

Algebra II

Prof. Dr. Uwe Jannsen Sommersemester 2007

§1 Unendliche Galoistheorie

Erinnerung: Eine algebraische Körpererweiterung L/K heißt **galoissch**, wenn sie normal und separabel ist. Hierfür muss L/K keinen endlichen Grad haben. Zum Beispiel ist für einen endlichen Körper \mathbb{F}_p mit p Elementen (p Primzahl) der algebraische Abschluss $\overline{\mathbb{F}_p}$ galoissch über \mathbb{F}_p . Wir definieren auch in dieser allgemeinen Situation

Definition 1.1 $Gal(L/K) := Aut_K(L) = \{\sigma : L \rightarrow L \mid \sigma \text{ Körperautomorphismus, } \sigma(x) = x \text{ für alle } x \in K\}$.

Der Hauptsatz der Galoistheorie gilt aber in der einfachen Form (Korrespondenz zwischen allen Untergruppen von $Gal(L/K)$ und allen Zwischenkörpern von L/K) nur für endliche Erweiterungen! Um hier eine richtige Aussage zu erhalten, braucht man eine Topologie auf $Gal(L/K)$:

Definition 1.2 Sei L/K eine Galoiserweiterung. Die **Krulltopologie** auf $G = Gal(L/K)$ ist dadurch definiert, dass für jedes Element $\sigma \in G$ die Nebenklassen

$$\sigma \cdot Gal(L/K') \quad , \quad K'/K \text{ endlich,}$$

eine Umgebungsbasis von σ bilden.

Dies liefert wirklich eine Topologie: nach Standardsätzen der Topologie haben wir zu zeigen: Seien $\sigma \in Gal(L/K')$ und $\tau \in Gal(L/K'')$ wie oben gegeben, und sei $\rho \in \sigma Gal(L/K') \cap \tau Gal(L/K'')$. Dann gibt es eine endliche Erweiterung K'''/K mit

$$\rho Gal(L/K''') \subseteq \sigma Gal(L/K') \cap \tau Gal(L/K'').$$

Dies gilt aber für $K''' = K' \cdot K''$ (Kompositum), denn es ist $Gal(L/K''') = Gal(L/K') \cap Gal(L/K'')$ und wegen $\rho \in \sigma Gal(L/K')$ folgt $\rho Gal(L/K''') \subseteq \sigma Gal(L/K')$ und ebenso folgt $\rho Gal(L/K''') \subseteq \tau Gal(L/K'')$.

Lemma 1.3 Mit dieser Topologie wird $G = Gal(L/K)$ eine **topologische** Gruppe, d.h., die Multiplikation

$$\mu : G \times G \rightarrow G, \quad (\sigma, \tau) \mapsto \sigma\tau$$

und die Inversenbildung

$$\iota : G \rightarrow G, \quad \sigma \mapsto \sigma^{-1}$$

sind stetige Abbildungen.

Beweis: selbst

Satz 1.4 $G = Gal(L/K)$ ist (bezüglich der Krulltopologie) kompakt (also insbesondere hausdorffsch) und total unzusammenhängend (d.h., für jedes $\sigma \in G$ ist die Zusammenhangskomponente von σ gleich $\{\sigma\}$).

Zum Beweis bemerken wir

Bemerkungen 1.5 (a) Sei H eine topologische Gruppe (siehe 1.3). Dann ist für jedes $\tau \in H$ die Linkstranslation

$$L_\tau : H \rightarrow H \quad , \quad \sigma \mapsto \tau\sigma$$

ein Homöomorphismus (entsprechend für die Rechtstranslation $R_\tau : \sigma \mapsto \sigma\tau$). Denn $L_\tau = \mu(\tau, -)$ ist stetig, mit Inversem $L_{\tau^{-1}}$. Also vermittelt τ Bijektionen

$$\begin{aligned} U_1 = \{ \text{Umgebungen der Eins} \} &\rightarrow U_2 = \{ \text{Umgebungen von } \tau \} \\ Z(1) &\rightarrow Z(\tau) \end{aligned}$$

wobei $Z(\sigma)$ die Zusammenhangskomponente eines Elements σ bezeichnet.

(b) Ist L/K endlich, so ist die Krulltopologie auf $\text{Gal}(L/K)$ die diskrete Topologie (da $\{\sigma\}$ offen ist für jedes $\sigma \in \text{Gal}(L/K)$, also jede Teilmenge).

Lemma 1.6 Die Abbildung

$$\begin{array}{ccc} h : \text{Gal}(L/K) & \rightarrow & \prod_{\substack{K'/K \text{ endlich, normal} \\ K' \subseteq L}} \text{Gal}(K'/K) \\ \sigma & \mapsto & (\sigma|_{K'}) \end{array}$$

ist injektiv mit abgeschlossenem Bild

$$\tilde{G} := \{(\sigma_{K'}) \in \prod \text{Gal}(K'/K) \mid \text{für } K' \subseteq K'' \text{ gilt } \sigma_{K''}|_{K'} = \sigma_{K'}\}.$$

(Sprechweise: Wir nennen eine Familie $(\sigma_{K'})$ kompatibel, wenn sie in \tilde{G} liegt).

Die Abbildung

$$G \xrightarrow{h} \tilde{G}$$

ist ein Homöomorphismus. (Hierbei trägt $\prod \text{Gal}(K'/K)$ die Produkttopologie bezüglich der diskreten Topologien auf den endlichen Gruppen $\text{Gal}(K'/K)$).

Erinnerung 1.7 Sei $(X_i)_{i \in I}$ eine Familie von topologischen Räumen. Die Produkttopologie auf

$$X = \prod_{i \in I} X_i$$

ist die Topologie, für die die Mengen

$$U = \prod_{i \in I} U_i$$

mit $U_i \subseteq X_i$ offen für alle i und $U_i = X_i$ für fast alle i eine Basis bilden (d.h., die offenen Mengen sind Vereinigungen dieser Mengen). Eine Subbasis bilden die Mengen

$$\prod_{\substack{i \in I \\ i \neq j}} X_i \times U_j$$

für $j \in I$ und $U_j \subseteq X_j$ offen (endliche Durchschnitte von diesen Mengen bilden eine Basis der Topologie).

Diese Produkttopologie ist die größte Topologie, für die alle Projektionen

$$p_i : X \rightarrow X_i$$

stetig sind. Ist Y ein topologischer Raum, so ist eine Abbildung $f : Y \rightarrow \prod_{i \in I} X_i$ genau dann stetig, wenn alle Komponentenabbildungen $f_i = p_i \circ f : Y \rightarrow X_i$ stetig sind. Dies liefert die universelle Eigenschaft

$$Abb_{st}(Y, \prod_{i \in I} X_i) \xrightarrow{\sim} \prod_{i \in I} Abb_{st}(Y, X_i),$$

wobei $Abb_{st}(Y, X)$ die Menge der stetigen Abbildungen $f : Y \rightarrow X$ bezeichnet.

Beweis von Lemma 1.6: Sei $(L_i)_{i \in I}$ die Familie der Zwischenkörper L_i von L/K mit L_i/K endlich und galoissch. Wir betrachten also

$$h : G := Gal(L/K) \rightarrow \prod_{i \in I} Gal(L_i/K) =: H$$

(a) h ist injektiv: Ist $\sigma|_{L_i} = id$ für alle $i \in I$, so ist $\sigma|_{K'} = id$ für alle Teilkörper K' von L/K die endlich über K sind (betrachte den Normalenkörper $N(K') \supset K' \supset K$, der einer der Körper L_i ist). Daher ist $\sigma = id$.

(b) $h(G) = \tilde{G}$: “ \subseteq ” klar

“ \supseteq ” Ist (σ_{L_i}) eine kompatible Familie, so definiere $\sigma \in Gal(L/K)$ mit $\sigma(x) = \sigma_{L_i}(x)$ für $x \in L_i$ (beachte $\bigcup_{i \in I} L_i = L$, s.o.).

(c) \tilde{G} ist abgeschlossen: Wir zeigen, dass das Komplement von \tilde{G} offen ist. Sei $(\sigma_i) \in \prod_{i \in I} Gal(L_i/K)$, $(\sigma_i) \notin \tilde{G}$, also nicht kompatibel. Also gibt es $j, k \in I$ mit $L_j \subseteq L_k$ aber $\sigma_k|_{L_j} \neq \sigma_j$. Dann ist die Menge

$$\{(\tau_i) \in \prod_{i \in I} Gal(L_i/K) \mid \tau_j = \sigma_j, \tau_k = \sigma_k\}$$

eine offene Umgebung von (σ_i) , die im Komplement von \tilde{G} liegt.

(d) h ist stetig: Die Mengen

$$U = U_{j, \sigma_j} = \prod_{i \neq j} Gal(L_i/K) \times \{\sigma_j\},$$

für $j \in I$ und $\sigma_j \in Gal(L_j/K)$, bilden eine Subbasis der Produkttopologie. Hat σ_j kein Urbild in $Gal(L/K)$, so ist $h^{-1}(U)$ leer, also offen (wir werden später sehen, dass dieser Fall nicht eintritt). Ist σ ein Urbild von σ_j in $Gal(L/K)$, so ist $h^{-1}(U) = \sigma \cdot Gal(L/L_j)$ offen.

(e) h ist offen aufs Bild: $h(\sigma Gal(L/L_j)) = h(G) \cap U_{j, \sigma_j}$ für $\sigma_j = \sigma|_{L_j}$. Also ist h ein Homöomorphismus und wir haben Lemma 1.6 bewiesen.

Hieraus folgt nun die erste Behauptung in Satz 1.4, da $\prod_{i \in I} Gal(L_i/K)$ nach dem Satz von Tychonov (siehe z.B. Lang ‘Real Analysis’ II §3 Theorem 3) kompakt ist, und \tilde{G} hierin

abgeschlossen. Für die zweite Behauptung genügt es zu zeigen, dass $H = \prod_{i \in I} Gal(L_i/K)$ total unzusammenhängend ist.

Dazu zeigen wir, dass $Z(1)$, die Zusammenhangskomponente der Eins in H , gleich $\{1\}$ ist (hieraus folgt mit 1.5 $Z(\sigma) = \sigma$ für alle $\sigma \in G$): Offenbar liegt $Z(1)$ in jeder Menge M , die 1 enthält und zugleich offen und abgeschlossen ist (aus $Z(1) = (Z(1) \cap M) \cup (Z(1) \cap CM)$ folgt $Z(1) \cap CM = \emptyset$, da $Z(1)$ zusammenhängend und $Z(1) \cap M \neq \emptyset$ ist). Damit liegt $Z(1)$ im Durchschnitt aller Untergruppen $U_{j,1} = \prod_{i \neq j} Gal(L_i/K) \times \{1\}$. Dieser Durchschnitt ist aber $\{1\}$.

Wir erhalten nun

Satz 1.8 (Hauptsatz der Galoistheorie für unendliche Erweiterungen) (a) Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = Gal(L/K)$. Dann ist die Zuordnung

$$\Psi : K' \rightsquigarrow Gal(L/K')$$

eine bijektive, Inklusions-umkehrende Bijektion zwischen den Zwischenkörpern von L/K und den *abgeschlossenen* Untergruppen von G . Die Umkehrabbildung ist

$$\Phi : U \rightsquigarrow L^U,$$

wobei $L^U = \{x \in L \mid ux = x \text{ für alle } u \in U\}$ der Fixkörper von U in L ist.

(b) Die offenen Untergruppen von G entsprechen gerade den Zwischenkörpern $K \subseteq K' \subseteq L$, für die K'/K endlich ist.

(c) Für einen Zwischenkörper $K \subseteq K' \subseteq L$ ist K'/K genau dann normal, wenn $Gal(L/K')$ ein Normalteiler in $Gal(L/K)$ ist. In diesem Fall hat man einen kanonischen Isomorphismus von topologischen Gruppen

$$Gal(L/K)/Gal(L/K') \xrightarrow{\sim} Gal(K'/K).$$

Wir benötigen

Lemma 1.9 Ist eine Untergruppe U einer topologischen Gruppe H offen, so ist sie auch abgeschlossen. Ist U abgeschlossen und von endlichem Index, so ist U auch offen.

Beweis: 1) Für jedes $h \in H$ ist die Nebenklasse hU wieder offen (1.5). Daher ist

$$H \setminus U = \bigcup_{h \notin U} hU$$

offen.

2) Ist $\sigma_1, \dots, \sigma_n$ ein Repräsentantensystem für H/U , $\sigma_1 \in U$, so ist $H \setminus U = \bigcup_{i=2}^n \sigma_i U$ abgeschlossen. \square

Lemma 1.10 Ist L/K galoissch und K' ein Zwischenkörper, der wieder galoissch über K ist, so ist der Homomorphismus

$$\begin{aligned} Gal(L/K) &\rightarrow Gal(K'/K) \\ \sigma &\mapsto \sigma|_{K'} \end{aligned}$$

surjektiv.

Beweis Sei Ω ein algebraischer Abschluss von L und $\bar{\sigma} \in Gal(K'/K)$. Der K -Homomorphismus

$$\varphi : K' \xrightarrow{\bar{\sigma}} K' \hookrightarrow L \hookrightarrow \Omega$$

lässt sich nach Algebra I, Lemma 16.9 zu einem Isomorphismus $\psi : \Omega \rightarrow \Omega$ fortsetzen, wobei wir K' vermöge $K' \hookrightarrow L \hookrightarrow \Omega$ einbetten. Wir erhalten also ein kommutatives Diagramm

$$\begin{array}{ccc} \Omega & \xrightarrow[\sim]{\psi} & \Omega \\ \downarrow L & & \downarrow L \\ K' & \xrightarrow{\bar{\sigma}} & K' \\ & \searrow & \swarrow \\ & K & \end{array}$$

Da L/K normal ist, gilt $\psi(L) \subseteq L$ (Ist $\alpha \in L$ und p das Minimalpolynom von α über K , so ist $\psi(\alpha)$ wieder eine Nullstelle von p , also in L). Durch Betrachtung von ψ^{-1} sehen wir, dass $\sigma = \psi|_L : L \rightarrow L$ ein Isomorphismus ist, also $\sigma \in Gal(L/K)$, und nach Konstruktion ist $\sigma|_{K'} = \bar{\sigma}$.

Beweis von Satz 1.8: (a): Wohldefiniertheit der Korrespondenz: Ist K'/K eine endliche Teilerweiterung von L/K , so ist $Gal(L/K')$ nach Definition offen, und nach 1.9 auch abgeschlossen. Ist K'/K eine beliebige Teilerweiterung, so ist

$$Gal(L/K') = \bigcap_{\nu} Gal(L/K_{\nu}),$$

wobei K_{ν}/K die endlichen Teilerweiterungen von K/K' durchläuft (jedes $\alpha \in K$ ist in der endlichen Teilerweiterung $K(\alpha)/K$ enthalten). Also ist $Gal(L/K')$ abgeschlossen.

Weiter ist klar, dass für Zwischenkörper $K' \subseteq K''$ von L/K die Inklusion $Gal(L/K'') \subseteq Gal(L/K')$ gilt und für abgeschlossene Untergruppen $U \leq V$ von $Gal(L/K)$ die Inklusion $L^V \subseteq L^U$.

Bijektivität der Korrespondenz: 1) Sei K' Zwischenkörper, dann ist $L^{Gal(L/K')} = K'$ also $\Phi\Psi = id$:

Die Inklusion " \supseteq " ist klar. Angenommen es gibt ein $\alpha \in L^{Gal(L/K')}$ mit $\alpha \notin K'$. Dann gibt es eine endliche Galoiserweiterung N/K' in L/K' mit $\alpha \in N$, und ein $\bar{\sigma} \in Gal(N/K')$ mit $\bar{\sigma}\alpha \neq \alpha$ (denn $N^{Gal(N/K')} = K'$ nach klassischer Galoistheorie). Aber nach 1.10 gibt es ein $\sigma \in Gal(L/K')$ mit $\sigma|_N = \bar{\sigma}$, also $\sigma\alpha \neq \alpha$. Widerspruch dazu dass $\alpha \in L^{Gal(L/K')}$!

2) Ist $H \leq Gal(L/K)$ eine abgeschlossene Untergruppe, so ist $Gal(L/L^H) = H$ also $\Psi\Phi = id$: Wir zeigen allgemeiner:

Lemma 1.11 Ist $H \leq Gal(L/K)$ eine beliebige Untergruppe und \overline{H} der Abschluss, so ist $\overline{H} = Gal(L/L^H)$.

Beweis Sei wieder $(L_i)_{i \in I}$ die Familie der Zwischenkörper von L/K mit L_i/K endlich galoissch. Sei $f_i : Gal(L/K) \rightarrow Gal(L_i/K)$ die Einschränkungabbildung und $H_i = f_i(H)$. Wegen $L = \bigcup_{i \in I} L_i$ liegt $\sigma \in Gal(L/K)$ genau dann in $Gal(L/L^H)$, wenn $\sigma|_{L_i}$ für alle $i \in I$

trivial auf $L_i^H = L_i^{H_i}$ operiert. Nach endlicher Galoistheorie gilt dies genau dann, wenn $\sigma|_{L_i} \in H_i$, denn $Gal(L_i/L_i^{H_i}) = H_i$. Also gilt

$\sigma \in Gal(L/L^H) \Leftrightarrow$ für alle $i \in I$ ist $f_i(\sigma) \in H_i$

\Leftrightarrow für alle $i \in I$ gibt es ein $\tau_i \in H$ mit $f_i(\tau_i) = f_i(\sigma)$

\Leftrightarrow für alle $i \in I$ gibt es ein $\tau_i \in H$ mit $\tau_i \in f_i^{-1}(f_i(\sigma)) = \sigma Gal(L/L_i)$

\Leftrightarrow für alle $i \in I$ ist $\sigma Gal(L/L_i) \cap H \neq \emptyset$

$\Leftrightarrow \sigma \in \overline{H}$,

denn die Mengen $\sigma Gal(L/L_i)$ bilden eine Umgebungsbasis von σ (ist K'/K endlicher Zwischenkörper von L/K und $N(K')/K$ der Normalenkörper, so ist $Gal(L/N(K')) \subseteq Gal(L/K')$).

b) Wir zeigen, dass die offenen Untergruppen $U \leq Gal(L/K)$ den endlichen Zwischenerweiterungen entsprechen:

Ist K'/K eine endliche Erweiterung, $K' \subset L$, so ist nach Definition der Krulltopologie $Gal(L/K')$ offen. Ist umgekehrt $U \leq Gal(L/K)$ eine offene Untergruppe, so gibt es einen Zwischenkörper $K \subseteq K' \subset L$ mit K'/K endlich, so dass $Gal(L/K') \subseteq U$. Es folgt

$$K \subseteq L^U \subseteq L^{Gal(L/K')} = K'$$

und damit die Endlichkeit von L^U/K .

c) Ist K'/K ein Zwischenkörper von L/K und $\sigma \in Gal(L/K)$, so gilt offenbar

$$Gal(L/\sigma(K')) = \sigma Gal(L/K) \sigma^{-1}.$$

Ist K'/K normal, so gilt $\sigma(K') = K'$, also $Gal(L/\sigma(K')) = Gal(L/K')$ für alle σ , also ist dies ein Normalteiler. Ist umgekehrt $Gal(L/K')$ ein Normalteiler, so folgt mit der Galoiskorrespondenz $\sigma(K') = K'$ für alle $\sigma \in Gal(L/K)$. Hieraus folgt, dass K'/K normal ist: Ist $\alpha \in K'$ und $\tilde{\alpha}$ ein Konjugiertes von α in einem algebraischen Abschluss \overline{L} von L , also eine andere Nullstelle des Minimalpolynoms von α über K , so gibt es nach Algebra I, Satz 16.15, eine K -Einbettung $\psi : L \rightarrow \overline{L}$ mit $\psi(\alpha) = \tilde{\alpha}$. Da L/K galoissch ist, gilt $\psi(L) \subseteq L$ und $\sigma = \psi|_L \in Gal(L/K)$. Wegen $\sigma(K') = K'$ folgt $\tilde{\alpha} \in K'$!

Nach 1.10 ist weiter

$$Gal(L/K) \rightarrow Gal(K'/K)$$

surjektiv mit Kern $Gal(L/K')$. Mit dem Homomorphiesatz folgt die Isomorphie

$$Gal(L/K)/Gal(L/K') \xrightarrow{\sim} Gal(K'/K).$$

Wir haben noch die Topologie zu betrachten. Rechts nehmen wir die Krulltopologie. Links sei die Quotiententopologie (bezüglich der Krulltopologie auf $Gal(L/K)$ und der Surjektion $\pi : Gal(L/K) \rightarrow Gal(L/K)/Gal(L/K')$) betrachtet:

Ist $f : X \rightarrow Y$ eine Abbildung, wobei X ein topologischer Raum ist, so gibt es eine feinste Topologie auf Y , für die f stetig ist: definiere

$$V \subseteq Y \text{ offen} \quad :\Leftrightarrow \quad f^{-1}(V) \subseteq X \text{ offen}.$$

Diese Topologie heißt die Finaltopologie bezüglich f . Ist f surjektiv, so spricht man auch von der Quotiententopologie.

Dass, mit diesen Topologien, der obige Gruppenhomomorphismus ein Homöomorphismus ist, folgt nun aus der Übungsaufgabe 2) ii).

§2 Projektive und induktive Limiten

Um Galoisgruppen konzeptioneller beschreiben zu können, führen wir projektive Limiten ein, die auch in anderen Gebieten der Mathematik wichtig sind. Der duale Begriff (im Sinne der Kategorientheorie) ist der von induktiven Limiten.

Definition 2.1 Eine (teil-)geordnete Menge (I, \leq) heißt filtrierend (oder gerichtet, oder induktiv geordnet), wenn gilt:

Für je zwei Elemente $i, j \in I$ gibt es ein $k \in I$ mit $i \leq k$ und $j \leq k$.

Beispiele 2.2 (a) Jede totalgeordnete Menge ist filtrierend, zum Beispiel (\mathbb{N}, \leq) .

(b) Die Potenzmenge $\mathfrak{P}(M)$ einer Menge M ist bezüglich der Inklusion \subseteq filtrierend.

(c) Sei L/K eine Körpererweiterung. Die Menge aller Zwischenkörper K' ist bezüglich der Inklusion filtrierend geordnet.

(d) Dasselbe gilt für alle endlichen Teilerweiterungen K'/K , und ebenso für alle endlichen normalen Teilerweiterungen K''/K .

(e) \mathbb{N} mit der Teilerordnung $|$ ist filtrierend geordnet.

Definition 2.3 Sei I eine filtrierend geordnete Menge. Ein induktives (bzw. projektives) System von Mengen ist eine Familie

$$((X_i)_{i \in I}, (\alpha_{ij})_{i \leq j}) \quad (\text{bzw. } ((X_i)_{i \in I}, (\beta_{ji})_{i \leq j}))$$

von Mengen X_i (für $i \in I$) und Abbildungen

$$\begin{aligned} \alpha_{ij} &: X_i \rightarrow X_j \quad (\text{für } i \leq j \text{ in } I) \\ (\text{bzw. } \beta_{ji} &: X_j \rightarrow X_i \quad (\text{für } i \leq j \text{ in } I)) \end{aligned}$$

so dass gilt

$$\begin{aligned} \alpha_{jk} \circ \alpha_{ij} &= \alpha_{ik} \quad \text{für } i \leq j \leq k \\ (\text{bzw. } \beta_{ji} \circ \beta_{kj} &= \beta_{ki} \quad \text{für } i \leq j \leq k). \end{aligned}$$

Die Abbildungen α_{ij} (bzw. β_{ji}) heißen die Übergangsabbildungen des Systems.

Man erhält also den Begriff des projektiven Systems aus dem eines induktiven Systems durch “Umdrehen der Pfeile”. Ebenso hat man projektive und induktive Systeme von Gruppen (die X_i sind Gruppen und die Übergangsabbildungen sind Homomorphismen) oder Ringen (...) oder topologischen Räumen (....).

Beispiele 2.4 (a) Sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Dann erhält man ein projektives System von Ringen über (\mathbb{N}, \leq) durch

$$\begin{aligned} n &\mapsto R/\mathfrak{a}^n \\ m \leq n &\mapsto R/\mathfrak{a}^n \rightarrow R/\mathfrak{a}^m. \end{aligned}$$

Insbesondere hat man das projektive System

$$(\mathbb{Z}/p^n\mathbb{Z})_{n \in \mathbb{N}}$$

mit Übergangsabbildungen

$$\dots \rightarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow \dots \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

(b) Man erhält ein **projektives** System von abelschen Gruppen über $(\mathbb{N}, |)$ durch

$$\begin{aligned} n &\mapsto \mathbb{Z}/n\mathbb{Z} \\ m | n &\mapsto \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}. \end{aligned}$$

(c) Man erhält ein **induktives** System über $(\mathbb{N}, |)$ durch

$$\begin{aligned} n &\mapsto \mathbb{Z}/n\mathbb{Z} \\ m | n &\mapsto \mathbb{Z}/m \rightarrow \mathbb{Z}/n\mathbb{Z} \\ &\quad \bar{a} \mapsto \frac{n}{m} \cdot \bar{a}. \end{aligned}$$

(d) Sei L/K eine Galoiserweiterung. Dann ist die Menge $\mathcal{K} = \mathcal{K}_{L/K}$ der endlichen galoisschen Körpererweiterungen K'/K induktiv geordnet (2.2(d)), und wir erhalten ein projektives System von endlichen Gruppen über K durch

$$\begin{aligned} K' &\mapsto \text{Gal}(K'/K) \\ K' \subseteq K'' &\mapsto \text{Gal}(K''/K) \rightarrow \text{Gal}(K'/K). \end{aligned}$$

Definition 2.5 (a) Der projektive Limes $X = \varprojlim_{i \in I} X_i$ eines projektiven Systems (X_i, β_{ji})

von Mengen ist definiert als die Menge

$$\varprojlim_{i \in I} X_i := \{(x_i) \in \prod_{i \in I} X_i \mid \beta_{ji}(x_j) = x_i \text{ für alle } i \leq j\}$$

der **kompatiblen Familien** im Produkt $\prod_{i \in I} X_i$.

(b) Der induktive Limes $\varinjlim_{i \in I} X_i$ eines induktiven Systems (X_i, α_{ij}) von Mengen ist definiert als der Quotient

$$\varinjlim_{i \in I} X_i := \prod_{i \in I} X_i / \sim$$

der disjunkten Vereinigung $\coprod_{i \in I} X_i$ der Mengen X_i nach der folgenden Äquivalenzrelation \sim : für $x_i \in X_i$ und $x_j \in X_j$ gilt

$$x_i \sim x_j \iff \exists k \in I, i, j \leq k \text{ mit } \alpha_{ik}(x_i) = \alpha_{jk}(x_j) \text{ in } X_k.$$

Haben die X_i Zusatzstrukturen, so überträgt sich dies üblicherweise auf die Limiten. Hat man z.B. ein projektives (bzw. induktives) System von Gruppen, so ist der projektive (bzw. induktive) Limes wieder eine Gruppe. Entsprechendes gilt für Ringe etc.

Beispiele 2.6 (vergleiche 2.4) (a) Sei R ein Ring und \mathfrak{a} ein Ideal. Dann heißt

$$\hat{R} := \varprojlim_n R/\mathfrak{a}^n$$

die \mathfrak{a} -adische Kompletterung von R und ist ein Ring. Die Elemente von \hat{R} sind kompatible Familien $(\bar{a}_n)_{n \in \mathbb{N}}$ mit $\bar{a}_n \in R/\mathfrak{a}^n$.

Die Kompatibilität heißt, dass für Repräsentanten a_n von \bar{a}_n gilt:

$$a_{n+1} \equiv a_n \pmod{\mathfrak{a}^n}.$$

Man hat einen Ringhomomorphismus

$$\begin{aligned} \varphi : R &\rightarrow \hat{R} \\ a &\mapsto (\bar{a})_{n \in \mathbb{N}}, \end{aligned}$$

der im allgemeinen weder injektiv noch surjektiv ist. Offenbar ist

$$\ker \varphi = \bigcap_{n \geq 1} \mathfrak{a}^n.$$

Sei zum Beispiel $R = \mathbb{Z}$ und $\mathfrak{a} = (p)$ das von einer Primzahl p erzeugte Hauptideal. Dann heißt

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n \mathbb{Z}$$

die **p -adische Kompletterung** von \mathbb{Z} . Die Abbildung $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_p$ ist injektiv, da offenbar $\bigcap_{n \geq 1} (p^n) = 0$. Jedes Element $\bar{\alpha} \in \mathbb{Z}/p^n \mathbb{Z}$ wird durch ein eindeutig bestimmtes Element $\alpha \in \mathbb{Z}$ mit $0 \leq \alpha < p^n$ repräsentiert werden, und dieses kann wiederum in eindeutiger Weise als

$$\alpha = \sum_{i=0}^{n-1} q_i p^i$$

mit Zahlen $0 \leq q_i \leq p-1$ geschrieben werden (p -adische Entwicklung). Daher kann jedes Element $\alpha \in \mathbb{Z}_p$ in eindeutiger Weise als eine formale Reihe

$$(*) \quad \alpha = \sum_{i=0}^{\infty} a_i p^i \quad (a_i \in \mathbb{Z}, 0 \leq a_i \leq p-1)$$

geschrieben werden: setzen wir

$$\alpha_n = \sum_{i=0}^{n-1} a_i p^i \in \mathbb{Z} \quad (n \geq 1),$$

so bedeutet $(*)$ die kompatible Familie

$$(\alpha_n \bmod (p^n))_{n \geq 1}.$$

Dies zeigt, dass es überabzählbar viele Elemente in \mathbb{Z}_p gibt (die Menge der Familien $(a_i)_{i \geq 0}$ mit $a_i \in \{0, \dots, p-1\}$ ist überabzählbar). Insbesondere ist $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ nicht surjektiv. \mathbb{Z}_p heißt auch der Ring der **(ganzen) p -adischen Zahlen**.

(b) Man definiert $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. Hierbei ist der projektive Limes wie in 2.4(b) durch $(\mathbb{N}, |)$ indiziert. Ist $n \in \mathbb{N}$ und

$$n = p_1^{n_1} \dots p_r^{n_r}$$

die Primfaktorzerlegung, so hat man bekanntlich eine kanonische Zerlegung

$$(2.6.1) \quad \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$$

(chinesischer Restsatz). Dies ist kompatibel mit den Übergangsabbildungen: für $m | n$ ist

$$m = p_1^{m_1} \dots p_r^{m_r}$$

mit $m_i \leq n_i$ ($i = 1, \dots, r$), und das Diagramm

$$(2.6.2) \quad \begin{array}{ccccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/p_1^{m_1}\mathbb{Z} & \times \dots \times & \mathbb{Z}/p_r^{n_r}\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/p_1^{m_1}\mathbb{Z} & \times \dots \times & \mathbb{Z}/p_r^{m_r}\mathbb{Z} \end{array}$$

ist kommutativ. Dies liefert einen kanonischen Ringisomorphismus

$$\hat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p,$$

wobei das Produkt rechts über alle Primzahlen läuft. (Hierfür ist es am besten, wenn man formal $n = \prod_p p^{n_p}$ schreibt, wobei das Produkt über alle Primzahlen läuft und $n_p = 0$ für fast alle p , und die rechte Seite von (2.6.1) als

$$\prod_p \mathbb{Z}/p^{n_p}\mathbb{Z},$$

entsprechend für (2.6.2)).

(c) Für das induktive System $(\mathbb{Z}/n\mathbb{Z})_{n \in \mathbb{N}}$ von 2.4 (c) erhält man einen Isomorphismus von abelschen Gruppen

$$\varinjlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z},$$

der $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ auf die Restklasse von $\frac{a}{n}$ mod \mathbb{Z} abbildet: Für jedes feste $n \in \mathbb{N}$ ist die Abbildung

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \hookrightarrow & \mathbb{Q}/\mathbb{Z} \\ a + n\mathbb{Z} & \mapsto & \frac{a}{n} + \mathbb{Z} \end{array}$$

ein wohldefinierter, injektiver Gruppenhomomorphismus. Dieser ist kompatibel mit den Übergangsabbildungen: für $m \mid n$ ist

$$\begin{array}{ccccc}
 a + m\mathbb{Z} & \xrightarrow{\quad} & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\quad} & \frac{a}{m} + \mathbb{Z} \\
 \downarrow & & \downarrow & \searrow & \parallel \\
 \frac{n}{m}a + n\mathbb{Z} & \xrightarrow{\quad} & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\quad} & \frac{na}{mn} + \mathbb{Z} \\
 & & & \nearrow & \\
 & & & \mathbb{Q}/\mathbb{Z} &
 \end{array}$$

kommutativ. Hieraus folgt leicht die Behauptung (vergleiche auch Übungsaufgabe 3(i)).

Die Gruppe \mathbb{Q}/\mathbb{Z} wird auch die ‘‘Prüfergruppe’’ genannt. Sie ist isomorph zur Gruppe $\mu(\mathbb{C})$ aller Einheitswurzeln in \mathbb{C}^\times , vermöge der Abbildung

$$\begin{array}{ccc}
 \mathbb{Q}/\mathbb{Z} & \xrightarrow{\sim} & \mu(\mathbb{C}) \\
 \frac{p}{q} + \mathbb{Z} & \mapsto & e^{2\pi i \frac{p}{q}}.
 \end{array}$$

(d) Ist L/K eine Galoiserweiterung, so ist nach Lemma 1.6

$$(2.6.3) \quad Gal(L/K) \xrightarrow{\sim} \varprojlim_{K' \in \mathcal{K}_{L/K}} Gal(K'/K)$$

wobei $\mathcal{K}_{L/K}$ die gerichtete Menge der endlichen normalen Teilerweiterungen K'/K von L/K ist.

(e) Ist $(X_i)_{i \in I}$ ein projektives System von topologischen Räumen, so versteht man

$$\varprojlim_{i \in I} X_i \subseteq \prod_{i \in I} X_i$$

mit der Unterraumtopologie, bezüglich der Produkttopologie auf dem Produkt rechts.

(f) Wendet man dies auf die Beispiele (a), (b) und (d) an, bezüglich der diskreten Topologien auf den R/\mathfrak{a}^n , bzw. $\mathbb{Z}/n\mathbb{Z}$, bzw. $Gal(K'/K)$, so erhalten $\hat{R} = \varprojlim R/\mathfrak{a}^n$, \mathbb{Z}_p , $\hat{\mathbb{Z}}$ und $\varprojlim Gal(K'/K)$ Topologien. Weiter sieht man leicht, dass man so topologische Gruppen, für \hat{R} , \mathbb{Z}_p und $\hat{\mathbb{Z}}$ sogar topologische Ringe (die Multiplikation ist ebenfalls stetig) erhält. Lemma 1.6 besagt dann, dass der Isomorphismus (2.6.3) auch ein Homöomorphismus ist, also ein Isomorphismus topologischer Gruppen.

Wir können nun die absolute Galoisgruppe

$$G_{\mathbb{F}_q} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$$

eines endlichen Körpers \mathbb{F}_q mit q Elementen beschreiben.

Satz 2.7 Es gibt einen kanonischen Isomorphismus von topologischen Gruppen

$$\hat{\mathbb{Z}} \xrightarrow{\sim} G_{\mathbb{F}_q}.$$

Beweis Für jede natürliche Zahl n gibt es genau eine Erweiterung vom Grad n über \mathbb{F}_q , nämlich \mathbb{F}_{q^n} . Diese ist galoissch, und es gibt einen kanonischen Isomorphismus

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ 1 \bmod n\mathbb{Z} &\mapsto \text{Fr}_q, \end{aligned}$$

wobei Fr_q der Frobeniusautomorphismus ist, der durch die Vorschrift

$$\text{Fr}_q(x) = x^q \quad (\text{für alle } x \in \mathbb{F}_{q^n})$$

gegeben ist. Dies ist kompatibel mit den Übergangsabbildungen: Es ist genau dann $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, wenn $m \mid n$, und dann ist

$$\begin{array}{ccccc} 1 & & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & & \text{Fr}_q \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) & & \text{Fr}_q \end{array}$$

kommutativ. Das projektive System $(\text{Gal}(K'/\mathbb{F}_q))_{K' \in K_{\overline{\mathbb{F}_q}/\mathbb{F}_q}}$ identifiziert sich also mit dem projektiven System $(\mathbb{Z}/n\mathbb{Z})_{n \in (\mathbb{N}, \mid)}$ aus 2.4 (b); entsprechend erhält man einen Isomorphismus

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \rightarrow \varprojlim_n \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \varprojlim_{K'} \text{Gal}(K'/\mathbb{F}_q)$$

der projektiven Limiten, der eine kompatible Familie $(\bar{a}_n)_n$ links auf die kompatible Familie $(\text{Fr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}^{a_n})_n$ rechts abbildet. Die Behauptung des Satzes folgt mit 2.6 (d), (e) und (f).

Bemerkung 2.8 Wir haben die Abbildung

$$\begin{aligned} \mathbb{Z} &\rightarrow \hat{\mathbb{Z}} \xrightarrow{\sim} \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), \\ 1 &\mapsto 1 \mapsto \text{Fr}_q \end{aligned}$$

wobei Fr_q der Frobeniusautomorphismus von $\overline{\mathbb{F}_q}$ ist: $\text{Fr}_q(x) = x^q$. Der erste Homomorphismus ist injektiv aber nicht surjektiv, da schon keine der Kompositionen

$$\mathbb{Z} \rightarrow \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \rightarrow \mathbb{Z}_p$$

injektiv ist (2.6(a)). Aber es gilt, dass \mathbb{Z} dicht in $\hat{\mathbb{Z}}$ (und damit auch dicht in $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$) liegt (Beweis selbst!).

§3 Kohomologie von Gruppen und pro-endlichen Gruppen

Die folgende Definition ist parallel formuliert für den Fall, dass Topologien auf G und A gegeben sind, wobei man stetige Abbildungen betrachtet, oder dass keine Topologie vorliegt (äquivalent: die Topologie ist die diskrete, so dass alle Abbildungen stetig sind).

Definition 3.1 Sei G eine (topologische) Gruppe und A ein (stetiger) G -Modul, d.h., eine abelsche Gruppe A zusammen mit einer (stetigen) Verknüpfung

$$\begin{aligned}\mu : G \times A &\rightarrow A \\ (\sigma, a) &\mapsto \sigma a\end{aligned}$$

für die gilt

$$\begin{aligned}\sigma(a+b) &= \sigma a + \sigma b \\ \sigma_1(\sigma_2 a) &= (\sigma_1 \sigma_2) a \\ 1a &= a\end{aligned}$$

für alle $a, b \in A, \sigma, \sigma_1, \sigma_2 \in G$ und das Einselement $1 \in G$. Für $n \in \mathbb{N}_0$ definiere die Gruppe der (stetigen) n -Ketten auf G mit Koeffizienten in A

$$C^n(G, A) = \{f : G^n \rightarrow A \mid f \text{ stetig}\}$$

(wobei $C^0(G, A) = \{f : G^0 = \{*\} \rightarrow A\} = A$) sowie das n -te **Differential**

$$\partial^n : C^n(G, A) \rightarrow C^{n+1}(G, A)$$

durch

$$\begin{aligned}\partial^0(a)(\sigma) &= \sigma a - a, \\ \partial^1(f)(\sigma_1, \sigma_2) &= \sigma_1 f(\sigma_2) - f(\sigma_1 \sigma_2) + f(\sigma_1), \\ \partial^n(f)(\sigma_1, \dots, \sigma_{n+1}) &= \sigma_1 f(\sigma_2, \dots, \sigma_n) \\ &\quad + \sum_{i=1}^n (-1)^i f(\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_n) \\ &\quad + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n) \text{ für } n \geq 1\end{aligned}$$

Lemma 3.2 ∂^n ist wohldefiniert, und

$$C^0(G, A) \xrightarrow{\partial^0} C^1(G, A) \xrightarrow{\partial^1} C^2(G, A) \rightarrow$$

ist ein **Komplex**, d.h., es ist $\partial^{n+1} \partial^n = 0$ für alle n .

