Algebra A

Wintersemester 2002/03

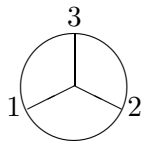
W. Ebeling

Institut für Mathematik
Universität Hannover
Postfach 6009
30060 Hannover
E-mail: ebeling@math.uni-hannover.de

1 Einleitung

Die Algebra befasst sich mit dem Studium von algebraischen Strukturen. Wir werden in dieser Vorlesung Gruppen, Ringe, Polynome und Körper studieren. Bevor wir mit der Theorie beginnen, möchte ich drei Anwendungsbeispiele darstellen, mit denen wir uns im Laufe der Vorlesung auch weiter auseinandersetzen werden.

Beispiel 1.1 Wir betrachten die folgende Figur.



(Die Zahlen sind nur zur Hilfe angegeben.) Wie sehen die Symmetrien dieser Figur aus? Drehen der Figur liefert

$$(1,2,3) \mapsto (1,2,3), \quad (1,2,3) \mapsto (2,3,1), \quad (1,2,3) \mapsto (3,1,2).$$

Darüber hinaus können wir Spiegelungen betrachten:

$$(1,2,3) \mapsto (1,3,2), \quad (1,2,3) \mapsto (3,2,1), \quad (1,2,3) \mapsto (2,1,3).$$

Wir sehen auch, dass die Hintereinanderausführung von zwei Symmetrien wieder eine der bereits aufgeführten Symmetrien ergibt. Die Identität wirkt als neutrales Element und zu jeder Symmetrie gibt es eine dazu inverse Symmetrie. Die Symmetrien der Figur bilden eine Gruppe. Diese Gruppe nennt man die *Symmetriegruppe* der Figur. Die angebene Beschriebung zeigt, dass wir diese Gruppe mit der Gruppe aller Permutationen der Zahlen $1, 2, 3$ identifizieren können, die wir bereits in Lineare Algebra B betrachtet haben. Wir sehen also, dass Gruppen als Symmetriegruppen von bestimmten geometrischen Objekten auftreten können.

Beispiel 1.2 Wir betrachten Gleichungen der Form

$$ax + by = c, \quad a, b, c \in \mathbb{Z}.$$

Eine solche Gleichung nennt man eine *diophantische Gleichung*. Wir suchen nach ganzzahligen Lösungen einer solchen Gleichung. Wir werden ein Kriterium für die Lösbarkeit einer solchen Gleichung herleiten, und wir werden sehen, wie man die Lösungen einer solchen Gleichung praktisch bestimmen kann.

Beispiel 1.3 Die Kodierungstheorie befasst sich mit sogenannten fehlerkorrigierenden Kodes, die zur korrekten Übermittlung von Daten notwendig sind. Solche Kodes werden zum Beispiel bei der CD angewandt. Wir betrachten hier als Beispiel nur *binäre* Kodes, d.h. Kodes, bei denen nur die Symbole 0 und 1 verwendet werden, deren Wörter also Folgen von Bits sind. Bei der Übermittlung solcher Folgen können nun Fehler auftreten, d.h. eine 0 wird irrtümlich als 1 gelesen und umgekehrt. Um solche Fehler entdecken und nachträglich korrigieren zu können, baut man eine gewisse Redundanz ein. Ein Standardbeispiel ist das *Parity Check Bit*. Wir betrachten das Beispiel des *(3,2)-Parity-Check-Kodes*. Hier bestehen die zu übermittelnden Botschaften aus zwei Bits. Wir fügen dazu ein drittes Bit wie folgt zu:

Botschaft	Kodewort
00	000
01	011
10	101
11	110

Wenn bei der Übermittlung der Kodewörter ein Fehler auftritt, also zum Beispiel 101 als 100 übermittelt wird, so kann man diesen Fehler entdecken, da das empfangene Wort eine ungerade Anzahl von 1'en enthält. Dieser Fehler kann aber nicht korrigiert werden, da das Wort 100 mit gleicher Wahrscheinlichkeit von 000, 110 oder 101 herkommen konnte.

Die Menge $\{0,1\}$ nennt man das *Alphabet* des Codes. Diese Menge kann mit der Struktur eines *Körpers* versehen werden. Wir definieren eine Addition und Multiplikation wie folgt:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Die Menge $\{0,1\}$ mit dieser Struktur nennt man den Körper $\mathbb{F}_2$. Ein Kode C der *Länge* n ist eine Teilmenge von $\mathbb{F}_2^n$. Es sei C ein Code der Länge n. Dann kann man ein Kodewort $a_0a_1\dots a_{n-1}$ von C auch durch ein Polynom

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_2[x]$$

vom Grad $\leq n-1$ mit Koeffizienten im Körper $\mathbb{F}_2$ darstellen.

Es sei $p(x) \in \mathbb{F}_2[x]$ ein Polynom von einem Grad kleiner als n. Dann ist der *von* $p(x)$ *erzeugte Polynomkode* derjenige Kode, der aus allen Polynomen vom Grad kleiner als n besteht, die durch $p(x)$ teilbar sind. Z.B. ist der oben betrachtete (3,2)-Parity-Check-Kode C ein Polynomkode. Er wird durch das Polynom $p(x) = 1 + x$ erzeugt. Denn es gilt

$$0 = 0(1+x), \quad x + x^2 = x(1+x), \quad 1 + x^2 = (1+x)(1+x).$$

Also sind alle Polynome in C durch $1+x$ teilbar. Andererseits gilt

$$(a_0 + a_1x + a_2x^2)(1+x) = a_0 + (a_0+a_1)x + (a_1+a_2)x^2 + a_2x^3.$$

Daraus folgt, dass ein durch $1+x$ teilbares Polynom vom Grad kleiner als 3 aus $\mathbb{F}_2[x]$ von der Form

$$a_0 + (a_0+a_1)x + a_1x^2$$

sein muss. Die Summe der Koeffizienten eines solchen Polynoms ist aber 0. Also liegt ein solches Polynom in C.

2 Gruppen

Wir erinnern zunächst an die Definition einer Gruppe, die wir schon in Lineare Algebra A hatten.

Definition Eine Menge G zusammen mit einer Verknüpfung $*$ heißt *Gruppe* genau dann, wenn folgende Axiome erfüllt sind:

(A) $(a*b)*c = a*(b*c)$ für alle $a,b,c \in G$ (*Assoziativgesetz*).

(N) Es gibt ein $e \in G$ mit $a*e = a$ für alle $a \in G$ (*Neutrales Element*).

(I) Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a*a' = e$ (*Inverses Element*).

Die Gruppe heißt *abelsch* (oder *kommutativ*), falls zusätzlich folgendes Axiom erfüllt ist:

(K) $a*b = b*a$ für alle $a,b \in G$ (*Kommutativgesetz*).

Beispiel 2.1 Als Beispiele für Gruppen hatten wir bereits betrachtet: $(\mathbb{R},+)$ und $(\mathbb{R}^*,\cdot)$ sind abelsche Gruppen. $(\mathrm{GL}(n),*)$ mit der Verknüpfung $A*B := AB$ für $A,B \in \mathrm{GL}(n)$ ist eine Gruppe.

