Algebra II
Sommersemester 2003

Prof. Dr. Annette Huber-Klawitter

Fassung vom 14. Juli 2003

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

Math. Institut
Augustusplatz 10/11
04109 Leipzig

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

Kapitel 0

Einführung

Fortsetzung der Algebra I

In der Algebra I hatten wir ein großes Ziel: die Behandlung von Polynomgleichungen und der Frage nach ihrer Lösbarkeit. Es stellte sich heraus, dass dies auf das Studium von endlichen Körpererweiterungen hinauslief:

Satz 0.1. *Sei L/K eine Körpererweiterung. Sei $\alpha \in L$ Nullstelle von $0 \neq P \in K[X]$. Dann ist $K(\alpha)$ eine endliche Erweiterung von K. Ist L/K endlich, so ist jedes Element von L Nullstelle eines irreduziblen Polynoms mit Koeffizienten in K.*

Wesentliches Hilfmittel war Galoistheorie, die Eigenschaften von Körpererweiterungen in Form in Eigenschaften von Gruppen kodiert.

Theorem 0.2 (Hauptsatz der Galois-Theorie). *Sei L/K eine endliche Galoiserweiterung von Körpern. Sei $\mathcal{G}$ die Menge der Untergruppen von $\mathrm{Gal}(L/K)$ und $\mathcal{K}$ die Menge der Zwischenkörper von L/K. Dann gibt es zwei Abbildungen*

$$\begin{array}{ccccc} \mathcal{G} & \xrightarrow{\kappa} & \mathcal{K} & \xrightarrow{\gamma} & \mathcal{G} \\ G & \mapsto & L^G & & \\ & & F & \mapsto & \mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\,|_F = \mathrm{id}\} \end{array}$$

(i) Dann sind die obigen Abbildungen κ und γ inklusionsumkehrend und invers zueinander. Insbesondere sind beide Abbildungen bijektiv.

(ii) Für jeden Zwischenkörper ist L/F galois, und es gilt $[L : F] = \mathrm{Gal}(L/F)$. Für jede Untergruppe $H \subset \mathrm{Gal}(L/K)$ gilt

$$[L : L^H] = |H|, [L^H : K] = [\mathrm{Gal}(L/K) : H] \ .$$

(iii) Für $L \supset F \supset K$ ist F/K normal (und dann auch galois), genau dann wenn $H = \mathrm{Gal}(L/F)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ ist. In diesem Fall ist

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

Um diesen Satz effektiv anwenden zu können, benötigten wir alternative Charakterisierungen von "galois":

Satz 0.3. *Sei L/K endliche Körpererweiterung. Dann sind äquivalent.*

(i) L/K *ist galois;*

(ii) $|\operatorname{Gal}(L/K)| = [L : K]$*;*

(iii) L/K *ist normal und separabel;*

(iv) $L^{\operatorname{Gal}(L/K)} = K$*.*

Dabei ist L/K normal und separabel, wenn jedes irreduzible Polynom in $K[X]$, das ein Nullstelle in L hat, dort bereits so viele unterschiedliche Nullstellen hat wie sein Grad angibt.
Die Stärke des Hauptsatzes der Galoistheorie liegt darin, dass er angewendet werden kann, ohne auf seinen Beweis einzugehen!
Im ersten Teil der Algebra I beschäftigten wir uns mit (endlichen) Gruppen und ihren Eigenschaften. Dies erwies sich als nötige Vorbereitung für eine erfolgreich Anwendung des Hauptsatzes der Galoistheorie.
In ersten Teil der Algebra II werden wir weitere Anwendungen des Hauptsatzes kennenlernen, die das Bild abrunden sollen. Danach wird es darum gehen, Hilfsmittel bereitzustellen, die im weiteren Studium gebraucht werden.

Moduln

Die Definition eines Moduls ist wörtlich die gleiche wie die eines Vektorraums - nur wird Körper durch Ring ersetzt. Es stellt sich schnell heraus, dass Moduln eine wesentlich kompliziertere Struktur als Vektorräume haben.
Wir werden ein ähnliches Programm wie in der Gruppentheorie abarbeiten: Morphismen, Kerne, Summen, Tensorprodukt usw.
Danach werden wir Moduln über Hauptidealringen klassifizieren. Ein Spezialfall wurde bereits erwähnt, aber nicht bewiesen:

Theorem 0.4 (Elementarteilersatz). *Jede endlich erzeugte abelsche Gruppe ist direktes Produkt von endlich vielen zyklischen Gruppen.*

$$G \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$$

Ein anderer Spezialfall ist der Satz über die Jordansche Normalform.
Dies sind die ersten Beispiele aus dem großen Gebiet der kommutativen Algebra, die die Grundlage der algebraischen Geometrie und Zahlentheorie bildet.

Homologische Algebra

Im dritten Teil werden wir homologische Algebra studieren. Kohomologie wurde in der Topologie entwickelt zum Beweis von Ausagen wie:

Theorem 0.5 (Topologische Invarianz der Dimension). *Sei $\phi : \mathbb{R}^n \to \mathbb{R}^m$ ein Homoöomorphismus (stetig, bijektiv, Umkehrabbildung stetig). Dann ist $n = m$.*

Für $n = 0$ genügt ein Abzählargument. Für $n = 1$ argumentiert man über den Zusammenhang: $\mathbb{R} \setminus \{0\}$ ist nicht zusammenhängend, $\mathbb{R}^n \setminus \{0\}$ für $n > 1$ ist es. Der allgemeine Fall ist schwieriger und wurde erst mit Hilfe von singulärer Homologie befriedigend gelöst.
Singuläre Homologie ordnet jedem topologischen Raum eine Folge von Vektorräumen (oder Moduln) zu. Unterscheiden sich die Homologiegruppen, so sind die topologischen Räume nicht homöomorph. Eine ähnliche Methode haben wir ja auch zum Studium von Körpern benutzt. Um die Rechenregeln für Homologiegruppen zu beweisen, benötigt man einige rein algebraische Sätze. Diese sind Gegenstand der homologischen Algebra.
Homologie und homologische Algebra werden vor allem in der Geometrie (Topologie, Differentialgeometrie, komplexe Geometrie, algebraische Geometrie) verwendet. In den letzten 50 Jahren wurden große Teile der Zahlentheorie geometriesiert, daher finden homologische Methoden auch in Algebra und Zahlentheorie eine Anwendung. Unter dem Stichwort nichtkommutative Geometrie finden sie Eingang in die Funktionalanalysis.

Literatur

Weiterhin: S. Lang: Algebra, S. Bosch: Algeba.
Kommutative Algebra: Atiyah, MacDonald: Commutative Algebra.
Homologische Algebra: Manin, Drinfeld: Homological Algebra.

Kapitel 1

Ergänzungen zur Galoistheorie

Der Satz vom primitiven Element

Ein Polynom hieß *separabel* (I Definition 8.10), wenn seine irreduziblen Faktoren separabel sind. Ein irreduziebles Polynom hieß separabel, wenn es keine doppelten Nullstellen über dem algebraischen Abschluss hat. Dies konnte man testen, in dem man die formale Ableitung des Polynoms bildet.
Wir haben bisher nicht gezeigt:

Lemma 1.1. *Sei $P \in K[X]$ ein separables Polynom. Dann ist der Zerfällungskörper von P galois über K.*

Beweis: Der Zerfällungskörper L von P ist normal über K (I Satz 8.3). Wir müssen also zeigen, dass er separabel ist. Tatsächlich überprüfen wir ein anderes Kriterium, nämlich

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

Wir argumentieren mit vollständiger Induktion nach $[L : K]$. Der Fall $L = K$ ist trivial. Sei $\alpha \in L \smallsetminus K$ eine Nullstelle von P und $Q \in K[X]$ das Minimalpolynom von P. Wir betrachten die Körperkette

$$L \supset K(\alpha) \supset K \ .$$

L kann als Zerfällungskörper des separablen Polynoms $P \in K(\alpha)[X]$ aufgefasst werden. Nach Induktionsvoraussetzung ist $L/K(\alpha)$ galois, also

$$K(\alpha) = L^{\mathrm{Gal}(L/K(\alpha))} \ .$$

Also ist $F := L^{\mathrm{Gal}(L/K)} \subset K(\alpha)$. Sei $x \in F$. Es hat die Form

$$x = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

mit $n = \deg P$, $a_i \in K$. Da α separabel ist, hat P n verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n \; in L$, eine davon ist α. Es gibt also

$$\sigma_i : K(\alpha) \to L$$

mit $\sigma_i(\alpha) = \alpha_i$. Da L/K normal ist, setzt sich dieser Homomorphismus fort zu $\sigma_i : L \to L$. Es folgt

$$x = \sigma_i(x) = a_0 + a_1\alpha_i + \cdots + a_{n-1}\alpha_i^{n-1} \; .$$

Damit hat das Polynom

$$(a_0 - x) + a_1 X + \cdots + a_{n-1}X^{n-1} \in F[X]$$

n verschiedene Nullstellen. Es ist also identisch gleich null, d.h. $x = a_0 \in K$. Dies beweist $K = F$. □

Damit ist es nun auch in Charakteristik $p > 0$ leicht, Galoiserweiterungen zu definieren.

Korollar 1.2. *Sei L/K endlich und separabel. Dann ist L enthalten in einer Galoiserweiterung E/K. Es gibt nur endliche viele Zwischenkörper von L/K.*

Beweis: Sei $L = K(\alpha_1, \ldots, \alpha_n)$, P_i das Minimalpolynom von α_i und $P = \prod P_i$. Nach Voraussetzung ist P separabel. Wir wählen für E den Zerfällungskörper von von P. Dies ist eine endliche Galoiserweiterung von K. Nach dem Hauptsatz der Galoistheorie entsprechend die Zwischenkörepr von E/K genau den Untergruppen von $\mathrm{Gal}(E/K)$. Da diese Gruppe endlich ist, hat sie nur endliche viele Untergruppen. Also hat E/K (und dann erst recht L/K) nur endliche viele Zwischenkörper. □

Korollar 1.3 (Der Satz vom primitiven Element). *Sei L/K endlich und separabel. Dann ist die Erweiterung einfach, d.h. es gibt $\alpha \in L$ mit $L = K(\alpha)$.*

Das Element α heißt dann primitives Element. Dieser Satz erleichtert vieles. Z.B. ist die Galoisgruppe einer primitiven Erweiterung sehr einfach zu verstehen.

Beweis: Sei K ein unendlicher Körper. Seien $\alpha, \beta \in L$. Wir betrachten

$$\{\alpha + c\beta \mid c \in K\} \; .$$

Diese Menge hat unendliche viele Elemente. Andererseits ist die Menge der Körper $K(\alpha + c\beta) \subset L$ endlich nach dem letzten Korollar. Also gibt es $c_1 \neq c_2 \in L$ mit

$$K(\alpha + c_1\beta) = K(\alpha + c_2\beta) \; .$$

Wir nennen diesen Körper F. Er enthäalt $\alpha + c_i\beta$, also auch die Differenz $(c_1 - c_2)\beta$. Wegen $c_1 \neq c_2 \in K$ enthält er auch β. Also enthält er auch α. Es gilt

$$K(\alpha, \beta) = K(\alpha + c_i\beta) \; .$$

Allgemein ist $L = K(\alpha_1, \ldots, \alpha_n)$. Das obige Argument erlaubt es, die Anzahl der Erzeuger schrittweise auf einen zu reduzieren.
Es fehlt noch der Fall eines endlichen Körpers K. Dieser folgt aus dem nächsten Satz. □

Satz 1.4. *Sei K ein Körper, $G \subset K^*$ eine Untergruppe. Dann ist G zyklisch.*

Bemerkung. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers zyklisch. Ein Erzeuger von K^* ist dann auch ein primitives Element.

Beweis: G ist endlich und abelsch. Dann gilt

$$G \cong P_{p_1} \times \cdots \times P_{p_n}$$

wobei die p_i die Primteiler von $|G|$ sind und P_{p_i} die zugehörigen p_i-Sylowgruppen. (Sie sind eindeutig, da G abelsch ist. Die natürliche Abbildung von rechts nach links ist injektiv, da die Ordnungen teilerfremd sind. Sie ist bijektiv, da die Ordnungen der beiden Gruppen gleich sind.) Nach dem chinesischen Restsatz ist zu zeigen, dass P_{p_i} zyklisch ist.
Sei nun $a_i \in P_{p_i}$ ein Element der maximalen Ordnung m_i. Das Element $a = a_1 \ldots a_n$ hat die Ordnung $m = m_1 \ldots m_n$. Die Ordnung aller Elemente von G teilt dieses m. Also sind alle Elemente von G Nullstellen des Polynoms $X^m - 1$, d.h. $|G| \leq m$. Wegen $m = | < a > |$ ist $|G| = m$ und a ein Erzeuger von G. □

Statt des Sylowsatzes kann man natürlich auch den Elementarteilersatz benutzen.