Beweis: $\partial^n \partial^{n-1} = 0$: selbst nachrechnen oder in einschlägigen Büchern nachsehen, wo es auch konzeptionellere Beweise gibt. Sind wir im Fall einer topologischen Gruppe und eines stetigen G -Moduls A , so ist $\partial^n(f)$ wieder stetig, da $\mu : G \times A \rightarrow A$ und die Verknüpfung $g \times G \rightarrow G$ stetig sind.

Definition 3.3 (a) Die n -te (stetige) **Kohomologie(gruppe)** von G mit Koeffizienten in A ist definiert als die n -te Homologie dieses Komplexes, d.h.,

$$H^n(G, A) = \ker \partial^n / \operatorname{Im} \partial^{n-1}$$

für $n \geq 0$ (wobei $\partial^{-1} := 0$). Beachte: Wegen $\partial^n \partial^{n-1} = 0$ gilt $\operatorname{Im} \partial^{n-1} \subseteq \ker \partial^n$.

(b) Die Elemente in

$$Z^n(G, A) = \ker \partial^n = \{f \in C^n(G, A) \mid \partial^n f = 0\}$$

heißen die (stetigen) n -**Kozykel** (von G mit Koeffizienten in A).

(c) Die Elemente in

$$B^n(G, A) = \text{im } \partial^{n-1} = \{f \in C^n(G, A) \mid f = \partial^{n-1}g \text{ für } g \in C^{n-1}(G, A)\}$$

heißen die n -**Koränder**.

Es ist also $H^n(G, A) = Z^n(G, A)/B^n(G, A)$.

Dies ist ein Spezialfall einer allgemeinen Konstruktion:

Bemerkung/Definition 3.4 (a) Eine Folge

$$\dots \rightarrow C^0 \xrightarrow{\partial^0} C^1 \rightarrow \dots \rightarrow C^n \xrightarrow{\partial^n} C^{n+1} \xrightarrow{\partial^{n+1}} \dots$$

von abelschen Gruppen $C^i (i \in \mathbb{Z})$ und Homomorphismen von abelschen Gruppen nennt man **Komplex** (von abelschen Gruppen), wenn $\partial^{n+1} \circ \partial^n = 0$ für alle $n \in \mathbb{Z}$.

(b) In diesem Fall heißt

$$H^n(C) := \ker \partial^n / \text{im } \partial^{n-1}$$

die n -te **Kohomologie**(gruppe) des Komplexes (Beachte: $\partial^n \circ \partial^{n-1} = 0$ bedeutet gerade $\text{im } \partial^{n-1} \subseteq \ker \partial^n$).

(c) Ein Komplex (C, ∂) heißt **exakt**, wenn an allen Stellen $\ker \partial^n = \text{im } \partial^{n-1}$ gilt, also wenn die Kohomologie überall verschwindet (Die Kohomologie misst also die Abweichung von der Exaktheit).

(d) Sei C ein Komplex. Ist $C^n = 0$ für alle $n < 0$, so nennt man C einen positiven Komplex und schreibt nur $C^0 \rightarrow C^1 \rightarrow \dots$, entsprechend für negative Komplexe $\dots \rightarrow C^{-1} \rightarrow C^0$, wo $C^n = 0$ für $n > 0$.

Der Komplex $C(G, A)$ aus 3.1 ist also ein positiver Komplex. Eine verwandte Definition ist

Definition 3.5 (a) Eine Sequenz

$$A^m \xrightarrow{\partial^m} A^{m+1} \rightarrow \dots \rightarrow A^{n-1} \xrightarrow{\partial^{n-1}} A^n$$

von abelschen Gruppen A^i und Gruppenhomomorphismen ∂^i (mit $m < n$) heißt ein **Komplex**, wenn $\partial^i \circ \partial^{i-1} = 0$ für alle i , $m < i < n$, und heißt weiter **exakt an der Stelle i** ($m < i < n$), wenn $\text{im } \partial^{i-1} = \ker \partial^i$, sowie **exakt**, wenn dies für alle i , $m < i < n$, gilt (es gibt also keine Bedingung an den Stellen m und n).

(b) Eine exakte Sequenz

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$$

heißt **kurze exakte Sequenz**.

Lemma 3.6 Eine Sequenz

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$$

ist exakt genau dann, wenn gilt

- (i) i ist injektiv,
- (ii) p ist surjektiv,
- (iii) $\text{im}(i) = \ker(p)$.

Beweis $\ker(i) = \text{im}(0 \rightarrow A) = 0$ gilt genau dann wenn i injektiv ist und $\text{im}(p) = \ker(C \rightarrow 0) = C$ gilt genau dann, wenn p surjektiv ist.

Bemerkung 3.7 In diesem Fall liefert der Homomorphiesatz eine Isomorphie $B/i(A) \xrightarrow{\sim} C$, und wir können $i(A)$ mit A identifizieren. Ist umgekehrt $p : B \rightarrow C$ eine Epimorphismus von abelschen Gruppen und $A = \ker(p)$, so erhalten wir eine exakte Sequenz

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0,$$

wobei i die Inklusion ist. In diesem Sinne entspricht eine kurze exakte Sequenz

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

einer Beziehung

$$B/A \xrightarrow{\sim} C.$$

Wir betrachten nun die Kohomologiegruppen in niedrigen Dimensionen, $n = 0, 1, 2$:

$H^0(\mathbf{G}, \mathbf{A})$:

Lemma 3.8 Es gibt eine kanonische Isomorphie

$$H^0(G, A) \cong A^G$$

wo $A^G = \{a \in A \mid \sigma a = a \text{ für alle } \sigma \in G\}$ der **Fixmodul** von A unter G ist.

Beweis Es ist $H^0(G, A) = \ker \partial^0$, und ∂^0 identifiziert sich mit

$$\begin{array}{l} A \xrightarrow{\partial^0} C^1(G, A) \\ a \mapsto f : G \rightarrow A \text{ mit } f(\sigma) = \sigma a - a. \end{array}$$

Daher ist $\ker \partial^0 = A^G$.

$H^1(\mathbf{G}, \mathbf{A})$:

$Z^1(G, A)$ ist die Gruppe der (stetigen) Abbildungen $f : G \rightarrow A$ mit

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Diese werden auch **verschränkte Homomorphismen** genannt. Die Gruppe $B^1(G, A)$ der 1-Koränder ist die Gruppe von Abbildungen $f : G \rightarrow A$ von der Form

$$f(\sigma) = \sigma a - a$$

für ein festes $a \in A$. Wir sehen sofort

Lemma 3.9 Operiert G trivial auf A (d.h., $\sigma a = a$ für alle $\sigma \in G, a \in A$), so ist

$$H^1(G, A) = \text{Hom}(G, A) \quad (\text{bzw. } \text{Hom}_{\text{cont}}(G, A))$$

die Gruppe der Homomorphismen von G nach A (bzw. die Gruppe der stetigen Homomorphismen, wenn wir Topologien haben).

$H^2(G, A)$:

$Z^2(G, A)$ ist die Gruppe der (stetigen) Abbildungen $f : G \times G \rightarrow A$ mit

$$f(\sigma\tau, \rho) + f(\sigma, \tau) = f(\sigma, \tau\rho) + \sigma f(\tau, \rho).$$

Diese heißen auch **Faktorensysteme**. Die 2-Koränder sind die Funktionen von der Form

$$f(\sigma, \tau) = g(0) - g(\sigma\tau) + \sigma g(\tau)$$

für eine beliebige (stetige) Abbildung $g : G \rightarrow A$; man nennt diese die **trivialen Faktorensysteme**.

Die Faktorensysteme haben mit Gruppenerweiterungen zu tun. Wir beschreiben dies nur für Gruppen ohne Topologie.

Definition 3.10 Seien G und A Gruppen (nicht notwendig kommutativ). Eine **Gruppenerweiterung von G mit A** ist eine exakte Sequenz

$$1 \rightarrow A \xrightarrow{\iota} E \xrightarrow{\pi} G \rightarrow 1,$$

d.h., ι und π sind Gruppenhomomorphismen, ι ist injektiv, π ist surjektiv, und es ist $\text{im } \iota = \ker \pi$.

Im Folgenden fassen wir ι immer als Inklusion auf, indem wir $a \in A$ mit $\iota(a) \in G$ identifizieren. Dann haben wir also eine Gruppe E , die A als Normalteiler enthält, so dass $E/A \xrightarrow{\sim} G$.

Lemma 3.11 Sei A abelsch. Dann wird A zu einem G -Modul, indem man für $a \in A$ und $g \in G$ definiert

$$g(a) = \hat{g}a\hat{g}^{-1}.$$

wobei $\hat{g} \in E$ ein Lift von g ist, also ein Urbild von g unter $\pi : E \twoheadrightarrow G$.

Beweis: Da A ein Normalteiler ist, ist $g(a) \in A$.

Da A kommutativ ist, ist $g(a)$ unabhängig von \hat{g} . Ist nämlich \tilde{g} ein anderer Lift von g , so ist $\tilde{g} = \hat{g}b$ für ein $b \in A$ (da $\hat{g}^{-1}\tilde{g} \in \ker \pi = A$), und damit

$$\tilde{g}a\tilde{g}^{-1} = \hat{g}bab^{-1}\hat{g}^{-1} = \hat{g}a\hat{g}^{-1},$$

da A kommutativ ist.

A ist ein G -Modul: Offenbar ist $1(a) = a$. Weiter ist für $a, a' \in A$

$$\begin{aligned} g(a \cdot a') &= \hat{g}aa'\hat{g}^{-1} = \hat{g}a\hat{g}^{-1}\hat{g}a'g^{-1} \\ &= g(a) \cdot g(a'), \end{aligned}$$

die Operation von G also verträglich mit der (hier multiplikativ geschriebenen) Verknüpfung von A . Die Beziehung $(gh)(a) = g(h(a))$ ist klar, da $\hat{g}\hat{h}$ ein Lift von gh ist, wenn \hat{g} bzw. \hat{h} Lifts von g bzw. h sind.

Wir ordnen nun der Gruppenerweiterung ein Faktorensystem zu. Sei

$$s : G \rightarrow E$$

ein Schnitt von $\pi : E \rightarrow G$, also eine Abbildung mit $\pi s = id_G$ (Für jedes $g \in G$ wählt also s einen Lift \hat{g} von g aus; nach dem Auswahlaxiom gibt es eine solche Abbildung immer). Für $\sigma, \tau \in G$ werden $s(\sigma) \cdot s(\tau)$ und $s(\sigma\tau)$ unter π beide auf $\sigma\tau$ abgebildet; sie unterscheiden sich also um ein Element in $\ker \pi = A$. Es gibt also ein eindeutig bestimmtes $f(\sigma, \tau) \in A$ mit

$$s(\sigma) \cdot s(\tau) = f(\sigma, \tau) \cdot (\sigma\tau).$$

Lemma 3.12 (i) Die Abbildung $f : (\sigma, \tau) \mapsto f(\sigma, \tau)$ ist ein Faktorensystem, d.h., ein 2-Kozykel.

(ii) Die zugehörige Kohomologieklassse

$$[f] \in H^2(G, A).$$

ist unabhängig von der Wahl des Schnittes s .

Beweis (i) Dies folgt aus der Assoziativität $s(\sigma)(s(\tau)s(\rho)) = (s(\sigma)s(\tau))s(\rho)$:

$$\begin{aligned} s(\sigma)(s(\tau)s(\rho)) &= s(\sigma)f(\tau, \rho)s(\tau\rho) = s(\sigma)f(\tau, \rho)s(\sigma)^{-1}s(\sigma)s(\tau\rho) \\ &= \sigma(f(\tau, \rho))s(\sigma)s(\tau\rho) \text{ (nach Definition 3.11)} \\ &= \sigma(f(\tau, \rho))f(\sigma, \tau\rho)s(\sigma\tau\rho) \\ (s(\sigma)s(\tau))s(\rho) &= f(\sigma, \tau)s(\sigma\tau)s(\rho) \\ &= f(\sigma\tau)f(\sigma\tau, \rho)s(\sigma\tau\rho) \end{aligned}$$

Hieraus folgt die 2-Kozykeleigenschaft (multiplikative Schreibweise!)

$$\sigma(f(\tau, \rho))f(\sigma, \tau\rho) = f(\sigma, \tau)f(\sigma\tau, \rho)$$

□

(ii) Sei $t : G \rightarrow E$ ein weiterer Schnitt, d.h., Rechtsinverses von π ($\pi t = id_G$). Dann gibt es für jedes $\sigma \in G$ ein Element $a(\sigma) \in A$ mit

$$t(\sigma) = a(\sigma) \cdot s(\sigma).$$

Ist nun $g(\sigma, \tau)$ der 2-Kozykel zu t , d.h.,

$$t(\sigma)t(\tau) = g(\sigma, \tau)t(\sigma\tau),$$

so folgt

$$\begin{aligned} a(\sigma)s(\sigma)a(\tau)s(\tau) &= g(\sigma, \tau)a(\sigma\tau)s(\sigma\tau) \\ &\parallel \\ a(\sigma)\sigma(a(\tau))f(\sigma, \tau)s(\sigma\tau), \end{aligned}$$

also

$$g(\sigma, \tau) = f(\sigma, \tau) \cdot \sigma(a(\tau))a(\sigma\tau)^{-1}a(\sigma).$$

Damit unterscheiden sich f und g nur an den 1-Korand

$$(\sigma, \tau) \mapsto \sigma(a(\tau))a(\sigma, \tau)^{-1}a(\sigma).$$

Definition 3.13 Zwei Gruppenerweiterungen von G mit A

$$\begin{array}{ccccccccc} 1 & \rightarrow & A & \rightarrow & E & \rightarrow & G & \rightarrow & 1 \\ 1 & \rightarrow & A & \rightarrow & E' & \rightarrow & G & \rightarrow & 1 \end{array}$$

heißen **äquivalent**, wenn es ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \rightarrow & A & \rightarrow & E & \rightarrow & G & \rightarrow & 1 \\ & & \parallel & & \downarrow \varphi & & \parallel & & \\ 1 & \rightarrow & A & \rightarrow & E' & \rightarrow & G & \rightarrow & 1 \end{array}$$

mit einem Gruppenisomorphismus φ gibt.

Es gilt dann:

Satz 3.14 Die Zuordnung aus 3.12 induziert eine Bijektion

$$Ext(G, A) \xrightarrow{\sim} H^2(G, A),$$

wobei $Ext(G, A)$ die Menge der Äquivalenzklassen von Gruppenerweiterungen von G mit A ist; dabei sei die Struktur von A als G -Modul fixiert.

Beweis: Übungsaufgabe.

§4 Grundlagen über Moduln und homologischen Algebra

Sei R ein Ring mit Eins (nicht notwendig kommutativ).

Definition 4.1 (a) Ein (linker) R -Modul ist eine abelsche Gruppe $(M, +)$ zusammen mit einer Verknüpfung

$$\begin{aligned} R \times M &\rightarrow M \\ (r, m) &\mapsto rm \end{aligned}$$

so dass gilt

- (i) $r(m+n) = rm+rn$
- (ii) $(r+s)m = rm+sm$
- (iii) $(rs)m = r(sm)$
- (iv) $1m = m$

für alle $r, s \in R$ und $m, n \in M$.

(b) Seien M und N R -Moduln. Eine Abbildung $\varphi : M \rightarrow N$ heißt **Homomorphismus von R -Moduln** (oder R -linear), wenn gilt:

- (i) $\varphi(m_1+m_2) = \varphi(m_1) + \varphi(m_2)$ für alle $m_1, m_2 \in M$ (d.h., φ ist ein Gruppenhomomorphismus von $(M, +)$ nach $(N, +)$),
- (ii) $\varphi(rm) = r\varphi(m)$ für alle $m \in M, r \in R$.

Sei $Hom_R(M, N)$ die abelsche Gruppe der R -linearen Abbildungen von M nach N .

Bemerkungen 4.2 (a) Ein rechter R -Modul M ist ebenso definiert, wobei man allerdings die Eigenschaft (iii) ersetzt durch

$$(iii') \quad (rs)m = s(rm).$$

Schreibt man die Verknüpfung anders, nämlich

$$\begin{aligned} M \times R &\rightarrow M \\ (m, r) &\mapsto mr, \end{aligned}$$

so wird hieraus die einleuchtendere Beziehung

$$m(rs) = (mr)s.$$

(b) Für einen kommutativen Ring sind Links- und Rechtsmoduln dasselbe.

(c) Wie üblich nennt man eine R -lineare Abbildung $\varphi : M \rightarrow N$ Monomorphismus (bzw. Epimorphismus, bzw. Isomorphismus), wenn sie injektiv (bzw. surjektiv, bzw. bijektiv) ist.

(d) Die Komposition von R -linearen Abbildungen ist wieder linear. Das Inverse eines R -Moduls-Isomorphismus ist wieder R -linear.

Beispiele 4.3 (a) Jede abelsche Gruppe A wird zu einem \mathbb{Z} -Modul durch die Definition

$$na = a + \dots + a \quad (n\text{-mal}) \quad \text{für } n \in \mathbb{N},$$

$$\begin{aligned} 0a &= 0 \\ (-n)a &= -(na) \quad \text{für } n \in \mathbb{N}. \end{aligned}$$

Man sieht, dass abelsche Gruppen und \mathbb{Z} -Moduln dasselbe sind.

(b) Ist $(M_i)_{i \in I}$ eine Familie von R -Moduln, so werden die abelschen Gruppen

$$\prod_{i \in I} M_i \supseteq \bigoplus_{i \in I} M_i$$

zu R -Moduln durch die Definition $r(m_i)_{i \in I} := (rm_i)_{i \in I}$.

Bezeichnung: **diskretes Produkt** bzw. **direkte Summe** der R -Moduln M_i .

(c) Ist K ein Körper, so ist ein K -Modul dasselbe wie ein K -Vektorraum.

Definition 4.4 Ein R -Modul M heißt freier R -Modul, wenn es eine Familie $(m_i)_{i \in I}$ von Elementen $m_i \in M$ gibt, so dass gilt: Jedes Element $m \in M$ besitzt eine eindeutige Darstellung

$$m = \sum_{i \in I} r_i m_i,$$

wobei $r_i \in R$ und $r_i = 0$ für fast alle $i \in I$ (so dass die Summe rechts endlich ist, wenn wir die Summanden mit $r_i = 0$ weglassen). Eine solche Familie $(m_i)_{i \in I}$ heißt Basis von M .

Beispiele 4.5 (a) Sei I eine Menge. Dann ist der R -Modul

$$F_R(I) := \bigoplus_{i \in I} R$$

frei mit Basis $(e_i)_{i \in I}$, wobei $e_i = (\delta_{ji})_{j \in I}$, mit dem Kronecker-Symbol

$$\delta_{ij} = \begin{cases} 1 & , \quad j = i \\ 0 & , \quad j \neq i \end{cases}$$

(mit $0, 1 \in R$). $F_R(I)$ heißt auch der freie R -Modul über I . Manchmal identifiziert man e_i mit i und schreibt die Elemente als formale Linearkombinationen

$$\sum_{i \in I} r_i i,$$

mit $r_i \in R, r_i = 0$ für fast alle i .

(b) Der \mathbb{Z} -Modul $M = \mathbb{Z}/5\mathbb{Z}$ ist nicht frei, denn für jedes $m \in \mathbb{Z}/5\mathbb{Z}$ ist $1 \cdot m = m = 6 \cdot m$. Aber M ist ein freier Modul über dem Ring $\mathbb{Z}/5\mathbb{Z}$.

Lemma 4.6 (universelle Eigenschaft des freien Moduls) Sei M ein R -Modul und $(m_i)_{i \in I}$ eine Familie von Elementen $m_i \in M$. Dann gibt es genau einen R -Modul-Homomorphismus

$$\varphi : F_R(I) \rightarrow M$$

mit $\varphi(e_i) = m_i$ für alle $i \in I$ (Es gilt also $\text{Hom}_R(F_R(I), M) \xrightarrow{\sim} \text{Abb}(I, M)$ vermöge $\varphi \mapsto (\varphi(e_i))_{i \in I}$).

Beweis: Setze $\varphi((r_i)) = \sum_{i \in I} r_i m_i$.

Bemerkungen 4.7 M ist genau dann frei mit Basis $(m_i)_{i \in I}$ wenn das obige φ ein Isomorphismus ist.

Definition 4.8 Sei M ein R -Modul. Ein (R -)Untermodul von M ist eine Teilmenge $N \subseteq M$, für die gilt:

- (i) N ist Untergruppe bezüglich $+$,
- (ii) für alle $n \in N$ und $r \in R$ gilt $rn \in N$.

Lemma 4.9 Ist $\varphi : M \rightarrow N$ ein Homomorphismus von R -Moduln, so ist $\ker \varphi$ ein Untermodul von M und $\text{im } \varphi$ ein Untermodul von N .

Beweis: leicht!

Satz 4.10 Ist M ein R -Modul und $N \subseteq M$ ein Untermodul, so wird die Faktorgruppe

$$M/N$$

zu einem R -Modul durch die Definition

$$r(m + N) := rm + N \quad \text{für } r \in R, m \in M$$

(also $r \cdot \bar{m} = \overline{rm}$, wenn \bar{m} die Nebenklasse von $m \in M$ bezeichnet). Die Surjektion $\pi : M \rightarrow M/N$ ist R -linear.

Beweis: selbst!

Bemerkungen 4.11 Der Homomorphiesatz sowie erster und zweiter Isomorphiesatz übertragen sich auf R -Moduln:

- (a) Eine R -lineare Abbildung $\varphi : M \rightarrow N$ induziert einen R -Modul-Isomorphismus

$$M/\ker \varphi \xrightarrow{\sim} \text{im } \varphi.$$

- (b) Für Untermoduln $N_1, N_2 \subset M$ hat man einen R -Modul-Isomorphismus

$$N_1/(N_1 \cap N_2) \xrightarrow{\sim} (N_1 + N_2)/N_2.$$

- (c) Für Untermoduln $M_3 \subset M_2 \subset M_1$ hat man einen R -Isomorphismus

$$(M_1/M_3)/(M_2/M_3) \xrightarrow{\sim} M_1/M_2.$$

Wir kommen nun zur homologischen Algebra von R -Moduln.

Definition 4.12 Wir definieren Komplexe von R -Moduln wieder als Sequenzen

$$\dots \rightarrow M^n \xrightarrow{\partial^n} M^{n+1} \xrightarrow{\partial^{n+1}} M^{n+2} \rightarrow \dots,$$

wobei die M^n R -Moduln sind und die ∂^n lineare Abbildungen mit $\partial^{n+1}\partial^n = 0$. Die n -te Kohomologie ist der R -Modul

$$H^n(M^\cdot) = \ker \partial^n / \text{im } \partial^{n-1}$$

und der Komplex heißt exakt an der Stelle n wenn $H^n(M^\cdot) = 0$ bzw. exakt, wenn er an allen Stellen exakt ist.

Definition 4.13 Seien C^\cdot und D^\cdot Komplexe von R -Moduln, wobei R ein Ring ist (für $R = \mathbb{Z}$ haben wir also einfach Komplexe von abelschen Gruppen). Ein Morphismus von Komplexen (von R -Moduln)

$$\varphi : C^\cdot \rightarrow D^\cdot$$

ist eine Kollektion von Homomorphismen von R -Moduln

$$\varphi^i : C^i \rightarrow D^i,$$

die kompatibel mit den Differentialen sind, d.h., für die alle Quadrate

$$\begin{array}{ccc}
 \vdots & & \vdots \\
 \uparrow & & \uparrow \\
 C^{i+1} & \xrightarrow{\varphi^{i+1}} & D^{i+1} \\
 \partial_C^i \uparrow & & \uparrow \partial_D^i \\
 C^i & \xrightarrow{\varphi^i} & D^i \\
 \uparrow & & \uparrow \\
 \vdots & & \vdots
 \end{array}$$

kommutativ sind (hierbei sind ∂_C^i und ∂_D^i die Differentialen für C^\cdot bzw. D^\cdot). Es muss also gelten $\varphi^{i+1}\partial_C^i = \partial_D^i\varphi^i$ (vereinfachte Schreibweise, ohne Grade: $\varphi\partial_C = \partial_D\varphi$).

Lemma 4.13 Ein Morphismus von Komplexen

$$\varphi : C^\cdot \rightarrow D^\cdot$$

induziert Homomorphismen

$$\varphi_*^i = H^i(\varphi) : H^i(C) \rightarrow H^i(D)$$

in der Kohomologie. Dabei gilt $(id_C)_*^i = id_{H^i(C)}$ und $(\psi\varphi)_* = \psi_*\varphi_*$ für einen weiteren Morphismus von Komplexen $\psi : D^\cdot \rightarrow E^\cdot$.

Beweis Wegen der Kompatibilität mit den Differentialen induziert

$$\varphi^i : C^i \rightarrow D^i$$

Abbildungen

$$\begin{array}{ccc}
 \ker \partial_C^i & \rightarrow & \ker \partial_D^i \\
 \text{im } \partial_C^{i-1} & \rightarrow & \text{im } \partial_D^{i-1}
 \end{array}$$

und daher eine wohldefinierte R -lineare Abbildung

$$\begin{array}{ccc}
 \varphi_*^i : & H^i(C) & \rightarrow & H^i(D), \\
 [a] := a \text{ mod } \text{im } \partial_C^{i-1} & \mapsto & \varphi^i(a) \text{ mod } \text{im } \partial_D^{i-1} =: [\varphi^i(a)]
 \end{array}$$

(für $a \in \ker \partial_C^i$). Die weiteren Aussagen sind klar.

Auch im Folgenden bezeichne $[a]$ die Kohomologieklass eines Zyklus a .

Definition 4.14 Eine Sequenz

$$C^\cdot \xrightarrow{\phi} D^\cdot \xrightarrow{\Psi} E^\cdot$$

von (Morphismen von) Komplexen heißt exakt, wenn die Sequenz

$$C^i \xrightarrow{\phi^i} D^i \xrightarrow{\psi^i} E^i$$

für alle i exakt ist.

Satz 4.15 (lange exakte Kohomologiesequenz) Sei R ein Ring und

$$0 \rightarrow C^\cdot \xrightarrow{\phi} D^\cdot \xrightarrow{\Psi} E^\cdot \rightarrow 0$$

eine kurze exakte Sequenz von Komplexen von R -Moduln. Dann gibt es kanonische R -Modulhomomorphismen

$$\delta^i : H^i(E^\cdot) \rightarrow H^{i+1}(C^\cdot)$$

für alle i (Verbindungshomomorphismen genannt), so dass die Sequenz

$$\dots \rightarrow H^{i-1}(E^\cdot) \xrightarrow{\delta^{i-1}} H^i(C^\cdot) \xrightarrow{\phi_*^i} H^i(D^\cdot) \xrightarrow{\psi_*^i} H^i(E^\cdot) \xrightarrow{\delta^i} H^{i+1}(C^\cdot) \rightarrow \dots$$

exakt ist.

Beweis Wir haben ein kommutatives Diagramm

(4.15.1)

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & C^{i+2} & \xrightarrow{\phi^{i+2}} & D^{i+2} & \longrightarrow & E^{i+2} \longrightarrow 0 \\
 & & \uparrow \partial_C \quad (4) & & \uparrow \partial_D & & \uparrow \\
 0 & \longrightarrow & C^{i+1} & \xrightarrow{\phi^{i+1}} & D^{i+1} & \xrightarrow{\psi^{i+1}} & E^{i+1} \longrightarrow 0 \\
 & & \uparrow \partial_C \quad (2) & & \uparrow \partial_D \quad (3) & & \uparrow \partial_E \\
 0 & \longrightarrow & C^i & \xrightarrow{\phi^i} & D^i & \xrightarrow{\psi^i} & E^i \longrightarrow 0 \\
 & & \uparrow \partial_C & & \uparrow \partial_D \quad (1) & & \uparrow \partial_E \\
 0 & \longrightarrow & C^{i-1} & \longrightarrow & D^{i-1} & \xrightarrow{\psi^{i-1}} & E^{i-1} \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

wobei die Zeilen kurze exakte Sequenzen sind.

1) **Exaktheit bei $H^i(D)$** : Es ist klar, dass $\psi_*\phi_* = 0$ (da $\psi_*\phi_* = (\psi\phi)_* = 0_* = 0$). Sei $[d^i] \in H^i(D)$ mit $\psi_*[d^i] = 0$. Dann gibt es ein $e^{i-1} \in E^{i-1}$ mit $\psi^i(d^i) = \partial_E e^{i-1}$. Wegen der Surjektivität von ψ^{i-1} gibt es ein $d^{i-1} \in D^{i-1}$ mit $\psi^{i-1}d^{i-1} = e^{i-1}$. Es folgt

$$\psi^i(d^i - \partial_D d^{i-1}) = \partial_E e^{i-1} - \psi^i \partial_D d^{i-1} = \partial_E \psi^{i-1} d^{i-1} - \psi^i \partial_D d^{i-1} = 0$$

(Kommutativität von (1)). Wegen Exaktheit der i -ten Zeile gibt es also ein $c^i \in C^i$ mit $\phi^i c^i = d^i - \partial_D d^{i-1}$. Es gilt dafür

$$\phi^{i+1} \partial_C c^i = \partial_D \phi^i c^i = \partial_D d^i - \partial_D \partial_D d^{i-1} = 0$$

wegen Kommutativität von (2), wegen $\partial_D \partial_D = 0$ und da d^i ein Zykel ist. Da ϕ^{i+1} injektiv ist, folgt $\partial_C c^i = 0$, d.h., c^i ist ein Zykel. Es folgt

$$[d^i] = [d^i - \partial_D d^{i-1}] = [\phi^i c^i] = \phi_*^i [c^i] \in \text{im } \phi_*^i.$$

2) **Definition von δ^i** : Sei $[e^i] \in H^i(E)$, also $e^i \in E^i$ mit $\partial_E e^i = 0$. Wegen Surjektivität von ψ^i gibt es ein $d^i \in D^i$ mit $\psi^i d^i = e^i$. Betrachte nun

$$\partial_D d^i \in D^{i+1}.$$

Es gilt

$$\begin{aligned} \psi^{i+1} \partial_D d^i &= \partial_E \psi^i d^i && \text{Kommutativität von (3)} \\ &= \partial_E e^i = 0 && \text{(Voraussetzung)}. \end{aligned}$$

Wegen Exaktheit der i -ten Zeile gibt es also ein $c^{i+1} \in C^{i+1}$ mit $\phi^{i+1} c^{i+1} = \partial_D d^i$. Für dieses Element gilt

$$\phi^{i+2} \partial_C c^{i+1} = \partial_D \phi^{i+1} c^{i+1} = \partial_D \partial_D d^i = 0$$

(Kommutativität von (4) und $\partial_D \partial_D = 0$), also $\partial_C c^{i+1} = 0$, da ϕ^{i+2} injektiv ist. Also ist c^{i+1} ein Zykel. Wir setzen

$$(4.15.2) \quad \delta([e^i]) = [c^{i+1}] \in H^{i+1}(C).$$

Fazit: Die Definition von δ^i kann wie folgt veranschaulicht werden:

$$\begin{array}{ccc} c^{i+1} & \xrightarrow{\phi^{i+1}} & \partial_D d^i \\ & & \uparrow \partial_D \\ & & d^i \xrightarrow{\psi^i} e^i \end{array}$$

Wohldefiniertheit: Sei $\tilde{e}^i \in E^i$ ein anderer Zykel mit $[\tilde{e}^i] = [e^i]$, und seien $\tilde{d}^i \in D^i$ (mit $\phi^i \tilde{d}^i = \tilde{e}^i$) und $\tilde{c}^{i+1} \in C^{i+1}$ (mit $\phi^{i+1} \tilde{c}^{i+1} = \partial_D \tilde{d}^i$) entsprechend wie oben gewählt. Wir haben zu zeigen, dass $[\tilde{c}^{i+1}] = [c^{i+1}] \in H^{i+1}(C)$.

Nach Voraussetzung gibt es ein $e^{i-1} \in E^{i-1}$ mit

$$\tilde{e}^i = e^i + \partial_C e^{i-1},$$

und wegen Surjektivität von ψ^{i-1} gibt es ein $d^{i-1} \in D^{i-1}$ mit $\psi^{i-1}d^{i-1} = e^{i-1}$. Wir berechnen

$$\begin{aligned}\psi^i(\tilde{d}^i - d^i - \partial_D d^{i+1}) &= \tilde{e}^i - e^i - \psi^i \partial_D d^{i+1} \\ &= \tilde{e}^i - e^i - \partial_E \psi^{i-1} d^{i-1} && \text{(Kommutativität von (1))} \\ &= \tilde{e}^i - e^i - \partial_E e^{i-1} = 0.\end{aligned}$$

Wegen der Exaktheit der i -ten Zeile gibt es also ein $c^i \in C^i$ mit $\phi^i c^i = \tilde{d}^i - d^i - \partial_D d^{i+1}$. Wir behaupten, dass

$$(4.15.3) \quad \widetilde{c^{i+1}} = c^{i+1} + \partial_C c^i,$$

woraus $[\widetilde{c^{i+1}}] = [c^{i+1}]$ folgt. Es ist

$$\begin{aligned}\phi^{i+1}(\widetilde{c^{i+1}} - c^{i+1}) &= \partial_D \tilde{d}^i - \partial_D d^i \\ &= \partial_D(\tilde{d}^i - d^i - \partial_D d^{i+1}) && \text{(wegen } \partial_D \partial_D = 0) \\ &= \partial_D \phi^i c^i = \phi^{i+1} \partial_C c^i && \text{(Kommutativität von (2))}\end{aligned}$$

Wegen Injektivität von ϕ^{i+1} folgt hieraus (4.15.3).

Exaktheit bei $H^i(E)$: Es ist leicht zu sehen, dass $\delta^i \psi_*^i = 0$: Ist $[e_i] \in \text{im } \psi_*^i$, so können wir oben $d^i \in Z^i(D)$, d.h., als *Zykel* wählen. Dann ist $\partial_D d^i = 0$, also $c^{i+1} = 0$, nach Definition (4.15.2) also $\delta([e^i]) = 0$. Sei nun umgekehrt $\delta([e^i]) = 0$, also (mit obigen Bezeichnungen) $[c^{i+1}] = 0$, d.h.,

$$c^{i+1} = \partial_C c^i$$

für ein $c^i \in C^i$. Es folgt (weiter mit obigen Bezeichnungen)

$$\begin{aligned}\partial_D d^i &= \phi^{i+1} c^{i+1} = \phi^{i+1} \partial_C c^i \\ &= \partial_D \phi^i c^i && \text{(Kommutativität von (2))}.\end{aligned}$$

Für $\tilde{d}^i = d^i - \phi^i c^i$ gilt also $\partial_D \tilde{d}^i = 0$, d.h., $\tilde{d}^i \in Z^i(D)$ und $\psi^i \tilde{d}^i = \psi^i d^i - \psi^i \phi^i c^i = \psi^i d^i = e^i$ (wegen $\psi^i \phi^i = 0$), also

$$\psi_*^i[\tilde{d}^i] = [e^i].$$

Exaktheit bei $H^{i+1}(C)$: Übungsaufgabe!

Da i beliebig war, folgt die Behauptung.

Corollar 4.16 (Schlangenlemma) Sei

$$(4.16.1) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\ & & \uparrow f & & \uparrow g & & \uparrow h & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von R -Moduln mit exakten Zeilen. Dann hat man eine kanonische exakte Sequenz

$$(4.16.2) \quad 0 \rightarrow \ker f \rightarrow \ker g \rightarrow \ker h \xrightarrow{\delta} \text{coker } f \rightarrow \text{coker } g \rightarrow \text{coker } h \rightarrow 0.$$

Hierbei definiert man:

Definition 4.17 Sei $\varphi : M \rightarrow N$ ein Homomorphismus von R -Moduln. Dann heißt

$$\text{coker } \varphi := N/\text{im}\varphi$$

der **Cokern** von φ .

Bemerkung: Mit dieser Definition haben wir immer eine exakte Sequenz

$$0 \rightarrow \ker \varphi \xrightarrow{i} M \xrightarrow{\varphi} N \xrightarrow{p} \text{coker } \varphi \rightarrow 0$$

wobei i die Inklusion ist und p die kanonische Projektion.

Beweis des Schlangenlemmas: Wir fassen (4.16.1) als eine kurze exakte Sequenz von Komplexen auf, wobei wir oberhalb und unterhalb mit Nullen ergänzen:

$$\begin{array}{ccccccc}
 & & \cdots & & \cdots & & \cdots \\
 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \longrightarrow 0 \\
 & & \uparrow f & & \uparrow g & & \uparrow h \\
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 \longrightarrow 0 \\
 & & \cdots & & \cdots & & \cdots
 \end{array}$$

Die lange exakte Kohomologiesequenz aus 4.15 liefert dann gerade (4.16.2): Die Kohomologie bei A, B und C ist gerade $\ker f, \ker g$ und $\ker h$, und die Kohomologie bei A', B' und C' ist gerade $A'/\text{im } f, B'/\text{im } g$ und $C'/\text{im } h$. Der Homomorphismus δ in (4.16.2) ist gerade der Verbindungshomomorphismus. Alle anderen Kohomologiegruppen sind null.

Bemerkungen 4.18 (a) Das folgende Diagramm mit exakten Zeilen *und Spalten* liefert eine Erklärung des Namens und die Definition der Abbildungen (und – durch 'Dia-

grammjagd' – auch einen Beweis des Schlangenlemmas):

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 \delta & \dashrightarrow & \text{coker } f & \longrightarrow & \text{coker } g & \longrightarrow & \text{coker } h \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & f & & g & & h \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \longrightarrow 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 0 & \longrightarrow & \text{ker } f & \longrightarrow & \text{ker } g & \longrightarrow & \text{ker } h \dashrightarrow \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Die untere Sequenz der Kerne wird von α und β induziert, die obige Sequenz der Cokerne von α' und β' . Der Homomorphismus δ ist wie folgt definiert: Für $c \in \text{ker } h \subseteq C$ sei b ein Lift von c in B ($\beta(b) = c$) und $b' = g(b) \in B'$. Dann "liegt b' schon in A' " (wenn wir α' als Inklusion auffassen), genauer gibt es ein $a' \in A'$ mit $\alpha(a') = b'$ (da $\beta'(b') = h(c) = 0$ und $\text{ker } \beta' = \text{im } \alpha'$). Man hat dann

$$\delta(c) = \text{Klasse von } a' \text{ in } \text{coker } f.$$

Dies folgt aus den Definitionen in 4.15. Andererseits kann man, mit den hier beschriebenen Abbildungen, auch leicht die Wohldefiniertheit von δ und die Exaktheit von (4.16.2) beweisen.

