Universität Duisburg-Essen
- Campus Duisburg -

Fakultät für Mathematik

Ausgewählte Kapitel der Algebra

von
Wolfgang Hümbs und Klaus Kuzyk
SS 2011

Die vorliegende Version ist eine ergänzte und
korrigierte Fassung vom Sommersemester 2010

Duisburg / Haan, im SS 2011
Wolfgang Hümbs
Klaus Kuzyk

Die Autoren bedanken sich herzlich bei Herrn Viktor Vehreschild
für das sorgfältige Setzen des Manuskripts in Latex.

Die Autoren bedanken sich herzlich bei Herrn Sebastian Rehmer
für das Überarbeiten der Version vom SS 2010 in Latex.

Inhaltsverzeichnis

Einleitung

In dieser Vorlesung werden Grundlagen der Artinschen Zopfgruppen und der Ring- bzw. Modultheorie behandelt.

Die Zopfgruppen B_n wurden nach Vorarbeiten von Gauss und Hurwitz 1925 von Artin eingeführt. Sie besitzen fundamentale Anwendungen in der Mathematik, z.B. in der Homotopie- und Knotentheorie. Weiterhin fand V. Jones in der Mitte der achtziger Jahre neue Darstellungen der Zopfgruppen, welche zu einer neuen Invariante, dem Jones-Polynom, führten. Es gibt u.a. fünf Definitionen der Zopfgruppen: eine Darstellung der Gruppe B_n mit $(n-1)$-Generatoren und speziellen Relationen, die geometrische Definition, als Untergruppe der Automorphismusgruppe einer freien Gruppe, als Fundamentalgruppe eines Konfigurationsraumes und schließlich als „Mapping Class Group“. Daher ist es nicht verwunderlich, dass es fundamentale Anwendungen in der Chemie, Molekularbiologie, Robotertechnik, Physik und Kryptographie gibt.

Bzgl. der Ringtheorie werden u.a. der Chinesische Restsatz für kommutative Ringe mit Eins und Noethersche Ringe besprochen. Ein Kapitel über Sequenzen von Modulhomomorphismen schließt die Vorlesung ab.

Naturgemäß konnten diese Gebiete nicht erschöpfend behandelt werden, lediglich bei den Noetherschen Ringen konnte durch die Beschränkung auf kommutative Ringe mit Eins mit der Lasker-Noetherschen-Primärzerlegung ein gewisser inhaltlich befriedigender Abschluss erreicht werden. Stillschweigend werden natürliche Ergebnisse aus der Gruppentheorie benutzt. Deshalb wurden sie in einem Glossar (Kapitel 2) zusammengefasst. Da an mehreren Stellen auch Beispiele von Gruppen aus der Topologie präsentiert werden, erschien ein kurzer Anhang über mengentheoretische Topologie angebracht. Die Übungsaufgaben dienen wie üblich zur Vertiefung des Stoffs.

Duisburg/Haan im SS 2010,
Wolfgang Hümbs und Klaus Kuzyk

1. Verknüpfungen

Definition 1.1.
Sei M eine nichtleere Menge. Unter einer (zweistelligen) ***Verknüpfung*** *oder* ***Operation in M*** *versteht man eine Abbildung*

$$f\colon M \times M \to M.$$

Bemerkung 1.2.

(i) Schreiben wir die Verknüpfung als $a * b$, dann muss die Operation für ***jedes*** *geordnete Paar (a, b), $a, b \in M$, definiert sein. Es gibt viele Regeln, die zuerst wie Operationen aussehen. Z. B. ist aber die Division auf $\mathbb{R}$ keine Verknüpfung, denn der Quotient des geordneten Paares $(1, 0)$ ist undefiniert, da die Division durch Null nicht erlaubt ist.*

(ii) Die Verknüpfung $a * b$ muss eindeutig definiert sein. Sei $a * b$ für $a, b \in \mathbb{R}$ die Zahl, deren Quadrat ab ist. Nun gilt $ab = 2 \cdot 8 = 16$ und $x^2 = 16 \Leftrightarrow x = \pm 4$. Diese Zuordnung wäre nicht eindeutig, demnach ist $a * b$ keine Verknüpfung auf $\mathbb{R}$.

(iii) Per definitionem muss $a * b$ in M liegen. Man sagt auch, M sei abgeschlossen unter der Operation "$*$". Bezüglich einer Multiplikation $a \cdot b$ sagt man auch, die Multiplikation $a \cdot b$ sei abgeschlossen, wenn das Produkt wieder in M liegt. Das kanonische Skalarprodukt, z.B. im $\mathbb{R}^2$, also

$$f\colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R},\ f(a, b) = a_1 b_1 + a_2 b_2 \quad \textit{mit } \boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \textit{ und } \boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

ist keine Verknüpfung, weil die Operation aus dem zweidimensionalen euklidischen Raum $\mathbb{R}^2$ herausführt.

Beispiel 1.3.

(i) Die Operation $a * b = \frac{a+b}{ab}$ *ist keine Verknüpfung auf der Menge* $\mathbb{Z}$*, weil z.B.* $1 * 2 = \frac{1+2}{1 \cdot 2} = \frac{3}{2}$ *keine ganze Zahl ist, d.h.* $\mathbb{Z}$ *unter "*$*$*" nicht abgeschlossen ist. Weiterhin wäre* $1 * 0$ *nicht definiert.*

(ii) Die Verknüpfung $x * y = x + y + 1$ *ist auf* $\mathbb{Z}$ *kommutativ, assoziativ und besitzt ein neutrales bzw. inverses Element.*

Beweis.

a) Es gilt
$x * y = x + y + 1$ und $y * x = y + x + 1 = x + y + 1$,
also ist "$*$" kommutativ.

b) Weiterhin hat man
$x * (y * z) = x * (y + z + 1) = x + (y + z + 1) + 1 = x + y + z + 2$
sowie
$(x * y) * z = (x + y + 1) * z = (x + y + 1) + z + 1 = x + y + z + 2$,
d.h. die Verknüpfung "$*$" ist assoziativ.

c) Wir lösen die Gleichung $x * e = x$ nach e auf:
$x * e = x + e + 1 = x$, d.h. $e = -1$
Die Probe ergibt: $x * (-1) = x + (-1) + 1 = x$.
Die Verknüpfung ist kommutativ, so dass man natürlich auch
$(-1) * x = (-1) + x + 1 = x$ erhält.
Damit besitzt "$*$" das neutrale Element -1.

d) Abschließend lösen wir $x * x' = -1$ nach x' auf:
$x * x' = x + x' + 1 = -1$, d.h. man findet $x' = -x - 2$.
Die Probe liefert: $x * (-x - 2) = x + (-x - 2) + 1 = -1$
sowie $(-x - 2) * x = (-x - 2) + x + 1 = -1$.
Jedes Element x besitzt also das Inverse $-x - 2$.

□

2. Grundbegriffe der Gruppentheorie

In diesem Abschnitt stellen wir einige Grundbegriffe der Gruppentheorie vor und zeigen exemplarisch Anwendungen in anderen Disziplinen.

Definition 2.1.
Eine ***Gruppe*** *ist eine Menge G mit einer Abbildung*

$$G \times G \to G;\ (a, b) \mapsto a * b,$$

die folgende Axiome erfüllt:
(G1) Assoziativgesetz: Für alle $a, b, c \in G$ gilt $(a * b) * c = a * (b * c)$.
(G2) Existenz eines neutralen Elementes e: Es gibt ein $e \in G$ mit $a*e = e*a = a$ für alle $a \in G$.
(G3) Existenz des Inversen: Zu jedem $a \in G$ existiert $a^{-1} \in G$ mit $a * a^{-1} = a^{-1} * a = e$.

Definition 2.2.
Eine Gruppe G heißt ***abelsch*** *(oder kommutativ), falls gilt*

$$a * b = b * a \quad \textit{für alle} \quad a, b \in G.$$

Bemerkung 2.3.
Abelsche Gruppen schreibt man meistens additiv und nichtabelsche Gruppen multiplikativ. Mit dieser Schreibweise sind dann auch die neutralen Elemente 0 *bzw.* 1*. Entsprechendes gilt für die Inversen $-a$ bzw. a^{-1}.*

Bemerkung 2.4 (Eigenschaften und Rechenregeln in Gruppen)**.**

(i) In einer Gruppe ist das neutrale Element e und zu jedem a das Inverse a^{-1} eindeutig bestimmt. Für alle $a, b \in G$ gilt:

$$(a^{-1})^{-1} = a \quad \text{und} \quad (ab)^{-1} = b^{-1}a^{-1}.$$

(ii) In einer Gruppe ist ein Produkt von n Faktoren unabhängig von der Klammerung. In einer abelschen Gruppe ist ein Produkt von n Faktoren insbesondere auch unabhängig von der Reihenfolge. Es gilt:

a) $a^n := a \cdot \ldots \cdot a$ *für n Faktoren und* $n \in \mathbb{N}$.

b) $a^0 := e; \quad a^{-n} := (a^{-1})^n, \quad$ *für* $n \in \mathbb{N}$.

c) $a^{m+n} = a^m \cdot a^n; \ (a^m)^n = a^{mn}; \ (a^m)^{-1} = (a^{-1})^m;$
sowie $(ab)^n = a^n b^n, \ $ *falls* $ab = ba$ *und* $m, n \in \mathbb{Z}$.

Beispiel 2.5 (Beispiele für Gruppen)**.**

(i) Schon bekannte Gruppen sind: Jeder Körper, Ring oder Vektorraum ist eine abelsche Gruppe bzgl. der Addition. Für einen Körper K ist $K^* = K - \{0\}$ eine abelsche Gruppe bzgl. der Multiplikation.

(ii) Die symmetrische Gruppe

$$S_n := \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} : f \text{ ist bijektiv } \}$$

besitzt genau $n!$ Elemente. Jede Permutation aus $S_n, n \geq 2$ ist ein Produkt von Transpositionen, das sind Permutationen, die zwei Ziffern vertauschen und alle anderen fest lassen. Eine Permutation heißt gerade (ungerade), falls sie Produkt einer geraden (ungeraden) Anzahl von Transpositionen ist.

Beispiel

Die symmetrische Gruppe S_3 besitzt $3! = 6$ Elemente:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Man schreibt auch abkürzend z.B. $\sigma_2 = (1,2)$ *und* $\sigma_5 = (1,3)$*. Dann wird* S_3 *von* σ_2 *und* σ_5 *erzeugt, d.h. es gilt*

$$S_3 = \langle (1,2), (1,3) \rangle.$$

Bemerkung 2.6 (Wichtige und schon bekannte Gruppen aus der Linearen Algebra)**.**

(i) Es sei K *ein Körper. Mit* $K^{n\times n}$ *bezeichnen wir die Menge der* $(n * n)$*-Matrizen mit Koeffizienten aus* K*. Die Verknüpfung ist jeweils die Matrixmultiplikation.*

(ii) Die ***allgemeine lineare*** *(general linear)* ***Gruppe*** *über* K*:*

$$GL(n,K) := \left\{ A \middle| A \in K^{n\times n},\ A \text{ ist invertierbar} \right\}.$$

(iii) Die ***spezielle lineare Gruppe****:*

$$SL(n,K) := \left\{ A \middle| A \in K^{n\times n},\ detA = 1 \right\}.$$

(iv) Die ***orthogonale Gruppe****:*

$$O(n,K) := \left\{ A \middle| A \in K^{n\times n},\ AA^T = E \right\}.$$

(v) Die ***spezielle orthogonale Gruppe****:*

$$SO(n,K) := \{ A | A \in O(n,K),\ detA = 1 \}.$$

(vi) Die ***unitäre Gruppe****:*

$$U(n,K) := \left\{ A \middle| A \in K^{n\times n},\ \overline{U}^T U = E \right\}.$$

Speziell:

$$U(1) = \{ z \in GL(1,\mathbb{C}) |\ \overline{z}z = 1 \} \cong S^1 = \{ z \in \mathbb{C} || z | = 1 \}.$$

Bemerkung 2.7 (Wichtige Gruppen aus der Topologie)**.**
Fundamentalgruppe, höhere Homotopiegruppen, Homologiegruppen, Cohomologiegruppen, topologische Gruppen, ...

In diesem Abschnitt soll exemplarisch mit Hilfe der Fundamentalgruppe folgendes wichtiges Konstruktionsverfahren vorgestellt werden. Eine gegebene Struktur kann z.B. an die Gruppenaxiome erinnern, wird allerdings erst durch **Äquivalenzklassenbildung** zur Gruppe gemacht. Ein bekanntes Beispiel aus der Analysis sind die $\mathcal{L}^p$-Räume, die erst duch Äquivalenzklassenbildung zu normierten Räumen werden.

Wir betrachten das in der Topologie wichtige Homöomorphieproblem: Für zwei gegebene topologische Räume X und Y soll man entscheiden, ob sie homöomorph sind (topologische Grundbegriffe sind im Anhang **Topologische Räume** zusammengefasst). Wenn man einen Homöomorphismus $f : X \to Y$ konstruieren kann, ist das Problem gelöst. Hat man den Verdacht, dass $X \not\approx Y$ gilt, muss man eine topologische Invariante angeben, die zwar X, aber nicht Y hat. Kann man weder einen Homöomorphismus noch eine adäquate topologische Invariante angeben, bleibt das Problem offen.

Gleichzeitg bemerken wir, dass man mit algebraischen Methoden topologische Fragestellungen behandeln kann.

Definition 2.8.
Sei X ein topologischer Raum und I das Einheitsintervall $[0, 1]$. Ein ***Weg*** *w in X ist eine stetige Abbildung*

$$w : I \to X$$

Dabei heißt $w(0)$ der Anfangspunkt und $w(1)$ der Endpunkt des Weges. Weiterhin heißt w geschlossen, falls $w(0) = w(1)$ und konstant, falls $w(s) = w(0)$ für alle $s \in [0, 1]$ gilt.

In der angelsächsischen Literatur wird die Menge der Wege in X von x nach y oft mit $PX(x, y)$ bezeichnet (Path $\widehat{=}$ Weg). Die „Zeitvariable“ t reservieren wir für die Homotopie. Stimmt der Endpunkt eines Weges w (in X) mit dem Anfangspunkt eines Weges v überein, dann kann man die Wege addieren, indem man w und v nacheinander mit doppelter Geschwindigkeit durchläuft.

Definition 2.9.
Für $x, y, z \in X$ ist die Addition von Wegen definiert durch

$$\begin{aligned} PX(x,y) \times PX(y,z) &\xrightarrow{+} PX(x,z), \\ (w,v) &\mapsto v+w, \\ \text{mit } (v+w)(s) &:= \begin{cases} w(2s) & \text{für } 0 \le s \le \frac{1}{2}, \\ w(2s-1) & \text{für } \frac{1}{2} \le s \le 1. \end{cases} \end{aligned}$$

Bemerkung 2.10.
Wir notieren die Verknüpfung "+" hier wie in der Analysis als $v+w$, obwohl man in der Algebra die Komposition oft konsequent von links nach rechts liest.

Definition 2.11.
Man erhält den inversen Weg $-w$, indem man w in umgekehrter Reihenfolge durchläuft:

$$(-w)(s) := w(1-s) \text{ für } 0 \le s \le 1.$$

Feststellung 2.12.
Es gilt:

(i) $-(v+w) = (-w)+(-v)$
Man denke an die Inversenbildung in Grupppen: $(AB)^{-1} = B^{-1}A^{-1}$

(ii) $-(-w) = w$.

Bemerkung 2.13.
Die bisherigen Rechenregeln erinnern also an das Rechnen in Gruppen. Allerdings gibt es bzgl. der Addition von Wegen kein eindeutiges neutrales und inverses Element. Weiterhin ist die Addition von Wegen nicht assoziativ, denn es gilt:

$$\begin{aligned} (u+(v+w))(s) &= \begin{cases} (v+w)(2s) & \text{für } 0 \le s \le \frac{1}{2}, \\ u(2s-1) & \text{für } \frac{1}{2} \le s \le 1 \end{cases} \\ &= \begin{cases} w(4s) & \text{für } 0 \le s \le \frac{1}{4}, \\ v(4s-1) & \text{für } \frac{1}{4} \le s \le \frac{1}{2}, \\ u(2s-1) & \text{für } \frac{1}{2} \le s \le 1 \end{cases} \end{aligned}$$

$$
\begin{aligned}
((u+v)+w)(s) &= \begin{cases} w(2s) & \text{für } 0 \le s \le \frac{1}{2}, \\ (u+v)(2s-1) & \text{für } \frac{1}{2} \le s \le 1 \end{cases} \\
&= \begin{cases} w(2s) & \text{für } 0 \le s \le \frac{1}{2}, \\ v(4s-2) & \text{für } \frac{1}{2} \le s \le \frac{3}{4}, \\ u(4s-3) & \text{für } \frac{3}{4} \le s \le 1 \end{cases}
\end{aligned}
$$

Die Abbildungen $u + (v + w)$ und $(u + v) + w$ haben zwar dieselben Anfangs- bzw. Endpunkte und das gleiche Bild, sie wirken aber auf verschiedene Teile des Einheitsintervalls und bekanntlich sind zwei Abbildungen $f : A \to B$ und $g : C \to D$ genau dann gleich, wenn $f = g$ und $C = A$ sowie $D = B$ gilt.

Man erhält eine befriedigende algebraische Struktur, wenn man nun zu geeigneten Äquivalenzklassen von Wegen übergeht. Zwei Wege werden dann als äquivalent bezeichnet, wenn die Anfangs- und Endpunkte jeweils übereinstimmen und ein Weg aus dem anderen durch eine Homotopie (stetige Deformation) hervorgeht.

Definition 2.14.
Seien w und w' zwei Wege aus $PX(x, y)$. Dann heißt w äquivalent zu w', Schreibweise $w \sim w'$, falls es eine stetige Abbildung

$$\rho : [0, 1] \times [0, 1] \to X$$

existiert mit

$$
\begin{aligned}
\rho(s, 0) &= w(s), \\
\rho(s, 1) &= w'(s), \\
\rho(0, t) &= x, \\
\rho(1, t) &= y
\end{aligned}
$$

*für alle s und t aus $[0, 1]$. Dann heißt ρ auch **Homotopie** von w nach w' (relativ zu Anfangs- und Endpunkt).*

Feststellung 2.15.
Für alle $x, y \in X$ ist " $\sim$ " eine Äquivalenzrelation und ist mit der Addition von Wegen verträglich.

Definition 2.16.

(i) Die Menge der Äquivalenzklassen $PX(x,y)/\sim$ wird mit $\Pi X(x,y)$ bezeichnet. Die Äquivalenzklasse $[w]$ heißt auch Homotopieklasse.

(ii) Die Addition der Homotopieklassen wird definiert durch

$$\begin{aligned} \Pi X(x,y) \times \Pi X(y,z) &\xrightarrow{+} \Pi X(x,z), \\ ([w],[v]) &\mapsto [v]+[w], \\ [v]+[w] &:= [v+w]. \end{aligned}$$

Feststellung 2.17.
Die Addition von Homotopieklassen erfüllt zwar das Assoziativgesetz, aber bzgl. einer Gruppenstruktur gibt es kein eindeutig bestimmtes neutrales bzw. inverses Element.

Satz 2.18.
Für alle $x \in X$ bei wegweise zusammenhängendem X bildet $\Pi X(x,x)$ bzgl. der Addition von Homotopieklassen eine Gruppe. Diese Gruppe heißt ***Fundamentalgruppe*** *und wird mit $\pi_1(X,x)$ oder auch nur mit $\pi_1(X)$ bezeichnet, weil sie vom Fußpunkt x unabhängig ist. Die Fundamentalgruppe ist eine topologische Invariante.*

Beispiel 2.19.

(i) Es gilt $\pi_1(\mathbb{R}^n) = 0$, denn für alle Wege $w \in P\mathbb{R}^n(x,x)$ gilt $w \sim c_x$, d.h. man kann jede Schleife innerhalb $\mathbb{R}^n$ auf einen Punkt zusammenziehen. Eine Homotopie ist gegeben durch

$$\rho(s,t) = (1-t)w(s) + tx \quad \text{für } s,t \in [0,1].$$

Da O_x das einzige Element von $\pi_1(\mathbb{R}^n)$ ist, ist die Fundamentalgruppe das n-dimensionalen euklidischen Raum die triviale Gruppe.

(ii) Für $S^1 = \{(x,y) \in \mathbb{R}^2 | x^2+y^2 = 1\}$ gilt $\pi_1(S^1) = \mathbb{Z}$. Anschaulich ist das klar, denn das sind alle Wege, die n-mal in positiver bzw. in negativer Richtung durchlaufen werden.

(iii) Der Einheitskreis und die Einpunktvereinigung S_{x_0} von S^1 mit einem Geradenstück besitzen beide die Fundamentalgruppe $\mathbb{Z}$, sind also ***homotopieäquivalent****, aber nicht homöomorph. Es gibt keinen Homöomorphismus zwischen S^1 und S_{x_0}, denn trennt man S^1 bzw. S_{x_0} in x_0, dann bleibt die Restriktion stetig, S^1 besitzt weiterhin eine Zusammenhangskomponente, aber S_{x_0} hat durch die Trennung zwei Zusammenhangskomponenten; und das ist bekanntlich unter einer stetigen Abbildung nicht möglich.*

Definition und Bemerkung 2.20 (Homomorphismen von Gruppen)**.**

(i) Eine Abbildung $f : G \to G'$ einer Gruppe G in eine Gruppe G' heißt ***Homomorphismus****, wenn*

$$f(a * b) = f(a) * f(b) \quad \text{für alle } a, b \in G$$

gilt. Ferner heißt ein Homomorphismus

- ***Epimorphismus****, falls er surjektiv ist.*
- ***Monomorphismus****, falls er injektiv ist.*
- ***Isomorphismus****, falls er bijektiv ist.*
- ***Automorphismus****, falls er ein Isomorphimus und $G' = G$ ist.*

(ii) Ein schon bekanntes Beispiel einer Automorphismengruppe

$$Aut(G) := \{f : G \to G \text{ ist Automorphismus}\}$$

ist die Automorphismengruppe von K^n (K ist Körper und K^n wird aufgefasst als Vektorraum über K):

$$Aut(K^n) = \{f : K^n \to K^n | f \text{ ist linear und } detf \neq 0\}.$$

(iii) Für alle $g \in G$ ist der innere Automorphismus

$$i_g : G \to G;\ i_g(x) = gxg^{-1} \quad \text{für } x \in G$$

ein Element von $Aut(G)$.

(iv) Automorphismengruppen spielen auch in der Funktionentheorie eine herausragende Rolle:

a) Die Elemente der Automorphismengruppe von $\mathbb{CP}^1$ (Riemannsche Zahlenkugel) sind die Möbiustransformationen.

b) Die Ordnung einer Automorphismengruppe einer kompakten Riemannschen Fläche vom Geschlecht $g > 1$ ist kleiner gleich $84(g-1)$.

c) Die Automorphismengruppe von $\mathbb{C}$ sind die Funktionen

$$f(z) = az + b, \quad a \in \mathbb{C}\setminus\{0\}\,,\ b \in \mathbb{C}.$$

(v) Ein Graph $\Gamma = (V, E)$ besteht aus einer (höchstens abzählbaren) Punktmenge V (vertices) und einer Kantenmenge E (edges), wobei jede Kante $e \in E$ zwischen zwei Punkten $v_1, v_2 \in V$ verläuft. Ein Graph heißt orientiert, wenn jede Kante $e \in E$ mit einer Orientierung versehen ist.

(vi) Ein Automorphismus eines Graphen ist eine bijektive Abbildung der Menge der Punkte auf sich, die verbundene Punkte in verbundene überführt.

(vii) Die Dieder-Gruppe D_4 ist die Automorphismengruppe des Quadrats.

Lemma und Definition 2.21 (Untergruppen)**.**

(i) Eine nichtleere Teilmenge H einer Gruppe G heißt Untergruppe von G, falls H unter der Multiplikation von G ageschlossen ist und mit dieser Multiplikation selbst eine Gruppe ist.

(ii) $H \subseteq G$ ist Untergruppe von $G \Leftrightarrow H \neq \emptyset$ und $ab, a^{-1} \in H$ für alle $a, b \in H$.

(iii) G und $\{e\}$ sind die trivialen Untergruppen.

(iv) Bilder und Urbilder unter Homomorphismen sowie beliebige Durchschnitte von Untergruppen sind Untergruppen.

Bemerkung 2.22 (Einbettung einer Gruppe in eine Permutationsgruppe)**.**

(i) Jede Gruppe G ist isomorph zu einer Untergruppe von $S(G) = \{f : G \to G |\ f$ ist bijektiv$\}$.

(ii) Jede endliche Gruppe mit n Elementen ist isomorph zu einer Untergruppe von S_n.

Satz und Definition 2.23.

(i) Für eine Untergruppe H einer Gruppe G heißen

$$aH := \{ah \mid h \in H\} \quad bzw. \quad Ha := \{ha \mid h \in H\}, \quad für\ a \in G.$$

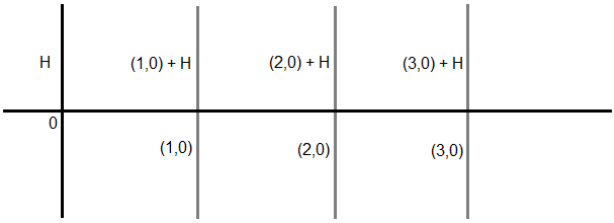
***Linksnebenklassen** bzw. **Rechtsnebenklassen** von H in G.*

(ii) G ist die disjunkte Vereinigung der verschiedenen Links- bzw. Rechtsnebenklassen von H. Alle Links- bzw. Rechtsnebenklassen von H enthalten so viele Elemente wie H.

Beispiel 2.24.
Als Beispiel betrachten wir die Ebene des Vektorraums $\mathbb{R}^2$. Bezüglich der (Vektor-)Addition ist $G = \mathbb{R}^2$ eine Gruppe und $H = \{(0, y)^T \in \mathbb{R}^2\}$ offensichtlich eine Untergruppe mit inversem Element $(0, -y)^T$. Für die linken Nebenklassen gilt dann

$$\begin{pmatrix} x \\ y \end{pmatrix} + H = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 | y \in \mathbb{R}, x = const. \right\} =: {}_xH$$

Die Ebene wird also in disjunkte Streifen zerlegt:



Wir bemerken noch, dass z.B. $(1, 7) + H$ und $(1, 49) + H$ die gleiche Nebenklasse ${}_1H$ bezeichnen, denn beide ergeben die vertikale Gerade $x = 1$. In der Tat sind die Nebenklassen entweder gleich oder disjunkt, genauer:

Seien $g_1, g_2 \in G$ und $g \in g_1 H$ sowie $g \in g_2 H$. Dann gilt $g = g_1 h_1 = g_2 h_2$ mit $h_1, h_2 \in H$. Aus $g_1 h_1 = g_2 h_2$ folgt durch Multiplikation mit h_1^{-1} $g_1 = g_2 h_2 h_1^{-1}$ und somit $g_1 H = g_2 h_2 h_1^{-1} = g_2(h_2 h_1^{-1} H) = g_2 H$, denn die Multiplikation eines Gruppenelements mit der Gruppe ergibt wieder die (ganze) Gruppe. Ein weiteres Beispiel ist die Zerlegung der Sphäre S^3 in (disjunkte) kongruente Kreise, die sogenannte Hopf-Fibration.

(iii) *Die Anzahl $|G|$ der Elemente*

- *a) von G heißt die* ***Ordnung*** *der Gruppe G.*
- *b) Die Anzahl $[G : H]$ der verschiedenen Links- bzw. Rechtsnebenklassen von H in G ist der* ***Index*** *einer Untergruppe H von G.*

(iv) ***Satz von Lagrange***
Für eine Untergruppe H von G gilt

$$|G| = [G : H]|H|.$$

(v) ***Ordnung einer Gruppenelementes***
Die Ordnung $a \in G$ ist $ord(a) := |\langle a \rangle|$, wobei $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ die von a erzeugte Untergruppe von G ist, d.h. die Ordnung von a ist entweder ∞ oder die kleinste natürliche Zahl n mit $a^n = e$. Für $ord(a) < \infty, k \in \mathbb{Z}$ gilt:

$$a^k = e \Leftrightarrow ord(a) \text{ teilt } k.$$

(vi) ***Kleiner Fermatscher Satz***
Für eine endliche Gruppe G gilt $a^{|G|} = e$ für alle $a \in G$.

(vii) *Eine Untergruppe H von G heißt* ***Normalteiler*** *(normale Untergruppe) von G, falls $aH = Ha$ für alle $a \in G$ gilt, d.h. die Linksnebenklassen stimmen mit den Rechtsnebenklassen überein. Äquivalent dazu ist:*

$$\begin{aligned} aHa^{-1} &= H \quad \text{für alle } a \in G \\ aha^{-1} &= H \quad \text{für alle } a \in G \text{ und } h \in H. \end{aligned}$$

(viii) a) *Jede Gruppe besitzt die trivialen Normalteiler* $\{e\}$ *und* G.

b) *Jede Untergruppe einer abelschen Gruppe* G *ist Normalteiler von* G.

c) *Die alternierende Gruppe* A_n, *d.h. die Untergruppe aller geraden Permutationen, ist ein Normalteiler von* S_n.

d) *In jeder Gruppe* G *ist das* ***Zentrum***

$$Z(G) := \{g \in G : gx = xg \text{ für alle } x \in G\}$$

von G *ein Normalteiler.*

e) *Die Menge* $Inn(g)$ *für* $g \in G$ *aller inneren Automorphismen* $i_g, i_g(x) = gxg^{-1}$ *ist ein Normalteiler von* $Aut(G)$.

f) *Die spezielle unimodulare Gruppe vom Grad* n

$$SL(n,\mathbb{Z}) := \left\{U \in \mathbb{Z}^{n\times n} \middle| detU = 1\right\}$$

ist ein Normalteiler in $GL(n,\mathbb{Z})$ *vom Index 2.*

g) *Für einen Normalteiler* N *von* G *wird die Menge* G/N *der Nebenklassen von* N *in* G *durch*

$$(gN)(hN) := ghN \text{ für } g,h \in G$$

zu einer Gruppe, der ***Faktorgruppe*** G/N *von* G *nach* N. *Die kanonische Projektion* $p_N : G \to G/N$ *ist ein Homomorphismus mit* $Kern(p_N) = N$.