Wir hatten bereits den folgenden Satz bewiesen:

Satz 2.1 *Ist G eine Gruppe, so gilt:*

(a) *Das neutrale Element $e \in G$ ist eindeutig bestimmt und hat auch die Eigenschaft $e*a = a$ für alle $a \in G$.*

(b) *Das inverse Element a' zu einem Element $a \in G$ ist eindeutig bestimmt und hat auch die Eigenschaft $a'*a = e$. Wir bezeichnen es mit a^{-1}.*

(c) *$(a^{-1})^{-1} = a$ für alle $a \in G$.*

(d) *$(a*b)^{-1} = b^{-1}*a^{-1}$ für alle $a,b \in G$.*

(e) *Es gelten die folgenden Kürzungsregeln:*

$$a * x = a * \tilde{x} \Rightarrow x = \tilde{x} \text{ und } y * a = \tilde{y} * a \Rightarrow y = \tilde{y}.$$

Wir wollen nun weitere Beispiele für Gruppen betrachten.

Beispiel 2.2 $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sind abelsche Gruppen, $(\mathbb{N}, +)$ ist keine Gruppe, da z.B. 2 kein inverses Element in $\mathbb{N}$ besitzt.

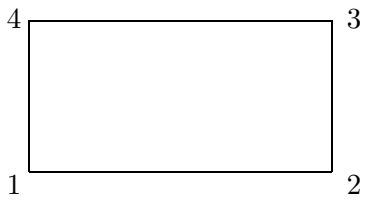
Eine weitere Klasse von Beispielen sind Symmetriegruppen von geometrischen Figuren.

Definition Es sei F eine geometrische Figur in der Ebene oder im Raum. Eine *Symmetrie der Figur* F ist eine bijektive Abbildung $f : F \to F$, die Abstände erhält, d.h. für alle Punkte $p, q \in F$ ist der Abstand von $f(p)$ zu $f(q)$ gleich dem Abstand von p zu q.

Die Menge aller Symmetrien einer geometrischen Figur bildet mit der Hintereinanderausführung als Verknüpfung eine Gruppe, da die Hintereinanderausführung von zwei abstandserhaltenden Abbildungen wieder abstandserhaltend ist und das Inverse einer abstandserhaltenden Abbildung ebenfalls abstandserhaltend ist. Man nennt diese Gruppe die *Symmetriegruppe der Figur*.

In Beispiel 1.1 haben wir ein Beispiel einer solchen Symmetriegruppe gesehen.

Beispiel 2.3 Als weiteres Beispiel betrachten wir die Symmetriegruppe eines Rechtecks mit ungleichen Seiten:



Wir haben die folgenden Symmetrien, die die Abstände erhalten: die Spiegelung a an einer horizontalen Achse durch den Mittelpunkt, d.h.

$$a : (1, 2, 3, 4) \mapsto (4, 3, 2, 1),$$

die entsprechende Spiegelung b an einer vertikalen Achse durch den Mittelpunkt, d.h.

$$b : (1, 2, 3, 4) \mapsto (2, 1, 4, 3),$$

und die Drehung c um 180° um den Mittelpunkt, d.h.

$$c : (1, 2, 3, 4) \mapsto (3, 4, 1, 2).$$

Schließlich ist die identische Abbildung e eine Symmetrie. Die Gruppentafel sieht nun wie folgt aus

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Diese Gruppe nennt man auch die *Kleinsche Vierergruppe* nach dem Mathematiker Felix Klein (1849–1925).

Notation Wir lassen im Folgenden das Verknüpfungszeichen $*$ weg, d.h. $a * b$ wird einfach als ab geschrieben.

Definition Eine nichtleere Teilmenge H einer Gruppe G heißt *Untergruppe* von G genau dann, wenn die folgenden Bedingungen erfüllt sind:

(UG1) Für alle $a, b \in H$ gilt $ab \in H$.

(UG2) Für alle $a \in H$ gilt $a^{-1} \in H$.

Satz 2.2 *Eine Untergruppe H einer Gruppe G ist mit der induzierten Verknüpfung eine Gruppe.*

Beweis. Wir müssen zeigen, dass die Gruppenaxiome in H erfüllt sind. Nach (UG1) induziert die Verknüpfung auf G eine Verknüpfung auf H. Das Assoziativgesetz gilt in H, da es in G gilt. Da H nicht leer ist, enthält H mindestens ein Element $h \in H$. Nach (UG2) ist auch $h^{-1} \in H$. Damit ist auch $e = hh^{-1} \in H$. Nach (UG2) liegt zu jedem Element $a \in H$ das inverse Element a^{-1} in H. Also erfüllt H die Gruppenaxiome. □

Bemerkung 2.1 Die Bedingungen (UG1) und (UG2) sind zu der folgenden einzigen Bedingung äquivalent

(UG) Für alle $a, b \in H$ gilt $ab^{-1} \in H$.

Beispiel 2.4 Die Gruppe $\mathbb{Z}$ ist eine Untergruppe von $\mathbb{Q}$, $\mathbb{Q}$ ist eine Untergruppe von $\mathbb{R}$ und $\mathbb{R}$ ist eine Untergruppe von $\mathbb{C}$.

Beispiel 2.5 In Lineare Algebra B haben wir Permutationen der Menge $\{1, 2, \ldots, n\}$ betrachtet und gezeigt, dass die Menge der Permutationen mit der Hintereinanderschaltung als Verknüpfung eine Gruppe bildet. Diese Gruppe heißt die *symmetrische Gruppe von n Elementen* und wird mit S_n bezeichnet. Es sei A_n die Menge aller geraden Permutationen. Da die Hintereinanderschaltung von zwei geraden Permutationen wieder gerade ist und auch das Inverse einer geraden Permutation gerade ist, ist A_n eine Untergruppe von S_n. Sie wird die *alternierende Gruppe von n Elementen* genannt.

Definition Die Anzahl der Elemente einer Gruppe G wird mit $|G|$ bezeichnet und die *Ordnung der Gruppe* genannt. Die Gruppe G heißt *endliche Gruppe*, wenn $|G|$ endlich ist, andernfalls heißt G *unendliche Gruppe*.

Beispiel 2.6 Die Ordnung der Gruppe S_n ist $n!$, wie wir in Lineare Algebra B gesehen haben.

Eine wichtige Klasse von Gruppen sind die zyklischen Gruppen.

Definition Eine Gruppe G heißt *zyklisch* genau dann, wenn ein Element $g \in G$ existiert, so dass $G = \{g^n \mid n \in \mathbb{Z}\}$. in diesem Fall sagt man, dass g die zyklische Gruppe G *erzeugt*.

Bemerkung 2.2 Eine zyklische Gruppe G ist abelsch, da

$$g^n g^m = g^{n+m} = g^m g^n.$$

Beispiel 2.7 Die Gruppe $\mathbb{Z}$ ist eine unendliche zyklische Gruppe, die von dem Element 1 (oder -1) erzeugt wird.

