1 Polynome ungleich Null sind. Wie in Algebra I gilt $\dim_k k[X]/(q_i) = \deg q_i$, also ist der M zugrundeliegende Vektorraum endlich dimensional. Umgekehrt sei M N-dimensional, $m \in M$ beliebig. Dann ist die Menge

$$\{m, Xm, X^2m, \ldots, X^n m$$

linear abhängig über k, d.h. es gibt $a_i \in k$ mit

$$\sum_{i=0}^{n} a_i X^i m = 0 \ .$$

Das Polynom $\sum a_i X^i$ annuliert m, also ist m torsion. □

Korollar 2.17. *Sei V ein endlich dimensionaler k-Vektorraum, $\theta : V \to V$ eine k-lineare Abbildung. Dann gibt es eine Basis von V, so dass die darstellende Matrix die Form*

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \cdots & \\ 0 & & & A_n \end{pmatrix}$$

mit A_i von der Form

$$\begin{pmatrix} 0 & & & & 0 & -a_0 \\ 1 & 0 & & & & -a_1 \\ 0 & 1 & 0 & & & -a_2 \\ & & & \cdots & & \\ & & & 1 & 0 & -a_{n-2} \\ 0 & & & 0 & 1 & -a_{n-1} \end{pmatrix} .$$

Dabei können die charakteristischen Polynome

$$\mathrm{Char}(A_i) = a_0 + a_1 X + \cdots + a_m X^m$$

als Potenzen von irreduziblen Polynomen angenommen werden.

Beweis: Wir wenden den Elementarteilersatz auf den $k[X]$-Modul V an, dabei zerlegen wir die Elementarteiler q_i mittels chinesischem Restsatz weiter in Potenzen von irreduziblen Faktoren:

$$V \cong k[X]/(f_1) \times \cdots \times k[X]/(f_n) \ .$$

Die Matrix A_i gehört zu $k[X]/(f_i)$. Wir bestimmen also die Matrix der Multiplikation mit X auf einem $k[X]/(f)$. Sei $f = a_0 + \cdots + a_{m-1}X^{m-1} + X^m$. Wir

wählen als Basis die Nebenklassen von $1, X, \ldots, X^{m-1}$. Die lineare Abbildung ist Multiplikation mit X. Also

$$\theta(1) = 1 \cdot X, \theta(X) = 1 \cdot X^2, \ldots, \theta(X^{m-2}) = 1 \cdot X^{m-1},$$
$$\theta(X^{m-1}) = X^m = -(a_0 + \cdots + a_{m-1}X^{m-1}) \ .$$

Dies ergibt genau eine Matrix vom angegebenen Typ. Das charakteristische Polynom berechnet man durch Entwicklung nach der ersten Zeile. □

Korollar 2.18 (Jordansche Normalform). *Sei V ein $\mathbb{C}$-Vektoraum, $\theta : V \to V$ eine lineare Abbildung. Dann gibt es eine Basis von V, so dass die Matrix von θ die Gestalt*

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \cdots & \\ 0 & & & A_n \end{pmatrix}$$

mit A_i von der Form

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

Beweis: Wieder haben wir eine Zerlegung in $\mathbb{C}[X]/(f_i)$'s, wobei die f_i Potenzen von irreduziblen Polynomen sind, d.h. $f_i = (X-a)^m$. Diesmal wählen wir als Basis $1, (X-a), \ldots, (X-a)^{n-1}$. Diese Elemente sind tatsächlich linear unabhängig, da sie verschiedene Grade kleiner n haben. In dieser Basis gilt

$$\begin{aligned} \theta(1) &= X = (X-a) + a \\ \theta(X-a) &= X(X-a) = [(X-a)+a](X-a) = (X-a)^2 + a(X-a) \\ \theta((X-a)^2) &= X(X-a)^2 = [(X-a)+a](X-a)^2 = (X-a)^3 + a(X-a)^2 \\ &\cdots \\ \theta((X-a)^{m-1}) &= (X-a)^m X + a(X-a)^{m-1}X = a(X-a)^{m-1}X \mod f_i \end{aligned}$$

Die Matrix hat dann die angegebene Gestalt. □

Bemerkung. Natürlich funktioniert das über jedem algebraisch abgeschlossenen Körper. Die Eindeutigkeitsaussgen im Elementarteilersatz übersetzen sich ebenfalls in Eindeutigkeitsaussagen in der Jordanschen Normalform.
Dieser Beweis ist eleganter, als der in linearen Algebra geführte - allerdings ist es nicht so offensichtlich, wie man daraus eine Konstruktionsvorschrift gewinnt.

Kapitel 3

Noethersche Ringe

Definition 3.1. *Sei A ein Ring, M ein A-Modul. M heißt* noethersch*, wenn jede Kette*

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

von Untermoduln von M stabil wird, d.h. $M_i = M_{i+1}$ ab einem Index i_0. Der Ring A heißt noethersch*, wenn er noethersch ist als A-Modul, d.h. jede Kette*

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

von Idealen wird stabil.

Beispiel. (i) Sei M eine endlich abelsche Gruppe. Dann ist M noethersch als $\mathbb{Z}$-Modul.

(ii) Ein Vektorraum ist noethersch genau dann, wenn er endlich-dimensional ist.

(iii) Sei $A = k[X_1, X_2, X_3, \dots]$ der Polynomring in unendlich vielen Variablen. Dann wird die Kette von Idealen

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots$$

nicht stationär. Dieser Ring ist nicht noethersch.

Lemma 3.2. *Sei M ein A-Modul. M ist genau dann noethersch, wenn alle Untermoduln von M endlich erzeugt sind.*

Beweis: Sei $N \subset M$ ein Untermodul. Angenommen, N ist nicht endlich erzeugt. Wir konstruieren eine Kette

$$N_1 \subset N_2 \subset N_3 \subset \dots$$

von Untermoduln von N: Sei $x_1 \in N \setminus \{0\}$ und $N_1 =< x_1 >$ der von x_1 erzeugte Untermodul. Sei $x_2 \in N \setminus N_1$. Da N nicht endlich erzeugt ist, gibt es dieses x_2. Sei nun $N_2 =< x_1, x_2 >$. Iterativ wählen wir $x_i \in N \setminus N_{i-1}$ und setzen

$N_i =< x_1, \ldots, x_i >$. Diese Kette von Untermoduln von M wird nicht stabil, also ist M nicht noethersch.
Seien umgekehrt alle Untermoduln von M endlich erzeugt,

$$M_1 \subset M_2 \subset M_3 \subset \ldots$$

eine Kette von Untermoduln. Sei $N = \bigcup_{i \geq 1} M_i$. Nach Voraussetzung ist dieser Modul endlich erzeugt, $N =< x_1, \ldots, x_n >$. Dann gibt es i_j mit $x_j \in M_{i_j}$. Sei k das Maximum der endlich vielen i_j. Dann gilt $x_j \in M_k$ für alle j, d.h. $N \subset M_k$. Für $i \geq k$ ist dann $N \subset M_k \subset N$, die Kette ist stationär. □

Beispiel. Ein Ring ist also noethersch, wenn alle Ideale endlich erzeugt sind. Dies gilt insbesondere für Hauptidealringe und erst recht für Körper.

Korollar 3.3. *Sei M ein noetherscher Modul, N ein Untermodul. Dann sind auch N und M/N noethersch.*

Beweis: Jeder Untermodul von N ist ein Untermodul von M, also ebenfalls endlich erzeugt. Jeder Untermodul T von M/N hat ein endlich erzeugtes Urbild in M. Die Nebenklassen der Erzeuger erzeugen dann T. □

Korollar 3.4. *Sei A ein noetherscher Ring, $I \subset A$ ein echtes Ideal. Dann ist A/I noethersch.*

Beweis: Nach dem vorherigen Korollar ist A/I noethersch als A-Modul. Damit sind alle Ideale von A/I endlich erzeugt als A-Moduln, also auch endlich erzeugt als A/I-Moduln. □

Bemerkung. Unterringe von noetherschen Ringen sind im allgemeinen nicht noethersch! Jeder Integritätsbereich ist in seinem Quotientenkörper enthalten, der natürlich ein noetherscher Ring ist.

Satz 3.5. *Sei A ein noetherscher Ring, S eine multiplikative Teilmenge. Dann ist $S^{-1}A$ noethersch.*

Beweis: Sei $I \subset S^{-1}A$ ein Ideal, J das Urbild von I unter der kanonischen Abbildung $\phi : A \to S^{-1}A$. Nach Voraussetzung ist J endlich erzeugt. Seien $x_1, \ldots, x_n$ diese Erzeuger und $y_i = \phi(x_i)$ ihre Bilder in I. Sei $\frac{a}{s} \in I$. Dann gilt $\frac{sa}{1} \in I \cap \phi(A)$. Sei b ein Urbild dieses Elementes in J. Dann gilt

$$\begin{aligned} b = a_1 x_1 + \ldots a_n x_n \qquad & \text{für } a_i \in A \\ \Rightarrow \frac{sa}{1} = a_1 y_1 + \ldots a_n y_n \Rightarrow \frac{a}{s} &= \frac{a_1}{s} y_1 + \cdots + \frac{a_n}{s} y_n \end{aligned}$$

Damit ist I endlich erzeugter $S^{-1}A$-Modul. □

Satz 3.6. *Sei*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

eine kurze exakte Sequenz von A-Moduln. M_2 ist noethersch genau dann, wenn M_1 und M_2 noethersch sind.

Beweis: Den Schluss von M_2 auf M_1 und M_3 haben wir bereits gezeigt. Seien nun M_1 und M_3 noethersch. Sei

$$N_1 \subset N_2 \subset N_3 \subset \dots$$

eine Kette von Untermoduln von M_2. Dann wird die Kette

$$N_1 \cap M_1 \subset N_2 \cap M_2 \subset N_3 \cap M \subset \dots$$

von Untermoduln von M_1 stabil. Genauso wird die Kette

$$N_1/N_1 \cap M_1 \subset N_2/N_2 \cap M_1 \subset N_3/N_3 \cap M \subset \dots$$

von Untermoduln von $M_2/M_1 \cong M_3$ stabil.

Behauptung. *Sei $N \subset N'$ mit $N \cap M_1 = N' \cap M_1$ in M_1 und $N/N \cap M_1 = N'/N' \cap M_1$ in M_2. Dann ist $N = N'$.*

Sei $x' \in N'$. Modulo $N' \cap M_1$ liegt es in N, d.h. es gibt $x \in N$ mit $x' - x \in N' \cap M_1 = N \cap M_1 \subset N$. Damit gilt $x' \in N$.
Diesen Schluss können wir nun auf unsere Kette anwenden, sie ist stabil. □

Korollar 3.7. *Wenn M noetherscher A-Modul ist, dann ist M endlich erzeugt als Modul. Ist A noethersch und M endlich erzeugt, so ist M noethersch.*

Beweis: Die erste Aussage ist ein Spezialfall von Lemma 3.2. Ist A noethersch, so sind nach Satz 3.6 auch A^2, A^3 etc. frei. Ist M endlich erzeugt, so ist M als Quotient eines A^n wieder noethersch. □

Theorem 3.8 (Hilberts Basissatz). *Sei A noetherscher Ring. Dann ist $A[X]$ noethersch.*

Korollar 3.9. *Sei A endlich erzeugter Ring über $\mathbb{Z}$ oder einem Körper. Dann ist A noethersch.*

Beweis: $\mathbb{Z}$ und Körper k sind noethersch als Hauptidealringe. Nach dem Theorem sind dann auch $\mathbb{Z}[X_1, \dots, X_n]$ und $k[X_1, \dots, X_n]$ noethersch. Endlich erzeugte Ringe sind Quotienten dieser Polynomringe. □

Beispiel. $\mathbb{Z}[\sqrt{-5}]$ ist noethersch. Er wird von $\sqrt{-5}$ erzeugt.

Korollar 3.10. *Sei k algebraisch abgeschlossener Körper, $V \subset \mathbb{A}_k^n$ eine affine Varietät. Dann wird V durch endlich viele Gleichungen in $k[X_1, \dots, X_n]$ definiert.*

Beweis: Nach Definition ist $V = V(S)$ für eine Teilmenge $S \subset k[X_1, \dots, X_n]$. Es gilt $V = V(I)$, wobei $I = I(S)$ das von S erzeugte Ideal ist. Da $k[X_1, \dots, X_n]$ noethersch ist, gibt es endliche viele Erzeuger $f_1, \dots, f_m$ von $I(S)$. Es gilt dann $V(I) = V(f_1, \dots, f_m)$. □

Beweis des Theorems: Sei $I \subset A[X]$ ein Ideal. Für $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ mit $a_n \neq 0$ heißt a_n führender Koeffizient. Sei

$$\mathfrak{a} = \{a \in A \mid a \text{ führender Koeffizient eines } P \in I \} \cup \{0\} .$$

Dies ist ein Ideal. Da A noethersch ist, ist $\mathfrak{a} = (a_1, \ldots, a_k)$. Sei a_i führender Koeffizient von $P_i \in I$. Wir betrachten

$$I' = (P_1, \ldots, P_k) \subset I \subset A[X] .$$

Sei $n_i = \deg P_i$ und n das Maximum dieser Grade. Bezüglich dieser P_i können wir eine Variante des Euklidischen Algorithmus verwenden. Sei $P \in I$ beliebig mit $m = \deg P$, a der führende Koeffizient von P. Wegen $a \in \mathfrak{a}$ gibt es $u_i \in A$ mit $a = \sum u_i a_i$. Wir betrachten

$$P - \sum u_i P_i X^{m-n_i} \in I .$$

Der Grad dieses Polynoms ist echt kleiner als m. Dieses Verfahren kann iteriert werden, solange $m \geq n_i$. Wir erhalten damit

$$P = P' + R \text{ mit } \ P' \in I', \deg R < n .$$

Wir haben gezeigt

$$I \subset (1, X, \ldots, X^{n-1}) + I' ,$$

d.h. I ist in einem endlich erzeugten $A[X]$-Modul enthalten. Das genügt nicht! Genauer: Sei $I'' = \{P \in I \mid \deg P < m\}$. Dies kein $A[X]$-Ideal, wohl aber ein A-Modul. Er ist enthalten in dem A-Modul, der von $1, X, \ldots, X^{n-1}$ erzeugt wird. Da A noethersch ist, ist auch I'' endlich erzeugt als A-Modul. Es gilt

$$I = I''A[X] + I'$$

und sowohl $I''A[X]$ und I' sind endlich erzeugte $A[X]$-Moduln. □

Der folgende Satz ist eine sehr mächtige Anwendung von Argumenten mit noetherschen Ringen.

Satz 3.11. *Sei k ein Körper, $E = k[X_1, \ldots, X_n]/I$ ebenfalls. Dann ist E eine endliche algebraische Erweiterung von k.*

Beweis: Seien $x_1, \ldots, x_n$ die Bilder der X_i. Seien, nach Umnummerieren, $x_1, \ldots, x_r$ algebraisch unabhängig und $x_{r+1}, \ldots, x_n$ algebraisch abhängig von $x_1, \ldots, x_r$. Sei

$$F = k(x_1, \ldots, x_r) .$$

Dann ist E/F eine endlich erzeugte algebraische Erweiterung, also endlich dimensional als F-Vektorraum.

Behauptung. *F ist endlich erzeugter Ring über k, d.h. von der Form $k[T_1, \ldots, T_k]/J$.*

Sei $y_1, \ldots, y_m$ eine Basis von E/F. Für $i, j = 1, \ldots, n$ erhalten wir Gleichungen

$$x_i = \sum_i f_{ij} y_j \ , y_i y_j = \sum_k f_{ijk} y_k$$

mit Koeffizienten in F. Sei F_0 der von k und den f_{ij} und f_{ijk} erzeugte Ring. Da er endlich erzeugt ist, ist er noethersch. Wir betrachten nun E als F_0-Modul. Er wird von $y_1, \ldots, y_m$ erzeugt, denn unsere Gleichungen erlauben es, jedes Polynom in den x_i als Linearkombination der y_j mit Koeffizienten in F_0 zu schreiben. Damit ist E noetherscher F_0-Modul.
Weiter gilt $F \subset E$ als F_0-Moduln. Als Untermodul eines noetherschen Moduls ist F noethersch, also endlich erzeugter F_0-Modul. Insgesamt ist F endlich erzeugte Ringerweiterung von k, wie behauptet.
Um unseren Satz zu beweisen, können wir nun E durch F ersetzen.

Behauptung. *Es ist $F = k(x_1, \ldots, x_r)$ mit algebraisch unabhängigen Elementen x_i und gleichzeitig $F = k[T_1, \ldots, T_k]/J$. Dann ist $r = 0$.*

Wir betrachten zunächst den Fall $r = 1$, d.h. $F = k(X)$. Seien $T_i = F_i/G_i$ für $i = 1, \ldots, k$ mit $F_i, G_i \in k[X]$. Polynome in den T_i haben als Nenner nur Produkte der Primfaktoren der G_i. Das Inverse von $G_1 G_2 \cdots G_i + 1$ kann nicht in dieser Form geschrieben werden. Dies ist ein Widerspruch.
Für $r > 1$ argumentieren wir mit Induktion: Wir ersetzen k durch $k(x_1, \ldots, x_{r-1})$. Der Spezialfall zeigt dann $k(x_1, \ldots, x_r) = k(x_1, \ldots, x_{r-1})$. □

Geometrische Interpretation

Damit haben wir eine Version des Hilbertschen Nullstellensatz bewiesen.

Theorem 3.12. *Sei k ein algebraisch abgeschlossener Körper. Dann sind alle maximalen Ideale von $k[X_1, \ldots, X_n]$ von der Form*

$$\mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n)$$

für $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_k$.

Beweis: Ideal der angegebenen Form sind tatsächlich maximal, denn der Einsetzungshomorphismus

$$\Phi_a : k[X_1, \ldots, X_n] \to k \qquad X_i \mapsto a_i$$

induziert einen Isomorphismus $k[X_1, \ldots, X_n]/\mathfrak{m}_a \to k$.
Sei nun $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ ein maximales Ideal. Auf den Körper $E = k[X_1, \ldots, X_n]/\mathfrak{m}$ wenden wir den vorherigen Satz an. Er ist eine algebraische Erweiterung von k. Da k algebraisch abgeschlossen ist, folgt $E = k$. Sei α_i das Bild von X_i in $k[X_1, \ldots, X_n]/\mathfrak{m} = k$. Dann liegen die $X_i - \alpha_i$ im Kern der Projektionsabbildung, also in $\mathfrak{m}$. Es gilt $(X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_n - \alpha_n) \subset \mathfrak{m}$. Da beide Ideale maximal sind, stimmen sie überein. □

Wir haben also eine Bijektion zwischen maximalen Idealen des Polynomrings und Punkten des affinen Raums. Der Name Nullstellensatz wird in der folgenden Version klarer.

Korollar 3.13. *Sei k ein algebraisch abgeschlossener Körper, I ein Ideal von $k[X_1, \ldots, X_n]$. Dann ist entweder $I = (1)$ oder $V(I) \neq \emptyset$.*

Beweis: Falls $I \neq (1)$, dann ist I in einem echten Ideal $\mathfrak{m}$ enthalten. Nach dem Theorem ist $\mathfrak{m} = \mathfrak{m}_a$ für ein $a \in \mathbb{A}_k^n$. Dies ist der gesuchte Punkt. □

Korollar 3.14. *Sei $V(S) \subset \mathbb{A}^n$ eine algebraische Varität definiert durch S. Dann gilt*

$$I(V(S)) = \sqrt{I(S)}$$

Hierbei bezeichnet

$$\sqrt{I} = \{f \in k[X_1, \ldots, X_n] \mid \text{ es gibt } n \in \mathbb{N} \text{ mit } f^n \in I\}$$

das Radikal *von I.*

Beweis: Sei $I = I(S)$.

Behauptung. $\sqrt{I} \subset I(V(S))$.

Sei $f \in \sqrt{I}$, d.h. es gibt $n \in \mathbb{N}$ mit $f^n \in I$. Dann gilt $f(a) = 0$ für alle $a \in V(S)$, also auch $f^n(a) = 0$ für alle $a \in V(S)$.

Behauptung. $\sqrt{I} \supset I(V(S))$

Sei $f \in I(V(S))$. Ohne Einschränkung gilt $f \neq 0$. Wir betrachten den Ring $k[X_1, \ldots, X_n, Y]$ und hierin das Ideal J, dass von I und $1 - Yf$ erzeugt wird. Dann gilt

$$V(J) = \{(a_1, \ldots, a_n, b) \mid (a_1, \ldots, a_n) \in V(I), 1 - bf(a_1, \ldots, a_n)\}$$

Nach Voraussetzung ist aber $f(a_1, \ldots, a_n) = 0$ auf $V(I)$, also gilt $V(J) = \emptyset$. Nach Korollar 3.13 ist dann $J = (1)$, d.h. es gibt Polynome $g_i \in k[X_1, \ldots, X_n, Y]$ für $i = 0, \ldots, m$ und Polynome $h_i \in I$ für $i = 1, \ldots, m$, so dass

$$1 = g_0(1 - fY) + g_1 h_1 + \cdots + g_m h_m$$

Wir setzen f^{-1} für Y ein und multiplizieren dann mit einer geeigenten Potenz von f, um eine Gleichung in $k[X_1, \ldots, X_n]$ zu erhalten. Dies ist der gesuchte Ausdruck. □

Wir betrachten nun die Abbildungen

$$I(\cdot) : \{\text{Teilmengen von } \mathbb{A}_k^n\} \to \{\text{Ideale von } k[X_1, \ldots, X_n]\}$$
$$V(\cdot) : \{\text{Teilmengen von } k[X_1, \ldots, X_n]\} \to \{\text{affine Untervarietäten von } \mathbb{A}_k^n\}$$

Beide sind inklusionsumkehrend. Wir fassen zusammen, was wir über diese Abbildungen wissen:

Satz 3.15. *Sei $M \subset \mathbb{A}_k^n$, $S \subset k[X_1, \ldots, X_n]$ Dann gilt*

$$V(I(M)) = \overline{M} \qquad I(V(S)) = \sqrt{I(S)}$$

($\overline{M}$ Abschluss bezüglich der Zariski-Topologie). Die Abbildungen $I(\cdot)$ und $V(\cdot)$ sind inverse Bijektionen zwischen der Menge der affinen Varietäten in $\mathbb{A}_k^n$ und den Idealen I mit $I = \sqrt{I}$.

Beweis: (i) Die zweite Aussage ist genau Korollar 3.14.

(ii) Sei $V = V(I)$ eine Varietät. Dann gilt $V(I(V)) = V(\sqrt{I}) = V(I)$, da eine gemeinsame Nullstelle der Elemente von J auch Nullstelle aller Elemente von $\sqrt{J}$ ist.

(iii) Sei $J = \sqrt{J}$ ein Ideal. Dann folgt $I(V(J)) = \sqrt{J} = J$.

