Springer-Lehrbuch

Algebra

von
Siegfried Bosch

7., überarb. Aufl.

Springer 2009

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 540 92811 9

Inhaltsverzeichnis: Algebra – Bosch

2. Ringe und Polynome

Vorbemerkungen

Ein *Ring* ist eine additiv geschriebene abelsche Gruppe R, auf der zusätzlich eine Multiplikation definiert ist, wie etwa beim Ring $\mathbb{Z}$ der ganzen Zahlen. Dabei verlangt man, dass R ein Monoid bezüglich der Multiplikation ist und dass Addition und Multiplikation im Sinne der Distributivgesetze miteinander verträglich sind. Wir werden die Multiplikation in Ringen stets als *kommutativ* voraussetzen, abgesehen von einigen Betrachtungen in Abschnitt 2.1. Bilden die von Null verschiedenen Elemente eines Ringes sogar eine (abelsche) Gruppe bezüglich der Multiplikation, so handelt es sich um einen *Körper*. Die Definition eines Rings geht dem Sinne nach auf R. Dedekind zurück. Bei Dedekind waren Ringe zahlentheoretisch motiviert durch das Rechnen mit ganzen Zahlen in algebraischen Zahlkörpern, also durch das Studium algebraischer Gleichungen mit *ganzzahligen* Koeffizienten. Wir werden jedoch auf Ringe ganzer algebraischer Zahlen nur am Rande eingehen. Wichtiger sind für uns Körper als Koeffizientenbereiche algebraischer Gleichungen sowie Polynomringe über Körpern. Im Folgenden wollen wir den Polynombegriff etwas näher erläutern. Polynome sind bei der Handhabung algebraischer Gleichungen und insbesondere algebraischer Körpererweiterungen von grundlegender Bedeutung.

Wenn man eine algebraische Gleichung

$$(*) \qquad x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

lösen möchte, etwa mit Koeffizienten $a_1, \ldots, a_n$ aus einem Körper K, so liegt es nahe, die unbekannte Größe x zunächst als "variabel" anzusehen. Man betrachtet dann sozusagen die zugehörige Funktion $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, welche einem Element x den Funktionswert $f(x)$ zuordnet, und bemüht sich darum, deren Nullstellen zu bestimmen. Dabei muss man streng genommen natürlich den Definitionsbereich festlegen, in dem x variieren darf, beispielsweise K selbst oder für $K = \mathbb{Q}$ auch die reellen oder die komplexen Zahlen. Man nennt $f(x)$ eine *polynomiale Funktion* in x oder in nicht ganz korrekter Sprechweise auch ein *Polynom* in x.

Das Auffinden eines geeigneten Definitionsbereiches, der groß genug ist, um "alle" Nullstellen von f zu enthalten, ist jedoch ein grundsätzliches Problem. Aus historischer Sicht ist an dieser Stelle der Fundamentalsatz der Algebra von entscheidender Bedeutung. Er besagt nämlich für $K \subset \mathbb{C}$, dass alle Lösungen

von $(*)$ komplexe Zahlen sind. Es ist daher angemessen, $f(x)$ in diesem Falle als polynomiale Funktion auf $\mathbb{C}$ zu interpretieren. Probleme anderer Art ergeben sich, wenn man algebraische Gleichungen mit Koeffizienten aus einem endlichen Körper $\mathbb{F}$ betrachten möchte; vgl. 2.3/6 oder Abschnitt 3.8 zur Definition solcher Körper. Besteht $\mathbb{F}$ etwa aus den Elementen $x_1, \ldots, x_q$, so ist

$$g(x) = \prod_{j=1}^{q}(x - x_j) = x^q + \ldots + (-1)^q x_1 \ldots x_q$$

eine polynomiale Funktion, die auf ganz $\mathbb{F}$ verschwindet, obwohl ihre "Koeffizienten" nicht alle Null sind. Hieraus folgt, dass man je nach betrachtetem Definitionsbereich von der polynomialen Funktion $f(x)$, die einer algebraischen Gleichung $(*)$ zugeordnet ist, nicht unbedingt auf die Koeffizienten der Gleichung $(*)$ zurückschließen kann.

Um solche Schwierigkeiten auszuräumen, rückt man von der Vorstellung ab, ein Polynom sei eine *Funktion* auf einem bestimmten Definitionsbereich und versucht, zwei Gesichtspunkte zu realisieren. Zum einen möchte man, dass Polynome in umkehrbar eindeutiger Weise durch ihre "Koeffizienten" charakterisiert sind. Daneben soll aber auch der Funktionscharakter von Polynomen erhalten bleiben, und zwar in der Weise, dass man in Polynome jeweils Elemente aus beliebigen Körpern (oder Ringen), die den gegebenen Koeffizientenbereich erweitern, einsetzen kann. Dies erreicht man, indem man ein Polynom mit Koeffizienten $a_0, \ldots, a_n$ als formale Summe $f = \sum_{j=0}^{n} a_j X^j$ erklärt, was letztendlich bedeutet, dass man unter f lediglich die Folge der Koeffizienten $a_0, \ldots, a_n$ zu verstehen hat. Setzt man den Koeffizientenbereich K als Körper (oder auch als Ring) voraus, so kann man in gewohnter Weise Polynome addieren und multiplizieren, indem man die üblichen Rechenregeln formal anwendet. Auf diese Weise bilden die Polynome mit Koeffizienten aus K einen Ring $K[X]$. Zudem kann man Elemente x aus beliebigen Erweiterungskörpern (oder Erweiterungsringen) $K' \supset K$ in Polynome $f \in K[X]$ einsetzen; man ersetze nämlich die Variable X jeweils durch x und betrachte den resultierenden Ausdruck $f(x)$ als Element in K'. Insbesondere können wir von den Nullstellen von f in K' reden. Wir werden diesen Formalismus für Polynome einer Variablen in 2.1 und für Polynome mehrerer Variablen in 2.5 genauer studieren.

Das Problem der Lösung algebraischer Gleichungen mit Koeffizienten aus einem Körper K formuliert sich somit in etwas präziserer Form als Problem, für normierte Polynome mit Koeffizienten in K, also für Polynome des Typs $f = X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$, die Nullstellen in geeigneten Erweiterungskörpern K' von K zu finden. Bevor man mit der eigentlichen Arbeit hierzu beginnt, ist noch eine nunmehr triviale Bemerkung angebracht: Lässt sich das Polynom f in $K[X]$ als Produkt zweier Polynome $g, h \in K[X]$ schreiben, also $f = gh$, so genügt es zur Bestimmung der Nullstellen von f, die Nullstellen von g und h separat zu bestimmen. Für $x \in K'$ gilt nämlich $f(x) = (gh)(x) = g(x)h(x)$, wie man ohne Schwierigkeiten verifiziert. Da diese Gleichung in einem Körper zu lesen ist, verschwindet f genau dann in x, wenn g oder h dort verschwinden. Man sollte also zur Vereinfachung des Problems die

algebraische Gleichung $f(x) = 0$ zu Gleichungen niedrigeren Grades reduzieren, indem man f in $K[X]$ als Produkt normierter Faktoren niedrigeren Grades schreibt. Ist dies nicht mehr möglich, so nennt man f bzw. die algebraische Gleichung $f(x) = 0$ *irreduzibel*.

Diese Überlegungen zeigen insbesondere, dass man Faktorisierungen von Polynomen studieren muss. Wir werden dies in 2.4 tun. Ausgehend von der Tatsache, dass man durch Polynome mit Rest dividieren kann, werden wir zeigen, dass in $K[X]$ in gleicher Weise wie im Ring $\mathbb{Z}$ der ganzen Zahlen der Satz von der eindeutigen Primfaktorzerlegung gilt. Jedes normierte Polynom lässt sich somit in eindeutiger Weise als Produkt normierter irreduzibler Polynome schreiben. Weitere Überlegungen in 2.7 und 2.8 beschäftigen sich im Anschluss hieran mit Kriterien der Irreduzibilität, also mit der Frage, wie man entscheiden kann, ob ein gegebenes Polynom $f \in K[X]$ irreduzibel ist oder nicht.

Das Studium von Faktorzerlegungen im Polynomring $K[X]$ ist aber auch noch vor einem anderen Hintergrund von großem Interesse. Um dies näher zu erläutern, gehen wir kurz auf den Begriff des *Ideals* eines Rings ein, der mit zu den Grundlagen über Ringe gehört und in 2.2 behandelt wird. Ein Ideal $\mathfrak{a}$ eines Ringes R ist eine additive Untergruppe von R, so dass aus $r \in R$, $a \in \mathfrak{a}$ stets $ra \in \mathfrak{a}$ folgt. Ideale verhalten sich in vielerlei Hinsicht wie Normalteiler bei Gruppen. Insbesondere kann man den Restklassenring $R/\mathfrak{a}$ eines Ringes R nach einem Ideal $\mathfrak{a} \subset R$ bilden, den Homomorphiesatz beweisen usw.; vgl. 2.3. Die Einführung von Idealen erfolgte gegen Ende des 19. Jahrhunderts im Zusammenhang mit Versuchen, den Satz über die eindeutige Primfaktorzerlegung in Ringen ganzer algebraischer Zahlen zu beweisen. Als man eingesehen hatte, dass dieser Satz in solchen Ringen nicht uneingeschränkt gültig ist, hatte man sich eine gewisse Zeit mit Zerlegungen in so genannte *ideale Zahlen* behelfen wollen. Doch Dedekind bemerkte schließlich, dass man nicht einzelne Elemente faktorisieren sollte, sondern gewisse Teilmengen eines Ringes, die er Ideale nannte. So bewies Dedekind 1894 den Satz über die eindeutige Primfaktorzerlegung für Ideale in Ringen ganzer algebraischer Zahlen. Heute bezeichnet man Ringe ohne Nullteiler, in denen dieser Satz gilt, als *Dedekind-Ringe*.

Für uns ist wichtig, dass der Polynomring $K[X]$ über einem Körper K ein *Hauptidealring* ist, d. h. dass jedes Ideal $\mathfrak{a} \subset K[X]$ von der Form (f) ist, also von einem einzigen Element $f \in K[X]$ erzeugt wird. Dieses Resultat beweisen wir in 2.4/3 und zeigen dann, dass in jedem Hauptidealring der Satz von der eindeutigen Primfaktorzerlegung gilt. Untersuchungen dieser Art führen in direkter Weise zu dem Verfahren von Kronecker, welches wir allerdings erst in 3.4/1 genauer besprechen werden. Das Verfahren gestattet es in einfacher Weise, für eine irreduzible algebraische Gleichung $f(x) = 0$ mit Koeffizienten aus einem Körper K einen Erweiterungskörper K' anzugeben, der eine Lösung dieser Gleichung enthält. Man setze nämlich $K' = K[X]/(f)$, wobei die Restklasse $\overline{X}$ zu $X \in K[X]$ die gewünschte Lösung ist. Wenn auch dieses Verfahren noch keinen Aufschluss über die genauere Struktur des Körpers K' gibt, etwa im Hinblick auf eine Auflösung durch Radikale, so liefert es doch einen wertvollen Beitrag zur Frage der Existenz von Lösungen.

Zur Illustration des Rechnens in Hauptidealringen gehen wir zum Schluss des Kapitels in 2.9 noch auf die so genannte Elementarteilertheorie ein, ein Thema, das im Grunde genommen der Linearen Algebra zuzuordnen ist. Als Verallgemeinerung von Vektorräumen über Körpern studieren wir dort "Vektorräume" oder, wie man sagt, *Moduln* über Hauptidealringen.

2.1 Ringe, Polynomringe einer Variablen

Definition 1. *Ein* Ring (mit Eins) *ist eine Menge R mit zwei inneren Verknüpfungen, geschrieben als Addition "+" und Multiplikation "$\cdot$", so dass folgende Bedingungen erfüllt sind*:

(i) *R ist eine kommutative Gruppe bezüglich der Addition.*

(ii) *R ist ein Monoid bezüglich der Multiplikation, d. h. die Multiplikation ist assoziativ, und es existiert in R ein Einselement bezüglich der Multiplikation.*

(iii) *Es gelten die Distributivgesetze, d. h.*

$$(a+b)\cdot c = a\cdot c + b\cdot c, \qquad c\cdot(a+b) = c\cdot a + c\cdot b, \qquad \textit{für } a,b,c \in R.$$

R heißt kommutativ, *falls die Multiplikation kommutativ ist.*[1]

Bei den Distributivgesetzen (iii) haben wir auf der rechten Seite der Gleichungen jeweils auf eine spezielle Klammerung verzichtet. Man vereinbart nämlich, dass wie beim Rechnen mit gewöhnlichen Zahlen das Multiplikationszeichen stärker bindet als das Additionszeichen. Das Nullelement der Addition wird bei Ringen stets mit 0 bezeichnet, das Einselement der Multiplikation mit 1. Dabei ist auch $1 = 0$ zugelassen. Dies ist jedoch nur im Nullring möglich, der lediglich aus dem Nullelement 0 besteht. Man bezeichnet den Nullring meist ebenfalls mit 0, wobei man natürlich streng genommen zwischen 0 als Element und 0 als Ring zu unterscheiden hat. Für das Rechnen in Ringen gelten ähnliche Regeln wie für das Rechnen mit gewöhnlichen Zahlen, z. B.

$$0\cdot a = 0 = a\cdot 0, \qquad (-a)\cdot b = -(ab) = a\cdot(-b), \qquad \text{für } a,b \in R.$$

Man beachte aber, dass etwa aus $ab = ac$ bzw. $a\cdot(b-c) = 0$ (wobei $a \neq 0$) nicht automatisch $b = c$ folgt. Auf letztere Gleichung kann man im Allgemeinen nur in Integritätsringen schließen (siehe weiter unten) oder dann, wenn es zu a ein inverses Element bezüglich der Multiplikation gibt. Bei der Anwendung von Kürzungsregeln in allgemeinen Ringen ist daher Vorsicht geboten.

Ist R ein Ring und $S \subset R$ eine Teilmenge, so nennt man S einen *Unterring* von R, wenn S bezüglich der Addition eine Untergruppe sowie bezüglich der Multiplikation ein Untermonoid von R ist. Insbesondere ist S mit den von R induzierten Verknüpfungen selbst wieder ein Ring. Man nennt das Paar $S \subset R$ auch eine *Ringerweiterung*.

[1] Wir gehen in diesem Abschnitt zwar auf einige Notationen und Beispiele für nichtkommutative Ringe ein, werden ansonsten aber, wenn nichts anderes gesagt ist, unter einem Ring stets einen *kommutativen* Ring verstehen.

Für einen Ring R bezeichnet man mit

$$R^* = \{a \in R\,;\ \text{es existiert } b \in R \text{ mit } ab = ba = 1\}$$

die Menge der multiplikativ invertierbaren Elemente oder *Einheiten* von R. Man prüft leicht nach, dass R^* eine Gruppe bezüglich der Multiplikation ist. Es heißt R *Schiefkörper*, wenn $R \neq 0$ und $R^* = R - \{0\}$ gilt, d. h. wenn $1 \neq 0$ gilt und weiter jedes von 0 verschiedene Element aus R eine Einheit ist. Ist zusätzlich die Multiplikation von R kommutativ, so heißt R *Körper*. Ein Element a eines Ringes R heißt *Nullteiler*, wenn ein $b \in R - \{0\}$ mit $ab = 0$ oder $ba = 0$ existiert. In Körpern und Schiefkörpern gibt es außer der 0 keine weiteren Nullteiler. Wir nennen einen kommutativen Ring R *nullteilerfrei* oder *Integritätsring*, wenn $R \neq 0$ ist und R nur 0 als Nullteiler besitzt. Im Folgenden seien einige Beispiele für Ringe angeführt.

(1) $\mathbb{Z}$ ist ein Integritätsring, dessen Einheitengruppe aus den Elementen 1 und -1 besteht.

(2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ bilden Körper, die Hamiltonschen Quaternionen $\mathbb{H}$ einen Schiefkörper. Der Vollständigkeit halber sei hier an die Konstruktion von $\mathbb{H}$ erinnert. Man gehe aus von einem 4-dimensionalen $\mathbb{R}$-Vektorraum V mit Basis e, i, j, k. Sodann setze man

$$\begin{gathered} e^2 = e, \quad ei = ie = i, \quad ej = je = j, \quad ek = ke = k, \\ i^2 = j^2 = k^2 = -e, \\ ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j, \end{gathered}$$

und erkläre das Produkt beliebiger Elemente aus V durch $\mathbb{R}$-lineare Ausdehnung. Mit dieser Multiplikation sowie mit der Vektorraumaddition ist V ein (nicht-kommutativer) Ring $\mathbb{H}$, ja sogar ein Schiefkörper, mit e als Einselement. Indem man den Körper $\mathbb{R}$ der reellen Zahlen mit $\mathbb{R}e$ identifiziert, kann man $\mathbb{R}$ als Teilkörper von $\mathbb{H}$ auffassen, d. h. als Unterring, der ein Körper ist. In ähnlicher Weise lässt sich auch $\mathbb{C}$ als Teilkörper von $\mathbb{H}$ deuten.

(3) Es sei K ein Körper. Dann ist $R = K^{n\times n}$, die Menge der $(n\times n)$-Matrizen mit Koeffizienten in K, unter der gewöhnlichen Addition und Multiplikation von Matrizen ein Ring mit Einheitengruppe

$$R^* = \{A \in K^{n\times n}\,;\ \det A \neq 0\}.$$

R ist für $n \geq 2$ nicht kommutativ und besitzt in diesem Falle auch von Null verschiedene Nullteiler. Etwas allgemeiner können wir sagen, dass die Menge der Endomorphismen eines Vektorraumes V (oder auch einer abelschen Gruppe G) einen Ring bildet. Dabei ist die Addition von Endomorphismen mit Hilfe der Addition auf V bzw. G definiert, die Multiplikation als Komposition von Endomorphismen.

(4) Sei X eine Menge und R ein Ring. Dann ist R^X, die Menge der R-wertigen Funktionen auf X, ein Ring, wenn man für $f, g \in R^X$ setzt:

$$f+g\colon X \longrightarrow R, \qquad x \longmapsto f(x)+g(x),$$
$$f\cdot g\colon X \longrightarrow R, \qquad x \longmapsto f(x)\cdot g(x).$$

Gilt speziell $X = \{1,\dots,n\} \subset \mathbb{N}$, so ist R^X mit dem n-fachen kartesischen Produkt $R^n = R \times \ldots \times R$ zu identifizieren, wobei die Ringstruktur von R^n durch die Formeln

$$(*) \qquad \begin{aligned}(x_1,\dots,x_n)+(y_1,\dots,y_n) &= (x_1+y_1,\dots,x_n+y_n),\\ (x_1,\dots,x_n)\cdot(y_1,\dots,y_n) &= (x_1\cdot y_1,\dots,x_n\cdot y_n)\end{aligned}$$

beschrieben wird. Null- bzw. Einselement werden gegeben durch die Elemente $0 = (0,\dots,0)$ bzw. $1 = (1,\dots,1)$. Die Gleichung $(1,0,\dots,0)\cdot(0,1,\dots,1) = 0$ zeigt, dass R^n für $n \geq 2$ im Allgemeinen nicht-triviale Nullteiler besitzt, auch wenn R selbst ein Integritätsring ist. Man nennt R^n das n-fache *ringtheoretische Produkt* von R mit sich selbst. Allgemeiner kann das ringtheoretische Produkt

$$P = \prod_{x\in X} R_x$$

einer Familie von Ringen $(R_x)_{x\in X}$ gebildet werden. Addition und Multiplikation auf P werden analog zu den Formeln $(*)$ komponentenweise definiert. Sind die R_x Exemplare ein und desselben Rings R, so stimmen die Ringe $\prod_{x\in X} R_x$ und R^X in natürlicher Weise überein.

Von nun an wollen wir uns auf kommutative Ringe beschränken. Wir werden daher unter einem *Ring*, wenn nichts anderes gesagt ist, stets einen *kommutativen Ring* verstehen. Sei im Folgenden R ein solcher Ring. Als wichtiges Beispiel einer Ringerweiterung wollen wir den *Polynomring* $R[X]$ aller Polynome einer Variablen X über R erklären. Wir setzen $R[X] := R^{(\mathbb{N})}$, wobei diese Gleichung zunächst nur im Sinne von Mengen gemeint ist; $R^{(\mathbb{N})}$ bezeichne wie gewohnt die Menge aller Abbildungen $f : \mathbb{N} \longrightarrow R$, für die $f(i) = 0$ für fast alle $i \in \mathbb{N}$ gilt. Indem wir eine Abbildung $f : \mathbb{N} \longrightarrow R$ mit der zugehörigen Folge $(f(i))_{i\in\mathbb{N}}$ der Bilder in R identifizieren, können wir

$$R^{(\mathbb{N})} = \{(a_i)_{i\in\mathbb{N}}\,;\, a_i \in R,\ a_i = 0 \text{ für fast alle } i \in \mathbb{N}\}$$

schreiben. Um eine Ringstruktur auf $R^{(\mathbb{N})}$ zu erhalten, definieren wir die Addition wie im obigen Beispiel (4) als komponentenweise Addition bzw. als übliche Addition von Abbildungen unter Benutzung der Addition auf R, d. h.

$$(a_i)+(b_i) := (a_i+b_i).$$

Im Gegensatz hierzu wird die Multiplikation nicht komponentenweise erklärt; wir verwenden eine Konstruktion, wie sie auch der Multiplikation polynomialer Funktionen zugrundeliegt:

$$(a_i)\cdot(b_i) := (c_i),$$

wobei

$$c_i := \sum_{\mu+\nu=i} a_\mu b_\nu.$$

Man kann nun nachprüfen, dass $R^{(\mathbb{N})}$ mit den genannten Verknüpfungen einen Ring bildet; das Nullelement wird gegeben durch die Folge $(0,0,0,\ldots)$, das Einselement durch die Folge $(1,0,0,\ldots)$. Den so gewonnenen Ring bezeichnet man mit $R[X]$ und nennt ihn den *Ring der Polynome in einer Variablen X über R*. Etwas plausibler wird diese Definition, wenn man für Elemente in $R[X]$ die übliche Polynomschreibweise verwendet; man schreibt Elemente $(a_i) \in R[X]$ nämlich in der Form

$$\sum_{i\in\mathbb{N}} a_i X^i \qquad \text{oder} \qquad \sum_{i=0}^{n} a_i X^i,$$

wobei n so groß gewählt ist, dass $a_i = 0$ für $i > n$ gilt. Die "Variable" X, deren Bedeutung wir sogleich noch genauer erklären werden, ist dabei zu interpretieren als die Folge $(0,1,0,0,\ldots)$. In der Polynomschreibweise werden Addition und Multiplikation in $R[X]$ wie gewohnt gegeben durch die Formeln

$$\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i,$$
$$\sum_i a_i X^i \cdot \sum_i b_i X^i = \sum_i \Big(\sum_{\mu+\nu=i} a_\mu \cdot b_\nu \Big) X^i.$$

Um R als Unterring von $R[X]$ aufzufassen, ist es üblich, Elemente aus R als konstante Polynome in $R[X]$ zu interpretieren, also R mit seinem Bild unter der Abbildung $R \hookrightarrow R[X]$, $a \longmapsto aX^0$, zu identifizieren. Dies ist erlaubt, da diese injektive Abbildung die Ringstrukturen auf R und $R[X]$ respektiert, also ein Homomorphismus ist, wie wir sagen werden.

Ist nun $R \subset R'$ eine Ringerweiterung und $f = \sum a_i X^i$ ein Polynom in $R[X]$, so kann man beliebige Elemente $x \in R'$ für die "Variable" X einsetzen und somit den Wert $f(x) = \sum a_i x^i$ von f in x berechnen. Es gibt f daher Anlass zu einer wohldefinierten Abbildung $R' \longrightarrow R'$, $x \longmapsto f(x)$, wobei für zwei Polynome $f, g \in R[X]$ stets

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

gilt. Man bemerke dabei, dass für die rechte Gleichung die Kommutativität der Multiplikation in R' benutzt wird bzw., was ausreicht, die Vertauschbarkeitsrelation $ax = xa$ für $a \in R$, $x \in R'$. Wir rechnen daher im Polynomring $R[X]$ mit der "Variablen" X sozusagen wie mit einer universell variierbaren Größe, wobei Gleichungen in $R[X]$ wiederum in Gleichungen übergehen, wenn man für X Einsetzungen im gerade beschriebenen Sinne vornimmt.

Für ein Polynom $f = \sum a_i X^i \in R[X]$ bezeichnet man den i-ten Koeffizienten a_i jeweils als den *Koeffizienten vom Grad i* von f. Weiter definiert man den *Grad* von f durch

$$\operatorname{grad} f := \max\{i\,;\, a_i \neq 0\};$$

dem Nullpolynom 0 wird der Grad $-\infty$ zugeordnet. Im Falle $\operatorname{grad} f = n \geq 0$ heißt a_n der höchste Koeffizient oder der Leitkoeffizient von f. Ist dieser 1, so sagt man, f sei *normiert*. Jedes Polynom $f \in R[X] - \{0\}$, dessen höchster Koeffizient a_n eine Einheit ist, lässt sich durch Multiplikation mit a_n^{-1} normieren.

Bemerkung 2. *Es sei $R[X]$ der Polynomring einer Variablen X über einem Ring R. Für Polynome $f, g \in R[X]$ gilt dann*

$$\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$$
$$\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g,$$

wobei man sogar $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$ hat, sofern R ein Integritätsring ist.

Beweis. Die Behauptung ist unmittelbar zu verifizieren, falls f oder g das Nullpolynom ist. Gelte daher $m = \operatorname{grad} f \geq 0$ sowie $n = \operatorname{grad} g \geq 0$, etwa $f = \sum a_i X^i$, $g = \sum b_i X^i$. Dann folgt $a_i + b_i = 0$ für $i > \max(m, n)$, also $\operatorname{grad}(f+g) \leq \max(m, n)$. In ähnlicher Weise ergibt sich $\sum_{\mu+\nu=i} a_\mu b_\nu = 0$ für $i > m + n$ und somit $\operatorname{grad}(f \cdot g) \leq m + n$. Ist jedoch R ein Integritätsring, so schließt man aus $\operatorname{grad} f = m$, $\operatorname{grad} g = n$, dass die Koeffizienten a_m, b_n nicht verschwinden und somit, dass $\sum_{\mu+\nu=m+n} a_\mu b_\nu = a_m b_n$ als Koeffizient vom Grad $m + n$ in $f \cdot g$ nicht verschwindet. Folglich gilt $\operatorname{grad}(f \cdot g) = m + n$. □

Es gibt eine ganze Reihe von Eigenschaften, die sich von einem Ring R auf den Polynomring $R[X]$ vererben. Als einfaches Beispiel behandeln wir die Nullteilerfreiheit.