Definition Die *Ordnung eines Elements* g in einer Gruppe G ist die kleinste positive ganze Zahl r, so dass $g^r = e$ ist. Wenn keine solche Zahl r existiert, so sagt man, dass die Ordnung des Elements g *unendlich* ist.

Satz 2.3 *Wenn g ein Element der Ordnung k der Gruppe G ist, dann ist $H = \{g^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G der Ordnung k.*

Definition In diesem Fall nennt man H *die von g erzeugte zyklische Untergruppe* von G.

Beweis. Wir zeigen zunächst, dass H eine Untergruppe von G ist. Das Axiom (UG1) ist erfüllt, da $g^m g^n = g^{m+n} \in H$, (UG2), da $(g^m)^{-1} = g^{-m} \in H$ für alle $m, n \in \mathbb{Z}$ ist.

Nun zeigen wir, dass H die Ordnung k hat.

Es sei zunächst $k = \infty$. Dann zeigen wir, dass alle Elemente g^n verschieden sind. Denn angenommen, $g^n = g^m$, wobei $m < n$. Dann gilt $n - m > 0$ und $g^{n-m} = e$. Das ist aber eine Widerspruch dazu, dass g unendliche Ordnung hat. Also ist die Ordnung von H unendlich.

Es sei nun $k < \infty$. Dann zeigen wir:

Behauptung $H = \{g^0 = e, g^1, g^2, \ldots, g^{k-1}\}$.

Beweis. Zunächst zeigen wir, dass die Elemente g^n, $n = 0, 1, \ldots, k-1$, alle verschieden sind. Angenommen, $g^n = g^m$, wobei $0 \leq m < n \leq k-1$. Dann folgt $g^{n-m} = e$ mit $0 < n - m < k$. Dies widerspricht der Minimalität von k, der Ordnung von g. Also sind die Elemente g^0, g^1, $\ldots$, g^{k-1} alle

verschieden. Für ein beliebiges anderes Element g^m können wir $m = qk + r$ mit $0 \leq r < k$ schreiben. Dann gilt

$$g^m = g^{qk+r} = \left(g^k\right)^q (g^r) = (e^q)\,(g^r) = g^r.$$

Also liegt g^m in H. Damit ist die Behauptung bewiesen. □

Aus der Behauptung folgt nun, dass $|H| = k$. □

Beispiel 2.8 Die von der Zahl 2 in $\mathbb{Z}$ erzeugte zyklische Untergruppe von $\mathbb{Z}$ enthält alle geraden Zahlen und wir bezeichnen diese Untergruppe mit $2\mathbb{Z} = \{2n \,|\, n \in \mathbb{Z}\}$.

Satz 2.4 *Ist G eine endliche Gruppe der Ordnung n und besitzt G ein Element g der Ordnung n, so ist G eine zyklische Gruppe, die von g erzeugt ist.*

Beweis. Es sei H die von g erzeugte zyklische Untergruppe von G. Nach dem vorhergehenden Satz hat H die Ordnung n. Aus $H \subset G$ und $|H| = |G| = n < \infty$ folgt aber $H = G$. Also ist G die von g erzeugte zyklische Gruppe. □

Beispiel 2.9 Es sei C_n die Gruppe der Drehungen eines regulären n-Ecks in der Ebene. Dann ist C_n eine zyklische Gruppe der Ordnung n, die von einer Drehung um den Winkel $\frac{2\pi}{n}$ erzeugt wird. Denn C_n hat die Ordnung n: Wenn wir die Ecken des n-Ecks mit $1, 2, \ldots n$ bezeichnen, so werden bei einer Drehung die Eckennummern zyklisch vertauscht. Bezeichnet g die Drehung des n-Ecks um den Winkel $\frac{2\pi}{n}$, so hat g die Ordnung n. Nach Satz 2.4 ist C_n zyklisch von der Ordnung n und wird von g erzeugt.

Beispiel 2.10 Die Kleinsche Vierergruppe ist nicht zyklisch, da sie die Ordnung 4 hat, aber kein Element der Ordnung 4 besitzt.

Definition Es seien $(G, *)$ und $(H, \cdot)$ zwei Gruppen. Eine Abbildung $f : G \to H$ heißt *Gruppenhomomorphismus* genau dann, wenn gilt

$$f(a * b) = f(a) \cdot f(b).$$

Ein bijektiver Gruppenhomomorphismus heißt *Isomorphismus*. Die Gruppen G und H heißen *isomorph*, falls es einen Isomorphism $f : G \to H$ gibt. In diesem Fall schreiben wir $G \cong H$.

Beispiel 2.11 (1) Es seien G und H Gruppen und e das neutrale Element von H. Die Abbildung $f : G \to H$ mit $f(a) = e$ für alle $a \in G$ ist ein Gruppenhomomorphismus.

(2) Ist H eine Untergruppe von G, so ist die Inklusionsabbildung $i : H \to G$ ein Gruppenhomomorphismus.

(3) Es sei $f : \mathbb{Z} \to \{1, -1\}$ definiert durch $f(n) = 1$, falls n gerade, und $f(n) = -1$, falls n ungerade. Dann ist f ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\{1, -1\}, \cdot)$

Satz 2.5 *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(i) *$f(e_G) = e_H$, wobei e_G bzw. e_H das neutrale Element von G bzw. H ist.*

(ii) *$f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.*

Beweis. (i) Da f ein Gruppenhomomorphismus ist, gilt

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G).$$

Daraus folgt

$$e_H = f(e_G)^{-1} f(e_G) = f(e_G)^{-1} f(e_G) f(e_G) = e_H f(e_G) = f(e_G).$$

(ii) Nach (i) gilt

$$f(a) f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H.$$

Da das inverse Element zu $f(a)$ eindeutig bestimmt ist, folgt $f(a^{-1}) = f(a)^{-1}$. □

Satz 2.6 *Zyklische Gruppen der gleichen Ordnung sind isomorph.*

Beweis. Es seien G und H zyklische Gruppen, die von g bzw. h erzeugt werden. Wenn G und H unendliche Ordnung haben, so definieren wir $f : G \to H$ durch $f(g^r) = h^r$ für alle $r \in \mathbb{Z}$. Dann ist f bijektiv. Es gilt

$$f(g^r g^s) = f(g^{r+s}) = h^{r+s} = h^r h^s = f(g^r) f(g^s).$$

Also ist f ein Isomorphismus.

Wenn G und H die Ordnung n haben, so definieren wir $f : G \to H$ durch $f(g^r) = h^r$ für $r = 0, 1, \ldots, n-1$. Dann ist f bijektiv. Für $0 \le r, s \le n-1$ sei $r + s = kn + l$, wobei $0 \le l \le n-1$. Dann gilt

$$f(g^r g^s) = f(g^{r+s}) = f(g^{kn+l}) = f((g^n)^k g^l) = f(e^k g^l) = f(g^l) = h^l$$

und

$$f(g^r) f(g^s) = h^r h^s = h^{r+s} = h^{kn+l} = (h^n)^k h^l = e^k h^l = h^l.$$

Also ist f ein Isomorphismus. □

Also ist jede zyklische Gruppe entweder isomorph zu $\mathbb{Z}$ oder zu C_n für ein gewisses n. Im nächsten Abschnitt werden wir eine weitere wichtige Klasse von zyklischen Gruppen kennenlernen, die Gruppen $\mathbb{Z}_n$. Aus dem obigen Satz folgt $\mathbb{Z}_n \cong C_n$.