(iv) Wegen $M \subset \overline{M}$ gilt $I(M) \supset I(\overline{M})$. Offensichtlich ist $V(I(M))$ eine affine Varietät, die M enthält. Nach Definition ist also $\overline{M} \subset V(I(M))$. Dann folgt

$$I(\overline{M}) \supset I(V(I(M))) = \sqrt{I(M)} = I(M)$$

Zusammen also

$$I(M) = I(\overline{M}) \Rightarrow V(I(M)) = V(I(\overline{M})) = \overline{M}$$

□

Die Koordinatenringe von affinen Varietäten sind genau die reduzierten endlich erzeugten k-Algebren, d.h. solche mit $x^n = 0 \Rightarrow x = 0$ für alle Elemente x. Sie können jedoch Nullteiler haben!

Kapitel 4

Primideale

In diesem Kapitel ist A wieder ein beliebiger Ring (kommutativ mit Eins).

Definition 4.1. *Ein Ideal $\mathfrak{p} \subset A$ heißt* Primideal*, falls $\mathfrak{p} \neq A$ und aus $ab \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Die Menge der Primideale von A heißt Spektrum* $\operatorname{Spec} A$.

Beispiel. $A = \mathbb{Z}$, $\mathfrak{p} = (p)$. Die Bedingung bedeutet also $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$, d.h. p ist eine Primzahl – oder $p = 0$. Die Primideale von $\mathbb{C}[X]$ sind von den Polynomen $(X - a)$ für $a \in \mathbb{C}$ erzeugt, außerdem gibt es noch $\mathfrak{p} = 0$.

Lemma 4.2. *$\mathfrak{p} \subset A$ ist ein Primideal genau dann, wenn $A/\mathfrak{p}$ ein Integritätsring ist. Alle maximalen Ideale sind prim.*

Beweis: $ab \in \mathfrak{p}$ ist äquivalent zu $ab = 0$ in $A/\mathfrak{p}$. Wenn $A/\mathfrak{p}$ nullteilerfrei ist, dann gilt $a = 0$ oder $b = 0$ in $A/\mathfrak{p}$, d.h. $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Die Umkehrung gilt ebenfalls. Ist $\mathfrak{m}$ maximales Ideal, so ist $A/\mathfrak{m}$ ein Körper, also ein Integritätsbereich. □

Beispiel. In $k[X, Y]$ sind (X) und (X, Y) Primideale, denn die Quotienten sind isomorph zu $k[Y]$ bzw. k.

Lemma 4.3. *Sei $f : A \to B$ ein Ringhomomorphismus, $\mathfrak{p} \subset B$ ein Primideal. Dann ist $f^{-1}\mathfrak{p}$ ein Primideal. f^{-1} definiert eine Abbildung*

$$f^* : \operatorname{Spec} B \to \operatorname{Spec} A$$

Beweis: Die Abbildung $A \to B/\mathfrak{p}$ hat den Kern $f^{-1}\mathfrak{p}$, also ist $A/f^{-1}\mathfrak{p} \to B/pf$ wohldefiniert und injektiv. Die Nullteilerfreiheit von $B/\mathfrak{p}$ impliziert, dass auch $A/f^{-1}\mathfrak{p}$ nullteilerfrei ist, also $f^{-1}\mathfrak{p}$ ein Primideal. □

Bemerkung. Ist umgekehrt $\mathfrak{q} \subset A$ ein Primideal, so betrachtet man das Ideal $B\mathfrak{q} \subset B$. Dies ist im allgemeinen kein Primideal.

Beispiel. $\mathbb{Z} \to \mathbb{Z}[i]$, $\mathfrak{q} = (2)$. Dann ist $\mathbb{Z}[i]\mathfrak{q} = (2)$. Es gilt $2 = (1 + i)(1 - i)$, aber $(1 + i) \notin (2)$. Also ist dies kein Primideal. Tatsächlich gilt $(1 + i) = (1 - i)$ und $(2) = (1 + i)^2 \subset \mathbb{Z}[i]$.

Bemerkung. In manchen Ringen gilt statt einer eindeutigen Zerlegung von Elementen in Primfaktoren wenigstens eine eindeutige Zerlegung von Idealen in Produkte von Primidealen. Wichtigstes Beispiel sind die Ganzheitsringe von Zahlkörpern aus Definition 0.7. In diesem Zusammenhang, nämlich als "ideale Elemente" wurden Ideale ursprünglich eingeführt.

Beispiel. In $\mathbb{Z}[\sqrt{-5}]$ sind

$$\mathfrak{p}_1 = (2, 1+\sqrt{-5}), \mathfrak{p}_2 = (2, 1-\sqrt{-5}), \mathfrak{p}_3 = (3, 1+\sqrt{)}\mathfrak{p}_4 = (3, 1-\sqrt{-5})$$

Primideale, denn z.B.

$$\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}[X]/(X^2+5, 2, X+1) \cong \mathbb{F}_2[X]/(X^2+5, X+1) \cong \mathbb{F}_2$$

ist nullteilerfrei. Es gilt

$$\mathfrak{p}_1\mathfrak{p}_2 = (4, 2 \pm 2\sqrt{-5}, 6) = (2) \ .$$

Geometrische Interpretation

Definition 4.4. *Sei X ein topologischer Raum. X heißt* irreduzibel*, wenn aus $X = A_1 \cup A_2$ für abgeschlossene Teilmengen $A_1, A_2 \subset X$ folgt, dass $X = A_1$ oder A_2. Anderfalls heißt X reduzibel.*

Für metrische Räume ist der Begriff uninteressant: nur einpunktige metrische Räume sind irreduzibel. Anders für Varietäten:

Beispiel. Sei $V = V(XY) \subset \mathbb{A}^2$. Dann gilt $V = V(X) \cup V(Y)$, ist also reduzibel. $V(X)$ ist irreduzibel, da echte Untervarietäten endlich sind.

Satz 4.5. *Sei k ein algebraische abgeschlossener Körper, $V \subset \mathbb{A}^n_k$ eine affine Varietät. Dann sind äquivalent:*

(i) V irreduzibel.

(ii) $I(V)$ ist ein Primideal.

(iii) $k[V]$ ist ein Integritätsbereich.

(iv) Jede offene nichtleere Teilmenge ist dicht in V.

Beweis: Es gilt $k[V] = k[X_1, \ldots, X_n]/I(V)$. Die Äquivalenz von (ii) und (iii) ist also nur Lemma 4.2.
Sei V irreduzibel, $fg = 0$ in $k[V]$. Dann gilt

$$V = V(f) \cup V(g)$$

denn in jedem Punkt von V verschwindet ein Faktor. Es folgt (ohne Einschränkung) $V = V(f)$, d.h. f verschwindet in jedem Punkt von V, also $f = 0$ in $k[V]$.

Sei V reduzibel, $V = A_1 \cup A_2$ zwei echte abgeschlossene Teilmengen. Dann ist nach Hilbertschem Nullstellensatz $I(A_i) \supsetneq I(V)$. Sei $f_i \in I(A_i) \setminus I(V)$. Dann gilt $f_1 f_2 \in I(V)$, denn in jedem Punkt von V verschwindet einer der beiden Faktoren. Damit ist $I(V)$ kein Primideal.
Wir zeigen nun (i)$\Leftrightarrow$ (iv). Sei $U \subset V$ offen, nichtleer. Dann ist

$$V = \overline{U} \cup (V \setminus U)$$

Vereinigung von abgeschlossenen Teilmengen. Ist V irreduzibel, so gilt $V = \overline{U}$ oder $V = V \setminus U$. Im letzteren Fall ist $U = \emptyset$, d.h. für nichtleere offene Teilmengen gilt $V = \overline{U}$. Ist V reduzibel, so gibt eine echte Zerlegung $V = V_1 \cup V_2$ in abgeschlossene Teilmengen. Sei $U = V \setminus V_2$. Diese Menge ist dann nicht dicht. $\square$

Beispiel. $\mathbb{A}^n$ ist irreduzibel.

Zusammen mit Satz 3.15 erhalten wir also eine Bijektion zwischen $\operatorname{Spec} k[V]$ und der Menge der irreduziblen Untervarietäten von V.

Definition 4.6. *Sei V eine irreduzible affine Varietät. Dann heißt der Quotientenkörper*

$$k(V) = Q(k[V])$$

des Rings der regulären Funktionen Funktionenkörper von V.

Bemerkung. In vielen, vor allem älteren Büchern gehört Irreduzibilität zur Definition von Varietät. Reduzible Varietäten heißen dann *algebraische Mengen*.

Satz 4.7. *Sei $V \subset \mathbb{A}_k^n$ eine affine Varietät.*

(i) Es gilt

$$V = V_1 \cup \cdots \cup V_r$$

für irreduziblen Teilmengen V_i.

(ii) Gibt es keine Enthaltenseinsrelationen zwischen den V_i, d.h. ist kein V_i überflüssig, so sind diese eindeutig bestimmt und heißen irreduzible Komponenten von V.

(iii) Sind $W, V_1 \ldots, V_r \subset V$ abgeschlossene irreduzible Teilmengen mit $W \subset V_1 \cup \ldots V_r$. Dann folgt $V_0 \subset V_i$ für ein $i \in \{1, \ldots, r\}$.

Beweis: Wir zeigen zunächst die Existenz. Wir betrachten die Menge Σ der abgeschlossenen Teilmengen von V, die nicht in dieser Form dargestellt werden können. Angenommen Σ ist nicht leer. Ihm entspricht einer gewissen Menge von Primidealen von $k[X_1, \ldots, X_n]$. Da der Ring noethersch ist, hat diese Menge ein maximales Element. Sei V_0 das zugehörige minimale Elemente von Σ. Die Menge V_0 ist nicht selbst irreduzibel, sonst hätten wir bereits eine Darstellung gefunden. Es gibt also A_1, A_2 echte abgeschlossene Teilmengen von V_0 mit

$$V_0 = A_1 \cup A_2$$

Nach Wahl von V_0 lassen sich dann A_1, A_2 in der Form

$$A_i = V_1^i \cup \cdots \cup V_{r_i}^i$$

schreiben. Dann folgt

$$V_0 = V_1^1 \cup \cdots \cup V_{r_1}^1 \cup V_1^2 \cup \cdots \cup V_{r_2}^2$$

Dies ist ein Widerspruch zur Behauptung, also ist Σ leer. Insbesonder auch $V \neq \Sigma$.
Nun zeigen (iii). Es gilt

$$W = (W \cap V_1) \cup \ldots (W \cap V_r)$$

Da W irreduzibel ist, gilt $W = (W \cap V_i)$ für einen Faktor, d.h. $W \subset V_i$.
Hieraus folgt leicht die Eindeutigkeit: Seien

$$V = V_1 \cup \cdots \cup V_r = W_1 \cup \ldots W_s$$

zwei Zerlegungen in irreduzible Untervarietäten ohne überflüssige Faktoren. Nach (iii) gilt $V_1 \subset W_i$ für ein i. Ebenfalls nach (iii) gilt $W_i \subset V_j$ für ein j. Da es keine Enthaltenseinsrelationen zwischen den V_1 gibt, folgt $i = j$ und $V_1 = W_i$. Ebenso argumentiert man für alle V_i und W_j. □

Definition 4.8. *(i) Sei A ein Ring. Die* Krulldimension *von A (oder* Spec *A) ist die maximale Länge n einer Kette von verschiedenen Primidealen von A:*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \ .$$

(ii) Sei k algebraisch abgeschlossener Körper, V eine affine Varietät. Die Dimension *von V ist die maximale Länge einer Kette von (nichtleeren) irreduziblen abgeschlossenen Teilmengen von V:*

$$V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n$$

Korollar 4.9. *Die Dimension von V stimmt mit der Dimension von $k[V]$ überein.*

Beweis: Satz 3.15 und Satz 4.5 □

Beispiel. Körper haben die Krulldimension 0. Hauptidealringe wie $\mathbb{Z}$ oder $k[X]$ haben die Krulldimension 1. Die maximalen Ketten haben die Form $0 \subset (p)$ für ein Primelement p. In $k[X,Y]$ gibt es die Kette $0 \subset (X) \subset (X,Y)$, also ist die Dimension wenigstens 2.

Beispiel. In $\mathbb{A}^n$ gibt es die Kette

$$\mathbb{A}^n \supset V(X_1) \supset V(X_1, X_2) \supset \cdots \supset V(X_1, \ldots, X_n)$$

Es gilt $\dim \mathbb{A}^n \geq n$. Tatsächlich gilt Gleichheit! Für den Beweis holen wir weit aus.

Lokale Ringe

Definition 4.10. *Ein Ring heißt* lokal, *wenn er nur ein eindeutiges maximales Ideal hat.*

Beispiel. diskrete Bewertungsringe, Körper.

Satz 4.11. *Sei A ein Ring, $\mathfrak{p}$ ein Primideal, $S = A \setminus \mathfrak{p}$. Dann ist $A_\mathfrak{p} := S^{-1}A$ ein lokaler Ring. Er heißt* Lokalisierung *von A an $\mathfrak{p}$.*

Beweis: Sei $s, t \in A \setminus \mathfrak{p}$. Nach Definition eines Primideals ist dann auch $st \in A \setminus \mathfrak{p}$. Da $\mathfrak{p} \neq A$, gilt $1 \in S$. Andererseits ist $0 \notin S$. Die Menge ist multiplikativ, also ist $A_\mathfrak{p}$ definiert.
Wir bestimmen die Einheiten von $A_\mathfrak{p}$. Es sind Brüche a/s für die es a'/s' $(s, s' \in S)$ mit

$$1 = \frac{a}{s}\frac{a'}{s'} \Leftrightarrow \text{es gibt } t \in S \text{ mit} t(aa' - s's) = 0 \ .$$

Wegen $aa't = ss't \in S$ folgt dann $a, a' \notin S$. Ein Bruch ist also invertierbar, falls Zähler und Nenner in S liegen. Wir betrachten

$$\mathfrak{m} = A_\mathfrak{p} \setminus \mathbb{A}_\mathfrak{p}^* = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\}$$

Dies ist ein Ideal, nämlich $S^{-1}\mathfrak{p}$. Jedes andere echte Ideal ist in $\mathfrak{m}$ enthalten. □

Definition 4.12. *Eine Eigenschaft P eines Moduls heißt* lokal, *wenn:*
M hat $P \Leftrightarrow M_\mathfrak{p}$ hat P für alle Primideale.

Lemma 4.13. *Sei M ein A-Modul. Dann sind äuqivalent:*

(i) $M = 0$.

(ii) $M_\mathfrak{p}$ *für alle* $\mathfrak{p} \in \operatorname{Spec} A$.

(iii) $M_\mathfrak{m}$ *für alle* $\mathfrak{m} \in |\operatorname{Spec} A|$.

Beweis: Die Implikationen von (i) nach (ii) nach (iii) sind klar. Sei nun $M \neq 0$ und es gelte (iii). Sei $x \in M \setminus \{0\}$. Sei $I = \{a \in A \mid ax = 0\}$. Dies ist ein Ideal ungleich A. Jedes Ideal ist in einem maximalen Ideal enthalten. Sei also $I \subset \mathfrak{m}$. Nach Voraussetzung ist $\frac{x}{1} \in M_\mathfrak{m} = 0$, also gibt es $s \in S = A \setminus \mathfrak{m}$ mit $sx = 0$. Nach Definition gilt dann $s \in I \subset \mathfrak{m}$, Widerspruch. □

Lemma 4.14. *Sei $\phi : M \to N$ ein Modulhomomorphismus. Dann sind äquivalent:*

(i) ϕ *ist injektiv (surjektiv, bijektiv).*

(ii) $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ *ist injektiv (surjektiv, bijektiv) für alle* $\mathfrak{p} \in \operatorname{Spec} A$.

(iii) $\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{p}$ *ist injektiv (surjektiv, bijektiv) für alle* $\mathfrak{m} \in |\operatorname{Spec} A|$.

Beweis: Wir betrachten die exakte Sequenz

$$0 \to \operatorname{Ker}\phi \to M \to N \to \operatorname{Im}\phi \to 0 \ .$$

Diese Sequenz bleibt exakt bei Anwenden von S^{-1} (Übungsaufgabe), also

$$0 \to (\operatorname{Ker}\phi)_{\mathfrak{p}} \to M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to (\operatorname{Im}\phi)_{\mathfrak{p}} \to 0 \ .$$

Mit anderen Worten: $\operatorname{Ker}(\phi_{\mathfrak{p}}) = (\operatorname{Ker}\phi)_{\mathfrak{p}}$. Die Behauptung folgt nun aus dem vorhergehenden Lemma. □

Warum lokal, Lokalisierung?

Satz 4.15. *Sei k algebraisch abgeschlossener Körper, $V \subset \mathbb{A}^n_k$ eine affine Varietät, $a \in V$ ein Punkt, $\mathfrak{m}$ das zugehörige maximale Ideal von $k[V]$. Dann gilt*

$$k[V]_{\mathfrak{m}} = \{(\phi, U_f) \mid f \in k[V] \text{ mit } f(a) \neq 0, \phi \in k[U_f]\}/\sim$$

wobei $U_f = V \setminus V(f)$ nach Satz 1.23 affine offene Teilmenge ist und

$$(\phi, U_f) \sim (\psi, U_g) \Leftrightarrow \phi|_{U_h} = \psi|_{U_h}$$

für ein h mit $h(a) \neq 0$ und $U_h \subset U_f \cap U_g$.

Die Äquivalenzklassen der (ϕ, U_f) heißen *Funktionenkeime in a.*

Beweis: Die Voraussetzung $f(a) \neq 0$ ist äquivalent zu $f \notin \mathfrak{m}$. Nach Satz 1.23 gilt $k[U_f] \cong k[V]_f$. Der Satz hat also die rein algebraische Formulierung

$$k[V]_{\mathfrak{m}} = \{(\phi, f) \mid f \notin \mathfrak{m}, \phi \in k[V]_f\}/\sim$$

Wir machen die Äquivalenzrelation ebenfalls explizit. $U_h \subset U_f$ ist äquivalent zu $V(h) \supset V(f) \Leftrightarrow \sqrt{(h)} \subset \sqrt{(f)} \Leftrightarrow f \mid h^n$ für ein $n \geq 1$. Wegen $U_h = U_{h^n}$ können wir also ohne Einrschränkung annehmen, dass $f \mid h$ und $g \mid h$. Sei $h = fx$. Dann ist Restriktionsabbildung $k[U_f] \to k[U_h]$ gegeben durch $\frac{a}{f^i} \mapsto \frac{ax^i}{h^i}$. Es gilt also $(a/f^i, U_f) \sim (b/g^j, U_g)$, falls es ein $h = fx = gy$ gibt mit $h(a) \neq 0$ und $ax^i/h^i = by^j/h^j$ in $k[V]_h$, also wenn es $n \geq 1$ gibt mit

$$h^n(h^j x^i a - h^i x^j b) = 0$$

Wir haben natürliche Abbildungen $k[V]_f \to k[V]_{\mathfrak{m}}$. Nach der obigen Diskussion hängt das Bild von $\phi_f \in k[V]_f$ in $k[V]_{\mathfrak{m}}$ nur von der Äquivalenzklasse ab.
Jedes Element von $k[V]_{\mathfrak{m}}$ hat die Form a/f für ein $f \notin \mathfrak{m}$, ist also im Bild eines ϕ_f. Ist $a/f = b/g$ in $k[V]_m$, so gibt es $h \notin \mathfrak{m}$ mit $hga = hfb$ in $k[V]$. Die Restriktionen von a/f und b/g nach U_{hfg} stimmen dann überein, also gehören sie zur selben Äquivalenzklasse. □

Wir übertragen dies auf beliebige Ringe.

Spektren

Definition 4.16. *Sei A ein Ring. Eine Teilmenge $V \subset \operatorname{Spec} A$ heißt* abgeschlossen*, falls sie von der Form*

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid I \subset \mathfrak{p}\}$$

für ein Ideal $I \subset A$ ist. $\operatorname{Spec} A \setminus V$ *heißt dann* offen.

Beispiel. Sei $A = \mathbb{Z}$, also $I = (f)$ für ein $f \in \mathbb{Z}$. Dann ist $V(f) = V((f)) = \{(p) \mid p \mid f\}$ die Menge der Primteiler von f, also endlich. Eine offene Teilmenge von $\operatorname{Spec} \mathbb{Z}$ ist also immer Komplement einer endlichen Mengen.

Satz 4.17. $\operatorname{Spec} A$ *ist ein topologischer Raum.*

Beweis: Wir überprüfen die Axime in Termen von abgeschlossen Mengen, also

(i) $\emptyset$ und $\operatorname{Spec} A$ sind abgeschlossen.

(ii) Sind I_1, I_2' Ideale, dann ist $V(I_1) \cup V(I_2)$ abgeschlossen.

(iii) Seien $I_j, j \in J$ eine Menge von Idealen. Dann ist $\bigcup_{j\in J} V(I_j)$ abgeschlossen.

Es gilt $V((0)) = \operatorname{Spec} A$, denn $(0) \subset \mathfrak{p}$ für alle Primideale. Es gilt $V((1)) = \emptyset$, denn $1 \notin \mathfrak{p}$ für alle Primideale.

$$V(I_1) \cup V(I_2) = \{\mathfrak{p} \mid I_1 \subset \mathfrak{p} \text{ oder } I_2 \subset \mathfrak{p}\}$$
$$V(I_1 I_2) = \{\mathfrak{p} \mid I_1 I_2 \subset \mathfrak{p}\}$$

Ist $I_1 \subset \mathfrak{p}$, dann folgt $I_1 I_2 \subset \mathfrak{p}$, also

$$V(I_1) \cup V(I_2) \subset V(I_1 I_2)\ .$$

Angenommen, die Inklusion ist echt, d.h. es gibt $\mathfrak{p}$ mit $\mathfrak{p} \subset I_1 I_2$, aber $\mathfrak{p}$ ist werder in I_1 noch in I_2 enthalten. Dann gibt es Elemente $a_1 \in I_1 \setminus \mathfrak{p}$ und $a_2 \in I_2 \setminus \mathfrak{p}$. Das Produkt $a_1 a_2 \in I_1 I_2 \subset \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, folgt $a_1 \in \mathfrak{p}$ oder $a_2 \in \mathfrak{p}$. Dies ist ein Widerspruch. Schließlich:

$$\bigcap_{j\in J} V(I_j) = \{\mathfrak{p} \mid I_j \subset \mathfrak{p} \text{ für alle } j \in J\} = \left\{\mathfrak{p} \mid \sum_{j\in J} I_j \subset \mathfrak{p}\right\} = V\left(\sum_{j\in J} I_j\right)$$

□

Bemerkung. Ein Punkt von $\operatorname{Spec} A$ heißt *abgeschlossen*, wenn $\{\mathfrak{p}\} \subset \operatorname{Spec} A$ eine abgeschlossene Menge ist, also $V(I) = \{\mathfrak{p}\}$. Dies ist genau dann der Fall, wenn $\mathfrak{p}$ ein maximales Ideal ist. $|\operatorname{Spec} A|$ ist die Menge der abgeschlossenen Punkte von $\operatorname{Spec} A$.