(ix) ***Homomorphiesatz***
Ist $f : G \to G'$ *ein Homomorphismus, so gilt* $G/Kern(f) \cong Bild(f)$.
Folgerung: $|G| = |Kern(f)| \cdot |Bild(f)|$.

(x) ***Erster Isomorphiesatz***
Seien H, K *Untergruppen einer Gruppe* G *mit* $hKh^{-1} = K$ *für alle* $h \in H$. *Dann gilt:*

$$H/(H \cap K) \cong HK/K.$$

(xi) ***Zweiter Isomorphiesatz***
Sei $K \subset N$ Normalteiler einer Gruppe G. Dann ist N/K Normalteiler in G/K und

$$G/N \cong (G/K)/(N/K)$$

Definition 2.25 (Operationen von Gruppen auf Mengen)**.**
Sei G eine Gruppe und M eine nichtleere Menge. G ***operiert auf*** *M, falls ein Produkt $G \times M \to M$ definiert ist mit*

$$\begin{aligned} ex &= x \text{ für alle } x \in M, \\ g(hx) &= (gh)x \text{ für alle } x \in M,\ g, h \in G. \end{aligned}$$

Beispiel 2.26.

(i) *Die spezielle lineare Gruppe*

$$SL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} \middle| ad - bc = 1 \right\}$$

operiert durch die gebrochen linearen Funktionen auf der oberen Halbebene

$$\mathbb{H} = \{z \in \mathbb{C} | Im(z) > 0\},$$

d.h. das Produkt

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}$$

liegt auch wieder in $\mathbb{H}$.

(ii) *Die in der Topologischen Quantenfeldtheorie und Stringtheorie bekannte endliche Gruppe*

$$G = \left\{ (\xi_0, \xi_1, \xi_2, \xi_3, \xi_4) \in \mathbb{C}^5 \middle| \xi_i^5 = 1 \text{ und } \prod_{i=0}^{4} \xi_i = 1 \right\}$$

operiert auf dem projektiven Raum $\mathbb{CP}^4$ *via*

$$\begin{aligned} G \times \mathbb{CP}^4 \to \mathbb{CP}^4 &= (\xi_0, \xi_1, \xi_2, \xi_3, \xi_4) \cdot (x_0 : x_1 : x_2 : x_3 : x_4) \\ &= (\xi_0 x_0 : \xi_1 x_1 : \xi_2 x_2 : \xi_3 x_3 : \xi_4 x_4) \end{aligned}$$

Bzgl. der Restriktion

$$G \times Y_z \to Y_z$$

erhält diese Gruppenoperation z.B. die quintischen Hyperflächen $Y_z \subset \mathbb{CP}^4$*, die durch die Gleichungen*

$$x_0^5 + x_1^5 + x_2^5 + x_3^5 + x_4^5 - 5z x_0 x_1 x_2 x_3 x_4 = 0$$

mit dem komplexen Parameter z *definiert sind.*

Definition 2.27 (Bahn bzw. Orbit)**.**
Für $x \in M$ *heißt* $Gx := \{gx | g \in G\}$ ***Bahn*** *oder* ***Orbit*** *von* x *unter der Operation von* G *auf* M*.*
Die Operation von G *auf* M *heißt* ***transitiv****, falls nur eine Bahn in* G *von* M *existiert, d.h. zu allen* $y, z \in M$ *gibt es* $g \in G$ *mit* $z = gy$*.*

Bemerkung 2.28.
Zwei Bahnen sind entweder gleich oder disjunkt und M *ist die disjunkte Vereinigung der verschiedenen Bahnen.*

Definition 2.29 (Transformationsgruppe)**.**
Eine Transformation einer Menge M *ist eine bijektive Abbildung* $f : M \to M$*. Eine Menge* G *von Transformationen von* M *heißt auch Transformationsgruppe, wenn die Komposition* $g_1 \circ g_2$ *für* g_1 *und* g_2 *aus* G *erklärt ist und das Inverse* g^{-1} *(die existierende Umkehrabbildung) sowie die identische Abbildung id (das neutrale Element* e *von* G*) zu* G *gehören. Offensichtlich erfüllen diese Daten die Gruppenaxiome. Ein schon bekanntes Beispiel ist die symmetrische Gruppe* S_n*.*

Satz 2.30 (Cayley)**.**
Jede Gruppe G *ist isomorph zu einer Transformationsgruppe.*

Beweis
Seien $g_1, g_2 \in G$. Wir betrachten die Abbildung $T_g : G \to G$, $T_g(x) = gx$ und behaupten, dass $T_G = \{T_g | g \in G\}$ die Gruppenaxiome erfüllt.

(i) Wegen $T_{g_1} T_{g_2} : x \to g_1(g_2 x) = (g_1 g_2)x$ und $T_{g_1 g_2} : x \to (g_1 g_2)x$ liegt eine Verknüpfung von $T_g \times T_g \to T_g$ vor, und das Assoziativgesetz ist aufgrund der Komposition von Abbildungen erfüllt.

(ii) Mit der Beobachtung $T_g T_{g-1} : x \to g(g^{-1}) = x = id$ und $T_{g-1} T_g : x \to g^{-1}(gx) = x = id$ ergibt sich das inverse Element zu T_{g-1}.

(iii) Mit $T_e : x \to ex = x$ ist die Identität das neutrale Element. Es bleibt noch zu zeigen, dass $f : G \to T_G$, $f(g) = T_g$ ein Gruppenisomorphismus ist. Offensichtlich ist f wegen $f(g_1 g_2) = T_{g_1 g_2} = T_{g_1} T_{g_2} = f(g_1) f(g_2)$ ein Homomorphismus. Da jedes T_g das Urbild g besitzt, ist f surjektiv. Schließlich ist f injektiv. Wir zeigen: $f(g_1) = f(g_2) \Rightarrow g_1 = g_2$. Sei also $T_{g_1} = T_{g_2}$, d.h. es folgt $g_1 = T_{g_1}(e) = T_{g_2}(e) = g_2$.

Definition 2.31 (Freie Gruppe)**.**
Es sei G eine Gruppe und $E \subset G$ ein Erzeugendensystem von G. Dann hat jedes Element $g \in G, g \neq 1$, eine Darstellung der Form $g = x_1^{n_1} \cdot \ldots \cdot x_k^{n_k}$ mit $x_1, \ldots, x_k \in E$ und $n_1, \ldots, n_k \in \mathbb{Z}$. Diese Darstellung ist i.a. nicht eindeutig, da zwischen den Elementen von E gewisse Relationen gelten können. Bei diesen Relationen unterscheidet man zwischen 'allgemeinen' oder speziellen Relationen. Die ersten folgen aus den Gruppenaxiomen und gelten daher in jeder Gruppe, z.B. $xx^{-1} = x^{-1}x = 1$. Die speziellen Relationen sind diejenigen, die nicht aus Gruppenaxiomen folgen und nur in bestimmten Gruppen gelten; z.B. gilt in abelschen Gruppen die spezielle Relation $xy = yx$, und in Gruppen der Ordnung n gilt die spezielle Relation $x^n = 1$. Die Gruppe der ganzzahligen $(2,2)$-Matrizen mit Determinante $+1$ wird von den Matrizen $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ erzeugt, und es gelten die speziellen Relationen $A^2 B^{-3} = 1$ und $A^4 = 1$. Eine Gruppe, in der keine spezielle Relationen gelten, heißt eine freie Gruppe.

Definition 2.32.
Ein Erzeugendensystem E einer Gruppe heißt frei (oder: E erzeugt G frei), wenn gilt: besteht in G eine Relation $x_1^{\epsilon_1} \cdot \ldots \cdot x_k^{\epsilon_k} = 1$ mit $x_1, \ldots, x_k \in E$ und $\epsilon_1, \ldots, \epsilon_k \in \{-1, 1\}$, so gibt es ein j mit $1 \leq j \leq k-1$ und $x_j = x_{j+1}$ und $\epsilon_j = -\epsilon_{j+1}$. Eine Gruppe heißt freie Gruppe, wenn sie ein freies Erzeugendensystem besitzt. Nun stellt sich natürlich sofort die Frage nach der Existenz freier Gruppen: gibt es überhaupt freie Gruppen? Die Beantwortung liefert:

Satz 2.33.
Sei n eine positive Zahl. Dann gibt es eine freie Gruppe, die durch eine Menge von n Elementen frei erzeugt wird. Da nun die Dartstellung eines Elements $g \neq 1$ einer freien Gruppe G eindeutig ist, folgt aus:

Satz 2.34.
Sei E ein freies Erzeugendensystem der freien Gruppe G. Dann hat jedes von 1 verschiedene Element $x \in G$ eine eindeutig bestimmte Darstellung der Form $x = x_1^{n_1} \cdot \ldots \cdot x_k^{n_k}$ mit $x_1, \ldots, x_k \in E$, $n_1, \ldots, n_k \in \mathbb{Z} - \{0\}$ und $x_j \neq x_{j+1}$ für $1 \leq j \leq k-1$. Aus der linearen Algebra ist bekannt, dass ein Vektorraumhomomorphismus durch die Bilder der Elemente einer Basis bestimmt wird. Für eine freie Gruppe analog:

Satz 2.35.
Sei E ein freies Erzeugendensystem der Gruppe G und sei H eine beliebige Gruppe. Dann gibt es zu jeder Funktion $S : E \to H$ genau einen Homomorphismus $S^* : G \to H$ mit $S^*|E = S$. Also genügt es auch hier die Bilder der freien Erzeugenden anzugeben, um einen Homomorphismus $G \to H$ zu bestimmen.

Satz und Definition 2.36.
Je zwei freie Erzeugendensysteme einer freien Gruppe haben gleiche Mächtigkeit; diese Mächtigkeit heißt der Rang der freien Gruppe. Zwei freie Gruppen sind genau dann isomorph, wenn sie gleichen Rang haben. Zu jeder Kardinalzahl α gibt es eine freie Gruppe vom Rang α.

Weitere bekannte Eigenschaften von freien Gruppen sind:

(i) Eine von einer Menge E mit mindestens 2 Elementen frei erzeugte Gruppe ist nicht abelsch.

(ii) *Eine endliche Gruppe G ist nicht frei, wenn $G \neq 1$.*

(iii) *Eine freie Gruppe von E mit $|E| \geq 2$ frei erzeugt, hat triviales Zentrum, d.h. das Zentrum enthält nur das Einselement.*

(iv) *Jede Untergruppe H einer freien Gruppe ist frei.*

3. Artinsche Zopfgruppen

In diesem Abschnitt sollen die Artinschen Zopfgruppen eingeführt werden. Deshalb beginnen wir mit der

Definition 3.1.
Die Artinschen Zopfgruppen B_n werden durch die $(n-1)$ Generatoren $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ erzeugt, die den Relationen

$$\sigma_i \sigma_j = \sigma_j \sigma_i \text{ für } |i-j| > 1$$

und

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \text{ für } |i-j| = 1$$

genügen.

Bemerkung 3.2.

(i) Per definitionem ist $B_1 = \{1\}$ die triviale Gruppe.

(ii) Die Gruppe B_2 wird durch einen Generator erzeugt und die Menge der Relationen ist leer. Also ist B_2 eine unendliche zyklische Gruppe und isomorph zu den ganzen Zahlen $\mathbb{Z}$.
Klar, denn $f : B_2 \to \mathbb{Z};\ \sigma^k \mapsto k$ ist offensichtlich der gewünschte Isomorphismus.

Zur Wiederholung soll das Rechnen mit Generatoren geübt werden.

Beispiel 3.3.

$$G = \langle a, b, c, d, e \mid d = e^2, bda = 1, ab^{-1}c = 1, ac^{-1}b^{-1} = 1, de = c \rangle$$

ist isomorph zur zyklischen Gruppe der Ordnung 12. Wir entfernen sukzessive alle Generatoren bis wir die Präsentation $\langle a | a^{12} = 1 \rangle$ erhalten und beginnen mit $d = e^2$ um d zu eliminieren.

Beweis
Wir benutzen die erste Relation $d = e^2$ um den Generator d zu entfernen. So erhalten wir die Darstellung

$$\langle a, b, c, e \mid be^2a = 1, ab^{-1}c = 1, ac^{-1}b^{-1} = 1, e^3 = c\rangle.$$

Mit der letzten Gleichung $c = e^3$ entfernen wir c:

$$\langle a, b, e \mid be^2a = 1, ab^{-1}e^3 = 1, ae^{-3}b^{-1} = 1\rangle$$

Mit $b = e^3a \;\Leftrightarrow\; ab^{-1}e^3 = 1$ entfernen wir b:

$$\langle a, e \mid e^3ae^2a = 1, ae^{-3}a^{-1}e^{-3} = 1\rangle \text{ oder } \langle a, e \mid e^3ae^2a = 1, e^3ae^3 = a\rangle$$

Umschreiben der ersten Gleichung zu $e^3ae^3e^{-1}a = 1$ und ersetzen von e^3ae^3 durch a ergibt die Darstellung

$$\langle a, e \mid ae^{-1}a = 1, e^3ae^3 = a\rangle \text{ oder } \langle a, e \mid e = a^2, e^3ae^3 = a\rangle.$$

Schließlich entfernen wir e mit der ersten Relation und erhalten die Darstellung $\langle a \mid a^6aa^6 = a\rangle$, i.e. $\langle a \mid a^{12} = 1\rangle$. Das ist die zyklische Gruppe der Ordnung 12.

Beispiel 3.4.
Gegeben sei die Artinsche Zopfgruppe B_3 mit den Generatoren σ_1 und σ_2. Mit $\Delta = \Delta_3 = \sigma_1\sigma_2\sigma_1$ gilt:

(i) $\Delta\sigma_1 = \sigma_2\Delta$,

(ii) $\Delta\sigma_2 = \sigma_1\Delta$,

(iii) Δ^2 *kommutiert mit beiden Generatoren.*

Beweis
Offensichtlich ist $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ die einzige Relation in B_3.
(i) $\Delta\sigma_1 = \sigma_1\sigma_2\sigma_1\sigma_1 = \sigma_2\sigma_1\sigma_2\sigma_1 = \sigma_2\Delta$.
(ii) $\Delta\sigma_2 = \sigma_1\sigma_2\sigma_1\sigma_2 = \sigma_1\sigma_1\sigma_2\sigma_1 = \sigma_1\Delta$.
(iii)

$$\begin{aligned}
\Delta^2\sigma_1 &= \sigma_1\sigma_2\sigma_1\underline{\sigma_1\sigma_2\sigma_1}\sigma_1 \\
&= \sigma_1\underline{\sigma_2\sigma_1\sigma_2}\sigma_1\sigma_2\sigma_1 \\
&= \sigma_1\sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1 \\
&= \sigma_1\Delta^2
\end{aligned}$$

$$\begin{aligned}\Delta^2\sigma_2 &= \underline{\sigma_1\sigma_2\sigma_1}\sigma_1\sigma_2\sigma_1\sigma_2\\ &= \sigma_2\sigma_1\sigma_2\sigma_1\underline{\sigma_2\sigma_1\sigma_2}\\ &= \sigma_2\sigma_1\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\\ &= \sigma_2\Delta^2\end{aligned}$$

Beispiel 3.5.
In der Zopfgruppe B_n, $(n > 2)$ folgt für zwei Zöpfe mit $\beta^n = \gamma^n$ nicht notwendig $\beta = \gamma$, d.h. es gibt keine eindeutig bestimmten Wurzeln.

Beweis
Seien $\beta = \sigma_1\sigma_2$ und $\gamma = \sigma_2\sigma_1$ aus B_3. Dann gilt:

$$\begin{aligned}&\beta^3 = (\sigma_1\sigma_2)^3 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\\ &= \sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1 = (\sigma_2\sigma_1)^3 = \gamma^3\end{aligned}$$

Man hat $\beta^3 = \gamma^3$, aber $\beta \neq \gamma$.

Beispiel 3.6.
Ein beliebiges Produkt eines nicht trivialen konjugierten Zopfes kann trivial sein.

Beweis
Sei $\Delta_3 = \sigma_1\sigma_2\sigma_1$ und $\beta = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$. Konjugation von β mit Δ_3 ergibt $\Delta_3\beta\Delta_3^{-1}$ und durch Multiplikation mit β folgt $\beta\Delta_3\beta\Delta_3^{-1} = 1$
Genauer:

$$\begin{aligned}\Delta_3\beta\Delta_3^{-1} &= \underline{\sigma_1\sigma_2\sigma_1}\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\\ &= \sigma_2\sigma_1\underline{\sigma_2\sigma_1\sigma_2}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\\ &= \sigma_2\sigma_1\sigma_1\underline{\sigma_2\sigma_1\sigma_1^{-1}\sigma_2^{-1}}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\\ &= \sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\end{aligned}$$

, also $\beta\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1} = 1$.

Beispiel 3.7.
Wir zeigen die folgenden Relationen in B_3:

(i) $\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2$

(ii) $\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1} = \sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$

(iii) $\sigma_1^{-1}\sigma_2^{-1}\sigma_1 = \sigma_2\sigma_1^{-1}\sigma_2^{-1}$

(iv) $\sigma_1\sigma_2^{-1}\sigma_1^{-1} = \sigma_2^{-1}\sigma_1^{-1}\sigma_2$

(v) $\sigma_1^{-1}\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2^{-1}$

Beweis

(i) Es gilt $\sigma_1 = \sigma_1$, also

$$\sigma_1\sigma_2\sigma_1^{-1}\sigma_1\sigma_2^{-1}\sigma_1 = \sigma_2^{-1}\sigma_2\sigma_1\sigma_2\sigma_2^{-1}$$

d.h.

$$\sigma_1\sigma_2\sigma_1^{-1}\sigma_1\sigma_2^{-1}\sigma_1 = \sigma_2^{-1}\sigma_1\sigma_2\sigma_1\sigma_2^{-1}$$

und nach Multiplikation mit $\sigma_2\sigma_1^{-1}$ folgt

$$\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_2\sigma_1^{-1}$$

d.h.

$$\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2,$$

also die Behauptung.

(ii) Das ist die Inversenbildung der Relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$.

(iii) Aus $\sigma_1^{-1}\sigma_2^{-1} = \sigma_1^{-1}\sigma_2^{-1}$ folgt

$$\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_1 = \sigma_1^{-1}\sigma_2^{-1}.$$

Mit (ii) hat man

$$\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1 = \sigma_2^{-1}\sigma_2\sigma_1^{-1}\sigma_2^{-1}.$$

Multiplikation mit σ_2 ergibt schließlich die Behauptung.

(iv) Das ist die Inversenbildung von (i).

(v) Hier liegt das Inverse von (iii) vor.

Bemerkung 3.8.
Die Umformungen (i) und (iii) kann man auch von „unten nach oben“ lesen, weil alle Umformungen umkehrbar (äquivalent) sind.

Definition 3.9.
*Ein Zopfwort w heißt **σ-positiv** (**σ-negativ**), wenn unter den Buchstaben, die in w erscheinen nur der Buchstabe mit dem kleinsten Index positiv ist, d.h. σ_i erscheint, aber σ_i^{-1} nicht. Entsprechendes gilt für σ-negativ, d.h. hier erscheint σ_i^{-1}, aber nicht σ_i.*

Beispiel 3.10.
Das Zopfwort $\sigma_3\sigma_2\sigma_3^{-1}$ ist σ-positiv. Der Buchstabe mit dem kleinsten Index ist σ_2, denn es gibt kein $\sigma_1^{\pm}$. Weiterhin kommt nur σ_2 und nicht σ_2^{-1} vor. Im Gegensatz dazu ist $\sigma_2^{-1}\sigma_3\sigma_2$, welches äquivalent zu $\sigma_3\sigma_2\sigma_3^{-1}$ ist, weder σ-positiv noch σ-negativ. Der Buchstabe mit dem kleinsten Index ist wieder σ_2, aber beide Buchstaben σ_2^{-1} und σ_2 erscheinen.

Bemerkung 3.11.
Dass $\sigma_3\sigma_2\sigma_3^{-1}$ äquivalent zu $\sigma_2^{-1}\sigma_3\sigma_2$ ist, sieht man leicht ein:

$$\sigma_2^{-1}\sigma_3\sigma_2 = \sigma_2^{-1}\sigma_3\sigma_2\sigma_3\sigma_3^{-1} = \sigma_2^{-1}\sigma_2\sigma_3\sigma_2\sigma_3^{-1} = \sigma_3\sigma_2\sigma_3^{-1}$$

Dazu vergleiche auch Beispiel 3.7 (v).

Definition 3.12.
Seien die Wörter w_1 und w_2 aus B_n. Dann gilt $w_1 <_n w_2$, wenn $w_1^{-1}w$ ein äquivalentes Wort aus B_n besitzt, das σ-positiv ist.

Beispiel 3.13.
Sei $w_1 = \sigma_2$ und $w_1 = \sigma_3\sigma_2$. Unter den Wörtern aus B_4, die den Quotienten $(\sigma_2)^{-1}\sigma_3\sigma_2$ repräsentieren ist $\sigma_2^{-1}\sigma_3\sigma_2$ ein Wort, das weder σ-positiv noch σ-negativ ist. Aber es gibt das äquivalente Wort $\sigma_3\sigma_2\sigma_3^{-1}$ (und viele andere), das σ-positiv ist. Da $\sigma_3\sigma_2\sigma_3$ ein σ-positives Wort aus B_4 ist, gilt $\sigma_2 <_4 \sigma_3\sigma_2$.

Satz 3.14.
Ein σ-positives Zopfwort ist nicht trivial.

Beweis. In [Dehor] werden vier verschiedene Beweise gegeben, vgl. S.73, 175, 190 und 224. □

Definition 3.15.
Sei w ein Zopfwort. Dann ist die Verschiebung (shifting) $sh(w)$ von w definiert, indem man jeden Buchstaben σ_i in w durch σ_{i+1} und jedes σ_i^{-1} durch σ_{i+1}^{-1} ersetzt.

Definition 3.16.
Ein Zopfwort w heißt σ_i-positiv, wenn es wenigstens den Buchstaben σ_i enthält, aber weder σ_i^{-1} noch $\sigma_j^{\pm 1}$ mit $j < i$. Analog heißt w σ_i-negativ, wenn es wenigstens σ_i^{-1} enthält, aber weder σ_i noch ein $\sigma_j^{\pm 1}$ mit $j < 1$. Schließlich heißt w σ_i-frei, wenn es kein $\sigma_j^{\pm 1}$ enthält mit $j \leq i$.

Beispiel 3.17.

(i) $\sigma_2\sigma_3$ *ist* σ_2*-positiv.*

(ii) $\sigma_2^{-1}\sigma_3\sigma_2$ *ist* σ_2*-positiv* ***innerhalb*** B_4*, weil es äquivalent zu* $\sigma_3\sigma_2\sigma_3^{-1}$ *ist.*

Sei $B_\infty = \bigcup_{n\geq 1} B_n$ der induktive Limes der Gruppen B_n bezüglich der Inklusionen i. Per definitionem liegt jedes Element von B_∞ in irgendeinem B_n. Die Gruppenstruktur von B_∞ ist eine natürliche Erweiterung der Gruppenstruktur B_n. B_∞ besitzt unendlich viele Generatoren $\sigma_1, \sigma_2, \ldots$, die den bekannten Relationen gehorchen.

Zur Erinnerung:
Der Homomorphismus $i : B_n \mapsto B_{n+1}$, $i(\sigma_i) = \sigma_i$ mit $i = 1, 2, \ldots, n-1$ definiert einen injektiven Gruppenhomomorphismus und heißt auch natürliche Inklusion.

Satz 3.18.
Es gilt

$$\sigma_1 >_\infty \sigma_2 >_\infty \sigma_3 >_\infty \ldots$$

Beweis.
Offensichtlich ist $\sigma_{i+1}^{-1}\sigma_i$ für jedes i σ-positiv. □

Definition 3.19.
Sei G eine Gruppe. Eine Teilmenge $\mathcal{P} \subset G$ mit $e \in \mathcal{P}$ heißt ***Kegel****, wenn gilt*

(i) $\mathcal{P} \cdot \mathcal{P} \subseteq \mathcal{P}$, *d.h.* $\mathcal{P}$ *ist eine Unterhalbgruppe von* G;

(ii) $\mathcal{P} \cup \mathcal{P}^{-1} = G$, *mit* $\mathcal{P}^{-1} = \left\{x \in G \middle|\ x^{-1} \in \mathcal{P}\right\}$

(iii) $\mathcal{P} \cap \mathcal{P}^{-1} = \{e\}$.

Bemerkung 3.20.

(i) Eine Teilmenge $\mathcal{P} \subset G$ *heißt* ***positiver Kegel*** *(auf* G*), wenn* $\mathcal{P}$ *unter der Multiplikation abgeschlossen und* $G - \{e\}$ *die disjunkte Vereinigung von* P *und* P^{-1} *ist (s. Dehornoy).*

(ii) Insbesondere bei Dubrovin besitzt ein Kegel die Eigenschaften (i) und (ii). Hat er zusätzlich noch die Eigenschaft (iii) wird er "principal cone", d.h. Prinzipalkegel oder Hauptkegel bzw. auch "pure cone", d.h. reiner Kegel, genannt.

Beispiel 3.21.
$(\mathbb{Z}, +)$ *ist ein Kegel mit* $P = \mathbb{Z}^+ = \{n \in \mathbb{Z} |\ n \geq 0\}$ *und* $P^{-1} = \mathbb{Z}^- = \{n \in \mathbb{Z} |\ n \leq 0\}$.

Definition 3.22.
Eine Ordnung " $\leq$ *" auf einer Gruppe heißt* ***Rechtsordnung*** *(rechtsinvariant) bzw. die Gruppe heißt rechtsorderable, wenn gilt:*

$$x \leq y \ \Rightarrow xz \leq yz \quad \text{für alle } x, y, z \in G.$$

Entsprechend wird eine ***Linksordnung*** *definiert, d.h. es gilt:*

$$x \leq y \ \Rightarrow zx \leq zy \quad \text{für alle } x, y, z \in G.$$

Eine natürliche Fragestellung ist jetzt: Ist eine gegeben Gruppe orderabel (links- und rechtsorderabel) oder wenigstens rechtsorderabel (linksorderabel)?

Satz und Definition 3.23.

(i) Eine Gruppe G *heißt rechtsorderabel, wenn ein Kegel* $\mathcal{P} \subset G$ *existiert. In diesem können wir eine (totale) Rechtsordnung "* $\leq_r$ *" mit* $x \leq_r y \Leftrightarrow yx^{-1} \in \mathcal{P}$ *definieren.*

(ii) Umgekehrt, wenn eine totale Ordnung " $\leq$ " auf der Menge G mit $x \leq y \Rightarrow xz \leq yz$ für alle $z \in G$ existiert, dann erfüllt $P = \{g \in G | e \leq g\}$ offensichtlich die Bedingungen eines Kegels.

(iii) P definiert auch eine Linksordnung: $x \leq_l y \Leftrightarrow x^{-1}y \in P$.

Satz 3.24.
Dir durch $\mathcal{P}$ definierte Rechtsordnung ist äquivalent zur (durch $\mathcal{P}$ definierten) Linksordnung, genau dann wenn $g\mathcal{P}g^{-1} = \mathcal{P}$ für alle g in G gilt.

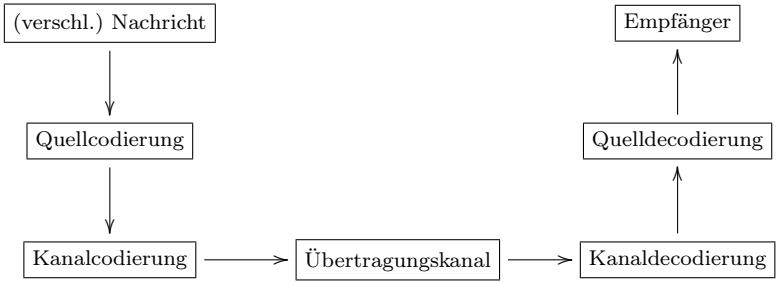
Beweis.
" $\Rightarrow$ ": Wir nehmen die Äquivalenz $x \leq_l y \Leftrightarrow x \leq_r y$ an und wollen zeigen $g\mathcal{P}g^{-1} = \mathcal{P}$. Also sei $p \in \mathcal{P}, g \in G$, dann folgt $e \leq p \Rightarrow geg^{-1} = e \leq gpg^{-1} \in \mathcal{P}$. Weiterhin folgt aus $g\mathcal{P}g^{-1} \subseteq \mathcal{P}$ (durch Multiplikation mit g bzw g^{-1}) offensichtlich $\mathcal{P} \subseteq g^{-1}\mathcal{P}g \subseteq \mathcal{P}$, d.h. $g\mathcal{P}g^{-1} = \mathcal{P}$.
" $\Leftarrow$ " Annahme $g\mathcal{P}g^{-1} = \mathcal{P}$. Wir wollen zeigen: $yx^{-1} \in \mathcal{P} \Leftrightarrow x^{-1}y \in \mathcal{P}$. Man hat $x^{-1}(yx^{-1})x = x^{-1}y \in \mathcal{P}$, wenn $yx^{-1} \in \mathcal{P}$, sowie $y^{-1}(xy^{-1})y = y^{-1}x \in \mathcal{P}$, wenn $xy^{-1} \in \mathcal{P}$. □

Theorem 3.25 (Dubrovin)**.**
Die Überlagerungsgruppe von $SL(2, \mathbb{R})$ ist rechtsorderabel, d.h. besitzt einen Kegel $\mathcal{P}$. Sie ist aber nicht orderabel, d.h. sie hat keinen Kegel $\mathcal{P}$ mit $g\mathcal{P}g^{-1} = \mathcal{P}$.