Bemerkung 3. *Es sei R ein Integritätsring. Dann ist auch der Polynomring $R[X]$ ein Integritätsring. Weiter gilt $(R[X])^* = R^*$.*

Beweis. Man benutze die Formel $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$ aus Bemerkung 2. □

Wir wollen schließlich noch zeigen, dass in Polynomringen eine *Division mit Rest* möglich ist, ähnlich wie im Ring $\mathbb{Z}$ der ganzen Zahlen. Dieses Hilfsmittel wird in 2.4 benutzt, um zu zeigen, dass in Polynomringen über Körpern der Satz von der eindeutigen Primfaktorzerlegung gilt.

Satz 4. *Es sei R ein Ring und $g = \sum_{i=0}^{d} a_i X^i \in R[X]$ ein Polynom, dessen höchster Koeffizient a_d eine Einheit in R ist. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit*

$$f = qg + r, \qquad \operatorname{grad} r < d.$$

Beweis. Wir bemerken zunächst, dass stets $\operatorname{grad}(qg) = \operatorname{grad} q + \operatorname{grad} g$ für Polynome $q \in R[X]$ gilt, auch wenn R kein Integritätsring ist. Der höchste Koeffi-

zient a_d von g ist nämlich eine Einheit. Ist daher q vom Grad $n \geq 0$ mit höchstem Koeffizienten c_n, so gilt $c_n a_d \neq 0$. Dies ist aber der höchste Koeffizient von qg, so dass $\operatorname{grad}(qg) = n + d$ folgt.

Nun zur Eindeutigkeit der Division mit Rest. Hat f zwei Darstellungen der gewünschten Art, etwa $f = qg + r = q'g + r'$, so folgt $0 = (q - q')g + (r - r')$ sowie nach vorstehender Überlegung

$$\operatorname{grad}(q - q') + \operatorname{grad} g = \operatorname{grad}(r - r').$$

Da r und r' vom Grad $< d$ sind, gilt dasselbe auch für $r - r'$, und man erhält $\operatorname{grad}(q - q') + \operatorname{grad} g < d$. Dies kann aber wegen $\operatorname{grad} g = d$ nur für $q = q'$ richtig sein. Hieraus ergibt sich insbesondere $r = r'$ und somit die Eindeutigkeit der Division mit Rest.

Um die Existenz der Division mit Rest zu zeigen, schließen wir mit Induktion nach $n = \operatorname{grad} f$. Für $\operatorname{grad} f < d$ setze man $q = 0$ und $r = f$. Gilt andererseits $f = \sum_{i=0}^{n} c_i X^i$ mit $c_n \neq 0$ und $n \geq d$, so ist

$$f_1 = f - c_n a_d^{-1} X^{n-d} g$$

ein Polynom mit $\operatorname{grad} f_1 < n$. Dieses besitzt nach Induktionsvoraussetzung eine Zerlegung $f_1 = q_1 g + r_1$ mit Polynomen $q_1, r_1 \in R[X]$, $\operatorname{grad} r_1 < d$. Dann folgt aber mit

$$f = (q_1 + c_n a_d^{-1} X^{n-d}) g + r_1$$

die gewünschte Zerlegung für f. □

Die gerade gegebene Argumentation kann insbesondere als konstruktives Verfahren benutzt werden, um die Division mit Rest im Polynomring $R[X]$ in expliziter Weise durchzuführen, ähnlich wie dies auch im Ring $\mathbb{Z}$ der ganzen Zahlen geschieht. Als Beispiel betrachte man die Polynome

$$f = X^5 + 3X^4 + X^3 - 6X^2 - X + 1, \qquad g = X^3 + 2X^2 + X - 1$$

aus $\mathbb{Z}[X]$:

$$\begin{array}{rrrrrl}
(X^5 & +3X^4 & +X^3 & -6X^2 & -X & +1) : (X^3 + 2X^2 + X - 1) = X^2 + X - 2 \\
\cline{1-4}
X^5 & +2X^4 & +X^3 & -X^2 & & \\
\cline{1-4}
 & X^4 & & -5X^2 & -X & \\
 & X^4 & +2X^3 & +X^2 & -X & \\
\cline{2-5}
 & & -2X^3 & -6X^2 & & +1 \\
 & & -2X^3 & -4X^2 & -2X & +2 \\
\cline{3-6}
 & & & -2X^2 & +2X & -1
\end{array}$$

Im ersten Schritt subtrahieren wir $X^2 g$ von f, im zweiten dann Xg von $f - X^2 g$ und im dritten $-2g$ von $f - X^2 g - Xg$. Es bleibt $-2X^2 + 2X - 1$ als Rest, so dass wir die Gleichung

$$f = (X^2 + X - 2)g + (-2X^2 + 2X - 1)$$

erhalten.

Abschließend sei angemerkt, dass man die Konstruktion des Polynomrings $R[X]$ in verschiedener Hinsicht verallgemeinern kann. So werden wir beispielsweise in 2.5 Polynomringe in mehreren Variablen definieren. Man kann aber auch von Beginn an die Menge $R^{(\mathbb{N})}$ durch $R^{\mathbb{N}}$ ersetzen, also durch die Menge *aller* Abbildungen von $\mathbb{N}$ nach R. Verfährt man ansonsten wie bei der Konstruktion des Polynomrings $R[X]$, so erhält man den Ring $R[\![X]\!]$ der *formalen Potenzreihen* in einer Variablen X über R. Seine Elemente lassen sich als *unendliche* Reihen $\sum_{i=0}^{\infty} a_i X^i$ darstellen.

Aufgaben

1. *Man verifiziere, dass für Elemente a, b eines Ringes R stets die Relationen $0 \cdot a = 0$ und $(-a) \cdot b = -(a \cdot b)$ gelten.*
2. *Wir haben den Polynomring $R[X]$ nur für einen kommutativen Ring R definiert. Man überlege, inwieweit es sinnvoll ist, Polynomringe auch im Rahmen nicht notwendig kommutativer Ringe zu betrachten.*
3. Man führe die in Satz 4 beschriebene Division mit Rest im Polynomring $\mathbb{Z}[X]$ in folgenden Fällen explizit durch:
   (i) $f = 3X^5 + 2X^4 - X^3 + 3X^2 - 4X + 7, \quad g = X^2 - 2X + 1.$
   (ii) $f = X^5 + X^4 - 5X^3 + 2X^2 + 2X - 1, \quad g = X^2 - 1.$
4. Sei K ein Körper und $g \in K[X]$ ein Polynom einer Variablen vom Grad $d > 0$. Man beweise die Existenz der so genannten *g-adischen Entwicklung*: Zu $f \in K[X]$ gibt es eindeutig bestimmte Polynome $a_0, a_1, \ldots \in K[X]$ vom Grad $< d$, $a_i = 0$ für fast alle i, mit $f = \sum_i a_i g^i$.
5. Es sei R ein Ring, der ein *nilpotentes* Element $a \neq 0$ enthalte; nilpotent bedeutet, dass es ein $n \in \mathbb{N}$ mit $a^n = 0$ gibt. Man zeige, dass die Einheitengruppe R^* eine echte Untergruppe der Einheitengruppe $(R[X])^*$ ist.
6. Man bestimme den kleinsten Unterring von $\mathbb{R}$, welcher $\mathbb{Q}$ und $\sqrt{2}$ enthält, und zeige, dass dieser bereits ein Körper ist.
7. Es sei R ein Ring. Man beweise, dass eine formale Potenzreihe $\sum a_i X^i \in R[\![X]\!]$ genau dann eine Einheit ist, wenn a_0 eine Einheit in R ist.
8. Man beweise, dass die Quaternionen $\mathbb{H}$ aus Beispiel (2) einen Schiefkörper bilden.

2.2 Ideale

Ideale sind für Ringe von ähnlich fundamentaler Bedeutung wie Normalteiler für Gruppen. Ein Normalteiler einer Gruppe ist zugleich auch eine Untergruppe. Dagegen ist ein Ideal eines Ringes im Allgemeinen kein Unterring, denn Ideale müssen nicht unbedingt das Einselement der Multiplikation enthalten.

Definition 1. *Es sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt ein* Ideal *in R, wenn gilt*:

(i) $\mathfrak{a}$ *ist eine additive Untergruppe von R.*

(ii) $r \in R$, $a \in \mathfrak{a} \Longrightarrow ra \in \mathfrak{a}$.

Jeder Ring R enthält stets die so genannten *trivialen* Ideale, nämlich das *Nullideal* $\{0\}$, auch mit 0 bezeichnet, und das *Einheitsideal* R. Ist R ein Körper, so sind dies die einzigen Ideale in R. Ausgehend von beliebigen Idealen $\mathfrak{a}, \mathfrak{b} \subset R$ kann man die folgenden Ideale bilden:

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &:= \{a + b\,;\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}, \\ \mathfrak{a} \cdot \mathfrak{b} &:= \{\sum_{i=1}^{<\infty} a_i b_i\,;\, a_i \in \mathfrak{a},\, b_i \in \mathfrak{b}\}, \\ \mathfrak{a} \cap \mathfrak{b} &:= \{x\,;\, x \in \mathfrak{a} \text{ und } x \in \mathfrak{b}\}. \end{aligned}$$

Es gilt stets $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Im Übrigen kann man in analoger Weise das Produkt von endlich vielen Idealen sowie Summe und Durchschnitt beliebig vieler Ideale bilden. Dabei besteht die Summe $\sum \mathfrak{a}_i$ einer Familie von Idealen $(\mathfrak{a}_i)_{i \in I}$ aus allen Elementen der Form $\sum a_i$ mit $a_i \in \mathfrak{a}_i$, wobei $a_i = 0$ für fast alle $i \in I$. Für $a \in R$ nennt man $Ra := \{ra\,;\, r \in R\}$ das *von a erzeugte Hauptideal*. Allgemeiner erklärt man für $a_1, \ldots, a_n \in R$ das von diesen Elementen *erzeugte Ideal* in R durch

$$(a_1, \ldots, a_n) := Ra_1 + \ldots + Ra_n = \{r_1 a_1 + \ldots + r_n a_n\,;\, r_1, \ldots, r_n \in R\}.$$

Es ist dies das kleinste Ideal in R, welches $a_1, \ldots, a_n$ enthält, und zwar in dem Sinne, dass jedes weitere Ideal in R, welches die Elemente $a_1, \ldots, a_n$ enthält, auch das Ideal $(a_1, \ldots, a_n)$ enthält. In analoger Weise kann man das von einer beliebigen Familie $(a_i)_{i \in I}$ von Elementen aus R erzeugte Ideal in R betrachten, nämlich das Ideal $\sum_{i \in I} Ra_i$.

Definition 2. *Es sei $\mathfrak{a}$ ein Ideal eines Ringes R. Eine Familie $(a_i)_{i \in I}$ von Elementen aus $\mathfrak{a}$ heißt ein* Erzeugendensystem *von $\mathfrak{a}$, wenn $\mathfrak{a} = \sum_{i \in I} Ra_i$ gilt, wenn also $\mathfrak{a}$ mit dem von der Familie $(a_i)_{i \in I}$ erzeugten Ideal übereinstimmt. Man nennt $\mathfrak{a}$* endlich erzeugt, *wenn $\mathfrak{a}$ ein endliches Erzeugendensystem besitzt. Weiter heißt $\mathfrak{a}$* Hauptideal, *wenn $\mathfrak{a}$ von einem einzigen Element erzeugt wird, wenn es also ein $a \in \mathfrak{a}$ mit $\mathfrak{a} = (a)$ gibt. Ist R Integritätsring und ist jedes Ideal in R Hauptideal, so nennt man R einen* Hauptidealring.

Die trivialen Ideale eines Ringes sind stets Hauptideale. Im Übrigen bilden die Untergruppen der Form $m\mathbb{Z} \subset \mathbb{Z}$ Hauptideale im Integritätsring $\mathbb{Z}$. Da dies gemäß 1.3/4 die einzigen Untergruppen von $\mathbb{Z}$ sind, kann es auch keine weiteren Ideale in $\mathbb{Z}$ geben. Insbesondere folgt:

Satz 3. *$\mathbb{Z}$ ist ein Hauptidealring.*

Erzeugende Elemente von Hauptidealen sind nicht eindeutig bestimmt; man kann sie zumindest durch Einheiten abändern. In Integritätsringen erhält man auf diese Weise aber bereits alle möglichen Erzeugenden eines Hauptideals:

Bemerkung 4. *In einem Integritätsring R stimmen zwei Hauptideale $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ genau dann überein, wenn es eine Einheit $c \in R^*$ mit $b = ca$ gibt.*

Beweis. Es gelte $\mathfrak{a} = \mathfrak{b}$, wobei wir ohne Einschränkung $\mathfrak{a} = \mathfrak{b} \neq 0$ annehmen dürfen. Dann hat man $b \in \mathfrak{a}$, also gibt es ein $c \in R$ mit $b = ca$. Ebenso gibt es wegen $a \in \mathfrak{b}$ ein $c' \in R$ mit $a = c'b$. Damit folgt $b = ca = cc'b$, bzw.

$$(1 - cc')b = 0.$$

Da nun R Integritätsring ist und b wegen $\mathfrak{b} \neq 0$ von Null verschieden sein muss, folgt $cc' = 1$, d. h. c ist eine Einheit. Die umgekehrte Implikation ist trivial. □

Wir nennen zwei Elemente a, b eines Ringes R (zueinander) *assoziiert*, wenn es eine Einheit $c \in R^*$ mit $b = ca$ gibt. Somit können wir sagen, dass in einem Integritätsring zwei Elemente genau dann dasselbe Hauptideal erzeugen, wenn sie assoziiert sind. In allgemeineren Ringen gilt diese Aussage nicht mehr, man vergleiche hierzu Aufgabe 7 in Abschnitt 2.3.

Wir wollen schließlich noch als Beispiel den Polynomring $\mathbb{Z}[X]$ betrachten. Das von X erzeugte Hauptideal beschreibt sich durch

$$(X) = \{\sum a_i X^i \in \mathbb{Z}[X] \,;\, a_0 = 0\},$$

das von 2 erzeugte Hauptideal durch

$$(2) = \{\sum a_i X^i \in \mathbb{Z}[X] \,;\, a_i \text{ ist gerade für alle } i\}.$$

Da es in $\mathbb{Z}[X]$ keine Nichteinheit gibt, welche sowohl 2 als auch X als Vielfaches besitzt, kann man leicht sehen, dass

$$(2, X) = \{\sum a_i X^i \in \mathbb{Z}[X] \,;\, a_0 \text{ ist gerade}\}$$

ein Ideal in $\mathbb{Z}[X]$ ist, welches kein Hauptideal darstellt. Insbesondere ist $\mathbb{Z}[X]$ kein Hauptidealring.

Aufgaben

1. *Es seien $\mathfrak{a} = (a_1, \ldots, a_m)$ und $\mathfrak{b} = (b_1, \ldots, b_n)$ Ideale in einem Ring R. Man gebe Erzeugendensysteme für die Ideale $\mathfrak{a} + \mathfrak{b}$ sowie $\mathfrak{a} \cdot \mathfrak{b}$ an und diskutiere auch das Ideal $\mathfrak{a} \cap \mathfrak{b}$.*

2. *Man überlege, unter welchen Bedingungen die Vereinigung zweier Ideale oder allgemeiner einer Familie von Idealen eines Ringes R wieder ein Ideal ist.*

3. *Es sei K ein Körper. Man betrachte $K^2 = K \times K$ als ringtheoretisches Produkt sowie auch als K-Vektorraum. Man vergleiche die Begriffe Unterring, Ideal und Untervektorraum am Beispiel dieses Ringes.*

4. Man berechne folgende Ideale in $\mathbb{Z}$, indem man ein erzeugendes Element angibt:

$$(2) + (3), \qquad (4) + (6), \qquad (2) \cap (3), \qquad (4) \cap (6).$$

5. Sei R ein Ring, X eine Menge und $Y \subset X$ eine Teilmenge. Man untersuche, welche der folgenden Teilmengen des Rings R^X der Abbildungen $X \longrightarrow R$ einen Unterring bzw. ein Ideal bilden:

$$M_1 = \{f \in R^X \,;\, f \text{ ist konstant auf } Y\},$$
$$M_2 = \{f \in R^X \,;\, f(Y) = 0\},$$
$$M_3 = \{f \in R^X \,;\, f(y) \neq 0 \text{ für alle } y \in Y\},$$
$$M_4 = \{f \in R^X \,;\, f(y) = 0 \text{ für fast alle } y \in Y\}.$$

   In welchen Fällen erhält man unter geeigneten Bedingungen an Y Hauptideale?

6. Sei R ein Ring. Man zeige, dass die Teilmenge

$$\{a \in R \,;\, \text{es existiert ein } n \in \mathbb{N} \text{ mit } a^n = 0\}$$

   ein Ideal in R definiert (das so genannte *Radikal* oder *Nilradikal* von R).

7. Sei K ein Körper. Man bestimme alle Ideale im Ring der formalen Potenzreihen $K[\![X]\!]$. (Man benutze Aufgabe 7 aus Abschnitt 2.1.)

2.3 Ringhomomorphismen, Faktorringe

Der Begriff des Homomorphismus wird in natürlicher Weise auch für Ringe erklärt.

Definition 1. *Es seien R und R' Ringe. Eine Abbildung $\varphi\colon R \longrightarrow R'$ heißt* Ringhomomorphismus, *wenn gilt*:

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ *für alle $a, b \in R$, d. h. φ ist ein Gruppenhomomorphismus bezüglich der Addition.*

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *für alle $a, b \in R$ und $\varphi(1) = 1$, d. h. φ ist ein Monoidhomomorphismus bezüglich der Multiplikation.*

Man verifiziert ohne Schwierigkeiten, dass die Komposition zweier Ringhomomorphismen wieder ein Ringhomomorphismus ist. Wie üblich heißt ein Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ ein *Isomorphismus*, wenn φ ein Inverses besitzt, d. h. wenn es einen Ringhomomorphismus $\psi\colon R' \longrightarrow R$ mit $\psi \circ \varphi = \mathrm{id}_R$ und $\varphi \circ \psi = \mathrm{id}_{R'}$ gibt. Äquivalent hierzu ist, dass der Homomorphismus φ bijektiv ist. Injektive (bzw. surjektive) Ringhomomorphismen $R \longrightarrow R'$ nennt man auch *Monomorphismen* (bzw. *Epimorphismen*). Ein *Endomorphismus* von R ist ein

Homomorphismus $R \longrightarrow R$ und ein *Automorphismus* von R ein Isomorphismus $R \longrightarrow R$.

Bemerkung 2. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus. Dann gilt*:
(i) $\ker\varphi = \{a \in R\,;\, \varphi(a) = 0\}$ *ist ein Ideal in R.*
(ii) $\operatorname{im}\varphi = \varphi(R)$ *ist ein Unterring von R'.*
(iii) *φ induziert einen Gruppenhomomorphismus $R^* \longrightarrow R'^*$ zwischen den Einheitengruppen von R und R'.*

Die Behauptungen sind unmittelbar nachzuprüfen. Man beachte dabei, dass das Bild eines Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ im Allgemeinen kein Ideal in R' ergibt. Handelt es sich bei R und R' um Körper, so spricht man auch von *Körperhomomorphismen*.

Bemerkung 3. *Es sei K ein Körper und R ein Ring, $R \neq 0$. Dann ist jeder Homomorphismus $\varphi\colon K \longrightarrow R$ injektiv. Insbesondere ist jeder Homomorphismus zwischen Körpern injektiv.*

Beweis. Es ist $\ker\varphi$ ein Ideal in K, sogar ein echtes Ideal, da $\varphi(1) = 1 \neq 0$ gilt. Somit folgt $\ker\varphi = 0$, da ein Körper außer dem Nullideal keine weiteren echten Ideale besitzt. □

Zu jedem Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \longrightarrow R$, nämlich die durch $n \longmapsto n \cdot 1$ definierte Abbildung. Dabei ist $n \cdot 1$ für $n \geq 0$ als n-fache Summe des Einselementes $1 \in R$ aufzufassen und entsprechend für $n < 0$ als $(-n)$-fache Summe von -1. Für eine Ringerweiterung $R \subset R'$ ist die Inklusionsabbildung $R \hookrightarrow R'$ ein (triviales) Beispiel eines Ringhomomorphismus. Weiter hat man in dieser Situation zu jedem $x \in R'$ einen so genannten *Einsetzungshomomorphismus*

$$R[X] \longrightarrow R', \qquad f = \sum a_i X^i \longmapsto f(x) = \sum a_i x^i,$$

der ein Ringhomomorphismus ist. Das Einsetzen von Elementen $x \in R'$ in Polynome $f, g \in R[X]$ hatten wir schon in 2.1 besprochen, ebenso die Verträglichkeiten $(f+g)(x) = f(x) + g(x)$ sowie $(f \cdot g)(x) = f(x) \cdot g(x)$, die für einen Ringhomomorphismus gefordert werden.

Es sei im Folgenden R ein Ring und $\mathfrak{a}$ ein Ideal in R. Wir wollen die Konstruktion der Faktorgruppe G/N einer Gruppe G nach einem Normalteiler N auf die Ringsituation übertragen und einen so genannten *Faktor-* oder *Restklassenring* $R/\mathfrak{a}$ konstruieren, zusammen mit einem surjektiven Ringhomomorphismus $\pi\colon R \longrightarrow R/\mathfrak{a}$, welcher $\ker\pi = \mathfrak{a}$ erfüllt. Zunächst können wir $R/\mathfrak{a}$ als abelsche Gruppe bilden, indem wir $\mathfrak{a}$ als Untergruppe (und damit als Normalteiler) der additiven Gruppe von R auffassen. Es besteht $R/\mathfrak{a}$ somit aus allen Restklassen der Form $x + \mathfrak{a}$ mit $x \in R$, wobei die Addition in $R/\mathfrak{a}$ durch die Formel

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$$

beschrieben wird. Dass diese Verknüpfung wohldefiniert ist und $R/\mathfrak{a}$ zu einer abelschen Gruppe macht, haben wir in 1.2 nachgewiesen. Wir führen nun in analoger Weise eine Multiplikation in $R/\mathfrak{a}$ ein, indem wir für Restklassen $x+\mathfrak{a}$, $y+\mathfrak{a}$ aus $R/\mathfrak{a}$ definieren:

$$(x+\mathfrak{a})\cdot(y+\mathfrak{a}) := (x\cdot y)+\mathfrak{a}.$$

Um die Wohldefiniertheit dieser Verknüpfung zu überprüfen, müssen wir zeigen, dass die Restklasse $(x\cdot y)+\mathfrak{a}$ nicht von der Wahl der Repräsentanten x, y zu den Restklassen $x+\mathfrak{a}$ und $y+\mathfrak{a}$ abhängt. Gilt etwa $x'+\mathfrak{a} = x+\mathfrak{a}$, also $x' = x+a$ mit $a\in\mathfrak{a}$, und entsprechend $y'+\mathfrak{a} = y+\mathfrak{a}$, also $y' = y+b$ mit $b\in\mathfrak{a}$, so hat man $x'y' = xy+ay'+xb\in(xy)+\mathfrak{a}$, d. h.

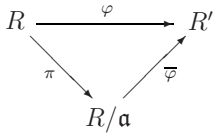
$$(xy)+\mathfrak{a} = (x'y')+\mathfrak{a}.$$

Folglich ist die Multiplikation in $R/\mathfrak{a}$ wohldefiniert, und es ist unmittelbar ersichtlich, dass die Ringeigenschaften sich von R auf $R/\mathfrak{a}$ übertragen. Im Übrigen ist die kanonische Projektion

$$\pi\colon R\longrightarrow R/\mathfrak{a},\qquad x\longmapsto x+\mathfrak{a},$$

ein Ringhomomorphismus mit $\ker\pi = \mathfrak{a}$, der wie in 1.2/6 eine universelle Eigenschaft erfüllt:

Satz 4. (Homomorphiesatz). *Sei $\varphi\colon R\longrightarrow R'$ ein Ringhomomorphismus und $\mathfrak{a}\subset R$ ein Ideal mit $\mathfrak{a}\subset\ker\varphi$. Dann existiert eindeutig ein Ringhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a}\longrightarrow R'$, so dass das Diagramm*



kommutiert. Es gilt

$$\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi,\qquad \ker\overline{\varphi} = \pi(\ker\varphi),\qquad \ker\varphi = \pi^{-1}(\ker\overline{\varphi}).$$

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $\mathfrak{a} = \ker\varphi$ gilt.

Korollar 5. *Ist $\varphi\colon R\longrightarrow R'$ ein surjektiver Ringhomomorphismus, so ist R' kanonisch isomorph zu $R/\ker\varphi$.*

Zum *Beweis von Satz* 4 wendet man 1.2/6 auf die additive Gruppe von R an. Sodann hat man nur noch nachzuprüfen, dass der nach 1.2/6 existierende Gruppenhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a}\longrightarrow R'$ bereits ein Ringhomomorphismus ist. Da $\overline{\varphi}$ charakterisiert ist durch die Gleichung

$$\overline{\varphi}(x+\mathfrak{a}) = \varphi(x),\qquad x\in R,$$

ist dies unmittelbar klar. □

Im Übrigen lassen sich die Isomorphiesätze 1.2/8 und 1.2/9, welche wir in Abschnitt 1.2 aus dem Homomorphiesatz 1.2/6 gefolgert hatten, ohne Schwierigkeiten von der Gruppensituation auf die hier betrachtete Ringsituation übertragen bzw. aus dem gerade bewiesenen Homomorphiesatz für Ringe herleiten; man ersetze den Begriff des Normalteilers jeweils durch den Begriff des Ideals in einem Ring.

Als natürliche Beispiele für Restklassenringe können wir die Ringe $\mathbb{Z}/m\mathbb{Z}$ betrachten, die wir in 1.3 lediglich als abelsche Gruppen aufgefasst hatten. Setzen wir $m > 0$ voraus, so ist also $\mathbb{Z}/m\mathbb{Z}$ ein Ring mit m Elementen.

Satz 6. *Für $m \in \mathbb{Z}$, $m > 0$, ist äquivalent*:

(i) *m ist eine Primzahl.*

(ii) *$\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring.*

(iii) *$\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.*

Beweis. Wir bezeichnen mit $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ die zu einem Element $x \in \mathbb{Z}$ gehörige Restklasse modulo $m\mathbb{Z}$. Sei zunächst Bedingung (i) gegeben, also m eine Primzahl. Dann ist $m > 1$ und folglich $\mathbb{Z}/m\mathbb{Z}$ nicht der Nullring. Gilt nun $\overline{a} \cdot \overline{b} = 0$ für zwei Zahlen $a, b \in \mathbb{Z}$, so hat man $ab \in m\mathbb{Z}$, und man sieht, etwa unter Benutzung der Primfaktorzerlegungen für a, b bzw. ab, dass m ein Teiler von a oder b ist. Also ergibt sich $a \in m\mathbb{Z}$ oder $b \in m\mathbb{Z}$, d. h. $\overline{a} = 0$ oder $\overline{b} = 0$, und es ist $\mathbb{Z}/m\mathbb{Z}$ Integritätsring, wie in (ii) gefordert.