Beispiel. $|\operatorname{Spec}\mathbb{Z}|$ ist die Menge der (positiven) Primzahlen.
$|\operatorname{Spec}\mathbb{C}[X]| = \{(X-\alpha) \mid \alpha \in \mathbb{C}\} \cong \mathbb{C}$.
Ist A lokal, so hat $|\operatorname{Spec} A|$ nur ein Element.

Beispiel. Ist V eine affine Varietät, so ist nach dem Hilbertschen Nullstellensatz $|\operatorname{Spec} k[V]| = V$. Die Zariski-Topologie auf V wird von der Zariski-Topologie auf $\operatorname{Spec} k[V]$ induziert. Umgekehrt entsprechen die Elemente von $\operatorname{Spec} k[V]$ der Menge der irreduziblen Teilmengen von V. V ist dicht in $\operatorname{Spec} k[V]$. (Übungsaufgabe)

Lemma 4.18. *Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist die Abbildung $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ mit $\mathfrak{p} \mapsto f^{-1}\mathfrak{p}$ stetig.*

Beweis: Nach Lemma 4.3 ist die Abbildung wohldefiniert. Wir müssen überprüfen, dass die Urbilder abgeschlossener Mengen abgeschlossen sind. Sei $I \subset A$ ein Ideal.

Behauptung. *$(f^*)^{-1}V(I) \subset \operatorname{Spec} B$ ist abgeschlossen.*

$\mathfrak{p} \in (f^*)^{-1}V(I)$ bedeutet $f^*\mathfrak{p} = f^{-1}\mathfrak{p} \in V(I)$, d.h. $I \subset f^{-1}\mathfrak{p} \Leftrightarrow f(I) \subset \mathfrak{p}$. Dies ist genau dann der Fall, wenn $\mathfrak{p} \in V(J)$, wobei J das von $f(I)$ in B erzeugte Ideal ist. □

Ein Homöomorphismis ist eine stetige, bijektive Abbildung, derem Umkehrabbildung stetig ist.

Satz 4.19. *Sei $I \subset A$ ein Ideal, $\pi : A \to A/I$ die Projektion. Dann induziert $\pi^* : \operatorname{Spec} A/I \to \operatorname{Spec} A$ einen Homöomorphismus zwischen $\operatorname{Spec} A/I$ und $V(I)$.*

Beweis: Sei $\mathfrak{p} \subset A/I$ ein Primideal, $\pi^*\mathfrak{p} = \pi^{-1}\mathfrak{p}$ enthält also $\pi^{-1}(0) = I$. Mit anderen Worten: $\pi^*(\mathfrak{p}) \in V(I)$. Sei umgekehrt $I \subset \mathfrak{q} \subset A$ ein Primideal.

Behauptung. $\pi^{-1}(\pi(\mathfrak{q}) = \mathfrak{q}$.

Sei $a \in \pi^{-1}(\pi(\mathfrak{q})$, d.h. $\pi(a) \in \pi(\mathfrak{q})$. Dies bedeutet $a \in \mathfrak{q} + I$. Wegen $I \subset \mathfrak{q}$ folgt $a \in \mathfrak{q}$. Die umgekehrte Inklusion ist trivial.

Behauptung. *$\pi(\mathfrak{q}) \subset A/I$ ist ein Primideal.*

Als Bild eines Moduls ist $\pi(\mathfrak{q})$ ein Modul, also ein Ideal. Seien $\overline{a}, \overline{b} \in A/I$ mit $\overline{a}\overline{b} \in \pi(\mathfrak{q})$. Seien a, b Urbilder von $\overline{a}$ und $\overline{b}$. Dann gilt $ab \in \mathfrak{q}$ nach der vorherigen Behauptung.j Da $\mathfrak{q}$ ein Primideal ist, folgt $a \in \mathfrak{q}$ oder $b \in \mathfrak{q}$ und damit $\overline{a} \in \pi(\mathfrak{q})$ oder $\overline{b} \in \pi(\mathfrak{q})$. Da $\pi^{-1}\pi\mathfrak{q}$ ein Primideal ist, gilt $1 \notin \pi(\mathfrak{q})$.
Die Abbildungen π und π^* sind also invers zueinander. Die Stetigkeit von $\operatorname{Spec} A/I \to V(I)$ ist ein Spezialfall des letzten Lemmas. Sei $V(J) \subset \operatorname{Spec} A/I$ abgeschlossen, wobei $J \subset A/I$ ein Ideal. Dann ist $\pi^*(V(I)) = V(\pi^{-1}(J))$, also ebenfalls abgeschlossen. □

Satz 4.20. *Sei $S \subset A$ eine multiplikative Teilmenge, $\phi : A \to S^{-1}A$ die natürliche Abbildung. Dann induziert $\phi^* : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ einen Homöomorphismus zwischen $\operatorname{Spec} S^{-1}A$ und $\{\mathfrak{p} \in \operatorname{Spec} A \mid S \cap \mathfrak{p} = \emptyset\}$.*

Korollar 4.21. *Sei speziell $f \in A$ nicht nilpotent, $S = \{1, f, f^2, f^3, \dots\}$, $A_f := S^{-1}A$. Dann induziert ϕ^* eine Bijektion zwischen* $\operatorname{Spec} A_f$ *und der offenen Menge* $U_f = \operatorname{Spec} A \setminus V(f) = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\}$.

Beweis des Satzes. Sei $\mathfrak{q} \subset S^{-1}A$ prim. Dann gilt

$$\phi^*\mathfrak{q} = \phi^{-1}\mathfrak{q} = \{a \in A \mid \frac{a}{1} \in \mathfrak{q}\} \ .$$

Angenommen, es gibt $f \in S \cap \phi^*\mathfrak{q}$, dann ist $\frac{f}{1} \in \mathfrak{q}$ eine Einheit. Dies ist ein Widerspruch zu $\mathfrak{q}$ prim.
Sei nun $\mathfrak{p} \subset A$ ein Primideal mit $S \cap \mathfrak{p} = \emptyset$. Wir betrachten $S^{-1}\mathfrak{p} \to S^{-1}A$.

Behauptung. *Diese Abbildung ist injektiv.*

Sei nämlich $\frac{a}{s}$ im Kern, d.h. es gibt $t \in S$ mit $ta = 0$. Das bedeutet dann auch $\frac{a}{s} = 0$ in $S^{-1}\mathfrak{p}$.

Behauptung. $S^{-1}\mathfrak{p}$ *ist ein Primideal.*

Seien $\frac{a}{s}, \mathfrak{b}t \in S^{-1}$ mit $\frac{c}{u} = \frac{ab}{st}$ für $c \in \mathfrak{p}$ d.h. es gibt $v \in S$ mit $v(cst - abu) = 0$. Dies impliziert, dass $vabu \in \mathfrak{p}$. Dies ist ein Primideal und nach Voraussetzung $v, u \notin \mathfrak{p}$. Dann muss $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ sein. Weiter gilt $S^{-1}A = S^{-1}\mathfrak{p}$ genau dann, wenn $\frac{1}{1} = \mathfrak{a}s$ für ein $a \in \mathfrak{p}$ und $s \in S$. Dies bedeutet, dass es $t \in S$ gibt mit $t(a - s) = 0 \in \mathfrak{p}$. Dies impliziert $ts \in \mathfrak{p}$, ein Widerspruch. Damit ist $S^{-1}\mathfrak{p}$ tatsächlich prim.

Behauptung. *Die Abbildungen ϕ^* und S^{-1} sind invers zueinander.*

Sei $\mathfrak{q} \subset S^{-1}A$. Zu zeigen ist $S^{-1}\phi^{-1}\mathfrak{q} = \mathfrak{q}$. Die Inklusion $\subset$ ist klar. Sei nun $\frac{a}{s} \in \mathfrak{q}$. Dann gilt $\frac{a}{s} = \frac{a}{1}\mathfrak{1}s$. Als Einheit kann $\frac{1}{s}$ nicht in $\mathfrak{q}$ liegen. Da $\mathfrak{q}$ ein Primideal ist, folgt $\frac{a}{1} \in \mathfrak{q}$, also $a \in \phi^{-1}\mathfrak{q}$ und damit $\frac{a}{s} \in S^{-1}\phi^{-1}\mathfrak{q}$.
Sei $\mathfrak{p} \subset A$ prim mit $\mathfrak{p} \cup S = \emptyset$. Zu zeigen ist $\phi^{-1}S^{-1}\mathfrak{p} = \mathfrak{p}$. Zunächst $\supset$. Sei also $a \in \mathfrak{p}$. Dann ist $\frac{a}{1} \in S^{-1}\mathfrak{p}$ und $a \in \phi^{-1}S^{-1}\mathfrak{p}$. Für $\subset$ sei $\frac{a}{1} \in S^{-1}\mathfrak{p}$, d.h. es gibt $b \in \mathfrak{p}$ und $s \in S$ mit $\frac{a}{1} = bs$. Also gibt es $t \in S$ mit $t(as - b) = 0$. Hieraus folgt $tsa \in \mathfrak{p}$. Wegen $\mathfrak{p}$ prim und $s, t \notin \mathfrak{p}$ folgt $a \in \mathfrak{p}$.
Die Bijektivität und Stetigkeit ist damit gezeigt. Sei $V(J) \subset \operatorname{Spec} S^{-1}A$ abgeschlossen. Die gleichen Rechnungen wie oben zeigen, dass dann $\phi^*(V(J)) = \phi^*(\operatorname{Spec} S^{-1}A) \cap V(\phi^{-1}(J))$. Also ist das Bild abgeschlossen in der Relativtopologie. □

Bemerkung. Spektren von Ringen sind die Grundbausteine der algebraischen Geometrie über nicht algebraisch abgeschlossenen Körpern oder beliebigen Ringen, genau wie offene Kugeln in $\mathbb{R}^n$ die Grundbautsteine der Differentialtopologie sind. Ein *Schema* ist ein topologischer Raum mit einer offenen Überdeckung durch $\operatorname{Spec} A_i$'s für Ringe A_i, so dass die Übergangsabbildungen lokal durch Isomorphismen von Ringen induziert werden. Dies erlaubt geoemtrische Argumente und Begriffe in der Algebra zu verwenden.
Damit kehren wir zu unserer Dimensionsfrage zurück.

Theorem 4.22. *Sei k ein Körper. Dann hat $A = k[X_1, \ldots, X_n]$ die Dimension n. Jede Kette von Primidealen kann zu einer Kette der Länge n erweitert werden. Ist*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$$

eine maximale Kette, dann hat $A/\mathfrak{p}_i$ die Dimension $n - i$.

Beweis: Die Aussage über die Dimension von $A/\mathfrak{p}_i$ folgt aus den vorherigen Aussagen. Einerseits induzieren die Primideale $\mathfrak{p}_j$ für $j \geq i$ eine Kette von Primidealen in $A/\mathfrak{p}_i$ der Länge $n - i$. Ist andererseits $0 = \mathfrak{q}_i \subset \mathfrak{q}_{i+} \ldots \mathfrak{q}_m$ eine Kette von Primidealen in $A/\mathfrak{p}_i$, so können ihre Urbilder in A mit $\mathfrak{p}_0, \ldots, \mathfrak{p}_i$ zu einer Kette der Länge m zusammengefasst werden. Da alle maximalen Ketten die gleiche Länge haben, folgt $m = n$. Die Aussage soll nun mit Induktion über die Anzahl der Variablen n gezeigt werden. Die Aussage ist wahr für $n = 0$, da die einzige Kette von Idealen

$$0 \subset k$$

ist. Der Induktionschrit wird in einem Lemma zusammengefasst. □

Lemma 4.23. *Sei A ein n-dimensionaler Ring, in dem jede Kette von Primidealen zu einer Kette der Länge n verfeinert werden kann. Dann hat $A[X]$ die Dimension $n + 1$, und jede Kette von Primidealen kann zu einer Kette dieser Länge verfeinert werden.*

Der untenstehende Beweis ist falsch bzw. hat eine Lücke. Es ist mir nicht klar, ob er mit den bisher benutzten Methoden möglich ist. Die Aussage folgt aber aus Noethernormalisierung, Satz 5.15.

Beweis: Wir fixieren zunächst ein Primideal $\mathfrak{p}$ von A und betrachten die Menge J der Primideale $\mathfrak{P}$ von $A[X]$ mit $\mathfrak{P} \cap A = \mathfrak{p}$. Ein Beispiel für ein solches Primideal ist $A[X]\mathfrak{p}$. Dieses Primideal ist in allen an $\mathfrak{P} \in J$ enthalten.

Behauptung. *Die einzige Enthaltenseinsrelation in J ist $A[X]\mathfrak{p} \subset \mathfrak{P}$.*

Wir nutzen zunächst die Bijektion $V(I)$ zu $\operatorname{Spec} A[X]/I$ für $I = A[X]\mathfrak{p}$. Hierbei bleiben alle Enthaltenseinsrelationen erhalten. Es ist $A[X]/A[X]\mathfrak{p} \cong (A/\mathfrak{p})[X]$. Es genügt es also, den Fall $\mathfrak{p} = 0$, A ein Integritätsring zu betrachten. Sei $S = A \setminus \{0\}$. Wir nutzen die Bijektion zwischen $\operatorname{Spec} S^{-1}A[X]$ und der Menge der Primideale von $A[X]$, die leeren Schnitt mit S haben. Wieder bleiben alle Enthaltenseinsrelationen erhalten. Wegen $S^{-1}(A[X]) \cong (S^{-1}A)[X]$ können wir also ohne Einschränkung annehmen, dass A ein Körper ist. In diesem Fall ist die Aussage klar, da $k[X]$ ein Hauptidealring ist.
Sei nun $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \mathfrak{p}_n$ eine Kette von Primidealen in A. Dann ist

$$A[X]\mathfrak{p}_0 \subset A[X]\mathfrak{p}_1 \subset \ldots A[X]\mathfrak{p}_n \subset (\mathfrak{p}_n, X)$$

eine Kette von Primidealen in $A[X]$ der Länge $n+1$. Also hat $A[X]$ mindestens die Dimension $n + 1$. Sei andererseits

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_m$$

eine Kette von echten Inklusionen von Primidealen von $A[X]$ mit $m > n$. Sei $\mathfrak{p}_i = \mathfrak{P}_i \cap A$. Sollte die Menge der $\mathfrak{p}_i$ weniger als $n+1$ Elemente haben, so verfeinern wir die Kette wie folgt.
Sei j der kleinste Index mit $\mathfrak{p}_j = \mathfrak{p}_{j+1}$. Nach dem vorher gezeigten folgt aus $\mathfrak{p}_j = \mathfrak{p}_{j+1}$ die Gleichheit $\mathfrak{P}_j = A[X]\mathfrak{p}_j$. Da A die Dimension n hat, tritt dieser Fall auch wirklich ein. Die Kette $\mathfrak{P}_i$ für $i \geq j$ induziert eine Kette von Primidealen in $A/\mathfrak{P}_j \cong (A/\mathfrak{p}_j)[X]$. Der Ring $A/\mathfrak{p}_j$ hat die Dimension $n-j$, also hat dieser Teil der Kette nach Induktionsannahme die Länge $n-j+1$. Zusammen mit den ersten j Schritten ergibt sich $m = n+1$. □

Korollar 4.24. *Sei k algebraisch abgeschlossener Körper. Dann hat $\mathbb{A}_k^n$ die Dimension n. Ist $V \subset \mathbb{A}_k^n$ eine irreduzible affine Varietät der Dimension d, so gibt es eine Kette von irreduziblen Untervarietäten*

$$V_0 \subsetneq V_1 \cdots \subsetneq V = V_d \subsetneq V_{d+1} \subsetneq \cdots \subsetneq V_n = \mathbb{A}_k^n$$

Insbesondere ist $d \leq n$.

Kapitel 5

Ganze Ringerweiterungen

Satz 5.1. *Seien $A \subset R$ Ringe, $x \in R$. Dann sind äquivalent:*

(i) *Es gibt $a_1, \ldots, a_n \in A$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.*

(ii) *$A[x] = \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in A\}$ ist ein endlich erzeugter A-Modul.*

(iii) *Es gibt einen Teilring $B \subset R$, der A und x enthält und der endlich erzeugter A-Modul ist.*

Beispiel. Seien speziell $A \subset R$ Körper. Dann bedeuten die Bedingungen:

(i) x ist algebraisch über A.

(ii) $A[x]$ ist ein endlich dimensionaler A-Vektorraum.

(iii) $A, \{x\} \subset B$ und B ist ein endlich dimensionaler A-Vektorraum.

In dieser Form ist der Satz aus der Algebra bekannt. Der Beweis bleibt derselbe.

Beweis: $(i) \Rightarrow (ii)$: Sei $M \subset R$ der A-Modul, der von $1, x, \ldots, x^{n-1}$ erzeugt wird. Nach Vorraussetzung gilt

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

Rekursiv erhält man also $x^{n+j} \in M$ für alle j. Es folgt $A[x] \subset M$. Die umgekehrte Inklusion ist klar. Insbesondere ist $A[x]$ endlich erzeugt.
$(ii) \Rightarrow (iii)$: Wähle $B = A[x]$.
$(iii) \Rightarrow (i)$: B werde von $y_1, \ldots, y_n$ also A-Modul erzeugt. Wegen $x \in B$ gilt $xy_i \in B$. Es gibt also Koeffizienten $a_{ij} \in A$ mit

$$xy_i = \sum_j a_{ij} y_j$$

Dies kann als ein lineares Gleichungssystem für die y_j gelesen werden. Sei d die Determinante der Koeffizientenmatrix, also das charakteristische Polynom von

(a_ij). Die Spalten der Koeffizientenmatrix sind linear abhängig. Nach Lemma 5.2 folgt $y_id = 0$ für $i = 1, \ldots, n$. Da B von den y_i erzeugt wird, folgt $bd = 0$ für alle $b \in B$, insbesondere auch $1d = 0$. Das charakteristische Polynom ist die gesuchte Polynomialgleichung für x. □

Lemma 5.2. *Sei R ein Ring, B eine quadratische Matrix mit Koeffiziente in B. Wenn das Gleichungssystem $By = 0$ eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n)$ hat, so folgt $\lambda_i \det B = 0$ für alle i.*

Beweis: Falls R nullteilerfrei ist, kann die Rechnung im Quotientenkörper erfolgen. Die Aussagen über die Determinanten folgen dann aus der linearen Algebra. Für den allgmeinen Fall gehen wir die Beweise durch: Die Determinante wird durch die Leibniz-Formel definiert. Sie ist multilinear und alternierend in den Zeilen und Spalten. Insbesondere bleibt sie unverändert, wenn man ein Vielfaches einer Spalte zu einer anderen addiert. Wir multiplizieren also die Spalte i mit λ_i (dies mutlipliziert die Determinante mit λ_i und addieren dann das λ_j-fache der Spalte j für alle $j \neq i$. In der neuen Matrix verschwindet die i-te Spale, also auch die Determinante. □

Definition 5.3. *Ein Element $x \in R$, welches eine der äquivalenten Bedingungen aus Satz 5.1 erfüllt, heißt* ganz über A. *R heißt* ganze Erweiterung von A, *wenn alle Elemente von R ganz sind. Die Menge*

$$B = \{x \in R \mid x \text{ ist ganz über } A\}$$

heißt ganzer Abschluss *von A in R.*

Beispiel. Sei $K/\mathbb{Q}$ endlich. Nach Definition 0.7 ist $\mathcal{O}_K$ ist der ganze Abschluss von $\mathbb{Z}$ in K.

Korollar 5.4. *Der ganze Abschluss ist ein Ring.*

Beweis: Es gilt $x + y, x - y, xy \in A[x, y]$. Sei x ganz über A. Dann ist $A[x]$ ein A-Modul mit Erzeugern $\{x_1, \ldots, x_n\}$. Sei y ganz über A. Dann ist $A[y]$ ein A-Modul mit Erzeugern $\{y_1, \ldots, y_m\}$. Dann sind die Elemente x_iy_j Erzeuger von $A[x, y]$, denn in $\alpha = \sum a_{kl}x^ky^l$ können x und y durch die x_i und y_j ausgedrückt werden. Durch Ausmultiplizieren erhält man eine Darstellung von α in Termen der x_iy_j. Also ist $A[x, y]$ endlich erzeugt. Nach Satz 5.1 sind dann alle Elemente von $A[x, y]$ ganz über A. □

Korollar 5.5 (Transitivität). *Seien $A \subset B$, $B \subset C$ ganze Ringerweiterungen. Dann ist $A \subset C$ ganz.*

Beweis: Sei $x \in C$. Es erfüllt also eine Gleichung

$$x^n + b_1x^{n-1} + \cdots + b_n = 0 \ , b_i \in B$$

B ist ganz über A, also ist $A[b_i]$ endlich erzeugter A-Modul. Wie beim letzten Beweis folgt $A[b_1, \ldots, b_n]$ endlich erzeugter A-Modul. Wegen $x \in A[b_1, \ldots, b_n]$ ist x ganz über A (Satz 5.1). □

Definition 5.6. *Sei A ein Integritätsring. A heißt* ganz abgeschlossen*, wenn A mit seinem ganzen Abschluss im Quotientenkörper übereinstimmt.*

Beispiel. Hauptidealringe (z.B. $\mathbb{Z}$, diskrete Bewertungsringe) sind ganz abgeschlossen.

Beweis: Sei A ein Hauptidealring, K der Quotientenkörper, $x \in K$ ganz über A. Dann ist

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \; a_i \in A$$

Sei $x = a/b$ mit a und b teilerfremd. Die Gleichung wird mit b^n multipliziert:

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0 \; .$$

b teilt jeden Summanden außer dem ersten, also folgt $b \mid a^n$. Dies ist ein Widerspruch zur Teilerfremdheit. Es folgt $b \in A^*$, $x \in A$. □

Beispiel. Ganzheitsringe $\mathcal{O}_K$ sind ganz abgeschlossen.

Beweis: Sei $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}$ in K, $\mathcal{O}'$ der ganze Abschluss von $\mathcal{O}$ in K. Wegen der Transitivität von ganzen Erweiterung ist dann $\mathcal{O}'$ ganz über Z, also $\mathcal{O}' \subset \mathcal{O}$. □

Primideale in ganzen Ringerweiterungen

Satz 5.7. *Sei $A \subset B$ eine ganze Ringerweiterung.*

(i) Sei $\subset \mathbf{B}$ ein Ideal und $\mathfrak{a} = A\cap$. Dann ist $B/$ ganze Ringerweiterung von $A/\mathfrak{a}$.

(ii) Sei $S \subset A$ mulitplikative Teilmenge. Dann ist $S^{-1}B$ ganze über $S^{-1}A$.