Bemerkung 3.26.
Ähnlich sind die Zopfgruppen rechtsorderabel, aber nicht orderabel. Gewöhnlich besitzen sie viele Kegel $\mathcal{P}$, aber keinen Kegel mit $g\mathcal{P}g^{-1} = P$.

Anwendung 3.27 (Zopfgruppen in der Kryptologie)**.**
*In diesem Abschnitt werden einige Anwendungen der Zopfgruppen in der Kryptologie behandelt. Bezüglich der **Kryptographie**, darunter verstehen wir die Verschlüsselung(Chiffrierung) und Entschlüsselung(Dechiffrierung) von Daten, wird insbesondere gezeigt, wie man in der „Public-Key-Kryptographie" einen gemeinsamen Schlüssel erzeugen kann.*

Um diesen Abschnitt autark zu gestalten, werden noch einmal die wichtigsten Feststellungen aus der Codierungstheorie wiederholt. Die wichtigsten Kriterien eines Übertragungskanals kann man grob durch folgende Skizze ausdrücken:



Die eventuell schon verschlüsselte Nachricht wird in der **Quellcodierung** für die Datenendgeräte in eine Binärzeichenfolge transformiert. Schließlich wird bzgl. der **Kanalcodierung** die Bitfolge noch mit Prüfinformationen zum Erkennen bzw. Korrigieren etwaiger während der Übertragung der Nachricht auftretender Fehler versehen.

Definition 3.28.
Seien x und y Codewörter der Länge n über einem Alphabet A. Dann ist die Hamming-Distanz gegeben durch

$$d_H(x,y) = \sum_{i=1}^{n} d(x_i, y_i) \text{ mit } d(x_i, y_i) = \begin{cases} 1, & \text{für } x_i = y_i \\ 0, & \text{für } x_i \neq y_i \end{cases}$$

Die Hamming-Distanz zählt also die Stellen in denen sich die Codewörter unterscheiden und erfüllt offensichtlich die Eigenschaften einer Metrik. Weiterhin ist bzgl. eines Codes C der mindestens zwei Wörter enthält der minimale Abstand wichtig: $d_{min}(C) = min\{d(x,y)|x,y \in C, x \neq y\}$.

Beispiel 3.29.
Gegeben sei der binäre Code $C = \{0000, 0011, 1111\}$. Man sagt dann auch, C sei ein $(4,3,2)$-Code, da die Länge der Wörter gleich vier ist, der Code aus drei Wörtern besteht und schließlich der minimale Abstand gleich zwei ist.

Das wesentliche Ergebnis ist nun:

Satz 3.30.

(i) Ein Code ist n-fehlererkennend genau dann, wenn $d_{min}(C) \geq n+1$ *gilt. Ein Abstand* d $(= d_{min})$ *ist also ein* $(d-1)$*-fehlererkennender Code.*

(ii) Ein Code C ist m-fehlerkorrigierend genau dann, wenn $d_{min}(C) \geq 2m+1$ *gilt. Ein Code mit dem minimalen Abstand d ist als genau ein* $[\frac{d-1}{2}]$*-fehlerkorrigierender Code. Hier bezeichnet, wie üblich,* $[x]$ *die Gauß-Klammer, d.h. die größte ganze Zahl kleiner gleich x.*

Beispiel 3.31.

(i) Der binäre Code $C = \{00000, 10011, 11111\}$ *ist 1-fehlererkennend.*

(ii) Der binäre Code $C = \{00000, 01111\}$ *ist 1-fehlerkorrigierend.*

Eine natürliche Fragestellung ist nun: Wie leicht kann man einen Code brechen? Dazu gibt es eine Vielzahl von Beispielen: die Enigma, der Navajo-Code,...

Wir notieren hier

Beispiel 3.32.
Der ***Vernam-Code*** *wurde 1917 von Gilbert Vernam eingeführt, aber erst über dreißig Jahre später konnte Shannon zeigen, dass er nicht zu brechen ist.*

Das Protokoll des Vernam-Codes lautet:

1) Der Quelltext wird als binäre Sequenz von Nullen und Einsen geschrieben(codiert).

2) Der geheime Schlüssel ist eine (vollständig) zufällige binäre Folge derselben Länge wie der Quelltext.

3) Man erhält den verschlüsselten Text indem man den Schlüssel zum Quelltext modulo zwei addiert, also $c_i = p_i \oplus k_i$ *für* $i = 1, 2, ..., N$.

Dabei wurde die in der angloamerikanischen Literatur übliche Bezeichnungen cypher text, plain text und secret key benutzt. Die Entschlüsselung erfolgt via $p_i = c_i \oplus k_i$ *für* $i = 1, 2, ..., N$.

Quelltext:	*01011110*
Schlüssel:	*10001011*
verschl. Nachricht:	*11010101*

Wenn der Schlüssel immer zufällig gewählt wird, ist der Code nicht zu brechen, da der codierte Text keine Rückschlüsse auf den Quelltext zulässt. Ein Problem ist aber dann der regelmäßige Schlüsselaustausch.

Es stellt sich jetzt die Frage, ob man nicht einen öffentlichen Schlüssel benutzen kann. Eine einfache Methode ist folgendes Protokoll.

1. *Alice und Bob einigen sich auf eine endliche, zyklische Gruppe und ein erzeugendes Element g in G. Diese Daten sind öffentlich.*
2. *Alice denkt sich eine Geheimzahl a und sendet g^a zu Bob.*
3. *Bob wählt die Geheimzahl b und sendet g^b zu Alice.*
4. *Alice berechnet $K_A = (g^b)^a = g^{ba} = g^{ab}$ und Bob berechnet $K_B = (g^a)^b = g^{ab}$.*

Da eine zyklische Gruppe abelsch ist, kann jetzt g^{ab} als gemeinsamer Schlüssel verwendet werden.

Beispiel 3.33.
Eine Möglichkeit ist das Ko-et al. Schlüsselaustauschprotokoll, vgl. Garber in [Ber 10, S. 351].

Öffentlicher Schlüssel:	*Ein Zopf P in B_n*
Privater Schlüssel von Alice:	*Ein Zopf s aus LB_n*
Privater Schlüssel von Alice:	*Ein Zopf r aus UB_n*

Dabei bezeichnet LB_n die Untergruppe von B_n, die von den Generatoren $\sigma_1, ..., \sigma_{m-1}$ erzeugt wird mit $m = \lfloor \frac{n}{2} \rfloor$.
Entsprechend ist UB_n die von den Generatoren $\sigma_{m+1}, ..., \sigma_{n-1}$ erzeugte Untergruppe.

Alice sendet Bob die Nachricht: $N_A = sPs^{-1}$.
Bob sendet Alice die Nachricht: $N_B = rPr^{-1}$.

Der geheime gemeinsame Schlüssel ist nun: $K = srPr^{-1}s^{-1}$.

Alice kennt nun s, s^{-1} *und* P.

Sie empfängt N_B *und kann nun* $K = sN_Bs^{-1}$ *berechnen.*

Bob dagegen besitzt r, r^{-1} *und* P, *d.h. er kann mit der empfangenen Nachricht* N_A *auch* $K = rN_Ar^{-1}$ *berechnen, denn aufgrund der gemachten Vorraussetzungen kommutieren* r *und* s.

Zur Illustration:

Wir wählen die Zopfgruppe B_{12} *und* $s = \sigma_4\sigma_5\sigma_2$ *sowie* $r = \sigma_7\sigma_{10}\sigma_9$ *und den öffentlichen Schlüssel* $P = \sigma_1\sigma_2\sigma_3$.

Alice berechnet $srPr^{-1}s^{-1}$ *und Bob berechnet* $rsPs^{-1}r^{-1}$.

Nun gilt:

$$\begin{aligned} srPr^{-1}s^{-1} &= \sigma_4\sigma_5\sigma_2\sigma_7\sigma_{10}\sigma_9\sigma_1\sigma_2\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1}\sigma_2^{-1}\sigma_5^{-1}\sigma_4^{-1} \\ &= \sigma_4\sigma_2\sigma_7\sigma_{10}\sigma_9\sigma_1\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1}\sigma_4^{-1} \\ &= \sigma_2\sigma_7\sigma_{10}\sigma_9\sigma_1\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1} \end{aligned}$$

sowie

$$\begin{aligned} rsPs^{-1}r^{-1} &= \sigma_7\sigma_{10}\sigma_9\sigma_4\sigma_5\sigma_2\sigma_1\sigma_2\sigma_8\sigma_2^{-1}\sigma_5^{-1}\sigma_4^{-1}\sigma_9^{-1}\sigma_8^{-1}\sigma_7^{-1} \\ &= \sigma_7\sigma_{10}\sigma_9\sigma_4\sigma_2\sigma_1\sigma_8\sigma_4^{-1}\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1} \\ &= \sigma_7\sigma_{10}\sigma_9\sigma_2\sigma_1\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1} \\ &= \sigma_2\sigma_7\sigma_{10}\sigma_9\sigma_1\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1} \end{aligned}$$

Wir haben also den gemeinsamen Schlüssel $K = \sigma_2\sigma_7\sigma_{10}\sigma_9\sigma_1\sigma_8\sigma_9^{-1}\sigma_{10}^{-1}\sigma_7^{-1}$ *gefunden.*

4. Wissenswertes über Ringe und Moduln

Es werden in diesem Kapitel einige Grundtatsachen über Ringe und Moduln, die bereits aus der (Linearen) Algebra bekannt sind, ohne Beweise wiederholt. Lediglich der Chinesische Restsatz für beliebige kommutative Ringe dürfte neu sein und wird bewiesen. In einer mündlichen Prüfung sollte der Beweis des Chinesischen Restsatzes stets parat sein.

Definition 4.1.
*Sei R eine nichtleere Menge. R heißt **Ring**, wenn zwei Abbildungen*

$$+ : R \times R \to R \quad \textit{und}$$
$$\cdot : R \times R \to R$$

gegeben sind, so dass gelten:

(i) $(R, +)$ *ist eine abelsche Gruppe,*

(ii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $(\forall x, y, z \in R)$ ***Assoziativgesetz**,*

(iii) $x \cdot (y + z) = x \cdot y + x \cdot z$ *und*
$(x + y) \cdot z = x \cdot z + y \cdot z$ $(\forall x, y, z \in R)$ ***Distributivgesetz**.*

Bemerkung 4.2.

*(i) R heißt **kommutativer Ring**, wenn R ein Ring ist und $\cdot$ zusätzlich kommutativ ist, d.h. $x \cdot y = y \cdot x$ für alle $x, y \in R$ gilt.*

(ii) R heißt Ring mit 1, falls R ein Ring ist und ein Element $1 \in R$ existiert mit $1 \cdot x = x \cdot 1$ für alle $x \in R$.

Im Folgenden wird unter "Ring" stets ein kommutativer Ring mit 1 verstanden. Nicht-kommutative Ringe werden explizit als solche gekennzeichnet.

Beispiel 4.3.
Die Menge der $n \times n$-Matrizen über $\mathbb{R}$ bildet für $n \geq 2$ einen nicht-kommutativen Ring.

Beispiel 4.4.

(i) $\mathbb{Z}$ *ist ein Ring.*

(ii) Jeder Körper ist ein Ring.

(iii) Ist R ein Ring, so ist die Menge der Polynome $R[T_1, ..., T_n]$ in den Unbestimmten $T_1, ..., T_n$ ein Ring.

(iv) Ist R ein Ring, so ist die Menge $R[T_1, T_2, T_3, ...]$ der Polynome in den abzählbar vielen Unbestimmten $T_1, T_2, T_3, ...$ ein Ring.

(v) Die Menge $\mathcal{O}(\mathbb{C})$ aller holomorphen Funktionen $\mathbb{C} \to \mathbb{C}$ bildet mit den kanonischen Verknüpfungen einen Ring.

(vi) Sei $M \neq \emptyset$ eine Menge. Die Menge $Abb(M, \mathbb{R})$ aller Abbildungen von M nach $\mathbb{R}$ bildet mit den kanonischen Verknüpfungen einen Ring.

Definition 4.5.
Sei R ein Ring und $S \subset R$ mit $S \neq \emptyset$. S heißt ***Unterring*** *von S, wenn S die 1 von R enthält und $x + y \in S$ sowie $xy \in S$ für alle $x, y \in S$ gelten.*

Definition 4.6.
Sei R ein Ring. Ein Element $e \in R$ heißt ***Einheit****, wenn es ein $x \in R$ mit $ex = 1$ gibt. Die Menge aller Einheiten von R wird mit R^* bezeichnet.*

Bemerkung 4.7.
$(R^*, \cdot)$ ist eine Gruppe.

Beispiel 4.8.

(i) $K^* = K \setminus \{0\}$ für jeden Körper

(ii) $\mathbb{Z}^* = \{-1, 1\}$

(iii) *In* $K[T]$ *(*K *Körper) sind die Einheiten die konstanten Polynome* $\neq 0$.

Definition 4.9.
$x \in R$ *heißt* ***Nullteiler****, wenn es ein* $y \neq 0$ *gibt mit* $xy = 0$. R *heißt* ***nullteilerfrei****, wenn* $R \neq \{0\}$ *gilt und* 0 *der einzige Nullteiler ist. Eine nullteilerfreier Ring wird auch* ***Integritätsring*** *genannt.*

Beispiel 4.10.

(i) $\mathbb{Z}$ *ist Integritätsring.*

(ii) *Alle Körper sind Integritätsringe.*

(iii) *Alle Polynomringe* $K[T_1, ..., T_n]$ *(*K *Körper) sind Integritätsringe.*

(iv) *Der nicht-kommutative Ring der* $n \times n$*-Matrizen über* $\mathbb{R}$ *besitzt für* $n \geq 2$ *Nullteiler.*

Satz 4.11.
Jeder endliche Integritätsring ist ein Körper.

Definition 4.12.
R, S *seien Ringe und* $\varphi : R \to S$ *eine Abbildung.*
φ *heißt* ***Ringhomomorphismus*** $:\Leftrightarrow$

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y), \\ \varphi(xy) &= \varphi(x)\varphi(y), \quad (x, y \in R) \\ \varphi(1) &= 1 \end{aligned}$$

(i) *Ein bijektiver Ringhomomorphismus heißt* ***Ringisomorphismus****.*

(ii) *Ein surjektiver Ringhomomorphismus heißt* ***Ringepimorphismus****.*

(iii) *Ein injektiver Ringhomomorphismus heißt* ***Ringmonomorphismus****.*

(iv) *Gilt* $R = S$*, so wird ein Ringhomomorphismus* ***Ringendomorphismus*** *genannt.*

(v) *Gilt $R = S$, so heißt ein Ringisomorphismus auch* ***Ringautomorphismus****.*

Bemerkung 4.13.
Ist φ ein Ringisomorphismus, so gilt dies auch für φ^{-1}.

Beispiel 4.14.
Ist S ein Unterring von R, so ist die Inklusion $S \hookrightarrow R$ ein Ringmonomorphismus.

Definition 4.15.
Zwei Ringe R und S heißen ***isomorph*** $:\Leftrightarrow$
Es gibt einen Ringisomorphismus $\varphi : R \to S$.
Man schreibt dann auch $R \cong S$.

Eine besondere Bedeutung in der Ringtheorie besitzen die Ideale, etwa vergleichbar mit der Rolle der Normalteiler in der Gruppentheorie.

Definition 4.16.
$\mathfrak{A} \subset R$ *heißt* ***Ideal*** $:\Leftrightarrow$
$\mathfrak{A}$ *ist Untergruppe von $(R, +)$ und $R\mathfrak{A} \subset \mathfrak{A}$ $(*)$.*
Dabei bezeichnet $R\mathfrak{A}$ die Menge $\{xa | x \in R, a \in \mathfrak{A}\}$. Man bezeichnet die Eigenschaft $(*)$ auch als ***Absorptionseigenschaft****.*

Bemerkung 4.17.
Sei $x \in R$. Dann ist $(x) := \{rx | r \in R\}$ ein Ideal.

Definition 4.18.
Die Ideale vom Typ (x) $(x \in R)$ heißen ***Hauptideale****. Ein Integritätsring, in dem jedes Ideal ein Hauptideal ist, heißt* ***Hauptidealring****.*

Beispiel 4.19.

(i) *$\mathbb{Z}$ ist Hauptidealring.*

(ii) *Jeder Körper K ist Hauptidealring.*

(iii) *Alle Polynomringe $K[T]$ (K Körper) sind Hauptidealringe.*

(iv) Der Ring $\mathbb{Z}\left[\sqrt{-1}\right]$ *der Gaußschen Zahlen ist ein Hauptidealring.*

Bemerkung 4.20.
Der Durchschnitt beliebig vieler Ideale in einem Ring ist wieder ein Ideal.

Definition 4.21.
Ist $(\mathfrak{A}_j)_{j\in J}$ *eine Familie von Idealen in* R*, so nennt man*

$$\sum_{j\in J}\mathfrak{A}_j := \left\{ \sum_{j\in J} a_j \middle| a_j \in \mathfrak{A}_j \text{ und } a_j \neq 0 \text{ nur für endlich viele } j \right\}$$

die ***Summe*** *der Ideale* $\mathfrak{A}_j$*.*

Bemerkung 4.22.
$\sum_{j\in J}\mathfrak{A}_j$ *ist ein Ideal.*

Definition 4.23.
Seien $\mathfrak{A}_1, \mathfrak{A}_2$ *Ideale im Ring* R*.*

$$\mathfrak{A}_1 \cdot \mathfrak{A}_2 := \left\{ \sum_{j=1}^{k} a_j^{(1)} a_j^{(2)} \middle| a_j^{(1)} \in \mathcal{A}_1,\ a_j^{(2)} \in \mathcal{A}_2,\ k \in \mathbb{N}_0 \right\}$$

heißt das ***Produkt*** *von* $\mathfrak{A}_1$ *und* $\mathfrak{A}_2$*.*

Bemerkung 4.24.

(i) $\mathfrak{A}_1 \cdot \mathfrak{A}_2$ *ist ein Ideal.*

(ii) $\mathfrak{A}_1 \cdot \mathfrak{A}_2 \subset (\mathfrak{A}_1 \cap \mathfrak{A}_2)$

Satz 4.25.
Sei $\mathfrak{A}$ *ein Ideal im Ring* S*.*
Dann ist $S/\mathfrak{A} := \{s + \mathfrak{A} | s \in S\}$ *mit den kanonischen Verknüpfungen*

$$(r + \mathfrak{A}) + (s + \mathfrak{A}) := (r + s) + \mathfrak{A} \quad \text{und}$$
$$(r + \mathfrak{A}) \cdot (s + \mathfrak{A}) := (rs) + \mathfrak{A},\ (r, s \in S)$$

ein Ring.

Definition 4.26.
*$S/\mathfrak{A}$ heißt **Faktorring**.*

Definition 4.27.
*Ist φ ein Ringhomomorphismus, so heißt Kern $\varphi := \varphi^{-1}(0)$ der **Kern** von φ und Bild φ das **Bild** von φ.*

Bemerkung 4.28.

(i) Der Kern eines Ringhomomorphismus ist ein Ideal.

(ii) Das Bild eines Ringepimorphismus ist ein Ideal.

Bemerkung 4.29.
Sei S ein Ring und $\mathfrak{A}$ ein Ideal in S. Die kanonische Projektion

$$\begin{aligned} pr : S &\to S/\mathfrak{A} \\ S &\mapsto S + \mathfrak{A} \end{aligned}$$

ist ein Ringepimorphismus mit $Kern(pr) = \mathfrak{A}$.

Satz 4.30 (Homomorphiesatz)**.**
Ist $\varphi : R \to S$ ein Ringisomorphismus, so gilt

$$R/Kern(\varphi) \cong Bild(\varphi).$$

Satz 4.31 (1. Isomorphiesatz)**.**
R sei Unterring von S und $\mathfrak{A}$ Ideal in S. Dann gelten:

(i) $R + \mathfrak{A}$ ist Unterring von S,

(ii) $R \cap \mathfrak{A}$ ist ein Ideal von R,

(iii) $R/(R \cap \mathfrak{A}) \cong (R + \mathfrak{A})/\mathfrak{A}$.

Satz 4.32 (2. Isomorphiesatz)**.**
$\mathfrak{A}_1, \mathfrak{A}_2$ seien Ideale in S mit $\mathfrak{A}_1 \subset \mathfrak{A}_2$. Dann gelten:

(i) $\mathfrak{A}_2/\mathfrak{A}_1$ ist ein Ideal von $S/\mathfrak{A}_1$,

(ii) $S/\mathfrak{A}_2 \cong (S/\mathfrak{A}_1)/(\mathfrak{A}_2/\mathfrak{A}_1)$.

Besonders wichtige Klassen von Idealen sind die Primideale und die maximalen Ideale.

Definition 4.33.
Ein Ideal $\mathfrak{P}$ *von* S *heißt* ***Primideal****, wenn* $\mathfrak{P} \neq S$ *gilt und für* $x, y \in S$ *aus* $xy \in \mathfrak{P}$ *folgt, dass* $x \in \mathfrak{P}$ *oder* $y \in \mathfrak{P}$.

Beispiel 4.34.
In $\mathbb{Z}$ *sind die Primideale gegeben durch* (p) *mit* p *Primzahl.*

Definition 4.35.
Ein Ideal $\mathfrak{A}$ *von* S *heißt* ***maximal****, wenn* $\mathfrak{A} \neq S$ *gilt und für jedes Ideal* $\mathfrak{B}$ *mit* $\mathfrak{A} \subset \mathfrak{B} \subset S$ *folgt, dass* $\mathfrak{B} = S$ *oder* $\mathfrak{B} = \mathfrak{A}$.

Satz 4.36.
Für ein Ideal $\mathfrak{P}$ *von* S *gilt:*
$\mathfrak{P}$ *ist Primideal* $\Leftrightarrow$ $S/\mathfrak{P}$ *Integritätsring.*

Satz 4.37.
Für ein Ideal $\mathfrak{A}$ *von* S *gilt:*
$\mathfrak{A}$ *ist maximal* $\Leftrightarrow$ $S/\mathfrak{A}$ *Körper.*

Bemerkung 4.38.
Ein maximales Ideal ist ein Primideal.

Bemerkung 4.39.
Ist $\varphi : R \to S$ *ein Ringhomomorphismus und* $\mathfrak{P}$ *ein Primideal in* S*, so ist auch* $\varphi^{-1}(\mathfrak{P})$ *ein Primideal in* R.

Satz 4.40.
Jedes Ideal $\mathfrak{B} \neq S$ *ist in einem maximalen Ideal* $\mathfrak{A}$ *von* S *enthalten.*

Korollar 4.41.
Jeder Ring $S \neq \{0\}$ *besitzt ein maximales Ideal.*

Definition 4.42.
$\mathfrak{A}$ sei ein Ideal in S. Gilt dann für $s_1, s_2 \in S$

$$s_1 + \mathfrak{A} = s_2 + \mathfrak{A},$$

*so sagt man hierfür, dass s_1 **kongruent zu** s_2 **modulo** $\mathfrak{A}$ ist und schreibt auch $s_1 \equiv s_2(\mathfrak{A})$*

Definition 4.43.
*Zwei Ideale $\mathfrak{A}_1, \mathfrak{A}_2$ in S heißen **comaximal** :⇔*
$\mathfrak{A}_1 + \mathfrak{A}_2 = S$

Bemerkung 4.44.
Sind $x_1, x_2 \in \mathbb{Z}$ mit $x_1 \neq x_2$ teilerfremd, so sind die Hauptideale $(x_1), (x_2)$ in $\mathbb{Z}$ comaximal.

Bemerkung 4.45.
Sind $R_1, ..., R_n$ Ringe, so ist

$$\prod_{j=1}^{n} R_j := \bigtimes_{j=1}^{n} R_j$$

mit den kanonischen Verknüpfungen ein Ring.

Der folgende Satz ist neben seiner eigenständigen Bedeutung ein unentbehrliches Beweishilfsmittel in der Algebra, insbesondere in der Kommutativen Algebra.

Theorem 4.46 (Chinesischer Restsatz).
Seien $n \geq 2$, S ein Ring und $\mathfrak{A}_1, ..., \mathfrak{A}_n$ paarweise comaximale Ideale.

(i) Zu beliebigen $x_1, ..., x_n$ aus S gibt es ein $x \in S$ mit

$$\begin{aligned} x &\equiv x_1(\mathfrak{A}_1) \\ &\vdots \\ x &\equiv x_n(\mathfrak{A}_n) \end{aligned}$$

(ii) *Die Abbildung* $g : S \to \prod_{i=1}^{n}(R/\mathfrak{A}_i)$ *mit*

$$g(s) = (s + \mathfrak{A}_1, ..., s + \mathfrak{A}_n)$$

ist ein Ringepimorphismus mit

$$Kern(g) = \prod_{i=1}^{n} \mathfrak{A}_i = \bigcap_{i=1}^{n} \mathfrak{A}_i,$$

und es gilt

(iii)

$$S/\prod_{i=1}^{n} \mathfrak{A}_i = S/\bigcap_{i=1}^{n} \mathfrak{A}_i \cong \prod_{i=1}^{n}(S/\mathfrak{A}_i)$$

Beweis.

(i) Sei $j \in \{1, ..., n\}$ beliebig, aber fest. Da $\mathfrak{A}_j + \mathfrak{A}_i = S$ für alle $i \in \{1, ..., j-1, j+1, ..., n\}$ gilt, existieren $a_i \in \mathfrak{A}_j$, $b_i \in \mathfrak{A}_i$ mit $1 = a_i + b_i$. Folglich gilt

$$1 = \prod_{i=1}^{j-i}(a_i + b_i) + \prod_{i=j+1}^{n}(a_i + b_i).$$

Multipliziert man die Produkte aus, so enthält in der dann entstehenden Summe von Produkten jedes Produkt außer $b_1 \cdots b_{j-1}b_{j+1} \cdots b_n$ einen Faktor aus dem Ideal $\mathfrak{A}_j$. Damit gilt

$$1 = b_1 \cdots b_{j-1}b_{j+1} \cdots b_n + a$$

mit $a \in \mathfrak{A}_j$ und $b_1 \cdots b_{j-1}b_{j+1} \cdots b_n \in \mathfrak{A}_1 \cdots \mathfrak{A}_{j-1}\mathfrak{A}_{j+1} \cdots \mathfrak{A}_n$.
Mit $z_j = b_1 \cdots b_{j-1}b_{j+1} \cdots b_n$ gilt also

$$\begin{aligned} z_j &\equiv 1(\mathfrak{A}_j) \\ z_j &\equiv 0(\mathfrak{A}_1 \cdots \mathfrak{A}_{j-1}\mathfrak{A}_{j+1} \cdots \mathfrak{A}_n) \end{aligned}$$

Wegen Bemerkung 4.24(ii) gilt

$$\mathfrak{A}_1 \cdots \mathfrak{A}_{j-1}\mathfrak{A}_{j+1} \cdots \mathfrak{A}_n \subset (\mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_{j-1} \cap \mathfrak{A}_{j+1} \cap \ldots \cap \mathfrak{A}_n) \subset \mathfrak{A}_i$$

Somit ist $z_j \equiv 0(\mathfrak{A}_i)$ für alle $i \in \{1, ..., j-1, j+1, ..., n\}$. Da zudem $z_j \equiv 1(\mathfrak{A}_j)$ gilt, folgt für $x := x_1 z_1 + \ldots + x_n z_n$, dass

$$\begin{aligned} x &\equiv x_1(\mathfrak{A}_1) \\ &\vdots \\ x &\equiv x_n(\mathfrak{A}_n) \end{aligned}$$

gilt.

(ii) Dass g ein Ringhomomorphismus ist, ist trivial. Sei

$$(x_1 + \mathfrak{A}_1, \ldots, x_n + \mathfrak{A}_n) \in \prod_{i=1}^{n} S/\mathfrak{A}_i.$$

Gemäß (i) gibt es ein $x \in S$ mit

$$\begin{aligned} x &\equiv x_1(\mathfrak{A}_1) \\ &\vdots \\ x &\equiv x_n(\mathfrak{A}_n), \end{aligned}$$

also $g(x) = (x_1 + \mathfrak{A}_1, \ldots, x_n + \mathfrak{A}_n)$, d.h. g ist ein Ringepimorphismus. Weiter gilt

$$\begin{aligned} & x \in Kern(g) \\ \Leftrightarrow \quad & x + \mathfrak{A}_1 = \mathfrak{A}_1, \ldots, x + \mathfrak{A}_n = \mathfrak{A}_n \\ \Leftrightarrow \quad & x \in \bigcap_{i=1}^{n} \mathfrak{A}_i, \\ & \text{d.h. } Kern(g) = \bigcap_{i=1}^{n} \mathfrak{A}_i \end{aligned}$$

Weiter gilt nach 4.24(ii):

$$\prod_{i=1}^{n} \mathfrak{A}_i \subset \bigcap_{i=1}^{n} \mathfrak{A}_i.$$

$\bigcap_{i=1}^{n} \mathfrak{A}_i \subset \prod_{i=1}^{n} \mathfrak{A}_i$ wird induktiv gezeigt.

Da die Aussage auch für $n = 1$ Sinn macht wird als Induktionsanfang $N = 1$ gewählt und die Aussage ist trivial.
$n \to n+1$:
Im Beweis zu (i) wurde gezeigt, dass es eine Darstellung $1 = a + b$ mit $a \in \mathfrak{A}_1$ und $b \in \mathfrak{A}_2 \cdots \mathfrak{A}_{n+1}$ gibt. Sei $z \in \cap_{i=1}^{n+1} \mathfrak{A}_i$. Dann gilt

$$z \in \bigcap_{i=2}^{n+1} \mathfrak{A}_i \overset{(Ind.-Vor.)}{\subset} \prod_{i=2}^{n+1} \mathfrak{A}_i.$$

Wegen $z \in \mathfrak{A}_i (\forall i = 1, \ldots, n+1)$, $a \in \mathfrak{A}_1$ und $b \in \mathfrak{A}_2 \cdots \mathfrak{A}_{n+1}$ erhält man schließlich

$$z = z \cdot a + z \cdot b \in \prod_{i=1}^{n+1} \mathfrak{A}_i.$$

(iii) folgt aus (ii).

