

Skript zur Algebra I

Vorlesung im Sommersemester 2009
an der Technischen Universität Berlin

Prof. Dr. F. Heß

18. Juni 2009

Inhaltsverzeichnis

1	Gruppen	3
1.1	Notation	3
1.2	Halbgruppen	4
1.3	Gruppen	8
1.4	Nebenklassen	11
1.5	Normalteiler	13
1.6	Homomorphismen	15
1.7	Faktorgruppen	17
1.8	Zyklische Gruppen	20
1.9	Direkte Produkte	22
1.10	Semidirekte Produkte	26
1.11	Operationen von Gruppen auf Mengen	30
1.12	Sylowsätze	33
1.13	Anwendungen auf endliche Gruppen	37
1.14	Weitere Themen	39
1.14.1	Gruppenerweiterungen	40
1.14.2	Kompositionsreihen	41
1.14.3	Einfache Gruppen	41
1.14.4	Auflösbare Gruppen	42
1.14.5	Freie Gruppen	43
2	Ringe I	45
2.1	Grundlagen	45
2.2	Ideale und Homomorphismen	48
2.3	Faktorringe	49
2.4	Nullteiler	51
2.5	Schiefkörper, Körper und einfache Ringe	54
2.6	Direkte Produkte und orthogonale Idempotente	55
2.7	Chinesischer Restsatz	57
2.8	Charakteristik und Primringe	60

2.9	Noethersche Ringe	61
2.10	Maximale Ideale	62
2.11	Integritätsringe und Primideale	64
2.12	Teilbarkeit in Ringen	66
2.13	Lokale Ringe und Lokalisierung	72
3	Polynomringe	81
3.1	Univariate Polynomringe	81
3.2	Polynomringe über Körpern	85
3.3	Nullstellen von Polynomen	86
3.4	Basissatz von Hilbert	88
3.5	Satz von Gauß	89
3.6	Irreduzibilität von Polynomen	93
3.7	Multivariate Polynomringe	96
3.8	Symmetrische Polynome	98
3.9	Resultanten und Diskriminanten	101
3.10	Potenzreihen- und Laurentreihenringe	105
3.11	Monoid- und Gruppenringe	108
4	Moduln I	111
4.1	Grundlagen	111
4.2	Noethersche und Artinsche Moduln	116
4.3	Matrizen über Ringen	120
4.4	Moduln und Matrizen über Hauptidealringen	122
4.5	Gröbnerbasen	131

Kapitel 1

Gruppen

1.1 Notation

Die Symbole $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ bezeichnen die ganzen, rationalen, reellen und komplexen Zahlen. Die positiven ganzen Zahlen werden mit $\mathbb{Z}^{\geq 1}$ bezeichnet. Weitere Variationen dieser Schreibweise erklären sich von selbst.

Ist R ein Körper (oder auch nur ein Ring), so bezeichnet $R^{n \times m}$ die Menge der $n \times m$ Matrizen mit Einträgen aus R .

Bei den Mächtigkeiten von Mengen unterscheiden wir nur endliche Mächtigkeiten und unendlich (∞). Zum Rechnen mit ∞ beziehungsweise in der Teilerrelation verwenden wir folgende Konvention:

$$n \cdot \infty = \infty \cdot m = \infty \text{ und } n | \infty \text{ für alle } n, m \in \mathbb{Z}^{\geq 1} \cup \{\infty\}. \quad (1.1)$$

Ebenso nehmen wir $n | 0$ für alle $n \in \mathbb{Z} \setminus \{0\} \cup \{\infty\}$ an. Das Minimum einer leeren Menge ist ∞ . Die weitere Verwendung von ∞ in Formeln geschieht dann auf entsprechend sinnvolle Weise.

Der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache ganzer Zahlen wird mit \gcd beziehungsweise lcm bezeichnet (greatest common divisor und least common multiple).

Wir schreiben $p^r || n$, wenn p eine Primzahl ist und p^r die größte Potenz von p ist, welche n teilt.

Sind G, H Mengen, $f : G \rightarrow H$ eine Abbildung, $A \subseteq G$, und $B \subseteq H$, so schreiben wir $f(A) = \{f(a) \mid a \in A\}$ für das Bild von A unter f und $f^{-1}(B) = \{a \in G \mid f(a) \in B\}$ für das Urbild von B unter f .

Seien X, I Mengen und $U_i \subseteq X$ Teilmengen von X für $i \in I$. Dann bezeichnen wir mit $\cup_{i \in I} U_i = \cup \{U_i \mid i \in I\}$ die Vereinigung und mit $\cap_{i \in I} U_i = \cap \{U_i \mid i \in I\}$ den Durchschnitt der U_i . Die Notation $\dot{\cup}_{i \in I} U_i$ bedeutet, daß zusätzlich $U_i \cap U_j = \emptyset$

für alle $i, j \in I$ mit $i \neq j$ gilt. Die Notation $\dot{\cup}\{U_i \mid i \in I\}$ hingegen bedeutet, daß für $U, V \in \{U_i \mid i \in I\}$ mit $U \neq V$ auch $U \cap V = \emptyset$ gilt.

Mit $\delta_{i,j}$ bezeichnen wir das Kronecker-Delta, für welches $\delta_{i,j} = 1$ für $i \neq j$ und $\delta_{i,i} = 0$ für $i = j$ gilt.

Ist X eine Menge, so bezeichnen wir mit id_X die Funktion $\text{id}_X : X \rightarrow X$ mit $\text{id}_X(x) = x$ für alle $x \in X$.

1.2 Halbgruppen

Seien X, Y Mengen. Eine *Verknüpfung* \circ auf X mit Operatorbereich Y ist eine Funktion $\circ : Y \times X \rightarrow X$. Die Funktionsanwendung $\circ(a, b)$ wird in Infixnotation $a \circ b$ geschrieben. Für $Y = X$ sprechen wir auch einfach nur von einer Verknüpfung auf X . Beispiele für Verknüpfungen sind $+$ und \cdot auf \mathbb{Z} oder die Hintereinanderausführung von Abbildungen auf der Menge X der Abbildungen einer Menge in sich selbst. Für $A \subseteq Y$ und $B \subseteq X$ definieren wir $A \circ B = \{a \circ b \mid a \in A, b \in B\}$ sowie $a \circ B = \{a\} \circ B$ und $A \circ b = A \circ \{b\}$ für $a \in A$ und $b \in B$.

Eine Verknüpfung \circ auf X heißt *assoziativ*, wenn $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in X$ gilt. Für eine assoziative Verknüpfung braucht man daher nicht zu klammern, Ausdrücke der Form $a_1 \circ \dots \circ a_n$ werden mit Hilfe einer beliebigen Klammerung definiert. Eine Verknüpfung heißt *kommutativ*, wenn $a \circ b = b \circ a$ für alle $a, b \in X$ gilt.

Eine *Halbgruppe* G ist ein Tupel (X, \circ) bestehend aus einer Menge X und einer assoziativen Verknüpfung \circ auf X . Ist \circ zusätzlich kommutativ, so heißt (X, \circ) *kommutativ* oder *abelsch*. Die Ordnung $\#G$ einer Halbgruppe ist $\#X$.

Seien $G = (X, \circ_X)$ und $H = (Y, \circ_Y)$ Halbgruppen. Ein *Homomorphismus* $f : G \rightarrow H$ der Halbgruppen G und H besteht aus einer Funktion $g : X \rightarrow Y$ mit $g(a \circ_X b) = g(a) \circ_Y g(b)$ für alle $a, b \in X$. Man sagt, daß f strukturerhaltend sei. Notationsweise nimmt man es hier normalerweise nicht so genau (die genaue Bedeutung ist meist vom Kontext her klar) und benutzt die gleichen Symbole für G und X beziehungsweise H und Y , und für f und g .

Für Homomorphismen wird die folgende Standardnomenklatur verwendet: $f : G \rightarrow H$ ist ein *Monomorphismus* $:\Leftrightarrow f : G \rightarrow H$ ist ein injektiver Homomorphismus. $f : G \rightarrow H$ ist ein *Epimorphismus* $:\Leftrightarrow f : G \rightarrow H$ ist ein surjektiver Homomorphismus. $f : G \rightarrow H$ ist ein *Isomorphismus* $:\Leftrightarrow f : G \rightarrow H$ ist ein bijektiver Homomorphismus. $f : G \rightarrow H$ ist ein *Endomorphismus* $:\Leftrightarrow f : G \rightarrow H$ ist ein Homomorphismus und es gilt $G = H$. $f : G \rightarrow H$ ist ein *Automorphismus* $:\Leftrightarrow f : G \rightarrow H$ ist ein Endomorphismus und Isomorphismus.

Die Hintereinanderausführung von Homomorphismen ist wieder ein Homomorphismus. Die inverse Abbildung eines Isomorphismus ist wieder ein Isomor-

phismus. Zwei Halbgruppen G und H heißen isomorph (strukturgleich), wenn es einen Isomorphismus zwischen ihnen gibt, in Zeichen $G \cong H$. Isomorphie ist eine Äquivalenzrelation.

Sei G eine Halbgruppe mit Verknüpfung \circ . Ein Element $e \in G$ heißt *linksneutrales* Element von G , wenn $e \circ x = x$ für alle $x \in G$ gilt. Ein Element $e \in G$ heißt *rechtsneutrales* Element von G , wenn $x \circ e = x$ für alle $x \in G$ gilt. Ein *neutrales* Element von G ist ein links- und rechtsneutrales Element von G .

Falls es in G ein neutrales Element gibt, so ist es eindeutig bestimmt: Sind $e_1, e_2 \in G$ neutrale Elemente, so gilt nach Voraussetzung $e_1 = e_1 \circ e_2 = e_2$. Eine Halbgruppe G mit neutralem Element heißt *Monoid*.

Sei G ein Monoid mit Verknüpfung \circ und neutralem Element e . Sind $a, b \in G$ mit $a \circ b = e$, so heißt a *Links inverses* von b und b *Rechts inverses* von a . Ist b Links inverses von a und Rechts inverses von a , so heißt b *Inverses* von a . Ein Element $a \in G$ heißt (*rechts-/links-*)*invertierbar*, wenn es ein (*Rechts-/Links-*)*Inverses* $b \in G$ von a gibt. Das neutrale Element e ist invertierbar mit Inversem e .

1.2 Lemma. *Sei G ein Monoid mit Verknüpfung \circ und neutralem Element e .*

- (i) *Links- und zugleich rechtsinvertierbare Elemente sind invertierbar und das Inverse ist eindeutig bestimmt.*
- (ii) *Ist $a \in G$ invertierbar mit Inversem $b \in G$, so ist auch b invertierbar und besitzt das Inverse a .*
- (iii) *Sind $a, b \in G$ invertierbar mit Inversen $c, d \in G$, also $a \circ c = c \circ a = e$ und $b \circ d = d \circ b = e$, so ist auch $a \circ b$ invertierbar und besitzt das Inverse $d \circ c$.*

Beweis. (i): Sei $b \in G$ links- und rechtsinvertierbar mit Linksinversem a und Rechtsinversem c . Dann gilt $a = a \circ e = a \circ (b \circ c) = (a \circ b) \circ c = e \circ c = c$. Also ist $a = c$ zugleich Links- und Rechtsinverse, und daraus folgt die Aussage.

(ii): Es gilt $a \circ b = b \circ a = e$ aufgrund der Definition von b . Damit erfüllt a aber auch die Definition eines Inversen von b .

(iii): Es gilt $(a \circ b) \circ (d \circ c) = a \circ (b \circ d) \circ c = a \circ c = e$ und analog $(d \circ c) \circ (a \circ b) = e$, also ist $d \circ c$ das Inverse von $a \circ b$. \square

1.3 Beispiel. Sei $G = \{f \mid f : \mathbb{Z} \rightarrow 2\mathbb{Z}\}$ mit $\circ =$ Komposition von Abbildungen. Dann ist G zusammen mit \circ eine Halbgruppe. Wir wollen ein Beispiel linksneutral, aber nicht rechtsneutralen Elemente finden. Finde also $e, g \in G$ mit $e \circ f = f$ für alle $f \in G$ und $g \circ e \neq g$. Wir definieren

$$e : x \mapsto \begin{cases} x & \text{für } x \text{ gerade,} \\ 2x & \text{sonst,} \end{cases}$$

sowie $g : x \mapsto 2x$. Dann gilt in der Tat $e(f(x)) = f(x)$ für alle $x \in \mathbb{Z}$, da $f(x)$ gerade ist, und $g(e(1)) = g(2) = 4 \neq 2 = g(1)$, also $g \circ e \neq g$. Wir erhalten weitere linksneutrale Elemente, indem wir die Definition von e für $x \neq 1$ und x ungerade unter der Maßgabe $e(x) \in 2\mathbb{Z}$ beliebig abändern. Dies zeigt, daß linksneutrale Elemente im allgemeinen nicht eindeutig bestimmt sind.

1.4 Beispiel. Sei $G = \{f \mid f : \mathbb{Z} \rightarrow \mathbb{Z}\}$ mit $\circ =$ Komposition von Abbildungen. Dann ist G zusammen mit \circ ein Monoid mit neutralem Element id . Wir wollen ein Beispiel linksinvertierbarer, aber nicht rechtsinvertierbarer Elemente finden. Finde also $f, g \in G$ mit $f \circ g = \text{id}$ und $g \circ f \neq \text{id}$, also g injektiv und nicht surjektiv, und f surjektiv und nicht injektiv. Wir können damit zum Beispiel

$$g : x \mapsto 2x \quad \text{und} \quad f : x \mapsto x \operatorname{div} 2$$

wählen. Die Abbildung

$$h : x \mapsto \begin{cases} x \operatorname{div} 2 & \text{für } x \text{ gerade,} \\ 0 & \text{sonst.} \end{cases}$$

ist ebenfalls ein Linksinverses von g , also sind Linksinverse linksinvertierbarer Elemente im allgemeinen nicht eindeutig bestimmt.

Sei G ein Monoid mit Verknüpfung \circ und neutralem Element e . Für ein linksinvertierbares $a \in G$ und $b \in G$ besitzt die Gleichung $a \circ x = b$ höchstens eine Lösung $x \in G$: Durch Multiplikation der Gleichung von links mit einem Linksinversen $c \in G$ von a erhalten wir $x = e \circ x = (c \circ a) \circ x = c \circ (a \circ x) = c \circ b$. Ist c sogar ein Inverses von a , so liefert $x = c \circ b$ auch stets eine Lösung der Gleichung $a \circ x = b$.

Die *Kürzungsregel* ist eine Variante dieser Aussage: Ist $a \in G$ linksinvertierbar und gilt $a \circ x_1 = a \circ x_2$ für $x_1, x_2 \in G$, so folgt $x_1 = x_2$. Ein äquivalente Formulierung der Kürzungsregel ist die folgende: Die Abbildung $G \rightarrow G$, $x \mapsto a \circ x$ ist injektiv. Diese Aussagen gelten analog für rechtsinverse Elemente.

Besitzt G endliche Ordnung, so sind linksinvertierbare (oder rechtsinvertierbare) Elemente bereits invertierbar: Ist $a \in G$ linksinvertierbar, so ist die Abbildung $x \mapsto a \circ x$ nach der Kürzungsregel injektiv und wegen $\#G < \infty$ auch surjektiv. Also gibt es $c \in G$ mit $a \circ c = e$. Die Behauptung folgt damit aus Lemma 1.2, (i). Entsprechend besitzt dann die Gleichung $a \circ x = b$ immer genau eine Lösung.

Wir untersuchen nun kurz, inwieweit neutrale Elemente durch Homomorphismen wieder auf neutrale Elemente, und inverse Elemente wieder auf inverse Elemente abgebildet werden. Seien G, H Monoide mit den neutralen Elementen e_G und e_H . Sei $f : G \rightarrow H$ ein Homomorphismus. Dann gilt nicht notwendigerweise $f(e_G) = e_H$, obwohl man dies vielleicht erwarten würde.

1.5 Beispiel. Als Beispiel für dieses Verhalten betrachten wir $G = (\mathbb{R} \setminus \{0\}, \cdot)$, $H = (\mathbb{R}^{2 \times 2}, \cdot)$ und

$$f : G \rightarrow H, \quad x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}.$$

Man rechnet leicht nach, daß f ein Homomorphismus ist und $f(1) \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ gilt.

1.6 Lemma. Seien G, H Monoide mit den neutralen Elementen e_G und e_H und $f : G \rightarrow H$ ein Homomorphismus.

- (i) Ist $f(e_G)$ invertierbar oder f ein Epimorphismus, so gilt $f(e_G) = e_H$.
- (ii) Es gelte $f(e_G) = e_H$. Ist $a \in G$ invertierbar mit Inversem $b \in G$, so ist $f(a)$ invertierbar mit Inversem $f(b)$.

Beweis. (i): Sei $f(e_G)$ invertierbar. Dann gilt $f(e_G)^2 = f(e_G^2) = f(e_G)$. Verknüpfung beider Seiten der Gleichung mit dem Inversen von $f(e_G)$ liefert $f(e_G) = e_H$.

Sei f ein Epimorphismus und $b \in H$. Dann gibt es $a \in G$ mit $f(a) = b$ und $bf(e_G) = f(a)f(e_G) = f(ae_G) = f(a) = b$ und analog $f(e_G)b = b$. Also ist $f(e_G)$ neutrales Element von H .

(ii): Es gilt $f(a)f(b) = f(ab) = f(e_G) = e_H$ und analog $f(b)f(a) = e_H$. Also ist $f(b)$ das Inverse von $f(a)$. \square

Die obige Notation unter Verwendung des Symbols \circ ist teilweise etwas unständlich. Zur Vereinfachung betrachten wir die Symbole \cdot und $+$ und führen ein paar Konventionen ein.

Verwenden wir das Symbol \cdot anstelle von \circ , so lassen wir \cdot auch häufig aus: Dann bedeutet ab also eigentlich $a \cdot b$. Das neutrale Element bezeichnen wir mit 1 anstelle von e . Ist a invertierbar, so bezeichnen wir das Inverse von a mit a^{-1} . Die Formeln des Lemmas 1.2 sehen dann recht eingängig so aus:

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

Die Kürzungsregel lautet ebenfalls eingängiger: $ax_1 = ax_2 \Rightarrow x_1 = x_2$. Sind $a_i \in G$ für $1 \leq i \leq n$ und $n \in \mathbb{Z}^{\geq 1}$, so definieren wir $\prod_{i=1}^n a_i = a_1 \cdots a_n$. Falls es das neutrale Element 1 gibt, definieren wir das leere Produkt als 1 (Fall $n = 0$). Damit setzen wir $a^n = \prod_{i=1}^n a$ für $n \in \mathbb{Z}^{\geq 0}$. Ist a invertierbar, so definieren wir zusätzlich $a^{-n} = (a^n)^{-1}$. Nach Lemma 1.2, (iii) gilt $(a^n)^{-1} = (a^{-1})^n$.

Das Symbol $+$ verwenden wir nur für kommutative Verknüpfungen. Das neutrale Element bezeichnen wir dann mit 0 anstelle von e . Ist a invertierbar, so bezeichnen wir das Inverse von a mit $-a$. Die Formeln des Lemmas 1.2 sehen dann so aus:

$$-(-a) = a \quad \text{und} \quad -(a+b) = (-a) + (-b).$$

Die Kürzungsregel lautet: $a + x_1 = a + x_2 \Rightarrow x_1 = x_2$. Sind $a_i \in G$ für $1 \leq i \leq n$ und $n \in \mathbb{Z}^{\geq 1}$, so definieren wir $\sum_{i=1}^n a_i = a_1 + \cdots + a_n$. Falls es das neutrale Element 0 gibt, definieren wir die leere Summe als 0 (Fall $n = 0$). Damit setzen wir $na = \sum_{i=1}^n a$ für $n \in \mathbb{Z}^{\geq 0}$. Ist a invertierbar, so definieren wir zusätzlich $(-n)a = -(na)$. Nach Lemma 1.2, (iii) gilt $-(na) = n(-a)$.

Die Abbildungen $(n, a) \mapsto a^n$ und $(n, a) \mapsto na$ liefern Beispiele für Verknüpfungen auf G mit Operatorbereich $\mathbb{Z}^{\geq 1}$.

1.3 Gruppen

1.7 Definition. Eine Gruppe G ist ein Monoid, in welchem jedes Element invertierbar ist.

In diesem Abschnitt und den nachfolgenden Abschnitten schreiben wir die Verknüpfung aller auftretenden Gruppen als \cdot .

Will man (kleine) Gruppen explizit beschreiben, so kann man ihre Gruppentafel, also den Graph der Verknüpfung, angeben. Die Verknüpfung in einer Gruppe wird auch Gruppengesetz genannt.

Eine äquivalente Charakterisierung einer Gruppe mit „minimalen Axiomen“ ist die folgende.

1.8 Satz. Für eine Halbgruppe G sind äquivalent.

- (i) G ist eine Gruppe.
- (ii) G besitzt ein linksneutrales Element e , und für jedes $a \in G$ gibt es ein $b \in G$ mit $ba = e$.

Beweis. (i) \Rightarrow (ii): Ist klar.

(ii) \Rightarrow (i): Sei $a \in G$. Es gibt $b \in G$ und $c \in G$ mit $ba = e$ und $cb = e$. Dann gilt $bab = eb = b$. Multiplikation dieser Gleichung von links mit c liefert $ab = eab = cbab = ceb = e$. Damit gilt weiter $ae = aba = ea = a$. Da a beliebig war, ist e folglich ein neutrales Element von G und a invertierbar. \square

1.9 Beispiel. Beispiele für abelsche Gruppen sind $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ oder die Menge der Vektoren eines Vektorraums zusammen mit der Vektoraddition.

Mengen von Automorphismen zusammen mit der Verknüpfung $\circ =$ Komposition von Abbildungen liefern im allgemeinen nichtabelsche Gruppen: Beispiele sind die Menge der Automorphismen eines Vektorraums beziehungsweise die Menge der invertierbaren Matrizen über einem Körper (zusammen mit der Matrixmultiplikation), oder die Menge der Permutationen $S(X) = \{f : X \rightarrow X \mid f \text{ bijektiv}\}$ für eine Menge X .

Ist H ein Monoid und G die Menge der invertierbaren Elemente von H , so ist G zusammen mit der (eingeschränkten) Verknüpfung von H nach Lemma 1.2 eine Gruppe.

1.10 Definition. Sei G eine Gruppe und $U \subseteq G$. Dann heißt U eine Untergruppe von G , wenn U mit der (eingeschränkten) Verknüpfung von G eine Gruppe bildet. In Zeichen schreiben wir hierfür $U \leq G$.

Speziell besitzen U und G das gleiche neutrale Element und die gleichen Inversen (also das Inverse von $a \in U$ in U ist gleich dem Inversen von a in G). Dies folgt aus Lemma 1.6 unter Verwendung des Inklusionshomomorphismus $U \rightarrow G$. Ist V eine Untergruppe von G und U eine Untergruppe von V , so ist U auch eine Untergruppe von G . Sind U, V Untergruppen von G mit $U \subseteq V$, so ist U auch eine Untergruppe von V .

Für $A \subseteq G$ sei $A^{-1} = \{a^{-1} \mid a \in A\}$. Ist $B \subseteq G$, so gilt $(AB)^{-1} = B^{-1}A^{-1}$. Ist U eine Untergruppe von G , so gilt $U^{-1} = U$, da jedes Element von U in U invertierbar ist, und $UU = U$, unter Beachtung von $1 \in U$ und $U = 1U \subseteq UU \subseteq U$.

Zum Überprüfen der Untergruppeneigenschaft einer Teilmenge $U \subseteq G$ ist folgendes Lemma mitunter hilfreich:

1.11 Lemma. Sei G eine Gruppe und $U \subseteq G$ mit $U \neq \emptyset$. Dann sind äquivalent.

(i) U ist eine Untergruppe von G .

(ii) $UU^{-1} \subseteq U$.

Beweis. (i) \Rightarrow (ii): Ist klar.

(ii) \Rightarrow (i): Mit $a = 1$ gilt $b \in U \Rightarrow b^{-1} \in U$, also enthält U Inverse. Sind $a, b \in U$, so gilt $b^{-1} \in U$ und $ab = a(b^{-1})^{-1} \in U$, also liefert \cdot von G auch eine Verknüpfung auf U . Mit $a = b \in U$ gilt $1 = ab^{-1} \in U$, also enthält U das neutrale Element von G . Damit sind die Eigenschaften einer Untergruppe wie in der Definition nachgewiesen. \square

Sei G eine Gruppe und $M \subseteq G$. Dann definieren wir

$$\langle M \rangle = \left\{ \prod_{i=1}^s a_i^{r_i} \mid s \in \mathbb{Z}^{\geq 0}, a_i \in M, r_i \in \mathbb{Z} \right\},$$

wobei das leere Produkt das neutrale Element 1 von M und $\langle \emptyset \rangle = \{1\}$ sei. Für $M = \{g_1, \dots, g_n\}$ schreiben wir kurz $\langle M \rangle = \langle g_1, \dots, g_n \rangle$.

1.12 Satz. Ist G eine Gruppe und $M \subseteq G$, so ist $\langle M \rangle$ eine Untergruppe von G und es gilt $\langle M \rangle = \cap \{U \mid M \subseteq U \leq G\}$.

Beweis. Da $1 \in \langle M \rangle$ gilt, und $\langle M \rangle$ Produkte und Inverse von Elementen aus $\langle M \rangle$ enthält, ist $\langle M \rangle$ eine Untergruppe von G .

Für Untergruppen U von G ist die Bedingung $M \subseteq U$ äquivalent zu $\langle M \rangle \subseteq U$. Daher folgt $\langle M \rangle \subseteq \cap \{U \mid M \subseteq U \leq G\}$. Da ein U im Schnitt gleich $\langle M \rangle$ ist, folgt \supseteq und damit die Gleichheit. \square

1.13 Definition. Die Untergruppe $\langle M \rangle$ heißt die von M in G erzeugte Untergruppe. Gilt $G = \langle M \rangle$, so heißen die Elemente aus M Erzeuger von G und M ein Erzeugendensystem von G .

Gilt $G = \langle g \rangle$ für ein $g \in G$, so heißt G zyklisch. Die Ordnung eines $g \in G$ ist definiert als $\text{ord}(g) = \#\langle g \rangle$. Der Exponent von G ist $m = \text{lcm} \{ \text{ord}(g) \mid g \in G \}$.

Desweiteren sind zyklische Gruppen offensichtlich auch abelsch.

1.14 Beispiel. Es gilt $M \subseteq \langle M \rangle$, und $M = \langle M \rangle$ genau dann, wenn M eine Untergruppe von G ist. Es gilt $(\mathbb{Z}, +) = \langle 1 \rangle$ und $(\mathbb{Q}, +) = \langle \{1/n \mid n \in \mathbb{Z}^{>0}\} \rangle$. Speziell ist \mathbb{Z} zyklisch, und $(\mathbb{Q}, +)$ nicht endlich erzeugbar.

Die Ordnung eines Elements ist entweder eine positive ganze Zahl oder unendlich. Der Exponent von G ist ebenfalls entweder eine positive ganze Zahl oder unendlich. Es gibt Gruppen, in denen jedes $g \in G$ eine endliche Ordnung besitzt, aber der Exponent unendlich ist (Beispiel ist einfach, kommt aber später, siehe Beispiel 1.35).

1.15 Lemma. Sei G eine Gruppe.

(i) Für die Ordnung von $g \in G$ gilt $\text{ord}(g) = \min\{n \geq 1 \mid g^n = 1\}$.

(ii) Sei $g \in G$ und $s \in \mathbb{Z}$. Dann ist $g^s = 1$ genau dann, wenn $\text{ord}(g) \mid s$ gilt.

(iii) Für den Exponenten m von G gilt $m = \min\{n \geq 1 \mid g^n = 1 \text{ für alle } g \in G\}$.

Beweis. (i): Es gilt $\langle g \rangle = \{1, g, g^{-1}, g^2, g^{-2}, \dots\}$. Nehmen wir zunächst an, daß das Minimum unendlich ist, es also kein $n \geq 1$ mit $g^n = 1$ gibt. Dann sind die g -Potenzen in $\langle g \rangle$ paarweise verschieden: Denn wäre dies nicht der Fall, so gäbe es $a, b \in \mathbb{Z}$ mit $a < b$ und $g^a = g^b$. Dann folgt $g^{b-a} = 1$ und $b - a \geq 1$, im Widerspruch zur Annahme. Also ist $\text{ord}(g)$ endlich.

Wir nehmen nun an, daß das Minimum endlich ist und bezeichnen es mit s . Es gilt also $g^s = 1$. Dann folgt $\langle g \rangle = \{1, g, \dots, g^{s-1}\}$. Denn für $a \in \mathbb{Z}$ gibt es $\lambda \in \mathbb{Z}$ mit $0 \leq a + \lambda s \leq s - 1$ und $g^a = g^{\lambda s} (g^s)^\lambda = g^{a + \lambda s}$. Die Elemente $1, g, \dots, g^{s-1}$ sind aber auch paarweise verschieden, wie man wegen der Minimalität von s wie oben sieht. Es folgt $\text{ord}(g) = s$.

(ii): Es gelte $\text{ord}(g)|s$. Für $\text{ord}(g) = \infty$ folgt $s = 0$ und es gilt $g^s = 1$. Für $\text{ord}(g) < \infty$ gilt $g^s = (g^{\text{ord}(g)})^{s/\text{ord}(g)} = 1$ nach (i).

Es gelte nun $g^s = 1$. Für $s = 0$ ergibt sich in jedem Fall $\text{ord}(g)|s$. Wir nehmen daher $s \neq 0$ an, es folgt $\text{ord}(g) < \infty$. Division mit Rest liefert $s = q \text{ord}(g) + r$ mit $0 \leq r < \text{ord}(g)$ und $g^s = g^{q \text{ord}(g) + r} = (g^{\text{ord}(g)})^q g^r = g^r = 1$. Da $\text{ord}(g)$ minimal ≥ 1 mit dieser Eigenschaft ist, folgt $r = 0$.

(iii): Sei s das Minimum. Nach der Definition des Exponenten und (i) ist m unendlich oder es gilt $g^m = 1$ für alle $g \in G$. Nach der Definition von s folgt $m \geq s$. Ist s unendlich, so ist (iii) gültig. Ist s endlich, so folgt $\text{ord}(g)|s$ für alle $g \in G$ wegen (ii), also $m|s$ und damit $m = s$. \square

1.4 Nebenklassen

Sei G eine Gruppe und U eine Untergruppe von G . Für $a, b \in G$ definieren wir eine Relation \sim durch $a \sim b :\Leftrightarrow ab^{-1} \in U$. Wir erinnern an die Definition von AB , aB und Ab aus dem ersten Absatz von Abschnitt 1.2.

Für $A, B \subseteq G$ und $c \in G$ gilt $A \subseteq B \Leftrightarrow Ac \subseteq Bc \Leftrightarrow cA \subseteq cB$, wegen der Invertierbarkeit von c .

1.16 Lemma. (i) Die Relation \sim ist eine Äquivalenzrelation.

(ii) Für $a, b \in G$ gelten die Äquivalenzen:

$$a \sim b \Leftrightarrow ab^{-1} \in U \Leftrightarrow a \in Ub \Leftrightarrow Ua \subseteq Ub \Leftrightarrow Ua = Ub.$$

(iii) Die Äquivalenzklassen von \sim sind von der Form Ub für $b \in G$ und haben alle die gleiche Kardinalität $\#U$.

(iv) Wir erhalten eine Partition von G in der Form $G = \dot{\cup} \{Ub \mid b \in G\}$.

Beweis. (i): Seien $a, b, c \in G$ beliebig. Es gilt $a \sim a$, denn $aa^{-1} = 1 \in U$. Für $a \sim b$ gilt auch $b \sim a$, denn $ab^{-1} \in U$ impliziert $ba^{-1} = (ab^{-1})^{-1} \in U$ nach Lemma 1.2. Für $a \sim b$ und $b \sim c$ gilt auch $a \sim c$, denn $ab^{-1} \in U$ und $bc^{-1} \in U$ implizieren $ac^{-1} = (ab^{-1})(bc^{-1}) \in U$.

(ii): Die erste Äquivalenz gilt per Definition. Die zweite Äquivalenz folgt durch Multiplikation von rechts mit b beziehungsweise mit b^{-1} . Die dritte Äquivalenz folgt in der Richtung \Rightarrow durch Multiplikation von links mit U unter Beachtung von $U(Ub) = (UU)b = Ub$ wegen der Assoziativität und $1 \in U$, und in der Richtung \Leftarrow wegen $a \in Ua$ wegen $1 \in U$. Die vierte Äquivalenz folgt aus der Symmetrie von \sim durch Vertauschen von a und b .

(iii): Wegen (ii) sind die Äquivalenzklassen in der Tat von der Form Ub . Die Abbildung $U \rightarrow Ub, x \mapsto xb$ ist bijektiv, da b invertierbar ist. Also gilt $\#U = \#Ub$.

(iv): Gilt allgemein, jede Äquivalenzrelation liefert eine Partition der unterliegenden Menge (und umgekehrt). \square

1.17 Definition. Die Äquivalenzklassen Ub für $b \in G$ heißen Rechtsnebenklassen von U . Eine Teilmenge $R \subseteq G$ heißt Rechtsnebenklassenrepräsentantensystem von U in G , wenn R aus jeder Rechtsnebenklasse genau ein Element enthält.

Analog erhalten wir durch $a \sim b :\Leftrightarrow a^{-1}b \in U$ Linksnebenklassen aU und Linksnebenklassenrepräsentantensysteme. Lemma 1.16 und Definition 1.17 gelten entsprechend für Linksnebenklassen. Für abelsche Gruppen besteht zwischen Links- und Rechtsnebenklassen kein Unterschied, es gilt $aU = Ua$.

1.18 Lemma. Die Menge der Rechtsnebenklassen und die Menge der Linksnebenklassen sind gleichmächtig.

Beweis. Betrachte die Abbildung $\phi : Ua \mapsto a^{-1}U$. Man sieht mit Lemma 1.2 leicht, daß ϕ wohldefiniert und surjektiv ist. Gilt $a^{-1}U = b^{-1}U$, so folgt $U = ab^{-1}U$, also $ab^{-1} \in U$ und $Ua = Ub$ nach Lemma 1.16, (ii). Daher ist ϕ auch injektiv. \square

1.19 Definition. Der Index von U in G ist die Mächtigkeit der Nebenklassenmengen,

$$(G : U) = \#\{Ub \mid b \in G\} = \#\{aU \mid a \in G\}.$$

Gilt $(G : U) = 1$ für eine Untergruppe U von G , so folgt $G = U$. Bezeichnen wir mit 1 auch die Einheitsgruppe $\{1\}$, so gilt $(G : 1) = \#G$.

Für den folgenden Satz erinnern wir an die Konvention (1.1).

1.20 Satz (Lagrange). Seien G eine Gruppe und U, V Untergruppen von G mit $U \subseteq V$. Dann gilt

$$(G : V)(V : U) = (G : U).$$

Beweis. Wir beweisen die Aussage zuerst für den Fall $U = 1$, da es hier etwas anschaulicher ist. Nach Lemma 1.16, (iv) gilt $G = \dot{\cup}\{Vb \mid b \in G\}$. Dies ist eine disjunkte Vereinigung von $(G : V)$ Mengen, welche nach Lemma 1.16, (iii) gleichmächtig von der Kardinalität $\#V = (V : 1)$ sind. Dies zeigt die Aussage des Satzes für den Fall $U = 1$.

Für den allgemeinen Fall seien $R_{G,V}$ ein Linksnebenklassensystem von V in G und $R_{V,U}$ ein Linksnebenklassensystem von U in V . Dann gilt $G = \dot{\cup}\{xV \mid x \in R_{G,V}\}$ und $V = \dot{\cup}\{yU \mid y \in R_{V,U}\}$. Außerdem gilt $xV = \dot{\cup}\{xyU \mid y \in R_{V,U}\}$

für alle $x \in G$, da Multiplikation mit x von links injektiv ist. Daher folgt $G = \dot{\cup} \{xyU \mid x \in R_{G,V}, y \in R_{V,U}\}$, wobei die xyU für verschiedene $x \in R_{G,V}$ oder $y \in R_{V,U}$ paarweise disjunkt und insbesondere verschieden sind. Dies zeigt, daß $R_{G,U} := R_{G,V}R_{V,U}$ ein Linksnebenklassenrepräsentantensystem von U in G ist und daß $\#R_{G,U} = \#R_{G,V}\#R_{V,U}$ gilt. Wegen $\#R_{G,U} = (G : U)$, $\#R_{G,V} = (G : V)$ und $\#R_{V,U} = (V : U)$ ergibt sich die Aussage des Satzes. \square

1.21 Korollar. Sei G eine endliche Gruppe. Für jedes $a \in G$ gilt $\text{ord}(a) \mid \#G$ und $a^{\#G} = 1$. Der Exponent von G ist ein Teiler von $\#G$.

Beweis. Per Definition gilt $\text{ord}(a) = \#\langle a \rangle$. Nach Satz 1.20 angewendet mit $V = \langle a \rangle$ und $U = 1$ folgt $\#\langle a \rangle \mid \#G$.

Nach Lemma 1.15, (i) gilt $a^{\text{ord}(a)} = 1$. Dann ist $\#G/\text{ord}(a)$ eine ganze Zahl mit $\#G = \text{ord}(a)(\#G/\text{ord}(a))$ und es gilt $a^{\#G} = (a^{\text{ord}(a)})^{\#G/\text{ord}(a)} = 1^{\#G/\text{ord}(a)} = 1$.

Die Aussage über den Exponenten folgt direkt aus der Definition des Exponenten, denn das kleinste gemeinsame Vielfache von Teilern einer Zahl ist wieder ein Teiler der Zahl. \square

Die erste Aussage von Korollar 1.21 heißt kleiner Satz von Fermat.

1.22 Beispiel. Sei $m \in \mathbb{Z}^{\geq 0}$. Wir betrachten die abelsche Gruppe $(\mathbb{Z}, +)$ und ihre Untergruppe $m\mathbb{Z}$. Die Menge der Nebenklassen von $m\mathbb{Z}$ in \mathbb{Z} wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet. Es gilt $a \sim b \Leftrightarrow a - b \in m\mathbb{Z} \Leftrightarrow a \equiv b \pmod{m}$ für $a, b \in \mathbb{Z}$.

Ein Repräsentantensystem wird durch $R = \{0, \dots, m-1\}$ gegeben, ein anderes durch $\{\lfloor -m/2 \rfloor + 1, \dots, \lfloor m/2 \rfloor\}$. Es gilt $\#(\mathbb{Z}/m\mathbb{Z}) = m$ für $m \neq 0$ und $\#(\mathbb{Z}/m\mathbb{Z}) = \infty$ für $m = 0$.

Wir können $\mathbb{Z}/m\mathbb{Z}$ sogar zu einer abelschen Gruppe machen, indem wir die Addition zweier Nebenklassen vertreterweise definieren, $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) := (a + b) + m\mathbb{Z}$. Das neutrale Element ist $m\mathbb{Z}$, und das zu $a + m\mathbb{Z}$ inverse Element ist $(-a) + m\mathbb{Z}$. Diese Addition entspricht der Addition modulo m auf dem Vertretersystem $R = \{0, \dots, m-1\}$.

Wegen $\mathbb{Z} = \langle 1 \rangle$ gilt auch $\mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z} \rangle$, also ist $(\mathbb{Z}/m\mathbb{Z}, +)$ zyklisch.

1.5 Normalteiler

1.23 Definition. Sei G eine Gruppe und U eine Untergruppe. Dann heißt U Normalteiler von G und U normal in G , wenn $xU = Ux$ für alle $x \in G$ gilt. In Zeichen schreiben wir hierfür $U \trianglelefteq G$.

Die Bedeutung von Normalteilern liegt darin, daß die Links- und Rechtsnebenklassen gleich sind und damit ein Gruppengesetz auf den *Nebenklassen* durch

vertreterweise Anwendung des Gruppengesetzes von G definiert werden kann, ähnlich wie im Beispiel 1.22. Diese Konstruktion wird im Abschnitt 1.7 beschrieben.

Das folgende Lemma enthält zunächst ein paar einfache Aussagen über Normalteiler.

1.24 Lemma. *Sei G eine Gruppe.*

- (i) *Eine Untergruppe U von G ist genau dann ein Normalteiler, wenn $xUx^{-1} \subseteq U$ für alle $x \in G$ gilt.*
- (ii) *Die Untergruppen $\{1\}$ und G sind Normalteiler von G .*
- (iii) *Ist G abelsch, so ist jede Untergruppe ein Normalteiler.*
- (iv) *Ist I eine Indexmenge und N_i ein Normalteiler von G für alle $i \in I$, so ist $\bigcap_{i \in I} N_i$ ein Normalteiler von G .*
- (v) *Ist N ein Normalteiler von G und U eine Untergruppe von G , so ist $UN = NU$ eine Untergruppe von G . Ist U zusätzlich Normalteiler von G , so ist UN ebenfalls Normalteiler von G .*
- (vi) *Ist U eine Untergruppe von G mit $(G : U) = 2$, so ist U ein Normalteiler von G .*

Beweis. (i): Multiplikation von rechts mit x^{-1} beziehungsweise mit x ergibt die Äquivalenz der Bedingungen $xU = Ux$ für alle $x \in G$ und $xUx^{-1} = U$ für alle $x \in G$. Sei $x \in G$ mit $xUx^{-1} \subseteq U$. Für $y = x^{-1}$ gilt dann $y^{-1}Uy \subseteq U$, also $U \subseteq yUy^{-1}$. Da y mit x alle Gruppenelemente annimmt, ergibt sich aus $xUx^{-1} \subseteq U$ für alle $x \in G$ auch $yUy^{-1} \supseteq U$ für alle $y \in G$, also $xUx^{-1} = U$ für alle $x \in G$.

(ii): Für $\{1\}$ gilt $x1x^{-1} = xx^{-1}1 = 1$, also $x\{1\}x^{-1} \subseteq \{1\}$ für alle $x \in G$. Für G gilt $xGx^{-1} \in G$, also $xGx^{-1} \subseteq G$ für alle $x \in G$.

(iii): Ist U eine Untergruppe von G und $g \in U$, so gilt $xgx^{-1} = xx^{-1}g = g \in U$ für alle $x \in G$, also $xUx^{-1} \subseteq U$ für alle $x \in G$.

(iv): Sei $g \in \bigcap_i N_i$. Dann gilt $g \in N_i$ für alle $i \in I$ und $xgx^{-1} \in N_i$ für alle $i \in I$ und für alle $x \in G$. Also folgt $xgx^{-1} \in \bigcap_i N_i$ für alle $x \in G$. Da g beliebig war, folgt $x(\bigcap_i N_i)x^{-1} \subseteq \bigcap_i N_i$ für alle $x \in G$.

(v): Sei $nu \in NU$ mit $n \in N$ und $u \in U$. Wegen $Nu = uN$ gibt es ein $n' \in N$ mit $nu = un' \in UN$. Also folgt $NU \subseteq UN$, und analog $UN \subseteq NU$, zusammen $UN = NU$. Wegen $1 \in U$ und $1 \in N$ gilt $1 \in UN$. Weiter ergibt sich $UN(UN)^{-1} = UNN^{-1}U^{-1} = UNNU = UNU = UUN = UN$. Nach Lemma 1.11 ist UN eine Untergruppe von G .

(vi): Es gilt $G = U \dot{\cup} xU = U \dot{\cup} Ux$ für jedes $x \in G \setminus U$. Also folgt $xU = Ux$. \square

Ist V ein Normalteiler von G und U ein Normalteiler von V , so ist U zwar eine Untergruppe von G , im allgemeinen jedoch kein Normalteiler von G .

1.25 Beispiel. Sei $G = \text{GL}_2(\mathbb{R})$ und $U = \langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \rangle$. Sei $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so daß $x^2 = 1$ und $x^{-1} = x$ ist. Dann gilt $x \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} x^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \notin U$. Folglich ist U eine Untergruppe, aber kein Normalteiler von G .

1.26 Definition. Eine Gruppe G heißt einfach, wenn $\{1\}$ und G die einzigen Normalteiler von G sind.

1.6 Homomorphismen

Ein Homomorphismus der Gruppen G und H ist ein Homomorphismus der unterliegenden Halbgruppen, wie in Abschnitt 1.2 definiert. Zusätzlich zu den Bezeichnungen von Abschnitt 1.2 führen wir folgende Notation ein.

Die Menge der Homomorphismen von G nach H wird mit $\text{Hom}(G, H)$ bezeichnet. Die Menge der Endomorphismen von G wird mit $\text{End}(G)$ bezeichnet. Die Menge der Automorphismen von G wird mit $\text{Aut}(G)$ bezeichnet.

Die Menge $\text{End}(G)$ zusammen mit der Hintereinanderausführung von Abbildungen ist ein Monoid. Die Untergruppe der invertierbaren Elemente von $\text{End}(G)$ ist gerade $\text{Aut}(G)$.

Sei $\phi \in \text{Hom}(G, H)$. Das *Bild* von ϕ ist $\phi(G) = \{\phi(x) \mid x \in G\}$ und wird auch mit $\text{im}(\phi)$ bezeichnet. Der *Kern* von ϕ ist $\phi^{-1}(\{1\}) = \{x \in G \mid \phi(x) = 1\}$ und wird mit $\ker(\phi)$ bezeichnet.

1.27 Lemma. Sei $\phi \in \text{Hom}(G, H)$.

- (i) Es gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$ für alle $a \in G$.
- (ii) Für eine Untergruppe V von H ist $\phi^{-1}(V)$ eine Untergruppe von G . Ist V ein Normalteiler von H , so ist $\phi^{-1}(V)$ ein Normalteiler von G .
- (iii) Für eine Untergruppe U von G ist $\phi(U)$ eine Untergruppe von H . Ist ϕ surjektiv und U ein Normalteiler von G , so ist $\phi(U)$ ein Normalteiler von H .
- (iv) Der Kern $\ker(\phi)$ ist ein Normalteiler von G .
- (v) ϕ ist genau dann ein Monomorphismus, wenn $\ker(\phi) = \{1\}$ gilt.
- (vi) ϕ ist auf den Nebenklassen von $\ker(\phi)$ in G konstant.
- (vii) Ist G einfach, so ist ϕ konstant (gleich 1) oder injektiv.

Beweis. (i): Folgt direkt aus Lemma 1.6.

(ii): Nach (i) gilt $1 \in \phi^{-1}(V)$. Für $a, b \in \phi^{-1}(V)$ folgt $b^{-1} \in \phi^{-1}(V^{-1}) = \phi^{-1}(V)$ und $ab^{-1} \in \phi^{-1}(V)\phi^{-1}(V) \subseteq \phi^{-1}(VV) = \phi^{-1}(V)$. Also ist $\phi^{-1}(V)$ nach Lemma 1.11 eine Untergruppe von G . Sei V ein Normalteiler und $a \in \phi^{-1}(V)$. Dann gilt $\phi(xax^{-1}) = \phi(x)\phi(a)\phi(x)^{-1} \in V$ für alle $x \in G$. Also folgt $xax^{-1} \in \phi^{-1}(V)$ und $x\phi^{-1}(V)x^{-1} \subseteq \phi^{-1}(V)$ für alle $x \in G$.

(iii): Es gilt $1 \in \phi(U)$. Für $a, b \in \phi(U)$ folgt $b^{-1} \in \phi(U^{-1}) = \phi(U)$ und $ab^{-1} \in \phi(U)\phi(U) \subseteq \phi(UU) = \phi(U)$. Also ist $\phi(U)$ eine Untergruppe von H . Sei U ein Normalteiler und ϕ surjektiv. Sei $b \in \phi(U)$ und $y \in H$. Dann gibt es $a \in U$ und $x \in G$ mit $yby^{-1} = \phi(x)\phi(a)\phi(x)^{-1} = \phi(xax^{-1}) \in \phi(U)$ wegen $xax^{-1} \in U$. Es folgt $y\phi(U)y^{-1} \subseteq \phi(U)$ für alle $y \in H$.

(iv): Folgt aus (ii) und Lemma 1.24, (ii).

(v): Seien $a, b \in G$. Dann gilt $\phi(a) = \phi(b) \Leftrightarrow \phi(ab^{-1}) = 1 \Leftrightarrow ab^{-1} \in \ker(\phi)$. Für $\ker(\phi) = 1$ folgt aus $\phi(a) = \phi(b)$ damit $a = b$. Ist umgekehrt ϕ injektiv, so folgt aus $a \in \ker(\phi)$ beziehungsweise $\phi(a) = 1$ wegen $\phi(1) = 1$ bereits $a = 1$.

(vi): Für $a \in G$ und $n \in \ker(\phi)$ gilt $\phi(an) = \phi(a) = \phi(na)$. Also nimmt ϕ für alle Elemente der Nebenklasse $a\ker(\phi) = \ker(\phi)a$ den Wert $\phi(a)$ an.

(vii): Folgt aus (iv) und der Definition von einfach. \square

Für Monoide gilt die Aussage (i) von Lemma 1.27 im allgemeinen nicht mehr.

1.28 Lemma. Sei $\phi : G \rightarrow H$ ein Epimorphismus der Gruppen G und H . Für eine Untergruppe U von G ist $\phi(U)$ eine Untergruppe von H . In dieser Weise liefert ϕ eine inklusionserhaltende Bijektion der Menge der Untergruppen U von G mit $\ker(\phi) \subseteq U$ auf die Menge der Untergruppen von H . Für eine Untergruppe U von G mit $\ker(\phi) \subseteq U$ gilt dabei:

$$(i) \quad (G : U) = (H : \phi(U)).$$

(ii) U ist genau dann ein Normalteiler von G , wenn $\phi(U)$ ein Normalteiler von H ist.

Beweis. Nach Lemma 1.27, (iii) ist $\phi(U)$ eine Untergruppe von H . Ebenfalls klar ist, daß ϕ inklusionserhaltend ist. Für eine beliebige Untergruppe U von G gilt $\phi^{-1}(\phi(U)) = U\ker(\phi)$. Für $\ker(\phi) \subseteq U$ folgt $U\ker(\phi) = U$ und $\phi^{-1}(\phi(U)) = U$. Die Surjektivität von ϕ liefert $\phi(\phi^{-1}(V)) = V$ für jede Untergruppe V von H . Also liefert ϕ eine Bijektion der besagten Untergruppen.

Zum Beweis von (i) beachten wir die folgende Äquivalenz: Für $a, b \in G$ gilt $ab^{-1} \in U \Leftrightarrow \phi(a)\phi(b)^{-1} \in \phi(U)$. Die Richtung \Rightarrow ist klar. Gilt $\phi(a)\phi(b)^{-1} \in \phi(U)$, so folgt $\phi(ab^{-1}) \in \phi(U)$ und damit $ab^{-1} \in \phi^{-1}(\phi(U)) = U$. Weil ϕ surjektiv ist, überführt ϕ mit dieser Äquivalenz die Linksnebenklassenzerlegung von G

bezüglich U in die Linksnebenklassenzerlegung von H bezüglich $\phi(U)$ (analog für Rechtsnebenklassen). Es folgt $(G : U) = (H : \phi(U))$.

Die Aussage (ii) folgt aus Lemma 1.27, (ii) und (iii). \square

Die Aussage von Lemmas 1.28 kann man sich sehr gut anhand einer graphischen Darstellung des Untergruppengitters der U mit $\ker(\phi) \leq U \leq G$ und der $V = \phi(U)$ mit $\{1\} \leq V \leq H$ veranschaulichen beziehungsweise merken.

1.7 Faktorgruppen

Sei G eine Gruppe und N ein Normalteiler von G . Sei G/N die Menge $\{gN \mid g \in G\}$ der Nebenklassen von N in G . Wir definieren eine Verknüpfung \cdot auf G/N durch $gN \cdot hN := (gh)N$.

1.29 Satz. *Die Menge G/N zusammen mit \cdot ist eine Gruppe. Die Abbildung $g \mapsto gN$ definiert einen Epimorphismus $\pi : G \rightarrow G/N$ mit $\ker(\pi) = N$.*

Beweis. Zunächst ist \cdot wohldefiniert: Seien $g, h, \tilde{g}, \tilde{h} \in G$ mit $gN = \tilde{g}N$ und $hN = \tilde{h}N$. Dann gibt es $n_1, n_2 \in N$ mit $\tilde{g} = gn_1$ und $\tilde{h} = hn_2$. Wegen der Normalteilereigenschaft von N gibt es $\tilde{n}_1 \in N$ mit $n_1h = h\tilde{n}_1$. Damit gilt

$$\tilde{g}N \cdot \tilde{h}N = \tilde{g}\tilde{h}N = gn_1hn_2N = gh\tilde{n}_1n_2N = ghN = gN \cdot hN.$$

Die Assoziativität, Existenz des neutralen Elements (hier $1_{G/N} = N$) und der Inversen (hier $(gN)^{-1} = g^{-1}N$) folgt direkt aus den entsprechenden Eigenschaften von G . Die Homomorphieeigenschaft gilt per Definition von \cdot und die Surjektivität ist klar. Weiter gilt $\pi(g) = N \Leftrightarrow gN = N \Leftrightarrow g \in N$, also $\ker(\pi) = N$. \square

1.30 Definition. Die Gruppe G/N heißt die Faktorgruppe von G nach dem Normalteiler N . Der Epimorphismus $\pi : G \rightarrow G/N$ heißt kanonischer Epimorphismus.

Eine alternative Form der Definition von \cdot ist $gN \cdot hN := gNhN$, denn es gilt $gNhN = ghN$ aufgrund von $Nh = hN$.

Ist \sim eine Äquivalenzrelation auf G , so können die Klassen in G/\sim genau dann durch vertreterweise Multiplikation zu einer Gruppe gemacht werden, wenn \sim mit der Multiplikation in G verträglich ist, d.h. wenn für alle $a, b, c, d \in G$ die Implikation $(a \sim b \text{ und } c \sim d) \Rightarrow ac \sim bd$ gilt. Diese Äquivalenzrelationen \sim entsprechen aber genau den durch Normalteiler erhaltenen Äquivalenzrelationen.

Aus Lemma 1.27, (iv) und Satz 1.29 erhalten wir, daß Normalteiler und Kerne von Homomorphismen das gleiche sind.

1.31 Satz (Homomorphiesatz). *Sei*

$$\phi : G \rightarrow H$$

ein Homomorphismus der Gruppen G und H und N ein Normalteiler von G mit $N \subseteq \ker(\phi)$. Sei

$$\pi : G \rightarrow G/N$$

der kanonische Epimorphismus. Dann gibt es genau einen Homomorphismus

$$\psi : G/N \rightarrow H$$

mit $\psi \circ \pi = \phi$. Ferner gilt $\psi(G/N) = \phi(G)$ und $\ker(\psi) = \ker(\phi)/N$.

Beweis. Wenn der Satz stimmen soll, muß notwendigerweise $\psi(gN) = \phi(g)$ gelten. Also definieren wir $\psi : G/N \rightarrow H$ durch $gN \mapsto \phi(g)$. Wegen Lemma 1.27, (vi) ist ψ wohldefiniert und erfüllt per Definition $\psi \circ \pi = \phi$. Da π surjektiv ist, kann es nur eine Abbildung ψ mit $\psi \circ \pi = \phi$ geben (Kürzungsregel von rechts), und da π und ϕ Homomorphismen sind, muß auch ψ ein Homomorphismus sein: Sind $x, y \in G/N$, so gibt es $a, b \in G$ mit $\pi(a) = x$ und $\pi(b) = y$. Dann gilt

$$\begin{aligned} \psi(xy) &= \psi(\pi(a)\pi(b)) = \psi(\pi(ab)) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \psi(\pi(a))\psi(\pi(b)) = \psi(x)\psi(y). \end{aligned}$$

Die Aussage $\psi(G/N) = \phi(G)$ folgt aus $\psi \circ \pi = \phi$. Schließlich gilt $\ker(\psi) = \{gN \mid \phi(g) = 1\} = \{gN \mid g \in \ker(\phi)\} = \ker(\phi)/N$. \square

1.32 Korollar. *Sei $\phi : G \rightarrow H$ ein Homomorphismus der Gruppen G und H . Dann gilt*

$$G/\ker(\phi) \cong \phi(G)$$

unter $g\ker(\phi) \mapsto \phi(g)$.

Beweis. Wähle $N = \ker(\phi)$ in Satz 1.31. Dann $\ker(\psi) = N/N = \{N\}$ und $\text{im}(\psi) = \phi(G)$. Also $G/N \cong \phi(G)$ unter ψ . \square

Korollar 1.32 zeigt, daß die Betrachtung beliebiger Epimorphismen $G \rightarrow H$ und die Betrachtung kanonischer Epimorphismen $G \rightarrow G/N$ bis auf Isomorphie das gleiche ist.

1.33 Satz (Erster Isomorphiesatz). *Sei G eine Gruppe, U eine Untergruppe von G und N ein Normalteiler von G . Dann gilt*

$$NU/N \cong U/(N \cap U).$$

Speziell ist NU eine Untergruppe von G und $N \cap U$ ein Normalteiler von U .

Beweis. Nach Lemma 1.24, (v) ist NU eine Untergruppe von G . Wegen $N \subseteq NU$ ist N auch ein Normalteiler von NU . Betrachte den Homomorphismus $\phi : U \rightarrow NU/N, u \mapsto Nu$, der durch Einschränkung von $\pi : G \rightarrow G/N$ auf U erhalten wird. Die Surjektivität von ϕ ist klar. Für den Kern gilt $\ker(\phi) = \ker(\pi) \cap U = N \cap U$. Daher ist $N \cap U$ ein Normalteiler von U und Korollar 1.32 liefert $U/(N \cap U) \cong NU/N$. \square

1.34 Satz (Zweiter Isomorphiesatz). *Sei G eine Gruppe und U, V Normalteiler von G mit $U \subseteq V$. Dann ist V/U ein Normalteiler von G/U und es gilt*

$$(G/U)/(V/U) \cong G/V.$$

Beweis. Wir wenden Satz 1.31 auf $\phi : G \rightarrow G/V$ und $\pi : G \rightarrow G/U$ an und erhalten den Epimorphismus $\psi : G/U \rightarrow G/V, gU \mapsto gV$ mit $\ker(\psi) = \ker(\phi)/U = V/U$. Also ist V/U ein Normalteiler von G/U und Korollar 1.32 liefert die gewünschte Isomorphieaussage. \square

1.35 Beispiel. Wir betrachten $(\mathbb{Z}, +)$ beziehungsweise Untergruppen und Faktorgruppen. Seien $n, m \in \mathbb{Z}^{\geq 1}$. Zunächst stimmt die Konstruktion von $(\mathbb{Z}/n\mathbb{Z}, +)$ aus Beispiel 1.22 mit der Konstruktion der Faktorgruppe von $(\mathbb{Z}, +)$ und ihrer Untergruppe $(n\mathbb{Z}, +)$ überein.