Bemerkung 2.3 Ein Gruppenhomomorphismus $f : G \to H$ von einer *zyklischen* Gruppe G auf eine beliebige Gruppe H ist schon durch das Bild eines erzeugenden Element $g \in G$ bestimmt. Denn gilt $f(g) = h$, so folgt aus der Definition des Gruppenhomomorphismus, dass $f(g^r) = f(g)^r = h^r$ für alle $r \in \mathbb{Z}$ gilt.

Satz 2.7 *Ist $f : G \to H$ ein Isomorphismus und gilt $f(g) = h$, so haben g und h die gleiche Ordnung.*

Beweis. Angenommen, g hat die Ordnung m und h hat die Ordnung n. Ist $m < \infty$, so gilt

$$h^m = f(g)^m = f(g^m) = f(e) = e.$$

Daraus folgt, dass auch n endlich ist und $n \leq m$ gilt.

Ist n endlich, so gilt

$$f(g^n) = f(g)^n = h^n = e = f(e).$$

Da f bijektiv ist, folgt daraus $g^n = e$. Also ist auch m endlich und es gilt $n \leq m$.

Also sind entweder m und n beide endlich und es gilt $m = n$, oder $m = n = \infty$. □

3 Quotientengruppen

Eine wichtige Konstruktionsmethode für Gruppen ist die Quotientenkonstruktion, die wir nun betrachten wollen. Dazu führen wir den Begriff einer Äquivalenzrelation ein.

Eine *Relation* R auf einer Menge M ist eine Teilmenge von $M \times M$. Für $(a, b) \in R$ schreiben wir $a \sim b$.

Definition Eine Relation $\sim$ auf einer Menge M heißt *Äquivalenzrelation*, wenn die folgenden Bedingungen erfüllt sind:

(R) $a \sim a$ für alle $a \in M$ (*Reflexivität*).

(S) Für alle $a, b \in M$ gilt: Aus $a \sim b$ folgt $b \sim a$ (*Symmetrie*).

(T) Für alle $a, b, c \in M$ gilt: Aus $a \sim b$ und $b \sim c$ folgt $a \sim c$ (*Transitivität*).

Ist $\sim$ eine Äquivalenzrelation auf M und $a \in M$, dann heißt

$$[a] := \bar{a} := \{x \in M \mid x \sim a\}$$

die *Äquivalenzklasse* von a. Die Menge aller Äquivalenzklassen heißt die *Quotientenmenge* von M nach $\sim$ und wird mit $M/\sim$ bezeichnet. Es gilt also

$$M/\sim := \{[a] \mid a \in M\}.$$

Satz 3.1 *Ist $\sim$ eine Äquivalenzrelation auf M, dann gilt:*

(i) *Aus $a \sim b$ folgt $[a] = [b]$.*

(ii) *Aus $[a] \cap [b] \neq \emptyset$ folgt $a \sim b$.*

(iii) *Die Äquivalenzklassen bilden eine* Partition *von M, d.h. M kann als die disjunkte Vereinigung der verschiedenen Äquivalenzklassen geschrieben werden.*

Beweis. (i) Es sei $a \sim b$ und $x \in [a]$. Dann gilt $x \sim a$ und aus der Transitivität folgt $x \sim b$. Also gilt $x \in [b]$. Daraus folgt $[a] \subset [b]$.

Aus der Symmetrie folgt $b \sim a$ und wir können in dem obigen Argument die Rollen von a und b vertauschen. Also folgt $[b] \subset [a]$ und damit $[a] = [b]$.

(ii) Es sei $x \in [a] \cap [b]$. Dann gilt $x \sim a$ und $x \sim b$. Aus der Symmetrie und Transitivität folgt dann $a \sim b$.

(iii) Aus (i) und (ii) folgt, dass zwei Äquivalenzklassen entweder gleich oder disjunkt sind. Aus der Reflexivität folgt, dass jedes Element $a \in M$ in der Äquivalenzklasse $[a]$ liegt. Also ist M die disjunkte Vereinigung aller Äquivalenzklassen. □

Beispiel 3.1 Es sei n eine feste positive ganze Zahl und a, b seien zwei ganze Zahlen. Dann definieren wir

$$a \equiv b \bmod n :\Leftrightarrow n|(a-b).$$

Für $a \equiv b \bmod n$ sagen wir: *a ist kongruent zu b modulo n.* Hier bedeutet $n|(a-b)$: n teilt $a-b$. Dies definiert eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. (i) Für alle $a \in \mathbb{Z}$ gilt $n|(a-a)$. Also gilt $a \equiv a \bmod n$.

(ii) Aus $a \equiv b \bmod n$ folgt $n|(a-b)$, also auch $n|-(a-b)$. Daher gilt $n|(b-a)$ und $b \equiv a \bmod n$.

(iii) Es gelte $a \equiv b \bmod n$ und $b \equiv c \bmod n$. Dann folgt $n|(a-b)$ und $n|(b-c)$, also $n|((a-b)+(b-c))$. Also gilt $n|(a-c)$ und $a \equiv c \bmod n$. □

Definition Die Menge der Äquivalenzklassen unter der Äquivalenzrelation $a \equiv b \bmod n$ heißt die *Menge der ganzen Zahlen modulo n* und wird mit $\mathbb{Z}_n$ bezeichnet.

Beispiel 3.2 Die Äquivalenzklassen modulo 3 sind

$$\begin{aligned} [0] &= \{\dots, -3, 0, 3, 6, 9, \dots\}, \\ [1] &= \{\dots, -2, 1, 4, 7, 10, \dots\}, \\ [2] &= \{\dots, -1, 2, 5, 8, 11, \dots\}. \end{aligned}$$

Also ist $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Wir können die Kongruenzrelation modulo n auf $\mathbb{Z}$ auch so definieren: $a \equiv b \bmod n$ genau dann, wenn $a - b \in n\mathbb{Z}$, wobei $n\mathbb{Z}$ die Untergruppe von $\mathbb{Z}$ ist, die aus allen Vielfachen von n besteht. Wir wollen nun diese Kongruenzrelation auf beliebige Untergruppen von Gruppen erweitern.

Definition Es sei G eine Gruppe, H eine Untergruppe von G und $a, b \in G$. Dann sagen wir, *a ist kongruent zu b modulo H*, in Zeichen $a \equiv b \bmod H$, genau dann, wenn $ab^{-1} \in H$ gilt.

Satz 3.2 *Die Relation $a \equiv b \bmod H$ ist eine Äquivalenzrelation auf G. Die Äquivalenzklasse von a ist von der Form $Ha := \{ha \mid h \in H\}$.*

Definition Die Menge $Ha := \{ha \mid h \in H\}$ wird eine *Rechtsnebenklasse* von H in G genannt. Das Element a heißt ein *Repräsentant* der Rechtsnebenklasse Ha.