□

Korollar 4.47 (Simultankongruenzen in $\mathbb{Z}$)**.**
Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und paarweise teilerfremd. Zu $x_1, \ldots, x_n \in \mathbb{Z}$ gibt es dann ein $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv x_1 (\mathfrak{A}_1) \\ &\vdots \\ x &\equiv x_n (\mathfrak{A}_n) \end{aligned}$$

Alle Lösungen sind gegeben durch $x + a_1 \cdots a_n k$ $(k \in \mathbb{Z})$.

Beweis. Unter Beachtung von Bemerkung 4.44 folgt die Existenz aus dem Chinesischen Restsatz. Für zwei Lösungen x, y gilt nach (ii) des Chinesischen Restsatzes

$$x - y \in \bigcap_{i=1}^{n} (a_i) = \prod_{i=1}^{n} (a_i),$$

d.h. $x - y$ ist ein Vielfaches von $a_1 \cdots a_n$. □

Beispiel 4.48.
Es soll die kleinste positive Lösung des Kongruenzsystems

$$\begin{aligned} x &\equiv 1\ (10) \\ x &\equiv -1\ (3) \\ x &\equiv 6\ (7) \end{aligned}$$

gefunden werden. $3, 7, 10$ *sind paarweise teilerfremd. Gemäß dem Beweis des Chinesischen Restsatzes (i) sind zunächst Zahlen* z_1, z_2, z_3 *zu finden mit*

$$\left.\begin{aligned} z_1 &\equiv 1\ (10) \\ z_1 &\equiv 0\ (21) \end{aligned}\right\} \quad \text{eine Lösung ist } z_1 = 21,$$

$$\left.\begin{aligned} z_2 &\equiv 1\ (3) \\ z_2 &\equiv 0\ (70) \end{aligned}\right\} \quad \text{eine Lösung ist } z_2 = -140,$$

$$\left.\begin{aligned} z_3 &\equiv 1\ (7) \\ z_3 &\equiv 0\ (30) \end{aligned}\right\} \quad \text{eine Lösung ist } z_3 = -90,$$

$x = 21 + 140 - 540 = -379$ *ist dann eine Lösung. Gemäß Korollar 4.47 sind dann alle Lösungen gegeben durch* $x + 210k$ $(k \in \mathbb{Z})$. *Die kleinste positive Lösung ist also* $x = 41$.

Definition 4.49.
R sei Integritätsring mit $a, b \in R$.
a ***teilt*** $b :\Leftrightarrow \exists c \in R$ *mit* $b = ac$.
Man schreibt: $a|b$

Beispiel 4.50.
In jedem Integritätsring gilt: 0 *teilt* 0.

Definition 4.51.
R sei Integritätsring.
$a, b \in R$ *heißen* ***assoziiert*** $(a \sim b) :\Leftrightarrow \exists e \in R^*$ *mit* $a = be$.

Definition 4.52.
R sei Integritätsring.

*$a \in R \backslash (R^* \cup \{0\})$ heißt **irreduzibel** $:\Leftrightarrow$ aus $a = bc$ folgt, dass a oder b Einheiten sind.*

Beispiel 4.53.

(i) Das Polynom $T^2 + 1$ ist irreduzibel in $\mathbb{R}[T]$.

(ii) Das Polynom $T^2 + 1$ ist reduzibel in $\mathbb{C}[T]$.

Definition 4.54.
R sei Integritätsring.
*$p \in R \backslash (R^* \cup \{0\})$ heißt **Primelement** $:\Leftrightarrow$ Aus $p|ab$ für $a, b \in R$ folgt: $p|a$ oder $p|b$*

Bemerkung 4.55.
Primelemente sind irreduzibel.

Bemerkung 4.56.
In einem Hauptidealring gilt: (p) ist Primideal $\neq \{0\} \Leftrightarrow$ p ist Primelement

Definition 4.57.
*Ein Integritätsring R heißt **faktoriell** $:\Leftrightarrow$ Jedes $a \in R \backslash (R^* \cup \{0\})$ lässt sich bis auf die Reihenfolge und Assoziiertheit eindeutig als Produkt von Primelementen schreiben.*

Satz 4.58.
Hauptidealringe sind faktoriell.

Satz 4.59.
In faktoriellen Ringen fallen die irreduziblen Elemente mit den Primelementen zusammen.

Theorem 4.60 (Satz von Gauß).
R faktoriell $\Rightarrow$ der Polynomring $R[T_1, \ldots, T_n]$ ist faktoriell.

Satz 4.61.
R faktoriell $\Rightarrow$ der Polynomring $R[T_1, T_2, T_3 \ldots]$ in abzählbar vielen Unbestimmten ist faktoriell.

Satz 4.62.
Für einen Körper K ist der formale Potenzreihenring $K[[T]]$ faktoriell.

Beispiel 4.63.
Der Integritätsring $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell.

Moduln lassen sich als Verallgemeinerung von Ringen auffassen.

Definition 4.64.
*Seien R ein Ring und $F \neq \emptyset$ eine Menge. F heißt **R-Modul** $:\Leftrightarrow$*
es gibt zwei Abbildungen

$$+ : F \times F \to F,$$
$$\cdot : R \times F \to F,$$

so dass gelten:

(i) $(F, +)$ *ist eine abelsche Gruppe.*

(ii) $r_1(r_2x_1) = (r_1r_2)x_1$

(iii) $r_1(x_1 + y_1) = r_1x_1 + r_1y_1$

(iv) $(r_1 + r_2)x_1 = r_1x_1 + r_2x_1$

(v) $1x_1 = x_1$

für alle $r_1, r_2 \in R$ und $x_1, x_2 \in F$.

Beispiel 4.65.

(i) Jeder K-Vektorraum (K Körper) ist ein K-Modul.

(ii) Jede abelsche Gruppe ist ein $\mathbb{Z}$-Modul.

(iii) Jeder Ring R ist ein R-Modul.

(iv) Jedes Ideal in einem Ring R ist ein R-Modul.

Definition 4.66.
*Seien F ein R-Modul und $\emptyset \neq L \subset F$. L heißt **Untermodul** von $F :\Leftrightarrow$*

(i) $u + v \in L$ *für alle* $u, v \in L$

(ii) $ru \in L$ *für alle* $r \in R, u \in L$

Beispiel 4.67.
Fasst man einen Ring R als Modul über sich selbst auf, so sind die Untermoduln von R genau die Ideale von R.

Bemerkung 4.68.
Der Durchschnitt beliebig vieler Untermoduln ist wieder ein Untermodul.

Definition 4.69.
Ist $(L_j)_{j\in J}$ eine Familie von Untermoduln eines R-Moduls F, so heißt

$$\sum_{j\in J} L_j = \left\{ \sum_{j\in J} v_j \,\middle|\, v_j \in L_j,\ v_j \neq 0 \text{ nur für endlich viele } j \right\}$$

die ***Summe*** *der L_j. Ist für $v \in \sum_{j\in J} L_j$ die Darstellung $v = \sum_{j\in J} v_j$ eindeutig, so spricht man auch von einer* ***direkten Summe*** *und schreibt*

$$\bigoplus_{j\in J} L_j \text{ für } \sum_{j\in J} L_j.$$

Bemerkung 4.70.
$\sum_{j\in J} L_j$ ist wieder ein Untermodul von F.

Definition 4.71.
Ist M eine Teilmenge des R-Moduls F, so heißt

$$\langle M\rangle := \bigcap_{\substack{L\supset M,\\ L \text{ Untermodul von } F}} L$$

der ***von*** *M* ***erzeugte Untermodul*** *von F. M heißt dann* ***Erzeugendensystem*** *von $\langle M\rangle$.*

Insbesondere gilt dieses Konstruktionsprinzip auch für Ideale eines Ringes R, sofern dieser als Modul über sich selbst aufgefasst wird, da die Ideale von R genau die Untermoduln von R sind.

Bemerkung 4.72.
Es gilt

$$\langle M \rangle = \left\{ \sum_{j=1}^{n} r_j x_j \;\middle|\; r_j \in R,\ x_j \in M,\ n \in \mathbb{N}_0 \right\}$$

Definition 4.73.
Ein R-Modul F heißt ***endlich-erzeugt****, falls er ein endliches Erzeugendensystem besitzt.*

Definition 4.74.
Sind F_1, F_2 R-Moduln, so heißt $\varphi : F_1 \to F_2$ ein ***R-Modulhomomorphismus*** $:\Leftrightarrow$

$$\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2),$$
$$\varphi(rx_1) = r\varphi(x_1) \text{ für alle } r \in R,\ x_1, x_2 \in F_1.$$

Ist φ bijektiv, so heißt φ ein ***R-Modulisomorphismus****. F_1 und F_2 heißen dann* ***isomorph*** *($F_1 \cong F_2$).*
Ist φ surjektiv, so heißt φ ein ***R-Modulepimorphismus****.*
Ist φ injektiv, so heißt φ ein ***R-Modulmonomorphismus****.*
Gilt $F_1 = F_2$, so heißt φ ein ***R-Modulendomorphismus****.*
Gilt $F_1 = F_2$ und ist φ bijektiv, so heißt φ ein ***R-Modulautomorphismus****.*

Bemerkung 4.75.
Ist φ ein R-Modulisomorphismus, so ist auch φ^{-1} ein R-Modulisomorphismus.

Definition 4.76.
Ist φ ein R-Modulhomomorphismus, so heißt Kern $\varphi := \varphi^{-1}\{0\}$ der ***Kern*** *von φ und das* ***Bild*** *von φ wird mit Bild φ bezeichnet.*

Bemerkung 4.77.
Kern und Bild eines R-Modulhomomorphismus sind Untermoduln.

Bemerkung 4.78.
Für einen R-Modul F und einen Untermodul L von F wird die Faktorgruppe F/L mit den kanonisch induzierten Verknüpfungen zu einem R-Modul.

Definition 4.79.
F/L heißt ***Faktormodul***

Beispiel 4.80.
Die kanonische Projektion

$$\begin{aligned} pr: \ & F \to F/L, \\ & x \mapsto x + L \end{aligned}$$

ist ein R-Modulepimorphismus.

Satz 4.81 (Homomorphiesatz)**.**
Für einen R-Modulhomomorphismus $\varphi : F_1 \to F_2$ gilt

$$F_1/Kern\ \varphi \cong Bild\ \varphi$$

Satz 4.82 (1. Isomorphiesatz)**.**
Sind L_1, L_2 Untermoduln des R-Moduls F, so gilt

$$(L_1 + L_2)/L_1 \cong L_2/(L_1 \cap L_2)$$

Satz 4.83 (2. Isomorphiesatz)**.**
Sind L_1, L_2 Untermoduln des R-Moduls F mit $L_1 \subset L_2$, so gilt

$$F/L_2 \cong (F/L_1)/(L_2/L_1)$$

Definition 4.84.
Sei F ein R-Modul.

(i) $A \subset F$ *heißt* ***linear unabhängig*** $:\Leftrightarrow$ *für jedes endliche $\Lambda \subset A$ gilt:*

$$\left(\sum_{\lambda \in \Lambda} r_\lambda \lambda = 0 \text{ mit } r_\lambda \in R \right) \Rightarrow r_\lambda = 0 \text{ für alle } \lambda \in \Lambda$$

(ii) $A \subset F$ *heißt* ***Basis*** *von F* $:\Leftrightarrow$ *A ist linear-unabhängig mit $\langle A \rangle = F$*

(iii) F *heißt* ***frei*** $:\Leftrightarrow$ *F besitzt eine Basis.*

Satz 4.85.
F sei ein R-Modul. Dann gilt: F ist frei $\Leftrightarrow$ es gibt ein $A \subset F$, so dass sich jedes $z \in F$ eindeutig in der Form schreiben lässt

$$z = \sum_{a \in A} r_a \cdot a \text{ mit } r_a \in R \text{ und } r_a \neq 0 \text{ nur für endliche viele } a \in A.$$

Beispiel 4.86.

(i) Jede endliche abelsche Gruppe, aufgefasst als $\mathbb{Z}$-Modul ist nicht frei.

(ii) Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht frei.

(iii) Jeder K-Modul (K Körper) ist frei.

Satz 4.87.
Für einen freien R-Modul ist die Kardinalität einer Basis eindeutig bestimmt.

Definition 4.88.
Die Kardinalität einer Basis eines freien R-Moduls F heißt der ***Rang von*** *F.*

Satz 4.89.
Jeder R-Modul ist isomorph zu einem Faktormodul eines freien R-Moduls.

Satz 4.90.
Seien F_1, F_2 R-Moduln, F_2 frei und $\varphi : F_1 \to F_2$ ein R-Modulepimorphismus. Dann existiert ein Untermodul L von F_1, so dass gilt

$$F_1 = L \oplus Kern\ \varphi.$$

5. Noethersche Ringe

Noethersche Ringe sind in vielen Gebieten von Bedeutung, insbesondere in der kommutativen Algebra, die ihrerseits die Grundlage der Algebraischen Geometrie bildet, aber auch in der Algebraischen Zahlentheorie, da sie die Klasse der für dieses Gebiet unentbehrlichen Dedekindringe umfassen. Sie umfassen weiterhin die Klasse der Hauptidealringe[1]. Mit diesen und den faktoriellen Ringen[1] haben die Noetherschen Integritätsringe gemeinsam, dass sich jedes ihrer (nicht-trivialen) Elemente als Produkt von irreduziblen Elementen schreiben lässt, wenn auch i.A. nicht mehr eindeutig. Von vielen in der Zahlentheorie vorkommenden Noetherschen Ringen wusste bereits Kummer in der Mitte des 19. Jahrhunderts, dass in ihnen der Satz von der eindeutigen Primelementzerlegung nicht mehr gilt. Da diese Ringe für die Zahlentheorie unentbehrlich waren, versuchte Dedekind jene Ringklassen zu klassifizieren, in denen zumindest noch eine eindeutige Zerlegbarkeit der Ideale in ein Produkt von Primidealen möglich ist. Diese Fragestellung führte ihn auf die bereits erwähnten, nach ihm benannten Ringe. Auf Dedekind-Ringe wird abrissartig (und **ohne Beweise**, die man z.B. in [Lan86] finden kann) eingegangen. Die Primärzerlegung in beliebigen Noetherschen Ringen beendet dann dieses Kapitel.

Noethersche Ringe zeichnen sich durch eine gewisse Endlichkeitseigenschaft aus („Stationarität“ aufsteigender Idealketten). Die Bedeutung von Endlichkeitsbedingungen sind in der Algebra bereits aus der Gruppentheorie bekannt, in der im Theorieaufbau strikt nach endlichen, endlich-erzeugten und beliebigen Gruppen unterschieden wird. Aus der Analysis oder Topologie ist die überragende Bedeutung der Kompakta bekannt, die sich ebenfalls durch eine Endlichkeitsbedingung (Existenz endlicher Teilüberdeckungen zu gegebenen Überdeckungen) auszeichnen.

[1] Diese Ringklassen sind zwar aus der Linearen Algebra bzw. Algebra 1 bekannt, ihre wichtigsten Eigenschaften wurden jedoch in Abschnitt 3 noch einmal aufgeführt.

Neben den Noetherschen Ringen werden auch kurz die Artischen Ringe betrachtet, die durch eine zur Noetherzität duale Endlichkeitsbedingung (Stationarität absteigender Idealketten) definiert werden.

Der wichtigste Satz dieses Abschnittes ist der Hilbertsche Basissatz, welcher besagt, dass sich die Noetherzität eines Ringes auch auf die Polynomringe über diesem Ring überträgt. Auch sein Beweis sollte verinnerlicht werden. Eine wichtige Anwendung des Hilbertschen Basissatzes in der Algebraischen Geometrie besteht darin, dass es bei der Behandlung unendlich vieler polynominaler Gleichungen über einem algebraisch-abgeschlossenen Körper stets genügt, nur endlich viele dieser Gleichungen zu betrachten. Ausführliches über Noethersche Ringe findet man in [Lan02] oder [Grö68].

Der Bequemlichkeit halber werden in diesem gesamten Kapitel nur kommutative Ringe R mit 1 betrachtet.

Bemerkung 5.1.
Seien F ein R-Modul und $F_1 \subset F_2 \subset F_3 \subset \dots$ eine aufsteigende Kette von Untermoduln von F. Dann ist auch $\cup_{i=1}^{\infty} F_i$ ein Untermodul von F.

Beweis.
Seien $a, b \in \cup_{i=1}^{\infty} F_i$ und $i_0, i_1 \in I$ mit $a \in F_{i_0}$ und $b \in F_{i_1}$. Dann liegt $a + b$ in $F_{i_1} \subset \cup_{i=1}^{\infty} F_i$. Ähnlich folgt $ra \in \cup_{i=0}^{\infty} F_i$ für $r \in R$. □

Satz 5.2.
Sei F ein R-Modul. Dann sind die folgenden Aussagen äquivalent:

(i) Jeder Untermodul von F ist endlich erzeugt.

(ii) Ist $F_1 \subset F_2 \subset F_3 \dots$ eine Kette von Untermoduln von F, so existiert ein $s \in \mathbb{N}$ mit $F_s = F_{s+1} = F_{s+2} = \dots$ (Stationaritätsbedingung)

(iii) Jede nichtleere Menge $\mathcal{F}$ von Untermoduln hat bzgl. „$\subset$“ ein maximales Element F_0.

Beweis.
(i) $\Rightarrow$ (ii).
Nach Bemerkung 5.1 ist $\tilde{F} := \cup_{i=1}^{\infty} F_i$ ein Untermodul von F, der nach Voraussetzung (i) ein endliches Erzeugendensystem $\{e_1, \ldots, e_t\}$ besitzt. Es gibt also ein s mit $\{e_1, \ldots, e_t\} \subset F_s$, alsdann $F \subset F_s$, d.h. $F_s = F_{s+1} = F_{s+2} = \ldots$.
(ii) $\Rightarrow$ (iii).
Annahme: $\mathcal{F}$ besitzt kein maximales Element F_0. Dann gibt es zu F_0 ein $F_1 \in \mathcal{F}$ mit $F_0 \subsetneq F_1$ und Iteration ergibt eine Untermodulkette $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots$ im Widerspruch zu (ii).
(iii) $\Rightarrow$ (i).
Sei $\tilde{F}$ ein Untermodul von F und bezeichne $\mathcal{F}$ die Menge aller endlich erzeugten Untermoduln von $\tilde{F}$. $\mathcal{F}$ besitzt nach Voraussetzung ein maximales Element F_0. Wäre $F_0 \neq \tilde{F}$ und $y \in \tilde{F} \backslash F_0$, so wäre $F_0 + \langle y \rangle$ ein endlich erzeugter echter Obermodul von F_0 im Widerspruch zur Maximalität von F_0. Also gilt $F_0 = \tilde{F}$, d.h. $\tilde{F}$ ist endlich erzeugt. □

Definition 5.3.

*(i) Ein R-Modul F, der eine (und damit jede) Bedingung aus Satz 5.2 erfüllt, heißt **Noethersch**.*

*(ii) Ein Ring R heißt **Noethersch**, wenn er als Modul über sich selbst Noethersch ist.*

Bemerkung 5.4.
Ein Ring ist genau dann Noethersch, wenn in Satz 5.2 der Begriff „Untermodul“ durch „Ideal“ ersetzt wird.

Beweis.
Die Untermoduln des R-Moduls R sind genau die Ideale von R. □

Satz 5.5.
Sei F ein R-Modul und G ein Untermodul von F. Dann gilt:
F ist Noethersch $\Leftrightarrow$ G und F/G sind Noethersch.

Beweis.
„⇒“
Die Behauptung bzgl. des Untermoduls G folgt unmittelbar aus Satz 5.2 (i). Sei nun G ein Untermodul von F und $\pi : F \to F/G$ die kanonische Projektion und $\overline{F}_1 \subset \overline{F}_2 \subset \ldots$ eine aufsteigende Kette von Untermoduln von F/G. Dann ist $\pi^{-1}(\overline{F}_1) \subset \pi^{-1}(\overline{F}_2) \subset \ldots$ eine aufsteigende Kette von Untermoduln von F, die wegen der Noetherzität von F stationär wird, d.h. es gibt ein s mit $\pi^{-1}(\overline{F}_s) = \pi^{-1}(\overline{F}_{s+1}) = \ldots$. Wegen der Surjektivität von π folgt $\overline{F}_s = \overline{F}_{s+1} = \ldots$. Damit ist „⇒“ bewiesen.
„⇐“
Sei H ein Untermodul von F. Bezeichne $\pi : H \to H/(H \cap G)$ die kanonische Projektion. Nach dem 1. Isomorphiesatz für Moduln gilt $H/(H \cap G) \cong (H + G)/G$. $(H + G)/G$ ist ein Untermodul von F/G, und da F/G nach Voraussetzung endlich erzeugt ist, gilt dies auch für $(H + G)/G$. Wegen $H/(H \cap G) \cong (H + G)/G$ existieren also $z_1, \ldots, z_s \in H$ mit $H/(H \cap G) = \langle \pi(z_1), \ldots, \pi(z_s) \rangle$.
Da G nach Voraussetzung Noethersch ist, existieren $w_1, \ldots, w_t$ mit $H \cap G = \langle w_1, \ldots, w_t \rangle$. Es gilt dann $H = \langle \pi(z_1), \ldots, \pi(z_s), w_1, \ldots, w_t \rangle =: H_0$ Offensichtlich gilt $H \cap G \subset H_0 \subset H$. Da $H_0/(H \cap G)$ das Erzeugendensystem $\{\pi(z_1), \ldots, \pi(z_s)\}$ von $H/(H \cap G)$ enthält, folgt zusammen mit $H/(H \cap G) \subset H_0/(H \cap G)$ die Gleichheit $H/(H \cap G) = H_0/(H \cap G)$. Ist nun $z \in H$, so ist $\pi(z) \in H/(H \cap G) = H_0/(H \cap G)$, d.h. es existieren $w \in H_0$, $v \in H \cap G \subset H_0$ mit $z = w + v \in H_0$, d.h. $H \subset H_0$. Insgesamt also $H = H_0$. H ist also endlich erzeugt. Da H beliebig gewählt war, ist somit gemäß Satz 5.2 auch „⇐“ bewiesen. □

Beispiel 5.6.

(i) Alle endlichen Ringe, wie etwa $\mathbb{Z}/n\mathbb{Z}$ sind Noethersch.

(ii) Alle Hauptidealringe sind Noethersch.

Beispiel 5.7.
Sei K ein Körper. Der Polynomring $K[T_1, T_2, \ldots]$ in abzählbar vielen Unbestimmten ist nicht Noethersch.

Das folgt daraus, dass die Idealkette $(T_1) \subset (T_1, T_2) \subset \ldots$ offensichtlich nicht stationär wird. Mit $K[T_1, T_2, \ldots]$ ist ein Beispiel gefunden, welches zeigt,

dass nicht jeder faktorielle Ring Noethersch ist. Umgekehrt ist klar, dass nicht jeder Noethersche Ring faktoriell ist, da Noethersche Ringe i.A. nicht einmal Integritätsringe sind. Man betrachte das Beispiel $\mathbb{Z}/6\mathbb{Z}$.

In einer gewissen formalen Dualtiät zu den Noetherschen Ringen stehen die Artinschen Ringe.

Definition 5.8.
Ein Ring R heißt ***Artinsch*** $:\Leftrightarrow$
Jede absteigende Idealkette $\mathfrak{A}_0 \supset \mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \dots$ wird stationär.

Satz 5.9.
Ein Artinscher Integritätsring R ist ein Körper.

Beweis.
Sei $x \in R \setminus \{0\}$. Es ist zu zeigen, dass x ein multiplikatives Inverses besitzt. Da R Artinsch ist, wird die Idealkette $(x) \supset (x^2) \supset (x^3) \supset \dots$ stationär; es gibt also insbesondere ein $s \in \mathbb{N}$ mit $x^s = x^{s+1}$, d.h. $x^s = x^{s+1}y$ für ein $y \in R$. Da R ein Integritätsring ist und $x \neq 0$ folgt $1 = xy$. Also ist R ein Körper. □

Satz 5.9 erlaubt es sofort, Noethersche Ringe anzugeben, die nicht Artinsch sind.

Beispiel 5.10.
Der Noethersche (Integritäts-)Ring $\mathbb{Z}$ ist nicht Artinsch.

Es gibt natürlich auch Ringe, die sowohl Noethersch als auch Artinsch sind.

Beispiel 5.11.
Alle endlichen Ringe sind Noethersch und Artinsch.

Es wird nun gezeigt, dass der **wichtige** Ring $\mathcal{O}(\mathbb{C})$ aller holomorphen Funktionen $\mathbb{C} \to \mathbb{C}$ **weder** Noethersch **noch** Artinsch ist.

Beispiel 5.12.
Sei $\mathcal{O}(\mathbb{C}) := \{f : \mathbb{C} \to \mathbb{C} |\ f$ ist holomorph$\}$. $\mathcal{O}(\mathbb{C})$ ist weder Noethersch noch Artinsch.

Der folgende Beweis kann übergangen werden, falls keine Kenntnisse in Funktionentheorie vorhanden sind.

Beweis. Es wird zunächst gezeigt, dass $\mathcal{O}(\mathbb{C})$ nicht Noethersch ist. Ein Lehrsatz der Funktionentheorie [DKR08] besagt, dass jeder positive Divisor auf $\mathbb{C}$ ein Hauptdivisor ist $(*)$. Die Mengen $\mathfrak{A}_n \subset \mathcal{O}(\mathbb{C})$ mit

$$\mathfrak{A}_n := \{h \in \mathcal{O}(\mathbb{C}) |\ h(n+k) = 0\ (\forall k \in \mathbb{N})\}$$

sind offensichtlich Ideale von $\mathcal{O}(\mathbb{C})$ und (wegen $(*)$) nicht leer.

Definiere für $n \in \mathbb{N}$ die Divisoren $D_n : \mathbb{C} \to \mathbb{Z}$ durch

$$D_n(z) := \begin{cases} 1, & \text{für } z = n+k\ (k \in \mathbb{N}) \\ 0, & \text{sonst.} \end{cases}$$

Die D_n sind positiv und es gibt gemäß $(*)$ holomorphe $h_n \in \mathcal{O}(\mathbb{C})$ mit $(h_n) = D_n$. Es gilt dann $h_n(n) \neq 0$ und $h_n(n+k) = 0$ für alle $k \in \mathbb{N}$, d.h. $h_n \in \mathfrak{A}_{n+1} \backslash \mathfrak{A}_n$. Mithin gilt also

$$\mathfrak{A}_0 \underset{\neq}{\subset} \mathfrak{A}_1 \underset{\neq}{\subset} \mathfrak{A}_2 \underset{\neq}{\subset} \dots,$$

d.h. die Idealkette wird nicht stationär. Folglich ist $\mathcal{O}(\mathbb{C})$ nicht Noethersch.

Nun wird gezeigt, dass $\mathcal{O}(\mathbb{C})$ auch nicht Artinsch ist. $\mathcal{O}(\mathbb{C})$ ist ein Integritätsring. Seien hierzu $f, g \in \mathcal{O}(\mathbb{C})$ mit $f \cdot g \equiv 0$ auf $\mathbb{C}$. Wären $f \not\equiv 0$ und $g \not\equiv 0$ auf $\mathbb{C}$, so gäbe es ein $p \in \mathbb{C}$ mit $f(p) \neq 0$ und daher auch aus Stetigkeitsgründen eine offene Umgebung $U \subset \mathbb{C}$ von p mit $f(w) \neq 0$ für alle $w \in U$. Auf U gilt dann $g(w) \equiv 0$. Nach dem Identitätssatz der Funktionentheorie [DR72] gilt dann aber $g \equiv 0$ auf ganz $\mathbb{C}$. Folglich ist $\mathcal{O}(\mathbb{C})$ nullteilerfrei und alsdann ein Integritätsring.

Annahme: $\mathcal{O}(\mathbb{C})$ ist Artinsch. Dann wäre $\mathcal{O}(\mathbb{C})$ ein Artinscher Integritätsring und somit nach Satz 5.9 ein Körper. Dies ergibt einen Widerspruch, da z.B. die holomorphe Funktion *sin* Nullstellen besitzt und daher kein multiplikatives Inverses. $\mathcal{O}(\mathbb{C})$ ist also nicht Artinsch. □

Man wird verzweifelt Ausschau halten nach einem Artinschen Ring, der nicht Noethersch ist, denn es gilt:

Satz 5.13.
Jeder Artinsche Ring ist Noethersch[2].

[2] Bei den Beziehungen zwischen Artinschen Ringen und Noetherschen Ringen ist zu beachten, dass in diesem Kapitel nur kommutative Ringe mit Eins betrachtet werden. Bei nicht-kommutativen Ringen liegen die Verhältnisse verwickelter. Der Fall beliebiger Ringe wird ausführlich in [Kas77] behandelt.

Für einen Beweis wird auf [Lan02] verwiesen.

Es wird nun der Hilbertsche Basissatz in Angriff genommen. Es handelt sich hierbei um den mit Abstand wichtigsten Satz, der in diesem Kapitel bewiesen wird.

Satz 5.14.
Sei R Noethersch. Dann ist auch der Polynomring $R[T]$ Noethersch.

Beweis. Es wird (i) aus Satz 5.2 für Ideale angewandt. Annahme: Es gibt ein nicht endlich erzeugtes Ideal $\mathfrak{A}$ in $R[T]$. Definiere eine Polynomfolge $P_j \in \mathfrak{A}$ ($\mathfrak{A} \neq \emptyset$ ist klar) rekursiv durch $P_1 \neq 0, P_1 \in \mathfrak{A}$ mit $grad(P_1) =: g_1$ minimal.