Sei $[m]$ die Multiplikation mit m in $(\mathbb{Z}, +)$. Dies liefert einen Isomorphismus $\mathbb{Z} \rightarrow m\mathbb{Z}$. Sei $\pi : m\mathbb{Z} \rightarrow m\mathbb{Z}/nm\mathbb{Z}$ der kanonische Epimorphismus. Dann ist $\pi \circ [m]$ ein Epimorphismus mit $\ker(\pi \circ [m]) = n\mathbb{Z}$. Nach Satz 1.31 folgt $\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/nm\mathbb{Z}$. Nach Satz 1.34 gilt $(\mathbb{Z}/nm\mathbb{Z})/(n\mathbb{Z}/nm\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

Wir betrachten als weiteres Beispiel die Gruppe $(\mathbb{Q}, +)$, ihre Untergruppe \mathbb{Z} und die Faktorgruppe \mathbb{Q}/\mathbb{Z} . Jedes Element aus \mathbb{Q}/\mathbb{Z} hat endliche Ordnung, und jede Zahl aus $\mathbb{Z}^{\geq 1}$ wird als Ordnung angenommen. Daher ist der Exponent von \mathbb{Q}/\mathbb{Z} unendlich.

Seien $\phi_i : G_i \rightarrow G_{i+1}$ Homomorphismen der Gruppen G_i und G_{i+1} für $n \leq i \leq m$ und $n, m \in \mathbb{Z}$. Man nennt dies eine Sequenz von Gruppenhomomorphismen. Die Sequenz heißt exakt bei i mit $n+1 \leq i \leq m$, wenn $\phi_{i-1}(G_{i-1}) = \ker(\phi_i)$ gilt. Die Sequenz heißt exakt, wenn sie bei allen i exakt ist.

Ist $\pi : G \rightarrow G/N$ der kanonische Epimorphismus und $i : N \rightarrow G$ der Inklusionsmonomorphismus, so ist die Sequenz $1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \rightarrow 1$ exakt. Die äußeren Abbildungen können hierbei nur auf eine Weise definiert werden und sind daher klar. Ist allgemeiner eine exakte Sequenz $1 \rightarrow M \xrightarrow{j} G \xrightarrow{\phi} H \rightarrow 1$ gegeben, so gilt $M \cong \ker(\phi)$ und $H \cong G/\ker(\phi)$ nach Korollar 1.32.

Solche Sequenzen kommen in vielen Bereichen der Algebra, insbesondere in der homologischen Algebra, vor. Man betrachtet dort natürlich kompliziertere (als die genannten) Sequenzen und Diagramme von Homomorphismen.

1.8 Zyklische Gruppen

Zyklische Gruppen sind die einfachsten Gruppen. Wir wenden jetzt die bisher behandelte Theorie auf sie an.

1.36 Satz. *Eine Gruppe G von Primzahlordnung ist zyklisch.*

Beweis. Sei $g \in G$ mit $g \neq 1$. Dann ist $\text{ord}(g) > 1$ und nach Korollar 1.21 ein Teiler von $\#G$. Also folgt $\text{ord}(g) = \#G$ und daher $G = \langle g \rangle$. \square

1.37 Lemma. *Sei G eine Gruppe.*

(i) *Sei $g \in G$ und $n = \text{ord}(g)$. Dann gilt*

$$\text{ord}(g^k) = \begin{cases} n/\text{gcd}(n, k) & \text{für } n < \infty, \\ \infty & \text{sonst.} \end{cases}$$

(ii) *Sei G zyklisch mit $G = \langle g \rangle$. Dann gilt*

$$G = \langle g^k \rangle \Leftrightarrow \begin{cases} \text{gcd}(\#G, k) = 1 & \text{für } \#G < \infty, \\ k = \pm 1 & \text{sonst.} \end{cases}$$

Beweis. (i): Für $n = \infty$ ist $\text{ord}(g^k) = \infty$ nach Lemma 1.15, (i) klar. Für $n < \infty$ ist $\text{ord}(g^k)$ nach Lemma 1.15, (ii) gleich der kleinsten ganzen Zahl $m > 0$ mit $mk \equiv 0 \pmod{n}$. Es gilt $m = n/\text{gcd}(n, k)$.

(ii): Gelte $\#G < \infty$. Dann ist $G = \langle g^k \rangle$ genau dann, wenn $\text{ord}(g^k) = \#G$ ist, und dies ist nach (i) genau dann der Fall, wenn $\text{gcd}(\#G, k) = 1$ ist.

Gelte $\#G = \infty$. Die Implikation \Leftarrow ist klar. Für \Rightarrow gibt es nach Annahme ein $n \in \mathbb{Z}$ mit $g = (g^k)^n$. Dann gilt $g^{kn-1} = 1$, also $kn = 1$ wegen $\text{ord}(g) = \infty$. Es folgt $k = \pm 1$. \square

1.38 Definition. Für $n \in \mathbb{Z}^{\geq 1}$ ist die Eulersche Phi-Funktion definiert als

$$\phi(n) = \#\{m \mid 1 \leq m \leq n, \text{gcd}(m, n) = 1\}.$$

Nach Lemma 1.37, (ii) ist $\phi(n)$ gleich der Anzahl der Erzeuger einer endlichen zyklischen Gruppe der Ordnung n . Für eine Primzahl p gilt $\phi(p) = p-1$. In diesem Fall ist jedes Element $\neq 1$ ein Erzeuger, wie auch im Beweis von Theorem 1.36 gesehen. Eine unendliche zyklische Gruppe hat nach Lemma 1.37, (ii) dagegen genau zwei Erzeuger.

1.39 Lemma. *Die Untergruppen von $(\mathbb{Z}, +)$ sind genau von der Form $d\mathbb{Z}$ für ein $d \in \mathbb{Z}$, wobei d bis auf das Vorzeichen eindeutig bestimmt ist.*

Beweis. Es ist klar, daß $d\mathbb{Z}$ eine Untergruppe von \mathbb{Z} ist. Sei umgekehrt U eine Untergruppe von \mathbb{Z} und $d = (\mathbb{Z} : U)$. Mit \mathbb{Z} ist \mathbb{Z}/U ebenfalls zyklisch, es gilt $\mathbb{Z}/U = \langle 1+U \rangle$ und $\text{ord}(1+U) = \#(\mathbb{Z}/U) = d$. Sei $s \in \mathbb{Z}$. Nach der Konstruktion der Faktorgruppe gilt $s \in U$ genau dann, wenn $s+U = 0$ in \mathbb{Z}/U ist. Nach Lemma 1.15, (ii) gilt $s+U = s \cdot 1+U = 0$ genau dann, wenn $\text{ord}(1+U) \mid s$. Es folgt, daß $s \in U$ genau dann ist, wenn $d \mid s$ gilt. Also ergibt sich $U = d\mathbb{Z}$.

Die Eindeutigkeit von d bis auf das Vorzeichen folgt aus Lemma 1.37, (ii). \square

Man kann Lemma 1.39 auch direkter zeigen. Eine Möglichkeit ist, sich $d \in U$ mit $d \geq 1$ minimal zu wählen (wir nehmen hier $U \neq 0$ an, für $U = 0$ ist das Lemma klar). Dann gilt bereits $U = d\mathbb{Z}$. Denn ist $a \in U$, so erhalten wir nach Division durch d die Gleichung $a = qd + r$ und den Rest r mit $0 \leq r < d$. Es folgt $r = a - qd \in U$. Da d minimal in U mit $d \geq 1$ ist, folgt $r = 0$ und $a \in d\mathbb{Z}$.

1.40 Satz. *Sei G zyklisch.*

- (i) *Es gilt $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ für genau ein $n \geq 0$, nämlich $n = \#G$ für $\#G < \infty$ und $n = 0$ für $\#G = \infty$. Die Isomorphieklasse von G ist damit bereits durch $\#G$ eindeutig bestimmt.*
- (ii) *Sei g ein Erzeuger von G . Die Zuordnung $d \mapsto \langle g^d \rangle$ liefert eine Bijektion der Menge der Teiler $d \geq 1$ von $\#G$ auf die Menge der Untergruppen von G . Es gilt $(G : \langle g^d \rangle) = d$.*
- (iii) *Jede Untergruppe und jede Faktorgruppe einer zyklischen Gruppe ist zyklisch.*

Beweis. (i): Sei $g \in G$ ein Erzeuger von G . Wir definieren eine Abbildung $\phi : \mathbb{Z} \rightarrow G$ durch $x \mapsto g^x$. Man sieht direkt, daß ϕ ein Epimorphismus ist. Nach Korollar 1.32 gilt dann $\mathbb{Z}/\ker(\phi) \cong G$. Sei $n = \#G$ für $\#G < \infty$ und $n = 0$ für $\#G = \infty$. Nach Lemma 1.39 und Beispiel 1.22 ist $\ker(\phi) = n\mathbb{Z}$. Also gilt $\mathbb{Z}/n\mathbb{Z} \cong G$.

Die Eindeutigkeit von n in Abhängigkeit von $\#G$ ergibt sich aus $\#G = \#(\mathbb{Z}/n\mathbb{Z})$ aufgrund der Isomorphie. Für $\#G < \infty$ folgt $\#G = \#(\mathbb{Z}/n\mathbb{Z}) = n \neq 0$ und für $\#G = \infty$ folgt $n = 0$ nach Beispiel 1.22. Also ist n durch $\#G$ eindeutig bestimmt. Sind schließlich G und H zyklische Gruppen mit $\#G = \#H$, so folgt $G \cong (\mathbb{Z}/n\mathbb{Z}, +) \cong H$.

(iii): Die Aussage über die Untergruppen folgt aus (ii). Die Surjektivität des kanonischen Epimorphismus zeigt, daß die Klassen eines Erzeugendensystems der Gruppe ein Erzeugendensystem der Faktorgruppe liefern. Damit sind Faktorgruppen zyklischer Gruppen ebenfalls zyklisch. Oder anders ausgedrückt sind homomorphe Bilder zyklischer Gruppen zyklisch.

(ii): Sei D die Menge der Teiler $d \geq 1$ von $\#G$ und $d \in D$. Wir betrachten zuerst $\#G = \infty$. In diesem Fall ist $D = \mathbb{Z}^{\geq 1}$ per Definition. Nach (i) können wir $G = \mathbb{Z}$ annehmen. Nach Lemma 1.37, (ii) gilt $g = \pm 1$ und $\langle g^d \rangle = d\mathbb{Z}$. Damit folgt $(G : \langle g^d \rangle) = (\mathbb{Z} : d\mathbb{Z}) = \#(\mathbb{Z}/d\mathbb{Z}) = d$. Außerdem ergibt sich aus Indexgründen, daß $d \mapsto \langle g^d \rangle$ injektiv ist. Die Surjektivität folgt aus Lemma 1.39.

Wir nehmen nun $n = \#G < \infty$ an. Es gibt einen Epimorphismus $\phi : \mathbb{Z} \rightarrow G$ mit $\phi(1) = g$ und $\ker(\phi) = n\mathbb{Z}$, und dieser liefert nach Lemma 1.28 eine indexerhaltende Bijektion $U \mapsto \phi(U)$ der Untergruppen U von \mathbb{Z} mit $U \supseteq n\mathbb{Z}$ auf die Menge der Untergruppen von G . Nach dem bereits Bewiesenen von (ii) ist $U = d\mathbb{Z}$ mit $d|n$ wegen $U \supseteq n\mathbb{Z}$ und wir erhalten durch Einschränkung von $d \mapsto d\mathbb{Z}$ von $\mathbb{Z}^{\geq 1}$ auf D eine Bijektion von D auf die Menge der Untergruppen U von \mathbb{Z} mit $U \supseteq n\mathbb{Z}$. Durch Komposition beider Bijektionen erhalten wir schließlich eine Bijektion $d \mapsto \phi(d\mathbb{Z}) = \langle g^d \rangle$ von D auf die Menge der Untergruppen von G . \square

1.41 Bemerkung. Die algorithmischen Verhältnisse der Isomorphie in Satz 1.40, (i) sind nicht so klar wie die Theorie, und hierauf beruhen Anwendungen in der Computersicherheit und speziell Kryptographie. Konkret betrachtet man Situationen, in denen Bilder unter dem Isomorphismus ϕ aus dem Beweis leicht, aber Urbilder (vermutlich) nur sehr schwer berechnet werden können. Die Urbildberechnung nennt man auch das diskrete Logarithmusproblem, denn zu $b \in G$ sucht man $x \in \mathbb{Z}$ mit $b = g^x$. Die Untersuchung der Komplexität dieses Problems zählt zu den aktuellen Forschungsgebieten in der Kryptographie.

1.9 Direkte Produkte

1.42 Definition. Seien I eine Indexmenge und G_i Gruppen. Das direkte Produkt $\prod_{i \in I} G_i$ der G_i wird wie folgt definiert. Als Menge gilt $\prod_{i \in I} G_i = \{f : I \rightarrow \cup_{i \in I} G_i \mid f(i) \in G_i \text{ für alle } i \in I\}$, also das kartesische Produkt der Mengen G_i . Das Gruppengesetz wird koordinatenweise definiert, das heißt für $f, g \in \prod_{i \in I} G_i$ sei $h = fg \in \prod_{i \in I} G_i$ durch $h(i) = f(i)g(i)$ für alle $i \in I$ definiert.

Das neutrale Element e von $\prod_{i \in I} G_i$ ist dann durch $e(i) = 1$ für alle $i \in I$ gegeben. Ist $I = \{1, \dots, n\}$ so schreiben wir auch $G_1 \times \dots \times G_n$ statt $\prod_{i \in I} G_i$. Die Definition des Produkts stimmt mit der „üblichen“ Definition von Tupeln überein, wenn man die Tupel als $(f(i))_{i \in I}$ oder (f_1, \dots, f_n) schreibt.

Das direkte Produkt besitzt die Projektionen $\pi_i : \prod_{i \in I} G_i \rightarrow G_i$, $\pi_i(f) = f(i)$ und Injektionen $\iota_i : G_i \rightarrow \prod_{i \in I} G_i$, $a \mapsto f$ mit $f(i) = a$ und $f(j) = 1$ für alle $j \in I$ mit $j \neq i$. Die Projektionen sind Epimorphismen und die Injektionen sind Monomorphismen. Es gilt $\pi_i \circ \iota_i = \text{id}$.

Die direkte Summe der G_i wird definiert als $\coprod_{i \in I} G_i = \{f \in \prod_{i \in I} G_i \mid f(i) = 1 \text{ für fast alle } i \in I\}$ und ist eine Untergruppe von $\prod_{i \in I} G_i$. Es besitzt die eingeschränkten Injektionen ι_i und Projektionen π_i . Für endliche Indexmengen gilt $\coprod_{i \in I} G_i = \prod_{i \in I} G_i$.

Das direkte Produkt und die direkte Summe können unter ausschließlicher Verwendung von Homomorphismen bis auf Isomorphie eindeutig charakterisiert werden. Dies führt in die Kategorientheorie. Es ist hilfreich, sich die Aussagen der folgenden Definition in Diagrammform zu zeichnen. Man erkennt, daß die Begriffe direktes Produkt und direkte Summe „dual“ sind. Dies motiviert auch die Notation \coprod als umgekehrtes \prod (entsprechend nennt man die direkte Summe auch Koprodukt).

Eine Gruppe G zusammen mit Homomorphismen $\pi_i : G \rightarrow G_i$ heißt *universelles direktes Produkt*, wenn es für jede Gruppe H und Homomorphismen $\phi_i : H \rightarrow G_i$ genau einen Homomorphismus $\psi : H \rightarrow G$ mit $\phi_i = \pi_i \circ \psi$ für alle $i \in I$ gibt.

Eine Gruppe G zusammen mit Homomorphismen $\iota_i : G_i \rightarrow G$ heißt *universelle direkte Summe*, wenn es für jede Gruppe H und Homomorphismen $\phi_i : G_i \rightarrow H$ genau einen Homomorphismus $\psi : G \rightarrow H$ mit $\phi_i = \psi \circ \iota_i$ für alle $i \in I$ gibt.

1.43 Satz. *Universelle direkte Produkte und Summen sind bis auf Isomorphie eindeutig bestimmt.*

Das direkte Produkt zusammen mit den Projektionen ist ein universelles direktes Produkt. Die direkte Summe zusammen mit den Injektionen ist eine universelle direkte Summe.

Beweis. Zum Beweis der Eindeutigkeit sei G' zusammen mit den π'_i ein weiteres universelles direktes Produkt. Dann gibt es Homomorphismen $\psi : G' \rightarrow G$ mit $\pi'_i = \pi_i \circ \psi$ und $\psi' : G \rightarrow G'$ mit $\pi_i = \pi'_i \circ \psi'$. Wir erhalten $\pi_i = \pi_i \circ \psi \circ \psi'$ und $\pi'_i = \pi'_i \circ \psi' \circ \psi$. Aufgrund der Eindeutigkeitsaussage der universellen Eigenschaften folgt $\psi \circ \psi' = \text{id}$ und $\psi' \circ \psi = \text{id}$, denn die Identitäten erfüllen $\pi_i = \pi_i \circ \text{id}$ und $\pi'_i = \pi'_i \circ \text{id}$. Also sind G und G' isomorph. Der Beweis für die universelle direkte Summe erfolgt analog.

Zum Beweis der zweiten Aussage. Die Bedingungen $\pi_i \circ \psi = \phi_i$ zeigen, daß notwendigerweise $\psi(x) = (\phi_i(x))_{i \in I}$ gelten muß. Man sieht sofort, daß dadurch ein Homomorphismus ψ definiert wird. Also besitzt das direkte Produkt die universelle Eigenschaft. Die Bedingungen $\psi \circ \iota_i = \phi_i$ und die Homomorphieeigenschaft von ψ zeigen, daß notwendigerweise $\psi(f) = \prod_{i \in I} \phi_i(f(i))$ gelten muß. Dies macht Sinn, da in dem Produkt nur endlich viele Faktoren $\neq 1$ sind. Man prüft leicht nach, daß dadurch in der Tat ein Homomorphismus ψ definiert wird. Also besitzt auch die direkte Summe die universelle Eigenschaft. \square

Eine Anwendung von Satz 1.43 ist die folgende, die man natürlich auch leicht direkt nachweisen kann: Sind $f_i : G_i \rightarrow H_i$ für $i \in I$ Homomorphismen, dann gibt es einen Produkthomomorphismus $f = \prod_{i \in I} f_i : \prod_{i \in I} G_i \rightarrow \prod_{i \in I} H_i$ mit $f(g)(i) = f_i(g(i))$ beziehungsweise $\pi_i \circ f \circ \iota_i = f_i$ für alle $i \in I$, wobei $\iota_i : G_i \rightarrow \prod_{i \in I} G_i$ die i -te Inklusion und $\pi_i : \prod_{i \in I} H_i \rightarrow H_i$ die i -te Projektion ist.

Es folgen einige Rechenregeln für direkte Produkte.

1.44 Lemma. *Seien G_i, H_i für $i \in I$ Gruppen.*

- (i) $\# \prod_{i \in I} G_i = \prod_{i \in I} \# G_i$.
- (ii) $\prod_{i \in I} G_i$ ist genau dann abelsch, wenn G_i für alle $i \in I$ abelsch ist.
- (iii) Für $\sigma \in S(I)$ gilt $\prod_{i \in I} G_i \cong \prod_{i \in I} G_{\sigma(i)}$ unter $f \mapsto f \circ \sigma$.
- (iv) Für $I = I_1 \dot{\cup} I_2$ gilt $(\prod_{i \in I_1} G_i) \times (\prod_{i \in I_2} G_i) \cong \prod_{i \in I} G_i$.
- (v) $\prod_{i \in I} f_i : \prod_{i \in I} G_i \rightarrow \prod_{i \in I} H_i$ ist genau dann ein Homomorphismus (Isomorphismus, Epimorphismus, Monomorphismus) wenn f_i für alle $i \in I$ ein Homomorphismus (Isomorphismus, Epimorphismus, Monomorphismus) ist.
- (vi) Ist N_i Normalteiler von G_i für alle $i \in I$, so ist $\prod_{i \in I} N_i$ ein Normalteiler von $\prod_{i \in I} G_i$ und es gilt $\prod_{i \in I} G_i / \prod_{i \in I} N_i \cong \prod_{i \in I} G_i / N_i$.

Beweis. Die Aussagen sind klar. Wir beweisen nur (v).

Die Sequenz

$$1 \rightarrow N_i \rightarrow G_i \rightarrow G_i/N_i \rightarrow 1$$

ist exakt für alle $i \in I$. Durch Anwenden von $\prod_{i \in I}$ (und nach (v)) erhalten wir die exakte Sequenz

$$1 \rightarrow \prod_{i \in I} N_i \rightarrow \prod_{i \in I} G_i \rightarrow \prod_{i \in I} G_i/N_i \rightarrow 1.$$

Daraus folgt (v). □

Lemma 1.44, (iii) kann also als „Kommutativität“ und (iv) als „Assoziativität“ des direkten Produkts aufgefaßt werden.

Der folgende Satz liefert ein Kriterium, wann eine Gruppe isomorph zu einem endlichen direkten Produkt ist.

1.45 Satz.

- (i) Für das endliche direkte Produkt $G = \prod_{i=1}^n G_i$ sei $N_i = \iota_i(G_i)$ für alle $1 \leq i \leq n$. Dann sind die N_i Normalteiler von G und es gilt

$$\begin{aligned} G &= N_1 \cdots N_n, \\ N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_n) &= 1 \text{ für alle } 1 \leq i \leq n. \end{aligned} \quad (1.46)$$

Ferner gilt $x_i x_j = x_j x_i$ für alle $x_i \in N_i, x_j \in N_j$ und $1 \leq i, j \leq n$ mit $i \neq j$.

- (ii) Eine Gruppe G ist genau dann isomorph zu einem endlichen direkten Produkt, wenn es Normalteiler N_i von G gibt, welche die Bedingung (1.46) erfüllen.

Ist dies der Fall, so gibt es einen Isomorphismus $\phi : G \rightarrow \prod_{i=1}^n N_i$ mit $\phi|_{N_i} = \iota_i$ für alle $1 \leq i \leq n$, wobei die ι_i die Inklusionen $N_i \rightarrow \prod_{i=1}^n N_i$ sind.

Beweis. (i): Die Aussage (i) des Satzes ist einfach und kann direkt nachgerechnet werden.

(ii): Die Implikation „ \Rightarrow “ der zweiten Aussage folgt direkt aus (i). Sind für „ \Leftarrow “ die N_i Normalteiler von G mit den angegebenen Eigenschaften, so definiere $\psi : \prod_i N_i \rightarrow G$ durch $(x_1, \dots, x_n) \mapsto x_1 \cdots x_n$. Dies ist ein Homomorphismus: Es gelte $1 \leq i, j \leq n$ mit $i \neq j$. Wegen der Normalteilereigenschaft von N_i und N_j gibt es $x'_i \in N_i$ und $x'_j \in N_j$ mit $x_i x_j = x_j x'_i$ und $x_i x_j = x'_j x_i$. Es folgt $x_j x'_i = x'_j x_i$, also $x'_i x_i^{-1} = x_j^{-1} x'_j \in N_i \cap N_j = 1$. Es ergibt sich $x'_i x_i^{-1} = x_j^{-1} x'_j = 1$, also $x'_i = x_i$ und $x'_j = x_j$. Damit folgt $x_i x_j = x_j x_i$ für alle $x_i \in N_i$ und $x_j \in N_j$ und ψ ist in der Tat ein Homomorphismus. Wegen $G = N_1 \cdots N_n$ ist ψ dazu surjektiv. Aus $x_1 \cdots x_n = 1$ folgt $x_1^{-1} = x_2 \cdots x_n \in N_1 \cap (N_2 \cdots N_n) = 1$. Also $x_1 = 1$ und induktiv $x_i = 1$ für alle $1 \leq i \leq n$. Daher ist ψ auch injektiv und insgesamt also ein Isomorphismus.

Ist G isomorph zu einem Produkt, so gibt es die N_i . Gibt es die N_i , so liefert $\phi = \psi^{-1}$ den gewünschten Isomorphismus, wobei ψ wie eben konstruiert wird. \square

Trifft die Bedingung von Satz 1.45 zu, so sagen wir auch, daß G das innere direkte Produkt der N_i sei.

Wir betrachten jetzt zwei Anwendungen direkter Produkte.

1.47 Satz. Für $n, m \in \mathbb{Z} \setminus \{0\}$ mit $\gcd(n, m) = 1$ gilt die Isomorphie (additiver abelscher Gruppen)

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Sei $G = G_1 \times G_2$ mit G_1, G_2 zyklisch von endlicher Ordnung. Dann ist G genau dann zyklisch, wenn G_1 und G_2 zyklisch von teilerfremder Ordnung sind.

Beweis. Wir betrachten den Homomorphismus $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $x \mapsto (x + n\mathbb{Z}, x + m\mathbb{Z})$. Es gilt $\ker(\phi) = \text{lcm}(n, m)\mathbb{Z} = nm\mathbb{Z}$. Dann ist $\mathbb{Z}/nm\mathbb{Z}$ zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ isomorph. Aus Anzahlgründen muß diese Untergruppe aber bereits ganz $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sein.

Die Implikation „ \Leftarrow “ folgt aus der ersten Aussage. Für „ \Rightarrow “ nehmen wir $d = \text{gcd}(\#G_1, \#G_2) > 0$ an. Dann gibt es in G_1 eine Untergruppe der Ordnung d und in G_2 eine Untergruppe der Ordnung d . Dann gibt es in $G = G_1 \times G_2$ zwei verschiedene Untergruppen der gleichen Ordnung, also kann G nach Satz 1.40, (ii) nicht zyklisch sein. \square

Als Übungsaufgabe betrachte man in Satz 1.47 auch die Fälle, in denen mindestens eine Gruppe zyklisch von unendlicher Ordnung ist.

Der folgende Satz heißt Hauptsatz für endlich erzeugte abelsche Gruppen.

1.48 Satz. *Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, n \in \mathbb{Z}^{\geq 0}$, Primzahlen p_i und Exponenten $e_i \in \mathbb{Z}^{\geq 1}$ für $1 \leq i \leq n < \infty$ mit*

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^n \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Die Zahlen r, n und p_i, e_i sind (bis auf Reihenfolge) eindeutig durch die Isomorphieklasse von G bestimmt.

Beweis. Der Satz ist ein Spezialfall des Satzes über endlich erzeugte Moduln über Hauptidealringen, den wir später beweisen. \square

1.10 Semidirekte Produkte

Bei direkten Produkten kommutieren die Elemente aus den einzelnen Faktoren. Semidirekte Produkte sind eine Verallgemeinerung von direkten Produkten, bei denen dies im allgemeinen nicht mehr der Fall ist.

1.49 Lemma. *Sei $x \in G$. Durch $\phi_x(a) = xax^{-1}$ für $a \in G$ wird ein Automorphismus $\phi_x \in \text{Aut}(G)$ definiert.*

Durch $x \mapsto \phi_x$ wird ein Homomorphismus $\phi : G \rightarrow \text{Aut}(G)$ definiert.

Beweis. Es gilt $\phi_x(ab) = xabx^{-1} = xax^{-1}xbx^{-1} = \phi_x(a)\phi_x(b)$, also ist ϕ_x ein Homomorphismus. Wie man direkt nachrechnet, gilt $\phi_{x^{-1}} \circ \phi_x = \phi_x \circ \phi_{x^{-1}} = \text{id}$, also ist ϕ_x ein Isomorphismus.

Es gilt $\phi_{xy}(a) = xyax(yx)^{-1} = xyay^{-1}x^{-1} = (\phi_x \circ \phi_y)(a)$ für alle $a \in G$. Dies zeigt $\phi_{xy} = \phi_x \circ \phi_y$, also ist ϕ ein Homomorphismus. \square

1.50 Definition. Die Automorphismen ϕ_x heißen innere Automorphismen von G . Die Anwendung von ϕ_x auf a nennt man auch Konjugation von a mit x . Zwei Elemente $a, b \in G$ heißen konjugiert, wenn es $x \in G$ mit $b = \phi_x(a)$ gibt.

Wir merken kurz an, daß die durch Konjugation gegebene Relation auf G eine Äquivalenzrelation ist. Dies folgt direkt aus der Homomorphieeigenschaft von $x \mapsto \phi_x$ gemäß Lemma 1.49.

Ist N ein Normalteiler von G und ϕ_x ein innerer Automorphismus, so gilt $\phi_x(N) = N$.

Zur Definition des semidirekten Produkts ist es eingängiger, zuerst das innere semidirekte Produkt zu betrachten. Sei G eine Gruppe, N ein Normalteiler von G und U eine Untergruppe von G . Es gelte $G = NU$ und $N \cap U = 1$. Dann nennen wir G das innere semidirekte Produkt von N und U . Für $n_1, n_2 \in N$ und $u_1, u_2 \in U$ gilt $n_1 u_1 n_2 u_2 = n_1 u_1 n_2 u_1^{-1} u_1 u_2 = (n_1 \phi_{u_1}(n_2))(u_1 u_2)$ mit $n_1 \phi_{u_1}(n_2) \in N$ wegen der Normalteilereigenschaft und $u_1 u_2 \in U$. Dies motiviert die folgende Definition des (äußeren) semidirekten Produkts.

1.51 Definition. Seien N und U Gruppen und $\psi : U \rightarrow \text{Aut}(N)$, $x \mapsto \psi_x$ ein Homomorphismus. Das semidirekte Produkt $N \rtimes_{\psi} U$ von N und U bezüglich ψ wird wie folgt definiert. Als Menge gilt $N \rtimes_{\psi} U = N \times U$. Die Gruppenoperation ist $(n_1, u_1) \cdot (n_2, u_2) = (n_1 \psi_{u_1}(n_2), u_1 u_2)$.

Es ist eine Übungsaufgabe, zu zeigen, daß das semidirekte Produkt $N \rtimes_{\psi} U$ eine Gruppe ist. Das semidirekte Produkt kommt mit zwei Injektionen $\iota_1 : N \rightarrow N \rtimes_{\psi} U$, $x \mapsto (x, 1)$ und $\iota_2 : U \rightarrow N \rtimes_{\psi} U$, $x \mapsto (1, x)$ sowie einer Projektion $\pi_2 : N \rtimes_{\psi} U \rightarrow U$, $(x, y) \mapsto y$. Die Injektionen sind Monomorphismen und die Projektion ist ein Epimorphismus. Es gilt $\ker(\pi_2) = \iota_1(N)$, so daß $\iota_1(N)$ ein Normalteiler von $N \rtimes_{\psi} U$ ist.

Ist $\iota_2(U)$ sogar ein Normalteiler von G , so folgt $(n, 1)(1, u)(n, 1)^{-1} = (n, u) \cdot (n^{-1}, 1) = (n \psi_u(n)^{-1}, 1) \in \iota_2(U)$ für alle $n \in N$ und $u \in U$, also $n \psi_u(n)^{-1} = 1$, $\psi(u) = \text{id}$ für alle $u \in U$ und $G \cong N \times U$.

Eine exakte Sequenz

$$1 \rightarrow N \xrightarrow{\iota_1} G \xrightarrow{\pi_2} U \rightarrow 1$$

heißt rechts zerfallend, wenn es (einen „Schnitt“) $\chi : U \rightarrow G$ mit $\pi_2 \circ \chi = \text{id}$ gibt.

1.52 Satz. Für eine Gruppe G sind äquivalent.

- (i) G ist isomorph zu einem semidirekten Produkt $N \rtimes_{\psi} U$.
- (ii) Es gibt einen Normalteiler N von G und eine Untergruppe U von G mit

$$G = NU \text{ und } N \cap U = 1.$$

(iii) Es gibt Gruppen N und U und eine rechts zerfallende exakte Sequenz

$$1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} U \rightarrow 1.$$

Hierbei entsprechen sich die Gruppen N und U aus (i), (ii) und (iii) sowie die Homomorphismen $\psi : U \rightarrow \text{Aut}(N)$ aus (i) und $\phi : U \rightarrow \text{Aut}(N)$, $x \mapsto \phi_x$ aus (ii) (wie in Lemma 1.49) in natürlicher Weise.

Beweis. (i) \Rightarrow (ii): Folgt aus den oben genannten Eigenschaften des semidirekten Produkts, indem für N und U aus (ii) die Gruppen $N' = \iota_1(N)$ und $U' = \iota_2(U)$ verwendet werden.

Seien $(1, u) \in U'$ und $(n, 1) \in N'$. Dann gilt $(1, u)^{-1} = (1, u^{-1})$ und weiter $(1, u)(n, 1)(1, u)^{-1} = (\psi_u(n), u)(1, u^{-1}) = (\psi_u(n), 1)$. Insofern entspricht Konjugation von Elementen aus N' mit Elementen aus U' also der Anwendung von ψ .

(ii) \Rightarrow (i): Wir definieren $\psi = \phi$, wobei $\phi : U \rightarrow \text{Aut}(N)$, $x \mapsto \phi_x$ wie in Lemma 1.49 ist. Weiter definieren wir $f : N \rtimes_{\psi} U \rightarrow G$ durch $(n, u) \mapsto nu$. Nach der Motivation zur Definition des semidirekten Produkts ist f ein Homomorphismus. Wegen $G = NU$ ist f surjektiv und wegen $N \cap U = 1$ injektiv.

(ii) \Rightarrow (iii): Es gilt $G/N \cong NU/N \cong U/U \cap N \cong U$ nach Satz 1.33, wobei wir $G = NU$ und $N \cap U = 1$ verwenden. Wir definieren i als die Inklusionsabbildung $N \rightarrow G$ und $\pi : G \rightarrow U$ als kanonischen Epimorphismus gefolgt vom Isomorphismus $G/N \cong U$. Die Abbildung $\chi : U \rightarrow G$ definieren wir als die Inklusion. Dann gilt $\pi(\chi(u)) = u$ für alle $u \in U$, also folgt (iii).

(iii) \Rightarrow (ii): Wir definieren $N' = i(N)$ und $U' = \chi(U)$. Sei $g \in G$ beliebig. Wir setzen $u = \chi(\pi(g)) \in U'$. Es folgt $\pi(gu^{-1}) = \pi(g)\pi(u^{-1}) = \pi(g)\pi(\chi(\pi(g))^{-1}) = \pi(g)((\pi \circ \chi)(\pi(g)^{-1})) = \pi(g)\pi(g)^{-1} = 1$, also $gu^{-1} \in \ker(\pi) = N'$ nach Voraussetzung. Mit $n = gu^{-1} \in N'$ folgt $g = nu$, also $G = N'U'$.

Sei $g \in N' \cap U'$. Wegen $g \in U'$ gilt $g = \chi(h)$ und $\pi(g) = \pi(\chi(h)) = h$ für ein $h \in U$. Wegen $g \in N'$ gilt $\pi(g) = h = 1$. Also folgt $g = \chi(h) = 1$ und damit $N' \cap U' = 1$. \square

Eine Folgerung aus dem Satz ist, daß für nicht-triviales $\phi : U \rightarrow \text{Aut}(N)$ das semidirekte Produkt $N \rtimes_{\phi} U$ nicht abelsch ist, da $\iota_2(U)$ auf $\iota_1(N)$ durch Konjugation nicht-trivial operiert.

Trifft die Bedingung (ii) aus Satz 1.52 zu, so nennen wir U auch ein *Komplement* von N in G .

1.53 Beispiel. Die Symmetriegruppe D_n eines regelmäßigen n -Ecks mit $n \geq 3$ wird von der Drehung d um $360/n$ Grad und der Spiegelung s erzeugt. Formal gilt $d^n = 1$, $s^2 = 1$ und $ds = sd^{-1}$ beziehungsweise $sds^{-1} = d^{-1}$. Die Gruppe D_n heißt auch Diedergruppe.

Sei $N = \langle d \rangle$ und $U = \langle s \rangle$. Dann gilt $\#N = n$ und $\#U = 2$. Außerdem gilt $D_n = NU$ und $N \cap U = 1$, da keine Drehung eine Spiegelung darstellt. Wegen $sds^{-1} = d^{-1} \in N$ ist N dann ein Normalteiler von D_n . Mit Satz 1.52 folgt $D_n \cong N \rtimes_\phi U$, wobei ϕ wie in Lemma 1.49 definiert ist.

Der folgende Satz enthält noch ein paar einfache Beobachtungen über semidirekte Produkte endlicher Gruppen.

1.54 Satz. *Seien N und U endliche Gruppen und $\psi : U \rightarrow \text{Aut}(N)$ ein Homomorphismus.*

(i) *Gilt $\gcd(\#U, \#\text{Aut}(N)) = 1$, so folgt*

$$N \rtimes_\psi U = N \times U.$$

(ii) *Sei U einfach und $\phi : U \rightarrow \text{Aut}(N)$ ein Monomorphismus. Für jeden Homomorphismus $\psi : U \rightarrow \text{Aut}(N)$ mit $\psi(U) \subseteq \phi(U)$ gilt dann*

$$N \rtimes_\psi U = N \times U \text{ oder } N \rtimes_\psi U \cong N \rtimes_\phi U.$$

(iii) *Gilt $\gcd(\#N, \#U) = 1$, so gibt es in $N \rtimes_\psi U$ genau eine zu N isomorphe Untergruppe.*

Beweis. (i): Wegen $\gcd(\#U, \#\text{Aut}(N)) = 1$ folgt $\psi(U) = \{\text{id}\}$ nach Satz 1.20. Daraus ergibt sich direkt $N \rtimes_\psi U = N \times U$.

(ii): Da U einfach ist, gilt $\psi(U) = \{\text{id}\}$ oder ψ ist injektiv. Für $\psi(U) = \{\text{id}\}$ folgt $N \rtimes_\psi U = N \times U$ wie in (i). Ist ψ injektiv, so folgt $\psi(U) = \phi(U)$ wegen $\psi(U) \subseteq \phi(U)$ und $\#U < \infty$. Wir erhalten einen Automorphismus σ von U durch $\sigma(u) = \phi^{-1}(\psi(u))$ für alle $u \in U$, so daß mit der Indexschreibweise $\phi_u = \phi(u)$ von oben $\psi_u = \phi_{\sigma(u)}$ für alle $u \in U$ gilt. Damit definieren wir $f : N \rtimes_\psi U \rightarrow N \rtimes_\phi U$ durch $(n, u) \mapsto (n, \sigma(u))$. Dies ist ein Homomorphismus, denn es gilt

$$\begin{aligned} f((n_1, u_1)(n_2, u_2)) &= f((n_1\psi_{u_1}(n_2), u_1u_2)) = (n_1\psi_{u_1}(n_2), \sigma(u_1u_2)) \\ &= (n_1\phi_{\sigma(u_1)}(n_2), \sigma(u_1)\sigma(u_2)) = (n_1, \sigma(u_1))(n_2, \sigma(u_2)) \\ &= f((n_1, u_1))f((n_2, u_2)) \end{aligned}$$

für alle $n_1, n_2 \in N$ und $u_1, u_2 \in U$. Außerdem ist f offenbar bijektiv, also ein Isomorphismus.

(iii): Sei $f : N \rightarrow N \rtimes_\psi U$ ein Monomorphismus. Wegen $\gcd(\#N, \#U) = 1$ gilt dann $\pi_2(f(n)) = 1$ für alle $n \in N$ und folglich $f(N) = \iota_1(N)$. \square

1.11 Operationen von Gruppen auf Mengen

Gruppen treten häufig als Automorphismengruppen auf, sie operieren also zum Beispiel auf Mengen (Algebra 1, im folgenden), Vektorräumen (Darstellungstheorie, Jordan Normalform, letztere später), auf Körpern (Algebra 2, Galoistheorie), auf topologischen Räumen oder auf Riemannschen Flächen (Topologie, Geometrie) und so weiter. In jedem dieser Fälle soll die Operation der Gruppe die Struktur der unterliegenden Objekte erhalten. Da Mengen keine zusätzliche Struktur haben, werden hier die schwächsten beziehungsweise nur die allgemeinsten Anforderungen gestellt.

1.55 Definition. Sei G eine Gruppe und X eine Menge. Eine Operation von G auf X ist eine Verknüpfung $\circ : G \times X \rightarrow X$, $(g, x) \mapsto g \circ x$ auf X mit Operatorbereich G , so daß

$$(i) \quad (gh) \circ x = g \circ (hx) \text{ für alle } g, h \in G \text{ und } x \in X,$$

$$(ii) \quad 1 \circ x = x \text{ für alle } x \in X$$

gilt. Wir nennen X dann auch eine G -Menge.

Anstelle von $g \circ x$ schreiben wir meistens wieder $g \cdot x = gx$. Das folgende Lemma liefert eine alternative, kompaktere Definition einer Operation von G auf X . Man erinnere sich daran, daß $S(X)$ die Automorphismen (strukturerehaltende Bijektionen) von X sind.

1.56 Lemma. Sei G eine Gruppe und X eine Menge. Eine Operation von G auf X liefert einen Homomorphismus $\phi : G \rightarrow S(X)$, $g \mapsto (x \mapsto gx)$.

Ist umgekehrt $\phi : G \rightarrow S(X)$ ein Homomorphismus, so erhalten wir eine Operation von G auf X durch $gx = \phi(g)(x)$.

Beweis. Durch einfaches Nachrechnen. □

Wir nennen ϕ aus Lemma 1.56 die zur Operation von G auf X gehörige *Permutationsdarstellung* von G .

Besitzt X eine zusätzliche (algebraische) Struktur, so kann man eine Operation von G auf X durch einen Homomorphismus $G \rightarrow \text{Aut}(X)$ wie im Lemma definieren und erspart sich somit die explizite Angabe der Axiome für die Operation.

1.57 Beispiel. Drehungen und Spiegelungen liefern eine Operation von D_n auf einem n -Eck.

Die Permutationsgruppe $S(X)$ operiert auf X .

Ist X ein Normalteiler von G , so operiert G auf X durch Konjugation $g \circ n = gng^{-1}$. Entsprechend haben wir $\phi : G \rightarrow \text{Aut}(X)$, $g \mapsto \phi_g$ mit Hilfe von inneren Automorphismen. Durch diese Operation wird sogar die Gruppenstruktur von X respektiert.

Sei U eine Untergruppe von G . Dann operiert G auf den Linksnebenklassen durch Multiplikation von links, $g \circ hU = ghU$. Entsprechend erhalten wir die Permutationsdarstellung $\phi : G \rightarrow S(X)$ mit $X = \{gU \mid g \in U\}$. Für $U = \{1\}$ ist ϕ injektiv.

Der Strukturvergleich von G -Mengen X und Y erfolgt mit G -equivarianten Abbildungen oder G -Abbildungen: Dieses sind Abbildungen $f : X \rightarrow Y$ mit $gf(x) = f(gx)$ für alle $g \in G$ und $x \in X$.

Sei X eine G -Menge. Wir definieren eine Relation \sim auf X wie folgt. Es gelte $x \sim y$ genau dann, wenn es $g \in G$ mit $y = gx$ gibt. Dies ist eine Äquivalenzrelation, wie man leicht nachrechnet. Die Äquivalenzklasse von x bezeichnen wir mit Gx . Es gilt $Gx = \{gx \mid g \in G\}$.

1.58 Definition. Die Äquivalenzklassen Gx heißen Bahnen (Orbits) von $x \in X$ unter G . Der Stabilisator von x in G ist $\text{Stab}_G(x) = \{g \in G \mid gx = x\}$. Die Menge der Fixpunkte der Operation von G auf X ist $\text{Fix}_G(X) = \{x \in X \mid gx = x \text{ für alle } g \in G\}$.

Die Gruppe G operiert transitiv auf X , wenn es für jedes $x, y \in X$ ein $g \in G$ mit $y = gx$ gibt. Die Gruppe G operiert treu auf X , wenn aus $gx = x$ für alle $x \in X$ die Gleichung $g = 1$ folgt. Die Gruppe G operiert frei auf X , wenn aus $gx = x$ für ein $x \in X$ bereits $g = 1$ folgt.

Die G -Menge X heißt homogener Raum, wenn G auf X transitiv operiert. Die G -Menge X heißt prinzipal-homogener Raum oder G -Torsor, wenn G auf X transitiv und frei operiert.

Man sieht leicht, daß G genau dann transitiv auf X operiert, wenn $X = Gx$ für ein (jedes) $x \in X$ gilt. Ebenso leicht sieht man, daß G genau dann treu auf X operiert, wenn die zugehörige Permutationsdarstellung $\phi : G \rightarrow S(X)$ injektiv ist. Allgemein gilt $\ker(\phi) = \bigcap_{x \in X} \text{Stab}_G(x)$.

1.59 Satz. Sei X eine G -Menge.

- (i) $\text{Stab}_G(x)$ ist eine Untergruppe von G und es gilt $\text{Stab}_G(gx) = g\text{Stab}_G(x)g^{-1}$ für alle $g \in G$ und $x \in X$.
- (ii) Es gilt $\#Gx = (G : \text{Stab}_G(x))$ und $\#Gx \mid \#G$.

(iii) Ist $V \subseteq X$ ein Vertretersystem der Bahnen von X unter G , so gilt

$$\#X = \#\text{Fix}_G(X) + \sum_{\substack{x \in V, \\ (G : \text{Stab}_G(x)) \neq 1}} (G : \text{Stab}_G(x)).$$

Beweis. (i): Die Untergruppeneigenschaft von $\text{Stab}_G(x)$ ist klar. Außerdem sieht man sofort $g\text{Stab}_G(x)g^{-1} \subseteq \text{Stab}_G(gx)$ für alle $g \in G$. Mit g durchläuft auch g^{-1} ganz G . Für $y = gx$ folgt $g^{-1}\text{Stab}_G(y)g \subseteq \text{Stab}_G(g^{-1}y)$, also $\text{Stab}_G(gx) \subseteq g\text{Stab}_G(x)g^{-1}$ für alle $g \in G$.

(ii): Definiere $\phi : Gx \rightarrow \{g\text{Stab}_G(x) \mid g \in G\}$ durch $gx \mapsto g\text{Stab}_G(x)$. Die Abbildung ϕ ist wohldefiniert und injektiv: Für $g, h \in G$ gilt $gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in \text{Stab}_G(x) \Leftrightarrow g\text{Stab}_G(x) = h\text{Stab}_G(x)$. Die Surjektivität von ϕ ist offensichtlich. Es folgt $\#Gx = (G : \text{Stab}_G(x))$, und daraus ergibt sich schließlich $\#Gx \mid \#G$.

(iii): Es gilt $X = \dot{\cup}_{x \in V} Gx$ und daher $\#X = \sum_{x \in V} (G : \text{Stab}_G(x))$ nach (ii). Nun gilt $x \in \text{Fix}_G(X)$ genau dann, wenn $\#Gx = (G : \text{Stab}_G(x)) = 1$ ist. Aufspalten der Summe liefert (iii). \square

1.60 Definition. Sei G eine Gruppe und $M \subseteq G$. Der Zentralisator von M in G ist definiert als

$$Z_G(M) = \{g \in G \mid gm = mg \text{ für alle } m \in M\}$$

und der Normalisator $N_G(M)$ von M in G ist definiert als

$$N_G(M) = \{g \in G \mid gM = Mg\}.$$

Das Zentrum von G ist $Z(G) = Z_G(G)$.

Für jedes M gilt $Z_G(M) \leq N_G(M) \leq G$. Für $M = \{x\}$ gilt $Z_G(M) = N_G(M)$. Eine Gruppe G ist genau dann abelsch, wenn $Z(G) = G$ gilt. Der Normalisator $N_G(U)$ einer Untergruppe U von G ist die größte Untergruppe von G , in der U ein Normalteiler ist.

Wir betrachten die Operation von G durch Konjugation auf sich selbst. Es ist also $X = G$ und die Operation wird durch $\phi : G \rightarrow S(X)$, $g \mapsto \phi_g$ beziehungsweise durch $g \circ x = gxg^{-1}$ für $g \in G$ und $x \in X$ beschrieben.

1.61 Lemma. Das Zentrum $Z(G)$ von G ist ein Normalteiler von G und es gilt

$$Z(G) = \ker(\phi) = \text{Fix}_G(X).$$

Beweis. Es gilt $\phi_g = 1$ genau dann, wenn $\phi_g(x) = gxg^{-1} = x$ für alle $x \in X$ ist. Dies zeigt $\ker(\phi) = Z(G)$ und $Z(G)$ ist ein Normalteiler von G . Weiter gilt $\text{Fix}_G(X) = \{x \in X \mid gxg^{-1} = x \text{ für alle } g \in G\} = \{g \in G \mid xgx^{-1} = g \text{ für alle } x \in G\} = Z(G)$. \square

Die Anzahl der einelementigen Konjugationsklassen von G ist also durch $\#Z(G)$ gegeben.

Wir betrachten jetzt die Operation von G durch Konjugation auf der Menge X der Untergruppen von G . Für $U \in X$ gilt also $g \circ U = gUg^{-1}$. Die Menge Y der zu einer gegebenen Untergruppe U von G konjugierten Untergruppen ist gleich dem Orbit $G \circ U$.

1.62 Lemma. *Für den Normalisator $N_G(U)$ gilt $N_G(U) = \text{Stab}_G(U)$.*

Die Anzahl der zu U konjugierten Untergruppen von G ist gleich $(G : N_G(U))$.

Beweis. Die erste Aussage folgt direkt aus der Definition von $N_G(U)$. Die zweite Aussage folgt aus Theorem 1.59, (ii) unter Beachtung von $Y = G \circ U$ und $N_G(U) = \text{Stab}_G(U)$. \square

1.12 Sylowsätze

Wir beweisen jetzt zwei Sätze über die Existenz und Anzahl gewisser Untergruppen einer endlichen Gruppe.

1.63 Lemma. *Seien $n, m, e \in \mathbb{Z}^{\geq 1}$ und p eine Primzahl mit $n = p^e m$ und $m \not\equiv 0 \pmod{p}$. Dann gibt es für alle $d \in \mathbb{Z}$ mit $0 \leq d \leq e$ ein $x \in \mathbb{Z}^{\geq 1}$ mit $x \equiv 1 \pmod{p}$ und*

$$\binom{n}{p^d} = p^{e-d} m x.$$

Beweis. Es gilt

$$\binom{n}{p^d} = \frac{n}{p^d} \binom{n-1}{p^d-1} = p^{e-d} m \binom{n-1}{p^d-1}.$$

Wir setzen $x = \binom{n-1}{p^d-1}$, so daß $x \in \mathbb{Z}^{\geq 1}$ und $\binom{n}{p^d} = p^{e-d} m x$ gilt, und nur noch $x \equiv 1 \pmod{p}$ zu zeigen ist. Im folgenden schreiben wir die Indizes i mit $1 \leq i \leq p^d - 1$ in der Form $i = p^{e_i} x_i$ mit $x_i \not\equiv 0 \pmod{p}$ und $0 \leq e_i \leq d - 1$. Wir erhalten:

$$\begin{aligned} x &= \prod_{i=1}^{p^d-1} \frac{n-i}{p^d-i} = \prod_{i=1}^{p^d-1} \frac{p^e m - p^{e_i} x_i}{p^d - p^{e_i} x_i} = \prod_{i=1}^{p^d-1} \frac{p^{e-e_i} m - x_i}{p^{d-e_i} - x_i} \\ &= \frac{\lambda p + \alpha}{\mu p + \alpha} \end{aligned}$$

mit $\lambda, \mu, \alpha \in \mathbb{Z}$ und $\alpha \equiv \prod_{i=1}^{p^d-1} (-x_i) \pmod p$ wegen $e_i < d \leq e$. Es folgt $(\mu p + \alpha)x = \lambda p + \alpha$, also $\alpha x \equiv \alpha \pmod p$ und wegen $\alpha \not\equiv 0 \pmod p$ schließlich $x \equiv 1 \pmod p$. \square

1.64 Definition. Sei G eine Gruppe und p eine Primzahl. Dann heißt G eine p -Gruppe, wenn $\#G = p^e$ mit $e \in \mathbb{Z}^{\geq 0}$ ist.

Sei U eine weitere Gruppe. Dann heißt U eine p -Untergruppe von G , wenn U eine Untergruppe von G und eine p -Gruppe ist. Ferner heißt U eine p -Sylowgruppe von G , wenn U eine p -Untergruppe von G ist und $(G : U) \not\equiv 0 \pmod p$ gilt.

1.65 Satz (1. Satz von Sylow). *Sei G eine endliche Gruppe mit $\#G = p^e m$ und $m \not\equiv 0 \pmod p$ für eine Primzahl p . Sei $N(d) = \#\{U \mid U \leq G \text{ und } \#U = p^d\}$.*

Dann gilt $N(d) \equiv 1 \pmod p$ für $0 \leq d \leq e$. Speziell gibt es daher für jedes solche d mindestens eine p -Untergruppe U von G mit $\#U = p^d$.

Beweis. Sei $X = \{T \mid T \subseteq G \text{ und } \#T = p^d\}$. Wir zeigen unten, daß

$$\#X = \lambda p^{e-d+1} + N(d)p^{e-d}m \quad (1.66)$$

für ein $\lambda \in \mathbb{Z}$ gilt. Nach Lemma 1.63 gilt andererseits $\#X = \binom{\#G}{p^d} = p^{e-d}mx$ mit $x \equiv 1 \pmod p$. Division von (1.66) durch p^{e-d} liefert damit $mx = \lambda p + N(d)m$, also $N(d) \equiv x \equiv 1 \pmod p$ wie behauptet.

Zum Beweis von (1.66) definieren wir $G_T = \{g \in G \mid gT = T\}$. Es ist sofort einsichtig, daß G_T eine Untergruppe von G ist. Wir führen jetzt mehrere Überlegungen durch, die sich zum vollständigen Beweis zusammensetzen.

Überlegung 1: Für jedes $T \in X$ und $g \in T$ gilt $G_T g \subseteq T$ und $\#G_T = \#G_T g$. Wegen $\#T = p^d \geq 1$ ergibt sich

$$\#G_T \leq p^d \text{ für alle } T \in X. \quad (1.67)$$

Überlegung 2: Aufgrund von (1.67) definieren die Mengen X_1 und X_2 mit

$$\begin{aligned} X_1 &= \{T \mid T \in X \text{ mit } \#G_T < p^d\}, \\ X_2 &= \{T \mid T \in X \text{ mit } \#G_T = p^d\} \end{aligned}$$

eine Partition von X . Im folgenden berechnen wir $\#X$ mittels

$$\#X = \#X_1 + \#X_2. \quad (1.68)$$

Überlegung 3: Wir wollen $\#X_2$ berechnen. Dazu klären wir, wann in (1.67) das Gleichheitszeichen steht: Für jede Untergruppe U von G mit $\#U = p^d$ gilt

$$\{T \mid T \in X \text{ mit } G_T = U\} = \{Ug \mid g \in G\}. \quad (1.69)$$

Zum Beweis der Inklusion \subseteq in (1.69) sei $g \in T$. Wegen $G_T g \subseteq T$ und $\#G_T g = \#G_T = p^d = \#T$ gilt $T = G_T g = Ug$. Zum Beweis der Inklusion \supseteq in (1.69) bemerken wir $Ug \in X$ wegen $\#U = p^d$, und $G_{Ug} = U$ wegen $hUg = Ug \Leftrightarrow h \in U$ für alle $h \in G$.

Für X_2 erhalten wir

$$\begin{aligned} X_2 &= \{T \mid T \in X \text{ mit } \#G_T = p^d\} \\ &= \dot{\cup}_{U \leq G, \#U = p^d} \{T \mid T \in X \text{ mit } G_T = U\} \\ &= \dot{\cup}_{U \leq G, \#U = p^d} \{Ug \mid g \in G\}, \end{aligned} \quad (1.70)$$

wobei die letzte Gleichung aus (1.69) folgt. Für $U \leq G$ mit $\#U = p^d$ gilt nun $\#\{Ug \mid g \in G\} = (G : U) = p^{e-d}m$. Damit ergibt sich

$$\begin{aligned} \#X_2 &= \sum_{U \leq G, \#U = p^d} \#\{Ug \mid g \in G\} = \sum_{U \leq G, \#U = p^d} p^{e-d}m \\ &= N(d)p^{e-d}m \end{aligned} \quad (1.71)$$

Überlegung 4: Wir wollen $\#X_1$ berechnen. Dazu definieren wir eine Operation \circ von G auf X durch $g \circ T = gT$. Damit gilt zunächst $G_T = \text{Stab}_G(T)$ per Definition. Für X_1 erhalten wir weiter

$$\begin{aligned} X_1 &= \{T \mid T \in X \text{ mit } \#\text{Stab}_G(T) < p^d\} \\ &= \{T \mid T \in X \text{ mit } p^{e-d+1} \mid (G : \text{Stab}_G(T))\} \\ &= \{T \mid T \in X \text{ mit } p^{e-d+1} \mid \#(G \circ T)\} \\ &= \dot{\cup} \{G \circ T \mid T \in X, p^{e-d+1} \mid \#(G \circ T)\} \end{aligned} \quad (1.72)$$

unter Verwendung von Theorem 1.59, (ii) in der dritten Gleichung. Nach (1.72) ist $\#X_1$ eine Summe von durch p^{e-d+1} teilbaren ganzen Zahlen und daher von der Form

$$\#X_1 = \lambda p^{e-d+1} \quad (1.73)$$

für ein $\lambda \in \mathbb{Z}$.

Schlußüberlegung: Aus (1.68), (1.71) und (1.73) erhalten wir schließlich (1.66) wie gewünscht. \square

1.74 Korollar. *Sei G eine endliche Gruppe.*

- (i) *Zu jedem Primteiler p von $\#G$ gibt es ein $g \in G$ mit $\text{ord}(g) = p$.*
- (ii) *Die Gruppe G ist genau dann eine p -Gruppe, wenn es für jedes $g \in G$ ein $r \in \mathbb{Z}$ mit $\text{ord}(g) = p^r$ gibt.*

Beweis. (i): Zunächst gibt es nach Satz 1.65 ein $U \leq G$ mit $\#U = p$. Dann ist U nach Satz 1.36 zyklisch. Für $g \in U$ mit $U = \langle g \rangle$ gilt dann $\text{ord}(g) = p$.

(ii): Die Implikation „ \Rightarrow “ folgt aus Satz 1.20. Für die Implikation „ \Leftarrow “ nehmen wir an, daß G keine p -Gruppe ist. Dann gibt es einen Primteiler $q \neq p$ von $\#G$ und nach (i) auch ein Element $g \in G$ mit $\text{ord}(g) = q$, im Widerspruch zur Annahme. \square

Korollar 1.74, (i) heißt auch Satz von Cauchy.

1.75 Lemma. *Sei G eine p -Gruppe. Ist X eine G -Menge, so gilt*

$$\#X \equiv \#\text{Fix}_G(X) \pmod{p}.$$

Beweis. Folgt aus Theorem 1.59, (iii) wegen $(G : \text{Stab}_G(x)) \equiv 0 \pmod{p}$ für $(G : \text{Stab}_G(x)) \neq 1$. \square

1.76 Satz (2. Satz von Sylow). *Sei G eine endliche Gruppe mit $\#G = p^e m$ und $m \not\equiv 0 \pmod{p}$ für eine Primzahl p .*

(i) *Jede p -Untergruppe von G ist in einer p -Sylowgruppe von G enthalten.*

(ii) *Je zwei p -Sylowgruppen von G sind konjugiert.*

(iii) *Die Anzahl der p -Sylowgruppen von G teilt m .*

Beweis. Sei $X = \{U \mid U \leq G \text{ mit } \#U = p^e\}$ die Menge der p -Sylowgruppen von G . Wir definieren eine Operation von G auf X durch Konjugation, also $g \circ U = gUg^{-1}$. Hier ist gUg^{-1} wegen $\#gUg^{-1} = \#U$ wieder eine p -Sylowgruppe von G .