(b) In Büchern wird oft das leichtere Schlangenlemma bewiesen und die lange exakte Kohomologiesequenz daraus abgeleitet.

Corollar 4.19 Sei

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

eine exakte Sequenz von abelschen Gruppen und sei $n \in \mathbb{N}$. Dann hat man eine exakte Sequenz

$$0 \rightarrow A[n] \rightarrow B[n] \rightarrow C[n] \rightarrow A/n \rightarrow B/n \rightarrow C/n \rightarrow 0.$$

Für eine abelsche Gruppe D sei hierbei

$$D[n] := \{d \in D \mid n \cdot d = 0\}$$

die Gruppe der n -Torsionselemente und

$$D/n := D/nD,$$

mit $nD = \{nd \mid d \in D\} \subseteq D$.

Beweis: Schlangenlemma auf

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\
 & & \uparrow n & & \uparrow n & & \uparrow n \\
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0
 \end{array}$$

anwenden, wobei \xrightarrow{n} die n -Multiplikation $x \mapsto nx$ bezeichnet.

Corollar 4.20 (vergleiche Beispiel 2.6 (c))

$$\mathbb{Q}/\mathbb{Z}[n] \cong \mathbb{Z}/n\mathbb{Z}$$

Beweis: Anwendung von 4.19 auf die exakte Sequenz

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

wobei $\mathbb{Q}[n] = 0$ und $\mathbb{Q}/n\mathbb{Q} = 0$.

§5 Anwendung auf Gruppenkohomologie

Sei G eine Gruppe oder eine topologische Gruppe.

Definition 5.1 Seien A und B zwei (stetige) G -Moduln. Eine Abbildung

$$\varphi : A \rightarrow B$$

heißt **(Homo-)Morphismus von G -Moduln**, wenn φ ein (stetiger) Gruppenhomomorphismus ist und wenn gilt:

$$\varphi(\sigma a) = \sigma \varphi(a) \quad \text{für alle } \sigma \in G \text{ und } a \in A.$$

Lemma 5.2 Ein Homomorphismus $\varphi : A \rightarrow B$ von G -Moduln induziert einen kanonischen Homomorphismus von abelschen Gruppen in der Gruppenkohomologie

$$\varphi_* : H^i(G, A) \rightarrow H^i(G, B)$$

für alle $i \geq 0$. Es gilt dabei $id_* = id$ und $(\psi\varphi)_* = \psi_*\varphi_*$ für einen weiteren Homomorphismus von G -Moduln $\psi : B \rightarrow C$.

Beweis: φ induziert einen Homomorphismus

$$\varphi^i : C^i(G, A) \rightarrow C^i(G, B)$$

auf den (stetigen) i -Koketten durch

$$(f : G^i \rightarrow A) \mapsto (\varphi \circ f : G^i \rightarrow B).$$

Es folgt sofort aus den Definitionen, dass die φ^i kompatibel mit den Differentialen sind ($\partial\varphi^i = \varphi^{i+1}\partial$), also einen Morphismus

$$\varphi : C^\cdot(G, A) \rightarrow C^\cdot(G, B)$$

von Komplexen induzieren. Die Behauptung folgt nun durch Übergang zur Kohomologie (Lemma 4.13).

Satz 5.3 (lange exakte Kohomologiesequenz) Sei

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

eine exakte Sequenz von (stetigen) G -Moduln, d.h., α und β seien G -Modul-Homomorphismen und die Sequenz sei exakt. Im Fall von stetigen G -Moduln gelte

$$(5.3.1) \quad \begin{array}{l} \beta \text{ besitzt einen stetigen Schnitt als Mengenabbildung,} \\ \text{d.h., es gibt eine stetige Abbildung } s : C \rightarrow B \\ \text{(nicht notwendig ein Homomorphismus) mit } \beta s = id_C. \end{array}$$

Dann gibt es eine kanonische exakte Kohomologiesequenz

$$\begin{array}{ccccccccccc} 0 & \rightarrow & H^0(G, A) & \xrightarrow{\alpha_*} & H^0(G, B) & \xrightarrow{\beta_*} & H^0(G, C) & \xrightarrow{\delta} & H^1(G, A) & \rightarrow & \dots \\ \dots & \rightarrow & H^i(G, A) & \xrightarrow{\alpha_*} & H^i(G, B) & \xrightarrow{\beta_*} & H^i(G, C) & \xrightarrow{\delta} & H^{i+1}(G, A) & \rightarrow & \dots \end{array}$$

Beweis: Wir haben nur zu zeigen, dass

$$0 \rightarrow C^\cdot(G, A) \xrightarrow{\alpha} C^\cdot(G, B) \xrightarrow{\beta} C^\cdot(G, C) \rightarrow 0$$

eine kurze exakte Sequenz (von Komplexen) ist; dann folgt die Behauptung durch Übergang zur Kohomologie (Satz 4.15). Es ist also zu zeigen, dass für jedes i die Sequenz

$$0 \rightarrow C^i(G, A) \xrightarrow{\alpha^i} C^i(G, B) \xrightarrow{\beta^i} C^i(G, C) \rightarrow 0$$

exakt ist. Die Injektivität von α^i und die Exaktheit bei $C^i(G, B)$ folgt leicht aus der Exaktheit von $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C$. Sei nun $s : C \rightarrow B$ ein (stetiger) Schnitt von β . Die Existenz von s folgt aus dem Auswahlaxiom bzw. (im stetigen Fall) aus der Annahme (5.3.1). Dann ist die Abbildung

$$\begin{array}{ccc} s^i : C^i(G, C) & \rightarrow & C^i(G, B) \\ f & \mapsto & s \circ f \end{array}$$

ein mengentheoretischer Schnitt von β^i , d.h., es gilt $\beta^i s^i = id$. Hieraus folgt sofort die Surjektivität von β^i , also die Exaktheit bei $C^i(G, C)$.

Proposition 5.4 (Wechsel der Gruppe) (a) Seien G und G' (topologische) Gruppen, sei A ein (stetiger) G -Modul und A' ein (stetiger) G' -Modul. Weiter seien

$$\pi : G' \rightarrow G \quad , \quad \varphi : A \rightarrow A'$$

(stetige) Gruppenhomomorphismen mit

$$\varphi(\pi(g'))(a) = g'\varphi(a)$$

für alle $a \in A$ und alle $g' \in G'$ ((π, φ) heißt dann ein **kompatibles Paar**). Dann erhalten wir hieraus kanonische Homomorphismen

$$(\pi, \varphi)_* : H^n(G, A) \rightarrow H^n(G', A')$$

für alle $n \geq 0$.

(b) (Funktorialität) Es ist $(id_G, id_A)_* = id$. Ist

$$\pi' : G'' \rightarrow G' \quad , \quad \varphi' : A' \rightarrow A''$$

ein weiteres kompatibles Paar, so ist $(\pi\pi', \varphi'\varphi)$ kompatibel und es gilt

$$(\pi\pi', \varphi'\varphi)_* = (\pi', \varphi')_*(\pi, \varphi)_* : H^n(G, A) \rightarrow H^n(G'', A'').$$

Beweis (a): Wir erhalten die kanonischen Homomorphismen

$$\begin{array}{ccc} C^n(G, A) & \longrightarrow & C^n(G', A') \\ (f : G^n \rightarrow A) & \mapsto & (\varphi \circ f \circ \pi^n : (G')^n \longrightarrow A') \\ & & \downarrow \qquad \qquad \downarrow \\ & & G^n \longrightarrow A \end{array}$$

Diese sind offenbar kompatibel mit den Differentialen und induzieren also einen Morphismus von Komplexen

$$C(G, A) \rightarrow C(G', A').$$

Die Behauptung folgt nun aus Lemma 4.13.

(b): Dies folgt sofort aus der Konstruktion und 4.13.

Beispiele/Definition 5.5 (a) Sei $H \leq G$ eine Untergruppe und A ein (stetiger) G -Modul. Dann wird A ein (stetiger) H -Modul durch Restriktion der Operation auf H . Das Paar

$$i : H \hookrightarrow G \quad , \quad id : A \rightarrow A$$

ist kompatibel und definiert einen kanonischen Homomorphismus

$$Res : H^n(G, A) \rightarrow H^n(H, A),$$

für jedes $n \geq 0$, den man die **Restriktion** von G nach H nennt.

(b) Sei $N \trianglelefteq G$ ein Normalteiler und A ein (stetiger) G -Modul. Dann wird der Fixmodul

$$A^N$$

ein (stetiger) G/N -Modul durch die Definition

$$(gN)a := ga \quad \text{für alle } g \in G \text{ und } a \in A.$$

(dies ist wohldefiniert, da $na = a$ für alle $n \in N$, falls $a \in A^N$). Das Paar

$$\pi : G \twoheadrightarrow G/N \quad , \quad i : A^N \hookrightarrow A$$

ist nach Konstruktion kompatibel und definiert einen kanonischen Homomorphismus

$$\text{Inf} : H^n(G/N, A^N) \rightarrow H^n(G, A) ,$$

für jedes $n \geq 0$, den man die **Inflation** von G/N nach G nennt.

Wir wenden dies nun auf die sogenannte Galoiskohomologie an.

Definition 5.6 Sei L/K eine (möglicherweise unendliche) Galoiserweiterung von Körpern und $G = \text{Gal}(L/K)$ die Galoisgruppe, versehen mit der Krulltopologie. Ein **diskreter G -Modul** ist ein stetiger G -Modul A , wobei A die diskrete Topologie trägt.

Lemma 5.7 Sei A ein G -Modul. Dann sind äquivalent:

- (a) A ist diskreter G -Modul.
- (b) Für alle $a \in A$ ist der Stabilisator

$$\text{St}_G(a) = \{g \in G \mid ga = a\}$$

(vergleiche Algebra I, Def. 17.4) offen in G .

- (c) $A = \bigcup_{U \leq G} A^U$, wobei die Vereinigung über alle offenen Untergruppen von G läuft.

Beweis (a) \Rightarrow (b): Für $a \in A$ restringiere

$$\begin{aligned} \mu : G \times A &\rightarrow A \\ (g, x) &\mapsto gx \end{aligned}$$

auf die offene Menge $G \times \{a\}$. Das Urbild der offenen Menge $\{a\}$ ist gerade $\text{St}_G(a) \times \{a\}$.

(b) \Rightarrow (c): Für $a \in A$ gilt $a \in A^{\text{St}_g(a)}$.

(c) \Rightarrow (a): Sei $a \in A$ und sei $U \leq G$ eine offene Untergruppe mit $a \in A^U$. Für $(g, b) \in \mu^{-1}(\{a\})$ ist dann $Ug \times \{b\}$ eine offene Umgebung von (g, b) mit $\mu(Ug \times \{b\}) = \{gb\} = \{a\}$.

Beispiele 5.8 (a) In der Situation von 5.6 sind $(L, +)$ und (L^\times, \cdot) stetige $\text{Gal}(L/K)$ -Moduln.

(b) Jeder Untermodul eines stetigen G -Moduls ist wieder ein stetiger G -Modul.

Bemerkungen 5.9 (a) Ein stetiger $\text{Gal}(L/K)$ -Modul A heißt auch ein **Galoismodul** für L/K , und

$$H^n(\text{Gal}(L/K), A)$$

heißt die n -te **Galoiskohomologie** von A . Sie wird auch kürzer mit $H^n(L/K, A)$ bezeichnet.

(b) Sei insbesondere K_s der separable Abschluss eines Körpers K (die Menge aller über K separablen Elemente in dem algebraischen Abschluss \overline{K} von K). Dann ist K_s/K galoissch, und

$$G_K := Gal(K_s/K)$$

heißt die **absolute Galoisgruppe** von K (vergleiche 2.7 für den Fall $K = \mathbb{F}_q$). Für einen diskreten G_K -Modul A schreibt man auch

$$H^n(K, A) := H^n(K_s/K, A) = H^n(G_K, A).$$

Das Verständnis der absoluten Galoisgruppen und ihrer Galoiskohomologie ist ein wichtiges Thema der Zahlentheorie/arithmetischen Geometrie.

Sei nun weiter L/K eine Galoiserweiterung mit Galoisgruppe $G = Gal(L/K)$, und sei A ein diskreter G -Modul. Ist L' ein Zwischenkörper von L/K , der galoissch über K ist, und ist $U_{L'} = Gal(L/L')$ der zugehörige abgeschlossene Normalteiler in G , so ist

$$A^{U_{L'}}$$

ein $Gal(L'/K)$ -Modul (vermöge der Isomorphie $Gal(L'/K) \cong G/U_{L'}$), und für einen weiteren Zwischenkörper L'' mit $L \supseteq L'' \supseteq L' \supseteq K$ und L''/K galoissch gilt

$$A^{U_{L'}} = (A^{U_{L''}})^{Gal(L''/L')}$$

für die Untergruppe $Gal(L''/L') \subseteq Gal(L''/K)$.

$$\begin{array}{ccc}
 L & & 1 \\
 \downarrow & & \downarrow \\
 L'' & & U_{L''} = Gal(L/L'') \\
 Gal(L''/L') \downarrow & & \downarrow \\
 L' & & U_{L'} = Gal(L/L') \\
 Gal(L'/K) \downarrow & & \downarrow \\
 K & & G = Gal(L/K)
 \end{array}
 \left. \vphantom{\begin{array}{ccc} L & & 1 \\ \downarrow & & \downarrow \\ L'' & & U_{L''} = Gal(L/L'') \\ Gal(L''/L') \downarrow & & \downarrow \\ L' & & U_{L'} = Gal(L/L') \\ Gal(L'/K) \downarrow & & \downarrow \\ K & & G = Gal(L/K) \end{array}} \right) Gal(L''/K)$$

Wir haben also eine Inflationsabbildung

$$(5.10.1) \quad Inf_{L''/L'} : H^n(L'/K, A^{U_{L'}}) \rightarrow H^n(L''/K, A^{U_{L''}})$$

Weiter ist nach 5.4 (b) klar, dass für eine weitere galoissche Teilerweiterung L'''/K mit $L''' \supseteq L'' \supseteq L'$ gilt

$$(5.10.2) \quad Inf_{L'''/L'} = Inf_{L'''/L''} \circ Inf_{L''/L'},$$

sowie $Inf_{L'/L'} = id$.

Insbesondere erhalten wir ein induktives System

$$(5.10.3) \quad (H^n(L'/K, A^{U_{L'}}))_{L' \in \mathcal{K}(L/K)},$$

mit den Inflationen (5.10.1) als Übergangsabbildungen, wobei $\mathcal{K}(L/K)$ die induktiv geordnete Menge der *endlichen* galoisschen Teilerweiterungen von L/K ist (vergleiche 2.4 (d)). Für diese ist jeweils $U_{L'}$ offen und $Gal(L'/K)$ endlich.

Weiter hat man für $L', L'' \in \mathcal{K}(L/K)$ und $L' \subseteq L''$ ein kommutatives Diagramm

$$(5.10.4) \quad \begin{array}{ccc} H^n(L''/K, A^{U_{L''}}) & & \\ \uparrow \text{Inf}_{L''/L'} & \searrow \text{Inf}_{L/L''} & \\ H^n(L'/K, A^{U_{L'}}) & & H^n(L/K, A) \end{array}$$

nach (5.10.3) für $L'' = L$. Nach der universellen Eigenschaft des induktiven Limes (siehe Übungsaufgabe 3) liefert dies einen kanonischen Homomorphismus

$$(5.10.5) \quad \lim_{\substack{\longrightarrow \\ L' \in \mathcal{K}(L/K)}} H^n(L'/K, A^{U_{L'}}) \rightarrow H^n(L/K, A).$$

Explizit wird ein Element links, repräsentiert durch ein $x \in H^n(L'/K, A^{U_{L'}})$ für ein $L' \in \mathcal{K}(L/K)$, abgebildet auf $\text{Inf}_{L/L'}(x)$.

Der folgende Satz zeigt, dass man die Galoiskohomologie von L/K als induktiven Limes der Kohomologien der endlichen Gruppen $Gal(L'/K)$ berechnen kann.

Satz 5.10 Die Abbildung (5.10.5) ist ein Isomorphismus.

Beweis: Nach Definition wird $\text{Inf}_{L/L'}$ durch den Morphismus von Komplexen

$$\begin{array}{ccccccc} \cdots & \longrightarrow & C^{n-1}(G, A) & \xrightarrow{\partial} & C^n(G, A) & \xrightarrow{\partial} & C^{n+1}(G, A) & \longrightarrow & \cdots \\ & & \uparrow \alpha^{n-1} & & \uparrow \alpha^n & & \uparrow \alpha^{n+1} & & \\ \cdots & \longrightarrow & C^{n-1}(Gal(L'/K), A^{U_{L'}}) & \xrightarrow{\partial} & C^n(Gal(L'/K), A^{U_{L'}}) & \xrightarrow{\partial} & C^{n+1}(Gal(L'/K), A^{U_{L'}}) & \longrightarrow & \cdots \end{array}$$

induziert. Hierbei ist $\alpha^r(f) = ifp^r$ für eine r -Kokette $g : Gal(L'/K)^r \rightarrow A^{U_{L'}}$, wobei $p : G \twoheadrightarrow Gal(L'/K) = G/U_{L'}$ die Projektion und $i : A^{U_{L'}} \hookrightarrow A$ die Inklusion ist. Offenbar sind alle α^r injektiv.

Surjektivität von (5.10.5): Es genügt zu zeigen: Ist $f \in C^n(G, A)$, so gibt es ein $L' \in \mathcal{K}(L/K)$ und ein $g \in C^n(Gal(L'/K), A^{U_{L'}})$ mit $\alpha^n(g) = f$. Ist nämlich f ein n -Kozykel, so ist g ebenfalls ein Kozykel, wegen $\alpha^{n+1}\partial g = \partial\alpha^n g = \partial f = 0$ und Injektivität von α^{n+1} , und damit ist $[f] = [\alpha g] = \alpha_*[g] = \text{Inf}_{L/L'}[g]$.

Sei also $f : G^n \rightarrow A$ ein Element in $C^n(G, A)$, also eine stetige Abbildung. Mit G ist auch G^n kompakt, also auch $f(G^n)$, da A als diskreter topologischer Raum offenbar Hausdorffsch ist. Da A diskret ist, bedeutet dies, dass $f(G^n)$ endlich ist. Da jedes Element $a \in A$ im Fixmodul A^U für eine offene Untergruppe $U \leq G$ liegt, gibt es eine offene Untergruppe $U \leq G$ mit

$$f(G^n) \subseteq A^U.$$

Dabei können wir durch Übergang zu einer offenen Untergruppe annehmen, dass $U \trianglelefteq G$ ein offener Normalteiler ist (Ist $U = \text{Gal}(L/K')$ für eine endliche Teilerweiterung K'/K , so betrachte $U' = \text{Gal}(L/L')$ für die normale Hülle L'/K von K'/K).

Weiter ist wegen der Stetigkeit von f und der Diskretheit von A für jedes $g = (g_1, \dots, g_n) \in G^n$ die Menge $f^{-1}(\{f(g_1, \dots, g_n)\})$ offen, enthält also eine offene Umgebung $g_1 U_1 \times \dots \times g_n U_n =: U(g)$ von g , mit offenen Untergruppen U_1, \dots, U_n von G . Wie oben können wir annehmen, dass die U_i offene Normalteiler von G sind. Da G^n kompakt ist, wird G^n von endlich vielen $U(g^{(1)}, \dots, U(g^{(r)})$ überdeckt. Sei N der Durchschnitt des obigen U und aller U_i , die in den endlich vielen $U(g^{(\nu)})$ auftreten. Dann hängt f nur von den Nebenklassen modulo N ab, ist also konstant auf allen Mengen

$$g_1 N \times \dots \times g_n N$$

für alle $(g_1, \dots, g_n) \in G^n$. Außerdem hat f wegen $N \subseteq U$ Bild in A^N .

Ist nun $L' = L^N$, so ist nach (unendlicher) Galoistheorie L'/K eine **endliche** Galoiserweiterung und $N = \text{Gal}(L/L') = U_{L'} = \ker(G \xrightarrow{P} \text{Gal}(L'/K))$, und nach Konstruktion liegt f im Bild von

$$\alpha^n : C^n(\text{Gal}(L'/K), A^{U_{L'}}) \rightarrow C^n(G, A)$$

(Urbild von f ist g mit $g((p(g_1), \dots, p(g_n))) = f(g_1, \dots, g_n)$).

Injektivität von (5.10.5): Sei $g \in Z^n(\text{Gal}(L'/K), A^{U_{L'}})$ mit $\text{Inf}_{L/L'}[g] = [\alpha^n_{L/L'} g] = 0$. Es gibt also ein $f_1 \in C^{n-1}(G, A)$ mit $\partial f_1 = \alpha^n_{L/L'} g$. Nach dem ersten Schritt gibt es eine endliche galoissche Teilerweiterung L''/K und ein $g_1 \in C^{n-1}(\text{Gal}(L''/K), A^{U_{L''}})$ mit $\alpha^{n-1}_{L/L''} g_1 = f_1$. Dabei können wir annehmen, dass $L'' \supseteq L'$ (Verkleinern des Normalteilers N oben). Bilden wir dann

$$\alpha^r_{L''/L'} : C^r(\text{Gal}(L'/K) A^{U_{L'}}) \rightarrow C^r(\text{Gal}(L''/K), A^{U_{L''}})$$

wie oben, so folgt

$$\alpha^n_{L/L''} \alpha^n_{L''/L'} g = \alpha^n_{L/L'} g = \partial f_1 = \partial \alpha^{n-1}_{L/L''} g_1 = \alpha^n_{L/L''} \partial g_1,$$

also $\alpha^n_{L''/L'} g = \partial g_1$ wegen Injektivität von $\alpha^n_{L/L''}$. Dies bedeutet, dass $\text{Inf}_{L''/L'}[g] = [\alpha^n_{L''/L'} g] = 0$, also dass $[g]$ im induktiven Limes gleich 0 ist.

Wir führen noch ein nützliches Hilfsmittel zur Berechnung von Kohomologie ein. Sei G eine Gruppe mit diskreter Topologie oder $G = \text{Gal}(L/K)$ für eine Galoiserweiterung L/K , versehen mit der Krulltopologie.

Lemma/Definition 5.11 Sei A eine abelsche Gruppe und

$$M^G(A) = \{f : G \rightarrow A \mid f \text{ stetig} \}$$

wobei A die diskrete Topologie trägt. Dann wird $M^G(A)$ ein diskreter G -Modul durch die Definition

$$(gf)(h) := f(hg)$$

für $g, h \in G$ und heißt der **coinduzierte Modul** zu A .

Beweis der Behauptungen: 1) $M^G(A)$ ist ein G -Modul: Es ist klar, dass $1 \cdot f = f$ und dass $g(f_1 + f_2) = gf_1 + gf_2$ für $g \in G$. Weiter gilt

$$\begin{aligned}(g_1(g_2f))(h) &= (g_2f)(hg_1) = f((hg_1)g_2) \\ &= f(h(g_1g_2)) = ((g_1g_2)f)(h),\end{aligned}$$

also $g_1(g_2f) = (g_1g_2)f$ für $g_1, g_2 \in G$.

2) $M^G(A)$ ist ein diskreter G -Modul: Für G mit diskreter Topologie ist nichts zu zeigen; sei also $G = \text{Gal}(L/K)$ eine Galoisgruppe. Ist $f : G \rightarrow A$ stetig, wobei A die diskrete Topologie hat, so gibt es nach dem Beweis von Satz 5.10 einen offenen Normalteiler $N \trianglelefteq G$, so dass $f(g) = f(gn)$ für alle $n \in N$. Dies bedeutet aber $f = nf$ für alle $n \in N$. Der Stabilisator von f in G enthält also N , ist also offen.

Bemerkungen 5.12 Für G mit diskreter Topologie ist $M^G(A)$ einfach die Menge aller Abbildungen $f : G \rightarrow A$. Insbesondere hat man für eine *endliche* Gruppe G einen Gruppenisomorphismus

$$\begin{aligned}M^G(A) &\xrightarrow{\sim} \bigoplus_{\sigma \in A} A \\ f &\mapsto (f(\sigma^{-1}))_{\sigma \in G},\end{aligned}$$

und dies wird ein Isomorphismus von G -Moduln, wenn G rechts wie folgt operiert:

$$\tau(a_\sigma)_{\sigma \in G} = (a_{\tau^{-1}\sigma})_{\sigma \in G}.$$

Insbesondere gibt es einen Isomorphismus von G -Moduln

$$M^G(\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}[G],$$

wobei $\mathbb{Z}[G]$ der Gruppenring ist (siehe Übungsaufgabe 11). Der Nutzen der coinduzierten G -Moduln liegt in der folgenden Eigenschaft:

Proposition 5.13 (a) Unter den Voraussetzungen von 5.11 gilt

$$H^n(G, M^G(A)) = 0 \quad \text{für alle } n > 0.$$

(b) Weiter gibt es einen kanonischen Isomorphismus

$$H^0(G, M^G(A)) \cong A.$$

Beweis (a) Sei $n \geq 1$ und $f \in Z^n(G, M^G(A))$. Definiere eine Abbildung

$$h : G^{n-1} \rightarrow M^G(A)$$

durch

$$h(g_1, \dots, g_{n-1})(g) := f(g, g_1, \dots, g_{n-1})(1).$$

Dann ist h wohldefiniert und stetig (bezüglich der diskreten Topologie auf $M^G(A)$): Nach dem Beweis von Satz 5.10 gibt es wegen der Stetigkeit von f einen offenen Normalteiler $N \trianglelefteq G$, so dass $f : G^n \rightarrow M^G(A)$ über $(G/N)^n$ faktorisiert. Daher hängt $h(g_1, \dots, g_{n-1})$

nur von $g \bmod N$ ab, ist also stetig, d.h., in $M^G(A)$, und weiter faktorisiert h über $(G/N)^{n-1}$ und ist somit stetig.

Weiter berechnen wir für $g_1, \dots, g_n, g \in G$ mit Definition 3.1

$$\begin{aligned} & ((\partial_n h)(g_1, \dots, g_n))(g) \\ &= [g_1 h(g_2, \dots, g_n) + \sum_{i=1}^{n-1} (-1)^i h(g_1, \dots, g_i g_{i+1}, \dots, g_n) + (-1)^n h(g_1, \dots, g_{n-1})](g) \\ &= [f(g g_1, g_2, \dots, g_n) + \sum_{i=1}^{n-1} (-1)^i f(g, g_1, \dots, g_i g_{i+1}, \dots, g_n) + (-1)^n h(g, g_1, \dots, g_{n-1})](1) \\ &= [-(\partial f)(g, g_1, \dots, g_n) + g f(g_1, \dots, g_n)](1) = (g f(g_1, \dots, g_n))(1) = f(g_1, \dots, g_n)(g) \end{aligned}$$

wegen $\partial f = 0$. Also ist $f = \partial h \in B^n(G, M^G(A))$ wie behauptet.

(b): Für $f \in M^G(A)$ gilt: $f \in M^G(A) \Leftrightarrow f(h) = f(hg)$ für alle $h, g \in G \Leftrightarrow f$ ist konstant. Die Abbildung $a \mapsto f$ mit $f(g) = a$ für alle $g \in G$ induziert also den Isomorphismus in (b).

Corollar 5.14 Ist G eine endliche Gruppe, so ist $H^n(G, \mathbb{Z}[G]) = 0$ für alle $n > 0$.

Lemma 5.15 Sei A ein diskreter G -Modul. Dann ist die Abbildung

$$\begin{aligned} i_A : A &\hookrightarrow M^G(A) \\ a &\mapsto f_a \text{ mit } f_a(g) = ga \end{aligned}$$

ein injektiver Homomorphismus von G -Moduln (wobei rechts A nur als abelsche Gruppe aufgefasst wird).

Beweis Für $h \in G$ ist $f_{ha}(g) = g(ha) = (gh)a = f_a(gh) = (hf_a)(g)$, also $f_{ha} = hf_a$.

Bemerkung 5.16 Setzen wir $B := \text{coker } i_A = M^G(A)/A$, so erhalten wir eine kurze exakte Sequenz von diskreten G -Moduln

$$0 \rightarrow A \hookrightarrow M^G(A) \rightarrow B \rightarrow 0.$$

In der langen exakten Kohomologiesequenz

$$0 \rightarrow A^G \rightarrow (M^G(A))^G \rightarrow B^G \rightarrow H^1(G, A) \rightarrow \dots$$

ist nach 5.13 $H^n(G, M^G(A)) = 0$ für $n \geq 1$. Dies liefert eine exakte Sequenz

$$0 \rightarrow A^G \hookrightarrow A \rightarrow B^G \rightarrow H^1(G, A) \rightarrow 0$$

und Isomorphismen

$$H^{i-1}(G, B) \xrightarrow{\sim} H^i(G, A).$$

Hierdurch kann man die Kohomologie von A im Grad i (man spricht auch von Dimension i) durch die Kohomologie von B im Grad $i - 1$ berechnen. Dies heißt die Methode der **Dimensionsverschiebung**.

Eine andere Anwendung ist:

Satz 5.17 Sei G eine endliche Gruppe der Ordnung N . Für jeden G -Modul A und jedes $n > 0$ gilt

$$N \cdot H^n(G, A) = 0.$$

Beweis: Wir haben die Homomorphismen von G -Moduln

$$\begin{array}{ccc} A & \xrightarrow{i} & M^G(A) & \xrightarrow{\pi} & A \\ a & \mapsto & (\sigma \mapsto \sigma a) & & \\ & & f & \mapsto & \sum_{\sigma \in G} \sigma^{-1} f(\sigma). \end{array}$$

Für $i = i_A$ (und allgemeine $G!$) siehe 5.15. Die Abbildung $\pi = \pi_A$ ist nur für endliches G definiert. Die Additivität ist klar, und für $\tau \in G$ gilt

$$\pi(\tau f) = \sum_{\sigma \in G} \sigma^{-1} f(\sigma \tau) = \sum_{\sigma \in G} \tau(\sigma \tau)^{-1} f(\sigma \tau) = \tau \pi(f).$$

Offenbar gilt $\pi i = N$, d.h., $\pi(i(a)) = N \cdot a$. Dann ist auch die Komposition

$$H^n(G, A) \xrightarrow{i_*} H^n(G, M^G(A)) \xrightarrow{\pi_*} H^n(G, A)$$

die Multiplikation mit N ($N_* = N$, wie man aus der Definition sieht). Andererseits ist diese Komposition null, da $H^n(G, M^G(A)) = 0$ ($n > 0$). Es folgt die Behauptung.

§6 Hilbert 90 und Kummer-Theorie

Satz 6.1 (Hilberts Satz 90) Sei L/K eine Galoiserweiterung mit Galoisgruppe G . Dann ist

$$H^1(L/K, L^\times) = H^1(G, L^\times) = 0.$$

Beweis: Nach der Limeseigenschaft Satz 5.10 genügt es, dies für endliche Galoiserweiterungen zu zeigen (Beachte: Für einen Zwischenkörper M von L/K ist $L^\times \text{Gal}(L/M) = M^\times$ nach Galoistheorie). Sei also G endlich und

$$f : G \rightarrow L^\times$$

ein 1-Kozykel. Wegen der linearen Unabhängigkeit von Körperhomomorphismen (Algebra I, Corollar 20.3) ist dann

$$\sum_{\sigma \in G} f(\sigma) \sigma$$

nicht die Nullabbildung; es gibt also ein $\alpha \in L^\times$ mit

$$\beta := \sum_{\sigma \in G} f(\sigma) \sigma(\alpha) \neq 0,$$

d.h., $\beta \in L^\times$. Für $\tau \in G$ gilt dann weiter wegen der Kozykel-Eigenschaft ($f(\tau\sigma) = \tau f(\sigma) \cdot f(\tau)$)

$$\tau(\beta) = \sum_{\sigma \in G} \tau f(\sigma) \tau \sigma(\alpha) = \sum_{\sigma \in G} f(\tau)^{-1} f(\tau\sigma) \tau \sigma(\alpha) = f(\tau)^{-1} \beta.$$

Daher ist

$$f(\tau) = \tau(\beta)^{-1} \cdot \beta = \tau(\beta^{-1}) \cdot (\beta^{-1})^{-1} \quad \text{für alle } \tau \in G,$$

also ein f Korand.

Dieser Satz hat viele Anwendungen; eine davon ist die Kummer-Theorie (vergleiche auch Algebra I, §20):

Sei K ein Körper und K_s ein separabler Abschluss von K . Weiter sei n eine natürliche Zahl, die in K invertierbar ist (d.h., $\text{char}(K) \nmid n$) und $\mu_n \subseteq K_s^\times$ die Gruppe der n -ten Einheitswurzeln in K_s . Dann ist μ_n zyklisch von der Ordnung n (siehe Algebra I, Lemma 15.6(e)). Jede separable Erweiterung L von K fassen wir als Teilkörper von K_s auf. Für jedes solche L sei $\mu_n(L) = \mu_n \cap L$ die Menge der n -ten Einheitswurzeln in L .

Satz 6.2 (Kummer-Isomorphismus) Sei L/K eine galoissche Körpererweiterung. Dann gibt es einen Isomorphismus

$$(L^\times)^n \cap K^\times / (K^\times)^n \xrightarrow{\delta} H^1(L/K, \mu_n(L)),$$

der für ein $\alpha \in K^\times$ mit $\alpha = \beta^n, \beta \in L$, die Klasse von α auf die Klasse des Kozykels

$$\sigma \mapsto \frac{\sigma(\beta)}{\beta} \in \mu_n(L)$$

abbildet.

Beweis: Wir haben eine exakte Sequenz von diskreten $\text{Gal}(L/K)$ -Moduln

$$1 \rightarrow \mu_n(L) \hookrightarrow L^\times \xrightarrow{n} (L^\times)^n \rightarrow 1,$$

wobei \xrightarrow{n} für den Homomorphismus $x \mapsto x^n$ steht. Dies liefert die exakte Kohomologiesequenz

$$K^\times \xrightarrow{n} (L^\times)^n \cap K^\times \xrightarrow{\delta} H^1(L/K, \mu_n(L)) \rightarrow H^1(L/K, L^\times) = 0.$$

Hierbei haben wir benutzt, dass mit $G = \text{Gal}(L/K)$ gilt: $(L^\times)^G = K^\times, ((L^\times)^n)^G = (L^\times)^n \cap K^\times$, sowie $H^1(G, L^\times) = 0$ (Hilbert 90). Weiter ist δ der Verbindungshomomorphismus. Wegen der Exaktheit der Kohomologiesequenz folgt die Surjektivität von δ und die Behauptung des Satzes mit dem Homomorphiesatz, da das Bild der ersten Abbildung $(K^\times)^n$ ist. Die explizite Beschreibung von δ folgt aus der Definition von δ und des Differentials $\partial^0 : L^\times \rightarrow C^1(G, L^\times)$.

Corollar 6.3 Es gibt einen Isomorphismus

$$K^\times / (K^\times)^n \xrightarrow{\delta} H^1(K, \mu_n).$$

Beweis: Dies folgt aus 6.2 für $L = K_s$, weil $(K_s^\times)^n \cap K^\times = K^\times$ gilt: Für jedes $\alpha \in K^\times$ gibt es nämlich ein $\beta \in K_s^\times$ mit $\beta^n = \alpha$. Denn zunächst gibt es ein solches β im algebraischen Abschluss, als Nullstelle des Polynoms $X^n - \alpha$, aber β ist in K_s , da dieses Polynom separabel ist (wegen $\text{char}(K) \nmid n$, vergleiche Algebra I, Beweis von Satz 20.5).

Bemerkung 6.4 Wir haben also eine exakte Sequenz von diskreten G_K -Moduln

$$1 \rightarrow \mu_n \rightarrow K_s^\times \xrightarrow{n} K_s^\times \rightarrow 1,$$

die sogenannte **Kummer-Sequenz**. Corollar 6.3 folgt auch direkt aus der zugehörigen Kohomologiesequenz.

Satz 6.2 kann noch zu einer Existenzaussage verschärft werden.

Definition 6.5 K enthalte alle n -ten Einheitswurzeln (d.h., es gelte $\mu_n(K) = \mu_n$). Eine Galoiserweiterung L/K heie Kummer-Erweiterung vom Exponenten n , wenn L/K abelsch vom Exponenten n ist.

Hier definieren wir fur $n \in \mathbb{N}$:

Definition 6.6 (a) Eine abelsche Gruppe A heit von Exponenten n , wenn $nA = 0$, d.h., $na = 0$ fur alle $a \in A$.

(b) Eine Galoiserweiterung L/K heit abelsch (bzw. abelsch vom Exponenten n), wenn $\text{Gal}(L/K)$ abelsch (bzw. abelsch von Exponenten n) ist.

Satz 6.7 (Kummer-Korrespondenz) Es gelte $\mu_n \subseteq K$. Dann gibt es zueinander inverse, inklusionserhaltende Bijektionen

$$\mathcal{K} := \left\{ \begin{array}{l} \text{endliche Kummer-} \\ \text{Erweiterungen } L/K \\ \text{vom Exponenten } n \end{array} \right\} \begin{array}{c} \xrightarrow{\phi} \\ \xleftarrow{\psi} \end{array} \left\{ \begin{array}{l} \text{Untergruppen } \Delta \subseteq K^\times \\ \text{mit } (K^\times)^n \subseteq \Delta \text{ und} \\ \Delta/(K^\times)^n \text{ endlich} \end{array} \right\} =: \mathcal{D}$$

mittels der Zuordnungen

$$\begin{array}{ccc} L & \xrightarrow{\phi} & \Delta_L := (L^\times)^n \cap K^\times \\ L_\Delta := L(\sqrt[n]{\Delta}) & \xleftarrow{\psi} & \Delta. \end{array}$$

Hierbei sei $L(\sqrt[n]{\Delta}) = L(\sqrt[n]{\alpha} \mid \alpha \in \Delta)$.

Beweis: Fur $L \in \mathcal{K}$ gilt $(K^\times)^n \subseteq \Delta_L \subseteq K^\times$, und nach Satz 6.2 haben wir einen Isomorphismus

$$\Delta_L/(K^\times)^n \xrightarrow{\sim} H^1(\text{Gal}(L/K), \mu_n).$$

Da L/K endlich ist, ist $H^1(\text{Gal}(L/K), \mu_n)$ offenbar endlich, also liegt Δ_L in \mathcal{D} . Ist umgekehrt $\Delta \in \mathcal{D}$, so ist fur jedes $\alpha \in \Delta$ die Erweiterung $K(\sqrt[n]{\alpha})/K$ galoissch, mit zyklischer Galoisgruppe von Exponenten n (wegen $\mu_n \subseteq K$, nach der Kummer-Theorie aus Algebra I, §20). Seien $\alpha_1, \dots, \alpha_r \in \Delta$ Elemente, deren Nebenklassen ein Representantensystem fur die endliche Gruppe $\Delta/(K^\times)^n$ bilden. Fur jedes $\alpha \in \Delta$ gilt dann $\alpha = \alpha_{i_1} \dots \alpha_{i_s} \gamma^n$ mit $i_1, \dots, i_s \in \{1, \dots, r\}$ und $\gamma \in K^\times$ und daher

$$K(\sqrt[n]{\alpha}) \subseteq K(\sqrt[n]{\alpha_{i_1}}, \dots, \sqrt[n]{\alpha_{i_s}}).$$

Daher ist $L_\Delta = K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\alpha_1}, \dots, \sqrt[n]{\alpha_r})$ das Kompositum der $K(\sqrt[n]{\alpha_i})$ und daher endlich uber K und abelsch vom Exponenten n (beachte Algebra I, Lemma 21.4), also in \mathcal{K} . Die Zuordnungen ϕ und ψ sind also wohldefiniert.