Weiter folgt aus (ii), dass für jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z} - \{0\}$ die Abbildung

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}, \qquad \overline{x} \longmapsto \overline{a} \cdot \overline{x},$$

injektiv und somit wegen der Endlichkeit von $\mathbb{Z}/m\mathbb{Z}$ sogar bijektiv ist. Insbesondere ist das Einselement von $\mathbb{Z}/m\mathbb{Z}$ im Bild dieser Abbildung enthalten, so dass $\overline{a}$ jeweils ein inverses Element bezüglich der Multiplikation besitzt. Dies bedeutet aber, dass $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist, wie in (iii) gefordert.

Sei schließlich $\mathbb{Z}/m\mathbb{Z}$ wie in (iii) als Körper oder allgemeiner als nullteilerfrei angenommen. Insbesondere folgt dann $\mathbb{Z}/m\mathbb{Z} \neq 0$ und somit $m > 1$. Um zu zeigen, dass m eine Primzahl ist, betrachte man einen Teiler $d \in \mathbb{N}$ von m mit einer Gleichung $m = da$. Es folgt $\overline{d} \cdot \overline{a} = 0$, und die Nullteilerfreiheit von $\mathbb{Z}/m\mathbb{Z}$ ergibt $\overline{d} = 0$ oder $\overline{a} = 0$. Im ersten Fall ist m ein Teiler von d, d. h. $d = m$, und im zweiten Fall ist m ein Teiler von a, d. h. $a = m$ und somit $d = 1$. Also hat m höchstens sich selbst und 1 als Teiler und ist damit eine Primzahl. □

Für eine Primzahl p ist also $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen; man verwendet hierfür die Notation $\mathbb{F}_p$. Mit Teilbarkeitstheorie kann man allgemeiner zeigen, dass für ganze Zahlen $m > 1$ die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^*$ aus allen Restklassen $\overline{a}$, $a \in \mathbb{Z}$, besteht, für die a teilerfremd zu m ist. Als Nächstes wollen wir die Aussage von Satz 6 in einen etwas allgemeineren Zusammenhang stellen.

Definition 7. *Es sei R ein Ring.*

(i) *Ein Ideal $\mathfrak{p} \subset R$ heißt* prim *oder* Primideal, *wenn $\mathfrak{p}$ von R verschieden ist und wenn für $a, b \in R$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.*

(ii) *Ein Ideal $\mathfrak{m} \subset R$ heißt* maximal, *wenn $\mathfrak{m}$ von R verschieden ist und wenn gilt: Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a} \subset R$, so folgt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.*

Beispielsweise ist das Nullideal eines Ringes R genau dann ein Primideal, wenn R ein Integritätsring ist.

Satz 8. *Es sei R ein Ring.*

(i) *Ein Ideal $\mathfrak{p} \subset R$ ist genau dann ein Primideal, wenn $R/\mathfrak{p}$ ein Integritätsring ist.*

(ii) *Ein Ideal $\mathfrak{m} \subset R$ ist genau dann ein maximales Ideal, wenn $R/\mathfrak{m}$ ein Körper ist.*

Insbesondere ist jedes maximale Ideal ein Primideal.

Beweis. Zunächst überlegt man sich, dass $\mathfrak{p}$ genau dann ein echtes Ideal in R ist, wenn der Restklassenring $R/\mathfrak{p}$ nicht der Nullring ist, entsprechend für $\mathfrak{m}$. Aussage (i) ist dann leicht einzusehen. Bezeichnet man mit $\overline{a}, \overline{b} \in R/\mathfrak{p}$ die Restklassen zu Elementen $a, b \in R$, so ist

$$a \cdot b \in \mathfrak{p} \quad \Longrightarrow \quad a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

offenbar äquivalent zu

$$\overline{a} \cdot \overline{b} = 0 \quad \Longrightarrow \quad \overline{a} = 0 \text{ oder } \overline{b} = 0.$$

Weiter ist Aussage (ii) eine Konsequenz der beiden folgenden Lemmata:

Lemma 9. *Ein Ideal $\mathfrak{m} \subset R$ ist genau dann maximal, wenn das Nullideal $0 \subset R/\mathfrak{m}$ maximal ist.*

Lemma 10. *Das Nullideal $0 \subset R$ eines Ringes R ist genau dann maximal, wenn R ein Körper ist.*

Beweis von Lemma 9. Sei $\pi\colon R \longrightarrow R/\mathfrak{m}$ die kanonische Projektion. Man prüft leicht nach, dass die Zuordnungen

$$\begin{aligned} R \supset \quad \mathfrak{a} \quad &\longmapsto \pi(\mathfrak{a}) \subset R/\mathfrak{m}, \\ R \supset \pi^{-1}(\mathfrak{b}) &\longmapsto \quad \mathfrak{b} \quad \subset R/\mathfrak{m}, \end{aligned}$$

eine Bijektion definieren zwischen den Idealen $\mathfrak{a}$ von R mit $\mathfrak{m} \subset \mathfrak{a} \subset R$ und den Idealen $\mathfrak{b} \subset R/\mathfrak{m}$. Hieraus ist die behauptete Äquivalenz unmittelbar ersichtlich.

Alternativ kann man die Behauptung auch in expliziter Weise verifizieren. Zunächst sei daran erinnert, dass $\mathfrak{m}$ genau dann ein echtes Ideal in R ist, wenn der Restklassenring $R/\mathfrak{m}$ nicht der Nullring ist. Ist nun $\mathfrak{m}$ ein echtes Ideal in R, so ist $\mathfrak{m}$ genau dann maximal, wenn für $a \in R$–$\mathfrak{m}$ stets $\mathfrak{m} + Ra = R$ gilt, wenn es

also zu jedem solchen a Elemente $r \in R$ und $m \in \mathfrak{m}$ mit $ra + m = 1$ gibt. Unter Verwendung der Projektion $\pi\colon R \longrightarrow R/\mathfrak{m}$ sieht man, dass diese Bedingung genau dann erfüllt ist, wenn es zu $\overline{a} \in R/\mathfrak{m} - \{0\}$ stets ein Element $\overline{r} \in R/\mathfrak{m}$ gibt mit $\overline{r} \cdot \overline{a} = 1$, also genau dann, wenn das Nullideal in $R/\mathfrak{m}$ maximal ist. □

Beweis von Lemma 10. Sei $0 \subset R$ maximal und $a \in R$ von 0 verschieden. Dann folgt $aR = R$, und es existiert ein $b \in R$ mit $ab = 1$. Somit hat man $R^* = R - \{0\}$, d. h. R ist ein Körper. Umgekehrt ist unmittelbar klar, dass das Nullideal in einem Körper maximal ist. □

Die Sätze 6 und 8 geben eine vollständige Übersicht über Primideale und maximale Ideale in $\mathbb{Z}$:

Korollar 11. *Ein Ideal in $\mathbb{Z}$ ist genau dann prim, wenn es von der Form $p\mathbb{Z}$ mit einer Primzahl p oder mit $p = 0$ ist. Ein Ideal in $\mathbb{Z}$ ist genau dann maximal, wenn es ein von Null verschiedenes Primideal ist.*

Man muss lediglich benutzen, dass $\mathbb{Z}$ nach 2.2/3 Hauptidealring ist und dass das Nullideal in einem Integritätsring stets prim ist. Zum Schluss dieses Abschnitts wollen wir noch den so genannten *Chinesischen Restsatz* beweisen.

Satz 12. *Sei R ein Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ paarweise* koprime *Ideale, d. h. es gelte $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Ist dann $\pi_i\colon R \longrightarrow R/\mathfrak{a}_i$ jeweils die kanonische Projektion, so ist der Homomorphismus*

$$\varphi\colon R \longrightarrow R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \qquad x \longmapsto (\pi_1(x), \ldots, \pi_n(x)),$$

surjektiv und erfüllt $\ker \varphi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, *induziert also einen Isomorphismus*

$$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i.$$

Dabei bezeichnet $\prod_{i=1}^n R/\mathfrak{a}_i = R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$ das ringtheoretische Produkt der Restklassenringe $R/\mathfrak{a}_i$.

Beweis. Wir wollen zunächst zeigen, dass für $j = 1, \ldots, n$ die Ideale $\mathfrak{a}_j$ und $\bigcap_{i \neq j} \mathfrak{a}_i$ koprim sind, ihre Summe also gleich R ist. Sei im Folgenden ein solcher Index j fest gewählt. Da $\mathfrak{a}_j$ nach Voraussetzung zu den restlichen $\mathfrak{a}_i$ koprim ist, gibt es für $i \neq j$ Elemente $a_i \in \mathfrak{a}_j$, $a_i' \in \mathfrak{a}_i$ mit $a_i + a_i' = 1$. Somit folgt

$$1 = \prod_{i \neq j} (a_i + a_i') \in \mathfrak{a}_j + \prod_{i \neq j} \mathfrak{a}_i \subset \mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i,$$

d. h. es gilt $\mathfrak{a}_j + \bigcap_{i \neq j} \mathfrak{a}_i = R$ wie behauptet.

Für $j = 1, \ldots, n$ existieren daher Gleichungen $d_j + e_j = 1$ mit Elementen $d_j \in \mathfrak{a}_j$, $e_j \in \bigcap_{i \neq j} \mathfrak{a}_i$, und es folgt

$$\pi_i(e_j) = \begin{cases} 1 & \text{für} \quad i = j, \\ 0 & \text{für} \quad i \neq j. \end{cases}$$

Damit sieht man unmittelbar ein, dass φ surjektiv ist. Geht man nämlich von einem Element $y = (y_1, \ldots, y_n) \in R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$ aus und wählt jeweils ein π_i-Urbild $x_i \in R$ zu y_i, so gilt

$$\varphi\Big(\sum_{i=1}^{n} x_i e_i\Big) = y.$$

Die Aussage über den Kern von φ ist trivial. Somit folgt die behauptete Isomorphie aus dem Homomorphiesatz. □

Ist $\mathfrak{a}$ ein Ideal in einem Ring R, so sagt man, dass zwei Elemente $x, y \in R$ *kongruent modulo* $\mathfrak{a}$ sind, in Zeichen $x \equiv y \mod \mathfrak{a}$, wenn x und y dieselbe Restklasse in $R/\mathfrak{a}$ definieren, d. h. wenn $x - y \in \mathfrak{a}$ gilt. Ist dabei $\mathfrak{a}$ ein Hauptideal Ra, so schreibt man statt "mod $\mathfrak{a}$" häufig auch "mod a". Unter Benutzung einer solchen Sprechweise können wir die Surjektivität der Abbildung φ in Satz 12 auch folgendermaßen formulieren: Zu $x_1, \ldots, x_n \in R$ gibt es ein $x \in R$ mit $x \equiv x_i \mod \mathfrak{a}_i$ für $i = 1, \ldots, n$. Für den Ring $\mathbb{Z}$ der ganzen Zahlen hat der Chinesische Restsatz somit folgende Form:

Korollar 13. *Es seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd. Dann ist das System simultaner Kongruenzen $x \equiv x_i \mod a_i$, $i = 1, \ldots, n$, für beliebige Zahlen $x_1, \ldots, x_n \in \mathbb{Z}$ lösbar. Ist x eine Lösung, so ist diese eindeutig bestimmt modulo $a_1 \cdot \ldots \cdot a_n$. Die Gesamtheit der Lösungen bildet daher eine Restklasse des Typs $x + a_1 \cdot \ldots \cdot a_n\mathbb{Z}$.*

Man muss sich lediglich überlegen, dass für teilerfremde Zahlen $a, a' \in \mathbb{Z}$

$$(a, a') = (1) \quad \text{sowie} \quad (a \cdot a') = (a) \cap (a')$$

gilt; man vergleiche hierzu auch 2.4/13. Im Übrigen liefert der Beweis des Chinesischen Restsatzes auch ein praktisches Verfahren zur Lösung simultaner Kongruenzen. In einem ersten Schritt konstruiert man für $j = 1, \ldots, n$ Zahlen $d_j \in (a_j)$, $e_j \in (\prod_{i \neq j} a_i)$, mit $d_j + e_j = 1$, etwa unter Verwendung des *Euklidischen Algorithmus*; vgl. hierzu 2.4/15. Sodann ist $x = \sum_{i=1}^{n} x_i e_i$ eine Lösung des Systems $x \equiv x_i \mod a_i$, $i = 1, \ldots, n$, und jede weitere Lösung entsteht durch Addition eines Vielfachen von $\prod_{i=1}^{n} a_i$.

Aufgaben

1. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus. Welche Aussagen gelten für die Bilder von Idealen $\mathfrak{a} \subset R$ bzw. die Urbilder von Idealen $\mathfrak{a}' \subset R'$? Man untersuche diese Frage insbesondere auch für Primideale und maximale Ideale.*

2. *Es sei R ein Ring. Für $x \in R$ betrachte man den Einsetzungshomomorphismus*

$$\varphi_x \colon R[X] \longrightarrow R, \qquad \sum a_i X^i \longmapsto \sum a_i x^i.$$

Man beschreibe den Kern von φ_x und überlege insbesondere, wann dieser ein Primideal bzw. ein maximales Ideal in $R[X]$ ist.

3. Man verallgemeinere die Isomorphiesätze 1.2/8 und 1.2/9 auf die Ringsituation, indem man Ringe statt Gruppen und Ideale statt Normalteiler betrachte.

4. Sei $\varphi \colon R \longrightarrow R'$ ein Ringhomomorphismus und $x \in R'$. Man zeige: Es gibt genau einen Ringhomomorphismus $\Phi \colon R[X] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X) = x$. Es entsprechen also die Ringhomomorphismen $\Phi \colon R[X] \longrightarrow R'$ mit $\Phi|_R = \varphi$ in bijektiver Weise den Elementen von R'.

5. Sei R ein Integritätsring und $\Phi \colon R[X] \longrightarrow R[X]$ ein Ringhomomorphismus mit $\Phi|_R = \mathrm{id}_R$. Man zeige: Φ ist genau dann ein Automorphismus, wenn es $a \in R^*$ und $b \in R$ gibt mit $\Phi(X) = aX + b$.

6. Sei $\mathfrak{p}$ ein Primideal eines Ringes R. Man zeige, dass $\mathfrak{p}R[X]$, das von $\mathfrak{p}$ in $R[X]$ erzeugte Ideal, ebenfalls ein Primideal ist.

7. Sei K ein Körper und $K[X,Y] = K[X][Y]$ der Polynomring über K in zwei Variablen X und Y. Im Restklassenring $R = K[X,Y]/(XY^2)$ bezeichne $\overline{X}$ bzw. $\overline{Y}$ jeweils die Restklasse von X bzw. Y. Man zeige, dass die Elemente $\overline{X}$ und $\overline{X} + \overline{X} \cdot \overline{Y}$ aus R nicht assoziiert sind, dass die von ihnen in R erzeugten Hauptideale aber übereinstimmen. Hinweis: Man betrachte das Ideal aller Elemente $\overline{f} \in R$ mit $\overline{f} \cdot \overline{X} = 0$ bzw. das Ideal aller Elemente $f \in K[X,Y]$ mit $fX \in (XY^2)$.

8. Sei R ein Ring. Man zeige, dass $\{\sum a_i X^i \in R[X] \,;\, a_1 = 0\}$ ein Unterring von $R[X]$ ist und dass dieser isomorph zu $R[X][Y]/(X^2 - Y^3)$ ist.

2.4 Primfaktorzerlegung

Wesentliche Eigenschaften des Ringes $\mathbb{Z}$ der ganzen Zahlen oder des Polynomrings $K[X]$ über einem Körper K fußen auf der Tatsache, dass man in diesen Ringen eine Division mit Rest zur Verfügung hat. Wir wollen von Integritätsringen ausgehen, die eine solche Division ermöglichen, und zeigen, dass diese Ringe Hauptidealringe sind. In Hauptidealringen wiederum werden wir die Existenz der eindeutigen Primfaktorzerlegung beweisen.

Definition 1. *Ein Integritätsring R mit einer Abbildung $\delta \colon R - \{0\} \longrightarrow \mathbb{N}$ heißt ein* euklidischer Ring, *wenn gilt: Zu Elementen $f, g \in R$, $g \neq 0$, gibt es stets Elemente $q, r \in R$ mit*

$$f = qg + r, \quad \textit{wobei} \;\; \delta(r) < \delta(g) \;\; \textit{oder} \;\; r = 0.$$

Die Abbildung δ wird als Grad- *oder* Normabbildung *des euklidischen Rings R bezeichnet.*

Jeder Körper ist aus trivialen Gründen ein euklidischer Ring. Wir wollen aber noch einige interessantere Beispiele betrachten.

(1) $\mathbb{Z}$ ist ein euklidischer Ring mit der gewöhnlichen Division mit Rest, als Gradabbildung $\delta\colon \mathbb{Z}-\{0\} \longrightarrow \mathbb{N}$ kann man die Abbildung $a \longmapsto |a|$ betrachten.

(2) Ist K ein Körper, so ist der Polynomring $K[X]$ mit der gewöhnlichen Polynomdivision mit Rest ein euklidischer Ring, $\delta\colon K[X]-\{0\} \longrightarrow \mathbb{N}$ ist die Abbildung $f \longmapsto \operatorname{grad} f$. Man vergleiche hierzu 2.1/4

(3) $\mathbb{Z}[i] := \{x+iy\,;\, x,y \in \mathbb{Z}\} \subset \mathbb{C}$ ist ein euklidischer Ring unter der Gradabbildung

$$\delta\colon \mathbb{Z}[i]-\{0\} \longrightarrow \mathbb{N}, \qquad x+iy \longmapsto x^2+y^2 = |x+iy|^2.$$

Man nennt $\mathbb{Z}[i]$ den *Ring der ganzen Gaußschen Zahlen*. Zur Charakterisierung der Division mit Rest in $\mathbb{Z}[i]$ beachte man, dass der Abstand benachbarter Punkte aus $\mathbb{Z}[i]$ höchstens $\sqrt{2}$ beträgt. Zu $f,g \in \mathbb{Z}[i]$, $g \neq 0$, gibt es daher $x,y \in \mathbb{Z}$ mit $|fg^{-1}-(x+iy)| \leq \frac{1}{2}\cdot\sqrt{2} < 1$. Setzt man nun $q := (x+iy)$, $r := f-qg$, so hat man $|r| < |g|$, also

$$f = qg + r \quad \text{mit} \quad \delta(r) < \delta(g) \text{ oder } r = 0.$$

(4) Sei $d \neq 0,1$ eine ganze Zahl, und sei d quadratfrei in dem Sinne, dass d kein Quadrat einer natürlichen Zahl >1 als Teiler besitzt. Man betrachte zu d den folgenden Unterring von $\mathbb{C}$:

$$R_d = \begin{cases} \mathbb{Z}+\sqrt{d}\cdot\mathbb{Z}, & \text{falls } d \equiv 2,3 \mod 4 \\ \mathbb{Z}+\frac{1}{2}(1+\sqrt{d})\cdot\mathbb{Z}, & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

Für $d=-1$ erhält man den oben diskutierten Ring der ganzen Gaußschen Zahlen. Die Ringe R_d sind in der Zahlentheorie von besonderem Interesse. Man möchte wissen, ob R_d faktoriell ist, d. h. ob in R_d jeweils der Satz von der eindeutigen Primfaktorzerlegung gilt. Da ein euklidischer Ring Hauptidealring ist und ein Hauptidealring faktoriell ist, vgl. Satz 2 und Korollar 11, untersucht man in erster Approximation, für welche Werte von d der Ring R_d euklidisch ist. Als Gradabbildung $\delta\colon R_d-\{0\} \longrightarrow \mathbb{N}$ bietet sich hier die so genannte "Norm" an, gegeben durch $\delta(a+b\sqrt{d}) = |a^2-b^2d|$; zur allgemeinen Definition der Norm vgl. Abschnitt 4.7. Man kann zeigen, dass R_d genau für folgende Werte von d unter dieser Gradabbildung euklidisch ist:

$$d = -1,-2,-3,-7,-11,$$
$$d = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73.$$

Darüber hinaus weiß man, dass R_d für $d<0$ in noch genau den folgenden Fällen faktoriell ist:

$$d = -19,-43,-67,-163.$$

Für $d > 0$ hingegen ist R_d faktoriell in einer Vielzahl weiterer Fälle. Bezüglich Details konsultiere man etwa H. Hasse [6], §16.6.

Satz 2. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Wir gehen wie in 1.3/4 vor. Sei $\mathfrak{a} \subset R$ ein Ideal; ohne Einschränkung gelte $\mathfrak{a} \neq 0$. Man wähle unter den Elementen a von $\mathfrak{a} - \{0\}$ eines mit der Eigenschaft, dass $\delta(a)$ minimal unter der Gradabbildung δ unseres euklidischen Rings R ist. Dann gilt schon $\mathfrak{a} = (a)$. Ist nämlich $f \in \mathfrak{a}$, $f = qa + r$ mit $\delta(r) < \delta(a)$ oder $r = 0$, so folgt $r = f - qa \in \mathfrak{a}$. Wegen der Minimalität von $\delta(a)$ muss $r = 0$ gelten und somit $f = qa \in (a)$. Dies zeigt $\mathfrak{a} \subset (a)$. Die umgekehrte Inklusion ist trivial, so dass $\mathfrak{a} = (a)$ Hauptideal ist. □

Korollar 3. *Die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ sowie der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe auch Hauptidealringe.*

Als Nächstes wollen wir Primfaktorzerlegungen in Hauptidealringen studieren. Wir sagen, dass in einem Integritätsring R ein Element x das Element y *teilt*, in Zeichen $x \mid y$, wenn es ein $c \in R$ mit $cx = y$ gibt. Äquivalent zu dieser Gleichung ist $y \in (x)$. Ist x kein Teiler von y, so schreibt man $x \nmid y$.

Definition 4. *Es sei R ein Integritätsring und $p \in R$ eine von 0 verschiedene Nichteinheit.*

(i) *p heißt* irreduzibel, *falls für jede Zerlegung $p = xy$ mit $x, y \in R$ gilt: $x \in R^*$ oder $y \in R^*$. Es heißt p* reduzibel, *falls p nicht irreduzibel ist.*

(ii) *p heißt* primes Element *oder* Primelement, *wenn aus $p \mid xy$ mit $x, y \in R$ stets $p \mid x$ oder $p \mid y$ folgt, d. h. mit anderen Worten, wenn das Hauptideal (p) prim ist.*

Im Ring $\mathbb{Z}$ der ganzen Zahlen entsprechen die irreduziblen Elemente abgesehen vom Vorzeichen genau den Primzahlen im üblichen Sinne, während im Polynomring $K[X]$ über einem Körper K insbesondere die linearen Polynome $X - a$ mit $a \in K$ irreduzibel sind. Für $K = \mathbb{C}$ sind hierdurch bis auf Assoziiertheit alle irreduziblen Polynome beschrieben, wie wir später anhand des Fundamentalsatzes der Algebra sehen werden. Im Allgemeinen gibt es jedoch über einem Körper K irreduzible Polynome vom Grad > 1, in $\mathbb{R}[X]$ etwa das Polynom $X^2 + 1$. Im Übrigen werden wir in Satz 6 sehen, dass die Begriffe irreduzibles Element und Primelement in Hauptidealringen übereinstimmen, also insbesondere in $\mathbb{Z}$ bzw. $K[X]$.

Bemerkung 5. *Es sei R ein Integritätsring und $p \in R$ eine von 0 verschiedene Nichteinheit.*

(i) *Wenn (p) ein maximales Ideal in R ist, so ist p ein Primelement.*

(ii) *Wenn p ein Primelement ist, so ist p irreduzibel.*

Beweis. Ist (p) ein maximales Ideal in R, so auch ein Primideal nach 2.3/8, und es folgt, dass p ein Primelement ist. Dies zeigt die Behauptung (i). Zum Nachweis von (ii) sei p als Primelement angenommen. Gilt dann $p = xy$ mit $x, y \in R$, so ergibt sich $p \,|\, x$ oder $p \,|\, y$ aufgrund der Primelementeigenschaft von p. Nehmen wir $p \mid x$ an, so existiert also ein $c \in R$ mit $pc = x$, und es folgt $p = xy = pcy$. Da R ein Integritätsring ist, hat man $cy = 1$ und somit $y \in R^*$, d. h. p ist irreduzibel. □

In Hauptidealringen können wir die Aussage der soeben bewiesenen Bemerkung erheblich verschärfen; man vergleiche auch 2.3/6.

Satz 6. *Es sei R ein Hauptidealring und $p \in R$ eine von 0 verschiedene Nichteinheit. Dann ist äquivalent*:

(i) *p ist irreduzibel.*

(ii) *p ist Primelement.*

(iii) *(p) ist maximales Ideal in R.*

Beweis. Unter Benutzung von Bemerkung 5 bleibt nur noch die Implikation von (i) nach (iii) nachzuweisen. Sei also p irreduzibel, und sei $\mathfrak{a} = (a)$ ein Ideal in R mit $(p) \subset (a) \subset R$. Dann existiert ein $c \in R$ mit $p = ac$. Da p irreduzibel ist, folgt $a \in R^*$ oder $c \in R^*$. Im ersten Fall hat man $(a) = R$ und im zweiten $(a) = (p)$. Somit ist (p) maximal. □

Als Folgerung hierzu können wir leicht die Existenz von Primfaktorzerlegungen in Hauptidealringen beweisen. Es braucht nur eine Faktorisierung in irreduzible Elemente durchgeführt werden.

Satz 7. *Es sei R ein Hauptidealring. Dann lässt sich jedes $a \in R - (R^* \cup \{0\})$ als Produkt von Primelementen schreiben.*[2]

Beweis. Man fixiere ein Element $a \in R - (R^* \cup \{0\})$. Ist a irreduzibel (und damit prim), so ist nichts zu zeigen. Anderenfalls zerlege man a in das Produkt bc zweier Nichteinheiten aus R. Diese Konstruktion kann man dann für b sowie c wiederholen usw. Zum Beweis des Satzes ist lediglich zu zeigen, dass das Verfahren nach endlich vielen Schritten abbricht. Für die uns interessierenden Ringe $\mathbb{Z}$ und $K[X]$, wobei K ein Körper sei, ist dies unmittelbar klar. In $\mathbb{Z}$ etwa gilt $|b|, |c| < |a|$ bei einer Faktorisierung von a in Nichteinheiten b, c. Entsprechend hat man $\operatorname{grad} b, \operatorname{grad} c < \operatorname{grad} a$ in $K[X]$, wie man mit 2.1/2 sieht. Bei der beschriebenen Zerlegung von a nimmt daher der Betrag bzw. Grad bei jedem Schritt echt ab, so dass das Verfahren nach endlich vielen Schritten abbrechen muss.