Überlegung 1: Sei $P \in X$. Dann gilt $P \leq N_G(P)$ und $(G : P) = m \not\equiv 0 \pmod{p}$. Nach Theorem 1.59, (ii) und Lemma 1.62 folgt damit $\#(G \circ P) = (G : \text{Stab}_G(P)) = (G : N_G(P)) \mid (G : P) = m$. Wir erhalten $\#(G \circ P) \mid m$ für alle $P \in X$.

Überlegung 2: Für jedes $P \in X$ und jede p -Untergruppe H von G gibt es $g \in G$ mit $H \leq gPg^{-1}$. Zum Beweis dieser Aussage betrachten wir die Operation von H auf $G \circ P$ durch Konjugation. Aufgrund von Lemma 1.75 (angewendet mit $H = G$ und $X = G \circ P$) und $\#(G \circ P) \mid m$ wie eben bewiesen gilt $\#\text{Fix}_H(G \circ P) \equiv \#(G \circ P) \not\equiv 0 \pmod{p}$. Daher gibt es $Q \in G \circ P$ mit $hQh^{-1} = Q$ für alle $h \in H$. Also folgt $H \leq N_G(Q)$ und $QH \leq N_G(Q)$. Nun ist QH/Q eine p -Gruppe, da $QH/Q \cong H/Q \cap H$ gilt und $H/Q \cap H$ mit H eine p -Gruppe ist. Daher ist QH eine p -Gruppe und mit $Q \leq QH$ gilt $QH = Q$ aus Indexgründen. Daher folgt $H \leq Q$. Wegen $Q \in G \circ P$ gibt es $g \in G$ mit $Q = gPg^{-1}$, also auch $H \leq gPg^{-1}$, was zu beweisen war.

(i): Sei H eine p -Untergruppe von G . Nach Satz 1.65 gibt es eine p -Sylowgruppe P von G und X ist nicht leer. Nach der Überlegung 2 gibt es ein $g \in G$ mit $H \leq gPg^{-1}$, und gPg^{-1} ist ebenfalls eine p -Sylowgruppe von G .

(ii): Folgt aus Überlegung 2 mit H einer p -Sylowgruppe und aus Indexgründen.

(iii): Sei $P \in X$. Nach (ii) ist $G \circ P$ die Menge aller p -Sylowgruppen von G . Dann folgt (iii) aus $\#(G \circ P) | m$, was in Überlegung 1 bewiesen wurde. \square

1.13 Anwendungen auf endliche Gruppen

In diesem Abschnitt wenden wir die Ergebnisse der vorhergehenden Abschnitte exemplarisch zur Strukturbestimmung einiger endlicher Gruppen an, und zwar in Abhängigkeit der Primfaktorisation ihrer Ordnung.

Bisher wissen wir bereits das folgende: Für $\#G = 1$ gilt $G = \{1\}$, und für $\#G = p$ mit p Primzahl gilt $G \cong \mathbb{Z}/p\mathbb{Z}$. Im folgenden Satz wird der Fall $\#G = p^2$ geklärt.

1.77 Satz. *Sei G eine Gruppe.*

- (i) *Ist G eine p -Gruppe mit $G \neq 1$, so gilt $Z(G) \neq 1$.*
- (ii) *Ist $G/Z(G)$ zyklisch, so ist G abelsch.*
- (iii) *$(G : Z(G))$ ist keine Primzahl.*
- (iv) *Für $\#G = p^2$ ist G abelsch und es gilt $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Beweis. (i): Ist $X = G$ und operiert G durch Konjugation auf X , so ergibt sich $\#Z(G) = \#\text{Fix}_G(X) \equiv \#X \equiv 0 \pmod{p}$ nach Lemma 1.61 und nach Lemma 1.75. Es folgt $\#Z(G) \neq 1$.

(ii): Sei $h \in G$ mit $G/Z(G) = \langle hZ(G) \rangle$. Dann gibt es für alle $g_1, g_2 \in G$ ein $r_1, r_2 \in \mathbb{Z}$ und $z_1, z_2 \in Z(G)$ mit $g_1 = h^{r_1}z_1$ und $g_2 = h^{r_2}z_2$. Dann gilt $g_1g_2 = h^{r_1}z_1h^{r_2}z_2 = h^{r_1}h^{r_2}z_2z_1 = h^{r_2}h^{r_1}z_2z_1 = h^{r_2}z_2h^{r_1}z_1 = g_2g_1$.

(iii): Ist $(G : Z(G))$ Primzahl, so ist $G/Z(G)$ nach Satz 1.36 zyklisch, daher G abelsch und $Z(G) = G$, also $(G : Z(G)) = 1$, im Widerspruch zur Annahme.

(iv): Wegen $\#Z(G) \in \{p, p^2\}$ nach (i) gilt $\#Z(G) = p^2$ nach (iii), also ist $G = Z(G)$ abelsch und es ergibt sich eine der beiden Isomorphismen aufgrund von Satz 1.48. \square

Als nächstes betrachten wir den Fall $\#G = pq$ mit Primzahlen p, q und $p < q$.

1.78 Satz. *Sei G eine endliche Gruppe mit $G \neq 1$ und p der kleinste Primteiler von $\#G$. Ist U eine Untergruppe von G mit $(G : U) = p$, so ist U ein Normalteiler von G .*

Beweis. Es gilt $N_G(U) = U$ oder $N_G(U) = G$. Im zweiten Fall ist U aufgrund der Definition des Normalisators ein Normalteiler von G .

Sei also $N_G(U) = U$. Die Gruppe G operiere auf ihren Untergruppen mittels \circ durch Konjugation. Es gilt $N_G(U) = \text{Stab}_G(U)$ nach Lemma 1.62 und $\#(G \circ U) = (G : \text{Stab}_G(U)) = (G : N_G(U)) = (G : U) = p$ nach Satz 1.59, (ii). Sei $\phi : G \rightarrow S(G \circ U)$, $g \mapsto (x \mapsto g \circ x)$ die zu \circ gehörige Permutationdarstellung von G auf $G \circ U$. Es gilt $\ker(\phi) = \cap_{H \in G \circ U} \text{Stab}_G(H) \leq \text{Stab}_G(U) = U$. Weiter gilt $(G : \ker(\phi)) | \#S(G \circ U) = p!$ und $(G : \ker(\phi)) = (G : U)(U : \ker(\phi)) = p(U : \ker(\phi))$. Da $p!$ von p genau einmal geteilt wird, ergibt sich $(U : \ker(\phi)) | (p-1)!$. Da p der kleinste Primteiler von $\#G$ ist, folgt daraus $(U : \ker(\phi)) = 1$, also $U = \ker(\phi)$ und U ist ein Normalteiler von G . \square

1.79 Lemma. *Ist G zyklisch von Primzahlordnung p , so ist $\text{Aut}(G)$ zyklisch von der Ordnung $p-1$.*

Beweis. Der Beweis ist zwar einfach, verwendet aber Begriffe aus der Ringtheorie, die erst später eingeführt werden.

(Wir können $G = \mathbb{Z}/p\mathbb{Z}$ annehmen. Dann ist $\text{Aut}(G) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, der multiplikativen Gruppe des endlichen Körpers $\mathbb{Z}/p\mathbb{Z}$. Diese hat Ordnung $p-1$ und ist nach Satz 3.11 zyklisch.) \square

1.80 Satz. *Sei G eine Gruppe mit $\#G = pq$, wobei p, q Primzahlen mit $p < q$ sind. Für $q \not\equiv 1 \pmod{p}$ gilt*

$$G \cong \mathbb{Z}/pq\mathbb{Z}.$$

Für $q \equiv 1 \pmod{p}$ existiert ein nicht-trivialer Homomorphismus $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Damit gilt

$$\text{entweder } G \cong \mathbb{Z}/pq\mathbb{Z} \text{ oder } G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$$

Beweis. Sei P eine p -Sylowgruppe von G und Q eine q -Sylowgruppe von G , welche nach Satz 1.65 existieren. Es gilt $\#P = p$ und $\#Q = q$. Nach Satz 1.36 gilt ferner $P \cong \mathbb{Z}/p\mathbb{Z}$ und $Q \cong \mathbb{Z}/q\mathbb{Z}$ und beide Gruppen sind einfach.

Nach Satz 1.78 ist Q ein Normalteiler von G . Dies können wir auch mit Satz 1.65 und Satz 1.76 sehen: Ist n_q die Anzahl der q -Sylowgruppen, so gilt $n_q | p$ und $n_q = 1 + \lambda q$, also $\lambda = 0$ und $n_q = 1$ wegen $p < q$.

Wegen $Q \cap P = \{1\}$ aufgrund der teilerfremden Ordnungen folgt $G = QP$, denn QP ist semidirektes Produkt von Q und P und damit $\#QP = \#Q\#P = \#G$. Also ist G semidirektes Produkt von Q und P . Es gibt daher ein $\psi : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ mit $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z}$.

Für $q \not\equiv 1 \pmod{p}$ gilt $\gcd(\#(\mathbb{Z}/p\mathbb{Z}), \#\text{Aut}(\mathbb{Z}/q\mathbb{Z})) = \gcd(p, q-1) = 1$ nach Lemma 1.79 und es folgt $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ nach Satz 1.54, (i) und Satz 1.47.

Für $q \equiv 1 \pmod p$ existiert ϕ nach Lemma 1.79 und Satz 1.40. Dann gilt $\psi(\mathbb{Z}/p\mathbb{Z}) \subseteq \phi(\mathbb{Z}/p\mathbb{Z})$ aufgrund von Satz 1.40 (ii), da $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ nach Lemma 1.79 zyklisch und ϕ injektiv ist. Nach Satz 1.54, (ii) folgt $G \cong \mathbb{Z}/pq\mathbb{Z}$ wie zuvor oder $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$.

Schließlich gilt $\mathbb{Z}/pq\mathbb{Z} \not\cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$, denn $\mathbb{Z}/pq\mathbb{Z}$ ist abelsch und $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$ ist nicht abelsch, da ϕ nicht-trivial ist. \square

Wir betrachten jetzt Gruppen G der Ordnung $8 = 2^3$.

1.81 Lemma. *Sei G eine 2-Gruppe vom Exponenten 2. Dann ist G abelsch und es gilt $G \cong (\mathbb{Z}/2\mathbb{Z})^{\log_2(\#G)}$.*

Beweis. Seien $a, b \in G$. Dann gilt $a^{-1} = a$, $b^{-1} = b$ und $(ab)^{-1} = ab$. Es folgt $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, und G ist abelsch. Die Isomorphieaussage folgt aus Satz 1.48. \square

Wir bemerken, daß das Lemma für 3-Gruppen vom Exponenten 3 bereits für $\#G = 27$ falsch ist.

Seien $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ mit $i^2 = -1$. Wir definieren die *Quaternionengruppe* Q_8 als die durch a und b erzeugte Untergruppe von $\text{GL}_2(\mathbb{C})$.

1.82 Satz. *Die D_4 und die Q_8 sind bis auf Isomorphie die einzigen nicht abelschen Gruppen der Ordnung 8.*

Beweis. Hausaufgabe. \square

Für die Quaternionengruppe gibt man üblicherweise die Erzeuger i, j, k mit $i^2 = j^2 = k^2 = -1$ und $ij = k$, $jk = i$ und $ki = j$ anstelle von a und b an. Es gilt zum Beispiel $i = a$, $j = b$, $k = ab$.

Mit Ausnahme des Falls $\#G = 12$ haben wir damit alle Isomorphietypen von Gruppen G mit $\#G \leq 15$ bestimmt. Das Ergebnis ist in Abbildung 1.1 zusammengefaßt (wir schreiben dort $C_n = \mathbb{Z}/n\mathbb{Z}$).

Wie die obige Diskussion schon andeutet, ist der Fall $\#G = 2^r$ recht unangenehm. Für $\#G = 16$ gibt es zum Beispiel 14 Gruppen und für $\#G = 512$ bereits 10 494 213 Gruppen.

1.14 Weitere Themen

Wir wollen kurz auf einige weitere Themen in der Gruppentheorie eingehen.

#G	G
1	C_1
2	C_2
3	C_3
4	$C_4, C_2 \times C_2$
5	C_5
6	C_6, D_3
7	C_7
8	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, D_4, Q_8$
9	$C_9, C_3 \times C_3$
10	C_{10}, D_5
11	C_{11}
12	$C_{12}, C_2 \times C_6, D_6, A_4, \text{weitere Gruppe}$
13	C_{13}
14	C_{14}, D_7
15	C_{15}

Tabelle 1.1: Vertreter der Isomorphieklassen endlicher Gruppen

1.14.1 Gruppenerweiterungen

Gruppenerweiterungen sind eine Verallgemeinerung von semidirekten Produkten. Wir betrachten eine exakte Sequenz

$$1 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} U \rightarrow 1 \quad (1.83)$$

und nennen G eine Erweiterung von N und U mit den Strukturhomomorphismen i und π . Wir wollen Gruppenerweiterungen „strukturerhaltend“ vergleichen: Seien G_1 und G_2 Erweiterungen von N und U mit den Strukturhomomorphismen $i_j : N \rightarrow G_j$ und $\pi_j : G_j \rightarrow U$ für $1 \leq j \leq 2$. Ein Homomorphismus $\phi : G_1 \rightarrow G_2$ der Erweiterungen G_1 und G_2 ist ein Gruppenhomomorphismus $\phi : G_1 \rightarrow G_2$ mit $\phi \circ i_1 = i_2$ und $\pi_1 = \pi_2 \circ \phi$.

Der Erweiterungshomomorphismus ϕ ist ein (Erweiterungs)isomorphismus, wenn es einen Erweiterungshomomorphismus $\psi : G_2 \rightarrow G_1$ mit $\phi \circ \psi = \text{id}$ und $\psi \circ \phi = \text{id}$ gibt. Das ist genau dann der Fall, wenn ϕ als Gruppenhomomorphismus ein Isomorphismus ist.

Die Fragestellung ist nun, wie das Gruppengesetz einer Gruppenerweiterung G von N und U anhand der Strukturhomomorphismen i und π bestimmt werden kann und wie die Isomorphieklassen der Gruppenerweiterungen von N und U aussehen. Beschränken wir uns auf den Fall, daß (1.83) rechts zerfällt, so ist G

semidirektes Produkt von N und U und das Gruppengesetz auf G wird durch $\phi : U \rightarrow \text{Aut}(N)$ wie beschrieben gegeben.

Der allgemeine Fall in (1.83) ist komplizierter, aber im Prinzip ähnlich zum Fall eines semidirekten Produkts: Mit Hilfe zweier Abbildungen, die nur von N und U abhängen, definiert man ein Gruppengesetz auf $N \times U$, und auf diese Weise werden alle Gruppenerweiterungen G von N und U erhalten. Zwei solche Gruppenerweiterungen sind isomorph, wenn die zugehörigen Abbildungen eine (technische, aber konkrete) Bedingung erfüllen. Diese Aussagen sind Inhalt des *Satzes von Schreier* über Gruppenerweiterungen.

Der *Satz von Schur-Zassenhaus* sagt aus, daß die exakte Sequenz (1.83) für $\#G < \infty$ und $\text{gcd}\{\#N, \#U\} = 1$ rechts zerfällt. Darüberhinaus sind die möglichen Bilder von U in G konjugiert.

Ist N abelsch, so vereinfacht sich die Situation im Satz von Schreier etwas. In diesem Fall stehen die Isomorphieklassen der Erweiterungen von N und U in Bijektion zu einer abelschen Gruppe, die mit $H^2(U, N)$ bezeichnet wird (das ist eine Kohomologiegruppe).

Wir nennen (1.83) eine *zentrale* Erweiterung, wenn $i(N) \leq Z(G)$ gilt.

1.14.2 Kompositionsreihen

Eine Normalreihe ist eine Kette (oder Filtrierung) der Form

$$N_0 = 1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G. \quad (1.84)$$

Die Faktorgruppen N_{i+1}/N_i sind genau dann einfach, wenn sich zwischen N_i und N_{i+1} keine echte Zwischengruppe und Normalteiler von N_{i+1} einfügen läßt. Ist das der Fall und gilt $N_{i+1} \neq N_i$ für alle i , so ist die Normalreihe maximal und heißt Kompositionsreihe.

Der *Satz von Jordan Hölder* sagt aus, daß zwei solche Kompositionsreihen mit den Gliedern N_i und N'_i bis auf die Reihenfolge isomorphe Faktorgruppen N_{i+1}/N_i und N'_{i+1}/N'_i besitzen. Es gibt also eine Permutation π der Indizes mit $N_{i+1}/N_i \cong N'_{\pi(i)+1}/N'_{\pi(i)}$.

Man kann sich diese Aussage gut an dem Beispiel $\mathbb{Z}/n\mathbb{Z}$ mit $n = \prod_i p_i^{e_i}$ klar machen (beachte $q\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$). Der Satz von Jordan-Hölder liefert in diesem Fall die Eindeutigkeit der Primfaktorisation ganzer Zahlen.

1.14.3 Einfache Gruppen

Ausgehend von endlichen Gruppen N und U können wir mit Hilfe von Gruppenerweiterungen und dem Satz von Schreier bis auf Isomorphie jede endliche

Gruppe G mit (1.83) bestimmen. Ist umgekehrt eine endliche Gruppe G gegeben, so betrachten wir konkret einen Normalteiler N von G und die Faktorgruppe $U = G/N$. Interessant ist dies allerdings nur für $N \neq 1$. Wir können dabei N auch maximal wählen, so daß $U = G/N$ einfach ist.

Wenden wir dieses Verfahren iterativ auf N und so weiter an, so werden wir auf die Betrachtung von Kompositionsreihen geführt.

Die Bestimmung aller endlichen Gruppen kann damit durch die Betrachtung sukzessiver Gruppenerweiterungen mit einfachen U (Reihenfolge egal nach Jordan-Hölder) erfolgen. Die einfachen endlichen Gruppen können somit als einfachste Bausteine beliebiger endlicher Gruppen angesehen werden.

Die *Klassifikation der endlichen einfachen Gruppen* war von Mitte der 50er bis Mitte der 80er Jahre des letzten Jahrhunderts ein großes Problem, welches nun gelöst scheint. Man gibt eine Reihe von (Matrix)Gruppentypen an, welche bis auf Isomorphie alle erfassen. Der „Beweis“ ist ungefähr 15000 Seiten lang. Eine interessante Beschreibung findet sich unter

http://en.wikipedia.org/wiki/Classification_of_finite_simple_groups
http://en.wikipedia.org/wiki/List_of_finite_simple_groups

1.14.4 Auflösbare Gruppen

Eine endliche Gruppe heißt auflösbar, wenn sie eine Kompositionsreihe mit zyklischen Faktorgruppen (notwendigerweise von Primzahlordnung) besitzt. Eine auflösbare Gruppe setzt sich also aus den einfachsten einfachen Gruppen mittels Gruppenerweiterung zusammen.

Sei f ein Polynom über einem Körper K . Die Bedeutung auflösbarer Gruppen liegt in der Beschreibung der Lösungen $x \in K$ von $f(x) = 0$ in Form von Wurzelausdrücken wie bei der pq -Formel im quadratischen Fall (dies motiviert auch den Namen „auflösbar“, wird in der VL Algebra 2 behandelt).

Der *Satz von Feit-Thompson* besagt, daß jede endliche Gruppe mit ungerader Gruppenordnung auflösbar ist (ca. 300 Seiten lang, 1963).

Als Beispiel für einfache und auflösbare Gruppen betrachten wir Permutationsgruppen $S_n = S(\{1, \dots, n\})$ und die alternierenden Gruppen $A_n = \{g \in S_n \mid \text{sign}(g) = 1\}$.

1.85 Satz. *Die alternierende Gruppe A_n ist genau dann einfach und nicht abelsch, wenn $n \geq 5$ gilt.*

Die symmetrische Gruppe S_n ist genau dann nicht auflösbar, wenn $n \geq 5$ gilt.

Beweis. Der Beweis besteht im wesentlichen aus detaillierten Rechnungen und ist ansonsten nicht sonderlich erhellend. Siehe die Lehrbücher von Meyberg oder Fischer/Sacher. \square

Die *Kommutatorgruppe* von G ist $K(G) = \{aba^{-1}b^{-1} \mid a, b \in G\}$ und ist ein Normalteiler von G . Die *Abelianisierung* von G ist $G^{\text{ab}} = G/K(G)$. Dies ist eine abelsche Gruppe mit der folgenden Eigenschaft. Sei $\pi : G \rightarrow G^{\text{ab}}$ der kanonische Epimorphismus. Ist H eine abelsche Gruppe und $\phi : G \rightarrow H$ ein Homomorphismus, so gilt $\ker(\phi) \subseteq K(G)$ und nach Satz 1.31 gibt es ein eindeutig bestimmtes $\psi : G^{\text{ab}} \rightarrow H$ mit $\phi = \psi \circ \pi$.

Die *i-te Kommutatorgruppe* von G wird rekursiv definiert durch $K_0(G) = G$ und $K_i(G) = K(K_{i-1}(G))$. Es gilt der folgende Satz, der nicht schwer zu beweisen ist: Eine Gruppe G ist genau dann auflösbar, wenn es $n \in \mathbb{Z}$ mit $K_n(G) = 1$ gibt.

1.14.5 Freie Gruppen

Bei der Beschreibung der D_n gehen wir von Erzeugern s und d und gewissen Relationen zwischen den Erzeugern aus, konkret $s^2 = 1$, $d^n = 1$ und $dsds = 1$. Freie Gruppen formalisieren eine solche informelle Beschreibung.

Wir betrachten ein *Alphabet* X und endliche *Worte* $X^* = \cup_{n \in \mathbb{Z}_{\geq 0}} X^n$ bestehend aus *Zeichen* aus dem Alphabet X . Dann ist X^* bezüglich der Aneinanderhängung von Worten ein Monoid, wobei das neutrale Element durch das leere Wort $()$ gegeben wird. Der Monoid X^* heißt der von X erzeugte *freie Monoid*.

Für Gruppen benötigen wir noch Inverse. Seien X^{-1} eine zu X disjunkte Menge und $f : X \rightarrow X^{-1}$, $g : X^{-1} \rightarrow X$ Bijektionen. Wir schreiben auch $f(x) = x^{-1}$ und $g(y) = y^{-1}$.

Wir nennen ein Wort aus $(X \cup X^{-1})^*$ *reduziert*, wenn es kein Teilwort der Form xx^{-1} für ein $x \in X \cup X^{-1}$ enthält. Die Menge der reduzierten Worte sei mit $F(X)$ bezeichnet.

Wir definieren eine Reduktionabbildung $r : (X \cup X^{-1})^* \rightarrow F(X)$ wie folgt. Entferne aus $w \in (X \cup X^{-1})^*$ alle Teilworte der Form xx^{-1} . Wiederhole dies, bis keine solchen Teilworte mehr in w auftreten.

Man kann dann per Induktion zeigen, daß r eine wohldefinierte Abbildung $r : (X \cup X^{-1})^* \rightarrow F(X)$ ist, daß $r(vw) = r(r(v)r(w))$ für alle $v, w \in (X \cup X^{-1})^*$ gilt, und daß r mit der Monoidoperation in $(X \cup X^{-1})^*$ verträglich ist, daß also aus $r(v_1) = r(v_2)$ und $r(w_1) = r(w_2)$ auch $r(v_1w_1) = r(v_2w_2)$ für alle $v_1, v_2, w_1, w_2 \in (X \cup X^{-1})^*$ folgt.

Durch $v \circ w = r(vw)$ wird damit ein Gruppengesetz auf $F(X)$ definiert. Wir nennen $(F(X), \circ)$ zusammen mit der Inklusion $i : X \rightarrow F(X)$ die von X erzeugte *freie Gruppe*. Eine Gruppe G heißt *frei*, wenn $G \cong F(X)$ für eine Menge X gilt.

Es gilt die folgende universelle Eigenschaft für freie Gruppen: Ist G eine Gruppe und $j : X \rightarrow G$ eine Abbildung, so gibt es genau einen Homomorphismus $f : F(X) \rightarrow G$ mit $f \circ i = j$. Gilt $G = \langle j(X) \rangle$, so ist f ein Epimorphismus und es gilt $G \cong F(X)/\ker(f)$.

Sei $R \subseteq F(X)$. Dann heißt $G = F(X)/N_{F(X)}(R)$ die Gruppe mit den Erzeugern X und den Relationen R (die durch X und R präsentierte Gruppe). Eine Gruppe heißt endlich präsentierbar, wenn es eine Menge X und $R \subseteq F(X)$ mit $\#X < \infty$, $\#R < \infty$ und $G \cong F(X)/N_{F(X)}(R)$ gibt.

Als Beispiel betrachten wir $X = \{s, d\}$ und $R = \{s^2, d^3, dsds\}$. Dies liefert $D_3 \cong F(X)/N_{F(X)}(R)$.

Für eine endliche Menge X und $R = \{xyx^{-1}y^{-1} \mid x, y \in X\}$ erhalten wir die von X erzeugte freie abelsche Gruppe $F(X)/N_{F(X)}(R) \cong \mathbb{Z}^{\#X}$.

Das *Wortproblem* für $F(X)$ und R besteht darin, für gegebenes $w \in F(X)$ zu entscheiden, ob $w \in N_{F(X)}(R)$ gilt. Hierfür gibt es keinen allgemeingültigen Algorithmus, das Wortproblem ist *unentscheidbar*.

Für eine Untergruppe U einer freien Gruppe gilt der *Untergruppensatz von Schreier*, daß U ebenfalls frei ist.

Kapitel 2

Ringe I

In diesem Kapitel wird die Ringtheorie einführend behandelt.

2.1 Grundlagen

In diesem Abschnitt und den folgenden Abschnitten gehen wir ganz analog wie bei Gruppen bezüglich Untergruppen, Homomorphismen, Normalteiler, Homomorphiesatz und den Isomorphiesätzen vor.

Ein *Halbring* R ist eine Menge R mit zwei Verknüpfungen $+$ und \cdot , so daß $(R, +)$ eine abelsche Gruppe und (R, \cdot) eine Halbgruppe ist und die Distributivgesetze $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$ gelten.

Ist (R, \cdot) ein Monoid, so heißt R ein *Ring*.

Ist (R, \cdot) kommutativ, so heißt R *kommutativ*.

Die Konventionen aus Kapitel 1, Abschnitt 1.2 gelten auch hier für $(R, +)$ und (R, \cdot) . Speziell schreiben wir 0 für das eindeutig bestimmte neutrale Element von $(R, +)$ (genannt das Nullelement) und 1 für das eindeutig bestimmte neutrale Element von (R, \cdot) (genannt das Einselement), sofern R ein Ring ist. Auch lassen wir \cdot in den meisten Fällen wieder aus.

Aufgrund des Distributivgesetzes gilt $0x = x0 = 0$ für alle $x \in R$. Denn es gilt beispielsweise $0x = (0 + 0)x = 0x + 0x$, und mit der additiven Kürzungsregel folgt $0 = 0x$ für alle $x \in R$.

Der *Nullring* $R = \{0\}$ ist ein Ring mit Einselement $1 = 0$. Gilt umgekehrt für einen Ring $1 = 0$, so ist R bereits der Nullring, denn für $x \in R$ gilt $x = 1x = 0x = 0$. Ist R ungleich dem Nullring, so gilt also $1 \neq 0$.

Sei R ein Ring. Ein Element $x \in R$ heißt *invertierbar* mit *Inversem* $y \in R$, wenn x in (R, \cdot) invertierbar mit Inversem y ist. Wir erinnern an Lemma 1.2 und schreiben wieder $y = x^{-1}$. Das Nullelement 0 von R ist dann und nur dann

invertierbar, wenn R der Nullring ist. Ein invertierbares Element von R heißt auch eine *Einheit* von R . Die Menge der Einheiten von R zusammen mit der Verknüpfung \cdot bildet eine Gruppe, die *Einheitengruppe* R^\times von R .

Ein Ring mit $1 \neq 0$ heißt *Schiefkörper*, wenn $R^\times = R \setminus \{0\}$ gilt. Ist R kommutativ, so heißt R *Körper*.

2.1 Beispiel. Wir geben ein paar grundlegende Beispiele für Ringe an, an denen man die nachfolgenden Definition und Sätze ausprobieren kann. Weitere Ringe werden später definiert.

Der wohl grundlegendste Ring ist \mathbb{Z} . Dies ist ein kommutativer Ring, in dem nur die Elemente $-1, 1$ invertierbar sind. Weitere Beispiele für Ringe sind die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Diese Ringe sind ebenfalls kommutativ, nun ist aber jedes Element $\neq 0$ invertierbar.

Die Menge der quadratischen $n \times n$ Matrizen $\mathbb{R}^{n \times n}$ bildet mit der Matrixaddition und Matrixmultiplikation einen Ring. Die Menge der Endomorphismen $\text{End}(V)$ eines n -dimensionalen Vektorraums V bildet mit der punktweisen Addition und der Hintereinanderausführung von Funktionen einen Ring, den Endomorphismenring von V . Analog bildet die Menge der Endomorphismen einer abelschen Gruppe G einen Ring. Diese Ringe sind im allgemeinen nicht kommutativ.

Eine weitere wichtige Klasse von kommutativen Ringen sind die Polynomringe, die erst später formal eingeführt werden. Eine informelle, aber eigentlich fast ausreichende Definition geht wie folgt. Man wählt sich einen kommutativen Ring R und Variablen (Unbekannte) x_1, \dots, x_n . Der Polynomring $R[x_1, \dots, x_n]$ in x_1, \dots, x_n über R besteht dann aus allen Polynomen in den x_1, \dots, x_n mit Koeffizienten aus R . Diese sind formale Ausdrücke der Form $\sum_{i=1}^r a_i x_1^{e_{i,1}} \cdots x_n^{e_{i,n}}$ für $r \in \mathbb{Z}^{\geq 0}$, $a_i \in R$ und $e_{i,j} \in \mathbb{Z}^{\geq 0}$. Die Addition, Multiplikation sowie der Test auf Gleichheit werden so ausgeführt, wie man es beim Rechnen mit Variablen gewöhnt ist.

In der Geometrie treten Ringe der folgenden Art auf. Sei X eine Menge und R ein Ring. Die Menge der Funktionen $R^X = \{f \mid f : X \rightarrow R\}$ bildet mit der punktweisen Addition und Multiplikation einen Ring. Je nach Bereich stellt man weitere Anforderung an die Funktionen wie zum Beispiel Stetigkeit oder Differenzierbarkeit.

Seien R und S Halbringe (mit den Verknüpfungen $+$ und \cdot , die im allgemeinen für R und S verschieden sind, die wir aber mit denselben Symbolen bezeichnen, da jeweils klar sein wird, welche Verknüpfung gemeint ist, ebenso für die Null- und Einselemente). Ein *Homomorphismus* der Halbringe R und S wird durch eine Abbildung $f : R \rightarrow S$ gegeben, für die $f : (R, +) \rightarrow (S, +)$ und $f : (R, \cdot) \rightarrow (S, \cdot)$

Homomorphismen sind (in anderen Worten, f ist additiv und multiplikativ, es gilt $f(x + y) = f(x) + f(y)$ und $f(xy) = f(x)f(y)$ für alle $x, y \in R$). Analog wie bei Halbgruppen werden wieder *Monomorphismen*, *Epimorphismen*, *Endomorphismen*, *Isomorphismen* und *Automorphismen* definiert.

Ist $f : R \rightarrow S$ ein Homomorphismus der Halbringe R und S , so gilt $f(0) = 0$ nach Lemma 1.6 beziehungsweise Lemma 1.27, (i). Sind R und S Ringe, so gilt dann allerdings nicht unbedingt $f(1) = 1$, wie das folgende Beispiel zeigt.

2.2 Beispiel. Definieren wir $G = (\mathbb{R}, +, \cdot)$, $H = (\mathbb{R}^{2 \times 2}, +, \cdot)$ und $f : G \rightarrow H$ wie in Beispiel 1.5, so erhalten wir einen Ringhomomorphismus f mit $f(1) \neq 1$.

Durch koordinatenweise Addition und Multiplikation wird $\mathbb{Z} \times \mathbb{Z}$ zu einem Ring mit Einselement $1 = (1, 1)$. Definieren wir $f : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ durch $x \mapsto (x, 0)$, so ist f ein Ringhomomorphismus mit $f(1) = (1, 0) \neq 1$.

Unter einem *Homomorphismus* der Ringe R und S verstehen wir daher einen Homomorphismus f der Halbringe R und S mit $f(1) = 1$.

In der Literatur herrscht bei den Definitionen von Halbring, Ring und den entsprechenden Homomorphismen allerdings kein Standard. Mitunter wird Halbring auch Ring und ein Ring auch Ring mit Einselement genannt. Man muß daher stets nachschauen, was der Autor eines Texts unter einem Ring und unter Homomorphismen eines Rings genau versteht.

Seien R, S Halbringe mit $R \subseteq S$. Ist die Inklusionsabbildung $R \rightarrow S$ ein Homomorphismus der Halbringe R und S , so nennen wir R einen *Unterhalbring* von S . Umgekehrt nennen wir S auch *Erweiterungshalbring* von R und das Paar (R, S) eine *Halbringerweiterung*, in Zeichen S/R .

Seien R, S Ringe mit $R \subseteq S$. Ist die Inklusionsabbildung $R \rightarrow S$ ein Homomorphismus der Ringe R und S , so nennen wir R einen *Unterring* von S . Umgekehrt nennen wir S auch *Erweiterungsring* von R und das Paar (R, S) eine *Ringerweiterung*, in Zeichen S/R . Manche Autoren nennen S/R auch eine *unitäre Ringerweiterung*, denn hier stimmen die Einselemente von R und S per Definition überein.

2.3 Lemma. *Seien R, S Ringe und $\phi : R \rightarrow S$ ein Homomorphismus. Dann gilt $\phi(R^\times) \subseteq S^\times$ und $\phi(x^{-1}) = \phi(x)^{-1}$ für alle $x \in R^\times$.*

Beweis. Folgt aus Lemma 1.6. □

Homomorphismen von Schiefkörpern und Körpern sind Homomorphismen der unterliegenden Ringe (hier genügte auch Halbringe zu fordern, da Einselemente automatisch auf Einselemente abgebildet werden). Entsprechend werden *Teil(schief)körper*, *Erweiterung(schief)körper* und *(Schief)Körpererweiterung* definiert.

2.2 Ideale und Homomorphismen

Ideale spielen für Ringe die gleiche Rolle, die Normalteiler für Gruppen einnehmen.

Sei R ein Halbring und $A, B \subseteq R$. Dann definieren wir $AB = \{\sum_{i=1}^n a_i b_i \mid n \in \mathbb{Z}^{\geq 0} \text{ und } a_i \in A, b_i \in B \text{ für } 1 \leq i \leq n\}$. Weiter definieren wir $aB = \{a\}B$ und $Ab = A\{b\}$ für $a \in A$ und $b \in B$.

2.4 Definition. Sei R ein Halbring und I eine Untergruppe von $(R, +)$. Gilt $RI \subseteq I$, so heißt I ein Linksideal von R . Gilt $IR \subseteq I$, so heißt I ein Rechtsideal. Ist I ein Links- und Rechtsideal von R , so heißt I ein Ideal von R . Die Menge der Ideale von R wird mit $\mathfrak{I}(R)$ bezeichnet.

Wegen $II \subseteq RI \subseteq I$ sind Linksideale I Unterhalbringe von R . Das gleiche gilt für Rechtsideale. Beispiel für Ideale sind $I = \{0\}$ und $I = R$, wobei wir $I = R$ das *triviale Ideal* von R nennen. Ist R ein Ring, so sind Ideale I im allgemeinen keine Unterringe von R , denn im allgemeinen gilt nicht mehr $1 \in I$. Als Beispiel betrachten wir $R = \mathbb{Z}$ und $I = 3\mathbb{Z}$.

Ist R ein Ring, so impliziert die Bedingung $RIR \subseteq I$ bereits, daß I eine Untergruppe von $(R, +)$ ist. Ist R kommutativ, so genügt hierfür die Bedingung $RI \subseteq I$. In der Definition eines Ideals brauchen wir für Ringe daher nicht vorauszusetzen, daß I eine additive Untergruppe von R ist.

Sei R ein Halbring und $M \subseteq R$. Wir definieren das von M erzeugte Ideal (M) als $(M) = \bigcap_I I$, wobei der Schnitt über Ideale I von R mit $I \supseteq M$ geht. Es gilt $(M) = RMR + RM + MR + \langle M \rangle$, wobei $\langle M \rangle$ die von M erzeugte additive Gruppe bezeichnet. Ist R ein Ring, so vereinfacht sich dieser Ausdruck zu $(M) = RMR$. Ist R kommutativ, so erhalten wir $(M) = RM + \langle M \rangle$. Ist R ein kommutativer Ring, so gilt schließlich $(M) = RM$. Zum Beweis dieser Aussagen stellt man fest, daß die definierten Mengen Ideale sind und auch in jedem Ideal J mit $M \subseteq J$ enthalten sind.

Sei $f : R \rightarrow S$ ein Homomorphismus der Halbringe R und S . Dann sind *Kern* und *Bild* von f definiert als $\ker(f) = \{x \in R \mid f(x) = 0\}$ und $\text{im}(f) = f(R) = \{f(x) \mid x \in R\}$.

Es folgen ein paar elementare Eigenschaften von Idealen und Homomorphismen. Die folgenden Lemmata gelten sowohl für Halbringe als auch für Ringe.

2.5 Lemma. Sei $f : R \rightarrow S$ ein Homomorphismus der (Halb)Ringe R und S .

- (i) Urbild und Bild von Unter(halb)ringen von R und S bezüglich f sind wieder Unter(halb)ringe.
- (ii) Ist J ein Ideal von S , so ist $f^{-1}(J)$ ein Ideal von R . Ist f ein Epimorphismus und I ein Ideal von R , so ist $f(I)$ ein Ideal von S .

- (iii) $\ker(f)$ ist ein Ideal von R .
- (iv) Sind I, J Ideale von R , so sind auch $I + J = \{x + y \mid x \in I, y \in J\}$, IJ und $I \cap J$ Ideale von R .
- (v) Ist I Ideal von R und $I \cap R^\times \neq \emptyset$, so folgt $I = R$.
- (vi) Ist U ein Unter(halb)ring von R und I ein Ideal von R , so ist $U + I$ ein Unter(halb)ring von R .

Beweis. Hausaufgabe. □

2.6 Lemma. Sei $f : R \rightarrow S$ ein Epimorphismus der Halbringe R und S . Dann liefert $U \mapsto f(U)$ eine inklusionserhaltende Bijektion der Menge der Unter(halb)ringe U von R mit $U \supseteq \ker(f)$ auf die Menge der Unter(halb)ringe von S . Hierbei ist U genau dann ein Ideal von R , wenn $f(U)$ ein Ideal von S ist.

Beweis. Hausaufgabe. □

Sei $f : R \rightarrow S$ ein Ringhomomorphismus. Es ist eine übliche Operation, Ideale von S zu Idealen von R und umgekehrt zu machen. Dies geschieht mit den Abbildungen $f^* : \mathfrak{I}(S) \rightarrow \mathfrak{I}(R)$ durch $J \mapsto f^{-1}(J)$ und $f_* : \mathfrak{I}(R) \rightarrow \mathfrak{I}(S)$ durch $I \mapsto Sf(I)S$.

2.7 Satz. Die Abbildungen f^* und f_* besitzen die folgenden Eigenschaften.

- (i) f_* erhält Summen und Produkte von Idealen.
- (ii) Ist f ein Epimorphismus, so gilt $f_*(f^*(J)) = J$ und $f_*(I) = f(I)$. Ferner erhält f^* Summen, Produkte und Schnitte von Idealen.

Beweis. Hausaufgabe. □

2.3 Faktorringer

Wir kommen zur Konstruktion des Faktorrings. Sei R ein Halbring und I ein Ideal von R . Wir definieren zunächst die abelsche Gruppe $R/I = (R, +)/(I, +)$ als Faktorgruppe der abelschen Gruppen $(R, +)$ und $(I, +)$. Dann führen wir auf R/I eine Multiplikation \cdot durch $(x + I) \cdot (y + I) = (xy + I)$ ein.

2.8 Satz. Die abelsche Gruppe R/I zusammen mit \cdot ist ein Halbring. Der kanonische Epimorphismus $x \mapsto x + I$ der additiven Gruppen von R und R/I definiert einen Epimorphismus $\pi : R \rightarrow R/I$ der Halbringe R und R/I .

Ist R ein Ring, so ist R/I ebenfalls ein Ring und π ein Ringhomomorphismus.

Beweis. Zum Nachweis der Halbringeigenschaft von R/I ist nur die Wohldefiniertheit von \cdot zu zeigen. Die Assoziativität und Distributivität folgen dann sofort aus den entsprechenden Eigenschaften der Multiplikation von R .

Seien $x_1, x_2, y_1, y_2 \in R$ mit $x_1 + I = x_2 + I$ und $y_1 + I = y_2 + I$. Dann gibt es $u, v \in I$ mit $x_2 = x_1 + u$ und $y_2 = y_1 + v$. Es folgt $x_2 y_2 + I = (x_1 + u)(y_1 + v) + I = x_1 y_1 + u y_1 + x_1 v + uv + I = x_1 y_1 + I$, wegen $u y_1, x_1 v, uv \in I$ aufgrund der Idealeigenschaft von I .

Die Epimorphismeigenschaft von π ergibt sich direkt aus der Definition der Multiplikation \cdot von R/I .

Ist R ein Ring, so ist auch R/I ein Ring und π ein Ringhomomorphismus, denn das Einselement von R/I ist $1 + I$ und es gilt $\pi(1) = 1 + I$. \square

Wir nennen R/I den *Faktorring* oder auch *Restklassenring* von R nach I und $\pi : R \rightarrow R/I$ den *kanonischen Epimorphismus*. Ist R kommutativ, so ist auch R/I kommutativ.

Wir führen die allgemeine *modulo-Schreibweise* ein: Für $x, y \in R$ schreiben $x \equiv y \pmod{I}$ genau dann, wenn $x - y \in I$ gilt.

Aus Lemma 2.5, (iii) und Satz 2.8 erhalten wir, daß Ideale und Kerne im Prinzip das gleiche sind.

Die folgenden Sätze gelten sowohl für Halbringe als auch für Ringe.

2.9 Satz. Sei $\phi : R \rightarrow S$ ein Homomorphismus der (Halb)Ringe S und R und I ein Ideal von R mit $I \subseteq \ker(\phi)$. Sei

$$\pi : R \rightarrow R/I$$

der kanonische Epimorphismus. Dann gibt es genau einen Homomorphismus

$$\psi : R/I \rightarrow S$$

mit $\psi \circ \pi = \phi$. Ferner gilt $\psi(R/I) = \phi(R)$ und $\ker(\psi) = \ker(\phi) + I$.

Beweis. Der Satz gilt für die unterliegenden abelschen Gruppen von R , S und R/I . Die Homomorphieeigenschaft ergibt sich aus der Multiplikativität von ϕ und ψ (wie im Beweis von Satz 1.31) sowie $\phi(1) = 1$ und $\pi(1) = 1$ im Fall, daß R und S Ringe sind. \square

2.10 Korollar. Sei $\phi : R \rightarrow S$ ein Homomorphismus der (Halb)Ringe R und S . Dann gilt

$$R/\ker(\phi) \cong \phi(R)$$

unter $x + \ker(\phi) \mapsto \phi(x)$.

Korollar 2.10 zeigt, daß die Betrachtung beliebiger Epimorphismen $R \rightarrow S$ und die Betrachtung kanonischer Epimorphismen $R \rightarrow R/N$ bis auf Isomorphie das gleiche ist.

2.11 Satz (Erster Isomorphiesatz). *Sei R ein (Halb)Ring, U ein Unter(halb)ring von R und I ein Ideal von R . Dann gilt*

$$(U + I)/I \cong U/(U \cap I).$$

Speziell ist $U + I$ ein Unter(halb)ring von R und $U \cap I$ ein Ideal von U .

Beweis. Folgt aus Satz 2.9 analog wie im Gruppenfall. \square

2.12 Satz (Zweiter Isomorphiesatz). *Seien R ein (Halb)Ring und I, J Ideale von R mit $I \subseteq J$. Dann ist J/I ein Ideal von R/I und es gilt*

$$(R/I)/(J/I) \cong R/J.$$

Beweis. Folgt aus Satz 2.9 analog wie im Gruppenfall. \square

2.13 Beispiel. Bezüglich der vertreterweisen Addition und Multiplikation wird $\mathbb{Z}/n\mathbb{Z}$ ein Ring. Für $a \in \mathbb{Z}$ und $n \in \mathbb{Z}^{\geq 1}$ sei $a = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$. Wir definieren $a \bmod n = r$. Damit können wir auch auf $M = \{0, \dots, n-1\}$ eine Addition durch $x \oplus y = (x + y) \bmod n$ und Multiplikation durch $x \odot y = (xy) \bmod n$ definieren. Die Abbildung $\phi : M \rightarrow \mathbb{Z}/n\mathbb{Z}$, $x \mapsto x + n\mathbb{Z}$ ist dann ein Ringisomorphismus.

2.4 Nullteiler

Wir untersuchen nun die nicht invertierbaren Elemente eines Rings etwas genauer.

Sei R ein Ring. Sind $a, b \in R$ mit $a \neq 0$, $b \neq 0$ und $ab = 0$, so heißen a (*linker*) und b (*rechter*) *Nullteiler* von R . Ist $a \in R$ weder ein linker noch ein rechter Nullteiler, so nennen wir a ein *reguläres Element* von R . Der Ring R heißt *nullteilerfrei*, wenn R keine Nullteiler besitzt bzw. wenn jedes Element regulär ist. Ist $a \in R$ und $n \in \mathbb{Z}^{\geq 0}$ mit $a^n = 0$, so heißt a *nilpotent*. Für einen kommutativen Ring R definieren wir das (*Nil*-)Radikal von R als $\text{Rad}(R) = \{x \in R \mid x \text{ ist nilpotent}\}$. Ist $\text{Rad}(R) = \{0\}$, so heißt R *reduziert*.

Es folgen einfache Eigenschaften von Nullteilern und des Radikals von R .

2.14 Lemma. *Sei R ein Ring.*

- (i) *Für jedes $a \in R \setminus \{0\}$ gilt: Die Abbildungen $R \rightarrow R$, $x \mapsto ax$ und $R \rightarrow R$, $x \mapsto xa$ sind genau dann injektiv, wenn a kein Nullteiler ist.*

- (ii) Nullteiler sind keine Einheiten. Sind $a, b \in R$ keine Nullteiler, so ist auch ab kein Nullteiler. Der Ring R ist genau dann nullteilerfrei, wenn $R \setminus \{0\}$ bezüglich \cdot eine Halbgruppe ist.
- (iii) Nilpotente Elemente ungleich Null sind Nullteiler. Für R kommutativ ist $\text{Rad}(R)$ ein Ideal von R .

Beweis. (i): Sind die Abbildungen injektiv, so gilt $ax = 0 \Rightarrow x = 0$ und $xa = 0 \Rightarrow x = 0$ für beliebiges $x \in R$, also ist a kein Nullteiler. Ist umgekehrt a kein Nullteiler, so gilt $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$ für beliebige $x, y \in R$, wegen $a \neq 0$. Analog für $xa = ya$. Also sind die Abbildungen injektiv.

(ii): Sei $a \in R^\times$. Für $b \in R$ folgt aus $ab = 0$, daß $a^{-1}(ab) = (a^{-1}a)b = 0$ ist. Also ist a kein linker Nullteiler. Analog für $ba = 0$ und a ist auch kein rechter Nullteiler.

Seien $a, b \in R$ beide keine Nullteiler. Für $a = 0$ oder $b = 0$ gilt $ab = 0$, und ab ist kein Nullteiler. Für $a \neq 0$ und $b \neq 0$ sind die Abbildungen aus (i) und ihre Hintereinanderausführungen $x \mapsto (ab)x$, $x \mapsto x(ab)$ injektiv. Folglich ist ab kein Nullteiler.

Die letzte Aussage ist nur eine Umformulierung der Definition eines Nullteilers und der zweiten Aussage.

(iii): Sei $x \in \text{Rad}(R)$, $x \neq 0$. Sei $n \in \mathbb{Z}^{\geq 0}$ minimal mit $x^n = 0$. Es gilt $n \geq 2$. Dann folgt $x^{n-1}x = xx^{n-1} = 0$ mit $x^{n-1} \neq 0$, also ist x linker und rechter Nullteiler. Für die Idealeigenschaft siehe Hausaufgaben. \square

2.15 Beispiel. Sei $R = \mathbb{Z}$. Es gibt keine nilpotenten Elemente außer 0. Es gibt keine Nullteiler.

2.16 Beispiel. Sei $n \in \mathbb{Z}^{\geq 1}$ und $R = \mathbb{Z}/n\mathbb{Z}$. Sei $a \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod{n}$. Es gilt daher $a + n\mathbb{Z} \neq 0$ in R . Sei $d = \text{gcd}(a, n)$.

Für $d > 1$ ist a ein Nullteiler von R . Denn mit $b = n/d$ gilt $b \not\equiv 0 \pmod{n}$, also $b + n\mathbb{Z} \neq 0$ und $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 0$ wegen $ab \equiv 0 \pmod{n}$.

Für $d = 1$ ist a eine Einheit von R . Denn aus $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 0$ folgt $ab \equiv 0 \pmod{n}$, dann $b \equiv 0 \pmod{n}$ wegen $d = 1$ und damit $b + n\mathbb{Z} = 0$. Daher ist $x \mapsto (a + n\mathbb{Z})x$ nach Lemma 2.14, (i) injektiv und wegen $\#(\mathbb{Z}/n\mathbb{Z}) < \infty$ auch surjektiv. Es gibt also ein $x = \lambda + n\mathbb{Z} \in R$ mit $(a + n\mathbb{Z})x = \lambda a + n\mathbb{Z} = 1 + n\mathbb{Z} = 1$. Daher ist a invertierbar.

Die letzte Aussage zeigt, daß es zu $a, n \in \mathbb{Z}$ mit $\text{gcd}(a, n) = 1$ ganze Zahlen $\lambda, \mu \in \mathbb{Z}$ mit $\lambda a + \mu n = 1$ gibt. Dies ist auch die Aussage des Satzes von Bezout beziehungsweise die Ausgabe des erweiterten euklidischen Algorithmus, wobei allgemeiner $\lambda a + \mu n = \text{gcd}(a, n)$ erhalten werden kann.

Indem wir umgekehrt $\lambda a + \mu n = 1$ modulo n betrachten, sehen wir, daß $\lambda + n\mathbb{Z}$ das Inverse von $a + n\mathbb{Z}$ ist. Die Bedeutung des erweiterten euklidischen Algorithmus liegt darin, daß λ, μ damit konkret ausgerechnet werden können.

Aus diesen Überlegungen folgt $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}, \gcd(a, n) = 1\}$ und $\#(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)$.

Die Elemente aus $\mathbb{Z}/n\mathbb{Z}$ sind für $n \neq 0$ also entweder Null, Einheiten oder Nullteiler. In \mathbb{Z} gibt es darüberhinaus Elemente, die weder Null, Einheiten oder Nullteiler sind.

2.17 Beispiel. Sei p eine Primzahl. Da $\gcd(a, p) = 1$ für jedes $a \in \mathbb{Z}$ mit $a \not\equiv 0 \pmod{p}$ gilt, sind alle Elemente ungleich Null von $\mathbb{Z}/p\mathbb{Z}$ invertierbar und $\mathbb{Z}/p\mathbb{Z}$ daher ein Körper. Für eine Primzahl p heißt \mathbb{F}_p der *endliche Körper* mit p Elementen.

2.18 Beispiel. Sei $R = K^{n \times n}$ für $K = \mathbb{Q}$ oder $K = \mathbb{R}$ etc. Obere Dreiecksmatrizen $A \in K^{n \times n}$ mit 0 auf der Diagonalen sind nilpotent (denn das charakteristische Polynom einer solchen Matrix A ist x^n , und nach dem Satz von Cayley-Hamilton gilt $A^n = 0$). Matrizen $A \in K^{n \times n}$ mit $\det(A) \neq 0$ sind Einheiten (invertierbar, denn die inverse Matrix existiert). Matrizen $A \in K^{n \times n}$ mit $\det(A) = 0$ sind Nullteiler (wähle $v \in K^n$, $v \neq 0$ mit $Av = 0$ und setze $B = (v, \dots, v) \in K^{n \times n}$. Dann gilt $AB = 0$).

Wir erweitern die Definition des Radikals wie folgt. Ist I ein Ideal des kommutativen Rings R und $\pi_I : R \rightarrow R/I$ der kanonische Epimorphismus, so setzen wir $\text{Rad}(I) = \pi_I^{-1}(\text{Rad}(R/I)) = \{x \in R \mid \exists n \geq 1 : x^n \in I\}$. Diese Definition paßt formal nicht zur vorigen Definition, das Radikal von R ist gleich dem Radikal des Nullideals von R (und nicht gleich dem Radikal des trivialen Ideals R). Man muß also das Radikal eines Rings und das Radikal eines Ideals unterscheiden.

2.19 Lemma. Sei $f : R \rightarrow S$ ein Homomorphismus der Ringe R und S und seien I ein Ideal von R und J ein Ideal von S . Es gilt $f^{-1}(\text{Rad}(J)) = \text{Rad}(f^{-1}(J))$. Ist f surjektiv, so gilt auch $f(\text{Rad}(I)) = \text{Rad}(f(I))$ für $I \supseteq \ker(f)$.

Beweis. Für $x \in f^{-1}(\text{Rad}(J))$ gibt es $n \geq 1$ mit $f(x)^n \in J$. Also folgt $x^n \in f^{-1}(J)$ und $x \in \text{Rad}(f^{-1}(J))$. Gilt umgekehrt $x \in \text{Rad}(f^{-1}(J))$, so gibt es $n \geq 1$ mit $x^n \in f^{-1}(J)$. Dann ergibt sich $f(x)^n \in f(f^{-1}(J)) \subseteq J$, also $f(x) \in \text{Rad}(J)$.

Ist f surjektiv, so gilt $f(f^{-1}(J)) = J$ und $f^{-1}(f(I)) = I$ wegen $I \supseteq \ker(f)$. Setze $J = f(I)$. Nach dem bereits gezeigten gilt $f^{-1}(\text{Rad}(J)) = \text{Rad}(f^{-1}(J)) = \text{Rad}(I)$. Durch Anwendung von f ergibt sich mit $f(f^{-1}(\text{Rad}(J))) = \text{Rad}(J) = \text{Rad}(f(I))$ die zu zeigende Aussage $\text{Rad}(f(I)) = f(\text{Rad}(I))$. \square

Wegen Lemma 2.14 ist $R^{\text{red}} = R/\text{Rad}(R)$ definiert. Es gilt $\text{Rad}(R^{\text{red}}) = \{0\}$, also ist R^{red} reduziert. Für einen Homomorphismus $f : R \rightarrow S$ kommutativer Ringe erhalten wir mit dem Homomorphiesatz in natürlicher Weise einen eindeutig bestimmten Homomorphismus $f^{\text{red}} : R^{\text{red}} \rightarrow S^{\text{red}}$. Ist $g : S \rightarrow T$ ein weiterer Homomorphismus kommutativer Ringe, so gilt $(g \circ f)^{\text{red}} = g^{\text{red}} \circ f^{\text{red}}$. Außerdem gilt $\text{id}_R^{\text{red}} = \text{id}_{R^{\text{red}}}$.

2.5 Schiefkörper, Körper und einfache Ringe

In diesem Abschnitt betrachten wir die Situationen, daß es in einem Ring R keine Nullteiler und keine Ideale I mit $I \neq \{0\}$ und $I \neq R$ gibt.

Sei R ein Ring. Besitzt R nur $\{0\}$ und R als Ideale, so heißt R *einfach*.

2.20 Satz. *Sei R ein Ring.*

- (i) *Schiefkörper und Körper sind einfache Ringe.*
- (ii) *Ist R einfach und $\phi : R \rightarrow S$ ein Halbringhomomorphismus, so ist ϕ entweder konstant gleich 0 oder injektiv.*
- (iii) *Ist $R \neq 0$ kommutativ und einfach, so ist R ein Körper.*
- (iv) *Ist $R \neq 0$ endlich und nullteilerfrei, so ist R ein Körper.*

Beweis. (i): Für jedes Ideal $I \neq 0$ gilt $I \cap R^\times \neq \emptyset$, also $I = R$.

(ii): Klar, da $\ker(\phi) = \{0\}$ oder $\ker(\phi) = R$ gelten muß. Ist ϕ ein Ringhomomorphismus, so ist ϕ wegen $\phi(1) = 1$ immer injektiv.

(iii): Sei $x \in R$, $x \neq 0$. Dann ist Rx ein Ideal von R , da R kommutativ ist, und es gilt $Rx \neq \{0\}$, da R ein Einselement besitzt und somit $x \in Rx$ gilt. Es folgt $Rx = R$, da R einfach ist. Daher gilt $1 \in Rx$, es gibt also $y \in R$ mit $1 = yx$, also $x \in R^\times$. Wegen $1 \neq 0$ folgt, daß $R \setminus \{0\} = R^\times$ gilt.

(iv): Die Schiefkörpereigenschaft wird analog zu Beispiel 2.16 gezeigt. Man kann sie sogar folgern, wenn nur vorausgesetzt wird, daß R ein Halbring ist.

Der schwierige (und recht lange) Teil des Beweises besteht dann darin, zu zeigen, daß jeder endliche Schiefkörper kommutativ ist (siehe Meyberg 2). \square

2.21 Beispiel. Wir geben ein Beispiel eines nicht-kommutativen einfachen Rings $R \neq 0$, der kein Schiefkörper ist. Wir betrachten $R = K^{n \times n}$ für einen Körper K . Ist $M \in R$ und $M \neq 0$, so ist es nicht schwer zu sehen, daß es $A_i, B_i \in R$ mit $\sum_i A_i M B_i = 1$ gibt. Folglich enthält jedes Ideal ungleich 0 eine Einheit und ist gleich R . Daher ist R einfach. Für $n \geq 2$ enthält R aber auch nicht invertierbare Matrizen und ist daher kein Schiefkörper (Details siehe Meyberg 1, Seite 120).

Die vollen Matrixringe $R = K^{n \times n}$ sind also stets einfache Ringe.

2.22 Beispiel. Wir geben ein Beispiel eines nicht-kommutativen Schiefkörpers an. Wir betrachten dazu einen Unterring des nicht-kommutativen, einfachen Rings $\mathbb{C}^{2 \times 2}$.

Sei

$$R = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\},$$

wobei \bar{u}, \bar{v} die konjugiertkomplexen Zahlen von u, v bezeichnen. Nachrechnen zeigt, daß R unter Addition, Negierung und Multiplikation abgeschlossen ist. Außerdem enthält R die Einheitsmatrix. Daher ist R ein Ring mit Eins. Darüberhinaus gilt

$$\det \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = |u|^2 + |v|^2,$$

damit ist jede von Null verschiedene Matrix invertierbar, und die Inversen haben die Form

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}^{-1} = (|u|^2 + |v|^2)^{-1} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix},$$

liegen also wieder in R . Damit ist R also ein Schiefkörper. Da R die Erzeuger der Gruppe Q_8 enthält, diese waren

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

ist R nicht kommutativ und heißt Quaternionenschiefkörper.