Beweis: Sei $x \in B$. Es erfüllt eine Gleichung

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

für $a_i \in A$. Wir reduzieren diese Gleichung mod und erhalten (i).
Sei $x/s \in S^{-1}B$. Wieder erfüllt x eine Gleichung wie oben. Multiplikation mit s^{-n} ergibt

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

Damit ist x/s ganz über $S^{-1}A$. □

Satz 5.8. *Sei B ein Integritätsring, $A \subset B$ ein Unterring, so dass B ganz über A ist. Dann gilt:*

$$B \text{ Körper } \Leftrightarrow A \text{ Körper}$$

Beweis: Sei A ein Körper, $0 \neq b \in B$. Nach Satz 5.1 ist $B' = A[b]$ ein endlich dimensionaler A-Vektorraum. Die Multiplikation mit B ist eine A-lineare Abbildung $B' \to B'$. Da B nullteilerfrei ist, ist diese Abbildung injektiv. Da B' endlich dimensional ist, ist sie dann auch surjektiv. Also hat b ein multiplikatives Inverses in $B' \subset B$.
Umgekehrt sei B ein Körper, $0 \neq a \in A$. Sei $b = a^{-1} \in B$. Dieses Element ist ganz über A, erfüllt also eine Gleichung

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \; a_i \in A \; .$$

Diese Gleichung wird mit a^{n-1} multipliziert.

$$b + a_1 + a_2 a + \ldots a_n a^{n-1} = 0 \; .$$

Alle Summanden außer dem ersten liegen in A, also auch b. □

Korollar 5.9. *Sei $A \subset B$ eine ganze Ringeerweiterung. Sei $\mathfrak{q} \subset B$ ein Primideal und $\mathfrak{p} = A \cap \mathfrak{q}$. Dann ist $\mathfrak{q}$ maximal genau dann, wenn $\mathfrak{p}$ maximal.*

Beweis: Nach Satz 5.7 ist $B/\mathfrak{q}$ ganz über $A/\mathfrak{p}$. Nach Definition von $\mathfrak{p}$ ist die natürliche Abbildung injektiv. Beides sind Integritätsbereiche. Nach Satz 5.8 ist dann $B/\mathfrak{q}$ Körper genau dann, wenn $A/\mathfrak{p}$ es ist. Mit anderen Worten: $\mathfrak{q}$ maximal genau dann, wenn $\mathfrak{p}$ maximal. □

Korollar 5.10. *Sei $A \subset B$ ganze Ringerweiterung, $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} B$ mit $\mathfrak{q} \subset \mathfrak{q}'$ und $\mathfrak{q} \cap A = \mathfrak{q} \cap A$. Dann gilt $\mathfrak{q} = \mathfrak{q}'$.*

Beweis: Sei $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Nach Satz 5.7 ist $B_\mathfrak{p}$ ganz über $A_\mathfrak{p}$. Die natürliche Abbildung ist injektiv. Wegen $S \cap \mathfrak{q} = S \cap \mathfrak{q}' = \emptyset$ können wir ohne Einschränkung A durch $A_\mathfrak{p}$ ersetzen, d.h. $\mathfrak{p}$ ist maximal. Nach Korollar 5.9 sind dann auch $\mathfrak{q}$, $\mathfrak{q}'$ maximal. Aus $\mathfrak{q} \subset \mathfrak{q}'$ folgt daher Gleichheit. □

Theorem 5.11. *Sei $A \subset B$ ganze Ringerweiterung und $\mathfrak{p} \subset A$ ein Primideal. Dann gibt es ein Primideal $\mathfrak{q}$ von von B, so dass $\mathfrak{q} \cap A = \mathfrak{p}$.*

Beweis: $B_\mathfrak{p}$ ist ganz über $A_\mathfrak{p}$. Sei $\mathfrak{n}$ ein maximales Ideal von $B_\mathfrak{p}$. Dann ist nach Korollar 5.9 $\mathfrak{n} \cap A_\mathfrak{p}$ maximal. Da $A_\mathfrak{p}$ lokal ist, gilt $\mathfrak{n} \cap A_\mathfrak{p} = A$. Wir setzen

$$\mathfrak{q} = \{b \in B \mid \frac{b}{1} \in \mathfrak{n}\}$$

Dann gilt $\mathfrak{q} \cap A = \{a \in A \mid \frac{a}{1} \in \mathfrak{n} \cap_\mathfrak{p}\} = \mathfrak{p}$ wie gesucht. Die letzte Aussage ist nur eine Umformulierung. □

Theorem 5.12 (Going-Up). *Sei $A \subset B$ ganze Ringerweiterung und $\mathfrak{p} \subset A$ ein Primideal. Sei*

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$$

eine Kette von Primidealen von A und für $m < n$

$$\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$$

eine Kette von Primidealen von B mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für $i \leq m$. Dann kann die Kette fortgesetzt werden zu einer Kette von Idealen

$$\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$$

mit $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ für $i \leq n$.

Beweis: Per Induktion reduzieren wir uns sofort auf den Fall $m = 1$, $n = 2$. Sei $\overline{A} = A/\mathfrak{p}_1$ und $\overline{B} = B/\mathfrak{q}_1$. Dann ist $\overline{A} \subset \overline{B}$ und die Erweiterung ist ganz nach Satz 5.7. Wir wenden das vorherige Theorem an auf das Primideal $\overline{\mathfrak{p}}_2 = \mathfrak{p}_2/\mathfrak{p}_1$ und finden $\overline{\mathfrak{q}}_2 \subset \overline{B}$. Sei $\mathfrak{q}_2$ das Urbild in B.
Die Aussage zur Dimension erhalten wir, wenn wir Going-Up auf eine maximale Kette von Primidealen anwenden. □

Korollar 5.13. *Sei $A \subset B$ eine ganze Ringerweiterung. Dann ist* $\operatorname{Spec} B \to \operatorname{Spec} A$ *surjektiv, und es gilt* $\dim A = \dim B$.

Beweis: Die Surjektivität ist Theorem 5.11. Sei

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$$

eine Kette von Primidealen von B. Wir setzen $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. Nach Korollar 5.10 gilt $\mathfrak{p}_i \subsetneq \mathfrak{p}_{i+1}$. Also gilt $\dim A \geq \dim B$. Ist umgekehrt eine Kette von Primidealen von A gegeben, so liftet sich diese nach Going-Up to einer Kette von B. Dies bedeutet $\dim B \geq \dim A$. □

Beispiel. Die Ganzheitsringe $\mathcal{O}_K$ sind eindimensional, da sie ganz über dem eindimensionalen Ring $\mathbb{Z}$ sind. Jedes Primideal von $\mathcal{O}_K$ enthält eine eindeutige Primzahl p.

Korollar 5.14. *Sei $k \subset A$ eine Ringerweiterung, wobei k ein Körper ist und A endlich dimensional als k-Vektorraum. Dann sind alle Primideale von A maximal und* $\operatorname{Spec} A$ *hat nur endlich viele Punkte.*

Beweis: A ist ganz über k, also gilt $0 = \dim k = \dim A$ (Krulldimension). Dies bedeutet, das alle Ketten von Primidealen die Länge 0 haben, d.h. jedes Primideal ist maximal.
Seien $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ paarweise verschieden Primideale von A. Diese sind coprim, d.h. $\mathfrak{m}_i + \mathfrak{m}_j = A$ für $i \neq j$, das die linke Seite echte größer als $\mathfrak{m}_i$ ist. Nach dem chinesischen Restsatz folgt dann

$$A/\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cong \prod_{i=1}^{n} A/\mathfrak{m}_i$$

Dies erlaubt die Vektorraumdimension abzuschätzen:

$$\dim_k A \geq \dim_k A/\mathfrak{m}_1 \cap \ldots \mathfrak{m}_n = \sum \dim_k A/\mathfrak{m}_i \geq n$$

denn jeder der Körper $A/\mathfrak{m}_i$ ist wenigsten 1-dimensional als k-Vektorraum. Dies bedeutet, dass $\dim_k A$ eine obere Schranke für die Anzahl der maximalen Primideale ist. □

Satz 5.15 (Noether Normalisierung). *Sei A ein Integritätsbereich, der endlich erzeugt über einem Körper k ist. Dann gibt es es algebraisch unabhängige Elemente $x_1, \ldots, x_n$ von A, so dass A von endlicher Modul über $B = k[x_1, \ldots, x_d]$ ist. Insbesondere ist A ganz über B. Es gilt $n = \dim A$.*

Beweis: Sei m die Anzahl der Erzeuger von A. Wir beweisen die erste Aussage durch Induktion über m. Wenn sie algebraisch unabhängig sind, so gilt $A = k[x_1, \ldots, x_m]$ und die Aussage ist wahr. Andernfalls genügt es, einen Unterring $B \subset A$ zu finden, der von $m-1$ Elementen erzeugt wird und so dass A endlicher B-Modul ist.
Seien $y_1, \ldots, y_m$ die Erzeuger. Sie erfüllen nach Vorraussetzung eine nicht-triviale polynomiale Relation

$$f(y_1, \ldots, y_m) = 0$$

d.h. $f \in k[Y_1, \ldots, Y_m] \setminus \{0\}$. Seien $r_2, \ldots, r_m \in \mathbb{N}$ und

$$z_i = y_i - y_1^{r_i} \qquad\qquad i = 2, \ldots, m$$

Dann gilt

$$f(y_1, z_2 + y_1^{r_1}, \ldots, z_m + y_m^{r_m}) = 0$$

d.h. $y_1, z_2, \ldots, z_m$ sind Nullstellen des Polynoms

$$f_{r_2,\ldots,r_m} = f(Y_1, Z_2 + Y_1^{r_1}, \ldots, Z_m + Y_1^{r_m}) \in k[Y_1, Z_2, \ldots, Z_m]$$

Behauptung. *Das Tupel $r = (r_2, \ldots, r_m)$ kann so gewählt werden, dass $f_r \neq 0$.*

Jeder Monom $a \prod_{i=1}^m Y_i^{b_i}$ in f ergibt eine Summe von Monomen in f_r, darunter der Monom

$$aY_1^{b_1 + r_2 b_2 + \ldots r_m b_m}$$

Durch geeignete schnellwachsende Wahlen der r_i

$$0 \ll r_1 \ll r_2 \ll \cdots \ll r_m$$

kann erreicht werden, dass diese Monome paarweise verschiedene Grade haben, also alle in f_r auftauchen. Damit ist das Polynom ungleich 0. Außderm taucht einer dieser Terme als Monom höchsten Grades in f_r auf, d.h.

$$f_r = bY_1^N + \text{Terme vom Grad} < N$$

mit $b \neq 0$. Die Gleichhung $f_r(y_1, z_2, \ldots, z_m) = 0$ besagt dann, dass y_1 ganz über $B = k[z_2, \ldots, z_m]$ ist.
Nach Korollar 5.13 gilt $\dim A = \dim B \geq n$. Es genügt also, die umgekehrte Inklusion im Fall $k[X_1, \ldots, X_n]$ zu zeigen. Sei also

$$0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_N$$

eine Kette von Primidealen in $k[X_1, \ldots, X_n]$. Wir betrachten $A' = k[X_1, \ldots, X_n]/\mathfrak{p}_1$. Die Bilder $x_1, \ldots, x_n$ der X_i erfüllen eine nichttriviale Relation $f \in \mathfrak{p}_1$. Auf diese

Elemente wenden wir unser obiges Verfahren an. Es gibt also $y_1, \ldots, y_d \in A'$, so dass A' ganz über $B' = k[y_1, \ldots, y_d]$. Nach Konstruktion ist $d < n$. Nach Induktionsannahme ist $\dim A' = \dim B' = d$. Daher hat die Kette von Primidealen

$$0 = \mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \mathfrak{p}_N/\mathfrak{p}_1$$

Länge $N - 1 \leq d < n$. Dies bedeutet $N \leq n$. □

Bemerkung. Hieraus folgt sofort, dass alle Ringe, die endlich erzeugt über einen Körper sind, endliche Dimension haben. Dies gilt insbesonder für die Ringe von regulären Funktionen auf einer Varietät.

Geometrische Interpretation

Diese Sätze haben auch eine geometrische Bedeutung. Um dies zu formulieren, tragen wir eine Definition nach:

Definition 5.16. *Sei k ein algebraisch abgeschlossener Körper, $V \subset \mathbb{A}_k^n$ und $W \subset \mathbb{A}_k^m$ affine Varietäten. Eine Abbildung $f : V \to W$ heißt* regulär*, wenn es $f_1, \ldots, f_m \in k[V]$ gibt mit $f(x) = (f_1(x), \ldots, f_m(x))$ für alle $x \in V$.*

Satz 5.17. *Sei V eine affine irreduzible Varität der Dimension m. Dann gibt es eine reguläre Abbildung $V \to \mathbb{A}^m$, so dass gilt:*

(i) $k[\mathbb{A}^m] \to k[V]$ ist injektiv und $k[V]$ endlich als Modul über $k[\mathbb{A}^m]$.

(ii) Die Erweiterung von Funktionenkörpern $k(\mathbb{A}^m) \to k(V)$ ist endlich.

(iii) f ist surjektiv und jeder Punkt $x \in \mathbb{A}^n$ hat endlich viele Urbilder.

Bemerkung. Wir können daher die Dimension von V aus dem Transzendenzgrad von $k(V)/k$ berechnen.

Beweis: Nach Definition ist $k[V]$ endlich erzeugter Ring über k. Es ist ein Integritätsbereich, da V irreduzibel ist. Nach Noether Normalisierung ist $k[V]$ ganz über $k[x_1, \ldots, x_m]$ für algebraisch unabhängige Elemente $x_i \in k[V]$ und $m = \dim k[V] = \dim V$. Wir definieren $f = (x_1, \ldots, x_m)$. Dies ist eine reguläre Abbildung

$$f : V \to \mathbb{A}^m$$

Nach Konstruktion ist $k[\mathbb{A}^m] = k[x_1, \ldots, x_m] \subset k[V]$. Die Endlichkeit von $k[V]$ als $k[\mathbb{A}^m]$-Modul ist dann Noether Normalisierung.
Hieraus folgt sofort die Aussage über die Funktionenkörper. Da die Erweiterung von Ringen ganz ist, erhalten wir eine surjektive Abbildung

$$f^{\#} : \operatorname{Spec} k[V] \to \operatorname{Spec} k[\mathbb{A}^r]$$

Hierbei ist $f^{\#}(\mathfrak{p})$ maximal genau dann, wenn $\mathfrak{p}$ es ist. Also ist die Abbildung auch auf maximalen Idealen surjektiv. Nach dem Hilbertschen Nullstellensatz bedeutet dies, das f surjektiv ist.

Sei $y \in \mathbb{A}^m$ ein Punkt. Wir betrachten $\{x \in V \mid f(x) = y\}$. Mit Hilbertschem Nullstellensatz entspricht dies der Menge der maximalen Ideale von $k[V]$, die $\mathfrak{m}_y$ enthalten. Dies entspricht wiederum den maximalen Idealen von $k[V]/k[V]\mathfrak{m}_y$. Dieser Ring ist endlich erzeugter Modul über $k[\mathbb{A}^m]/\mathfrak{m}_y = k$. Nach Korollar 5.14 hat er nur endliche viele maximale Ideale. □

Kapitel 6

Ganzheitsringe

Sei $K/\mathbb{Q}$ eine endliche Erweiterung, $\mathcal{O}_K$ der Ganzheitsring. Wir wissen aus dem letzten Kapitel, dass dies ein ganz abgeschlossener, 1-dimensionaler Ring ist.

Theorem 6.1. *Sei $K/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O}_K \subset K$ der Ganzheitsring. Dann ist $\mathcal{O}_K \cong \mathbb{Z}^d$ mit $d = [K : \mathbb{Q}]$.*

Korollar 6.2. *$\mathcal{O}$ ist noethersch.*

Beweis: $\mathcal{O}$ ist endlich erzeugter $\mathbb{Z}$-Modul, also erst recht endlich erzeugt als Ring. □

Vorüberlegungen

$\mathcal{O} \subset K$ ist eine torsionsfreie abelsche Gruppe. Daher ist ist $\mathcal{O}_K$ endlich erzeugt genau dann, wenn $\mathcal{O} \cong \mathbb{Z}^N$ für ein N.

Lemma 6.3. *Sei $x \in K$. Dann gibt es $m \in \mathbb{Z}$ mit $mx \in \mathcal{O}_K$.*

Beweis: x erfüllt $x^n + a_1 x^{n-1} + a_2 x^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Q}$. Sei m der Hauptnenner der a_i. Multiplikation der Gleichung mit m^n ergibt

$$(mx)^n + a_1 m(mx)^{n-2} + \ldots m^n a_n = 0 \ .$$

Also gilt $mx \in \mathcal{O}_K$. □

Korollar 6.4. *$\mathcal{O}_K$ enthält eine freie Gruppe vom Rang $d = [K : \mathbb{Q}]$.*

Beweis: Sei $x_1, \ldots, x_d$ eine Basis von K über $\mathbb{Q}$. Seien $m_1, \ldots, m_d \in \mathbb{Z}$, so dass $m_i x_i \in \mathcal{O}_K$.

Behauptung. *$< m_1 x_1, \ldots, m_d x_d >$ hat Rang d.*

Wäre der Rang kleiner als d, so hätten wir eine Relation

$$n_1(m_1 x_1) + n_2(m_2 x_2) + \cdots + n_d(m_d x_d) = 0 \ ,$$

dies ist ein Widerspruch zu linearen Unabhängigkeit von $x_1, \ldots, x_d$. □

Lemma 6.5. *Sei $M \subset K$ eine endlich erzeugte abelsche Gruppe. Dann gilt* $\mathrm{rg}M \leq d$.

Beweis: Sei $M_{\mathbb{Q}} = \{\frac{m}{s} \mid m \in M, s \in \mathbb{Z}\} \subset K$. Dies ist ein $\mathbb{Q}$-Vektorraum der Dimension höchstens d.

Behauptung. $\dim M_{\mathbb{Q}} = \mathrm{rg}M$.

Sei $x_1, \ldots, x_k$ eine Basis von M als $\mathbb{Z}$-Modul. Dies ist eine Basis von $M_{\mathbb{Q}}$ als $\mathbb{Q}$-Vektorraum, da ein linear unabhängiges Erzeugendensystem. □

Insgesamt: Wenn $\mathcal{O}_K$ endlich erzeugt ist als abelsche Gruppe, dann $\mathcal{O}_K \cong \mathbb{Z}^d$.

Lemma 6.6. *Für den Beweis von Theorem 6.1 genügt es zu zeigen, dass $\mathcal{O}_K \subset M \subset K$ wobei M eine endlich erzeugte abelsche Gruppe ist.*

Beweis: M endlich erzeugt $\Rightarrow$ M noetherscher $\mathbb{Z}$-Modul. $\mathcal{O}_K \subset M \Rightarrow \mathcal{O}_K$ noethersch. Der Rest des Theorems folgt aus Korollar 6.4 und Lemma 6.5. □

Norm, Spur und Diskriminante

Wir gehen zunächst zu allgemeinen Körpererweiterungen über. Sei L/K algebraische Erweiterung der Charakteristik 0, $\alpha \in L$ und $\mathrm{Min}(\alpha) \in K[X]$ das Minimalpolynom von α.

Lemma 6.7. $\mathrm{Min}(\alpha)$ *ist das charakteristische Polynom* $\det(X\,\mathrm{id} - m_\alpha)$ *der K-linearen Multiplikationsabbildung $m_\alpha : K(\alpha) \to K(\alpha)$ mit $x \mapsto \alpha x$.*

Beweis: Sei P das charakteristische Polynom. Es hat den Grad $[K(\alpha) : K] = \deg \mathrm{Min}(\alpha)$. Es ist normiert. Es gilt $P(m_\alpha)$ als Abbildung $K(\alpha) \to K(\alpha)$. Auswerten in 1 ergibt $P(\alpha) = 0$. Also erfüllt P alle Eigenschaften von $\mathrm{Min}(\alpha)$. □

Seien $\alpha_1, \ldots, \alpha_d$ die d verschiedenen ($\mathrm{Char}\, K = 0$!) Nullstellen von $\mathrm{Min}(\alpha)$ in $\overline{K}$. Jedes α_i definiert einen Körperhomomorphismus $\sigma_i : K(\alpha) \to \overline{K}$ mit $\sigma_i(\alpha)_i$. Dies sind alle Körperhomomorphismen $\sigma : K(\alpha) \to K$ mit $\sigma|_K = \mathrm{id}$.

Lemma 6.8. *Es gilt*

$$\mathrm{Min}(\alpha) = \prod_{i=1}^{d}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)) \ .$$

Beweis: Klar □

Bemerkung. $K(\alpha)/K$ ist galois genau dann, wenn alle $\alpha_i \in K(\alpha)$. Dann ist $\{\sigma_1, \ldots, \sigma_d\} = \mathrm{Gal}(K(\alpha)/K)$.

Definition 6.9. *Sei L/K endliche Körpererweiterung, $\alpha \in L$. Das* charakteristische Polynom *von α ist $P_\alpha = \det(X\,\mathrm{id} - m_\alpha)$, wobei m_α die Multiplikationsabbildung mit α ist. Die* Norm *von α ist $N_{L/K}(\alpha) = \det(m_\alpha)$. Die* Spur *von α ist $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha)$.*

Bemerkung. Es gilt $P_\alpha(X) = X^{[L:K]} - \mathrm{Tr}(\alpha)X^{[L:K]-1} + \cdots + (-1)^{[L:K]}N(\alpha)$.

Lemma 6.10. *Sei* $\mathrm{Char}\, K = 0$, $[L : K] = d$. *Seien* $\alpha_1, \ldots, \alpha_d$ *die Nullstellen von* $\mathrm{Min}(\alpha)$, *jede mit Vielfachheit* $[L : K(\alpha)]$. *Seien* $\sigma_1, \ldots, \sigma_d : L \to \overline{K}$ *die Einbettungen mit* $\sigma_i|_K = \mathrm{id}$. *Dann gilt*

$$P_\alpha(X) = \mathrm{Min}(\alpha)^{[L:K(\alpha)]} = \prod_{i=1}^{e}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha))$$
$$\mathrm{Tr}_{L/K}(\alpha) = \sum \alpha_i = \sum \sigma_i(\alpha)$$
$$N_{L/K}(\alpha) = \prod \alpha_i = \prod \sigma_i(\alpha)\ .$$

Beweis: Es genügt, die Aussge für P_α zu zeigen. Es gilt

$$\{\alpha_1, \ldots, \alpha_d\} = \{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$$

als Mengen mit Vielfachheit, denn jede der $[K(\alpha) : K]$ vielen Einbettungen $K(\alpha) \to \overline{K}$ lässt sich auf $[L : K(\alpha)]$ viele Weisen nach L fortsetzen. Der Fall $L = K(\alpha)$ ist Lemma 6.7. Sei nun $r : [L : K(\alpha)]$.

Behauptung. $P_{L/K} = P^r_{K(\alpha)/K}$.

Sei $y_1, \ldots, y_r$ eine Basis von $L/K(\alpha)$, $z_1, \ldots, z_q$ eine Basis von $K(\alpha)/K$. Dann ist $\{y_i z_j \mid i = 1, \ldots, r, j = 1, \ldots, q\}$ eine Basis von L/K. Sei $M = (m_{jk})$ die Matrix der Multiplikation mit α bezüglich er z_j, d.h. $m_\alpha(z_j) = \sum_k m_{jk} z_k$. Dann gilt $m_\alpha(y_i z_j) = \sum_k m_{jk} y_i z_k$. Die Matrix von m_α bezüglich der Basis $y_i z_j$ ist eine diagonale Blockmatrix aus r Kopien von M. □

Korollar 6.11. *Sei* L/K *Erweiterung von Zahlkörpern,* $\alpha \in \mathcal{O}_L$. *Dann gilt* $P_\alpha \in \mathcal{O}_K[X]$. *Insbesondere ist* $\mathrm{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in \mathcal{O}_K$.