[2] Unter einem Produkt von Elementen eines Ringes verstehen wir naturgemäß immer ein *endliches* Produkt.

Wir wollen hier noch ein Argument angeben, welches auch für einen beliebigen Hauptidealring R zeigt, dass man a in ein (endliches) Produkt irreduzibler Elemente zerlegen kann. Folgende Hilfsaussage wird benötigt:

Lemma 8. *Jeder Hauptidealring R ist* noethersch, *d. h. jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ wird stationär in dem Sinne, dass es ein $n \in \mathbb{N}$ gibt mit $\mathfrak{a}_i = \mathfrak{a}_n$ für alle $i \geq n$.*

Die Aussage ist leicht zu verifizieren. Da die Vereinigung einer aufsteigenden Kette von Idealen wieder ein Ideal ergibt, kann man das Ideal $\mathfrak{a} = \bigcup_{i \geq 1} \mathfrak{a}_i$ bilden; dieses ist ein Hauptideal, etwa $\mathfrak{a} = (a)$. Wegen $a \in \mathfrak{a}$ gibt es ein $n \in \mathbb{N}$ mit $a \in \mathfrak{a}_n$, so dass $(a) \subset \mathfrak{a}_n \subset \mathfrak{a} = (a)$ folgt. Die Idealkette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ wird somit bei $\mathfrak{a}_n$ stationär.

Nun wollen wir den Allgemeinfall von Satz 7 beweisen. Es bezeichne S die Menge aller Hauptideale in R, die von Elementen $a \in R - (R^* \cup \{0\})$ erzeugt werden, wobei a keine endliche Faktorisierung in irreduzible Elemente besitze. Zu zeigen ist $S = \emptyset$. Gilt $S \neq \emptyset$, so gibt es aufgrund von Lemma 8 ein maximales Element in S, d. h. ein Element $\mathfrak{a} \in S$ mit der Eigenschaft, dass aus einer echten Inklusion $\mathfrak{a} \subsetneq \mathfrak{b}$ von Idealen in R notwendig folgt, dass $\mathfrak{b}$ nicht zu S gehört. Sei also $\mathfrak{a} = (a)$ ein solches maximales Element. Dann ist das erzeugende Element a reduzibel, etwa $a = a_1 a_2$ mit Nichteinheiten $a_1, a_2 \in R$. Folglich haben wir echte Inklusionen

$$(a) \subsetneq (a_1), \qquad (a) \subsetneq (a_2),$$

und es ergibt sich, dass (a_1) und (a_2) nicht zu S gehören können. Es haben daher a_1 und a_2 Faktorisierungen in irreduzible Elemente, und damit gilt dasselbe auch für das Produkt $a = a_1 a_2$ im Widerspruch zu $(a) \in S$. Somit folgt $S = \emptyset$, und Satz 7 ist bewiesen. □

Zerlegungen in Primelemente wie in Satz 7 erfüllen eine gewisse Eindeutigkeitsaussage.

Lemma 9. *Es sei R ein Integritätsring. Für ein Element $a \in R$ habe man Zerlegungen*

$$a = p_1 \ldots p_r = q_1 \ldots q_s$$

in Primelemente p_i und irreduzible Elemente q_j. Dann gilt $r = s$, und nach eventueller Umnummerierung der q_j ist p_i assoziiert zu q_i für $i = 1, \ldots, r$.

Beweis. Aus $p_1 \mid q_1 \ldots q_s$ folgt aufgrund der Primelementeigenschaft von p_1, dass es ein j mit $p_1 \,|\, q_j$ gibt. Nach Umnummerierung der q_j dürfen wir $j = 1$ annehmen. Es gibt also eine Gleichung $q_1 = \varepsilon_1 p_1$, wobei ε_1 Einheit sein muss, da q_1 irreduzibel ist. Somit folgt

$$p_2 \ldots p_r = \varepsilon_1 q_2 \ldots q_s,$$

und man kann das Verfahren induktiv fortsetzen, um die Behauptung zu erhalten. □

Satz und Definition 10. *Es sei R ein Integritätsring. Dann ist äquivalent*:

(i) *Jedes $a \in R - (R^* \cup \{0\})$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von irreduziblen Elementen schreiben.*

(ii) *Jedes $a \in R - (R^* \cup \{0\})$ lässt sich als Produkt von Primelementen schreiben.*

Ein Integritätsring R, der die vorstehenden äquivalenten Bedingungen erfüllt, heißt faktoriell. *Man sagt auch, dass in R der* Satz von der eindeutigen Primfaktorzerlegung *gilt.*

In einem faktoriellen Ring ist ein Element a genau dann irreduzibel, wenn es prim ist.

Beweis. Es gelte die Bedingung (i). Wir wollen zeigen, dass dann jedes irreduzible Element von R schon prim ist. Sei also $a \in R$ irreduzibel, und seien $x, y \in R$ mit $a \mid xy$. Zu zeigen ist $a \mid x$ oder $a \mid y$. Hierzu dürfen wir annehmen, dass x und y keine Einheiten sind. Seien $x = x_1 \dots x_r$, $y = y_1 \dots y_s$ Zerlegungen in irreduzible Elemente gemäß (i). Dann folgt $a \mid (x_1 \dots x_r y_1 \dots y_s)$, und die Eindeutigkeitsaussage in (i) hat zur Folge, dass a als irreduzibles Element zu einem x_i oder einem y_j assoziiert ist. Daher gilt $a \mid x$ oder $a \mid y$, und a ist Primelement. Mit dieser Überlegung ist die Implikation von (i) nach (ii) unmittelbar klar. Die Umkehrung folgt mit Lemma 9, da eine Zerlegung in Primelemente nach Bemerkung 5 insbesondere eine Zerlegung in irreduzible Elemente ist.

Wir haben gerade gesehen, dass unter der Bedingung (i) jedes irreduzible Element prim ist, dass also irreduzible Elemente in faktoriellen Ringen prim sind. Die Umkehrung hierzu ergibt sich wiederum aus Bemerkung 5. □

Die Aussage von Satz 7 können wir nun neu formulieren:

Korollar 11. *Jeder Hauptidealring ist faktoriell.*

Körper sind aus trivialen Gründen faktoriell. Aber auch die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ sowie der Polynomring $K[X]$ über einem Körper K sind als euklidische Ringe Hauptidealringe und damit faktoriell. Wir werden in 2.7/1 zeigen, dass der Polynomring $R[X]$ über einem faktoriellen Ring R selbst wieder faktoriell ist. Somit kann man sehen, dass etwa der Ring $\mathbb{Z}[X]$ faktoriell ist, obwohl er kein Hauptidealring ist. Gleiches gilt für den Polynomring $K[X,Y] := K[X][Y]$ in zwei Variablen X und Y über K.

Es ist üblich, Primfaktorzerlegungen in faktoriellen Ringen R durch Zusammenfassen assoziierter Primelemente zu Potenzen in der Form

$$a = \varepsilon p_1^{\nu_1} \dots p_r^{\nu_r}$$

zu schreiben, wobei ε eine Einheit ist. Formal besitzt dann jedes $a \in R - \{0\}$ eine solche Primfaktorzerlegung (mit Exponenten $\nu_i = 0$, wenn a Einheit ist). Um Primfaktorzerlegungen weiter zu standardisieren, kann man in R ein Vertretersystem P von Primelementen auswählen, d. h. eine Teilmenge P bestehend

aus Primelementen, so dass P aus jeder Klasse zueinander assoziierter Primelemente genau eines enthält. Dann kann man Primfaktorzerlegungen in R in der Form

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

schreiben, wobei nunmehr $\varepsilon \in R^*$ sowie die Exponenten $\nu_p(a) \in \mathbb{N}$ eindeutig bestimmt sind; natürlich gilt $\nu_p(a) = 0$ für fast alle $p \in P$, so dass das Produkt in Wahrheit endlich ist. In $\mathbb{Z}$ ist es üblich, P als die Menge der (positiven) Primzahlen zu wählen, in $K[X]$ nimmt man für P die Menge aller normierten irreduziblen (oder Prim-) Polynome, d. h. aller irreduziblen Polynome, deren höchster Koeffizient 1 ist.

Wir wollen im Folgenden noch auf die Begriffe größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches eingehen. Sei R ein Integritätsring, und seien $x_1, \ldots, x_n \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von $x_1, \ldots, x_n$, wenn gilt:

(i) $d \,|\, x_i$ für $i = 1, \ldots, n$, d. h. d ist gemeinsamer Teiler aller x_i.

(ii) Ist $a \in R$ gemeinsamer Teiler der x_i, also $a \,|\, x_i$ für $i = 1, \ldots, n$, so folgt $a \,|\, d$.

Es ist dann d eindeutig bis auf Assoziiertheit, und man verwendet die Notation $d = \mathrm{ggT}(x_1, \ldots, x_n)$. Im Falle $d = 1$ bezeichnet man $x_1, \ldots, x_n$ als *teilerfremd*.

Ein Element $v \in R$ heißt *kleinstes gemeinsames Vielfaches* von $x_1, \ldots, x_n$, wenn gilt:

(i) $x_i \,|\, v$ für $i = 1, \ldots, n$, d. h. v ist gemeinsames Vielfaches aller x_i.

(ii) Ist $a \in R$ gemeinsames Vielfaches der x_i, d. h. $x_i \,|\, a$ für $i = 1, \ldots, n$, so folgt $v \,|\, a$.

Auch in diesem Falle ist v eindeutig bis auf Assoziiertheit, man schreibt $v = \mathrm{kgV}(x_1, \ldots, x_n)$. Wie üblich beweist man:

Satz 12. *Es sei R ein faktorieller Ring. Ist dann P ein Vertretersystem der Primelemente von R und sind*

$$x_i = \varepsilon_i \prod_{p \in P} p^{\nu_p(x_i)}, \qquad i = 1, \ldots, n,$$

Primfaktorzerlegungen von Elementen $x_1, \ldots, x_n \in R - \{0\}$, so existieren $\mathrm{ggT}(x_1, \ldots, x_n)$ und $\mathrm{kgV}(x_1, \ldots, x_n)$, und zwar gilt (bis auf Assoziiertheit)

$$\mathrm{ggT}(x_1, \ldots, x_n) = \prod_{p \in P} p^{\min(\nu_p(x_1), \ldots, \nu_p(x_n))},$$

$$\mathrm{kgV}(x_1, \ldots, x_n) = \prod_{p \in P} p^{\max(\nu_p(x_1), \ldots, \nu_p(x_n))}.$$

In Hauptidealringen lassen sich der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache idealtheoretisch charakterisieren.

Satz 13. *Es seien $x_1 \ldots, x_n$ Elemente eines Integritätsrings R.*

(i) *Falls $(x_1 \ldots, x_n)$, das von den x_i in R erzeugte Ideal, ein Hauptideal ist, also von einem Element $d \in R$ erzeugt wird, so gilt $d = \mathrm{ggT}(x_1 \ldots, x_n)$.*

(ii) *Falls $(x_1) \cap \ldots \cap (x_n)$ ein Hauptideal ist, also von einem Element $v \in R$ erzeugt wird, so gilt $v = \mathrm{kgV}(x_1 \ldots, x_n)$.*

Beweis. (i) Gelte $(x_1 \ldots, x_n) = (d)$. Dann folgt $x_i \in (d)$ und somit $d \,|\, x_i$ für alle i. Außerdem gibt es wegen $d \in (x_1 \ldots, x_n)$ eine Gleichung $d = \sum_{i=1}^{n} a_i x_i$ mit gewissen Elementen $a_i \in R$. Hieraus ergibt sich, dass jeder gemeinsame Teiler der x_i auch ein Teiler von d ist, d. h. $d = \mathrm{ggT}(x_1 \ldots, x_n)$.

(ii) Gelte $\bigcap_{i=1}^{n}(x_i) = (v)$. Dann ist v Element aller Ideale (x_i), also gemeinsames Vielfaches aller x_i. Sei nun a ein weiteres gemeinsames Vielfaches der x_i. Dann folgt $a \in (x_i)$ für alle i, also $a \in \bigcap_{i=1}^{n}(x_i) = (v)$ und somit $v \mid a$, d. h. $v = \mathrm{kgV}(x_1 \ldots, x_n)$. □

Als Beispiel für eine Anwendung der gerade gegebenen idealtheoretischen Charakterisierung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen wollen wir eine spezielle Version des Chinesischen Restsatzes 2.3/12 betrachten.

Korollar 14. *Es sei R ein Hauptidealring und $a = \varepsilon p_1^{\nu_1} \ldots p_r^{\nu_r}$ eine Primfaktorzerlegung in R mit einer Einheit ε und paarweise nicht-assoziierten Primelementen p_i. Dann sind die Ideale $(p_1^{\nu_1}), \ldots, (p_r^{\nu_r})$ paarweise koprim in R, und es gilt $a = \mathrm{kgV}(p_1^{\nu_1}, \ldots, p_r^{\nu_r})$ sowie $(a) = \bigcap_{i=1}^{r}(p_i^{\nu_i})$. Insbesondere existiert aufgrund von 2.3/12 ein kanonischer Isomorphismus*

$$R/(a) \xrightarrow{\sim} R/(p_1^{\nu_1}) \times \ldots \times R/(p_n^{\nu_n}).$$

In euklidischen Ringen R gibt es ein konstruktives Verfahren zur Bestimmung des größten gemeinsamen Teilers zweier Elemente $x, y \in R$, nämlich den *Euklidischen Algorithmus*. Durch iterative Anwendung von Beziehungen des Typs $\mathrm{ggT}(x, y, z) = \mathrm{ggT}(\mathrm{ggT}(x, y), z)$ eignet sich dieses Verfahren auch zur Bestimmung des größten gemeinsamen Teilers von mehr als zwei Elementen.

Satz 15. (Euklidischer Algorithmus). *Es sei R ein euklidischer Ring. Für zwei Elemente $x, y \in R - \{0\}$ betrachte man die Folge $z_0, z_1, \ldots \in R$, die induktiv gegeben ist durch*:

$$\begin{aligned} z_0 &= x, \\ z_1 &= y, \\ z_{i+1} &= \begin{cases} \text{der Rest von } z_{i-1} \text{ bei Division durch } z_i, \text{ falls } z_i \neq 0, \\ 0 \text{ sonst.} \end{cases} \end{aligned}$$

Dann gibt es einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Für dieses n gilt $z_n = \mathrm{ggT}(x, y)$.

Beweis. Es sei $\delta\colon R-\{0\} \longrightarrow \mathbb{N}$ die Gradabbildung von R. Nach Definition der Folge $z_0, z_1, \ldots$ hat man für $i > 0$ unter der Bedingung $z_i \neq 0$ eine Gleichung der Form

$$z_{i-1} = q_i z_i + z_{i+1},$$

wobei $\delta(z_{i+1}) < \delta(z_i)$ oder $z_{i+1} = 0$ gilt. Die Folge der Grade $\delta(z_i)$ ist daher für $i > 0$ streng monoton fallend, jedenfalls solange $z_i \neq 0$ gilt und $\delta(z_i)$ erklärt ist. Somit kann $z_i \neq 0$ aber nur für endlich viele $i \in \mathbb{N}$ gelten, und es gibt einen kleinsten Index $n \in \mathbb{N}$ mit $z_{n+1} = 0$. Wegen $z_0 \neq 0 \neq z_1$ ist $n > 0$. Man betrachte nun die Gleichungen

$$\begin{aligned}
&(\mathrm{E}_0) && z_0 = q_1 z_1 + z_2,\\
&\vdots && \vdots\\
&(\mathrm{E}_{n-2}) && z_{n-2} = q_{n-1} z_{n-1} + z_n,\\
&(\mathrm{E}_{n-1}) && z_{n-1} = q_n z_n.
\end{aligned}$$

Es folgt $z_n \,|\, z_{n-1}$ aus (E_{n-1}), dann $z_n \,|\, z_{n-2}$ aus (E_{n-2}) usw., bis man schließlich $z_n \,|\, z_1$ und $z_n \,|\, z_0$ erhält. Es ist also z_n ein gemeinsamer Teiler von x und y. Ist $a \in R$ ein weiterer gemeinsamer Teiler von x und y, so folgt $a \mid z_2$ aus (E_0), dann $a \,|\, z_3$ aus (E_1) usw., bis man schließlich zu $a \,|\, z_n$ gelangt. Also ist z_n wie behauptet der größte gemeinsame Teiler von x und y. □

Der Euklidische Algorithmus gestattet es nicht nur, den größten gemeinsamen Teiler d zweier Elemente x, y eines euklidischen Rings R zu bestimmen, sondern er liefert zusätzlich auch eine explizite Darstellung dieses Teilers in der Form $d = ax + by$. Im obigen Beweis erhält man nämlich aus (E_{n-2}) eine Darstellung von $d = z_n$ als Linearkombination in z_{n-2}, z_{n-1}, unter Hinzunahme von (E_{n-3}) als Linearkombination in z_{n-3}, z_{n-2} usw., bis d schließlich unter Benutzung von (E_0) als Linearkombination von $x = z_0$ und $y = z_1$ dargestellt ist. Die Konstruktion einer solchen Darstellung wird z. B. bei dem praktischen Verfahren zur Lösung simultaner Kongruenzen 2.3/13 benötigt, die allgemeine Existenz ist hingegen bereits in Hauptidealringen gegeben, wie wir in Satz 13 gesehen haben.

Abschließend wollen wir noch auf einige Anwendungen der in diesem Abschnitt erzielten Resultate hinweisen. Wir können aus 2.3/8 und Satz 6 nochmals folgern, dass für ein $p \in \mathbb{Z}$, $p > 0$, der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ genau dann ein Körper ist, wenn p eine Primzahl ist. Ebenso ist für einen Körper K der Restklassenring $L = K[X]/(f)$ nach dem von einem Polynom $f \in K[X]$ erzeugten Hauptideal genau dann ein Körper, wenn f irreduzibel ist. Man sieht leicht (vgl. den Beweis zu 3.4/1), dass die Restklasse von X in L nunmehr Nullstelle von f ist. Dabei fasse man K vermöge des kanonischen Homomorphismus $K \longrightarrow L$ (dieser ist nach 2.3/3 injektiv) als Teilkörper von L auf und entsprechend f als Polynom mit Koeffizienten in L. Wir werden dieses auf L. Kronecker zurückgehende Verfahren in 3.4/1 benutzen, um zu einem gegebenen Polynom $f \in K[X]-K$, welches in K keine Nullstelle besitzt, einen Erweiterungskörper

L zu konstruieren, so dass f eine Nullstelle in L hat. Beispielsweise sieht man mit Hilfe des Homomorphiesatzes unmittelbar

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C},$$

indem man den Einsetzungshomomorphismus

$$\mathbb{R}[X] \longrightarrow \mathbb{C}, \qquad \sum a_n X^n \longmapsto \sum a_n i^n,$$

betrachtet, der X auf die komplexe Zahl i abbildet. Auf ähnliche Weise zeigt man

$$\mathbb{R}[X]/(X-a) \simeq \mathbb{R}$$

für beliebiges $a \in \mathbb{R}$.

Aufgaben

1. *Welche Ringe R haben die Eigenschaft, dass der Polynomring $R[X]$ ein Hauptidealring ist*?
2. *Es folgt aus Satz* 13, *dass sich in einem Hauptidealring der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache zweier Elemente stets idealtheoretisch charakterisieren lassen. Man untersuche, ob dies auch allgemeiner in faktoriellen Ringen gilt.*
3. Man beweise, dass der Unterring $R = \mathbb{Z} + \sqrt{-5}\cdot\mathbb{Z} \subset \mathbb{C}$ nicht faktoriell ist, indem man die Faktorisierungen $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ betrachtet und zeigt, dass die Elemente $2, 3$, $(1+\sqrt{-5})$, $(1-\sqrt{-5})$ jeweils irreduzibel und paarweise nichtassoziiert sind. Handelt es sich bei diesen Elementen um Primelemente?
4. Sei K ein Körper und $R = K[X][Y]/(X^2-Y^3)$ der Integritätsring aus Aufgabe 8 in 2.3. Man zeige: Die Restklassen $\overline{X}$ und $\overline{Y}$ zu $X, Y \in K[X][Y]$ sind irreduzibel in R, aber nicht prim.
5. Sei G eine zyklische Gruppe endlicher Ordnung, und seien $a, b \in G$. Dann ist die von a und b in G erzeugte Untergruppe von der Ordnung $\mathrm{kgV}(\mathrm{ord}\, a, \mathrm{ord}\, b)$.
6. Man zeige, dass $2 = (1+i)(1-i)$ die Primfaktorzerlegung von 2 in $\mathbb{Z}[i]$ ist.
7. Man berechne mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler der folgenden Polynome aus $\mathbb{Q}[X]$:
$$f = X^3 + X^2 + X - 3, \qquad g = X^6 - X^5 + 6X^2 - 13X + 7.$$
8. Man bestimme alle irreduziblen Polynome vom Grad ≤ 3 im Polynomring $\mathbb{F}_2[X]$.
9. Für eine Primzahl $p \in \mathbb{N}$ betrachte man folgende Teilmenge des Körpers $\mathbb{Q}$ der rationalen Zahlen:
$$\mathbb{Z}_p := \{0\} \cup \left\{ \frac{x}{y} \in \mathbb{Q}\,;\, x, y \in \mathbb{Z}-\{0\} \text{ mit } \nu_p(x) - \nu_p(y) \geq 0 \right\}$$
Man zeige: $\mathbb{Z}_p$ ist ein Unterring von $\mathbb{Q}$, ein Hauptidealring, aber kein Körper. Man gebe alle Einheiten sowie alle Primelemente von $\mathbb{Z}_p$ an.
10. Man zeige: Ein Ring R ist genau dann noethersch in dem Sinne, dass jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset R$ stationär wird, wenn jedes Ideal in R ein endliches Erzeugendensystem besitzt.

2.5 Polynomringe in mehreren Variablen

In 2.1 hatten wir zu einem Ring R den Polynomring $R[X]$ in einer Variablen X betrachtet. Durch Iteration kann man den Polynomring in n Variablen $X_1, \ldots, X_n$ über R konstruieren:

$$R[X_1, \ldots, X_n] := (\ldots((R[X_1])[X_2])\ldots)[X_n].$$

Andererseits ist es möglich, die Definition aus 2.1 in direkter Weise auf den Fall mehrerer Variablen zu verallgemeinern. Und zwar wollen wir im Folgenden für ein kommutatives Monoid M einen "Polynomring" $R[M]$ definieren, derart dass M als das (multiplikative) Monoid der "Monome" in $R[M]$ interpretiert werden kann. Für $M = \mathbb{N}$ werden wir auf diese Weise den Polynomring $R[X]$ in einer Variablen erhalten, für $M = \mathbb{N}^n$ den Polynomring $R[X_1, \ldots, X_n]$ in n Variablen und für $M = \mathbb{N}^{(I)}$ den Polynomring $R[\mathfrak{X}]$ in einem durch eine beliebige Indexmenge I indizierten System von Variablen $\mathfrak{X} = (X_i)_{i\in I}$. Dabei betrachte man auf $\mathbb{N}$, $\mathbb{N}^n$, $\mathbb{N}^{(I)}$ jeweils die (komponentenweise) Addition als Monoidverknüpfung.

Es sei im Folgenden M ein beliebiges kommutatives Monoid, dessen Verknüpfung wir als *Addition* schreiben. Sodann erkläre man $R[M]$ durch

$$R[M] = R^{(M)} = \{(a_\mu)_{\mu\in M}\,;\, a_\mu \in R, a_\mu = 0 \text{ für fast alle } \mu\}$$

mit den Verknüpfungen

$$(a_\mu)_{\mu\in M} + (b_\mu)_{\mu\in M} := (a_\mu + b_\mu)_{\mu\in M}, \qquad (a_\mu)_{\mu\in M} \cdot (b_\mu)_{\mu\in M} := (c_\mu)_{\mu\in M},$$

wobei

$$c_\mu = \sum_{\lambda+\nu=\mu} a_\lambda \cdot b_\nu.$$

Man prüft ohne Schwierigkeiten nach, dass $R[M]$ unter diesen Verknüpfungen ein Ring ist. Dabei ergibt sich für das Monoid $M = \mathbb{N}$ der natürlichen Zahlen der bereits in 2.1 konstruierte Polynomring einer Variablen $R[X]$. Aber auch in den übrigen Fällen kann man in $R[M]$ eine Polynom-Schreibweise einführen: Für $\mu \in M$ betrachte man $X^\mu := (\delta_{\mu,\lambda})_{\lambda\in M}$ als Element von $R[M]$, wobei $\delta_{\mu,\lambda}$ das Kronecker-Symbol ist, d. h. man hat $\delta_{\mu,\lambda} = 1$ für $\mu = \lambda$ und $\delta_{\mu,\lambda} = 0$ für $\mu \neq \lambda$. Es wird X^μ auch als das zu μ gehörige *Monom* in $R[M]$ bezeichnet. Die Elemente aus $R[M]$ schreiben sich dann in der Form $\sum_{\mu\in M} a_\mu X^\mu$ mit eindeutig bestimmten Koeffizienten $a_\mu \in R$, die für fast alle $\mu \in M$ verschwinden. Wie in $R[X]$ hat man für Addition und Multiplikation die bekannten Formeln:

$$\sum_{\mu\in M} a_\mu X^\mu + \sum_{\mu\in M} b_\mu X^\mu = \sum_{\mu\in M} (a_\mu + b_\mu) X^\mu,$$
$$\sum_{\mu\in M} a_\mu X^\mu \cdot \sum_{\mu\in M} b_\mu X^\mu = \sum_{\mu\in M} \Big(\sum_{\lambda+\nu=\mu} a_\lambda \cdot b_\nu\Big) X^\mu.$$

In gewohnter Weise ist $0 = \sum_{\mu \in M} 0 \cdot X^\mu$ als Nullpolynom das Nullelement und entsprechend X^0 (mit $0 \in M$ als neutralem Element des Monoids M) das Einselement von $R[M]$. Auch kann man R als Unterring von $R[M]$ betrachten, indem man ein Element $a \in R$ jeweils mit dem zugehörigen "konstanten Polynom" aX^0 identifiziert. Der Polynomring $R[M]$ erfüllt folgende universelle Eigenschaft:

Satz 1. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus und $\sigma\colon M \longrightarrow R'$ ein Monoidhomomorphismus, wobei R' für die Abbildung σ als Monoid unter der Ringmultiplikation aufgefasst werde. Dann existert ein eindeutig bestimmter Ringhomomorphismus $\Phi\colon R[M] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X^\mu) = \sigma(\mu)$ für alle $\mu \in M$.*

Beweis. Zum Nachweis der Eindeutigkeitsaussage betrachte man ein Element $\sum_{\mu \in M} a_\mu X^\mu \in R[M]$. Wenn dann ein Homomorphismus Φ mit den geforderten Eigenschaften existiert, so folgt notwendig

$$\Phi(\sum a_\mu X^\mu) = \sum \Phi(a_\mu X^\mu) = \sum \Phi(a_\mu)\Phi(X^\mu) = \sum \varphi(a_\mu)\sigma(\mu).$$

Umgekehrt kann man natürlich, um die Existenzaussage zu erhalten, Φ durch diese Gleichung definieren. Die Eigenschaften eines Ringhomomorphismus prüft man ohne Schwierigkeiten nach, indem man benutzt, dass φ ein Ringhomomorphismus und σ ein Monoidhomomorphismus ist. □

Die in Satz 1 bewiesene Eigenschaft wird *universell* genannt, da sie Polynomringe des Typs $R[M]$ bis auf kanonische Isomorphie eindeutig charakterisiert. Im Einzelnen bedeutet dies folgendes: Man gehe aus von einer Ringerweiterung $R \subset S$ und einem Monoidhomomorphismus $\iota\colon M \longrightarrow S$ mit S als Monoid unter der Multiplikation und nehme an, dass die in Satz 1 beschriebene Abbildungseigenschaft gilt, dass es also zu jedem Ringhomomorphismus $\psi\colon R \longrightarrow R'$ und zu jedem Monoidhomomorphismus $\tau\colon M \longrightarrow R'$ mit R' als Monoid unter der Multiplikation genau einen Ringhomomorphismus $\Psi\colon S \longrightarrow R'$ mit $\Psi|_R = \psi$ und $\Psi \circ \iota = \tau$ gibt. Dann sind die Erweiterungen $R \subset R[M]$ und $R \subset S$ kanonisch isomorph.