2.6 Direkte Produkte und orthogonale Idempotente

Seien I eine Indexmenge und R_i Halbringe (Ringe) für $i \in I$. Das direkte Produkt $\prod_{i \in I} R_i$ wird zunächst als das direkte Produkt der abelschen Gruppen $(R_i, +)$ definiert. Wir führen auf $\prod_{i \in I} R_i$ eine Multiplikation durch $(fg)(i) = f(i)g(i)$ für alle $i \in I$ und $f, g \in \prod_{i \in I} R_i$ ein. Man sieht sofort, daß $\prod_{i \in I} R_i$ ein Halbring beziehungsweise ein Halbring ist, wobei das Einselement gegebenenfalls gleich e mit $e(i) = 1$ für alle $i \in I$ ist. Das leere direkte Produkt ist der Nullring.

Mit dieser Definition ziehen sich die Aussagen aus Abschnitt 1.9 analog durch, wenn man „Gruppe“ durch „Halbring“ („Ring“), „Normalteiler“ durch „Ideal“ und „+“ durch „ \cdot “ ersetzt (dies liegt im wesentlichen daran, daß die Aussagen und Beweise mittels Homomorphismen, Kernen und Erzeugnissen mehr oder weniger allgemein formuliert werden können). Wir überlassen es daher dem Leser, sich die entsprechenden Ergebnisse klarzumachen. Wir heben nur folgendes hervor:

Ist $R = \prod_{i=1}^n R_i$ und fassen wir die R_i mittels ι_i als Teilmengen von R auf, so sind die R_i Ideale von R . Ein Element $e \in R$ ist genau dann Einselement von R , wenn die i -te Projektion von e ein Einselement von R_i für alle i ist.

2.23 Lemma. *Es sei R isomorph zu einem direkten Produkt von Ringen R_i , also $R \cong \prod_{i \in I} R_i$. Dann gilt $R^\times \cong \prod_{i \in I} R_i^\times$. Für endliches I gilt $\text{Rad}(R) \cong \prod_{i \in I} \text{Rad}(R_i)$.*

Beweis. Sei $\phi : R \rightarrow \prod_i R_i$ der Isomorphismus. Elemente in $\prod_i R_i$ sind genau dann Einheiten, wenn in jeder Koordinate eine Einheit steht. Daher $\phi(R^\times) = (\prod_i R_i)^\times = \prod_i R_i^\times$. Weiter gilt $\text{Rad}(\prod_i R_i) \subseteq \prod_i \text{Rad}(R_i)$ durch koordinatenweise Betrachtung. Sei $x = (x_1, \dots, x_n) \in \prod_i \text{Rad}(R_i)$ mit $n = \#I$, und seien $n_i \in \mathbb{Z}^{\geq 0}$ mit $x_i^{n_i} = 0$ für alle $1 \leq i \leq n$. Setze $m = \prod_i n_i$. Dann gilt $x^m = 0$, also $x \in \text{Rad}(\prod_i R_i)$ und damit $\text{Rad}(\prod_i R_i) = \prod_i \text{Rad}(R_i)$. Es folgt $\phi(\text{Rad}(R)) = \text{Rad}(\prod_i R_i) = \prod_i \text{Rad}(R_i)$. \square

Als ringtheoretische Ergänzung von Abschnitt 1.9 betrachten wir jetzt noch orthogonale Idempotente. Sei R ein Ring. Ist $a \in R$ mit $a^2 = a$, so heißt a ein *idempotentes* Element von R . Seien $e_1, \dots, e_n \in R \setminus \{0\}$ idempotente Elemente von R mit $e_i e_j = 0$ für alle $i \neq j$ und $re_i = e_i r$ für alle i und $r \in R$. Dann heißen e_1, \dots, e_n *orthogonale Idempotente* von R . Gilt außerdem $1 = \sum_{i=1}^n e_i$, so sprechen wir von einer *Zerlegung des Einselements von R in orthogonale Idempotente*. Orthogonale Idempotente sind Nullteiler.

Ist $R = \prod_{i=1}^n R_i$ ein Produkt der Ringe R_i , so erhalten wir eine Zerlegung des Einselements von R in die orthogonalen Idempotenten $e_i = (\delta_{i,j})_{1 \leq j \leq n}$ für $1 \leq i \leq n$, wie man leicht nachrechnet. Fassen wir R_i mittels der Injektion ι_i als Teilmenge von R auf, so gilt $R_i = Re_i$ und R_i ist ein Ideal von R . Hiervon gilt auch die Umkehrung:

2.24 Satz. *Sei R ein Ring. Für eine Zerlegung des Einselements von R in orthogonale Idempotente e_1, \dots, e_n sind die Re_i Ringe mit den Einselementen e_i und Ideale von R , und $\phi : R \rightarrow \prod_{i=1}^n Re_i$, $x \mapsto (xe_i)_{1 \leq i \leq n}$ liefert einen Isomorphismus mit Inversem $\psi : \prod_{i=1}^n Re_i \rightarrow R$, $(x_i)_{1 \leq i \leq n} \mapsto \sum_i x_i$.*

Beweis. Seien die e_i eine Zerlegung des Einselements 1 von R in orthogonale Idempotente. Wegen $re_i = e_i r$ für alle $r \in R$ folgt $R(Re_i)R \subseteq Re_i$ und Re_i ist ein Ideal von R . Wegen $(re_i)e_i = re_i^2 = re_i$ und $e_i \in Re_i$ wegen $1 \in R$ (und andersherum analog) ist e_i Einselement von Re_i und Re_i damit ein Ring. Also ist auch $\prod_i Re_i$ ein Ring mit Einselement $e = (e_i)_i$.

Die Additivität von ϕ ist klar. Wegen $(r_1 e_i)(r_2 e_i) = (r_1 r_2) e_i$ für alle $r_1, r_2 \in R$ und alle i sowie $\phi(1) = (e_i)_i = e$ ist ϕ ein Homomorphismus.

Die Additivität von ψ ist ebenfalls klar. Weiter gilt $\psi(e) = \psi((e_i)_i) = \sum_i e_i = 1$. Sind $r_i, s_i \in R$ beliebig, so gilt $\psi((r_i e_i)_i (s_i e_i)_i) = \psi((r_i s_i e_i)_i) = \sum_i r_i s_i e_i$ wegen $r e_i = e_i r$ und $e_i^2 = e_i$. Andererseits gilt $\psi((r_i e_i)_i) \psi((s_i e_i)_i) = \sum_i r_i e_i \sum_i s_i e_i = \sum_i r_i s_i e_i$ wegen $r e_i = e_i r$, $e_i e_j = 0$ für $i \neq j$ und $e_i^2 = e_i$. Damit ist ψ auch multiplikativ und ein Homomorphismus.

Schließlich gilt $\psi(\phi(x)) = \sum_i x e_i = x \sum_i e_i = x$ wegen $1 = \sum_i e_i$, und $\phi(\psi((r_j e_j)_j)) = ((\sum_j r_j e_j) e_i)_i = (r_i e_i)_i$, wegen $e_j e_i = 0$ für $j \neq i$ und $e_i^2 = e_i$. Also ist ϕ ein Isomorphismus mit Inversem ψ . \square

Gemäß unseren Definitionen sind die $R e_i$ allerdings keine Unterringe von R .

2.25 Beispiel. Sei R ein Ring und X eine Menge. Wir betrachten den Funktionsring R^X aus Beispiel 2.1. Das Einselement e von R^X erfüllt $e(x) = 1$ für alle $x \in X$. Sei $X = \dot{\cup}_i X_i$ eine endliche Partition von X und seien $\chi_i \in R^X$ die charakteristischen Funktionen von X_i . Es gilt also $\chi_i(x) = 1$ für $x \in X_i$ und $\chi_i(x) = 0$ für $x \in X \setminus X_i$. Dann bilden die χ_i eine Zerlegung des Einselements von R^X in orthogonale Idempotente. Satz 2.24 liefert $R^X \cong \prod_i R^{X_i}$ wegen $R \chi_i \cong R^{X_i}$ mittels $f \chi_i \mapsto f|_{X_i}$.

2.7 Chinesischer Restsatz

Der Isomorphismus in Satz 1.47 ist auch multiplikativ und liefert daher einen Ringisomorphismus $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ für teilerfremde $n, m \in \mathbb{Z}^{\geq 1}$. Der chinesische Restsatz ist eine Verallgemeinerung dieser Aussage.

Sei R ein Ring. Zwei Ideale I, J von R heißen *komaximal*, wenn $I + J = R$ gilt.

Im folgenden Satz ist $\prod_i I_i$ das Produkt von Idealen, während $\prod_i R/I_i$ das direkte Produkt der Ringe R/I_i ist.

2.26 Satz (Chinesischer Restsatz). *Sei R ein Ring und seien I_1, \dots, I_n Ideale von R . Sei $\phi : R \rightarrow \prod_{i=1}^n R/I_i$ der Homomorphismus mit $x \mapsto (x + I_1, \dots, x + I_n)$. Dann gilt:*

- (i) $\ker(\phi) = \bigcap_{i=1}^n I_i$.
- (ii) ϕ ist genau dann surjektiv, wenn die I_i paarweise komaximal sind.
- (iii) Sind die I_i paarweise komaximal mit $I_i I_j = I_j I_i$, so gilt $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$ und ϕ liefert eine Isomorphie

$$R / \prod_{i=1}^n I_i \cong \prod_{i=1}^n R / I_i.$$

Beweis. Es ist klar, daß ϕ ein Homomorphismus ist (denn ϕ ist koordinatenweise gleich dem kanonischen Epimorphismus $R \rightarrow R/I_i$).

(i): Es gilt $\ker(\phi) = \{x \in R \mid x \in I_i \text{ für alle } 1 \leq i \leq n\} = \bigcap_{i=1}^n I_i$.

(ii): Seien die I_i paarweise komaximal. Dann gibt es $d_{i,j} \in I_i$ mit $1 = d_{i,j} + d_{j,i}$ für alle $i \neq j$. Setze $e_i = \prod_{j \neq i} d_{j,i}$. Dann gilt

$$e_i \equiv \begin{cases} 0 \pmod{I_j} & \text{für alle } j \neq i, \\ 1 \pmod{I_i}. \end{cases}$$

Sei $(x_1 + I_1, \dots, x_n + I_n) \in \prod_i R/I_i$ beliebig. Setze $x = \sum_i x_i e_i$. Dann gilt $x = \sum_i x_i e_i \equiv x_i \pmod{I_i}$ für alle i , also $\phi(x) = (x_1 + I_1, \dots, x_n + I_n)$ und ϕ ist surjektiv.

Sei nun umgekehrt ϕ surjektiv. Sei $b_i = (\delta_{i,j} + I_j)_j$. Nach Voraussetzung gibt es $b'_i \in \phi^{-1}(\{b_i\})$. Setze $a'_i = 1 - b'_i$ und sei π_j die j -te Projektion. Wegen $\pi_j(\phi(b'_i)) = \pi_j(b_i) = 0$ für alle $j \neq i$ gilt $b'_i \in I_j$ für alle $j \neq i$. Wegen $\pi_i(\phi(a'_i)) = \pi_i(1 - b_i) = 0$ gilt $a'_i \in I_i$. Für $j \neq i$ erhalten wir also $1 = a'_i + b'_i$ mit $a'_i \in I_i$ und $b'_i \in I_j$. Somit sind I_i und I_j komaximal.

(iii): Die Isomorphie folgt aus (i), (ii), dem Homomorphiesatz und $\bigcap_i I_i = \prod_i I_i$.

Zum Beweis von $\bigcap_i I_i = \prod_i I_i$ verwenden wir eine Hilfsaussage: Für Ideale I, J_1, \dots, J_n mit $I + J_i = R$ für alle i folgt $I + J_1 \cdots J_n = R$. Die Hilfsaussage ergibt sich wie folgt:

$$R = \prod_{i=1}^n R = \prod_{i=1}^n (I + J_i) \subseteq I(\dots) + (\dots)I + \prod_{i=1}^n J_i \subseteq I + \prod_{i=1}^n J_i \subseteq R.$$

Der Beweis von $\bigcap_i I_i = \prod_i I_i$ erfolgt per Induktion. Der Fall $n = 1$ ist klar. Für $n = 2$ ergibt sich

$$I_1 \cap I_2 \subseteq (I_1 \cap I_2)R \subseteq (I_1 \cap I_2)(I_1 + I_2) \subseteq I_2 I_1 + I_1 I_2 \subseteq I_1 I_2 \subseteq I_1 \cap I_2.$$

Für den Schluß von n auf $n + 1$ ergibt sich unter Verwendung der Hilfsaussage und des Falls $n = 2$:

$$\prod_{i=1}^{n+1} I_i = \left(\prod_{i=1}^n I_i \right) I_{n+1} = \left(\prod_{i=1}^n I_i \right) \cap I_{n+1} = (\bigcap_{i=1}^n I_i) \cap I_{n+1} = \bigcap_{i=1}^{n+1} I_i.$$

□

Wir wollen den chinesischen Restsatz mit Satz 2.24 vergleichen. Indem wir R durch $R/\bigcap_i I_i$ ersetzen, können wir ohne Einschränkung aufgrund des zweiten Isomorphiesatzes annehmen, daß $\bigcap_i I_i = \{0\}$ gilt. Die im Beweis des chinesischen

Restsatzes konstruierten e_i stellen eine Zerlegung der 1 von R in orthogonale Idempotente dar und Multiplikation mit e_i liefert einen Epimorphismus $R \rightarrow Re_i$ mit Kern I_i . Somit gilt $R/I_i \cong Re_i$ und wir erhalten Isomorphismen

$$R \rightarrow \prod_i R/I_i \rightarrow \prod_i Re_i.$$

Wir bemerken, daß das Bild von I_i im Produkt $\prod_i R/I_i$ beziehungsweise im Produkt $\prod_i Re_i$ gleich dem Ideal $\{(x_j)_j \mid x_j \text{ beliebig und } x_i = 0\}$ ist.

In der Situation von Satz 2.24 erhalten wir umgekehrt paarweise komaximale Ideale I_i mit $\cap_i I_i = \{0\}$ als Kerne der Multiplikationsabbildung $R \rightarrow Re_i$ mit e_i .

Satz 2.24 und Satz 2.26 sind daher unterschiedliche Formulierungen oder Kriterien für den Sachverhalt, daß ein Ring ein direktes Produkt von Ringen ist.

2.27 Beispiel. Für teilerfremde Zahlen $n, m \in \mathbb{Z}$ sind die Ideale $n\mathbb{Z}$ und $m\mathbb{Z}$ komaximal. Daher gilt $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Der chinesische Restsatz wird für das Lösen *simultaner Kongruenzen* verwendet. Zu paarweise teilerfremden Zahlen $n_i \in \mathbb{Z}$ und beliebigen $x_1, \dots, x_n \in \mathbb{Z}$ kann man nach Satz 2.26 ein $x \in \mathbb{Z}$ mit $x \equiv x_i \pmod{n_i}$ für alle i finden. Außerdem ist x modulo $\prod_i n_i$ eindeutig bestimmt.

2.28 Beispiel. $R = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Es ist leichter, im direkten Produkt zu rechnen: $(2, 0)$ ist nilpotent, denn $(2, 0)^2 = (0, 0)$. $(1, 0)$ ist nicht nilpotent, aber ein Nullteiler, denn $(1, 0)(0, 1) = (0, 0)$. $(1, 2)$ ist eine Einheit (sogar idempotent), denn $(1, 2)(1, 2) = 1$. Ebenso ist $(3, 2)$ eine Einheit.

Sei $\phi : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ der Isomorphismus aus dem chinesischen Restsatz. Was sind die Urbilder der obigen Elemente in $\mathbb{Z}/12\mathbb{Z}$? Orthogonale Idempotente in $\mathbb{Z}/12\mathbb{Z}$ sind $e_1 = -3$ und $e_2 = 4$. Damit $\phi(e_1) = (1, 0)$ und $\phi(e_2) = (0, 1)$. Weiter $\phi^{-1}((2, 0)) = 2e_1 + 0e_2 = 6$, $6^2 = 36 = 0 \pmod{12}$, $\phi^{-1}((1, 2)) = e_1 + 2e_2 = 5$, $5^2 = 25 = 1 \pmod{12}$.

2.29 Bemerkung. Die Interpolation von Polynomen kann ebenfalls als Anwendung des chinesischen Restsatzes (genauer als Anwendungen der Urbildberechnung im chinesischen Restsatz) angesehen werden. Das im Beweis von Satz 2.26 gegebene Verfahren entspricht der Lagrangeschen Interpolation, wohingegen das nachfolgende Newtonverfahren die Newtonschen Interpolation liefert. Wenn wir später Polynomringe behandeln, gehen wir hierauf noch einmal ein.

Das Newtonverfahren liefert eine Methode, mit der Urbilder unter dem Isomorphismus im chinesischen Restsatz effizienter als mit dem im Beweis angegebenen Verfahren berechnet werden können. Die sogenannte Formel von Garner ist ein Spezialfall dieses Vorgehens für $R = \mathbb{Z}$.

Setze $\tilde{e}_i = \prod_{j=1}^{i-1} d_{j,i}$ mit den $d_{j,i}$ aus dem Beweis von Satz 2.26. Dann setze $y_1 = x_1$ und induktiv $y_{i+1} = y_i + (x_{i+1} - y_i)\tilde{e}_{i+1}$ für $1 \leq i \leq n-1$. Dann gilt $y_n \equiv x_j \pmod{I_j}$ für $1 \leq j \leq n$. Dieses Verfahren benötigt weniger Multiplikationen als das Verfahren aus dem Beweis von Satz 2.26.

Der Beweis der Korrektheit dieses Verfahrens ist eine Hausaufgabe.

2.8 Charakteristik und Primringe

Ist R ein Ring, so gibt es genau einen Homomorphismus $\phi: \mathbb{Z} \rightarrow R$ mit $\phi(1) = 1$. Für $n \in \mathbb{Z}$ ist nämlich $\phi(n) = \phi(n \cdot 1) = n \cdot 1$, wobei $n \cdot 1 = 1 + \dots + 1$ mit jeweils n Einsen (einmal aus \mathbb{Z} und einmal aus R). Die Homomorphieeigenschaft rechnet man direkt nach. Für $n \in \mathbb{Z}$ und $x \in R$ gilt außerdem $n \cdot x = \sum_{i=1}^n x = (\sum_{i=1}^n 1)x = \phi(n)x$.

Nach Lemma 1.39 gibt es ein eindeutig bestimmtes $c \in \mathbb{Z}^{\geq 0}$, so daß $\ker(\phi) = c\mathbb{Z}$, und wir erhalten eine Einbettung von $\mathbb{Z}/c\mathbb{Z}$ in R .

2.30 Definition. Wir definieren die Charakteristik von R als $\text{char}(R) = c$.

2.31 Satz. Sei R ein Ring.

- (i) Es gilt $\text{char}(R)x = 0$ für alle $x \in R$. Für $\text{char}(R) > 0$ ist $\text{char}(R)$ der Exponent von $(R, +)$.
- (ii) Für R nullteilerfrei und $R \neq 0$ ist $\text{char}(R) = 0$ oder $\text{char}(R)$ eine Primzahl.

Beweis. (i): Mit $n = \text{char}(R)$ gilt $n \cdot 1 = \sum_{i=1}^n 1 = 0$. Für $x \in R$ ergibt sich $n \cdot x = \sum_{i=1}^n x = (\sum_{i=1}^n 1)x = 0x = 0$. Für $n > 0$ hat also jedes x in $(R, +)$ eine Ordnung kleiner gleich n und 1 hat Ordnung genau n .

(ii): Sei $n = \text{char}(R)$. Für $n \neq 0$ gilt zunächst $n \geq 2$ wegen $R \neq 0$. Weiter wird $\mathbb{Z}/n\mathbb{Z}$ injektiv nach R durch ϕ eingebettet. Da R nullteilerfrei ist, gilt dies auch für $\mathbb{Z}/n\mathbb{Z}$. Also muß n eine Primzahl sein. \square

Sei R ein Ring. Wir definieren den *Primring* von R als

$$\cap \{U \mid U \text{ Unterring von } R\}.$$

Sei R ein Schiefkörper. Wir definieren den *Primkörper* von R als

$$\cap \{U \mid U \text{ Unterschiefkörper von } R\}.$$

2.32 Satz. Sei R Ring und $\phi: \mathbb{Z} \rightarrow R$ wie oben.

- (i) $\phi(\mathbb{Z})$ ist gleich dem Primring von R .

- (ii) Ist R nullteilerfrei und $R \neq 0$, so ist der Primring isomorph zu \mathbb{Z} oder $\mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl.
- (iii) Für einen Schiefkörper R ist der Primkörper isomorph zu \mathbb{Q} oder $\mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl.

Beweis. (i): Für einen Unterring U von R folgt $\phi(\mathbb{Z}) \subseteq U$. Da $\phi(\mathbb{Z})$ ein Unterring ist, folgt die Behauptung.

(ii): Folgt aus (i), $\phi(\mathbb{Z}) \cong \mathbb{Z}/\text{char}(R)\mathbb{Z}$ und weil $\text{char}(R) = 0$ oder eine Primzahl ist.

(iii): Der Primkörper enthält den Primring. Ist $\text{char}(R)$ eine Primzahl, so ist der Primring bereits Körper und die Behauptung folgt. Ist $\text{char}(R) = 0$ und ist U ein Schiefkörper mit $\phi(\mathbb{Z}) \subseteq U$, so liefert $\mathbb{Q} \rightarrow U$, $n/m \mapsto \phi(n)/\phi(m)$ einen wohldefinierten Monomorphismus, woraus sich der Rest der Behauptung ergibt. \square

2.33 Satz. Sei R ein kommutativer Ring der Charakteristik p , wobei p eine Primzahl ist. Dann gilt $(x + y)^p = x^p + y^p$ für alle $x, y \in R$. Ferner definiert $x \mapsto x^p$ einen Endomorphismus von R , welcher Frobeniusendomorphismus (zur Potenz p) genannt wird.

Beweis. Die erste Aussage folgt durch Anwendung des binomischen Satzes und weil die binomischen Koeffizienten außer dem ersten und dem letzten alle durch p teilbar und daher hier Null sind. Die Teilbarkeit ergibt sich aus Lemma 1.63.

Wegen $(xy)^p = x^p y^p$ und $1^p = 1$ handelt es sich bei $x \mapsto x^p$ tatsächlich um einen Endomorphismus. \square

Iterieren liefert Frobeniusendomorphismen $x \mapsto x^{p^k}$ zu Potenzen p^k . Wir sprechen auch von Frobeniusautomorphismen, wenn die Frobeniusendomorphismen injektiv und surjektiv sind.

2.9 Noethersche Ringe

Wir kommen zu einer Definition, die in gewisser Weise der Endlichdimensionalität von Vektorräumen entspricht.

2.34 Definition. Ein Halbring R , in dem jede nicht leere Menge von Idealen ein bezüglich der Inklusionsrelation maximales Element besitzt, heißt noethersch.

2.35 Satz. Sei R ein Halbring. Dann sind äquivalent:

- (i) Jedes Ideal von R kann durch endlich viele Elemente aus R erzeugt werden.

(ii) Jede aufsteigende Kette von Idealen $I_1 \subseteq I_2 \subseteq \dots$ von R wird stationär, es gibt also $n \in \mathbb{Z}^{\geq 1}$ mit $I_m = I_n$ für alle $m \in \mathbb{Z}^{\geq n}$.

(iii) R ist noethersch.

Beweis. (i) \Rightarrow (ii): Sei $I = \cup_{i \geq 1} I_i$. Dann ist I ein Ideal von R welches nach Voraussetzung endlich erzeugt werden kann. Da die Erzeuger Elemente der I_i sind, gibt es ein $n \in \mathbb{Z}^{\geq 1}$, so daß alle Erzeuger in I_n liegen. Damit gilt $I_m = I_n$ für alle $m \in \mathbb{Z}^{\geq n}$.

(ii) \Rightarrow (iii): Beweis durch Widerspruch. Falls es eine nicht-leere Menge M von Idealen ohne maximales Element gibt, so gibt es zu jedem $I \in M$ ein $J \in M$ mit $I \subsetneq J$. Induktiv erhalten wir die Existenz einer aufsteigenden Kette $I_1 \subsetneq I_2 \subsetneq \dots$, im Widerspruch zu (ii).

(iii) \Rightarrow (i): Sei I ein Ideal von R und M die Menge der Ideale von R , die jeweils durch endlich viele Elemente aus I erzeugt werden können. Dann gibt es in M ein maximales Ideal J , und aufgrund der Konstruktion von M folgt $J = I$. \square

2.36 Beispiel. Der Ring \mathbb{Z} ist noethersch, da jedes Ideal nach Lemma 1.39 sogar von nur einem Element erzeugt werden kann. Einfache Ringe (also auch Körper) sind noethersch.

2.37 Beispiel. Sei $I = \mathbb{Z}$ und $R = \prod_{i \in I} \mathbb{Z}$. Dann ist R nicht noethersch. Die Mengen $I_i = \{f \in R \mid f(j) = 0 \text{ für } j \notin \{1, \dots, i\}\}$ bilden eine echt aufsteigende Kette von Idealen von R , die nicht stationär wird.

2.38 Satz. Faktorringe noetherscher Halbringe sind noethersch. Epimorphe Bilder noetherscher Ringe sind noethersch.

Beweis. Ist $f : R \rightarrow S$ ein Epimorphismus und J ein Ideal von S , so ist $f^{-1}(J)$ ein Ideal von R und nach Voraussetzung endlich erzeugt. Damit ist dann auch $f(f^{-1}(J)) = J$ endlich erzeugt. \square

2.39 Bemerkung. Unterringe noetherscher Ringe sind nicht unbedingt noethersch. Als Beispiel (Begriffe werden später eingeführt) kann man einen Polynomring R in unendlich vielen Variablen und dessen Quotientenkörper K betrachten. Dann ist K als Körper noethersch, aber R ist nicht noethersch.

2.10 Maximale Ideale

2.40 Definition. Sei R ein Halbring. Ein Ideal \mathfrak{m} von R heißt maximales Ideal von R , wenn $\mathfrak{m} \neq R$ ist und für alle Ideale I von R mit $\mathfrak{m} \subseteq I \subseteq R$ bereits $I = \mathfrak{m}$ oder $I = R$ gilt.

2.41 Lemma. Sei R ein Halbring und \mathfrak{m} ein Ideal von R .

- (i) Ist \mathfrak{m} ein maximales Ideal und I ein beliebiges Ideal von R mit $I \not\subseteq \mathfrak{m}$, so gilt $I + \mathfrak{m} = R$.
- (ii) \mathfrak{m} ist genau dann maximales Ideal von R , wenn $R/\mathfrak{m} \neq 0$ und einfach ist.
- (iii) Ist R kommutativ mit Einselement, so ist \mathfrak{m} genau dann maximal, wenn R/\mathfrak{m} ein Körper ist.

Beweis. (i): Da $I + \mathfrak{m}$ ein Ideal von R mit $\mathfrak{m} \subsetneq I + \mathfrak{m}$ ist, folgt $I + \mathfrak{m} = R$.

(ii): Folgt aus Lemma 2.6.

(iii): Folgt aus (i) und Satz 2.20, da $R/\mathfrak{m} \neq 0$ ein einfacher kommutativer Ring ist. \square

2.42 Beispiel. Die maximalen Ideale von \mathbb{Z} sind genau die Ideale $p\mathbb{Z}$, wobei p eine Primzahl ist.

2.43 Definition. Sei M eine Menge und \leq eine Relation auf M . Dann heißt \leq eine Halbordnung auf M , wenn die Eigenschaften

$$x \leq x, \quad (x \leq y \text{ und } y \leq x) \Rightarrow x = y, \quad (x \leq y \text{ und } y \leq z) \Rightarrow x \leq z$$

für alle $x, y, z \in M$ gelten. Gilt dazu $x \leq y$ oder $y \leq x$ für alle $x, y \in M$, so heißt \leq eine Ordnung auf M .

Sei \leq eine Halbordnung auf M . Für jede Teilmenge X von M schränkt sich \leq zu einer Halbordnung auf X ein. Eine Kette von M ist eine Teilmenge X von M , auf der \leq eine Ordnung definiert.

Sei \leq eine Halbordnung auf M . Ein Element $m \in M$ mit $m \leq x \Rightarrow x = m$ für alle $x \in M$ heißt maximales Element von M . Sei $X \subseteq M$. Ein Element $s \in M$ mit $x \leq s$ für alle $x \in X$ heißt obere Schranke von X in M . Die Menge M heißt induktiv geordnet, wenn jede nicht leere Kette X von M eine obere Schranke in M besitzt.

2.44 Satz (Lemma von Zorn). Sei M eine bezüglich \leq induktiv geordnete, nicht leere Menge. Dann gibt es ein maximales Element m von M .

Das Lemma von Zorn ist äquivalent zum Auswahlaxiom, welches von den üblichen Axiomen der Mengenlehre unabhängig ist. Es handelt sich hierbei also eher um eine Annahme, die man treffen oder auch nicht treffen kann. Es ist für gewöhnlich praktisch, das Auswahlaxiom anzunehmen (haben wir schon für (ii) \Rightarrow (iii) in Satz 2.35 getan).

2.45 Satz. *Sei R ein Ring und I ein Ideal von R mit $I \neq R$. Dann gibt es ein maximales Ideal \mathfrak{m} von R mit $I \subseteq \mathfrak{m}$.*

Beweis. Wir definieren $M = \{J \mid J \text{ Ideal von } R \text{ mit } J \neq R \text{ und } I \subseteq J\}$. Die Inklusionsrelation \subseteq liefert eine Halbordnung auf M , wie man unmittelbar sieht.

Wir behaupten, daß M sogar induktiv geordnet ist. Sei dazu $X \subseteq M$ eine nicht leere Kette. Wir müssen zeigen, daß X eine obere Schranke in M besitzt, daß es also ein Ideal $\mathfrak{m}_X \in M$ mit $J \subseteq \mathfrak{m}_X$ für alle $J \in X$ gibt. Definiere $\mathfrak{m}_X := \cup_{J \in X} J$. Wie im Beweis von Lemma 2.41 ist dies ein Ideal ein Ideal von R . Es bleibt $\mathfrak{m}_X \neq R$ zu zeigen, um $\mathfrak{m}_X \in M$ zu erhalten. Nun gilt aber $1 \notin J$ für alle $J \in X$, folglich $1 \notin \mathfrak{m}_X$, also $\mathfrak{m}_X \neq R$.

Wegen $I \in M$ ist M nicht leer. Nun wenden wir das Lemma von Zorn an und erhalten die Existenz eines Ideals $\mathfrak{m} \in M$, welches bezüglich \subseteq in M maximal ist. Es gilt also $\mathfrak{m} \neq R$ und $\mathfrak{m} \subsetneq J \Rightarrow J = R$ für jedes Ideal von R , und somit ist \mathfrak{m} ein maximales Ideal von R . \square

Die Aussage des Satzes gilt entsprechend für Links- und Rechtsideale. Nach dem Lemma von Zorn besitzt jede nicht-leere, bezüglich \subseteq induktiv geordnete Menge M von Idealen ein maximales Element. Für einen noetherschen Ring ist jede nicht-leere Menge von Idealen bezüglich \subseteq induktiv geordnet. Dies ist gleichbedeutend mit Aussage von Satz 2.35, (ii) (und ist für nicht-noethersche Ringe im allgemeinen falsch). Damit erhalten wir die Implikation (ii) \Rightarrow (iii) in Satz 2.35 auch mit Hilfe des Zornschen Lemmas.

2.46 Lemma. *Seien R, S Halbringe und sei $\phi : R \rightarrow S$ Epimorphismus. Ist \mathfrak{m} ein maximales Ideal von S , so ist $\phi^{-1}(\mathfrak{m})$ ein maximales Ideal von R .*

Beweis. Wir bekommen durch ϕ einen Isomorphismus $R/\phi^{-1}(\mathfrak{m}) \rightarrow S/\mathfrak{m}$. Da $R/\phi^{-1}(\mathfrak{m})$ mit S/\mathfrak{m} einfach ist, muß $\phi^{-1}(\mathfrak{m})$ maximal sein. \square

2.47 Beispiel. Die Aussage gilt im allgemeinen nicht, wenn ϕ nur ein Homomorphismus ist. Betrachte $R = \mathbb{Z}$, $S = \mathbb{Q}$ und ϕ den Inklusionshomomorphismus. Wähle $\mathfrak{m} = \{0\}$. Dann ist \mathfrak{m} maximales Ideal von \mathbb{Q} , aber $\phi^{-1}(\mathfrak{m}) = \{0\}$ ist kein maximales Ideal von \mathbb{Z} .

Die Aussage gilt aber für endlich erzeugte k -Algebren, wobei k ein Körper ist. Diese Klasse von Ringen spielen in der algebraischen Geometrie eine wichtige Rolle.

2.11 Integritätsringe und Primideale

Wir betrachten im folgenden nur noch kommutative Halbringe und Ringe.

2.48 Definition. Sei R ein kommutativer Halbring.

Ein Ideal \mathfrak{p} von R heißt Primideal von R , wenn $\mathfrak{p} \neq R$ ist und für alle $a, b \in R$ aus $ab \in \mathfrak{p}$ bereits $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

Gilt $R \neq 0$ und ist R nullteilerfrei, so heißt R Integritätshalbring. Besitzt R darüberhinaus ein Einselement, so heißt R Integritätsring (englisch: Domain).

2.49 Satz. Sei R ein kommutativer Halbring und \mathfrak{p} ein Ideal von R mit $\mathfrak{p} \neq R$. Dann sind äquivalent:

- (i) \mathfrak{p} ist Primideal,
- (ii) Sind $\mathfrak{a}, \mathfrak{b}$ Ideale von R , so folgt aus $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ bereits $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$.
- (iii) $R \setminus \mathfrak{p}$ mit der Multiplikation aus R ist eine Halbgruppe,
- (iv) R/\mathfrak{p} ist Integritätshalbring,
- (v) \mathfrak{p} ist Kern eines Homomorphismus $\phi : R \rightarrow S$, wobei S ein Integritätshalbring ist.

Beweis. (i) \Rightarrow (ii): Gilt $\mathfrak{a} \not\subseteq \mathfrak{p}$, so gibt es $a \in \mathfrak{a} \setminus \mathfrak{p}$. Für $b \in \mathfrak{b}$ gilt dann $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, und aus (i) ergibt sich $b \in \mathfrak{p}$. Da b beliebig war, folgt $\mathfrak{b} \subseteq \mathfrak{p}$.

(ii) \Rightarrow (i): Seien $a, b \in R$ mit $ab \in \mathfrak{p}$. Für $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ gilt $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, wegen $\mathfrak{a} = Ra + \mathbb{Z}a$, $\mathfrak{b} = Rb + \mathbb{Z}b$ und folglich $\mathfrak{a}\mathfrak{b} = Rab + \mathbb{Z}ab = (ab) \subseteq \mathfrak{p}$. Also ergibt sich nach Voraussetzung $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$, und daraus $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

(i) \Rightarrow (iii): Seien $a, b \in R \setminus \mathfrak{p}$. Da \mathfrak{p} nach Annahme Primideal ist, muß $ab \notin \mathfrak{p}$ gelten, denn sonst wäre $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

(iii) \Rightarrow (iv): R/\mathfrak{p} ist genau dann nullteilerfrei, wenn Bedingung (iii) gilt.

(iv) \Rightarrow (v): Wähle $S = R/\mathfrak{p}$ und den Restklassenepimorphismus. Nach Voraussetzung $\mathfrak{p} \neq R$ ist $S \neq 0$ und daher ein Integritätshalbring.

(v) \Rightarrow (i): Seien $a, b \in R$ und $ab \in \mathfrak{p} = \ker(\phi)$. Dann gilt $\phi(ab) = \phi(a)\phi(b) = 0$. Da S nullteilerfrei ist, folgt $\phi(a) = 0$ oder $\phi(b) = 0$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Wegen $\mathfrak{p} \neq R$ nach Voraussetzung ist \mathfrak{p} Primideal. \square

2.50 Beispiel. Die Primideale von \mathbb{Z} sind genau die Ideale $p\mathbb{Z}$, wo p eine Primzahl ist.

2.51 Beispiel. Sei R kommutativ mit $R \neq 0$. Das Ideal $\{0\}$ ist genau dann Primideal, wenn R nullteilerfrei ist. Der Nullring $R = 0$ besitzt kein Primideal.

2.52 Satz. Sei R ein kommutativer Ring.

- (i) Jedes maximale Ideal von R ist ein Primideal von R .

(ii) Zu jedem Ideal I von R mit $I \neq R$ gibt es ein Primideal \mathfrak{p} von R mit $I \subseteq \mathfrak{p}$.

Beweis. (i): Sei \mathfrak{m} maximales Ideal von R . Dann gilt $1 \neq 0$ und R/\mathfrak{m} ist ein Körper. Da Körper auch Integritätsringe sind, ist \mathfrak{m} ein Primideal.

(ii): Wegen $I \neq R$ gilt $1 \neq 0$. Wähle \mathfrak{p} als ein maximales Ideal \mathfrak{m} mit $I \subseteq \mathfrak{m}$, welches nach Satz 2.45 existiert. Nach (i) ist \mathfrak{m} ein Primideal. \square

2.53 Satz. Seien R, S kommutative Halbringe und sei $\phi : R \rightarrow S$ ein Homomorphismus mit $(\phi(R)) = S$. Ist dann \mathfrak{p} ein Primideal von S , so ist $\phi^{-1}(\mathfrak{p})$ ein Primideal von R .

Beweis. Wir bekommen durch ϕ einen Monomorphismus $R/\phi^{-1}(\mathfrak{p}) \rightarrow S/\mathfrak{p}$. Der Halbring $R/\phi^{-1}(\mathfrak{p})$ ist mit S/\mathfrak{p} nullteilerfrei. Ferner gilt $(\phi(\phi^{-1}(\mathfrak{p}))) \subseteq \mathfrak{p} \neq S$ und daher nach Annahme $\phi^{-1}(\mathfrak{p}) \neq R$. \square

Die Bedingung $(\phi(R)) = S$ ist beispielsweise erfüllt, wenn R und S kommutative Ringe sind (wegen $\phi(1) = 1$).

2.54 Beispiel. Die Aussage gilt nicht, wenn die Voraussetzung $(\phi(R)) = S$ nicht gemacht wird. Zum Beispiel sei $R = \mathfrak{p}$ Primideal von S und ϕ die Inklusionsabbildung. Dann ist $R = \phi^{-1}(\mathfrak{p})$ kein Primideal. Speziell kann \mathfrak{p} selbst auch ein Einselement besitzen: Man wähle zum Beispiel $R = \mathbb{Q}$, $S = \mathbb{Q} \times \mathbb{Q}$ und ϕ die Einbettung von \mathbb{Q} in die erste Koordinate von $\mathbb{Q} \times \mathbb{Q}$. Das Ideal $\mathbb{Q} \times \{0\}$ ist ein Primideal (sogar maximales Ideal) von $\mathbb{Q} \times \mathbb{Q}$, aber $\phi^{-1}(\mathbb{Q} \times \{0\}) = \mathbb{Q}$ ist kein Primideal von \mathbb{Q} .

Homomorphe Bilder von Primidealen sind im allgemeinen keine Primideale mehr.

2.12 Teilbarkeit in Ringen

Die gewohnte Teilbarkeitslehre von \mathbb{Z} kann verallgemeinert werden. Man setzt üblicherweise voraus, daß die zu betrachtenden Ringe kommutativ mit $1 \neq 0$ sind und keine Nullteiler besitzen.

2.55 Definition. Sei R ein Integritätsring und $a, b \in R$.

Das Element a heißt Teiler von b , wenn es $c \in R$ mit $b = ca$ gibt. Entsprechend sagt man, daß a das Element b teilt, oder daß b ein Vielfaches von a ist, in Zeichen $a \mid b$.

Das Element a heißt assoziiert zu b , wenn $c \in R$ mit $b = ca$ eine Einheit von R ist, wenn also äquivalenterweise $a \mid b$ und $b \mid a$ gilt (in Zeichen $a \sim b$).

Ein Element $c \in R$ heißt größter gemeinsamer Teiler der Elemente $a_1, \dots, a_n \in R$, wenn $c \mid a_i$ für alle i gilt und wenn für alle $d \in R$ mit $d \mid a_i$ für alle i bereits $d \mid c$ folgt. Wir schreiben $c = \gcd(a_1, \dots, a_n)$, obwohl c nur bis auf Multiplikation mit Einheiten eindeutig bestimmt ist. Im allgemeinen kann nicht davon ausgegangen werden, daß $\gcd(a_1, \dots, a_n)$ existiert. Elemente $a_1, \dots, a_n \in R$ heißen teilerfremd, wenn für $c \in R$ mit $c \mid a_i$ für alle i bereits $c \in R^\times$ folgt. Da sich je zwei solche c gegenseitig teilen, existiert also $\gcd(a_1, \dots, a_n)$ und es gilt $\gcd(a_1, \dots, a_n) \in R^\times$.

Ein Element $c \in R$ heißt kleinstes gemeinsames Vielfaches der Elemente $a_1, \dots, a_n \in R$, wenn $a_i \mid c$ für alle i gilt und wenn für alle $d \in R$ mit $a_i \mid d$ für alle i bereits $c \mid d$ folgt. Wir schreiben $c = \text{lcm}(a_1, \dots, a_n)$, obwohl c nur bis auf Multiplikation mit Einheiten eindeutig bestimmt ist. Im allgemeinen kann nicht davon ausgegangen werden, daß $\text{lcm}(a_1, \dots, a_n)$ existiert.

Ein Element $p \in R \setminus R^\times$ mit $p \neq 0$ heißt Primelement von R , wenn aus $p \mid (ab)$ für alle $a, b \in R$ bereits $p \mid a$ oder $p \mid b$ folgt.

Ein Element $q \in R \setminus R^\times$ mit $q \neq 0$ heißt irreduzibel, wenn aus $q = ab$ für alle $a, b \in R$ bereits $a \in R^\times$ oder $b \in R^\times$ folgt.

Ein Ideal heißt Hauptideal, wenn es von einem Element erzeugt werden kann.

Die Definition von Teiler und assoziierten Elementen verwendet man so auch für nicht notwendigerweise nullteilerfreie, kommutative Ringe.

2.56 Beispiel. Die Definition stimmt mit den bekannten Definitionen für \mathbb{Z} überein. Primelemente und irreduzible Elemente in \mathbb{Z} stimmen überein.

2.57 Beispiel. Sei $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ als Teilring von \mathbb{R} . Wegen $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ ist $\varepsilon = 1 + \sqrt{2}$ eine Einheit in R . Da ε^k für $k \in \mathbb{Z}^{\geq 0}$ eine streng monoton wachsende Folge in \mathbb{R} definiert, gilt $\#R^\times = \infty$.

Man kann zeigen, daß in $\mathbb{Z}[\sqrt{2}]$ die Menge der Primelemente mit der Menge der irreduziblen Elemente übereinstimmt.

2.58 Beispiel. Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ als Teilring von \mathbb{C} . Man kann zeigen, daß hier $R^\times = \{-1, 1\}$ gilt und beispielsweise $21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ eine Zerlegung von 21 in irreduzible, aber nicht prime Elemente ist.

2.59 Lemma. Sei R ein Integritätsring.

- (i) Es gilt $1 \mid a$, $a \mid 0$ und $a \mid a$ für alle $a \in R$. Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$ für alle $a, b, c \in R$.
- (ii) Es gilt $a \mid 1$ genau dann, wenn $a \in R^\times$. Es gilt $a \mid b$ für alle $a \in R^\times$ und $b \in R$.

- (iii) Für $a|b$ gilt auch $ax|bx$ für alle $x \in R$. Für $a|x_i$ gilt $a|\sum_i r_i x_i$ für alle $r_i, x_i \in R$.
- (iv) Es gilt $a|b$ genau dann, wenn $Ra \supseteq Rb$ für alle $a, b \in R$. Es gilt $a \sim b$ genau dann, wenn $Ra = Rb$ ist.
- (v) Sind $a_i \in R$ und $c \in R$ mit $Rc = \sum_i Ra_i$, so gilt $c = \gcd(a_1, \dots, a_n)$.
- (vi) Sind $a_i \in R$ und $c \in R$ mit $Rc = \cap_i Ra_i$, so gilt $c = \text{lcm}(a_1, \dots, a_n)$.

Beweis. Die meisten Punkte sind einfach und werden ausgelassen.

(v): Wegen $a_i \in Rc$ gilt $c|a_i$ für alle i . Sei $d \in R$ mit $d|a_i$ für alle i . Dann folgt $Rd \supseteq \sum_i Ra_i = Rc$, also $d|c$.

(vi): Es gilt $c \in Ra_i$, also $a_i|c$ für alle i . Sei $d \in R$ mit $a_i|d$ für alle i . Dann gilt $Rd \subseteq \cap_i Ra_i = Rc$, also $c|d$. \square

2.60 Satz. Sei R Integritätsring und $a \in R \setminus R^\times$, $a \neq 0$. Dann gilt:

- (i) Das Element a ist genau dann Primelement von R , wenn Ra Primideal von R ist.
- (ii) Das Element a ist genau dann irreduzibel, wenn Ra maximal in der Menge der von R verschiedenen Hauptideale ist.
- (iii) Jedes Primelement ist irreduzibel.
- (iv) Je zwei irreduzible Elemente sind entweder assoziiert oder teilerfremd.

Beweis. (i): Ergibt sich aus den Definitionen von Primideal und Primelement sowie aus Lemma 2.59, (iv): Für $x, y \in R$ gilt die Äquivalenz $x|y \Leftrightarrow y \in Rx$. Damit ist die Implikation $p|ab \Rightarrow p|a \vee p|b$ äquivalent zur Implikation $ab \in Rp \Rightarrow a \in Rp \vee b \in Rp$, und diese ist die definierende Implikation für die Primidealeigenschaft von Rp .

(ii): a ist genau dann irreduzibel, wenn für alle $b \in R \setminus R^\times$ die Implikation $b|a \Rightarrow b \sim a$ gilt. Diese Implikation ist aber äquivalent zu $Rb \supseteq Ra \Rightarrow Rb = Ra$. Die Menge der von R verschiedenen Hauptideale ist gleich $\{Rb | b \in R \setminus R^\times\}$. Zusammen ergibt sich (ii).

(iii): Sei $p \in R$ Primelement und $p = ab$ mit $a, b \in R$. Wegen $p|ab$ folgt $p|a$ oder $p|b$. Gilt beispielsweise $a = cp$ mit $c \in R$, so folgt $p = ab = cpb$, und daraus $1 = cb$ durch Kürzen von p ($p \neq 0$ und R nullteilerfrei), also $b \in R^\times$. Analog für $b = cp$, und p ist also irreduzibel.

(iv): Seien $a, b \in R$ irreduzibel. Falls a, b nicht teilerfremd sind, gibt es ein $c \in R \setminus R^\times$, $c \neq 0$ mit $c|a$ und $c|b$. Dann gibt es $e, d \in R$ mit $a = dc$ und $b = ec$. Da a irreduzibel ist, folgt $d \in R^\times$. Nun gilt $b = ed^{-1}a$ und wegen $a \notin R^\times$ ergibt sich $ed^{-1} \in R^\times$, da b irreduzibel ist. Folglich sind a und b assoziiert. \square

Im folgenden verstehen wir unter einem Produkt von Elementen eines Rings (wie auch zuvor) immer ein Produkt von endlich vielen Elementen. Unendliche Produkte von Elementen sind in der Algebra zunächst nicht definiert, hierfür braucht man noch einen Konvergenzbegriff.

2.61 Definition. Ein Integritätsring R heißt faktorieller Ring (oder ZPE Ring), wenn sich jedes $a \in R$, $a \neq 0$ bis auf Einheiten und die Reihenfolge der Faktoren auf genau eine Weise als Produkt von irreduziblen Elementen schreiben läßt (englisch: Unique Factorisation Domain, UFD).

2.62 Beispiel. Der Ring \mathbb{Z} ist ein faktorieller Ring. Es gilt zum Beispiel $-6 = 2 \cdot (-3) = (-1) \cdot 2 \cdot 3$ mit den irreduziblen Elementen $2, -3, 3$ und der Einheit -1 .

2.63 Satz. Sei R ein Integritätsring. Dann sind äquivalent:

- (i) R ist faktorieller Ring.
- (ii) Jedes $a \in R$, $a \neq 0$ ist Produkt irreduzibler Elemente, und jedes irreduzible Element ist Primelement.
- (iii) Jedes $a \in R$, $a \neq 0$ ist Produkt von Primelementen.

Beweis. (i) \Rightarrow (ii): Sei q irreduzibel und $a, b \in R$ mit $q \mid (ab)$, also $ab = cq$ für ein $c \in R$. Das Element q kommt daher wegen der Eindeutigkeit in der Faktorisierung von ab in irreduzible Elemente vor. Diese setzt sich wegen der Eindeutigkeit aus der Faktorisierung von a und von b in irreduzible Elemente zusammen. Also kommt q in einer dieser Faktorisierungen vor, daher $q \mid a$ oder $q \mid b$.

(ii) \Rightarrow (iii): Klar.

(iii) \Rightarrow (i). Ist q irreduzibel, so kann q nicht als Produkt von mehr als einer Nichteinheit geschrieben werden. Also besteht die Faktorisierung von q in Primelemente aus nur einem Element, nämlich q selbst. Also ist q ein Primelement.

(ii) \Rightarrow (i): Seien $\varepsilon q_1 \cdots q_r = \varepsilon' q'_1 \cdots q'_s$ zwei Faktorisierungen in Primelemente q_i, q'_j und Einheiten $\varepsilon, \varepsilon'$ mit $r \leq s$. Für $r = 0$ muß auch $s = 0$ gelten, da Produkte von Primelementen beziehungsweise Nichteinheiten keine Einheiten sind. Für $r \geq 1$ gilt $s \geq 1$ und $q'_s \mid q_i$ für ein i . Da q_i irreduzibel ist, ist q'_s assoziiert zu q_i . Vertauschen von q_i und q_r und Kürzen von q'_s liefert $\varepsilon q_1 \cdots q_{r-1} = \varepsilon'' q'_1 \cdots q'_{s-1}$ mit $\varepsilon'' \in R^\times$. Per Induktion folgt die Eindeutigkeitsaussage. \square

Sei R ein faktorieller Ring und $P \subseteq R$ ein Vetretersystem der Äquivalenzklassen der Primelemente von R unter Assoziation (zum Beispiel die Menge der Primzahlen anstelle der Menge der Primelemente von \mathbb{Z}).

Für $a \in R$, $a \neq 0$ und $p \in R$ bezeichnen wir mit $v_p(a)$ die Vielfachheit, mit der p in der Faktorisierung von a in Primelemente aus P vorkommt. Es gilt also

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)},$$

wobei fast alle $v_p(a)$ gleich Null sind und $\varepsilon \in R^\times$ ist.

2.64 Korollar. Sei R ein Integritätsring und $a_1, \dots, a_n \in R$.

1. Es gilt $\gcd(a_1, \dots, a_n) = \prod_{p \in P} p^{\min\{v_p(a_i) \mid 1 \leq i \leq n\}}$.
2. Es gilt $\text{lcm}(a_1, \dots, a_n) = \prod_{p \in P} p^{\max\{v_p(a_i) \mid 1 \leq i \leq n\}}$.
3. Für $a, b \in R$, $a, b \neq 0$ ist ab assoziiert zu $\gcd(a, b)\text{lcm}(a, b)$.

Beweis. Klar. □

2.65 Satz. Sei R ein noetherscher Integritätsring. Dann läßt sich jedes Element von R ungleich Null als Produkt von irreduziblen Elementen von R schreiben.

Beweis. Sei $M = \{Rx \mid x \in R \setminus \{0\}, x \text{ läßt sich nicht als Produkt irreduzibler Elemente schreiben}\}$. Es ist zu zeigen, daß M leer ist. Falls M nicht leer ist, gibt es nach Satz 2.35 ein maximales Ideal Ra in M . Dann ist a nicht irreduzibel, es gibt also $b, c \in R \setminus R^\times$ mit $a = bc$. Wegen $Rb \supsetneq Ra$ und $Rc \supsetneq Ra$ gilt $Rb, Rc \notin M$ und b und c lassen sich als Produkt von irreduziblen Elementen schreiben. Damit läßt sich auch $a = bc$ als Produkt von irreduziblen Elementen schreiben, im Widerspruch zu $Ra \in M$.

Ein direkterer Beweis geht wie folgt: Jedes $a \in R \setminus R^\times$ mit $a \neq 0$ besitzt einen irreduziblen Teiler. Für a irreduzibel ist nichts zu zeigen. Andernfalls gibt einen Teiler $b \in R \setminus R^\times$ mit $b \neq 0$ und $b \not\sim a$ beziehungsweise $Rb \supsetneq Ra$. Jeder irreduzible Teiler von b ist auch ein irreduzibler Teiler von a . Induktiv erhalten wir eine Kette von echten Teilern beziehungsweise eine Kette echt aufsteigender Hauptideale, welche nach Voraussetzung nach endlich vielen Schritten abbricht. Dann ist das letzte Element der Kette ein irreduzibler Teiler von a .

Sei $a \in R \setminus R^\times$ mit $a \neq 0$. Ist a irreduzibel, sind wir fertig. Andernfalls gibt es einen irreduziblen Teiler q von a , so daß für $b \in R$ mit $a = qb$ und $b \neq 0$ gilt $b \notin R^\times$ und $Rb \supsetneq Ra$. Induktiv erhalten wir eine echt aufsteigende Kette, die nach Voraussetzung nach endlich vielen Schritten mit einem irreduziblen Element q abbricht. Dann ist a das Produkt der gefundenen, irreduziblen q . □

2.66 Definition. Ein Integritätsring R heißt Hauptidealring, wenn jedes Ideal von R Hauptideal ist (englisch: Principal Ideal Domain, PID).

2.67 Beispiel. Der Ring \mathbb{Z} ist Hauptidealring. Körper sind Hauptidealringe.

2.68 Bemerkung. In der Definition genügt es schon, R nur als Integritätshalbring vorauszusetzen. Die Hauptidealringeigenschaft bewirkt, daß R notwendigerweise ein Einselement haben muß: Für das Ideal R folgt speziell $R = Rc$ mit einem $c \in R$. Es gibt $e \in R$ mit $c = ec = ce$, und zu jedem $x \in R$ gibt es $y \in R$ mit $x = yc$. Nun ist $xe = (yc)e = y(ce) = yc = x$, also ist e Einselement von R .

2.69 Satz. Sei R ein Hauptidealring. Dann gilt:

(i) R ist noethersch und faktoriell.

(ii) Sind $a_i \in R$, so gibt es $\lambda_i \in R$ mit $\gcd(a_1, \dots, a_n) = \sum \lambda_i a_i$.

Beweis. (i): Die erste Aussage ist klar, da jedes Ideal nur einen Erzeuger benötigt. Für die zweite Aussage zeigen wir zuerst, daß jedes irreduzible Element von R ein Primelement von R ist: Sei $a \in R \setminus R^\times$, $a \neq 0$ irreduzibel. Dann ist $Ra \neq R$ und maximal in der Menge der Hauptideale. Da jedes Ideal Hauptideal ist, ist Ra also maximales Ideal von R , und somit Primideal. Nach Lemma 2.60, (i) ist a ein Primelement. Die zweite Aussage folgt nun damit aus der ersten Aussage, Satz 2.65 und Satz 2.63.

(ii): Folgt aus der Hauptidealeigenschaft und Lemma 2.59, (v). \square

Die Aussage (ii) des Satzes nennt man auch Satz von Bézout.

2.70 Definition. Ein Integritätsring R heißt euklidischer Ring, wenn es eine Abbildung $d : R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ mit der folgenden Eigenschaft gibt: Zu $a, b \in R$, $b \neq 0$ gibt es $h, r \in R$ mit $a = hb + r$ und $r = 0$ oder $d(r) < d(b)$.

Die in der Definition verlangte Abbildung d heißt Gradfunktion. Die Zerlegung $a = hb + r$ mit $r = 0$ oder $d(r) < d(b)$ heißt Division mit Rest r .

2.71 Beispiel. Der Ring \mathbb{Z} wird mit $x \mapsto |x|$ als Gradfunktion zum euklidischen Ring.

2.72 Satz. Jeder euklidische Ring ist ein Hauptidealring.

Beweis. Sei I ein Ideal von R und $a \in I$, $a \neq 0$ ein Element mit $d(a) = \min\{d(b) \mid b \in I \setminus \{0\}\}$. Sei $b \in I$. Division mit Rest liefert $b = ha + r$, also $r = b - ha \in I$. Nach Wahl von a ist $d(r) < d(a)$ nicht möglich, also gilt $r = 0$. Es folgt $I = Ra$. Damit ist R ein Integritätsring, in dem jedes Ideal Hauptideal ist. \square

In der Definition vom euklidischen Ring könnte man sich wieder auf die Voraussetzung beschränken, daß R nur ein Integritätshalbring ist.

In euklidischen Ringen können größte gemeinsame Teiler mit dem euklidischen Algorithmus berechnet werden. Genauer liefert der euklidische Algorithmus angewendet auf $a, b \in R$ Elemente $\lambda, \mu \in R$ mit $\gcd(a, b) = \lambda a + \mu b$.

2.13 Lokale Ringe und Lokalisierung

2.73 Definition. Sei R ein kommutativer Ring. Wenn R genau ein maximales Ideal besitzt, dann heißt R lokaler Ring.

2.74 Satz. Ein kommutativer Ring R ist genau dann lokal, wenn $R \setminus R^\times$ ein Ideal von R ist.

Für einen lokalen Ring R ist $R \setminus R^\times$ das maximale Ideal von R .

Beweis. „ \Rightarrow “: Bezeichne \mathfrak{m} das maximale Ideal von R und sei $x \in R \setminus R^\times$. Dann gilt $R \neq Rx$, da x keine Einheit ist. Da es ein maximales Ideal von R gibt, welches Rx enthält, folgt $Rx \subseteq \mathfrak{m}$, also $x \in \mathfrak{m}$ und $R \setminus R^\times \subseteq \mathfrak{m}$. Da \mathfrak{m} keine Einheiten enthalten kann, gilt sogar $R \setminus R^\times = \mathfrak{m}$.

„ \Leftarrow “: Ist $\mathfrak{m} = R \setminus R^\times$ ein Ideal, so ist es aus dem eben genannten Grund maximal und enthält auch jedes weitere Ideal $\neq R$ von R . Daher besitzt R nur dieses eine maximale Ideal \mathfrak{m} . \square

Sei $R \neq 0$ ein kommutativer Halbring und U eine nicht-leere, multiplikativ abgeschlossene Teilmenge von R . Wir wollen eine „Bruchrechnung“ mit Elementen aus R im Zähler und Elementen aus U im Nenner definieren. Dazu führen wir auf der Menge $R \times U$ eine Äquivalenzrelation \sim ein. Für $(r_1, u_1), (r_2, u_2) \in R \times U$ gelte $(r_1, u_1) \sim (r_2, u_2)$ genau dann, wenn es ein $t \in U$ mit $t(r_1u_2 - r_2u_1) = 0$ gibt.