Bemerkung. Falls $\mathcal{O}_L \cong \mathcal{O}_K^d$ (im Allgemeinen falsch!), so hat die Matrix von m_α Einträge in $\mathcal{O}_K$ und die Aussage ist klar.

Beweis: $P_\alpha(X) = \prod(X - \sigma(\alpha))$ mit σ wie im Lemma. Nach Vorraussetzung erfüllt α eine Gleichung

$$X^n + a_1 X^{n-1} + \cdots + a_0 = 0\ a_i \in \mathcal{O}_K$$

Dann erfüllt $\sigma(\alpha)$ dieselbe Gleichung, ist also ebenfalls ganz über $\mathcal{O}_K$. Da $\mathcal{O}_K$ ein Ring ist, liegen dann alle Koeffizienten von P_α in $\mathcal{O}_L \cap K = \mathcal{O}_K$. □

Beispiel. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3})$, $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. Wir wählen die Basis $1, \sqrt{3}$. Sei $\alpha = a + b\sqrt{3}$. Die Multiplikation mit α hat die Matrix

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

Also ist die Spur $2a$, die Norm $a^2 - 3b^2$, das charakteristische Polynom

$$P_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = X^2 - 2aX + (a^2 - 3b^2)$$

Für $b \neq 0$ ist dies das Minimalpolynom von α. Für $b = 0$ gilt $X^2 - 2aX + a^2 = (X - a)^2 = \mathrm{Min}(\alpha)^2$.

Definition 6.12. *Sei $A \subset B$ eine Ringerweiterung, B ein freier A-Modul vom Rang d. Die* Spurpaarung *ist die symmetrische A-bilineare Abbildung*

$$(\cdot,\cdot) : B \times B \to A \ , (x, y) = \mathrm{Tr}_{B/A}(xy) \ .$$

Die Diskriminante $\mathcal{D}_{B/A}$ *ist das Ideal, das von*

$$D(x_1, \ldots, x_d) = \det(\mathrm{Tr}(x_i x_j)_{i,j})$$

erzeugt wird, wobei $x_1, \ldots, x_d$ eine Basis von B ist.

Bemerkung. Uns interessiert vor allem L/K endliche Köpererweiterung, aber auch $\mathcal{O}_K/\mathbb{Z}$.

Beispiel. Sei $L = \mathbb{Q}[X]/X^2 + pX + q$ mit $p, q \in \mathbb{Q}$. Dies ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum, Basis $1, X$. Es gilt $\mathrm{Tr}(1) = 2$. Muliplikation mit X hat die Matrix

$$\begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

also, $\mathrm{Tr}(X) = -q$.
Es gilt

$$D(1, X) \ = \ \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(X) \\ \mathrm{Tr}(X) & \mathrm{Tr}(X^2) \end{pmatrix} \ = \ \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} \ = \ p^2 \ - \ 4q$$

Dies ist genau die Diskriminate der quadratischen Gleichung.

Lemma 6.13. *Sei $y_1, \ldots, y_d \in B$ mit $y_i = \sum a_{ij} x_j$. Dann gilt*

$$D(y_1, \ldots, y_d) = \det(a_{ij})^2 D(x_1, \ldots, x_d)$$

Insbesondere ist $\mathcal{D}_{B/A}$ wohldefiniert.

Beweis: Es gilt

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}(\sum_{i,j} a_{pi} a_{qj} x_i x_j) = \sum a_{pi} a_{qj} \mathrm{Tr}(x_i x_j)$$

Es folgt

$$(\mathrm{Tr}(y_p y_q))_{pq} = (a_{pi})_{pi} (\mathrm{Tr}(x_i x_j))_{ij} (a_q j)^t$$

wobei ^{t} die transponierte Matrix ist. Dies impliziert die Gleichheit der Determinanten. □

Exkurs in die bilineare Algebra

Sei $(\cdot,\cdot) : V \times V \to k$ eine symmetrische Bilinearform, (k Körper, V ein Vektorraum). Sei $v_1, \ldots, v_d$ eine Basis von V, $M = (v_i, v_j)_{ij}$ die zugehörige symmetrische Matrix. Dann gilt für $v = \sum a_i v_i, w = \sum_j b_j v_j$

$$(v,w) = (\sum a_i v_i, \sum_j b_j v_j) = \sum_{i,j} a_i (v_i, v_j) b_j = (a_1, \ldots, a_d) M (b_1, \ldots, b_d)^t$$

Definition 6.14. *Die Bilinearform $(\cdot,\cdot)$ heißt nicht-degeneriert, wenn aus $(v,w) = 0$ für alle w die Gleichung $v = 0$ folgt.*

Lemma 6.15. *$(\cdot,\cdot)$ ist nichtdegeneriert genau dann, wenn die zugehörige Matrix M invertierbar ist, also genau dann, wenn* $\det M \neq 0$.

Beweis: Falls M nicht invertierbar ist, so gibt es v mit $v^t M = 0$, also auch $v^t M w = 0$ für alle w. Sei nun M invertierbar, $v = \sum a_i v_i$. Der Fall $d = 1$ ist trivial, also sei $d > 1$. Wähle $(c_1, \ldots, c_d)$ mit

$$a_1 c_1 + \cdots + a_d c_d \neq 0$$

Wir lösen das Gleichungssystem $Mw = (c_1, \ldots, c_d)^t$. Dies ist möglich, da M invertierbar ist. Es folgt $v^t M w \neq 0$. □

Bemerkung. Die Diskriminante entscheidet also, ob die Spurpaarung nichtdegeneriert ist.

Beispiel. $K = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$. Es gilt

$$\mathcal{D} = D(1, \sqrt{3}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{3}) \\ \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(3) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} = 12$$

Lemma 6.16. *Sei $(\cdot,\cdot)$ nicht-degnererierte symmetrsiche Bilinearform, $v_1, \ldots, v_d$ eine Basis. Dann gibt es eine* duale Basis *$w_1, \ldots, w_d$ mit $(v_i, w_j) = \delta_{ij}$.*

Beweis: Die Bestimmung von w_j bedeutet das Lösen eines linearen Gleichungssystems $Mw_j = (0, \ldots, 1, \ldots, 0)$ (mit 1 an der j-ten Stelle. Dies ist möglich, da M invertierbar ist. □

Satz 6.17. *Sei L/K endliche Körpererweiterung der* Char 0. *Dann ist $\mathcal{D}_{L/K} \neq 0$. Die Spurpaarung ist nicht-degeneriert.*

Beweis: Es gilt $\mathrm{Tr}(\alpha) = \sum \sigma_i(\alpha)$, wobei $\sigma_i : L \to \overline{K}$ die Einbettungen mit $\sigma_i|_K = \mathrm{id}$ durchläuft. Sei $x_1, \ldots, x_d$ eine Basis von L über K. Es gilt

$$\begin{aligned} D(x_1, \ldots, x_d) &= \det(\mathrm{Tr}(x_i y_j)_{ij}) = \det(\sum_k \sigma_k(x_i x_j))_{ij} \\ &= \det(\sum_k \sigma_k(x_i)\sigma_k(x_j))_{ij} = \det((\sigma_k(x_i))_{ik}(\sigma_k(x_j))_{kj}) = \det(\sigma_i(x_j))^2 \end{aligned}$$

Angenommen diese Determinante verschwindet. Dann gibt es $u_1, \ldots, u_d \in \overline{K}$ mit $\sum_i u_i \sigma_i(x_j) = 0$ für alle j. Da die x_j eine Basis sind, folgt $\sum u_i \sigma_i = 0$ als Abbildungen $L^* \to \overline{K}$. Als Gruppenhomomorphismen $L^* \to \overline{K}^*$ sind die σ_i jedoch linear unabhänging (siehe unten Satz 6.18, vergleiche Beweis des Hauptsatzes der Galois-Theorie in Bosch §4.6 Satz 2). □

Beispiel. $L = \mathbb{Q}[X]/X^2 + pX + q$ hatte Diskriminante $p^2 - 4q$. Diese Zahl verschwindet genau dann, wenn $X^2 + pX + q$ eine doppelte Nullstelle hat, also wenn L kein Körper ist.

Beweis von Theorem 6.1. Sei $\mathcal{O} \subset K$ der Ganzheitsring. Nach Lemma 6.6 genügt es zu zeigen, dass $\mathcal{O}$ in einem endlich erzeugten $\mathbb{Z}$-Modul $M \subset K$ enthalten ist. Sei $x_1, \ldots, x_d$ eine Basis von $K/\mathbb{Q}$. Ohne Einschränkung gilt $x_i \in \mathcal{O}$. Sei $y_1, \ldots, y_d$ die duale Basis bezüglich der Spurpaarung.

Behauptung. $\mathcal{O} \subset < y_1, \ldots, y_d >_{\mathbb{Z}}$.

Sei $z \in \mathcal{O}$. Wir schreiben $z = \sum b_j y_j$ mit $b_j \in \mathbb{Q}$, da die y_j eine Basis bilden. Es gilt $x_i z \in \mathcal{O}$, da $\mathcal{O}$ ein Ring ist. Nach Korollar 6.11 ist $\mathrm{Tr}(x_i z) \in \mathbb{Z}$. Es folgt weiter

$$\mathrm{Tr}(x_i z) = \sum \mathrm{Tr}(x_i b_j y_j) = \sum b_j \mathrm{Tr}(x_i y_j) = b_i$$

□

Nachtrag:

Satz 6.18. *Sei G eine Gruppe, K ein Körper, $\chi_1, \ldots, \chi_n : G \to K^*$ paarweise verschiedene Gruppenhomomorphismen. Dann sind die Abbildungen linear unabhängig als Abbildungen $G \to K$.*

Beweis: Induktion nach n. Der Fall $n = 1$ ist wahr, denn $\chi_1 \neq 0$. Seien nun $\chi_1, \ldots, \chi_{n-1}$ linear unabhängig, aber $\chi_1, \ldots, \chi_{n-1}, \chi_n$ linear abhängig, d.h. es gibt $\alpha_1, \ldots, \alpha_{n-1} \in L$ mit

$$\alpha_1 \chi_1 + \cdots + \alpha_{n-1} \chi_{n-1} = \chi_n \in \mathrm{Abb}(G, L) \ ,$$

d.h. für alle $g \in G$ gilt

$$\alpha_1 \chi_1(g) + \cdots + \alpha_{n-1} \chi_{n-1}(g) = \chi_n(g) \in L \ .$$

In dieser Gleichung ersetzen wir g durch gh, also

$$\alpha_1 \chi_1(g)\chi_1(h) + \cdots + \alpha_{n-1} \chi_{n-1}(g)\chi_{n-1}(h) = \chi_n(g)\chi_n(h) \in L \ .$$

Diese Gleichung multiplizieren wir mit $\chi(h^{-1}) = \chi_n(h)^{-1}$:

$$\alpha_1 \chi_1(g) \frac{\chi_1(h)}{\chi_n(h)} + \cdots + \alpha_{n-1} \chi_{n-1}(g) \frac{\chi_{n-1}(h)}{\chi_n(h)} = \chi_n(g) \in L \ .$$

Wir bilden die Differenz zur ersten Gleichung für g:

$$\alpha_1 \chi_1(g) \left(1 - \frac{\chi_1(h)}{\chi_n(h)}\right) + \cdots + \alpha_{n-1} \chi_{n-1}(g) \left(1 - \frac{\chi_{n-1}(h)}{\chi_n(h)}\right) = 0 \in L \ .$$

Diese Gleichung gilt für alle g (und festes h), aber die χ_i für $i \leq n-1$ sind linear unabhängig. Es folgt

$$\alpha_i \left(1 - \frac{\chi_i(h)}{\chi_n(h)}\right) = 0 \ .$$

Wären alle $\alpha_i = 0$, so wäre $\chi_n = 0$. Also gibt es ein i_0 mit $\alpha_{i_0} \neq 0$. Es folgt

$$1 = \frac{\chi_{i_0}(h)}{\chi_n(h)} \Leftrightarrow \chi_n(h) = \chi_{i_0}(h) \ .$$

Dies gilt für alle $h \in G$, also ist $\chi_n = \chi_{i_0}$, Widerspruch. □

Lokale Ringe

Definition 6.19. *Ein* Dedekindring *ist ein ganz abgeschlossener, noetherscher Integritätsbereich der Dimension* 1*.*

Wir haben also gezeigt, dass $\mathcal{O}_K$ ein Dedekindring ist.

Bemerkung. Ein anderes Beispiel für einen Dedekindring ist $k[V(f)]$ für eine 1-dimensionale Untervarietät $V(f) \subset \mathbb{A}_k^2$ wobei

$$\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)(P) \neq 0 \qquad \text{für alle } P \in V(f)$$

Nach dem Satz für implizite Funktionen ist dies genau die Bedingung, die erfüllt sein muss, um $V(f)$ zu einer Untermannigfaltigkeit zu machen, d.h. $V(f)$ hat keine Singularitäten.

Theorem 6.20. *Ein noetherscher Ring A ist genau dann ein Dedekindring, wenn für alle $\mathfrak{p} \in \operatorname{Spec} A$ mit $\mathfrak{p} \neq 0$, der lokale Ring $A_\mathfrak{p}$ ein diskreter Bewertungsring ist.*

Wenn wir genügend Zeit haben, werden wir wenigstens die schächere Aussage zeigen: Sei $0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$. Dann ist $\mathcal{O}_{K,\mathfrak{p}}$ ein diskreter Bewertungsring. Mit anderen Worten: In Ganzheitsringen gilt die Eindeutigkeit der Primfaktorzerlegung lokal.

Kapitel 7

Gebrochene Ideale und die Klassengruppe

In diesem Kapitel studieren wir Ideale in Dedekindringen.

Definition 7.1. *Sei A ein Dedekindring mit Quotientenkörper K. Ein* gebrochenes *Ideal von A ist ein A-Untermodul $0 \neq I \subset K$, so dass es $d \in A \setminus \{0\}$ gibt mit $dI \subset A$, d.h. ein gemeinsamer Hauptnenner.*

Bemerkung.

- Ein Ideal $I \subset A$ ist ein gebrochenes Ideal (mit $d = 1$).
- $I \neq 0$ ist ein gebrochenes Ideal, genau dann, wenn es ein endlich erzeugter A-Untermodul von K ist.

  Beweis: Sei $I =< x_1, \ldots, x_n >_A$, d der Hauptnenner der x_i, dann gilt $dI \subset A$. Ist umgekehrt $dI \subset A$, so ist dI ein Ideal eines noetherschen Rings, also endlich erzeugt. Dann ist auch I endlich erzeugt. □

- Die Menge der gebrochenen Ideale hat eine Addition und Multiplikation

$$I + I' = \{a + b \mid a \in I, b \in I'\} \subset K$$
$$I \cdot I' = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in I'\} \subset K$$

  Wir werden zeigen, dass die gebrochenen Ideale ungleich 0 eine abelsche Gruppe bezüglich der Multiplikation bilden.

- Gebrochene Ideale heißen auch *invertierbare Ideale* (bezüglich der Multiplikation).

Theorem 7.2. *Sei A ein Dedekindring. Dann ist jedes maximale Ideal invertierbar als gebrochenes Ideal, d.h. zu I existiert I^{-1} mit $I \cdot I^{-1} = A$.*

Bemerkung. Wäre A ein Hauptidealring, so wären alle gebrochenen Ideale von der Form Ab mit $b \in Q(A)$. Das inverse Ideal wäre einfach Ab^{-1}.

Lemma 7.3. *Sei A noetherscher Ring, $0 \neq I$ ein Ideal. Dann gibt es Primideale ungleich 0 mit $I \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$.*

Beweis: Sei Φ die Menge der echten Ideale I von A, für die das Lemma nicht gilt, d.h. die kein Produkt von Primidealen enthalten. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I_0. I_0 ist nicht prim, also gibt es $x, y \in A \setminus I_0$ mit $xy \in I_0$. Nach Voraussetzung

$$I_0 \subsetneq I_0 + (x), I_0 + (y) \Rightarrow I_0 + (x), I_0 + (b) \notin \Phi$$

Also gibt es Primideale ungleich null mit

$$\mathfrak{p}_1 \dots \mathfrak{p}_n \subset I_0 + (x), \mathfrak{q}_1 \dots \mathfrak{q}_m \subset I_0 + (b) \Rightarrow$$
$$\mathfrak{p}_1 \dots \mathfrak{p}_n \mathfrak{q}_1 \dots \mathfrak{q}_m \subset (I_0 + (x))(I_0 + (y)) = I_0$$

Dies ist ein Widerspruch. □

Beweis des Theorems: Sei $\mathfrak{m} \subset A$ maximal, $\mathfrak{m} \neq 0$. Sei

$$\mathfrak{m}' = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Dies ist ein A-Untermodul von $Q(A)$. Für $0 \neq y \in \mathfrak{m}$ folgt $y\mathfrak{m}' \in A$, also ist dies ein gebrochenes Ideal. Schließlich gilt nach Definition $\mathfrak{m}\mathfrak{m}' \subset A$. Da $\mathfrak{m}$ ein Ideal ist, gilt $A \subset \mathfrak{m}'$. Es folgt

$$\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$$

Da $\mathfrak{m}$ maximal ist, gilt

$$\mathfrak{m}'\mathfrak{m} = \mathfrak{m} \text{ oder } \mathfrak{m}'\mathfrak{m} = A$$

Behauptung. $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ *ist unmöglich.*

Angenommen, $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$. Sei $x \in \mathfrak{m}' \Rightarrow x\mathfrak{m} \subset \mathfrak{m}$. Iterativ folgt

$$x^2\mathfrak{m} = x(x\mathfrak{m}) \subset x(\mathfrak{m}) \subset \mathfrak{m} \Rightarrow x^n\mathfrak{m} \subset \mathfrak{m} \text{ für alle } n \geq 1$$

Sei $0 \neq d \in \mathfrak{m}$, also $x^n d \in A$ für alle n. Dann ist $A[x]$ ein gebrochenes Ideal, also endlich erzeugter A-Modul. Also ist x ganz über A. Dies bedeutet wiederum, dass $x \in A$, da A ganz abgeschlossen ist. Also $\mathfrak{m}' \subset A$. Die Inklusion $A \subset \mathfrak{m}'$ war trivial, also haben wir $A = \mathfrak{m}'$ gezeigt. Insgesamt:

$$A = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Sei nun $0 \neq a \in \mathfrak{m}$, also $(a) \neq 0$. Nach Lemma 7.3 gibt es Primideale ungleich null mit $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a)$. Ohne Einschränkung sei n minimal. Es folgt

$$\mathfrak{m} \supset (a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$$

Angenommen, für alle i ist $\mathfrak{p}_i$ ist nicht in $\mathfrak{m}$ enthalten, d.h. es gibt $x_i\mathfrak{p} \setminus \mathfrak{m}$. Dann gilt $x_1 \dots x_n \in \mathfrak{p}_1 \dots \mathfrak{p}_n \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $\mathfrak{m}$ Primideal. Also gibt es ein i mit $\mathfrak{p}_i \subset \mathfrak{m}$, z.B. $i = n$.

$$\mathfrak{m} \supset (a) \supset \mathfrak{m}I \text{ mit } I = \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}$$

I ist nicht in (a) enthalten, da n minimal gewählt war. Sei $b \in I \setminus (a)$. Wegen $\mathfrak{m}I \subset (a)$ folgt $\mathfrak{m}b \subset (a) = Aa$. Dies impliziert $\mathfrak{m}ba^{-1}a \subset A$. Also nach Definition: $ba^{-1} \in \mathfrak{m}' = A \Leftrightarrow b \in (a)$. Dies ist ein Widerspruch zur Zahl von b. □

Theorem 7.4. *Sei A ein Dedekindring,* Spec A *die Menge der Primideale von A.*

(i) Jedes gebrochene Ideal schreibt sich eindeutig als

$$I = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^{v_\mathfrak{p}(I)}$$

mit $v_\mathfrak{p}(I) \in \mathbb{Z}$ fast alle null.

(ii) Es gilt $v_\mathfrak{p}(I) \geq 0$ für alle $\mathfrak{p}$ genau dann, wenn I ein ganzes Ideal ist.

(iii) Der Monoid der gebrochenen Ideale ist eine Gruppe.

Beweis: Zur Existenz: Es gilt $dI \subset A$, $I = (dI)(d^{-1}$. Daher genügt es, die Produktzerlegung für ganze Ideale zu zeigen. Sei Φ die Menge der Ideale, die keine Primidealfaktorisierung hat. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I. Es ist $I \neq A$, da $A = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^0$. Also ist $I \subset \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$. Sei $\mathfrak{p}' = \mathfrak{p}^{-1}$ das Inverse als gebrochenes Ideal. Es folgt

$$I \subset \mathfrak{p} \Rightarrow I\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$$

Wegen $A \subset \mathfrak{p}'$ folgt auf jeden Fall $I\mathfrak{p}' \subset I$.

Behauptung. $I \subsetneq I\mathfrak{p}'$

Angenommen, die Ideale sind gleich. Sei $x \in \mathfrak{p}'$. Nach Annahme ist $xI \subset I$, also iterativ $x^n I \subset I$ für alle n. Ein Hauptnenner für I ist auch ein Hauptnenner für $A[x]$, also ist dieser Modul endlich erzeugt und x ganz über A. Damit ist $x \in A$. Wir haben $\mathfrak{p}' = A$ gezeigt, dies ist ein Widerspruch.
Nach Wahl von $I \in \Phi$ ist nun $I\mathfrak{p}' \notin \Phi$. Es gilt

$$\mathfrak{p}'I = \mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n} \Rightarrow I = \mathfrak{p}\mathfrak{p}'I = \mathfrak{p}\mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n}$$

Tatsächlich sind hierbei die Exponenten alle größer gleich 0.
Zur Eindeutigkeit: Sei $\prod \mathfrak{p}^{n_\mathfrak{p}} = \prod \mathfrak{p}^{m^-\mathfrak{p}}$, also $\prod \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = A$. Wir schreiben die Gleichung so um, dass alle Exponenten größer gleich Null und minimal sind. Wir erhalten also

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k} = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$$

mit $\mathfrak{p}_i \neq \mathfrak{q}_j$ für alle i, j und $n_i, m_j > 0$. Es gilt $\mathfrak{p}_1 \subset \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$. Also enthält $\mathfrak{p}_1$ eines der $\mathfrak{q}_j$ (wie im Beweis von Theorem 7.2). Da A ein Dedekindring ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_j$, Widerspruch.
Die Behauptung über die Gruppenstruktur ist klar. □

Korollar 7.5. *Sei A ein lokaler Dedekindring, d.h. es gibt nur genau ein maximales Ideal. Dann ist A ein diskreter Bewertungsring.*

Beweis: Sei $\mathfrak{p}$ das maximale Ideal von A. Wir definieren

$$v : K^* \to \mathbb{Z} \qquad a \mapsto v_{\mathfrak{p}}((a))$$

wobei $v(I)$ die ganze Zahl des Theorems ist. Diese Zuordnung erfüllt automatisch die Rechenregeln einer Bewertung.