Beweis. (i) Die Relation ist reflexiv, da für alle $a \in G$ gilt $aa^{-1} = e \in H$.

(ii) Aus $a \equiv b \bmod H$ folgt $ab^{-1} \in H$. Da H eine Untergruppe ist, ist auch $(ab^{-1})^{-1} = ba^{-1} \in H$. Also folgt $b \equiv a \bmod H$. Die Relation ist daher symmetrisch.

(iii) Aus $a \equiv b \bmod H$ und $b \equiv c \bmod H$ folgt $ab^{-1} \in H$ und $bc^{-1} \in H$. Da H eine Untergruppe ist, gilt $ab^{-1}bc^{-1} = ac^{-1} \in H$, also $a \equiv c \bmod H$. Daher ist die Relation auch transitiv.

Wir zeigen nun: $[a] = Ha$. Es sei zunächst $x \in [a]$. Dann gilt $x \equiv a \bmod H$. Also ist $h := xa^{-1} \in H$. Nun gilt aber $x = ha$. Also ist $x \in Ha$. Damit gilt $[a] \subset Ha$. Sei umgekehrt $x \in Ha$. Dann gibt es ein $h \in H$ mit $x = ha$. Daraus folgt aber $xa^{-1} = h \in H$, also $x \equiv a \bmod H$ und damit $x \in [a]$. Daraus folgt $Ha \subset [a]$ und damit $[a] = Ha$. □

Beispiel 3.3 Die Rechtsnebenklassen von A_3 in S_3 sind

$$\begin{aligned} [(1,2,3)] &= \{(1,2,3),(2,3,1),(3,1,2)\} = A_3(1,2,3) \\ [(1,3,2)] &= \{(1,3,2),(3,2,1),(2,1,3)\} = A_3(1,3,2) \end{aligned}$$

Lemma 3.1 *Zwischen je zwei Rechtsnebenklassen von H in G gibt es eine bijektive Abbildung.*

Beweis. Es sei Ha eine Rechtsnebenklasse von H in G. Um die Behauptung zu zeigen, genügt es, eine bijektive Abbildung von H nach Ha zu konstruieren.

Wir definieren $\psi : H \to Ha$ durch $\psi(h) = ha$. Nach Definition der Menge Ha ist ψ surjektiv. Die Abbildung ψ ist auch injektiv: Dazu nehmen wir $\psi(h_1) = \psi(h_2)$ an. Daraus folgt $h_1 a = h_2 a$. Indem wir beide Seiten dieser Gleichung von rechts mit a^{-1} multiplizieren, erhalten wir $h_1 = h_2$. Also ist ψ bijektiv. □

Satz 3.3 (Satz von Lagrange) *Ist G eine endliche Gruppe und H eine Untergruppe von G, so teilt die Ordnung von H die Ordnung von G.*

Beweis. Die Rechtsnebenklassen von H in G bilden eine Partition von G. Also kann G als die disjunkte Vereinigung

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$$

für gewisse endlich viele Elemente $a_1, a_2, \ldots, a_k \in G$ geschrieben werden. Nach Lemma 3.1 ist die Anzahl der Elemente in jeder Rechtsnebenklasse gleich, nämlich $|H|$. Da die obige Vereinigung disjunkt ist, folgt $|G| = k|H|$. Also teilt $|H|$ die Ordnung $|G|$ von G. □

Definition Es sei H eine Untergruppe von G. Die Anzahl der verschiedenen Rechtsnebenklassen von H in G heißt der *Index* von H in G und wird mit $[G : H]$ bezeichnet.

Korollar 3.1 *Ist G eine endliche Gruppe und H eine Untergruppe von G, so gilt*

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

Korollar 3.2 *Ist G eine endliche Gruppe und a ein Element von G, so teilt die Ordnung von a die Ordnung von G.*

Beweis. Es sei $H := \{a^r \mid r \in \mathbb{Z}\}$ die von a erzeugte zyklische Untergruppe von G. Nach Satz 2.3 ist die Gruppenordnung von H gleich der Ordnung von a. Also teilt die Ordnung von a nach dem Satz von Lagrange die Ordnung von G. □

Korollar 3.3 *Ist G eine endliche Gruppe und a ein Element von G, dann gilt*

$$a^{|G|} = e.$$

Beweis. Es sei m die Ordnung von a. Nach Korollar 3.2 gilt $|G| = mk$ für ein $k \in \mathbb{Z}$. Also gilt

$$a^{|G|} = a^{mk} = (a^m)^k = e^k = e.$$

□

Korollar 3.4 *Ist die Ordnung der Gruppe G eine Primzahl, so ist G zyklisch.*

Beweis. Es sei $|G| = p$, wobei p eine Primzahl ist. Nach Korollar 3.2 hat jedes Element die Ordnung 1 oder p. Ordnung 1 hat aber nur das neutrale Element. Da $|G| \geq 2$ gibt es also mindestens ein Element a der Ordnung p. Nach Satz 2.4 ist G zyklisch. □

Wir wollen nun auf der Quotientenmenge G/H eine Gruppenstruktur definieren. Dies ist allerdings nicht immer möglich, sondern nur in dem Fall, dass H ein Normalteiler ist.

Definition Eine Untergruppe H einer Gruppe G heißt *Normalteiler* von G, falls für alle $g \in G$ und $h \in H$ gilt: $g^{-1}hg \in H$.

Satz 3.4 *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*

Beweis. Es sei H eine Untergruppe der abelschen Gruppe G. Dann gilt für alle $g \in G$ und $h \in H$

$$g^{-1}hg = hg^{-1}g = h \in H.$$

Also ist H ein Normalteiler. □

Satz 3.5 *Es sei N ein Normalteiler einer Gruppe G. Dann bildet die Menge der Rechtsnebenklassen $G/N = \{Ng \,|\, g \in G\}$ zusammen mit der Verknüpfung*

$$(Ng_1) \cdot (Ng_2) := N(g_1g_2)$$

eine Gruppe.

Definition Diese Gruppe heißt die *Quotientengruppe* oder *Faktorgruppe* von G nach N.

Beweis. Die Verknüpfung auf G/N ist mit Hilfe von Repräsentanten g_1 und g_2 der Rechtsnebenklassen definiert. Wir müssen zunächst zeigen, dass diese Verknüpfung *wohldefiniert* ist, d.h. nicht von der Auswahl der Repräsentanten abhängt. Das bedeutet, dass wir zeigen müssen, dass, wenn wir andere Elemente $h_1 \in Ng_1$ und $h_2 \in Ng_2$ in den gleichen Rechtsnebenklassen wählen, die Rechtsnebenklassen $N(h_1h_2)$ und $N(g_1g_2)$ übereinstimmen.