2.75 Lemma. Die Relation \sim ist eine Äquivalenzrelation.

Beweis. Reflexivität und Symmetrie sind unmittelbar einsichtig. Für die Transitivität muß etwas gerechnet werden. Es gelte $(r_1, u_1) \sim (r_2, u_2)$ und $(r_2, u_2) \sim (r_3, u_3)$. Wir können also schreiben

$$\begin{aligned} t(r_1u_2 - r_2u_1) &= 0, \\ s(r_2u_3 - r_3u_2) &= 0 \end{aligned}$$

mit $t, s \in U$. Wir multiplizieren die erste Gleichung mit su_3 und die zweite mit tu_1 und erhalten

$$\begin{aligned} st(r_1u_2u_3 - r_2u_1u_3) &= 0 \\ st(r_2u_1u_3 - r_3u_1u_2) &= 0. \end{aligned}$$

Addition dieser Gleichungen und Ausklammern von u_2 liefert

$$stu_2(r_1u_3 - r_3u_1) = 0$$

mit $stu_2 \in U$. \square

Die Verwendung von t in der Definition von \sim ist deswegen erforderlich, da wir aus $u_2(r_1u_3 - r_3u_1) = 0$ zum Schluß nicht ohne weiteres auf $r_1u_3 - r_3u_1 = 0$ schließen können. Enthält U keine Nullteiler von R , so wäre dies möglich.

Für $r \in R$ und $u \in U$ schreiben wir die Äquivalenzklasse von (r, u) bezüglich \sim in der Form r/u . Um die Menge der Äquivalenzklassen $R \times U / \sim = \{r/u \mid (r, u) \in R \times U\}$ zu einem Ring zu machen, definieren wir Addition und Multiplikation vertreterweise wie in der Bruchrechnung.

$$\begin{aligned} r_1/u_1 + r_2/u_2 &:= (r_1u_2 + r_2u_1)/(u_1u_2) \\ r_1/u_1 \cdot r_2/u_2 &:= (r_1r_2)/(u_1u_2), \end{aligned}$$

für alle $(r_1, u_1), (r_2, u_2) \in R \times U$.

2.76 Definition. Wir bezeichnen $R[U^{-1}] := (R \times U / \sim, +, \cdot)$ als die Lokalisierung von R bezüglich U .

2.77 Satz. Sei R ein kommutativer Halbring und U eine nicht-leere, multiplikativ abgeschlossene Teilmenge von R . Dann ist $R[U^{-1}]$ ein kommutativer Ring.

Beweis. Zur Wohldefiniertheit der oben definierten Operationen. Seien $(r_1, u_1), (r'_1, u'_1) \in R \times U$ mit $r_1/u_1 = r'_1/u'_1$, also $tr_1u'_1 = tr'_1u_1$ für ein $t \in U$. Es genügt zu zeigen, daß $(r'_1u_2 + r_2u'_1)/(u'_1u_2) = (r_1u_2 + r_2u_1)/(u_1u_2)$ und $(r'_1r_2)/(u'_1u_2) = (r_1r_2)/(u_1u_2)$ für alle $(r_2, u_2) \in R \times U$ gilt. Dann sind die Definitionen unabhängig von der Wahl der Vertreter auf der linken Seite, per Symmetrie dann auch auf der rechten Seite, und zusammen dann auf der linken und rechten Seite simultan. Für die Addition ergibt sich

$$\begin{aligned} t(r_1u_2 + r_2u_1)(u'_1u_2) &= tr_1u_2u'_1u_2 + tr_2u_1u'_1u_2 \\ &= tr'_1u_2u_1u_2 + tr_2u_1u'_1u_2 \\ &= t(r'_1u_2 + r_2u'_1)(u_1u_2) \end{aligned}$$

und für die Multiplikation ergibt sich

$$tr'_1r_2u_1u_2 = tr_1r_2u'_1u_2.$$

Dies sind genau die Bedingungen für die Klassengleichheit und somit ist die Wohldefiniertheit bewiesen.

Die Assoziativität und Distributivität von $+$ und \cdot lassen sich aufgrund der Wohldefiniertheit direkt für die Vertreter (r, u) verifizieren.

Es gilt offenbar $(r_1u)/(u_1u) = (r_1/u_1)$ für alle $(r_1, u_1) \in R \times U$ und $u \in U$. Das Nullelement von $R[U^{-1}]$ ist $0/u$ für beliebiges $u \in U$, denn $0/u + r_1/u_1 = (r_1u)/(u_1u) = r_1/u_1$. Das Einselement von $R[U^{-1}]$ ist u/u für beliebiges $u \in U$, denn $(u/u) \cdot (r_1/u_1) = (r_1u)/(u_1u) = r_1/u_1$. \square

Für die Summe $r_1/u + r_2/u$ mit gleichem Hauptnenner gilt $r_1/u + r_2/u = (r_1u + r_2u)/u^2 = ((r_1 + r_2)u)/(uu) = (r_1 + r_2)/u$, wie gewohnt.

2.78 Definition. Wir definieren eine äußere Verknüpfung $R \times R[U^{-1}] \rightarrow R[U^{-1}]$ durch $r \cdot (r_1/u_1) := (rr_1)/u_1$.

Mit der Definition gilt zum Beispiel $r \cdot 1 = (ru)/u$ für jedes $u \in U$. Gilt $1 \in U$, so erhalten wir $r \cdot 1 = r/1$.

Die folgenden Sätze sind wieder für Halbringe als auch Ringe richtig.

2.79 Satz. Sei R ein kommutativer (Halb)Ring. Die Abbildung

$$\iota_U : R \rightarrow R[U^{-1}], \quad r \mapsto r \cdot 1$$

ist ein (Halb)Ringhomomorphismus mit den folgenden Eigenschaften.

- (i) $\iota_U(U) \subseteq R[U^{-1}]^\times$ und $\iota_U(R)R[U^{-1}] = R[U^{-1}]$.
- (ii) $\ker(\iota_U) = \{r \in R \mid ur = 0 \text{ für ein } u \in U\}$.
- (iii) Für $r \in R$ und $u \in U$ gilt $r/u = \iota_U(r)\iota_U(u)^{-1}$.

Beweis. Sei $u \in U$. Für die Additivität beachten wir mit obiger Bemerkung über den Hauptnenner $\iota_U(r_1 + r_2) = ((r_1 + r_2)u)/u = (r_1u + r_2u)/u = (r_1u)/u + (r_2u)/u = \iota_U(r_1) + \iota_U(r_2)$ für alle $r_1, r_2 \in R$. Für die Multiplikativität beachten wir $\iota_U(r_1r_2) = (r_1r_2u)/u = (r_1ur_2u)/(u^2) = (r_1u)/u \cdot (r_2u)/u = \iota_U(r_1)\iota_U(r_2)$ für alle $r_1, r_2 \in R$. Besitzt R ein Einselement, so gilt ferner $\iota_U(1) = (1u)/u = u/u = 1$.

(i): Die Elemente u_1/u_2 für $u_1, u_2 \in U$ besitzen offenbar die Inversen u_2/u_1 und sind daher Einheiten in $R[U^{-1}]$. Da U nicht-leer ist, enthält das Ideal $\iota_U(R)R[U^{-1}]$ Einheiten, es gilt also $\iota_U(R)R[U^{-1}] = R[U^{-1}]$.

(ii): Sei $r \in \ker(\iota_U)$. Dann gibt es $u' \in U$ mit $ru'/u' = 0$. Also gibt es ein $u'' \in U$ mit $ru'/u' = 0/u''$. Schließlich gibt es ein $t \in U$ mit $tu'u''r = 0tu' = 0$ in R . Wegen $u = tu'u'' \in U$ gilt also $ur = 0$. Gelte umgekehrt $ur = 0$ für ein $u \in U$. Mit $\iota_U(ur) = \iota_U(u)\iota_U(r) = 0$ und $\iota_U(u) \in R[U^{-1}]^\times$ nach (i) folgt $\iota_U(r) = 0$, also $r \in \ker(\iota_U)$.

(iii): Es gilt $\iota_U(r) = ru'/u'$ und $\iota_U(u) = uu''/u''$ für $u', u'' \in U$. Dann folgt $\iota_U(r)\iota_U(u)^{-1} = (ru'u'')/(uu'u'') = r/u$. \square

Aus Aussage (i) oder (ii) folgt, daß $R[U^{-1}] = \{0\}$ für $0 \in U$ gilt. In einem Integritätsring R gilt $\ker(\iota_U) = 0$ falls $0 \notin U$, und $\iota_U : R \rightarrow R[U^{-1}]$ ist ein Monomorphismus.

Wir kommen jetzt zur universellen Eigenschaft der Lokalisierung. Eine universelle Eigenschaft ist informell folgendes. Mit Hilfe von Strukturabbildungen

formalisiert man die wesentlichen Eigenschaften einer Konstruktion, wie zum Beispiel beim direkten Produkt (Projektionen), der direkten Summe (Injektionen) oder auch des Faktorrings (kanonischer Epimorphismus). Dann stellt man noch eine Minimalitätsforderung (die Universalität) an die Konstruktion.

Die wesentliche Eigenschaft der Lokalisierung ist die folgende. Seien R ein kommutativer (Halb)Ring und $U \subseteq R$ eine nicht-leere, multiplikativ abgeschlossene Menge. Sei $\iota : R \rightarrow S$ ein Homomorphismus. Wir nennen S eine schwache Lokalisierung von R bezüglich U mit Strukturhomomorphismus ι , wenn $\iota(U) \subseteq S^\times$ gilt (diese Terminologie ist nicht Standard und wir verwenden sie nur in diesem Abschnitt). Wir nennen S eine Lokalisierung von R bezüglich U mit Strukturhomomorphismus ι , wenn die folgende universelle Bedingung erfüllt ist: Für jede weitere schwache Lokalisierung T von R bezüglich U mit Strukturhomomorphismus ϕ gibt es genau einen Homomorphismus $\psi : S \rightarrow T$ mit $\phi = \psi \circ \iota$.

2.80 Satz. *Der Ring $R[U^{-1}]$ ist eine Lokalisierung von R mit Strukturhomomorphismus ι_U . Lokalisierungen S von R bezüglich U sind bis auf Isomorphie eindeutig bestimmt.*

Beweis. Zunächst gilt wie erforderlich $\iota_U(U) \subseteq R[U^{-1}]^\times$, so daß $R[U^{-1}]$ eine schwache Lokalisierung von R bezüglich U mit Strukturhomomorphismus ι_U ist.

Sei $\phi : R \rightarrow T$ mit $\phi(U) \subseteq T^\times$. Wir definieren $\psi : R[U^{-1}] \rightarrow T$ durch $r/u \mapsto \phi(r)\phi(u)^{-1}$. Aufgrund der Homomorphieeigenschaft von ϕ ist ψ zunächst wohldefiniert: Für $r/u = r'/u'$ gibt es $t \in U$ mit $tru' = tr'u$. Daraus folgt durch Anwendung von ϕ die Gleichung $\phi(t)\phi(r)\phi(u') = \phi(t)\phi(r')\phi(u)$ und wegen $\phi(t) \in S^\times$ bereits $\phi(r)\phi(u') = \phi(r')\phi(u)$. Da $\phi(u), \phi(u') \in S^\times$ ergibt sich $\phi(r)\phi(u)^{-1} = \phi(r')\phi(u')^{-1}$.

Multiplikativität und Additivität folgen direkt aus den Rechenregeln in $R[U^{-1}]$, die gerade so gemacht sind.

Wegen $\psi(\iota_U(r)) = \psi((ru)/u) = \phi(ru)\phi(u)^{-1} = \phi(r)$ für $u \in U$ und wegen $\psi(1) = \psi(u/u) = \phi(u)\phi(u)^{-1} = 1$ ist ψ ein Homomorphismus mit $\psi \circ \iota_U = \phi$.

Sei ψ' ein anderer Homomorphismus mit $\psi' \circ \iota_U = \phi$, und sei $r/u \in R[U^{-1}]$ beliebig. Dann gilt $r/u = \iota_U(r)\iota_U(u)^{-1}$, und damit $\psi'(r/u) = \psi'(\iota_U(r)\iota_U(u)^{-1}) = \psi'(\iota_U(r))\psi'(\iota_U(u))^{-1} = \phi(r)\phi(u)^{-1}$. Daher gilt $\psi' = \psi$ und ψ ist eindeutig bestimmt.

Zur zweiten Aussage. Sei S eine Lokalisierung von R bezüglich U mit Strukturhomomorphismus ι . Nach der ersten Aussage ist $R[U^{-1}]$ ebenfalls eine solche Lokalisierung, mit Strukturhomomorphismus ι_U .

Wenn wir die universelle Eigenschaft von S auf $R[U^{-1}]$ anwenden, erhalten wir den Homomorphismus $\psi_1 : S \rightarrow R[U^{-1}]$ mit $\iota_U = \psi_1 \circ \iota$. Wenn wir die universelle Eigenschaft von $R[U^{-1}]$ auf S anwenden, erhalten wir den Homomorphismus $\psi_2 : R[U^{-1}] \rightarrow S$ mit $\iota = \psi_2 \circ \iota_U$. Damit folgt $\iota = \psi_2 \circ \psi_1 \circ \iota$ und $\iota_U = \psi_1 \circ \psi_2 \circ \iota_U$.

Wenn wir die universelle Eigenschaft von S auf S anwenden, erhalten wir den Homomorphismus $\text{id}_S : S \rightarrow S$ mit $\iota = \text{id}_S \circ \iota$. Wenn wir die universelle Eigenschaft von $R[U^{-1}]$ auf $R[U^{-1}]$ anwenden, erhalten wir den Homomorphismus $\text{id}_{R[U^{-1}]} : R[U^{-1}] \rightarrow R[U^{-1}]$ mit $\iota_U = \text{id}_{R[U^{-1}]} \circ \iota_U$.

Aufgrund der obigen Gleichungen für $\iota = \psi_2 \circ \psi_1 \circ \iota$ und $\iota_U = \psi_1 \circ \psi_2 \circ \iota_U$ folgt wegen der Eindeutigkeitsaussage in der universellen Eigenschaft $\psi_2 \circ \psi_1 = \text{id}_S$ und $\psi_1 \circ \psi_2 = \text{id}_{R[U^{-1}]}$. \square

Man kann die Lokalisierungen $R[U^{-1}]$ bis auf Isomorphie also auch durch eine universelle Eigenschaft definieren. Für die Existenz ist aber noch das Konstruktionsverfahren anzugeben.

Der nachfolgende Satz gibt Rechenregeln für Lokalisierungen an, ähnlich dem zweiten Isomorphiesatz für Faktoringe. Insbesondere liefern mehrfache Lokalisierungen mit dem „gleichen“ U nichts Neues.

2.81 Satz. *Sei R kommutativer (Halb)Ring.*

- (i) *Ist $U \subseteq R^\times$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge, so gilt $R[U^{-1}] \cong R$.*
- (ii) *Sind $U \subseteq V \subseteq R$ nicht-leere, multiplikativ abgeschlossene Teilmengen, so gilt $R[V^{-1}] \cong R[U^{-1}][\iota_U(V)^{-1}]$.*
- (iii) *Ist $U \subseteq R$ eine nicht-leere, multiplikativ abgeschlossene Teilmenge, so gilt $R[U^{-1}] \cong \iota_U(R)[\iota_U(U)^{-1}]$.*

Beweis. Aufgabe. Folgt leicht aus der universellen Eigenschaft. \square

Ist R ein kommutativer Ring, U eine nicht-leere Teilmenge mit $1 \notin U$ und $V = U \cup \{1\}$, so gilt wegen $\iota_U(1) = 1$ nach Aussage (ii) trotzdem $R[U^{-1}] = R[V^{-1}]$. Daher setzen wir für den Fall, daß R ein Einselement hat, üblicherweise $1 \in U$ voraus.

Man wendet Lokalisierung an, wenn man einen Ring „vereinfachen“ möchte. Die guten Eigenschaften von R übertragen sich auf $R[U^{-1}]$, und weitere können hinzukommen.

Wir vergleichen die Idealtheorie in R und $R[U^{-1}]$ für einen kommutativen Ring R und eine multiplikativ abgeschlossene Teilmenge U von R mit $1 \in U$. Die Idealtheorie in $R[U^{-1}]$ stellt sich dabei als Vereinfachung der Idealtheorie in R heraus. Seien $\mathfrak{I}(R)$ und $\mathfrak{I}(R[U^{-1}])$ die Mengen der Ideale von R beziehungsweise $R[U^{-1}]$. Im folgenden schreiben wir zur Vereinfachung der Notation ι für ι_U . Wir betrachten die üblichen Abbildungen

$$\begin{aligned} \iota_* : \mathfrak{I}(R) &\rightarrow \mathfrak{I}(R[U^{-1}]), I \mapsto \iota(I)R[U^{-1}], \\ \iota^* : \mathfrak{I}(R[U^{-1}]) &\rightarrow \mathfrak{I}(R), J \mapsto \iota^{-1}(J). \end{aligned}$$

Sei I ein Ideal von R . Sei $\bar{I} = \{r \in R \mid \exists u \in U \text{ mit } ur \in I\}$. Man prüft leicht nach, daß \bar{I} ein Ideal von R mit $\bar{I} \supseteq I$ ist und daß $\overline{\bar{I}} = \bar{I}$ gilt. Wir nennen \bar{I} (nur hier) den Abschluß von I bezüglich U . Gilt $\bar{I} = I$, so nennen wir I bezüglich U abgeschlossen. Bei der Berechnung von \bar{I} muß man also aus den Elementen von I soweit möglich alle Elemente von U herausdividieren, um das abgeschlossene Ideal \bar{I} aus I zu erhalten.

Im folgenden sei \mathfrak{I}_U die Menge der abgeschlossenen Ideale von R und $\pi_I : R \rightarrow R/I$ der kanonische Epimorphismus.

2.82 Satz. *Mit den eingeführten Bezeichnungen gelten*

- (i) $\iota_*(\iota^*(J)) = J$ und $\iota^*(\iota_*(I)) = \bar{I}$ für alle $J \in \mathfrak{I}(R[U^{-1}])$ und alle $I \in \mathfrak{I}(R)$.
- (ii) Es gilt $\text{im}(\iota^*) = \mathfrak{I}_U$, so daß ι_* und ι^* zueinander inverse, inklusionserhaltende Bijektionen der Mengen \mathfrak{I}_U und $\mathfrak{I}(R[U^{-1}])$ liefern.
- (iii) Für $I \in \mathfrak{I}(R)$ gilt $(R/I)[\pi_I(U)^{-1}] \cong R[U^{-1}]/\iota_*(I)$.
- (iv) ι^* erhält Inklusionen, Summen, Schnitte, Produkte und Radikale etc. Dasselbe gilt für ι_* eingeschränkt auf \mathfrak{I}_U .

Beweis. (i): Für $J \in \mathfrak{I}(R[U^{-1}])$ gilt allgemein $\iota_*(\iota^*(J)) = \iota(\iota^{-1}(J))R[U^{-1}] \subseteq J$. Für $r/u \in J$ ist aber auch $r/1 \in J$ nach Multiplikation mit $u/1 \in R[U^{-1}]$, und damit $r \in \iota^{-1}(r/1)$. Daher $r/1 \in \iota(\iota^{-1}(J))$ und $r/u \in \iota(\iota^{-1}(J))R[U^{-1}]$ nach Multiplikation mit $1/u \in R[U^{-1}]$. Wir haben damit $\iota_*(\iota^*(J)) = \iota(\iota^{-1}(J))R[U^{-1}] = J$ gezeigt.

Für $I \in \mathfrak{I}(R)$ gilt $\iota^*(\iota_*(I)) = \iota^{-1}(\iota(I)R[U^{-1}]) = \{r \in R \mid \exists u \in U \text{ mit } ur \in I\} = \bar{I}$. Zum Beweis der zweiten Gleichung beachten wir zuerst $\iota(I)R[U^{-1}] = \{x/u' \mid x \in I, u' \in U\}$, wie man leicht sieht. Weiter gilt $r \in \iota^{-1}(\iota(I)R[U^{-1}])$ für $r \in R$ genau dann, wenn $\iota(r) = r/1 \in \iota(I)R[U^{-1}] = \{x/u' \mid x \in I, u' \in U\}$ ist, wenn also $r/1 = x/u'$ für ein $x \in I$ und $u' \in U$ gilt. Dies ist aber äquivalent dazu, daß es $u \in U$ mit $ur \in I$ gibt.

(ii): Für $J \in \mathfrak{I}(R[U^{-1}])$ gilt nach Aussage (i) nun $\overline{\iota^*(J)} = \iota^*(\iota_*(\iota^*(J))) = \iota^*(J)$, also $\text{im}(\iota^*) \subseteq \mathfrak{I}_U$. Für $I \in \mathfrak{I}_U$ gilt nach Aussage (i) aber auch $I = \bar{I} = \iota^*(\iota_*(I))$, also $I \in \text{im}(\iota^*)$ und somit $\text{im}(\iota^*) = \mathfrak{I}(R[U^{-1}])$. Daher sind ι_* und ι^* nach Aussage (i) zueinander inverse Bijektionen der Mengen \mathfrak{I}_U und $\mathfrak{I}(R[U^{-1}])$.

(iii): Wir betrachten $S = (R/I)[\pi_I(U)^{-1}]$ und $\phi = \iota_{\pi_I(U)} \circ \pi_I : R \rightarrow S$. Wegen $\phi(U) \subseteq S^\times$ gibt es $\psi : R[U^{-1}] \rightarrow S$ nach Satz 2.80 mit $\psi(r/u) = (r + I)/(u + I)$. Dies zeigt, daß ψ surjektiv ist. Die Inklusion $\ker(\psi) \supseteq \iota_*(I)$ ist wegen $\iota_*(I) = \{x/u \mid x \in I, u \in U\}$ klar. Sei nun $r/u \in R[U^{-1}]$ mit $\psi(r/u) = 0$. Dann gibt es $u' \in U$ mit $(u' + I)(r + I) = 0 + I$ beziehungsweise mit $u'r \in I$ (nach dem

Kriterium, wann Elemente in einer Lokalisierung Null sind). Also gilt $r \in \bar{I}$ und $r/u \in \iota_*(\bar{I}) = \iota_*(I)$ nach Aussage (i). Dies zeigt $\ker(\psi) = \iota_*(I)$.

(iv): Die Aussagen für ι^* sind eine Hausaufgabe. Wegen der Bijektivität von ι_* und ι^* auf \mathfrak{J}_U und $\mathfrak{J}(R[U^{-1}])$ folgen die Aussagen hier dann auch für ι_* (vergleiche Satz 2.7). Zusatz zum Radikal: Es gilt zunächst ebenfalls ganz allgemein $\iota^*(\text{Rad}(J)) = \text{Rad}(\iota^*(J))$ für alle $J \in \mathfrak{J}(R[U^{-1}])$, siehe Lemma 2.19. Mit $I = \iota^*(J)$, $J = \iota_*(I)$ und durch Anwenden von ι_* ergibt sich $\text{Rad}(\iota_*(I)) = \iota_*(\text{Rad}(I))$ für alle $I \in \mathfrak{J}(R)$. \square

Wenn die Definitionen etwas modifiziert werden, kann Aussage (iii) auch in der hübschen Form $(R/I)[U^{-1}] \cong R[U^{-1}]/I[U^{-1}]$ geschrieben werden. Die Merkregel ist: Lokalisierung und Faktorisierung kommutieren!

Sei $I = \ker(\iota)$. Dann können wir den Strukturhomomorphismus $\iota : R \rightarrow R[U^{-1}]$ nach dem Homomorphiesatz in $\pi_I : R \rightarrow R/I$ und einen Monomorphismus $\phi : R/I \rightarrow R[U^{-1}]$ faktorisieren. Hierbei ist $R[U^{-1}]$ eine schwache Lokalisierung von R/I bezüglich $\pi_I(U)$ mit Strukturhomomorphismus ϕ . Weiter gilt $I = \iota^*(\iota_*(\{0\})) = \overline{\{0\}}$ und $\iota_*(I) = \iota_*(\{0\}) = \{0\}$. Nach (iii) folgt $(R/I)[\pi_I(U)^{-1}] \cong R[U^{-1}]/\iota_*(I) \cong R[U^{-1}]$. Dies zeigt, daß $R[U^{-1}]$ auch eine Lokalisierung von R/I bezüglich $\pi_I(U)$ mit injektivem Strukturhomomorphismus ϕ ist. Eine Lokalisierung mit beliebigem Strukturhomomorphismus kann also immer als eine Faktorisierung und eine anschließende Lokalisierung mit injektivem Strukturhomomorphismus aufgefaßt werden.

2.83 Satz. *Sei R kommutativer Ring und U eine multiplikativ abgeschlossene Teilmenge von R mit $1 \in U$ und $0 \notin U$. Dann übertragen sich die Eigenschaften Ring, Integritätsring, einfach, noethersch, faktoriell, Hauptidealring und euklidisch auf $R[U^{-1}]$. Die Nullteiler von $R[U^{-1}]$ sind genau die Bilder der Nullteiler von R , bis auf Multiplikation mit Einheiten. Es gilt $\text{Rad}(R[U^{-1}]) = \text{Rad}(R)R[U^{-1}]$.*

Beweis. Aufgabe, nachrechnen und die Abbildungen ι , ι_* und ι^* verwenden. Gilt zum Beispiel $R[U^{-1}] = 0$, so folgt $1 \in \ker(\iota_U)$, also gibt es $u \in U$ mit $u1 = 0$, das heißt $0 \in U$. Für $0 \notin U$ folgt also $R[U^{-1}] \neq 0$. Die Primelemente von $R[U^{-1}]$ werden für R faktoriell durch Primelemente π von R mit $\pi \nmid u$ für alle $u \in U$ gegeben. Die euklidische Gradfunktion δ_U auf $R[U^{-1}]$ wird durch $\delta_U(r/u) = \min\{\delta(x) \mid x \in \overline{(r)}\}$ gegeben.

Ist $(a/r)(b/s) = 0$ mit $a/r \neq 0$ und $b/s \neq 0$, so gibt es ein $t \in U$ mit $tab = 0$ und es gilt $ta \neq 0$ wegen $a/r \neq 0$ und $tb \neq 0$ wegen $b/s \neq 0$. Also sind a und b Nullteiler in R . \square

2.84 Korollar. *Unter der Voraussetzung $0 \notin U$ (und mit den Bezeichnungen von Satz 2.82 gilt):*

- (i) Ein Primideal \mathfrak{p} von R ist genau dann abgeschlossen, wenn $\mathfrak{p} \cap U = \emptyset$ gilt.
- (ii) Die Abbildungen ι_* und ι^* bilden die Menge der abgeschlossenen Primideale von R und die Menge der Primideale von $R[U^{-1}]$ bijektiv aufeinander ab.
- (iii) Nicht abgeschlossene Primideale werden durch ι_* auf das triviale Ideal von $R[U^{-1}]$ abgebildet.
- (iv) Abgeschlossene maximale Ideale von R werden durch ι_* auf maximale Ideale von $R[U^{-1}]$ abgebildet.

Beweis. (i): Gilt $\mathfrak{p} \cap U = \emptyset$, so folgt aus $ur \in \mathfrak{p}$ für $u \in U$ und $r \in R$ wegen $u \notin \mathfrak{p}$ bereits $r \in \mathfrak{p}$, also $\bar{\mathfrak{p}} = \mathfrak{p}$. Gilt $\mathfrak{p} \cap U \neq \emptyset$, so gibt es $u \in \mathfrak{p} \cap U$ und es gilt $ur \in \mathfrak{p}$ für alle $r \in R$, also $\bar{\mathfrak{p}} = R \neq \mathfrak{p}$.

(ii): Die Abbildung ι^* bildet Primideale auf abgeschlossene Primideale ab, nach Satz 2.53 und Satz 2.82, (ii). Sei \mathfrak{p} ein abgeschlossenes Primideal von R . Nach (i) gilt $\mathfrak{p} \cap U = \emptyset$. Betrachte $R[U^{-1}]/\iota_*(\mathfrak{p})$. Nach Satz 2.82, (iii) gilt $R[U^{-1}]/\iota_*(\mathfrak{p}) \cong (R/\mathfrak{p})[\pi_{\mathfrak{p}}(U)^{-1}]$. Da \mathfrak{p} ein Primideal ist, ist $(R/\mathfrak{p})[\pi_{\mathfrak{p}}(U)^{-1}]$ mit R/\mathfrak{p} wegen $0 \notin \pi_{\mathfrak{p}}(U)$ wegen $\mathfrak{p} \cap U = \emptyset$ nach Satz 2.83 ein Integritätsring. Dann ist auch $\iota_*(\mathfrak{p})$ ein Primideal.

(iii): Ist \mathfrak{p} nicht abgeschlossen, so gilt $\mathfrak{p} \cap U \neq \emptyset$ nach (i). Für $u \in \mathfrak{p} \cap U$ folgt $u/1 \in \iota_*(\mathfrak{p})$, also enthält $\iota_*(\mathfrak{p})$ eine Einheit ist daher gleich $R[U^{-1}]$.

(iv): Sei \mathfrak{m} ein abgeschlossenes maximales Ideal von R . Da \mathfrak{m} ein Primideal ist, ist auch $\iota_*(\mathfrak{m})$ nach (ii) ein Primideal von R . Weiter ist $(R/\mathfrak{m})[\pi_{\mathfrak{m}}(U)^{-1}]$ mit R/\mathfrak{m} wegen $0 \notin \pi_{\mathfrak{m}}(U)$ nach Satz 2.83 ein Körper. Wie in (ii) schließen wir, daß $R[U^{-1}]/\iota_*(\mathfrak{m})$ ein Körper und $\iota_*(\mathfrak{m})$ damit ein maximales Ideal ist. \square

2.85 Beispiel. Sei $R = \mathbb{Z}$, $R[U^{-1}] = \mathbb{Z}[1/2]$ und $I = n\mathbb{Z}[1/2]$ mit $n \in \mathbb{Z}^{\geq 1}$. Wir zerlegen $n = 2^v n_1$ mit n_1 ungerade. Dann gilt $I = n_1\mathbb{Z}[1/2]$, da $1/2$ eine Einheit in $\mathbb{Z}[1/2]$ ist. Unter Verwendung von ι^* für die Ideale von $\mathbb{Z}[1/2]$ und \mathbb{Z} wie oben sieht man ebenfalls $\iota^*(n\mathbb{Z}[1/2]) = n_1\mathbb{Z}$ nach Aussage (i). Nach Aussage (ii) und Aussage (iii) ergibt sich dann beispielsweise $\mathbb{Z}[1/2]/n\mathbb{Z}[1/2] \cong \mathbb{Z}/n_1\mathbb{Z}$.

Zusammenfassend schließlich ein paar typische Situationen.

2.86 Definition. Sei R ein kommutativer Ring. Für ein Primideal \mathfrak{p} ist $U = R \setminus \mathfrak{p}$ nicht-leer und multiplikativ abgeschlossen. Der Ring $R[U^{-1}]$ wird Lokalisierung von R an \mathfrak{p} genannt und mit $R_{\mathfrak{p}}$ bezeichnet.

2.87 Satz. Sei R ein kommutativer Ring. Für ein Primideal \mathfrak{p} von R ist $R_{\mathfrak{p}}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{p}R_{\mathfrak{p}}$.

Ist R ein Integritätsring, so ist das Nullideal $\{0\}$ ein Primideal von R und $R_{\{0\}}$ ein Körper.

Beweis. Wegen $1 \notin \mathfrak{p}R_{\mathfrak{p}}$ ist $\mathfrak{p}R_{\mathfrak{p}}$ ein echtes Ideal von R . Sei $x/y \in R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$. Dann gilt $x \in R \setminus \mathfrak{p} = U$ und somit $y/x \in R_{\mathfrak{p}}$ nach Definition von $R_{\mathfrak{p}}$. Folglich $x/y \in R_{\mathfrak{p}}^{\times}$, so daß nach Satz 2.74 der Ring $R_{\mathfrak{p}}$ lokal mit maximalem Ideal $\mathfrak{p}R_{\mathfrak{p}}$ ist.

Der Ring $R_{\mathfrak{p}}$ ist ein lokaler Ring mit maximalem Ideal $\{0\}$. Also gilt $R_{\mathfrak{p}}^{\times} = R_{\mathfrak{p}} \setminus \{0\}$ und $R_{\mathfrak{p}}$ ist damit nach Satz 2.74 ein Körper. \square

2.88 Definition. Sei R ein kommutativer Ring und U die multiplikativ abgeschlossene Menge aller Elemente von R , die keine Nullteiler sind. Der Ring $R[U^{-1}]$ heißt voller Quotientenring von R und wird mit $\text{Quot}(R)$ bezeichnet.

Für einen Integritätsring R ist $\text{Quot}(R)$ ein Körper und wird Quotientenkörper von R genannt.

Der Homomorphismus $\iota_U : R \rightarrow \text{Quot}(R)$ mit U wie in der Definition ist injektiv. Daher können wir R als einen Teilring von $\text{Quot}(R)$ auffassen. Für einen Integritätsring R gilt $\text{Quot}(R) = R_{\{0\}}$.

2.89 Beispiel. Sei $R = \mathbb{Z}$. Der Quotientenkörper von \mathbb{Z} ist \mathbb{Q} . Für eine Primzahl p und das Primideal $\mathfrak{p} = p\mathbb{Z}$ gilt $R_{\mathfrak{p}} = \{x/y \mid x, y \in \mathbb{Z} \text{ und } p \nmid y\}$. Das maximale Ideal ist $\mathfrak{p}R_{\mathfrak{p}} = \{x/y \mid x, y \in \mathbb{Z} \text{ und } p \nmid y, p \mid x\}$.

Ein weiteres Beispiel ist $\mathbb{Z}[1/3] = \{x/3^i \mid i \in \mathbb{Z}^{\geq 0}, x \in \mathbb{Z}\}$ oder $\mathbb{Z}[1/2, 1/3] = \{x/(2^i 3^j) \mid i, j \in \mathbb{Z}^{\geq 0}, x \in \mathbb{Z}\}$. In beiden Ringen ist 3 eine Einheit mit unendlicher Ordnung. In $\mathbb{Z}[1/2, 1/3]$ sind die Einheiten 2 und 3 sogar unabhängig, das heißt $2^i 3^j = 1$ geht nur für $i = 0$ und $j = 0$.

2.90 Beispiel. Sei $R = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $U = \langle (1, 0) \rangle$. Um $R[U^{-1}]$ zu bestimmen, berechnen wir zuerst das Bild von R in $R[U^{-1}]$ unter ι_U . Es gilt $\ker(\iota_U) = \{r \in R \mid ur = 0 \text{ für ein } u \in U\} = \{0\} \times \mathbb{Z}/5\mathbb{Z}$. Also ist $\iota_U(R) \cong R/\ker(\iota_U) \cong \mathbb{Z}/3\mathbb{Z}$. Da $\iota_U(U) \subseteq \iota_U(R)^{\times}$ gilt hier bereits $R[U^{-1}] = \iota_U(R)$. Für $R = \mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $U = \langle (3, 0) \rangle$ ergäbe sich beispielsweise $R[U^{-1}] \cong \mathbb{Z}[1/3]$.

2.91 Beispiel. Enthält U ein nilpotentes Element, so folgt $0 \in U$ und es gilt $R[U^{-1}] = 0$.

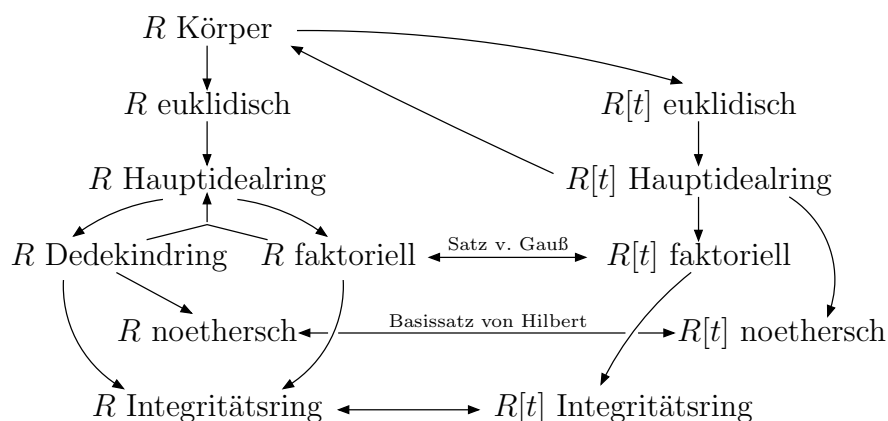
2.92 Bemerkung. Für $U = \emptyset$ definieren wir noch $R[U^{-1}] = R$. Alle Sätze dieses Abschnitts gelten dann trivialerweise, wenn R ein kommutativer Ring ist (aber nicht alle gelten, wenn R nur ein kommutativer Halbring ist).

2.93 Bemerkung. Die meisten Aussagen dieses Abschnitts können für nicht kommutative Ringe R geeignet verallgemeinert werden, wenn man U stets aus dem Zentrum $Z(R) = \{x \in R \mid xy = yx \text{ für alle } y \in R\}$ von R wählt, wenn also die Elemente aus U mit allen Elementen von R kommutieren.

Kapitel 3

Polynomringe

Wir betrachten in diesem Kapitel kommutative Ringe R (mit Einselement) und die zugehörigen Polynomringe $R[t]$. Eine Übersicht über die behandelten beziehungsweise zu behandelnden Ringeigenschaften und Beziehungen wird in der folgenden Abbildung gegeben.



Die vertikalen Implikationen wurden im wesentlichen schon bewiesen. Wir beschäftigen uns jetzt speziell mit den horizontalen Implikationen.

3.1 Univariate Polynomringe

3.1 Definition. Seien R, S kommutative Ringe und $\phi : R \rightarrow S$ ein Homomorphismus. Wir definieren äußere Verknüpfungen $\cdot : R \times S \rightarrow S$ durch $r \cdot x = \phi(r)x$ sowie $+$: $R \times S \rightarrow S$ durch $r + x = \phi(r) + x$ und $+$: $S \times R \rightarrow S$ durch $x + r = x + \phi(r)$, und nennen S mit diesen äußeren Verknüpfungen die durch ϕ definierte R -Algebra. Als Schreibweise verwenden wir wie üblich $rx = r \cdot x$.

Sind S und T R -Algebren bezüglich der Homomorphismen $\phi : R \rightarrow S$ und $\psi : R \rightarrow T$, so verstehen wir unter einem R -Algebrahomomorphismus einen Ringhomomorphismus $f : S \rightarrow T$ mit $f \circ \phi = \psi$. Analog werden R -Algebra Mono-, Epi-, Iso-, Endo- und Automorphismen definiert.

Eine zu $f \circ \phi = \psi$ äquivalente Bedingung ist die R -Linearität von f , $f(rx) = rf(x)$ für alle $r \in R$ und $x \in S$: Es gilt $\phi(r) = r \cdot 1_S$, $\psi(r) = r \cdot 1_T$ und $f(\phi(r)) = f(r \cdot 1_S) = rf(1_S) = r \cdot 1_T = \psi(r)$ und umgekehrt $f(rx) = f(\phi(r)x) = f(\phi(r))f(x) = \psi(r)f(x) = rf(x)$.

Die Homomorphieeigenschaft von ϕ impliziert die üblichen bzw. erwarteten Assoziativitäts- und Distributivitätseigenschaften von \cdot , die zur Grundlage einer allgemeineren Definition von R -Algebra gemacht werden können. In unserem speziellen Fall stimmen die Definition aber überein.

Bei den lokalen Ringen haben wir $R[U^{-1}]$ in ähnlicher Weise als R -Algebra aufgefaßt.

Nun zur Definition des (univariaten) Polynomrings. Sei R ein kommutativer Ring. Wir setzen

$$R[t] = \{f \mid f : \mathbb{Z}^{\geq 0} \rightarrow R \text{ mit } f(i) = 0 \text{ für fast alle } i \in \mathbb{Z}^{\geq 0}\}.$$

Für $f, g \in R[t]$ definieren wir $f + g \in R[t]$ durch

$$(f + g)(i) = f(i) + g(i)$$

und $f \cdot g \in R[t]$ durch

$$(f \cdot g)(i) = \sum_{\nu + \mu = i} f(\nu)g(\mu),$$

wobei ν, μ über alle Zahlen in $\mathbb{Z}^{\geq 0}$ laufen. Man sieht leicht, daß $R[t]$ mit den inneren Verknüpfungen $+$ und \cdot ein Ring ist. Das Nullelement von $R[t]$ wird durch die Funktion gegeben, welche jedes i auf 0 abbildet. Das Einselement von $R[t]$ wird durch die Funktion gegeben, welche $i = 0$ auf das Einselement 1 von R und $i \neq 0$ auf 0 abbildet. Mit t bezeichnen wir die Funktion, die $i = 1$ auf 1 und $i \neq 1$ auf 0 abbildet.

Wir erhalten auch einen Monomorphismus $\phi : R \rightarrow R[t]$, $r \mapsto h_r$ mit $h_r(i) = r \delta_{0,i}$ (Kronecker-Delta). Damit kann R als Teilring von $R[t]$ aufgefaßt werden und $R[t]$ wird zu einer R -Algebra. Es gilt $\phi(1) = 1$.

3.2 Definition. Sei R kommutativer Ring. Die eben definierte R -Algebra $R[t]$ zusammen mit dem Element t heißt Polynomring in der Variablen t über R . Die Elemente von $R[t]$ heißen Polynome in der Variablen t über R .

Zur Veranschaulichung ist es besser, die Elemente von $R[t]$ mittels t auszudrücken. Man sieht aufgrund der Definitionen sofort, daß für $f \in R[t]$ folgendes gilt: $f = \sum_{i=0}^n a_i t^i = \sum_{i=0}^n \phi(a_i) t^i$ mit $a_i = f(i) \in R$ und $n \in \mathbb{Z}^{\geq 0}$, so daß $f(j) = 0$ für alle $j > n$. Zwischen a_i und t^i steht hier die äußere Multiplikation. Die obigen Verknüpfungen sind gerade so gemacht, daß sich die erwarteten Rechenregeln für Polynome ergeben.

Zwei Polynome sind genau dann gleich, wenn alle vor den t^i auftretenden Koeffizienten gleich sind. Speziell soll hier hervorgehoben werden, daß Polynome nicht als Funktionen aufgefaßt werden, wie vielleicht aus der Analysis gewohnt. Ist k der endliche Körper mit zwei Elementen, so liefern $t \mapsto 1$ und $t \mapsto t^2 + t + 1$ die gleichen Funktionen $k \rightarrow k$, die Polynome 1 und $t^2 + t + 1$ sind aber verschiedene Elemente von $k[t]$.

Wir definieren noch ein paar grundlegende Begriffe im Zusammenhang mit Polynomringen und Polynomen. Die Polynome t^i heißen Monome. Die Polynome at^i heißen Terme. Sei $f \in R[t]$ mit $f = \sum_{i=0}^n a_i t^i$. Die a_i heißen die Koeffizienten von f . Der Grad von f ist $\deg(f) = \max\{i \mid 0 \leq i \leq n \text{ und } a_i \neq 0\}$. Es gilt insbesondere $\deg(0) = -\infty$ für $0 \in R[t]$. Für $\deg(f) \geq 0$ heißt $a_{\deg(f)}$ Leitkoeffizient von f . Der Term $a_{\deg(f)} t^{\deg(f)}$ heißt führender Term von f . Der Koeffizient a_0 heißt Absolutkoeffizient. Das Polynom f heißt normiert, wenn der Leitkoeffizient gleich 1 ist. Gilt $\deg(f) \leq 0$, so heißt das Polynom konstant. Gilt $\deg(f) = 1$, so heißt das Polynom linear (weiter quadratisch, kubisch, quartisch, quintisch, sextisch, septisch, oktisch, nonisch etc.).

Sind $f, g \in R[t]$ so gilt $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ und $\deg(fg) \leq \deg(f) + \deg(g)$ unter Nachverfolgen der führenden Terme und unter Verwendung von „sinnvollen“ Rechenregeln für $-\infty$. Die zweite Ungleichung wird hier zur Gleichung, wenn R nullteilerfrei ist.

3.3 Satz. *Sei R ein kommutativer Ring. Der Polynomring $R[t]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist. In diesem Fall gilt $R[t]^\times = R^\times$.*

Beweis. Ist $R[t]$ nullteilerfrei, so ist auch R als Teilring nullteilerfrei. Sind umgekehrt $f, g \in R[t] \setminus \{0\}$ mit $\deg(f) \geq 1$, so gilt $\deg(fg) = \deg(f) + \deg(g) \geq 1$, also $fg \neq 0$, also ist $R[t]$ mit R nullteilerfrei.

Gilt $fg = 1$, so folgt $\deg(f) + \deg(g) = 0$. Wegen $\deg(f) \geq 0$ und $\deg(g) \geq 0$ gilt $\deg(f) = \deg(g) = 0$, also $f, g \in R$. \square

Als Zusatz zur Aussage des Satzes bemerken wir, daß ein Polynom $f \neq 0$, dessen Leitkoeffizient kein Nullteiler ist, ebenfalls kein Nullteiler in $R[t]$ ist, denn es gilt $\deg(fg) = \deg(f) + \deg(g)$ für alle $g \in R[t]$.

In $(\mathbb{Z}/4\mathbb{Z})[t]$ gilt $(2t + 1)^2 = 1$, also $2t + 1 \in (\mathbb{Z}/4\mathbb{Z})[t]^\times$ als Gegenbeispiel zur zweiten Aussage von Satz 3.3, falls R nicht nullteilerfrei ist.

Sei S eine R -Algebra. Sei $f = \sum_i a_i t^i \in R[t]$ fest gewählt. Für $x \in S$ definieren wir $f(x) = \sum_i a_i x^i$ und erhalten die Polynomfunktion $S \rightarrow S$, $x \mapsto f(x)$. Wir sprechen von der Auswertung von f an x . Für $S = R[t]$ und $x = t$ gilt $f(t) = f$.

Sei nun $x \in S$ fest gewählt. Dann erhalten wir einen R -Algebrahomomorphismus $\phi_x : R[t] \rightarrow S$ durch $\phi_x(f) = f(x) = \sum_i a_i x^i$, wo $f = \sum_i a_i t^i \in R[t]$ mit $a_i \in R$ ist. Dieser R -Algebrahomomorphismus wird als Einsetzhomomorphismus bezeichnet.

Sei S eine R -Algebra und $x \in S$. Wir nennen S einen Polynomring über R in der Variablen x , wenn S die folgende universelle Eigenschaft besitzt: Für jede R -Algebra T und jedes Element $y \in T$ gibt es genau einen R -Algebrahomomorphismus $\psi : S \rightarrow T$ mit $\psi(x) = y$.

3.4 Satz. *Die R -Algebra $R[t]$ ist ein Polynomring über R in der Variablen t .*

Je zwei Polynomringe über R sind isomorph.

Beweis. Die R -Algebra $R[t]$ zusammen mit $t \in R[t]$ erfüllt die universelle Eigenschaft: Der Einsetzhomomorphismus $\phi_y : R[t] \rightarrow T$, $f \mapsto f(y)$ liefert gerade den gesuchten R -Algebrahomomorphismus $\psi : R[t] \rightarrow T$. Aufgrund der R -Algebrahomomorphieeigenschaft ist auch klar, daß ψ durch die Vorgabe von $t \mapsto y$ eindeutig bestimmt wird, denn es gilt notwendigerweise $\psi(\sum_i a_i t^i) = \sum_i a_i \psi(t)^i = \sum_i a_i y^i$.

Seien S_1, S_2 zwei kommutative R -Algebren, die jeweils die universelle Eigenschaft mit $x_1 \in S_1$ und $x_2 \in S_2$ erfüllen. Dann gibt es R -Algebrahomomorphismen $\psi_1 : S_1 \rightarrow S_2$ mit $\psi_1(x_1) = x_2$ und $\psi_2 : S_2 \rightarrow S_1$ mit $\psi_2(x_2) = x_1$. Folglich gilt $\psi_2 \circ \psi_1 : S_1 \rightarrow S_2$ mit $\psi_2(\psi_1(x_1)) = x_1$ und $\psi_1 \circ \psi_2 : S_2 \rightarrow S_1$ mit $\psi_1(\psi_2(x_2)) = x_2$. Da auch die Identitäten auf S_1 und S_2 diese Eigenschaften haben, folgt aus der Eindeutigkeitsaussage der universellen Eigenschaft, daß $\psi_2 \circ \psi_1 = \text{id}$ und $\psi_1 \circ \psi_2 = \text{id}$, also $S_1 \cong S_2$ als R -Algebren gilt. \square

Man kann die universelle Eigenschaft also als alternative Definition des Polynomrings nehmen. Aus der universellen Eigenschaft folgt, daß Polynomringe bis auf Isomorphie eindeutig bestimmt sind. Für die Existenz ist aber noch das Konstruktionsverfahren anzugeben.

3.5 Satz (Polynomdivision). *Sei R ein kommutativer Ring. Seien $f, g \in R[t]$ und g habe invertierbaren Leitkoeffizienten. Dann gibt es eindeutig bestimmte $q, r \in R[t]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.*

Beweis. Beweis der Existenz induktiv über $\deg(f)$. Für $\deg(f) < \deg(g)$ wähle $q = 0$ und $r = f$. Es gelte jetzt $\deg(f) \geq \deg(g)$. Wähle $c \in R$ mit $\deg(f - ct^{\deg(f)-\deg(g)}g) < \deg(f)$. Dies ist möglich, da der Leitkoeffizient von g invertierbar ist. Induktiv gibt es $q', r \in R[t]$ mit $f - ct^{\deg(f)-\deg(g)}g = q'g + r$ und

$\deg(r) < \deg(g)$. Setze $q = q' + ct^{\deg(f)-\deg(g)}$. Dann gilt $f = qg + r$, wie erforderlich.

Zur Eindeutigkeit bildet man die Differenz von $f = q_1g + r_1$ und $f = q_2g + r_2$ und erhält $(q_1 - q_2)g = r_1 - r_2$. Da g einen invertierbaren Leitkoeffizienten hat, muß $q_1 - q_2 = 0$ gelten, weil die linke Seite sonst einen Grad $\geq \deg(g) > \deg(r_1 - r_2)$ hätte. Dann folgt aber $r_1 - r_2 = 0$ und die Eindeutigkeit ist bewiesen. \square

Bei der Polynomdivision haben wir die Kommutativität von R gar nicht ausgenutzt. Man kann in der Tat Polynomringe und Polynomdivision geeignet für nicht kommutative Ringe definieren. Man muß dann beispielsweise zwischen Links- und Rechtsdivision unterscheiden. In der Vorlesung gehen wir hier aber nicht näher darauf ein.

3.2 Polynomringe über Körpern

3.6 Satz. *Sei R ein kommutativer Ring. Dann sind äquivalent:*

- (i) R ist ein Körper,
- (ii) $R[t]$ ist ein euklidischer Ring,
- (iii) $R[t]$ ist ein Hauptidealring.

Beweis. (i) \Rightarrow (ii): $R[t]$ ist offenbar ein Integritätsring. Darüberhinaus ist Proposition 3.5 für alle $g \neq 0$ anwendbar, und \deg erfüllt die Bedingungen einer euklidischen Gradfunktion. (ii) \Rightarrow (iii): Wurde bereits bewiesen. (iii) \Rightarrow (i): Wir betrachten den Einsetzhomomorphismus $\phi_0 : R[t] \rightarrow R$, der durch $t \mapsto 0$ definiert wird. Als Teilring von $R[t]$ ist R selbst Integritätsring. Daher ist $\ker(\phi)$ ein Primideal und als solches im Hauptidealring $R[t]$ maximal. Da ϕ surjektiv ist, ist folglich $R \cong R[t]/\ker(\phi)$ ein Körper. \square

Aufgrund von Satz 3.6 sehen wir, daß $\mathbb{Z}[t]$ kein Hauptidealring ist. Ein (maximales) Ideal, welches kein Hauptideal ist, wird zum Beispiel durch $2\mathbb{Z}[t] + t\mathbb{Z}[t]$ gegeben. Die Ergebnisse des Abschnitts 3.5 zeigen, daß $\mathbb{Z}[t]$ immerhin ein faktorieller Ring ist, und daß $2, t$ Primelemente in $\mathbb{Z}[t]$ sind.

3.7 Korollar. *Sei K ein Körper. Jedes $f \in K[t] \setminus \{0\}$ besitzt eine eindeutige Faktorisierung $f = c \prod p^{n_p}$ mit $c \in K^\times$, normierten irreduziblen $p \in K[t]$ und $n_p \geq 0$.*

Wir bemerken, daß irreduzible Polynome in $K[t]$ einen Grad ≥ 1 besitzen und daß lineare Polynome irreduzibel sind. Als Beispiel eines nicht-linearen, irreduziblen Polynoms betrachte man $f = t^2 + 1$ in $\mathbb{R}[t]$. Allerdings ist f in $\mathbb{C}[t]$ nicht mehr irreduzibel, es gilt $f = (t - i)(t + i)$ mit $i^2 = -1$.

3.8 Korollar. Sei K ein Körper und $f \in K[t]$ irreduzibel. Dann ist $K[t]/fK[t]$ ein Körper, welcher K als Teilkörper enthält.

Beweis. Für die letzte Aussage beachten wir $K \cap fK[t] = \{0\}$. Indem wir K dann mit den Klassen $\{x + fK[t] \mid x \in K\}$ identifizieren, wird K ein Teilkörper von $K[t]/fK[t]$. \square

Mit dem letzten Korollar kann man sich aus gegebenen Körpern neue konstruieren. Diese Methode wird sehr oft verwendet. Zum Beispiel gilt $\mathbb{C} \cong \mathbb{R}[t]/(x^2 + 1)$.

3.3 Nullstellen von Polynomen

3.9 Definition. Sei R kommutativer Ring und S eine kommutative R -Algebra. Sei $f \in R[t]$. Ein Element $b \in S$ heißt Nullstelle (oder Wurzel) von f in S wenn $f(b) = 0$ gilt.

Sei $b \in R$. Wird $f \in R[t]$ von $t - b$ in $R[t]$ geteilt, so gilt $f(b) = 0$. Denn es gibt $g \in R[t]$ mit $f = (t - b)g$, und Einsetzen von b liefert $f(b) = (b - b)g(b) = 0$. Hiervon gilt auch die Umkehrung:

3.10 Satz. Sei R ein kommutativer Ring und $f \in R[t]$ vom Grad $n \geq 0$. Für jede Nullstelle $b \in R$ wird f von $t - b$ geteilt.

Ist R ein Integritätsring, so besitzt f höchstens n Nullstellen in R .

Beweis. Division mit Rest durch $g = t - b$ liefert $q \in R[t]$ und $r \in R$ mit $f = q(t - b) + r$. Daraus folgt $f(b) = r = 0$, folglich ist f durch $t - b$ teilbar. Ist nun R Integritätsring und $a \neq b$ eine weitere Nullstelle von f in R , so gilt $f(a) = q(a)(a - b)$ und folglich $q(a) = 0$, da R Integritätsring ist. Wegen $\deg(q) = \deg(f) - 1$ erhält man induktiv, daß es höchstens n Nullstellen von f in R geben kann. \square

Die zweite Aussage in Satz 3.10 wird falsch, wenn R kein Integritätsring ist. Als Gegenbeispiel betrachte man $R = \mathbb{Z} \times \mathbb{Z}$. Für das Polynom $f = (t - (1, 1))(t - (2, 2))$ gilt nämlich auch $f = (t - (1, 2))(t - (2, 1))$, so daß f vier verschiedene Nullstellen in R hat und darüberhinaus sich nicht eindeutig faktorisieren läßt.

3.11 Satz. Jede endliche Untergruppe U der multiplikativen Gruppe K^\times eines Körpers K ist zyklisch.

Beweis. Sei $n = \#U$ und m der Exponent von U . Dann gilt $m \leq n$ und jedes der n Elemente von U ist Nullstelle des Polynoms $t^m - 1$ in K . Da $t^m - 1$ nach Satz 3.10 maximal m Nullstellen haben kann, folgt $n = m$. Eine abelsche Gruppe der Ordnung n und des Exponenten n ist jedoch zyklisch. \square

Ist R ein Integritätsring, $f \in R[t]$ mit $\deg(f) \geq 0$ und $b \in R$, so gibt es nach wiederholter Anwendung von Satz 3.10 ein eindeutig bestimmtes $m \in \mathbb{Z}^{\geq 1}$ und $g \in R[t]$ mit $f = (t - b)^m g$ und $g(b) \neq 0$.

3.12 Definition. Die Zahl m heißt die Vielfachheit von b in f . Für $m > 1$ nennen wir b eine mehrfache Nullstelle.

Wir können R in seinen Quotientenkörper $K = \text{Quot}(R)$ einbetten und erhalten eine Einbettung $R[t] \rightarrow K[t]$. Unter Verwendung von Satz 3.10 und Korollar 3.7 können wir also $f \in R[t]$ mit $\deg(f) \geq 0$ in der Form

$$f = g \prod_b (t - b)^{v_{t-b}(f)} \quad (3.13)$$

schreiben, wobei das Produkt über alle Nullstellen von f in R geht, insbesondere endlich ist, und $g \in R[t]$ mit $g(b) \neq 0$ für jede Nullstelle b von f in R erfüllt. Die Exponenten v_{t-b} sind dabei wie nach Satz 2.63 definiert und stimmen mit der Vielfachheit von b überein. Als Verschärfung von Satz 3.10 ergibt sich, daß f auch mit Vielfachheiten gezählt höchstens $\deg(f)$ Nullstellen besitzt.

Die Einfachheit oder Mehrfachheit einer Nullstelle kann wie folgt festgestellt werden.

3.14 Definition. Die Ableitung des Polynoms $f \in R[t]$ mit $f = \sum_{i=0}^n a_i t^i$ ist definiert als $f' = \sum_{i=1}^n i a_i t^{i-1}$.

Die Ableitung erfüllt die (üblichen) Rechenregeln $(f + g)' = f' + g'$, $(fg)' = f'g + fg'$, $(af)' = af'$ für $f, g \in R[t]$ und $a \in R$.

3.15 Satz. Sei R ein Integritätsring und $f \in R[t]$ mit $\deg(f) \geq 0$. Das Element $b \in R$ ist mehrfache Nullstelle von f genau dann, wenn $f(b) = 0$ und $f'(b) = 0$.

Beweis. Wir schreiben f wie oben $f = (t - b)^m g$. Durch Ableiten erhalten wir $f' = (x - b)^m g' + m(x - b)^{m-1} g$. Ist $m > 1$ so gilt offenbar $f(b) = 0$ und $f'(b) = 0$. Ist umgekehrt $m = 1$ so gilt $f' = (x - b)g' + g$ und folglich $f'(b) = g(b) \neq 0$. Für $f'(b) = 0$ muß daher $m > 1$ gelten. \square

3.16 Korollar. Sei K ein Körper, $f \in K[t]$ irreduzibel und F ein Erweiterungskörper von K .

- (i) Gilt $\text{char}(K) = 0$, so hat f nur einfache Nullstellen in F .
- (ii) Hat f mehrfache Nullstellen in F , so gilt $\text{char}(K) = p > 0$ und f ist von der Form $f = g(t^p)$ mit $g \in K[t]$.

Beweis. (i): Wegen $\text{char}(K) = 0$ und $\deg(f) \geq 1$ gilt $f' \neq 0$. Daher folgt aus $\deg(f') < \deg(f)$ und der Irreduzibilität von f , daß $\text{gcd}\{f, f'\} = 1$ und somit $1 = \lambda f + \mu f'$ mit geeigneten $\lambda, \mu \in K[t]$ ist. Dies gilt dann auch in $F[t]$, und f und f' haben folglich keine gemeinsamen Nullstellen in F . Wegen Satz 3.15 besitzt f also keine mehrfachen Nullstellen in F .