Definition 1.5. *Sei L/K eine endliche Galoiserweiterung. Eine Normalbasis von L ist ein Element $\alpha \in L$, so dass $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)$ eine Basis von L als K-Vektorraum ist.*

Lemma 1.6. *Eine Normalbasis ist automatische primitiv.*

Beweis: Das Minimapolynom von α ist $P = \prod(X - \sigma(\alpha))$, hat also den Grad $[L : K]$. Wegen $[K(\alpha) : K] = \deg P$ folgt $L = K(\alpha)$. □

Beispiel. Für $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ ist $\sqrt{3}$ keine Normalbasis, wohl aber $\sqrt{3} + 1$.

Theorem 1.7 (Existenz einer Normalbasis). *Sei L/K endlich und galois. Dann existiert eine Normalbasis.*

Beweis: Sei $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$, $\alpha \in L$. Angenommen, α ist keine Normalbasis. Dann sind die Elemente $\{\sigma_i(\alpha) \mid i = 1, \ldots, n\}$ linear abhängig über K, d.h. es gibt nichttriviale $a_i \in K$ mit

$$a_1\sigma_1(\alpha) + a_2\sigma_2(\alpha) + \cdots + a_n\sigma_n(\alpha) = 0 \ .$$

Auf diese Gleichung wenden wir σ_j^{-1} an und erhalten

$$a_1\sigma_j^{-1}\sigma_1(\alpha) + \cdots + a_n\sigma_j^{-1}\sigma_n(\alpha) = 0 \ .$$

Dies fassen wir als lineares Gleichungssystem in L mit Unbekannten a_i auf. Es hat eine nichttriviale Lösung, also

$$\det(\sigma_j^{-1}\sigma_i(\alpha))_{i,j} =\neq 0 \ .$$

Um das Theorem zu zeigen, müssen wir also ein α finden, für das diese Determinante verschwindet.
Sei β ein primitives Element. Die gesuchte Normalbasis ist ein Polynom in β, gesucht sind die Koeffizienten. Wir betrachten das Minimalpolynom

$$F(X) = \prod_{i=1}^{n}(X - \sigma_i(\beta)) \in L[X]$$

und für jedes $\sigma \in \mathrm{Gal}(L/K)$

$$G^\sigma(X) = \frac{F(X)}{X - \sigma(X)} \ .$$

Wir lassen σ die $\sigma_j^{-1}\sigma_i$ durchlaufen. Die Determinante dieser Matrix mit Einträgen in $L[X]$ sei

$$D(X) = \det\left((G^{\sigma_j^{-1}\sigma_i}(X))_{i,j}\right) \in L[X] \ .$$

Setzt man β ein, so verschwindet $G^\sigma(\beta)$ für $\sigma \neq \mathrm{id}$, aber $G^{\mathrm{id}}(\beta) \neq 0$, denn $F(X)$ hat keine doppelten Nullstellen. Es folgt

$$D(\beta) = \det(G^{\mathrm{id}}(\beta)\delta_{ij}) \neq 0$$

wobei δ_{ij} die Einheitsmatrix ist. Also ist D nicht das Nullpolynom. Hat K unendlich viele Elemente, so gibt es $\gamma \in K$ mit $D(\gamma) \neq 0$.

Behauptung. *$G^{\mathrm{id}}(\gamma)$ ist die gesuchte Normalbasis.*

Wegen $\gamma \in K$ gilt

$$\sigma G^{\mathrm{id}}(\gamma) = \frac{\sigma F(\gamma)}{\sigma(\gamma) - \sigma(\beta)} = \frac{F(\gamma)}{\gamma - \sigma(\beta)} = G^\sigma(\gamma) \ .$$

Daher ist $D(\gamma) \neq 0$ genau das Kriterium, das zu überprüfen ist.
Es bleibt der Fall, dass L ein endlicher Körper ist. Er wird mit linearer Algebra behandelt. Nach I Satz 9.12 ist dann $\mathrm{Gal}(L/K)$ zyklisch mit Erzeuger der Frobenius ϕ.

Behauptung. *ϕ hat das Minimalpolynom $X^n - 1$.*

Einerseits gilt $\phi^n = \mathrm{id}$. Hat das Minimalpolynom von ϕ einen kleineren Grad, so sind die Elemente $\mathrm{id}, \phi, \ldots, \phi^{n-1}$ linear abhängig über K. Dies wäre ein Widerspruch zur linearen Unabhängigkeit von Körperhomomorphismen I Satz 9.2.

Der Vektorraum L hat die Dimension n. Charakteristisches Polynom und Minimalpolynom haben nun den gleichen Grad, sind also nach dem Satz von Cayley-Hamilton gleich. In der linearen Algebra zeigt man, dass dann ein zyklischer Vektor existiert, d.h. ein $\alpha \in L$ mit $\alpha, \phi(\alpha), \ldots, \phi^{n-1}(\alpha)$ Basis von L. Dies ist die Normalbasis. (Siehe Lorenz, Lineare Algebra II, BI Wissenschaftsverlag, S. 168). □

Unendliche Galoiserweiterungen

Bisher haben wir uns auf endliche Körpererweiterungen konzentriert. Allgemein:

Definition 1.8. *Sei L/K algebraisch. Die Erweiterung heißt* galois*, wenn sie normal und separabel ist. Ihre Galoisgruppe ist*

$$\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \textit{Körperautomorphismus mit } \sigma\mid_K = \mathrm{id}\} \ .$$

Alle Aussagen über unendliche algebraische Erweiterungen werden auf endliche zurückgespielt. Die entscheidende Beobachtung ist die folgende:

Lemma 1.9. *Sei L/K algebraisch. Sei $\mathcal{F}$ die Menge der Zwischenkörper von L/K ist, die endlich über K sind. Sei $\mathcal{G} \subset \mathcal{F}$ die Teilmenge der Körper, die galois über K sind. Dann gilt*

$$L = \bigcup_{\mathcal{F}} F$$

Ist L/K galois, so können die Zwischenkörper galois angenommen werden.

Beweis: Sei $\alpha \in L$. Dann ist $K(\alpha) \in \mathcal{F}$, also liegt α auch auf der rechten Seite. Ist L/K galois, so liegt die normale Hülle von $K(\alpha)$ in L, ist also ein Element von $\mathcal{G}$. □

Satz 1.10. *Sei L/K galois, $F \in \mathcal{F}$. Dann ist $\sigma \mapsto \sigma|_F$ ein Gruppenhomomorphismus*

$$\phi_F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \ .$$

Für $F \subset E$ Elemente von $\mathcal{G}$ sei

$$\phi_{E/F} : \mathrm{Gal}(E/K) \to \mathrm{Gal}(F/K)$$

der entsprechende Homomorphismus. Dann ist

$$\Phi : \mathrm{Gal}(L/K) \to \prod_{F \in \mathcal{G}} \mathrm{Gal}(F/K) \ , \ \Phi(\sigma)_F = \phi_F(\sigma)$$

ein injektiver Gruppenhomomorphismus mit Bild

$$\varprojlim_{\mathcal{G}} \mathrm{Gal}(F/K) = \{(\sigma_F)_F \in \prod_{F \in \mathcal{G}} \mathrm{Gal}(F/K) \mid \phi_{E/F}(\sigma_E) = \sigma_F \textit{ für alle } E/F\}$$

Beweis: Die Aussagen für ϕ_F und $\phi_{E/F}$ sind eine Wiederholung des Argumentes, das für den dritten Teil des Beweises des Hauptsatzes der Galoistheorie gebraucht wurde: $\sigma(F) \subset F$, da F/K normal. Ebenso ist klar, dass das Bild von Φ in der angegebenen Menge landet.

Behauptung. Φ *ist injektiv.*

$\Phi(\sigma) = \mathrm{id}$ bedeutet $\sigma \mid_F = \mathrm{id}$ für alle $F \in \mathcal{G}$. Wegen 1.9 folgt daraus $\sigma = \mathrm{id}$.

Behauptung. *Jedes Element von* $\varprojlim_{\mathcal{G}} \mathrm{Gal}(F/K)$ *liegt im Bild.*

Gegeben sei ein $(\sigma_F)_F$, $\alpha \in L$. Dann gibt es $F \in \mathcal{G}$ mit $\alpha \in F$. Wir definieren $\sigma(\alpha) = \sigma_F(\alpha)$. Wegen der Verträglichkeitsbedingung an die σ_F ist dies unabhängig von F. Offensichtlich ist $\sigma \in \mathrm{Gal}(L/K)$ das gesuchte Urbild. □

Wir versehen $\mathrm{Gal}(L(K)$ nun mit einer Topologie.

Definition 1.11. *Sei L/K galois, $F \in \mathcal{G}$. Dann erhält* $\mathrm{Gal}(F/K)$ *die diskrete Topologie (alle Teilmengen sind offen).* $\mathrm{Gal}(L/K)$ *erhält die Teilraumtopologie der Produkttopologie auf* $\prod F \in \mathcal{G}\, \mathrm{Gal}(F/K)$. *Man nennt dies die* proendliche Topologie *auf* $\mathrm{Gal}(L/K)$.

Die Galoisgruppe wird damit zu einer topologischen Gruppe. Um die Topologie zu verstehen, genügt es, offene Umgebungen von id zu verstehen. Eine Umgebungsbasis von id sind die Kerne der ϕ_F.

Theorem 1.12 (Hauptsatz der Galoistheorie). *Sei L/K eine Galoiserweiterung von Körpern. Sei $\mathcal{G}$ die Menge der abgeschlossenen Untergruppen von* $\mathrm{Gal}(L/K)$ *und $\mathcal{K}$ die Menge der Zwischenkörper von L/K. Dann gibt es zwei Abbildungen*

$$\begin{array}{ccccc} \mathcal{G} & \xrightarrow{\kappa} & \mathcal{K} & \xrightarrow{\gamma} & \mathcal{G} \\ G & \mapsto & L^G & & \\ & & F & \mapsto & \mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \mid_F = \mathrm{id}\} \end{array}$$

(i) Dann sind die obigen Abbildungen κ und γ inklusionsumkehrend und invers zueinander. Insbesondere sind beide Abbildungen bijektiv.

(ii) Für jeden Zwischenkörper ist L/F galois.

(iii) Für $L \supset F \supset K$ ist F/K normal (und dann auch galois), genau dann wenn $H = \mathrm{Gal}(L/F)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ *ist. In diesem Fall ist*

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/F)\ .$$

Bemerkung. (i) Der Quotient in (iii) ist als auch als Quotient topologischer Gruppen gemeint.

(ii) Teil des Hauptsatzes ist die Ausage $L^{\mathrm{Gal}(L/K)} = K$. Dies ist äquivalent dazu, dass L/K galois ist.

(iii) Für endliche Erweiterungen ist $\mathrm{Gal}(L/K)$ diskret, es gibt keine topologischen Bedingungen.

(iv) Offene Untergruppen von $\mathrm{Gal}(L/K)$ sind automatisch abgeschlossen und haben endlichen Index. Sie entsprechen den endlichen Zwischenkörpern F/K.

Beweis: Vergleiche Lorenz, Algebra I §12. Die Aussagen werde alle mit Lemma 1.9 auf den endlichen Fall zurückgeführt. □

Kummertheorie

Theorem 1.13. *Sei K ein Körper, $(\mathrm{Char}\, K, n) = 1$. K enthalte eine primitive n-te Einheitswurzel.*

(i) Sei L/K galois, $\mathrm{Gal}(L/K)$ zyklisch der Ordnung n. Dann ist $L = K(\alpha)$, wobei das Minimalpolynom von α gegeben ist durch

$$X^n - a \quad \text{für ein} \quad a \in K$$

(ii) Sei $a \in K$, L der Zerfällungskörper von $X^n - a$. Dann ist $\mathrm{Gal}(L/K)$ zyklisch von der Ordnung d ein Teiler von n mit $\alpha^d \in K$.