Behauptung. *v ist surjektiv.*

Sei $\mathfrak{p}$ das maximale Ideal, $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann folgt $(\pi) \subset \mathfrak{p}$, aber (π) ist nicht in $\mathfrak{p}^2$ enthalten. Nach dem Strukturtheorem gilt $(\pi) = \mathfrak{p}^v$ für $v \geq 0$. Es bleibt nur $(\pi) = \mathfrak{p}$ übrig. Nach Definition ist $v(\pi) = v_{\mathfrak{p}}(\mathfrak{p}) = 1$. □

Korollar 7.6. *Sei A ein Dedekindring, $\mathfrak{p}$ ein maximales Ideal. Dann ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring.*

Beweis: Es genügt zu zeigen, dass $A_{\mathfrak{p}}$ ebenfalls ein Dedekindring ist. Als Lokalisierung ist $A_{\mathfrak{p}}$ ebenfalls noethersch und ganz abgeschlossen (leicht). Die Dimension ist 1. □

Bemerkung. In diesem Sinne sind Dedekindringe lokal Ringe mit eindeutiger Primfaktorzerlegung - aber natürlich nicht global. Ist I ein invertierbares Ideal, so ist jedes $I_{\mathfrak{p}} \cong A_{\mathfrak{p}}$ $A_{\mathfrak{p}}$-Modul. Geometrisch gesprochen: I ist ein Geradenbündel über A.

Definition 7.7. *Sei A ein Dedekindring. Die* Idealklassengruppe *von A ist*

$$\mathrm{Cl}(A) = \frac{\textit{Gruppe der gebrochenen Ideale} \neq 0}{\textit{Hauptideale} \neq 0}$$

Ist speziell $A = \mathcal{O}_K$ für einen Zahlkörper K, so heißt $\mathrm{Cl}_K = \mathrm{Cl}(\mathcal{O}_K)$ auch Klassengruppe *von K. Die* Klassenzahl *h ist die Anzahl der Elemente von Cl_K.*

Bemerkung. $h = 1$ bedeutet, dass jedes Ideal ein Hauptideal ist. Die Klassenzahl misst also, wie weit $\mathcal{O}_K$ davon abweicht, ein Hauptidealring zu sein. Sie ist endlich (tief!)

Lemma 7.8. *Die Klassengruppe ist isomorph zur Halbgruppe der echten Ideale ungleich 0 mit Äquivalenzrelation $I(g) \sim I(f)$ für $f, g \in A \setminus \{0\}$.*

Beweis: Sei C' die im Lemma definierte Halbgruppe. Sie bildet sich in die Klassengruppe ab. Jedes gebrochene Ideal ist äquivalent zu einem echten Ideal, also ist die Abbildung surjektiv. Die Äquivalenzrelation ist offensichtlich die gleiche, also ist sie auch injektiv. □

Dieser Beschreibung sieht man die Existenz des Inversen nicht an! Man spart also keine Arbeit gegenüber unserem Ansatz.

Exkurs

Sei $V(f) \subset \mathbb{A}^2$ eine ebene Kurve. Dann gibt es eine endliche Überlagerung $\pi : V(f) \to \mathbb{A}^1$. Wenn $V(f)$ singularitätenfrei ist (d.h. $(\partial f/\partial x, \partial f/\partial y) \neq 0$ auf $V(f)$), so kann man zeigen, dass $k[V]$ der ganze Abschluss von $k[\mathbb{A}^1]$ in $k(V)$ ist, d.h. ebenfalls ein Dedekindring. Ein Geradenbündel auf $V(f)$ ist ein Morphismus von Varietäten $E \to V(f)$, so dass E lokal von der Form $U \times \mathbb{A}^1$ für $U \subset V(f)$ ist. Man zeigt dann, dass die Elemente der Klassengruppe genau zur multiplikativen Gruppe (Tensor-Produkt) der Isomorphieklassen von Geradenbündeln korrespondieren.
Ein anderes Analogon gibt es in der Theorie der kompakten Riemannschen Flächen, d.h. der 1-dimensionalen kompakten komplexen Mannigfaltigkeiten. Der Körper $k(V)$ wird dann ersetzt durch den Körper der meromorphen Funktionen auf X. Dann kann die Gruppe der Geradenbündel mit analytischen Methoden beschrieben werden. Es gilt

$$\mathrm{Pic}(X) \cong \mathbb{Z} \times \mathbb{C}^g/\Lambda$$

(g das Geschlecht von X, Λ ein Gitter in $\mathbb{C}^g$.) Tatsächlich gibt es aber eine Kategorienäquivalenz zwischen der kompakten Riemannschen Flächen und glatten projektiven Kurven über $\mathbb{C}$.
Wichtig in der analytischen Theorie ist die Kompaktheit. Für Varietäten bedeutet dies, dass wir besser mit Überlagerungen von $\mathbb{P}^1$ arbeiten sollten. Dafür betrachtet man quasi-projektiven Varietäten, die wir nicht definiert haben.
Ganzheitsringe entsprechen wiederum affinen Kurven. Es fehlen Punkte im "Unendlichen". Diese sind bekannt: sie entsprechen den Einbettungen von K nach $\mathbb{R}$ oder $\mathbb{C}$. Die analytischen Eigenschaften von Zahlkörpern müssen ebenfalls benutzt werden, wenn man die Klassengruppe studieren will.

Beispiel

$K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Es gilt $\mathcal{O} \cong \mathbb{Z}[X]/X^2 + 5$. Wir bestimmen die Primideale: Sei $\mathfrak{p} \subset \mathcal{O}$ prim, $(p) = \mathfrak{p} \cap \mathbb{Z}$ für $p \in \mathbb{Z}$ Primzahl.

(i) $p = 2$: Wir haben

$$\mathcal{O}/(2) = \mathbb{Z}[X]/(X^2 + 5, 2) = \mathbb{F}_2[X]/X^2 + 1 = \mathbb{F}_2[X]/(X + 1)^2$$

Also ist (2) selbst kein Primideal von $\mathcal{O}$. Es gibt genau ein Primideal, das 2 enthält. Modulo 2 wird es von $X + 1$ erzeugt, also $P_2 = (2, \sqrt{-5} + 1)$.

(ii) $p = 3$

$$\begin{aligned}\mathcal{O}/(3) = \mathbb{Z}[X]/(X^2 + 5, 3) = \mathbb{F}_3[X]/X^2 - 1 = \mathbb{F}_2[X]/(X + 1)(X - 1)\\ = \mathbb{F}_3[X]/X - 1 \times \mathbb{F}_3[X]/X + 1\end{aligned}$$

Es gibt zwei Primideale, die 3 enthalten, nämlich $P_3 = (3, \sqrt{-5} + 1)$, $P_3' = (3, \sqrt{-5} - 1)$. Es gilt $(3) = P_3 P_3'$ in $\mathcal{O}$. Wichtig für diese Berechnung war nur, dass 5 eine Quadratzahl modulo 3 war.

(iii) $p = 5$

$$\mathcal{O}/(5) = \mathbb{Z}[X]/(X^2 + 5, 5) = \mathbb{F}_5[X]/X^2$$

$P_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ ist das einzige Primideal, das 5 enthält. Es gilt $(5) = P_5^2$.

(iv) $p = 7$

$$\mathcal{O}/(7) = \mathbb{Z}[X]/(X^2 + 5, 7) = \mathbb{F}_3[X]/X^2 - 2 = \mathbb{F}_2[X]/(X + 3)(X - 3)$$
$$= \mathbb{F}_3[X]/X - 3 \times \mathbb{F}_3[X]/X + 3$$

$P_7 = (7, \sqrt{-5} \pm 3)$ (wie Fall $p = 3$)

(v) $p = 11$ In diesem Fall ist 5 keine Quadratzahl modulo 11, das Ideal (11) ist prim in $\mathcal{O}$.

beim Rechnen modulo Hauptideale gilt also: $P_2^2 \sim 1$, $P_5 \sim 1$, $P_3 \sim (P_3')^{-1}$, $P_{11} \sim 1$ etc.
Frage: Ist P_2 ein Hauptideal? Falls $P_2 = (\alpha)$, so gibt es x, y mit

$$x\alpha = 2 \Rightarrow N(x)N(\alpha) = N(2) = 4$$
$$y\alpha = \sqrt{-5} + 1 \Rightarrow N(y)N(\alpha) = N(\sqrt{-5} + 1) = 6$$

Dies impliziert $N(\alpha) = 2$. Sei $\alpha = a_1 + a_2\sqrt{-5}$ $(a_i \in \mathbb{Z})$

$$a_1^2 - 5a_2^2 = 2$$

Dies führt also auf die Theorie der Lösbarkeit der quadratischen Gleichungen in $\mathbb{Z}$. Die obige ist modulo 4 nicht lösbar, also ist P_2 kein Hauptideal.

Man sieht bereits in diesem Beispiel: die Bestimmung der Klassengruppe ist schwierig, da sie unendlich viele Erzeuger und unendlich viele Relationen hat!

Die Frage nach Primidealen in $\mathbb{Z}[\sqrt{d}]$ führt auf die Frage, ob d eine Primzahl ist modulo p oder nicht. Dies wird durch Gauß' quadratisches Reziprozitätsgesetzt zufriedenstellend beantwortet.

Kapitel 8

Homologische Algebra

In diesem Kapitel fixieren wir einen Ring A. Es schadet nicht, sich einen Körper vorzustellen.

Komplexe

Definition 8.1. *Ein Diagramm*

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle k} \\ M_3 & \xrightarrow{g} & M_4 \end{array}$$

von Modulhomomorphismen heißt kommutativ*, falls* $k \circ f = g \circ h$.

Definition 8.2. *Sei* $[n, m] \subset \mathbb{Z}$ *ein Intervall (hierbei ist* $n, m = \infty$ *erlaubt). Ein* Komplex *von Moduln ist ein Folge* M^i *(für* $i \in I$*)von Moduln und Modulhomomorphismen* $d^i : M^i \to M^{i+1}$*, so dass gilt* $d^i \circ d^{i-1} = 0$*. Wir schreiben*

$$M^n \xrightarrow{d^n} M^{n+1} \xrightarrow{d^{n+1}} M^{n+1} \to \cdots \to M^m \ .$$

d^i *heißt* Differential *oder* Randabbildung.

Beispiel. Eine exakte Sequenz ist ein Komplex.

Ein beschränkter Komplex kann durch Ergänzen von Nullen zu einem unbeschränkten Komplex werden. Im folgdenden werden wir daher immer $I = \mathbb{Z}$ betrachten.

Bemerkung. Wir haben aufsteigende (oder kohomologische) Komplexe definiert. Man kann natürlich auch absteigende (oder homologische) Komplexe betrachten. Dann schreibt man die Indizes unten. Die Theorie ist völlig symmetrisch.

Beispiel. Sei X eine glatte Mannigfaltigkeit, $A^p(X)$ seien die glatten Differentialformen auf X. Mit der äußeren Ableitung d bilden diese einen Komplex von $\mathbb{R}$-Vektorräumen der Länge $n = \dim X$.

$$0 \to A^0(X) \to A^1(X) \to A^2(X) \to \cdots \to A^n(X) \to 0 \ .$$

Die Bedingung $d^i \circ d^{i-1} = 0$ bedeutet $\operatorname{Im} d^{i-1} \subset \operatorname{Ker} d^i$.

Definition 8.3. *Sei (M^*, d) ein Komplex. Dann heißen*

$$Z^i(M^*) = \operatorname{Ker} d^i, \qquad B^i(M^*) = \operatorname{Im} d^{i-1}, \qquad H^i(M^*) = Z^i(M^*)/B^i(M^*)$$

*Modul der i-*Zyklen, der *i-*Ränder und *i-*ter Kohomologiemodul *von M^*.*

Es gilt $H^i(M^*) = 0$ für alle i genau dann, wenn der Komplex eine exakte Sequenz ist.

Definition 8.4. *Seien M^* und N^* Komplexe. Ein* Morphismus von Komplexen *ist eine Folge von Modulhomomorphismen $f^i : M^i \to N^i$, so dass die Diagramme*

$$\begin{array}{ccc} M^i & \xrightarrow{d^i} & M^{i+1} \\ {\scriptstyle f^i}\downarrow & & \downarrow{\scriptstyle f^{i+1}} \\ N^i & \xrightarrow{d^i} & N^{i+1} \end{array}$$

kommutieren.

Definition 8.5. *Eine* kurze exakte Sequenz von Komplexen *ist eine Folge von Komplexmorphismen*

$$0 \to M_1^* \to M_2^* \to M_3^* \to 0 \ ,$$

so dass für alle i die induzierte Sequenz von Moduln $0 \to M_1^i \to M_2^i \to M_3^i \to 0$ exakt ist.

Komplexmorphismen induzieren Abbildungen auf den Kohomologiemoduln. Unser wichtigstes Ziel ist der Beweis des folgendes Resultats:

Satz 8.6 (Lange exakte Kohomologiesequenz). *Sei*

$$0 \to M_1^* \to M_2^* \to M_3^* \to 0$$

eine kurze exakte Sequenz von Komplexen. Dann gibt es eine natürliche lange exakte Sequenz von Moduln

$$\cdots \to H^i(M_1^*) \to H^i(M_2^*) \to H^i(M_3^*) \xrightarrow{\delta^i} H^{i+1}(M_1^*) \to H^{i+1}(M_2^*) \to \dots \ .$$

Bemerkung. Kohomologie taucht in vielen verschiedenen Zusammenhängen auf. Stets wird sie durch lange exakte Kohomologiesequenzen berechenbar.

Wir arbeiten uns langsam an den Beweis heran.

Diagrammjagden

Lemma 8.7 (Fünferlemma). *Sei*

$$\begin{array}{ccccccccc}
M_1 & \xrightarrow{k} & M_2 & \xrightarrow[h]{} & M_3 & \xrightarrow{g} & M_4 & \xrightarrow{l} & M_5 \\
\downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\
N_1 & \xrightarrow{k} & N_2 & \xrightarrow[h']{} & N_3 & \xrightarrow[g']{} & N_4 & \xrightarrow[l']{} & N_5
\end{array}$$

ein kommutatives Diagramm mit exakten Zeilen. Sind f_2 und f_4 Isomorphismen, f_1 surjektiv und f_5 injektiv, dann ist f_3 ein Isomorphismus.

Bemerkung. Oft betrachtet man den Spezialfall $M_1 = N_1 = M_5 = N_5 = 0$, also einen Morphismus von kurzen exakten Sequenzen.

Beweis: Es empfiehlt sich, die Elemente in das Diagramm hineinzuschreiben. Sei $x_3 \in \operatorname{Ker} f_3$. Es folgt $f_4 g x_3 = g' f_3 x_3 = 0$, also liegt $g x_3$ im Kern der injektiven Abbildung f_4. Dies bedeutet $x_3 \in \operatorname{Ker} g = \operatorname{Im} h$. Sei x_2 ein Urbild. Wegen $h' f_2 x_2 = f_3 h x_2 = f_3 x_3 = 0$ gilt $f_2 x_2 \in \operatorname{Ker} h' = \operatorname{Im} k'$. Sei $y_1 \in N_1$ ein Urbild. Da die Abbildung f_1 surjektiv ist, gibt es ein Urbild x_1 ein M_1. Wegen $f_2 k x_1 = k' f_1 x_1 = k' y_1 = f_2 x_2$ und der Injektivität von f_2 folgt $k x_1 = x_2$. Es folgt $hk x_1 = h x_2 = x_3$. Wegen $h \circ k = 0$ ist also $x_3 = 0$, d.h. $\operatorname{Ker} f_3 = 0$.
Sei nun $y_3 \in M_3$. Sei $y_4 = h' y_3$. Wegen der Surjektivität von f_4 hat y_4 ein Urbild x_4. Es gilt $f_5 l x_4 = l' f_4 x_4 = l' y_4 = l' h' y_3 = 0$, da $l' h' = 0$. Da f_5 injektiv ist, folgt $l x_4 = 0$, d.h. $x_4 \in \operatorname{Ker} l = \operatorname{Im} g$. Sei x_3 ein Urbild von x_4. Wir betrachten $y_3 - f_3 x_3$. Es gilt $g' y_3 - g' f_3 x_3 = g' y - f_4 g x_3 = g' y - f_4 x_4 = 0$, d.h.

$$y_3 - f_3 x_3 \in \operatorname{Ker} g' = \operatorname{Im} h' \ .$$

Sei y_2 ein Urbild. Wegen der Bijektivität von f_2 gibt es hiervon ein Urbild x_2 in M_2. Es folgt

$$(y_3 - f_3 x_3) - f_3 h x_2 = (y_3 - f_3 x_3) - h' f_2 x_2 = (y_3 - f_3 x_3) - h' y_2 = 0 \ .$$

Damit liegt y_3 im Bild von f_3. □

Beweise dieser Art nennt man auch Diagrammjagden. Wir kommen gleich zu einem noch umfangreicheren Fall.
Wir tragen eine Definition nach:

Definition 8.8. *Sei $f : M \to N$ ein Modulhomomorphismus. Dann heißt*

$$\operatorname{Coker}(f) = N / f(M)$$

Kerkern *von f.*

Satz 8.9 (Schlangenlemma). *Wir betrachten ein kommutatives Diagram*

$$\begin{array}{ccccccc} & & M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 \longrightarrow 0 \\ & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} \\ 0 & \longrightarrow & N_1 & \xrightarrow{f'} & N_2 & \xrightarrow{g'} & N_3 \end{array}$$

mit exakten Zeilen. Dann ist der Verbindungshomomorphismus

$$\delta = f'^{-1} \circ d_2 \circ g^{-1} : \operatorname{Ker} d_3 \to \operatorname{Coker} d_2$$

ein wohldefinierter Modulhomomorphismus, und wir haben eine exake Sequenz

$$\operatorname{Ker} d_1 \xrightarrow{f} \operatorname{Ker} d_2 \xrightarrow{g} \operatorname{Ker} d_3 \xrightarrow{\delta} \operatorname{Coker} d_1 \xrightarrow{f'} \operatorname{Coker} d_2 \xrightarrow{g'} \operatorname{Coker} d_3 \ .$$

Bemerkung. Der Beweis ist nicht schwer - nur lang. Auch hier gilt: selbermachen ist einfacher als nachvollziehen.

Beweis: Wir beginnen mit einer Präzisierung der Definition von δ. Sei $z_3 \in \operatorname{Ker} d_3 \subset M_3$. Nach Voraussetzung ist die Abbildung g surjektiv, also existiert ein Urbild v_2 in M_2. Nun betrachten wir $d_2(v_2) \in N_2$. Wegen der Kommutativität des rechten Quadrats gilt

$$g' d_2(v_2) = d_3 g(v_2) = d_3(z_3) = 0 \ .$$

Also gilt $d_2(v_2) \in \operatorname{Ker} g' = \operatorname{Im} f'$. $\delta(z_3)$ wird definiert durch ein Urbild von $d_2(v_2)$ in N_1.

Behauptung. $\delta(z_3) \in \operatorname{Coker} d_1$ *ist unabängig von Wahlen.*

Nach Voraussetzung ist f' injektiv, also hängt $\delta(z_3)$ nur von der Wahl von v_2 ab. Sei also v_2' eine andere Wahl. Dann gilt $v_2 - v_2' \in \operatorname{Ker} g = \operatorname{Im} f$. Sei w_1 ein Urbild in M_1. Wegen der Kommutativität des linken Quadrats gilt

$$f' d_1 w_1 = d_2 f w_1 = d_2(v_2 - v_2') \Rightarrow d_1 w_1 = f'^{-1}(d_2(v_2)) - f'^{-1}(d_2(v_2')) \ .$$

Also ist $f'^{-1}(d_2(v_2)) = f'^{-1}(d_2(v_2'))$ in $N_1 / \operatorname{Im} d_1$.

Behauptung. δ *ist ein Modulhomomorphismus.*

Seien $z_3, z_3' \in \operatorname{Ker} d_3$, v_2 und v_2' die Urbilder in M_2. Wir wählen $v_2 + v_2'$ als Urbild von $z_3 + z_3'$. Da d_2 und f' Modulhomomorphismen sind, gilt

$$\delta(z_3) + \delta(z_3') = f'^{-1} d_2(v_2) + f'^{-1} d_2(v_2') = f'^{-1} d_2(v_2 + v_2') = \delta(Z_3 + z_3') \ .$$

Das analoge Argument funktioniert auch für skalare Vielfache.

Behauptung. *Alle Abbildungen der Sequenz aus dem Schlangenlemma sind wohldefiniert.*

Wir betrachten $\operatorname{Ker} d_1 \to M_1 \xrightarrow{f} M_2$. Sei $x_1 \in \operatorname{Ker} d_1$. Wegen der Kommutativität des ersten Quadrates ist $d_2 f x_1 = f' d_1 x = f' 0 = 0$, also $f(x_1) \in \operatorname{Ker} d_2$. Umgekehrt betrachten wir $N_1 \to N_2 \to \operatorname{Coker} d_2$. Sei $y_1 \in \operatorname{Im} d_1$, also $y_1 = d_1 x_1$ für ein $x_1 \in M_1$. Dann gilt $f' y_1 = f' d_1 x_1 = d_2 f x_1$, also $f' y_1 = 0$ in $\operatorname{Coker} d_2$. Dann faktorisiert $N_1 \to \operatorname{Coker} d_2$ über $N_1 / \operatorname{Im} d_1$.
Dasselbe Argument zeigt, dass $\operatorname{Ker} d_2 \to M_2 \xrightarrow{g} M_3$ über $\operatorname{Ker} d_3$ faktorisiert und $N_2 \to N_3 \to \operatorname{Coker} d_3$ über $\operatorname{Coker} d_3$.
Nun muss Exaktheit an jeder Stelle der Sequenz verifiziert werden. Wir zeigen jeweils zuerst die Inklusion Im $\subset$ Ker (d.h. die Verknüpfung der beiden Abbildungen ist null), danach die umgekehrte.

Behauptung. $\operatorname{Ker} d_1 \to \operatorname{Ker} d_2 \to \operatorname{Ker} d_3$ *ist exakt.*

Sei $x_1 \in \operatorname{Ker} d_1 \subset M_1$. Dann ist $gfx_1 = 0$ in M_3, also auch $fgx_1 = 0$ in $\operatorname{Ker} d_3$. Sei umgekehrt

$$y_2 \in \operatorname{Ker}(g : \operatorname{Ker} d_2 \to \operatorname{Ker} d_3) \subset \operatorname{Ker}(g : M_2 \to M_3) \ .$$

Nach Vorraussetzung gibt es ein Urbild $x_1 \in M_1$. Es folgt $f' d_1 x_1 = d_2 f x_1 = d_2 y_2 = 0$, da $y_2 \in \operatorname{Ker} d_2$. Die Abbildung f' ist injektiv, also folgt $d_1 x_1 = 0$. Damit gilt $y_2 \in \operatorname{Im}(f : \operatorname{Ker} d_1 \to \operatorname{Ker} d_2)$.