(ii): Es muß $f' = 0$ gelten, da sonst wie eben $\text{gcd}\{f, f'\} = 1$ wäre und es keine mehrfachen Nullstellen in F geben könnte. Wegen $f' = 0$ muß $\text{char}(K) > 0$ gelten und die Monome in f haben nur durch p teilbare Exponenten. Also ist f von der Gestalt $f = g(t^p)$. \square

Ist R ein Integritätsring mit $\text{char}(R) = p$ und hat das Polynom $f = t^p - c$ eine Nullstelle $b \in R$, so gilt $f = t^p - b^p = (t - b)^p$. Also hat f genau eine Nullstelle, und die mit Vielfachheit p .

3.4 Basissatz von Hilbert

3.17 Satz. *Sei R ein kommutativer Ring. Der Polynomring $R[t]$ ist genau dann noethersch, wenn R noethersch ist.*

Beweis. Sei $R[t]$ noethersch und I ein Ideal von R . Das von I in $R[t]$ erzeugte Ideal J ist nach Voraussetzung endlich erzeugt, $J = \sum_{i=1}^n R[t]f_i$ mit geeigneten $f_i \in R[t]$. Sei $\phi_0 : R[t] \rightarrow R$, $f \mapsto f(0)$ der Einsetzhomomorphismus bezüglich 0. Wegen $I \subseteq J$ folgt $I = \phi_0(I) \subseteq \phi_0(J)$ durch Anwendung von ϕ_0 . Auf der anderen Seite gilt wegen $J = R[t]I$ auch $\phi_0(J) \subseteq I$, zusammen also $\phi_0(J) = I$. Es folgt $I = \phi_0(J) = \sum_{i=1}^n Rf_i(0)$ und I ist ebenfalls endlich erzeugt.

Sei nun R noethersch und J ein Ideal von $R[t]$. Wir weisen die Existenz einer endlichen Menge $M \subseteq J$ mit der folgenden Eigenschaft nach: Für jedes $f \in J$ mit $f \neq 0$ gibt es $e \in \mathbb{Z}^{\geq 0}$, $\lambda_1, \dots, \lambda_n \in R$ und $f_1, \dots, f_n \in M$ mit

$$\deg\left(f - t^e \sum_{i=1}^n \lambda_i f_i\right) < \deg(f). \quad (3.18)$$

Wenn wir dies iteriert $\deg(f) + 1$ mal anwenden, reduzieren wir f modulo dem Ideal $R[t]M$ zu Null. Daraus folgt $f \in R[t]M$, also $J = R[t]M$ und J ist endlich erzeugt.

Sei $J_i = \{f \in J \mid \deg(f) \leq i\}$ und $I_i = \{a_i \mid \sum_{j=0}^i a_j t^j \in J_i\}$ für $i \in \mathbb{Z}^{\geq 0}$. Da J_i additiv und unter Multiplikation mit Elementen aus R abgeschlossen ist, handelt es sich bei I_i um ein Ideal von R . Wegen $tJ_i \subseteq J_{i+1}$ gilt $I_i \subseteq I_{i+1}$. Da R noethersch ist, gibt es $m \in \mathbb{Z}^{\geq 0}$ mit $I_i = I_m$ für alle $i \geq m$ und die I_0, \dots, I_m sind jeweils endlich erzeugt. Für $0 \leq i \leq m$ gibt es daher endliche Mengen $M_i \subseteq J_i$ derart,

daß die Leitkoeffizienten der Polynome eines jeden M_i die zugehörigen Leitkoeffizientenideale I_i erzeugen. Wir setzen $M = \cup_{i=0}^m M_i$. Aufgrund der Konstruktion von M und wegen $I_i = I_m$ für $i \geq m$ sieht man direkt, daß jeder führende Term eines $f \in J$ als führender Term eines Polynoms der Form $t^e \sum_{i=0}^n \lambda_i f_i$ mit $e \in \mathbb{Z}^{\geq 0}$, $\lambda_i \in R$ und $f_i \in M$ auftritt, daß also (3.18) gilt. \square

Der Basissatz von Hilbert liefert eine reine Existenzaussage für endliche Erzeugendensysteme von Idealen, jedoch kein sinnvolles Verfahren, wie diese zu konstruieren sind. Als Hilbert diesen Satz Ende des 19. Jahrhunderts bewies, sorgte dieser auch aufgrund seiner nicht konstruktiven Natur für erhebliches Aufsehen. Die Invariantentheorie war zu dieser Zeit ein großes und wichtiges Forschungsgebiet in der Mathematik und man schlug sich darin mit der expliziten Berechnung von Erzeugern gewisser Ideale herum. Von Gordan, einem Hauptvertreter der Invariantentheorie, stammt die Aussage, es handle sich beim Basissatz von Hilbert nicht um Mathematik, sondern um Theologie. In der Folge wurde die Axiomatisierung der Algebra vorangetrieben und man gewöhnte sich an formale, nicht konstruktive Beweise.

3.5 Satz von Gauß

Sei R ein faktorieller Ring. Wir wollen im folgenden das Faktorisierungsverhalten von Polynomen aus $R[t]$ über dem Quotientenkörper $K = \text{Quot}(R)$ von R und über R selbst untersuchen. Als Hilfsmittel verwenden wir dazu Bewertungen.

Wir beginnen zuerst mit einer allgemeinen Aussage.

3.19 Proposition. *Sei $\phi : R \rightarrow S$ ein Homomorphismus der kommutativen Ringe R und S . Dann läßt sich ϕ zu einem Homomorphismus $\psi : R[t] \rightarrow S[t]$ fortsetzen, welcher durch koeffizientenweise Anwendung von ϕ definiert ist. Ist ϕ surjektiv, so ist auch ψ surjektiv. Ferner gilt $\ker(\psi) = \ker(\phi)R[t]$.*

Beweis. Kann man direkt nachrechnen. Eine andere Argumentation ist die folgende. Wir verknüpfen ϕ mit dem Einbettungshomomorphismus $S \rightarrow S[t]$ und erhalten so $S[t]$ als R -Algebra. Der Einsetzhomomorphismus $\phi_t : R[t] \rightarrow S[t]$ wendet dann ϕ koeffizientenweise auf die Elemente von $R[t]$ an. Wir setzen also $\psi = \phi_t$. Die Aussagen über die Surjektivität und den Kern sind dann klar. \square

3.20 Proposition. *Sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Durch koeffizientenweise Reduktion modulo \mathfrak{a} erhalten wir einen Epimorphismus $\phi : R[t] \rightarrow (R/\mathfrak{a})[t]$. Folglich gilt $R[t]/\mathfrak{a}R[t] \cong (R/\mathfrak{a})[t]$ und $\mathfrak{a}R[t]$ ist genau dann ein Primideal in $R[t]$, wenn \mathfrak{a} ein Primideal in R ist.*

Beweis. Folgt aus Proposition 3.19, angewendet auf den Reduktionshomomorphismus $R \rightarrow R/\mathfrak{a}$, und dem Homomorphiesatz. Ferner gilt, daß $\mathfrak{a}R[t]$ genau dann Primideal ist, wenn $R[t]/\mathfrak{a}R[t]$ ein Integritätsring ist, und daß \mathfrak{a} genau dann Primideal ist, wenn R/\mathfrak{a} und damit $(R/\mathfrak{a})[t]$ ein Integritätsring ist. Die bereits bewiesene Isomorphie liefert daher die zu beweisende Äquivalenz. \square

Wir kommen nun zu den Bewertungen. Sei P ein Repräsentantensystem der Primelemente von R . Jedes $x \in R \setminus \{0\}$ besitzt eine eindeutige Faktorisierung $x = \varepsilon \prod_{p \in P} p^{n_p}$, wobei $\varepsilon \in R^\times$ sowie $n_p \in \mathbb{Z}^{\geq 0}$ mit $n_p = 0$ für fast alle $p \in P$. Wir setzen $v_p(x) = n_p$ und $v_p(0) = \infty$ und erhalten damit für jedes $p \in P$ eine Abbildung $v_p : R \rightarrow \mathbb{Z} \cup \{\infty\}$. Für $x, y \in R$ gilt dann offenbar $v_p(xy) = v_p(x) + v_p(y)$ und $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ unter Beachtung „sinnvoller“ Rechenregeln mit ∞ . Dies motiviert die folgende, allgemeine Definition.

3.21 Definition. Sei R ein Integritätsring. Unter einer (nicht-archimedischen, exponentiellen) Bewertung auf R verstehen wir eine Abbildung $v : R \rightarrow \mathbb{R} \cup \{\infty\}$ mit den folgenden Eigenschaften für alle $x, y \in R$.

- (i) $v(x) = \infty$ genau dann, wenn $x = 0$,
- (ii) $v(xy) = v(x) + v(y)$,
- (iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Ein weiteres Beispiel einer Bewertung wird durch die negierte Gradfunktion $-\deg$ auf $R[t]$ gegeben.

Normalerweise betrachtet man solche Bewertungen für den Fall, daß R ein Körper ist. Daher ist das folgende Lemma nützlich.

3.22 Lemma. Eine Bewertung auf dem Integritätsring R läßt sich auf eindeutige Weise zu einer Bewertung auf $K = \text{Quot}(R)$ fortsetzen.

Beweis. Man definiert $v(x/y) = v(x) - v(y)$. Die Bedingungen (i)-(iii) ergeben sich durch direktes Nachrechnen. Die Eindeutigkeit ergibt sich aus Bedingung (ii): Für $v(x/y)$ muß gelten: $v(x/y) + v(y) = v(x)$, wodurch $v(x/y)$ eindeutig festgelegt wird. \square

Ist R ein faktorieller Ring, so erhalten wir nun durch die Fortsetzung der v_p auf K für jedes $x \in K^\times$ eine eindeutige Faktorisierung $x = \varepsilon \prod_{p \in P} p^{v_p(x)}$ mit geeignetem $\varepsilon \in R^\times$. Für nicht faktorielle Ringe kann man sich die Bewertungen v als Exponenten in verallgemeinerten Faktorisierungen vorstellen.

3.23 Definition. Sei v eine Bewertung auf einem Körper K .

(i) Die Menge $R_v = \{x \in K \mid v(x) \geq 0\}$ heißt Bewertungsring von v .

(ii) Die Menge $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$ heißt Bewertungsideal von v .

3.24 Lemma. *Der Bewertungsring R_v ist ein Ring und das Bewertungsideal \mathfrak{p}_v ist ein Primideal in R_v .*

Beweis. Ergibt sich unmittelbar aus Definition 3.21, (i)-(iii). \square

Man kann darüberhinaus zeigen, daß \mathfrak{p}_v das einzige Primideal von R_v und somit maximal ist. Außerdem sind genau die Elemente in $R_v \setminus \mathfrak{p}_v$ Einheiten in R_v , kurz R_v ist ein lokaler Ring. Wir benötigen diese Aussagen für das folgende aber nicht.

3.25 Satz. *Eine Bewertung v des Integritätsrings R läßt sich zu einer Bewertung w auf $R[t]$ durch $w(f) = \min_i v(a_i)$ für $f = \sum_i a_i t^i \in R[t]$ fortsetzen.*

Beweis. Die Bedingungen (i) und (iii) aus Definition 3.21 ergeben sich direkt aus der Definition von w : Es gilt $w(f) = \infty$ genau dann, wenn alle $v(a_i) = \infty$, also $f = 0$. Für $g = \sum_i b_i t^i$ sehen wir weiterhin $w(f + g) = \min_i v(a_i + b_i) \geq \min_i \min\{v(a_i), v(b_i)\} = \min\{\min_i v(a_i), \min_i v(b_i)\} = \min\{w(f), w(g)\}$. Bedingung (ii) ist der Inhalt des nachfolgenden Lemmas von Gauß. \square

3.26 Lemma (Gauß). *Für alle $f, g \in R[t]$ gilt $w(fg) = w(f) + w(g)$.*

Beweis. Die Aussage gilt im Fall $f = 0$ oder $g = 0$. Wir nehmen daher $f \neq 0$ und $g \neq 0$ an. Wir setzen v auf $K = \text{Quot}(R)$ fort und betrachten die Aussage von Lemma 3.26 in $K[t]$. Allgemein gilt $w(ch) = v(c) + w(h)$ für $c \in K$ und $h \in K[t]$. Wir verwenden dies für die folgende Normierung. Seien r, s Indizes, für die $w(f) = v(a_r)$ und $w(g) = v(b_s)$ gilt, wobei $f = \sum_i a_i t^i$ und $g = \sum_i b_i t^i$. Wir setzen $\tilde{f} = f/a_r$ und $\tilde{g} = g/b_s$. Die Ungleichung $v(a_i/a_r) = v(a_i) - v(a_r) \geq 0$ ist scharf. Daher gilt $w(\tilde{f}) = 0$ und analog $w(\tilde{g}) = 0$. Zum Beweis des Lemmas genügt nun also $w(\tilde{f}\tilde{g}) = 0$ zu zeigen, da hieraus

$$\begin{aligned} w(fg) &= w(a_r \tilde{f} b_s \tilde{g}) = v(a_r b_s) + w(\tilde{f}\tilde{g}) = v(a_r b_s) + w(\tilde{f}) + w(\tilde{g}) \\ &= v(a_r) + v(b_s) + w(\tilde{f}) + w(\tilde{g}) = w(a_r \tilde{f}) + w(b_s \tilde{g}) = w(f) + w(g) \end{aligned}$$

folgt.

Offenbar gilt $\tilde{f}, \tilde{g} \in R_v[t]$. Sei $\phi : R_v[t] \rightarrow (R_v/\mathfrak{p}_v)[t]$ wie in Proposition 3.20 der Homomorphismus, der die Koeffizienten reduziert. Für $h \in R_v[t]$ gilt $w(h) = 0$ genau dann, wenn $\phi(h) \neq 0$. Wir haben also $\phi(\tilde{f}) \neq 0$ und $\phi(\tilde{g}) \neq 0$ wegen $w(\tilde{f}) = 0$ und $w(\tilde{g}) = 0$. Da $(R_v/\mathfrak{p}_v)[t]$ mit R_v/\mathfrak{p}_v ein Integritätsring ist, ergibt sich $\phi(\tilde{f}\tilde{g}) = \phi(\tilde{f})\phi(\tilde{g}) \neq 0$ und daraus $w(\tilde{f}\tilde{g}) = 0$. \square

3.27 Satz. Sei V eine Menge von Bewertungen des Körpers K und $R = \bigcap_{v \in V} R_v$. Sei $f \in R[t]$ normiert. Sind $g, h \in K[t]$ normiert mit $f = gh$, so gilt $g, h \in R[t]$.

Beweis. Wir setzen $v \in V$ wie in Satz 3.25 zur Bewertung w auf $K[t]$ fort. Dann gilt $w(f) = 0$, $w(g), w(h) \leq 0$ und $w(f) = w(g) + w(h)$. Es folgt $w(g) = w(h) = 0$, also $g, h \in R_v[t]$. Da dies für jedes $v \in V$ gilt, ergibt sich $g, h \in R[t]$. \square

Satz 3.27 ist ein Beispiel für das Lokal-Global Prinzip. Der Ring R wird global durch alle $v \in V$ definiert. Wir beweisen die Aussage lokal, daß heißt bezüglich R_v für jedes $v \in V$ einzeln, und können dann durch Kombination der lokalen Aussagen die globale Aussage für R erhalten.

Nach diesen allgemeinen Überlegungen kehren wir nun zu dem Fall zurück, daß R faktoriell ist.

3.28 Korollar. Sei R faktoriell, $K = \text{Quot}(R)$ und $f \in R[t]$ normiert. Sind $g, h \in K[t]$ normiert mit $f = gh$, so gilt $g, h \in R[t]$.

Beweis. Sei $V = \{v_p \mid p \in P\}$ die Menge der auf K fortgesetzten Bewertungen v_p . Für $x \in K$ gilt dann $x \in R$ genau dann, wenn $v_p(x) \geq 0$ für alle $p \in P$. Dies heißt $R = \bigcap_{v \in V} R_v$. Die Aussage folgt nun mit Satz 3.27. \square

Das Faktorisierungsverhalten normierter Polynome in $R[t]$ entspricht also dem in $K[t]$. Wir wenden uns jetzt auch nicht normierten Polynomen zu. Wir bezeichnen mit w_p die Fortsetzungen von v_p auf $K[t]$ wie oben.

3.29 Definition. Der Inhalt $I(f)$ eines Polynoms $f \in K[t] \setminus \{0\}$ ist definiert als $I(f) = \prod_{p \in P} p^{w_p(f)}$. Das Polynom f heißt primitiv, wenn $I(f) = 1$ ist.

Der Inhalt von f ist offenbar gleich dem größten gemeinsamen Teiler der Koeffizienten von f . Ferner gilt $f \in R[t]$ genau dann, wenn $I(f) \in R$. Aus Lemma 3.26 folgt $I(fg) = I(f)I(g)$. Ähnlich wie im Beweis von Lemma 3.26 können wir jedes Polynom $f \in R[t] \setminus \{0\}$ primitiv machen, indem wir seinen Inhalt $I(f)$ herausdividieren: Das Polynom $\tilde{f} = f/I(f)$ liegt in $R[t]$ und ist primitiv. Wir bemerken, daß $I(f)$ und \tilde{f} , aber nicht jedoch die Eigenschaft, primitiv zu sein, von der Wahl von P abhängen.

3.30 Satz (Gauß). Sei R kommutativ. Dann ist $R[t]$ genau dann faktoriell, wenn R faktoriell ist. In diesem Fall bestehen die Primelemente von $R[t]$ genau aus den Primelementen von R und den primitiven Polynomen in $R[t]$, welche in $K[t]$ für $K = \text{Quot}(R)$ irreduzibel sind.

Beweis. Ist $R[t]$ faktoriell, so muß auch R faktoriell sein, denn da $R[t]$ nullteilerfrei ist, enthält jede Faktorisierung von Elementen aus R in Primelemente aus $R[t]$ nur solche Faktoren, welche aus R stammen. Diese Faktoren sind auch Primelemente von R , wie man direkt an der Definition sehen kann.

Sei nun umgekehrt R faktoriell. Die Primelemente von R bleiben Primelemente in $R[t]$. Ist nämlich p ein solches, so ist R/pR und damit auch $R[t]/pR[t] \cong (R/pR)[t]$ unter Verwendung von Proposition 3.20 ein Integritätsring.

Sei nun $q \in R[t]$ primitiv und irreduzibel in $K[t]$. Wir wollen zeigen, daß q Primelement ist. Seien $f, g \in R[t]$, so daß $q \mid fg$ gilt. Da q Primelement in $K[t]$ ist, gibt es $h \in K[t]$, so daß etwa $f = qh$ gilt. Mit Lemma 3.26 sehen wir $I(q)I(h) = I(f) \in R$. Wegen $I(q) = 1$ folgt also $I(h) \in R$ und somit $h \in R[t]$. Daher gilt $q \mid f$ in $R[t]$.

Sei $f \in R[t] \setminus \{0\}$. Wir wollen zeigen, daß f in die bereits diskutierten Primelemente von $R[t]$ faktorisiert. Wir schreiben zunächst $f = a\tilde{f}$ mit $a = I(f)$ und $\tilde{f} \in R[t]$. Das Element a faktorisiert in R , und dies liefert auch eine Faktorisierung in Primelemente in $R[t]$. Für $\deg(f) = 0$ gilt $\tilde{f} = 1$ und wir sind fertig. Für $\deg(f) \geq 1$ sei $\tilde{f} = c \prod_i \tilde{f}_i$ eine Faktorisierung in irreduzible Polynome \tilde{f}_i in $K[t]$ mit $c \in K^\times$. Wir können durch geeignete Skalierung mit dem Inhalt annehmen, daß die \tilde{f}_i primitiv sind und somit auch in $R[t]$ liegen. Da \tilde{f} ebenfalls primitiv ist, folgt durch Anwendung von $I(\cdot)$ und aus der Multiplikativität von $I(\cdot)$, daß $c \in R^\times$ gilt. Daher faktorisiert \tilde{f} in die Primelemente $c\tilde{f}_1$ von $R[t]$ und \tilde{f}_i von $R[t]$ für $i > 1$. \square

Beispiele für Primelemente in $\mathbb{Z}[t]$ sind $t, -t, t+3, 2t-1, t^2-3, 5t^2-2, \dots$

3.6 Irreduzibilität von Polynomen

Es ist im allgemeinen nicht einfach, die Irreduzibilität eines Polynoms festzustellen oder seine Faktorisierung anzugeben. Es gibt keine expliziten Formeln, mit denen diese Fragen direkt beantwortet werden könnten, und man greift daher auf Algorithmen bzw. Rechenverfahren zurück. Die Entwicklung solcher Algorithmen ist ein Forschungsgebiet der Computeralgebra. Im folgenden geben wir zwei Irreduzibilitätskriterien an und beschreiben die Faktorisierungsmethode von Kronecker für Polynome über \mathbb{Z} .

3.31 Satz (Reduktionssatz). *Sei $\phi : R \rightarrow S$ ein Homomorphismus der Integritätsringe R und S und $\psi : R[t] \rightarrow S[t]$ seine Fortsetzung wie in Proposition 3.19. Sei $f \in R[t]$ mit $\deg(\psi(f)) = \deg(f)$ und $\psi(f)$ irreduzibel in $S[t]$. Sind dann $g, h \in R[t]$ mit $f = gh$, so folgt $g \in R$ oder $h \in R$.*

Beweis. Es gilt $\deg(g) + \deg(h) = \deg(f) = \deg(\psi(f)) = \deg(\psi(g)) + \deg(\psi(h))$. Wegen $\deg(\psi(g)) \leq \deg(g)$ und $\deg(\psi(h)) \leq \deg(h)$ ergibt sich $\deg(\psi(g)) = \deg(g)$ und $\deg(\psi(h)) = \deg(h)$. Es ist daher nicht möglich, daß $\deg(g) \geq 1$ und $\deg(h) \geq 1$ gilt, weil sonst $\psi(f)$ das Produkt der nicht konstanten Polynome $\psi(g)$ und $\psi(h)$ und somit nicht irreduzibel wäre. \square

Als Beispiel betrachten wir das Polynom $f = t^3 + 6t^2 + 8t + 4 \in \mathbb{Z}[t]$ und den Reduktionshomomorphismus $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$. Es gilt $\psi(f) = t^3 - t + 1 \in (\mathbb{Z}/3\mathbb{Z})[t]$. Da $\psi(f)$ keine Nullstelle in $\mathbb{Z}/3\mathbb{Z}$ besitzt, ist es irreduzibel. Folglich ist auch f irreduzibel.

Dieses Beispiel könnte den Gedanken nahelegen, daß es für jedes irreduzible Polynom $f \in \mathbb{Z}[t]$ eine Primzahl p gäbe, so daß $\psi(f) \in (\mathbb{Z}/p\mathbb{Z})[t]$ irreduzibel wäre. Dies ist jedoch nicht richtig. Das Polynom $f = t^4 - 16t^2 + 4$ ist irreduzibel in $\mathbb{Z}[t]$ und faktorisiert beispielsweise modulo jeder Primzahl entweder in zwei irreduzible Polynome vom Grad zwei oder vier Linearfaktoren. Der Beweis dieses Faktorisierungsverhaltens kann unter Verwendung der Galoistheorie geführt werden.

Satz 3.31 kann jedoch auch nutzbringend eingesetzt werden, wenn $\psi(f)$ nicht unbedingt als irreduzibel vorausgesetzt wird, sondern wenn nur Geeignetes über die möglichen Zerlegungen von $\psi(f)$ bekannt ist. Dieser Ansatz wird in dem folgenden Satz benutzt.

3.32 Satz (Irreduzibilitätskriterium von Eisenstein). *Sei R ein faktorieller Ring und $f = \sum_{i=0}^n a_i t^i \in R[t]$ ein primitives Polynom. Gibt es ein Primelement $p \in R$ mit $p \mid a_i$ für $0 \leq i \leq n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$, so ist f irreduzibel in $K[t]$ mit $K = \text{Quot}(R)$.*

Beweis. Wir nehmen an, daß f nicht irreduzibel in $K[t]$ ist. Wegen der Primitivität von f gibt es dann nach Satz 3.30 Polynome $g, h \in R[t]$ mit $f = gh$, $\deg(g) \geq 1$ und $\deg(h) \geq 1$. Sei $S = R/pR$ und $\psi : R[t] \rightarrow S[t]$ der koeffizientenweise Reduktionshomomorphismus. Weil p ein Primelement ist, ist S ein Integritätsring. Wegen $p \nmid a_n$ gilt nun $\deg(\psi(g)) = \deg(g)$ und $\deg(\psi(h)) = \deg(h)$ wie im Beweis von Satz 3.31. Wegen $p \mid a_i$ gilt weiterhin $\psi(f) = \psi(a_n)t^n = \psi(g)\psi(h)$. Sei $L = \text{Quot}(S)$. Da $L[t]$ faktoriell ist, sind $\psi(g)$ und $\psi(h)$ von der Form $\psi(g) = bt^r$ und $\psi(h) = ct^s$ mit $b, c \in S$. Wegen $r, s \geq 1$ ist dann $\psi(g)(0) = \psi(h)(0) = 0$, also $p \mid g(0)$ und $p \mid h(0)$. Damit ist p^2 ein Teiler von $g(0)h(0) = f(0) = a_0$, im Widerspruch zur Voraussetzung. \square

Satz 3.32 kann zum Beispiel auf die Polynome $f = t^n - p \in \mathbb{Z}[t]$ und $g = t^{p-1} + \dots + t + 1 \in \mathbb{Z}[t]$ angewendet werden, wo $n \geq 1$ und p eine Primzahl ist. Für g benötigt man allerdings zuerst noch einen Trick. Als Hinweis betrachte man $g = (t^p - 1)/(t - 1)$ und die durch $t \mapsto t + 1$ definierte Abbildung.

Wir beschreiben nun das Verfahren von Kronecker zur Faktorisierung von Polynomen über \mathbb{Z} . Nach Satz 3.30 können wir uns dabei auf primitive Polynome beschränken.

3.33 Proposition. *Sei K ein Körper. Sind $a_0, \dots, a_n \in K$ paarweise verschieden und $b_0, \dots, b_n \in K$, so gibt es ein eindeutig bestimmtes Polynom $f \in K[t]$ mit $\deg(f) \leq n$ und $f(a_i) = b_i$ für $0 \leq i \leq n$.*

Beweis. Zum Beweis der Eindeutigkeit sei $g \in K[t]$ ein weiteres Polynom mit $g(a_i) = b_i$. Wir setzen $h = f - g$. Dann gilt $\deg(h) \leq n$ und $h(a_i) = 0$ für $0 \leq i \leq n$. Nach Satz 3.10 muß dann $h = 0$ gelten. Für die Existenz verwenden wir den chinesischen Restsatz. Die Polynome $t - a_i$ sind irreduzibel und nach Voraussetzung paarweise teilerfremd. Daher gibt es ein $g \in K[t]$ mit $g \equiv b_i \pmod{t - a_i}$ und folglich $g(a_i) = b_i$ für $0 \leq i \leq n$. Wir können das gesuchte f mit $\deg(f) \leq n$ dann als den Rest der Division von g durch $\prod_{i=0}^n (t - a_i)$ definieren. \square

Die Berechnung des Polynoms $f \in K[t]$ kann mit dem Lagrangeschen Interpolationspolynom oder dem Newtonschen Interpolationsverfahren erfolgen.

Sei nun $f \in \mathbb{Z}[t]$ primitiv und $g, h \in \mathbb{Z}[t]$ mit $f = gh$. Dann ist $g = \pm 1$ oder $\deg(g) \geq 1$. Für paarweise verschiedene $a_i \in \mathbb{Z}$ mit $0 \leq i \leq \deg(g)$ gilt $f(a_i) = g(a_i)h(a_i)$, also $g(a_i) \mid f(a_i)$. Das Polynom g ist durch die Werte $g(a_i)$ eindeutig bestimmt. Sind die $f(a_i) \neq 0$, so gibt es für $g(a_i)$ nur endlich viele Möglichkeiten. Hieraus ergibt sich folgende Strategie, um alle Teiler von f vom Grad r zu bestimmen:

1. Bestimme paarweise verschiedene $a_0, \dots, a_r \in \mathbb{Z}$ mit $f(a_i) \neq 0$.
2. Berechne $B = \{(b_i) \in \mathbb{Z}^{r+1} : b_i \mid f(a_i) \text{ für } 0 \leq i \leq r\}$.
3. Konstruiere $g \in \mathbb{Q}[t]$ für jedes $(b_i) \in B$ unter Benutzung von Proposition 3.33.
4. Teste $\deg(g) = r$, $g \in \mathbb{Z}[t]$ und $g \mid f$.

Es ist klar, daß dies ein endliches Verfahren zur Faktorisierung von primitiven Polynomen über \mathbb{Z} liefert:

1. Ist $f \neq \pm 1$, so gibt es nichts (mehr) zu tun.
2. Bestimme einen Teiler $g \neq \pm 1$ von f kleinsten Grades.
3. Setze $f \leftarrow f/g$ und fahre mit 1. fort.

Der Teiler in Schritt 2 ist wegen der Minimalität irreduzibel. Gegebenenfalls verwendet man aus Normierungsgründen nur Teiler g mit positiven Leitkoeffizienten.

Als einfaches Beispiel betrachten wir $f = t^3 - 15t^2 + 71t - 105$ und wollen alle Linearfaktoren in f bestimmen. Da f normiert ist, müssen die Linearfaktoren ebenfalls normiert sein. Durch Auswertung bei $t = 0$ ersehen wir, daß nur $t - b$

mit $b \mid 105$ in Frage kommen kann. Wir haben $105 = 3 \cdot 5 \cdot 7$. Nachrechnen ergibt, daß $f(3) = f(5) = f(7) = 0$ ist. Also gilt $f = (t - 3)(t - 5)(t - 7)$.

Abschließend bemerken wir, daß sich das Verfahren von Kronecker rekursiv zur Faktorisierung von Polynomen über $\mathbb{Z}[t_1, \dots, t_n]$ (Definition im nächsten Abschnitt) und den entsprechenden Quotientenkörpern verallgemeinern läßt.

Moderne Algorithmen zur Polynomfaktorisierung verwenden andere, effizientere Ansätze als das Verfahren von Kronecker.

3.7 Multivariate Polynomringe

Sei R ein kommutativer Ring. Iterieren wir die Konstruktion eines univariaten Polynomrings, so erhalten wir multivariate Polynomringe.

3.34 Definition. Sei R ein kommutativer Ring und $n \in \mathbb{Z}^{\geq 0}$. Die R -Algebra $R[t_1] \cdots [t_n]$ zusammen mit den Elementen t_1, \dots, t_n heißt Polynomring in den Variablen t_1, \dots, t_n über R . Wir verwenden die Schreibweise $R[t_1, \dots, t_n]$.

Die Elemente von $R[t_1, \dots, t_n]$ heißen Polynome in den Variablen t_1, \dots, t_n über R .

Jedes Element $f \in R[t_1, \dots, t_n]$ läßt sich in der Form

$$f = \sum_{i_1, \dots, i_n=0}^m a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

mit eindeutig bestimmten $a_{i_1, \dots, i_n} \in R$ schreiben. Die Polynome $x_1^{i_1} \cdots x_n^{i_n}$ heißen Monome, die Polynome $a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$ heißen Terme und die a_{i_1, \dots, i_n} heißen die Koeffizienten von f . Man kann jetzt verschiedene Gradfunktionen definieren. Zu Gewichten w_1, \dots, w_n kann man beispielsweise $\deg(x_1^{e_1} \cdots x_n^{e_n}) = \sum_i w_i e_i$ setzen und diese Gradfunktion per Maximumsbildung auf $R[t_1, \dots, t_n]$ fortsetzen. Für $f, g \in R[t_1, \dots, t_n]$ gilt wieder $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ und $\deg(fg) \leq \deg(f) + \deg(g)$ mit Gleichheit, falls R nullteilerfrei ist. Der Totalgrad ist durch $w_i = 1$ für $1 \leq i \leq n$ gegeben. Polynomdivision bezüglich dieser allgemeineren Gradfunktionen ist im allgemeinen jedoch nicht mehr möglich (wenn nicht alle w_i bis auf ein w_j gleich Null sind). Ein Polynom f heißt homogen vom Grad d , wenn alle darin auftretenden Terme den gleichen Totalgrad d haben.

Eine R -Algebra S mit Elementen $x_1, \dots, x_n \in S$ heißt ein Polynomring über R in den Variablen x_1, \dots, x_n , wenn es für jede R -Algebra T und Elemente $y_1, \dots, y_n \in T$ genau einen R -Algebrahomomorphismus $\psi : S \rightarrow T$ mit $\psi(x_i) = y_i$ gibt.

Die Aussagen über univariate Polynomringe übertragen sich iterativ auf multivariate Polynomringe, soweit keine speziellen Annahmen über R getroffen wurden, die sich nicht iterativ fortsetzen.

3.35 Satz. *Sei R kommutativer Ring.*

- (i) $R[t_1, \dots, t_n]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist. In diesem Fall gilt $R[t_1, \dots, t_n]^\times = R^\times$.
- (ii) $R[t_1, \dots, t_n]$ ist ein Polynomring in t_1, \dots, t_n über R und ist bis auf Isomorphie eindeutig bestimmt.
- (iii) $R[t_1, \dots, t_n]$ ist genau dann noethersch, wenn R noethersch ist.
- (iv) $R[t_1, \dots, t_n]$ ist genau dann faktoriell, wenn R faktoriell ist.

Beweis. Per Induktion unter Verwendung der entsprechenden Aussagen für den univariaten Fall. □

Die Homomorphismen ψ aus der universellen Eigenschaft heißen wieder Einsetzhomomorphismen. Aufgrund von Aussage (ii) ist $R[t_1, \dots, t_n]$ für $\sigma \in S_n$ auch ein Polynomring über R in den Variablen $t_{\sigma(1)}, \dots, t_{\sigma(n)}$.

Ist S eine R -Algebra, $f \in R[t_1, \dots, t_n]$ und sind $y_1, \dots, y_n \in S$, so schreiben wir $f(y_1, \dots, y_n)$ für das Bild von f unter dem durch $t_i \mapsto y_i$ definierten Einsetzhomomorphismus $R[t_1, \dots, t_n] \rightarrow S$. Gilt $f(y_1, \dots, y_n) = 0$, so nennen wir (y_1, \dots, y_n) eine Nullstelle von f in S . Für $n > 1$ entsprechen Nullstellen von f in R keinen besonderen Faktoren von f , wie das bei $n = 1$ und Linearfaktoren der Fall ist.

Lineare Abbildungen von k -Vektorräumen können durch Angabe der Werte auf einer Basis (über k linear unabhängiges Erzeugendensystem) eindeutig definiert werden. Die Situation hier ist ganz analog: R -Algebrahomomorphismen mit Definitionsbereich $R[t_1, \dots, t_n]$ und Bildbereich eine R -Algebra können durch die Angabe der Werte auf t_1, \dots, t_n eindeutig definiert werden. Der von R und den t_1, \dots, t_n erzeugte Teilring von $R[t_1, \dots, t_n]$ ist bereits ganz $R[t_1, \dots, t_n]$. Die t_1, \dots, t_n bilden daher ein „Erzeugendensystem von $R[t_1, \dots, t_n]$ über R “. Für ein Polynom $f = \sum_{i_1, \dots, i_n=0}^m a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \in R[t_1, \dots, t_n]$ mit $f = 0$ folgt, daß alle $a_{i_1, \dots, i_n} = 0$ sind. In diesem Sinn sind die t_1, \dots, t_n also auch „über R algebraisch unabhängig“. Dies motiviert folgende Definition.

3.36 Definition. Sei R ein kommutativer Ring und S eine kommutative R -Algebra mit $R \subseteq S$. Die Elemente $y_1, \dots, y_n \in S$ heißen algebraisch unabhängig über R , wenn der Einsetzhomomorphismus $\psi : R[t_1, \dots, t_n] \rightarrow S$ mit $\psi(t_i) = y_i$ injektiv ist.

Die t_1, \dots, t_n aus $R[t_1, \dots, t_n]$ sind stets algebraisch unabhängig über R .

Für über R algebraisch unabhängige $y_1, \dots, y_n \in S$ und den Einsetzhomomorphismus $\psi : R[t_1, \dots, t_n] \rightarrow S$ mit $\psi(t_i) = y_i$ ist $\psi(R[t_1, \dots, t_n])$ eine zu $R[t_1, \dots, t_n]$ isomorphe R -Teilalgebra von S . Die y_i verhalten sich also über R wie Variablen. Zum Beispiel können wir $S = R[t_1, \dots, t_n]$ und $y_i = t_i^2$ wählen.

3.37 Definition. Sei R ein Integritätsring und $n \geq 1$. Der Quotientenkörper von $R[t_1, \dots, t_n]$ heißt Körper der rationalen Funktionen in t_1, \dots, t_n über R und wird mit $R(t_1, \dots, t_n)$ bezeichnet.

Es gilt offenbar $R(t_1, \dots, t_n) \cong \text{Quot}(R[t_1, \dots, t_i])(t_{i+1}, \dots, t_n)$ für $0 \leq i < n$. Wir fassen $R(t_1, \dots, t_n)$ wieder als R -Algebra mit den ausgezeichneten Elementen t_1, \dots, t_n auf.

3.8 Symmetrische Polynome

Sei R kommutativer Ring und $\text{Aut}_R(R[t_1, \dots, t_n])$ die Automorphismengruppe der R -Algebra $R[t_1, \dots, t_n]$. Wir wollen einen Monomorphismus $\phi : S_n \rightarrow \text{Aut}_R(R[t_1, \dots, t_n])$ und somit eine Operation von S_n auf $R[t_1, \dots, t_n]$ durch $\sigma \cdot f = \phi(\sigma)(f)$ definieren.

Sei $\sigma \in S_n$. Wir betrachten den Einsetzhomomorphismus $\phi(\sigma) : R[t_1, \dots, t_n] \rightarrow R[t_1, \dots, t_n]$, $f \mapsto f(t_{\sigma(1)}, \dots, t_{\sigma(n)})$. Offenbar gilt $\phi(\sigma) \in \text{Aut}_R(R[t_1, \dots, t_n])$, da $\phi(\sigma) \in \text{End}_R(R[t_1, \dots, t_n])$ und da $\phi(\sigma)$ bijektiv ist. Ferner ist leicht einsehbar, daß $\phi : S_n \rightarrow \text{Aut}_R(R[t_1, \dots, t_n])$, $\sigma \mapsto \phi(\sigma)$ ein Homomorphismus und injektiv ist. Damit gilt $\sigma(f + g) = \sigma f + \sigma g$, $\sigma(fg) = (\sigma f)(\sigma g)$ und $\sigma(rf) = r(\sigma f)$ für alle $f, g \in R[t_1, \dots, t_n]$, $r \in R$ und $\sigma \in S_n$.

Sei $G \leq S_n$ und $R[t_1, \dots, t_n]^G = \{f \mid f \in R[t_1, \dots, t_n] \text{ und } \sigma f = f\}$. Dann ist $R[t_1, \dots, t_n]^G$ ein Teilring von $R[t_1, \dots, t_n]$, genannt Invariantenring von $R[t_1, \dots, t_n]$ bezüglich G , und die Elemente von $R[t_1, \dots, t_n]^G$ heißen G -invariante Polynome. Wir sind speziell an $G = S_n$ interessiert, und in diesem Fall heißen die G -invarianten Polynome auch symmetrische Polynome und $R[t_1, \dots, t_n]^G$ Ring der symmetrischen Polynome.

Sei $f \in R[t_1, \dots, t_n][t]$. Wir definieren $s_i \in R[t_1, \dots, t_n]$ durch

$$f = \prod_{i=1}^n (t - t_i) = \sum_{i=0}^n (-1)^i s_i t^{n-i}. \quad (3.38)$$

Es gilt beispielsweise $s_0 = 1$, $s_1 = \sum_{i=1}^n t_i$ und $s_n = \prod_{i=1}^n t_i$. Allgemein gilt

$$s_i = \sum_{j_1 < \dots < j_i} t_{j_1} \cdots t_{j_i}. \quad (3.39)$$

Wir können die Operation von S_n auf $R[t_1, \dots, t_n]$ auf $R[t_1, \dots, t_n][t]$ durch $\sigma t = t$ fortsetzen.

3.40 Lemma. *Die s_i sind symmetrisch und homogen vom Grad i , für $0 \leq i \leq n$.*

Beweis. Es gilt $\sigma f = \prod_{i=1}^n (t - t_{\sigma(i)}) = \prod_{i=1}^n (t - t_i) = f$. Wegen $\sigma t = t$ folgt $\sigma(s_i) = s_i$ für $0 \leq i \leq n$ nach (3.38). Die Aussage über die Homogenität und den Grad folgt aus (3.39). \square

3.41 Definition. Das Polynom s_i heißt das i -te elementar-symmetrische Polynom in t_1, \dots, t_n , für $1 \leq i \leq n$.

3.42 Satz. *Jedes symmetrische Polynom in t_1, \dots, t_n läßt sich als Polynom in s_1, \dots, s_n schreiben. Die s_1, \dots, s_n sind algebraisch unabhängig über R .*

Beweis. Wir schicken eine Definition und eine Bemerkung über elementar-symmetrische Polynome voraus.

Zu Beweiszwecken definieren wir das Gewicht des Monoms $t_1^{e_1} \cdots t_n^{e_n}$ als $w(t_1^{e_1} \cdots t_n^{e_n}) = \sum_{i=1}^n i e_i$ und das Gewicht von $f \in R[t_1, \dots, t_n]$ als das Maximum der Gewichte der in f vorkommenden Monome. Dies ist gerade die durch die Gewichte $w_i = i$ definierte Gradfunktion. Dann folgt aus $w(f) \leq d$ für den Totalgrad $\deg(f(s_1, \dots, s_n)) \leq d$.

Sei $\tilde{s}_i = s_i(t_1, \dots, t_{n-1}, 0)$. Ersetzen von t_n durch 0 und Kürzen von t in Gleichung (3.38) zeigt, daß \tilde{s}_i für $1 \leq i \leq n-1$ die elementar-symmetrischen Polynome in den Variablen t_1, \dots, t_{n-1} sind (man kann dies auch an (3.39) direkt sehen).

Sei $f \in R[t_1, \dots, t_n]^{S_n}$ mit $\deg(f) = d$. Wir zeigen die folgende, genauere Aussage:

$$\text{Es gibt } g \in R[t_1, \dots, t_n] \text{ mit } w(g) \leq d \text{ und } f = g(s_1, \dots, s_n). \quad (3.43)$$

Der Beweis von (3.43) erfolgt per Induktion über n . Für $n = 1$ gilt $s_1 = t_1$, $w = \deg$ und (3.43) ist mit $g = f$ trivialerweise korrekt. Wir nehmen nun an, (3.43) sei korrekt für $n-1$ Variablen für $n \geq 2$ und führen eine weitere Induktion über d durch.

Für $d = 0$ ist f konstant und (3.43) ist mit $g = f$ wiederum trivialerweise korrekt. Sei nun $d > 0$. Wir nehmen an, daß (3.43) für kleinere Grade als d gültig ist. Dann ist $f(t_1, \dots, t_{n-1}, 0)$ als Polynom in $R[t_1, \dots, t_{n-1}]$ symmetrisch vom Grad $\leq d$ und nach der Induktionsannahme gibt es $g_1 \in R[t_1, \dots, t_{n-1}]$ mit $w(g_1) \leq d$ und $f(t_1, \dots, t_{n-1}, 0) = g_1(\tilde{s}_1, \dots, \tilde{s}_{n-1})$. Wegen $\deg(\tilde{s}_i) = \deg(s_i)$ und obiger Bemerkung über w gilt $\deg(g_1(s_1, \dots, s_{n-1})) \leq d$. Setze $f_1 = f - g_1(s_1, \dots, s_{n-1})$. Dann gilt $\deg(f_1) \leq d$ und f_1 ist symmetrisch. Weiter ist $f_1(t_1, \dots, t_{n-1}, 0) = 0$, unter Verwendung obiger Bemerkung über die \tilde{s}_i . Also gilt $t_n | f_1$ und wegen der

Symmetrie $s_n | f_1$ in $R[t_1, \dots, t_n]$. Daher gibt es $f_2 \in R[t_1, \dots, t_n]$ mit $f_1 = s_n f_2$, f_2 symmetrisch und $\deg(f_2) \leq d - n < d$. Nach der Induktionsannahme gibt es $g_2 \in R[t_1, \dots, t_n]$ mit $w(g_2) \leq d - n$ und $f_2 = g_2(s_1, \dots, s_n)$. Mit $g = g_1 + t_n g_2 \in R[t_1, \dots, t_n]$ folgt $f = g(s_1, \dots, s_n)$ und $w(g) \leq d$. Damit ist (3.43) gezeigt.

Der Beweis der algebraischen Unabhängigkeit erfolgt wieder mit Induktion über n . Für $n = 1$ ist die Aussage wegen $s_1 = t_1$ trivialerweise korrekt. Sei $f \in R[t_1, \dots, t_n]$ ein Polynom ungleich Null kleinsten Totalgrads mit $f(s_1, \dots, s_n) = 0$. Schreibe $f = \sum_{i=0}^m f_i t_n^i$ mit $f_i \in R[t_1, \dots, t_{n-1}]$. Hier gilt $f_0 \neq 0$, da sonst $f = t_n g$, $s_n g(s_1, \dots, s_n) = 0$ und damit $g(s_1, \dots, s_n) = 0$ mit $g \neq 0$ gälte, im Widerspruch zur Minimalität von $\deg(f)$. Wir erhalten $0 = f(s_1, \dots, s_n) = \sum_{i=0}^m f_i(s_1, \dots, s_{n-1}) s_n^i$ in $R[t_1, \dots, t_n]$ und nach $t_n \mapsto 0$ ergibt sich $f_0(\tilde{s}_1, \dots, \tilde{s}_{n-1}) = 0$ mit $f_0 \neq 0$, im Widerspruch zur Induktionsannahme. \square

Mit Galoistheorie, Aussagen über ganze Ringerweiterungen und über transzendente Körpererweiterungen läßt sich dieser Satz relativ gesehen leichter und kürzer, aber nicht konstruktiv beweisen. Die Relevanz des angegebenen Beweises liegt daher vornehmlich darin, daß er ein Verfahren zur Berechnung der g liefert.

Das Polynom g ist im übrigen eindeutig bestimmt, was aus der algebraischen Unabhängigkeit der s_i folgt.

3.44 Korollar. Sei $\psi : R[t_1, \dots, t_n] \rightarrow R[t_1, \dots, t_n]$ der durch $t_i \mapsto s_i$ definierte Einsetzhomomorphismus. Dann gilt $\text{im}(\psi) = R[t_1, \dots, t_n]^{S_n}$ und $\ker(\psi) = \{0\}$.

Beweis. Die Inklusion $\text{im}(\psi) \subseteq R[t_1, \dots, t_n]^{S_n}$ ist klar. Der Rest ist genau die Aussage des Satzes, nur anders formuliert. \square

Für $g_1, \dots, g_r \in R[t_1, \dots, t_n]$ setzen wir $R[g_1, \dots, g_r] = \{f(g_1, \dots, g_r) \mid f \in R[t_1, \dots, t_n]\}$. Dann ist $R[g_1, \dots, g_r]$ die von g_1, \dots, g_r erzeugte R -Unteralgebra von $R[t_1, \dots, t_n]$. Damit können wir Satz 3.42 auch so formulieren:

$$R[t_1, \dots, t_n]^{S_n} = R[s_1, \dots, s_n].$$

Die elementar-symmetrischen Polynome s_i sind nicht die einzigen algebraisch unabhängigen Polynome, mit denen dies geht. Eine andere, gebräuchliche Wahl sind die Potenzsummen S_i der Nullstellen von $f = \prod_{i=1}^n (t - t_i)$, also

$$S_i = \sum_{j=1}^n t_j^i. \quad (3.45)$$

Da die S_i symmetrisch sind, gilt $R[S_1, \dots, S_i] \subseteq R[s_1, \dots, s_n]$ für alle $i \geq 1$.

3.46 Proposition. *Es gelten die Newtonschen Relationen*

$$\begin{aligned} (-1)^k k s_k + \sum_{i=0}^{k-1} (-1)^i s_i S_{k-i} &= 0 \quad \text{für } 1 \leq k \leq n, \\ \sum_{i=0}^n (-1)^i s_i S_{k-i} &= 0 \quad \text{für } k \geq n. \end{aligned}$$

Beweis. Ein direkter Beweis kann induktiv durch Nachrechnen relativ leicht geführt werden. Für einen mehr konzeptuellen Beweis siehe Satz 3.61. \square

3.47 Korollar. *Ist $n! \in R^\times$, so gilt*

$$R[S_1, \dots, S_n] = R[s_1, \dots, s_n].$$

Wir betrachten jetzt eine Anwendung, in der symmetrische Polynome vorkommen.

3.48 Definition. Sei $f = c \prod_{i=1}^n (t - t_i)$. Die Diskriminante von f ist definiert als

$$D(f) = c^{2n-2} \prod_{i < j} (t_i - t_j)^2 = (-1)^{n(n-1)/2} c^{2n-2} \prod_{i \neq j} (t_i - t_j).$$

Für $c = 1$ handelt es sich hierbei um ein symmetrisches Polynom in den Variablen t_1, \dots, t_n , welches folglich als Polynom g_f in den Koeffizienten von f geschrieben werden kann. Daher gilt für $f \in K[t]$ stets $D(f) \in K$.

3.49 Beispiel. Für $f = t^2 + bt + c$ gilt $D(f) = b^2 - 4c$. Für $f = x^3 + at + b$ gilt $D(f) = -4a^3 - 27b^2$.

Diskriminanten kann man von jedem (normierten) Polynom über einem kommutativen Ring bilden, indem man die die Koeffizienten von f für die Variablen in g_f einsetzt.

Eine Anwendung von Diskriminanten ist es, nur anhand der Koeffizienten eines Polynoms (und der Formel für die Diskriminante) festzustellen, ob das Polynom mehrfache Nullstellen besitzt oder nicht.

3.9 Resultanten und Diskriminanten

Sei R ein Integritätsring und seien $f = \sum_{i=0}^n a_{n-i} t^i$, $g = \sum_{j=0}^m b_{m-j} t^j$ Polynome vom Grad n beziehungsweise m über R mit $n, m \geq 1$. Wir wollen eine Formel in den Koeffizienten von f und g angeben, mit der wir feststellen können, ob f und g einen gemeinsamen Teiler in $K[t]$ besitzen.

Sei $V = \{h \in K[t] \mid \deg(h) \leq n + m - 1\}$ (zusammen mit der Addition und Multiplikation mit Skalaren) der K -Vektorraum der Polynome über K vom Grad kleiner gleich $n + m - 1$. Wir erhalten einen Isomorphismus $\phi : V \rightarrow K^{n+m}$ durch $\sum_{i=0}^{n+m-1} c_{n+m-1-i}t^i \mapsto (c_0, \dots, c_{n+m-1})$ und definieren die Sylvestermatrix $S(f, g)$ als die Matrix mit den Zeilen $\phi(f), \phi(xf), \dots, \phi(x^{m-1}f), \phi(g), \phi(xg), \dots, \phi(x^{n-1}g)$. Es gilt $S(f, g) \in R^{(n+m) \times (n+m)}$.

3.50 Definition. Die Resultante von f und g ist definiert als

$$\text{Res}(f, g) = \det(S(f, g)).$$

3.51 Satz. Sei R ein Integritätsring und $K = \text{Quot}(R)$. Seien $f, g \in R[t]$ nicht konstante Polynome. Die Resultante $\text{Res}(f, g)$ von f und g besitzt die folgenden Eigenschaften:

(i) $\text{Res}(g, f) = (-1)^{nm} \text{Res}(f, g)$ und

$$\text{Res}(fh, g) = \text{Res}(f, g) \text{Res}(h, g)$$

für $h \in R[t]$.

(ii) $\text{Res}(f, g) = 0$ genau dann, wenn $\text{gcd}(f, g) \neq 1$ in $K[x]$.

(iii) $\text{Res}(f, g) \in R \cap (fR[t] + gR[t])$.

(iv) Seien $f = a_0 \prod_{i=1}^n (t - \alpha_i)$ und $g = b_0 \prod_{j=1}^m (t - \beta_j)$ mit $a_0, b_0 \neq 0$ und $\alpha_i, \beta_j \in K$. Dann gilt

$$\text{Res}(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$$

Beweis. (i): Die Matrix $S(g, f)$ geht aus der Matrix $S(f, g)$ durch nm Zeilenvertauschungen hervor. Dies zeigt die erste Aussage. Für die zweite Aussage verwenden wir ohne Beweis, daß es zu f, g, h stets einen Körper gibt, über dem f, g, h in Linearfaktoren zerfallen. Dann folgt die Gleichung direkt aus (iii).

(ii): Es gilt $\text{gcd}(f, g) = 1$ in $K[t]$ genau dann, wenn $\text{lcm}(f, g) = fg$ in $K[t]$ gilt. Letzteres gilt genau dann, wenn es keine $u, v \in K[t] \setminus \{0\}$ mit $\deg(u) \leq m - 1$, $\deg(v) \leq n - 1$ und $uf + vg = 0$ gibt. Dies aber bedeutet gerade, daß die Zeilen von $S(f, g)$ linear unabhängig sind, also $\text{Res}(f, g) = \det(S(f, g)) \neq 0$ gilt.

(iii): Nach den Entwicklungsregeln für Determinanten gilt $\text{Res}(f, g) \in R$. Für $\text{Res}(f, g) = 0$ ist nichts weiter zu zeigen. Gelte also $\text{Res}(f, g) \neq 0$. Da $S(f, g)$ vollen Rang hat, gibt es eine eindeutig bestimmte Linearkombination der Zeilen von

$S(f, g)$, welche $(0, \dots, 0, 1)$ liefert. In Polynomschreibweise (also nach Anwenden von ϕ^{-1}) erhalten wir die Existenz von eindeutig bestimmten $u, v \in K[t]$ mit $\deg(u) \leq m-1$, $\deg(v) \leq n-1$ und $1 = uf + vg$, wobei die Koeffizienten von u und v gerade die Koeffizienten der besagten Linearkombination sind. Nach der Cramerschen Regel sind die Koeffizienten von u und v daher von der Form $x/\text{Res}(f, g)$ für $x \in R$. Es gilt also $\text{Res}(f, g)u \in R[t]$ und $\text{Res}(f, g)v \in R[t]$ und somit $\text{Res}(f, g) = (\text{Res}(f, g)u)f + (\text{Res}(f, g)v)g \in fR[t] + gR[t]$.

(iv): Wir schicken eine Vorbemerkung voraus. Sei $\phi : R \rightarrow S$ ein Homomorphismus mit $\phi(a_0), \phi(b_0) \neq 0$, den wir koeffizientenweise zu $\phi : R[t] \rightarrow S[t]$ fortsetzen. Dann gilt $\phi(\text{Res}(f, g)) = \text{Res}(\phi(f), \phi(g))$, aufgrund der Entwicklungssätze für Determinanten. Sind $\alpha_i, \beta_j \in R$ und gilt

$$\text{Res}(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j),$$

so erhalten wir daher auch

$$\text{Res}(\phi(f), \phi(g)) = \phi(a_0)^m \phi(b_0)^n \prod_{i=1}^n \prod_{j=1}^m (\phi(\alpha_i) - \phi(\beta_j))$$

mit $\phi(f) = \phi(a_0) \prod_{i=1}^n (t - \phi(\alpha_i))$ und $\phi(g) = \phi(b_0) \prod_{j=1}^m (t - \phi(\beta_j))$. Es genügt daher, (iv) nur für den Polynomring

$$R = \mathbb{Z}[c, d, x_1, \dots, x_n, y_1, \dots, y_m] \quad (3.52)$$

und $f = c \prod_{i=1}^n (t - x_i)$, $g = d \prod_{j=1}^m (t - y_j)$ zu zeigen, da daraus der allgemeine Fall mittels des Einsetzhomomorphismus $\phi(c) = a_0$, $\phi(d) = b_0$, $\phi(x_i) = \alpha_i$ und $\phi(y_j) = \beta_j$ erhalten wird.

Sei nun R besagter Ring aus (3.52) und $\phi : R \rightarrow R$ der Einsetzhomomorphismus, der x_i nach y_j abbildet und ansonsten alle Variablen in sich selbst überführt. Wir setzen ϕ zu $\phi : R[t] \rightarrow R[t]$ koeffizientenweise fort. Dann gilt $\text{Res}(\phi(f), g) = 0$ nach (ii), da $\phi(f)$ und g die gemeinsame Nullstelle $y_j \in R$ besitzen. Sei R_0 der Polynomring über \mathbb{Z} in den Variablen von R außer x_i . Wir setzen $R_0[x_i]$ und R gleich. Fassen wir nun $\text{Res}(f, g)$ als Element des Polynomrings $R_0[x_i]$ auf, so besitzt $\text{Res}(f, g)$ wegen $\text{Res}(f, g)(y_j) = \phi(\text{Res}(f, g)) = \text{Res}(\phi(f), g) = 0$ die Nullstelle $y_j \in R_0$. Nach Satz 3.10 gibt es ein $h \in R_0[x_i] = R$ mit $\text{Res}(f, g) = (x_i - y_j)h$. Da R faktoriell ist und die Elemente $x_i - y_j$ für $1 \leq i \leq n$ und $1 \leq j \leq m$ paarweise nicht assoziierte Primelemente von R sind, folgt

$$\text{Res}(f, g) = w \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) \quad (3.53)$$

mit einem $w \in R$.

Die Absolutkoeffizienten von f und g sind $a_n = a_0(-1)^n x_1 \cdots x_n$ und $b_m = b_0(-1)^m y_1 \cdots y_m$. Die Anwendung der Leibnizregel auf die Berechnung der Resultante zeigt

$$\begin{aligned} \text{Res}(f, g) &= a_0^m b_m^n + (-1)^{nm} b_0^n a_n^m + \cdots \\ &= a_0^m b_0^m (-1)^{nm} (y_1 \cdots y_m)^n + b_0^n a_0^m (x_1 \cdots x_n)^m + \cdots \end{aligned} \quad (3.54)$$

Auf der anderen Seite gilt

$$w \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j) = w (x_1 \cdots x_n)^m + (-1)^{nm} w (y_1 \cdots y_m)^n + \cdots \quad (3.55)$$

Aus (3.53), (3.54) und (3.55) ergibt sich wie gewünscht $w = a_0^m b_0^n$. \square

Die Definition der Resultante liefert eine Formel für $\text{Res}(f, g)$ in den Koeffizienten von f und g . Auf der anderen Seite liefert Satz 3.51, (iii) eine Formel für $\text{Res}(f, g)$ in den Nullstellen von f und g . Diese kann auch noch wie folgt geschrieben werden:

$$\text{Res}(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i) = b_0^n \prod_{j=1}^m f(\beta_j).$$

3.56 Korollar. Sei R ein Integritätsring und $f = c \prod_{i=1}^n (t - t_i) \in R[t]$ mit $n \geq 1$. Dann gilt

$$D(f) = (-1)^{n(n-1)/2} c^{n-\deg(f')-2} \text{Res}(f, f').$$

Beweis. Es gilt $f'(t_i) = c \prod_{j \neq i} (t_i - t_j)$. Daher ergibt sich

$$\begin{aligned} \text{Res}(f, f') &= c^{\deg(f')} \prod_{i=1}^n f'(t_i) = c^{\deg(f')+n} \prod_{i=1}^n \prod_{j \neq i} (t_i - t_j) \\ &= (-1)^{n(n-1)/2} c^{\deg(f')+n} \prod_{i < j} (t_i - t_j)^2 \\ &= (-1)^{n(n-1)/2} c^{\deg(f')+n-(2n-2)} D(f). \end{aligned}$$

\square

Das Korollar liefert eine Möglichkeit, Diskriminanten von Polynomen nur aus ihren Koeffizienten zu berechnen (vergleiche Beispiel 3.49).