Die Erweiterungen in (ii) heißen *Kummererweiterungen.*

Beispiel. Sei $K = \mathbb{F}_2$. Dann ist der Zerfällungskörper von $X^2 + X + 1$ quadratisch, aber nicht vom Kummertyp. Für $\mathrm{Char}\, K = p = n$ gilt der Satz *nicht.*

Beweis: In I Satz 7.18 haben wir den größten Teil von (ii) gesehen. Die Nullstellen von $X^n - a$ in L sind genau die $\zeta^i\alpha$ für $i = 0, \ldots, n-1$, wobei ζ eine primitive n-te Einheitswurzel in K ist. Man erhält eine injektive Abbildung

$$\mathrm{Gal}(L/K) \to L^* \quad \sigma \mapsto \frac{\alpha}{\sigma\alpha} \ .$$

Diese stellte sich als Gruppenhomomorphismus heraus. Das Bild ist in der Gruppe der n-ten Einheitswurzeln enthalten, also ist die Ordnung ein Teiler von n. Als endliche Untergruppe von L^* ist die Galoisgruppe nach 1.4 zyklisch. Aus dem Bild kann wiederum das Minimalpolynom bestimmt werden, es ist von der Form $X^d - b$ mit Nullstelle α.
Wirklich interessant ist also (i). Dies ist etwas aufwändiger und wird verschoben. □

Definition 1.14. *Sei L/K galois. Eine Abbildung*

$$f : \mathrm{Gal}(L/K) \to L^*$$

heißt Kozykel, *falls $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$. f heißt* Korand, *falls es $\alpha \in L^*$ gibt mit $f(\sigma) = \alpha/\sigma(\alpha)$.*

Lemma 1.15. *Jeder Korand ist ein Kozykel. Kozykel und Koränder sind Gruppen bezüglich der Multiplikation von Funktionen.*

Beweis: Sei f ein Korand.

$$f(\sigma)(\sigma f(\tau)) = \frac{\alpha}{\sigma(\alpha)}\frac{\sigma\alpha}{\sigma\tau(\alpha)} = \frac{\alpha}{\sigma\tau(\alpha)} = f(\sigma\tau) \ .$$

Seien f, g Kozykel.

$$(fg)(\sigma\tau) = f(\sigma\tau)g(\sigma\tau) = f(\sigma)\sigma(f(\tau))g(\sigma)\sigma(g(\tau)) = fg(\sigma)\sigma(fg(\tau)) \ .$$

Für Koränder ist noch klarer. □

Definition 1.16. *Der Quotient*

$$H^1(L/K, L^*) = \frac{Kozykel}{Koränder}$$

heißt 1*-te* Galoiskohomologiegruppe *mit Werten in* L^**.*

Satz 1.17. *Sei L/K endlich und galois. Dann gilt*

$$H^1(L/K, L^*) = 1 \ .$$

Jeder Kozykel ist ein Korand.

Beweis: Sei $f : \mathrm{Gal}(L/K) \to L^*$ ein Kozykel. Zu $x \in L$ betrachten wir

$$b = \sum_{\tau \in \mathrm{Gal}(L/K)} f(\tau)\tau(x) \ .$$

Da die τ's linear unabhängig sind, gibt es ein x mit $b \neq 0$. Es folgt

$$\sigma(b) = \sigma\left(= \sum_{\tau \in \mathrm{Gal}(L/K)} f(\tau)\tau(x)\right) = \sum_{\tau} \sigma(f(\tau))\sigma\tau(x))$$
$$= \sum f(\sigma\tau)f(\sigma^{-1})\sigma\tau(x) = f(\sigma^{-1})b$$

wobei wir die Kozykelbedingung ausgenutzt haben. Also gilt $f(\sigma) = b/\sigma(b)$. □

Satz 1.18 (Hilbert 90). *Sei L/K galois,* $\mathrm{Gal}(L/K)$ *ist zyklisch mit Erzeuger sigma$_0$. Für $\alpha \in L^*$ sind äquivalent:*

(i) $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) = 1$

(ii) Es gibt $\beta \in L^*$ mit $\alpha = \beta/\sigma_0(\beta)$

Beweis: Zunächst die einfache Richtung: (ii) nach (i).

$$\prod_\sigma \sigma \frac{\beta}{\sigma_0(\beta)} = \frac{\prod_\sigma \sigma(\beta)}{\prod_\sigma \sigma\sigma_0(\beta)} = 1 \ .$$

Für die Rückrichtung definieren wir

$$f : \mathrm{Gal}(L/K) \to L^* \ , \ \sigma_0^i \mapsto \alpha\sigma_0(\alpha) \dots \sigma_0^{i-1}(\alpha) \ .$$

Behauptung. *Die Abbildung ist wohldefiniert.*

$$\sigma_0^{n+i} \mapsto \alpha\sigma_0(\alpha) \dots \sigma_0^{n-1}(\alpha)\sigma^n(\alpha) \dots \sigma_0^{n+i-1}(\alpha) \ .$$

Nach der Voraussetzung (i) ist das Produkt der ersten n Faktoren 1. Weiterhin gilt $\sigma_0^n(\alpha) = \alpha$ etc., so dass man $f(\sigma_0^i$ zurückerhält.

Behauptung. *f ist ein Kozykel.*

$$f(\sigma_0^i\sigma_0^j) = \alpha \dots \sigma_0^{i-1}(\alpha)\sigma_o^i(\alpha) \dots \sigma_0^{i+j-1}(\alpha) = f(\sigma_0^i)\sigma_0^i(f(\sigma_0^j)) \ .$$

Nach dem letzten Satz existiert ein β mit

$$f(\sigma_0^i(\beta)) = \frac{\beta}{\sigma_0^i(\beta)} \ .$$

Speziell für $i = 1$ erhalten wir $\alpha = f(\sigma_0^1) = \beta/\sigma_0(\beta)$. □

Oft wird auch 1.17 als Hilbert 90 bezeichnet. Es handelt sich um den Satz Nummer 90 aus Hilberts *Zahlbericht* von 1897.

Beweis von Theorem 1.13 (i). Sei L/K und σ_0 wie in Hilbert 90. Außerdem enthalte K eine primitive n-te Einheitswurzel ζ, $(\mathrm{Char}\, K, n) = 1$. Wir wenden Hilbert 90 an auf ζ. Dazu berechnen wir

$$\prod_1^n \sigma_0^i(\zeta) = \zeta^n = 1 \ ,$$

da $\zeta \in K$. Also existiert ein β mit

$$\zeta = \frac{\beta}{\sigma_0(\beta)} \Leftrightarrow \sigma_0(\beta) = \zeta^{-1}\beta \ .$$

Es folgt induktiv $\sigma_0^i(\beta) = \zeta^{-i}\beta$. Also hat β n verschiedene Konjugierte, also $[K(\beta) : K] = n = [L : K]$. β ist primitiv. Außerdem ist $\sigma(\beta^n) = \sigma(\beta)^n = \zeta^i n\beta^n = \beta^n$. Damit liegt $a = \beta^n$ im Grundkörper K. □

Radikale

Wir erinnern noch einmal: Sei $P \in K[X]$, α eine Nullstelle. Dann kann α durch Radikale ausgedrückt werden, wenn $\alpha \in L$ und

$$L = K_n \supset K_{n-1} \supset \cdots \subset K_0 = K$$

wobei K_i/K_{i-1} eine Kummererweiterung ist. Ein Körper E/K ist *durch Radikale auflösbar* (kürzer *auflösbar*), wenn er in einem solchen L liegt.

Bemerkung. Das Wort *Radikal* bedeutet Wurzel, lateinisch Radix. Man vergleiche freie Radikale in der Chemie oder Radiesschen in der Biologie.
In Algebra I haben wir dies bereits mit der Auflösbarkeit von Gruppen in Zusammenhang gebracht.

Definition 1.19. *Sei G eine Gruppe. G heißt* auflösbar*, wenn es eine Kette von Untergruppen*

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

gibt, bei der $G_i \triangleleft G_{i-1}$ und G_{i-1}/G_i abelsch ist.

Theorem 1.20 (vergl. I Theorem 9.1). *Sei E/K eine endliche Erweiterung in Charakteristik 0. Dann sind äquivalent:*

(i) E/K ist auflösbar.

(ii) $\mathrm{Gal}(L/K)$ ist auflösbar.

Beweis: In der Algebra I haben wir die Richtung (i) nach (ii) gezeigt. Dort war $K = \mathbb{Q}$, aber dies spielte keine Rolle. Nun geht es um die Rückrichtung. Es genügt $L = E$ zu betrachten. Sei $G = \mathrm{Gal}(L/K)$,

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

die Kette aus der Definition.

Behauptung. *Sei H eine endliche abelsche Gruppe. Dann gibt es ein Kette von Untergruppen*

$$\{e\} = H_m \subset H_{m-1} \subset \cdots \subset H_0 = H \ ,$$

so dass die Quotienten zyklisch sind.

Sei $e \neq h \in H$ und $H' =< h >$. Falls $H = H'$, so ist H selbst zyklisch. Andernfalls betrachten wir H/H'. Dies ist eine abelsche Gruppe von kleinerer Ordnung. Nach Induktionsvoraussetzung gibt es eine Kette von Untergruppen von H/H' mit zyklischen Quotienten. Ihre Urbilder in H liefern (zusammen mit H') die gesuchte Kette für H.
Dies wenden wir auf alle Quotienten G_{i-1}/G_i an. Die Urbilder in G ergeben eine feinere Kette von Untergruppen von G mit zyklischen Quotienten. Sei nun also G_{i-1}/G_i zyklisch. Sei $K_i = L^{G_i}$ der zugehörige Zwischenkörper. Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(K_{i-1}/K_i) = G_{i-1}/G_i$, also zyklisch. Nach Theorem 1.13 ist dann K_{i-1}/K_i eine Kummererweiterung. □

Kapitel 2

Ringe und Moduln

Alle Ringe sind kommutativ mit Eins.

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 2.1. *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 2.2. *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 2.3. *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 2.4. *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 2.5. *(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 2.6. *(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.

(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 2.7. *(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*

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

(v) Ein Modul M heißt frei*, wenn er 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 2.8. *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 Z-Moduln haben unendliche viele Elemente.

Satz 2.9. *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 5.8. Sei $N = IA^n$, d.h. der Untermodul, der von den ax mit $a \in I$, $x \in A$ 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 2.10 (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 1.19, I Satz 1.20 und I Satz 1.21 liefern diese Ausagen für abelsche Gruppen. Die Verträglichkeit mit der A-Modulstruktur ist leicht zu überprüfen. □

Definition 2.11. *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 2.12 (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 2.13. *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 2.14. *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 2.15. *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 $m \in \mathbb{Z}/2$. 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 2.16 (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) $A \otimes M \cong M$.

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 $f = \tilde{f} \circ \theta$. □

Satz 2.17. *Sei $f : A \to B$ ein Ringhomomorphismus. Dann gibt es Funktoren*

$$\{A\text{-}Moduln\} \otimes \underset{\longleftarrow}{\overset{f_*}{\longrightarrow}} \{B\text{-}Moduln\}$$

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 2.18. *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.

Lemma 2.19. *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 2.20. *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:

$$a + b \mapsto \frac{a}{1} + \frac{b}{1} = \frac{a1 + b1}{1 \cdot 1} = \frac{a + b}{1}$$
$$ab \mapsto \frac{a}{1} fracb1 = \frac{ab}{1}$$

Der Kern ist

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

□

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

Definition 2.21. *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 2.22. *$S^{-1}M$ 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

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

($\hat{s}_i$ 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.

Kapitel 3

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 3.1. *$I \subset A$ 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 5.11), $\mathbb{Q}[i]$ (Übungsaufgabe). Keine Hauptidealringe sind $\mathbb{Q}[\sqrt{-5}]$, $k[X,Y]$ (betrachte $I = (X,Y)$).

Lemma 3.2. *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 3.3. *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 3.4. *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 $v(1) = v(1\dot{1}) = v(1) + v(1)$, 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 andere Ideal ungleich A 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

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

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 3.5. *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 3.6. *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 5.18 gezeigt. Dort ging es um Polynomringe, aber das Argument war allgemein. □

Definition 3.7. *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 3.8. *Hauptidealringe sind faktoriell.*

Beweis: Man vergleiche den Beweis von I Theorem 5.19, den Fall von Polynomringen. Tatsächlich wurde nur verwendet, dass in einem Hauptidealring gerechnet wird. □

Elementarteilersatz

Theorem 3.9 (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, z.B. I Theorem 2.10.

Theorem 3.10 (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 3.10 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 3.9 impliziert also die Eindeutigkeit in 3.10. 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 3.10 impliziert also die Existenz der Zerlegung in 3.10
Der Beweis ist aufwendiger, wir holen aus.