Behauptung. $\operatorname{Ker} d_2 \to \operatorname{Ker} d_3 \to \operatorname{Coker} d_1$ *ist exakt.*

Sei zunächst $y_2 \in \operatorname{Ker} d_2$ und $z_3 = g y_2$. Dann ist

$$\delta(z_3) = f'^{-1} d_2(y_2) = f^{-1} 0 = 0.$$

Umgekehrt sei $z_3 \in \operatorname{Ker} \delta$. Sei y_2 ein Urbild von z_3 in M_2. Es ist also $0 = \delta(z_3) = f'^{-1} d_2 y_2$. Wegen der Injektivität von f' folgt $d_2 y_2 = 0$, d.h. $y_2 \in \operatorname{Ker} d_2$. Dies ist das gesuchte Urbild.

Behauptung. $\operatorname{Ker} d_3 \to \operatorname{Coker} d_1 \to \operatorname{Coker} d_2$ *ist exakt.*

Sei $z_3 \in \operatorname{Ker} d_3$ und $\delta(z_3) = f'^{-1} d_2(y_2)$ für ein Urbild $y_2 \in M_2$. Dann gilt $f' \delta(z_3) = d_2(y_2) = 0$ in $\operatorname{Coker} d_2$. Sei umgekehrt $\overline{v}_1 \in \operatorname{Ker}(f' : \operatorname{Coker} d_1 \to \operatorname{Coker} d_2)$. Sei $v_1 \in N_1$ ein Repräsentant von $\overline{v}_1$. Es gilt $f'(v_1) \in \operatorname{Im} d_1$. Sei also y_2 das Urbild in M_2 und $z_3 = g(y_2)$. Dann ist $\delta(z_3) = f' - 1 d_2 y_2 = f'^{-1} f'(v_1) = v_1$ das gesuchte Urbild.

Behauptung. $\operatorname{Coker} d_1 \to \operatorname{Coker} d_2 \to \operatorname{Coker} d_3$ *ist exakt.*

Sei $\overline{x}_1 \in \operatorname{Coker} d_1$ und $x_1 \in N_1$ ein Repräsentant. Dann ist $g' f' x_1 = 0$, also auch $g' f' \overline{x}_1 = 0$ in $\operatorname{Coker} d_3$. Sei umgekehrt $\overline{w}_2 \in \operatorname{Ker}(g' : \operatorname{Coker} d_2 \to \operatorname{Coker} d_3)$, $w_2 \in N_2$ ein Repräsentant. Wir betrachten $g'(w_2)$. Dieses Element verschwindet in $N_3 / \operatorname{Im} d_3$, liegt also in $\operatorname{Im} d_3$. Sei z_3 ein Urbild in M_3, y_2 ein Urbild in M_2. Wir betrachten $w_2 - d_2 y_2 \in M_2$. Dieses Element liegt im Kern von g', denn

$$g' w_2 - g' d_2 y_2 = g' w_2 - d_3 g y_2 = g' w_2 - d_3 z_3 = g' w_2 - g' w_2 = 0 \ .$$

Sei $x_1 \in N_1$ das Urbild. Dann gilt

$$f'(\overline{x}_1) = w_2 - d_2 y_2 = \overline{w}_2 \in \operatorname{Coker} d_2 \ .$$

□

Korollar 8.10. *Sei*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von kurzen exakten Sequenzen. Mit je zweien der Abbildungen d_1, d_2, d_3 ist auch die dritte ein Isomorphismus.

Beweis: Das Fünferlemma (8.7) enthält den Schluss von d_1 und d_3 auf d_2. Seien nun d_1 und d_2 Isomorphismen. Wir wenden das Schlangenlemma an. Die Sequenz reduziert sich zu

$$0 \xrightarrow{f} 0 \xrightarrow{g} \operatorname{Ker} d_3 \xrightarrow{\delta} 0 \xrightarrow{f'} 0 \xrightarrow{g'} \operatorname{Coker} d_3$$

Dann muss auch $\operatorname{Ker} d_3 = 0$ sein. Außerdem ist die Abbildung $M_2 \to N_2 \to N_3$ surjektiv, also auch wenn man sie als $M_2 \to M_3 \to N_3$ auffasst. Dann muss auch d_3 surjektiv sein. Der letzte Fall ist völlig analog. □

Die eigentliche Anwendung des Schlangenlemmas ist aber die lange exakte Kohomologiesequenz. Dafür brauchen wir noch etwas Terminologie.

Die lange exakte Kohomologiesequenz

Beweis von 8.6: Wir betrachten einen Ausschnitt der exakten Sequnze von Komplexen Diagramm

$$\begin{array}{ccccccccc} & & \downarrow{\scriptstyle d_1^{i-1}} & & \downarrow{\scriptstyle d_2^{i-1}i} & & \downarrow{\scriptstyle d_3^{i-1}} & & \\ 0 & \longrightarrow & M_1^i & \longrightarrow & M_2^i & \longrightarrow & M_3^i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1^i} & & \downarrow{\scriptstyle d_2^i} & & \downarrow{\scriptstyle d_3^i} & & \\ 0 & \longrightarrow & M_1^{i+1} & \longrightarrow & M_2^{i+1} & \longrightarrow & M_3^{i+1}i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1^{i+1}} & & \downarrow{\scriptstyle d_2^{+1}i} & & \downarrow{\scriptstyle d_3^{i+1}} & & \end{array}$$

Wegen $B^i(M_j^*) \subset \operatorname{Ker} d_j^i$ und $\operatorname{Im} d_j^i \subset \operatorname{Ker} Z^{i+1}(M_j^*)$ induziert dies das kommutative Diagramm

$$\begin{array}{ccccccccc} & & M_1^i/B^i(M_1^*)^* & \longrightarrow & M_2^i/B^i(M_2^*) & \longrightarrow & M_3^i/B^i(M_3^*) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1^i} & & \downarrow{\scriptstyle d_2^i} & & \downarrow{\scriptstyle d_3^i} & & \\ 0 & \longrightarrow & Z^{i+1}(M_1^*) & \longrightarrow & Z^{i+1}(M_2^*) & \longrightarrow & Z^{i+1}(M_3^*) & & \end{array}$$

Die Surjektivität von $M_2^i/B^i(M_2^*) \to M_3^i/B^i(M_3^*)$ folgt aus der Surjektivität von $M_2^i \to M_3^i$. Die Exaktheit der ersten Zeile an den anderen Stellen folgt aus dem Schlangenlemma für d^{i-1}, Die Injektivität von $Z^{i+1}(M_1^*)@>>>Z^{i+1}(M_2^*)$ folgt aus der Injektivität von $M_1^{i+1} \to M_2^{i+1}$. Die Exaktheit der zweiten Zeile an den anderen Stelle ist im Schlangenlemma für d^{i+1} enthalten. Nun werden das Schlangenlemma anwenden. Es gilt

$$\begin{aligned}\operatorname{Ker}(d_j^i : M_j^i/B^i(M_j^*)^* \to Z^{i+1}(M_j^*)) &= Z^i(M_j^*)/B^i(M_j^*) = H^i(M_j^*)\\ \operatorname{Coker}(d_j^i : M_j^i/B^i(M_j^*)^* \to Z^{i+1}(M_j^*)) &= Z^{i+1}(M_j^*)/B^{i+1}(M_j^*) = H^{i+1}(M_j^*)\end{aligned}$$

Damit ist die Sequenz des Schlangenlemmas

$$H^i(M_1^*) \to H^i(M_2^*) \to H^i(M_3^*) \xrightarrow{\delta} H^{i+1}(M_1^*) \to H^{i+1}(M_2^*) \to H^{i+1}(M_3^*) \ .$$

Setzt man diese Sequenzen für alle $i \in \mathbb{Z}$ zusammen, so erhält man die lange exakte Kohomologiesequenz. □

Homotopien

Definition 8.11. *Eine* Homotopie von Komplexenmorphismen $f^*, g^* : M^* \to N^*$ *ist eine Folge von Modulhomomorphismen* $h^i : M^i \to N^{i-1}$*, so dass*

$$f^i - g^i = d^{i-1} \circ h^i + h^{i+1} \circ d^i \ .$$

Wir schreiben $f^* \sim_{h^*} g^*$.

Beispiel. Sei $\phi : X \to Y$ eine unendlich oft differenzierbare Abbildung von glatten Mannigfaltigkeiten. Dann induziert das Zurückziehen von Differentialformen $\omega_Y \mapsto \phi^*\omega_Y$ einen Komplexmorphismus $\Omega^*(Y) \to \Omega^*(X)$. Ein Isomorphismus von Mannigfaltigkeiten induziert einen Isomorphismus von Komplexesn.

Lemma 8.12. *Homotopie von Morphismen ist eine Äquivalenzrelation. Homotope Morphismen induzieren diesselbe Abbildung auf der Kohomologie.*

Beweis: Die Nullabbildung ist eine Homotopie von f^* nach f^*. Aus $f^* \sim_{h^*} g^*$ folgt $g^* \sim_{-h^*} f^*$. Sei $f_1^* \sim_{h^*} f_2^*$ und $f_2^* \sim_{k^*} f_3^*$. Dann ist

$$f_1^i - f_2^* + f_2^i - f_3^i = d^{i-1} \circ h^i + h^{i+1} \circ d^i + d^{i-1} \circ k^i + k^{i+1} \circ d^i \ .$$

Also gilt $f_1^* \sim_{h^*+k^*} f_3$.
Seien $f^* \sim_{h^*} g^* : M^* \to N^*$. Wir betrachten $\overline{x} \in H^i(M^*)$. Sei $x \in Z^i(M^*)$ ein Repräsentant. Dann gilt

$$\begin{aligned}H^i(f^*)(\overline{x}) - H^i(g^*)(\overline{x}) = f^i(x) - g^i(x) = d^{i-1}h^i(x) + h^{i+1} \circ d^i(x) = d^{i-1}h^i(x)\\ = 0 \in H^i(N^*)\end{aligned}$$

wegen $x \in \operatorname{Ker} d^i$ und $H^i(N^*) = Z^i(N^*)/\operatorname{Im} d^{i-1}$. □

Kapitel 9

Kategorien und Funktoren

Beispiel. Es gibt die Kategorie der Mengen, der Körper, der K-Vektorräume, der A-Moduln, der topologischen Räume, der Mannigfaltigkeiten, der Komplexe von A-Moduln,...

Definition 9.1. *Eine* Kategorie $\mathcal{C}$ *besteht aus einer Klasse von* Objekten $\mathrm{Ob}(\mathcal{C})$*, für je zwei Objekte* $A, B \in \mathrm{Ob}(\mathcal{C})$ *einer Menge von* Morphismen $\mathrm{Mor}_C\, h(A, B)$*, für je drei Objekte* A, B, C *einer Abbildung*

$$\circ : \mathrm{Mor}_{\mathcal{C}}(B, C) \times \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(A, C) \ ,$$

für jedes Objekt ein ausgezeichneter Morphismus $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$*, so dass folgende Axiome erfüllt sind:*

(i) $\mathrm{id}_A \in \mathrm{Mor}_{\mathcal{C}}(A, A)$ *operiert als Links- und Rechtsneutrales Element für die Komposition von Morphismen.*

(ii) Die Komposition ist assoziativ, d.h. für $f \in \mathrm{Mor}_{\mathcal{C}}(A, B)$*,* $g \in \mathrm{Mor}(B, C)$ *und* $h \in \mathrm{Mor}_{\mathcal{C}}(C, D)$ *gilt*

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

Beispiel. S. o. Die Morphismen sind Abbildungen, Körperhomomorphismen, lineare Abbildungen, Modulhomomorphismen, stetige Abbildungen, differenzierbare Abbildungen, Komplexhomomorphismen.

(i) glatte Mannigfaltigkeiten mit differenzierbaren Abbildungen

(ii) affine Varietäten mit regulären Abbildungen

(iii) ...

Exotischere Beispiele:

(i) Sei G eine Gruppe. Dann erhalten wir eine Kategorie mit einem Objekt, genannt $*$ und $\mathrm{Mor}_{\mathcal{C}}(*, *) = G$. Die Verknüpfung ist das Gruppengesetz, die Identität ist das neutrale Element.

(ii) Sei X ein topologischer Raum. Wir erhalten eine Kategorie mit Objekten die offenen Teilmengen von X und Morphismen die Inklusionen. In diesem Fall hat $\mathrm{Mor}(U, U')$ entweder genau ein oder gar kein Element.

(iii) Sei $(I, \leq)$ eine partiell geordnete Menge. Dann erhält man eine Kategorie mit $\mathrm{Ob}(\mathcal{C}) = I$ und $\mathrm{Mor}(i, j)$ hat genau ein Element, falls $i \leq j$, und ist $\emptyset$ andernfalls. Der Fall des topologischen Raums ist ein Sonderfall.

Definition 9.2. *Ein* kovarianter (kontravarianter) Funktor $F : \mathcal{C} \to \mathcal{C}$ *zwischen zwei Kategorien* $\mathcal{C}$ *und* $\mathcal{D}$ *ordnet jedem Objekt* $A \in \mathrm{Ob}(\mathcal{C})$ *ein Objekt* $F(A) \in \mathrm{Ob}(\mathcal{D})$ *zu und jedem Morphismus* $f : A \to B$ *in* $\mathcal{C}$ *einen Morphismus* $F(f) : F(A) \to F(B)$ *(bzw.*$F(f) : F(B) \to F(A)$*), so dass gilt*

$$f = g \circ h \in \mathcal{C} \Rightarrow F(f) = F(g) \circ F(h) \in \mathcal{D}$$

(bzw. $F(f) = F(h) \circ F(g)$ *in* $\mathcal{D}$*) und* $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.

Beispiel. (i) Der Vergissfunktor von der Kategorie der Gruppen in die Kategorie der Mengen: einer Gruppe wird die zugrundeliegende Menge zugeordnet. Ebenso gibt es Vergissfunktoren von A-Moduln nach Gruppen oder Mengen, von Mannigfaltigkeiten in topologische Räume etc.

(ii) Sei $A \to B$ ein Ringhomomorphismus. Dann gibt es den Restriktionsfunktor von B-Moduln nach A-Moduln und die Koeffizientenerweiterung $M \mapsto M \otimes_A B$ von A-Moduln nach B-Moduln. (Vergleiche Satz 1.17).

(iii) Sei A ein Ring, M ein A-Modul. Dann sind $\cdot \otimes_A M$ und $\mathrm{Hom}_A(\cdot, M)$ kovariante Funktoren von der Kategorie der A-Moduln in sich selbst. $\mathrm{Hom}_A(M, \cdot)$ ist kontravariant.

(iv) Es gibt einen Funktor von Integritätsringen nach Körpern, der jeden Integritätsring seinen Quotientenkörper zuordnet.

(v) Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dies definiert einen kovarianten Funktor zwischen den zugeordenten Kategorien. Eine kontravariante Variante erhält man durch $g \mapsto g^{-1}$.

(vi) De Rham-Kohomologie definiert einen kontravarianten Funktor von Mannigfaltigkeiten in reele Vektorräume. (Vergleiche das Beispiel nach Definition 8.4).

(vii) In der Galoistheorie studiert man den Funktor von der Kategorie der Zwischenkörper von L/K (Morphismen die Inklusionen) in Untergruppen von $\mathrm{Gal}(L/K)$ (Morphismen ebenfalls Inklusionen). Er ist kontravariant.

(viii) Eine Riemannsche Fläche ist eine eindimensionale komplexe Mannigfaltigkeit. Es gibt einen Funktor von kompakten Riemannschen Flächen in die Kategorie der endlichen Erweiterungen von $\mathbb{C}(t)$, der der Riemannschen Fläche den Körper der meromorphen Funktionen auf X zuordnet. Ist etwa $E = \mathbb{C}/\Gamma$ eine elliptische Kurve, so ist $\mathcal{M}(E)$ der Körper der

elliptischen Funktionen. Er ist isomorph zu $\mathbb{C}(t)[X]/X^2 = 4t^3 - g_2t^2 - t$, wie die Theorie der Weierstrassschen P-Funktion zeigt.

Ein Beispiel ist besonders wichtig:

Lemma 9.3. *Sei $\mathcal{C}$ eine Kategorie, A ein Objekt. Dann erhalten wir Funktoren von $\mathcal{C}$ in die Kategorie der Mengen durch*

$$B \mapsto \mathrm{Mor}_{\mathcal{C}}(A, B),$$
$$B \mapsto \mathrm{Mor}_{\mathcal{C}}(B, A).$$

Der erste ist kovariant, der zweite kontravariant.

Beweis: Auf Objekten haben wir die Funktoren angegeben. Sei nun $f : B \to B'$ ein Morphismus. Verknüpfen mit f definiert Abbildungen

$$f_* : \mathrm{Mor}_{\mathcal{C}}(A, B) \to \mathrm{Mor}_{\mathcal{C}}(A, B') \ , \ f^* : \mathrm{Mor}_{\mathcal{C}}(B, A) \to \mathrm{Mor}_{\mathcal{C}}(B', A) \ .$$

Man sieht sofort, dass $f_* \circ g_* = (f \circ g)_*$ und $f^* \circ g^* = (f \circ g)^*$. □

Man ist versucht die Kategorie der Kategorien zu definieren: Objekte sind Kategorien, Morphismen sind Funktoren. Die Idee ist nicht falsch, führt aber in mengentheoretische Schwierigkeiten.

Definition 9.4. *Seien $F, G : \mathcal{C} \to \mathcal{D}$ Funktoren. Eine* Transformation von Funktoren*η ist eine Klasse von Morphismen $\eta(A) : F(A) \to G(A)$ für alle Objekte A aus $\mathcal{C}$, so dass für alle $f : A \to B$ das Diagramm*

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta(A)} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow{\eta(B)} & G(B) \end{array}$$

kommutiert. η heißt Äquivalenz von Funktoren*, falls alle $\eta(A)$ bijektiv sind. Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heißt* Kategorienäquivalenz*, falls es einen Funktor $G : \mathcal{D} \to \mathcal{C}$ gibt, so dass $F \circ G$ und $G \circ F$ Äquivalent zum identischen Funktor auf $\mathcal{D}$ bzw. $\mathcal{C}$ sind.*

Beispiel. (i) Sei A ein Ring, $S \subset A$ eine multiplikative Teilmenge. Dann sind die Funktoren $M \mapsto S^{-1}M$ und $M \mapsto M \otimes_A S^{-1}A$ von A-Moduln nach $S^{-1}A$-Moduln äquvivalent (vergleiche Lemma 1.22).

(ii) Sei L/K eine endliche Galoiserweiterung. Dann ist der Funktor von Zwischenkörpern zu Untergruppen von $\mathrm{Gal}(L/K)$ eine Kategorienäquivalenz (Hauptsatz der Galoistheorie).

(iii) Sei $f : A \to A'$ ein Morphismus in $\mathcal{C}$. Dann induziert Verknüpfen mit f eine Transformation von Funktoren $f_* : \mathrm{Mor}_{\mathcal{C}}(\cdot, A) \to \mathrm{Mor}_{\mathcal{C}}(\cdot, A')$.

(iv) Der Funktor von kompakten Riemannschen Flächen nach endlichen Erweiterungen von $\mathbb{C}(t)$ ist eine Kategorienäuivalenz (nicht so ganz trivial!).

Bemerkung. In vielen Beispielen vernachlässigt man die Morphismen völlig. Man gibt etwa nur an, was mit den Objekten geschieht. Dies gibt einen falschen Eindruck! Objektiv gesehen steckt alle Information in den Morphismen.

Definition 9.5. *Sei $F : \mathcal{C} \to \underline{Sets}$ ein kontravianter Funktor, A ein Objekt von $\mathcal{C}$. Wir sagen, dass F durch A* dargestellt *wird, falls F äquivalent zu* $\mathrm{Mor}_{\mathcal{C}}(\cdot, A)$.

Man kann oft Funktoren benutzen, um Objekte zu definieren.

Satz 9.6 (Yoneda Lemma). *Falls F darstellbar ist, dann ist das darstellende Objekt eindeutig bis auf eindeutigen Isomorphismus. Seien F, F' darstellbare Funktoren. Dann gibt es eine natürliche Bijektivon zwischen Transformationen $F \to F'$ und Morphismen $A' \to A$ der darstellenden Objekte.*

Beweis: Wir beginnen mit der Aussage über Transformationen. Seien $\eta : F \to \mathrm{Mor}_{\mathcal{C}}(\cdot, A)$ und $\eta' : F' \to \mathrm{Mor}_{\mathcal{C}}(\cdot, A')$ die Äquivalenzen von Funktoren. Gegeben sei $f : A \to A'$. Dann ist $\theta(f) = (\eta')^{-1} \circ f_* \circ \eta : F \to F'$ eine Transformation von Funktoren. Umgekehrt induziert $\theta : F \to F'$ eine Transformation $\tilde{\theta} : \mathrm{Mor}_{\mathcal{C}}(\cdot, A) \to \mathrm{Mor}_{\mathcal{C}}(\cdot, A')$. Dann ist $\tilde{\theta}(A) : \mathrm{Mor}_{\mathcal{C}}(A, A) \to \mathrm{Mor}_{\mathcal{C}}(A, A')$. Sei $f = \tilde{\theta}(A)(\mathrm{id}_A) : A \to A'$.

Behauptung. $f_* = \tilde{\theta}$.

Sei B ein beliebiges Objekt, $g : B \to A$. Da $\tilde{\theta}$ eine Transformation von Funktoren ist, gilt

$$\begin{array}{ccc} \mathrm{Mor}_{\mathcal{C}}(B, A) & \xrightarrow{\tilde{\theta}(B)} & \mathrm{Mor}_{\mathcal{C}}(B, A') \\ {\scriptstyle g^*}\uparrow & & \uparrow{\scriptstyle g^*} \\ \mathrm{Mor}_{\mathcal{C}}(A, A) & \xrightarrow{\tilde{\theta}(A)} & \mathrm{Mor}_{\mathcal{C}}(A, A') \end{array}$$

Es gilt $g = g \circ \mathrm{id}_A = g^*(\mathrm{id}_A)$. Aus dem Diagramm lesen wir also $\tilde{\theta}(B)(g) = g^*(\tilde{\theta}(A)(\mathrm{id}_A)) = g^*(f)$ ab. Wegen $g^*(f) = g \circ f = f_*(g)$ ist dies die Behauptung. Sei nun F ein darstellbarer Funktor, A und A' seien darstellende Objekte. Dann induziert die identische Transformation $F \to F$ einen Morphismus $A \to A'$, die Umkehrung einen Morphismus $A' \to A$ und die beiden sind zueinander invers. □

Beispiel. Dieses völlig abstrakte Lemma haben wir schon konkret bei der Definition des Tensorproduktes benutzt. Dort handelte es sich um die Kategorie der A-Moduln. Für festes M, N wurde der Funktor

$$\mathrm{Mor}_{\mathrm{bilin}}(M \times N, \cdot)$$

betrachtet. Er wurde dargestellt durch $M \otimes_A N$. (Es handelt sich um einen kovarianten Funktor, nicht um einen kontravarianten).