Will man gemeinsamen Nullstellen zweier univariater Polynome berechnen, so bildet man mittels des euklidischen Algorithmus ihren größten gemeinsamen Teiler und findet dessen Nullstellen. Für Polynome in mehreren Variablen ist dieses Vorgehen nicht mehr möglich. Man kann dafür aber die Resultante wie folgt verwenden.

3.57 Beispiel. Das erste Beispiel liefert eine Anwendung der Resultante in der algebraischen Geometrie. Seien $f, g \in \mathbb{R}[x, y]$ nicht konstant. Die Punkte $(x_0, y_0) \in \mathbb{R} \times \mathbb{R}$ mit $f(x_0, y_0) = g(x_0, y_0) = 0$ bilden eine sogenannte affine algebraische Kurve. Das Auffinden gemeinsamer Nullstellen von f und g in $\mathbb{R} \times \mathbb{R}$ bedeutet also, die Schnittpunkte dieser Kurven zu berechnen.

Sei $r = \text{Res}_y(f, g)$. Diese Notation soll bedeuten, daß f, g als univariate Polynome in y über $\mathbb{R}[x]$ angesehen werden. Daher gilt $r \in \mathbb{R}[x]$. Sei $x_0 \in \mathbb{R}$. Falls $f(x_0, y)$ und $g(x_0, y)$ als Polynome in $\mathbb{R}[y]$ mindestens eine gemeinsame Nullstelle besitzen, so folgt $r(x_0) = 0$ nach Satz 3.51, (ii). Die Berechnung der gemeinsamen Nullstellen von f und g kann daher durch die Berechnung der Nullstellen x_0 von r und die Berechnung der gemeinsamen Nullstellen von $f(x_0, y)$ und $g(x_0, y)$ erfolgen (für $r = 0$ liegen die Kurven zumindest teilweise übereinander, f und g haben einen gemeinsamen Faktor).

Dieses Verfahren läßt sich im Prinzip für die Nullstellenberechnung von Polynomen $f_1, \dots, f_n \in K[t_1, \dots, t_n]$, K ein Körper, (in geeigneten Situationen) durch mehrfache, iterierte Berechnung von Resultanten verallgemeinern.

3.58 Beispiel. Die Diskriminante eines Polynoms ist eine Invariante, mit Hilfe derer man feststellen kann, ob f mehrfache Nullstellen über dem Grundring R oder einem Erweiterungsring S von R besitzt. Ist das Polynom f beispielsweise über \mathbb{Z} gegeben, so gilt $D(f) \in \mathbb{Z}$ und die Primfaktoren p von $D(f)$ liefern genau die Charakteristiken der endlichen Körper \mathbb{F}_q mit $q = p^m$ (und $m \leq \deg(f)$), über denen das Polynom mehrfache Nullstellen hat. Dies findet Anwendung in der algebraischen Zahlentheorie.

3.59 Beispiel. Ein weiteres, einfaches Beispiel aus der algebraischen Geometrie: Wenn man die Nullstellenmenge eines Polynoms als geometrische Struktur betrachtet, dann faßt man mehrfache Nullstellen als irreguläre (singuläre) Punkte der geometrischen Struktur auf. Sei beispielsweise $f = (y - x)(y + x) = y^2 - x^2 \in R[x, y]$. Die Nullstellenmenge von f in \mathbb{R}^2 ist gleich der Vereinigung der Geraden mit Steigung 1 und -1 durch den Ursprung. Für die Diskriminante von f als Polynom in y gilt nach obiger Formel $D(f) = 4x^2$. Daher hat f dann und nur dann eine doppelte Nullstelle in y , wenn $x = 0$ ist. Dies ist offenbar richtig, da sich die beiden Geraden genau im Ursprung $x = 0, y = 0$ schneiden.

3.10 Potenzreihen- und Laurentreihenringe

Sei R ein kommutativer Ring. Die Definition des (univariaten) Potenzreihenring $R[[t]]$ in der Variablen t über R erfolgt ganz analog zu der von $R[t]$, nur daß für die Funktionen $f : \mathbb{Z}^{\geq 0} \rightarrow R$ die Bedingung $f(i) = 0$ für fast alle $i \in \mathbb{Z}^{\geq 0}$ fallen

gelassen wird. Es handelt sich bei den Elementen von $R[[t]]$ also um „Polynome mit unendlich vielen Koeffizienten“. Die Operationen $+$ und \cdot werden genauso definiert, wobei die Summe in der Definition von \cdot stets endlich ist und daher Sinn macht. Der Potenzreihenring $R[[t]]$ ist wie $R[t]$ eine R -Algebra.

Der (multivariate) Potenzreihenring $R[[t_1, \dots, t_n]]$ wird dann als $R[[t_1]] \cdots [[t_n]]$ definiert. Wir fassen $R[[t_1, \dots, t_n]]$ als R -Algebra mit den ausgezeichneten Elementen t_1, \dots, t_n auf.

Die Elemente von $R[[t_1, \dots, t_n]]$ heißen Potenzreihen in t_1, \dots, t_n über R . Jedes $f \in R[[t_1, \dots, t_n]]$ kann in der Form

$$f = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} t_1^{i_1} \cdots t_n^{i_n}$$

mit $a_{i_1, \dots, i_n} \in R$ geschrieben werden.

3.60 Lemma. *Sei R kommutativ.*

(i) *Es gilt $R[[t_1, \dots, t_n]]^\times = \{f \mid f \in R[[t_1, \dots, t_n]] \text{ und } f(0, \dots, 0) \in R^\times\}$.*

(ii) *Ist R ein Körper, so ist $R[[t_1, \dots, t_n]]$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = \sum_{i=1}^n t_i R[[t_1, \dots, t_n]]$.*

Beweis. (i): Die Inklusion „ \subseteq “ ist unmittelbar einsichtig. Für „ \supseteq “ sei f ein Element der rechten Seite. Ohne Einschränkung können wir nach Normierung $f(0, \dots, 0) = 1$ annehmen. Setze $g = 1 - f$. Dann können wir $h = \sum_{i=0}^{\infty} g^i \in R[[t_1, \dots, t_n]]$ definieren (wie und warum?) und es gilt wie bei der geometrischen Reihe $h(1 - g) = hf = 1$.

(ii): Folgt direkt aus Aussage (i) und Satz 2.74. \square

Wir können in den Reihen auch endliche Hauptteile erlauben: Die Laurentreihenringe $R((t_1, \dots, t_n))$ in den Variablen t_1, \dots, t_n über R bestehen aus den Laurentreihen

$$f = \sum_{i_1, \dots, i_n \geq m} a_{i_1, \dots, i_n} t_1^{i_1} \cdots t_n^{i_n}$$

mit $a_{i_1, \dots, i_n} \in R$ und $m \in \mathbb{Z}$. Addition und Multiplikation werden wie erwartet definiert und involvieren für jeden Koeffizienten des Ergebnis nur endlich viele Operationen in R . Der Laurentreihenring $R((t_1, \dots, t_n))$ wird wieder als R -Algebra mit den ausgezeichneten Elementen t_1, \dots, t_n aufgefaßt.

Für einen Körper k kann man mit dem Lemma leicht sehen, daß $k((t))$ ebenfalls ein Körper ist und daß speziell $k((t)) \cong \text{Quot}(k[[t]])$ gilt.

Als Anwendung dieses Abschnitts und des Abschnitts über symmetrische Polynome betrachten wir die Beziehung zwischen den Koeffizienten s_i eines Polynoms und den Potenzsummen S_i seiner Nullstellen, welche ebenfalls symmetrische

Polynome sind. Sei $K = \mathbb{Q}(t_1, \dots, t_n)$ der Körper der rationalen Funktionen in t_1, \dots, t_n über \mathbb{Q} . Im folgenden verwenden wir stillschweigend die Einbettungen $K[t] \rightarrow K(t) \rightarrow K((t))$.

3.61 Satz. Für $g = \prod_{i=1}^n (1 - t_i t)$, $s_j = \sum_{i_1 < \dots < i_j} t_{i_1} \cdots t_{i_j}$ und $S_j = \sum_{i=1}^n t_i^j$ gilt:

$$(i) \quad g = \exp\left(-\sum_{j=1}^{\infty} S_j t^j / j\right).$$

$$(ii) \quad g'/g = -\sum_{j=1}^{\infty} S_j t^{j-1}.$$

$$(iii) \quad (-1)^k k s_k + \sum_{i=0}^{k-1} (-1)^i s_i s_{k-i} = 0 \text{ für } 1 \leq k \leq n \text{ und} \\ \sum_{i=0}^n (-1)^i s_i s_{k-i} = 0 \text{ für } k \geq n.$$

Beweis. (i): Wir rechnen mit $\log(1 - t) = -\sum_{j=1}^{\infty} t^j / j$ und $\exp(t) = \sum_{j=0}^{\infty} t^j / j!$. Es gilt $\log((1 - t_1)(1 - t_2)) = \log(1 - t_1) + \log(1 - t_2)$ und $\exp(\log(1 - t)) = 1 - t$. Wir erhalten $\log(g) = -\sum_{j=1}^{\infty} S_j t^j / j$ wegen der Regel für \log und $g = \exp(-\sum_{j=1}^{\infty} S_j t^j / j)$ durch Anwenden von \exp .

(ii): Ableiten beider Seiten von $\log(g) = -\sum_{j=1}^{\infty} S_j t^j / j$ liefert Aussage (ii).

(iii): Wegen $g = \sum_{i=0}^n (-1)^i s_i t^i$ und $g' = \sum_{i=0}^n i (-1)^i s_i t^{i-1}$ folgt Aussage (iii) durch Koeffizientenvergleich in der Gleichung $g' + g \sum_{j=1}^{\infty} S_j t^{j-1} = 0$, welche nach Aussage (ii) gilt. \square

Die Aussagen des Satzes können nun spezialisiert werden: Aussage (i) ist in $\mathbb{Q}[t_1, \dots, t_n][[t]]$ gegeben und bleibt daher für jeden Körper K mit $\text{char}(K) = 0$ und $t_1, \dots, t_n \in K$ wahr. Die Aussagen (ii) und (iii) sind über $\mathbb{Z}[t_1, \dots, t_n][t]$ gegeben (für (iii) noch mit g multiplizieren) und gelten daher für jeden Ring R und $t_1, \dots, t_n \in R$.

Die Zuordnung $K[t] \setminus \{0\} \rightarrow K((t))$, $f \mapsto f'/f$ für einen beliebigen Körper K heißt im übrigen logarithmische Ableitung und erfüllt $(fg)'/(fg) = f'/f + g'/g$.

Mittels Aussage (iii) kann man die Koeffizienten eines Polynoms und die Potenzsummen ineinander umrechnen, sofern die Charakteristik größer als n ist. Diese Relationen heißen wie schon erwähnt Newtonsche Relationen.

Der Satz kann für Endomorphismen endlichdimensionaler Vektorräume angewendet werden. Ist f das charakteristische Polynom eines Endomorphismus ϕ , so wird f durch die Spuren der Potenzen von ϕ eindeutig bestimmt, vorausgesetzt, die Charakteristik ist groß genug. Das ist vorteilhaft, wenn die Spuren besser zugänglich sind als die Koeffizienten von f . Eine Anwendung in diese Richtung erfolgt bei den Zetafunktionen von algebraischen Kurven über endlichen Körpern bzw. den charakteristischen Polynomen der zugehörigen Frobeniusendomorphismen.

3.11 Monoid- und Gruppenringe

Sei R ein Ring und G ein Monoid. Wir setzen

$$R[G] = \{f \mid f : G \rightarrow R \text{ und } f(x) = 0 \text{ für fast alle } x \in G \}.$$

Für $f, h \in R[G]$ definieren wir $f + h \in R[G]$ durch

$$(f + h)(x) = f(x) + h(x)$$

und $f \cdot h \in R[G]$ durch

$$(f \cdot h)(x) = \sum_{uv=x} f(u)h(v)$$

für alle $x \in G$, wobei die Summe über alle $u, v \in G$ mit $uv = x$ läuft. Die Summe erstreckt sich nur über endlich viele von Null verschiedene Summanden, so daß die Definition Sinn macht.

Man sieht leicht, daß $R[G]$ mit den inneren Verknüpfungen $+$ und \cdot ein Ring ist. Das Nullelement von $R[G]$ wird durch die Funktion f mit $f(x) = 0$ für alle $x \in G$ gegeben. Das Einselement von $R[G]$ wird durch die Funktion f mit $f(1) = 1$ und $f(x) = 0$ für $x \neq 1$ gegeben.

Seien $g \in G$ und $r \in R$. Mit $f_{r,g}$ bezeichnen wir die durch $f_{r,g}(g) = r$ und $f_{r,g}(x) = 0$ für $x \neq g$ definierte Funktion. Dies liefert einen Monomorphismus $R \rightarrow R[G]$, $r \mapsto f_{r,1}$, so daß wir R als Teilring von $R[G]$ auffassen können und $R[G]$ zu einer R -Algebra wird. Darüberhinaus erhalten wir einen Monomorphismus $G \rightarrow R[G]^\times$, $g \mapsto f_{1,g}$ und fassen G als Untergruppe von $R[G]^\times$ auf. Entsprechend schreiben wir auch g statt $f_{1,g}$.

3.62 Definition. Sei R ein Ring. Die eben definierte R -Algebra $R[G]$ zusammen mit dem Monomorphismus $G \rightarrow R[G]^\times$ heißt Monoidring von G über R . Ist G eine Gruppe, so heißt $R[G]$ auch Gruppenring von G über R .

Zur Veranschaulichung ist es besser, die Elemente von $R[G]$ mittels der g auszudrücken. Man sieht aufgrund der Definitionen sofort, daß für $f \in R[G]$ folgendes gilt:

$$f = \sum_{g \in G} a_g g,$$

mit $a_g = f(g)$ fast alle Null. Zwischen a_g und g steht hier die äußere Multiplikation. Die obigen Verknüpfungen sind gerade so gemacht, daß sich die „erwarteten“ Rechenregeln ergeben.

3.63 Beispiel. Für einen kommutativen Ring R und den Monoid $G = (\mathbb{Z}^{\geq 0}, +)$ ergibt sich $R[G] \cong R[t]$ und $R[G^n] \cong R[t_1, \dots, t_n]$. Für $G = (\mathbb{Z}/n\mathbb{Z}, +)$ ergibt sich $R[G] \cong R[t]/(t^n - 1)R[t]$.

Bei diesen Isomorphismen wird das Einselement von G auf t beziehungsweise der i -te Einheitsvektor e_i auf t_i abgebildet.

Motiviert durch das Beispiel können Polynomringe in beliebig vielen Variablen wie folgt definiert werden.

3.64 Definition. Sei R ein kommutativer Ring und I eine Menge. Sei $G \leq \prod_{j \in I} (\mathbb{Z}^{\geq 0}, +)$ der Untermonoid des Produkt der Monoide $(\mathbb{Z}^{\geq 0}, +)$, welcher aus allen Elementen des Produkts besteht, deren Koordinaten fast alle Null sind. Seien $t_i \in G$ mit $t_i(j) = \delta_{i,j}$ und $T = \{t_i \mid i \in I\}$. Dann heißt T die durch I indizierte Variablenmenge.

Der Polynomring $R[T]$ mit der durch I indizierten Variablenmenge T über R ist die R -Algebra $R[G]$ zusammen mit den $t_i \in T$ für $i \in I$.

3.65 Bemerkung. Für unendliches I ist $R[T]$ nicht mehr noethersch, auch wenn R noethersch ist. $R[T]$ ist aber immer noch faktoriell, wenn R faktoriell ist.

3.66 Bemerkung. Analog zu den multivariaten Polynomringen können wir auch $R[[G]]$ für einen Monoid definieren, wenn es für jedes $g \in G$ nur endlich viele $\nu, \mu \in G$ mit $\nu\mu = g$ gibt, damit die Summe in der Definition von \cdot wieder nur endlich ist.

3.67 Bemerkung. Mit Gruppenringen können interessante, nicht kommutative Ringe definiert werden.

Kapitel 4

Moduln I

Ein Modul ist ein „Vektorraum“ über K , wobei K nicht unbedingt ein Körper, sondern nur noch ein Ring zu sein braucht. Die Modultheorie kann als gemeinsame Verallgemeinerung der Ringtheorie und der linearen Algebra angesehen werden. Da die Theorie sehr umfangreich ist, können hier im wesentlichen nur grundlegende Definitionen und Sätze angeführt werden.

4.1 Grundlagen

Im folgenden bezeichnet R immer einen (nicht notwendigerweise kommutativen) Ring mit Eins. Ringhomomorphismen bilden Einselemente auf Einselemente ab.

4.1 Definition. Sei M eine abelsche Gruppe. Wir betrachten eine Multiplikation $\cdot : R \times M \rightarrow M$ mit

$$\begin{aligned} r \cdot (x + y) &= r \cdot x + r \cdot y, \quad (r + s) \cdot x = r \cdot x + s \cdot x \quad (\text{Distributivgesetze}) \\ (sr) \cdot x &= s \cdot (r \cdot x) \quad (\text{Assoziativitätsgesetz}) \end{aligned}$$

für alle $r, s \in R$ und $x, y \in M$. Außerdem gelte $1 \cdot x = x$ für alle $x \in M$. Dann heißt M zusammen mit \cdot ein R -Linksmodul.

Wie bei der Multiplikation in Ringen lassen wir \cdot fort und schreiben nur rx statt $r \cdot x$.

4.2 Beispiel. Jeder Vektorraum über einem Körper K ist ein K -Linksmodul. Jeder Ring R und jedes Linksideal von R ist ein R -Linksmodul. Umgekehrt ist jedes Linksideal von R ein R -Linksmodul. Abelsche Gruppen M sind \mathbb{Z} -Linksmoduln.

Ist M ein R -Linksmodul und $r \in R$, so ist die Abbildung $x \mapsto rx$ ein Endomorphismus der abelschen Gruppe M , entsprechend erhalten wir einen Homomorphismus $\phi : R \rightarrow \text{End}(M)$. Ist umgekehrt M eine abelsche Gruppe und

$\phi : R \rightarrow \text{End}(M)$ ein Homomorphismus, so definieren wir $rx = \phi(r)(x)$ für alle $r \in R$ und $x \in M$ und erhalten so einen R -Linksmodul M . Dies liefert also auch eine alternative Definition von R -Linksmodul.

Bei Linksmoduln wird R von links an M multipliziert. Analog zu Definition 4.1 definiert man R -Rechtsmoduln.

Für nicht kommutative Ringe ist es im allgemeinen nicht möglich, einen R -Linksmodul M zu einem R -Rechtsmodul zu machen, indem man $xr := rx$ definiert. Wegen der Assoziativgesetze müßte sonst gelten $(r_1r_2)x = x(r_1r_2) = (xr_1)r_2 = r_2(xr_1) = r_2(r_1x) = (r_2r_1)x$ für $r_1, r_2 \in R$ und $x \in M$. Für kommutative Ringe ergibt sich jedoch kein Problem und man läßt die Unterscheidung in Links- und Rechtsmoduln üblicherweise fallen.

Ist M ein R -Linksmodul, so kann man M auf die offensichtliche Weise zu einem R^{opp} -Rechtsmodul machen, wobei der Ring R^{opp} aus R entsteht, indem man die Multiplikation in R andersherum definiert bzw. ausführt. Entsprechend sind die Begriffe Linksmodul und Rechtsmodul symmetrisch und es genügt, sich nur auf Linksmoduln zu konzentrieren. Daher soll im folgenden ein R -Modul immer einen R -Linksmodul bezeichnen.

Bei Moduln M ist es häufig praktisch, zuerst an die additive Struktur und dann an die R -lineare Struktur zu denken.

4.3 Definition. Ein Homomorphismus $f : M \rightarrow N$ der R -Moduln M und N ist ein Homomorphismus der abelschen Gruppen M und N , welcher R -linear ist, für den also $f(rx) = rf(x)$ für alle $x \in M$ und $r \in R$ gilt.

Die Menge der Homomorphismen von M nach N wird mit $\text{Hom}_R(M, N)$ bezeichnet. Für $f, g \in \text{Hom}_R(M, N)$ definieren wir $f + g \in \text{Hom}_R(M, N)$ durch $(f + g)(x) = f(x) + g(x)$. Damit wird $\text{Hom}_R(M, N)$ zu einer abelschen Gruppe.

Wir benötigen weitere Definitionen, die auf der Hand liegen: Ist U eine Teilmenge von M und I ein Ideal von R , so definieren wir $IU = \{\sum_{i=1}^n r_i x_i \mid n \in \mathbb{Z}^{\geq 0}, r_i \in I, x_i \in U\}$. Ist $U \subseteq M$ eine Untergruppe des R -Moduls M und gilt $RU \subseteq U$, so heißt U ein Untermodul von M . Für jedes Ideal I von R und eine beliebige Teilmenge $U \subseteq M$ ist IU ein Untermodul von M . Für zwei Untermoduln U, V von M ist die Summe abelscher Gruppen $U + V$ wieder ein Untermodul von M (also unter Multiplikation mit R abgeschlossen), ebenso $U \cap V$. Analog wie für (abelsche) Gruppen definieren wir das direkte Produkt und die direkte Summe von Moduln. Wie bei Vektorräumen definieren wir Linearkombination, Erzeugendensystem, endlich erzeugt, linear unabhängig über R , Basis, innere und äußere direkte Summe, Mono-, Epi-, Iso-, Endo- und Automorphismen. Hintereinanderausführung von Abbildungen liefert einen Homomorphismus $\text{Hom}_R(M, N) \times \text{Hom}_R(N, P) \rightarrow \text{Hom}_R(M, P)$. Die zu einem Isomorphismus inverse Abbildung ist wieder ein Isomorphismus. Sei $f \in \text{Hom}_R(M, N)$. Dann sind der

Kern $\ker(f)$ und das Bild $\operatorname{im}(f)$ als abelsche Gruppen wegen der R -Linearität von f Untermoduln von M bzw. N . Für einen Untermodul U von M können wir M/U als Faktorgruppe abelscher Gruppen betrachten. Wegen $RU \subseteq U$ können wir auf den Klassen vertreterweise eine Multiplikation mit R definieren, dies macht M/U zu einem R -Modul, dem Faktormodul von M nach U . Der kanonische Epimorphismus abelscher Gruppen $\pi : M \rightarrow M/U$ ist dann (per Definition) R -linear, also $\pi \in \operatorname{Hom}_R(M/U, N)$. Der Kokern eines $f \in \operatorname{Hom}_R(M, N)$ ist als $N/\operatorname{im}(f)$ definiert.

Es gelten wieder Homomorphie- und Isomorphiesätze:

4.4 Satz. *Seien M, N R -Moduln.*

- (i) *Für $f \in \operatorname{Hom}_R(M, N)$ und U einen Untermodul von M mit $U \subseteq \ker(f)$ gibt es genau ein $g \in \operatorname{Hom}_R(M/U, N)$ mit $f = g \circ \pi$, wobei $\pi \in \operatorname{Hom}_R(M, M/U)$ der kanonische Epimorphismus ist.*
- (ii) *Für $f \in \operatorname{Hom}_R(M, N)$ gilt $M/\ker(f) \cong \operatorname{im}(f)$.*
- (iii) *Für Untermoduln U, V von M gilt $(U + V)/V \cong U/(U \cap V)$.*
- (iv) *Für Untermoduln U, V von M mit $U \subseteq V$ gilt $(M/U)/(V/U) \cong M/V$.*

Beweis. Für die unterliegenden abelschen Gruppen wurden diese Aussagen bereits in der Gruppentheorie gezeigt.

Zu (i) und (ii). Es gibt es zu jedem $x \in M/U$ ein $y \in \pi^{-1}(\{x\})$. Ist auch $r \in R$ beliebig, so gilt $g(rx) = g(r\pi(y)) = g(\pi(ry)) = f(ry) = rf(y) = rg(\pi(y)) = rg(x)$. Daher ist g R -linear, also $g \in \operatorname{Hom}_R(M/U, N)$, und Aussage (i) ist bewiesen. Aussage (ii) ist dann eine direkte Folgerung aus (i).

Die Isomorphismen aus (iii) und (iv) werden jeweils durch einen kanonischen Epimorphismus abelscher Gruppen induziert. Da diese kanonischen Epimorphismen hier zusätzlich R -linear sind, sind auch die induzierten Isomorphismen R -linear. \square

Wir kommen jetzt zu ein paar grundlegenden Begriffen, die bei Vektorräumen nur trivial auftreten oder zusammenfallen.

4.5 Definition. Sei M ein R -Modul. Für einen Untermodul U von M heißt $\operatorname{Ann}(U) = \{r \in R \mid rx = 0 \text{ für alle } x \in U\}$ der Annulator von U . Ferner heißt M treu, wenn $\operatorname{Ann}(M) = \{0\}$ gilt.

Die Menge der Torsionselemente (oder Nullteiler) von M ist $\operatorname{Tor}(M) = \{x \in M \mid \operatorname{Ann}(Rx) \neq \{0\}\} = \{x \in M \mid \exists r \in R \setminus \{0\} \text{ mit } rx = 0\}$. Der Modul M heißt ein Torsionsmodul, wenn $\operatorname{Tor}(M) = M$ ist, und torsionsfrei, wenn $\operatorname{Tor}(M) = \{0\}$ gilt.

Für einen K -Vektorraum V gilt $\text{Tor}(V) = \{0\}$. Falls $V \neq \{0\}$ gilt auch $\text{Ann}(V) = \{0\}$, ansonsten $\text{Ann}(V) = K$. Der Annulator ist ein Untermodul des R -Moduls R , also ein Linksideal von R . Für einen kommutativen Ring R ist $\text{Ann}(M)$ ein Ideal und jeder R -Modul M in natürlicher Weise auch ein treuer $R/\text{Ann}(M)$ -Modul.

Für einen torsionsfreien R -Modul $\neq \{0\}$ ist R notwendigerweise nullteilerfrei, denn für $a, b \in R \setminus \{0\}$ und $x \in M \setminus \{0\}$ ist nach Voraussetzung $bx \neq 0$ und $a(bx) \neq 0$, also $(ab)x \neq 0$ und daher $ab \neq 0$. Ein typisches Beispiel erhalten wir mit $M = R/I$, wobei I ein Ideal in R ist. Hier gilt $\text{Ann}(M) = I$ und $\text{Tor}(M) = M$.

4.6 Satz. *Sei R ein Integritätsring und M ein R -Modul. Dann ist $\text{Tor}(M)$ ein Untermodul von M und $M/\text{Tor}(M)$ ist torsionsfrei.*

Beweis. Für $x, y \in \text{Tor}(M)$ gibt es $r, s \in R \setminus \{0\}$ mit $rx = sy = 0$. Dann gilt $rs \neq 0$, da R nullteilerfrei ist, und $rs(x - y) = 0$. Daher $x - y \in \text{Tor}(M)$. Ferner gilt für $s \in R$ beliebig $r(sx) = s(rx) = 0$, also $sx \in \text{Tor}(M)$. Daher ist $\text{Tor}(M)$ ein Untermodul von M .

Sei $x \in M$ und $r \in R \setminus \{0\}$ mit $rx \in \text{Tor}(M)$. Dann gibt es $s \in R \setminus \{0\}$ mit $sx = 0$ und $s(rx) = r(sx) = 0$, folglich $(sr)x = 0$ und $sr \neq 0$. Es folgt $x \in \text{Tor}(M)$ und $M/\text{Tor}(M)$ ist daher torsionsfrei. \square

4.7 Definition. Sei M ein R -Modul. Der Rang von M ist das Supremum der Kardinalitäten von über R linear unabhängigen Teilmengen von M und wird mit $\text{rank}(M)$ bezeichnet.

Die Länge von M ist die Länge, also das Supremum der Anzahl der Inklusionen, von echt absteigenden Ketten $\cdots \supseteq M_i \supseteq M_{i+1} \supseteq \cdots$ von Untermoduln von M mit $i \in \mathbb{Z}$ und wird mit $\text{len}(M)$ bezeichnet.

Zum Beispiel hat $(\mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}$ den Rang eins und unendliche Länge. Der Nullmodul $\{0\}$ hat Rang Null und Länge Null. Für Vektorräume stimmen Rang und Länge überein. Rang und Länge sind unterschiedliche Verallgemeinerungen des Dimensionsbegriffs von Vektorräumen auf Moduln.

4.8 Definition. Der Modul M heißt frei, wenn er eine Basis besitzt.

Der Begriff „frei“ soll heißen, daß es ein Erzeugendensystem von M gibt, welches frei von nicht trivialen R -linearen Relationen ist. Die Moduln R^n sind frei, die Einheitsvektoren liefern eine Basis. Besitzt ein Modul M eine endliche Basis mit n Elementen, so gilt $M \cong R^n$, wobei der Isomorphismus durch die Abbildung gegeben ist, die den Elementen von M die Koordinaten in R bezüglich der Basiselemente zuordnet.

Nicht jeder Modul ist frei: Als Beispiel betrachte man den \mathbb{Z} -Modul $\mathbb{Z}/3\mathbb{Z}$. Für einen Integritätsring R können im allgemeinen nur torsionsfreie R -Moduln frei sein. Ist R nicht nullteilerfrei, so ist R als R -Modul zwar frei, aber nicht torsionsfrei, denn Nullteiler sind hier Torsionselemente.

Eine Basis eines R -Moduls M ist eine maximale Menge von R -linear unabhängigen Elementen aus M , durch Hinzunahme eines Elements geht die lineare Unabhängigkeit verloren. Trotzdem brauchen Basen nicht die gleiche Kardinalität zu besitzen. Es gibt beispielsweise einen (nicht-kommutativen) Ring R mit 1, für den $R^n \cong R^m$ für alle $n, m \in \mathbb{Z}^{\geq 1}$ gilt (siehe Abschnitt ?? oder Meyberg 1, Seite 178).

4.9 Satz. *Sei M ein R -Modul.*

- (i) *Seien $x_i \in M$ mit $i \in I$ und I eine Indexmenge. Dann ist M genau dann frei und die x_i sind eine Basis, wenn es für jeden Modul N und beliebige Elemente $y_i \in N$ genau einen Homomorphismus $f : M \rightarrow N$ mit $f(x_i) = y_i$ für alle $i \in I$ gibt.*
- (ii) *Sei R kommutativ. Seien die x_i für $i \in I$ eine Basis von M und die y_j für $j \in J$ ein Erzeugendensystem von M . Dann gilt $\#I \leq \#J$. Insbesondere hat jede Basis von M die gleiche Kardinalität.*

Beweis. Zu (i). Beweis ist einfach und vom Prinzip ähnlich wie bei den Polynomringen.

Zu (ii). Für $R = \{0\}$ ist der Satz korrekt: Alle Basen sind leer, so daß $\#I = 0 \leq \#J$ gilt.

Für $R \neq \{0\}$ gibt es ein maximales Ideal \mathfrak{m} von R . Dann ist $\mathfrak{m}M$ ein Untermodul von M und $M/\mathfrak{m}M$ ein R/\mathfrak{m} -Modul. Es ist klar, daß die $x_i + \mathfrak{m}M$ für $i \in I$ und die $y_j + \mathfrak{m}M$ für $j \in J$ Erzeugendensysteme von $M/\mathfrak{m}M$ sind. Wir zeigen, daß die $x_i + \mathfrak{m}M$ auch R/\mathfrak{m} -linear unabhängig sind: Denn für $\lambda_i \in R$ mit $\sum_{i \in I} \lambda_i x_i \in \mathfrak{m}M$ gibt es $\mu_i \in \mathfrak{m}$ mit $\sum_{i \in I} \lambda_i x_i = \sum_{i \in I} \mu_i x_i$, da die x_i ein Erzeugendensystem von M bilden. Die lineare Unabhängigkeit der x_i liefert dann $\lambda_i = \mu_i \in \mathfrak{m}$ für alle $i \in I$.

Da R/\mathfrak{m} ein Körper ist, handelt es sich bei $M/\mathfrak{m}M$ um einen R/\mathfrak{m} -Vektorraum mit der Basis $x_i + \mathfrak{m}M$ für $i \in I$ und dem Erzeugendensystem $y_j + \mathfrak{m}M$ für $j \in J$. Es folgt $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M) = \#I \leq \#J$.

Sind die y_j ebenfalls eine Basis, so ergibt sich $\#I = \#J$ und alle Basen haben die gleiche Kardinalität. \square

Aus (i) folgt, daß jeder endlich erzeugte R -Modul N epimorphes Bild eines freien Moduls R^n ist.

Wir bemerken, daß für einen kommutativen Ring R zusätzlich zur Aussage von (ii) folgendes gilt: Ist M frei vom endlichen Rang n , so ist jedes Erzeugendensystem bestehend aus n Elementen eine Basis von M (Korollar ??).

Eine andere als die oben erwähnte Situation nicht freier Moduln tritt beispielsweise für Integritätsringe R auf, die keine Hauptidealringe sind. Ist I ein Ideal, welches nur von mindestens zwei Elementen erzeugt werden kann, so ist I als R -Modul nicht frei. Man sieht dies wie folgt: Wäre I frei, so müßte I wegen $\text{rank}(I) = 1$ eine einelementige Basis besitzen. Dies aber bedeutet gerade, daß I ein Hauptideal ist.

Auch ist I dann zwar ein Untermodul von R , aber kein direkter Summand von R (wie das bei Untermoduln von Vektorräumen der Fall wäre). Dies gilt, weil aus $R \cong I \oplus N$ zunächst $N = \{0\}$ folgen würde, denn der Rang von R ist eins und der von $I \oplus N$ für $N \neq \{0\}$ größer gleich zwei, da N mit R torsionsfrei sein muß. Gilt nun aber $R \cong I$ und bezeichnet $\phi : R \rightarrow I$ den Isomorphismus, so ist $I = \phi(R) = R\phi(1)$ und I ist ein von $\phi(1)$ erzeugtes Hauptideal, im Widerspruch zur Annahme. Entsprechend ist auch nicht jeder (torsionsfreie) R -Modul von der Form R^n .

4.2 Noethersche und Artinsche Moduln

In diesem Abschnitt sind aufsteigende und absteigende Ketten von Untermoduln von Interesse.

4.10 Definition. Ein Modul heißt noethersch, wenn jede nicht leere Menge von Untermoduln von M ein bezüglich der Inklusionsrelation maximales Element enthält.

Ein Modul heißt artinsch, wenn jede nicht leere Menge von Untermoduln von M ein bezüglich der Inklusionsrelation minimales Element enthält.

Zum Beispiel ist jeder Hauptidealring R als R -Modul noethersch, aber im allgemeinen nicht artinsch. Ist $I \neq \{0\}$ ein Ideal von R , so ist R/I dann auch artinsch.

4.11 Satz. Sei R ein Ring und M ein R -Modul. Dann sind äquivalent.

- (i) Jede aufsteigende Kette von Untermoduln von M wird stationär.
- (ii) M ist noethersch.
- (iii) Für jede Familie von Untermoduln M_i mit $i \in I$ gibt es ein endliches $I_0 \subseteq I$ mit $\sum_{i \in I} M_i = \sum_{i \in I_0} M_i$.

(iv) Jeder Untermodul von M ist endlich erzeugt.

Beweis. (i) \Rightarrow (ii): Wenn (ii) nicht gilt, dann gibt es eine nicht-leere Menge X , die keinen maximalen Untermodul enthält. Zu jedem Modul aus X gibt es dann stets einen umfassenderen Modul aus X . Man kann daher (mittels Auswahlaxiom) eine aufsteigende, nicht stationäre Kette definieren.

(ii) \Rightarrow (iii): In der Menge aller Summen endlich vieler M_i gibt es ein maximales Element $N = \sum_{i \in I_0} M_i$, wobei $I_0 \subseteq I$ endlich ist. Wegen der Maximalität folgt $N + M_i = N$ für alle $i \in I$, also $\sum_{i \in I} M_i = N$.

(iii) \Rightarrow (i): Bilden die M_i eine aufsteigende Kette, so gibt es ein j für welches $\sum_i M_i = M_j$. Daher ist die Kette stationär.

(iv) \Rightarrow (iii): Seien a_j endlich viele Erzeuger von $\sum_{i \in I} M_i$. Für jedes j gibt es ein endliches $I_j \subseteq I$ mit $a_j \in \sum_{i \in I_j} M_i$. Dann leistet $I_0 = \cup_j I_j$ das Gewünschte.

(iii) \Rightarrow (iv): Sei U ein Untermodul. Zu $I = U$ definiere $M_i = Ri$ für $i \in I$. Dann gilt $U = \sum_{i \in I} M_i = \sum_{i \in I_0} M_i$ für ein endliches $I_0 \subseteq I$. Also ist I_0 endliches Erzeugendensystem von U . \square

Man beachte, daß in der Definition eines noetherschen Rings R Ideale, also R -Links- und Rechtsmoduln betrachtet werden. Die R -Untermoduln von R sind aber genau die Linksideale von R . Mit unserer Definition braucht daher ein noetherscher Ring nicht als R -Modul noethersch zu sein, umgekehrt ist dies aber der Fall.

4.12 Satz. Sei M ein R -Modul.

- (i) Ist M noethersch, so auch U und M/U für alle Untermoduln U von M .
- (ii) Sind U und M/U noethersch für einen Untermodul U von M , so ist auch M noethersch.
- (iii) Ist M endlich erzeugt und R als R -Modul noethersch, so ist M noethersch.

Beweis. (i): Aufsteigende Ketten von Untermoduln in U sind auch aufsteigende Ketten von Untermoduln von M und werden daher stationär. Analoges gilt für aufsteigende Ketten von Untermoduln in M/U und ihre Urbilder in M .

(ii): Sei U_i eine aufsteigende Kette in M und $U'_i = U \cap U_i$, $U''_i = (U_i + U)/U$. Es gibt ein n , so daß $U'_t = U'_n$ und $U''_t = U''_n$ für alle $t \geq n$ gilt. Wir zeigen nun $U_t = U_n$ für $t \geq n$. Sei $x \in U_t$. Wegen $U''_t = U''_n$ gibt es $y \in U_n$ mit $x - y \in U$. Folglich $x - y \in U \cap U_t = U'_t = U'_n \subseteq U_n$. Es ergibt sich $x \in U_n$.

(iii): Zunächst ist R^n nach (ii) noethersch, indem man $R^n/R \cong R^{n-1}$ beachtet und Induktion anwendet. Als epimorphes Bild von R^n ist dann auch M wiederum nach (ii) noethersch. \square

Es folgen die zu den beiden vorstehenden Sätzen analogen Sätze für artinsche Moduln.

4.13 Satz. *Sei R ein Ring und M ein R -Modul. Dann sind äquivalent.*

- (i) *Jede absteigende Kette von Untermoduln von M wird stationär.*
- (ii) *M ist artinsch.*
- (iii) *Für jede Familie von Untermoduln M_i mit $i \in I$ gibt es ein endliches $I_0 \subseteq I$ mit $\bigcap_{i \in I} M_i = \bigcap_{i \in I_0} M_i$.*

Beweis. (i) \Rightarrow (ii): Wenn (ii) nicht gilt, dann gibt es eine nicht-leere Menge X , die keinen minimalen Untermodul enthält. Zu jedem Modul aus X gibt es dann stets einen darin echt enthaltenen Modul aus X . Man kann daher (mittels Auswahlaxiom) eine absteigende, nicht stationäre Kette definieren.

(ii) \Rightarrow (iii): In der Menge aller Durchschnitte endlich vieler M_i gibt es ein minimales Element $N = \bigcap_{i \in I_0} M_i$. Wegen der Minimalität folgt $N \cap M_i = N$ für alle $i \in I$, also $\bigcap_{i \in I} M_i = N$.

(iii) \Rightarrow (i): Bilden die M_i eine absteigende Kette, so gibt es ein j für welches $\bigcap_i M_i = M_j$. Daher ist die Kette stationär. \square

4.14 Satz. *Sei M ein R -Modul.*

- (i) *Ist M artinsch, so auch U und M/U für alle Untermoduln U von M .*
- (ii) *Sind U und M/U artinsch für einen Untermodul U von M , so ist auch M artinsch.*
- (iii) *Ist M endlich erzeugt und R als R -Modul artinsch, so ist M artinsch.*

Beweis. (i): Absteigende Ketten von Untermoduln in U sind auch absteigende Ketten von Untermoduln von M und werden daher stationär. Analoges gilt für absteigende Ketten von Untermoduln in M/U und ihre Urbilder in M .

(ii): Sei U_i eine absteigende Kette in M und $U'_i = U \cap U_i$, $U''_i = (U_i + U)/U$. Es gibt ein n , so daß $U'_t = U'_n$ und $U''_t = U''_n$ für alle $t \geq n$ gilt. Wir zeigen nun $U_t = U_n$ für $t \geq n$. Sei $x \in U_n$. Wegen $U''_t = U''_n$ gibt es $y \in U_t$ mit $x - y \in U$. Folglich $x - y \in U \cap U_n = U'_n = U'_t \subseteq U_t$. Es ergibt sich $x \in U_t$.

(iii): Zunächst ist R^n nach (ii) artinscher Modul, indem man $R^n/R \cong R^{n-1}$ betrachtet und Induktion anwendet. Als epimorphes Bild von R^n ist dann auch M wiederum nach (ii) artinsch. \square

Wir nennen eine echt absteigende Kette wie in Definition 4.7 maximal oder eine Kompositionsreihe, wenn sich die Kette durch Einfügen bzw. Voranstellen oder Anhängen von weiteren Untermoduln (lokal) nicht verlängern läßt. Eine notwendige Bedingung ist also, daß M_{i+1} maximal in M_i für alle i ist. Eine endliche Kompositionsreihe (also eine Kompositionsreihe endlicher Länge) besitzt darüberhinaus notwendigerweise M und $\{0\}$ als Anfangs- und Endpunkt. Eine beliebige, echt absteigende Kette mit Anfangs- und Endpunkt M und $\{0\}$ und mit M_{i+1} maximal in M_i ist umgekehrt eine endliche Kompositionsreihe.

Der folgende Satz steht im Zusammenhang mit dem Satz von Jordan-Hölder-Schreier. Das wird in der Algebra 2 noch einmal genauer und allgemeiner aufgegriffen und bewiesen.

4.15 Satz. *Sei M ein Modul. Die Kompositionsreihen von M besitzen alle die gleichen, maximalen Längen $\text{len}(M)$.*

Beweis. Lassen wir aus. □

Wir vergleichen nun die Eigenschaften noethersch und artinsch mit der Länge $\text{len}(M)$.

4.16 Satz. *Sei M ein R -Modul. Dann sind äquivalent:*

- (i) M ist noethersch und artinsch.
- (ii) M besitzt eine endliche Kompositionsreihe.
- (iii) $\text{len}(M) < \infty$.

Beweis. (i) \Rightarrow (ii): Zu jedem Untermodul $U \neq \{0\}$ von M sei X_U die Menge aller von U verschiedener Untermoduln von U . Da M noethersch ist und $X_U \neq \emptyset$ gilt, gibt es darin ein bezüglich Inklusion maximales Element V , so daß V also ein maximaler Untermodul von U ist.

Wir definieren mit dieser Beobachtung induktiv eine echt absteigende Kette $M = M_0 \supsetneq M_1 \supsetneq \dots$. Da M artinsch ist, muß diese Kette nach endlich vielen Schritten abbrechen, es muß also $M_n = \{0\}$ für ein $n \in \mathbb{Z}^{\geq 0}$ gelten. Dies liefert eine endliche Kompositionsreihe.

(ii) \Rightarrow (iii): Nach Satz 4.15 stimmen $\text{len}(M)$ und die Länge der endlichen Kompositionsreihe überein, also gilt $\text{len}(M) < \infty$.

(iii) \Rightarrow (i): Ist M nicht noethersch oder nicht artinsch, so gibt es eine unendliche echt auf- oder absteigende Kette von Untermoduln von M . Daher gilt $\text{len}(M) = \infty$. □

Als Folgerung aus diesem Satz bemerken wir: Sind die Längen echt absteigender, endlicher Ketten von Untermoduln in M unbeschränkt, so enthält M auch eine echt absteigende Kette von Untermoduln unendlicher Länge.

4.17 Satz. *Sei M ein R -Modul und U ein Untermodul. Dann gilt $\text{len}(M) = \text{len}(U) + \text{len}(M/U)$.*

Beweis. Ketten von Untermoduln von U sind auch Ketten von Untermoduln von M . Urbilder von Ketten von Untermoduln von M/U unter dem kanonischen Epimorphismus sind wieder Ketten von Untermoduln von M , welche U enthalten. Gilt daher $\text{len}(U) = \infty$ oder $\text{len}(M/U) = \infty$, so folgt $\text{len}(M) = \text{len}(U) + \text{len}(M/U) = \infty$.

Sei nun $\text{len}(U) < \infty$ und $\text{len}(M/U) < \infty$. Die von Kompositionsreihen in U und M/U herrührenden Ketten endlicher Länge in M mit den Anfangs- und Endpunkten $\{0\}$, U und U , M können aneinandergelängt werden und liefern eine Kompositionsreihe von M der Länge $\text{len}(U) + \text{len}(M/U)$. Nach Satz 4.15 folgt $\text{len}(M) = \text{len}(U) + \text{len}(M/U)$. \square

Aus dem Satz ergibt sich auch $\text{len}(M_1 \oplus M_2) = \text{len}(M_1) + \text{len}(M_2)$.

4.3 Matrizen über Ringen

Ähnlich wie in der linearen Algebra sind Matrizen auch in der Modultheorie nützliche Objekte. Wir wollen nun Matrizen über Ringen betrachten.

Wir befassen uns zunächst mit Determinanten von Matrizen über beliebigen, kommutativen Ringen. Sei $S = \mathbb{Z}[x_{1,1}, \dots, x_{n,n}, y_{1,1}, \dots, y_{n,n}]$, $M = (x_{i,j})_{i,j}$ und $N = (y_{i,j})_{i,j}$, so daß $M, N \in S^{n \times n}$ gilt. Dann können wir M auch als Matrix über dem Quotientenkörper $\text{Quot}(S)$ von S auffassen und es ist $\det(M) = \sum_{\sigma \in S_n} \text{sign}(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)} \in S$, wie man es aus der linearen Algebra über Körpern gewöhnt ist. Analoges gilt für N . Für Determinanten gilt wie üblich $\det(MN) = \det(M) \det(N)$ und, daß \det eine alternierende Multilinearform ist. Man beachte, daß dies Gleichungen im Polynomring $S = \mathbb{Z}[x_{1,1}, \dots, x_{n,n}, y_{1,1}, \dots, y_{n,n}]$ sind, da Determinanten hier nichts anderes als Polynome in den Koeffizienten von M und N sind. Ist $M_{i,j} \in S^{(n-1) \times (n-1)}$ die Matrix, die durch Streichen der i -ten Zeile und j -ten Spalte von M entsteht, so gilt ferner $\det(M) = \sum_{i=1}^n (-1)^{i+j} x_{i,j} \det(M_{i,j})$.

Sei nun R ein beliebiger, kommutativer Ring. Da es einen kanonischen Homomorphismus $\mathbb{Z} \rightarrow R$ gibt und die $x_{i,j}$ und $y_{i,j}$ nirgends im Nenner auftreten, können wir sie auch durch spezielle Werte aus R ersetzen. Daher gelten die genannten Eigenschaften aufgrund der Homomorphieeigenschaft des Einsetzhomomorphismus auch für Matrizen über R .

Wir arbeiten auch häufig über Integritätsringen R . Hier kann man alles in $K = \text{Quot}(R)$ einbetten und so lineare Algebra über K anwenden. Zum Beispiel sind die Spalten- und Zeilenvektoren von $M \in R^{n \times n}$ genau dann über R linear unabhängig, wenn $\det(M) \neq 0$ gilt. Man beachte, daß linear unabhängig über R und linear unabhängig über K für $K = \text{Quot}(R)$ äquivalent sind (man kann Nenner rausmultiplizieren).

4.18 Satz. *Sei R ein kommutativer Ring.*

- (i) *Sei $A \in R^{n \times n}$, $x = (x_i)^t \in R^n$ und $b = (b_i)^t \in R^n$ mit $Ax = b$. Ist B_i die Matrix, deren i -te Spalte gleich b ist und die ansonsten mit A übereinstimmt, so gilt $\det(B_i) = x_i \det(A)$.*
- (ii) *Sei $M \in R^{n \times n}$ und $M' = ((-1)^{i+j} \det(M_{j,i}))_{i,j} \in R^{n \times n}$, wobei $M_{i,j}$ die Matrix ist, die durch Streichen der i -ten Zeile und j -ten Spalte von M entsteht. Dann gilt $MM' = M'M = \det(M)I_n$.*
- (iii) *Eine Matrix $M \in R^{n \times n}$ ist genau dann invertierbar, wenn $\det(M)$ in R invertierbar ist.*

Beweis. (i): Die i -te Spalte b in B_i ist gleich der Linearkombination der Spalten von A mit den Koeffizienten x_i . Sei $A_{i,j}$ die Matrix, die an der i -ten Spalte die j -Spalte von A hat und ansonsten mit A übereinstimmt. Dann gilt $\det(A_{i,j}) = \delta_{i,j} \det(A)$ (Kronecker-Delta) und aufgrund der Linearität der Determinante in der i -ten Spalte ergibt sich $\det(B_i) = \sum_{j=1}^n x_j \det(A_{i,j}) = x_i \det(A)$.

(ii): Für S statt R folgt die Behauptung als Polynomidentität, indem man die Einträge von M' nach (i) unter Verwendung der obigen Entwicklung für Determinanten und durch Kürzen von $\det(M)$ berechnet. Für $M' = (x_{i,j})_{i,j}$ ergibt sich genauer $x_{i,j} \det(M) = \det(\hat{M}_{i,j})$, wobei $\hat{M}_{i,j}$ die Matrix ist, die aus M entsteht, wenn wir die i -te Spalte von M durch den j -ten Einheitsvektor multipliziert mit $\det(M)$ ersetzen. Dann gilt $\det(\hat{M}_{i,j}) = (-1)^{i+j} \det(M) \det(M_{j,i})$ nach der Entwicklungsformel, da die i -te Spalte in $\hat{M}_{i,j}$ Null ist außer in der j -ten Zeile, wo $\det(M)$ steht. Folglich $x_{i,j} \det(M) = (-1)^{i+j} \det(M) \det(M_{j,i})$. Da S nullteilerfrei ist und $\det(M) \neq 0$ gilt, folgt durch Kürzen $x_{i,j} = (-1)^{i+j} \det(M_{j,i})$ als Polynomidentität.

Durch Spezialisierung der Variablen folgt die Behauptung dann auch für R .

(iii): Ist M invertierbar, so gilt $1 = \det(MM^{-1}) = \det(M) \det(M^{-1})$. Wegen $M^{-1} \in R^{n \times n}$ folgt auch $\det(M^{-1}) \in R$ und $\det(M)$ ist invertierbar in R .

Umgekehrt sei $M \in R^{n \times n}$ und M' wie in (ii). Ist $\det(M)$ invertierbar, so ist $M'/\det(M)$ über R definiert und invers zu M . \square

Satz 4.18, (i) ist als Cramersche Regel bekannt. Die Matrix M' in (ii) nennt man häufig Pseudoinverse von M .

Invertierbare Matrizen über Ringen heißen auch unimodular. Ist $T \in R^{n \times n}$, M ein R -Modul und $a_1, \dots, a_n, b_1, \dots, b_n \in M$ mit $(a_1, \dots, a_n)T = (b_1, \dots, b_n)$, so ist jedes b_i eine Linearkombination der a_i und der von den b_i erzeugte Untermodul U_2 von M ist also ein Untermodul des von den a_i erzeugten Moduls U_1 . Umgekehrt gilt für unimodulares T aber auch $(a_1, \dots, a_n) = (b_1, \dots, b_n)T^{-1}$, so daß sich jedes b_i als Linearkombination der a_i schreiben läßt und somit $U_1 = U_2$ gilt. Sind die a_i und die b_i Basen von M , so gibt es ein unimodulares $T \in R^{n \times n}$ mit $(a_1, \dots, a_n)T = (b_1, \dots, b_n)$.

4.19 Satz. Für beliebiges T gilt mit obiger Notation $\det(T)U_1 \subseteq U_2$ und $\det(T) \in \text{Ann}(U_1/U_2)$.

Beweis. Mit Satz 4.18, (ii) und der Pseudoinversen T' von T gilt $TT' = \det(T)I_n$. Daraus folgt $\det(T)(a_1, \dots, a_n) = (a_1, \dots, a_n)TT' = (b_1, \dots, b_n)T' \in U_2^n$, also $\det(T)U_1 \subseteq U_2$. Die Aussage über den Annulator folgt daraus direkt. \square

Typische unimodulare, elementare Transformationen sind durch folgende Operationen gegeben: Mit Einheit multiplizieren, Vertauschen, Vielfaches eines Elements zu einem anderen addieren. Über euklidischen Ringen läßt sich jede unimodulare Transformation in diese elementaren Transformationen faktorisieren, wie in Abschnitt 4.4 gezeigt wird.

4.4 Moduln und Matrizen über Hauptidealringen

In diesem Abschnitt bezeichnet R einen Hauptidealring. Wir leiten zuerst Aussagen über Matrixnormalformen her und wenden diese dann an, um Aussagen über endlich erzeugte Moduln über Hauptidealringen zu erhalten.

4.20 Lemma. (i) Seien $a_1, \dots, a_n \in R$. Dann gibt es eine unimodulare Matrix U in $R^{n \times n}$ mit $(a_1, \dots, a_n)U = (d, 0, \dots, 0)$, wobei $d = \text{gcd}\{a_1, \dots, a_n\}$ ist.

(ii) Seien $a_1, \dots, a_n \in R$. Dann gibt es eine Matrix A in $R^{n \times n}$, deren erste Zeile gleich (a_1, \dots, a_n) ist und für die $\det(A) = \text{gcd}\{a_1, \dots, a_n\}$ gilt.

Beweis. (i): Für $i < j$ gibt es $\lambda, \mu \in R$ mit $\lambda a_i + \mu a_j = c$ und $c = \text{gcd}\{a_i, a_j\}$. Die Matrix

$$T' = \begin{pmatrix} \lambda & -a_j/c \\ \mu & a_i/c \end{pmatrix}$$

ist in $R^{2 \times 2}$, unimodular und erfüllt $(a_i, a_j)T' = (c, 0)$. Wir können T' zu einer unimodularen Matrix $T \in R^{n \times n}$ machen, indem wir T' als (erweiterten) Diagonalblock in I_n einbetten, so daß gilt:

$$\begin{aligned} & (a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_n)T \\ &= (a_1, \dots, a_{i-1}, c, a_{i+1}, \dots, a_{j-1}, 0, a_{j+1}, \dots, a_n). \end{aligned}$$

Indem wir diese Schritte wiederholen und die so erhaltenen, unimodularen Transformationsmatrizen T aufmultiplizieren, erhalten wir schließlich ein unimodulares $U \in R^{n \times n}$ mit $(a_1, \dots, a_n)U = (d, 0, \dots, 0)$.

(ii): Sei U unimodular mit $(a_1, \dots, a_n)U = (d, 0, \dots, 0)$, $d = \gcd\{a_1, \dots, a_n\}$ und $\det(U) = 1$ (andernfalls eine Spalte von U durch $\det(U)$ dividieren). Sei B die Matrix, deren erste Zeile $(d, 0, \dots, 0)$ ist und die ansonsten mit I_n übereinstimmt. Dann gilt $\det(B) = d$ und die Matrix $A = BU^{-1}$ erfüllt die Bedingungen. \square

4.21 Definition. Sei $M = (m_{i,j}) \in R^{n \times m}$ und $I_j = \{i \mid 1 \leq i \leq n \text{ und } m_{i,j} \neq 0\}$. Wir setzen $j_0 = \max\{j \mid 1 \leq j \leq m \text{ und } I_j \neq \emptyset\}$, $i_j = \min I_j$ und definieren: M ist in unterer Spalten-Stufenform, wenn $i_1 < \dots < i_{j_0}$.

Sei $P \subseteq R$ ein Vertretersystem nicht-assoziierter Elemente von R und $R_b \subseteq R$ ein Vertretersystem für die Restklassen R/Rb für jedes $b \in P$. Die Matrix M in unterer Spalten-Stufenform heißt in unterer Spalten-Hermite-Normalform, wenn für jedes $j = 1, \dots, j_0$ gilt: $m_{i_j,j} \in P$ und $m_{i_j,k} \in R_{m_{i_j,j}}$ für $1 \leq k < j$.

Entsprechend können obere Spalten- und untere, obere Zeilen-Stufenformen für M definiert werden.

4.22 Satz. Zu einer Matrix $M \in R^{n \times m}$ gibt es eine unimodulare Matrix $T \in R^{m \times m}$, so daß MT in unterer Spalten-Stufenform ist. Sind Vertretersysteme P und R_b gegeben, so kann T so gewählt werden, daß MT in unterer Spalten-Hermite-Normalform ist. In diesem Fall ist MT eindeutig durch M bestimmt.

Beweis. Für $M = 0$ ist der Satz korrekt. Sei nun $M \neq 0$ und $(a_1, \dots, a_m) \neq 0$ die i -te Zeile von M für $1 \leq i \leq n$ minimal. Nach Lemma 4.20, (i) gibt es ein unimodulares $U_1 \in R^{m \times m}$, so daß die i -te Zeile von MU_1 von der Form $(d, 0, \dots, 0)$ mit $d = \gcd\{a_1, \dots, a_m\}$ ist. Alle Zeilen über der i -ten Zeile von MU_1 sind Null.

Sei M' die Matrix, die aus M durch Streichen der ersten i Zeilen von M und durch Streichen der ersten Spalte von M entsteht. Per Induktion gibt es eine unimodulare Matrix $U' \in R^{(m-1) \times (m-1)}$, so daß $M'U'$ in unterer Spalten-Stufenform ist. Wir definieren

$$U_2 = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix} \in R^{m \times m}$$

und $U = U_1U_2$. Die Matrix U ist unimodular. Dann gilt

$$MU = \begin{pmatrix} 0 & 0 \\ d & 0 \\ * & M'U' \end{pmatrix} \in R^{n \times m}$$

(die ersten Nullzeilen können auch wegfallen) und MU ist daher in unterer Spalten-Stufenform.

Durch Multiplikation der Spalten mit Einheiten erreichen wir die Bedingung $m_{i_j,j} \in P$, durch Addieren von Vielfachen der j -ten Spalte zu den k -ten Spalten mit $k < j$ für $j = 1, \dots, j_0$ erreichen wir die Bedingung $m_{i_j,k} \in R_{m_{i_j,j}}$. Aufgrund der Spalten-Stufenform bleibt die Matrix oberhalb der i_j -ten Zeile unverändert. Diese Transformationen entsprechen ebenfalls der Multiplikation mit einer unimodularen Matrix und liefern die untere Spalten-Hermite-Normalform von M .