Sind $P_1, \ldots, P_s \in \mathfrak{A}$ bereits definiert, so ist $(P_1, \ldots, P_s) \subsetneq \mathfrak{A}$, da $\mathfrak{A}$ nach Annahme nicht endlich erzeugt ist. Wähle nun $P_{s+1} \in \mathfrak{A}\backslash(P_1, \ldots, P_s)$ mit $grad(P_{s+1}) =: g_{s+1}$ minimal. Damit ist die Polynomfolge $P_1, P_2, \ldots$ wohldefiniert.

Wegen der Minimalität der g_i folgt $g_1 \leq g_2 \leq \ldots$. (Gäbe es nämlich ein s mit $g_s > g_{s+1}$, so müsste P_{s+1} in $(P_1, \ldots, P_s)$ liegen, da das Ideal $(P_1, \ldots, P_s)$ alle Polynome aus $\mathfrak{A}$ vom Grad $\leq g_s$ enthält, was einen Widerspruch zu $P_{s+1} \in \mathfrak{A}\backslash(P_1, \ldots, P_s)$ ergäbe.) Bezeichne γ_s den höchsten Koeffizienten des Polynoms $P_s = \gamma_s T^{g_s} + \ldots + \gamma_0$. Es gilt dann

$$(\gamma_1, \ldots, \gamma_s) \subsetneq (\gamma_1, \ldots, \gamma_s, \gamma_{s+1}) \text{ in } R \ (*)$$

Damit hat man eine unendlich aufsteigende Kette von Idealen in R, was der Noetherzität von R widerspricht. Es ist alsher nur noch $(*)$ zu beweisen.

Annahme: $\gamma_{s+1} \in (\gamma_1, \ldots, \gamma_s)$, d.h. $\gamma_{s+1} = r_1\gamma_1 + \ldots + r_s\gamma_s$ mit $r_j \in R$ $(**)$. Betrachte das Polynom $Q \in R[T]$ mit

$$Q(T) := \sum_{i=1}^{s} r_i P_i(T) T^{g_{s+1} - g_i}$$

Natürlich gilt $Q \in (P_1, \ldots, P_s)$. Da die P_i den Grad g_i haben, folgt $grad(Q) = g_{s+1}$. Weiter ist der höchste Koeffizient von Q offensichtlich $r_1\gamma_1 + \ldots + r_s\gamma_s \overset{(**)}{=} \gamma_{s+1}$. Da $grad(P_{s+1}) = g_{s+1}$ folgt (1) $grad(P_{s+1} - Q) < g_{s+1}$. Weil γ_{s+1} auch der höchste Koeffizient von P_{s+1} ist, folgt alsdann zusätzlich (2) $P_{s+1} - Q \in \mathfrak{A}\backslash(P_1, \ldots, P_s)$. (1) und (2) widersprechen aber der Wahl von P_{s+1}. Damit ist $(*)$ und mithin der Satz bewiesen. □

Theorem 5.15.
R sei Noethersch. Dann ist der Polynomring $R[T_1, T_2, \ldots, T_n]$ Noethersch.

Beweis. Dies folgt durch Induktion sofort aus Satz 5.14. □

In Theorem 5.15 ist der Fall, dass R ein Körper ist von solcher Bedeutung, dass er gesondert aufgeführt wird.

Korollar 5.16 (Hilbertscher Basissatz).
Es sei K ein Körper. Dann ist der Polynomring $K[T_1, T_2, \ldots, T_n]$ Noethersch.

Anwendung 5.17.
In der Algebraischen Geometrie befasst man sich u.a. mit den Nullstellengebilden von Teilmengen eines Polynomrings $K[T_1, T_2, \ldots, T_n]$.

Sei K ein algebraisch-abgeschlossener Körper. Jedes $Q \in K[T_1, T_2, \ldots, T_n]$ definiert eine Abbildung

$$\begin{aligned} Q : K^n &\to K \\ (t_1, \ldots, t_n) &\mapsto Q(t_1, \ldots, t_n) \end{aligned}$$

*Es sei nun $X \subset K[T_1, T_2, \ldots, T_n]$. Das **Nullstellengebilde** von X ist die Menge*

$$V(X) = \{P \in K^n \mid Q(P) = 0 \ (\forall Q \in X)\}$$

*Eine Teilmenge $A \in K^n$ heißt **affin-algebraisch**, wenn es ein $X \subset K[T_1, T_2, \ldots, T_n]$ gibt mit $A = V(X)$.*

Es ist nun für die Algebraische Geometrie von grundlegender Bedeutung, dass es bei affin-algebraischem A stets genügt, endliche Teilmengen von $K[T_1, T_2, \ldots, T_n]$ zu betrachten. Man betrachtet das von X erzeugte Ideal (X). Nach dem Hilbertschen Basissatz wird (X) von endlich vielen Polynomen $Q_1, \ldots, Q_s \in K[T_1, T_2, \ldots, T_n]$ erzeugt, d.h. $(X) = (Q_1, \ldots, Q_s)$. Es gilt nun $V(X) = V((Q_1, \ldots, Q_s))$. Wegen $(Q_1, \ldots, Q_s) = (X) \ni X$ folgt sofort $V((Q_1, \ldots, Q_s)) \subset V(X)$. Ist $H \in (Q_1, \ldots, Q_s)$
$= (X)$, so existieren $H_1, \ldots, H_t \in X$ und $P_1, \ldots, P_t \in K[T_1, T_2, \ldots, T_n]$ mit $H = H_1P_1 + \ldots + H_tP_t$. Ist dann $P \in V(X)$, so gilt $H_1(P) = \ldots = H_t(P) = 0$, folglich auch $H(P) = 0$. Völlig analog zeigt man $V((Q_1, \ldots, Q_s)) = V(\{Q_1, \ldots, Q_s\})$,

so dass man insgesamt $V(X) = V(\{Q_1, \ldots, Q_s\})$ hat. Es genügen also stets endlich viele Polynome, um eine affin-algebraische Menge als Nullstellengebilde darzustellen.

Anwendung 5.18.
R sei ein Noetherscher Ring. Weiter seien $t_1, \ldots, t_n$ Elemente, die nicht in R liegen. Die Ringadjunktion $R[t_1, \ldots, t_n]$ lässt sich bekanntlich (s. auch [Grö68]) als Untermodul von $R[T_1, \ldots, T_n]$ auffassen. Da $R[T_1, \ldots, T_n]$ Noethersch ist, folgt mit Satz 5.5 die Noetherzität der Adjunktionsringe $R[t_1, \ldots, t_s]$. Damit ist auch der Beispielvorrat zu Noetherschen Ringen immens erweitert worden.

Wie schon in Beispiel 5.7 gezeigt wurde, lässt sich der Hilbertsche Basissatz nicht mehr auf Polynomringe in abzählbar vielen Unbestimmten übertragen. Es gilt jedoch noch, wobei für einen Beweis auf [SS03] verwiesen wird:

Satz 5.19.
Sei R Noethersch. Dann ist auch der Ring $R[[T]]$ der formalen Potenzreihen Noethersch.

Die (bis auf Assoziiertheit und Reihenfolge) eindeutige Zerlegbarkeit in irreduzible Elemente in faktoriellen Ringen ist in Noetherschen Ringen zwar nicht immer gewährleistet; es gilt jedoch noch die Zerlegungseigenschaft.

Satz 5.20.
R sei ein Noetherscher Integritätsring. Dann ist jedes $a \in R \backslash (R^* \cup \{0\})$ als Produkt von irreduziblen Elementen darstellbar. (Dabei bezeichnet R^* wie üblich die Einheitengruppe von R.)

Beweis. Es wird zunächst gezeigt, dass a mindestens einen irreduziblen Faktor besitzt.
Fall 1: a ist irreduzibel. Dann ist nichts mehr zu zeigen.
Fall 2: a ist reduzibel. Dann gibt es eine Zerlegung $a = p_1 q_1$ mit $p_1, q_1 \notin R^*$. Ist p_1 irreduzibel, so ist man fertig. Ansonsten gibt es eine Zerlegung $p_1 = p_2 q_2$ mit $p_2, q_2 \notin R^*$. Ist p_2 irreduzibel, so ist man fertig. Iteration dieses Verfahrens muss einen irreduziblen Faktor p_n von a liefern, da man ansonsten eine aufsteigende Idealkette $(p_1) \subset (p_2) \subset \ldots$ erhalten würde, die nicht stationär ist. Dies widerspricht aber der Noetherzität von R. a besitzt also einen irreduziblen Faktor.

Da $a \in R\backslash(R^* \cup \{0\})$ beliebig war, gilt also, dass jedes $a \in R\backslash(R^* \cup \{0\})$ einen irreduziblen Faktor besitzt. Man erhält dann
$a = r_1 s_1$ mit $r_1, s_1 \notin R^*$ und r_1 irreduzibel;
Falls s_1 reduzibel ist, $s_1 = r_2 s_2$ mit $r_2, s_2 \notin R^*$ und r_2 irreduzibel;
Falls s_2 reduzibel ist, $s_2 = r_3 s_3$ mit $r_3, s_3 \notin R^*$ und r_3 irreduzibel;
$\vdots$
Falls s_{n-1} reduzibel ist, $s_{n-1} = r_n s_n$ mit $r_n, s_n \notin R^*$ und r_n irreduzibel.

Falls das Verfahren nicht abbricht, ergibt dies eine aufsteigende Kette von Idealen $(s_1) \subset (s_2) \subset (s_3) \subset \ldots$, die nicht stationär wird, was der Noetherzität von R widerspräche. Man erreicht also schließlich ein irreduzibles s_n und hat damit die irreduzible Zerlegung $a = r_1 r_2 \cdots r_n s_n$ gefunden. □

Bisher kennen wir noch keinen Noetherschen Ring, in dem die irreduzible Zerlegung nicht eindeutig ist.

Eine Zahl $m \in \mathbb{Z}\backslash\{0, 1\}$ heißt bekanntlich **quadratfrei**, wenn sie außer 1 keine ganze Quadratzahl als Teiler besitzt.

Sei $m \in \mathbb{Z}$ keine Quadratzahl. Dann sind die Ringe $\mathbb{Z}[\sqrt{m}]$ bekanntlich Integritätsringe und nach Anwendung 5.18 auch Noethersch.

Definition 5.21.
Die Abbildung

$$\begin{aligned} N : \mathbb{Z}[\sqrt{m}] &\to \mathbb{N}_0 \\ a + b\sqrt{m} &\mapsto |a^2 - mb^2| \end{aligned}$$

heißt ***Normfunktion*** *auf* $\mathbb{Z}[\sqrt{m}]$.

Bemerkung 5.22.
Für $a, b \in \mathbb{Z}[\sqrt{m}]$ *gilt* $N(ab) = N(a)N(b)$.

Beweis. Sei $a := x + y\sqrt{m}$ und $\overline{a} := x - y\sqrt{m}$. Dann gilt $N(a) = |a\overline{a}|$. Also: $N(a)N(b) = |a\overline{a}||b\overline{b}| = |ab\overline{a}\overline{b}| = |ab\overline{ab}| = N(ab)$, denn mit $b = v + w\sqrt{m}$ ist $\overline{a}\overline{b} = xv + myw - (xy + vy)\sqrt{m} = \overline{ab}$. □

Bemerkung 5.23.
Seien $a, b \in \mathbb{Z}[\sqrt{m}]$. *Dann gelten*

(i) *Aus $b \neq 0$ und $a|b$ folgt $N(a)|N(b)$ sowie $N(a) \leq N(b)$,*

(ii) *für jede Einheit e gilt $N(e) = 1$,*

(iii) *aus $a \sim b$ folgt $N(a) = N(b)$.*

Beweis.

(i) klar wegen Definition 5.21,

(ii) es gilt $e|1$, also $N(e)|N(1) = 1$,

(iii) folgt aus (ii) und Definition 5.21

□

Bemerkung 5.24.
Seien $a, b \in \mathbb{Z}[\sqrt{m}]$ und a sei ein echter Teiler von b (d.h. a ist nicht assoziiert zu b und a ist keine Einheit). Dann gilt: $N(a) < N(b)$.
*Man nennt N deshalb auch **monotone Normfunktion**.*

Beweis. Es gilt $b = a \cdot c$ mit $c \in \mathbb{Z}[\sqrt{m}]$ und c ist keine Einheit. Wäre mit $c = x + y\sqrt{m}$ $N(c) = |x^2 + my^2| = 1$, so wäre $1 = N(c) = c\bar{c}$, d.h. c wäre eine Einheit, d.h. $a \sim b$ Widerspruch. □

Bemerkung 5.25.
Sei $a \in \mathbb{Z}[\sqrt{m}]$. Dann gilt: a ist Einheit $\Leftrightarrow N(a) = 1$.

Beweis. „$\Rightarrow$“ wurde schon in Bemerkung 5.22 gezeigt; „$\Leftarrow$“ folgt aus dem Beweis zu Bemerkung 5.23. □

Es kann nun ein Noetherscher Ring angegeben werden, in dem die Zerlegung in irreduzible Elemente nicht eindeutig ist und der alsdann auch nicht faktoriell ist.

Beispiel 5.26.
Im Noetherschen Ring $\mathbb{Z}[\sqrt{-5}]$ ist die Zerlegung in irreduzible Elemente nicht eindeutig.

Beweis. In $\mathbb{Z}[\sqrt{-5}]$ gilt $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Wegen $N(2) = 4$, $N(3) = 9$, $N(1+\sqrt{-5}) = 6$ und $N(1-\sqrt{-5}) = 6$ sind mit Bemerkung 5.25 $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ Nicht-Einheiten ungleich 0. Die Norm $N(x)$ eines echten Teilers x einer dieser vier Zahlen müsste nach Bemerkung 5.23 (i) und Bemerkung 5.24 ein echter Teiler von $4, 9$ oder 6 sein, d.h. $N(x) = 2$ oder $N(x) = 3$. Elemente $x = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ mit $N(x) = |a^2 + 5b^2| = 2$ bzw. $N(x) = |a^2 + 5b^2| = 3$ gibt es aber offensichtlich nicht. $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ sind also irreduzibel, womit die Aussage des Beispiels verifiziert ist. □

Die Teilbarkeitstheorie in Integritätsringen ist ein wesentliches Anliegen der Zahlentheorie und der Verlust der eindeutigen Primzerlegung in beliebigen Integritätsringen zunächst ein Rückschlag für die Entwicklung der Theorie gewesen. Es war der geniale Gedanke Dedekinds, die eindeutige Primzerlegung zu ersetzen durch die Forderung nach einer eindeutigen Produktzerlegung der Ideale in Primideale. Hieraus liessen sich noch tiefliegende Folgerungen ziehen und daher sind die Ringe, die dieser Eigenschaft noch genügen, einer der Grundbausteine der Algebraischen Zahlentheorie. Sie werden zu Ehren Dedekinds als Dedekind-Ringe bezeichnet. Sie sind auch Noethersche Ringe. Es wird stichpunktartig auf den Begriff des Dedekindringes hingearbeitet und der Hauptsatz über Dedekindringe zitiert. Beweise werden völlig unterdrückt, da sie den Rahmen dieser Vorlesung sprengen würden.

Im Folgenden bezeichnen R, S Integritätsringe mit $R \subset S$.

Definition 5.27.

(i) $a \in S$ *heißt* ***ganz über*** R*, wenn es ein normiertes Polynom* $Q \in R[T]\setminus\{0\}$ *mit* $Q(a) = 0$ *gibt.*

(ii) S *heißt ganz über* R*, falls jedes* $a \in S$ *ganz über* R *ist.*

Beispiel 5.28.
$\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ *ist ganz über* $\mathbb{C}$ *als Nullstelle von* $T^2+1 \in \mathbb{C}[T]$*, aber nicht ganz über* $\mathbb{R}$*, da* $\mathbb{Z}[\sqrt{-1}] \not\subset \mathbb{R}$.

Definition 5.29.

(i) $\overline{R} := \{a \in S |\ a \text{ ist ganz über } R\}$ *heißt der* ***ganze Abschluss von*** R ***in*** S.

(ii) R *heißt* ***ganz-abgeschlossen****, wenn der ganze Abschluss von* R *in seinem Quotientenkörper gleich* R *ist.*

Satz 5.30.
$\overline{R}$ *ist ein Unterring von* S.

Beispiel 5.31.
$\mathbb{Z}$ *ist ganz-abgeschlossen.*

Satz 5.32.
Alle faktoriellen Ringe sind ganz-abgeschlossen.

Definition 5.33.
Sei d *quadratfrei. Der Körper* $\mathbb{Q}(\sqrt{d})$ *heißt* ***quadratischer Zahlkörper****. Der ganze Abschluss von* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt{d})$ *wird mit* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *bezeichnet.*

Satz 5.34.
$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ist ein freier* $\mathbb{Z}$*-Modul vom Rang* 2*, und es gilt weiter:*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{falls } d \equiv 2(4) \text{ oder } d \equiv 3(4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d \equiv 1(4) \end{cases}$$

Definition 5.35.
R *heißt* ***Dedekindscher Ring****, wenn gelten*

(i) R *ist ganz-abgeschlossen.*

(ii) *Jedes Primideal* $\mathfrak{P}$ *mit* $\{0\} \neq \mathfrak{P} \subset R$ *ist maximal.*

(iii) R *ist Noethersch.*

Satz 5.36.
Jeder Hauptidealring ist Dedekindsch.

Satz 5.37.
$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ist Dedekindsch.*

Theorem 5.38.
Ein Integritätsring R ist genau dann Dedekindsch, wenn sich jedes Ideal $\mathfrak{A}$ mit $\{0\} \neq \mathfrak{A} \underset{\neq}{\subset} R$ eindeutig (bis auf die Reihenfolge) als Produkt von Primidealen schreiben lässt.

Beispiel 5.39.
Wegen $-7 \equiv 1(4)$ ist der Noethersche Integritätsring $\mathbb{Z}[\sqrt{-7}]$ eine echte Teilmenge von $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und daher nicht ganz-abgeschlossen. $\mathbb{Z}[\sqrt{-7}]$ ist also kein Dedeking-Ring.

Nachdem sich anhand des Beispiels $\mathbb{Z}[\sqrt{-7}]$ gezeigt hat, dass nicht jeder Noethersche Integritätsring Dedekindsch ist, drängt sich nun die Frage auf, ob es für beliebige Noethersche Ringe (*nicht nur* für Noethersche Integritätsringe) nicht eine irgendwie geartete Zerlegung der Ideale gibt, die noch eine gewisse Ähnlichkeit mit der Primidealproduktzerlegung in Dedekindringen hat. Diese Frage wird durch das Theorem von Lasker-Noether beantwortet.

Definition 5.40.

*(i) Für ein Ideal $\mathfrak{A}$ von R wird $\sqrt{\mathfrak{A}} := \{z \in R |\ (\exists m \in \mathbb{N})\ z^m \in \mathfrak{A}\}$ das **Radikal von** $\mathfrak{A}$ genannt.*

*(ii) Ein Element $z \in \sqrt{\{0\}}$ heißt **nilpotent**.*

Bemerkung 5.41.
$\sqrt{\mathfrak{A}}$ ist ein Ideal von R.

Beweis. $0 \in \sqrt{\mathfrak{A}}$ ist klar. Seien $u, v \in \sqrt{\mathfrak{A}}$. Dann gibt es $l, k \in \mathbb{N}$ mit $u^l, v^k \in \sqrt{\mathfrak{A}}$. Es folgt

$$(u+v)^{l+k} = \sum_{j=0}^{l+k} \binom{l+k}{j} u^j v^{l+k-j}$$

Für $j \geq l$ liegt u^j in $\mathfrak{A}$. Für $j \leq l$ ist $l+k-j \geq k$, also liegt dann v^{l+k-j} in $\mathfrak{A}$. Da $\mathfrak{A}$ ein Ideal ist, folgt $(u+v)^{l+k} \in \mathfrak{A}$, d.h. $u+v \in \sqrt{\mathfrak{A}}$. □

Bemerkung 5.42.
Seien $\mathfrak{A}, \mathfrak{B}$ Ideale von R. Dann gelten

(i) $\mathfrak{A} \subset \sqrt{\mathfrak{A}}$

(ii) $\sqrt{\sqrt{\mathfrak{A}}} = \sqrt{\mathfrak{A}}$

(iii) $\mathfrak{A} \subset \mathfrak{B} \Rightarrow \sqrt{\mathfrak{A}} \subset \sqrt{\mathfrak{B}}$

(iv) $\sqrt{\mathfrak{A}\mathfrak{B}} = \sqrt{\mathfrak{A} \cap \mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{A}}$

Beweis.

(i) Klar, wegen $x = x^1$ für alle $x \in \mathfrak{A}$.

(ii) Gemäß (i) gilt $\sqrt{\mathfrak{A}} \subset \sqrt{\sqrt{\mathfrak{A}}}$. Gilt $z \in \sqrt{\sqrt{\mathfrak{A}}}$, so gibt es ein $l \in \mathbb{N}$ mit $z^l \in \sqrt{\mathfrak{A}}$, also gibt es ein $k \in \mathbb{N}$ mit $z^{lk} \in \mathfrak{A}$, d.h. $z \in \sqrt{\mathfrak{A}}$. Insgesamt also $\sqrt{\mathfrak{A}} = \sqrt{\sqrt{\mathfrak{A}}}$.

(iii) $x \in \sqrt{\mathfrak{A}} \Rightarrow \ (\exists k \in \mathbb{N})\ x^k \in \mathfrak{A} \subset \mathfrak{B} \Rightarrow x \in \sqrt{\mathfrak{B}}$

(iv) Da für Ideale allgemein gilt

$$\mathfrak{A}\mathfrak{B} \subset (\mathfrak{A} \cap \mathfrak{B}) \begin{cases} \subset \mathfrak{A} \\ \subset \mathfrak{B} \end{cases}$$

liefert (iii) $\sqrt{\mathfrak{A}\mathfrak{B}} \subset \sqrt{\mathfrak{A} \cap \mathfrak{B}} \subset (\sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}})$ $(*)$. Ist umgekehrt $z \in \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$, so existieren $k, l \in \mathbb{N}$ mit $z^k \in \mathfrak{A}$ und $z^l \in \mathfrak{B}$, d.h. $z^{k+l} = z^k z^l \in \mathfrak{A}\mathfrak{B}$; folglich $z \in \sqrt{\mathfrak{A}\mathfrak{B}}$. Mit $(*)$ folgt $\sqrt{\mathfrak{A}\mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{B}}$. Wiederum mit $(*)$ ergibt sich $\sqrt{\mathfrak{A}\mathfrak{B}} = \sqrt{\mathfrak{A} \cap \mathfrak{B}} = \sqrt{\mathfrak{A}} \cap \sqrt{\mathfrak{A}}$.

□

Die im Folgenden definierten Primärideale können als natürliche Verallgemeinerung der Primideale aufgefasst werden.

Definition 5.43.
Ein Ideal $\mathfrak{A} \neq R$ *von* R *heißt* ***primär*** $:\Leftrightarrow$
$uv \in \mathfrak{A}$ *und* $u \notin \mathfrak{A} \ \Rightarrow v \in \sqrt{\mathfrak{A}}$

Bemerkung 5.44.

(i) Primideale sind primär.

(ii) Für primäre Ideale $\mathfrak{A}$ ist $\sqrt{\mathfrak{A}}$ ein Primideal.

Beweis.

(i) (i) ist klar wegen $\mathfrak{A} \subset \sqrt{\mathfrak{A}}$.

(ii) Ist $uv \in \sqrt{\mathfrak{A}}$, so gibt es ein $k \in \mathbb{N}$ mit $(uv)^k = u^k v^k \in \mathfrak{A}$. Da $\mathfrak{A}$ primär ist, folgt o.E. $u \in \sqrt{\mathfrak{A}}$: Wegen $\mathfrak{A} \neq R$ ist $1 \notin \mathfrak{A}$. Wäre $1 \in \sqrt{\mathfrak{A}}$, so gäbe es ein $x \in \mathfrak{A}$ und ein $k \in \mathbb{N}$ mit $x^k = 1$. x wäre also eine Einheit und damit $\mathfrak{A} = R$. Widerspruch. Also gilt $\sqrt{\mathfrak{A}} \neq R$ und insgesamt folgt, dass $\sqrt{\mathfrak{A}}$ ein Primideal ist.

□

Definition 5.45.
*Ist $\mathfrak{A}$ primär, so heißt $\sqrt{\mathfrak{A}}$ das **zu** $\mathfrak{A}$ **gehörige Primideal**. Ist $\mathfrak{P}$ ein Primideal und $\mathfrak{A}$ primäre mit $\mathfrak{P} = \sqrt{\mathfrak{A}}$, so nennt man $\mathfrak{A}$ **zu** $\mathfrak{P}$ **gehörig**.*

Das folgende Lemma gibt zu zwei Idealen $\mathfrak{A}, \mathfrak{P}$ hinreichende Bedingungen dafür an, dass $\mathfrak{P}$ ein Primideal und $\mathfrak{A}$ zu $\mathfrak{P}$ gehörig ist.

Lemma 5.46.
Seien $\mathfrak{A}, \mathfrak{P}$ Ideale von R mit $\mathfrak{A} \neq R$ und $\mathfrak{P} \neq R$, so dass gelte

(i) $uv \in \mathfrak{A},\ u \notin \mathfrak{A} \Rightarrow v \in \mathfrak{P}$,

(ii) $u \in \mathfrak{P} \Rightarrow\ (\exists k \in \mathbb{N})\ u^k \in \mathfrak{A}$,

(iii) $\mathfrak{A} \subset \mathfrak{P}$.

Dann ist $\mathfrak{A}$ primär und $\mathfrak{P}$ das zugehörige Primideal.

Beweis. Aus (i) und (ii) folgt: $u, v \in \mathfrak{A}, u \notin \mathfrak{A} \Rightarrow v^k \in \mathfrak{A}$ für ein $k \in \mathbb{N}$, d.h. $\mathfrak{A}$ ist primär. Aus (ii) folgt $\mathfrak{P} \subset \sqrt{\mathfrak{A}}$. Sei nun $z \in \sqrt{\mathfrak{A}}$. Dann gibt es ein kleinstes $l \in \mathbb{N}$ mit $z^l \in \mathfrak{A}$. Ist $l = 1$, so ist bereits $z \in \mathfrak{P}$ wegen (iii). Ist $l > 1$, so hat man $z^l = z \cdot z^{l-1} \in \mathfrak{A}$ und, da l minimal gewählt war, $z^{l-1} \notin \mathfrak{A}$, alsdann nach (i) $z \in \mathfrak{P}$. Mithin gilt auch $\sqrt{\mathfrak{A}} \subset \mathfrak{P}$. Insgesamt also $\mathfrak{P} = \sqrt{\mathfrak{A}}$. Mit Bemerkung 5.44 (ii) folgt, dass $\mathfrak{A}$ zu $\mathfrak{P}$ gehörig ist. □

Bisher war R nur ein kommutativer Ring mit Eins. Im Falle, dass R Noethersch und $\mathfrak{A}$ primär ist mit zugehörigem Primideal $\mathfrak{P}$, lässt sich (ii) in Lemma 5.46 wesentlich verschärfen. Man kann dann die Unabhängigkeit von k von u erreichen.

Satz 5.47.
*Seien R Noethersch und $\mathfrak{A}$ primär mit zugehörigem Primideal $\mathfrak{P}$. Dann gibt es ein $k \in \mathbb{N}$, so dass **für alle** $u \in \mathfrak{P}$ gilt: $u^k \in \mathfrak{A}$.*

Beweis. Wegen der Noetherzität von R ist $\mathfrak{P}$ endlich erzeugt, etwa von $z_1, \ldots, z_s$. Da $\mathfrak{P} = \sqrt{\mathfrak{A}}$ gilt, existieren also natürliche Zahlen $t_1, \ldots, t_s$ mit $z_1^{t_1} \in \mathfrak{A}, \ldots, z_s^{t_s} \in \mathfrak{A}$. Alsdann: $z_j^t \in \mathfrak{A}$ für $t = sup(t_1, \ldots, t_s)$ und alle $j \in \mathbb{N}_s$. Jedes $z \in \mathfrak{P}$ besitzt eine Darstellung $z = \sum_{j=1}^{s} r_j z_j$ mit $r_j \in R$. Für $l := st$ folgt $z^l \in \mathfrak{A}$, da

$$z^l = \left(\sum_{j=1}^{s} r_j z_j \right)^{st} \overset{Multinomialsatz}{=} \sum_{\substack{f_1+\ldots+f_s=st \\ f_1,\ldots,f_s \geq 0}} \frac{(st)!}{f_1! f_2! \ldots f_s!} (r_1 z_1)^{f_1} \ldots (r_s z_s)^{f_s}$$

Mindestens ein f_j muss $\geq t$ sein, da ansonsten nicht $f_1 + \ldots + f_s = st$ gelten würde, d.h. mindestens ein z_j kommt in jedem Summanden mindestens zur Potenz t vor. Da $\mathfrak{A}$ ein Ideal ist, liegt also die gesamte Summe in $\mathfrak{A}$ und damit auch z^l. Damit ist das Lemma bewiesen. □

Nächstes Ziel ist es zu zeigen, dass in einem Noetherschen Ring R jedes Ideal $\mathfrak{Y} \neq R$ Durchschnitt von endlich vielen primären Idealen ist. Hierzu ist es wünschenswert, zunächst ein Kriterium zur Verfügung zu haben, welches erlaubt zu entscheiden, ob ein Ideal primär ist.