Definition 3.11. *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 3.12. *Sei M ein endlich erzeugter torsionsfreier Modul über einem Hauptidealring. Dann ist M frei.*

Wir arbeiten vor:

Lemma 3.13. *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 3.14. *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 3.12. 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 $a x_i \in < x_1, \ldots, x_n >$ für $i = 1, \ldots, N$. Wir definieren

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

M ist torsionsfrei, daher ist $\operatorname{Ker}\phi = \{x \in M \mid ax = 0\} = 0$. ϕ faktorisiert über $< x_1, \ldots, x_n > \cong A^n$. 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 3.15. *Sei A ein Hauptidealring, M endlich erzeugter A-Modul. Sei*

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

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 3.12 also frei. Die Sequenz

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

ist exakt. Nach Lemma 3.13 (ii) folgt $M \cong T \oplus F$. □

Beweis der Eindeutigkeit in Theorem 3.9. 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 2.9. 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 $T_1 = \{x \in M \mid p_1 x = 0\}$. 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}. T_1 ist ein $A/(p_1)$-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 $f_{ij} = e_{ij}$. 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 3.10. Sei F freier A-Modul vom Rang m, $M \subset F$ ein Untermodul. Nach Lemma 3.14 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 2.4), dass ein $k[X]$-Modul das Gleiche ist wie ein Vektorraum zusammen mit einem Endomorphismus.

Lemma 3.16. *Ein endlich erzeuter $k[X]$-Torsionsmodul ist das Gleiche wie ein endlich dimensionaler k-Vektorraum zusammen mit einer linearen Abbildung $\theta :\to V$.*

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 $\{m, Xm, X^2m, \dot{,}X^nm\}$ 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 3.17. *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

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

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 3.18 (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

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

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 $X, (X-a)X, \ldots, (X-a)^{n-1}X$. Diese Elemente sind tatsächlich linear unabhängig, da sie verschiedene Grade haben. In dieser Basis gilt

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

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.

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.*

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 Primdiealen. 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

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

Definition 4.4. *Ein Ring heißt* lokal*, wenn er nur ein eindeutiges maximales Ideal hat.*

Beispiel. diskrete Bewertungsringe, Körper.

Satz 4.5. *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. □

Warum lokal, Lokalisierung?

Definition 4.6. *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 4.7. Spec A *ist ein topologischer Raum.*

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

(i) $\emptyset$ und 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 $\mathfrak{p}$ enthält weder I_1 noch 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:

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

□

Bemerkung. Ein Punkt von 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 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.

Theorem 4.8 (Hilberts Nullstellensatz). *Sei k algebraisch abgeschlossenener Körper. Dann haben die maximalen Ideale von $k[X_1, \ldots, X_n]$ die Form*

$$(X - a_1, \ldots, X - a_n)$$

für $a_i \in k$. Es gibt ein Bijektion

$$k^n \to |\operatorname{Spec} k[X_1, \ldots, X_n]| \ .$$

Beweis: In nächsten Kapitel. □

Die Topologie auf $\operatorname{Spec} A$ induziert eine Topologie auf $|\operatorname{Spec} A|$. In diesem Fall: $I = (f_1, \dots, f_m) \subset k[X_1, \dots X_n]$, dann ist

$$V(I) \cap |\operatorname{Spec} A| = \{(X - a_1, \dots, X - a_n) \mid f_1, \dots, f_n \in (X - a_1, \dots, X - a_n)\} .$$

Die Bedingung $f \in ((X - a_1, \dots, X - a_n)$ ist äquivalent zu $f(a_1, \dots, f_n) = 0$. Unter der Bijektion mit k^n gilt also

$$V(I) \cap |\operatorname{Spec} A| = \{(a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0 \text{ für } i = 1, \dots m\} .$$

Die abgeschlossenen Mengen sind Nullstellenmengen von Mengen von Polynomen.
Die Topologie, die man so auf k^n (z.B. $\mathbb{C}^n$) erhält, heißt *Zariski-Topologie.*

Lemma 4.9. *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 4.10. *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 4.11. *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* $\operatorname{Spec} S^{-1}$ *und* $\{\mathfrak{p} \in \operatorname{Spec} A \mid S \cap \mathfrak{p} = \emptyset\}$.

Korollar 4.12. *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, 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.

Definition 4.13. *Eine Eigenschaft P eines Moduls heißt* lokal*, wenn: M hat $P \Leftrightarrow M_\mathfrak{p}$ hat P für alle Primideale.*

Lemma 4.14. *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 (I Satz 5.8). 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 4.15. *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

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

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. □

Definition 4.16. *Sei A ein Ring. Die* Krulldimension *von A (oder* $\operatorname{Spec} A$ *ist die maximale Länge n einer Kette von verschiedenen Primidealen von A:*

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

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.

Satz 4.17. *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 inuzieren 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. Der Induktionschrit wird in einem Lemma zusammengefasst. □

Lemma 4.18. *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.*

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 Spec $A[X]/I$ für $I = A[X]\mathfrak{p}$. Hierbei bleiben alle Enthaltenseinsrelationen erhalten. Es ist $A[X]/A[X]\mathfrak{p} \cong (A/\mathfrak{p})[X]$ genügt es also, den Fall $\mathfrak{p} = 0$, A ein Integritätsring zu betrachten. Sei $S = A \setminus \{0\}$. Wir nutzen die Bijektion zwischen 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

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

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.
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 $m = n+1$. □

Bemerkung. Wie vorher gesehen kann für algebraisch abgeschlossene Körper die Menge k^n mit $|\operatorname{Spec} k[X_1, \ldots, X_N]|$ identifiziert werden. Sie hat also die Krulldimension n. Insbesondere stimmen für $\mathbb{C}^n$ die Vektoraumdimension, die Krulldimension überein. Als reelle Mannigfaltigkeit ist die Dimension $2n$.

Kapitel 5

Noethersche Ringe

Definition 5.1. *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 Untermodul 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. Sei M eine endlich abelsche Gruppe. Dann ist M noethersch als $\mathbb{Z}$-Modul.

Lemma 5.2. *Sei A ein Hauptidealring, dann ist A noethersch.*

Beweis: Sei

$$(f_1) \subset (f_2) \subset (f_3) \subset$$

eine Kette von Idealen. Dann sind alle f_i Teiler von f_1. Bis auf Einheit gibt nur endlich viele Teiler von f_1, also können auch nur endlich viele verschiedene Terme in der Kette vorkommen. □

Beispiel. 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 5.3. *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 $N_i =< x_1, \dots, x_i >$. Diese Kette von Untermoduln von M wird nicht stabil, also ist M nicht noethersch.
Seien umgekehrt alle Untermoduln von M endlich erzeugt,

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

eine Kette von Untermoduln. Sei $N = \bigcup_{i \geq 1} M_i$. Nach Voraussetzung ist dieser Modul endlich erzeugt, $N =< x_1, \dots, x_n >$. 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.

Korollar 5.4. *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 5.5. *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 5.6. *Sei A ein noetherscher Ring, S eine multiplikative Teilmenge. Dann ist $S^{-1}A$ noethersch.*

Beweis: Wie wir beim Beweis von Satz 4.11 gesehen haben, sind die Ideal von $S^{-1}A$ von der Form $S^{-1}I$ für Ideale I von A. I ist endlich erzeugt als A-Modul, dann ist $S^{-1}I$ endlich erzeugt als $S^{-1}A$-Modul. □

Satz 5.7. *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. □

Theorem 5.8 (Hilberts Basissatz). *Sei A noetherscher Ring. Dann ist $A[X]$ noethersch.*

Korollar 5.9. *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.

Beweis des Theorems: Sei $I \subset A[X]$ ein Ideal. Für $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ 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 $\mathfrak{a} = (a_1, \dots, a_k)$. Sei a_i führender Koeffizient von $P_i \in I$. Wir betrachten

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

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

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

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 5.10. *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. Wir erhalten 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 k von 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.
$F \subset E$ als F_0-Moduln. Als Untermodul eines endlich erzeugten Moduls über einem noetherschen Ring ist F ein 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 $G_1 G_2 \ldots G_i + 1$ 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 $k(x_1, \ldots, x_r) = k(x_1, \ldots, x_{r-1})$. □

Damit haben wir den Hilbertschen Nullstellensatz bewiesen.

Beweis von Theorem 4.8: Sei k ein algebraisch abgeschlossener Körper, $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ 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. □

Wiederholung

Begriffe

- Ringe, Einheiten, Nullteiler, nullteilerfrei, Integritätsbereich, Primideale, maximale Ideale, lokale Ringe, Krulldimension
- Modul, Untermodul, Modulhomomorphismus, Quotienten, Summe (von Untermoduln), direkte Summe, direktes Produkt, Produkt (Ideal mal Modul), freie Moduln, Rang, Tensorprodukt
- multiplikative Teilmenge, Lokalisierung (speziell an Elementen oder Primidealen), lokale Eigenschaften
- exakte Sequenzenen
- Hauptideale, Hauptidealringe, diskrete Bewertungsringe, irreduzible Elemente, Primelemente, faktorielle Ringe
- Torsionselemente, Torsionsmoduln
- noethersche Ringe

Sätze

- Homomorphiesatz/Isomorphiesätze
- chinesischer Restsatz für beliebige Ringe, Eindeutigkeit der Primfaktorzerlegung für Hauptidealringe
- Elementarteilersatz (1. und 2. Version), Jordansche Normalform
- Zariski-Topologie, Primideale in Lokalisierung und Quotienten
- Dimension des Polynomrings
- Noethersche Ringe stabil unter Lokalisierung und Quotienten, noetherscher Modul versus endlich erzeugt
- Hilberts Basissatz, Hilberts Nullstellensatz

Kapitel 6

Homologische Algebra

In diesem Kapitel fixieren wir einen Ring A. Es schadet nicht, sich einen Körper vorzustellen.

Diagrammjagden

Definition 6.1. *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* $k \circ f = g \circ h$.

Lemma 6.2 (Fünferlemma). *Sei*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{k} & M_2 & \xrightarrow[h]{} & M_3 & \xrightarrow{g} & M_4 & \xrightarrow{l} & M_5 \\ {\scriptstyle f_1}\downarrow & & {\scriptstyle f_2}\downarrow & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ N_1 & \xrightarrow{k} & N_2 & \xrightarrow[h']{} & N_3 & \xrightarrow[g']{} & N_4 & \xrightarrow[l']{} & N_5 \end{array}$$

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.

Satz 6.3 (Schlangenlemma). *Wir betrachten ein kommutatives Diagram*

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{f'} & N_2 & \xrightarrow{g'} & N_3 & & \end{array}$$

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 6.4. *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 (6.2) 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.

Komplexe

Definition 6.5. *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, $\Omega^p(X)$ seien die glatten Differentialformen auf X. Mit der äußeren Ableitung d bilden diese einen Komplex von $\mathbb{R}$-Vektorräumen der Länge $n = \dim X$.

$$0 \to \Omega^0(X) \to \Omega^1(X) \to \Omega^2(X) \to \cdots \to \Omega^n(X) \to 0 \ .$$

Die Bedingung $d^i \circ d^{i-1} = 0$ bedeutet $\operatorname{Im} d^{i-1} \subset \operatorname{Ker} d^i$.

Definition 6.6. *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 6.7. *Sei M ein glatte Mannigfaltigkeit. Dann heißt*

$$H^i(X) = H^i(\Omega^*(X))$$

die i-te de Rham Kohomologie von X.

Beispiel. Sei X eine kompakte Fläche. Dann gilt $\dim H^0(X) = H^2(X) = 1$ und $\dim H^2(X) = 2g$, wobei g das Geschlecht von X ist (die Löcherzahl).

Dies zu beweisen sprengt den Rahmen dieser Vorlesung. Einfachere Fälle sind aber aus der Analysis bekannt.