Die Eindeutigkeitsaussagen erhält man am leichtesten aus der Interpretation der Spalten von MU als Modulbasis: Sei V der von den Spalten von M erzeugte R -Untermodul von R^n . Aufgrund der Spalten-Stufenform sind die Spalten ungleich Null von MU linear unabhängig und bilden daher eine Basis von V .

Wir betrachten zunächst die Eindeutigkeit der Zeilenindizes der Stufen und die Eindeutigkeit bis auf Assoziation der Elemente auf den Stufen. Sei V_i der Untermodul von V , dessen Elemente an den ersten $i-1$ Koordinaten Nulleinträge haben. Für die Menge $I = \{i_j \mid 1 \leq j \leq j_0\}$ der Zeilenindizes der Stufen in MU gilt dann $I = \{i \mid 1 \leq i \leq n \text{ und } V_i \neq V_{i+1}\}$. Also ist I unabhängig von U und eindeutig durch M bestimmt. Ferner liefert die Menge der i -ten Koordinaten der Elemente aus V_i ein Ideal von R , welches gerade durch das Element auf der Stufe in Zeile i erzeugt wird. Daher sind diese Elemente unabhängig von U und bis auf Assoziation eindeutig durch M bestimmt. Die Spalten b_j von MU für $1 \leq j \leq j_0$ sind dann ebenfalls bis auf Multiplikation mit Einheiten aus R und modulo $\sum_{\nu=j+1}^{j_0} Rb_\nu$ unabhängig von U und eindeutig durch M bestimmt. Hieraus folgt auch die Eindeutigkeit der Hermite-Normalform unter weiterer Reduktion für $j = 1, \dots, j_0$ nach links. \square

4.23 Satz. *Sei M ein Untermodul von R^n . Dann ist M frei vom Rang $\leq n$.*

Beweis. Mit R^n ist auch M noethersch und daher endlich erzeugt. Durch Anwendung der Hermite-Normalform auf die durch die Erzeuger gebildete Matrix erhalten wir eine Basis von M in unterer Spalten-Stufenform mit $\leq n$ Elementen. \square

Der Eindeutigkeitsbeweis in Satz 4.22 liefert ebenfalls die Existenz einer Basis bestehend aus $\leq n$ Elementen jedes Untermoduls von R^n . Wir brauchen dabei

nicht zu verwenden, daß M noethersch oder endlich erzeugt ist. Dies ergibt sich als Konsequenz der Überlegung.

Eine unimodulare Matrix $M \in R^{n \times n}$ kann nach dem Satz in eine untere Dreiecksmatrix mit Einheiten bzw. Einsen auf der Diagonalen transformiert werden. Indem noch links reduziert (Hermite-Normalform bilden), erhält man I_n . Dies zeigt, daß sich jede unimodulare Matrix über R in ein Produkt der elementaren, unimodularen Matrizen T' bzw. T aus dem Beweis von Lemma 4.20 zerlegen läßt. Für einen euklidischen Ring R sind diese Matrizen selbst wieder Produkte der am Ende von Abschnitt 4.1 erwähnten elementaren Matrizen, da im euklidischen Algorithmus wechselseitig Vielfache von Elementen bzw. Spalten voneinander abgezogen werden.

Will man Hermite-Normalformen über einem euklidischen Ring “von Hand” ausrechnen, kann man wie folgt vorgehen. Man führt den euklidischen Algorithmus bezüglich der Elemente der ersten Zeile aus, rechnet aber mit den ganzen Spalten. Hierbei addiert man also in jedem Schritt ein Vielfaches einer Spalte zu einer anderen Spalte. Bei Bedarf multipliziert man Spalten mit Einheiten. Zum Schluß sind in der ersten Zeile alle Elemente bis auf das erste Null. Das erste ist der größte gemeinsame Teiler der Ausgangszeilenelemente und kann auch Null sein. Dann fährt man induktiv mit der zweiten Spalte ab dem zweiten Element fort. Komplexitätstechnisch gibt es wesentlich effizientere Verfahren zur Hermite-Normalformberechnung.

Typische, praktische Verwendungszwecke der Hermite-Normalform sind in etwa die Berechnung einer Basis eines durch ein Erzeugendensystem gegebenen Moduls $M \subseteq R^n$, Test auf Gleichheit, Test auf Inklusion, Summen- und Schnittberechnung zweier solcher Moduln.

Eine r -Minore der Matrix $M \in R^{n \times m}$ für $r \leq \min\{n, m\}$ ist die Determinante einer $(r \times r)$ -Matrix, die durch Streichen von $n - r$ Zeilen und $m - r$ Spalten aus M entsteht. Wir definieren $d_r(M)$ als den größten gemeinsamen Teiler aller r -Minoren von M (ist bis auf Einheiten eindeutig bestimmt).

Wir nennen $M \in R^{n \times m}$ im folgenden diagonal, wenn M außerhalb der Diagonalen nur Nulleinträge besitzt (M muß also nicht unbedingt quadratisch sein).

4.24 Lemma. (i) Sei $M \in R^{n \times m}$ eine Diagonalmatrix mit den Diagonaleinträgen a_1, \dots, a_d für $d = \min\{n, m\}$. Dann gibt es unimodulare Matrizen $U \in R^{n \times n}$ und $V \in R^{m \times m}$, so daß UMV diagonal mit den Diagonaleinträgen b_1, \dots, b_d ist und $b_1 \mid \dots \mid b_d$ gilt.

(ii) Seien $M \in R^{n \times m}$ und $U \in R^{n \times n}$, $V \in R^{m \times m}$ unimodulare Matrizen. Dann gilt $d_{r-1}(M) \mid d_r(M)$ und $d_r(M) \sim d_r(UMV)$.

Beweis. (i): Sei M' die Diagonalmatrix mit a_i, a_j auf der Diagonalen und gelte

$i < j$. Die unimodularen Transformationen gehen wie folgt: Addiere die zweite Zeile von M' zur ersten. Wende T' aus Lemma 4.20, (i) von rechts auf M' an. Dies liefert

$$\begin{pmatrix} c & 0 \\ \mu a_j & d \end{pmatrix}$$

mit $c = \gcd\{a_i, a_j\}$ und $d = a_i a_j / c = \text{lcm}\{a_i, a_j\}$. Nun ziehen wir das $\mu a_j / c$ -fache der ersten Zeile von der zweiten Zeile ab und erhalten die Diagonalmatrix mit $c = \gcd\{a_i, a_j\}$, $d = \text{lcm}\{a_i, a_j\}$ auf der Diagonalen und es gilt $c \mid d$. Durch sukzessives Vorgehen für $(i, j) = (1, 2), (1, 3), \dots, (2, 3), (2, 4), \dots, (n-1, n)$ und Aufmultiplizieren der entsprechenden unimodularen Transformationsmatrizen folgt (i).

(ii): Eine r -Minore kann nach dem Laplaceschen Entwicklungssatz als Linearkombination von $(r-1)$ -Minoren geschrieben werden. Daher ist das von den r -Minoren erzeugte Hauptideal I in dem von den $(r-1)$ -Minoren erzeugten Hauptideal J enthalten. Wegen $I = Rd_r(M)$ und $J = Rd_{r-1}(M)$ folgt $d_{r-1}(M) \mid d_r(M)$.

Eine r -Minore von MV kann als R -Linearkombination von r -Minoren von M geschrieben werden, wegen der Linearität der Determinante in den Spalten und da jede Spalte von MV eine Linearkombination der Spalten von M ist. Daher folgt wie eben $d_r(M) \mid d_r(MV)$. Weil V unimodular ist, gilt auch $d_r(MV) \mid d_r(M)$ für MV und $M = (MV)V^{-1}$. Analog folgt die Aussage für UM und UMV . \square

4.25 Satz. Sei $M \in R^{n \times m}$ und $d = \min\{n, m\}$. Dann gibt es unimodulare Matrizen $U \in R^{n \times n}$ und $V \in R^{m \times m}$, so daß UMV diagonal ist und für die Diagonalelemente $b_1 \mid \dots \mid b_d$ gilt. Die b_i sind bis auf Multiplikation mit Einheiten eindeutig bestimmt.

Beweis. Wir wenden Lemma 4.20, (i) abwechselnd auf die erste Zeile (unimodulare Transformation von rechts) und erste Spalte (unimodulare Transformation von links) an. Die auftretenden Elemente in Position $(1, 1)$ erzeugen eine aufsteigende Kette von Idealen, welche stationär wird. Dann gilt aber, daß in der ersten Zeile und Spalte außer dem Element an Position $(1, 1)$ alle Elemente Null sind (das Element an Position $(1, 1)$ darf auch Null sein). Induktiv diagonalisieren wir dann die Matrix, die aus M durch Streichen der ersten Zeile und Spalte entsteht, durch unimodulare Transformationen von links und von rechts. Mit Lemma 4.24, (i) erreichen wir die aufsteigende Teilerbedingung.

Es gilt $d_r(UMV) \sim \prod_{i=1}^r b_i$ und somit nach Lemma 4.24, (ii) wegen $d_r(UMV) \sim d_r(M)$ auch $b_r \sim d_r(UMV) / d_{r-1}(UMV) \sim d_r(M) / d_{r-1}(M)$ für $d_{r-1}(M) \neq 0$. Gilt $d_r(M) = 0$ für r minimal, so folgt wegen der Teilerbedingung $b_i \neq 0$ für $1 \leq i \leq r-1$ und $b_i = 0$ für $r \leq i \leq d$. Folglich sind die b_r unabhängig von U, V und bis auf Assoziation eindeutig durch M bestimmt. \square

4.26 Definition. Matrizen UMV in der Diagonalf orm von Satz 4.25 nennt man auch in Smith-Normalform oder Elementarteilerform. Die Einträge b_i nennt man Elementarteiler von M . Man kann zusätzlich fordern, daß die b_i in einem Vertretersystem P liegen.

Will man die Smith-Normalform “von Hand” ausrechnen, kann man wie im Beweis vorgehen. Man tut so, als wollte man die Spalten-Hermite-Normalform ausrechnen und transformiert die erste Zeile in die Form $(*, 0, \dots, 0)$. Dann fährt man fort, die Zeilen-Hermite-Normalform auszurechnen und transformiert die erste Spalte in die Form $(*, 0, \dots, 0)^{tr}$. Dadurch wird im allgemeinen die erste Zeile wieder durcheinandergebracht, aber $*$ wird “kleiner”, bis $*$ alle Elemente der ersten Zeile und Spalte teilt, und diese dann ohne etwas wieder durcheinanderzubringen zu Null gemacht werden können. Komplexitätstechnisch gibt es wieder wesentlich effizientere Verfahren zur Smith-Normalformberechnung.

Wir verwenden jetzt den Satz über die Smith-Normalform, um Aussagen über endlich erzeugte Moduln über Hauptidealringen zu erhalten. Der Satz über die Smith-Normalform kann als Aussage über die Existenz und „diagonale“ Lage von Erzeugendensystemen von Moduln und Untermoduln gesehen werden.

4.27 Satz. Sei M ein endlich erzeugter Modul über dem Hauptidealring R . Dann gibt es $b_i \in R \setminus R^\times$ mit $b_1 \mid \dots \mid b_r$ und

$$M \cong R/b_1R \oplus \dots \oplus R/b_rR.$$

Hierbei sind r und die Elemente b_i bis auf Multiplikation mit Einheiten eindeutig durch M bestimmt.

Beweis. Beweis der Existenz. Da M endlich erzeugt ist, gibt es $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $f : R^n \rightarrow M$. Der Untermodul $N = \ker(f)$ ist nach Satz 4.23 endlich erzeugt und besitzt eine Basis w_i mit $m \leq n$ Elementen. Wir ergänzen diese Basis um $n - m$ Nullspalten w_{m+1}, \dots, w_n zu einem Erzeugendensystem und bezeichnen die resultierende Matrix mit $A \in R^{n \times n}$. Die Einheitsvektoren e_i in R^n bilden eine Basis von M , und es gilt $(e_1, \dots, e_n)A = (w_1, \dots, w_n)$. Nach Satz 4.25 angewendet auf A erhalten wir eine andere Basis e'_i von R^n und ein anderes Erzeugendensystem w'_i von N , so daß $w'_i = a_i e'_i$ mit $a_i \in R$ und $a_i \mid a_{i+1}$ gilt. Daraus ergibt sich $M \cong R^n/N \cong R/a_1 \oplus \dots \oplus R/a_n R$. Durch Fortlassen von Einheiten unter den a_i erhalten wir die gewünschten $b_1, \dots, b_r \in R \setminus R^\times$.

Den Beweis der Eindeutigkeit verschieben wir auf Bemerkung 4.29 und verwenden bis dahin nur die Existenzaussage von Satz 4.27. \square

4.28 Korollar. Sei M ein endlich erzeugter Modul über dem Hauptidealring R .

- (i) Es gibt einen freien Modul F , so daß $M \cong \text{Tor}(M) \oplus F$.

(ii) Ist M torsionsfrei, so ist M frei.

(iii) Mit den Bezeichnungen von Satz 4.27 gilt $\text{Ann}(M) = Rb_r$.

Beweis. Mit Satz 4.27 gilt $\text{Tor}(M) \cong \bigoplus_{b_i \neq 0} R/Rb_i$ und $F = \bigoplus_{b_i=0} R$. Daraus folgen (i) und (ii). Aussage (iii) ist aufgrund der aufsteigenden Teilerbedingung auch klar. \square

Wir merken an, daß die b_i auch Null sein können. Die Anzahl der b_i mit $b_i = 0$ ist gleich dem Rang von M (Beweis Hausaufgabe),

4.29 Bemerkung. Die Eindeutigkeit der b_i in Satz 4.27 wird mit folgenden, modultheoretischen Überlegungen erhalten und liefert einen alternativen Beweis der Eindeutigkeitsaussage von Satz 4.25.

Sei $M \cong R/b_1R \oplus \cdots \oplus R/b_rR$ mit $b_i \in R$ und $b_i \mid b_{i+1}$. Zunächst ist b_r bis auf Multiplikation mit Einheiten eindeutig durch $b_rR = \text{Ann}(M)$ gegeben. Für $b_r = 0$ gilt $b_{r-s+1} = \cdots = b_r = 0$, wobei $s = \text{rank}(M)$ eindeutig durch M bestimmt wird. Ohne Einschränkung können wir daher $b_r \neq 0$ annehmen. Sei p ein Primfaktor von b_r . Für $b \in R$ gilt $p(R/bR) = R/bR$ für $p \nmid b$ und $p(R/bR) \cong R/(b/p)R$ für $p \mid b$. Es folgt $pM \cong R/b'_1R \oplus \cdots \oplus R/b'_rR$ mit $b'_i \in R$ und $b_i = b'_i$ für $1 \leq i \leq r-d$ und $b_i = pb'_i$ für $r-d+1 \leq i \leq r$ für ein d sowie $b'_i \mid b'_{i+1}$. Per Induktion über die Anzahl der Teiler von b_r können wir annehmen, daß die b'_i bis auf Multiplikation mit Einheiten eindeutig durch pM bestimmt sind. Sei $M[p] = \{x \in M \mid px = 0\}$. Dann ist $M[p]$ ein R/pR -Vektorraum und die Anzahl der durch p teilbaren b_i ist gleich $d = \dim M[p]$. Dies zeigt, daß die b_i nur durch M und die aufsteigende Teilerbedingung eindeutig bestimmt sind.

Die Eindeutigkeitsaussage von Satz 4.25 ergibt sich dann aus der Interpretation von M als Transformationsmatrix einer Basis von R^t zu einem Erzeugendensystem eines Untermoduls U sowie der Isomorphie $R^t/U \cong \bigoplus_i R/b_iR$, wobei die b_i die Diagonalelemente der Smith-Normalform von M sind.

4.30 Bemerkung. Die Voraussetzung an die endliche Erzeugung kann nicht fallen gelassen werden, wie der \mathbb{Z} -Modul \mathbb{Q} zeigt.

Ein typischer, praktischer Verwendungszweck der Smith-Normalform ist damit, die Struktur bzw. Isomorphieklasse eines durch Erzeuger und R -Relationen gegebenen Moduls M (also eines Faktormoduls) explizit zu bestimmen. Die Elemente b_1, \dots, b_r aus Satz 4.27 sind bis auf Multiplikation mit Einheiten eindeutig bestimmt und heißen Elementarteiler des Moduls M .

Der folgende Satz ist die Primelementpotenzvariante des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen.

4.31 Satz. Sei M ein endlich erzeugter Modul über dem Hauptidealring R . Dann gibt es Primelemente $\pi_i \in R$, Exponenten $e_i \in \mathbb{Z}^{\geq 1}$ und $n \in \mathbb{Z}^{\geq 0}$ mit

$$M \cong R/\pi_1^{e_1}R \oplus \cdots \oplus R/\pi_r^{e_r}R \oplus R^n.$$

Die Isomorphieklasse von M ist durch die (π_i, e_i) und durch n bis auf die Reihenfolge oder Multiplikation der π_i mit Einheiten eindeutig bestimmt.

Beweis. Sind $a, b \in R$ teilerfremd, so gilt nach dem chinesischen Restsatz $R/Rab \cong R/Ra \oplus R/Rb$ auch als R -Moduln. Dies erlaubt es, die direkte Summe in Satz 4.27 weiter zu zerlegen, so daß die b_i nur noch Potenzen von Primelementen sind. Dies liefert die Existenz der π_i, e_i und von n .

Umgekehrt kann man mit dem chinesischen Restsatz $R/\pi_1^{e_1}R \oplus \cdots \oplus R/\pi_r^{e_r}R$ auch wieder zu $R/b_1R \oplus \cdots \oplus R/b_mR$ mit $b_i \in R \setminus R^\times$ und $b_i \mid b_{i+1}$ auf genau eine Weise zusammenfassen (für jedes Primelement die Potenzen aufsteigend in eine Zeile schreiben und rechtsbündig anordnen. Die b_i sind dann die Produkte der Primelementpotenzen in den Spalten). Die Eindeutigkeit der b_i nach Satz 4.27 impliziert dann die Eindeutigkeit der π_i und e_i wie behauptet. Die Zahl n ist als Rang von M eindeutig bestimmt. \square

4.32 Bemerkung. Für $R = \mathbb{Z}$ liefert der Satz den Struktursatz über endlich erzeugte, abelsche Gruppen.

Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $\phi : \mathbb{Z}^n \rightarrow G$. Die Bilder der Einheitsvektoren $\phi(e_i)$ sind Erzeuger von G , und die Elemente in $\ker(\phi)$ die Relationen. Ist $M \in \mathbb{Z}^{n \times n}$ eine Matrix, deren Spalten Erzeuger von $\ker(\phi)$ bilden, so kann die Struktur von G wie in Satz 4.27 mittels der Smith-Normalform $M' = (b_i \delta_{i,j})_{i,j}$ von M ermittelt werden: Es gilt $G \cong \mathbb{Z}/b_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/b_r\mathbb{Z}$. Für $\det(M) \neq 0$ folgt $\#G = |\prod_i b_i| = |\det(M')| = |\det(M)|$. Für $\det(M) = 0$ folgt $\#G = \infty$. Der betragsmäßig größte Eintrag in M' ist gleich dem Exponenten von G . Der Annulator von G ist gleich dem vom Exponenten erzeugten Ideal von \mathbb{Z} .

Analoges gilt für einen endlich erzeugten Modul V über einem Polynomring $R = k[t]$, wobei k ein Körper ist. Die Anzahlaussagen werden hier am besten durch Dimensionsaussagen ersetzt. Jeder R -Modul ist auch ein k -Vektorraum. Speziell gilt $\dim_k(R) = \infty$ und $\dim_k(R/Rb) = \deg(b)$ für $b \in R \setminus \{0\}$ nach der Eindeutigkeit der Reste der Polynomdivision. Eine Basis von R/Rb wird durch $1, t, \dots, t^{\deg(b)-1}$ gegeben. Beschreibt $M \in R^{n \times n}$ den Kern eines Epimorphismus $R^n \rightarrow V$ wie eben und ist $M' = (b_i \delta_{i,j})_{i,j}$ die Smith-Normalform von M , so gilt $V \cong R/b_1R \oplus \cdots \oplus R/Rb_r$ als R -Moduln. Daraus folgt $\dim_k(V) = \sum_i \deg(b_i) = \deg(\prod_i b_i) = \deg(\det(M')) = \deg(\det(M))$ für $\det(M) \neq 0$ und $\dim_k(V) = \infty$

für $\det(M) = 0$ nach Satz 4.27. Der Annulator von V ist das vom gradgrößten Eintrag von M' erzeugte Hauptideal von R .

Wir führen diese Überlegungen weiter und betrachten damit eine Anwendung von Satz 4.27 in der linearen Algebra. Sei V ein endlich dimensionaler k -Vektorraum und $\phi \in \text{End}_k(V)$. Wir machen V zu einem endlich erzeugten Modul über dem Hauptidealring $R = k[t]$ durch die Festlegung $tx = \phi(x)$. Ein Erzeugendensystem des R -Moduls V ist dann durch die Basis des k -Vektorraums V gegeben, wobei die Basiselemente im allgemeinen nicht mehr R -linear unabhängig sind. Nach Satz 4.27 gilt $V \cong R/Rb_1 \oplus \cdots \oplus R/Rb_r$ mit $b_i \in R$ und $b_i \mid b_{i+1}$. Seien $v_1, \dots, v_r \in V$ die Urbilder der Einheitsvektoren der rechten Seite in V . Mit $V_i = Rv_i$ gilt $V_i \cong R/Rb_i$ und $V = V_1 \oplus \cdots \oplus V_r$. Eine k -Basis von V_i wird durch $v_i, tv_i, t^2v_i, \dots, t^{n_i-1}v_i$ mit $n_i = \deg(b_i)$ gegeben, welches die Urbilder der k -Basis $1, t, \dots, t^{n_i-1}$ von R/Rb_i in V_i sind. Ist $b_i = \sum_{j=0}^{n_i-1} b_{i,j}t^j$, so gilt $t^{n_i} = -\sum_{j=0}^{n_i-1} b_{i,j}t^jv_i$ in R/Rb_i und $t^{n_i}v_i = -\sum_{j=0}^{n_i-1} b_{i,j}(t^jv_i)$ in V_i . Die k -Basen der V_i liefern zusammen also eine k -Basis von V , so daß die Darstellungsmatrix von ϕ bezüglich dieser Basis in rationaler kanonischer Form ist.

Wir können V entsprechend Satz 4.31 auch noch in kleinere Bestandteile zerlegen, wenn wir die b_i faktorisieren. Wir ziehen uns gleich auf den Fall $V \cong R/R(t-a)^n$ zurück und betrachten das Urbild v der Eins von $R/R(t-a)^n$ in V . Eine Basis von V wird wie eben betrachtet durch $v, tv, \dots, t^{n-1}v$ gegeben. Eine andere Basis von V erhalten wir mit $v, (t-a)v, (t-a)^2v, \dots, (t-a)^{n-1}v$, denn die t -Potenzen und die $(t-a)$ -Potenzen bilden beide k -Basen von $R/R(t-a)^n$. Wegen $t(t-a)^i = (t-a)^{i+1} + a(t-a)^i$ und $t(t-a)^{n-1} = (t-a)^n + a(t-a)^{n-1} \equiv a(t-a)^{n-1} \pmod{(t-a)^n}$ erhalten wir für die Operation von ϕ auf der Basis $v, (t-a)v, (t-a)^2v, \dots, (t-a)^{n-1}v$ die üblichen Jordankästchen. Eine solche Zerlegung der Operation von ϕ in mehrere Jordankästchen ist somit für allgemeine V nach Satz 4.31 immer möglich, wenn k algebraisch abgeschlossen ist (also jedes Polynom aus $k[t]$ in Linearfaktoren aus $k[t]$ faktorisiert werden kann, zum Beispiel $k = \mathbb{C}$). Wir erhalten in diesem Fall darüberhinaus eine Zerlegung der Darstellungsmatrix M von ϕ in der Form $M = M_1 + M_2$, wobei M_1 eine Diagonalmatrix und M_2 eine strikt untere Dreiecksmatrix (also nilpotent) ist. Entsprechend zerlegt sich ϕ in $\phi = \phi_1 + \phi_2$.

Wir wollen die Jordan-Normalform mittels der Smith-Normalform wie in den Überlegungen nach Bemerkung 4.32 berechnen. Dazu müssen wir die Matrix M bestimmen. Ist A die Darstellungsmatrix von ϕ bezüglich einer Basis v_i von V (also $(\phi(v_1), \dots, \phi(v_n)) = (v_1, \dots, v_n)A$), so bilden die Spalten von $M = tI_n - A$ eine Basis der Kerns N des Epimorphismus $f : R^n \rightarrow V$, welcher e_i nach v_i abbildet. Die Spalten sind nämlich einerseits im Kern N enthalten, wie man direkt nachrechnet: Ist $A = (a_{i,j})_{i,j}$ und $m_j = \sum_{i=1}^n (\delta_{i,j}t - a_{i,j})e_i$ die j -te Spalte von M ,

so folgt $f(m_j) = \sum_{i=1}^n (\delta_{i,j}t - a_{i,j})v_i = \phi(v_j) - \sum_{i=1}^n a_{i,j}v_i = 0$. Auf der anderen Seite gilt $\deg(\det(tI_n - M)) = n$ und für den von den Spalten von M erzeugten Untermodul N' von N die Gleichung $\dim_k(R^n/N') = \deg(\det(tI_n - M)) = n$ wie oben dargelegt. Wegen $\dim_k(R^n/N) = n$ und $N' \subseteq N$ folgt $N' = N$. Mit Hilfe von $M = tI_n - A$ und der Smith-Normalform kann man also die rationale kanonische Form oder die Jordan-Normalform von M berechnen. In der obigen Notation ist b_r (der Erzeuger des Annulators) das Minimalpolynom und $\det(tI_n - A) = \prod_i b_i$ das charakteristische Polynom von ϕ .

Darstellungsmatrizen A_1, A_2 von ϕ bezüglich verschiedener Basen von V liefern verschiedene charakteristische Matrizen $tI_n - A_1, tI_n - A_2$ und Kerne N_1, N_2 von R^n . Es gilt aber, daß R^n/N_1 und R^n/N_2 als R -Moduln isomorph sind. Wegen der Eindeutigkeit der Elementarteiler stimmen daher die Smith-Normalformen von $tI_n - A_1$ und $tI_n - A_2$ überein. Gleichsetzen zeigt, daß $tI_n - A_1$ und $tI_n - A_2$ als Matrizen äquivalent über R sind. Daher sind A_1 und A_2 genau dann ähnlich über k , wenn $tI_n - A_1$ und $tI_n - A_2$ über R äquivalent sind (Satz von Frobenius).

Nach Satz 4.19 gilt $\det(tI_n - A)R^n \subseteq N$ und äquivalenterweise $\det(tI_n - A)V = \{0\}$. Das ist der Satz von Cayley-Hamilton: Wenn man ϕ beziehungsweise M in sein charakteristisches Polynom $\det(tI_n - A)$ einsetzt, kommt die Nullabbildung beziehungsweise die Nullmatrix heraus.

Hausaufgabe: Wie findet man ausgehen von $M = tI_n - A$ die Basen, bezüglich derer die Darstellungsmatrix von ϕ in rationaler kanonischer Form oder in Jordan-Normalform ist?

4.5 Gröbnerbasen

Gröbnerbasen sind spezielle Erzeugendensysteme von Moduln über multivariaten Polynomringen und ermöglichen Algorithmen für eine Vielzahl von Berechnungsproblemen wie zum Beispiel den Test auf Zugehörigkeit von Elementen eines Moduls zu einem Untermodul. Sie stellen eine weitreichende Verallgemeinerung von Basen eines Untermoduls von $k[x]^n$ in Hermite-Normalform über einem univariaten Polynomring $k[x]$ über einem Körper dar. Im folgenden gehen wir nur auf die Grundidee ein, dies allerdings in einer recht allgemeinen Formulierung.

4.33 Definition. Sei R ein Integritätsring. Wir definieren eine „Theorie des Leitterms“ für R wie folgt.

Sei G ein abelscher Monoid mit Kürzungsregel und einer mit der Addition in G verträglichen Wohlordnung \geq sowie $d \geq 0$ für alle $d \in G$. Wir nennen G in diesem Abschnitt einen Gradbereich.

Für jedes $d \in G$ sei R_d eine Untergruppe der additiven Gruppe von R , so daß

$$R = \coprod_{d \in G} R_d$$

ist. Für die Multiplikation in R soll gelten $R_d R_e \subseteq R_{d+e}$ sowie $1 \in R_0$.

Wir nennen die Elemente aus $R_d \setminus \{0\}$ Terme oder homogene Elemente von R des Grads d . Jedes $f \in R$ ist also auf eindeutige Weise eine endliche Summe $f = \sum_{d \in G} f_d$ von Termen f_d von R . Ist $f \neq 0$ und d maximal in G mit $f_d \neq 0$, so definieren wir den Leitterm von f als $\text{lt}(f) = f_d$ und den Grad von f als $\text{deg}(f) = d$. Für $f = 0$ definieren wir $\text{lt}(f) = 0$ und $\text{deg}(f) = -\infty$.

Wir nennen R zusammen mit diesen Definitionen einen G -graduerten Ring. Ein Homomorphismus der G -graduerten Ringe R und G ist ein Ringhomomorphismus $\phi : R \rightarrow G$ mit $\phi(R_d) \subseteq G_d$ für alle $d \in G$.

Ist R ein G -graduierter Ring, so dehnen wir diese Definitionen auf einen R -Modul wie folgt aus.

4.34 Definition. Sei H ein Gradbereich und $G \subseteq H$ ein abelscher Untermonoid, so daß G bezüglich der Ordnung von H ebenfalls ein Gradbereich ist. Sei R ein G -graduierter Ring und M ein R -Modul. Für jedes $d \in H$ sei M_d eine Untergruppe der additiven Gruppe von M , so daß

$$M = \coprod_{d \in T} M_d$$

ist. Für die Multiplikation mit Elementen aus R soll gelten $R_d M_e \subseteq M_{d+e}$ für alle $d \in G$ und $e \in H$.

Wir nennen die Elemente aus $M_d \setminus \{0\}$ Terme oder homogene Elemente von M des Grads d . Jedes $f \in M$ ist also auf eindeutige Weise eine endliche Summe $f = \sum_{d \in G} f_d$ von Termen f_d von M . Ist $f \neq 0$ und d maximal in H mit $f_d \neq 0$, so definieren wir den Leitterm von f als $\text{lt}(f) = f_d$ und den Grad von f als $\text{deg}(f) = d$. Für $f = 0$ definieren wir $\text{lt}(f) = 0$ und $\text{deg}(f) = -\infty$.

Wir nennen M zusammen mit diesen Definitionen einen H -graduerten R -Modul. Ein Homomorphismus der H -graduerten R -Moduln M und N ist ein R -Modulhomomorphismus $\phi : M \rightarrow N$ mit $\phi(M_d) \subseteq N_d$ für alle $d \in H$.

Für $d \in H$ definieren wir $M(-d) = M$ als R -Modul und $M(-d)_e = M_{e-d}$, falls $e-d \in H$, und $M(-d)_e = 0$ sonst. Da mit e auch $e-d$ über alle Elemente aus H läuft, gilt $M(-d) = \coprod_{e \in H} M(-d)_e$ und $M(-d)$ ist ebenfalls ein H -graduierter Modul. Ist f ein Term von $M(-d)$ vom Grad n , so ist f auch ein Term von M vom Grad $n-d$.

In der Definition 4.34 werden nur Elemente aus G und aus H , nicht jedoch zwei Elemente aus H addiert. Es würde daher genügen, H als wohlgeordnete Menge zu definieren, auf der G mit den Ordnungsrelationen verträglich durch eine Verknüpfung $+$ operiert.

Aufgrund der Definitionen sind die M_d auch R_0 -Moduln.

4.35 Beispiel. Sei 0 der Nullmonoid. Ist R ein Ring und M ein R -Modul, so setzen wir $R_0 = R$ und $M_0 = M$ und erhalten R und M als 0 -graduierten Ring beziehungsweise als 0 -graduierten Modul.

4.36 Beispiel. Seien G_1, G_2 Gradbereiche. Dann können wir den abelschen Monoid $G_1 \times G_2$ zu einem Gradbereich machen, in dem wir $(x_1, y_1) \leq (x_2, y_2) : \Leftrightarrow y_1 < y_2$ oder $(y_1 = y_2$ und $x_1 \leq x_2)$ für $x_1, x_2 \in G_1$ und $y_1, y_2 \in G_2$ definieren.

Ist R ein G -graduierter Ring, so können wir damit $R[t]$ zu einem $G \times \mathbb{Z}^{\geq 0}$ -graduierten Ring machen, indem wir $R[t]_{(d,n)} = \{at^n \mid a \in R_d\}$ definieren.

Ist $k[t_1, \dots, t_n]$ und ist k ein 0 -graduierter Körper wie in Beispiel 4.35, so wird $k[t_1, \dots, t_n]$ induktiv zu einem $(\mathbb{Z}^{\geq 0})^n$ -graduierten Ring, wobei die Elemente aus $(\mathbb{Z}^{\geq 0})^n$ lexikographisch angeordnet sind. Die $k[t_1, \dots, t_n]_d$ sind hier auch ein-dimensionale k -Vektorräume, die jeweils von einem Monom in t_1, \dots, t_n erzeugt werden.

Für $k[t]$ erhalten wir einen $\mathbb{Z}^{\geq 0}$ -graduierten Ring, $M_d = \{at^d \mid a \in k\}$ und $\deg(t^d) = d$, wie gewohnt.

4.37 Beispiel. Ist R ein G -graduierter Ring und sind M_1, \dots, M_n H -graduierte R -Moduln, so können wir $M = \coprod_{i=1}^n M_i$ wie folgt zu einem H -graduierten R -Modul machen. Wir definieren $M_d = \coprod_{i=1}^n (M_i)_d$. Wie man leicht sieht, gilt $M = \coprod_{d \in H} M_d$ und M ist ein H -graduierter R -Modul.

4.38 Beispiel. Führen wir die Konstruktion aus Beispiel 4.37 mit $R = k[t_1, \dots, t_n]$ und $M_i = R$ wie in Beispiel 4.36 durch, so erhalten wir $\dim_k(R_d) = 1$ und $\dim_k((R^n)_d) = n$. Es ist aber mitunter wünschenswert, $\dim_k((R^n)_d) = 1$ zu haben. Dies kann mit der folgenden Konstruktion erreicht werden.

Sei R ein G -graduierter Ring und $H = G \times \mathbb{Z}^{\geq 0}$ wie in Beispiel 4.36. Wir identifizieren G mit dem Untermonoid $G \times \{0\}$. Sei $\iota_i : M_i \rightarrow M = \coprod_{i=1}^n M_i$ die i -te Einbettung. Für $e \in H$ mit $e = (d, i)$ definieren wir $M_e = \iota_i(M_d)$ für $1 \leq i \leq n$ und $M_e = 0$ sonst. Damit wird M zu einem H -graduierten R -Modul. Die Terme aus M werden durch \deg wieder lexikographisch angeordnet.

4.39 Beispiel. Sei M ein H -graduierter R -Modul und N ein Untermodul, welcher von Termen $f_i \in M$ erzeugt wird. Dann ist N ein H -graduierter R -Untermodul von M , wie man sich leicht überlegt: Ist $N_d = N \cap M_d$, so gilt $N = \coprod_{d \in H} N_d$. Daher wird auch $M/N = \coprod_{d \in H} M_d/N_d$ zu einem H -graduierten Modul, indem wir $(M/N)_d = M_d/N_d$ definieren.

4.40 Beispiel. Gröbnerbasen werden häufig nur für $R = k[t_1, \dots, t_n]$ und mit Hilfe von Monomordnungen, also mit der Multiplikation von Monomen verträglichen Ordnungen der Monome von $k[t_1, \dots, t_n]$, behandelt. Die Verbindung zu unseren allgemeinen Definitionen ist dabei wie folgt. Ist \leq eine solche Monomordnung, so definieren wir eine Termordnung \leq für Terme a, b durch $a \leq b$, wenn dies für die unterliegenden Monome gilt. Streng genommen ist dies keine Ordnung mehr, da für Terme a, b aus $a \leq b$ und $b \leq a$ nicht mehr $a = b$ folgt. Wir können jedoch eine Äquivalenzrelation \approx für Terme a, b durch $a \approx b : \Leftrightarrow (a \leq b \text{ und } b \leq a)$ definieren. (Gilt $a \approx b$, so gibt es $c \in k^\times$ mit $a = cb$.) Die Äquivalenzklasse von a sei mit $[a]$ bezeichnet. Damit definieren wir $G = \{[a] \mid a \text{ Term von } R\}$, $[a] + [b] = [ab]$ sowie $[a] \leq [b] \Leftrightarrow a \leq b$. Dann ist G ein Gradbereich und es gilt $k[t_1, \dots, t_n]_d = \{a \mid a \text{ Term von } R \text{ mit } [a] = d\} \cup \{0\}$, sowie $\deg(a) = [a]$ für Terme a von R .

Umgekehrt erhalten wir für einen G -graduierten Ring mit $a \leq b : \Leftrightarrow \deg(a) \leq \deg(b)$ eine Termordnung im obigen Sinn. Unsere Definition ist jedoch allgemeiner, da zum Beispiel für $R = k[t_1, \dots, t_n]$ und $G = \mathbb{Z}^{\geq 0}$ auch homogene Polynome vom Grad $d \in \mathbb{Z}^{\geq 0}$ als Terme vom Grad d aufgefaßt werden können.

In praktischen Situation geht man von Monomordnungen wie oben aus, und erhält daraus die graduierten Ringe beziehungsweise graduierten Moduln.

Im folgenden sei R ein G -graduierter Ring und M ein H -graduierter Modul. Die Grundidee ist nun, Berechnungen mit Elementen aus M auf Berechnungen mit Elementen aus M_d für $d \in H$ zurückzuführen. Die Annahme hierbei ist, daß letzteres relativ einfach ein soll, was aber von der konkreten Situation abhängt (zum Beispiel besteht für 0-graduierte Modul kein Unterschied in Berechnungen in M oder in den M_d , da $M_0 = M$ und es keine weiteren d gibt). Im folgenden ist es oft hilfreich, sich M als $\coprod_{d \in H} M_d$ vorzustellen.

4.41 Lemma. Seien $f, g_1, \dots, g_m \in M$ und $\lambda_i \in R$ mit $\text{lt}(f) = \sum_{i=1}^m \lambda_i \text{lt}(g_i)$. Dann gibt es $\mu_i \in R$ mit $\text{lt}(f) = \sum_{i=1}^m \mu_i \text{lt}(g_i)$ und $\mu_i = 0$ oder μ_i ein Term von R mit $\deg(\mu_i g_i) = \deg(f)$ für $1 \leq i \leq m$.

Beweis. Gilt $d = \deg(\lambda_i g_i) > \deg(f)$ für ein i , und ist d maximal mit dieser Eigenschaft, so addiert sich $\text{lt}(\lambda_i) \text{lt}(g_i)$ mit anderen $\text{lt}(\lambda_j) \text{lt}(g_j)$ gleichen Grads innerhalb M_d zu Null. Wir können daher die entsprechenden $\text{lt}(\lambda_i)$ und $\text{lt}(\lambda_j)$ aus λ_i beziehungsweise λ_j entfernen, ohne das Ergebnis der Summe $\sum_i \lambda_i \text{lt}(g_i)$ zu ändern, da die $\text{lt}(g_i)$ Terme sind. Da G wohlgeordnet ist, bricht dieser Reduktionsprozeß nach endlichen vielen Schritten mit $\lambda'_i \in R$ mit $\text{lt}(f) = \sum_i \lambda'_i \text{lt}(g_i)$ und $\deg(\lambda'_i g_i) \leq \deg(f)$ für alle i ab. Da $\text{lt}(f) = \sum_i \lambda'_i \text{lt}(g_i)$ ein Term ist, folgt $\text{lt}(f) = \sum_{\deg(\lambda'_i g_i) = \deg(f)} \text{lt}(\lambda'_i) \text{lt}(g_i)$ durch Einschränkung der Betrachtung auf $M_{\deg(f)}$. Also gibt es μ_i wie behauptet. \square

In Anwendungen gehen wir davon aus, daß wir effektiv feststellen können, ob es zu f und den g_i Elemente μ_i wie in Lemma 4.41 gibt, und daß wir diese gegebenenfalls effektiv berechnen können. Die Idee hierbei ist, daß dies leicht möglich sein sollte, da wir nur mit Termen arbeiten müssen. Wir bemerken, daß die μ_i im allgemeinen nicht eindeutig bestimmt sind.

Der folgende Satz liefert eine verallgemeinerte Polynomdivision mit Rest.

4.42 Satz. *Seien $f, g_1, \dots, g_m \in M$. Dann gibt es $\lambda_i \in R$ und $r \in M$ mit*

$$f = \sum_{i=1}^m \lambda_i g_i + r$$

sowie $\deg(\lambda_i g_i) \leq \deg(f)$ für $1 \leq i \leq m$ und $r = 0$ oder $\text{lt}(r) \notin \sum_{i=1}^m R \text{lt}(g_i)$.

Beweis. Für $\text{lt}(f) \notin \sum_{i=1}^m R \text{lt}(g_i)$ ist der Satz mit $\lambda_i = 0$ und $r = f$ wahr. Es gelte also $\text{lt}(f) \in \sum_{i=1}^m R \text{lt}(g_i)$. Nach Lemma 4.41 gibt es $\mu_i \in R$ mit $\text{lt}(f) = \sum_i \mu_i \text{lt}(g_i)$ und $\deg(\mu_i g_i) \leq \deg(f)$. Sei $h = f - \sum_i \mu_i g_i$. Dann gilt $\deg(h) < \deg(f)$, da sich der Leitterm von f weghebt. Da G wohlgeordnet ist, muß dieser Reduktionsprozeß mit $h = 0$ oder $h \notin \sum_{i=1}^m R \text{lt}(g_i)$ enden. \square

Der Beweis liefert aufbauend auf Lemma 4.41 ein Verfahren, wie die λ_i und r zu berechnen sind. Allerdings hängen die λ_i und r von den Wahlen der μ_i in den einzelnen Schritten des Verfahrens ab und sind somit im allgemeinen nicht eindeutig bestimmt.

Satz 4.42 motiviert folgende Definition.

4.43 Definition. Sei N ein Untermodul von M . Elemente $g_1, \dots, g_m \in N$ heißen eine Gröbnerbasis von N , wenn $\text{lt}(f) \in \sum_{i=1}^m R \text{lt}(g_i)$ für alle $f \in N$ gilt.

Ist N ein Untermodul von M , g_1, \dots, g_m eine Gröbnerbasis von N und $f \in M$, so können wir mit Satz 4.42 leicht feststellen, ob $f \in N$ gilt oder nicht. Wir berechnen dazu ein r wie in Satz 4.42, und dann gilt aufgrund der Gröbnerbasiseigenschaft $f \in N$ genau dann, wenn $r = 0$ gilt. Speziell sind die g_1, \dots, g_m auch ein Erzeugendensystem von N .

4.44 Satz. *Sei M noethersch. Dann besitzt jeder Untermodul N eine Gröbnerbasis.*

Beweis. Seien $g_1, \dots, g_m \in N$ ein endliches Erzeugendensystem von N und $T_m = \sum_{i=1}^m R \text{lt}(g_i)$. Sind die g_i keine Gröbnerbasis von N , so gibt es $f \in N$ mit $\text{lt}(f) \notin T_m$. Wir setzen $g_{m+1} = f$, $T_{m+1} = \sum_{i=1}^{m+1} R \text{lt}(g_i)$ und erhalten $T_m \subsetneq T_{m+1}$. Da M noethersch ist, muß diese Konstruktion abbrechen, es muß also ein n mit $\text{lt}(f) \in T_n$ für alle $f \in N$ geben. Dann ist g_1, \dots, g_n eine Gröbnerbasis von N . \square

Wir wollen im folgenden eine Charakterisierung von Gröbnerbasen angeben, die es erlaubt, ein Konstruktionsverfahren für Gröbnerbasen anzugeben.

4.45 Satz. *Seien $g_1, \dots, g_m \in M$ ein Erzeugendensystem von N . Die g_i sind genau dann eine Gröbnerbasis von N , wenn es für $f = \sum_{i=1}^m \lambda_i g_i$ mit beliebigen $\lambda_i \in R$ Elemente $\mu_i \in R$ mit $f = \sum_{i=1}^m \mu_i g_i$ und $\deg(\mu_i g_i) \leq \deg(f)$ gibt.*

Beweis. „ \Rightarrow “: Ergibt sich aus Satz 4.42, da dort nur $r = 0$ möglich ist.

„ \Leftarrow “: Es folgt $\text{lt}(f) = \sum_{\deg(\mu_i g_i) = \deg(f)} \text{lt}(\mu_i) \text{lt}(g_i)$, also $\text{lt}(f) \in \sum_i R \text{lt}(g_i)$. \square

Unser Ziel ist es, die Bedingung von Satz 4.45 nur für gewisse, endlich viele Vektoren $(\lambda_1, \dots, \lambda_m)$ mit $\deg(\lambda_i g_i) > \deg(f)$ für ein mindestens ein i überprüfen zu müssen, um auf die Gröbnerbasiseigenschaft der g_i schließen zu können.

Sei $F = \coprod_{i=1}^m R(-\deg(g_i))$ der G -graduierte R -Modul, der wie in Beispiel 4.37 für die G -graduierten Moduln $R(-\deg(g_i))$ definiert wird. Damit kann die Gradaussage $\deg(\mu_i g_i) \leq \deg(f)$ vereinfacht als $\deg((\mu_i)_i) \leq \deg(f)$ geschrieben werden, wobei $(\mu_i)_i$ als Element von F aufgefaßt wird. Für die unterliegenden R -Moduln (das heißt, wenn wir die Graduierung außer acht lassen) gilt $F = R^n$.

4.46 Satz. *Sei R noethersch und seien $g_1, \dots, g_m \in M$ ein Erzeugendensystem von N . Es gibt endlich viele Terme $(\lambda_{1,j}, \dots, \lambda_{m,j})$ von F mit der folgenden Eigenschaft. Sei $f_j = \sum_{i=1}^m \lambda_{i,j} g_i$. Dann sind die g_i genau dann eine Gröbnerbasis von N , wenn es $(\mu_{1,j}, \dots, \mu_{m,j}) \in F$ mit $f_j = \sum_{i=1}^m \mu_{i,j} g_i$ und $\deg((\mu_{1,j}, \dots, \mu_{m,j})) \leq \deg(f_j)$ für alle j gibt.*

Beweis. „ \Rightarrow “: Folgt aus Satz 4.45.

„ \Leftarrow “: Wir brauchen uns nur auf $(\lambda_{i,j})_i$ mit $\deg((\lambda_{i,j})_i) > \deg(f_j)$ zu beschränken. Wir betrachten den von allen Termen $(\lambda_i)_i \in F$ mit $\deg((\lambda_i)_i) > \deg(\sum_i \lambda_i g_i)$ erzeugten Untermodul V von F . Da F mit R noethersch ist, genügen zur Erzeugung von V endlich viele solcher $(\lambda_i)_i$, und diese seien mit $(\lambda_{i,j})_i$ bezeichnet. Zu den $(\lambda_{i,j})_i$ seien die f_j und die $(\mu_{i,j})_i$ wie in der Voraussetzung.

Seien $(\lambda_i)_i \in F$ und $f = \sum_i \lambda_i g_i$ mit $\deg((\lambda_i)_i) > \deg(f)$. Nach Satz 4.45 genügt es zu zeigen, daß es $(\mu_i)_i \in F$ mit $f = \sum_i \mu_i g_i$ und $\deg((\mu_i)_i) \leq \deg(f)$ gibt. Sei $d = \deg((\lambda_i)_i)$ und $(\lambda'_i)_i = (\lambda_i)_i - \text{lt}((\lambda_i)_i)$. Es gilt $\deg((\lambda'_i)_i) < d$ und $\text{lt}((\lambda_i)_i) \in V$. Daher gibt es $w_j \in R$ mit $\text{lt}((\lambda_i)_i) = \sum_j w_j (\lambda_{i,j})_i$. Nach Lemma 4.41 können wir ohne Einschränkung annehmen, daß $w_j = 0$ oder $\deg(w_j (\lambda_{i,j})_i) = \deg(\text{lt}((\lambda_i)_i)) = d$ gilt. Wir erhalten $(\lambda_i)_i = \text{lt}((\lambda_i)_i) + (\lambda'_i)_i = \sum_j w_j (\lambda_{i,j})_i + (\lambda'_i)_i$ und $f = \sum_i \lambda_i g_i = \sum_i \sum_j w_j \lambda_{i,j} g_i + \sum_i \lambda'_i g_i$. Wegen $f_j = \sum_i \lambda_{i,j} g_i = \sum_i \mu_{i,j} g_i$ erhalten wir weiter $f = \sum_j \sum_i w_j \mu_{i,j} g_i + \sum_i \lambda'_i g_i = \sum_i \lambda''_i g_i$ mit $(\lambda''_i)_i = \sum_j w_j (\mu_{i,j})_i + (\lambda'_i)_i \in F$. Wegen $\deg((\mu_{i,j})_i) < \deg((\lambda_{i,j})_i)$ nach Voraussetzung gilt auch $\deg(w_j (\mu_{i,j})_i) < \deg(w_j (\lambda_{i,j})_i) = d$. Mit $\deg((\lambda'_i)_i) < d$ ergibt sich zusammen $\deg((\lambda''_i)_i) < d$.

Gilt also $f = \sum_i \lambda_i g_i$ für $(\lambda_i)_i \in F$ mit $\deg((\lambda_i)_i) > \deg(f)$, so gibt es aufgrund der Voraussetzungen $(\lambda''_i)_i \in F$ mit $f = \sum_i \lambda''_i g_i$ und $\deg((\lambda''_i)_i) < \deg((\lambda_i)_i)$. Wegen der Wohlordnungseigenschaft erhalten wir nach endlich vielen Schritten $(\mu_i)_i = (\lambda''_i)_i \in F$ mit $f = \sum_i \mu_i g_i$ und $\deg((\mu_i)_i) \leq \deg(f)$. \square

Satz 4.46 wird auch (verallgemeinertes) Kriterium von Buchberger genannt. Es liefert eine Möglichkeit, Gröbnerbasen in endlichen vielen Schritten zu konstruieren.

4.47 Algorithmus. (Buchberger)

Input: Ein endliches Erzeugendensystem G des R -Untermoduls $N \neq 0$ von M , wobei M endlich erzeugt und R noethersch ist.

Output: Eine Gröbnerbasis von N .

1. Berechne die $(\lambda_{g,j})_g$ aus Satz 4.46 und $f_j = \sum_{g \in G} \lambda_{g,j} g$.
2. Berechne $f_j = \sum_{g \in G} \mu_{g,j} g + r_j$ für alle j wie in Satz 4.42.
3. Sind alle $r_j = 0$, so gebe G aus und terminiere.
4. Füge die r_j mit $r_j \neq 0$ zu G hinzu und gehe zu Schritt 1.

Beweis. Wir müssen zeigen, daß der Algorithmus nach endlichen vielen Schritten mit einer Gröbnerbasis von N terminiert.

Sei $T_G = \sum_{g \in G} R \text{lt}(g)$. Für $r_j \neq 0$ gilt $\text{lt}(r_j) \notin T_G$ nach Satz 4.42. Durch die Hinzunahme von diesen r_j zu G vergrößern wir also T_G . Da M noethersch ist (M ist endlich erzeugt und R ist noethersch), kann Schritt 4 nur endlich oft durchlaufen werden. Sind aber alle $r_j = 0$, so ist G nach Satz 4.46 eine Gröbnerbasis von N . \square

4.48 Beispiel. Wir betrachten eine konkrete Form von Satz 4.46 für $R = k[t_1, \dots, t_n]$ und $M = R$. Wir wählen G so, daß M_d für alle $d \in G$ ein von einem Monom erzeugter, eindimensionaler k -Vektorraum wird (wie in Beispiel 4.36 zum Beispiel).

Seien $g_1, \dots, g_m \in M$. Gilt $f = \sum_i \lambda_i g_i$ mit $d = \max_i \deg(\lambda_i g_i) > \deg(f)$. Dann besitzen alle $\lambda_i g_i$ mit $\deg(\lambda_i g_i) = d$, hiervon gibt es mindestens zwei, bis auf Vielfache aus k^\times den gleichen Leitterm v . Daher ist v durch das kleinste gemeinsame Vielfache der Leitterme der zugehörigen g_i teilbar. Seien konkret g_1 und g_2 unter diesen g_i und seien $\sigma_{1,2}, \sigma_{2,1}$ Terme mit $\sigma_{1,2} \text{lt}(g_1) = \sigma_{2,1} \text{lt}(g_2) = \text{lcm}\{\text{lt}(g_1), \text{lt}(g_2)\}$. Wir verwenden hier, daß k ein Körper ist und es ein kleinstes gemeinsames Vielfaches von Termen gibt. Wegen $\sigma_{1,2} \text{lt}(g_1) \mid \text{lt}(\lambda_1 g_1)$ und $\sigma_{2,1} \text{lt}(g_2) \mid \text{lt}(\lambda_1 g_1)$ gibt es Terme w_1, w_2 mit $\text{lt}(\lambda_1 g_1) = w_1 \sigma_{1,2} \text{lt}(g_1) = w_2 \sigma_{2,1} \text{lt}(g_2)$. Also

gilt auch $\text{lt}(\lambda_1) = w_1\sigma_{1,2}$. Gibt es nun $\mu_i \in R$ mit $\sigma_{1,2}g_1 - \sigma_{2,1}g_2 = \sum_i \mu_i g_i$ und $\deg(\mu_i g_i) \leq \deg(\sum_i \mu_i g_i) < d$, so definieren wir: $\lambda'_1 = \lambda_1 - w_1\sigma_{1,2} + w_1\mu_1$, $\lambda'_2 = \lambda_2 + w_1\sigma_{2,1} + w_1\mu_2$, $\lambda'_i = \lambda_i + w_1\mu_i$ für $i > 2$. Dann gilt $f = \sum_i \lambda_i g_i = \sum_i \lambda'_i g_i$, $\deg(\lambda'_i g_i) \leq \deg(\lambda_i g_i)$ und in der zweiten Summe gilt $\deg(\lambda'_i g_i) = d$ mindestens einmal weniger als $\deg(\lambda_i g_i) = d$ in der ersten Summe.

Iterieren wir diese Reduktion, so erhalten wir zwei Aussagen. Erstens: Seien die $\sigma_{i,j}$ Terme mit $\sigma_{i,j}\text{lt}(g_i) = \sigma_{j,i}\text{lt}(g_j)$ und die e_i Einheitsvektoren in R^m . Dann bilden die $\sigma_{i,j}e_i - \sigma_{j,i}e_j$ für alle $i \neq j$ eine Familie von $(\lambda_{1,j}, \dots, \lambda_{m,j})$ wie in Satz 4.46. Zweitens: Die Reduktionsprozedur liefert einen alternativen Beweis von Satz 4.46.

Sei N ein Untermodul von M . Wir definieren $\deg(N) = \{\deg(f) \mid f \in N\}$. Der Einfachheit halber nehmen wir nun an, daß R_0 ein Körper ist und daß R_d und M_e freie R_0 -Moduln vom Rang eins für alle $d \in G$ und $e \in H$ sind. Dies ist in vielen Anwendungen der Fall. Für jedes $d \in H$ wählen wir einen Erzeuger m_d von M_d .

4.49 Definition. Seien die $g_1, \dots, g_m \in M$ eine Gröbnerbasis von N . Dann heißen die g_i eine minimale Gröbnerbasis, wenn kein g_i fortgelassen werden kann, so daß die restlichen g_j eine Gröbnerbasis von N bilden.

Sind die $g_1, \dots, g_m \in M$ eine minimale Gröbnerbasis von N , so heißen die g_i eine reduzierte Gröbnerbasis, wenn $(g_i)_{\deg(g_i)} = m_{\deg(g_i)}$ und $(g_i)_d = 0$ für alle $d \in H$ mit $d < \deg(g_i)$ und $d \in \deg(M)$ sowie alle i gilt.

Die Existenz minimaler Gröbnerbasen ist klar. Eine Gröbnerbasis g_1, \dots, g_m von N ist genau dann minimal, wenn die $\text{lt}(g_1), \dots, \text{lt}(g_m)$ ein minimales Erzeugendensystem von $\text{lt}(N)$ bilden.

4.50 Satz. Sei N ein Untermodul von M . Besitzt N eine Gröbnerbasis, so gibt es mit den obigen Definitionen genau eine reduzierte Gröbnerbasis von N .

Beweis. Sei $g_1, \dots, g_m \in M$ eine minimale Gröbnerbasis von M , wobei wir ohne Einschränkung $\deg(g_i) < \deg(g_{i+1})$ annehmen dürfen. Durch Multiplikation mit Elementen aus R_0^\times können wir $(g_i)_{\deg(g_i)} = m_{\deg(g_i)}$ für alle i erreichen. Wir zeigen nun per Induktion über i , daß es eine minimale Gröbnerbasis g_1, \dots, g_m von N gibt, in der g_1, \dots, g_i den Reduktionsbedingungen genügen. Für $i = 1$ ist die Aussage klar, da $\deg(g_1)$ minimal in $\deg(N)$ ist. Für den Schritt $i - 1$ nach i bemerken wir, daß wir g_i durch ein Element der Form $g_i - \sum_{j=1}^{i-1} \lambda_j g_j$ mit $\deg(\lambda_j g_j) < \deg(g_i)$ ersetzen können, so daß $(g_i)_d = 0$ für alle $d < \deg(g_i)$ und $d \in \deg(N)$ gilt. Die resultierenden Elemente sind dann immer noch eine minimale Gröbnerbasis. Für $i = n$ erhalten wir per Induktion schließlich eine reduzierte Gröbnerbasis.

Der Beweis der Eindeutigkeit ist eine Hausaufgabe. \square

4.51 Bemerkung. Minimale Gröbnerbasen entsprechen der Spalten-Stufenform aus Definition 4.21, wohingegen reduzierte Gröbnerbasen der Hermite-Normalform entsprechen. Die Grade der Elemente einer minimalen Gröbnerbasis entsprechen den Zeilenindizes der Stufen in der Spalten-Stufenform und stellen (in aufsteigender Reihenfolge sortiert) eine Invariante des graduierten Moduls dar. Das Reduktionsverfahren in Satz 4.50 ist dem im Satz 4.22 nachempfunden.

4.52 Bemerkung. Reduzierte Gröbnerbasen lassen sich auch allgemein definieren, wenn man kanonische Erzeugendensysteme (zum Beispiel wieder reduzierte Gröbnerbasen) der R_0 -Untermoduln $\text{lt}(N)_d$ der M_d sowie Vertretersysteme der $M_d/\text{lt}(N)_d$ definiert, wobei $\text{lt}(N) = \sum_{f \in N} R \text{lt}(f)$ ist. Zum Beispiel sollen die $(g_i)_{\deg(g_i)}$ mit $\deg(g_i) = e$ kanonische Erzeuger von $\text{lt}(N)_e$ sein und die $(g_i)_d$ aus den Vertretersystemen von $M_d/\text{lt}(N)_d$ stammen. Der Beweis von Satz 4.50 kann dann im Prinzip relativ ähnlich geführt werden.