Definition 5.48.
*Ein Ideal $\mathfrak{A}$ von R wird **reduzibel** genannt, falls Ideale $\mathfrak{A}_1 \neq \mathfrak{A}$ und $\mathfrak{A}_2 \neq \mathfrak{A}$ existieren mit $\mathfrak{A} = \mathfrak{A}_1 \cap \mathfrak{A}_2$. Ist $\mathfrak{A}$ nicht reduzibel, so wird es **irreduzibel** genannt.*

Definition 5.49.
Für zwei Ideale $\mathfrak{A}_1, \mathfrak{A}_2$ von R heißt das Ideal

$$(\mathfrak{A}_1 : \mathfrak{A}_2) = \{z \in R |\ z\mathfrak{A}_2 \subset \mathfrak{A}_1\}$$

*der **Quotient** von $\mathfrak{A}_1$ und $\mathfrak{A}_2$.*

Bemerkung 5.50.
$(\mathfrak{A}_1 : \mathfrak{A}_2)$ *ist ein Ideal.*

Beweis. $0 \in (\mathfrak{A}_1 : \mathfrak{A}_2)$ ist klar. Seien $z_1, z_2 \in (\mathfrak{A}_1 : \mathfrak{A}_2)$. Sei $y \in \mathfrak{A}_2$. Dann gelten $z_1 y \in \mathfrak{A}_1$ und $z_2 y \in \mathfrak{A}_2$; folglich, da $\mathfrak{A}_1$ Ideal ist: $(z_1 + z_2)y \in \mathfrak{A}_1$. □

Bemerkung 5.51.

(i) $\mathfrak{A}_1 \subset \mathfrak{A}_2 \Rightarrow (\mathfrak{A} : \mathfrak{A}_2) \subset (\mathfrak{A} : \mathfrak{A}_1)$

(ii) $\mathfrak{A}_1 \subset (\mathfrak{A}_1 : \mathfrak{A}_2)$

(iii) $(\mathfrak{A}_1 : \mathfrak{A}_2)\mathfrak{A}_2 \subset \mathfrak{A}_1$

Beweis.

(i) Sei $z \in (\mathfrak{A} : \mathfrak{A}_2)$, also $z\mathfrak{A}_2 \subset \mathfrak{A}$. Wegen $\mathfrak{A}_1 \subset \mathfrak{A}_2$ gilt also erst recht $z\mathfrak{A}_1 \subset \mathfrak{A}$, d.h. $z \in (\mathfrak{A} : \mathfrak{A}_1)$.

(ii) Folgt sofort aus der Idealeigenschaft von $\mathfrak{A}_1$.

(iii) Sei $z \in (\mathfrak{A}_1 : \mathfrak{A}_2)\mathfrak{A}_2$, also $z = \sum_{j=1}^{t} z_j w_j$ $(t \in \mathbb{N}, z_j \in (\mathfrak{A}_1 : \mathfrak{A}_2), w_j \in \mathfrak{A}_2)$. Wegen $z_j w_j \in \mathfrak{A}_1$ $(\forall j \in \mathbb{N}_t)$ folgt $z \in \mathfrak{A}_1$.

□

Lemma 5.52.

(i) Für Ideale $\mathfrak{A}_i (i \in I)$ *und* $\mathfrak{A}$ *aus* R *gilt*

$$\left(\left(\bigcap_{i \in I} \mathfrak{A}_i \right) : \mathfrak{A} \right) = \bigcap_{i \in I} (\mathfrak{A}_i : \mathfrak{A})$$

(ii) $\mathfrak{A}$ *sei primär mit zugehörigem Primideal* $\mathfrak{P}$*. Für* $z \in R$ *gilt:*
$(\mathfrak{A} : (z)) = R$*, falls* $z \in \mathfrak{A}$*;*
$\sqrt{(\mathfrak{A} : (z))} = \mathfrak{P}$*, falls* $z \notin \mathfrak{A}$*.*

(iii) Seien $\mathfrak{P}$ *ein Primdideal und* $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ *Ideale mit* $\mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t \subset \mathfrak{P}$*. Dann gilt* $\mathfrak{A}_j \subset \mathfrak{P}$ *für mindestens ein* $j \in \mathbb{N}_t$*.*
Ist $\mathfrak{P} = \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t$*, so gilt* $\mathfrak{A}_j = \mathfrak{P}$ *für mindestens ein* $j \in \mathbb{N}_t$*.*

Beweis.

(i) Es gilt

$$\begin{aligned} z \in \left(\left(\bigcap_{i \in I} \mathfrak{A}_i \right) : \mathfrak{A} \right) \quad &\Leftrightarrow \quad z\mathfrak{A} \subset \bigcap_{i \in I} \mathfrak{A}_i \Leftrightarrow z\mathfrak{A} \subset \mathfrak{A}_i \ (\forall i \in I) \\ \Leftrightarrow z \in (\mathfrak{A}_i : \mathfrak{A}) \ (\forall i \in I) \quad &\Leftrightarrow \quad z \in \bigcap_{i \in I} (\mathfrak{A}_i : \mathfrak{A}) \end{aligned}$$

(ii) Ist $z \in \mathfrak{A}$, so folgt wegen der Idealeigenschaft von $\mathfrak{A}$: $rz \in \mathfrak{A}$ für alle $r \in R$, also auch $r(z) \subset \mathfrak{A}$ für alle $r \in R$, d.h. $(\mathfrak{A} : (z)) = R$.
Sei nun $z \notin \mathfrak{A}$. Für ein $w \in (\mathfrak{A} : (z))$ gilt $wz \in \mathfrak{A}$. Da $z \notin \mathfrak{A}$ und $\mathfrak{A}$ primär, folgt $w \in \sqrt{\mathfrak{A}} = \mathfrak{P}$ (,da $\mathfrak{P}$ zu $\mathfrak{A}$ gehörig.) Alsdann: $(\mathfrak{A} : (z)) \subset \mathfrak{P}$ $(*)$. Für jedes $u \in \mathfrak{A}$ gilt natürlich $u(z) \subset \mathfrak{A}$, da $\mathfrak{A}$ Ideal. Mithin: $\mathfrak{A} \subset (\mathfrak{A} : (z))$ $(**)$. Dies ergibt die Beziehungskette

$$\mathfrak{P} = \sqrt{\mathfrak{A}} \overset{(**)}{\subset} \sqrt{(\mathfrak{A} : (z))} \overset{(*)}{\subset} \sqrt{\mathfrak{P}} \overset{\mathfrak{P} Primideal}{=} \mathfrak{P}$$

Also gilt $\sqrt{(\mathfrak{A} : (z))} = \mathfrak{P}$.

(iii) Annahme: $\mathfrak{A}_j \not\subset \mathfrak{P}$ für alle $j \in \mathbb{N}_t$. Dann existiert zu jedem j ein $z_j \in \mathfrak{A}_j$ mit $z_j \notin \mathfrak{P}$. Es folgt

$$\prod_{j=1}^{t} z_j \in \bigcap_{j=1}^{t} \mathfrak{A}_j \overset{Vor.}{\subset} \mathfrak{P}$$

Da $\mathfrak{P}$ Primideal, folgt $z_j \in \mathfrak{P}$ für mindestens ein j. Widerspruch.
Gilt $\mathfrak{P} = \cap_{j=1}^{t} \mathfrak{A}_j$, so gilt $\mathfrak{P} \subset \mathfrak{A}_j$ $(\forall j \in \mathbb{N}_t)$. Die Annahme $\mathfrak{A}_j \not\subset \mathfrak{P}$ führte oben bereits zu einem Widerspruch. Also gilt $\mathfrak{P} = \mathfrak{A}_j$ $(\forall j \in \mathbb{N}_t)$.

□

Das Lemma findet Verwendung im Einzigkeitsnachweis des Lasker-Noether-Theorems.

Satz 5.53.
R sei Noethersch. Dann ist ein irreduzibles Ideal $\mathfrak{A} \neq R$ primär.

Beweis. Annahme: $\mathfrak{A}$ ist nicht primär. Es gibt dann $u, v \in R$ mit $uv \in \mathfrak{A}, u \notin \mathfrak{A}$ und $v^k \notin \mathfrak{A}$ für alle $k \in \mathbb{N}$. Gemäß Bemerkung 5.51 (i) erhält man eine aufsteigende Idealkette $(\mathfrak{A} : (v)) \subseteq (\mathfrak{A} : (v^2)) \subseteq \ldots$, die wegen der Noetherzität von R stationär wird. Sei $s \in \mathbb{N}$ mit $(\mathfrak{A} : (v^s)) = (\mathfrak{A} : (v^{s+1}))$. Wenn gezeigt werden kann:

$$\mathfrak{A} = (\mathfrak{A} + (u)) \cap (\mathfrak{A} + (v^s)), \quad (*)$$

so ist $\mathfrak{A}$ reduzibel im Widerspruch zur Voraussetzung, d.h. die Annahme ist falsch und alsdann $\mathfrak{A}$ primär. Es verbleibt $(*)$ zu zeigen.
"$\subset$": Hier ist nichts zu zeigen.
"$\supset$": Sei $z \in (\mathfrak{A} + (u)) \wedge (\mathfrak{A} + (v^s))$. Dann gelten $z = z_1 + bu$ mit $z_1 \in \mathfrak{A}$ und $b \in R$, und $z = z_2 + cv^s$ mit $z_2 \in \mathfrak{A}$ und $c \in R$. Folglich liegt $zv = z_1 v + buv$ in $\mathfrak{A}$ und damit auch $cv^{s+1} = zv - z_2 v$. Mithin $c \in (\mathfrak{A} : (v^{s+1}))$. Wegen $(\mathfrak{A} : (v^{s+1})) = (\mathfrak{A} : (v^s))$ also $c \in (\mathfrak{A} : (v^s))$, d.h. $cv^s \in \mathfrak{A}$. Wegen $z = z_2 + cv^s$ und $z_2, cv^s \in \mathfrak{A}$ folgt $z \in \mathfrak{A}$. Damit ist $(*)$ gezeigt. □

Satz 5.54.
In einem Noetherschen Ring lässt sich jedes Ideal $\mathfrak{A} \neq R$ als Durchschnitt endlich vieler primärer Ideale schreiben.

Beweis. Annahme: Die Aussage des Satzes ist nicht richtig. Sei $\mathcal{F}$ die Menge aller Ideale $\mathfrak{A} \neq R$, die sich nicht als Durschnitt endlich vieler primärer Ideale darstellen lassen. Nach Satz 5.2 besitzt dann $\mathcal{F}$ ein maximales Element $\mathfrak{A}_0$. Dann ist $\mathfrak{A}_0$ nicht primär, d.h. $\mathfrak{A}_0$ ist reduzibel gemäß Satz 5.53. Seien $\mathfrak{A}_1, \mathfrak{A}_2$ Ideale mit $\mathfrak{A}_1 \neq \mathfrak{A}_0, \mathfrak{A}_2 \neq \mathfrak{A}_0$ und $\mathfrak{A}_0 = \mathfrak{A}_1 \cap \mathfrak{A}_2$. Da $\mathfrak{A}_0$ maximal in $\mathcal{F}$ ist und $\mathfrak{A}_1 \neq \mathfrak{A}_0, \mathfrak{A}_2 \neq \mathfrak{A}_0, \mathfrak{A}_0 \underset{\neq}{\subset} \mathfrak{A}_1$ und $\mathfrak{A}_0 \underset{\neq}{\subset} \mathfrak{A}_2$ gelten, sind $\mathfrak{A}_1$ und $\mathfrak{A}_2$ als Durschnitt endlich vieler primärer Ideale darstellbar und damit auch $\mathfrak{A}_0$. Widerspruch. □

Eine Darstellung wie in Satz 5.54 ist natürlich nicht eindeutig. So können etwa Primärideale doppelt oder mehrfach auftreten, einige Primärideale können überflüssig sein etc. Dies führt zu

Definition 5.55.
*Eine Primärdarstellung $\mathfrak{A} = \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t$ wird **unverkürzbar** genannt, wenn $\mathfrak{A} \neq \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_{j-1} \cap \mathfrak{A}_j \cap \ldots \mathfrak{A}_t$ $(\forall j \in \mathbb{N}_t)$ gilt.*

Man drückt dies gelegentlich etwas salopp so aus: „In der Darstellung $\mathfrak{A} = \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t$ ist kein $\mathfrak{A}_j$ überflüssig“

Mit unverkürzbaren Primärzerlegungen ist immer noch keine Eindeutigkeit erreicht wie das folgende Lemma lehrt. Umgekehrt zeigt das Lemma auf, wie eine Eindeutigkeitsaussage überhaupt zu formulieren ist.

Lemma 5.56.
Der Durschnitt von Primäridealen $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$, die alle zu dem selben Primideal $\mathfrak{P}$ gehören, ist selber bereits ein Primärideal, welches zu $\mathfrak{P}$ gehört.

Beweis. Sei $uv \in \cap_{j=1}^{t} \mathfrak{A}_t$ mit $u \notin \cap_{j=1}^{n} \mathfrak{A}_t$, also $u \notin \mathfrak{A}_{j_0}$ für ein $j_0 \in \mathbb{N}_t$. Wegen $\cap_{j=1}^{t} \mathfrak{A}_j \subset \mathfrak{A}_{j_0}$ und $\mathfrak{A}_{j_0}$ primär folgt

$$v \in \sqrt{\mathfrak{A}_{j_0}} \overset{\mathfrak{A}_{j_0} \text{ zu } \mathfrak{P} \text{ gehörig}}{=} \mathfrak{P}$$

Für $u \in \mathfrak{P}$ gibt es wegen $\mathfrak{P} = \sqrt{\mathfrak{A}_j}$ $(\forall j \in \mathbb{N}_t)$ ein $s_j \in \mathbb{N}$ mit $u^{s_j} \in \mathfrak{A}_j$. Mit $s = sup(s_1, \ldots, s_t)$ also: $u^s \in \cap_{j=1}^{t} \mathfrak{A}_j$. Schließlich gilt noch

$$\bigcap_{j=1}^{t} \mathfrak{A}_j \subset \mathfrak{A}_{j_0} \subset \sqrt{\mathfrak{A}_{j_0}} = \mathfrak{P}$$

Mit Lemma 5.46 folgt die Behauptung. □

Theorem 5.57 (Lasker-Noether[3]).
Seien R ein Noetherscher Ring und $\mathfrak{Y} \neq R$ ein Ideal von R. Dann besitzt $\mathfrak{Y}$ eine unverkürzbare Darstellung $\mathfrak{Y} = \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t$, wobei die $\mathfrak{A}_j (j \in \mathbb{N}_t)$ primär sind und jeweils zu verschiedenen Primidealen $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ gehören, wobei zusätzlich die Primideale (bis auf die Reihenfolge) eindeutig bestimmt sind. Die Primärdeale $\mathfrak{A}_1, \ldots, \mathfrak{A}_t$ hingegen sind nicht eindeutig bestimmt.

Beweis. Die Existenz ist mit Satz 5.54 und Lemma 5.56 bereits gezeigt.
Zur Eindeutigkeit der Primideale: Sei $z \in R$. Nach Lemma 5.52 (i) gilt

$$(\mathfrak{Y} : (z)) = \left(\left(\bigcap_{i=1}^{t} \mathfrak{A}_i \right) : (z) \right) = \bigcap_{i=1}^{t} (\mathfrak{A}_i : (z))$$

[3] Emanuel Lasker war der bislang einzige deutsche Schachweltmeister und verteidigte diesen Titel 27 Jahre lang (1894-1921) und somit länger als jeder andere Schachweltmeister

Mittels 5.42 (iv) folgt dann

$$\sqrt{(\mathfrak{Y} : (z))} = \bigcap_{i=1}^{t} \sqrt{(\mathfrak{A}_i : (z))} \ (*)$$

Gemäß Lemma 5.52 (ii) gilt $(\mathfrak{A}_i : (z)) = R$, falls $z \in \mathfrak{A}_i$ und $\sqrt{(\mathfrak{A}_i : (z))} = \mathfrak{P}_i$, falls $z \notin \mathfrak{A}_i$. Also folgt aus $(*)$

$$\sqrt{(\mathfrak{Y} : (z))} = \bigcap_{\substack{i=1 \\ \text{und } z \notin \mathfrak{A}_i}}^{t} \mathfrak{P}_i \ (**)$$

Ist $\sqrt{(\mathfrak{Y} : (z))}$ bereits ein Primideal, so gilt nach Lemma 5.52 (iii) [unter Beachtung von $(*)$]: $\sqrt{(\mathfrak{Y} : (z))} = \mathfrak{P}_i$ für mindestens $i \in \mathbb{N}_t$.
Ist umgekehrt $i \in \mathbb{N}_t$, so gibt es, da die Darstellung $\mathfrak{Y} = \mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_t$ unverkürzbar ist, ein $z_i \in \cap_{s \neq i} \mathfrak{A}_s$ mit $z_i \notin \mathfrak{Y}$ und folglich auch $z_i \notin \mathfrak{A}_i$. Gemäß $(**)$ folgt $\sqrt{(\mathfrak{Y} : (z_i))} = \mathfrak{P}_i$. Damit ist gezeigt, dass die $\mathfrak{P}_i$ genau die Primideale in der Menge aller Ideale $\sqrt{(\mathfrak{Y} : (z))}$ $(z \in R)$ sind. Folglich gilt auch die Einzigkeitsaussage. □

Ein Beispiel, das aufzeigt, dass in der Lasker-Noether-Zerlegung die Primärideale i.A. nicht eindeutig bestimmt sind, wird in den Übungsaufgaben behandelt.

6. Sequenzen von Modulhomomorphismen

In diesem Abschnitt bezeichne R stets einen kommutativen Ring mit Eins.

Sequenzen von Modulhomomorphismen spielen in den verschiedensten Gebieten der Mathematik (Algebraische Topologie, Kommutative Algebra, ...) eine bedeutende Rolle. Dieser kurze, die Vorlesung schließende Abschnitt verfolgt die Intention, in die Begriffswelt der Sequenzen einzuführen und einige elementare Grundtatsachen der Homologischen Algebra zu beweisen, was teilweise einen Bestandteil der Übungsaufgaben darstellt. Eine systematische Darstellung der Homologischen Algebra findet man in [HS97].

Bemerkung 6.1.
F_1, F_2 seien R-Moduln. Dann ist

$$Hom(F_1, F_2) := \{f : \ F_1 \to F_2 |\ f \ R-Modulhomomorphismus\}$$

mit der offensichtlichen Addition ein $\mathbb{Z}$-Modul.

Beweis. Nachrechnen. □

Bemerkung 6.2.
F_1, F_2, L seien R-Moduln und $t \in Hom(F_1, F_2)$. Dann ist

$$t^* : Hom(F_2, L) \to Hom(F_1, L);\ f \mapsto f \circ t$$

ein $\mathbb{Z}$-Modulhomomorphismus.

Beweis.
Für $f, g \in Hom(F_1, F_2)$ gilt

$$t^*(f+g) = (f+g) \circ t = f \circ t + g \circ t = t^*(f) + t^*(g).$$

t ist also ein Homomorphismus abelscher Gruppen, d.h. ein $\mathbb{Z}$-Modulhomomorphismus. □

Definition 6.3.
*t^* heißt der **zu** t **duale Modulhomomorphismus**.*

Bemerkung 6.4.
Seien F, K, L R-Moduln und $s \in Hom(F,K)$, $t \in Hom(K,L)$. Dann gilt $(t \circ s)^* = s^* \circ t^*$.

Beweis.
Sei M ein weiterer R-Modul und $f \in Hom(L,M)$. Dann gilt

$$(t \circ s)^*(f) = f \circ (t \circ s) = (f \circ t) \circ s = (t^*(f)) \circ s = s^*(t^*(f)) = (s^* \circ t^*)(f),$$

d.h. $(t \circ s)^* = s^* \circ t^*$. □

Bemerkung 6.5.
Seien F, K, L R-Moduln. Dann ist

$$\Phi : Hom(F,K) \to Hom(Hom(K,L), Hom(F,L));\ t \mapsto t^*$$

ein $\mathbb{Z}$-Modulhomomorphismus.

Beweis.
Sei $f \in Hom(K,L)$. Für alle $s, t \in Hom(F,K)$ gilt dann

$$\Phi(s+t)(f) = f \circ (s+t) = f \circ s + f \circ t = s^*(f) + t^*(f) = \Phi(s)(f) + \Phi(t)(f),$$

d.h. $\Phi(s+t) = \Phi(s) + \Phi(t)$. □

Definition 6.6.
Seien (für $k \geq 2$) $F_1, \ldots, F_k$ R-Moduln und $t_j : F_j \to F_{j+1}$ (für $j \in \mathbb{N}_{k-1}$) R-Modulhomomorphismen. Dann heißt

$$F_1 \overset{t_1}{\to} F_2 \overset{t_2}{\to} F_3 \to \ldots \overset{t_{k-1}}{\to} F_k$$

*eine **Sequenz von Modulhomomorphismen**, im Folgenden kurz als **Sequenz** bezeichnet.*
*Eine Sequenz heißt **exakt** :⇔ $Kern(t_{j+1}) = Bild(t_j)$ $(\forall t \in \mathbb{N}_{k-2})$.*
*Eine Sequenz heißt **Komplex** :⇔ $t_{j+1} \circ t_j = 0$ $(\forall t \in \mathbb{N}_{k-2})$.*

Offensichtlich gilt

Bemerkung 6.7.

(i) Eine exakte Sequenz ist ein Komplex.

(ii) Eine Sequenz ist genau dann ein Komplex, wenn $Bild(t_j) \subset Kern(t_{j+1})$ *gilt* $(\forall t \in \mathbb{N}_{k-2})$.

Definition 6.8.
Die Sequenz $F_1 \overset{t_1}{\to} F_2 \to \ldots \overset{t_{k-1}}{\to} F_k$ *von R-Modulhomomorphismen sei ein Komplex. Dann heißt der Faktormodul* $Kern(t_j)/Bild(t_{j-1})$ *der j-te* ***Homologiemodul*** *des Komplexes* $(\forall j \in \{2, \ldots, k-1\})$.

Definition 6.9.
Bezeichne 0 *den Nullmodul, seien* F, K, L *R-Moduln und* $s \in Hom(F, K)$, $t \in Hom(K, L)$. *Ist dann die Sequenz*

$$0 \to F \overset{s}{\to} K \overset{t}{\to} L \to 0$$

exakt, so heißt sie ***kurze exakte Sequenz****.*

Beispiel 6.10.
Seien F *ein R-Modul und* L *ein Untermodul von* F. *Dann ist*

$$0 \to L \overset{inkl}{\to} F \overset{pr}{\to} F/L \to 0$$

eine kurze exakte Sequenz. (Dabei bezeichnet inkl die Inklusion und pr die kanonische Projektion.)

Bemerkung 6.11.
In einer kurzen exakten Sequenz

$$0 \to F \overset{s}{\to} K \overset{t}{\to} L \to 0$$

ist s *injektiv und* t *surjektiv.*

Beweis.
Wegen der Exaktheit gilt $Kern(s) = Bild(0 \to F) = 0$, d.h. f ist injektiv. Ebenfalls wegen der Exaktheit gilt $Bild(t) = Kern(L \to 0) = L$, d.h. g ist surjektiv. □

Definition 6.12.
Seien F, K, L R-Moduln, $s \in Hom(F,K)$, $t \in Hom(K,L)$ und $0 \to F \xrightarrow{s} K \xrightarrow{t} L \to 0$ eine kurze exakte Sequenz. Dann heißt die Sequenz ***spaltend*** $:\Leftrightarrow$ *Es existiert ein $u \in Hom(L,K)$ mit $t \circ u = id_L$.*

Lemma 6.13.
Eine kurze exakte Sequenz $0 \to F \xrightarrow{s} K \xrightarrow{t} L \to 0$ spaltet genau dann, wenn ein Untermodul K_0 von K mit $K = K_0 \oplus Bild(s)$ existiert. In diesem Fall ist $t_{|K_0}$ ein Modulisomorphismus.

Beweis.
" $\Rightarrow$ ": Da die Sequenz spaltet, existiert ein $u \in Hom(L,K)$ mit $t \circ u = id_L$. Sei $K_0 := Bild(u)$. Für $z \in K$ gilt $z = u(t(z)) + (z - u(t(z)))$. $u(t(z)) \in K_0$ ist klar und wegen $t(u(t(z))) = t(z)$ folgt $t(z - u(t(z))) = t(z) - t(z) = 0$, d.h. $z - u(t(z)) \in Kern(t)$. Folglich gilt $K = K_0 + Kern(t) = K_0 + Bild(s)$, da die Sequenz exakt ist.
Es verbleibt die Direktheit der Summe zu zeigen. Sei hierzu $z \in K_0 \cap Bild(s) = Bild(u) \cap Kern(t)$. Es gibt also ein $w \in L$ mit $z = u(w)$ und es ist $t(z) = 0$. Es ergibt sich $0 = t(z) = t(u(w)) = w$ und damit auch $0 = z$. Somit gilt $K = K_0 \oplus Bild(s)$. Dass $t_{|K_0} : K_0 \to L$ dann ein Modulisomorphismus ist, sieht man wie folgt ein.
Es ist $Kern(t_{|K_0}) = K_0 \cap Kern(t) = K_0 \cap Bild(s) = 0$, wie gerade gezeigt. D.h. $t_{|K_0}$ ist ein Modulmonomorphismus. Ist nun $w \in L$, so existiert (da t nach 6.11 ein Modulepimorphismus) ein $z \in K$ mit $t(z) = w$. Wegen $z = z_1 + z_2$ mit $z_1 \in K_0$ und $z_2 \in Bild(s) = Kern(t)$ folgt

$$t_{|K_0}(z_1) = t(z_1) = t(z_1) + 0 = t(z_1) + t(z_2) = t(z_1 + z_2) = t(z) = w.$$

Damit ist $t_{|K_0}$ auch als Modulepimorphismus nachgewiesen und somit ein Isomorphismus.
" $\Leftarrow$ ": Da $t_{|K_0}$ ein Ismorphismus ist, ist mit $inkl : K_0 \to K$ der Modulhomomorphismus $u : L \to K$ mit $u := inkl \circ (t_{|K_0})^{-1}$ wohldefiniert und es gilt offensichtlich $t \circ u = id_L$. □

Lemma 6.14.
Seien F, K, L R-Moduln, $s \in Hom(F,K)$, $t \in Hom(K,L)$ und

$0 \to F \xrightarrow{s} K \xrightarrow{t} L \to 0$ *ein kurze exake Sequenz. Die Sequenz spaltet genau dann, wenn es ein* $r \in Hom(F,K)$ *mit* $r \circ s = id_F$ *gibt.*

Beweis.
" $\Rightarrow$ " : Spaltet die Sequenz, so gibt es nach Lemma 6.13 einen Untermodul K_0 von K mit $K = K_0 \oplus Bild(s)$. Wegen der Exaktheit der Sequenz ist s ein Modulmonomorphismus und alsdann die Nachbeschränkung $s : F \to Bild(s)$ ein Isomorphismus. Mittels der Projektion

$$pr : K_1 \oplus Bild(s) \to Bild(s);\ z_1 + z \mapsto z$$

ist folglich $r := s^{-1} \circ pr : K \to F$ ein Modulhomomorphismus mit $r \circ s = id_F$.
" $\Leftarrow$ " : Existiere nun ein $r \in Hom(F,K)$ mit $r \circ s = id_F$. Für $z \in K$ gilt $z = (z - s(r(z))) + s(r(z))$. Wegen $r(z) = r(s(r(z)))$ folgt $r(z - s(r(z))) = 0$, d.h. $z - s(r(z)) \in Kern(r)$. Weiter gilt $s(r(z)) \in Bild(s)$. Mit $K_0 := Kern(r)$, also $K = K_0 + Bild(s)$. Diese Summe ist auch direkt. Da die Sequenz exakt ist, ist s surjektiv und daher gibt es zu $z \in K_0 \cap Bild(s)$ ein $w \in F$ mit $z = s(w)$ und somit folgt $0 = r(z) = r(s(w)) = w$ und damit auch $0 = z = s(w)$, d.h. $K_0 \cap Bild(s) = 0$, d.h. $K = K_0 \oplus Bild(s)$. □

Satz 6.15.
Seien F, K, L *R-Moduln,* $s \in Hom(F,K)$, $t \in Hom(K,L)$ *und die Sequenz* $F \xrightarrow{s} K \xrightarrow{t} L \to 0$ *sei exakt. Dann ist für jeden R-Modul* N *die folgende Sequenz exakt*

$$0 \to Hom(L,N) \xrightarrow{t^*} Hom(K,N) \xrightarrow{s^*} Hom(F,N).$$

Beweis.
Da die Sequenz exakt ist, ist t ein Modulepimorphismus. Sei $f \in Hom(L,N)$ mit $t^*(f) = 0$, d.h. $f \circ t = 0$. Die Surjektivität von t impliziert $f = 0$, d.h. t^* ist ein Modulmonomorphismus. Wegen der Exaktheit gilt $t \circ s = 0$. Folglich gilt für $f \in Hom(L,N)$ dann $(s^* \circ t^*)(f) = f \circ t \circ s = 0$, d.h. $s^* \circ t^* = 0$, d.h. $Bild(t^*) \subset Kern(s^*)$. Ist $g \in Kern(s^*)$, so ist $s^*(g) = g \circ s = 0$ und folglich $Bild(s) \subset Kern(g)$.
Bezeichne $pr : K \to K/Bild(s)$ die kanonische Projektion. Aus der Linearen Algebra ist bekannt, dass es dann ein eindeutig bestimmtes $\tilde{g} : K/Bild(s) \to N$ gibt mit $\tilde{g} \circ pr = g$. Wegen der Exaktheit der Sequenz gelten

$$Kern(t) = Bild(s) \text{ und } Bild(t) = L.$$

Also existiert, wie wiederum aus der Linearen Algebra bekannt, ein Isomorphismus

$$\tilde{t} : K/Bild(s) \to L \text{ mit } \tilde{t} \circ pr = t.$$

Sei $h := \tilde{g} \circ \tilde{t}^{-1}$. Dann erhält man

$$t^*(h) = h \circ t = \tilde{g} \circ \tilde{t}^{-1} \circ t = \tilde{g} \circ \tilde{t}^{-1} \circ \tilde{t} \circ pr = \tilde{g} \circ pr = g.$$

Nach Voraussetzung war $g \in Kern(s^*)$ beliebig gewählt, womit sich $Kern(s^*) \subset Bild(t^*)$ ergibt. Insgesamt gilt also $Kern(s^*) = Bild(t^*)$, was zu zeigen war. □

Bemerkung 6.16.
Seien F_1, F_2, L R-Moduln und $t \in Hom(F_1, F_2)$. Dann ist

$$t_* : Hom(L, F_1) \to Hom(L, F_2);\ f \mapsto t \circ f$$

ein $\mathbb{Z}$-Modulhomomorphismus.