Aus $h_1 \in Ng_1$ folgt $h_1g_1^{-1} = n_1 \in N$ und aus $h_2 \in Ng_2$ folgt $h_2g_2^{-1} = n_2 \in N$. Zu zeigen ist $Nh_1h_2 = Ng_1g_2$ oder $h_1h_2(g_1g_2)^{-1} \in N$. Nun gilt aber

$$h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = h_1n_2g_1^{-1} = h_1g_1^{-1}g_1n_2g_1^{-1} = n_1g_1n_2g_1^{-1}.$$

Da N ein Normalteiler ist, ist $g_1n_2g_1^{-1} = n_3 \in N$. Daraus folgt aber $n_1g_1n_2g_1^{-1} = n_1n_3 \in N$. Also folgt $h_1h_2(g_1g_2)^{-1} \in N$, was zu zeigen war. Deshalb ist die Verknüpfung wohldefiniert.

Nun müssen wir die Gruppenaxiome nachweisen.
Assoziativgesetz:

$$\begin{aligned}(Na \cdot Nb) \cdot Nc &= N(ab) \cdot Nc = N((ab)c)\\ Na \cdot (Nb \cdot Nc) &= Na \cdot N(bc) = N(a(bc)) = N((ab)c)\end{aligned}$$

Neutrales Element ist $Ne = N$ denn es gilt

$$Na \cdot Ne = N(ae) = Na.$$

Inverses Element: Das Inverse zu Na ist Na^{-1}, denn es gilt

$$Na \cdot Na^{-1} = N(aa^{-1}) = Ne.$$

Also ist G/N eine Gruppe. □

Ist G eine endliche Gruppe, so gilt für die Ordnung der Gruppe G/N:

$$|G/N| = [G : N] = |G|/|N|.$$

Beispiel 3.4 Die Gruppe $\mathbb{Z}_n$ ist die Quotientengruppe von $\mathbb{Z}$ nach der Untergruppe $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$.

Beweis. Da $\mathbb{Z}$ abelsch ist, ist jede Untergruppe ein Normalteiler. Es gilt

$$a \equiv b \bmod n\mathbb{Z} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n|(a-b) \Leftrightarrow a \equiv b \bmod n.$$

Also gilt $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ und die Verknüpfung auf $\mathbb{Z}_n$ ist definiert durch $[a] + [b] = [a + b]$. □

Die Gruppe $\mathbb{Z}_n$ ist eine zyklische Gruppe, die von $[1]$ erzeugt wird. Nach Satz 2.6 ist $\mathbb{Z}_n$ isomorph zu C_n. Als Beispiel stellen wir die Gruppentafel von $\mathbb{Z}_3$ auf:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Wenn es nicht zur Verwirrung führt, bezeichnen wir die Elemente von $\mathbb{Z}_n$ auch durch $0, 1, 2, \ldots, n-1$ anstelle von $[0], [1], [2], \ldots, [n-1]$.

Wir betrachten nun weiter Gruppenhomomorphismen.

Definition Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann definieren wir

$$\begin{aligned}\operatorname{Ker} f &:= \{g \in G \mid f(g) = e_H\},\\ \operatorname{Im} f &:= \{f(g) \mid g \in G\}.\end{aligned}$$

Satz 3.6 *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

(i) *$\operatorname{Ker} f$ ist ein Normalteiler von G.*

(ii) *f ist genau dann injektiv, wenn $\operatorname{Ker} f = \{e_G\}$ gilt.*

(iii) *$\operatorname{Im} f$ ist eine Untergruppe von H (nicht notwendig ein Normalteiler).*

Beweis. (i) Wir zeigen zunächst, dass $\operatorname{Ker} f$ eine Untergruppe von G ist. Dazu seien $a, b \in \operatorname{Ker} f$. Dann gilt

$$f(ab) = f(a)f(b) = e_H e_H = e_H, \text{ also } ab \in \operatorname{Ker} f$$

und

$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H, \text{ also } a^{-1} \in \operatorname{Ker} f.$$

Also ist $\operatorname{Ker} f$ eine Untergruppe von G.

Es sei nun $a \in \operatorname{Ker} f$ und $g \in G$. Dann gilt

$$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g)^{-1}e_H f(g) = f(g)^{-1}f(g) = e_H.$$

Daher ist $g^{-1}ag \in \operatorname{Ker} f$. Also ist $\operatorname{Ker} f$ ein Normalteiler.

(ii) Wenn f injektiv ist, dann gilt für $g \neq e_G$: $f(g) \neq e_H$. Also gilt $\operatorname{Ker} f = \{e_G\}$. Es sei umgekehrt $\operatorname{Ker} f = \{e_G\}$. Wir müssen zeigen, dass f injektiv ist. Dazu seien $g_1, g_2 \in G$ mit $f(g_1) = f(g_2)$. Dann gilt

$$f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_H, \text{ also } g_1 g_2^{-1} \in \operatorname{Ker} f.$$

Da $\operatorname{Ker} f = \{e_G\}$ gilt, folgt $g_1 g_2^{-1} = e_G$, also $g_1 = g_2$. Also ist f injektiv.

(iii) Es seien $h_1, h_2 \in \operatorname{Im} f$. Dann gilt $h_1 = f(g_1)$ und $h_2 = f(g_2)$ für $g_1, g_2 \in G$. Dann gilt $f(g_1)f(g_2) = f(g_1 g_2) \in \operatorname{Im} f$ und $f(g_1)^{-1} = f(g_1^{-1}) \in \operatorname{Im} f$. Also ist $\operatorname{Im} f$ eine Untergruppe von H. □

Satz 3.7 (Homomorphiesatz) *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Beweis. Es sei $K = \operatorname{Ker} f$. Wir definieren eine Abbildung $\psi : G/K \to \operatorname{Im} f$ durch $\psi(Kg) = f(g)$. Wir müssen zeigen:

(a) ψ ist wohldefiniert.

(b) ψ ist ein Gruppenhomomorphismus.

(c) ψ ist injektiv.

(d) ψ ist surjektiv.

Zu (a): Hierzu ist zu zeigen: Aus $Kg = Kg'$ folgt $f(g) = f(g')$. Es sei $Kg = Kg'$ für ein $g' \in G$. Dann gilt $g'g^{-1} = k \in K$. Daraus folgt

$$f(g') = f(kg) = f(k)f(g) = e_H f(g) = f(g).$$

Also ist ψ wohldefiniert.

Zu (b):

$$\psi(Kg_1Kg_2) = \psi(K(g_1g_2)) = f(g_1g_2) = f(g_1)f(g_2) = \psi(Kg_1)\psi(Kg_2).$$

Zu (c):

$$\psi(Kg) = e_H \Rightarrow f(g) = e_H \Rightarrow g \in K.$$

Also besteht der Kern von ψ nur aus der Rechtsnebenklasse K, die das neutrale Element von G/K ist. Daher ist ψ injektiv.

Zu (d): Nach Definition von ψ gilt $\operatorname{Im}\psi = \operatorname{Im} f$. Also ist ψ surjektiv. □

Beispiel 3.5 Es sei $f : \mathbb{Z} \to \mathbb{Z}_n$ mit $f(x) = [x]$. Dann ist f ein Gruppenhomomorphismus mit Kern $\operatorname{Ker} f = n\mathbb{Z}$. Aus dem Homomorphiesatz folgt $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Wenn man zwei Mengen M und N gegeben hat, dann kann man ihr kartesisches Produkt $M \times N := \{(x, y) \mid x \in M, y \in N\}$ bilden. Wir wollen nun zeigen, dass man auf dem kartesischen Produkt zweier Gruppen in natürlicher Weise eine Gruppenstruktur definieren kann.