Kapitel 10

Ext und Tor

Sei A ein fester Ring (kommutativ mit Eins), $\mathcal{A}$ die Kategorie der A-Moduln. Sei M ein fester A-Modul. Wir betrachten Funktoren

$$\mathrm{Hom}_A(M,\cdot), \mathrm{Hom}_A(\cdot,M), M\otimes\cdot : \mathcal{A}\to\mathcal{A}$$

Lemma 10.1. $\mathrm{Hom}_A(M,\cdot)$ *und* $M\otimes\cdot$ *sind kovariante Funktoren,* $\mathrm{Hom}_A(\cdot,M)$ *ist ein kontravarianter Funktor. Dabei sind* $\mathrm{Hom}_A(\cdot,M)$ *und* $M\otimes\cdot$ *rechtsexakt, d.h. für jede kurze exakte Sequenz*

$$0\to N_1\to N_2\to N_2\to 0$$

sind

$$M\otimes N_1\to M\otimes N_2\to M\otimes N_3\to 0$$
$$\mathrm{Hom}_A(N_3,M)\to\mathrm{Hom}_A(N_2,M)\to\mathrm{Hom}_A(N_1,M)\to 0$$

exakt. $\mathrm{Hom}_A(M,\cdot)$ *ist linksexakt, d.h. die Sequenz*

$$0\to\mathrm{Hom}_A(M,N_1)\to\mathrm{Hom}_A(M,N_2)\to\mathrm{Hom}_A(M,N_3)$$

ist exakt.

Beweis: Wir behandeln exemplarisch den Fall $\mathrm{Hom}_A(M,\cdot)$. Ist $f:N\to N'$ ein Homomorphismus, so ist

$$f^*:\mathrm{Hom}_A(M,N)\to\mathrm{Hom}_A(M,N') \qquad g\mapsto f\circ g$$

ebenfalls ein Homorphismus (nachrechnen) und definiert die kovariante Funktorialität (ebenfalls nachrechnen). Sei nun eine kurze exakte Sequenz wie im Lemma gegeben. Wir betrachten die induzierte Sequenz

$$0\to\mathrm{Hom}_A(M,N_1)\to\mathrm{Hom}_A(M,N_2)\to\mathrm{Hom}_A(M,N_3)$$

Wegen Funktorialität und $f^*(0)=0$ (Homomorphismus!) ist dies ein Komplex. Wir überprüfen die umkehrten Inklusionen.

Sei $f_1 : M \to N_1$. Angenommen, die Komposition

$$M \xrightarrow{f_1} N_1 \subset N_2$$

ist null. Dann ist auch $f_1 = 0$.
Sei $f_2 : M \to N_2$, so dass die Komposition

$$M \xrightarrow{f_2} N_2 \xrightarrow{d} N_3$$

verschwindet. Dann gilt $f_2(M) \subset \operatorname{Ker} d = N_1$. D.h. f_2 faktorisiert über $f_2 : M \to N_1$.
Die Rechnungen für $\operatorname{Hom}_A(\cdot, M)$ sind völlig analog. Die Aussage für $\otimes$ überprüft man am leichtesten über die universelle Eigenschaft. □

Lemma 10.2. *Sei F ein freier A-Modul. Dann sind $\operatorname{Hom}_A(F, \cdot)$ und $F \otimes \cdot$ exakt, d.h. kurze exakte Seqenzen werden auf kurze exakte Sequenzen abgebildet.*

Beweis: Nach Definition ist $F = \bigoplus_{i \in I} A$. Dann ist

$$\operatorname{Hom}_A(bigoplus_{i \in I} A, N) = \prod_{i \in I} \operatorname{Hom}_A(A, N) \cong \prod N$$

$$\left(\bigoplus_{i \in I} A \right) \otimes N = \bigoplus_{i \in I} A \otimes N \cong \bigoplus_{i \in I} N$$

(universelle Eigenschaft von $\bigoplus$, $f \mapsto f(1)$; Eigenschaft von $\otimes$) Beide Funktoren sind offensichtlich exakt. □

Definition 10.3. *Sei M ein A-Modul. Eine* freie Auflösung *von M ist ein Komplex*

$$\ldots F_n \to F_{n-1} \to \cdots \to F_0 \to 0$$

zusammen mit einer Abbildung $F_0 \to M$, so dass

$$\ldots F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

exakt ist. Sei $f : M \to M'$ ein Homomorphismus. Ein Morphismus von Auflösungen über *f ist ein Komplexmorphismus $F_* \to F'_*$, so dass das Diagramm*

$$\begin{array}{ccc} F_0 & \longrightarrow & M \\ \downarrow & & \downarrow f \\ F'_0 & \longrightarrow & M' \end{array}$$

kommutiert.

Beispiel. Wenn M selbst frei ist, so ist

$$0 \cdots \to 0 \to M \to 0$$

eine freie Auflösung mit Strukturabbildung die Identität. Ist A nullteilerfrei, $M = A/(f)$ für $f \neq 0$, so ist

$$0 \to A \xrightarrow{f\cdot} A \to 0$$

eine freie Aulösung, den Multiplikation mit f ist injektiv und das Bild (f).

Satz 10.4. *(i) Jeder Modul hat eine frei Auflösung.*

(ii) Sei $f : M \to M'$ ein Homomorphismus, F_* und F'_* freie Auflösungen von M und M'. Dann existiert ein Morphismus von Auflösungen über f.

(iii) Je zwei Homomorphismen von Auflösungen sind homotop.

Beweis: Sei $I \subset M$ ein Erzeugendensystem. Dann setzen wir $F_0(M) = \bigoplus_{i\in I} A$. Nach Konstruktion gibt es eine natürliche, surjektive Abbildung $F_0(M) \to M$. Sei M_1 der Kern dieser Abbildung. Wir setzen dann $F_1(M) = F_0(M_1)$. Dann ist die Sequenz

$$F_1(M) \to F_0(M) \to M \to 0$$

exakt. Dieses Verfahren setzen wir jeweils nach links fort.
Für den Beweis von (ii) betrachten wir die surjektive Abbildung $F'_0 \to M$. Da $\mathrm{Hom}(F_0, \cdot$ exakt ist, ist dann auch

$$\mathrm{Hom}(F_0, F'_0) \to \mathrm{Hom}(F_0, M')$$

surjektiv. Daher hat die Abbildung $F_0 \to M \to M'$ ein Urbild $f_0 : F_0 \to F'_0$. Dies bedeutet gerade, dass das Diagram

$$\begin{array}{ccccc} F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{d_0} & M \\ & & \downarrow & & \downarrow \\ & \longrightarrow & F'_0 & \xrightarrow{d'_0} & M' \end{array}$$

kommutiert. F_1 ist frei, daher ist die Sequenz

$$\mathrm{Hom}(F_1, F'_1) \to \mathrm{Hom}(F_1, F'_0) \to \mathrm{Hom}(F_1, M')$$

exakt. In der Mitte haben wir das Element $f_0 d_1$, dessen Bild rechts $d'_0 f_0 d_1 = d_0 d_1 = 0$ ist. Daher gibt es ein Urbild f_1 links. Dieses Verfahren wird fortgesetzt. Für den Beweis von (iii) seien f_*, g_* Morphismen von Auflösungen. Wir betrachten $f_* - g_*$. Gesucht sind Abbildungen $h_i : F_i \to F'_{i+1}$ mit

$$f_i - g_i = d'_{i+1} h_i + h_{i-1} d_i$$

Wir beginnen auf der Stufe 0. Die Sequenz

$$\mathrm{Hom}(F_0, F'_1) \to \mathrm{Hom}(F_0, F'_0) \to \mathrm{Hom}(F_0, M')$$

ist exakt. $f_0 - g_0$ hat das Bild $d_0 - d_0 = 0$, hat also ein Urbild h_0 links. Nach Konstruktion $f_0 - g_0 = d_1' h_0$. Die Sequenz

$$\mathrm{Hom}(F_1, F_2') \to \mathrm{Hom}(F_1, F_1') \to \mathrm{Hom}(F_1, F_0')$$

ist exakt. In der Mitte lebt $f_1 - g_1 - h_0 d_1$. Das Bild dieser Abbildung rechts ist

$$d_1' f_1 - d_1' g_1 - d_1' h_0 d_1 = f_0 d_0 - g_0 d_0 - (f_0 - g_0) d_0 = 0$$

Also gibt es ein Urbild h_1 links. Dieses Verfahren wird fortgesetzt. □

Bemerkung. Insbesondere sind je zwei Auflösungen von M homotopieäquivalent.

Anwenden von $\otimes M$ oder $\mathrm{Hom}(\cdot, M)$ bildet (wegen Funktorialität) Komplexe auf Komplexe ab.

Definition 10.5. *Seien M, N Moduln, F_* eine freie Auflösung von M. Dann setzen wir*

$$\mathrm{Ext}^i_A(M,N) = H^i(\mathrm{Hom}(F_*, N)) \qquad \mathrm{Tor}^A_i(M,N) = H_i(F_* \otimes N)$$

Lemma 10.6. Ext^i *und* Tor_i *sind wohldefinierte Funktoren. Es gilt* $\mathrm{Ext}^0 = \mathrm{Hom}$ *und* $\mathrm{Tor}_0 = \otimes$.

Beweis: Sind F_* und F_*' zwei freie Auflösunge von M, so sind die beiden Komplexe homotopieäquivalent. Dies bleibt unter Anwenden von $\mathrm{Hom}(\cdot, N)$ erhalten. Daher haben die Komplexe $\mathrm{Hom}(F_*, N)$ und $\mathrm{Hom}(F_*', N)$ isomorphe Homologie. Ist $f : M \to M'$ ein Homomorphismus, so existiert ein Morphismus von Auflösunge $f : F_* \to F_*'$, also auch ein Komplexhomomorphismus $f^* : \mathrm{Hom}(F_*, N) \to \mathrm{Hom}(F_*', N)$. Dieser induziert eine Abbildung auf der Homologie der Komplexe. Je zwei Wahlen für f sind homotop, also ist die induzierte Abbildung auf der Homologie unäbhängig von der Wahl. Hieraus folgt leicht die Funktorialität.
Nach Vorrausetzung ist $F_1 \to F_0 \to M \to 0$ exakt. Wegen der Linksexaktheit von Hom Exaktheit von

$$0 \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(F_0, N) \to \mathrm{Hom}(F_1, N)$$

Dies berechnet $\mathrm{Ext}^0(M, N)$ wie behauptet. Ebenso für $\otimes$. □

Beispiel. Sei F frei. Dann gilt $\mathrm{Ext}^i(F, N) = \mathrm{Tor}_i(F, N) = 0$ für $i > 0$, denn F kann als Auflösung von sich selbst gewählt werden.

Lemma 10.7. *Sei A ein Hauptidealring, M, N endlich erzeugte A-Moduln. Dann sind alle* $\mathrm{Tor}_i(M,N)$, $\mathrm{Ext}^i(M,N)$ *endliche erzeugte A-Moduln und verschwinden für $i \neq 0, 1$.*

Beweis: M ist endlich erzeugt, sei also $d_0 F_0 \to M$ surjektive Abbildung mit F_0 frei von endlichem Rang. Nach dem Elementarteilersatz ist $F_1 = \mathrm{Ker}\, d_0$ ebenfalls frei von endlichem Rang. Wir benutzen die freie Auflösung $[F_1 \to F_0]$ zur Berechnung der Funktoren. □

Der eigentliche Witz dieser Funktoren ist die lange exakte Kohomologiesequenz.

Satz 10.8. *Sei* $0 \to M_1 \to M_2 \to M_3 \to 0$ *eine kurze exakte Sequenz von Moduln,* N *ein weiterer Modul. Dann sind die folgenden Sequenzen exakt:*

$$\cdots \to \operatorname{Ext}^i(N, M_1) \to \operatorname{Ext}^i(N, M_2) \to \operatorname{Ext}^i(N, M_3) \to \operatorname{Ext}^{i+1}(N, M_1) \to \dots$$
$$\cdots \to \operatorname{Tor}_i(N, M_1) \to \operatorname{Tor}_i(N, M_2) \to \operatorname{Tor}_i(N, M_3) \to \operatorname{Tor}_{i-1}(N, M_1) \to \dots$$
$$\cdots \to \operatorname{Ext}^i(M_3, N) \to \operatorname{Ext}^i(M_2, N) \to \operatorname{Ext}^i(M_1, N) \to \operatorname{Ext}^{i+1}(M_3, N) \to \dots$$

Beweis: Sei F_* eine frei Auflösung von N. Wegen der Exaktheit von $\operatorname{Hom}(F_i, \cdot)$ und $F_i \otimes$ erhalten wir kurze exakte Sequenzen von Komplexen

$$0 \to \operatorname{Hom}(F_*, M_1) \to \operatorname{Hom}(F_*, M_2) \to \operatorname{Hom}(F_*, M_3) \to 0$$
$$0 \to F_* \otimes M_1 \to F_* \otimes M_2 \to F_* \otimes M_3 \to 0$$

Die induzierten langen exakten Sequenzen sind die beiden ersten aus dem Satz. Für die dritte seien F_* eine frei Auflösung von M_1 und F'_* eine frei Auflösung von M_3.

Behauptung. $F_* \oplus F'_*$ *ist eine freie Auflösung von* M_2 *und es gibt eine kurze exakte Sequenz von Auflösungen*

$$0 \to F_* \to F_* \oplus F'_* \to 0$$

Auf diese wenden wir $\operatorname{Hom}(\cdot, N)$ an. Wir erhalten eine kurze exakte Sequenz von Komplexen, die wieder eine lange exakte Kohomologiesequenz induziert. □

Beispiel. $A = \mathbb{Z}$, $M = \mathbb{Z}/(m)$, $N = \mathbb{Z}/(n)$ für $n > 0$. Wegen der kurzen exakten Sequenz

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to M \to 0$$

folgt

$$0 \to \operatorname{Hom}(M, N) \to \operatorname{Hom}(\mathbb{Z}, N) \xrightarrow{m} \operatorname{Hom}(\mathbb{Z}, N) \to \operatorname{Ext}^1(M, N) \to \operatorname{Ext}^1(\mathbb{Z}, N) \to \operatorname{Ext}^1(\mathbb{Z}, N) \to 0$$

Wegen $\operatorname{Ext}^1(\mathbb{Z}, N) = 0$ ($\mathbb{Z}$ frei), folgt

$$\operatorname{Ext}^1(M, N) \cong N/mN \cong \mathbb{Z}/(n) + (m) \cong \mathbb{Z}/\operatorname{ggT}(n, m)$$

Ebenso folgt

$$0 \to \operatorname{Tor}_1(M, N) \to \mathbb{Z} \otimes N \xrightarrow{m \otimes 1} \mathbb{Z} \otimes N \to M \otimes N \to 0$$

Also

$$\operatorname{Tor}_1(M, N) \cong \operatorname{Ker}(m : N \to N) = (m)/(n) \cap (m) \cong \mathbb{Z}/\operatorname{kgV}(n, m)$$

Definition 10.9. *Sei* A *ein noetherscher lokaler Ring mit maximalem Ideal* $\mathfrak{m}$ *und* $k = A/\mathfrak{m}$. *Der Ring heißt* regulär, *wenn*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$$

Bemerkung. Reguläre lokale Ringe der Dimension 1 sind genau die diskreten Bewertungsringe. (Nicht ganz offensichtlich!)

Definition 10.10. *Die* globale kohomologische Dimension *von A ist das Supremum über alle i, für die es Moduln M, N gibt mit* $\mathrm{Ext}^i(M,N) \neq 0$.

Theorem 10.11 (Serre). *Sei A ein lokaler noetherscher Ring. Dann sind äquivalent:*

(i) A ist regulär.

(ii) Die globale kohomologische Dimension von A stimmt mit der Krulldimension überein.

(iii) Die globale kohomologische Dimension ist endlich.

Beweis: Matsumura, Commutative ring theory, Theorem 19.2
Beweisidee: Geschickte Wahl von Auflösungen, Stichwort "Koszul-Komplex". □

Beispiel. Sei k algebraisch abgeschlossener Körper, $V = V(S) \subset \mathbb{A}^n$ mit $I(V) = (f_1, \ldots, f_m)$ eine affine Varietät der Dimension d. Dann sind alle lokalen Ringe von V regulär, genau dann wenn

$$\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$$

in allen Punkten von V den Rang $n - d$ hat. In diesem Fall heißt V *glatt* oder auch *nicht-singulär*.

Kapitel 11

Schlussbemerkungen

Was wir behandelt haben

Kommutative Algebra! Ringe und Moduln, Konstruktionen und Eigenschaften

- Grundlagen der algebraischen Geometrie: affine Varietäten, Hilbertscher Nullstellensatz, Noether-Normalisierung, Dimensionstheorie
- Grundlagen der algebraischen Zahlentheorie: Ganzheitsringe sind Dedekindringe

Hier schließen sich in natürlicher Weise große Theorien an.

Algebraische Geometrie

Definition 11.1. *Sei k ein algebraisch abgeschlossener Körper, $S \subset k[X_0, \ldots, X_n]$ eine Menge von homogenen Polynomen. Dann heißt*

$$V(S) = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid f(x_0, \ldots, x_n) = 0, f \in S\}$$

projektive Varietät *definiert durch S.*

Auch projektive Varietäten lassen sich mit der Zarikski-Topologie versehen. Affine Varietäten sind dann natürliche offene Untermengen von projektiven.

Theorem 11.2 (Satz von Bezout). *Seien $V_1, V_2 \subset \mathbb{P}^2_k$ Kurven, die durch je ein Polynom vom Grad n bzw. m definiert sind. Haben V_1 und V_2 nur isolierte Schnittpunkte, so beträgt die Anzahl (mit Vielfachheit gezählt) genau nm.*

Im Wintersemester: Lesekurs Algebraische Geometrie (Dr. Orlik)
Hier soll es vor allem um die Verallgemeinerung auf beliebigen Grundkörper oder sogar Grundring gehen.

Zahlentheorie

Theorem 11.3 (Dirichlet). *Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K^*$ endlich erzeugte abelsche Gruppe. Die Klassengruppe ist endlich.*

Im Sommersemester: Vorlesung Elementare Zahlentheorie (Huber-Klawitter) Braucht nichts von dem, was wir behandelt haben, ist aber schön. Es geht im wesentlichen um quadratische Zahlkörper, z.B. Reziprozitätsgesetz.

Was wir nicht behandelt haben

Halbeinfache Algebren und Darstellungstheorie

(Nichtkommutative) Ringe, die gleichzeit endlich dimensional über einem Körper k sind. Hier gibt es eine Strukturtheorie, die wesentlichen Bausteine sehen aus wie $M_n(E)$, wobei E/k ein Schiefkörper ist. Für $k = \mathbb{Q}$ ist dies wieder zahlentheoretisch wichtig.
Für allgemeine Körper ist es eng verwand mit Darstellungstheorie. Sei G ein endliche Gruppe. Eine Darstellung ist ein Gruppenhomomorphismus $G \to \mathrm{Aut}(V)$, wobei V ein k-Vektorraum ist (meist $k = \overline{k}$). Alternativ: G operiert durch lineare Abbildungen auf V. Die Kategorie der Darstellungen von G ist äquivalent zur Kategorie der $k[G]$-Moduln, wobei $k[G] = \bigoplus_{g\in G} kg$ der Gruppenring ist. Er ist eine endlichdimensionale k-Algebra. Jede endlichdimensionale Darstellung ist direkte Summe von irreduziblen. Diese lassen sich leicht klassifizieren. Ist G abelsch, so ist $k[G]$ kommutativ und die irreduziblen Darstellungen sind eindimensional.
Literatur: Serre: Representation theory; Lang: Algebra

Lie-Algebren

Lie-Algebren sind Vektorräume mit einer Verknüpfung $[\cdot,\cdot]$, die nicht assoziativ ist, sondern der Jacobi-Identität $[X,[Y,Z]]+[Y,[Z,X]]+[Z,[X,Y]] = 0$ genügt.

Beispiel. $V = M_n(k)$ mit $[A,B] = AB - BA$.

Diese können z.B. klassifiziert werden. Reelle Lie-Algebren sind wichtig, denn sie sind Tangentialräume von *Lie-Gruppen*, d.h. Gruppen wie $\mathrm{Gl}_N(\mathbb{R})$ und S^1, die gleichzeitig Mannigfaltigkeiten sind. Diese sind in der Physik oder überhaupt beim Studium von Differentialgleichungen enorm wichtig.

Arithmetische Geoemtrie

Mein Arbeitsgebiet ist arithmetische Geometrie, also Zahlentheorie mit den Methoden der algebraischen Geometrie.
Das größte Ergebnis der letzten Jahre war der Beweis der Vermutung von Shimura-Taniyama-Weil:

Theorem 11.4 (Wiles,Taylor-Wiles et. al.). *Jede elliptische Kurve über* $\mathbb{Q}$ *ist modular.*

Korollar 11.5 (Fermatsche Vermutung). *Für* $n > 2$ *hat die Gleichung*

$$x^n + y^n = z^n$$

nur die trivialen ganzzahligen Lösungen mit $x = 0$ *oder* $y = 0$.

Im Wintersemester: Vorlesung elliptische Kurve, aufbauend auf unserer Algebra 2
Eine elliptische Kurve ist eine glatte projektive Kurve vom Geschlecht 1. Konkret bedeutet dies: definiert durch ein homogenes Polynom vom Grad 3. Elliptische Kurve über $\mathbb{Q}$ bedeutet dann, dass die Definitionsgleichung rationale Koeffizienten hat. Über $\mathbb{C}$ ist jede elliptische Kurve von der Form $\mathbb{C}/\Gamma$, wobei $\Gamma \subset \mathbb{C}$ ein Gitter ist. Sie sieht also aus wie ein Torus.
Modular bedeutet, dass es eine surjektive holomorphe Abbildung

$$\mathbb{H}/\Gamma(N) \to E(\mathbb{C})$$

gibt, wobei $\mathbb{H}$ die obere Halbebene ist, $\Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$ die Untergruppe der Matrizen, die modulo N kongruent zur Einheitsmatrix sind; $E(\mathbb{C})$ die Punkte der elliptische Kurve über $\mathbb{C}$.
Elliptische Kurven sind einerseits noch so einfach, dass wir viel über sie wissen, andererseits so kompliziert, dass man sehr viel Interessantes sagen kann. So tragen sie automatisch ein Gruppengesetz, das man mit Hilfe des Satzes von Bezout konstruieren kann.
In der Vorlesung wollen wir zunächst den Fall $k = \mathbb{C}$ betrachten, um geometrische Anschauung zu gewinnen. Dann geht es um die algebraische Behandlung über endlichen Körpern und Zahlkörpern. Der Beweis des Theorems von Wiles liegt leider außerhalb unserer Reichweite. Aber der Beweis des Korollars ist vielleicht machbar.
Literatur: Silverman, Arithmetic of Elliptic Curves.

Inhaltsverzeichnis