Beweis. Analog zu Bemerkung 6.2. □

Definition 6.17.
t_* heißt der zu t ***coduale Modulhomomorphismus****.*

Bemerkung 6.18.
Seien F, K, L R-Moduln und $s \in Hom(F, K)$, $t \in Hom(K, L)$. Dann gilt $(t \circ s)_* = t_* \circ s_*$.

Beweis. Analog zu Bemerkung 6.4. □

Bemerkung 6.19.
Seien F, K, L R-Moduln. Dann ist

$$\Theta : Hom(F, K) \to Hom(Hom(L, F), Hom(L, K));$$
$$t \mapsto t_*$$

ein $\mathbb{Z}$-Modulhomomorphismus.

Beweis. Analog zu Bemerkung 6.5. □

Satz 6.20.
Seien F, K, L, N R-Moduln, $s \in Hom(F, K)$, $t \in Hom(K, L)$ und die Sequenz $0 \to F \xrightarrow{s} K \xrightarrow{t} L \to 0$ exakt. Dann ist auch die Sequenz

$$0 \to Hom(N, F) \xrightarrow{s_*} Hom(N, K) \xrightarrow{t_*} Hom(N, L)$$

exakt.

Beweis.
Wegen der Exaktheit ist s ein Modulmonomorphismus. Ist $f \in Hom(N, F)$ mit $s_*(f) = s \circ f = 0$, so ist also $f = 0$, was die Exaktheit von $0 \to Hom(N, F) \xrightarrow{s_*} Hom(N, K)$ impliziert.
Ist nun weiter $g \in Kern(t_*)$ mit $g \in Hom(N, K)$, so gilt $t_*(g) = t \circ g = 0$ und somit $Bild(g) \subset Kern(t) = Bild(s)$, wobei das Gleichheitszeichen wegen der Exaktheit gilt. Wegen der Injektivität von s folgt die Wohldefiniertheit von $f := s^{-1} \circ g$ und es gilt $s_*(f) = s \circ s^{-1} \circ g = g$, d.h. $g \in Bild(s_*)$. Folglich $Kern(t_*) \subset Bild(s_*)$.
Wegen der Exaktheit gilt $t \circ s = 0$, d.h. mit 6.18: $t_* \circ s_* = (t \circ s)_* = 0$, womit sich insgesamt $Kern(t_*) = Bild(g_*)$ ergibt. Somit ist auch die Sequenz $Hom(N, K) \xrightarrow{s_*} Hom(N, F) \xrightarrow{t_*} Hom(N, L)$ exakt. Damit ist dann die Exaktheit der Gesamtsequenz nachgewiesen. □

Sehr allgemeine und damit für Anwendungen naturgemäß sehr nützliche Aussagen gewinnt man, wenn man die Beziehungen von durch kommutativen Diagrammen gekoppelte exakte Sequenzen (oder auch Komplexen) von Modulhomomorphismen untersucht. Ein solcher Satz, der bereits in das weite Gebiet der Homologischen Algebra fällt, wird abschließend vorgestellt. Dass die hierbei verwendete Beweistechnik „diagram-chasing“ genannt wird, wird nach dem Studium des Beweises offensichtlich.

Satz 6.21. ***(Fünfer-Lemma)***
Für $j \in \mathbb{N}_5$ seien F_j, K_j R-Moduln, $t_j \in Hom(F_j, K_j)$ und für $i \in \mathbb{N}_4$ seien $a_i \in Hom(F_i, F_{i+1})$ und $b_i \in Hom(K_i, K_{i+1})$. Weiter sei das folgende Diagramm

kommutativ mit exakten Zeilen.

$$\begin{array}{ccccccccc} F_1 & \xrightarrow{a_1} & F_2 & \xrightarrow{a_2} & F_3 & \xrightarrow{a_3} & F_4 & \xrightarrow{a_4} & F_5 \\ t_1 \downarrow & & t_2 \downarrow & & t_3 \downarrow & & t_4 \downarrow & & t_5 \downarrow \\ K_1 & \xrightarrow{b_1} & K_2 & \xrightarrow{b_2} & K_3 & \xrightarrow{b_3} & K_4 & \xrightarrow{b_4} & K_5 \end{array}$$

Dann gelten:

(i) Sind t_2 und t_4 injektiv sowie t_1 surjektiv, dann ist t_3 injektiv.

(ii) Sind t_2 und t_4 surjektiv sowie t_5 injektiv, so ist t_3 surjektiv.

(iii) Sind t_1, t_2, t_4, t_5 Isomorphismen, so ist auch t_4 ein Isomorphismus.

Beweis.

(i) Sei $z \in F_3$ mit $t_3(z) = 0$

$\Rightarrow b_3(t_3(z)) = 0$

$\Rightarrow t_4(a_3(z)) = 0,$ da $b_3 \circ t_3 = t_4 \circ a_3$

$\Rightarrow a_3(z) = 0,$ da t_4 injektiv

$\Rightarrow \exists w \in F_2$ mit $a_2(w) = z,$ wegen der Exaktheit der ersten Zeile

$\Rightarrow b_2(t_2(w)) = 0,$ da $b_2 \circ t_2 = t_3 \circ a_2$

$\Rightarrow \exists v \in K_1$ mit $b_1(v) = t_2(w),$ wegen der Exaktheit der zweiten Zeile

$\Rightarrow \exists u \in F_1$ mit $t_1(u) = v,$ da t_1 surjektiv

$\Rightarrow t_2(a_1(u)) = b_1(t_1(u)) = b_1(v) = t_2(w)$

$\Rightarrow a_1(u) = w,$ da t_2 injektiv

$\Rightarrow z = a_2(w) = a_2(a_1(u)) = 0,$ da wegen der Exaktheit der ersten Zeile $a_2 \circ a_1 = 0$

$\Rightarrow t_3$ ist injektiv.

(ii) Sei $z \in K_3$

$\Rightarrow \exists y \in F_4$ mit $t_4(y) = b_3(z)$, da t_4 surjektiv

$\Rightarrow t_5(a_4(y)) = b_4(t_4(y)) = b_4(b_3(z)) = 0$, da $t_5 \circ a_4 = b_4 \circ t_4$ und wegen der Exaktheit der zweiten Zeile $b_4 \circ b_3 = 0$

$\Rightarrow a_4(y) = 0$, da t_5 injektiv

$\Rightarrow \exists x \in F_3$ mit $a_3(x) = y$ wegen der Exaktheit der ersten Zeile

$\Rightarrow b_3(t_3(x)) = t_4(a_3(x)) = t_4(y) = b_3(z)$

$\Rightarrow t_3(x) - z \in Kern(b_3)$

$\Rightarrow t_3(x) - z \in Bild(b_2)$, da die zweite Zeile exakt ist

$\Rightarrow \exists u \in K_2$ mit $b_2(u) = t_3(x) - z$

$\Rightarrow \exists w \in F_2$ mit $t_2(w) = u$, da t_2 surjektiv

$\Rightarrow t_3(x - a_2(w)) = t_3(x) - b_2(t_2(w))$, da $t_3 \circ a_2 = b_2 \circ t_2$

$\Rightarrow t_3(x - a_2(w)) = t_3(x) - b_2(u) = z$

$\Rightarrow t_3$ ist surjektiv.

(iii) Ist eine unmittelbare Konsequenz aus (i) und (ii).

□

Aus kommutativen Diagrammen von Moduln und Modulhomomorphismen mit exakten Zeilen lässt sich über einen verbindenden Modulhomomorphismus eine einzige exakte Sequenz von Modulhomomorphismen konstruieren. Dieses ist der Inhalt von

Satz 6.22 (**Schlangenlemma**)**.**

$$\begin{array}{rccccc} & F_1 & \xrightarrow{s_1} & F_2 & \xrightarrow{s_2} & F_3 \longrightarrow 0 \\ & a_1 \downarrow & & a_2 \downarrow & & a_3 \downarrow \\ 0 \longrightarrow & L_1 & \xrightarrow{t_1} & L_2 & \xrightarrow{t_2} & L_3 \end{array}$$

sei ein kommutatives Diagramm von R-Moduln $F_j, L_j (j \in \mathbb{N}_3)$ *und R-Modulhomomorphismen* $s_j, t_j (j \in \mathbb{N}_2)$ *und* $a_j (j \in \mathbb{N}_3)$*. Seien* $G_j := Kern(a_j)$ *und*

$K_j = L_j/Bild(a_j)(j \in \mathbb{N}_3)$).
Es existiert ein kanonischer Modulhomomorphismus $d : G_3 \to K_1$*, so dass die Sequenz* $G_1 \overset{s_{1|G_1}}{\to} G_2 \overset{s_{2|G_2}}{\to} G_3 \overset{d}{\to} K_1 \overset{\tilde{t}_1}{\to} K_2 \overset{\tilde{t}_2}{\to} K_3$ *exakt ist. Dabei bezeichnen für* $j \in \mathbb{N}_2$ $\tilde{t}_j$ *die durch* t_j *induzierten R-Modulhomomorphismen. d heißt* ***verbindender R-Modulhomomorphismus****.*

Beweis. Für $x \in G_1$ hat man $a_2(s_1(x)) = t_1(a_1(x)) = 0$ und folglich $s_1(s) \in G_2 = Kern(a_2)$. Damit ist $s_{1|G_1}$ wohldefiniert und die Wohldefiniertheit von $s_{2|G_2}$ folgt analog.
Aus der Exaktheit von $F_1 \overset{s_1}{\to} F_2 \overset{s_2}{\to} F_3$ folgt unmittelbar, dass $G_1 \overset{s_{1|G_1}}{\to} G_2 \overset{s_{2|G_2}}{\to} G_3$ ein Komplex ist. Sei nun $x \in G_2$ und $s_2(x) = 0$
$\Rightarrow$ $\exists z \in F_1$ mit $s_1(z) = x$
$\Rightarrow$ $t_1(a_1(z)) = a_2(s_1(z)) = a_2(x) = 0$, da $x \in G_2 = Kern(a_2)$
$\Rightarrow$ $a_1(z) = 0$, da wegen der Exaktheit von $L_1 \overset{t_1}{\longrightarrow} L_2 \overset{t_2}{\longrightarrow} L_3$ t_1 monomorph ist
$\Rightarrow$ $z \in G_1$
Damit ist die Exaktheit von $G_1 \overset{s_{1|G_1}}{\to} G_2 \overset{s_{2|G_2}}{\to} G_3$ gezeigt. Es bezeichne pr_2 die kanonische Projektion: $L_2 \to K_2$. Wegen $Bild(a_1) \subset Kern(pr_2 \circ t_1)$ induziert also t_1 kanonisch einen Modulhomomorphismus $\tilde{t}_1 : K_1 \to K_2$. Analog induziert t_2 kanonisch einen Modulhomomorphismus $\tilde{t}_2 : K_2 \to K_3$. Wegen der Exaktheit von $L_1 \overset{t_1}{\longrightarrow} L_2 \overset{t_2}{\longrightarrow} L_3$ gilt $t_2 \circ t_1 = 0$, was $\tilde{t}_2 \circ \tilde{t}_1 = 0$ impliziert und also $Bild(\tilde{t}_1) \subset Kern(\tilde{t}_2)$. Nun wird weiter die Exaktheit von $K_1 \overset{\tilde{t}_1}{\to} K_2 \overset{\tilde{t}_2}{\to} K_3$ gezeigt.
Seien $x \in Kern(\tilde{t}_2)$ und $z \in L_2$ mit $pr_2(z) = x$
$\Rightarrow$ $pr_3(t_2(z)) = \tilde{t}_2(pr_2(z)) = \tilde{t}_2(x) = 0$
$\Rightarrow$ $\exists w \in F_3$ mit $a_3(w) = t_2(z)$
$\Rightarrow$ $\exists u \in F_2$ mit $s_2(u) = w$, da s_2 wegen der Exaktheit ein Epimorphismus ist
$\Rightarrow$ $t_2(a_2(u)) = a_3(s_2(u)) = a_3(w) = t_2(z)$
$\Rightarrow$ Für $u_1 := z - a_2(u)$ gilt $pr_2(u_1) = pr_2(z) - pr_2(a_2(u)) = pr_2(z) - 0 = pr_2(z) = x$ und $t_2(u_1) = t_2(z) - t_2(a_2(u)) = t_2(z) - t_2(z) = 0$
$\Rightarrow$ $\exists y \in L_1$ mit $t_1(y) = u_1$ wegen der Exaktheit der Sequenz $L_1 \overset{t_1}{\longrightarrow} L_2 \overset{t_2}{\longrightarrow} L_3$
$\Rightarrow$ $\tilde{t}_1(pr_1(y)) = pr_2(t_1(y)) = pr_2(u_1) = x$.
Damit ist auch $Bild(\tilde{t}_1) \supset Kern(\tilde{t}_2)$ und damit insgesamt die Exaktheit der Sequenz $K_1 \overset{\tilde{t}_1}{\to} K_2 \overset{\tilde{t}_2}{\to} K_3$ gezeigt.
Es wird nun gezeigt, dass es zu jedem $x \in G_3$ und jedem $y \in F_2$ mit $s_2(y) = x$

genau ein $z \in L_1$ mit $t_1(z) = a_2(y)$ existiert. Sei hierzu $x \in G_3$
$(*) \Rightarrow \exists y \in F_2$ mit $s_2(y) = x$, da wegen der Exaktheit s_2 epimorph ist
$\Rightarrow\ t_2(a_2(y)) = a_3(s_2(y)) = a_3(x) = 0$, da $x \in G_3 = Kern(a_3)$.
Wegen der Exaktheit ist t_1 monomorph und $Kern(t_2) = Bild(t_1)$, $(**)$ d.h. es gibt genau ein $z \in F_1$ mit $t_1(z) = a_2(y)$. Es liegt nun nahe den verbindenden Homomorphismus $d : G_3 \to K_1$ vermittels $d(x) := pr_1(z)$ zu definieren. Hierzu ist zunächst zu zeigen, dass d wohldefiniert ist, da z von der Wahl von y in $(*)$ abhängig ist, d.h. es ist die Unabhängigkeit von y in der Definition von d zu zeigen. Ist $\tilde{y}$ ein weiteres Element aus F_2 mit $s_2(\tilde{y}) = x$, also $\tilde{y} = y + (\tilde{y} - y)$ mit dem y aus $(*)$, so ist $\tilde{y} - y \in F_2$ mit $s_2(\tilde{y} - y) = 0$, d.h. $\tilde{y} - y \in Bild(s_1) = Kern(s_2)$, d.h. $\exists w \in F_1$ mit $\tilde{y} = y + s_1(w)$. Dann gilt $t_1(z + a_1(w)) = t_1(z) + t_1(a_1(w)) = t_1(z) + a_2(s_1(w)) = a_2(y) + a_2(s_1(w)) = a_2(\tilde{y})$. Alsdann: $pr_1(z + a_1(w)) = pr_1(z) + pr_1(a_1(w)) = pr_1(z)$, d.h. d ist wohldefiniert.
Wählt man zu $x, \tilde{x}$ aus G_3 $y, \tilde{y}$ wie in $(*)$ und $z, \tilde{z}$ wie in $(**)$, so kann man offenbar zu $x + \tilde{x}$ die Elemente $y + \tilde{y}$ und $z + \tilde{z}$ sowie zu rx $(r \in R)$ die Elemente ry und rz wählen, so dass gemäß Definition von d und der Homomorphieeigenschaft von pr_1 die Homomorphieeigenschaft von d folgt.
Aufgrund der bereits bewiesenen Exaktheit der Sequenzen $G_1 \to G_2 \to G_3$ und $K_1 \to K_2 \to K_3$ ist das Schlangenlemma bewiesen, wenn abschließend noch die Exaktheit der Sequenz $G_2 \to G_3 \stackrel{d}{\to} K_1 \to K_2$ gezeigt wird.
Sei $x \in G_3$ mit $d(x) = 0$
$\Rightarrow\ pr_1(z) = 0$ [z wie in $(**)$]
$\Rightarrow\ \exists w \in F_1$ mit $a_1(w) = z$
$\Rightarrow\ t_1(z) = t_1(a_1(w)) = a_2(s_1(w))$
$\Rightarrow$ Mit y wie in $(*)$ und $\tilde{y} := y - s_1(w)$ gilt $s_2(\tilde{y}) = s_2(y) - s_2(s_1(w)) = s_2(y)$ [da $s_2 \circ s_1 = 0$] $= x$, da y wie in $(*)$ gewählt wurde,
und weiter: $a_2(\tilde{y}) = a_2(y) - a_2(s_1(w)) = a_2(y) - t_1(a_1(w)) = a_2(y) - t_1(z) \stackrel{(**)}{=} 0$
$\Rightarrow\ \tilde{y} \in G_2$ und $s_2(\tilde{y}) = x$, d.h. $Kern(d) \subset Bild(s_{2|G_2})$.
Ist nun $x = s_2(w)$ für ein $w \in G_2 = Kern(a_2)$, so kann man in $(*)$ $y = w$ wählen. Es folgt $a_2(w) = 0$ und mit z wie in $(**)$ folgt $t_1(z) = a_2(w) = 0$ und somit wegen der Injektivität von t_1: $z = 0$. Folglich $d(x) = pr_1(z) = 0$. Somit gilt also $Bild(s_{2|G_2}) \subset Kern(d)$. Insgesamt also $Kern(d) = Bild(s_{2|G_2})$.
Der Nachweis von $Bild(d) = Kern(\tilde{t}_1)$ bleibe dem Leser überlassen. Damit ist das Schlangenlemma bewiesen. $\square$

Mittels des Schlangenlemmas lässt sich sehr elegant der u.a. für die Algebraische Topologie bedeutsame Satz über lange exakte Homologiesequenzen beweisen. Vorab:

Bemerkung 6.23.
Gegeben seien zwei Komplexe $\mathcal{F}: \ldots \to F_{i-1} \overset{a_{i-1}}{\to} F_i \overset{a_i}{\to} F_{i+1} \to \ldots$ *und* $\mathcal{L}: \ldots \to L_{i-1} \overset{b_{i-1}}{\to} L_i \overset{b_i}{\to} L_{i+1} \to \ldots$ *von R-Moduln und R-Modulhomomorphismen. Dabei sei* $i \in \mathbb{Z}$. *Weiter seien* $t_i : F_i \to L_i$ *R-Modulhomomorphismen, so dass das Diagramm*

$$\begin{array}{ccccccc} \ldots \longrightarrow & F_{i-1} & \overset{a_{i-1}}{\longrightarrow} & F_i & \overset{a_i}{\longrightarrow} & F_{i+1} & \longrightarrow \ldots \\ & t_{i-1}\downarrow & & t_i\downarrow & & t_{i+1}\downarrow & \\ \ldots \longrightarrow & L_{i-1} & \overset{b_{i-1}}{\longrightarrow} & L_i & \overset{b_i}{\longrightarrow} & L_{i+1} & \longrightarrow \ldots \end{array}$$

kommutiert. Schließlich seien $H_i^{\mathcal{F}}$ *und* $H_i^{\mathcal{L}}$ *die i-ten Homologiemoduln der Komplexe* $\mathcal{F}$ *und* $\mathcal{L}$. *Dann induzieren die* t_i *kanonische R-Modulhomomorphismen* $\tilde{t}_i : H_i^{\mathcal{F}} \to H_i^{\mathcal{L}}$.

Beweis. Aufgabe 33. □

Satz 6.24 (**exakte lange Homologiesequenz**).
In dem kommutativen Diagramm

$$\begin{array}{ccccccc} & 0 & & 0 & & 0 & \\ & \downarrow & & \downarrow & & \downarrow & \\ \mathcal{F}: \cdots \longrightarrow & F_{i-1} & \overset{a_{i-1}}{\longrightarrow} & F_i & \overset{a_i}{\longrightarrow} & F_{i+1} & \longrightarrow \cdots \\ & t_{i-1}\downarrow & & t_i\downarrow & & t_{i+1}\downarrow & \\ \mathcal{L}: \cdots \longrightarrow & L_{i-1} & \overset{b_{i-1}}{\longrightarrow} & L_i & \overset{b_i}{\longrightarrow} & L_{i+1} & \longrightarrow \cdots \\ & s_{i-1}\downarrow & & s_i\downarrow & & s_{i+1}\downarrow & \\ \mathcal{N}: \cdots \longrightarrow & N_{i-1} & \overset{c_{i-1}}{\longrightarrow} & N_i & \overset{c_i}{\longrightarrow} & N_{i+1} & \longrightarrow \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ & 0 & & 0 & & 0 & \end{array}$$

von R-Moduln und R-Modulhomomorphismen seien $i \in \mathbb{Z}$, $\mathcal{F}, \mathcal{L}, \mathcal{N}$ Komplexe und alle Kolonnen seien exakt.
Dann gibt es kanonische Modulhomomorphismen $d_i : H_i^{\mathcal{N}} \to H_{i+1}^{\mathcal{F}}$, so dass die Sequenz

$$\cdots \longrightarrow H_{i-1}^{\mathcal{N}} \xrightarrow{d_{i-1}} H_i^{\mathcal{F}} \xrightarrow{\tilde{t}_i} H_i^{\mathcal{L}} \xrightarrow{\tilde{s}_i} H_i^{\mathcal{N}} \xrightarrow{d_i} H_{i+1}^{\mathcal{F}} \longrightarrow \cdots$$

exakt ist. Dabei bezeichnen $\tilde{t}_i$ und $\tilde{s}_i$ die durch t_i und s_i induzierten R-Modulhomomorphismen aus Bemerkung 6.23.

Beweis. Sei $i \in \mathbb{Z}$. Nach dem Schlangenlemma sind in dem Diagramm

$$\begin{array}{ccccccc} & & F_i/Bild(a_{i-1}) & \longrightarrow & L_i/Bild(b_{i-1}) & \longrightarrow & N_i/Bild(c_{i-1}) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & Kern(a_{i+1}) & \longrightarrow & Kern(b_{i+1}) & \longrightarrow & Kern(c_{i+1}) \end{array}$$

die Zeilen exakt. In dem Diagramm

$$\begin{array}{ccccc} 0 & & 0 & & 0 \\ \downarrow & & \downarrow & & \downarrow \\ H_i^{\mathcal{F}} & \longrightarrow & H_i^{\mathcal{L}} & \longrightarrow & H_i^{\mathcal{N}} \\ \downarrow incl & & \downarrow incl & & \downarrow incl \\ F_i/Bild(a_{i-1}) & \longrightarrow & L_i/Bild(b_{i-1}) & \longrightarrow & N_i/Bild(c_{i-1}) \\ \downarrow & & \downarrow & & \downarrow \\ Kern(a_{i+1}) & \longrightarrow & Kern(b_{i+1}) & \longrightarrow & Kern(c_{i+1}) \\ \downarrow pr & & \downarrow pr & & \downarrow pr \\ H_{i+1}^{\mathcal{F}} & \longrightarrow & H_{i+1}^{\mathcal{L}} & \longrightarrow & H_{i+1}^{\mathcal{N}} \\ \downarrow & & \downarrow & & \downarrow \\ 0 & & 0 & & 0 \end{array}$$

sind dann die zweite und fünfte Zeile ebenfalls exakt und es gibt nach dem Schlangenlemma einen verbindenden Homomorphismus $d_i : H_i^{\mathcal{N}} \longrightarrow H_{i+1}^{\mathcal{F}}$. Damit ist die Teilsequenz

$$H_i^{\mathcal{F}} \longrightarrow H_i^{\mathcal{L}} \longrightarrow H_i^{\mathcal{N}} \longrightarrow H_{i+1}^{\mathcal{F}} \longrightarrow H_{i+1}^{\mathcal{L}} \longrightarrow H_{i+1}^{\mathcal{N}}$$

der langen Homologiesequenz exakt. Da $i \in \mathbb{Z}$ beliebig gewählt war, folgt die Behauptung. □

A. Topologische Räume

In diesem Anhang werden einige Begriffe und Ergebnisse der mengentheoretischen Topologie aufgeführt. Eine umfassende Einführung in dieses Gebiet gibt [Kow60].

Ein **topologischer Raum** $(T, \mathcal{T})$ ist eine Menge T mit einem System $\mathcal{T}$ von Teilmengen von T, so dass gelten:

(T_1) $T \in \mathcal{T}$ und $\emptyset \in \mathcal{T}$
(T_2) Jede Vereinigung von Mengen aus $\mathcal{T}$ liegt in $\mathcal{T}$
(T_3) Jeder endliche Durchschnitt von Mengen aus $\mathcal{T}$ liegt in $\mathcal{T}$.

Die Elemente von $\mathcal{T}$ heißen **offene Mengen** von T und $\mathcal{T}$ heißt die Topologie von T.

Ist (T, d) ein metrischer Raum und $\mathcal{T}$ das System aller $U \subset T$ mit der Eigenschaft, dass zu jedem $a \in U$ ein $\varepsilon > 0$ existiert mit $\Delta_\varepsilon(a) := \{x \in T | d(x, a) < \varepsilon\} \subset U$, so definiert $\mathcal{T}$ eine Topologie auf T. Insbesondere sind damit die Anschauungsräume $\mathbb{R}^n$ und $\mathbb{C}^n$ kanonisch topologisiert, wenn für d die Euklidische Metrik gewählt wird.

Eine Menge $A \subset T$ heißt **abgeschlossen**, wenn $A^C := T \backslash A$ offen ist. Die Durchschnitte beliebig vieler und die Vereinigung endlich vieler abgeschlossender Mengen sind abgeschlossen.

Zu jedem $U \subset T$ gibt es eine größte offene Teilmenge $V \subset U$, nämlich die Vereinigung aller offenen Teilmengen von U. V heißt der **offene Kern** von U und wird mit $\overset{o}{U}$ bezeichnet. Ein $y \in \overset{o}{U}$ heißt ein **innerer Punkt** von U.

Zu jedem $U \subset T$ gibt es eine kleinste abgeschlossene Teilmenge V mit $U \subset V$, nämlich den Durchschnitt aller U umfassenden abgeschlossenen Teilmengen. V heißt die **abgeschlossene Hülle** von U und wird mit $\overline{U}$ bezeichnet. Die Punkte $y \in \overline{U}$ heißen **Berührungspunke** von U. Zwischen $\overline{U}$ und $\overset{o}{U}$ besteht die Beziehung $(\overset{o}{U})^C = \overline{U^C}$. Sind $X, Y \subset T$, so heißt X **dicht** in Y, falls $Y \subset \overline{X}$. T heißt **separabel**, wenn T eine abzählbare dichte Teilmenge besitzt.

Sind $x \in T, U \subset T$, so heißt, U **Umgebung von** x, wenn es ein $V \in \mathcal{T}$ mit $x \in V \subset U$ gibt. Man nennt $\mathcal{U}(x) := \{U | U \text{ Umgebung von } x\}$ den **Umgebungsfilter von** x. Sind $A, U \subset T$, so heißt U **Umgebung von** A, wenn ein $V \in \mathcal{T}$ mit $A \subset V \subset U$ existiert.

Ein topologischer Raum $(T, \mathcal{T})$ heißt T_2**-Raum** (oder auch **Hausdorff-Raum**), wenn zu allen $x, y \in T$ Umgebungen A von x und B von y existieren mit $A \cap B = \emptyset$. Alle metrischen Räume sind T_2-Räume; ebenso alle C^∞-differenzierbaren Mannigfaltigkeiten und damit auch alle Riemannschen Flächen. Der Sierpinski-Raum $\mathbb{S} := (S, \mathfrak{T})$ mit $S := \{0, 1\}$ und $\mathfrak{T} := \{\emptyset, \{0, 1\}, \{0\}\}$ ist kein T_2-Raum.

Eine Menge $\mathfrak{A} \subset \mathcal{T}$ heißt **Basis** von $\mathcal{T}$, wenn jedes $X \in \mathcal{T}$ Vereinigung von Mengen aus $\mathfrak{A}$ ist. Eine Menge $\mathfrak{W} \subset \mathcal{U}(x)$ heißt **Umgebungsbasis** von $x \in T$, wenn zu jedem $U \in \mathcal{U}(x)$ ein $V \in \mathfrak{W}$ mit $V \subset U$ existiert. Ist (T, d) ein metrischer Raum, so bilden die Kugeln $\Delta_\varepsilon(x)$ eine Umgebungsbasis von x und das System $(\Delta_\varepsilon(x))_{\varepsilon > 0, x \in T}$ ist eine Basis von (T, d). Ein topologischer Raum $(T, \mathcal{T})$ genügt dem **ersten Abzählbarkeitsaxiom**, wenn jedes $x \in T$ eine abzählbare Umgebungsbasis besitzt. $(T, \mathcal{T})$ genügt dem **zweiten Abzählbarkeitsaxiom**, falls $\mathcal{T}$ eine abzählbare Basis besitzt. Alle metrischen Räume genügen dem ersten Abzählbarkeitsaxiom, die Anschauungsräume $\mathbb{R}^n, \mathbb{C}^n$, alle C^∞-differenzierbaren Mannigfaltigkeiten sowie alle Riemannschen Flächen erfüllen das zweite Abzählbarkeitsaxiom. Das zweite Abzählbarkeitsaxiom impliziert das erste Abzählbarkeitsaxiom. Separable metrische Räume erfüllen das zweite Abzählbarkeitsaxiom, während topologische Räume, die dem zweiten Abzählbarkeitsaxiom genügen, bereits separabel sind.