Weiter gilt

$$(6.7.1) \quad K(\sqrt[n]{\Delta_L}) \subseteq L \quad , \text{ d.h.}, \quad \psi \phi L \subseteq L .$$

Für $\alpha \in \phi L = \Delta_L = (L^\times)^n \cap K^\times$ gilt nämlich $K(\sqrt[n]{\alpha}) \subseteq L$. Denn hier bezeichnet $\sqrt[n]{\alpha}$ ein Element $\gamma \in K_s$ mit $\gamma^n = \alpha$. Andererseits gilt nach Definition $\alpha = \beta^n$ für ein $\beta \in L^\times$. Damit folgt $(\gamma/\beta)^n = \alpha/\alpha = 1$, also $\gamma/\beta = \zeta \in \mu_n \subseteq K$. Es folgt $K(\gamma) = K(\beta) \subseteq L$. Insgesamt folgt $\psi \phi L = K(\sqrt[n]{\Delta_L}) \subseteq L$, also (6.7.1). Andererseits gilt

$$(6.7.2) \quad (L_\Delta^\times)^n \cap K^\times \supseteq \Delta \quad , \text{ d.h.}, \quad \phi \psi \Delta \supseteq \Delta .$$

Sei nämlich $L_\Delta = K(\sqrt[n]{\Delta})$ und $\alpha \in \Delta$. Dann gibt es ein $\beta \in L_\Delta$ mit $\beta^n = \alpha$, und es folgt $\alpha \in (L_\Delta^\times)^n \cap K^\times = \phi \psi \Delta$.

Weiter sind ϕ und ψ offenbar inklusionsend-erhaltend, d.h., es gilt

$$(6.7.3) \quad \begin{aligned} L \subset L' &\Rightarrow \Delta_L \subset \Delta_{L'} \\ \Delta \subset \Delta' &\Rightarrow L_\Delta \subset L_{\Delta'} . \end{aligned}$$

Wir zeigen nun $\psi \phi L = L$ für $L \in \mathcal{K}$. Nach Voraussetzung ist $Gal(L/K)$ eine endliche abelsche Gruppe von Exponenten n . Wir benutzen

Satz 6.8 (Hauptsatz über endliche abelsche Gruppen) Jede endlich abelsche Gruppe ist direktes Produkt von zyklischen Gruppen.

Beweis: Später.

Danach ist

$$(6.7.4) \quad Gal(L/K) = \bigoplus_{i=1}^r A_i$$

mit zyklischen Gruppen A_i , die notwendigerweise ebenfalls von Exponenten n sind. Die Projektionen

$$Gal(L/K) \twoheadrightarrow A_i$$

entsprechen nach Galoistheorie Teilerweiterungen $L_i \subseteq L$ mit $Gal(L_i/K) = A_i$ ($L_i = L^{A_i}$ mit $A_i = \bigoplus_{j \neq i} A_j$), und wegen (6.7.4) ist L das Kompositum der L_i . Nach der Kummertheorie für zyklische Erweiterungen (Algebra I, Satz 20.7) gibt es für jedes i ein $\alpha_i \in K$ mit $L_i = K(\sqrt[n]{\alpha_i})$ (Ist L_i/K zyklisch von Grad m_i , so gilt $m_i \mid n$, also $\mu_{m_i} \subseteq \mu_n \subset K$, und nach Algebra I 20.7 gibt es ein $\beta_i \in K$ mit $L_i = L(\sqrt[m_i]{\beta_i})$. Wir können dann $\alpha_i = \beta_i^{\frac{n}{m_i}}$ nehmen). Nach Konstruktion ist $\sqrt[n]{\alpha_i} \in L$, also $\alpha_i \in \Delta_L$, also $L_i \subseteq K(\sqrt[n]{\Delta_L})$. Damit liegt auch das Kompositum L in $K(\sqrt[n]{\Delta_L})$. Wegen (6.7.1) folgt Gleichheit.

Wir zeigen nun $\phi \psi \Delta = \Delta$. Sei $\tilde{\Delta} = \phi \psi \Delta$ und $\tilde{L} = L_\Delta = \psi \Delta$, so dass $\tilde{\Delta} = \Delta_{\tilde{L}}$. Nach (6.7.2) ist $\Delta \subseteq \tilde{\Delta}$, und wir erhalten ein Diagramm

$$\begin{array}{ccc} \tilde{\Delta}/(K^\times)^n = & (\tilde{L}^\times)^n \cap K^\times / (K^\times)^n & \xrightarrow[\sim]{\delta} H^1(\tilde{L}/K, \mu_n) \\ & \cup & \\ & \Delta/(K^\times)^n & \end{array}$$

Angenommen $\Delta \subsetneq \tilde{\Delta}$. Dann ist $U := \delta(\Delta/(K^\times)^n)$ eine echte Untergruppe von

$$H^1(\tilde{L}/K, \mu_n) = \text{Hom}(G, \mu_n)$$

wobei $G = \text{Gal}(\tilde{L}/K)$. Sei

$$H = \{\sigma \in G \mid \chi(\sigma) = 1 \text{ für alle } \chi \in U\},$$

Nach dem folgenden Satz 6.10 (siehe Bemerkung 6.11) ist $H \neq 1$. Andererseits gilt

$$\begin{aligned} \sigma \in H &\Leftrightarrow \delta(\alpha)(\sigma) = 1 \text{ für alle } \alpha \in \Delta \\ &\Leftrightarrow \sigma(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha} \text{ für alle } \alpha \in \Delta \\ &\Leftrightarrow \sigma = 1, \end{aligned}$$

da $\tilde{L} = K(\sqrt[n]{\Delta})$ – Widerspruch!. Daher gilt $\tilde{\Delta} = \Delta$, d.h., $\phi\psi\Delta = \Delta$, und Satz 6.7 ist bewiesen.

Definition 6.9 Für eine endliche abelsche Gruppe A heißt

$$A^\vee := \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

das **Pontrjagin-Dual** von A .

Satz 6.10 (Dualitätstheorie für endliche abelsche Gruppen) Sei A eine endliche abelsche Gruppe.

(a) A^\vee ist nicht-kanonisch isomorph zu A . Insbesondere ist A^\vee wieder endlich und abelsch und hat dieselbe Ordnung wie A

(b) Ist A vom Exponenten $n \in \mathbb{N}$, so gilt

$$A^\vee = \text{Hom}(A, \mathbb{Z}/n\mathbb{Z}).$$

(c) Die kanonische Abbildung

$$\begin{aligned} \varphi_A : A &\rightarrow A^{\vee\vee} \\ a &\mapsto (\chi \mapsto \chi(a)) \end{aligned}$$

ist ein Isomorphismus.

(d) Ist

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

eine exakte Sequenz von endlichen abelschen Gruppen, so ist

$$0 \rightarrow C^\vee \xrightarrow{\beta^\vee} B^\vee \xrightarrow{\alpha^\vee} A^\vee \rightarrow 0$$

exakt (Für einen beliebigen Homomorphismus $\varphi : A \rightarrow B$ sei dabei $\varphi^\vee : B^\vee \rightarrow A^\vee$ durch $B^\vee \ni \chi \mapsto \chi \circ \varphi \in A^\vee$ definiert).

(e) Für eine Untergruppe $U \leq A$ sei

$$U^\perp = \{\chi \in A^\vee \mid \chi|_U = 0\}.$$

Dann ist die Zuordnung

$$U \mapsto U^\perp$$

eine Inklusions-umkehrende Bijektion zwischen den Untergruppen von A und den Untergruppen von A^\vee . Dabei gilt $A^\vee/U^\perp \xrightarrow{\sim} U^\vee$.

Bemerkung 6.11 Aus diesem Satz folgt die Beziehung $H \neq \{1\}$ im obigen Beweis: Identifizieren wir die beiden zyklischen Gruppen μ_n und $\mathbb{Z}/n\mathbb{Z}$, so ist

$$\text{Hom}(G, \mu_n) \cong \text{Hom}(G, \mathbb{Z}/n\mathbb{Z}) = G^\vee.$$

Gehen wir zur additiven Schreibweise über, so erhalten wir für $U \leq G^\vee$ die exakte Sequenz

$$0 \rightarrow U \rightarrow G^\vee \rightarrow G^\vee/U \rightarrow 0$$

mit nicht-trivialem G^\vee/U und eine exakte Sequenz

$$0 \rightarrow (G^\vee/U)^\vee \rightarrow G^{\vee\vee} \rightarrow U^\vee \rightarrow 0$$

wobei $(G^\vee/U)^\vee$ nicht-trivial ist. Die Abbildung $G^{\vee\vee} \rightarrow U^\vee$ (die $\psi \in (G^\vee)^\vee$ auf $\psi|_U$ abbildet) hat also nicht-trivialen Kern. Benutzen wir die Isomorphie $\varphi_G : G \xrightarrow{\sim} G^{\vee\vee}$, so gibt es also ein $a \in G$, a nicht-trivial, mit $\varphi_G(a)(\chi) = \chi(a) = 0$ für alle $\chi \in U$. Dies liefert ein nicht-triviales Element in der Gruppe H oben.

Beweis von Satz 6.10: (b): Hat A den Exponenten n , so gilt für $\chi \in A^\vee$:

$$(n\chi)(a) = n \cdot \chi(a) = \chi(na) = \chi(0) = 0.$$

Insbesondere hat χ Bild in $\mathbb{Q}/\mathbb{Z}[n] = \mathbb{Z}/n\mathbb{Z}$ (vergleiche 4.20), und A^\vee ist wieder vom Exponenten n .

Es genügt im Folgenden, Gruppen von einem festen Exponenten n zu betrachten.

(a) Für $\mathbb{Z}/n\mathbb{Z}$ gilt kanonisch

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\vee \\ b &\mapsto (\varphi_b \text{ mit } \varphi_b(\bar{1}) = b) \end{aligned}$$

(also $\varphi_b(a) = ab$). Für eine endliche zyklische Gruppe A folgt eine nicht-kanonische Isomorphie $A \xrightarrow{\sim} A^\vee$ durch Wahl eines Isomorphismus $A \cong \mathbb{Z}/n\mathbb{Z}$. Für eine beliebige endliche abelsche Gruppe A gibt es nach Satz 6.8 zyklische Untergruppen A_1, \dots, A_r mit

$$A = A_1 \oplus \dots \oplus A_r.$$

Es gibt dann aber eine kanonische Isomorphie

$$(6.10.1) \quad \begin{aligned} A_1^\vee \oplus \dots \oplus A_r^\vee &\xrightarrow{\sim} (A_1 \oplus \dots \oplus A_r)^\vee \\ (\chi_1, \dots, \chi_r) &\mapsto \chi \text{ mit } \chi(a_1, \dots, a_r) = \sum_{i=1}^r \chi_i(a_i) \end{aligned}$$

Hieraus folgt (a).

(c): Dies folgt wieder leicht für zyklische Gruppen A : Ist A von der Ordnung n und a ein Erzeugendes, so gibt es für jedes $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ genau ein $\chi_{\bar{m}}$ mit $\chi_{\bar{m}}(a) = \bar{m}$. Der Homomorphismus

$$\varphi_A : A \rightarrow A^{\vee\vee}$$

ist dann injektiv, denn es ist $\chi_{\bar{1}}(ka) = \bar{k} \neq 0$ für $ka \neq 0$. Da $A^{\vee\vee}$ dieselbe Ordnung wie A hat, muss φ_A bijektiv sein. Der Fall eines beliebigen A folgt dann wieder mit (6.10.1).

(d) Die Exaktheit von

$$0 \rightarrow C^{\vee} \xrightarrow{\beta^{\vee}} B^{\vee} \xrightarrow{\alpha^{\vee}} A^{\vee}$$

folgt leicht. (Später werden wir dies im allgemeinen Rahmen von R -Moduln beweisen). Dann muss α^{\vee} surjektiv sein, denn es ist $|A^{\vee}| = |A| = |B| \cdot |C|^{-1} = |B^{\vee}| \cdot |C^{\vee}|^{-1} = |B^{\vee}/C^{\vee}|$, die Injektion $B^{\vee}/C^{\vee} \hookrightarrow A^{\vee}$ (Homomorphiesatz!) ist also ein Isomorphismus.

(e): Für Untergruppen $U, V \subseteq A$ ist die Beziehung

$$U \subseteq V \Rightarrow V^{\perp} \subseteq U^{\perp}$$

klar. Definieren wir nun auch für Untergruppen $X \subseteq A^{\vee}$ ein ‘orthogonales Komplement’

$$X^{\perp} = \{a \in A \mid \chi(a) = 0 \quad \forall \chi \in X\},$$

so zeigen wir, dass

$$X \mapsto X^{\perp}$$

eine Umkehrabbildung zu $U \mapsto U^{\perp}$ ist: Die exakte Sequenz

$$0 \rightarrow U \xrightarrow{i} A \rightarrow A/U \rightarrow 0$$

liefert nach (d) eine exakte Sequenz

$$0 \rightarrow (A/U)^{\vee} \rightarrow A^{\vee} \xrightarrow{i^{\vee}} U^{\vee} \rightarrow 0.$$

Aber offenbar ist gerade $U^{\perp} = \ker i^{\vee}$, dies liefert eine exakte Sequenz

$$0 \rightarrow U^{\perp} \xrightarrow{j} A^{\vee} \xrightarrow{i^{\vee}} U^{\vee} \rightarrow 0,$$

wobei j die Inklusion ist. Nochmaliges Dualisieren liefert ein kommutatives Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & U^{\vee\vee} & \xrightarrow{i^{\vee\vee}} & A^{\vee\vee} & \xrightarrow{j^{\vee}} & (U^{\perp})^{\vee} \longrightarrow 0 \\ & & \uparrow \wr & & \uparrow \wr & & \\ & & U & \longrightarrow & A & & \end{array}$$

mit exakter oberer Zeile. Offenbar ist gerade $U^{\perp\perp} = \ker(j^{\vee} \circ \varphi_A)$, und es folgt $U^{\perp\perp} = U$. Genauso folgt $X^{\perp\perp} = X$ für $X \leq A^{\vee}$.

§7 Moduln über Hauptidealringen und der Elementarteilersatz

Sei R ein Ring.

Definition 7.1 Sei M ein R -Modul. Die Länge von M (Bez. $\ell_R(M)$) ist das Supremum aller Längen ℓ von Ketten von Untermoduln

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_\ell = M.$$

(Es ist also $\ell_R(M) \in \mathbb{N}_0 \cup \{\infty\}$).

Lemma 7.2 (Additivität in exakten Sequenzen) (a) Ist

$$0 \rightarrow M' \xrightarrow{i} M \xrightarrow{\varphi} M'' \rightarrow 0$$

eine exakte Sequenz von R -Moduln, so gilt

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

Insbesondere hat M genau dann endliche Länge, wenn dies für M' und M'' gilt.

(b) Für R -Moduln M_1, M_2 gilt $\ell_R(M_1 \oplus M_2) = \ell_R(M_1) + \ell_R(M_2)$.

Beweis (a): (Wir fassen i als Inklusion auf) Hat man Ketten von Untermoduln

$$\begin{array}{ccc} 0 \subsetneq M'_1 \subsetneq \dots & \subsetneq & M'_r = M' \\ 0 \subsetneq M''_1 \subsetneq \dots & \subsetneq & M''_s = M'', \end{array}$$

so ist mit $M_i = \varphi^{-1}(M''_i)$

$$0 \subsetneq M'_1 \subsetneq \dots \subsetneq M'_r \subsetneq M_1 \subsetneq \dots \subsetneq M_s = M$$

eine Kette der Länge $r + s$. Dies zeigt

$$(7.2.1) \quad \ell_R(M) \geq \ell_R(M') + \ell_R(M'').$$

Sei umgekehrt

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_\ell = M$$

eine Kette von Untermoduln in M . Wir erhalten kommutative Diagramme mit exakten Zeilen

$$\begin{array}{ccccccc} 0 & \rightarrow & M_{i+1} \cap M' & \rightarrow & M_{i+1} & \rightarrow & \varphi(M_{i+1}) \rightarrow 0 \\ & & \cup & & \cup & & \cup \\ 0 & \rightarrow & M_1 \cap M' & \rightarrow & M_i & \rightarrow & \varphi(M_i) \rightarrow 0. \end{array}$$

Ist $\varphi(M_i) = \varphi(M_{i+1})$, so muss $M_i \cap M' \subsetneq M_{i+1} \cap M'$ sein, wie man zum Beispiel mit dem Schlangenlemma (4.16) sieht. Es gilt also $\varphi(M_i) \subsetneq \varphi(M_{i+1})$ oder $M_i \cap M' \subsetneq M_{i+1} \cap M'$, für jedes $0 \leq i \leq \ell - 1$. Hieraus folgt

$$(7.2.2) \quad \ell \leq \ell_R(M') + \ell_R(M'')$$

und damit die Gleichheit in (7.2.1). Der Zusatz folgt ebenfalls aus den obigen Überlegungen.

(b) folgt aus (a) und der exakten Sequenz

$$\begin{array}{ccccccc} 0 & \rightarrow & M_1 & \rightarrow & M_1 \oplus M_2 & \rightarrow & M_2 \rightarrow 0 \\ & & x & \mapsto & (x, 0), (x, y) & \mapsto & y \end{array}$$

Beispiel 7.3 Die Länge der abelschen Gruppen (= \mathbb{Z} -Moduln)

$$\begin{aligned} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/25\mathbb{Z} \end{aligned}$$

ist jeweils gleich 2, denn die Länge von $\mathbb{Z}/5\mathbb{Z}$ ist gleich 1, da diese Gruppe keine echte Untergruppe hat.

Sei nun R ein kommutativer Ring mit Eins.

Lemma/Definition 7.4 Sei M ein R -Modul.

(a) Sei $(M_i)_{i \in I}$ eine Familie von Untermoduln $M_i \subseteq M$. Dann ist

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in I} m_i \mid m_i \in M_i, \quad m_i = 0 \text{ für fast alle } i \in I \right\}$$

der kleinste Untermodul von M der alle M_i enthält und heißt die **Summe** der Untermoduln M_i .

(b) Sei $(x_i)_{i \in I}$ eine Familie von Elementen $x_i \in M$. Dann ist

$$\langle x_i \mid i \in I \rangle_R := \sum_{i \in I} Rx_i,$$

der kleinste Untermodul der alle x_i enthält und heißt **der von den x_i erzeugte Untermodul**. Hierbei sei $Rx := \{ax \mid a \in R\}$ für $x \in M$.

(c) Die Familie $(x_i)_{i \in I}$ heißt ein Erzeugendensystem von M , wenn $\langle x_i \mid i \in I \rangle_R = M$, also wenn es für jedes $x \in M$ Elemente $a_i \in R$ gibt, für alle $i \in I$, $a_i = 0$ für fast alle i , mit $x = \sum_{i \in I} a_i x_i$.

(d) M heißt **endlich erzeugt**, wenn M von endlich vielen Elementen erzeugt wird.

(e) M heißt **zyklischer** R -Modul, wenn M von einem Element erzeugt wird (d.h., $M = Rx$ für ein $x \in M$).

Beweis der Behauptungen: klar!

Beispiel 7.5 $\mathbb{Z}/25\mathbb{Z}$ ist zyklisch, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ nicht (warum?).

Definition 7.6 Sei M ein R -Modul.

(a) Eine Familie $(x_i)_{i \in I}$ von Elementen $x_i \in M$ heißt **linear unabhängig** (oder **frei**), wenn gilt: Ist

$$\sum_{i \in I} a_i x_i = 0$$

mit $a_i \in R$ ($i \in I$), $a_i = 0$ für fast alle $i \in I$, so gilt $a_i = 0$ für alle $i \in I$.

(b) Der Rang von M (Bezeichnung $rg(M)$) ist die maximale Anzahl linear unabhängiger Elemente in M (d.h., die maximale Kardinalität einer freien Familie in M).

Beispiele 7.7 (a) \mathbb{Z} und \mathbb{Q} haben beide den \mathbb{Z} -Rang 1 (vergleiche Übungsaufgabe 17).

(b) $\mathbb{Z}/25\mathbb{Z}$ hat Rang 0 als \mathbb{Z} -Modul und Rang 1 als $\mathbb{Z}/25\mathbb{Z}$ -Modul.

Definition 7.8 Sei R ein Integritätsring und M ein R -Modul.

- (a) Ein Element $x \in M$ heißt **Torsionselement**, wenn es ein $a \in R \setminus \{0\}$ gibt mit $ax = 0$.
- (b) M heißt ein Torsionsmodul, wenn jedes Element Torsionselement ist.
- (c) M heißt torsionsfrei, wenn $0 \in M$ das einzige Torsionselement ist.

Bespiel 7.9 (a) Offenbar ist für eine abelsche Gruppe (= \mathbb{Z} -Modul) A ein Element $a \in A$ genau dann ein Torsionselement, wenn es endliche Ordnung hat.

(b) \mathbb{Q}/\mathbb{Z} ist eine Torsionsgruppe (=Torsions- \mathbb{Z} -Modul), da jedes Element endliche Ordnung hat, aber \mathbb{Q}/\mathbb{Z} hat keinen endlichen Exponenten.

Bemerkung 7.10 Ein Modul über einem Integritätsring R ist genau dann ein Torsionsmodul, wenn er Rang null hat.

Sei nun R ein Hauptidealring (integer, jedes Ideal ist ein Hauptideal, d.h., von einem Element erzeugt). Nach Algebra I, Satz 6.18 ist R dann auch faktoriell, d.h., jedes Element $a \in R$ besitzt eine Primfaktorzerlegung

$$a = \varepsilon p_1 \dots p_r$$

mit einer Einheit ε und Primelementen p_1, \dots, p_r , wobei die p_i eindeutig bis auf Assoziiertheit sind.

Zur Erinnerung: Zwei Elemente α, β heißen assoziiert (Bez.: $\alpha \sim \beta$), wenn $\alpha = \varepsilon\beta$ mit einer Einheit ε . Weiter gilt für $\alpha, \beta \in R$: $\alpha \mid \beta \Leftrightarrow (\beta) \subseteq (\alpha)$, wobei $(\alpha) = \alpha R$ das von α erzeugte Hauptideal ist.

Lemma 7.11 Besitzt $a \in R$ die Primfaktorzerlegung $a = \varepsilon \cdot p_1 \dots p_r$ (ε Einheit, p_i prim), so ist

$$\ell_R(R/aR) = r.$$

Beweis Sei $a = \eta \cdot q_1^{n_1} \dots q_s^{n_s}$ mit einer Einheit η und paarweise nicht assoziierten Primelementen q_i , so dass $r = n_1 + \dots + n_s$. Nach dem Chinesischen Restsatz (Algebra I, Satz 3.24) gilt

$$R/aR \cong \bigoplus_{i=1}^s R/q_i^{n_i} R,$$

nach 7.2 (b) also $\ell_R(R/aR) = \sum_{i=1}^s \ell_R(R/q_i^{n_i} R)$.

Es genügt also, den Fall $a = p^n$ für ein Primelement p zu betrachten. Die Untermoduln von R/aR entsprechen bijektiv den Idealen $\mathfrak{a} \subseteq R$ mit $aR \subseteq \mathfrak{a}$, also, da R Hauptidealring ist, bijektiv den Teilern $1 = p^0, p^1, p^2, \dots, p^n$ von p^n . Daher ist $\ell_R(R/p^n R) = n$ wie behauptet.

Beispiel 7.12 Dies impliziert nochmals, dass $\mathbb{Z}/25\mathbb{Z}$ die Länge 2 hat.

Wir kommen nun zum Hauptresultat dieses Paragraphen.

Satz 7.13 (Elementarteilersatz) Sei F ein endlich erzeugter freier Modul über einem Hauptidealring R und $M \subseteq F$ ein Untermodul von Rang n . Dann gibt es eine Basis

$$x_1, \dots, x_n, x_{n+1}, \dots, x_m \quad (n \leq m)$$

von F und Elemente $\alpha_1, \dots, \alpha_n \in R \setminus \{0\}$ so dass gilt:

(i) $\alpha_1 x_1, \dots, \alpha_n x_n$ bilden eine Basis von M (insbesondere ist M selbst ein endlich erzeugter freier R -Modul).

(ii) $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i \leq n$.

Dabei sind die Elemente $\alpha_1, \dots, \alpha_n$ bis auf Assoziiertheit eindeutig durch M bestimmt und unabhängig von der Wahl der x_i . Man nennt $\alpha_1, \dots, \alpha_n$ die Elementarteiler von M .

Der Beweis erfolgt in mehreren Schritten.

Zunächst benötigen wir den folgenden Begriff:

Lemma/Definition 7.14 Sei y_1, \dots, y_m eine Basis von F . Für $x \in F$ setze

$$\text{cont}(x) = \text{ggT}(c_1, \dots, c_m),$$

falls $x = c_1 y_1 + \dots + c_m y_m$ mit $c_1, \dots, c_m \in R$. Die Klasse dieses Elements bis auf Assoziierte ist wohldefiniert und unabhängig von der Basis (y_1, \dots, y_m) , und heißt der **Inhalt** von x .

Beweis: Zunächst ist der ggT nur wohldefiniert bis auf Assoziierte, und bei fester Basis sind die c_i eindeutig durch x bestimmt. Um die Unabhängigkeit von der Basis zu zeigen, betrachten wir den R -Modul

$$F^* := \text{Hom}_R(F, R)$$

aller Linearformen auf F , d.h., aller R -linearen Abbildungen $\varphi : F \rightarrow R$. Die Menge

$$I(x) := \{\varphi(x) \mid \varphi \in F^*\}$$

bildet offenbar ein Ideal in R , und wir behaupten $I(x) = (\text{cont}(x))$, woraus die Unabhängigkeit von $\text{cont}(x)$ bis auf Assoziierte folgt, denn $I(x)$ ist unabhängig von der Basis.

Sei (y_1^*, \dots, y_m^*) die duale Basis von F^* , eindeutig bestimmt durch

$$y_i^*(y_j) = \delta_{ij}.$$

(Dass dies geht und eine Basis liefert, folgt sofort aus der universellen Eigenschaft des freien Moduls).

Aus der Theorie des ggT $[(\text{ggT}(c_1, \dots, c_m)) = (c_1, \dots, c_m)]$ folgt, dass

$$\text{ggT}(c_1, \dots, c_m) = \sum_{i=1}^m a_i c_i$$

für gewisse $a_1, \dots, a_m \in R$. Für die Linearform $\varphi = \sum_{i=1}^m a_i y_i^*$ folgt dann

$$\varphi(x) = \sum_{i=1}^m a_i c_i = \text{ggT}(c_1, \dots, c_m) = \text{cont}(x),$$

andererseits ist für jede beliebige Linearform $\psi = \sum_{i=1}^m b_i y_i^*$

$$\psi(x) = \sum_{i=1}^m a_i c_i \in (c_1, \dots, c_m) = (\text{cont}(x)),$$

und es folgt $I(x) = (\text{cont}(x))$ und damit die Behauptung.

Lemma 7.15 Sei $x \in F$.

(i) Es existiert ein $\varphi \in F^*$ mit $\varphi(x) = \text{cont}(x)$.

(ii) Für $\psi \in F^*$ gilt $\text{cont}(x) \mid \psi(x)$.

Dies wurde im obigen Beweis gezeigt.

Lemma 7.16 Sei $M \subseteq F$ ein Untermodul. Dann existiert ein $x \in M$ mit $\text{cont}(x) \mid \text{cont}(y)$ für alle $y \in M$.

Beweis: Betrachte die Menge J aller Ideale $(\text{cont}(y))$ mit $y \in M$. Diese Menge enthält ein maximales Element $(\text{cont}(x))$, denn sonst gäbe es eine unendliche echt aufsteigende Folge

$$(\text{cont}(y_1)) \subsetneq (\text{cont}(y_2)) \subsetneq \dots$$

von Idealen – dies wäre ein Widerspruch dazu, dass R (als Hauptidealring!) noethersch ist (vergleiche Algebra I, Proposition 5.7).

Sei $\varphi \in F^*$ mit $\varphi(x) = \text{cont}(x)$ (Lemma 7.15(i)). Wir behaupten

$$(7.16.1) \quad \varphi(x) \mid \varphi(y) \quad \text{für alle } y \in M.$$

Denn sei $y \in M$ und $d = \text{ggT}(\varphi(x), \varphi(y))$. Dann gibt es $a, b \in R$ mit $a\varphi(x) + b\varphi(y) = d$, also $\varphi(ax + by) = d$. Nach 7.15(ii) gilt andererseits

$$\text{cont}(ax + by) \mid \varphi(ax + by) = d$$

und wegen $d \mid \varphi(x) = \text{cont}(x)$ auch

$$\text{cont}(ax + by) \mid \text{cont}(x).$$

Aus der Maximalität von $(\text{cont}(x))$ folgt nun

$$\text{cont}(x) \sim \text{cont}(ax + by) \mid d \mid \varphi(y),$$

also (7.16.1).

Wir zeigen nun $\text{cont}(x) \mid \text{cont}(y)$. Wegen 7.15 (i) genügt es zu zeigen, dass für alle $\psi \in F^*$ gilt

$$(7.16.2) \quad \varphi(x) \mid \psi(y).$$

Nach 7.15 (ii) gilt $\varphi(x) \mid \psi(x)$, und nach (7.16.1) gilt $\varphi(x) \mid \varphi(y)$. Um (7.16.2) zu zeigen, können wir also y durch $y - \frac{\varphi(y)}{\varphi(x)}x$ ersetzen und damit annehmen, dass $\varphi(y) = 0$. Weiter können wir ψ durch $\psi - \frac{\psi(x)}{\varphi(x)}\varphi$ ersetzen und damit $\psi(x) = 0$ annehmen.

Sei dann $e = ggT(\varphi(x), \psi(y))$, und damit $e = a\varphi(x) + b\psi(y)$ mit $a, b \in R$. Es folgt

$$(\varphi + \psi)(ax + by) = a\varphi(x) + b\psi(y) = e,$$

wegen 7.15 (ii) also $cont(ax + by) \mid e \mid cont(x)$. Wegen der Maximalität von $(cont(x))$ folgt

$$cont(ax + by) \sim cont(x) = \varphi(x).$$

Hieraus folgt

$$\varphi(x) \sim e \mid \psi(y),$$

also (7.16.2).

Lemma 7.17 Sei A ein Integritätsring und F ein freier A -Modul mit Basis y_1, \dots, y_m . Dann ist $rg(F) = m$.

Beweis (vergleiche Übungsaufgabe 26) Offenbar ist $m \leq rg(F)$, da y_1, \dots, y_m linear unabhängig sind. Sei K der Quotientenkörper von A . Dann haben wir eine Injektion

$$\begin{aligned} \varphi : F = \bigoplus_{i=1}^m Ay_i &\hookrightarrow K^m \\ \sum_{i=1}^m a_i y_i &\mapsto (a_1, \dots, a_m). \end{aligned}$$

Sind $x_1, \dots, x_r \in F$ linear unabhängig über A , so sind $\varphi(x_1), \dots, \varphi(x_r)$ linear unabhängig über K (warum?). Also gilt $r \leq m$, d.h., $rg(F) \leq m$.

Lemma 7.18 Sei R ein Hauptidealring und F ein endlich erzeugter freier R -Modul. Jeder Untermodul $M \subseteq F$ ist dann wieder endlich erzeugt und frei.

Beweis: Induktion über $n = rg M \leq rg F < \infty$. Für $rg M = 0$ ist $M = 0$. Sei also $n > 0$. Nach Lemma 7.16 gibt es ein $x \in M$ mit $cont(x) \mid cont(y)$ für alle $y \in M$, und nach 7.15 (i) gibt es ein $\varphi \in F^*$ mit $\varphi(x) = cont(x)$. Andererseits gibt es nach Definition von $cont(x)$ ein (eindeutig bestimmtes) $x_1 \in F$ mit

$$x = cont(x) \cdot x_1$$

($x = \sum c_i y_i$ für eine Basis (y_1, \dots, y_m) von F , $cont(x) = ggT(c_1, \dots, c_m) =: c$, so $x_1 = \sum \frac{c_i}{c} y_i$). Setze nun

$$F' = \ker(\varphi) \quad , \quad M' = M \cap F'.$$

Dann gilt

$$(7.17.1) \quad F = Ax_1 \oplus F' \quad , \quad M = Ax \oplus M'.$$

Sei nämlich $y \in M$ Dann schreibe

$$y = \frac{\varphi(y)}{\varphi(x)} x + \left(y - \frac{\varphi(y)}{\varphi(x)} x \right)$$

(Dies ist wohldefiniert, da $\varphi(x) = cont(x) \mid \varphi(y)$ nach 7.15 (ii)). Rechts liegt der erste Summand in Rx , und der zweite in $M \cap \ker(\varphi) = M'$. Da y beliebig in M war, folgt

$M = Rx + M'$. Weiter ist die Summe direkt: Wegen $\varphi(ax) = a\varphi(x) = a \operatorname{cont}(x)$ und $\operatorname{cont}(x) \neq 0$ (da $M \neq 0$) liegt ax genau dann in $\ker(\varphi)$, wenn $a = 0$ ($M \subseteq F$ ist torsionsfrei). Analog zeigt man $F = Ax_1 \oplus F'$: ersetze x durch x_1 und benutze $\varphi(x_1) = 1$.

Aus der Zerlegung $M = Ax \oplus M'$ folgt $\operatorname{rg} M' < \operatorname{rg} M = n$. Mit Induktion über n folgt, dass M' endlich erzeugt wird und frei ist, also auch M .

Beweis der Existenzaussage von Satz 7.13: Durch Induktion über $n = \operatorname{rg} M$. Wie im Beweis von 7.18 ist für $n = 0$ nichts zu zeigen, und für $n > 0$ erhalten wir Zerlegungen

$$F = Ax_1 \oplus F' \quad , \quad M = Ax \oplus M'$$

mit $x = \operatorname{cont}(x)x_1$ und $\operatorname{cont}(x) = \varphi(x)$ gewählt wie oben, und wobei $M' \subseteq F'$.

Nach 7.18 ist $F' \subseteq F$ frei, und wegen $\operatorname{rg}(M') < n$ existiert nach Induktion eine Basis $x_2, \dots, x_n, x_{n+1}, \dots, x_m$ von F' und es existieren $\alpha_2, \dots, \alpha_n \in R \setminus \{0\}$ mit $\alpha_2 \mid \alpha_3 \mid \dots \mid \alpha_n$, so dass $\alpha_2 x_2, \dots, \alpha_n x_n$ eine Basis von M' bilden. Dann ist x_1, \dots, x_m eine Basis von F und mit $\alpha_1 = \operatorname{cont}(x)$ ist $x = \alpha_1 x_1, \alpha_2 x_2, \dots, \alpha_n x_n$ eine Basis von M . Weiter gilt noch $\alpha_1 \mid \alpha_2$: Sei nämlich $\psi \in F^*$ eine Linearform mit $\psi(x_2) = 1$ (zum Beispiel $\psi = x_2^*$ für die Dualbasis x_1^*, \dots, x_m^* von F^*). Nach Lemma 7.15 (ii) gilt dann wegen $\alpha_2 x_2 \in M$

$$\alpha_1 = \operatorname{cont}(x) \mid \psi(\alpha_2 x_2) = \alpha_2 .$$

Dies zeigt die Eigenschaften (i) und (ii) in Satz 7.13.

Zur Eindeutigkeitsaussage benutzen wir die beiden folgenden Resultate.

Lemma 7.19 Sei A ein beliebiger Ring, seien M_1, \dots, M_m A -Moduln und $N_i \subseteq M_i$ Untermoduln, für $i = 1, \dots, m$. Dann gibt es einen kanonischen R -Modul-Isomorphismus

$$(M_1 \oplus \dots \oplus M_m) / (N_1 \oplus \dots \oplus N_m) \xrightarrow{\sim} M_1 / N_1 \oplus \dots \oplus M_m / N_m .$$

Beweis: Der R -Modul-Homomorphismus

$$\begin{aligned} M_1 \oplus \dots \oplus M_m &\twoheadrightarrow M_1 / N_1 \oplus \dots \oplus M_m / N_m \\ (x_1, \dots, x_m) &\mapsto (x_1 \bmod N_1, \dots, x_m \bmod N_m) \end{aligned}$$

ist surjektiv und hat den Kern $N_1 \oplus \dots \oplus N_m$. Die Aussage folgt also mit dem Homomorphiesatz 4.11 (a).

Satz 7.20 Sei R ein Hauptidealring und M ein R -Modul. Gibt es einen Isomorphismus

$$M \xrightarrow{\sim} \bigoplus_{i=1}^n R / \alpha_i R$$

mit Nicht-Einheiten $\alpha_1, \dots, \alpha_n \in R \setminus \{0\}$, wobei $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i \leq n$, so sind n , sowie $\alpha_1, \dots, \alpha_n$ bis auf Assoziiertheit eindeutig durch M bestimmt.

Hieraus folgt

Beweis der Eindeutigkeitsaussage in Satz 7.13: Seien eine Basis x_1, \dots, x_m von F und $\alpha_1, \dots, \alpha_n \in R \setminus \{0\}$ wie in Satz 7.13 gegeben. Aus 7.19 folgt ein R -Modul-Isomorphismus

$$(7.19.1) \quad F/M = \bigoplus_{i=1}^m Rx_i / \left(\bigoplus_{i=1}^n R\alpha_i x_i \oplus \bigoplus_{i=n+1}^m 0 \right) \xrightarrow{\sim} \bigoplus_{i=1}^n R/\alpha_i R \oplus \bigoplus_{i=n+1}^m R,$$

mittels der Isomorphismen $R \xrightarrow{\sim} Rx_i$ ($a \mapsto ax_i$), die Isomorphismen $R\alpha_i \xrightarrow{\sim} R\alpha_i x_i$ und $R/\alpha_i R \xrightarrow{\sim} Rx_i/R\alpha_i x_i$ induzieren. Bezeichnen wir mit $N^{tor} \subset N$ den Torsionsmodul eines R -Moduls N , also die Menge aller Torsionselemente in N (vergleiche Übungsaufgabe 24), so induziert dies offenbar einen Isomorphismus

$$(7.19.2) \quad (F/M)^{tor} \xrightarrow{\sim} \bigoplus_{i=1}^n R/\alpha_i R.$$

Nach (7.19.2) und 7.20 sind die Nicht-Einheiten unter den α_i in (7.19.1), also auch in 7.13, eindeutig bestimmt, auch deren Anzahl r . Die restlichen $n - r$ Elemente α_i in (7.19.1) sind Einheiten, also alle assoziiert zu 1.