Definition Es seien G und H zwei Gruppen. Dann definieren wir auf $G \times H$ eine Verknüpfung $*$ wie folgt

$$(g_1, h_1) * (g_2, h_2) = (g_1g_2, h_1h_2).$$

Man kann leicht zeigen, dass $G \times H$ mit dieser Verknüpfung eine Gruppe bildet. Das neutrale Element ist (e_G, e_H) und das inverse Element zu (g, h) ist (g^{-1}, h^{-1}). Die Gruppe $G \times H$ heißt das *direkte Produkt* der Gruppen G und H.

Beispiel 3.6 Wir betrachten die Gruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$. Die Gruppentafel sieht wie folgt aus

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Daraus folgt, dass die Gruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorph zur Kleinschen Vierergruppe ist.

Wir haben bereits gesehen, dass die Kleinsche Vierergruppe keine zyklische Gruppe ist. Daraus folgt $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. Es gilt aber:

Satz 3.8 *Ist* $\mathrm{ggT}(m,n) = 1$*, so ist* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Beweis. Wir definieren $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ durch $f([r]) = ([r],[r])$. Diese Abbildung ist wohldefiniert, denn aus $r \equiv r' \bmod mn$ folgt $r \equiv r' \bmod m$ und $r \equiv r' \bmod n$.

Aus

$$f([r]+[s]) = f([r+s]) = ([r+s],[r+s]) = ([r],[r])+([s],[s]) = f([r])+f([s])$$

folgt, dass f ein Gruppenhomomorphismus ist.

Es sei nun $r \in \operatorname{Ker} f$. Dann gilt $r \equiv 0 \bmod m$ und $r \equiv 0 \bmod n$. Also ist r durch m und n teilbar. Da $\mathrm{ggT}(m,n) = 1$ ist r durch mn teilbar. Also gilt $r \equiv 0 \bmod mn$. Daraus folgt $[r] = 0$ und $\operatorname{Ker} f = \{0\}$. Nach dem Homomorphiesatz ist $\mathbb{Z}_{mn}$ isomorph zum Bild $\operatorname{Im} f$ von f. Nun gilt $|\mathbb{Z}_{mn}| = mn$ und $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$. Also ist $\operatorname{Im} f = \mathbb{Z}_m \times \mathbb{Z}_n$ und f ist ein Isomorphismus. □

4 Ringe

Definition Eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring mit* 1 genau dann, wenn die folgenden Eigenschaften erfüllt sind:

(AG) R bildet zusammen mit der Verknüpfung $+$ eine abelsche Gruppe.

(MA) Für alle $a, b, c \in R$ gilt

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(*Assoziativgesetz der Multiplikation*).

(D) Für alle $a, b, c \in R$ gilt

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ und } (b + c) \cdot a = b \cdot a + c \cdot a$$

(*Distributivgesetz*).

(MN) Es existiert ein Element $1 \in R$, so dass für alle $a \in R$ gilt

$$1 \cdot a = a \cdot 1 = a$$

(*Existenz der 1*).

Ein Ring mit 1 R heißt *kommutativ* genau dann, wenn gilt:

(MK) Für alle $a, b \in R$ gilt

$$a \cdot b = b \cdot a$$

(*Kommutativgesetz der Multiplikation*).

Beispiel 4.1 (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind kommutative Ringe mit 1.

(2) $\mathrm{Mat}(n, n)$ ist ein Ring mit 1, der für $n > 1$ nicht kommutativ ist.

(3) $\mathbb{Z}_n$ ist ein kommutativer Ring mit 1, wobei die Addition und Multiplikation durch $[x] + [y] = [x + y]$ und $[x] \cdot [y] = [x \cdot y]$ für $x, y \in \mathbb{Z}$ definiert sind.

Beweis. Wir wissen bereits, dass $\mathbb{Z}_n$ mit der Addition eine abelsche Gruppe bildet.

Da die Multiplikation mit Hilfe von Repräsentanten definiert ist, müssen wir zeigen, dass sie wohldefiniert ist. Angenommen, $[x] = [x']$ und $[y] = [y']$. Dann folgt $x \equiv x' \bmod n$ und $y \equiv y' \bmod n$. Also gilt $x = x' + kn$ und $y = y' + ln$ für $k, l \in \mathbb{Z}$. Dann gilt

$$x \cdot y = (x' + kn) \cdot (y' + ln) = x' \cdot y' + (ky' + lx' + kln)n.$$

Also folgt $x \cdot y \equiv x' \cdot y' \bmod n$ and $[x \cdot y] = [x' \cdot y']$. Daher ist die Multiplikation wohldefiniert.

Die restlichen Axiome folgen nun aus der Definition der Addition und Multiplikation und den Eigenschaften der ganzen Zahlen. Die 1 ist [1]. Wir zeigen als Beispiel das Distributivgesetz:

$$\begin{aligned} [x] \cdot ([y] + [z]) &= [x] \cdot [y + z] = [x \cdot (y + z)] \\ &= [x \cdot y + x \cdot z] \\ &= [x \cdot y] + [x \cdot z] = [x] \cdot [y] + [x] \cdot [z]. \end{aligned}$$

□

Verknüpfungstafeln für $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(4) Es sei $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$. Dann ist $\mathbb{Q}(\sqrt{2})$ ein kommutativer Ring mit 1.

Beweis. Zunächst müssen wir zeigen, dass $+$ und $\cdot$ Verknüpfungen auf $\mathbb{Q}(\sqrt{2})$ definieren. Es seien $a, b, c, d \in \mathbb{Q}$. Dann gilt

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

da $(a+b), (c+d) \in \mathbb{Q}$. Ebenso

$$(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Nun müssen wir zeigen, dass die Axiome eines kommutativen Ringes mit 1 erfüllt sind. Das neutrale Element der Addition ist $0 = 0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Das additive Inverse eines Elements $a + b\sqrt{2}$ ist $(-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Die 1 ist $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Die restlichen Axiome gelten in $\mathbb{Q}(\sqrt{2})$, da sie in $\mathbb{R}$ gelten. □

Aus den Ringaxiomen leitet man die folgenden Eigenschaften eines Ringes ab.

Satz 4.1 (Vorzeichenregeln) *Es sei R ein Ring mit 1. Dann gilt für alle $a, b \in R$:*

(i) $a \cdot 0 = 0 \cdot a = 0$.

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) = a \cdot b$.

(iv) $(-1) \cdot a = -a$.

(v) $(-1) \cdot (-1) = 1$.

Beweis. (i) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Addition von $-(a \cdot 0)$ auf beiden Seiten ergibt $0 = a \cdot 0$. Analog zeigt man $0 \cdot a = 0$.