Satz 6.8 (Poincaré Lemma). *Sei $U \subset \mathbb{R}^n$ offen und sternförmig. Dann gilt*

$$H^0(U) = \mathbb{R},$$
$$H^i(U) = 0 \text{ für alle } i \neq 0 \ .$$

Beweis: Dies ist ein analytischer Satz ist, vergleiche: Forster Analysis 3, §19 Satz 6. Seien $x_1, \ldots, x_n$ die Koordinaten in $\mathbb{R}^n$. Es ist $\Omega^0(U) = C_\infty(U)$ die Menge der glatten Funktionen. Sei $f \in \operatorname{Ker} d^0 = H^0(U)$, d.h.

$$df = \sum \frac{\partial f}{\partial x_i} dx_i = 0 \ .$$

Dies bedeutet, dass alle pariellen Ableitungen verschwinden. Damit ist die Funktion konstant, genauer lokalkonstant. Da U zusammenhängend ist, ist f konstant. Sei nun $\omega \in \operatorname{Ker} d^1$, d.h.

$$\omega = \sum f_i dx_i \text{ mit } d\omega = \sum_{i,j} \frac{\partial f_i}{\partial x_j} dx_j \wedge dx_i = 0 \ .$$

Dies bedeutet konkret $\frac{\partial f_i}{\partial x_j} = \frac{\partial f_j}{\partial x_i}$ für alle $i \neq j$. Diese Art von Systemen von Differentialgleichungen heißt totales Differntial und ist lösbar, d.h. es gibt $f \in C_\infty(M)$ mit $\frac{\partial f}{\partial x_i} = f_i$. Es gilt $\omega = df$, also $\omega = 0 \in H^1(U)$. Höhere Indizes werden durch mehr oder weniger geschicktes Rechnen auf diesen Fall zurückgeführt. Wir benutzen dafür weitere Begriffe der homologischen Algebra. □

Definition 6.9. *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.
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 6.10. *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 $H^i(N^*) = Z^i(N^*)/\operatorname{Im} d^{i-1}$. □

Korollar 6.11. *Sei $\iota^* : N^* \to M^*$ ein Unterkomplex, $p^* : M^* \to N^*$ ein Komplexhomomorphismus, so dass $p^*\iota^* = \mathrm{id}$ und $\iota^* p^* \sim \mathrm{id}$. Dann haben N^* und M^* diesselbe Kohomologie. In dieser Situation heißt N^* auch* Retrakt *von M^*.*

Beweis: Aus dem Lemma folgt $H^i(\iota^* p^*) = H^i(\mathrm{id}) = \mathrm{id}$. Daher sind die Modulhomomorphismen $H^i(p^*)$ und $H^i(\iota^*)$ zueinander invers. □

Beweis des Poincaré Lemmas. Zum Aufwärmen beginnen wir beginnen mit dem eindimensionalen Fall. U ist sternfömig mit Zentrum P. Wir definieren

$$h : \Omega^1(U) \to C_\infty(U) \ , \omega \mapsto \int_P^x \omega \ .$$

Dann setzen wir $p^0 = \mathrm{id}^0 - h \circ d, p^1 = \mathrm{id}^1 - d \circ h$. Nach Konstruktion gilt

$$p \sim \mathrm{id} : \Omega^*(U) \to \Omega^*(U) \ ,$$

Nach dem Hauptsatz der Differential und Integralrechnung ist $p^1 = 0$ und p^0 bildet $f \in C_\infty(U)$ auf die konstante Funktion $f(P)$ ab. Der Unterkomplex, der im Grad null aus den konstanten Funktionen besteht und sonst überall gleich null ist, ist also ein Retrakt von $\Omega^*(U)$. Die Kohomologie des Unterkomplexes ist die behauptete.
Der allgemeine Fall benutzt das gleiche Argument zusammen mit Induktion über die Anzahl der Variablen. Wir betrachten den Komplex $\Omega^*(U)$. Darin gibt es Unterkomplexe M_j^* der Differentialformen, die nur von den ersten j Variablen abhängen,

$$M_j^i = \left\{ \sum f(x_1, \ldots, x_j) dx_{n_1} \wedge \cdots \wedge dx_{n_i} \mid n_i \leq j \right\} \ .$$

Behauptung. *M_{j-1}^* ist ein Retrakt von M_j^*.*

Wir definieren

$$h_j^i : M_j^i \to M_{j-1}^i \ ,$$

durch Integration in Richtung x_j. Genauer:

$$f(x_1,\dots,x_j)dx_{n_1}\wedge\dots\wedge dx_{n_i} \mapsto \begin{cases} \left(\int_P^{x_j} f(x_1,\dots,x_j)dx_j\right) dx_{n_2}\wedge\dots dx_{n_i} & \text{falls } n_1 = j \\ 0 & n_1,\dots,n_i \neq j \end{cases}$$

Wie im eindimensionalen Fall definieren wir p^*, so dass $\mathrm{id} \sim_{h_j^*} p^*$. Die Abbildung p^* faktorisiert über M_{j-1}^i. Nach dem Korollar gilt dann induktiv

$$H^i(M_{j'}^*) = H^i(M_j^*) \ ,$$

Der Komplex M_0^* ist konzentriert in Grad 0 und besteht dort aus den konstanten Funktionen. Der Komplex M_n^* stimmt mit ganz $\Omega^*(U)$ überein. □

Definition 6.12. *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.

Satz 6.13 (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

$$\dots \to H^i(M_1^*) \to H^i(M_2^*) \to H^i(M_3^*) \xrightarrow{\delta^i} H^{i+1}(M_1^*) \to H^{i+1}(M_2^*) \to \dots \ .$$

Beweis: 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

$$\begin{array}{ccccccc} & & M_1^i/B^i(M_1^*)^* & \longrightarrow & M_2^i/B^i(M_2^*) & \longrightarrow & M_3^i/B^i(M_3^*) \longrightarrow 0 \\ & & \downarrow{\scriptstyle d_1^i} & & \downarrow{\scriptstyle d_2^i} & & \downarrow{\scriptstyle d_3^i} \\ 0 & \longrightarrow & Z^{i+1}(M_1^*) & \longrightarrow & Z^{i+1}(M_2^*) & \longrightarrow & Z^{i+1}(M_3^*) \end{array}$$

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. □

Theorem 6.14 (Mayer-Vietoris-Sequenz). *Sei X eine glatte Mannigfaltigkeit, U, V offene Untermannigfaltigkeiten mit $X = U \cup V$. Dann gibt es ein lange exakte Sequenz von de Rham-Kohomologiegruppen:*

$$\cdots H^i(X) \xrightarrow{\psi^i} H^i(U) \oplus H^i(V) \xrightarrow{\phi^i} H^i(U \cap V) \xrightarrow{\delta} H^{i+1}(X) \to \cdots$$

Dabei ist die Abbildung ψ von der Form $\omega \mapsto (\omega|_U, \omega|_V)$, die Abbildung ϕ von der Form $(\omega, \omega') \mapsto \omega|_{U\cap V} - \omega|_{U\cap V}$.

Beweis: Wir betrachten die Sequenz von Komplexen

$$0 \to \Omega^*(X) \xrightarrow{\psi^*} \Omega^*(U) \oplus \Omega^*(V) \xrightarrow{\phi^*} \Omega^*(U \cap V) \to 0$$

wobei die Abbildungen wie im Theorem angegeben definiert sind. Ist sie exakt, so ist die Mayer-Vietoris-Sequenz ein Spezialfall der langen exakten Kohomologiesequenz.
Wir betrachten die Sequenz für festen Index i. Eine Differentialform ω auf X ist eindeutig durch ihre Einschränkungen auf U und V charakterisiert. Also ist ψ^i injektiv.
Die Komposition $\phi^i\psi^i$ ist $\omega \mapsto \omega|_{U\cap V} - \omega|_{U\cap V} = 0$. Sei umgekehrt $(\omega, \omega') \in \operatorname{Ker} \phi^i$, d.h. die beiden Differentialformen stimmen auf $U\cap V$ überein. Zusammen definieren sie eine Differentialform auf $U \cup V = X$, das gesuchte Urbild unter ψ^i.

Behauptung. *ϕ^i ist surjektiv.*

Hier geht eine analytische Tatsache ein, die Teilung der Eins: Es gibt ein Paar von Funktionen $f_U, f_V : X \to [0,1]$ mit $f_U + f_V = 1$, wobei der Träger von f_U bzw. f_V in U enthalten ist (Warner, Foundations of Differentiable Manifolds and Lie Groups, Theorem 1.11). Sei nun ω eine Differentialform auf $U \cap V$.

$$\sigma_U = f_V \omega \ , \ \sigma_V = -f_V \omega \ .$$

Wegen $f_V = 0$ auf $U \setminus U \cap V$ kann σ_U als Differentialform auf ganz U aufgefasst werden, einfach mit Fortsetzung durch 0. Ebenso kann σ_V als Differentialform auf V aufgefasst werden. Es gilt

$$\phi^i(\sigma_U, \sigma_V) = f_U \omega + f_V \omega = \omega \ .$$

□

Beispiel. (i) Falls $U \cap V = \emptyset$, dann bedeutet dies $H^i(X) \to H^i(U) \oplus H^i(V)$ ist injektiv und surjektiv, also ein Isomorphismus.

(ii) Sei $X = S^1 \subset \mathbb{C}$ die Einheitskreislinie. Wir wählen $U = S^1 \setminus \{1\}$, $V = S^1 \setminus \{-1\}$. Als Mannigfaltigkeiten sind also U und V offene Intervalle. Ihre de Rham-Kohomologie ist nach dem Poincaré Lemma bekannt. Weiter ist $U \cap V$ disjunkte Vereinigung von zwei Intervallen. Auch hier ist die Kohomologie bekannt. Die Mayer-Vietoris Sequenz ist also

$$0 \to H^0(S^1) \to \mathbb{R} \oplus \mathbb{R} \xrightarrow{\phi} \mathbb{R} \oplus \mathbb{R} \to H^1(S^1) \to 0 \to 0 \to \\ H^2(S^1) \to 0 \to 0 \to H^3(S^1) \to 0 \to \cdots$$

Hieraus folgt $0 = H^2(S^1) = H^3(S^1) = H^i(S^1)$ für $i > 1$. Nun muss die Abbildung ϕ bestimmt werden. Es ist die zweite Abbildung im Theorem. Die Differentialformen ω und ω' sind nichts als konstante Funktionen auf U und V. Sie schränken sich zu konstanten Funktionen auf $U \cap V$ ein. Die Einschränkungsabbildung $H^0(U) \to H^0(U \cap V)$ ist also die Diagonalabbildung. Es gilt

$$\phi : \mathbb{R} \oplus \mathbb{R} \to \mathbb{R} \oplus \mathbb{R} \ , (x,y) \mapsto (x-y, x-y) \ .$$

Diese Abbildung hat eindimensionalen Kern und Bild. Dann ist auch der Kokern eindimensional. Damit haben wir gezeigt:

$$H^0(S^1) \cong H^1(S^1) \cong \mathbb{R} \ .$$

Allgemeiner:

Korollar 6.15. *Sei S^n für $n > 0$ die n-dimensionale Spähre, $V \subset \mathbb{R}^m$ sternförmig. Für $X = S^n \times V$ gilt*

$$H^0(X) \cong H^n(X) \cong \mathbb{R} \ ; H^i(X) = 0 \text{ für } i \neq 0, n \ .$$

Beweis: Beweis durch vollständige Induktion nach n für alle m gleichzeitig. Für $n = 1$ ist dies gerade das Beispiel von oben. Man beachte nur zusätzlich, dass eine Menge der Form Intervall mal sternförmig ebenfalls sternförmig ist.
Sei nun die Aussage für n bewiesen. Wir betrachten

$$S^{n+1} = \{(x_0, \ldots, x_{n+1}) \mid \sum x_i^2 = 1\} \ .$$

Der Nordpol sei der Punkt $N = (0, \ldots, 0, 1)$, der Südpol sei $S = (0, \ldots, 0, -1)$. Sei $U_N = S^{n+1} \setminus \{N\}, U_S = S^{n+1} \setminus \{S\}$ und $U_{NS} = U_N \cap U_S = S^{n+1} \setminus \{N, S\}$. $U_N \times V$ und $U_S \times V$ sind isomorph zu sternförmigen Mengen. Ihre Kohomologie wurde also im Poincaré Lemma 6.8 berechnet. Wir betrachten nun U_{SN}. Es ist isomorph zu $S^n \times (-1, 1)$, denn für festes x_{n+1} erhält man eine n-dimensionale Spähre vom Radius $1-x_{n+1}^2$. Nach Induktionsvoraussetzung ist die Kohomologie von $S^n \times (-1, 1) \times V$ ebenfalls bekannt. Die Mayer-Vietoris Sequenz liefert

$$\begin{aligned} 0 \to H^0(X) \to H^0(U_N) \oplus H^0(U_S) \xrightarrow{\phi} H^0(U_{NS}) \xrightarrow{\delta^1} H^1(X) \to 0 \cdots \\ 0 \to 0 \to H^i(X) \to 0 \to 0 \cdots \\ 0 \to H^n(U_{NS}) \to H^{n+1}(X) \to 0 \end{aligned}$$

Die Abbildung ϕ wird wie im $n = 1$ Fall analysiert. Sie ist surjektiv mit eindimensionalem Kern. Daher gilt $H^0(X) \cong \mathbb{R}$. Außerdem ist $\operatorname{Ker} \delta^1 = H^0(U_{NS}$. Dies impliziert $\operatorname{Im} \delta^1 = 0$. Hieraus folgt $H^1(X) = 0$. Die Aussage für die übrigen Indizes folgt unmittelbar. □

Korollar 6.16. *Sei $\mathbb{R}^n \cong \mathbb{R}^m$ als glatte Mannigfaltigkeit. Dann gilt $n = m$.*

Beweis: Wir betrachten $X = \mathbb{R}^n \setminus \{0\}$. Mittels Polarkoordinaten ist dies isomorph zu $S^{n-1} \times (0, \infty)$. Nach dem letzten Korollar gilt $H^{n-1}(X) \cong \mathbb{R}$ und $H^i(X) = 0$ für $i \neq 0, n-1$. Die Dimension von X (und damit auch $\mathbb{R}^n$) kann also aus der Kohomologie abgelesen werden. □

Bemerkung. Tatsächlich ist die Dimension eine topologische Invariante. Um dies zu zeigen, benutzt man die sogenannte *singuläre Kohomologie*.