Beweis von Satz 7.20: (Beachte: $\alpha \sim \beta \Leftrightarrow \alpha R = \beta R$) Sei

$$M \cong \bigoplus_{i=1}^n R/\alpha_i R \cong \bigoplus_{j=1}^m R/\beta_j R$$

mit $\alpha_{i+1} \mid \alpha_i$, $1 \leq i \leq n$, und $\beta_{j+1} \mid \beta_j$, $1 \leq j \leq m$ (wir vertauschen aus Notationstechnischen Gründen die Reihenfolge). Angenommen, es gibt ein $k \leq \min\{m, n\}$ mit $\alpha_k R \neq \beta_k R$; sei k minimal mit dieser Eigenschaft. Wegen $\alpha_i \sim \beta_i$ für $1 \leq i \leq k$ und $\alpha_{k+1}, \dots, \alpha_n \mid \alpha_k$ gilt

$$\alpha_k M \cong \bigoplus_{i=1}^{k-1} \alpha_k (R/\alpha_i R) \cong \bigoplus_{i=1}^{k-1} \alpha_k (R/\alpha_i R) \oplus \bigoplus_{j=k}^m \alpha_k (R/\beta_j R).$$

Mit Lemma 7.2 folgt

$$\ell_R(\alpha_k (R/\beta_k R)) = 0,$$

also $\alpha_k (R/\beta_k R) = 0$, d.h., $\alpha_k R \subseteq \beta_k R$. Entsprechend zeigt man $\beta_k R \subseteq \alpha_k R$, also $\alpha_k R = \beta_k R$ – Widerspruch!

Es gilt also $\alpha_i \sim \beta_i$ für alle $1 \leq i \leq \min\{m, n\}$.

Gilt nun etwa $m \leq n$, so folgt wiederum mit Lemma 7.2, dass $\bigoplus_{i=m+1}^n R/\alpha_i R$ die Länge 0 hat, also gleich 0 ist, woraus $m = n$ folgt, da die $R/\alpha_i R \neq 0$.

Beispiel 7.21 Für die \mathbb{Z} -Moduln $M = 2\mathbb{Z} \times 3\mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z} = F$ sind 2 und 3 nicht die Elementarteiler, da $2 \nmid 3$ und $3 \nmid 2$ (vergleiche Übungsaufgabe 25).

§8 Anwendungen des Elementarteilersatzes

Sei R ein Hauptidealring.

Proposition 8.1 Sei M ein endlich erzeugter R -Modul.

(a) Sei

$$M^{tor} = \{m \in M \mid m \text{ Torsionselement}\}$$

der zugehörige Torsionsuntermodul (vergleiche Übungsaufgabe 24). Dann ist M^{tor} endlich erzeugt und es ist

$$M = M^{tor} \oplus F$$

mit einem freien endlich erzeugten R -Modul F .

(b) Insbesondere ist M genau dann frei, wenn M torsionsfrei ist.

Beweis: (a): Seien $m_1, \dots, m_m \in M$ Erzeugende von M und sei $F_0 = R^m$. Dann ist F_0 frei vom Rang m , und wir haben einen R -Modul-Epimorphismus

$$\begin{aligned} \varphi : F_0 &\twoheadrightarrow M \\ (a_1, \dots, a_m) &\mapsto \sum_{i=1}^m a_i m_i . \end{aligned}$$

Sei $N = \ker(\varphi) \subseteq F_0$. Nach dem Elementarteilersatz (und Lemma 7.17) gibt es eine Basis x_1, \dots, x_m von F_0 und $\alpha_1, \dots, \alpha_n \in R \setminus \{0\}$, $n = \text{rg}(M) \leq m$, mit

$$N = \bigoplus_{i=1}^n R\alpha_i x_i .$$

Nach dem Homomorphiesatz und (7.19.1) gibt es R -Modulisomorphismen

$$(8.1.1) \quad \begin{aligned} M \cong F_0/N &\cong \bigoplus_{i=1}^n R/\alpha_i R \oplus \bigoplus_{i=n+1}^m R . \\ \sum_{i=1}^m \beta_i m_i \leftarrow \overline{(\beta_1, \dots, \beta_m)} & \\ \sum_{i=1}^m \gamma_i x_i \leftarrow (\gamma_1, \dots, \overline{\gamma_n}, \gamma_{n-1}, \dots, \gamma_m) . & \end{aligned}$$

Hierbei sei für $f \in F$ mit \overline{f} die Klasse von f in F/N bezeichnet und für $\beta \in R$ mit $\overline{\beta}$ die Klasse von β in $R/\alpha_i R$ ($i = 1, \dots, n$).

Auf der rechten Seite von (8.1.1) ist $\bigoplus_{i=1}^n R/\alpha_i R$ der Torsionsmodul und offenbar endlich erzeugt; weiter ist $\bigoplus_{i=n+1}^m R$ endlich erzeugt und frei. Dies impliziert (a). Genauer ist $\bigoplus_{i=1}^n R\varphi(x_i)$ der Torsionsmodul von M , $F = \bigoplus_{i=n+1}^m R\varphi(x_i)$ frei und M die direkte Summe dieser beiden Moduln.

(b) ist eine Konsequenz von (a): Ist M torsionsfrei, so ist $M_{tor} = 0$ und daher $M = F$ frei. Die Umkehrung ist offensichtlich und gilt für jeden Integritätsring.

Satz 8.2 Sei M ein endlich erzeugter R -Modul. Dann ist M Summe von zyklischen R -Moduln. Genauer gilt:

(a) Es gibt Nicht-Einheiten $\alpha_1, \dots, \alpha_m \in R$ mit $\alpha_i \mid \alpha_{i+1}$ für $i = 1, \dots, m - 1$ und einen Isomorphismus

$$(8.2.1) \quad M \cong \bigoplus_{i=1}^m R/\alpha_i R .$$

Dabei sind $\alpha_1, \dots, \alpha_m$ bis auf Assoziierte eindeutig; wir nennen diese Elemente auch die Elementarteiler von M .

(b) Für jedes Primelement $p \in R$ sei

$$M\{p\} := \{x \in M \mid p^n x = 0 \text{ für ein } n \in \mathbb{N}\}$$

der p -primäre Anteil von M , d.h., der Untermodul der Elemente, die durch eine p -Potenz annulliert werden. Sei P ein Repräsentantensystem für die Klassen modulo Assoziiertheit von Primelementen. Dann ist $M\{p\} = 0$ für fast alle p und es gilt

$$(8.2.2) \quad M^{\text{tor}} = \bigoplus_{p \in P} M\{p\}$$

(c) Für jedes $p \in P$ gibt es eindeutig bestimmte Zahlen $r_p \in \mathbb{N}_0$ und $n_1(p), n_2(p), \dots, n_{r_p}(p) \in \mathbb{N}$ mit

$$(8.2.3) \quad M\{p\} \cong \bigoplus_{i=1}^{r_p} R/p^{n_i(p)} R .$$

Beweis: (a) Der Isomorphismus folgt aus (8.1.1). Unter dem Isomorphismus (8.2.1) ist weiter M^{tor} isomorph zur Summe der $R/\alpha_i R$, für die α_i Nicht-Einheit und $\alpha_i \neq 0$ ist. Nach Satz 7.20 sind diese α_i eindeutig bestimmt. Die anderen α_i sind null, und ihre Anzahl ist nach 7.17 der Rang des freien R -Moduls M/M^{tor} .

(b) Offenbar ist $M\{p\}$ ein Untermodul. Ist in (8.2.1) $\alpha_i \sim \prod_{p \in P} p^{n_i(p)}$ die Primzerlegung, mit $n_i(p) \in \mathbb{N}_0$, $n_i(p) = 0$ für fast alle p , so ist nach dem Chinesischen Restsatz

$$M \underset{8.2.1}{\cong} \bigoplus_{i=1}^m R/\alpha_i R \cong \bigoplus_{i=1}^m \bigoplus_{p \in P} R/p^{n_i(p)} R .$$

Dabei entspricht offenbar

$$\bigoplus_{i=1}^m R/p^{n_i(p)} R$$

dem Untermodul $M\{p\}$. Dies liefert (b) und die Isomorphie (8.2.3) in (c): Die $n_i(p)$, die nicht null sind, sind wieder nach 7.20 eindeutig; denn nummerieren wir für festes p neu, so dass $1 \leq n_1(p) \leq n_2(p) \leq \dots \leq n_{r_p}(p)$ und $n_i(p) = 0$ für $r_p < i \leq m$, so gilt

$$p^{n_1(p)} \mid p^{n_2(p)} \mid \dots \mid p^{n_{r_p}(p)}$$

und $R/p^{n_i(p)} R = 0$ für $i > r_p$. Damit ist (c) gezeigt.

Bemerkungen 8.3: (a) Für $R = \mathbb{Z}$ folgt aus 8.2 (a) der Hauptsatz über endliche abelsche Gruppen Satz 6.8, und 8.2 (b) gibt einen neuen Beweis von Algebra I, Satz 14.1, wenn wir für P die Menge aller Primzahlen in \mathbb{N} nehmen.

(b) (Elementarteiler einer Matrix) Sei R ein Hauptidealring und

$$A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in M(m \times n, R)$$

eine $(m \times n)$ -Matrix mit Einträgen $a_{ij} \in R$. Dann liefert A eine R -lineare Abbildung

$$\begin{aligned} A : R^n &\rightarrow R^m \\ x &\mapsto Ax \end{aligned}$$

mit der üblichen Anwendung Ax von A auf einen Vektor x ($(Ax)_i = \sum_{j=1}^n a_{ij}x_j$, für $i = 1, \dots, m$). Umgekehrt ist jede R -lineare Abbildung $\varphi : R^n \rightarrow R^m$ von dieser Form, für eine eindeutig bestimmte Matrix $A \in M(m \times n, R)$ (Dies folgt aus der universellen Eigenschaft des freien Moduls R^m – oder durch direktes Nachrechnen; die i -te Spalte von A ist $\varphi(e_i)$ für die Standardbasis e_1, \dots, e_m von R^m).

Dann ist im A ein Untermodul des freien R -Moduls R^m , und wir können den Elementarteilersatz auf $M = \text{im } A \subseteq R^m = F$ anwenden. Die Elementarteiler von $\text{im } A \subseteq R^m$ heißen auch die **Elementarteiler von A**.

Ist umgekehrt $M \subseteq F \cong R^m$ Untermodul eines freien R -Moduls, so ist M endlich erzeugt, und es gibt einen R -Modul-Epimorphismus

$$R^n \rightarrow M$$

(vergl. Beweis von 8.1). Für die R -lineare Abbildung

$$\varphi : R^n \rightarrow M \hookrightarrow R^m = F$$

ist dann $\text{im } \varphi = M$. Ist φ durch die Matrix $A \in M(m \times n, R)$ gegeben, so sind also die Elementarteiler von M gleich den Elementarteilern der Matrix A . Weiter sind nach dem Beweis von 8.2 diese Elementarteiler gleich den Elementarteilern des R -Moduls $F/M = \text{coker } \varphi$ im Sinne von 8.2 (a), abgesehen von den eventuell zusätzlich auftretenden r Nullen, $r = \text{rg } F/M$.

In Verallgemeinerung von Satz 6.8 erhalten wir:

Satz 8.4 (Hauptsatz über endlich erzeugte abelsche Gruppen) Sei A eine endlich erzeugte abelsche Gruppe und P die Menge der Primzahlen. Dann gibt es eine Zerlegung in Untergruppen

$$(8.4.1) \quad A = F \oplus \bigoplus_{p \in P} \bigoplus_{i=1}^{r_p} Z_{p,i}$$

wobei F endlich erzeugt und frei ist, also $F \cong \mathbb{Z}^d$ mit $d \in \mathbb{N}_0$, und $Z_{p,i_p} \neq 0$ zyklisch von p -Potenz-Ordnung, etwa

$$Z_{p,i} \cong \mathbb{Z}/p^{n_i(p)}\mathbb{Z}$$

mit $n_i(p) \in \mathbb{N}$. Die Zahlen $d = \text{rg } A, r_p, n_i(p)$ sind dabei eindeutig bestimmt.

Beweis: Satz 8.2 für $R = \mathbb{Z}$.

Beispiel 8.5 (a) Bei der Zerlegung einer abelschen Gruppe in zyklische Faktoren ist deren minimale Anzahl nach 8.2 eindeutig bestimmt, als die Anzahl der Elementarteiler im Sinne von 8.2 (a). Diese Anzahl ist im Allgemeinen kleiner als die Anzahl der Faktoren in (8.4.1). Betrachte zum Beispiel

$$A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} .$$

Um die Elementarteiler zu bestimmen, fängt man ‘von oben’ an, d.h., durch Zusammennehmen der höchsten Primzahlpotenzen – das sind hier $4 = 2^2, 9 = 3^2$ und $5 = 5^1$, die das Produkt $4 \cdot 9 \cdot 5 = 180$ ergeben. Es geht weiter mit den nächsthöheren Potenzen, hier $4 = 2^2$ und $3 = 3^1$ mit Produkt 12. Dies Verfahren kann fortgeführt werden. Im Beispiel endet es mit 2 und die Elementarteiler sind also $2|12|180$, und es ist

$$A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

Produkt von drei (und nicht weniger) zyklischen Gruppen.

Eine zweite Anwendung des Elementarteilersatzes ist die Theorie der (verallgemeinerten) Jordan-Normalform. Sei K ein Körper, V ein endlich-dimensionaler K -Vektorraum und $\varphi : V \rightarrow V$ ein Endomorphismus (von K -Vektorräumen).

Beispiel 8.6 Zum Beispiel könnte $V = K^n$ und $\varphi = A$ eine $(n \times n)$ -Matrix über K sein.

Lemma 8.7 Sei $K[X]$ der Polynomring. Dann wird V zu einem $K[X]$ -Modul durch die Verknüpfung

$$(8.7.1) \quad \begin{aligned} K[X] \times V &\rightarrow V \\ \left(\sum_{i=1}^m a_i x^i, v\right) &\mapsto \left(\sum_{i=1}^m a_i \varphi^i\right)v = \sum_{i=1}^m a_i \varphi^i v . \end{aligned}$$

Beweis: Alle Moduleigenschaften kann man leicht nachrechnen.

Bemerkungen 8.8 (a) Sei A eine abelsche Gruppe und R ein beliebiger Ring mit Eins. Eine R -Modul-Struktur auf A

$$\mu : R \times A \rightarrow A, (r, a) \mapsto ra ,$$

zu gegeben ist dasselbe, wie einen Ringhomomorphismus

$$\phi : R \rightarrow \text{End}(A) = \text{Hom}_{\mathbb{Z}}(A, A)$$

von Ringen mit Eins (d.h., mit $\phi(1) = \text{id}$) zu geben. Denn: Ist μ gegeben, so definiere ϕ durch

$$(8.8.1) \quad \phi(r)(a) := ra ,$$

und ist ϕ gegeben, so definiere μ durch dieselbe Formel. Die Formel

$$r(a_1 + a_2) = ra_1 + ra_2 \quad (r \in R, a_1, a_2 \in A)$$

bedeutet gerade, dass ϕ wohldefiniert ist, d.h., $\phi(r)$ Homomorphismus von abelschen Gruppen, die Formel

$$(r_1 + r_2)a = r_1a + r_2a \quad (r_1, r_2 \in R, a \in A)$$

bedeutet, dass ϕ Homomorphismus abelscher Gruppen ist, und die Formel

$$r(sa) = (rs)a \quad (r, s \in R, a \in A)$$

bedeutet gerade, dass ϕ mit der Multiplikation verträglich ist, d.h., dass $\phi(rs) = \phi(r) \circ \phi(s)$. Weiter ist $\phi(1) = \text{id}$ genau dann, wenn $1a = a$ für alle $a \in A$.

(b) In der obigen Situation entspricht die $K[X]$ -Modul-Struktur von V gerade dem Ring-Homomorphismus

$$(8.8.2) \quad \begin{aligned} \phi : K[x] &\rightarrow \text{End}(V) \\ \sum_{i=1}^m a_i x^i &\mapsto \sum_{i=1}^m a_i \varphi^i. \end{aligned}$$

(c) Dieser ist wiederum durch die universelle Eigenschaft des Polynomrings (Algebra I, Satz 16.6) gegeben, zusammen mit der K -Modul-Struktur (= K -Vektorraum-Struktur) von V , die dem Ring-Homomorphismus

$$\begin{aligned} \psi : K &\rightarrow \text{End}_{\mathbb{Z}}(V) \\ a &\mapsto (v \mapsto av) \end{aligned}$$

entspricht. Die erwähnte universelle Eigenschaft von $K[X]$ besagt, dass wir ψ eindeutig zu einem K -Algebren-Homomorphismus

$$\phi : K[X] \rightarrow \text{End}(V)$$

mit $\phi(x) = \varphi$ fortsetzen können – dies ist natürlich gerade das ϕ in (8.8.2).

Definition 8.9 Sei $q = x^n + c_{n-1}x + \dots + c_1x + c_0$ ein normiertes Polynom über K . Dann heißt die Matrix

$$A(q) = \begin{pmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & \cdot & & \cdot \\ & & \cdot & \cdot & \cdot \\ & & & \cdot & \cdot \\ & & & & \cdot \\ & & & & 0 & -c_{n-2} \\ & & & & 1 & -c_{n-1} \end{pmatrix}$$

die Begleitmatrix zu q .

Lemma 8.10 Für $\varphi : V \rightarrow V$ sind die folgenden Bedingungen äquivalent.

(a) V ist φ -zyklisch, d.h., ein zyklischer $K[X]$ -Modul bezüglich der durch φ definierten Modulstruktur (8.7.1).

(b) Es gibt ein $v \in V$, so dass $v, \varphi v, \varphi^2 v, \dots, \varphi^{n-1} v$ eine Basis von V bilden.

(c) Es gibt eine Basis $b = (b_1, \dots, b_n)$ von V so dass die darstellende Matrix von φ bezüglich b die Begleitmatrix zu einem normierten Polynom $q \in K[X]$ ist.

Gelten die äquivalenten Bedingungen (a) bis (c), so ist $q = \chi_\varphi = p_\varphi$, wobei $\chi_\varphi \in K[X]$ das charakteristische Polynom von φ und $p_\chi \in K[x]$ das Minimalpolynom von φ auf V ist.

Beweis (a) \Rightarrow (c): Nach Voraussetzung gibt es ein $v \in V$, so dass $V = K[x]v$. Der Homomorphismus (von $K[x]$ -Moduln)

$$\begin{aligned} \psi : K[x] &\rightarrow V \\ f &\mapsto f(\varphi)v \end{aligned}$$

ist also surjektiv. Der Kern $\ker \psi$ kann nicht null sein, da V endlich-dimensional ist, $K[x]$ aber nicht. Also ist $\ker \psi = (q)$ für ein normiertes Polynom $q \in K[x]$, $q \neq 0$, und der Homomorphiesatz liefert einen Isomorphismus

$$\bar{\psi} : K[x]/(q) \xrightarrow{\sim} V \quad (\text{mit } \bar{\psi}(\bar{f}) = \psi(f)) .$$

Ist $\deg q = n$, so bilden links die Restklassen $1, \bar{x}, \dots, \overline{x^{n-1}}$ eine Basis (vergleiche Algebra I, Satz 9.5 (b)): Betrachte $\overline{g(x)} \in K[x]/(p)$ für $g(x) \in K[x]$. Ist $g(x) \neq 0$, so gibt es nach Polynomdivision $Q, R \in K[x]$ mit

$$g = Q \cdot q + R, \quad \deg r < n .$$

Es folgt $\overline{g(x)} = \overline{R(x)} = \sum_{i=0}^{n-1} a_i \bar{x}^i$ mit $a_i \in K$; d.h. $1, \bar{x}, \dots, \overline{x^{n-1}}$ bilden ein Erzeugendensystem. Die Elemente sind aber auch linear unabhängig:

Wäre $0 = \sum_{i=0}^{n-1} b_i \bar{x}^i = \overline{\sum_{i=0}^{n-1} b_i x^i}$ mit $b_0, \dots, b_{n-1} \in K$, nicht alle null, so wäre $0 \neq h(x) = \sum_{i=0}^{n-1} b_i x^i \in \ker \psi$, würde also von q geteilt, im Widerspruch dazu, dass $\deg h < n = \deg q$.

Damit bilden $v = \bar{\psi}(1) = \psi(1), \varphi v = \bar{\psi}(\bar{x}) = \psi(x), \dots, \varphi^{n-1} v = \bar{\psi}(\overline{x^{n-1}}) = \psi(x^{n-1})$ eine Basis von V . Ist

$$q(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$$

mit $c_0, \dots, c_{n-1} \in K$, so gilt $\overline{q(x)} = 0$ und damit

$$0 = \bar{\psi}(\overline{q(x)}) = \psi(q(x)) = q(\varphi)v = \sum_{i=0}^n c_i \varphi^i v ,$$

d.h., $\varphi(\varphi^{n-1}v) = \varphi^n v = - \sum_{i=0}^{n-1} c_i \varphi^i v$. Hieraus folgt nun sofort, dass die Darstellungsmatrix von φ bezüglich $v, \varphi v, \dots, \varphi^{n-1}v$ die Begleitmatrix $A(q)$ ist.

(c) \Rightarrow (b): Sei umgekehrt $x_1, \dots, x_n \in V$ eine Basis, so dass die zugehörige Darstellungsmatrix von φ die Begleitmatrix $A(q)$ zu einem normierten Polynom q ist, also etwa

$$\begin{pmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & \cdot & & \cdot \\ & & \cdot & \cdot & \cdot \\ & & & \cdot & \cdot \\ & & & & 0 & -c_{n-2} \\ & & & & 1 & -c_{n-1} \end{pmatrix} .$$

Dies bedeutet gerade $\varphi x_1 = x_2, \varphi x_2 = x_3, \dots, \varphi x_{n-1} = x_n$, also $x_i = \varphi^{i-1} x_1$ für $1 \leq i \leq n$, und (b) folgt mit $v = x_1$.

(b) \Rightarrow (a): Dies ist offensichtlich, denn unter Bedingung (b) gilt $V = K[x]v$.

Zum Zusatz: unter der Bedingung (c) gilt, mit obigen Bezeichnungen, auch noch

$$\varphi^n x_1 = \varphi(\varphi^{n-1} x_1) = \varphi(x_n) = - \sum_{i=1}^n c_{i-1} x_i$$

wegen $x_i = \varphi^{i-1} x_1$ also $\varphi^n x_1 = - \sum_{i=0}^{n-1} c_i \varphi^i x_1$, d.h.,

$$q(\varphi)x_1 = \sum_{i=0}^n c_i \varphi^i x_1 = 0 .$$

Die Surjektion

$$\begin{aligned} \alpha : K[x] &\rightarrow V \\ f &\mapsto f(\varphi)x_1 \end{aligned}$$

induziert also einen $K[x]$ -Modul-Epimorphismus

$$\bar{\alpha} : K[x]/(q) \rightarrow V .$$

Da die Dimension beider Vektorräume gleich ist, nämlich gleich $n = \deg q$ (für die linke Seite siehe den Schritt (a) \Rightarrow (c)), ist $\bar{\alpha}$ ein Isomorphismus. Die Surjektivität impliziert, dass jedes $w \in V$ von $q(\varphi)$ annulliert wird (da links jedes Element von $q(x)$ annulliert wird). Es ist also $q(\varphi) = 0$, so dass $p_\varphi | q$ für das Minimalpolynom p_φ von φ . Andererseits folgt $p_\varphi(\varphi)x_1 = 0$, also $p_\varphi(x) \in \ker \alpha = (q)$, d.h., $q | p_\varphi$, so dass $q = p_\varphi$.

Schließlich ergibt eine einfache Rechnung, dass das charakteristische Polynom von $A(q)$ gleich q ist, d.h., $q = \chi_\varphi$.

Satz 8.11 (Jordan-Weierstraß-Normalform)

(a) Es gibt eine Basis von V , so dass die assoziierte Darstellungsmatrix von φ die Blockdiagonalgestalt

$$(8.11.1) \quad A = \begin{pmatrix} A(q_1) & & & 0 \\ & A(q_2) & & \\ & & \ddots & \\ 0 & & & A(q_r) \end{pmatrix}$$

hat, wobei die $A(q_i)$ die Begleitmatrizen zu nicht-konstanten normierten Polynomen $q_i \in K[x]$ sind, die Potenzen von (normierten) Primpolynomen sind. Die $A(q_i)$ sind dabei bis auf Umordnung eindeutig. Hierbei gilt $\chi_\varphi(x) = \prod_{i=1}^r q_i$ und $p_\chi(x) = \text{kgV}(q_1, \dots, q_r)$.

(b) Jede Matrix $A \in M_n(K)$ ist ähnlich zu einer Matrix wie in (a), wobei die $A(q_i)$ bis auf Anordnung eindeutig sind. Hierbei gilt $\chi_A(x) = \prod_{i=1}^r q_i$ und $p_\chi(x) = \text{kgV}(q_1, \dots, q_r)$.

Beweis: Zunächst sind (a) und (b) äquivalent, da Ähnlichkeit von (Darstellungs-)Matrizen gerade einem Basiswechsel entspricht. Behauptung (a) folgt aus der $K[x]$ -Modul-Isomorphie nach Satz 8.2 (b) und (c)

$$V \cong \bigoplus_{i=1}^r K[x]/(q_i),$$

wobei die q_i nach 8.2 (b) und (c) bis auf Anordnung eindeutig sind, zusammen mit Lemma 8.10. (unter Benutzung, dass $x - \lambda_i$ nilpotent von der Ordnung η_i ist, vergleiche Lineare Algebra II, Beobachtung 5.9). Der Zusatz folgt leicht. Für $p_\chi(x)$ beachten wir: Ist $f(x) \in K[x]$, so gilt für eine Matrix A wie in 8.11.1 $f(A) = 0$ genau dann, wenn $f(A(q_i)) = 0$ für alle $i = 1, \dots, r$ (vergleiche Lineare Algebra II, Bemerkung 6.2).

Bemerkung 8.12 Hieraus folgen auch die Sätze über die Jordan-Normalform. Zerfällt nämlich $\chi_\varphi(x)$ über K (\Leftrightarrow alle q_i zerfallen über $K \Leftrightarrow p_\varphi(x)$ zerfällt über K), so ist für jedes i

$$q_i(x) = (x - \lambda_i)^{n_i}$$

für ein $\lambda_i \in K$ und ein $n_i \in \mathbb{N}$. Man zeigt nun leicht mit Lemma 8.10, dass für eine geeignete Basis von $K[x]/(q_i)$ die darstellende Matrix von $x = \varphi$ Jordannormalform hat. Beachte: Eine Zerlegung von V in eine direkte Summe von $K[x]$ -Untermoduln entspricht der Zerlegung von V in eine direkte Summe von φ -invarianten Teilräumen $U \subseteq V$ (d.h., $\varphi(U) \subseteq U$). Letzteres entspricht wieder einer Blockdiagonalform der darstellenden Matrix für geeignete Basen (siehe Lineare Algebra II, Lemma 4.16). Also ist $A(q_i)$ ähnlich zur Jordan-Matrix

$$\begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & \ddots & 1 \\ & & & \lambda_i \end{pmatrix}.$$

§9 Der Transzendenzgrad

Erinnerung: Eine Körpererweiterung L/K heißt transzendent, wenn sie nicht algebraisch ist.

Definition 9.1 Sei L/K eine Körpererweiterung.

(a) Eine Familie (x_1, \dots, x_n) von Elementen aus L heißt **algebraisch unabhängig** (oder **transzendent**) über K , wenn für jedes Polynom $f \in K[X_1, \dots, X_n]$ mit $f(x_1, \dots, x_n) = 0$

notwendigerweise $f = 0$ ist, d.h., wenn der Einsetzungshomomorphismus

$$\begin{aligned} K[X_1, \dots, X_n] &\rightarrow L \\ f(X_1, \dots, X_n) = \sum c_{\nu_1, \dots, \nu_n} X_1^{\nu_1} \dots X_n^{\nu_n} &\mapsto f(x_1, \dots, x_n) = \sum c_{\nu_1, \dots, \nu_n} x_1^{\nu_1} \dots x_n^{\nu_n} \end{aligned}$$

injektiv ist (Hier ist $K[X_1, \dots, X_n]$ der Polynomring in den n Variablen X_1, \dots, X_n).

(b) Eine beliebige Familie $(x_i)_{i \in I}$ von Elementen $x_i \in L$ heißt algebraisch unabhängig (oder transzendent) über K , wenn dies für jede endliche Teilfamilie $(x_{i_1}, \dots, x_{i_r})$ gilt.

Bemerkungen 9.2 (a) Für $n = 1$ wurde 9.1(a) schon in Algebra I, Definition 9.1 definiert, und L/K ist genau dann transzendent, wenn es ein transzendentes Element $x \in K$ gibt.

(b) 9.1(b) bedeutet ebenfalls, dass der Einsetzungshomomorphismus

$$\begin{aligned} K[X_i \mid i \in I] &\rightarrow L \\ f &\mapsto f(x_i) \end{aligned}$$

injektiv ist. Insbesondere erhalten wir dann eine Isomorphie

$$K(X_i \mid i \in I) \xrightarrow{\sim} K(x_i \mid i \in I),$$

wobei $K(X_i \mid i \in I) = \text{Quot}(K[X_i \mid i \in I])$ der sogenannte (rationale) **Funktionskörper in den Variablen X_i** ist und $K(x_i \mid i \in I) \subseteq L$ der von den x_i ($i \in I$) erzeugte Teilkörper von L (vergleiche Algebra I, 8.11, 8.12 und 9.6).

Definition 9.3 Sei L/K eine Körpererweiterung. Eine Familie $(x_i)_{i \in I}$ von Elementen $x_i \in L$ heißt **Transzendenzbasis von L über K** , wenn sie algebraisch unabhängig über K ist und L algebraisch über $K(x_i \mid i \in I)$ ist.

Genauso können wir auch für Teilmengen $\mathcal{X} \subseteq L$ definieren, wann sie algebraisch unabhängig über K sind oder eine Transzendenzbasis von L/K (durch Betrachtung der Familie $(x)_{x \in \mathcal{X}}$).

Sei L/K eine Körpererweiterung.

Lemma 9.4 Sei $\mathcal{X} \subseteq L$ algebraisch unabhängig über K , und sei $x \in L \setminus \mathcal{X}$. Dann ist x genau dann transzendent über $K(\mathcal{X}) := K(x \mid x \in \mathcal{X})$, wenn $\mathcal{X} \cup \{x\}$ algebraisch unabhängig über K ist.

Beweis (1) Sei x transzendent über $K(\mathcal{X})$. Angenommen $\mathcal{X} \cup \{x\}$ ist nicht algebraisch unabhängig über K . Dann gibt es $x_1, \dots, x_n \in \mathcal{X}$ und ein nicht-triviales Polynom $f \in K[X_1, \dots, X_{n+1}]$ mit $f(x_1, \dots, x_n, x) = 0$. Da (x_1, \dots, x_n) algebraisch unabhängig über K sind, kommt X_{n+1} in f in nicht-trivialer Potenz vor, und es folgt, dass x algebraisch über $k(x_1, \dots, x_n)$, also auch über $k(\mathcal{X})$ ist – Widerspruch!

(2) Sei $\mathcal{X} \cup \{x\}$ algebraisch unabhängig über K . Angenommen, x ist algebraisch über $K(\mathcal{X})$. Dann gibt es ein nicht-triviales Polynom $f \in K(\mathcal{X})[X]$ mit $f(x) = 0$. Ist

$$f(x) = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0$$

mit $a_i \in K(\mathcal{X})$, so gibt es endlich viele $x_1, \dots, x_n \in \mathcal{X}$, so dass $a_0, \dots, a_m \in K(x_1, \dots, x_n)$. Schreiben wir die a_i als Brüche

$$a_i = \frac{p_i(x_1, \dots, x_n)}{q_i(x_1, \dots, x_n)}$$

mit Polynomen $p_i, q_i \in K[X_1, \dots, X_n]$, $q_i \neq 0$, so erhalten wir durch Multiplikation mit $\prod_i q_i(x_1, \dots, x_n)$ eine Gleichung

$$b_m(x_1, \dots, x_n)x^m + \dots + b_1(x_1, \dots, x_n)x + b_0(x_1, \dots, x_n) = 0$$

mit Polynomen $b_i(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$, nicht alle gleich null. Dann ist

$$g(X_1, \dots, X_n, X_{n+1}) = \sum_{i=0}^m b_i(X_1, \dots, X_n)X_{n+1}^i$$

ein nicht-triviales Polynom in $K[X_1, \dots, X_{n+1}]$ mit $g(x_1, \dots, x_n, x) = 0$ – Widerspruch zur algebraischen Unabhängigkeit von $\mathcal{X} \cup \{x\}$.

Corollar 9.5 Eine Teilmenge $\mathcal{X} \subseteq L$ ist genau dann eine Transzendenzbasis von L/K , wenn sie eine maximale über K algebraisch unabhängige Teilmenge ist.

Beweis Gilt die letztere Bedingung, so ist nach 9.4 jedes $x \in L$ algebraisch über $k(\mathcal{X})$. Ist umgekehrt \mathcal{X} eine Transzendenzbasis von L/K , so gibt es nach 9.4 keine echt größere Teilmenge, die algebraisch unabhängig über K ist.

Corollar 9.6 Jede Körpererweiterung L/K besitzt eine (möglicherweise leere) Transzendenzbasis.

Beweis Ist L/K algebraisch, so ist nichts zu zeigen. Andernfalls ist die Menge \mathcal{M} der über K algebraisch unabhängigen Teilmengen $\mathcal{X} \subseteq L$ nicht leer und induktiv geordnet: Für eine Kette (total geordnete Teilmenge) $\mathcal{N} \subseteq \mathcal{M}$ ist $\bigcup_{\mathcal{X} \in \mathcal{N}} \mathcal{X}$ algebraisch unabhängig über K , also eine obere Schranke von \mathcal{N} in \mathcal{M} . Nach dem Zornschen Lemma (Lineare Algebra II, Lemma 11.13) besitzt \mathcal{M} also mindestens ein maximales Element; dies ist nach 9.5 eine Transzendenzbasis von L/K .

Sei weiter L/K eine Körpererweiterung.

Proposition 9.7 (Ergänzungssatz) Seien $\mathcal{X}', \mathcal{Y} \subseteq L$ Teilmengen. Ist \mathcal{X}' algebraisch unabhängig über K und L algebraisch über $K(\mathcal{Y})$, so lässt sich \mathcal{X}' durch Hinzunahme von Elementen aus \mathcal{Y} zu einer Transzendenzbasis \mathcal{X} von L/K vergrößern.

Beweis: Wieder mit dem Zornschen Lemma sieht man, dass es eine maximale Teilmenge $\mathcal{X}'' \subseteq \mathcal{Y}$ gibt, für die $\mathcal{X}' \cup \mathcal{X}''$ algebraisch unabhängig über K ist. Nach Lemma 9.4 ist dann jedes Element $y \in \mathcal{Y}$ algebraisch über $K(\mathcal{X}' \cup \mathcal{X}'')$. Dann ist $K(\mathcal{Y})$ algebraisch über $K(\mathcal{X}' \cup \mathcal{X}'')$ (vergleiche Algebra I, Satz 9.9). Nach Voraussetzung gilt dies dann auch für L , und damit ist $\mathcal{X}' \cup \mathcal{X}''$ eine Transzendenzbasis von L/K .

Bemerkungen 9.8 (a) Insbesondere enthält \mathcal{Y} eine Transzendenzbasis für L/K (Fall $\mathcal{X} = \emptyset$).

(b) In 9.7 können wir für \mathcal{Y} ein Erzeugendensystem von L über K nehmen (Fall $K(Y) = L$).

Beispiel 9.9 Sei $L = \mathbb{R}(x, y \mid x^2 + y^2 = 0)$ der Funktionenkörper der Quadrik $x^2 + y^2 = 0$. Dies ist so zu verstehen: Das Polynom $X^2 + Y^2 \in \mathbb{R}[X, Y]$ ist irreduzibel, denn sonst könnten wir es in zwei Linearfaktoren $(X - \alpha) \cdot (X - \beta)$ mit $\alpha, \beta \in \mathbb{R}[Y]$ aufspalten. (Fasse $\mathbb{R}[X, Y]$ als Polynomring $\mathbb{R}[Y][X]$ auf), was auf $\alpha^2 = -Y^2$ führen würde – Widerspruch. Daher ist

$$A = \mathbb{R}[X, Y]/(X^2 + Y^2)$$

integer, und wir setzen $L = \text{Quot}(A)$ (Quotientenkörper von A), wobei wir mit x und y die Bilder von X und Y in A (und L) bezeichnen. Dann ist $\{x, y\}$ ein Erzeugendensystem von L über \mathbb{R} (klar) und sowohl x als auch y liefert eine Transzendenzbasis von L/\mathbb{R} : Die Inklusion $\mathbb{R}[X] \hookrightarrow \mathbb{R}[X, Y]$ induziert einen injektiven Ringhomomorphismus von integren Ringen

$$\mathbb{R}[X] \hookrightarrow \mathbb{R}[X, Y]/(X^2 + Y^2) = A,$$

da offenbar $\mathbb{R}[X] \cap (X^2 + Y^2) = 0$. Dieser induziert wiederum eine Einbettung

$$\mathbb{R}(X) \hookrightarrow L$$

der Quotientenkörper (warum?) mit Bild $\mathbb{R}(x)$. Also ist x transzendent über \mathbb{R} ; andererseits ist y wegen der Gleichung $y^2 + x^2 = 0$ algebraisch über $\mathbb{R}(x)$, also auch L . Der Fall von y ist symmetrisch.

Satz 9.10 Zwei Transzendenzbasen \mathcal{X}, \mathcal{Y} einer Körpererweiterung L/K haben dieselbe Mächtigkeit.

Definition 9.11 Der **Transzendenzgrad** einer Körpererweiterung L/K wird definiert als

$$\text{tr. deg}(L/K) = |\mathcal{X}|,$$

wobei \mathcal{X} eine Transzendenzbasis von L/K ist.

Nach Satz 9.10 hängt diese Mächtigkeit nur von L/K ab.

Beispiel 9.12 Für den Körper $L = \mathbb{R}(x, y \mid x^2 + y^2 = 0)$ aus Beispiel 9.9 gilt $\text{tr. deg}(L/\mathbb{R}) = 1$.