Wir wollen dies hier kurz begründen, und zwar mit der üblichen Argumentation, die auch für andere universelle Eigenschaften anwendbar ist. Zu $R \hookrightarrow S$ und $\iota\colon M \longrightarrow S$ korrespondiert aufgrund der universellen Eigenschaft von $R[M]$ ein Ringhomomorphismus $\Phi\colon R[M] \longrightarrow S$, der die Identität auf R fortsetzt und für den $\Phi(X^\mu) = \iota(\mu)$, $\mu \in M$, gilt. Umgekehrt erhält man aus der universellen Eigenschaft von S und dem Monoidhomomorphismus $M \longrightarrow R[M]$, $\mu \longmapsto X^\mu$, einen Ringhomomorphismus $\Psi\colon S \longrightarrow R[M]$, der die Identität auf R fortsetzt und $\Psi(\iota(\mu)) = X^\mu$ für $\mu \in M$ erfüllt. Es sind dann $\Phi \circ \Psi$ und die identische Abbildung zwei Ringhomomorphismen $S \longrightarrow S$, die die Identität auf R fortsetzen und die $\iota(\mu)$ für $\mu \in M$ jeweils festlassen. Aus der Eindeutigkeit der Abbildungseigenschaft für S ergibt sich $\Phi \circ \Psi = \mathrm{id}$ und aus der Eindeutigkeit der Abbildungseigenschaft für $R[M]$ entsprechend $\Psi \circ \Phi = \mathrm{id}$.

Wir wollen nun $M = \mathbb{N}^n$ oder $M = \mathbb{N}^{(I)}$ setzen, also Polynomringe im engeren Sinne betrachten. Im Falle $M = \mathbb{N}^n$ erklären wir für $1 \leq i \leq n$ die i-te "Variable" X_i durch $X^{(0,\ldots,0,1,0\ldots0)}$, wobei die 1 im Exponenten gerade an der i-ten Stelle stehe. Für $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ gilt dann $X^\mu = X_1^{\mu_1} \ldots X_n^{\mu_n}$, und die Elemente von $R[\mathbb{N}^n]$ schreiben sich ausführlicher in der Form

$$\sum_{(\mu_1,\ldots,\mu_n)\in\mathbb{N}^n} a_{\mu_1\ldots\mu_n} X_1^{\mu_1} \ldots X_n^{\mu_n}$$

mit eindeutig bestimmten Koeffizienten $a_{\mu_1\ldots\mu_n} \in R$, die fast alle verschwinden. Anstelle von $R[\mathbb{N}^n]$ verwenden wir die Notation $R[X_1, \ldots, X_n]$ oder $R[X]$, wobei wir $X = (X_1, \ldots, X_n)$ als ein System von Variablen auffassen. In ähnlicher Weise verfahren wir im Falle von Monoiden der Form $M = \mathbb{N}^{(I)}$ mit einer beliebigen Indexmenge I. Für $i \in I$ sei ε_i dasjenige Element von $\mathbb{N}^{(I)}$, dessen Komponenten alle verschwinden, bis auf die i-te, die 1 sei. Setzt man dann $X_i = X^{\varepsilon_i}$, so gilt für $\mu = (\mu_i)_{i\in I} \in \mathbb{N}^{(I)}$ stets $X^\mu = \prod_{i\in I} X_i^{\mu_i}$, wobei man beachte, dass fast alle Faktoren dieses Produkts gleich 1 sind, das Produkt in Wahrheit also endlich ist. Die Elemente von $R[\mathbb{N}^{(I)}]$ lassen sich daher in der Form

$$\sum_{\mu\in\mathbb{N}^{(I)}} a_\mu \prod_{i\in I} X_i^{\mu_i}$$

schreiben, und zwar mit eindeutig bestimmten Koeffizienten $a_\mu \in R$, die fast alle verschwinden. Anstelle von $R[\mathbb{N}^{(I)}]$ verwenden wir auch die Notation $R[X_i\,;\, i \in I]$ oder $R[\mathfrak{X}]$ mit $\mathfrak{X} = (X_i)_{i\in I}$. Die Elemente von $R[\mathfrak{X}]$ sind jeweils Polynome in *endlich* vielen Variablen $X_{i_1}, \ldots, X_{i_n}$, und wir können $R[\mathfrak{X}]$ als Vereinigung aller Unterringe des Typs $R[X_{i_1}, \ldots, X_{i_n}]$ auffassen, wobei die Menge $\{i_1, \ldots, i_n\}$ über alle endlichen Teilmengen von I variiert. Insbesondere lassen sich Rechnungen, die nur endlich viele Elemente von $R[\mathfrak{X}]$ betreffen, stets in einem Polynomring in endlich vielen Variablen durchführen.

Wir werden Polynomringe in unendlich vielen Variablen im Wesentlichen nur zur Konstruktion algebraisch abgeschlossener Körper in Abschnitt 3.4 benötigen. Deswegen wollen wir uns im Folgenden der Einfachheit halber auf Polynomringe des Typs $R[X_1, \ldots, X_n]$ beschränken, obwohl die Resultate, die wir nachfolgend beweisen, in entsprechender Version auch für Polynomringe in beliebig vielen Variablen gültig sind. Zunächst stellt man fest, entweder durch direkte Rechnung oder unter Verwendung von Satz 1 (vgl. auch Aufgabe 3), dass man für $n > 0$ stets einen kanonischen Isomorphismus

$$R[X_1, \ldots, X_n] \simeq (R[X_1, \ldots, X_{n-1}])[X_n]$$

hat; dabei ist $R[X_1, \ldots, X_{n-1}]$ für $n = 1$ als R zu interpretieren. Dieser Isomorphismus gestattet es in manchen Fällen, Probleme über Polynome in mehreren Variablen in induktiver Weise auf Probleme in einer Variablen zurückzuführen.

Satz 2. *Ist R ein Integritätsring, so auch der Polynomring $R[X_1, \ldots, X_n]$.*

Beweis. Wir hatten bereits in 2.1/3 eingesehen, dass die Behauptung im Falle einer Variablen richtig ist. Benutzt man den Isomorphismus

$$R[X_1, \ldots, X_n] \simeq (R[X_1, \ldots, X_{n-1}])[X_n],$$

so ergibt sich daraus der Allgemeinfall mit Induktion nach der Anzahl der Variablen.

Man kann aber auch in direkter Weise sehen, dass das Produkt zweier von Null verschiedener Polynome

$$f = \sum a_\mu X^\mu, \quad g = \sum b_\nu X^\nu \quad \in R[X_1, \ldots, X_n]$$

nicht verschwindet, wenn R ein Integritätsring ist. Zu diesem Zweck ordne man die Indexmenge $\mathbb{N}^n$ lexikographisch, d. h. man schreibe $\mu < \mu'$ für Indizes

$$\mu = (\mu_1, \ldots, \mu_n), \quad \mu' = (\mu'_1, \ldots, \mu'_n) \quad \in \mathbb{N}^n,$$

wenn für ein gewisses i, $1 \leq i \leq n$,

$$\mu_1 = \mu'_1, \ldots, \quad \mu_{i-1} = \mu'_{i-1}, \quad \mu_i < \mu'_i$$

gilt. Ist dann $\overline{\mu} \in \mathbb{N}$ maximal (bezüglich lexikographischer Ordnung) unter allen μ mit $a_\mu \neq 0$, ebenso $\overline{\nu}$ maximal mit $b_\nu \neq 0$, so ist der Koeffizient des Monoms $X^{\overline{\mu}+\overline{\nu}}$ in fg gerade $a_{\overline{\mu}} b_{\overline{\nu}}$. Wenn R ein Integritätsring ist, folgt $a_{\overline{\mu}} b_{\overline{\nu}} \neq 0$ und somit $fg \neq 0$. □

Wir schreiben im Folgenden $|\mu| := \mu_1 + \ldots + \mu_n$ für den "Betrag" eines Elementes $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$. Ist dann $f = \sum a_\mu X^\mu$ ein Polynom in $R[X_1, \ldots, X_n]$, so bezeichnet man für $i \in \mathbb{N}$ mit $f_i := \sum_{|\mu|=i} a_\mu X^\mu$ den *homogenen Bestandteil von f vom Grad i*. Es ist also f Summe seiner homogenen Bestandteile, d. h. $f = \sum_{i=0}^{\infty} f_i$. Man nennt f *homogen*, wenn f gleich einem seiner homogenen Bestandteile ist, genauer *homogen vom Grad i*, wenn $f = f_i$ gilt. Ein homogenes Polynom $f \neq 0$ ist stets homogen von einem eindeutig bestimmten Grad $i \geq 0$, das Nullpolynom jedoch ist homogen von *jedem* Grad $i \geq 0$. Weiter heißt

$$\operatorname{grad} f = \max\{i \in \mathbb{N}\,;\, f_i \neq 0\} = \max\{|\mu|\,;\, a_\mu \neq 0\}$$

der *Totalgrad* von f, wobei $\operatorname{grad} f := -\infty$ gesetzt wird für $f = 0$. Im Falle einer Variablen stimmt der Totalgrad mit dem in 2.1 definierten Grad eines Polynoms überein. Analog zu 2.1/2 erhält man:

Satz 3. *Seien $f, g \in R[X_1, \ldots, X_n]$. Dann gilt*:

$$\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g),$$
$$\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g,$$

wobei man sogar $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$ *hat, falls R ein Integritätsring ist.*

Beweis. Die Abschätzung für $\operatorname{grad}(f+g)$ ist unmittelbar ersichtlich, wenn man Polynome in $R[X_1,\dots,X_n]$ als Summe ihrer homogenen Bestandteile schreibt. Gilt weiter $\operatorname{grad} f = r$ und $\operatorname{grad} g = s$, und sind $f = \sum_{i=0}^{r} f_i$, $g = \sum_{i=0}^{s} g_i$ Zerlegungen in homogene Bestandteile, so hat man für $r, s \geq 0$

$$f \cdot g = f_r \cdot g_s + (\text{homogene Bestandteile vom Grad } < r+s),$$

wobei $f_r \cdot g_s$ der homogene Bestandteil vom Grad $r+s$ in $f \cdot g$ ist. Somit folgt $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$. Ist R Integritätsring, so hat man mit $f_r, g_s \neq 0$ nach Satz 2 auch $f_r g_s \neq 0$, so dass sich der Grad von fg zu $r+s$ berechnet. □

Korollar 4. *Ist R ein Integritätsring, so gilt*

$$(R[X_1,\dots,X_n])^* = R^*.$$

Wir wollen schließlich noch die universelle Eigenschaft aus Satz 1, durch welche Polynomringe bis auf kanonische Isomorphie eindeutig charakterisiert sind, speziell für Polynomringe des Typs $R[X_1,\dots,X_n]$ formulieren. Da ein Monoidhomomorphismus $\sigma\colon \mathbb{N}^n \longrightarrow R'$ bereits durch die Bilder der kanonischen "Erzeugenden" von $\mathbb{N}^n$ eindeutig bestimmt ist, also durch die Bilder der Elemente des Typs $(0,\dots,0,1,0,\dots,0)$, erhält man aus Satz 1 folgende Version:

Satz 5. *Es sei $\varphi\colon R \longrightarrow R'$ ein Ringhomomorphismus, weiter seien Elemente $x_1,\dots,x_n \in R'$ gegeben. Dann existiert eindeutig ein Ringhomomorphismus $\Phi\colon R[X_1,\dots,X_n] \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X_i) = x_i$ für $i = 1,\dots,n$.*

Setzt man $x = (x_1,\dots,x_n)$ und $x^\mu = x_1^{\mu_1}\dots x_n^{\mu_n}$ für $\mu \in \mathbb{N}^n$, so lässt sich Φ wie im Falle einer Variablen durch

$$\Phi\colon R[X_1,\dots,X_n] \longrightarrow R', \qquad \sum a_\mu X^\mu \longmapsto \sum \varphi(a_\mu) x^\mu,$$

beschreiben. Man nennt Φ einen *Einsetzungs-* oder *Substitutionshomomorphismus*, da für X das Tupel x substituiert wird. Ist speziell R ein Unterring von R' und $\varphi\colon R \hookrightarrow R'$ die kanonische Inklusion, so bezeichnet man für $f = \sum a_\mu X^\mu \in R[X_1,\dots,X_n]$ das Bild unter Φ auch mit $f(x) = \sum a_\mu x^\mu$. Gilt $f(x) = 0$, so heißt x *Nullstelle* von f. Weiter benutzt man die Notation

$$R[x] := \Phi(R[X_1,\dots,X_n]) = \{\sum a_\mu x^\mu \,;\, a_\mu \in R, a_\mu = 0 \text{ für fast alle } \mu\}$$

für das Bild von $R[X_1,\dots,X_n]$ unter Φ. Es ist $R[x]$ oder in ausführlicher Schreibweise $R[x_1,\dots,x_n]$ der kleinste Unterring von R', welcher R und alle Komponenten $x_1,\dots,x_n$ von x enthält. In suggestiver Weise spricht man von $R[x]$ auch als von dem Ring aller Polynome in x (besser, aller polynomialen Ausdrücke in x), wobei R als Koeffizientenbereich dient.

Einsetzungshomomorphismen werden im weiteren Verlaufe eine wichtige Rolle spielen. Als Beispiel wollen wir bereits an dieser Stelle auf den Begriff der *Transzendenz* eingehen.

Definition 6. *Es sei $R \subset R'$ eine Ringerweiterung und $x = (x_1, \ldots, x_n)$ ein System von Elementen von R'. Das System x heißt* algebraisch unabhängig *oder* transzendent *über R, wenn für ein System $X = (X_1, \ldots, X_n)$ von Variablen der Ringhomomorphismus $R[X] \longrightarrow R'$, $f \longmapsto f(x)$, injektiv ist und somit einen Isomorphismus $R[X] \xrightarrow{\sim} R[x]$ induziert. Anderenfalls bezeichnet man x als* algebraisch abhängig.

Ein über R transzendentes System $x = (x_1, \ldots, x_n)$ hat somit die Eigenschaften eines Systems von Variablen. Wir haben bereits in der Einführung erwähnt, dass z. B. die aus der Analysis bekannten Zahlen e und $\pi \in \mathbb{R}$ jeweils transzendent über $\mathbb{Q}$ sind; Beweise hierfür gehen zurück auf Ch. Hermite [7] und F. Lindemann [12].

Schließlich wollen wir noch auf die *Reduktion der Koeffizienten* von Polynomen hinweisen. Es handelt sich dabei um Homomorphismen, die formal auch unter den Typus der Einsetzungshomomorphismen fallen. Ist $\mathfrak{a} \subset R$ ein Ideal und $\varphi\colon R \longrightarrow R/\mathfrak{a}$ der kanonische Homomorphismus, so kann man gemäß Satz 5 den Homomorphismus $\Phi\colon R[X] \longrightarrow (R/\mathfrak{a})[X]$ betrachten, der φ fortsetzt und X auf X abbildet. Man sagt, dass Φ die Koeffizienten von Polynomen aus $R[X]$ modulo dem Ideal $\mathfrak{a}$ reduziert. So führt etwa für eine Primzahl p der Homomorphismus $\mathbb{Z}[X] \longrightarrow \mathbb{Z}/(p)[X]$ Polynome mit ganzzahligen Koeffizienten über in Polynome mit Koeffizienten aus dem Körper $\mathbb{F}_p = \mathbb{Z}/(p)$.

Aufgaben

1. *Wir haben für ein kommutatives Monoid M den Polynomring $R[M]$ über einem Ring R definiert. Was ist zu beachten, wenn man $R[M]$ auch für nicht notwendig kommutative Monoide M erklären möchte?*
2. *Man untersuche, inwieweit sich die in diesem Abschnitt bewiesenen Resultate für Polynomringe der Form $R[X_1, \ldots, X_n]$ auf Polynomringe in beliebig vielen Variablen $R[\mathfrak{X}]$ verallgemeinern lassen.*
3. *Für zwei Monoide M, M' betrachte man das kartesische Produkt $M \times M'$ als Monoid unter komponentenweiser Verknüpfung. Man zeige, dass es einen kanonischen Ringisomorphismus $R[M][M'] \xrightarrow{\sim} R[M \times M']$ gibt.*
4. Es sei R ein Ring. Man betrachte $\mathbb{Z}$ sowie $\mathbb{Z}/m\mathbb{Z}$ für $m > 0$ jeweils als Monoid unter der Addition und zeige:
$$R[\mathbb{Z}] \simeq R[X, Y]/(1 - XY), \qquad R[\mathbb{Z}/m\mathbb{Z}] \simeq R[X]/(X^m - 1).$$
5. Sei K ein Körper und $f \in K[X_1, \ldots, X_n]$ ein homogenes Polynom vom Totalgrad $d > 0$. Man zeige, dass für jede Primfaktorzerlegung $f = p_1 \ldots p_r$ die Faktoren p_i homogen sind.
6. Man betrachte den Polynomring $R[X_1, \ldots, X_n]$ in n Variablen über einem Ring $R \neq 0$ und zeige: Die Anzahl der Monome in $R[X_1, \ldots, X_n]$ vom Totalgrad $d \in \mathbb{N}$ ist
$$\binom{n + d - 1}{n - 1}.$$

7. Sei K ein Körper und $\varphi\colon K[X_1,\dots,X_m] \longrightarrow K[X_1,\dots,X_n]$ ein Ringisomorphismus mit $\varphi|_K = \mathrm{id}_K$. Man zeige, es gilt $m = n$.

2.6 Nullstellen von Polynomen

Es sei K ein Körper und $f \in K[X]$ ein von Null verschiedenes Polynom einer Variablen X. Ist $\alpha \in K$ Nullstelle von f, so ist das Polynom $X - \alpha$ ein Teiler von f. Denn Division mit Rest von f durch $X - \alpha$ ergibt eine Gleichung

$$f = q \cdot (X - \alpha) + r$$

mit $\operatorname{grad} r < 1$, also $r \in K$, und Einsetzen von α zeigt $r = 0$. Es heißt α eine *Nullstelle der Vielfachheit* r, wenn $X - \alpha$ in der Primfaktorzerlegung von f genau mit r-ter Potenz vorkommt. Somit folgt aus Gradgründen:

Satz 1. *Es sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geq 0$. Dann hat f, gezählt mit Vielfachheiten, höchstens n Nullstellen in K. Die Anzahl ist genau dann gleich n, wenn f in $K[X]$ vollständig in Linearfaktoren zerfällt.*

Insbesondere folgt, dass ein Polynom, welches mehr Nullstellen hat, als sein Grad angibt, bereits das Nullpolynom sein muss. Ist daher K ein unendlicher Körper, so ist für ein Polynom $f \in K[X]$ die Gleichung $f = 0$ (Nullpolynom) äquivalent zu $f(\alpha) = 0$ für alle $\alpha \in K$ (bzw. für alle α aus einer gegebenen unendlichen Teilmenge von K). Dagegen ist für einen endlichen Körper $\mathbb{F}$ das Polynom

$$f = \prod_{a \in \mathbb{F}} (X - a) \in \mathbb{F}[X]$$

ein vom Nullpolynom verschiedenes Polynom mit $f(\alpha) = 0$ für alle $\alpha \in \mathbb{F}$.

Wir wollen ein Kriterium für das Vorliegen mehrfacher Nullstellen angeben. Man betrachte hierzu die Abbildung

$$D\colon K[X] \longrightarrow K[X], \qquad \sum_{i=0}^{n} c_i X^i \longmapsto \sum_{i=1}^{n} i c_i X^{i-1},$$

welche wie die gewöhnliche Differentiation definiert ist (man interpretiere ic_i wie üblich als die i-fache Summe von c_i mit sich selbst). Es ist D kein Ringhomomorphismus, sondern eine so genannte *Derivation*, d. h. D erfüllt folgende Regeln für $a, b \in K$, $f, g \in K[X]$:

$$D(af + bg) = aD(f) + bD(g), \qquad D(fg) = fD(g) + gD(f).$$

Statt Df schreibt man meist f' und nennt dies die erste *Ableitung* von f.

Satz 2. *Es sei $f \in K[X]$, $f \neq 0$, ein Polynom mit Koeffizienten aus einem Körper K. Eine Nullstelle α von f ist genau dann eine mehrfache Nullstelle (d. h. eine Nullstelle der Vielfachheit ≥ 2), wenn $(f')(\alpha) = 0$ gilt.*

Beweis. Ist r die Vielfachheit der Nullstelle α, so gibt es eine Zerlegung des Typs $f = (X - \alpha)^r g$ mit $g \in K[X]$, $g(\alpha) \neq 0$. Wegen

$$f' = (X - \alpha)^r g' + r(X - \alpha)^{r-1} g$$

ist $(f')(\alpha) = 0$ äquivalent zu $r \geq 2$. □

Korollar 3. *Ein Element $\alpha \in K$ ist genau dann eine mehrfache Nullstelle eines Polynoms $f \in K[X] - \{0\}$, wenn α Nullstelle von $\mathrm{ggT}(f, f')$ ist.*

Ist z. B. p eine Primzahl, so hat das Polynom $f = X^p - X \in \mathbb{F}_p[X]$ keine mehrfachen Nullstellen. Denn es gilt $f' = -1$, da die p-fache Summe $p \cdot 1$ des Einselementes $1 \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ verschwindet.

Aufgaben

1. *Sei K ein Körper mit unendlich vielen Elementen und $f \in K[X_1, \ldots, X_n]$ ein Polynom, welches auf K^n verschwindet. Man zeige $f = 0$, d. h. f ist das Nullpolynom.*
2. Sei K ein Körper. Man zeige: Zu $n \in \mathbb{N}$, $n > 1$, gibt es in der multiplikativen Gruppe K^* höchstens $n - 1$ Elemente der Ordnung n.
3. Sei K ein Körper. Man zeige, es gibt im Polynomring $K[X]$ unendlich viele normierte Primpolynome. Für den Fall, dass jedes nicht-konstante Polynom aus $K[X]$ mindestens eine Nullstelle in K besitzt, zeige man weiter, dass K aus unendlich vielen Elementen besteht.
4. Sei K ein Körper und sei $f = X^3 + aX + b \in K[X]$ ein Polynom, welches in $K[X]$ vollständig in Linearfaktoren zerfällt. Man zeige: Die Nullstellen von f sind genau dann paarweise verschieden, wenn die "Diskriminante" $\Delta = -4a^3 - 27b^2$ nicht verschwindet.

2.7 Der Satz von Gauß

Ziel dieses Abschnittes ist der Beweis des folgenden Resultats:

Satz 1 (Gauß). *Es sei R ein faktorieller Ring. Dann ist auch der Polynomring in einer Variablen $R[X]$ faktoriell.*

Als direkte Folgerungen erhält man:

Korollar 2. *Ist R ein faktorieller Ring, so ist der Polynomring $R[X_1, \ldots, X_n]$ faktoriell.*

Korollar 3. *Ist K ein Körper, so ist der Polynomring $K[X_1, \ldots, X_n]$ faktoriell.*

Insbesondere sieht man, dass es faktorielle Ringe gibt, die keine Hauptidealringe sind; man betrachte beispielsweise den Polynomring $K[X, Y]$ in zwei Variablen X, Y über einem Körper K oder den Polynomring einer Variablen $\mathbb{Z}[X]$. Zum Beweis des Satzes von Gauß sind einige Vorbereitungen notwendig. Wir beginnen mit der Konstruktion des *Quotientenkörpers* $Q(R)$ eines Integritätsringes R, wobei wir uns an der Konstruktion rationaler Zahlen als Brüche ganzer Zahlen orientieren. Man betrachte die Menge aller Paare

$$M = \{(a, b)\,;\, a \in R, b \in R - \{0\}\}.$$

Auf M führen wir eine Äquivalenzrelation "$\sim$" ein, indem wir setzen

$$(a, b) \sim (a', b') \quad \Longleftrightarrow \quad ab' = a'b.$$

Die Eigenschaften einer Äquivalenzrelation prüft man leicht nach; es gelten

$$\begin{aligned}
&\text{Reflexivität:} && (a, b) \sim (a, b) \ \text{ für alle } (a, b) \in M,\\
&\text{Symmetrie:} && (a, b) \sim (a', b') \implies (a', b') \sim (a, b),\\
&\text{Transitivität:} && (a, b) \sim (a', b'),\ (a', b') \sim (a'', b'') \implies (a, b) \sim (a'', b'').
\end{aligned}$$

Zum Nachweis der Transitivität etwa führt man folgende Rechnung durch:

$$\begin{aligned}
ab' = a'b \quad &\Longrightarrow \quad ab'b'' = a'bb'',\\
a'b'' = a''b' \quad &\Longrightarrow \quad a'bb'' = a''bb',
\end{aligned}$$

also

$$ab' = a'b,\ a'b'' = a''b' \quad \Longrightarrow \quad ab'b'' = a''bb'.$$

Da R ein Integritätsring ist, ergibt letztere Gleichung $ab'' = a''b$, also $(a, b) \sim (a'', b'')$.