Kapitel 7

Gruppenkohomologie

In diesem Kapitel sei G eine endliche Gruppe. Wir erinnern uns (I Definition 3.1): eine Abbildung $G \times M \to M$ heißt Operation, falls $em = m$ für alle $m \in M$ und das neutrale Element $e \in G$ und $(gh)m = g(hm)$ für alle $g, h \in G$, $m \in M$. Eine solche Operation war äquivalent zu einem Gruppenhomomorphismus

$$\phi : G \to \mathrm{Aut}(M) \ ,$$

wobei $\mathrm{Aut}(M)$ die Gruppe der bijektiven Abbildungen $M \to M$ ist.

Definition 7.1. *Ein* G-Modul *ist eine abelsche Gruppe M mit einer Operation*

$$G \times M \to M$$

der Gruppe G, so dass Operation und Gruppenstruktur verträglich sind, d.h.

$$g(m+n) = gm + gn \text{ für alle } g \in G, m, n \in M \ .$$

Ein Morphismus von G-Moduln *ist ein Gruppenhomomorphismus $f : M \to N$ zwischen G-Moduln, der gleichzeitig mit der Operation verträglich ist, d.h. $f(gm) = gf(m)$ für alle $g \in G$, $m \in M$.*

Beispiel. (i) Für beliebige G, M gibt es die triviale Darstellung Operation $(g, m) = m$.

(ii) Sei L/K eine endliche Körpererweiterung, $G = \mathrm{Gal}(L/K)$, $M = L$. Dann ist L ein G-Modul mit der natürlichen Operation von G, da alle Elemente von G Homomorphismen der abelschen Gruppe L sind.

(iii) Mit dem gleichen G wie eben ist auch $M = L^*$ mit der natürlichen Operation von G ein G-Modul, da die Elemente von G Null auf Null abbilden und mit der Multiplikation verträglich sind.

(iv) Sei M ein freier Z-Modul mit Basis $e_1, \ldots, e_n$, $G = S_n$. Dann setzt sich die Operation $(\sigma, e_i) \mapsto e_{\sigma(i)}$ auf den Basiselementen zu einer G-Modulstruktur auf M fort. Diese Operation haben wir in Algebra I bei der Definition des Vorzeichens von σ benutzt.

Lemma 7.2. *Ein G-Modul ist äquivalent zu einem Gruppenhomomorphismus*

$$G \to \mathrm{Aut}_{\mathbb{Z}}(M) \ ,$$

wobei $\mathrm{Aut}_{\mathbb{Z}}(M)$ *die Gruppe der Automorphismen des* $\mathbb{Z}$*-Moduls* M *ist.*

Beweis: $\mathrm{Aut}_{\mathbb{Z}}(M)$ ist eine Untergruppe von $\mathrm{Aut}(M)$. Zu zeigen ist also, dass das vorher erwähnte ϕ über $\mathrm{Aut}_{\mathbb{Z}}(M)$ faktorisiert. Sei $g \in G$, $\phi(G) : M \to M$ war durch $\phi(g)(m) = gm$ definiert. Nach dem Axiom eines G-Moduls gilt

$$\phi(g)(m+n) = g(m+n) = gm + gn = \phi(g)(m) + \phi(g)(n) \ ,$$

d.h. $\phi(g)$ ist ein Morphismus von $\mathbb{Z}$-Moduln. Da er bijektiv ist, ist er sogar ein Isomorphismus. □

Es gibt noch einen anderen Standpunkt.

Definition 7.3. *Sei G eine endliche Gruppe. Der* Gruppenring *von G ist*

$$\mathbb{Z}[G] = \bigoplus_{g \in G} \mathbb{Z} \ ,$$

mit der folgenden Multiplikation: Wir schreiben g für das Basiselement, das 1 *in der g-ten Komponente ist und* 0 *sonst. Dann ist*

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g,h \in G} a_g b_h gh \ .$$

Dies ist ein (im allgemeinen nichtkommutativer) Ring mit Einselement e.

Lemma 7.4. *Ein G-Modul ist dasselbe wie ein Linksmodul für den Ring $\mathbb{Z}[G]$. Ein Morphismus von G-Moduln ist dasselbe wie ein Homomorphismus von $\mathbb{Z}[G]$-Moduln.*

Beweis: Sei $G \times M \to M$ die Operation. Dann definiert man eine Skalarmultiplikation

$$\mathbb{Z}[G] \times M \to M \ , (\sum_{g \in G} a_g g, m) \mapsto \sum_{g \in G} a_g gm \ .$$

Alle Modulaxiome sind leicht zu überprüfen. Ist umkehrt eine Skalalmultiplikation mit $\mathbb{Z}[G]$ gegeben, so definiert $(g, m) \mapsto m$ die Operation. □

Alle Konstruktionen für Moduln (z.B. direkte Summe, Produkt) lassen sich also auch für G-Moduln ausführen. Im Falle des Tensorproduktes ist Vorsicht geboten. Tensorprodukte von Moduln über nichtkommutativen Ringen haben wir nicht behandelt.

Bemerkung. Natürlich kann man den Ring $\mathbb{Z}$ durch durch einen anderen kommutativen Ring A ersetzen. Man verlangt dann zusätzlich, dass die Operation auch mit der Skalarmultiplikation verträglich ist. Dies entspricht dann einem

$A[G]$-Modul. Ist speziell $A = k$ ein Körper, so spricht man von einer *Darstellung*. In diesem Fall nimmt man meist den Standpunkt der Abbildung

$$G \to \mathrm{Aut}_k(M)$$

ein, d.h. jedem Gruppenelement wird eine Matrix zugeordnet. Wir bleiben der Einfachheit halber bei $A = \mathbb{Z}$.
Wir erinnern uns: Ist M eine Menge mit der Operation einer Gruppe G, so ist $M^G = \{m \in M \mid gm = m \text{ für alle } g \in G\}$ die Teilmenge der Fixpunkte. Ist M ein G-Modul, so ist M^G ein Untermodul.
Wir wollen nun jedem G-Modul einen Komplex zuordnen.

Definition 7.5. *Sei G eine endliche Gruppe, M ein G-Modul. Für $n \in \mathbb{N}_0$ sei $X^n(G,M)$ die abelsche Gruppe der mengentheoretischen Abbildungen $G^{n+1} \to M$. Die Addition wird von der Addition auf M induziert. $X^n(G,M)$ wird zu einem G-Modul durch*

$$(gf)(g_0,\dots,g_n) = gf(g^{-1}g_0,\dots,g^{-1}g_n) \ .$$

Sei

$$C^n(G,M) := X^n(G,M)^G = \{f : G^{n+1} \to M \mid f(gg_0,\dots,gg_n) = gf(g_0,\dots,g_n) \ .$$

Sei $d^n : X^n(G,M) \to X^{n+1}(G,M)$ definiert durch

$$(d^n f) : G^{n+1} \to M \ , (g_0,\dot{,}g_{n+1}) \mapsto \sum_{i=0}^{n+1} (-1)^i f(g_0,\dots,\hat{g}_i,\dots,g_{n+1}) \ ,$$

wobei $(g_0,\dots,\hat{g}_i,\dots,g_n)$ bedeutet, dass $\hat{g}_i$ weggelassen wird.

Lemma 7.6. *d^n induziert eine Abbildung*

$$C^n(G,M) \to C^{n+1}(G,M) \ .$$

$(X^n(G,M), d^n)$ und $(C^n(G,M), d^n)$ sind Komplexe von abelschen Gruppen.

Beweis: Sei $f \in C^n(G,M)$. Wir müssen überprüfen, dass $d^n f$ eine G-lineare Abbildung ist.

$$\begin{aligned}(d^n f)(gg_0,\dots,gg_{n+1}) &= \sum_{i=0}^{n+1}(-1)^i f(fg_0,\dots,g\hat{g}_i,\dots,gg_{n+1}) \\ &= \sum_{i=0}^{n+1}(-1)^i gf(g_0,\dots,\hat{g}_i,\dots,g_{n+1}) = gd^n f(g_0,\dots,g_{n+1}) \ .\end{aligned}$$

Es genügt nun $d^{n+1}d^n = 0$ auf $X^n(G,M)$ zu überprüfen. Sei also $f \in X^n(G,M)$.

$$(d^{n+1}d^n f)(g_0,\dots,g_{n+2}) = \sum_{i=0}^{n+2}(-1)^i d^n f(g_0,\dots,\hat{g}_i,\dots,g_n) \ .$$

Die Berechnung von $d^n f$ fügt eine weitere Summe $\sum_{j=0}^{n+1}(-1)^j f(\dots)$ ein. Wir beachten, dass der j-te Eintrag von $g_0, \dots, \hat{g}_i, \dots, g_n$ entweder g_j ist (falls $j < i$) oder g_{j+1} (falls $j \geq i$). Daher

$$\begin{aligned}
&= \sum_{j<i}(-1)^{i+j} f(\dots, \hat{g}_j, \dots, \hat{g}_i, \dots) + \sum_{j\geq i}(-1)^{i+j} f(\dots, \hat{g}_i, \dots, \hat{g}_{j+1}, \dots) \\
&= \sum_{j<i}(-1)^{i+j} f(\dots, \hat{g}_j, \dots, \hat{g}_i, \dots) + \sum_{i\geq j}(-1)^{i+j} f(\dots, \hat{g}_j, \dots, \hat{g}_{i+1}, \dots) \\
&= \sum_{j<i}(-1)^{i+j} f(\dots, \hat{g}_j, \dots, \hat{g}_i, \dots) + \sum_{i<j}(-1)^{i+j-1} f(\dots, \hat{g}_j, \dots, \hat{g}_i, \dots) \\
&= 0 \ .
\end{aligned}$$

Dabei wurde (jeweils in der zweiten Summe) in der zweiten Zeile die Benennung von i und j vertauscht und in der dritten Zeile $i+1$ durch i ersetzt. □

Definition 7.7. *Sei $H^n(G, M)$ die n-te Kohomologie des Komplexes $C^*(G, M)$. Dies ist* Gruppenkohomologie von G mit Koeffizienten in M.

Bemerkung. Die Endlichkeitsbedingung an G haben wir nicht verwendet. Bei unendlichen Gruppen benutzt man aber meist Zusatzstrukturen aus. Bei $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ oder $\mathrm{GL}_n(\mathbb{R})$ etwa die Topologien.

Satz 7.8. *Sei G eine endliche Gruppe, M ein G-Modul. Es gilt*

$$\begin{aligned}
H^0(G, M) &\cong M^G \\
H^1(G, M) &\cong \{f : G \to M \mid f(gh) = f(g) + gf(h)\}/\sim
\end{aligned}$$

Dabei ist $f \sim 0$, falls es ein $m \in M$ gibt mit $f(g) = gm - m$. Die Abbildungen in $H^1(G, M)$ heißen auch verschränkte Homomorphismen.