Beweis von Satz 9.10 für den Fall, dass \mathcal{X} endlich ist: Sei etwa $\mathcal{X} = \{x_1, \dots, x_n\}$. Wir zeigen durch Induktion über n , dass $|\mathcal{Y}| \leq n = |\mathcal{X}|$. Durch Symmetrie folgt dann auch $|\mathcal{X}| \leq |\mathcal{Y}|$, also $|\mathcal{X}| = |\mathcal{Y}|$. Für $n = 0$ ist L/K algebraisch, also auch $\mathcal{Y} = \emptyset$. Sei also $n > 0$. Dann ist L/K nicht algebraisch, also $\mathcal{Y} \neq \emptyset$, etwa $y \in \mathcal{Y}$. Nach Proposition 9.7 können wir y durch eine Teilmenge aus \mathcal{X} zu einer Transzendenzbasis \mathcal{Z} von L/K ergänzen. Dann gilt $|\mathcal{Z}| \leq n$, denn sonst wäre $\mathcal{Z} = \{y\} \cup \mathcal{X}$, aber \mathcal{X} ist maximal algebraisch unabhängig. Man sieht leicht, dass $\mathcal{Y} \setminus \{y\}$ und $\mathcal{Z} \setminus \{y\}$ beides Transzendenzbasen von $L/K(y)$ sind

(ähnliche Schlüsse wie für Lemma 9.4 – Übungsaufgabe!), wobei $|\mathcal{Z} \setminus \{y\}| < n$. Nach Induktionsvoraussetzung ist dann $|\mathcal{Y} \setminus \{y\}| \leq |\mathcal{Z} \setminus \{y\}|$, also $|\mathcal{Y}| \leq |\mathcal{Z}| \leq n$.

Für den Fall, wo \mathcal{X} und \mathcal{Y} beide unendlich sind, brauchen wir einige mengentheoretische Vorbereitungen.

Satz 9.13 (Schröder-Bernstein) Seien M und N Mengen. Gibt es Injektionen $\sigma : M \hookrightarrow N$ und $\tau : N \hookrightarrow M$, so existiert eine Bijektion $\rho : M \rightarrow N$, d.h., M und N sind gleichmächtig ($|M| = |N|$).

Beweis: Sei $M' \subseteq M$ die Menge aller Elemente $x \in M$, so dass für alle $b \in \mathbb{N}_0$ gilt

$$x \in (\tau\sigma)^n(M) \Rightarrow x \in (\tau\sigma)^n\tau(N)$$

(mit $(\tau\sigma)^0 = id$). Ein $x \in M$ gehört also genau dann zu M' , wenn eine fortwährende Bildung von Urbildern (eindeutig falls existent!)

$$\begin{array}{ccccccc} x, & \tau^{-1}(x), & \sigma^{-1}\tau^{-1}(x), & \tau^{-1}\sigma^{-1}\tau^{-1}(x), & \dots \\ \cap & \cap & \cap & \cap & \\ M & N & M & N & \end{array}$$

entweder unendlich oft möglich ist oder bei einem Element aus N (nach einer ungeraden Anzahl von Schritten) endet. Erkläre nun $\rho : M \rightarrow N$ durch

$$\rho(x) = \begin{cases} \tau^{-1}(x) & , \quad x \in M' \\ \sigma(x) & , \quad x \notin M' \end{cases}$$

Dann ist ρ injektiv: Die Einschränkungen $\rho|_{M'}$ und $\rho|_{M \setminus M'}$ sind injektiv, und für $x \in M'$ und $y \in M \setminus M'$ mit $\rho(x) = \rho(y)$ folgt $\sigma(y) = \tau^{-1}(x)$, d.h., $\tau\sigma(y) = x$ und damit $y \in M'$ – Widerspruch! Weiter ist ρ surjektiv: Sei $z \in N$ und $x = \tau(z)$. Für $x \in M'$ gilt dann $\rho(x) = \tau^{-1}(x) = z$. Für $x \notin M'$ besitzt $z \in N$ ein Urbild $y = \sigma^{-1}(z) = \sigma^{-1}\tau^{-1}(z)$, da sonst $x \in M'$ nach Definition von M' . Wegen $x \notin M'$ gilt auch $y \notin M'$ und daher, nach Definition, $\rho(y) = \sigma(y) = z$.

Für Mengen M und N schreibe $|M| \leq |N|$ wenn, es eine Injektion $M \hookrightarrow N$ gibt. Der obige Satz lautet damit: $|M| \leq |N|$ und $|N| \leq |M| \Rightarrow |M| = |N|$.

Bemerkungen 9.14 Unter Benutzung des Auswahlaxioms (\Leftrightarrow Zornsches Lemma) folgt

$$|M| \leq |N| \Leftrightarrow \text{Es gibt eine Surjektion } f : N \rightarrow M.$$

Sei nämlich $f : N \rightarrow M$ eine Surjektion, so gibt es nach dem Auswahlaxiom einen Schnitt $s : M \rightarrow N$ von f ($f \circ s = id_M$), und s ist notwendigerweise injektiv. Ist umgekehrt $i : M \hookrightarrow N$ eine Injektion und $\overline{M} = N \setminus i(M)$, $M \neq \emptyset$ (sonst ist nichts zu zeigen), so wähle $m \in M$ und definiere eine Surjektion $f : N \rightarrow M$ durch

$$f(n) = \begin{cases} i^{-1}(n) & , \quad n \in i(M), \\ m & , \quad \text{sonst.} \end{cases}$$

Lemma 9.15 Ist $(M_i)_{i \in I}$ eine Familie von *endlichen* Mengen und ist die Indexmenge *unendlich*, so gilt für die disjunkte Vereinigung $\coprod_{i \in I} M_i$

$$|\coprod_{i \in I} M_i| = |I|.$$

Beweis: Ist I abzählbar unendlich, so ist dies klar (durch einfaches “Abzählen”). Im Allgemeinen betrachte die Menge \mathcal{P} aller Paare

$$P = (I_P, f_P)$$

wobei $I_P \subseteq I$ eine unendliche Teilmenge ist und $f : \coprod_{i \in I_P} M_i \rightarrow I_P$ eine Bijektion. Dann ist \mathcal{P} nicht leer, denn I enthält eine abzählbar unendliche Teilmenge I' und nach der Vorbemerkung gibt es ein Paar $(I', f) \in \mathcal{P}$. Definiere eine Ordnung \leq auf \mathcal{P} durch

$$P \leq P' \text{ wenn } I_P \subseteq I_{P'} \text{ und } f_P = f_{P'} \upharpoonright \coprod_{i \in I_P} M_i$$

(insbesondere gilt dann $f_{P'}(\coprod_{i \in I_P} M_i) = I_P$!). Diese Ordnung ist induktiv, denn für eine Kette $(P_\alpha)_{\alpha \in A}$ mit $P_\alpha = (I_\alpha, f_\alpha) \in \mathcal{P}$ definiere $P = (I_P, f_P) \in \mathcal{P}$ durch

$$\begin{aligned} I_P &= \bigcup_{\alpha \in A} I_\alpha \\ f_P &: \coprod_{i \in I_P} M_i \rightarrow I_P, \quad f_P \upharpoonright \coprod_{i \in I_\alpha} M_i = f_\alpha. \end{aligned}$$

Dann ist P wohldefiniert und eine obere Schranke für die Kette. Nach dem Zornschen Lemma besitzt \mathcal{P} also ein maximales Element (I_0, f_0) . Für dieses ist aber $I \setminus I_0$ endlich, denn sonst können wir eine abzählbare Menge $I_1 \subseteq I \setminus I_0$ und eine Bijektion $f_1 : \coprod_{i \in I_1} M_i \rightarrow I_1$ finden. Dann ist aber $(I_0 \cup I_1, f) \in \mathcal{P}$ mit

$$f \upharpoonright \coprod_{i \in I_0} M_i = f_0, \quad f \upharpoonright \coprod_{i \in I_1} M_i = f_1,$$

im Widerspruch zur Maximalität von (I_0, f_0) . Es bleibt zu zeigen:

Behauptung: Ist M eine unendliche Menge und N eine endliche Menge, so gilt $|M| = |M \coprod N|$.

Damit folgt dann nämlich wegen der Endlichkeit von $I \setminus I_0$

$$|\coprod_{i \in I} M_i| = |\coprod_{i \in I_0} M_i| = |I_0| = |I|.$$

Beweis der Behauptung: Die Behauptung ist klar falls M abzählbar unendlich ist. Im Allgemeinen sei $J \subseteq M$ eine abzählbar unendliche Teilmenge und $f : J \rightarrow J \coprod N$ eine Bijektion. Dann erhalten wir eine offensichtliche Bijektion $g : M \rightarrow M \coprod N$ durch

$$g(x) = \begin{cases} x & , \quad x \notin J, \\ f(x) & , \quad x \in J. \end{cases}$$

Beweis von Satz 9.10 für den Fall, dass \mathcal{X} und \mathcal{Y} unendlich sind: Seien \mathcal{X} und \mathcal{Y} zwei unendliche Transzendenzbasen von L/K . Jedes $x \in \mathcal{X}$ ist algebraisch über $K(\mathcal{Y})$. Es gibt also zu x eine endliche Teilmenge $\mathcal{Y}_x \subseteq \mathcal{Y}$, so dass x algebraisch über $K(\mathcal{Y}_x)$ ist. Da L für eine echte Teilmenge $\mathcal{Y}' \subsetneq \mathcal{Y}$ nicht algebraisch über $K(\mathcal{Y}')$ sein kann (Corollar 9.5), ist $\bigcup_{x \in \mathcal{X}} \mathcal{Y}_x = \mathcal{Y}$. Die Inklusionen $\mathcal{Y}_x \hookrightarrow \mathcal{Y}$ definieren daher eine surjektive Abbildung

$$\coprod_{x \in \mathcal{X}} \mathcal{Y}_x \twoheadrightarrow \mathcal{Y}.$$

Mit Bemerkung 9.14 und Lemma 9.15 folgt

$$|\mathcal{Y}| \leq |\coprod_{x \in \mathcal{X}} \mathcal{Y}_x| = |\mathcal{X}|.$$

Aus Symmetriegründen gilt auch $|\mathcal{X}| \leq |\mathcal{Y}|$, und aus Satz 9.11 folgt $|\mathcal{X}| = |\mathcal{Y}|$ q.e.d.

Der Transzendenzgrad ist additiv in Erweiterungen:

Satz 9.16 Für eine Kette $K \subseteq L \subseteq M$ von Körpererweiterungen gilt

$$\text{tr. deg}(M/K) = \text{tr. deg}(L/K) + \text{tr. deg}(M/L).$$

Beweis Dies folgt leicht mit den obigen Techniken – Übungsaufgabe!

§10 Lokalisierungen

Der folgende Begriff verallgemeinert den Begriff des Quotientenkörpers. Sei A ein kommutativer Ring mit Eins.

Definition 10.1 Eine Teilmenge $S \subseteq A$ heißt multiplikativ (oder multiplikativ abgeschlossen), wenn $1 \in S$ und wenn mit a und b in S auch $a \cdot b$ in S liegt.

Beispiele 10.2 (a) Für jedes $f \in A$ ist die Menge $\{f^n \mid n \in \mathbb{N}_0\}$ multiplikativ (wobei wir setzen: $f^0 := 1$).

(b) (*wichtig!*) Sei $\mathfrak{a} \subseteq A$ ein Ideal. Die Menge $A \setminus \mathfrak{a}$ ist genau dann multiplikativ, wenn \mathfrak{a} ein Primideal ist.

(c) Erinnerung: ein Element $f \in A$ heißt Nullteiler wenn es ein $g \neq 0$ in A gibt mit $f \cdot g = 0$. Die Menge U_A der Nicht-Nullteiler in A ist multiplikativ.

Sei $S \subseteq A$ multiplikativ. Betrachte auf der Menge $A \times S$ die folgende Relation

$$(a, s) \sim (a', s') :\Leftrightarrow \text{es ex. ein } t \in S \text{ mit } ts'a = tsa'$$

Dann ist \sim eine Äquivalenzrelation: Reflexivität und Symmetrie sind klar, und für die Transitivität “braucht man das t ” in der Definition, falls S Nullteiler hat:

$$t(s'a - sa') = 0 \quad , \quad t'(s''a' - s'a'') = 0 \quad \Rightarrow \quad t t' s' (s''a - sa'') = 0$$

Für $(a, s) \in A \times S$ sei $\frac{a}{s}$ die Äquivalenzklasse von (a, s) bezüglich \sim . Die Menge $A \times S / \sim$ der Äquivalenzklassen wird mit A_S (oder $S^{-1}A$ oder $A[S^{-1}]$) bezeichnet.

Satz/Definition 10.3 (a) A_S wird mit den Verknüpfungen

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

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

ein Ring (kommutativ, mit Eins) und heißt die Lokalisierung von A nach S .

(b) Die Abbildung

$$\varphi_{univ} : A \rightarrow A_S$$

$$a \mapsto \frac{a}{1}$$

ist ein Ringhomomorphismus und alle Elemente in $\varphi_{univ}(S)$ sind invertierbar in A_S .

(c) (universelle Eigenschaft) Ist $\varphi : A \rightarrow B$ ein Ringhomomorphismus derart, dass $\varphi(S)$ aus lauter invertierbaren Elementen besteht, so gibt es einen eindeutig bestimmten Ringhomomorphismus $\tilde{\varphi} : A_S \rightarrow B$, der das Diagramm

$$\begin{array}{ccc} A & \xrightarrow{\varphi_{univ}} & A_S \\ & \searrow \varphi & \swarrow \exists! \tilde{\varphi} \\ & B & \end{array}$$

kommutativ macht.

Beweis: (a) Wohldefiniertheit: Ist $\frac{a}{s} = \frac{a'}{s'}$ und $\frac{b}{t} = \frac{b'}{t'}$, so gibt es $s_1, s_2 \in S$ mit $s_1(s'a - sa) = 0$ und $s_2(t'b - tb') = 0$. Dann ist $s_1s_2[(s't'(at + bs) - st(a't' + b's'))] = 0$, also

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'}$$

sowie $s_1s_2[s't'ab - sta'b'] = 0$, also

$$\frac{ab}{st} = \frac{a'b'}{s't'}$$

Der Beweis der Ringeigenschaften ist einfach unter der Benutzung der "Kürzungsregel"

$$\frac{a}{s} = \frac{ta}{ts} \quad \text{für } t \in S.$$

(b) Wegen $\frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$ und $\frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$ ist φ_{univ} ein Ringhomomorphismus, und für $s \in S$ ist $\frac{1}{s}$ ein Inverses von $\varphi(s) = \frac{s}{1}$.

(c) Setze $\tilde{\varphi}(\frac{a}{s}) = \varphi(s)^{-1} \cdot \varphi(a)$. Dann folgen alle Eigenschaften einfach (Eindeutigkeit: $\varphi(a) = \tilde{\varphi}(\frac{a}{1}) = \tilde{\varphi}(\frac{a}{s} \cdot \frac{s}{1}) = \tilde{\varphi}(\frac{a}{s}) \cdot \tilde{\varphi}(\frac{s}{1}) = \tilde{\varphi}(\frac{a}{s}) \cdot \varphi(s) \Rightarrow \tilde{\varphi}(\frac{a}{s}) = \varphi(s)^{-1} \cdot \varphi(a)$).

Beispiele 10.4 (a) Enthält S die Null, so ist $A_S = 0$ (der Nullring).

(b) Für $f \in A$ und $S_f := \{f^n | n \in \mathbb{N}_0\}$ (vergl. 10.2 (a)) schreibt man auch A_f (oder $A[f^{-1}]$) für A_{S_f} .

(c) Allgemein sei für eine beliebige Menge $M \subseteq A$ definiert: $A[M^{-1}] := A[S_M^{-1}]$, wobei S_M die von M erzeugte multiplikative Teilmenge von A ist (existiert, als Durchschnitt aller multiplikativen Teilmengen S , die M enthalten). Dann hat $A[M^{-1}]$ eine analoge universelle Eigenschaft für Morphismen $\varphi : A \rightarrow B$, für die $\varphi(m)$ invertierbar ist für alle $m \in M$.

(d) Ist $\mathfrak{p} \subseteq A$ ein Primideal, so setze

$$A_{\mathfrak{p}} := A[(A \setminus \mathfrak{p})^{-1}].$$

(e) Ist $U_A \subseteq A$ die Menge der Nicht-Nullteiler (vgl. 4.2.(c)), so heißt

$$\text{Quot}(A) := A[U_A^{-1}]$$

der totale Quotientenring von A .

(f) Ist A ein Integritätsbereich, so ist $U_A = A \setminus \{0\}$ und $\text{Quot}(A)$ ist ein Körper (*jedes* $\frac{a}{b} \neq 0$ hat ein Inverses!), der übliche *Quotientenkörper* von A .

Lemma 10.5 Die Abbildung $A \rightarrow A_S$ ist genau dann injektiv, wenn S keine Nullteiler enthält. Insbesondere ist also $A \rightarrow \text{Quot}(A)$ injektiv.

Beweis: selbst

Satz 10.6. Sei $\varphi : A \rightarrow B$ ein Homomorphismus von Ringen, und seien $S \subseteq A$ und $T \subseteq B$ multiplikative Teilmengen mit $\varphi(S) \subseteq T$. Dann existiert genau ein Ringhomomorphismus $\varphi' : A_S \rightarrow B_T$ der φ fortsetzt, d.h., der

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \varphi_{univ} \downarrow & & \downarrow \varphi_{univ} \\ A_S & \xrightarrow{\varphi'} & B_T \end{array}$$

kommutativ macht.

Beweis: $(\varphi_{univ} \circ \varphi)(S)$ besteht ganz aus Einheiten; nach der universellen Eigenschaft 4.3. (c) gibt es also genau einen Ringhomomorphismus, der das untere Dreieck in

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & \searrow \varphi_{univ} \circ \varphi & \downarrow \\ A_S & \longrightarrow & B_T \end{array}$$

kommutativ macht.

Corollar 10.7. Seien

$$\begin{array}{ccccc} A & \xrightarrow{\varphi} & B & \xrightarrow{\psi} & C & \text{Ringhomomorphismen} \\ \cup & & \cup & & \cup & \\ S & \rightarrow & T & \rightarrow & U & \text{multiplikative Teilmengen} \end{array}$$

Dann gilt $\psi' \circ \varphi' = (\psi \circ \varphi)' : A_S \rightarrow C_U$.

Beweis: $\psi' \circ \varphi'$ leistet dieselbe Kommutativität wie $\psi \circ \varphi$.

Satz/Definition 10.8 Für einen A -Modul M und eine multiplikative Teilmenge $S \subseteq A$ definiere

$$M_S = (M \times S) / \sim$$

wobei $(m, s) \sim (m', s')$ falls ein $t \in S$ existiert mit $ts'm = tsm'$ (Andere Bezeichnungen: $S^{-1}M$ oder $M[S^{-1}]$). Die Äquivalenzklasse von (m, s) sei mit $\frac{m}{s}$ bezeichnet. Dann wird M_S ein A_S -Modul durch die Definitionen

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st} \quad , \quad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

für $m, n \in M$, $s, t \in S$ und $a \in A$.

(b) (universelle Eigenschaft) Es gibt einen kanonischen A -Modul-Homomorphismus $\varphi_{univ} : M \rightarrow M_S$, und für $s \in S$ ist

$$\begin{aligned} L_s : M_S &\rightarrow M_S \\ x &\mapsto s \cdot x \end{aligned}$$

ein Isomorphismus. Ist N ein weiterer A -Modul derart, dass für jedes $s \in S$ die Abbildung $L_s : N \rightarrow N$, $n \mapsto sn$, ein Isomorphismus ist, und ist $\varphi : M \rightarrow N$ ein A -Modul-Homomorphismus, so gibt es einen eindeutig bestimmten A -Modul-Homomorphismus $\tilde{\varphi} : M_S \rightarrow N$ der

$$\begin{array}{ccc} M & \xrightarrow{\varphi_{univ}} & M_S \\ & \searrow \varphi & \swarrow \exists! \tilde{\varphi} \\ & N & \end{array}$$

kommutativ macht. Weiter ist $\tilde{\varphi}$ ein A_S -Modul-Homomorphismus, wobei N ein A_S -Modul ist vermöge $\frac{a}{s}n = (L_s)^{-1}(an)$ für $n \in N$, $a \in A$ und $s \in S$.

(c) Insbesondere induziert jeder A -Modul-Homomorphismus $f : M \rightarrow N$ einen A_S -Modul-Homomorphismus

$$f_S : M_S \rightarrow N_S$$

mit $f_S(\frac{m}{s}) = \frac{f(m)}{s}$ für $m \in M$, $s \in S$.

Beweis der Behauptungen: Ähnlich wie für Satz 10.3.

Definition 10.9 (a) Für ein Primideal $\mathfrak{p} \subseteq A$ und die multiplikative Menge $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ schreibe $M_{\mathfrak{p}}$ statt $M_{S_{\mathfrak{p}}}$ (dies ist also ein $A_{\mathfrak{p}}$ -Modul).

(b) Für $S_f = \{f^n | f \in \mathbb{N}_0\}$, $f \in A$, schreibe M_f statt M_{S_f} (dies ist ein A_f -Modul).

Satz 10.10 Lokalisierung ist exakt, d.h., ist $S \subseteq A$ eine multiplikative Teilmenge und

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

eine exakte Sequenz von A -Moduln, so ist auch

$$(M_1)_S \xrightarrow{f_S} (M_2)_S \xrightarrow{g_S} (M_3)_S$$

exakt (Daher folgt dasselbe für beliebige exakte Sequenzen).

Beweis: Sei $\frac{m_2}{s} \in (M_2)_S$ mit $0 = g_S(\frac{m_2}{s}) = \frac{g(m_2)}{s}$. Dann existiert ein $r \in S$ mit $0 = rg(m_2) = g(rm_2)$. Nach Voraussetzung existiert ein $m_1 \in M_1$ mit $rm_2 = f(m_1)$. Es folgt $\frac{m_2}{s} = \frac{f(m_1)}{rs} = f_S(\frac{m_1}{rs})$, d.h., $\ker g_S \subseteq \text{im } f_S$. Die Inklusion $\text{im } f_S \subseteq \ker g_S$ ist klar, denn es gilt $g_S f_S = 0$, wegen $gf = 0$.

Beispiele 10.11: (a) Ist $N \subseteq M$ ein Untermodul, \mathfrak{p} ein Primideal, so gilt

$$(M/N)_{\mathfrak{p}} \cong M_{\mathfrak{p}}/N_{\mathfrak{p}}$$

(betrachte $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$).

(b) Ist

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

eine exakte Sequenz von abelschen Gruppen, so ist

$$(10.11.1) \quad 0 \rightarrow A_{\mathbb{Q}} \rightarrow B_{\mathbb{Q}} \rightarrow C_{\mathbb{Q}} \rightarrow 0$$

exakt, wobei wir definieren: $A_{\mathbb{Q}} := A_{(0)} = (\mathbb{Z} \setminus \{0\})^{-1}A$. Dies ist ein Modul über $(\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z} = \mathbb{Q}$, also ein \mathbb{Q} -Vektorraum, und es gilt $\dim_{\mathbb{Q}} A_{\mathbb{Q}} = \text{rg } A$ (siehe Übungsaufgabe 26). Aus der exakten Sequenz (10.11.1) und der Additivität der Dimension in exakten Sequenzen folgt

$$\text{rg } B = \text{rg } A + \text{rg } C.$$

Definition/Lemma 10.12 (a) Ein Ring A heißt lokal, wenn die folgenden äquivalenten Eigenschaften gelten:

- (i) A hat genau ein maximales Ideal \mathfrak{m} .
- (ii) Die Menge $A \setminus A^{\times}$ der Nichteinheiten ist ein Ideal.

(b) Es ist in diesem Fall $\mathfrak{m} = A \setminus A^{\times}$, und der Körper A/\mathfrak{m} heißt der Restklassenkörper von A .

Beweis der Behauptungen: Für jeden Ring A ist

$$(10.12.1) \quad A \setminus A^{\times} = \bigcup_{\substack{\mathfrak{a} \subsetneq A \\ \text{Ideal}}} \mathfrak{a},$$

denn es gilt für $f \in A$: $f \in A \setminus A^{\times} \Leftrightarrow 1 \notin (f) \Leftrightarrow (f) \neq A$.

Gilt nun (i), so ist $A \setminus A^{\times} = \mathfrak{m}$ (da alle $\mathfrak{a} \subseteq \mathfrak{m}$), und es folgt (ii). Gilt umgekehrt (ii), ist also $A \setminus A^{\times}$ ein Ideal, so enthält es alle Ideale $\mathfrak{a} \subsetneq A$, ist also maximal und das einzige maximale Ideal.

Beispiele 10.13: (a) Ein Körper ist ein lokaler Ring (mit maximalem Ideal (0)).

(b) Der Nullring ist kein lokaler Ring.

(c) Ist A ein lokaler Ring, so ist der Ring $R = A[[x_1, \dots, x_n]]$ der formalen Potenzreihen in den Variablen x_1, \dots, x_n ein lokaler Ring und der Ringhomomorphismus $A \rightarrow A[[x_1, \dots, x_n]]$ induziert einen Isomorphismus der Restklassenkörper: Wegen

$$A[[x_1, \dots, x_n]] = A[[x_1, \dots, x_{n-1}]][[x_n]]$$

können wir dies durch Induktion über n beweisen; es ist also ohne Einschränkung $n = 1$. Ein Element $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$ ist aber genau dann eine Einheit, wenn der konstante Term a_0 eine Einheit ist (Beweis selbst: löse $f \cdot g = 1$). Es folgt $A[[x]] \setminus A[[x]]^\times = (x) + \mathfrak{m} A[[x]]$ (\mathfrak{m} das maximale Ideal von A); dies ist aber ein Ideal.

Der folgende Satz liefert viele Beispiele für lokale Ringe.

Satz 10.14 Sei A ein Ring und $\mathfrak{p} \subseteq A$ ein Primideal. Dann ist die Lokalisierung $A_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}\mathfrak{p} = \left\{ \frac{a}{b} \mid a \in \mathfrak{p}, b \notin \mathfrak{p} \right\}$. Der Restklassenkörper $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ ist isomorph zu $\text{Quot}(A/\mathfrak{p})$.

Für einen Ringhomomorphismus $\varphi : A \rightarrow B$ und ein Ideal $\mathfrak{a} \subseteq A$ sei dabei $\mathfrak{a}B = \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in B \right\}$ das von \mathfrak{a} in B erzeugte Ideal, wobei wir für $a \in A$ und $b \in B$ setzen: $ab := \varphi(a) \cdot b$.

Beweis: 1) Wir zeigen zunächst die Gleichheit

$$(10.14.1) \quad \mathfrak{p}A_{\mathfrak{p}} = \left\{ \frac{b}{s} \mid b \in \mathfrak{p}, s \in A \setminus \mathfrak{p} \right\}.$$

Zunächst ist die rechte Seite ein Ideal in $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}A$, denn für $a \in A, b, c \in \mathfrak{p}$ und $s, t \in A \setminus \mathfrak{p}$ gilt

$$\begin{aligned} \frac{b}{s} + \frac{c}{t} &= \frac{tb + sc}{st} \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}, \\ \frac{a}{s} \cdot \frac{c}{t} &= \frac{ac}{st} \in (A \setminus \mathfrak{p})^{-1}\mathfrak{p}. \end{aligned}$$

Jedes Element $\sum_{i=1}^r b_i \frac{a_i}{t_i} \in \mathfrak{p}A_{\mathfrak{p}}$ (mit $b_i \in \mathfrak{p}, a_i \in A, t_i \in A \setminus \mathfrak{p}$) liegt also in $(A \setminus \mathfrak{p})^{-1}\mathfrak{p}$ (da $b_i \frac{a_i}{t_i} = \frac{b_i a_i}{t_i}$). Die umgekehrte Inklusion ist klar.

2) Hiermit sieht man, dass die folgenden Aussagen für $\frac{a}{s} \in A_{\mathfrak{p}}$ ($a \in A, s \in A \setminus \mathfrak{p}$) äquivalent sind:

$$(10.14.2) \quad \frac{a}{s} \notin \mathfrak{p}A_{\mathfrak{p}} \Leftrightarrow a \in A \setminus \mathfrak{p} \Leftrightarrow \frac{a}{s} \in A_{\mathfrak{p}}^\times.$$

Denn nach (10.14.1) gilt $\frac{a}{s} \notin \mathfrak{p}A_{\mathfrak{p}} \Rightarrow a \notin \mathfrak{p}$; weiter gilt $a \in A \setminus \mathfrak{p} \Rightarrow \frac{a}{s} \in A_{\mathfrak{p}}^\times$ (ein Inverses von $\frac{a}{s}$ ist dann $\frac{s}{a}$). Schließlich gilt: $\frac{a}{s} \in A_{\mathfrak{p}}^\times \Rightarrow \frac{a}{s} \notin \mathfrak{p}A_{\mathfrak{p}}$, denn sonst wäre $1 = \frac{a}{s} \cdot \left(\frac{a}{s}\right)^{-1} \in \mathfrak{p}A_{\mathfrak{p}}$, also $1 = \frac{b}{t}$ mit $b \in \mathfrak{p}, t \in A \setminus \mathfrak{p}$. Dann gäbe es ein $t' \in A \setminus \mathfrak{p}$ mit $t't = b$ im Widerspruch dazu, dass $t't \in A \setminus \mathfrak{p}$ aber $b \in \mathfrak{p}$. Mit (10.14.2) folgt nun $\mathfrak{p}A_{\mathfrak{p}} = A_{\mathfrak{p}} \setminus A_{\mathfrak{p}}^\times$, d.h., nach 10.12 ist $A_{\mathfrak{p}}$ lokal mit maximalem Ideal $\mathfrak{p}A_{\mathfrak{p}}$.

3) Der Ringhomomorphismus $A \rightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ induziert eine Einbettung $A/\mathfrak{p} \hookrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, und die universelle Eigenschaft des Quotientenkörpers induziert eine Einbettung

$$\text{Quot}(A/\mathfrak{p}) \hookrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

Diese ist auch surjektiv: Ist $\frac{a}{b} \in A_{\mathfrak{p}}$, mit $a \in A$ und $b \in A \setminus \mathfrak{p}$, so ist für die Restklassen \bar{a}, \bar{b} in A/\mathfrak{p} offenbar $\bar{b} \neq 0$, und das Element $\frac{\bar{a}}{\bar{b}} \in \text{Quot}(A/\mathfrak{p})$ wird auf die Restklasse von $\frac{a}{b}$ abgebildet.

Lokale Ringe sind insbesondere wegen der folgenden zwei Sätze interessant.

Satz 10.15 Für einen A -Modul M gilt

$$M = 0 \iff M_{\mathfrak{p}} = 0 \quad \text{für alle Primideale } \mathfrak{p} \subseteq A.$$

Beweis: Für die nicht-triviale Richtung sei $M_{\mathfrak{p}} = 0$ für alle Primideale $\mathfrak{p} \subseteq A$. Sei $x \in M$. Dann ist der **Annulator von x**

$$\text{ann}(x) := \{a \in A \mid ax = 0\}$$

offenbar ein Ideal in A . Gilt $x \neq 0$, so ist $1 \notin \text{ann}(x)$, also $\text{ann}(x)$ ein echtes Ideal in A . Dann gibt es ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $\text{ann}(x) \subseteq \mathfrak{m}$ (siehe Algebra I, Satz 16.8). Wegen $M_{\mathfrak{m}} = 0$ gibt es aber ein $b \notin \mathfrak{m}$ mit $bx = 0$, also $b \in \text{ann}(x)$, Widerspruch!

Corollar 10.16 Ein Homomorphismus von A -Moduln

$$\varphi : M \rightarrow N$$

ist genau dann injektiv (bzw. surjektiv, bzw. bijektiv), wenn dies für alle induzierten Homomorphismen

$$\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}} \quad (\mathfrak{p} \subseteq A \text{ Primideal})$$

(siehe 10.8 (c)) gilt.

Beweis: Sei

$$0 \rightarrow K \rightarrow M \xrightarrow{\varphi} N \rightarrow C \rightarrow 0$$

exakt (also $K = \ker \varphi$ und $C = \text{coker } \varphi$). Nach Satz 10.10 sind dann alle Sequenzen

$$0 \rightarrow K_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \xrightarrow{\varphi_{\mathfrak{p}}} N_{\mathfrak{p}} \rightarrow C_{\mathfrak{p}} \rightarrow 0$$

exakt. Zusammen mit Satz 10.15 folgt die Behauptung (Zum Beispiel: φ injektiv $\Leftrightarrow K = 0 \Leftrightarrow K_{\mathfrak{p}} = 0 \forall \mathfrak{p} \Leftrightarrow \varphi_{\mathfrak{p}}$ injektiv $\forall \mathfrak{p}$).

Satz 10.17 (Krull-Nakayama-Lemma) Sei A ein Ring und $I \subseteq A$ ein Ideal, welches in allen maximalen Idealen von A enthalten ist. Sei M ein A -Modul und $N \subseteq M$ ein Untermodul derart, dass M/N endlich erzeugt ist. Gilt $M = N + IM$, so ist schon $M = N$.

(Die Beziehung $M = N + IM$ sollte so gelesen werden, dass der Homomorphismus $\varphi : N/IN \rightarrow M/IM$ surjektiv ist, d.h., dass $im \varphi = N + IM/IM = M/IM$; es ist also " $M = N$ modulo I ").

Beweis Seien $m_1, \dots, m_t \in M$ derart, dass die Bilder in $\overline{M} := M/N$ ein minimales Erzeugendensystem bilden. Angenommen $t > 0$. Wegen $\overline{M} = I\overline{M}$ gibt es eine Gleichung

$$m_t = \sum_{j=1}^t a_j m_j \quad , \quad \text{mit } a_j \in I, j = 1, \dots, t.$$

Es folgt

$$(1 - a_t)m_t = \sum_{j=1}^{t-1} a_j m_j.$$

Aber $1 - a_t$ ist eine Einheit, denn sonst wäre $(1 - a_t)$ ein echtes Ideal, also $1 - a_t$ in einem maximalen Ideal \mathfrak{m} erhalten, woraus $1 \in \mathfrak{m}$ folgen würde – Widerspruch! Durch Multiplikation mit $(1 - a_t)^{-1}$ folgt, dass \overline{M} schon von m_1, \dots, m_{t-1} erzeugt wird – Widerspruch!

Corollar 10.18 Sei A ein lokaler Ring mit maximalem Ideal \mathfrak{m} und M ein endlich erzeugter A -Modul. Sind $m_1, \dots, m_t \in M$ Elemente, deren Restklassen $\overline{m}_1, \dots, \overline{m}_t$ den Modul $M/\mathfrak{m}M$ erzeugen, so wird M von m_1, \dots, m_t erzeugt.

Beachte: $M/\mathfrak{m}M$ ist ein endlich-dimensionaler Vektorraum über dem Restklassenkörper $k = A/\mathfrak{m}$!

Beweis: Anwendung von Satz 10.17 auf den von m_1, \dots, m_t erzeugten Untermodul $N = \langle m_1, \dots, m_t \rangle_A \subseteq M$ und $I = \mathfrak{m}$.

Bemerkung 10.19 Corollar 11.18 wird im Allgemeinen falsch, wenn M nicht endlich erzeugt ist: Sei p eine Primzahl. Für den $\mathbb{Z}_{(p)}$ -Modul \mathbb{Q} gilt $\mathbb{Q}/(p)\mathbb{Z}_{(p)}\mathbb{Q} = \mathbb{Q}/p\mathbb{Q} = 0$, aber $\mathbb{Q} \neq 0$. Tatsächlich ist \mathbb{Q} auch kein endlich erzeugter $\mathbb{Z}_{(p)}$ -Modul.

§11 Diskrete Bewertungsringe

Diese sind interessant für die (Kommutative) Algebra und die Zahlentheorie.

Definition 11.1 Sei K ein Körper. Eine **diskrete Bewertung** auf K ist eine Abbildung

$$v : K \setminus \{0\} \rightarrow \mathbb{Z}$$

mit den Eigenschaften

- (i) $v(x \cdot y) = v(x) + v(y)$,
- (ii) $v(x + y) \geq \min\{v(x), v(y)\}$,

für alle $x, y \in K \setminus \{0\}$.

Bemerkung 11.2 Offenbar bedeutet (i) gerade, dass $v : K^\times \rightarrow \mathbb{Z}$ ein Gruppenhomomorphismus ist. Ist die Bewertung **nicht-trivial**, d.h., v nicht der Nullhomomorphismus, so ist $im v = n\mathbb{Z}$ für ein eindeutig bestimmtes $n \in \mathbb{N}$, und v heißt **normiert**, wenn $im v = \mathbb{Z}$ ist. Beachte: Ist v nicht-trivial, $im v = n\mathbb{Z}$ mit $n \in \mathbb{N}$, so ist $\frac{1}{n}v$ normiert.

Beispiele 11.3 (a) Für eine Primzahl p definiere die p -adische Bewertung v_p auf \mathbb{Q} durch

$$v_p(x) = n_p,$$

falls

$$x = \pm \prod_q q^{n_q} \quad (n_q \in \mathbb{Z}, \text{ fast alle null})$$

die Primfaktorzerlegung von x ist (q läuft über alle Primzahlen). Zum Beispiel ist $v_3(12) = 1$, $v_2(12) = 2$, $v_p(12) = 0$ für $p > 3$. Für jedes p ist v_p eine normierte diskrete Bewertung auf \mathbb{Q} (Übungsaufgabe!).

(b) Sei k ein Körper und $k[x]$ der Polynomring. Für $f = \frac{p(x)}{q(x)} \in k(x)^\times$ setze

$$v_\infty(f) = -\deg p(x) + \deg q(x),$$

wobei $\deg p(x)$ der Grad eines Polynoms $p(x)$ ist. Dies ist eine normierte diskrete Bewertung auf $k(x)$ (Übungsaufgabe!).

Lemma/Definition 11.4 Sei v eine nicht-triviale diskrete Bewertung auf dem Körper K . Dann ist

$$(11.4.1) \quad A_v = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$$

ein lokaler Ring und heißt der **Bewertungsring von v** . Das maximale Ideal von A_v ist

$$(11.4.2) \quad \mathfrak{p}_v = \{x \in K^\times \mid v(x) > 0\} \cup \{0\},$$

und es ist

$$(11.4.3) \quad A_v^\times = \{x \in K^\times \mid v(x) = 0\}$$

die Gruppe der Einheiten von A_v .

Beweis der Behauptungen: Für $x, y \in K \setminus \{0\}$ mit $v(x), v(y) \geq 0$ ist $v(xy) = v(x)v(y) \geq 0$ und $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$. Hieraus folgt leicht, dass A_v ein Unterring von K ist (Fallunterscheidung für $x=0$ oder $y=0$). Ebenso sieht man, dass \mathfrak{p}_v ein Ideal in A_v ist. Weiter sieht man wegen der Homomorphieeigenschaft von v sofort, dass (11.4.3) gilt ($xy=1 \Rightarrow v(x)+v(y)=v(1)=0$). Zusammen mit (11.4.2) folgt $\mathfrak{p}_v = A_v \setminus A_v^\times$; mit 10.12 (ii) folgt also, dass A_v lokal mit maximalem Ideal \mathfrak{p}_v ist.

Beispiele 11.5 (a) Der Bewertungsring zur p -adischen Bewertung v_p auf \mathbb{Q} ist

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b \right\},$$

mit maximalem Ideal $p\mathbb{Z}_{(p)}$.