Somit definiert die Äquivalenzrelation "$\sim$" eine Klasseneinteilung auf M; es sei

$$Q(R) = M/\sim$$

die Menge der Äquivalenzklassen. Für $(a, b) \in M$ bezeichne $\frac{a}{b} \in Q(R)$ die zugehörige Äquivalenzklasse, so dass

$$\frac{a}{b} = \frac{a'}{b'} \quad \Longleftrightarrow \quad ab' = a'b$$

gilt. Man rechnet sofort nach, dass $Q(R)$ unter der gewöhnlichen Addition und Multiplikation von Brüchen

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'},$$

deren Wohldefiniertheit man wie üblich zeigt, ein Körper ist. Es wird $Q(R)$ als *Quotientenkörper* zu R bezeichnet. Weiter ist

$$R \longrightarrow Q(R), \qquad a \longmapsto \frac{a}{1},$$

ein injektiver Ringhomomorphismus, man kann also R als Unterring von $Q(R)$ auffassen. Für $R = \mathbb{Z}$ erhält man bekanntermaßen $Q(\mathbb{Z}) = \mathbb{Q}$, also den Körper der rationalen Zahlen. Ist K ein Körper und X eine Variable, so bezeichnet man den Quotientenkörper $Q(K[X])$ als *Körper der rationalen Funktionen* einer Variablen X mit Koeffizienten in K und schreibt $Q(K[X]) = K(X)$. Analog betrachtet man rationale Funktionenkörper $K(X_1, \ldots, X_n) = Q(K[X_1, \ldots, X_n])$ in endlich vielen Variablen $X_1, \ldots, X_n$ sowie allgemeiner den Funktionenkörper $K(\mathfrak{X}) = Q(K[\mathfrak{X}])$ in einem System von Variablen $\mathfrak{X} = (X_i)_{i \in I}$.

Die gerade beschriebene Konstruktion des Quotientenkörpers eines Integritätsringes kann in einem allgemeineren Rahmen durchgeführt werden. Man starte mit einem (nicht notwendig nullteilerfreien) Ring R und einem multiplikativen System $S \subset R$, d. h. mit einem multiplikativen Untermonoid von R. Dann kann man ähnlich wie oben den *Bruchring* (im Allgemeinen erhält man keinen Körper)

$$S^{-1}R = \{\frac{a}{s}\,;\, a \in R, s \in S\}$$

bilden, wobei man wegen möglicher Nullteiler bezüglich folgender Äquivalenzrelation arbeitet:

$$\frac{a}{s} = \frac{a'}{s'} \quad \Longleftrightarrow \quad \text{es existiert } s'' \in S \text{ mit } as's'' = a'ss''$$

Man schreibt statt $S^{-1}R$ auch R_S und nennt dies die *Lokalisierung* von R nach S. Dabei ist zu beachten, dass die kanonische Abbildung $R \longrightarrow S^{-1}R$ im Allgemeinen einen nicht-trivialen Kern besitzt. Dieser besteht aus allen Elementen $a \in R$, so dass ein $s \in S$ existiert mit $as = 0$. Im Falle eines Integritätsrings R (dies ist die Situation, die wir im Folgenden hauptsächlich zu betrachten haben) hat man $Q(R) = S^{-1}R$ für $S := R - \{0\}$.

Bemerkung 4. *Es sei R ein faktorieller Ring, P ein Repräsentantensystem der Primelemente von R. Dann besitzt jedes $\frac{a}{b} \in Q(R)^*$ eine eindeutige Darstellung*

$$\frac{a}{b} = \varepsilon \prod_{p \in P} p^{\nu_p},$$

wobei $\varepsilon \in R^*$ sowie $\nu_p \in \mathbb{Z}$ mit $\nu_p = 0$ für fast alle p. Insbesondere ist $\frac{a}{b} \in R$ äquivalent zu $\nu_p \geq 0$ für alle p.

Beweis. Unter Benutzung der Primfaktorzerlegung für a und b erhält man die Existenz der geforderten Darstellung. Die Eindeutigkeit ergibt sich aus der Eindeutigkeit der Primfaktorzerlegung in R, sofern man Zerlegungen mit $\nu_p \geq 0$ für alle p betrachtet. Auf diesen Fall kann man sich aber durch Erweiterung der Brüche, die man zu betrachten hat, beschränken. □

In der Situation von Bemerkung 4 schreiben wir anstelle von ν_p genauer $\nu_p(x)$, falls $x = \frac{a}{b}$, und setzen $\nu_p(0) := \infty$. Für $x, y \in Q(R)$ erhält man dann mit der Eindeutigkeitsaussage in Bemerkung 4 die Gleichung

$$\nu_p(xy) = \nu_p(x) + \nu_p(y).$$

Weiter setzen wir für Polynome einer Variablen $f = \sum a_i X^i \in Q(R)[X]$

$$\nu_p(f) := \min_i \nu_p(a_i),$$

wobei $f = 0$ äquivalent zu $\nu_p(f) = \infty$ ist. Außerdem gehört f genau dann zu $R[X]$, wenn $\nu_p(f) \geq 0$ für alle $p \in P$ gilt. Die folgende Eigenschaft der Funktion $\nu_p(\cdot)$ wird beim Beweis der Faktorialität von $R[X]$ an zentraler Stelle benötigt:

Lemma 5 (Gauß). *Es sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für $f, g \in Q(R)[X]$*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g).$$

Beweis. Wie bereits oben bemerkt, ist die Gleichung für konstante Polynome richtig, d. h. für $f, g \in Q(R)$, ja sogar für $f \in Q(R)$ und beliebiges $g \in Q(R)[X]$.

Zum Beweis des Allgemeinfalles darf man $f, g \neq 0$ annehmen. Aufgrund unserer Vorüberlegung darf man weiter ohne Beschränkung der Allgemeinheit f und g mit Konstanten aus $Q(R)^*$ multiplizieren. So kann man sich die Koeffizienten von f als Brüche vorstellen und f mit dem kleinsten gemeinsamen Vielfachen aller auftretenden Nenner multiplizieren, entsprechend für g. Auf diese Weise kann man annehmen, dass f und g Polynome mit Koeffizienten aus R sind. Dividiert man dann noch jeweils durch den größten gemeinsamen Teiler der Koeffizienten von f bzw. g, so erhält man folgende Situation:

$$f, g \in R[X], \qquad \nu_p(f) = 0 = \nu_p(g),$$

und es ist $\nu_p(fg) = 0$ zu zeigen. Hierzu betrachte man den Homomorphismus

$$\Phi\colon R[X] \longrightarrow (R/pR)[X],$$

welcher die Koeffizienten reduziert. Es besteht $\ker \Phi$ aus allen denjenigen Polynomen in $R[X]$, deren Koeffizienten sämtlich durch p teilbar sind, also

$$\ker \Phi = \{f \in R[X]\,;\, \nu_p(f) > 0\}.$$

Wegen $\nu_p(f) = 0 = \nu_p(g)$ hat man dann $\Phi(f), \Phi(g) \neq 0$. Da mit R/pR nach 2.1/3 auch $(R/pR)[X]$ ein Integritätsring ist, folgt

$$\Phi(fg) = \Phi(f) \cdot \Phi(g) \neq 0,$$

also $\nu_p(fg) = 0$. □

Korollar 6. *Es sei R ein faktorieller Ring und $h \in R[X]$ ein normiertes Polynom. Ist dann $h = f \cdot g$ eine Zerlegung von h in normierte Polynome $f, g \in Q(R)[X]$, so gilt bereits $f, g \in R[X]$.*

Beweis. Für jedes Primelement $p \in R$ gilt $\nu_p(h) = 0$ sowie $\nu_p(f), \nu_p(g) \leq 0$ aufgrund der Normiertheit von f und g. Aus dem Lemma von Gauß ergibt sich weiter

$$\nu_p(f) + \nu_p(g) = \nu_p(h) = 0,$$

so dass sogar $\nu_p(f) = \nu_p(g) = 0$ für alle p und damit $f, g \in R[X]$ folgt. □

Wir nennen ein Polynom $f \in R[X]$ mit Koeffizienten aus einem faktoriellen Ring R *primitiv*, wenn der größte gemeinsame Teiler aller Koeffizienten von f gleich 1 ist, d. h. wenn $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt. Beispielsweise sind normierte Polynome in $R[X]$ primitiv. Auch können wir ähnlich wie in Korollar 6 für ein Polynom $h \in R[X]$ und eine Zerlegung $h = f \cdot g$ in ein primitives Polynom $f \in R[X]$ und ein weiteres Polynom $g \in Q(R)[X]$ bereits $g \in R[X]$ schließen.

Wir werden im Folgenden häufiger benutzen, dass sich jedes von 0 verschiedene Polynom $f \in Q(R)[X]$ in der Form $f = a\tilde{f}$ mit einer Konstanten $a \in Q(R)^*$ und einem primitiven Polynom $\tilde{f} \in R[X]$ schreiben lässt. Man setze nämlich

$$a = \prod_{p \in P} p^{\nu_p(f)}, \qquad \tilde{f} = a^{-1} f,$$

wobei P ein Repräsentantensystem der Primelemente in R sei.

Nach diesen Vorbereitungen sind wir nunmehr in der Lage, den eingangs angekündigten Satz von Gauß zu beweisen, wobei wir gleichzeitig auch die Primelemente in $R[X]$ charakterisieren wollen.

Satz 7 (Gauß). *Es sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell. Ein Polynom $q \in R[X]$ ist genau dann ein Primelement in $R[X]$, wenn gilt:*

(i) *q ist Primelement in R oder*

(ii) *q ist primitiv in $R[X]$ und Primelement in $Q(R)[X]$.*

Insbesondere ist ein primitives Polynom $q \in R[X]$ genau dann prim in $R[X]$, wenn es prim in $Q(R)[X]$ ist.

Beweis. Sei zunächst q ein Primelement in R. Dann ist R/qR und somit auch $R[X]/qR[X] \simeq (R/qR)[X]$ ein Integritätsring, woraus folgt, dass q ein Primelement in $R[X]$ ist.

Als Nächstes betrachte man ein primitives Polynom $q \in R[X]$ mit der Eigenschaft, dass q ein Primelement in $Q(R)[X]$ ist. Um nachzuweisen, dass q auch Primelement in $R[X]$ ist, betrachte man $f, g \in R[X]$ mit $q \mid fg$ in $R[X]$. Dann gilt auch $q \mid fg$ in $Q(R)[X]$. Als Primelement in $Q(R)[X]$ teilt q einen der beiden Faktoren, etwa $q \mid f$, und es existiert ein $h \in Q(R)[X]$ mit $f = qh$. Auf letztere Gleichung wenden wir das Lemma von Gauß an. Da q primitiv ist, folgt für jedes Primelement $p \in R$

$$0 \leq \nu_p(f) = \nu_p(q) + \nu_p(h) = \nu_p(h)$$

und somit $h \in R[X]$, also $q \,|\, f$ in $R[X]$. Insbesondere ist q ein Primelement in $R[X]$.

Es bleibt jetzt noch nachzuweisen, dass $R[X]$ faktoriell ist und dass jedes Primelement in $R[X]$ vom Typ (i) bzw. (ii) ist. Hierfür reicht es, zu zeigen, dass jedes $f \in R[X]$, welches keine Einheit und nicht Null ist, in ein Produkt von Primelementen der gerade diskutierten Gestalt zerfällt. Um dies einzusehen, schreibe man f in der Gestalt $f = a\tilde{f}$, wobei $a \in R$ der größte gemeinsame Teiler aller Koeffizienten von f ist und $\tilde{f}$ folglich primitiv ist. Da a ein Produkt von Primelementen aus R ist, genügt es, zu zeigen, dass das primitive Polynom $\tilde{f}$ Produkt von primitiven Polynomen aus $R[X]$ ist, die prim in $Q(R)[X]$ sind. Sei $\tilde{f} = c\tilde{f}_1 \dots \tilde{f}_r$ eine Zerlegung in Primelemente aus $Q(R)[X]$, mit einer Konstanten $c \in Q(R)^*$. Nach geeigneter Wahl von c dürfen wir alle $\tilde{f}_i$ als primitiv in $R[X]$ voraussetzen. Dann gilt aufgrund des Lemmas von Gauß für jedes Primelement $p \in R$

$$\nu_p(\tilde{f}) = \nu_p(c) + \nu_p(\tilde{f}_1) + \dots + \nu_p(\tilde{f}_r)$$

und wegen

$$\nu_p(\tilde{f}) = \nu_p(\tilde{f}_1) = \dots = \nu_p(\tilde{f}_r) = 0$$

auch $\nu_p(c) = 0$; d. h. c ist Einheit in R. Ersetzt man nun $\tilde{f}_1$ durch $c\tilde{f}_1$, so sieht man, dass $\tilde{f}$ ein Produkt von Primelementen der gewünschten Form ist. □

Aufgaben

1. *Sei R ein faktorieller Ring und $\Phi\colon R[X] \longrightarrow R[X]$ ein Ringautomorphismus, der sich zu einem Automorphismus $\varphi\colon R \longrightarrow R$ beschränkt. Man vergleiche $\nu_p(f)$ mit $\nu_{\varphi(p)}(\Phi(f))$ für Polynome $f \in R[X]$ und Primelemente $p \in R$ und überlege, ob $\Phi(f)$ primitiv ist, wenn f primitiv ist. Man zeige für $a \in R$, dass ein Polynom f genau dann primitiv ist, wenn $f(X + a)$ primitiv ist.*

2. *Es sei R ein faktorieller Ring mit Quotientenkörper K und einem Repräsentantensystem von Primelementen P. Für $f \in K[X] - \{0\}$ bezeichne man mit $a_f := \prod_{p \in P} p^{\nu_p(f)}$ den "Inhalt" von f. Man formuliere die Aussage des Lemmas von Gauß (Lemma 5) in äquivalenter Form unter Benutzung des Inhalts.*

3. Man betrachte den rationalen Funktionenkörper $K(X)$ einer Variablen X über einem Körper K, sowie für eine Variable Y den Polynomring $K(X)[Y]$. Weiter seien $f(Y), g(Y) \in K[Y]$ teilerfremd mit $\operatorname{grad} f(Y) \cdot g(Y) \geq 1$. Man zeige, dass $f(Y) - g(Y)X$ irreduzibel in $K(X)[Y]$ ist.

4. Es sei R ein faktorieller Ring. Man zeige:
   (i) Ist $S \subset R$ ein multiplikatives System, so ist auch der Bruchring $S^{-1}R$ faktoriell. Wie verhalten sich die Primelemente von R zu denen von $S^{-1}R$?
   (ii) Für Primelemente $p \in R$ setze man $R_p := S_p^{-1}R$ mit $S_p = R - (p)$. Ein Polynom $f \in R[X]$ ist genau dann primitiv, wenn für jedes Primelement $p \in R$ das induzierte Polynom $f_p \in R_p[X]$ primitiv ist.

5. Universelle Eigenschaft der Bruchringe: Sei R ein Ring und $S \subset R$ ein multiplikatives System. Man zeige: Zu jedem Ringhomomorphismus $\varphi\colon R \longrightarrow R'$ mit $\varphi(S) \subset R'^*$ gibt es genau einen Ringhomomorphismus $\overline{\varphi}\colon S^{-1}R \longrightarrow R'$ mit $\varphi = \overline{\varphi} \circ \tau$; dabei bezeichne $\tau\colon R \longrightarrow S^{-1}R$ den kanonischen Homomorphismus, gegeben durch $a \longmapsto \frac{a}{1}$.
6. Partialbruchzerlegung: Es seien $f, g \in K[X]$ Polynome mit Koeffizienten aus einem Körper K, wobei g normiert sei mit Primfaktorzerlegung $g = g_1^{\nu_1} \dots g_n^{\nu_n}$ und paarweise nicht-assoziierten Primelementen $g_1, \dots, g_n$. Man zeige, dass es im Quotientenkörper $K(X) = Q(K[X])$ eine eindeutige Darstellung

$$\frac{f}{g} = f_0 + \sum_{i=1}^{n} \sum_{j=1}^{\nu_i} \frac{c_{ij}}{g_i^j}$$

mit Polynomen $f_0, c_{ij} \in K[X]$ gibt, wobei $\operatorname{grad} c_{ij} < \operatorname{grad} g_i$. Sind insbesondere die Primfaktoren g_i linear, so haben die c_{ij} Grad 0, sind also Konstanten. (Man beweise zunächst die Existenz einer Darstellung $fg^{-1} = f_0 + \sum_{i=1}^{n} f_i g_i^{-\nu_i}$ mit $g_i \nmid f_i$ und $\operatorname{grad} f_i < \operatorname{grad} g_i^{\nu_i}$ und wende dann auf f_i die g_i-adische Entwicklung an, siehe Aufgabe 4 aus 2.1.)

2.8 Irreduzibilitätskriterien

Es sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper. Wir wollen im Folgenden untersuchen, unter welchen Umständen ein gegebenes Polynom $f \in K[X] - \{0\}$ irreduzibel ist (bzw. prim, was in faktoriellen Ringen nach 2.4/10 ja dasselbe bedeutet). Man kann zu f stets ein $c \in K^*$ wählen, so dass $\tilde{f} = cf$ ein primitives Polynom in $R[X]$ ist, und es folgt mit dem Satz von Gauß 2.7/7, dass f bzw. $\tilde{f}$ genau dann irreduzibel in $K[X]$ ist, wenn $\tilde{f}$ irreduzibel in $R[X]$ ist. Somit kann die Irreduzibilität von Polynomen in $K[X]$ auf die Irreduzibilität von primitiven Polynomen in $R[X]$ zurückgeführt werden.

Satz 1 (Eisensteinsches Irreduzibilitätskriterium). *Es sei R ein faktorieller Ring und $f = a_n X^n + \dots + a_0 \in R[X]$ ein primitives Polynom vom Grad > 0. Weiter sei $p \in R$ ein Primelement mit*

$$p \nmid a_n, \qquad p \mid a_i \ \text{ für } \ i < n, \qquad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $R[X]$ und somit gemäß 2.7/7 auch in $Q(R)[X]$.

Beweis. Angenommen, f ist reduzibel in $R[X]$. Dann gibt es eine Zerlegung

$$f = gh \quad \text{mit} \quad g = \sum_{i=0}^{r} b_i X^i, \ h = \sum_{i=0}^{s} c_i X^i,$$

wobei $r + s = n$, $r > 0$, $s > 0$. Es folgt

$$\begin{aligned} a_n &= b_r c_s \neq 0, & p \nmid b_r, \qquad & p \nmid c_s, \\ a_0 &= b_0 c_0, & p \mid b_0 c_0, \qquad & p^2 \nmid b_0 c_0, \end{aligned}$$

und wir dürfen etwa $p \mid b_0$, $p \nmid c_0$ annehmen. Es sei nun $t < r$ maximal mit $p \mid b_\tau$ für $0 \leq \tau \leq t$. Setzen wir $b_i = 0$ für $i > r$ und $c_i = 0$ für $i > s$, so gilt

$$a_{t+1} = b_0 c_{t+1} + \ldots + b_{t+1} c_0,$$

und es ist a_{t+1} nicht durch p teilbar, denn $b_0 c_{t+1}, \ldots, b_t c_1$ sind durch p teilbar, nicht aber $b_{t+1} c_0$. Es folgt notwendig $t+1 = n$, aufgrund unserer Voraussetzung über f, und somit $r = n$, $s = 0$ im Widerspruch zu $s > 0$. □

Weiter wollen wir das so genannte *Reduktionskriterium* beweisen.

Satz 2. *Es sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f \in R[X]$ ein Polynom vom Grad > 0, dessen höchster Koeffizient nicht von p geteilt wird. Weiter sei $\Phi\colon R[X] \longrightarrow R/(p)[X]$ der kanonische Homomorphismus, welcher die Koeffizienten reduziert. Dann gilt*:

Ist $\Phi(f)$ irreduzibel in $R/(p)[X]$, so ist f irreduzibel in $Q(R)[X]$. Ist f zusätzlich primitiv, so ist f irreduzibel in $R[X]$.

Beweis. Wir nehmen zunächst $f \in R[X]$ als primitiv an. Ist dann f reduzibel, so gibt es in $R[X]$ eine Zerlegung $f = gh$ mit $\operatorname{grad} g > 0$ und $\operatorname{grad} h > 0$. Dabei kann p nicht den höchsten Koeffizienten von g bzw. h teilen, da p nicht den höchsten Koeffizienten von f teilt. Also gilt

$$\Phi(f) = \Phi(g)\Phi(h)$$

mit nicht-konstanten Polynomen $\Phi(g)$ und $\Phi(h)$, d. h. es ist $\Phi(f)$ reduzibel. Somit impliziert die Irreduzibilität von $\Phi(f)$ diejenige von f in $R[X]$.

Im Allgemeinfall schreiben wir $f = c \cdot \tilde{f}$ mit einer Konstanten $c \in R$ und einem primitiven Polynom $\tilde{f} \in R[X]$, wobei p weder c noch den höchsten Koeffizienten von $\tilde{f}$ teilen kann. Ist dann $\Phi(f)$ irreduzibel, so auch $\Phi(\tilde{f})$, und es folgt, wie wir gerade gesehen haben, dass $\tilde{f}$ irreduzibel in $R[X]$ ist. Hieraus schließt man mit dem Satz von Gauß 2.7/7, dass $\tilde{f}$ und damit auch f irreduzibel in $Q(R)[X]$ sind. □

Man kann übrigens das Eisensteinsche Irreduzibilitätskriterium auch mittels des Reduktionskriteriums beweisen. Hat man nämlich in der Situation von Satz 1 eine Zerlegung $f = gh$ mit Polynomen $g, h \in R[X]$ vom Grad $< n$, so können wir den Reduktionshomomorphismus $\Phi\colon R[X] \longrightarrow R/(p)[X]$ anwenden und erhalten die Gleichung $\overline{a}_n X^n = \Phi(f) = \Phi(g)\Phi(h)$. Hieraus erkennt man, dass $\Phi(g)$ und $\Phi(h)$, abgesehen von einem konstanten Faktor aus $R/(p)$, jeweils nicht-triviale Potenzen von X sind. Man kann nämlich die vorstehende Zerlegung in dem Polynomring $k[X]$ über dem Quotientenkörper k zu $R/(p)$ betrachten, der faktoriell ist. Somit ist der konstante Term von g und h jeweils durch p teilbar, und es folgt, dass der konstante Term von f durch p^2 teilbar ist, im Widerspruch zur Wahl von f.

Wir wollen noch einige konkrete Beispiele für die Anwendung der Irreduzibilitätskriterien angeben:

(1) Es sei k ein Körper, $K := k(t)$ der Körper der rationalen Funktionen in einer Variablen t über k. Dann ist für $n \geq 1$ das Polynom $X^n - t \in K[X]$ irreduzibel. Es ist nämlich $R := k[t]$ faktoriell, $t \in R$ prim und $X^n - t$ ein primitives Polynom in $R[X]$, so dass man das Eisensteinsche Kriterium mit $p := t$ anwenden kann.

(2) Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $f(X) = X^{p-1} + \ldots + 1$ irreduzibel in $\mathbb{Q}[X]$. Zum Nachweis können wir das Eisensteinsche Kriterium auf das Polynom $f(X+1)$ anwenden, wobei $f(X+1)$ genau dann irreduzibel ist, wenn dies für $f(X)$ gilt. Man hat

$$f(X) = \frac{X^p - 1}{X - 1},$$
$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1}.$$

Die Voraussetzungen des Eisensteinschen Kriteriums sind erfüllt, da $\binom{p}{p-1} = p$ sowie $p \mid \binom{p}{\nu}$ für $\nu = 1, \ldots, p-1$ gilt; dabei beachte man, dass

$$\binom{p}{\nu} = \frac{p(p-1)\ldots(p-\nu+1)}{1\ldots\nu}$$

für $\nu = 1, \ldots, p-1$ im Zähler einen Primfaktor p besitzt, im Nenner aber nicht, also durch p teilbar ist.

(3) $f = X^3 + 3X^2 - 4X - 1$ ist irreduzibel in $\mathbb{Q}[X]$. Man fasse f als primitives Polynom in $\mathbb{Z}[X]$ auf und reduziere die Koeffizienten modulo 3. Es bleibt dann zu zeigen, dass das Polynom

$$X^3 - X - 1 \in \mathbb{F}_3[X]$$

irreduzibel ist, was man elementar nachprüfen kann. Allgemeiner kann man zeigen (vgl. Aufgabe 2), dass für p prim das Polynom $X^p - X - 1$ irreduzibel in $\mathbb{F}_p[X]$ ist.

Aufgaben

1. Man zeige, dass folgende Polynome irreduzibel sind:
   (i) $X^4 + 3X^3 + X^2 - 2X + 1 \in \mathbb{Q}[X]$.
   (ii) $2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$.
   (iii) $X^2Y + XY^2 - X - Y + 1 \in \mathbb{Q}[X, Y]$.
2. Sei $p \in \mathbb{N}$ eine Primzahl. Man zeige, dass das Polynom $g = X^p - X - 1$ irreduzibel in $\mathbb{F}_p[X]$ ist. (g ist invariant unter dem Automorphismus $\tau\colon \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]$, $f(X) \longmapsto f(X+1)$; man lasse τ auf die Primfaktorzerlegung von g wirken.)

2.9 Elementarteilertheorie*

Als Verallgemeinerung von Vektorräumen über Körpern wollen wir in diesem Abschnitt Moduln über Ringen, speziell über Hauptidealringen, studieren. Wie wir sogleich sehen werden, sind abelsche Gruppen Beispiele für $\mathbb{Z}$-Moduln, also für Moduln über dem Ring $\mathbb{Z}$. Überhaupt ist das Studium abelscher Gruppen, insbesondere die Klassifikation endlich erzeugter abelscher Gruppen, eine nahe liegende Motivation für die hier präsentierte Theorie. Der Hauptsatz für endlich erzeugte Moduln über Hauptidealringen, der diese Klassifikation liefert, lässt aber auch noch andere interessante Anwendungen zu. Er enthält z. B. als Spezialfall die Normalformentheorie für Endomorphismen endlich-dimensionaler Vektorräume; vgl. Aufgabe 3. Wir werden im Folgenden als zentrales Resultat den so genannten Elementarteilersatz beweisen. Dieser klärt die Struktur endlich-rangiger Untermoduln von freien Moduln mit Koeffizienten aus einem Hauptidealring. Als Korollar ergibt sich der oben genannte Hauptsatz.