Beweis: Nach Definition ist $X^0(G, M) = \{f : G \to M\}$, hierin $C^0(G, M)$ die Untergruppe der f mit $f(gh) = gf(h)$. Wir betrachten

$$\phi : C^0(G, M) \to M \ , f \mapsto f(e) \ .$$

Dies ist offensichtlich verträglich mit der Addition. ϕ ist injektiv, denn aus $f(e) = 0$ folgt $f(g) = gf(0) = g0 = 0$. Sei $m \in M$. Wir definieren f durch $f(g) = gm$. Dies ist ein Urbild unter ϕ. Nach Definition gilt

$$d^0 f(g, h) = f(h) - f(g) \ .$$

Eine Abbildung liegt im Kern von d^0 genau dann, wenn sie konstant ist. Dies bedeutet $gf(e) = f(e)$, d.h. $f(e) \in M^G$.
Wir betrachten nun $C^1(G, M)$. Die Elemente sind Abbildungen $f : G^2 \to M$ mit $f(gg_0, gg_1) = gf(g_0, g_1)$. Wir betrachten

$$\psi : C^1(G, M) \to X^0(G, M) \ , \psi(f) : g \mapsto f(e, g) \ .$$

Wie in der Dimension 0 ist dies ein Isomorphismus von abelschen Gruppen, denn $f(g,h) = gf(e,g^{-1}h)$. Es gilt

$$\begin{aligned} d^1 f(g_0,g_1,g_2) &= f(g_1,g_2) - f(g_0,g_2) + f(g_0,g_1) \\ &= g_1 f(e,g_1^{-1}g_2) - g_0 f(e,g_0^{-1}g_2) + g_0 f(e,g_0^{-1}g_1) \end{aligned}$$

In Termen von $f' = \psi(f)$ bedeutet $d^1 f = 0$ also

$$g_0 f'(g_0^{-1}g_2) = g_1 f'(g_1^{-1}g_2) + g_0 f'(g_0^{-1}g_1)$$

oder äquivalent

$$f'(g_0^{-1}g_2) = g_0^{-1}g_1 f'(g_1^{-1}g_2) + f'(g_0^{-1}g_1) \ .$$

Setzt man speziell $g_1 = e$, so sieht man, dass f' ein verschränkter Homomorphismus ist. Sei andererseits f' ein verschränkter Homomorphismus. Es gilt auf jeden Fall

$$f'(e) = f'(g^{-1}g) = f'(g^{-1}) + g^{-1}f'(g) \ .$$

Speziell mit $g = e$ impliziert dies $f'(e) = 0$. Es gilt also für einen verschränkten Homomorphismus f'

$$\begin{aligned} &g_0^{-1}g_1 f'(g_1^{-1}g_2) + f'(g_0^{-1}g_1) \\ &\quad = g_0^{-1}g_1 f'(g_1^{-1}) + g_0^{-1}g_1 g_1^{-1} f'(g_2) + f'(g_0^{-1}) + g_0^{-1}f'(g_1) \\ &\quad\quad = g_0^{-1}[g_1 f'(g_1^{-1} + f'(g_1)] + [g_0^{-1}f'(g_2) + f'(g_0^{-1})] \\ &\quad\quad\quad = 0 + f'(g_0^{-1}g_2) \ . \end{aligned}$$

Wir haben also gezeigt, dass die Menge der Zyklen in $C^1(G,M)$ mit der Menge der verschränkten Homomorphismen identifiziert werden kann.
Bei $f \in d^0(C^0(G,M))$, d.h. $f = d^0(f_0)$. Nach Definition $f(g,h) = f_0(h) - f_0(g) = hf_0(e) - gf_0(e)$. Dann ist $\psi(f)(h) = f(e,h) = gf_0(e) - f_0(e)$. Mit $m = f(0)$ ist dies genau die Definition der Äquivalenzrelation. □

Korollar 7.9. *Ist M ein trivialer G-Modul, d.h. $M^G = M$, so ist $H^1(G,M) = \mathrm{Hom}(G,M)$.*

Beweis: Aus verschränkten Homomorphismen werden nun Homomorphismen, die Äquivalenzrelation ist trivial. □

Auch die triviale Operation liefert also interessante Invarianten von G!

Korollar 7.10. *Sei L/K eine endliche Galoiserweiterung. Dann ist*

$$H^1(\mathrm{Gal}(L/K), L^*) = H^1(L/K, L^*)$$

aus Definition 1.16.

Beweis: Wir haben die obige Berechnung als Definition benutzt. □

Allgemein schreibt man für $H^n(\mathrm{Gal}(L/K), M)$ auch $H^n(L/K, M)$. In Satz 1.17 (Hilbert 90) haben wir gezeigt, dass stets $H^1(L/K, L^*) = 1$.

Satz 7.11. *Sei L/K endliche Galoiserweiterung. Dann gilt $H^0(L/K, L) = K$ und $H^i(L/K, L) = 0$ für $i > 0$.*

Beweis: Der Fall $i = 0$ ist im wesentlichen erledigt. Nach Satz n=0,1 ist $H^0(L/K, L) = L^G = K$, da die Erweiterung galois ist. Für allgemeines i benutzt man die Existenz einer Normalbasis (Theorem 1.7). Es besagt, dass L als G-Modul isomorph zu $K[G]$ ist. Wir skizzieren den Rest des Argumentes: Es ist $C^n(G, K[G])$ ist isomorph zu dem Komplex $X^{n-1}(G, K)$ (mit trivialer Operation von G auf K). Dieser Komplex hat triviale Kohomologie (Übungsaufgabe oder z.B. Neukirch, Schmidt, Wingberg, Cohomology of Number Fields, Prop. 1.2.1). □

Satz 7.12 (Kohomologiesequenz). *Sei $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von G-Moduln. Dann gibt es eine kanonische lange exakte Sequenz*

$$\cdots \to H^n(G, M') \to H^n(G, M) \to H^n(G, M'') \to H^{n+1}(G, M') \to \cdots$$

Beweis: Offensichtlich induziert die Sequenz von Moduln eine Sequenz

$$0 \to C^*(G, M') \to C^*(G, M) \to C^*(G, M'') \to 0 \ .$$

Behauptung. *Diese Sequenz ist exakt.*

Sei $f : G^{n+1} \to M'$ ein Element von $C^n(G, M')$. Durch Verknüpfen mit $M' \to M$ wird dies zu einem Element von $C^n(G, M)$. Gilt $f(g_0, \ldots, g_n) = 0 \in M$, dann ist auch $f(g_0, \ldots, g_n) = 0 \in M'$, d.h. $f = 0$. Sei nun $f \in C^n(G, M)$, so dass die Verknüpfung mit $M \to M''$ Null liefert. Für jedes Tupel gilt also $f(g_0, \ldots, g_n) \in M'$, d.h. $f \in C^n(G, M')$.
Das Argument für die Surjektivität ist ein wenig komplizierter. Sei $f \in C^n(G, M'')$. Wir wählen für jedes $f(e, g_1, \ldots, g_n)$ ein Urbild in M. Dies definiert eine Abbildung $f' : \{e\} \times G^n \to M$. Diese wird G-äquivariant auch G^{n+1} fortgesetzt. Dieses Element von $C^n(G, M)$ ist das gesuchte Urbild von f.
Nach Satz 6.13 induziert eine exakte Sequenz von Komplexen eine lange exakte Sequenz von Kohomologiegruppen. □

Satz 7.13. *Sei L/K eine endliche Galoiserweiterung,* $(\mathrm{Char}(K), n) = 1$ *und K enthalte die Gruppe μ_n der n-ten Einheitswurzeln. Dann gilt*

$$(L^*)^n \cap K^*/(K^*)^n \cong H^1(L/K, \mu_n) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}/n) \ ,$$

wobei $(L^*)^n$ die Gruppe der n-ten Potenzen in L^* ist.

Beweis: Wir betrachten die Sequenz von $G = \mathrm{Gal}(L/K)$-Moduln

$$1 \to \mu_n \to L^* \xrightarrow{\cdot^n} (L^*)^n \to 1 \ .$$

Die erste Abbildung ist offensichtlich injektiv, die letzte surjektiv. Ein Element im Kern der n-Potenzierung sind die Einheitswurzeln. Damit ist die Sequenz exakt. Die zugehörige lange exakte Kohomologiesequenz lautet mit Hilbert 90 und da die Erweiterung galois ist:

$$1 \to \mu_n \to (K^*) \to ((L^*)^n) \cap K^* \to H^1(G, \mu_n) \to 0 \ .$$

Damit ist $H^1(G, \mu_n)$ in der angegebenen Art berechnet. Die Gruppe μ_n ist zyklisch mit n Elementen. Wegen $\mu_n \subset K$ ist die Operation der Galoisgruppe trivial, d.h. $\mathbb{Z}/n \cong \mu_n$ als G-Moduln. □

Läßt man in dem obigen Isomorphismus L immer größer werden, so erhält man schließlich

$$K^*/(K^*)^n \cong \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K, \mathbb{Z}/n) \ .$$

Zu einem Element a in K^* gehört eine Abbildung $\mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n$. Sei H der Kern dieser Abbildung. Dies ist ein Normalteiler. Der Fixkörper $L = \overline{K}^H$ hat Galoisgruppe isomorph zu einer Untergruppe von $\mathbb{Z}/n$. Tatsächlich entsteht er durch Adjungieren einer n-ten Wurzel von a. Wir sind gerade dabei, die Kummertheorie aus Kapitel 1 neu zu entdecken!

Bemerkung. Klassenkörpertheorie klassifiziert alle abelschen Erweiterungen von Zahlkörpern, also endlichen Erweiterungen von $\mathbb{Q}$. Wesentliches Hilfsmittel ist hier $H^2(L/K, \mu_n)$. Dies ist typischer Stoff einer Vorlesung algebraische Zahlentheorie II.

Kapitel 8

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 8.1. *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.
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 8.2. *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 2.17).

(iii) Es gibt einen Funktor von Integritätsringen nach Körpern, der jeden Integritätsring seinen Quotientenkörper zuordnet.

(iv) Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dies definiert einen kovarianten Funktor zwischen den zugeordenten Kategorien. Eine kontravariante Variante erhält man durch $g \mapsto \phi(g^{-1}$.

(v) De Rham-Kohomologie definiert einen kontravarianten Funktor von Mannigfaltigkeiten in reele Vektorräume. (Vergleiche das Beispiel nach Definition 6.9).

(vi) 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.

(vii) 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 8.3. *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 8.4. *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 2.22).

(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 8.5. *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 8.6 (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).

Definition 8.7. *Seien $F : \mathcal{C} \to \mathcal{D}$ und $G : \mathcal{D} \to \mathcal{C}$ Funktoren. F heißt* linksadjungiert *zu G und G heißt* rechtsadjungiert *zu F, falls es Transformationen von Funktoren $\mathrm{id}_{\mathcal{C}} \to G \circ F$ und $F \circ G \to \mathrm{id}_{\mathcal{D}}$ gibt, so dass die induzierte Abbildung*

$$\mathrm{Mor}_{\mathcal{D}}(F(A), B) \to \mathrm{Mor}_{\mathcal{C}}(A, G(B))$$

für alle $A \in \mathrm{Ob}(\mathcal{C})$ und $B \in \mathrm{Ob}(\mathcal{D})$ bijektiv ist.

Korollar 8.8. *Sei $F : \mathcal{C} \to \mathcal{D}$ ein Funktor. Falls der linksadunguierte von F exitiert, so ist er eindeutig bis auf Äquivalenz von Funktoren.*

Beweis: Dies ist ein Fall des Yoneda Lemmas. □

Beispiel. (i) Der Vergissfunktor von der Kategorie der Gruppen in die Kategorie der Mengen hat den linkdsadjungierten Funktor, der einer Menge S die freie Gruppe $F(S)$ über S zuordnet:

$$\mathrm{Mor}(F(S), G) = \mathrm{Abb}(S, G) \ .$$

(ii) Ebenso ist der Funktor, der einer Menge S den freien A-Modul über der Basis S zuordnet, linksadjungiert zum Vergissfunktor von Moduln nach Mengen.

(iii) Der Vergissfunktor von topologischen Räumen in Mengen hat den linksadjungierten Funktor, der eine Menge mit der diskreten Topologie (alle Teilmengen offen) versieht. Er hat auch einen rechtsadjungierten, nämlich den Funktor, der eine Menge mit der trivialen Topologie versieht (nur M und $\emptyset$ offen).

(iv) Sei $A \to B$ ein Ringhomomorphismus. Dann sind Restriktion und Koeffizientenerweiterung adjungiert.

Definition 8.9. *Eine Kategorie $\mathcal{C}$ heißt* additiv*, falls alle* $\mathrm{Mor}_{\mathcal{C}}(A, B)$ *abelsche Gruppen sind, die Verknüpfung $\circ$ $\mathbb{Z}$-bilinear ist und es ein Nullobjekt, endliche direkte Summen und Produkte gibt. Dabei ist* 0 *ein* Nullobjekt*, falls*

$$\mathrm{Mor}_{\mathcal{C}}(A, 0) = \mathrm{Mor}_{\mathcal{C}}(0, A) = 0 \ .$$

Für je zwei Objekte A, B ist die direkte Summe *(das* direkte Produkt*) ein Objekt $A \oplus B$, Morphismen $A \to A \oplus B$ und $B \to A \oplus B$, (bzw. $A \times B$ und Morphismen $A \times B \to A, B$), das universell ist mit dieser Eigenschaft, also*

$$\mathrm{Mor}_{\mathcal{C}}(A \oplus B, \cdot) = \mathrm{Mor}_{\mathcal{C}}(A, \cdot) \times \mathrm{Mor}_{\mathcal{C}}(B, \cdot)$$

bzw.

$$\mathrm{Mor}_{\mathcal{C}}(\cdot, A \oplus B) = \mathrm{Mor}_{\mathcal{C}}(\cdot, A) \times \mathrm{Mor}_{\mathcal{C}}(\cdot, B)$$

Beispiel. (i) Die Kategorie der K-Vektorräume ist additiv, ebenso abelsche Gruppen oder A-Moduln.