(b) Der Bewertungsring zur Grad-Bewertung v_∞ auf $k(x)$ (siehe 11.3 (b)) ist

$$A_\infty = \left\{ \frac{p(x)}{q(x)} \in k(x) \mid \deg q \geq \deg p \right\}.$$

(c) Ist $v : K^\times \rightarrow \mathbb{Z}$ eine nicht-triviale diskrete Bewertung und \tilde{v} die zugehörige normierte Bewertung (siehe Bemerkung 11.2), so ist $A_v = A_{\tilde{v}}$.

Definition 11.6 Ein Integritätsring A heißt **diskreter Bewertungsring**, wenn es eine diskrete Bewertung v auf $K = \text{Quot}(A)$ gibt, so dass $A = A_v$, der Bewertungsring von v .

Beispiele 11.7 Nach Beispiel 11.5 (a) ist für jede Primzahl p der Ring $\mathbb{Z}_{(p)}$ ein diskreter Bewertungsring.

Satz 11.8 Für einen Integritätsring A sind äquivalent:

- (a) A ist diskreter Bewertungsring.
- (b) A ist lokal und ein Hauptidealring.

Beweis (a) \Rightarrow (b): Sei $A = A_v$ für die diskrete Bewertung v auf K . Ohne Einschränkung sei v normiert (Bemerkung 11.5 (c)). Nach 11.4 ist A_v ein lokaler Ring. Sei $\pi \in A$ ein Element mit $v(\pi) = 1$ und sei $\mathfrak{a} \subseteq A$ ein Ideal. Sei

$$m = \min\{v(x) \mid x \in \mathfrak{a}\} \in \mathbb{N}_0$$

(Beachte: $v(x) \geq 0$ für alle $x \in A$). Dann gilt

$$(11.8.1) \quad \mathfrak{a} = (\pi^m).$$

Sei nämlich $x \in \mathfrak{a} \setminus \{0\}$. Dann ist $n := v(x) \geq m$ und für $u := x \cdot \pi^{-n} \in K^\times$ gilt $v(u) = v(x) + v(\pi^{-n}) = n - n = 0$. Also ist $u \in A^\times$ eine Einheit und

$$x = u \cdot \pi^n \in (\pi^m)$$

wegen $n \geq m$.

Umgekehrt gibt es nach Definition von m ein $y \in \mathfrak{a}$ mit $v(y) = m$, und wie eben folgt $y = v\pi^m$ mit einer Einheit $v \in A^\times$. Es folgt $\pi^m = v^{-1}y \in \mathfrak{a}$ und damit $(\pi^m) \subseteq \mathfrak{a}$.

(b) \Rightarrow (a): Sei A ein lokaler Hauptidealring. Das eindeutig bestimmte maximale Ideal $\mathfrak{m} \subseteq A$ ist dann ein Hauptideal; etwa $\mathfrak{m} = (\pi)$ für ein Element $\pi \in A$. Dann ist π ein Primelement. Ist π' ein weiteres Primelement in A , so ist (π') ein maximales Ideal (da A ein Hauptidealring ist, siehe Algebra I, Lemma 6.17), also gleich $\mathfrak{m} = (\pi)$, da A nur ein maximales Ideal hat. Also sind π' und π assoziiert. Es gibt also bis auf Assoziiertheit nur das Primelement π . Da A ein faktorieller Ring ist (Algebra I, Satz 6.18), gilt für jedes $x \in A \setminus \{0\}$

$$(11.8.2) \quad x = u \cdot \pi^n$$

mit einem eindeutig bestimmten $n \in \mathbb{N}_0$ und einer (eindeutig bestimmten) Einheit u . Entsprechend gilt dies für jedes $x \in K^\times$, wobei $n \in \mathbb{Z}$. Definiere nun die Abbildung $v : K^\times \rightarrow \mathbb{Z}$ durch

$$(11.8.3) \quad v(x) = n \quad \text{falls (11.8.2) gilt.}$$

Dann ist v eine diskrete Bewertung (siehe Übungsaufgabe 39). Weiter gilt offenbar $x \in A \setminus \{0\} \Leftrightarrow v(x) \geq 0$, also $A = A_v$.

Bemerkung 11.9 Sei A ein diskreter Bewertungsring.

(a) Ist v eine normierte diskrete Bewertung auf $K = \text{Quot}(A)$ mit $A = A_v$, so ist v eindeutig bestimmt. Sei nämlich v' eine zweite solche Bewertung und seien $\pi, \pi' \in A$ Elemente mit $v(\pi) = 1 = v'(\pi')$. Dann gilt nach dem Beweis von 11.8 (siehe (11.8.1)) $(\pi) = \mathfrak{m} = (\pi')$ für das maximale Ideal $\mathfrak{m} \subseteq A$, also $\pi' = u\pi$ für eine Einheit $u \in A^\times$, und damit $v(x) = v'(x)$ für alle $x \in K^\times$ (warum?).

(b) Jedes Element $\pi \in A$ mit $(\pi) = \mathfrak{m}$ (also mit $v(\pi) = 1$ für die eindeutig bestimmte normierte diskrete Bewertung v zu A) heißt **Primelement von A** (oder **Primelement für v**).

Beispiele 11.10 Ist p eine Primzahl, so ist p ein Primelement für die p -adische Bewertung v_p auf \mathbb{Q} .

§12 Das Tensorprodukt

Sei R ein kommutativer Ring mit Eins.

Satz/Definition 12.1 (a) Für zwei R -Moduln M, N gibt es einen bis auf eindeutige Isomorphie eindeutig bestimmten R -Modul $M \otimes_R N$, genannt das **Tensorprodukt** von M und N , mit der folgenden universellen Eigenschaft:

Es gibt eine R -bilineare Abbildung $\psi_{univ} : M \times N \rightarrow M \otimes_R N$ derart, dass für jede R -bilineare Abbildung $\psi : M \times N \rightarrow P$ in einem R -Modul P ein eindeutig bestimmter R -Modul-Homomorphismus $\tilde{\psi} : M \otimes_R N \rightarrow P$ existiert mit $\psi = \tilde{\psi} \circ \psi_{univ}$, d.h., so dass das Diagramm:

$$(12.1.1) \quad \begin{array}{ccc} M \times N & \xrightarrow{\psi_{univ}} & M \otimes_R N \\ & \searrow \psi & \swarrow \exists! \tilde{\psi} \\ & P & \end{array}$$

kommutativ ist. Das Element $\psi_{univ}((m, n))$ wird mit $m \otimes n$ bezeichnet.

(b) Jedes Element in $M \otimes_R N$ ist von der Form

$$\sum_{i=1}^k m_i \otimes n_i$$

für ein $k \in \mathbb{N}$ und $m_1, \dots, m_k \in M, n_1, \dots, n_k \in N$.

(c) Es gilt:

$$(12.1.2) \quad \begin{aligned} (m + m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n + n') &= m \otimes n + m \otimes n' \\ rm \otimes n &= r(m \otimes n) = m \otimes rn \end{aligned}$$

Zum Beweis: Man kann $M \otimes_R N$ durch "Erzeugende und Relationen" definieren, nämlich durch

$$M \otimes_R N = F_R(M \times N) / U ,$$

wobei $F_R(M \times N)$ der freie R -Modul auf $M \times N$ ist (siehe 4.5) und

$$U = \langle (rm + r'm', n) - r(m, n) - r'(m', n), (m, sn + s'n') - s(m, n) - s'(m, n') \rangle$$

der von den angegebenen Elementen (mit $m, m' \in M, n, n' \in N$ und $r, r', s, s' \in R$) erzeugte Untermodul. Wir schreiben hier zur Vereinfachung auch (m, n) für das zu (m, n) gehörige Basiselement von $F_R(M \times N)$. Durch das Herausdividieren von U , also der richtigen "Relationen", wird gerade erreicht, dass die Abbildung

$$\begin{aligned} \psi_{univ} : M \times N &\rightarrow F_R(M \times N) \rightarrow F_R(M \times N)/U \\ (m, n) &\mapsto (m, n) \mapsto m \otimes n := \text{Klasse von } (m, n) \end{aligned}$$

bilinear ist, und die universelle Eigenschaft ergibt sich aus der universellen Eigenschaft von $F_R(M \times N)$. Die Aussage in (b) folgt aus der Konstruktion, und (c) ist gerade die Bilinearität von ψ_{univ} . Die Details seien dem Leser überlassen.

Im Folgenden braucht man nur die in 12.1 stehenden Eigenschaften, nicht die Konstruktion des Tensorproduktes! Dies gilt zum Beispiel für den Beweis von

Proposition 12.2 Es gibt kanonische Isomorphismen für R -Moduln M, N, P :

- (a) $R \otimes_R M \cong M$
- (b) $M \otimes_R N \cong N \otimes_R M$
- (c) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$.

Beweis von (b): Wir haben eine Abbildung

$$\begin{aligned} M \otimes_R N &\rightarrow N \otimes_R M \\ m \otimes n &\mapsto n \otimes m \quad \text{für } m \in M, n \in N. \end{aligned}$$

Dies soll heißen: diese Abbildung ist wohldefiniert, weil sie aufgrund der universellen Eigenschaft von der bilinearen (folgt mit 12.1 (c)!) Abbildung

$$\begin{aligned} M \times N &\rightarrow M \otimes_R N \\ (m, n) &\mapsto n \otimes m \end{aligned}$$

induziert wird. Die Umkehrabbildung ist dann die analoge Abbildung

$$\begin{aligned} N \otimes_R M &\rightarrow M \otimes_R N \\ n \otimes m &\mapsto m \otimes n. \end{aligned}$$

Um dies nachzurechnen, braucht man nur die Verknüpfung auf den Erzeugenden $m \otimes n$ auszurechnen, wo die Behauptung trivial ist.

Entsprechend werden die Isomorphismen in (a) und (c) "gegeben" durch

$$r \otimes m \mapsto rm$$

(mit Umkehrabbildung $m \mapsto 1 \otimes m$) beziehungsweise

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

(mit Umkehrabbildung $m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p$).

Lemma 12.3 Für R -Moduln M, N werden die Mengen

$$\text{Abb}(M, N) := \text{Menge aller Abbildungen } f : M \rightarrow N$$

$$\text{Hom}_R(M, N) := \{f : M \rightarrow N \mid f \text{ } R\text{-Modul-Homomorphismus}\}$$

zu R -Moduln vermöge der Definition

$$\begin{aligned} (f + g)(m) &= f(m) + g(m) \\ (rf)(m) &= r(f(m)) \end{aligned}$$

$\text{Hom}_R(M, N)$ ist ein Untermodul von $\text{Abb}(M, N)$.

Beweis selbst.

Satz 12.4 Für R -Moduln M, N, P gibt es einen kanonischen R -Modul-Isomorphismus

$$\text{Hom}_R(M, \text{Hom}_R(N, P)) \cong \text{Hom}_R(M \otimes_R N, P)$$

Beweis: Sei $\text{Bil}_R(M, N, P)$ die Menge der R -bilinearen Abbildungen von $M \times N$ nach P . Dies ist ein Untermodul von $\text{Abb}(M \times N, P)$ (nachrechnen!) und man erhält eine Bijektion

$$\begin{aligned} \Psi : \text{Hom}_R(M, \text{Hom}_R(N, P)) &\xrightarrow{\sim} \text{Bil}_R(M, N, P) \\ \phi &\mapsto (\psi_\phi : (m, n) \mapsto \phi(m)(n)) \end{aligned}$$

(ψ_ϕ ist offenbar bilinear!). Die Umkehrabbildung ist nämlich

$$(\phi_\psi : m \mapsto (n \mapsto \psi(m, n))) \leftarrow \psi$$

($n \mapsto \psi(m, n)$ und ϕ_ψ sind R -linear!).

Weiter ist die Bijektion Ψ R -linear: $r\phi + r'\phi'$ wird auf die Abbildung

$$\begin{aligned} (m, n) &\mapsto (r\phi + r'\phi')(m)(n) \\ &= (r\phi(m) + r'\phi'(m))(n) \\ &= r(\phi(m)(n)) + r'(\phi'(m)(n)) \end{aligned}$$

abgebildet, also auf $r\psi_\phi + r'\psi_{\phi'}$.

Durch Verknüpfung mit der Bijektion (universelle Eigenschaft des Tensorproduktes)

$$\text{Bil}_R(M, N, P) \xrightarrow{\sim} \text{Hom}_R(M \otimes_R N, P), \quad \psi \mapsto \tilde{\psi},$$

die ebenfalls R -linear ist (mit der universellen Eigenschaft nachrechnen!) erhält man den gewünschten Isomorphismus von R -Moduln.

Wir betrachten im Folgenden immer kommutative Ringe mit Eins.

Bemerkung 12.5 (Vergleiche mit Algebra I, Definition 16.3) Sei $\varphi : A \rightarrow B$ ein Ringhomomorphismus. Dann wird B zu einem A -Modul durch die Verknüpfung

$$ab := \varphi(a) \cdot b \quad \text{für } a \in A, b \in B.$$

Die Schreibweise ab bedeutet im folgenden immer diese Verknüpfung. Genauer gesagt wird B hierdurch zu einer A -Algebra, d.h., einem Ring mit einer A -Modul-Struktur derart, dass die Addition im Ring B und A -Modul B übereinstimmt und dass

$$(ab) \cdot b' = a(b \cdot b') \quad (aa')b = a(a'b)$$

für alle $a, a' \in A$ und $b, b' \in B$, wobei hier der Punkt für die Ringmultiplikation in B steht, aber im Folgenden auch meist weggelassen wird. Hat man umgekehrt eine A -Algebra B , so erhält man einen Ringhomomorphismus (von Ringen mit Eins)

$$\varphi : A \rightarrow B, \quad a \mapsto a1_B$$

und die Konstruktionen sind zueinander invers.

Lemma/Definition 12.6 Sei $\varphi : A \rightarrow B$ ein Ringhomomorphismus und M ein A -Modul. Dann wird

$$B \otimes_A M$$

in eindeutiger Weise zu einem B -Modul, so dass gilt:

$$(12.6.1) \quad b' \cdot (b \otimes m) := b'b \otimes m \quad (\text{für } b, b' \in B, m \in M).$$

$B \otimes_A M$ mit dieser Struktur heißt die **Skalarerweiterung** von M (mit φ oder zu B).

Beweis: Wohldefiniertheit: Zu b' definiere die Abb.

$$\begin{aligned} \psi_{b'} &: B \times M \rightarrow B \otimes_A M \\ (b, m) &\mapsto b'b \otimes m \end{aligned}$$

Diese ist A -bilinear und definiert also eine A -lineare Abb.

$$\begin{aligned} \tilde{\psi}_{b'} &: B \otimes_A M \rightarrow B \otimes_A M \\ \text{mit } b \otimes m &\mapsto b'b \otimes m, \end{aligned}$$

die wir als die Multiplikation mit b' definieren; es sei also $b'y = \tilde{\psi}_{b'}(y)$ für $y \in B \otimes_A M$. Die Modulaxiome sind neben der Additivität von $\tilde{\psi}_{b'}$ die Eigenschaften

$$\tilde{\psi}_1 = id, \quad \tilde{\psi}_{(b'+b'')} = \tilde{\psi}_{b'} + \tilde{\psi}_{b''} \quad \text{und} \quad \tilde{\psi}_{(b'' \cdot b')} = \tilde{\psi}_{b''} \circ \tilde{\psi}_{b'}$$

und diese gelten, weil sie für die ψ 's gelten. Die Eigenschaft (12.6.1) macht die Verknüpfung eindeutig, weil die $b \otimes m$ Erzeugende von $B \otimes_A M$ sind.

Proposition 12.7 Seien $\varphi : A \rightarrow B$ und $\psi : A \rightarrow C$ Ringhomomorphismen. Dann hat $B \otimes_A C$ eine eindeutig bestimmte A -Algebren-Struktur, für die gilt:

$$(12.7.1) \quad b \otimes c \cdot b' \otimes c' = bb' \otimes cc'$$

Beweis: Nur die Wohldefiniertheit ist zu zeigen! Nach Konstruktion ist $B \otimes_A C$ ein A -Modul.

Nach 12.6 wird $B \otimes_A C$ ein B -Modul mit $b(b' \otimes c') = bb' \otimes c'$ für $b, b' \in B$ und $c' \in C$.

Analog wird $B \otimes_A C$ ein C -Modul (Operation rechts geschrieben), wobei $(b' \otimes c') \cdot c = b' \otimes c'c$. Weiter ist

$$\begin{aligned} B \times C &\rightarrow \text{Hom}_A(B \otimes_A C, B \otimes_A C) \\ (b, c) &\mapsto (\alpha \mapsto b\alpha c) \end{aligned}$$

A -bilinear, induziert also nach Satz 12.1 (a) eine A -lineare Abbildung

$$\psi : B \otimes_A C \rightarrow \text{Hom}_A(B \otimes_A C, B \otimes_A C),$$

nach (dem Beweis von) Satz 12.4 also eine A -bilineare Verknüpfung

$$\begin{aligned} B \otimes_A C \times B \otimes_A C &\rightarrow B \otimes_A C. \\ (\alpha, \beta) &\mapsto \alpha \cdot \beta := \psi(\alpha)(\beta) \end{aligned}$$

für die (12.7.1) gilt:

$$(b \otimes c) \cdot (b' \otimes c') = \psi(b \otimes c)(b' \otimes c') = bb' \otimes cc'$$

Hieraus folgt, dass $B \otimes_A C$ ein kommutativer Ring mit eins 1 wird (nachrechnen!).

Satz 12.8 (a) Die Abbildungen

$$\begin{aligned} i_B : B &\rightarrow B \otimes_A C & b &\mapsto b \otimes 1 \\ i_C : C &\rightarrow B \otimes_A C & c &\mapsto 1 \otimes c \end{aligned}$$

sind Ringhomomorphismen, und das folgende Diagramm ist kommutativ:

$$\begin{array}{ccc} & B & \\ \varphi \nearrow & & \searrow i_B \\ A & & B \otimes_A C \\ \psi \searrow & & \nearrow i_C \\ & C & \end{array} .$$

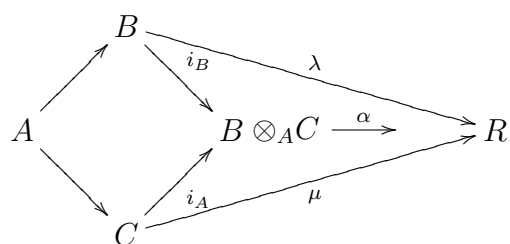
(b) (universelle Eigenschaft) Ist

$$\begin{array}{ccc} & B & \\ \varphi \nearrow & & \searrow \lambda \\ A & & R \\ \psi \searrow & & \nearrow \mu \\ & C & \end{array}$$

ein kommutatives Diagramm von Ringhomomorphismen, so gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\alpha : B \otimes_A C \rightarrow R$$

der das Diagramm



kommutativ macht.

Beweis: (a): klar.

(b) Die Abbildung

$$\begin{aligned}
 \lambda \cdot \mu : B \times C &\rightarrow R \\
 (b, c) &\mapsto \lambda(b) \cdot \mu(c)
 \end{aligned}$$

ist A -bilinear und induziert daher nach 2.4. einen eindeutig bestimmten Morphismus von A -Moduln

$$\alpha : B \otimes_A C \longrightarrow R$$

Dieser leistet das Gewünschte (nachrechnen!).

Wir zeigen nun eine Exaktheitsaussage für das Tensorprodukt. Wenn der Grundring R klar ist, schreiben wir auch nur \otimes für \otimes_R .

Vorbemerkung 12.9 Für Morphismen von R -Moduln $f : M_1 \rightarrow M_2$ und $g : N_1 \rightarrow N_2$ hat man einen kanonischen Morphismus von R -Moduln

$$\begin{aligned}
 f \otimes g : M_1 \otimes N_1 &\rightarrow M_2 \otimes N_2 \\
 m_1 \otimes n_1 &\mapsto f(m_1) \otimes g(n_1),
 \end{aligned}$$

entsprechend der bilinearen Abbildung $(m_1, n_1) \mapsto f(m_1) \otimes g(n_1)$.

Insbesondere hat man für jeden R -Modul N eine kanonische Abbildung

$$f_* = f \otimes id_N : M_1 \otimes N \rightarrow M_2 \otimes N$$

(Man sagt hierzu, das Tensorprodukt ist “funktoriell”).

Der folgende Satz ist extrem nützlich für das Rechnen mit Tensorprodukten.

Satz 12.10 (Rechtsexaktheit des Tensorproduktes) Ist

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0$$

eine exakte Sequenz von R -Moduln, so ist für jeden R -Modul N auch die Sequenz

$$M_1 \otimes_R N \xrightarrow{f_*} M_2 \otimes_R N \xrightarrow{g_*} M_3 \otimes_R N \rightarrow 0$$

exakt, wobei $f_* = f \otimes id_N$ und $g_* = g \otimes id_N$ wie in 12.9.

Beweis: (1) g_* ist surjektiv: $M_3 \otimes_R N$ wird erzeugt von Elementen $m_3 \otimes n$ mit $m_3 \in M, n \in N$. Für m_3 existiert $m_2 \in M_2$, mit $g(m_2) = m_3$. Dann ist $m_3 \otimes n = g_*(m_2 \otimes n)$.

(2) im $f_* \subseteq \ker g_*$: Es ist $g_* \circ f_* = g \circ f \otimes id_N = 0$.

(3) im $f_* \supseteq \ker g_*$: Sei $\varphi : M_2 \otimes_R N \rightarrow \text{coker } f_*$ die kanonische (surjektive) Abbildung. Wir konstruieren nun eine Abbildung $\psi : M_3 \otimes N \rightarrow \text{Coker } f_*$, die das Diagramm

$$\begin{array}{ccc} M_2 \otimes N & \xrightarrow{\varphi} & \text{Coker } f_* \\ & \searrow g_* & \uparrow \psi \\ & & M_3 \otimes N \end{array}$$

kommutativ macht ($\psi g_* = \varphi$). Dann folgt $\ker g_* \subseteq \ker \varphi = \text{im } f_*$.

Nach Definition ist $\varphi \circ f_* = 0$. Definiere nun eine bilineare Abbildung

$$b : M_3 \times N \rightarrow \text{coker } f_*, (m_3, n) \mapsto \varphi(m_2 \otimes n),$$

wobei $m_2 \in M_2$ mit $g(m_2) = m_3$. Ein solches m_2 existiert, da g surjektiv ist. Weiter ist b wohldefiniert: Ist $m'_2 \in M_2$ mit $g(m'_2) = m_3 = g(m_2)$, so ist $m_2 - m'_2 \in \ker g = \text{im } f$, also $m_2 - m'_2 = f(m_1)$ für ein $m_1 \in M_1$. Es folgt

$$m_2 \otimes n - m'_2 \otimes n = f(m_1) \otimes n = f_*(m_1 \otimes n),$$

also $\varphi(m_2 \otimes n) = \varphi(m'_2 \otimes n)$ wegen $\varphi f_* = 0$.

Die bilineare Abbildung b induziert nun einen R -Modul-Homomorphismus

$$\psi : M_3 \otimes_R N \rightarrow \text{coker } f_* .$$

Nach Konstruktion gilt dabei für $m_2 \in M_2$ und $n \in N$

$$(\psi \circ g_*)(m_2 \otimes n) = \psi(g(m_2) \otimes n) = b(g(m_2), n) = \varphi(m_2 \otimes n) .$$

Also ist $\psi \circ g_* = \varphi$.

Bemerkung 12.11 Die Sequenz

$$0 \rightarrow M_1 \otimes_R N \rightarrow M_2 \otimes_R N \rightarrow M_3 \otimes_R N \rightarrow 0$$

ist im Allgemeinen nicht an der Stelle $M_1 \otimes_R N$ exakt (das Tensorprodukt ist nur rechtsexakt und nicht exakt). Ein Gegenbeispiel ist das Folgende: Wir haben eine exakte Sequenz von \mathbb{Z} -Moduln

$$0 \rightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0 ,$$

wobei $\cdot n$ die Multiplikation mit der natürlichen Zahl n bedeutet. Tensorieren wir dies mit $\mathbb{Z}/n\mathbb{Z}$, so erhalten wir vermöge der Isomorphismen $\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ die exakte Sequenz

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$$

wobei $\cdot n$ die Nullabbildung, also nicht injektiv für $n \neq 1$ ist.

Die Rechtsexaktheit reicht aber für folgende Anwendung:

Corollar 12.12 Sei M ein R -Modul, und $\mathfrak{a} \subseteq R$ ein Ideal. Dann gibt es einen kanonischen Isomorphismus (von R - bzw. auch von R/\mathfrak{a} -Moduln)

$$R/\mathfrak{a} \otimes_R M \cong M/\mathfrak{a}M,$$

wobei $\mathfrak{a}M = \left\{ \sum_{i=1}^n a_i m_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, m_i \in M \right\}$.

Beweis: Nach Definition ist

$$0 \rightarrow \mathfrak{a} \rightarrow R \rightarrow R/\mathfrak{a} \rightarrow 0$$

exakt. Daher ist

$$\mathfrak{a} \otimes_R M \rightarrow R \otimes_R M \rightarrow R/\mathfrak{a} \otimes M \rightarrow 0$$

exakt. Vermöge der Isomorphie $R \otimes_R M \cong M$ erhalten wir eine exakte Sequenz

$$\mathfrak{a} \otimes_R M \xrightarrow{\psi} M \rightarrow R/\mathfrak{a} \otimes M \rightarrow 0$$

$$a \otimes m \mapsto a \cdot m, m \mapsto 1 \otimes m,$$

die die Behauptung zeigt: Offenbar ist $\text{im } \psi = \mathfrak{a}M$.

Eine weitere nützliche Eigenschaft für das Tensorprodukt ist:

Lemma 12.13 Ist $(M_i)_{i \in I}$ eine Familie von R -Moduln und N ein weiterer R -Modul, so gibt es einen kanonischen R -Modul-Isomorphismus

$$\begin{aligned} \left(\bigoplus_{i \in I} M_i \right) \otimes N &\xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes N), \\ \text{mit } (m_i) \otimes n &\mapsto (m_i \otimes n). \end{aligned}$$

Beweis Die Abbildung ergibt sich mittels der universellen Eigenschaft des Tensorprodukts aus der R -bilinearen Abbildung

$$((m_i)_{i \in I}, n) \mapsto (m_i \otimes n)_{i \in I}.$$

Die Umkehrabbildung ist definiert durch die universelle Eigenschaft der direkten Summe und die Abbildungen

$$M_i \otimes N \rightarrow \left(\bigoplus_{i \in I} M_i \right) \otimes N,$$

die durch $m_i \otimes n \mapsto \varphi_i(m_i) \oplus n$ "definiert sind", wobei $\varphi_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$ der kanonische Monomorphismus ist, mit $\varphi_j(m_j) = (n_i)_{i \in I}$, wobei $n_j = m_j$ und $n_i = 0$ für $i \neq j$.

Corollar 12.14 Sei I eine Menge und $R \rightarrow S$ ein Ringhomomorphismus. Für die Skalarerweiterung zu S des freien R -Moduls $F_R(I)$ über I gibt es einen kanonischen Isomorphismus von S -Moduln

$$\begin{aligned} S \otimes_R F_R(I) &\xrightarrow{\sim} F_S(I) \\ \text{mit } s \otimes e_i &\mapsto s e_i \end{aligned}$$

für die kanonische Basis $(e_i)_{i \in I}$ von $F_R(I)$ bzw. $F_S(I)$.

Beweis Wir haben die Isomorphismen

$$S \otimes_R F_R(I) = S \otimes_R \left(\bigoplus_{i \in I} Re_i \right) \xrightarrow{12.13} \bigoplus_{i \in I} S \otimes_R Re_i \xrightarrow{12.2(a)} \bigoplus_{i \in I} Se_i = F_S(I).$$

Bemerkungen 12.15 (a) Aus 12.10 folgt auch: Ist

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \rightarrow 0$$

eine exakte Sequenz von R -Moduln, so ist für jeden R -Modul N auch

$$(12.15.1) \quad M_1 \otimes N \xrightarrow{f_*} M_2 \otimes N \xrightarrow{g_*} M_3 \otimes N \rightarrow 0$$

exakt. Sei nämlich $M'_1 = \text{im } f = \ker g$. Dann ist nach 12.10

$$M'_1 \otimes N \rightarrow M_2 \otimes N \rightarrow M_3 \otimes N \rightarrow 0$$

exakt. Zusammen mit der Surjektivität von

$$M_1 \otimes N \rightarrow M'_1 \otimes N$$

folgt die Exaktheit von (12.15.1).

(b) Mit 12.10 und 12.14 kann man wie folgt Tensorprodukte “verstehen”. Für jeden R -Modul M hat durch die Wahl von Erzeugenden m_i ($i \in I$) eine Surjektion $F_R(I) \xrightarrow{\varphi} M$, $e_i \mapsto m_i$. Wendet man dies nochmals auf $\ker \varphi$ an, so erhält man eine exakte Sequenz

$$F_R(J) \rightarrow F_R(I) \xrightarrow{\varphi} M \rightarrow 0.$$

Dies nennt man eine **Präsentation** des Moduls M ; man beschreibt M durch Erzeugende (die m_i) und Relationen (die Erzeugenden von $\ker \varphi$). Ist nun $R \rightarrow S$ ein Ringhomomorphismus, so ist nach 12.10

$$S \otimes_R F_R(J) \rightarrow S \otimes_R F_R(I) \rightarrow S \otimes_R M \rightarrow 0$$

exakt, und dies lässt sich nach 12.14 schreiben als

$$F_S(I) \rightarrow F_S(J) \rightarrow S \otimes_R M \rightarrow 0.$$

$S \otimes_R M$ hat also “dieselben Erzeugenden und Relationen”, allerdings nun in freien S -Moduln, d.h., wir bilden die auftretenden Koeffizienten $a_i \in R$, $b_j \in R$ durch $R \rightarrow S$ in S ab.

(c) Für Polynome $f_1, \dots, f_m \in R[X_1, \dots, X_n]$ ist also zum Beispiel

$$S \otimes_R (R[X_1, \dots, X_n]/(f_1, \dots, f_m)) \cong S[X_1, \dots, X_n]/(f_1, \dots, f_m),$$

wobei die Polynome rechts in $S[X_1, \dots, X_n]$ aufgefasst sind.

Wir beschließen diesen Abschnitt mit der folgenden Beobachtung.

Satz 12.16 Sei A ein Ring, $S \subseteq A$ eine multiplikative Teilmenge und M ein A -Modul. Dann ist der Homomorphismus von A_S -Moduln

$$\begin{array}{l} A_S \otimes_A M \rightarrow M_S \\ \text{mit } \alpha \otimes m \mapsto \alpha \cdot \frac{m}{1} \end{array}$$

ein Isomorphismus.

Beweis Die Umkehrabbildung ist

$$\frac{1}{s} \otimes m \mapsto \frac{m}{s}.$$

Beispiel 12.17 Für eine abelsche Gruppe A ist der \mathbb{Q} -Vektorraum $A_{\mathbb{Q}}$ aus Beispiel 10.11 (b) (und Übungsaufgabe 26) also gleich $\mathbb{Q} \otimes_{\mathbb{Z}} A$. Entsprechend ist für jeden Integritätsring R mit Quotientenkörper K und für jeden R -Modul M

$$M_{(0)} = K \otimes_R M =: M_K$$

(und $rg M = \dim_K M_K$).

§13 Ganze Ringerweiterungen

Der folgende Begriff verallgemeinert den Begriff algebraischer Körpererweiterungen auf Ringe. Sei A ein Ring.

Definition 13.1 (a) Ein A -Modul M heißt endlich erzeugt (oder auch endlicher A -Modul), wenn er ein endliches Erzeugendensystem m_1, \dots, m_n besitzt (d.h., es ist $M = \{\sum_{i=1}^n a_i m_i \mid a_i \in A, i = 1, \dots, n\}$).

(b) Eine A -Algebra B heißt endlich (über A), wenn B als A -Modul endlich erzeugt ist.

Beispiele 13.2 (a) Ein Vektorraum V über einem Körper K ist genau dann ein endlicher K -Modul, wenn er endliche Dimensionen hat.

(b) Der Polynomring $A[X]$ ist keine endliche A -Algebra.

(c) Ist B eine endliche A -Algebra und C eine endliche B -Algebra, so ist C auch endliche A -Algebra.

(d) Ein A -Modul M ist genau dann endlich erzeugt, wenn es eine Surjektion

$$\psi : A^n \twoheadrightarrow M$$

von A -Moduln gibt.

Lemma/Definition 13.3 Sei B eine A -Algebra.

(a) Ein Element $b \in B$ heißt ganz über A , wenn die folgenden äquivalenten Bedingungen erfüllt sind.

(i) Es gibt ein normiertes Polynom

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in A[x]$$

mit $f(b) = 0$ in B , d.h., eine ‘Ganzheitsgleichung’

$$(13.3.1) \quad b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0 \quad \text{mit } a_0, \dots, a_{n-1} \in A.$$

(ii) $A[b] = \left\{ \sum_{i=0}^r \alpha_i b^i \mid r \in \mathbb{N}_0, \alpha_0, \dots, \alpha_r \in A \right\} \subset B$ ist eine endliche A -Algebra.

(iii) Es gibt einen treuen $A[b]$ -Modul M , der ein endlicher A -Modul ist. (Ein Modul M über einem Ring R heißt *treu*, wenn für jedes $r \in R$ gilt: aus $r \cdot m = 0$ für alle $m \in M$ folgt: $r = 0$).

(b) B heißt ganz über A , wenn jedes $b \in B$ ganz über A ist.

Beweis: der Äquivalenzen in (a):

(i) \Rightarrow (ii): Es gelte (13.3.1). Für jedes $q \in \mathbb{N}_0$ sei M_q der von $1, b, \dots, b^{n+q}$ erzeugte A -Untermodul von B . Dann ist für alle $q \geq 1$

$$b^{n+q} = -a_{n-1}b^{n+q-1} - \dots - a_1b^{1+q} - a_0b^q \in M_{q-1}.$$

Durch Induktion folgt

$$M_q = M_{q-1} \dots = M_0$$

und daher (ii).

(ii) \Rightarrow (iii) ist trivial, da $A[b]$ treuer $A[b]$ -Modul ist.

(iii) \Rightarrow (i): Seien m_1, \dots, m_n A -Erzeugende von M . Dann gibt es $a_{ij} \in A$ mit

$$b m_i = \sum_{j=1}^n a_{ij} m_j \quad \text{für alle } i = 1, \dots, n.$$

Für die $(n \times n)$ -Matrix $C = (b \cdot \delta_{ij} - a_{ij}) \in M_n(A[b])$ gilt also $C \underline{m} = 0$ für den Vektor $\underline{m} \in M^n$ mit Komponenten m_1, \dots, m_n . Für $d = \det C$ gilt dann

$$d m_i = 0 \quad \text{für alle } i = 1, \dots, n.$$

Dies folgt aus der *Cramerschen Regel*: Entsteht C_{ij} aus C durch Streichen der i -ten Zeile und j -ten Spalte, und ist $C' = ((-1)^{i+j} \det C_{ij})$ die sogenannte adjungierte Matrix, so zeigt man wie in der linearen Algebra, dass

$$C' \cdot C = (\det C) \cdot E,$$

wobei E die $(n \times n)$ -Einheitsmatrix ist.

Da m_1, \dots, m_n ganz M erzeugen, folgt $dm = 0$ für alle $m \in M$. Da M treuer $A[b]$ -Modul ist, folgt $d = 0$; also ist b Nullstelle des normierten Polynoms

$$p(x) = \det(E \cdot x - (a_{ij})) .$$

Beispiele 13.4 (a) Ist L/K eine Körpererweiterung, so ist L/K genau dann ganz, wenn L/K algebraisch ist (nach 13.3 (i)).

(b) $K[x]/K$ ist nicht ganz (x ist nicht ganz nach 13.3 (ii)).

(c) Jede endliche A -Algebra B ist ganz über A (benutze 13.3 (iii): B ist treuer $A[b]$ -Modul für alle $b \in B$).

Definition 13.5 Sei B eine A -Algebra. Für $b_1, \dots, b_n \in B$ sei $A[b_1, \dots, b_n] \subseteq B$ die von den b_i erzeugte A -Unteralgebra.

Offenbar ist $A[b_1, \dots, b_n] =$ Menge aller über A polynomialen Ausdrücke in den $b_i = \{f(b_1, \dots, b_n) \mid f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]\} =$ Bild des Einsetzungshomomorphismus $A[X_1, \dots, X_n] \rightarrow B, f(X_1, \dots, X_n) \mapsto f(b_1, \dots, b_n)$.

Lemma 13.6 Sei B eine A -Algebra. Sind $b_1, \dots, b_n \in B$ ganz über A , so ist $A[b_1, \dots, b_n] \subseteq B$ endlich über A .

Beweis: Durch Induktion über n (wobei der Induktionsanfang mit $n = 0$ trivial ist): Ist b_n ganz über A , so auch über $A[b_1, \dots, b_{n-1}]$. Nach 13.3 ist also $A[b_1, \dots, b_n] = A[b_1, \dots, b_{n-1}][b_n]$ endlich über $A[b_1, \dots, b_{n-1}]$, nach 13.2 (c) also auch endlich über A wenn $A[b_1, \dots, b_{n-1}]$ (nach Induktionsvoraussetzung) endlich über A ist.

Corollar/Definition 13.7 Sei B eine A -Algebra.

(a) Die Teilmenge B' der über A ganzen Elemente in B ist ein Unterring von B und heißt der ganze Abschluss von A in B .

(b) A heißt ganz abgeschlossen in B , wenn B' gleich dem kanonischen Bild von A in B ist (also $B' = \{a \cdot 1 \mid a \in A\}$).

Beweis dass B' ein Unterring ist: nach 13.6 sind mit b_1 und $b_2 \in B'$ auch $b_1 + b_2$ und $b_1 \cdot b_2 \in B'$; weiter sind 1 und -1 in B' .

Beispiel 13.8 Sei K ein Zahlkörper, also eine endliche Erweiterung von \mathbb{Q} . Dann heißt der ganze Abschluss von \mathbb{Z} in K der Ring der ganzen Zahlen in K ; Bezeichnung \mathcal{O}_K . Diese Ringe sind ein Hauptgegenstand der Algebraischen Zahlentheorie. Für $K = \mathbb{Q}(i)$ (mit $i = \sqrt{-1}$) ist zum Beispiel $\mathcal{O}_K = \mathbb{Z}[i]$.

Definition 13.9 Ein Integritätsbereich A heißt ganz abgeschlossen, wenn er ganz abgeschlossen in seinem Quotientenkörper $Quot(A)$ ist.

Lemma 13.10 Jeder faktorielle Ring R (also auch jeder Hauptidealring) ist ganz abgeschlossen.

Beweis Sei $\frac{a}{b} \in K = \text{Quot}(R)$, $a \in R$, $b \in R \setminus \{0\}$. Ohne Einschränkung seien a und b teilerfremd. Angenommen, es gibt $a_0, \dots, a_{n-1} \in R$ mit

$$\left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + a_1 \left(\frac{a}{b}\right) + a_0 = 0.$$

Die Gleichung

$$-a^n = a_{n-1}a^{n-1}b + \dots + a_1ab^{n-1} + a_0b^n$$

steht dann im Widerspruch zur Teilerfremdheit von a und b .