Es sei im Folgenden A zunächst ein beliebiger Ring, später dann ein Hauptidealring. Ein *A-Modul* ist eine abelsche Gruppe M, zusammen mit einer Multiplikation

$$A \times M \longrightarrow M, \qquad (a, x) \longmapsto a \cdot x,$$

die den üblichen "Vektorraum-Axiomen"

$$\begin{aligned} a \cdot (x + y) &= a \cdot x + a \cdot y, \\ (a + b) \cdot x &= a \cdot x + b \cdot x, \\ a \cdot (b \cdot x) &= (ab) \cdot x, \\ 1 \cdot x &= x, \end{aligned}$$

für $a, b \in A$, $x, y \in M$ genügt. *Homomorphismen* zwischen A-Moduln, auch *A-Homomorphismen* genannt, werden ebenso wie in der Theorie der Vektorräume definiert, desgleichen *Untermoduln* eines A-Moduls M sowie der *Restklassenmodul* M/N eines A-Moduls M nach einem Untermodul N. Der Homomorphiesatz 1.2/6 überträgt sich in nahe liegender Weise. Betrachtet man A als Modul über sich selbst, so sind die Ideale in A gerade die Untermoduln von A. Des Weiteren kann man für ein Ideal $\mathfrak{a} \subset A$ den Restklassenring $A/\mathfrak{a}$ als A-Modul auffassen.

Wie wir bereits erwähnt haben, lässt sich jede abelsche Gruppe G als $\mathbb{Z}$-Modul ansehen. Man definiere nämlich die Produktbildung $\mathbb{Z} \times G \longrightarrow G$, $(a, x) \longmapsto ax$, durch $ax = \sum_{i=1}^{a} x$ für $a \geq 0$ und $ax = -(-a)x$ für $a < 0$. Umgekehrt kann man aus jedem $\mathbb{Z}$-Modul M eine abelsche Gruppe G gewinnen, indem man die $\mathbb{Z}$-Multiplikation auf M vergisst. Es ist leicht zu sehen, dass sich auf diese Weise abelsche Gruppen und $\mathbb{Z}$-Moduln bijektiv entsprechen und dass sich diese Korrespondenz auch auf Homomorphismen, Untergruppen und Untermoduln sowie Restklassengruppen und Restklassenmoduln ausdehnt. Als weiteres Beispiel betrachte man einen Vektorraum V über einem Körper K sowie einen K-Endomorphismus $\varphi\colon V \longrightarrow V$. Es ist V ein Modul über dem Polynomring einer Variablen $K[X]$, wenn man die Multiplikation durch

$$K[X] \times V \longrightarrow V, \qquad (\sum a_i X^i, v) \longmapsto \sum a_i \varphi^i(v),$$

definiert. Umgekehrt ist jeder $K[X]$-Modul V insbesondere ein K-Vektorraum, wobei man die Multiplikation mit X als K-Endomorphismus $\varphi\colon V \longrightarrow V$ auffassen kann. Auf diese Weise entsprechen die Paare des Typs (V, φ), bestehend aus einem K-Vektorraum V und einem K-Endomorphismus $\varphi\colon V \longrightarrow V$, bijektiv den $K[X]$-Moduln.

Für eine Familie von Untermoduln $M_i \subset M$, $i \in I$, ist deren *Summe* wie üblich als Untermodul

$$M' = \sum_{i \in I} M_i = \{\sum_{i \in I} x_i \,;\, x_i \in M_i, x_i = 0 \text{ für fast alle } i \in I\}$$

von M erklärt. M' heißt *direkte Summe* der M_i, in Zeichen $M' = \bigoplus_{i \in I} M_i$, wenn jedes $x \in M'$ eine Darstellung des Typs $x = \sum_{i \in I} x_i$ mit eindeutig bestimmten Elementen $x_i \in M_i$ besitzt. Eine Summe $M_1 + M_2$ zweier Untermoduln von M etwa ist genau dann direkt, wenn $M_1 \cap M_2 = 0$ gilt. Weiter kann man zu einer Familie $(M_i)_{i \in I}$ von A-Moduln in natürlicher Weise einen A-Modul M bilden, der die direkte Summe der M_i ist. Man setze nämlich

$$M = \{(x_i)_{i \in I} \in \prod_{i \in I} M_i \,;\, x_i = 0 \text{ für fast alle } i\}$$

und identifiziere M_i jeweils mit dem Untermodul von M, der aus allen Familien $(x_{i'})_{i' \in I}$ mit $x_{i'} = 0$ für $i' \neq i$ besteht.

Eine Familie $(x_i)_{i \in I}$ von Elementen eines A-Moduls M heißt ein *Erzeugendensystem* von M, wenn $M = \sum_{i \in I} Ax_i$ gilt. Besitzt M ein endliches Erzeugendensystem, so heißt M *endlich erzeugt* oder einfach ein *endlicher* Modul.[3] Weiter nennt man das System $(x_i)_{i \in I}$ *frei* oder *linear unabhängig*, wenn aus einer Darstellung $\sum_{i \in I} a_i x_i = 0$ mit Koeffizienten $a_i \in A$ bereits $a_i = 0$ für alle $i \in I$ folgt. Ein freies Erzeugendensystem wird auch *Basis* genannt; jedes $x \in M$ hat dann eine Darstellung $x = \sum_{i \in I} a_i x_i$ mit eindeutig bestimmten Koeffizienten $a_i \in A$. In diesem Falle heißt M ein *freier* A-Modul. Beispielsweise ist A^n für $n \in \mathbb{N}$ ein freier A-Modul, ebenso $A^{(I)}$ für eine beliebige Indexmenge I.

Legt man anstelle von A einen Körper K als Koeffizientenring zugrunde, so geht die Theorie der A-Moduln über in die Theorie der K-Vektorräume. Überhaupt kann man in einem Modul M über einem Ring A weitgehend genauso rechnen wie in Vektorräumen über Körpern, mit einer Ausnahme, die zu beachten ist: Aus einer Gleichung $ax = 0$ für Elemente $a \in A$, $x \in M$ kann man meist nicht schließen, dass a oder x verschwinden, da zu $a \neq 0$ im Allgemeinen kein inverses Element a^{-1} in A zur Verfügung steht. Als Konsequenz besitzen A-Moduln, auch endlich erzeugte, nicht notwendig eine Basis. Für ein nichttriviales Ideal $\mathfrak{a} \subset A$ etwa ist der Restklassenring $A/\mathfrak{a}$ ein Beispiel eines solchen A-Moduls, der nicht frei ist.

[3] Man beachte den Sprachgebrauch: Im Gegensatz zu einer endlichen Gruppe, einem endlichen Ring oder Körper verlangt man von einem endlichen A-Modul *nicht*, dass dieser nur aus endlich vielen Elementen besteht.

Es sei nun A ein *Integritätsring*. Elemente x eines A-Moduls M, zu denen es ein $a \in A - \{0\}$ mit $ax = 0$ gibt, nennt man *Torsionselemente*. Da wir A als Integritätsring vorausgesetzt haben, bilden die Torsionselemente einen Untermodul $T \subset M$, den so genannten *Torsionsuntermodul*. Im Falle $T = 0$ heißt M *torsionsfrei*, im Falle $T = M$ ein *Torsionsmodul*. Beispielsweise ist jeder freie Modul torsionsfrei und jede endliche abelsche Gruppe, aufgefasst als $\mathbb{Z}$-Modul, ein Torsionsmodul. Weiter definiert man den *Rang* eines A-Moduls M, in Zeichen $\operatorname{rg} M$, als Supremum aller Anzahlen n, so dass es ein System linear unabhängiger Elemente $x_1, \ldots, x_n$ in M gibt. Der Rang eines Moduls ist damit ähnlich erklärt wie die Dimension eines Vektorraums. Es ist M genau dann ein Torsionsmodul, wenn der Rang von M verschwindet.

Bezeichnet S das System aller von Null verschiedenen Elemente in A sowie $K = S^{-1}A$ den Quotientenkörper von A, so kann man zu einem A-Modul M stets den K-Vektorraum $S^{-1}M$ konstruieren, indem man wie bei der Bildung von Bruchringen in Abschnitt 2.7 vorgeht. Man betrachte nämlich alle Brüche der Form $\frac{x}{s}$ mit $x \in M$ und $s \in S$, wobei man $\frac{x}{s}$ mit $\frac{x'}{s'}$ identifiziere, sofern es ein $s'' \in S$ mit $s''(s'x - sx') = 0$ gibt. Es ist dann $S^{-1}M$ mit den gewöhnlichen Regeln der Bruchrechnung ein K-Vektorraum, und man verifiziert ohne Schwierigkeiten, dass der Rang von M mit der Dimension von $S^{-1}M$ übereinstimmt. Der Kern der kanonischen Abbildung $M \longrightarrow S^{-1}M$, $x \longmapsto \frac{x}{1}$, ist gerade der Torsionsuntermodul $T \subset M$.

Im Folgenden setzen wir nun stets voraus, dass A ein *Hauptidealring* ist. Aus technischen Gründen benötigen wir den Begriff der *Länge* eines A-Moduls M, insbesondere eines A-Torsionsmoduls. Hierunter versteht man das Supremum $l_A(M)$ aller Längen ℓ von Ketten von Untermoduln des Typs

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

Beispielsweise hat der Null-Modul die Länge 0 und der freie $\mathbb{Z}$-Modul $\mathbb{Z}$ die Länge ∞. Für einen Vektorraum V über einem Körper K stimmt die Länge $l_K(V)$ überein mit der Vektorraumdimension $\dim_K V$.

Lemma 1. (i) *Es sei A ein Hauptidealring und $a \in A$ ein Element mit Primfaktorzerlegung $a = p_1 \ldots p_r$. Dann gilt $l_A(A/aA) = r$.*

(ii) *Ist ein A-Modul M die direkte Summe zweier Untermoduln M' und M'', so gilt $l_A(M) = l_A(M') + l_A(M'')$.*

Beweis. Wir beginnen mit Aussage (ii). Hat man Ketten von Untermoduln

$$0 \subsetneq M'_1 \subsetneq M'_2 \subsetneq \ldots \subsetneq M'_r = M',$$
$$0 \subsetneq M''_1 \subsetneq M''_2 \subsetneq \ldots \subsetneq M''_s = M'',$$

so ist

$$0 \subsetneq M'_1 \oplus 0 \subsetneq M'_2 \oplus 0 \subsetneq \ldots \subsetneq M'_r \oplus 0 \subsetneq M'_r \oplus M''_1 \subsetneq M'_r \oplus M''_2 \subsetneq \ldots \subsetneq M'_r \oplus M''_s = M$$

eine Kette der Länge $r+s$ in M. Also gilt $l_A(M) \geq l_A(M') + l_A(M'')$. Zum Nachweis der umgekehrten Abschätzung betrachte man eine Kette von Untermoduln

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_\ell = M$$

Es sei $\pi'' \colon M' \oplus M'' \longrightarrow M''$ die Projektion auf den zweiten Summanden, so dass $\ker \pi'' = M'$. Dann gilt für $0 \leq \lambda < \ell$ jeweils $M_\lambda \cap M' \subsetneq M_{\lambda+1} \cap M'$ oder $\pi''(M_\lambda) \subsetneq \pi''(M_{\lambda+1})$. Hieraus folgt $\ell \leq l_A(M') + l_A(M'')$ und damit die Aussage von (ii).

Nun ist auch Aussage (i) leicht zu verifizieren. Nach Umnummerieren der p_i können wir von einer Primfaktorzerlegung des Typs $a = \varepsilon p_1^{\nu_1} \ldots p_s^{\nu_s}$ mit einer Einheit ε und paarweise nicht-assoziierten Primelementen $p_1, \ldots, p_s$ ausgehen, wobei $r = \nu_1 + \ldots + \nu_s$. Aufgrund des Chinesischen Restsatzes in der Version 2.4/14 ist A/aA als Ring isomorph zu dem ringtheoretischen Produkt $\prod_{i=1}^s A/p_i^{\nu_i}A$, und im Sinne von A-Moduln schreibt sich diese Zerlegung in additiver Form als

$$A/aA \simeq A/p_1^{\nu_1}A \oplus \ldots \oplus A/p_s^{\nu_s}A.$$

Nach der bereits bewiesenen Aussage (ii) genügt es also, den Fall $a = p^\nu$ für ein Primelement $p \in A$ zu betrachten. Die Untermoduln von $A/p^\nu A$ entsprechen bijektiv den Idealen $\mathfrak{a} \subset A$ mit $p^\nu \in \mathfrak{a}$, also, da A Hauptidealring ist, bijektiv den Teilern $p^0, p^1, \ldots, p^\nu$ von p^ν. Da $p^{i+1}A$ jeweils in p^iA echt enthalten ist, ergibt sich $l_A(A/p^\nu) = \nu$, was zu zeigen war. □

Wir behandeln nunmehr den so genannten *Elementarteilersatz*, der sich als Schlüsselresultat für die Theorie endlich erzeugter Moduln über Hauptidealringen bzw. endlich erzeugter abelscher Gruppen herausstellen wird.

Theorem 2. *Es sei F ein endlicher freier Modul über einem Hauptidealring A sowie $M \subset F$ ein Untermodul vom Rang n. Dann existieren Elemente $x_1, \ldots, x_n \in F$, die Teil einer Basis von F sind, sowie Koeffizienten $\alpha_1, \ldots, \alpha_n \in A - \{0\}$, so dass gilt*:

(i) *$\alpha_1 x_1, \ldots, \alpha_n x_n$ bilden eine Basis von M.*
(ii) *$\alpha_i \,|\, \alpha_{i+1}$ für $1 \leq i < n$.*

Dabei sind die Elemente $\alpha_1, \ldots, \alpha_n$ bis auf Assoziiertheit eindeutig durch M bestimmt, unabhängig von der Wahl von $x_1, \ldots, x_n$. Man nennt $\alpha_1, \ldots, \alpha_n$ die Elementarteiler *von $M \subset F$.*

Bemerkung 3. *In obiger Situation ist der Untermodul $\bigoplus_{i=1}^n Ax_i \subset F$ eindeutig durch M bestimmt als* Saturierung M_{sat} *von M in F; dabei besteht M_{sat} aus allen Elementen $y \in F$, zu denen es ein $a \neq 0$ in A gibt mit $ay \in M$. Weiter gilt*

$$M_{\text{sat}}/M \simeq \bigoplus_{i=1}^n A/\alpha_i A.$$

Es soll zunächst gezeigt werden, wie man die Bemerkung aus der Existenzaussage des Theorems folgern kann. Einerseits gilt $\alpha_n \cdot (\bigoplus_{i=1}^n Ax_i) \subset M$, also $\bigoplus_{i=1}^n Ax_i \subset M_{\text{sat}}$. Sei umgekehrt $y \in M_{\text{sat}}$, etwa $ay \in M$ für ein $a \in A - \{0\}$. Man ergänze dann $x_1, \ldots, x_n$ durch Elemente $x_{n+1}, \ldots, x_r$ zu einer Basis von F (was aufgrund der Aussage von Theorem 2 möglich ist) und stelle y als Linearkombination der Basiselemente dar: $y = \sum_{j=1}^r a_j x_j$. Wegen $ay \in M$ ergibt sich $aa_j = 0$ bzw. $a_j = 0$ für $j = n+1, \ldots, r$, also $y \in \bigoplus_{i=1}^n Ax_i$ und somit $M_{\text{sat}} \subset \bigoplus_{i=1}^n Ax_i$. Insgesamt folgt $\bigoplus_{i=1}^n Ax_i = M_{\text{sat}}$. Um auch die zweite Behauptung von Bemerkung 3 einzusehen, betrachte man für festes i den A-Isomorphismus $A \xrightarrow{\sim} Ax_i$, $a \longmapsto ax_i$. Unter diesem korrespondiert das Ideal $\alpha_i A \subset A$ zu dem Untermodul $A\alpha_i x_i \subset Ax_i$, so dass $Ax_i / A\alpha_i x_i$ isomorph zu $A/\alpha_i A$ ist. Aus dieser Betrachtung ergibt sich leicht die Isomorphie zwischen $(\bigoplus_{i=1}^n Ax_i)/M$ und $\bigoplus_{i=1}^n A/\alpha_i A$. □

Zum Beweis von Theorem 2 benötigen wir den Begriff des *Inhalts* $\text{cont}(x)$ von Elementen $x \in F$. Um diesen zu definieren, betrachte man eine Basis $y_1, \ldots, y_r$ von F, stelle x als Linearkombination der y_j mit Koeffizienten aus A dar, etwa $x = \sum_{j=1}^r c_j y_j$, und setze $\text{cont}(x) = \text{ggT}(c_1, \ldots, c_r)$. Es bezeichnet also $\text{cont}(x)$ im strengen Sinne kein Element aus A, sondern eine Klasse assoziierter Elemente, wobei man $\text{cont}(0) = 0$ hat, auch im Falle $F = 0$. Um zu sehen, dass $\text{cont}(x)$ nicht von der Wahl der Basis $y_1, \ldots, y_r$ von F abhängt, betrachte man den A-Modul F^* aller A-Homomorphismen $F \longrightarrow A$, d. h. aller Linearformen auf F. Die Elemente $\varphi(x)$ mit $\varphi \in F^*$ bilden ein Ideal in A, also ein Hauptideal (c), und wir behaupten $c = \text{cont}(x)$. Um dies zu verifizieren, wähle man eine Gleichung $\text{cont}(x) = \sum_{j=1}^r a_j c_j$ mit Koeffizienten $a_j \in A$; vgl. 2.4/13. Ist dann $\varphi_1, \ldots, \varphi_r$ die duale Basis zu $y_1, \ldots, y_r$, definiert durch $\varphi_i(y_j) = 0$ für $i \neq j$ und $\varphi_i(y_i) = 1$, so ergibt sich $\varphi(x) = \text{cont}(x)$ für $\varphi = \sum_{j=1}^r a_j \varphi_j$. Da aber andererseits stets $\text{cont}(x) = \text{ggT}(c_1, \ldots, c_r)$ ein Teiler von $\psi(x)$ für $\psi \in F^*$ ist, erhält man $c = \text{cont}(x)$.

Wir wollen die Eigenschaften des Inhalts auflisten, die wir im Folgenden benötigen.

Lemma 4. *In der Situation von Theorem* 2 *gilt*:

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

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

(iii) *Es existiert ein* $x \in M$ *mit* $\text{cont}(x) \,|\, \text{cont}(y)$ *für alle* $y \in M$.

Beweis. Es muss nur noch Aussage (iii) gezeigt werden. Hierzu betrachte man die Menge aller Ideale des Typs $\text{cont}(y) \cdot A$, wobei y in M variiert. Unter allen diesen Idealen gibt es ein maximales Element, also eines, welches in keinem Ideal $\text{cont}(y) \cdot A$, $y \in M$, echt enthalten ist. Denn anderenfalls könnte man eine unendliche Folge y_i in M konstruieren mit

$$\text{cont}(y_1) \cdot A \subsetneq \text{cont}(y_2) \cdot A \subsetneq \ldots,$$

im Gegensatz dazu, dass A noethersch ist; vgl. 2.4/8. Es existiert also ein $x \in M$ mit der Eigenschaft, dass $\mathrm{cont}(x) \cdot A$ maximal im obigen Sinne ist. Weiter wähle man $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$. Wir zeigen zunächst

$$(*) \qquad \varphi(x) \,|\, \varphi(y) \text{ für alle } y \in M.$$

Sei $d = \mathrm{ggT}(\varphi(x), \varphi(y))$ für ein $y \in M$, das wir im Folgenden betrachten wollen. Dann gibt es $a, b \in A$ mit $a\varphi(x) + b\varphi(y) = d$, also $\varphi(ax + by) = d$. Aufgrund von (ii) folgt $\mathrm{cont}(ax + by) \,|\, d$ und wegen $d \,|\, \varphi(x)$ sogar $\mathrm{cont}(ax + by) \,|\, \mathrm{cont}(x)$. Die Maximalitätseigenschaft von x impliziert dann aber $\mathrm{cont}(ax + by) = \mathrm{cont}(x)$. Somit ist $\mathrm{cont}(x)$ ein Teiler von d und wegen $d \,|\, \varphi(y)$ auch ein Teiler von $\varphi(y)$. Dies verifiziert $(*)$.

Um $\mathrm{cont}(x) \,|\, \mathrm{cont}(y)$ zu erhalten, genügt es gemäß (i), für $\psi \in F^*$ die Relation $\varphi(x) \,|\, \psi(y)$ zu zeigen. Da $\varphi(x) \,|\, \psi(x)$ aufgrund von (ii) gilt sowie $\varphi(x) \,|\, \varphi(y)$ aufgrund von $(*)$, dürfen wir y durch $y - \frac{\varphi(y)}{\varphi(x)}x$ ersetzen und damit $\varphi(y) = 0$ annehmen. Indem wir diese Teilbarkeitsrelationen nochmals ausnutzen, können wir weiter ψ durch $\psi - \frac{\psi(x)}{\varphi(x)}\varphi$ ersetzen und damit $\psi(x) = 0$ annehmen. Sei unter diesen Voraussetzungen $d = \mathrm{ggT}(\varphi(x), \psi(y))$, etwa $d = a\varphi(x) + b\psi(y)$ mit $a, b \in A$. Dann gilt

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

d. h. $\mathrm{cont}(ax + by) \,|\, d$. Da nach Definition d ein Teiler von $\varphi(x)$ ist, ergibt sich $\mathrm{cont}(ax + by) \mid \varphi(x)$ und somit $\mathrm{cont}(ax + by) = \varphi(x)$ aufgrund der Maximalitätseigenschaft von x. Hieraus folgt $\varphi(x) \,|\, d$ und wegen $d \,|\, \psi(y)$ wie gewünscht $\varphi(x) \,|\, \psi(y)$. □

Wir kommen nun zum eigentlichen *Beweis von Theorem* 2, und zwar werden wir zur Herleitung der Existenzaussage zwei Induktionsbeweise führen, jeweils nach $n = \mathrm{rg}\, M$. Im ersten zeigen wir, dass jeder Untermodul $M \subset F$ frei ist, und benutzen dies im zweiten Induktionsbeweis, um die im Theorem formulierte Existenzaussage zu gewinnen. Im Falle $n = 0$ gilt auch $M = 0$, da M torsionsfrei ist, und es ist nichts zu zeigen. Sei also $n > 0$. Man wähle gemäß Lemma 4 (iii) ein $x \in M$ mit $\mathrm{cont}(x) \,|\, \mathrm{cont}(y)$ für alle $y \in M$. Es existiert dann ein $\varphi \in F^*$ mit $\varphi(x) = \mathrm{cont}(x)$, vgl. Lemma 4 (i), sowie ein (eindeutig bestimmtes) Element $x_1 \in F$ mit $x = \varphi(x)x_1$. Setzt man nun $F' = \ker \varphi$ und $M' = M \cap F'$, so gilt

$$(*) \qquad F = Ax_1 \oplus F', \qquad M = Ax \oplus M'.$$

Um die Formel für M zu erhalten, wähle man ein Element $y \in M$ und schreibe

$$y = \frac{\varphi(y)}{\varphi(x)}x + \big(y - \frac{\varphi(y)}{\varphi(x)}x\big),$$

wobei wegen $\varphi(x) \mid \varphi(y)$, vgl. Lemma 4 (ii) und (iii), der erste Term zu Ax gehört. Weiter liegt der zweite Term in M', da er sowohl in M, als auch in $\ker \varphi$ liegt. Insbesondere folgt $M = Ax + M'$. Weiter hat man $\varphi(x) \neq 0$ wegen $M \neq 0$

und daher $Ax \cap M' = 0$. Also ist M die direkte Summe der Untermoduln Ax und M'. In gleicher Weise zeigt man die Formel $F = Ax_1 \oplus F'$; man ersetze in vorstehender Argumentation jeweils x durch x_1 und benutze $\varphi(x_1) = 1$.

Aus der Zerlegung $M = Ax \oplus M'$ schließt man wegen $x \neq 0$ insbesondere $\operatorname{rg} M' < n$. Dann ist M' nach Induktionsvoraussetzung frei, notwendig vom Rang $n-1$, und es folgt, dass auch M frei ist. Dies beendet unseren ersten Induktionsbeweis.

Den zweiten Induktionsbeweis führen wir in gleicher Weise, bis wir zu den Zerlegungen $(*)$ gelangen. Aus dem ersten Induktionsbeweis wissen wir, dass F' als Untermodul von F frei ist. Wir haben also nach Induktionsvoraussetzung die Aussage von Theorem 2 für den Untermodul $M' \subset F'$ zur Verfügung. Somit existieren Elemente $x_2, \ldots, x_n \in F'$, die sich zu einer Basis von F' ergänzen lassen, sowie Elemente $\alpha_2, \ldots, \alpha_n \in A - \{0\}$ mit $\alpha_i \,|\, \alpha_{i+1}$ für $2 \leq i < n$ und mit der Eigenschaft, dass $\alpha_2 x_2, \ldots, \alpha_n x_n$ eine Basis von M' bilden. Insgesamt sind dann $x_1, \ldots, x_n$ Teil einer Basis von $F = Ax_1 \oplus F'$, und es bilden $\alpha_1 x_1, \ldots, \alpha_n x_n$ mit $\alpha_1 := \varphi(x)$ eine Basis von $M = Ax \oplus M'$. Für die Existenzaussage in Theorem 2 bleibt daher lediglich noch $\alpha_1 \,|\, \alpha_2$ nachzuweisen. Hierzu betrachte man eine Linearform $\varphi_2 \in F^*$, welche $\varphi_2(x_2) = 1$ erfüllt. Aufgrund von Lemma 4 (ii) und (iii) gilt dann $\varphi(x) \,|\, \varphi_2(\alpha_2 x_2)$, also $\alpha_1 \,|\, \alpha_2$. Damit ist die Existenzaussage von Theorem 2 bewiesen.

Es bleibt noch die Eindeutigkeit der α_i nachzuweisen. Im Hinblick auf weitere Anwendungen formulieren wir diese in etwas allgemeinerer Form.