Sind $(T_1, \mathcal{T}_1), (T_2, \mathcal{T}_2)$ zwei topologische Räume und $\varphi : T_1 \to T_2$ eine Ab-

bildung, so heißt φ **stetig in** x, wenn es zu jeder Umgebung W von $\varphi(x)$ eine Umgebung V von x gibt mit $f(V) \subset W$. φ heißt **stetig**, wenn φ in jedem Punkt x stetig ist. Dies ist äquivalent dazu, dass die Urbilder $\varphi^{-1}(A)$ offener Mengen A aus $\mathcal{T}_2$ offen in $\mathcal{T}_1$ sind und auch äquivalent dazu, dass die Urbilder $\varphi^{-1}(C)$ abgeschlossener Mengen C aus $\mathcal{T}_2$ abgeschlossen in $\mathcal{T}_1$ sind. Verknüpfungen stetiger Funktionen sind stetig. φ heißt **Homöomorphismus** (oder auch **topologisch**), wenn φ bijektiv und stetig und φ^{-1} ebenfalls stetig ist. Ist φ homöomorph, so heißen T_1 und T_2 **homöomorph**.

Beispiel A.1.

(i) Zwei offene, nichtleere Intervalle von $\mathbb{R}$ sind homöomorph, z.B. $M = (-1,1)$ und $N = (0,5)$: Mit $f : M \to N;\ f(x) = \frac{5}{2}(x+1)$ und $g : N \to M;\ g(x) = \frac{2}{5}x - 1$ gilt für die stetigen Geraden:

$$f \circ g = id_N, \quad \text{sowie} \quad g \circ f = id_M.$$

(ii) Man kann die rellen Zahlen $\mathbb{R}$ auf das offene Intervall $(-1,1)$ „zusammenziehen“:

$$f : (-1,1) \to \mathbb{R};\ f(x) = tan\left(\frac{\pi x}{2}\right)$$

ist bijektiv, stetig und besitzt die stetige Inverse

$$g : \mathbb{R} :\to (-1,1);\ g(x) = \frac{2}{\pi} arctan(x).$$

(iii) Die Rechtecke

$$S = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \ : \ x \in [-1,1], y \in [0,1] \right\}$$

und

$$T = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \ : \ x \in [-2,2], y \in [0,3] \right\}$$

sind via

$$f : S \to T;\ f(x,y) = \begin{pmatrix} 2x \\ 3y \end{pmatrix} \ \text{bzw. } g : T \to S;\ g(x,y) = \begin{pmatrix} x/2 \\ y/3 \end{pmatrix}$$

homöomorph.

Sind $(T, \mathcal{T})$ ein topologischer Raum und $\mathfrak{W}$ ein System offener Teilmengen von T, so heißt $\mathfrak{W}$ eine **offene Überdeckung** von $X \subset T$, falls $X \subset \bigcup_{W \in \mathfrak{W}} W$. Eine Teilmenge $\mathfrak{C}$ von $\mathfrak{W}$ heißt **Teilüberdeckung**, falls $\mathfrak{C}$ eine Überdeckung von X ist. T heißt **kompakt**, wenn T ein T_2-Raum ist und jede offene Überdeckung von T eine endliche Teilüberdeckung besitzt. Eine Teilmenge X von T heißt **kompakt**, wenn der topologische Raum $(X, \mathcal{T}|X)$ kompakt ist. Dabei ist die Topologie $\mathcal{T}|X$ definiert durch $\mathcal{T}|X := \{X \cap A | A \in \mathcal{T}\}$ und wird die **Spurtopologie** von $\mathcal{T}$ auf X genannt. X heißt **relativ kompakt**, falls $\overline{X}$ kompakt ist. Stetige Bilder kompakter Mengen sind kompakt. Jede abgeschlossene Menge eines kompakten Raumes ist kompakt. Jede stetige bijektive Abbildung eines kompakten Raumes in einen T_2-Raum ist ein Homöomorphismus. Jede kompakte Teilmenge eines T_2-Raumes ist abgeschlossen. Die Sphären S^n und der Torus $S^1 \times S^1$ sind kompakt. Die offene Einheitskugel $\Delta_1(0)$ des $\mathbb{R}^n$ ist relativ kompakt.

Sind $\mathcal{T}_1, \mathcal{T}_2$ Topologien auf T, so heißt $\mathcal{T}_2$ **feiner** als $\mathcal{T}_2$, falls $\mathcal{T}_1 \subset \mathcal{T}_2$ und $\mathcal{T}_2$ heißt **schwächer** als $\mathcal{T}_1$, falls $\mathcal{T}_2 \subset \mathcal{T}_1$. Die schwächste Topologie auf T ist $\{T, \emptyset\}$ und heißt **indiskrete Topologie**. Die feinste Topologie auf T ist die Potenzmenge $\mathcal{P}(T)$ von T und heißt **diskrete** Topologie auf T.

Eine Folge (x_n) in einem topologischen Raum $(T, \mathcal{T})$ heißt **konvergent gegen** $x \in \mathcal{T}$, wenn es zu jedem $U \in \mathcal{U}(x)$ ein $n_1 \in \mathbb{N}$ mit $x_n \in U$ für alle $n \geq n_1$ gibt. Der Limes ist nicht eindeutig bestimmt. In einem indiskreten Raum $(T, \mathcal{T})$ konvergiert jede Folge gegen jeden Punkt aus T. In T_2-Räumen ist der Limes eindeutig bestimmt.

In einem topologischen Raum $(T, \mathcal{T})$ heißen $A, B \in \mathcal{T}$ **Zerlegungsmengen**, wenn sie disjunkt sind mit $A \cup B = T$. Sind $\emptyset$ und T die einzigen Zerlegungsmengen, so heißt T **zusammenhängend**. $A \subset T$ heißt **zusammenhängende Teilmenge** von T, falls $(A, \mathcal{T}|A)$ zusammenhängend ist. Stetige Bilder zusammenhängender Teilmengen sind zusammenhängend. Die Anschauuungsräume $\mathbb{R}^n$ und $\mathbb{C}^n$, die Sphären S^n, der Torus $S^1 \times S^1$ und die Kugeln $\Delta_\varepsilon(a)$ in $\mathbb{R}^n$ sind zusammenhängend. Alle Riemannschen Flächen sind zusammenhängend. $\mathbb{Q}^n$ ist nicht zusammenhängend in $\mathbb{R}^n$.

Ein topologischer Raum $(X, \mathcal{T})$ heißt **wegzusammenhängend**, wenn es zu

jedem Paar $(x, y) \in X^2$ einen stetigen Weg $c_{(x,y)} : [0, 1] \to X$ gibt mit $c_{(x,y)}(0) = x$ und $c_{(x,y)}(1) = y$. Wegzusammenhängende Räume sind zusammenhängend. Stetige Bilder wegzusammenhängender Räume sind wegzusammenhängend. In den Anschauungsräumen $\mathbb{R}^n$ und $\mathbb{C}^n$ fallen die Begriffe wegzusammenhängend und zusammenhängend zusammen. Eine **Schleife** in X ist eine stetige Abbildung $S^1 \to X$. Eine Schleife in X heißt **zusammenziehbar**, wenn sie eine stetige Fortsetzung $K^2 \to X$ besitzt (mit $K^2 = \left\{(x, y) \in \mathbb{R}^2 \middle| x^2 + y^2 \leq 1\right\}$). Ein wegzusammenhängender topologischer Raum $(X, \mathcal{T})$ heißt **einfach-zusammenhängend**, wenn jede Schleife in X zusammenziehbar ist. Ein wegweise zusammenhängender Raum ist genau dann einfach-zusammenhängend, wenn seine Fundamentalgruppe [s. Satz 2.18] trivial ist. Die Anschauungsräume $\mathbb{R}^n$ und $\mathbb{C}^n$, der Sierpinski-Raum $\{0, 1\}$ mit der Topologie $\{\emptyset, \{0\}, \{0, 1\}\}$, der projektive Raum $\mathbb{CP}^1$ und die Sphären S^n (für $n \geq 2$) sind einfach-zusammenhängend. S^1, der Torus $S^1 \times S^1$ und $\mathbb{C}\setminus\{0\}$ sind nicht einfach-zusammenhängend.

Seien $(T, \mathcal{T})$ ein topologischer Raum, $\sim$ eine Äquivalenzrelation auf T, $[T]$ der Raum der Äquivalenzklassen und $\pi : T \to [T]$ die kanonische Projektion. Durch U offen in $[T] :\Leftrightarrow \pi^{-1}(U)$ offen in T, wird eine Topologie auf $[T]$ definiert, welche als **Quotiententopologie bzgl.** $\sim$ bezeichnet wird. Sie ist die schwächste Topologie auf $[T]$, so dass π stetig ist. Die T_2-Eigenschaft überträgt sich i.A. nicht von T auf $[T]$. Notwendige Bedingung (aber i.A. nicht hinreichend) dafür ist, dass die Äquivalenzklassen $[x]$ für $x \in T$ abgeschlossen in $[T]$ sind.

Eine stetige Abbildung zwischen zwei topologischen Räumen heißt **offen**, wenn sie offene Mengen auf offene Mengen abbildet und sie heißt **abgeschlossen**, wenn sie abgeschlossene Mengen auf abgeschlossene Mengen abbildet. Nichtkonstante holomorphe Funktionen sind offen. Jede stetige Abbildung eines kompakten Raumes in einen T_2-Raum ist abgeschlossen.

Ein T_2-Raum $(\hat{T}, \hat{\mathcal{T}})$ heißt **lokal-kompakt**, wenn jeder Punkt x eine kompakte Umgebung besitzt. Die Anschauungsräume $\mathbb{R}^n, \mathbb{C}^n$, alle C^∞-differenzierbaren Mannigfaltigkeiten und alle Riemannschen Flächen sind lokal-kompakt. Ist $(T, \mathcal{T})$ ein topologischer Raum und ∞ ein Symbol mit $\infty \notin T$, so ist $(\tilde{T}, \tilde{\mathcal{T}})$ mit $\tilde{T} := T \cup \{\infty\}$ und $\tilde{\mathcal{T}} := \mathcal{T} \cup \left\{\tilde{T}\backslash K \middle| K \subset T \text{ kompakt}\right\}$ ein kompakter topo-

logischer Raum. Ist T nicht kompakt, so ist T offen und dicht in $\tilde{T}$. $(\tilde{T}, \tilde{\mathcal{T}})$ heißt die **Alexandroff-Kompaktifizierung** von $(T, \mathcal{T})$. Sie ist genau dann ein T_2-Raum, wenn $(T, \mathcal{T})$ lokal-kompakt ist. Die Riemannsche Zahlenkugel S^2 ist bis auf Homöomorphie die Alexandroff-Kompaktifizierung von $\mathbb{C}$.

Ein T_2-Raum $(T, \mathcal{T})$ heißt **parakompakt**, wenn es zu jeder offenen Überdeckung eine **lokal-endliche Verfeinerung** gibt, d.h. wenn es zu jeder offenen Überdeckung $\mathfrak{A}$ von T eine offene Überdeckung $\mathfrak{B} := \{B_i\}_{i \in I}$ von T gibt mit

(i) $\mathfrak{B}$ ist **lokal-endlich**, d.h. zu jedem $a \in T$ existiert eine Umgebung U von a mit $U \cap B_i \neq \emptyset$ nur für endlich viele $i \in I$.

(ii) $\mathfrak{B}$ ist eine **Verfeinerung** von $\mathfrak{A}$, d.h. zu jedem V aus $\mathfrak{B}$ gibt es ein $U \in \mathfrak{A}$ mit $V \subset U$.

Die Anschauungsräume $\mathbb{R}^n$ und $\mathbb{C}^n$, alle C^∞-differenzierbaren Mannigfaltigkeiten und alle Riemannschen Flächen sind parakompakt. Kompakte Räume sind parakompakt. Eine Familie $\{f_j\}_{j \in J}$ stetiger Abbildungen $T \to [0, 1]$ heißt **Teilung der Eins**, wenn sie **lokal-endlich** ist, d.h. zu jedem $a \in T$ gibt es eine Umgebung U von a mit $f_{j|U} \equiv 0$ für alle j bis auf endlich viele Ausnahmen, und wenn $\sum_{j \in J} f_j(a) = 1$ für alle $a \in T$ gilt.

Eine Teilung der Eins heißt einer vorgegebenen Überdeckung $\mathfrak{A}$ **subordiniert**, wenn für alle $j \in J$ die Träger $\{a \in T | f_j(a) \neq 0\}$ der f_j Teilmenge einer Überdeckungsmenge $U_{i(j)}$ aus $\mathfrak{A}$ sind.

Ein T_2-Raum ist genau dann parakompakt, wenn es zu jeder offenen Überdeckung eine dieser Überdeckung subordinierte Teilung der Eins gibt. Bei den C^∞-differenzierbaren Mannigfaltigkeiten und Riemannschaen Flächen können die entsprechenden Teilungen der Eins sogar C^∞-differenzierbar gewählt werden [BJ73].

Sei I eine Indexmenge und $(T_i, \mathcal{T}_i)_{i \in I}$ eine Familie topologischer Räume und $T := \prod_{i \in I} T_i = \left\{ f : I \to \bigcup_{i \in I} T_i \middle| f(i) \in T_i (\forall i) \right\}$. Das System aller Mengen $\prod_{i \in I} U_i$ mit $U_i = T_i$ für alle bis auf endlich viele i und $U_i \in \mathcal{T}_i$ sonst, bildet die Basis einer Topologie $\mathcal{T}$ auf T, die als die **Produkttopologie** auf T

bezeichnet wird. Sie ist die schwächste Topologie auf T, so dass für alle $k \in I$ die Projektionen $\pi_k : T \to T_k;\ (a_i)_{i \in I} \mapsto a_k$ stetig werden. Die π_k sind offene Abbildungen. Das Produkt eines parakompakten Raumes mit einem kompakten Raum ist parakompakt. Tiefliegend ist das **Tychonoff-Theorem**: Das Produkt kompakter Räume ist kompakt.

B. Übungsaufgaben

Aufgabe1:
Gegeben sei die Operation

$$x * y := \frac{xy}{x + y + 1}$$

auf der Menge der positiven reellen Zahlen. Überprüfen Sie, ob diese Verknüpfung kommutativ bzw. assoziativ ist. Besitzt die Operation ein neutrales bzw. inverses Element?

Aufgabe 2:
Seien $M, N \in GL(n, \mathbb{R})$ sowie $x, y \in \mathbb{R}^n$.
Zeigen Sie, dass $GL(n, \mathbb{R}) \times \mathbb{R}^n$ für $n > 1$ versehen mit der Multiplikation

$$(M, x)(N, y) = (MN, My + x)$$

eine Gruppe bildet.

Aufgabe 3:
Gegeben sei die Gruppe G durch die Verknüpfungstafel

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Zeigen Sie, dass G zyklisch ist und geben Sie das erzeugende Element an.

Zur Erinnerung: Eine Gruppe G heißt zyklisch, wenn sie von einem Element $a \in G$ erzeugt wird, d.h. es gilt

$$G = \{a^n | n \in \mathbb{Z}\} = \langle a \rangle.$$

Aufgabe 4:
Zeigen Sie:

$$G = \langle a, b, c, d, e \mid d = e^2, bda = 1, ab^{-1}c = 1, ac^{-1}b^{-1} = 1, de = c \rangle$$

ist isomorph zur zyklischen Gruppe der Ordnung 12.
Hinweis: Entfernen Sie sukzessive alle Generatoren bis Sie die Präsentation $\langle a | a^{12} = 1 \rangle$ erhalten. Beginnen Sie mit $d = e^2$ um d zu eliminieren.

Aufgabe 5:
Gegeben sei die Artinsche Zopfgruppe B_3 mit den Generatoren σ_1 und σ_2. Zeigen Sie für $\Delta = \Delta_3 = \sigma_1\sigma_2\sigma_1$:

(i) $\Delta\sigma_1 = \sigma_2\Delta$,

(ii) $\Delta\sigma_2 = \sigma_1\Delta$,

(iii) Δ^2 kommutiert mit beiden Generatoren.

Aufgabe 6:
Beweisen oder widerlegen Sie:
In der Zopfgruppe B_n, $(n > 2)$ gibt es eindeutig bestimmte Wurzeln, d.h. wenn für zwei Zöpfe $\beta^n = \gamma^n$ gilt, dann folgt daraus $\beta = \gamma$.

Aufgabe 7:
Eine totalgeordnete Gruppe G heißt linksorderabel, wenn aus $g < h$ folgt, dass $fg < fh$ für alle $f, g, h \in G$. Zeigen Sie, dass in einer linksorderablen Gruppe G gilt:

(i) $1 < g \Rightarrow g^{-1} < 1$,

(ii) G ist torsionsfrei.

Zur Erinnerung: Ein Torsionselement ist ein Element endlicher Ordnung in einer Gruppe, also ein Element, für das eine natürliche Zahl existiert mit $g^n = 1$ (bzw. $n \cdot g = 0$ in additiver Schreibweise).

Alle Ringe in den Aufgaben 8 - 39 seien kommutativ und mit Eins!

Aufgabe 8:
Bestimme $\left(\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)^*$

Aufgabe 9:
Seien R ein Ring, $x \in R$ und $\mathcal{M}$ der Durchschnitt aller maximalen Ideale von R. Zeige:
$x \in \mathcal{M} \Leftrightarrow 1 - xy \ \in R^*$ für alle $y \in R$.

Aufgabe 10:
Bestimme eine Lösung des Zahlenrätsels

$$CHINA \cdot CHINA = *****CHINA$$

Dabei stehe jeder Buchstabe für eine Ziffer und jedes Sternchen für eine beliebige Ziffer. Es soll keine Zahl mit 0 beginnen.

Aufgabe 11:
Bestimme die größte negative Lösung des Kongruenzsystems

$$\begin{aligned} x &\equiv -1(2) \\ x &\equiv -2(3) \\ x &\equiv -3(5) \\ x &\equiv -4(7) \end{aligned}$$

Aufgabe 12:
Überprüfe, ob 2 irreduzibel in $\mathbb{Z}[\sqrt{-1}]$ ist.

Aufgabe 13:
Ein R-Modul P heißt **projektiv** :$\Leftrightarrow$ Es existiert ein R-Modul F, so dass $P \times F$ frei ist.
Beweise: P ist genau dann projektiv, wenn es zu jedem R-Modulepimorphismus $f : L \to P$ einen Untermodul L' von L gibt mit $L = L' \oplus Kern(f)$.

Aufgabe 14:
Zeige: Jeder freie Modul ist projektiv.

Aufgabe 15:
Seien $R_1, R_2 \neq \{0\}$ Ringe. Dann ist $R_1 \times \{0\}$ ein $(R_1 \times R_2)$-Untermodul des $R_1 \times R_2$-Moduls $R_1 \times R_2$. Zeige

(i) $R_1 \times \{0\}$ ist projektiv,

(ii) $R_1 \times \{0\}$ ist nicht frei.

Aufgabe 16:
Seien P ein projektiver Untermodul des Moduls F und F/P projektiv. Zeige: F ist ein projektiver Modul.

Aufgabe 17:
Überprüfe, ob der $\mathbb{Z}$-Modul $\mathbb{Q}$ projektiv ist.

Aufgabe 18:
Seien F_1, F_2 R-Moduln mit F_1 Noethersch und $\varphi : F_1 \to F_2$ ein R-Modulepimorphismus. Zeige: F_2 ist Noethersch.

Aufgabe 19:
Seien F_1, F_2 Noethersche R-Moduln. Zeige: $F_1 \times F_2$ ist Noethersch.

Aufgabe 20:
Seien F ein R-Modul und F_1, F_2 Untermoduln von F mit F/F_1 und F/F_2 Noethersch. Zeige: $F/(F_1 \cap F_2)$ ist Noethersch.

Aufgabe 21:
Gilt der Hilbertsche Basissatz auch in einer "Artinschen Version"? Genauer: K sei Körper. Ist dann der Polynomring $K[T]$ Artinsch? (Begründung!)

Aufgabe 22:
Ist der Ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ ein Dedekind-Ring? (Begründung!)

Aufgabe 23:
Seien $\mathfrak{A}_1, \mathfrak{A}_2$ Ideale in einem Ring R. Zeige: $\sqrt{\mathfrak{A}_1 + \mathfrak{A}_2} = \sqrt{\sqrt{\mathfrak{A}_1} + \sqrt{\mathfrak{A}_2}}$

Aufgabe 24:
Sei $\mathfrak{P}$ ein Primideal in einem Ring R. Zeige: $\sqrt{\mathfrak{P}} = \mathfrak{P}$.

Aufgabe 25:
Sei $\mathfrak{A}$ ein Ideal in einem Ring R mit $\sqrt{\mathfrak{A}}$ maximal. Zeige: $\mathfrak{A}$ ist primär.

Aufgabe 26:
Bestimme alle primären Ideale von $\mathbb{Z}$.

Aufgabe 27:
Betrachte im Polynomring $K[T_1, T_2]$ (K Körper) das Ideal $(T_1^2, T_1T_2) =: \mathfrak{A}$ und zeige, dass

$$\begin{aligned} \mathfrak{A} &= (T_1) \cap (T_1^2, T_2) \\ &= (T_1) \cap (T_1, T_2)^2 \end{aligned}$$

zwei unverkürzbare Darstellungen von $\mathfrak{A}$ als Durchschnitt von Primäridealen mit zugehörigen Primidealen (T_1) und (T_1, T_2) sind.
Damit ist, wie bereits in der Vorlesung erwähnt, gezeigt, dass die Primärideale in der Lasker-Noetherschen Primärzerlegung i.A. nicht eindeutig bestimmt sind.
Hinweis: Aufgabe 25 ist hilfreich.

Aufgabe 28:
Betrachte in $\mathbb{Z}[T]$ das Ideal $\mathfrak{A} := (3T, T^2)$. Zeige $\mathfrak{A} = (3, T^2) \cap (T)$ und überprüfe, ob dies eine unverkürzbare Darstellung von $\mathfrak{A}$ als Durchschnitt von Primäridealen ist.

Aufgabe 29:
Seien F ein R-Modul und $t : F \to F$ ein R-Modulendomorphismus. Beweise oder widerlege:

(i) Ist F Artinsch und t ein Monomorphismus, so ist t ein Isomorphismus.

(ii) Ist F Noethersch und t ein Epimorphismus, so ist t ein Isomorphismus.

Aufgabe 30:
Zeige, dass in einem Artinschen Ring jedes Primideal maximal ist.

Aufgabe 31:
Überprüfe, ob der Ring $C([0,1], \mathbb{R}) := \{g : [0,1] \to \mathbb{R} |\ g \text{ stetig}\}$ Noethersch ist.

Aufgabe 32:
Es sei $0 \to F_1 \to F_2 \to \ldots \to F_n \to 0$ eine exakte Sequenz endlicher $\mathbb{Z}$-Moduln. Beweise:

$$\prod_{i \equiv 0(2)} card(F_i) = \prod_{i \not\equiv 0(2)} card(F_i)$$

Aufgabe 33:
Gegeben seien zwei Komplexe

$$\mathfrak{F}: \ \ldots \to F_{i-1} \overset{a_{i-1}}{\to} F_i \overset{a_i}{\to} F_{i+1} \to \ldots$$

und

$$\mathfrak{L}: \ \ldots \to L_{i-1} \overset{b_{i-1}}{\to} L_i \overset{b_i}{\to} L_{i+1} \to \ldots$$

von R-Moduln und R-Modulhomomorphismen. Dabei sei $i \in \mathbb{Z}$. Weiter seien $t_i : F_i \to L_i$ R-Modulhomomorphismen, so dass das Diagramm

$$\begin{array}{ccccccc} \ldots \longrightarrow & F_{i-1} & \overset{a_{i-1}}{\longrightarrow} & F_i & \overset{a_i}{\longrightarrow} & F_{i+1} & \longrightarrow \ldots \\ & t_{i-1} \downarrow & & t_i \downarrow & & t_{i+1} \downarrow & \\ \ldots \longrightarrow & L_{i-1} & \overset{b_{i-1}}{\longrightarrow} & L_i & \overset{b_i}{\longrightarrow} & L_{i+1} & \longrightarrow \ldots \end{array}$$

kommutiert. Schließlich seien $H_i^{\mathfrak{F}}, H_i^{\mathfrak{L}}$ die i-ten Homologiemoduln [vgl. 6.8] der Komplexe $\mathfrak{F}$ und $\mathfrak{L}$.
Beweise: Die t_i induzieren kanonische R-Modulhomomorphismen $\tilde{t}_i : H_i^{\mathfrak{F}} \to H_i^{\mathfrak{L}}$.

Aufgabe 34:
Seien F, K, L R-Moduln und $s \in Hom(F, K)$.
Beweise oder widerlege: Aus der Exaktheit der Sequenz $0 \to F \overset{s}{\to} K$ folgt die Exaktheit der Sequenz $Hom(K, L) \overset{s^*}{\to} Hom(F, L) \to 0$.

Aufgabe 35:
M sei ein R-Modul. Zeige: M ist genau dann projektiv (vgl. Aufgabe 13), wenn jede kurze exakte Sequenz $0 \to F \to K \to M \to 0$ spaltet (F, K beliebige R-Moduln).

Aufgabe 36:
Seien F, K, L, M, N R-Moduln.

(i) Beweise: M ist genau dann projektiv (vgl. Aufgabe 13), wenn zu jedem Modulepimorphismus $g : L \to N$ und jedem Modulhomomorphismus $h : M \to N$ ein Modulhomomorphismus $k : M \to L$ existiert mit $g \circ k = h$.

(ii) Beweise: M ist genau dann projektiv, wenn für alle $s \in Hom(F, K)$ und $t \in Hom(K, L)$ aus der Exaktheit der Sequenz $F \xrightarrow{s} K \xrightarrow{t} L$ auch die Exaktheit der Sequenz $Hom(M, F) \xrightarrow{s_*} Hom(M, K) \xrightarrow{t_*} Hom(M, L)$ folgt.

Aufgabe 37:
Das folgende Diagramm von R-Moduln und R-Modulhomomorphismen

$$\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & & \downarrow \\
 & & & & F_1 & \xrightarrow{a_1} & F_2 & \xrightarrow{a_2} & F_3 \\
 & & & & s_1 \downarrow & & s_2 \downarrow & & s_3 \downarrow \\
0 & \longrightarrow & K_1 & \xrightarrow{b_1} & K_2 & \xrightarrow{b_2} & K_3 \\
 & & t_1 \downarrow & & t_2 \downarrow & & \\
 & & L_1 & \xrightarrow{c_1} & L_2 & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
\end{array}$$

sei kommutativ mit exakten Zeilen und Kolonnen.
Beweise: c_1 ist ein R-Modulmonomorphismus.

Aufgabe 38:
Das folgende Diagramm von R-Moduln und R-Modulhomomorphismen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_1 & \longrightarrow & F_2 & \longrightarrow & F_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K_1 & \longrightarrow & K_2 & \longrightarrow & K_3 & \longrightarrow & 0 \end{array}$$

sei kommutativ und die beiden Zeilen seien exakt. Zudem seien zwei der senkrechten Pfeile R-Modulisomorphismen. Dann gilt das auch für den dritten senkrechten Pfeil.

Aufgabe 39:
Das folgende Diagramm von R-Moduln und R-Modulhomomorphismen

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F_1 & \xrightarrow{a_1} & F_2 & \xrightarrow{a_2} & F_3 & \longrightarrow & 0 \\ & & d_1 \downarrow & & e_1 \downarrow & & f_1 \downarrow & & \\ 0 & \longrightarrow & K_1 & \xrightarrow{b_1} & K_2 & \xrightarrow{b_2} & K_3 & \longrightarrow & 0 \\ & & d_2 \downarrow & & e_2 \downarrow & & f_2 \downarrow & & \\ 0 & \longrightarrow & L_1 & \xrightarrow{c_1} & L_2 & \xrightarrow{c_2} & L_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

sei kommutativ und die drei Kolonnen seien exakt. Beweise:

(i) Sind die ersten beiden Zeilen exakt, so ist auch die dritte Zeile exakt.

(ii) Sind die erste und die dritte Zeile exakt und gilt $b_2 \circ b_1 = 0$, so ist auch die zweite Zeile exakt.

Aufgabe 40:
Beweise für den Sierpinski-Raum $\mathbb{S}$ die Gültigkeit von $\pi_1(\mathbb{S}) = 0$.

Literaturverzeichnis

[Ber10] *Berrick, A.J. et al* (2010): Introductory Lectures on Braids, Configurations and their Applications. World Scientific.

[BJ73] *Bröcker, T.; Jänich, K.* (1973): Einführung in die Differentialtopologie. Springer.

[Deh08] *Dehornoy, P. et al.* (2008): Ordering Braids. Mathematical Surveys and Monographs, Volume 148, AMS.

[DR72] *Diederich, K.; Remmert, R.* (1972): Funktionentheorie I. Springer.

[DKR08] *Duma, A.; Kuzyk, K.; Radtke, W.* (2008): Einführung in die Theorie der Riemannschen Flächen. FernUniv. Hagen.

[Grö68] *Gröbner, W.* (1968): Algebraische Geometrie I. Bibliographisches Institut.

[HS97] *Hilton, P.; Stammbach, U.* (1997): A Course in Homological Algebra. Springer (2. Aufl.).

[Kas77] *Kasch, F.* (1977): Moduln und Ringe. Teubner.

[KT08] *Kassel, Christian; Tuarev, Vladimir* (2008): Braid Groups GTM 247. Springer.

[Ka06] *Katz, Sheldon*(2006): Enumerative Geometry and String Theory. AMS.

[Kow60] *Kowalsky, H.-J.* (1960): Topologische Räume. Birkhäuser.

[Lan86] *Lang, S.* (1986): Algebraic Number Theory (2. Aufl.) Springer.

[Lan02] *Lang, S.* (2002): Algebra (2. Aufl.) Springer.

[Mat06] *Matveev, Sergey V.* (2006): Lectures in Algebraic Topology, EMS, Series of Lectures in Mathematics.

[Pin10] *Pinter, Charles C.* (2010): A Book of Abstract Algebra (2. Aufl.) Dover Publications.

[SS02] *Scharlau, W.; Schulte, M.* (2002): Algebra I. FernUniv. Hagen.

[SS03] *Scharlau, W.; Schulte, M.* (2003): Algebra II. FernUniv. Hagen.