Beispiele 13.11 Polynomringe $k[X_1, \dots, X_n]$ über einem Körper und diskrete Bewertungsringe sind ganz abgeschlossen, \mathbb{Z} ist ganz abgeschlossen.

§14 Symmetrische Polynome und die Diskriminante

Sei k ein Körper, $n \in \mathbb{N}$ und $k[X_1, \dots, X_n]$ der Polynomring in den Variablen X_1, \dots, X_n . Die symmetrische Gruppe n -ten Grades S_n operiert auf $k[X_1, \dots, X_n]$ durch $\sigma X_i := X_{\sigma(i)}$, d.h.,

$$\sigma f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

für $\sigma \in S_n$, also auch auf dem Körper $L = k(X_1, \dots, X_n) = \text{Quot}(k[X_1, \dots, X_n])$ (durch $\sigma \frac{f}{g} = \frac{\sigma f}{\sigma g}$).

Definition 14.1 (a) Ein Polynom $f \in k[X_1, \dots, X_n]$ heißt **symmetrisch**, wenn $\sigma f = f$ für alle $\sigma \in S_n$, also wenn es unter Vertauschungen der Variablen invariant bleibt.

(b) Der Fixkörper $K = L^{S_n} = k(X_1, \dots, X_n)^{S_n}$ heißt der **Körper der symmetrischen rationalen Funktionen** (in n Variablen) über k .

Beispiel 14.2 X_1X_2 , $X_1^2 + X_2^2$, $X_1^3 + X_1X_2 + X_2^3$ sind symmetrische Polynome.

Nach Galoistheorie (siehe Algebra I, Satz 12.7) ist L/K endlich galoissch mit Galoisgruppe S_n . Insbesondere ist $[L : K] = n!$.

Konstruktion 14.3 Betrachte das Polynom n -ten Grades

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

Operiert S_n wie üblich auf $L[X]$ (über die Koeffizienten), so wird f offenbar von jedem $\sigma \in S_n$ festgelassen, da $\prod_{i=1}^n (X - X_{\sigma(i)}) = \prod_{i=1}^n (X - X_i)$. Also hat $f(X)$ Koeffizienten in K . Schreiben wir also

$$(14.3.1) \quad f(X) = \prod_{i=1}^n (X - X_i) = \sum_{j=1}^n (-1)^j s_j(X_1, \dots, X_n) X^{n-j}$$

so ist jedes s_j ein symmetrisches Polynom in X_1, \dots, X_n und heißt das **j-te elementarsymmetrische Polynom**. Durch Ausmultiplizieren sehen wir

$$(14.3.2) \quad \begin{aligned} s_0 &= 1 \\ s_1 &= X_1 + X_2 + \dots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n \\ &\vdots \\ s_n &= X_1X_2 \dots X_n. \end{aligned}$$

Es ist also s_j homogen vom Grad j (alle Monome in s_j haben Grad j).

Bemerkung 14.4 Sei F ein Körper und

$$g(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in F[X]$$

ein normiertes Polynom n -ten Grades. Sei E/F ein Zerfällungskörper von g über F . Dann ist

$$g(X) = \prod_{i=1}^n (X - \alpha_i) \quad \text{in } E[X],$$

wobei die α_i die Nullstellen von g in F sind. Es folgt durch Vergleich mit (14.3.1)

$$(14.4.1) \quad g(X) = \sum_{j=1}^n (-1)^j s_j(\alpha_1, \dots, \alpha_n) X^{n-j}.$$

Es gilt also $a_i = (-1)^{n-i} s_{n-i}(\alpha_1, \dots, \alpha_n)$, d.h., die Koeffizienten werden (bis auf ein Vorzeichen) als die elementarsymmetrischen Polynome in den Nullstellen α_j gegeben.

Satz 14.5 Jede symmetrische rationale Funktion aus $k(X_1, \dots, X_n)$ ist eine rationale Funktion in den elementarsymmetrischen Polynomen s_1, \dots, s_n , d.h., es ist

$$K = k(X_1, \dots, X_n)^{S_n} = k(s_1, \dots, s_n).$$

Beweis: Es gilt $[L : K] = |S_n| = n!$ und $k(s_1, \dots, s_n) \subseteq K \subseteq L$. Es genügt also zu zeigen, dass

$$[L : k(s_1, \dots, s_n)] \leq n!.$$

Dies gilt aber, da L Zerfällungskörper des separablen Polynoms n -ten Grades $f(X) = \prod_{i=1}^n (X - X_i)$ über $k(s_1, \dots, s_n)$ ist (f ist separabel, da die Nullstellen X_i paarweise verschieden sind). L ist nämlich galoissch über $k(s_1, \dots, s_n)$ (Algebra I, Satz 12.7 (c)) und für die Galoisgruppe G gibt es einen Monomorphismus

$$G \hookrightarrow S_n$$

(Algebra I, Bemerkung 13.11)¹, so dass $[L : k(s_1, \dots, s_n)] = |G| \leq |S_n| = n!$.

Wir haben sogar:

¹ f ist irreduzibel, da f schon über K irreduzibel ist: S_n lässt keine echte Teilmenge von $\{X_1, \dots, X_n\}$ fest

Satz 14.5 (a) Die Elemente s_1, \dots, s_n sind algebraisch unabhängig über k .

(b) Ist $f \in k[X_1, \dots, X_n]$ ein symmetrisches Polynom, so gibt es ein eindeutig bestimmtes Polynom $g \in k[S_1, \dots, S_n]$ in den Variablen s_1, \dots, s_n mit

$$f = g(s_1, \dots, s_n).$$

Beweis: (a) Da $k(X_1, \dots, X_n)$ den Transzendenzgrad n über k hat und $k(X_1, \dots, X_n) = k(s_1, \dots, s_n)[X_1, \dots, X_n]/k(s_1, \dots, s_n)$ algebraisch ist (denn jedes X_i ist algebraisch über $k(s_1, \dots, s_n)$, siehe unten), müssen s_1, \dots, s_n algebraisch unabhängig sein, denn sonst wäre der Transzendenzgrad echt kleiner als n (beachte Proposition 9.7 für $\mathcal{X}' = \emptyset$) – Widerspruch!

(b) Daher ist der Einsetzungshomomorphismus

$$\begin{aligned} \varphi : k[S_1, \dots, S_n] &\rightarrow k[X_1, \dots, X_n] \\ h(S_1, \dots, S_n) &\mapsto h(s_1, \dots, s_n) \end{aligned}$$

injektiv mit Bild $k[s_1, \dots, s_n]$. Dies zeigt die Eindeutigkeit von g in (b). Weiter ist jedes X_i ganz über $k[s_1, \dots, s_n]$, als Nullstelle des normierten Polynoms $f(X) = \prod_{i=1}^n (X - X_i) \in k[s_1, \dots, s_n][X]$. Nach Lemma 13.6 ist $k[X_1, \dots, X_n] = k[s_1, \dots, s_n][X_1, \dots, X_n]$ also ganz über $k[s_1, \dots, s_n]$. Sei nun $f \in k[X_1, \dots, X_n]$ ein symmetrisches Polynom. Nach Satz 14.4 ist dann $f \in k(s_1, \dots, s_n)$. Andererseits ist f nach dem eben Bewiesenen ganz über $k[s_1, \dots, s_n]$. Da $k[s_1, \dots, s_n]$ ganz abgeschlossen in $k(s_1, \dots, s_n)$ ist (als Polynomring, siehe Beispiel 13.11), folgt $f \in k[s_1, \dots, s_n]$.

Beispiele 14.6 (vergleiche Beispiele 14.2) Es ist $X_1 X_2 = s_2$, $X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1 X_2 = s_1^2 - 2s_2$ und $X_1^3 + X_1 X_2 + X_2^3 = (X_1 + X_2)^3 - (X_1 + X_2)X_1 X_2 = s_1^3 - s_1 s_2$ in $k[X_1, X_2]$.

Wir kommen nun zum Begriff der Diskriminante eines Polynoms. Das Element

$$\Delta = \prod_{i < j} (X_i - X_j)^2 \in k[X_1, \dots, X_n]$$

ist offenbar ein symmetrisches Polynom, also

$$\Delta \in k[s_1, \dots, s_n].$$

Da die Koeffizienten A_i von $\prod_{i=1}^n (X - X_i)$ bis auf Vorzeichen gleich den s_i sind, ist Δ auch ein Polynom $\Delta(A_{n-1}, \dots, A_0)$ in A_0, \dots, A_{n-1} . Durch Einsetzen erhalten wir

Definition 14.7 Sei

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

ein Polynom in $k[X]$. Ist $f(X) = \prod_{i=1}^n (X - \alpha_i)$ in einem Zerfällungskörper von f über k , so heißt

$$\Delta_f = \prod_{i < j} (\alpha_i - \alpha_j)^2 = \Delta(a_{n-1}, \dots, a_0) \in k$$

die **Diskriminante** von f .

Bemerkungen 14.8 Es gilt $\Delta_f = 0$ genau dann, wenn f mehrfache Nullstellen hat, also $\Delta_f \neq 0 \Leftrightarrow f$ separabel.

Beispiel 14.9 Für $f(X) = X^2 + X + 1 \in \mathbb{Q}[X]$ sind die Nullstellen

$$\alpha_{1,2} = -\frac{1}{2} \pm \frac{\sqrt{1-4}}{2} \in \mathbb{C}.$$

Es ist also

$$\Delta_f(\alpha_1 - \alpha_2)^2 = (\sqrt{-3})^2 = -3.$$

Allgemein ist die Diskriminante des Polynoms

$$f(X) = X^2 + aX + b \in k[X]$$

gleich $a^2 - 4b$ (Übungsaufgabe!).

§15 Kategorien und Funktoren

Die Sprache der Kategorien und Funktoren ist unabdingbar für viele Aussagen in der heutigen Mathematik. Sie ist formal und weniger als Selbstzweck anzusehen, sondern eher als ein nützliches Mittel zum Formulieren und Einordnen von mathematischen Resultaten.

Wir diskutieren im Folgenden keine mengentheoretischen Fragen wie das Problem der ‘Menge aller Mengen’. Wir sprechen von Klassen, wenn wir ‘Mengen höherer Stufe’ behandeln; ein formaler Rahmen wurde durch die sogenannten ‘Universen’ nach Bourbaki geliefert. Bei der Bildung der ‘Klasse aller Mengen’, die selbst keine Menge (derselben Stufe) ist, wird also die obige Russell’sche Antinomie vermieden.

Definition 15.1 Eine Kategorie \mathcal{C} besteht aus

- (i) einer Klasse $ob(\mathcal{C})$ von Objekten,
- (ii) einer Menge $Hom_{\mathcal{C}}(A, B)$ für je zwei Objekte A, B , deren Elemente **Pfeile** oder **Morphismen** von A nach B genannt werden,
- (iii) sowie einer Verknüpfung für alle Objekte A, B, C

$$\begin{aligned} Hom_{\mathcal{C}}(B, C) \times Hom_{\mathcal{C}}(A, B) &\rightarrow Hom_{\mathcal{C}}(A, C) \\ (g, f) &\mapsto g \circ f \quad (\text{oder } gf). \end{aligned}$$

Dabei soll gelten

- (a) Zu jedem $A \in ob(\mathcal{C})$ gibt es ein Element $1_A \in Hom_{\mathcal{C}}(A, A)$ (genannt **Identität** von A) mit

$$f1_A = f = 1_B f$$

für $f \in Hom_{\mathcal{C}}(A, B)$.

- (b) (Assoziativität) Für f, g wie oben und $h \in Hom_{\mathcal{C}}(C, D)$ gilt

$$h(gf) = (hg)f$$

in $\text{Hom}_{\mathcal{C}}(A, D)$.

Dies ist der üblichen Situation von Hom-Mengen nachempfunden. Tatsächlich bekommen wir so die meisten Beispiele:

Beispiele 15.2 (a) Die Kategorie $\underline{\text{Sets}}$ aller Mengen wird definiert durch

$$\begin{aligned} \text{ob}(\underline{\text{Sets}}) &= \text{Klasse aller Mengen} \\ \text{Hom}_{\underline{\text{Sets}}}(A, B) &= \text{Menge aller Abbildungen } f : A \rightarrow B . \end{aligned}$$

Die Verknüpfung ist die übliche Komposition von Abbildungen, und $1_A \in \text{Hom}_{\underline{\text{Sets}}}(A, A)$ ist die Identität $\text{id}_A : A \rightarrow A$.

(b) Entsprechend werden viele Kategorien gebildet:

(1) Kategorie $\underline{\text{Gr}}$ der Gruppen: Objekte: Gruppen, $\text{Hom}_{\underline{\text{Gr}}}(G, H) =$ Menge der Gruppenhomomorphismen von G nach H , Verknüpfung: Komposition.

(2) Kategorie $\underline{\text{Mod}}_R$ der Moduln über einem Ring: Morphismen = R -Modulhomomorphismen, Verknüpfung = Komposition.

(3) Kategorie $\underline{\text{Top}}$ der topologischen Räume, Morphismen = stetige Abbildungen, mit der Komposition als Verknüpfung.

(4) Kategorie der topologischen Gruppen: Morphismen = stetige Gruppenhomomorphismen, mit der Komposition als Verknüpfung.

(c) Es gibt aber auch andere Kategorien. Sei (I, \leq) eine geordnete Menge. Definiere die Kategorie \underline{I} durch $\text{ob}(\underline{I}) = I$ (die Objekte sind also die *Elemente* von I !),

$$\text{Hom}_{\underline{I}}(i, j) = \begin{cases} \{*\} & , \quad i \leq j , \\ \emptyset & , \quad \text{sonst} \end{cases}$$

(Im ersten Fall besteht die Morphismenmenge also aus genau einem Element, das wir mit $*$ bezeichnen). Die Verknüpfung ist die einzig mögliche: der einzige Fall, wo beide Mengen nicht leer sind, ist

$$\text{Hom}_{\underline{I}}(j, k) \times \text{Hom}_{\underline{I}}(i, j) \rightarrow \text{Hom}_{\underline{I}}(i, k)$$

für $i \leq j \leq k$, wo $(*, *)$ auf $*$ abgebildet wird.

(d) Die kleinste Kategorie der Welt: $\mathcal{C}_0 : \mathcal{C}_0$ hat nur ein Objekt $*$ und es ist $\text{Hom}_{\mathcal{C}_0}(*, *) = \{\text{id}_*\}$.

(e) Sei G eine Gruppe. Definiere die Kategorie \underline{G} wie folgt: \underline{G} hat nur ein Objekt $*$ und es ist $\text{Hom}_{\underline{G}}(*, *) = G$ mit der Verknüpfung $G \times G \rightarrow G$, die durch das Gruppengesetz gegeben ist.

Definition 15.3 Ein Morphismus $f : A \rightarrow B$ in einer Kategorie \mathcal{C} heißt

(a) **Monomorphismus**, wenn für alle Objekte X in \mathcal{C} und alle Morphismen $g_1, g_2 : X \rightarrow A$ gilt

$$f g_1 = f g_2 \quad \Rightarrow \quad g_1 = g_2$$

(d.h., f ist links kürzbar),

(b) **Epimorphismus**, wenn für alle Objekte X in \mathcal{C} und alle Morphismen $h_1, h_2 : B \rightarrow X$ gilt

$$h_1 f = h_2 f \quad \Rightarrow \quad h_1 = h_2$$

(d.h., f ist rechts kürzbar), und

(c) **Isomorphismus**, wenn es einen Morphismus $g : B \rightarrow A$ in \mathcal{C} gibt mit

$$gf = 1_A \quad \text{und} \quad fg = 1_B$$

(Das g ist dann eindeutig bestimmt und heißt das Inverse von f).

Bemerkungen 15.4 (a) Sei $f : A \rightarrow B$ ein Morphismus in einer Kategorie \mathcal{C} . Für alle Objekte X in \mathcal{C} induziert f eine Abbildung

$$\begin{aligned} f_* : \text{Hom}_{\mathcal{C}}(X, A) &\rightarrow \text{Hom}_{\mathcal{C}}(X, B) \\ g &\mapsto fg \end{aligned}$$

und eine Abbildung

$$\begin{aligned} f^* : \text{Hom}_{\mathcal{C}}(B, X) &\rightarrow \text{Hom}_{\mathcal{C}}(A, X) \\ h &\mapsto hf. \end{aligned}$$

(b) Offenbar ist f genau dann Monomorphismus, wenn f_* injektiv ist für alle X , und Epimorphismus, wenn f^* injektiv (!) für alle X ist.

Beispiele 15.5 (a) In den Kategorien Sets, Gr, Mod_R sind Morphismen genau dann Monomorphismen (bzw. Epimorphismen), wenn sie injektiv (bzw. surjektiv) sind, und genau dann Isomorphismus, wenn sie Monomorphismus und Epimorphismus sind.

(b) In Top ist eine stetige Abbildung $f : X \rightarrow Y$ genau dann Monomorphismus, wenn sie injektiv ist und genau dann Epimorphismus, wenn sie dichtes Bild hat. Eine bijektive stetige Abbildung ist kein Isomorphismus; Isomorphismen sind per Definition die Homöomorphismen.

(c) Für eine geordnete Menge (I, \leq) ist in der Kategorie I aus Beispiel 15.2 (c) jeder Morphismus Monomorphismus und Epimorphismus, aber die einzigen Isomorphismen sind die Identitäten.

Definition 15.6 Sei \mathcal{C} eine Kategorie. Dann ist die **duale Kategorie** \mathcal{C}^{op} durch ‘Umdrehen der Pfeile’ definiert: $ob(\mathcal{C}^{op}) = ob(\mathcal{C})$ und $\text{Hom}_{\mathcal{C}^{op}}(A, B) = \text{Hom}_{\mathcal{C}}(B, A)$ mit den von \mathcal{C} induzierten Kompositionen.

Bemerkungen 15.7 Ein Morphismus $f : A \rightarrow B$ in \mathcal{C} ist genau dann ein Monomorphismus (Epimorphismus, Isomorphismus), wenn er ein Epimorphismus (Monomorphismus, Isomorphismus) in \mathcal{C}^{op} ist.

Wir diskutieren noch einige kategorielle Begriffe – Stichwort Limiten.

Definition 15.8 Sei $(M_i)_{i \in I}$ eine Familie von Objekten in einer Kategorie \mathcal{C} . Ein Objekt M in \mathcal{C} zusammen mit Morphismen $\pi_i : M \rightarrow M_i$ für alle $i \in I$ heißt **Produkt der M_i** (Bez.: $M = \prod_{i \in I} M_i$), wenn es folgende universelle Eigenschaft erfüllt:

Ist N ein Objekt in \mathcal{C} und sind $f_i : N \rightarrow M_i$ Morphismen für alle $i \in I$, so gibt es einen eindeutig bestimmten Morphismus $f : N \rightarrow M$, der das Diagramm

$$\begin{array}{ccc}
 \prod_{i \in I} M_i = M & & \\
 \uparrow & \searrow \pi_i & \\
 \exists! f \downarrow & & M_i \\
 N & \nearrow f_i &
 \end{array}$$

kommutativ macht. $(M = \prod_{i \in I} M_i, \pi_i)$ ist also universell für Morphismen in die M_i , für alle $i \in I$.

Definition 15.9 Die **Summe** einer Familie $(M_i)_{i \in I}$ von Objekten in \mathcal{C} wird dual erklärt, also (vergleiche 15.6) durch Umdrehen der Pfeile: Ein Objekt $\prod_{i \in I} M_i$ in \mathcal{C} mit Morphismen $\iota_i : M_i \rightarrow \prod_{i \in I} M_i$ für alle $i \in I$ heißt Summe der M_i , wenn es für jedes weitere Objekt N und Morphismen $g_i : M_i \rightarrow N$ einen eindeutig bestimmten Morphismus $g : \prod_{i \in I} M_i \rightarrow N$ gibt, der

$$\begin{array}{ccc}
 & \prod_{i \in I} M_i & \\
 \nearrow \iota_i & \downarrow \exists! g & \\
 M_i & & N \\
 \searrow g_i & &
 \end{array}$$

kommutativ macht. $(\prod_{i \in I} M_i, \iota_i)$ ist also universelles Ziel für Morphismen von allen M_i .

Bemerkungen 15.10 Produkte und Summen müssen nicht existieren, aber wenn sie existieren, sind sie bis auf kanonische Isomorphie eindeutig (dies folgt leicht aus den universellen Eigenschaften).

Beispiele 15.11 (a) In Sets, Gr, Ab (=Kategorie der abelschen Gruppen) und Top existieren beliebige Produkte, gegeben jeweils durch das kartesische Produkt der unterliegenden Mengen (vergleiche 1.7 für Top).

(b) In Sets existieren auch beliebige Summen; die Summe der Familie $(M_i)_{i \in I}$ ist dabei gegeben durch die disjunkte Vereinigung $\prod_{i \in I} M_i (= \bigcup_{i \in I} M_i)$.

(c) In Ab und Mod_R existieren ebenfalls beliebige Summen, sie sind gegeben durch die bereits früher eingeführten direkten Summen

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \in \prod_{i \in I} M_i \mid x_i = 0 \text{ für fast alle } i \in I\}.$$

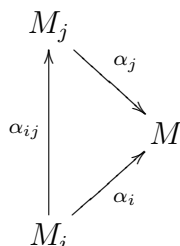
(d) In Gr existieren ebenfalls beliebige Summen (im Sinne von Kategorien); für eine Familie $(G_i)_{i \in I}$ von Gruppen ist dies gegeben durch das sogenannte ‘freie Produkt’ $*_{i \in I} G_i$,

das sogar bei abelschen G_i im Allgemeinen nicht-kommutativ ist (man betrachtet beliebige ‘Worte’ $g_{i_1}g_{i_2}\dots g_{i_n}$ mit Elementen $g_{i_\nu} \in G_{i_\nu}$, die nur vereinfacht werden können, wenn zwei benachbarte g_i aus derselben Gruppe G_i sind, so dass man sie multiplizieren kann).

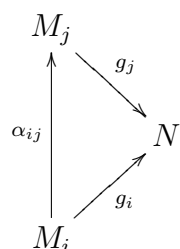
Definition 15.12 Sei (I, \leq) eine induktiv geordnete Menge und (M_i, α_{ij}) ein induktives System über I in \mathcal{C} , d.h., man hat Objekte $M_i \in \mathcal{C}$ (d.h., $\in \text{ob}(\mathcal{C})$) für alle $i \in I$ und Morphismen $\alpha_{ij} : M_i \rightarrow M_j$ (genannt Übergangsmorphismen) für alle $i, j \in I$ mit $i \leq j$, so dass gilt

$$\alpha_{ii} = \text{id}_{M_i}, \quad \alpha_{jk}\alpha_{ij} = \alpha_{ik} \quad \text{für } i \leq j \leq k.$$

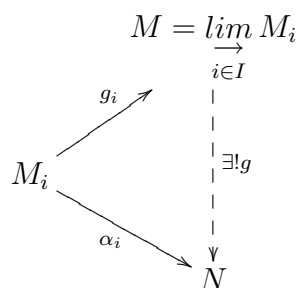
Ein Objekt M in \mathcal{C} zusammen mit Morphismen $\alpha_i : M_i \rightarrow M$ für alle $i \in I$, so dass das Diagramm



für alle $i \leq j$ kommutiert, heißt **induktiver Limes** der M_i (genauer: von (M_i, α_{ij})); Bez.: $M = \varinjlim_{i \in I} M_i$, wenn folgende universelle Eigenschaft gilt: Ist N ein Objekt in \mathcal{C} und sind Morphismen $g_i : M_i \rightarrow N$ für alle $i \in I$ gegeben, so dass



für alle $i \leq j$ kommutiert, so gibt es einen eindeutig bestimmten Morphismus $g : M = \varinjlim_{i \in I} M_i \rightarrow N$, so dass



für alle $i \in I$ kommutiert. $(\varinjlim_{i \in I} M_i, \alpha_i)$ ist also universell für “Morphismen aus dem universellen System heraus”.

Definition 15.13 Projektive Systeme $(M_i, \beta_{ji})_{\substack{i \in I \\ j \geq i}}$ über einer induktiv geordneten Menge (I, \leq) und der **projektive Limes** $\varprojlim_{i \in I} M_i$ eines solchen werden dual definiert, also

wieder durch Umdrehen der Pfeile: Es existieren

$$\beta_{ji} : M_j \rightarrow M_i \quad \text{für } j \geq i$$

mit $\beta_{ji}\beta_{kj} = \beta_{ki}$ für $k \geq j \geq i$, $\beta_{ii} = id_{M_i}$, und für ein Objekt N und Morphismen $h_i : N \rightarrow M_i$ für alle $i \in I$ gilt:

$$\begin{array}{ccc}
 \begin{array}{ccc}
 & M_j & \\
 h_j \nearrow & & \downarrow \beta_{ji} \\
 N & & M_i \\
 h_i \searrow & & \\
 & &
 \end{array}
 & \text{kommutativ } \forall j \geq i & \implies &
 \begin{array}{ccc}
 \varprojlim_{i \in I} M_i & & \\
 \downarrow \alpha_i & \searrow & \\
 \exists! h & & M_i \\
 \downarrow & \nearrow h_i & \\
 N & &
 \end{array}
 \end{array}
 \quad \text{kommutativ } \forall i.$$

Wieder müssen induktive oder projektive Limiten nicht existieren, sind aber eindeutig bis auf kanonische Isomorphie, wenn sie existieren.

Beispiele 15.14 In Sets, Gr, Ab und Mod_R existieren beliebige induktive und projektive Limiten; sie wurden in 2.5 beschrieben. Auch in Top existieren beliebige induktive und projektive Limiten; letztere wurden in 2.6 (e) beschrieben.

Insbesondere ist in Sets

$$\varprojlim_{i \in I} M_i = \{(x_i)_{i \in I} \in \prod_{i \in I} M_i \mid \beta_{ji}(x_j) = x_i \quad \text{für alle } j \geq i\}$$

sowie

$$\varinjlim_{i \in I} M_i = \prod_{i \in I} M_i / \sim,$$

wobei für $x_i \in M_i$ und $x_j \in M_j$ gilt: $x_i \sim x_j \Leftrightarrow$ es existiert ein $k \in I$ mit $k \geq i, j$ und $\alpha_{ik}(x_i) = \alpha_{jk}(x_j)$.

Bemerkung 15.15 Mit der expliziten Beschreibung von *Produkten* und *projektiven Limiten* in Sets lassen sich die universellen (und damit charakterisierenden!) Eigenschaften von Produkt, Summe, induktiver und projektiver Limes ganz kurz hinschreiben (Bezeichnungen wie in 15.8, 15.9, 15.12, 15.13)

$$(1) \quad \prod_{i \in I} \text{Hom}_{\mathcal{C}}(N, M_i) \xrightarrow{\sim} \text{Hom}_{\mathcal{C}}(N, \prod_{i \in I} M_i)$$

$$(f_i) \mapsto f$$

$$(2) \quad \prod_{i \in I} \text{Hom}_{\mathcal{C}}(M_i, N) \xrightarrow{\sim} \text{Hom}_{\mathcal{C}}(\prod_{i \in I} M_i, N)$$

$$(g_i) \mapsto g$$

$$(3) \quad \varprojlim_{i \in I} \text{Hom}_{\mathcal{C}}(M, M_i) \xrightarrow{\sim} \text{Hom}_{\mathcal{C}}(M, \varprojlim_{i \in I} M_i)$$

$$(h_i) \mapsto h$$

$$(4) \quad \lim_{\leftarrow i \in I} \text{Hom}_{\mathcal{C}}(M_i, M) \xrightarrow{\sim} \text{Hom}_{\mathcal{C}}(\lim_{\rightarrow i \in I} M_i, M)$$

$$(g_i) \mapsto g$$

Wir kommen nun zu “Abbildungen zwischen Kategorien”:

Definition 15.16 Seien \mathcal{A}, \mathcal{B} zwei Kategorien. Ein **kovarianter Funktor** $F : \mathcal{A} \rightarrow \mathcal{B}$ von \mathcal{A} nach \mathcal{B} ist eine Zuordnung, die

- (i) jeden Objekt A in \mathcal{A} ein Objekt $F(A)$ in \mathcal{B} zuordnet, und
- (ii) jeden Morphismus $f : A \rightarrow B$ in \mathcal{A} einen Morphismus $F(f) : F(A) \rightarrow F(B)$ in \mathcal{B} zuordnet.

Dabei muss gelten

- (a) $F(1_A) = 1_{F(A)}$ für alle $A \in \text{ob}(\mathcal{A})$.
- (b) Für Morphismen $f : A \rightarrow B, g : B \rightarrow V$ in \mathcal{A} gilt $F(gf) = F(g)F(f) : F(A) \rightarrow F(C)$,

Definition 15.17 Ein **kontravarianter Funktor** $G : \mathcal{A} \rightarrow \mathcal{B}$ wird als ein kovarianter Funktor $\mathcal{A} \rightarrow \mathcal{B}^{op}$ (oder, äquivalent: $\mathcal{A}^{op} \rightarrow \mathcal{B}$) definiert, d.h., G “dreht Pfeile um”: Für $f : A \rightarrow B$ haben wir also (i) und (a), sowie

$$(ii') \quad G(f) : G(B) \rightarrow G(A),$$

und entsprechend

$$(b') \quad G(gf) = G(f)G(g) \text{ für } A \xrightarrow{f} B \xrightarrow{g} C.$$

Beispiele 15.18 (a) Wir haben den **Vergissfunktork**

$$V : \underline{Gr} \rightarrow \underline{Sets}$$

$$\begin{array}{ccc} G & \mapsto & G \\ f & \mapsto & f, \end{array}$$

der nur die Gruppenstruktur vergisst.

(b) Entsprechend haben wir einen Vergissfunktork

$$V : \underline{Ringe} \rightarrow \underline{Ab}$$

auf der Kategorie der Ringe (mit Ringhomomorphismen), der einen Ring R auf die abelsche Gruppe $(R, +)$ abbildet, sowie weitere Vergissfunktoren

$$\underline{Mod}_R \rightarrow \underline{Ab} \quad , \quad \underline{Top} \rightarrow \underline{Sets}.$$

(c) Sei $\varphi : A \rightarrow B$ ein Ringhomomorphismus. Dann haben wir einen Restriktionsfunktork

$$Res_{B/A} : \underline{Mod}_B \rightarrow \underline{Mod}_A$$

$$\begin{array}{ccc} M & \mapsto & M \\ f & \mapsto & f. \end{array} \quad \text{mit Operation von } A \text{ via } \varphi$$

Weiter ist die Skalarerweiterung ein Funktor

$$B \otimes_A : \underline{Mod}_A \rightarrow \underline{Mod}_B$$

$$\begin{array}{ccc} M & \mapsto & B \otimes_A M \\ f : M_1 \rightarrow M_2 & \mapsto & f_* : B \otimes_A M_1 \rightarrow B \otimes_A M_2, \end{array}$$

siehe 12.9.

(d) Sei R ein Ring. Die Bildung des freien Moduls gibt einen Funktor

$$\begin{aligned} F_R : \quad \underline{Sets} &\rightarrow \underline{Mod}_R \\ I &\mapsto F_R(I) \\ (f : I \rightarrow J) &\mapsto (f_* : F_R(I) \rightarrow F_R(J)). \end{aligned}$$

Hierbei ist f_* der R -Modul-Homomorphismus, der das kanonische Basiselement e_i ($i \in I$) von $F_R(I)$ auf das Basiselement $e_{f(i)} \in F_R(J)$ abbildet – aufgrund der universellen Eigenschaft des freien Moduls gibt es genau einen R -Modul-Homomorphismus f_* mit dieser Eigenschaft. Man rechnet leicht nach, dass F_R ein Funktor ist, d.h., dass

$$\begin{aligned} (gf)_* &= g_*f_* \quad \text{für } I \xrightarrow{f} J \xrightarrow{g} K \\ \text{und } (id_I)_* &= id_{F_R(I)} \quad \text{für alle } I. \end{aligned}$$

Definition 15.19 Seien $F : \mathcal{A} \rightarrow \mathcal{B}$ und $G : \mathcal{B} \rightarrow \mathcal{C}$ Funktoren. Dann ist die Komposition $G \circ F : \mathcal{A} \rightarrow \mathcal{C}$ definiert durch

$$\begin{aligned} (G \circ F)(A) &= G(F(A)) \quad \text{für } A \in ob(\mathcal{A}), \\ (G \circ F)(f) &= G(F(f)) \quad \text{für } f : A \rightarrow B \text{ in } \mathcal{A}. \end{aligned}$$

Man sieht leicht, dass dies wieder ein Funktor ist. Dieser ist kovariant, wenn F und G beide kovariant oder beide kontravariant sind, und kontravariant sonst.

Definition 15.20 Sei \mathcal{C} eine Kategorie. Für jedes Objekt A in \mathcal{C} ist der **kovariante Hom-Funktor**

$$h^A = Hom_{\mathcal{C}}(A, -) : \mathcal{C} \rightarrow \underline{Sets}$$

definiert durch

$$\begin{aligned} h^A(X) &= Hom_{\mathcal{C}}(A, X), \quad \text{für } X \in ob(\mathcal{C}), \\ h^A(f) &= f_* : Hom_{\mathcal{C}}(A, X) \rightarrow Hom_{\mathcal{C}}(A, Y), \quad \text{für } f : X \rightarrow Y \text{ in } \mathcal{C}. \end{aligned}$$

siehe 15.4. Der **kontravariante Hom-Funktor**

$$h_A = Hom_{\mathcal{C}}(-, A) : \mathcal{C} \rightarrow \underline{Sets}$$

ist definiert durch

$$\begin{aligned} h_A(X) &= Hom_{\mathcal{C}}(X, A), \quad \text{für } X \in ob(\mathcal{C}), \\ h_A(f) &= f^* : Hom_{\mathcal{C}}(Y, A) \rightarrow Hom_{\mathcal{C}}(X, A), \quad \text{für } f : X \rightarrow Y \text{ in } \mathcal{C}. \end{aligned}$$

Wichtig sind auch “Abbildungen zwischen Funktoren”:

Definition 15.21 Seien \mathcal{A} und \mathcal{B} Kategorien und $F, G : \mathcal{A} \rightarrow \mathcal{B}$ zwei Funktoren von \mathcal{A} nach \mathcal{B} . Ein **Morphismus von Funktoren** (oder auch **natürliche Transformation**) $u : F \rightarrow G$ von F nach G besteht aus Morphismen in \mathcal{B}

$$u_A : F(A) \rightarrow G(A)$$

für alle Objekte A in \mathcal{A} . Dabei soll gelten, dass für alle Morphismen $f : A \rightarrow A'$ das Diagramm

$$\begin{array}{ccc} F(A) & \xrightarrow{u_A} & G(A) \\ F(f) \downarrow & & \downarrow G(f) \\ F(A') & \xrightarrow{u_{A'}} & G(A') \end{array}$$

kommutativ ist (Hierfür sagt man auch, dass die durch die u_A gegebene Zuordnung “natürlich” ist).

Beispiel 15.22 Sei G eine Gruppe und \underline{Mod}_G die Kategorie der G -Moduln. Dann haben wir für jedes $i \geq 0$ einen Funktor

$$H^i(G, -) : \underline{Mod}_G \rightarrow \underline{Ab}$$

durch die i -te Kohomologie: Für einen G -Modul A ordnen wir zu

$$A \mapsto H^i(G, A)$$

und für einen G -Modul-Homomorphismus $f : A \rightarrow A'$ ordnen wir zu

$$f \mapsto f_* : H^i(G, A) \rightarrow H^i(G, A')$$

(es ist also $H^i(G, f) = f_*$). Wir hatten in 5.2 gesehen, dass dies “funktoriell ist”, d.h., dass die Funktoraxiome $(gf)_* = g_*f_*$ und $(id_A)_* = id_{H^i(G,A)}$ gelten.

Ist nun $H \leq G$ eine Untergruppe, so haben wir einen entsprechenden Funktor

$$H^i(H, -) : \underline{Mod}_G \rightarrow \underline{Ab}$$

(jeder G -Modul ist auch ein H -Modul) und einen Morphismus von Funktoren

$$Res : H^i(G, -) \rightarrow H^i(H, -)$$

gegeben durch die Restriktionen

$$Res : H^i(G, A) \rightarrow H^i(H, A)$$

für alle G -Moduln A . Tatsächlich ist für jeden G -Modul-Homomorphismus $f : A \rightarrow A'$ das Diagramm

$$\begin{array}{ccc} H^i(G, A) & \xrightarrow{Res} & H^i(H, A) \\ f_* \downarrow & & \downarrow f_* \\ H^i(H, A) & \xrightarrow{Res} & H^i(H, A') \end{array}$$

kommutativ; dies folgt leicht aus den Definitionen.

Definition 15.23 Ein Morphismus von Funktoren

$$u : F \rightarrow G$$

$(F, G : \mathcal{A} \rightarrow \mathcal{B})$ heißt **Isomorphismus von Funktoren** (oder **natürliche Äquivalenz**), wenn alle Morphismen

$$u_A : F(A) \xrightarrow{\sim} G(A)$$

Isomorphismen sind.

Offenbar bilden dann die Inversen u_A^{-1} einen Morphismus von Funktoren $u^{-1} : G \rightarrow F$ und es gilt $u^{-1} \circ u = Id_{\mathcal{A}}$ und $u \circ u^{-1} = Id_{\mathcal{B}}$, wobei die Komposition von Morphismen von Funktoren in offensichtlicher Weise definiert ist und $Id_{\mathcal{A}} : \mathcal{A} \rightarrow \mathcal{A}$ der identische Funktor einer Kategorie \mathcal{A} ist ($Id_{\mathcal{A}}(A) = A$; $Id_{\mathcal{A}}(f) = f$).

Man schreibt $F \simeq G$, wenn es einen Isomorphismus $u : F \rightarrow G$ von Funktoren gibt.

Definition 15.24 Ein Funktor $F : \mathcal{A} \rightarrow \mathcal{B}$ heißt Äquivalenz von Kategorien, wenn es einen Funktor $G : \mathcal{B} \rightarrow \mathcal{A}$ gibt mit

$$G \circ F \simeq Id_{\mathcal{A}} \quad , \quad F \circ G \simeq Id_{\mathcal{B}} .$$

\mathcal{A} und \mathcal{B} heißen dann äquivalente Kategorien und G heißt ein Quasi-Inverses von F .

Es kommt selten vor, dass man ein echtes Inverses findet, d.h., ein G mit $G \circ F = Id_{\mathcal{A}}$ und $F \circ G = Id_{\mathcal{B}}$.

Beispiel 15.25 Sei k ein Körper und $n \in \mathbb{N}$ und sei \underline{Vek}_k die Kategorie der endlich-dimensionalen k -Vektorräume. Sei $M_0 = k^n$, aufgefasst als $M_n(k)$ -Modul. Nach Sätzen von Wedderburn hat man eine Kategorienäquivalenz

$$\begin{array}{ccc} F : \underline{Vek}_k & \rightarrow & \underline{Mod}_{M_n(k)} \\ V & \mapsto & M_0 \otimes_k V \end{array}$$

mit Quasi-Inversem

$$M \mapsto \underline{Hom}_{M_n(k)}(M_0, M) .$$