Lemma 5. *Es sei A ein Hauptidealring und $Q \simeq \bigoplus_{i=1}^{n} A/\alpha_i A$ ein A-Modul, wobei $\alpha_1, \ldots, \alpha_n \in A - \{0\}$ Nichteinheiten mit $\alpha_i \,|\, \alpha_{i+1}$ für $1 \leq i < n$ sind. Dann sind $\alpha_1, \ldots, \alpha_n$ bis auf Assoziiertheit eindeutig durch Q bestimmt.*

Beweis. Aus technischen Gründen invertieren wir die Nummerierung der α_i und betrachten zwei Zerlegungen

$$Q \simeq \bigoplus_{i=1}^{n} A/\alpha_i A \simeq \bigoplus_{j=1}^{m} A/\beta_j A$$

mit $\alpha_{i+1} \mid \alpha_i$ für $1 \leq i < n$ sowie $\beta_{j+1} \mid \beta_j$ für $1 \leq j < m$. Falls es einen Index $k \leq \min\{m, n\}$ mit $\alpha_k A \neq \beta_k A$ gibt, so wähle man k minimal mit dieser Eigenschaft. Da $\alpha_i A = \beta_i A$ für $1 \leq i < k$ und da $\alpha_{k+1}, \ldots, \alpha_n$ sämtlich Teiler von α_k sind, zerlegt sich $\alpha_k Q$ zu

$$\alpha_k Q \simeq \bigoplus_{i=1}^{k-1} \alpha_k \cdot (A/\alpha_i A) \simeq \bigoplus_{i=1}^{k-1} \alpha_k \cdot (A/\alpha_i A) \oplus \alpha_k \cdot (A/\beta_k A) \oplus \ldots .$$

Wir benutzen nun Lemma 1. Wegen $l_A(Q) < \infty$ ergibt sich durch Vergleich beider Seiten $l_A(\alpha_k \cdot (A/\beta_k A)) = 0$. Letzteres bedeutet aber $\alpha_k \cdot (A/\beta_k A) = 0$ bzw. $\alpha_k A \subset \beta_k A$. Entsprechend zeigt man $\beta_k A \subset \alpha_k A$ und somit $\alpha_k A = \beta_k A$, im Widerspruch zu unserer Annahme. Es gilt daher $\alpha_i A = \beta_i A$ für alle Indizes i mit

$1 \le i \le \min\{m,n\}$. Hat man weiter $m \le n$, so folgt, wiederum unter Benutzung von Lemma 1, dass $\bigoplus_{i=m+1}^{n} A/\alpha_i A$ von der Länge 0 ist, also verschwindet, so dass sich $m = n$ ergibt. □

Abschließend wollen wir noch erläutern, wie die Eindeutigkeitsaussage von Theorem 2 aus vorstehendem Lemma gefolgert werden kann. Man habe also in der Situation des Theorems Elementarteiler $\alpha_1, \dots, \alpha_n$ mit $\alpha_i \mid \alpha_{i+1}$ sowie $\beta_1, \dots, \beta_n$ mit $\beta_i \mid \beta_{i+1}$, $1 \le i < n$. Dann gilt gemäß Bemerkung 3, für deren Beweis wir lediglich die Existenzaussage von Theorem 2 verwendet haben,

$$\bigoplus_{i=1}^{n} A/\alpha_i A \simeq \bigoplus_{i=1}^{n} A/\beta_i A.$$

Da A/aA für Einheiten $a \in A$ verschwindet, folgt aus Lemma 5, dass die Nichteinheiten unter den $\alpha_1, \alpha_2, \dots$ mit den Nichteinheiten unter den $\beta_1, \beta_2, \dots$ bis auf Assoziiertheit übereinstimmen. Die restlichen α_i und β_i sind dann Einheiten. Es gilt daher $\alpha_i A = \beta_i A$ für $1 \le i \le n$, und der Beweis zu Theorem 2 ist beendet. □

Wir wollen jetzt noch eine konstruktive Beschreibung der Elementarteiler angeben, die insbesondere für explizite Berechnungen von Interesse ist.

Satz 6. *Es sei A ein Hauptidealring, F ein endlicher freier A-Modul mit Basis $x_1, \dots, x_r$ sowie $M \subset F$ ein Untermodul vom Rang n mit zugehörigen Elementarteilern $\alpha_1, \dots, \alpha_n$. Weiter seien $z_1, \dots, z_m \in M$ Elemente, die ein (nicht notwendig freies) Erzeugendensystem von M bilden. Für $j = 1, \dots, m$ gelte $z_j = \sum_{i=1}^{r} a_{ij} x_i$ mit Koeffizienten $a_{ij} \in A$, und es sei μ_t für $t = 1, \dots, n$ der größte gemeinsame Teiler aller t-Minoren der Koeffizientenmatrix $D = (a_{ij})$.*[4] *Dann gilt $\mu_t = \alpha_1 \dots \alpha_t$. Insbesondere folgt $\alpha_1 = \mu_1$ sowie $\alpha_t \mu_{t-1} = \mu_t$ für $t = 2, \dots, n$.*

Man nennt $\alpha_1, \dots, \alpha_n$ auch die Elementarteiler der Matrix D.

Beweis. Wir verifizieren die Behauptung zunächst für den Fall $t = 1$. Es ist $(\alpha_1) \subset A$ dasjenige Ideal, welches von allen Elementen des Typs $\varphi(z)$ mit $z \in M$ und $\varphi \in F^*$ erzeugt wird; dies ist unmittelbar aus der Aussage (oder dem Beweis) von Theorem 2 abzulesen. Indem wir auf die Elemente z_j die Linearformen der zu $x_1, \dots, x_r$ dualen Basis von F^* anwenden, sehen wir, dass dasselbe Ideal auch von allen Koeffizienten a_{ij} erzeugt wird. Dies bedeutet aber, dass α_1 der größte gemeinsame Teiler aller 1-Minoren von D ist.

Um die Aussage für beliebiges t zu erhalten, ist es zweckmäßig, das *t-fache äußere Produkt* $\bigwedge^t F$ zu betrachten. Für unsere Zwecke genügt es, die Basis $x_1, \dots, x_r$ von F zu fixieren und $\bigwedge^t F$ als freien A-Modul zu erklären, für den

[4] Die t-Minoren von D sind die Determinanten der $(t \times t)$-Untermatrizen von D. Da D, aufgefasst als $(r \times m)$-Matrix mit Koeffizienten aus dem Quotientenkörper $Q(A)$, den Rang n hat, gilt $n \le \min(r, m)$.

die Symbole $x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \leq i_1 < \ldots < i_t \leq r$ eine Basis bilden. Für eine Permutation $\pi \in \mathfrak{S}_t$, also eine bijektive Selbstabbildung von $\{1, \ldots, t\}$, setzt man weiter

$$x_{i_{\pi(1)}} \wedge \ldots \wedge x_{i_{\pi(t)}} = (\operatorname{sgn} \pi) \cdot x_{i_1} \wedge \ldots \wedge x_{i_t},$$

wobei $\operatorname{sgn} \pi$ das Signum der Permutation π bezeichnet; vgl. 5.3. Definiert man dann noch $x_{i_1} \wedge \ldots \wedge x_{i_t} = 0$, falls die Indizes i_j nicht paarweise verschieden sind, so hat man das so genannte t-fache "äußere Produkt" $x_{i_1} \wedge \ldots \wedge x_{i_t}$ für beliebige Indizes $i_1, \ldots, i_t \in \{1, \ldots, r\}$ erklärt, also für jeweils t Elemente der Basis $x_1, \ldots, x_r$. Durch A-multilineare Ausdehnung erhält man dann das äußere Produkt $z_1 \wedge \ldots \wedge z_t$ von beliebigen Elementen $z_1, \ldots, z_t \in F$. Nach Konstruktion ist dieses Produkt multilinear und alternierend in den Faktoren. Es ergibt sich beispielsweise für Elemente der Form $z_j = \sum_{i=1}^{r} a_{ij} x_i$

$$\begin{aligned} z_1 \wedge \ldots \wedge z_t &= (\sum_{i=1}^{r} a_{i1} x_i) \wedge \ldots \wedge (\sum_{i=1}^{r} a_{it} x_i) \\ &= \sum_{i_1, \ldots, i_t = 1}^{r} a_{i_1 1} \ldots a_{i_t t}\ x_{i_1} \wedge \ldots \wedge x_{i_t} \\ &= \sum_{1 \leq i_1 < \ldots < i_t \leq r} (\sum_{\pi \in \mathfrak{S}_t} (\operatorname{sgn} \pi) \cdot a_{i_{\pi(1)} 1} \ldots a_{i_{\pi(t)} t})\ x_{i_1} \wedge \ldots \wedge x_{i_t}, \end{aligned}$$

wobei die Koeffizienten $\sum_{\pi \in \mathfrak{S}_t} (\operatorname{sgn} \pi) \cdot a_{i_{\pi(1)} 1} \ldots a_{i_{\pi(t)} t}$ gerade die t-Minoren der Koeffizientenmatrix von $z_1, \ldots, z_t$ bezüglich der Basis $x_1, \ldots, x_r$ sind. Man kann diese Rechnung übrigens auch dazu verwenden, um einzusehen, dass die obige Definition von $\bigwedge^t F$ zusammen mit dem t-fachen äußeren Produkt von Elementen aus F in natürlicher Weise unabhängig von der Wahl der Basis $x_1, \ldots, x_r$ ist.

Wir betrachten nun wieder die ursprünglich gegebenen Elemente $z_1, \ldots, z_m$ aus M und nehmen zunächst an, dass diese eine Basis von M bilden, genauer, dass $z_i = \alpha_i x_i$ für $i = 1, \ldots, m$ gilt mit Elementen $\alpha_i \in A - \{0\}$, welche der Teilbarkeitsrelation $\alpha_i \mid \alpha_{i+1}$ genügen. Eine solche Situation ist aufgrund des Elementarteilersatzes für $m = n$ durch geeignete Wahl von $x_1, \ldots, x_r$ sowie $z_1, \ldots, z_m$ stets zu realisieren. Man sieht dann, dass das t-fache äußere Produkt $\bigwedge^t M$ in natürlicher Weise ein Untermodul von $\bigwedge^t F$ ist; es bilden nämlich die Elemente $x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \leq i_1 < \ldots i_t \leq r$ eine Basis von $\bigwedge^t F$ sowie die Elemente $\alpha_{i_1} \ldots \alpha_{i_t} x_{i_1} \wedge \ldots \wedge x_{i_t}$ mit $1 \leq i_1 < \ldots i_t \leq m$ eine Basis von $\bigwedge^t M$. Insbesondere erkennt man das Produkt $\alpha_1 \ldots \alpha_t$, etwa aufgrund der bereits für $t = 1$ durchgeführten Betrachtung, als ersten Elementarteiler des Problems $\bigwedge^t M \subset \bigwedge^t F$.

In der Situation des Satzes bilden $z_1, \ldots, z_m$ ein nicht notwendig freies Erzeugendensystem von M. Es folgt, dass die t-fachen äußeren Produkte des Typs $z_{i_1} \wedge \ldots \wedge z_{i_t}$ mit $1 \leq i_1 < \ldots < i_t \leq m$ den A-Modul $\bigwedge^t M$ erzeugen; man benutze eine Rechnung, wie wir sie oben durchgeführt haben. Aufgrund des bereits erledigten Falles $t = 1$ berechnet sich der erste Elementarteiler zu $\bigwedge^t M \subset \bigwedge^t F$ als größter gemeinsamer Teiler aller Koeffizienten aus A, die man

benötigt, um die Elemente $z_{i_1} \wedge \ldots \wedge z_{i_t}$ als Linearkombinationen der Basiselemente $x_{i_1} \wedge \ldots \wedge x_{i_t}$, $1 \leq i_1 < \ldots i_t \leq r$, darzustellen. Diese Koeffizienten sind aber, wie wir oben gesehen haben, die t-Minoren der Matrix D, d. h. der erste Elementarteiler zu $\bigwedge^t M \subset \bigwedge^t F$ ist μ_t. Andererseits hatten wir diesen Elementarteiler aber schon als $\alpha_1 \ldots \alpha_t$ erkannt, so dass $\mu_t = \alpha_1 \ldots \alpha_t$ folgt. □

Es sei hier noch ein weiteres konstruktives Verfahren angeführt, mit welchem man in der Situation von Satz 6 die Elementarteiler der Matrix $D = (a_{ij})$ bzw. von $M \subset F$ bestimmen kann, und zwar für den Fall, dass A ein *euklidischer Ring* ist. Hierzu betrachte man A^m als freien A-Modul mit der kanonischen Basis $e_1, \ldots, e_m$ sowie den A-Homomorphismus

$$A^m \longrightarrow F, \qquad e_j \longmapsto z_j,$$

welcher bezüglich der Basen $e_1, \ldots, e_m$ von A^m sowie $x_1, \ldots, x_r$ von F durch die Matrix D beschrieben wird. Wir zeigen im Folgenden, dass man D durch elementare Zeilen- und Spaltenumformungen — hiermit meinen wir Vertauschung von Zeilen (bzw. Spalten) sowie Addition eines Vielfachen einer Zeile (bzw. Spalte) zu einer weiteren Zeile (bzw. Spalte) — in die Gestalt

$$\begin{pmatrix} \alpha_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 & 0 & \ldots & 0 \\ . & . & \ldots & . & . & \ldots & . \\ 0 & 0 & \ldots & \alpha_n & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ . & . & \ldots & . & . & \ldots & . \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

mit $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < n$ bringen kann. Diese Umformungen kann man interpretieren als Multiplikation von links und rechts mit jeweils einer invertierbaren Matrix $S \in A^{(r \times r)}$ bzw. $T \in A^{(m \times m)}$. Die resultierende Matrix SDT beschreibt ebenfalls die Abbildung f, allerdings bezüglich geeigneter anderer Basen $e'_1, \ldots, e'_m$ von A^m und $x'_1, \ldots, x'_r$ von F. Insbesondere folgt, dass M durch $\alpha_1 x'_1, \ldots, \alpha_n x'_n$ erzeugt wird, d. h. $\alpha_1, \ldots, \alpha_n$ sind die Elementarteiler von D bzw. $M \subset F$.

Um nun die Matrix $D = (a_{ij})$ durch elementare Zeilen- und Spaltenumformungen in die gewünschte Gestalt zu bringen, benutzen wir die Gradabbildung $\delta\colon A - \{0\} \longrightarrow \mathbb{N}$ des euklidischen Rings A. Für $D = 0$ ist nichts zu zeigen. Sei also $D \neq 0$. Es ist unsere Strategie, D mittels elementarer Umformungen so abzuändern, dass sich das Minimum

$$d = \min\{\delta(a)\,;\, a \text{ ist Koeffizient } \neq 0 \text{ von } D\}$$

schrittweise verringert. Da δ Werte in $\mathbb{N}$ annimmt, muss dieses Verfahren nach endlich vielen Schritten abbrechen. Ist dann $a \neq 0$ ein Koeffizient der transformierten Matrix mit minimalem Grad $\delta(a)$, so zeigen wir mittels Division mit

Rest, dass a alle anderen Koeffizienten der Matrix teilt; a ist also der erste Elementarteiler von D.

Im Einzelnen gehen wir wie folgt vor. Indem wir Zeilen und Spalten in D vertauschen, können wir $d = \delta(a_{11})$ annehmen, dass also $\delta(a_{11})$ minimal ist unter allen $\delta(a_{ij})$ mit $a_{ij} \neq 0$. Ist eines der Elemente der 1. Spalte, etwa a_{i1}, nicht durch a_{11} teilbar, so teile man a_{i1} mit Rest durch a_{11}, etwa $a_{i1} = qa_{11} + b$ mit $\delta(b) < \delta(a_{11})$, und ziehe das q-fache der 1. Zeile von der i-ten Zeile ab. Als Resultat entsteht an der Position $(i, 1)$ das Element b. Das Minimum d der Grade von nichtverschwindenden Koeffizienten von D hat sich daher verringert, und man starte das Verfahren erneut. Entsprechend können wir mit der 1. Zeile verfahren. Da d Werte in $\mathbb{N}$ annimmt, also nicht beliebig oft verringert werden kann, ist nach endlich vielen Schritten jedes Element der 1. Spalte sowie der 1. Zeile ein Vielfaches von a_{11}, und wir können durch Addition von Vielfachen der 1. Zeile zu den restlichen Zeilen der Matrix annehmen, dass $a_{i1} = 0$ für $i > 1$ gilt. Entsprechend können wir mit der 1. Zeile verfahren und auf diese Weise $a_{i1} = a_{1j} = 0$ für $i, j > 1$ erreichen. Dabei dürfen wir weiter annehmen, dass das Minimum d mit $\delta(a_{11})$ übereinstimmt; ansonsten ist das Verfahren wiederum neu zu starten. Existieren nun $i, j > 1$ mit $a_{11} \nmid a_{ij}$, so dividiere man a_{ij} mit Rest durch a_{11}, etwa $a_{ij} = qa_{11} + b$, wobei dann $b \neq 0$ mit $\delta(b) < \delta(a_{11})$ gilt. Man addiere die 1. Zeile zur i-ten Zeile und subtrahiere anschließend das q-fache der 1. Spalte von der j-ten Spalte. Auf diese Weise wird, neben anderen Änderungen, a_{ij} durch b ersetzt, wobei nun $\delta(b) < \delta(a_{11}) = d$ gilt. Man starte daher das Verfahren erneut. Nach endlich vielen Schritten gelangt man so zu einer Matrix (a_{ij}) mit $a_{i1} = a_{1j} = 0$ für $i, j > 1$ sowie mit der Eigenschaft, dass a_{11} jedes andere Element a_{ij} mit $i, j > 1$ teilt. Man behandele dann in gleicher Weise die Untermatrix $(a_{ij})_{i,j>1}$ von $D = (a_{ij})$, sofern diese nicht bereits Null ist. Führt man dieses Verfahren in induktiver Weise fort, so gelangt man schließlich nach endlich vielen Schritten zu einer Matrix, auf deren Hauptdiagonale die gesuchten Elementarteiler stehen und deren sonstige Einträge alle verschwinden.

Wir wollen als Nächstes aus dem Elementarteilersatz den *Hauptsatz für endlich erzeugte Moduln über Hauptidealringen* ableiten, wobei wir die Aussage in zwei Teile aufspalten. A sei im Folgenden wieder ein *Hauptidealring*.

Korollar 7. *Es sei M ein endlich erzeugter A-Modul sowie $T \subset M$ der zugehörige Torsionsuntermodul. Dann ist T endlich erzeugt, und es gibt einen freien Untermodul $F \subset M$ mit $M = T \oplus F$, wobei* $\operatorname{rg} M = \operatorname{rg} F$. *Insbesondere ist M frei, falls M keine Torsion hat.*

Korollar 8. *Es sei M ein endlich erzeugter Torsionsmodul über A sowie $P \subset A$ ein Vertretersystem der Primelemente von A. Für $p \in P$ bezeichne*

$$M_p = \{x \in M \,;\, p^n x = 0 \text{ für geeignetes } n \in \mathbb{N}\}$$

*den so genannten Untermodul der p-*Torsion *in M. Dann gilt*

$$M = \bigoplus_{p \in P} M_p,$$

wobei M_p für fast alle $p \in P$ verschwindet. Weiter gibt es zu jedem $p \in P$ natürliche Zahlen $1 \leq \nu(p,1) \leq \ldots \leq \nu(p,r_p)$ mit

$$M_p \simeq \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)}A.$$

Die Zahlen $r_p, \nu(p,j_p)$ sind durch die Isomorphie

$$M \simeq \bigoplus_{p\in P} \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)}A$$

eindeutig bestimmt, und es gilt $r_p = 0$ für fast alle p.

In Kombination besagen die beiden Resultate, dass jeder endlich erzeugte A-Modul M zu einer direkten Summe der Form

$$A^d \oplus \bigoplus_{p\in P} \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)}A$$

isomorph ist, mit Zahlen d, r_p und $\nu(p,j_p)$ wie oben, die eindeutig durch M bestimmt sind. Dies ist die eigentliche Aussage des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen. Bevor wir zum Beweis kommen, wollen wir diesen Hauptsatz auch noch speziell für endlich erzeugte $\mathbb{Z}$-Moduln formulieren, als *Hauptsatz über endlich erzeugte abelsche Gruppen.*

Korollar 9. *Es sei G eine endlich erzeugte abelsche Gruppe, P sei die Menge der Primzahlen. Dann gestattet G eine Zerlegung in Untergruppen*

$$G = F \oplus \bigoplus_{p\in P} \bigoplus_{j_p=1}^{r_p} G_{p,j_p},$$

wobei F frei ist, etwa $F \simeq \mathbb{Z}^d$, und G_{p,j_p} zyklisch von p-Potenz-Ordnung, etwa $G_{p,j_p} \simeq \mathbb{Z}/p^{\nu(p,j_p)}\mathbb{Z}$ mit $1 \leq \nu(p,1) \leq \ldots \leq \nu(p,r_p)$. Die Zahlen $d, r_p, \nu(p,j_p)$ sind eindeutig durch G bestimmt, ebenso die Untergruppen $G_p = \bigoplus_{j_p=1}^{r_p} G_{p,j_p}$, wobei r_p für fast alle $p \in P$ verschwindet.

Wenn G eine endlich erzeugte Torsionsgruppe ist, also ein über $\mathbb{Z}$ endlich erzeugter Torsionsmodul, so besitzt G keinen freien Anteil und besteht daher, wie man insbesondere mit Korollar 9 sieht, nur aus endlich vielen Elementen. Umgekehrt ist jede endliche abelsche Gruppe natürlich eine endlich erzeugte Torsionsgruppe.

Nun zum *Beweis von Korollar* 7. Ist $z_1, \ldots, z_r$ ein Erzeugendensystem des A-Moduls M, so definiere man einen A-Homomorphismus $f\colon A^r \longrightarrow M$, indem man die kanonische Basis von A^r auf $z_1, \ldots, z_r$ abbilde. Dann ist f surjektiv,

und es folgt $M \simeq A^r/\ker f$ aufgrund des Homomorphiesatzes. Auf die Situation $\ker f \subset A^r$ können wir nun den Elementarteilersatz anwenden. Es existieren also Elemente $x_1, \ldots, x_r$, die eine Basis von A^r bilden, sowie Elemente $\ldots \alpha_1, \ldots, \alpha_n \in A$, $n = \operatorname{rg}(\ker f)$, so dass $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von $\ker f$ ist. Hieraus ergibt sich

$$M \simeq A^{r-n} \oplus \bigoplus_{i=1}^{n} A/\alpha_i A.$$

Unter dem betrachteten Isomorphismus korrespondiert $\bigoplus_{i=1}^n A/\alpha_i A$ zu dem Torsionsuntermodul $T \subset M$, sowie A^{r-n} zu einem freien Modul $F \subset M$, und es gilt $M = T \oplus F$. Im Übrigen ist $T \simeq \bigoplus_{i=1}^n A/\alpha_i A$ endlich erzeugt, so dass Korollar 7 bewiesen ist. □

Zum *Beweis von Korollar* 8 nehmen wir M als Torsionsmodul an, so dass M wie im Beweis zu Korollar 7 isomorph zu der direkten Summe $\bigoplus_{i=1}^n A/\alpha_i A$ ist. Man zerlege die α_i in Primfaktoren, etwa $\alpha_i = \varepsilon_i \prod_{p\in P} p^{\nu(p,i)}$ mit Einheiten ε_i und Exponenten $\nu(p,i)$, die fast alle verschwinden. Aufgrund des Chinesischen Restsatzes 2.4/14 folgt

$$A/\alpha_i A \simeq \bigoplus_{p\in P} A/p^{\nu(p,i)} A$$

und somit

$$M \simeq \bigoplus_{p\in P} \bigoplus_{i=1}^{n} A/p^{\nu(p,i)} A.$$

In dieser Zerlegung korrespondiert $\bigoplus_{i=1}^n A/p^{\nu(p,i)}A$ offenbar gerade zu dem Untermodul $M_p \subset M$ der p-Torsion und ist deshalb eindeutig bestimmt; die Restklasse von p in Restklassenringen der Form $A/p'^r A$ mit $p' \in P - \{p\}$ ist nämlich jeweils eine Einheit. Somit folgt aus obiger Zerlegung insbesondere $M = \bigoplus_{p\in P} M_p$. Verzichtet man nun in der Zerlegung

$$M_p \simeq \bigoplus_{i=1}^{n} A/p^{\nu(p,i)} A$$

auf Terme $A/p^{\nu(p,i)}A$ mit $\nu(p,i) = 0$, die ohnehin trivial sind, und ordnet im Übrigen für fixiertes p die Exponenten $\nu(p,i)$ in aufsteigender Reihenfolge an, etwa

$$M_p \simeq \bigoplus_{j_p=1}^{r_p} A/p^{\nu(p,j_p)} A$$

mit $1 \leq \nu(p,1) \leq \ldots \leq \nu(p,r_p)$, so ergibt sich unter Benutzung der Eindeutigkeitsaussage in Lemma 5 insgesamt die Behauptung von Korollar 8. □

Die in diesem Abschnitt behandelten Methoden und Resultate basieren in grundlegender Weise auf der idealtheoretischen Charakterisierung 2.4/13 des

größten gemeinsamen Teilers, also auf einer Charakterisierung, die in Hauptidealringen gilt, nicht jedoch in allgemeineren faktoriellen Ringen; vgl. Abschnitt 2.4, Aufgabe 2. Aus diesem Grunde ist eine Übertragung der Elementarteilertheorie auf endlich erzeugte Moduln etwa über faktoriellen Ringen nicht möglich.

Aufgaben

A sei stets ein Hauptidealring.

1. *Man betrachte eine Zerlegung $M = T \oplus F$ eines endlich erzeugten A-Moduls M in einen Torsionsmodul T und einen freien Modul F und diskutiere die Eindeutigkeit einer solchen Zerlegung. Dasselbe Problem studiere man für eine Zerlegung der Form $M = M' \oplus M''$ mit $M' \simeq A/p^r A$ sowie $M'' \simeq A/p^s A$ für ein Primelement $p \in A$.*
2. *Ein torsionsfreier A-Modul ist frei, sofern er endlich erzeugt ist. Gilt dies auch für beliebige torsionsfreie A-Moduln?*
3. *Man leite die Normalformentheorie für Endomorphismen endlich-dimensionaler Vektorräume aus Korollar 8 ab.*
4. Man bestimme die Elementarteiler der folgenden Matrix:

$$\begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix} \in \mathbb{Z}^{(3\times 3)}$$

5. Es seien $a_{11}, \ldots, a_{1n} \in A$ Elemente mit $\mathrm{ggT}(a_{11}, \ldots, a_{1n}) = 1$. Man zeige, es gibt Elemente $a_{ij} \in A$, $i = 2, \ldots, n$, $j = 1, \ldots, n$, so dass die Matrix $(a_{ij})_{i,j=1,\ldots,n}$ in $A^{(n\times n)}$ invertierbar ist.
6. Es sei $f\colon L \longrightarrow M$ ein A-Homomorphismus zwischen endlich erzeugten freien A-Moduln. Man zeige:
   (i) Es existiert ein freier Untermodul $F \subset L$ mit $L = \ker f \oplus F$.
   (ii) Es existieren Basen $x_1, \ldots, x_m$ von L, $y_1, \ldots, y_n$ von M sowie Elemente $\alpha_1, \ldots, \alpha_r \in A - \{0\}$, $r \leq \min\{m, n\}$, so dass $f(x_i) = \alpha_i y_i$ für $i = 1, \ldots, r$ und $f(x_i) = 0$ für $i > r$. Zusätzlich kann man $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < r$ erreichen.
7. Man gebe ein einfaches Argument an, mit dessen Hilfe sich die Aussage von Theorem 2 auf endlich-rangige Untermoduln M von (nicht notwendig endlich-rangigen) freien A-Moduln F verallgemeinern lässt.