(ii) Die Kategorie der topologischen Räume oder die Kategorie der Gruppen sind nicht additiv.

(iii) Die Kategorie der Ringe ist additiv. (Betrachtet man Ringe mit Eins, so muss man auf die Bedingung $0 \neq 1$ verzichteten oder das Nullobjekt fehlt). Die Kategorie der Körper ist nicht additiv, da es im allgemeinen keine direkten Summen gibt.

(iv) In der Kategorie der abelschen Gruppen stimmen direkte Summe und direktes Produkt überein. Aber z.B. in der Kategorie der topologischen Räume ist die disjunkte Vereinigung die direkte Summe und das Produkt das direkte Produkt. In der Kategorie der Gruppen erhält man das freie Produkt und das direkte Produkt.

Definition 8.10. *Seien $\mathcal{A}, \mathcal{B}$ additive Kategorien. Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt* additiv*, falls* $\mathrm{Mor}_{\mathcal{A}}(A, B) \to \mathrm{Mor}_{\mathcal{B}}(F(A), F(B))$ *ein Gruppenhomomorphismus ist.*

Beispiel. Ist $\mathcal{A}$ additiv, dann hat $\mathrm{Mor}_A\, h(\cdot, A)$ Werte in der Kategorie der abelschen Gruppen. Der Funktor ist additiv.

Definition 8.11. *Sei $\mathcal{A}$ eine additive Kategorie, $f : A \to B$ ein Morphismus. Ein Objekt K mit einem Morphismus $K \to A$ heißt* Kern *von f, falls*

$$\mathrm{Mor}_{\mathcal{A}}(X, K) = \{g \in \mathrm{Mor}_{\mathcal{A}}(X, A) \mid f \circ g = 0\} \ .$$

Ein Objekt C mit einem Morphismus $B \to C$ heißt Kokern *von f, falls*

$$\mathrm{Mor}_{\mathcal{A}}(C, Y) = \{h \in \mathrm{Mor}(B, Y) \mid h \circ f = 0\} \ .$$

Eine Kategorie $\mathcal{A}$ heißt abelsch*, falls $\mathcal{A}$ additiv ist, jeder Morphismus $f : A \to B$ Kern und Kokern hat und*

$$\mathrm{Coker}(\mathrm{Ker}(f) \to A) \cong \mathrm{Ker}(B \to \mathrm{Coker}(f)) \ .$$

Beispiel. Prototyp einer abelschen Kategorie ist die Kategorie der abelschen Gruppen, ebenso die Kategorie der Vektorräume oder die Kategorie der A-Moduln. Ebenso die Kategorie der Komplexe von A-Moduln. Nicht abelsch ist die Kategorie der Ringe mit Eins.

Die homologische Algebra aus dem letzten Kapitel funktioniert wörtlich in allen abelschen Kategorien.

Definition 8.12. *Seien $\mathcal{A}$, $\mathcal{B}$ abelsche Kategorien, $F : \mathcal{A} \to \mathcal{B}$ sei additiv. F heißt* linksexakt *bzw.* rechtsexakt*, falls eine kurze exakte Sequenz*

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

auf eine exakte Sequenz

$$0 \to F(A_1) \to F(A_2) \to F(A_3)$$

(bzw. $F(A_1) \to F(A_2) \to F(A_3) \to 0$) abgebildet wird.

Beispiel. (i) $\mathrm{Mor}_{\mathcal{A}}(\cdot, A)$ und $\mathrm{Mor}_{\mathcal{A}}(A, \cdot)$ sind linksexakt. Auf der Kategorie der Vektorräume sind sie sogar exakt.

(ii) $\otimes_A M$ ist ein rechtsexakter Funktor auf der Kategorie der A-Moduln. Falls M frei ist, ist er sogar exakt.

(iii) Lokalisieren ist ein exakter Funktor auf der Kategorie der A-Moduln.

(iv) Auf der Kategorie der G-Moduln ist $M \mapsto M^G$ ein linksexakter Funktor.

Wie im Fall der Gruppenkohomologie dient Kohomologie oft dazu, aus einem linksexakten Funktor eine lange exakte Kohomologiesequenz zu machen.

Kapitel 9

Ausblick

Algebraische Geometrie

Eine *affine Varietät* über $\mathbb{C}$ wird durch eine Teilmenge von $M \subset \mathbb{C}[X_1, \ldots, X_n]$ definiert:

$$V(M) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid P(x_1, \ldots, x_n) = 0 \text{ für alle } P \in M\} \ .$$

Da der Polynomring noethersch ist, (Hilberts Basissatz Theorem 5.8, genügen nur endliche viele Gleichungen. Hilberts Nullstellensatz 4.8 erlaubt es, die Punkte von M mit den maximalen Idealen von $\mathbb{C}[X_1, \ldots, X_n]/I$ zu identifizieren, wobei I das Ideal der Polynome ist, die auf ganz $V(M)$ verschwinden. Mit der Zariski-Topologie erhalten wir einen topologischen Raum.
Eine *projektive Varietät* über $\mathbb{C}$ wird durch eine Teilmenge von homogenen Polynomen in $\mathbb{C}[X_0, \ldots, X_n]$ definiert:

$$V(M) = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{C}) \mid P(x_0, \ldots, x_n) = 0 \text{ für alle } P \in M\} \ .$$

Auch projektive Varietät werden mit der Zariski-Topologie versehen. Lokal ist eine affine Varietät affin.
Algebraische Geometrie beschäftigt sich mit den Eigenschaften von Varietäten, z.B.:

Theorem 9.1 (Satz von Bezout). *Seien $V_1, V_2 \subset \mathbb{P}^2(\mathbb{C})$ Kurven, die durch je ein Polynom vom Grad n bzw. m definiert werden. Haben V_1 und V_2 nur isolierte Schnittpunkte, dann beträgt die Anzahl der Schnittpunkte, mit Vielfachheit gezählt, genau nm.*

Die Schwierigkeiten sind natürlich zunächst einmal, die Begriffe "isolierte Schnittpunkte" und "Vielfachheit" zu definieren.
Man kann bei diesen Überlegungen leicht $\mathbb{C}$ durch einen anderen algebraische abgeschlossenen Körper ersetzen. Bei allgemeinen Körpern haben die Gleichungen jedoch nur noch wenige Lösungen:

Theorem 9.2 (Faltings, Mordellvermutung). *Sei V eine algebraische Kurve über $\mathbb{Q}$ vom Geschlecht mindestens 2. Dann hat V nur endlich viele Punkte über $\mathbb{Q}$.*

Beispiel. Für $V \subset \mathbb{P}^2(\mathbb{Q})$ eine ebene Kurve vom Grad d läßt sich das Geschlecht als $(d-1)(d-2)/2$ berechnen. Das Theorem von Faltings deckt also die Fermatgleichung $x^d + y^d = 1$ für $d > 3$ ab. Sie hat nur endliche viele rationale Lösungen.

Die Punktmengen sind also zur Definition von Varitäten über beliebigen Körpern nicht geeignet. Die Definition über das Spektrum $\operatorname{Spec} k[X_1, \ldots, X_n]/I$ funktioniert jedoch tadellos.
Der Funktionenkörper einer Varietät ist die Menge der Morphismen $V \to \mathbb{P}^1$ - nachdem man definiert hat, was ein Morphismus ist.
Algebraische Geometrie lebt von geometrischen Ideen und Begriffen. Die grundlegenden Sätze müssen mit Mitteln der kommutativen Algebra gezeigt werden. Wie in allen geometrischen Disziplinen spielt Kohomologie eine sehr große Rolle.

Zahlentheorie

Objekte der Zahlentheorie sind $\mathbb{Z}$, $\mathbb{Q}$ und ihre endlichen Erweiterungen.

Definition 9.3. *Ein* Zahlkörper *ist eine endliche Körpererweiterung von $\mathbb{Q}$. Der* Ganzheitsring *eine Zahlkörpers K ist*

$$\mathcal{O}_K = \{x \in K \mid \text{ es gibt } n, a_i \in \mathbb{Z} \text{ mit } x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0\}$$

In der algebraischen Zahlentheorie zeigt man, dass diese Ringe Dedekindringe sind: noethersche, eindimensional, alle lokalen Ringe sind diskrete Bewertungsringe. Im allgemeinen sind sie jedoch keine Hauptidealringe. Die Eindeutigkeit der Primfaktorzerlegung ist falsch.

Beispiel. Der Ganzheitsring von $\mathbb{Q}(\omega)$ mit $\omega^N = 1$ ist $\mathbb{Z}[\omega]$, von $\mathbb{Q}(i)$ ist $\mathbb{Z}[i]$, von $\mathbb{Q}(\sqrt{-5})$ ist $\mathbb{Z}[\sqrt{-3}]$.

Die beiden ersten echten Sätze der Zahlentheorie sind die Endlicherzeugtheit der Einheitengruppe $\mathcal{O}^*$ und die Endlichkeit der Klassenzahl, d.h. der Ordnung von

$$\frac{\text{Halbgruppe der Ideale ungleich Null von } \mathcal{O}}{\text{Halbgruppe der Hauptideale ungleich Null}} .$$

Eine der Folgerungen der Klassenkörpertheorie ist die Existenz eines Klassenkörpers:

Theorem 9.4. *Sei K ein Zahlkörper. Dann gibt es eine endliche Erweiterung F/K, so dass $\mathcal{O}_F$ ein Hauptidealring ist. Die Galoisgruppe* $\operatorname{Gal}(F/K)$ *ist isomorph zur Klassengruppe von K.*

Man verwendet beimm Beweis dieser Sätze viel Algebra, auch Galoiskohomologie, aber auch ein wenig Analysis. Es gibt auch einen ganzen Zweig der Zahlentheorie, den man analytisch nennt. Hier studiert man Funktionen wie die Riemannsche ζ-Funktion:

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p \text{ prim}} (1 - p^{-s})^{-1} \ .$$

Die Reihe und das Produkt konvergieren für $\Re s > 1/2$. Die Funktion setzt sich aber zu einer meromorphen Funktion auf $\mathbb{C}$. Einziger Pol ist 1.
Aus dem Verhalten der ζ-Funktion kann man Eigenschaften der Primzahlen ablesen.

Theorem 9.5 (Primzahlsatz). *Für $x \in \mathbb{R}$ sei $\pi(x)$ die Anzahl der Primzahlen kleiner gleich x. Dann ist $\pi(x)$ assymtotisch gleich $x/\log(x)$.*

Die berühmte Riemannsche Vermutung läßt feinere Aussagen zu.

Arithmetische Geometrie

Dies ist die Vereinigung von algebraischer Geometrie und Zahlentheorie. Man studiert Polynomgleichungen über $\mathbb{Z}$, indem man die zugehörigen geometrischen Objekte studiert. Dieser Zugang hat sich in den letzten Jahrzehnten als viel fruchtbarer erwiesen als das isolierte Studium von Zahlkörpern. Der größte Erfolg der letzten Zeit war der Beweis der Vermutung von Shimura-Taniyama-Weil:

Theorem 9.6 (Wiles, Taylor-Wiles et. al). *Jede elliptische Kurve über $\mathbb{Q}$ ist modular.*

Eine elliptische Kurve ist eine glatte Kurve vom Geschlecht 1. Über $\mathbb{Q}$ bedeutet, dass sie durch ein rationales Polynom definiert wird. Modular bedeutet, dass es eine surjektive holomorphe Abbildung $\mathbb{H}/\Gamma(N) \to E(\mathbb{C})$ gibt, wobei $\mathbb{H}$ die obere Halbebene ist und $\Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$ die Untergruppe der Matrizen, die modulo N kongruent zur Einheitsmatrix sind.

Darstellungstheorie

Ein Thema, dass zu kurz kam: Endliche Gruppen studiert man durch ihre *Darstellungen*, d.h. die Abbildunge $G \to \mathrm{Aut}_{\mathbb{C}}(V)$, wobei V ein endlichdimensionaler $\mathbb{C}$-Vektorraum ist. Es gibt nur endliche Bausteine aus der alle Darstellungen zusammengesetzt sind.
Ein ähnliches Phänomen tritt auf, wenn man Darstellungen von Liegruppen (Gruppen, die gleichzeitig Mannigfaltigkeiten sind) studiert. Man stellt nun zusätzlich maßtheoretische Bedingungen. Dann sind die Darstellungen von kompakten Liegruppen automatisch endlich dimensional. Mehr noch, man gewisse kompakten Liegruppen über ihre Darstellungstheorie vollständig klassifizieren.

Sonstiges

Damit ist die Liste natürlich noch lange nicht abgeschlossen...