(ii)

$$\begin{aligned} & a \cdot (-b) + a \cdot b = a \cdot (-b+b) = a \cdot 0 \overset{\text{(i)}}{=} 0 \\ \Rightarrow \quad & a \cdot (-b) = -(a \cdot b). \end{aligned}$$

Analog $(-a) \cdot b = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) \overset{\text{(ii)}}{=} -(a \cdot (-b)) \overset{\text{(ii)}}{=} -(-(a \cdot b)) = a \cdot b$.

(iv) $(-1) \cdot a \overset{\text{(ii)}}{=} -(1 \cdot a) = -a$.

(v) $(-1) \cdot (-1) \overset{\text{(iii)}}{=} 1 \cdot 1 = 1$. □

Bemerkung 4.1 Ist $1 = 0$, so gilt $R = \{0\}$. Denn für $a \in R$ gilt $a = a \cdot 1 = a \cdot 0 = 0$. Der Ring $R = \{0\}$ heißt der *triviale Ring*. Alle anderen Ringe heißen *nichttrivial*.

5 Integritätsbereiche und Körper

Gilt in einem Ring mit 1

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0?$$

Beim Beispiel $\mathbb{Z}_4$ haben wir gesehen $[2] \cdot [2] = [0]$.

Definition Es sei R ein kommutativer Ring mit 1. Ein Element $a \in R$, $a \neq 0$, heißt *Nullteiler*, falls es ein $b \in R$, $b \neq 0$, gibt mit $a \cdot b = 0$.

Beispiel 5.1 $R = \mathbb{Z}_4$, $[2]$ ist ein Nullteiler, denn $[2] \cdot [2] = [0]$.

Definition Ein nichttrivialer kommutativer Ring R mit 1 heißt *Integritätsbereich*, falls R keine Nullteiler hat.

Beispiel 5.2 (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Integritätsbereiche.
(2) $\mathbb{Z}_4$ ist kein Integritätsbereich, da $[2]$ ein Nullteiler von $\mathbb{Z}_4$ ist.

Satz 5.1 (Kürzungsregel) *Ist R ein Integritätsbereich und $a \in R$, $a \neq 0$, dann gilt für alle $b, c \in R$:*

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

Beweis. Aus $a \cdot b = a \cdot c$ folgt $a \cdot (b - c) = a \cdot b - a \cdot c = 0$. Da $a \neq 0$ kein Nullteiler ist, folgt $b - c = 0$, also $b = c$. □

Definition Ein *Körper* ist ein Ring R mit 1, bei dem $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe bildet, d.h. R ist ein nichttrivialer kommutativer Ring mit 1 mit der Eigenschaft

(MI) Für alle $a \in R$ mit $a \neq 0$ gibt es ein $a^{-1} \in R$ mit

$$a \cdot a^{-1} = 1$$

(*Existenz des multiplikativen Inversen*).

Beispiel 5.3 (1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper.
(2) $\mathbb{Z}$ und $\mathbb{Z}_4$ sind keine Körper.
(3) $\mathbb{Q}(\sqrt{2})$ ist ein Körper. Ist $a + b\sqrt{2} \neq 0$, so gilt

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Satz 5.2 *Ein Körper ist ein Integritätsbereich.*

Beweis. Es sei K ein Körper und $a, b \in K$ mit $a \cdot b = 0$. Ist $a \neq 0$, so existiert ein inverses Element $a^{-1} \in K$. Also

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

□

Satz 5.3 *Ein endlicher Integritätsbereich ist ein Körper.*

Beweis. Es sei R ein endlicher Integritätsbereich. Wir müssen zeigen, dass jedes Element $a \neq 0$ ein multiplikatives Inverses besitzt. Dazu betrachten wir die Abbildung

$$\begin{array}{rccc} l_a: & R & \longrightarrow & R \\ & x & \longmapsto & a \cdot x \end{array}.$$

Diese Abbildung ist injektiv:

$$l_a(x) = l_a(y) \Leftrightarrow a \cdot x = a \cdot y \overset{\text{Satz 5.1}}{\Rightarrow} x = y.$$

Da R endlich ist, ist l_a auch surjektiv. Also gibt es ein $b \in R$ mit $l_a(b) = a \cdot b = 1$. □

Satz 5.4 *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Es sei zunächst n eine Primzahl. Nach dem vorherigen Satz reicht es zu zeigen, dass $\mathbb{Z}_n$ ein Integritätsbereich ist. Es sei $[a] \cdot [b] = [0]$ in $\mathbb{Z}_n$. Dann folgt $n|ab$. Da n eine Primzahl ist, gilt $n|a$ oder $n|b$. Also gilt $[a] = [0]$ oder $[b] = [0]$. Also besitzt $\mathbb{Z}_n$ keine Nullteiler.

Es sei nun n keine Primzahl. Dann können wir $n = rs$ schreiben, wobei r und s ganze Zahlen mit $1 < r < n$ und $1 < s < n$ sind. Dann gilt $[r] \neq [0]$ und $[s] \neq [0]$, aber $[r] \cdot [s] = [rs] = [0]$. Also besitzt $\mathbb{Z}_n$ Nullteiler und ist kein Körper. □

6 Polynomringe

Definition Es sei R ein kommutativer Ring mit 1. Ein *Polynom* über dem Ring R ist ein Ausdruck

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

wobei $a_0, a_1, a_2, \ldots, a_n \in R$ und $n \in \mathbb{N}$. Hier ist x eine Unbestimmte. Das Element a_i heißt der *Koeffizient* von x^i in $p(x)$. Einen Term $0x^i$ lassen wir weg und für $1x^i$ schrieben wir einfach x^i. Die größte Zahl n mit $a_n \neq 0$ heißt der *Grad* des Polynoms $p(x)$, in Zeichen $n = \operatorname{grad} p(x)$. Sind alle Koeffizienten von $p(x)$ gleich Null, so heißt $p(x)$ das *Nullpolynom*. Den Grad des Nullpolynoms definieren wir als $-\infty$.

Definition Die Menge aller Polynome in x über dem kommutativen Ring mit 1 R wird mit $R[x]$ bezeichnet. Also

$$R[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \,|\, a_i \in R, i = 0, \ldots, n\}.$$

Wir definieren eine Addition und Multiplikation von Polynomen

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{und} \quad q(x) = \sum_{i=0}^{m} b_i x^i$$

durch

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i,$$

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} c_k x^k, \quad \text{wobei} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Die Menge $R[x]$ zusammen mit dieser Addition und Multiplikation bildet einen kommutativen Ring mit 1, der der *Polynomring mit Koeffizienten aus* R heißt. Die Null ist das Nullpolynom und die 1 das konstante Polynom 1.

Satz 6.1 (Gradformel) *Wenn R ein Integritätsbereich ist und $p(x)$ und $q(x)$ Polynome in $R[x]$ sind, so gilt*

$$\operatorname{grad}(p(x) \cdot q(x)) = \operatorname{grad} p(x) + \operatorname{grad} q(x).$$

Beweis. Ist eins der beiden Polynome das Nullpolynom, so ist auch $p(x) \cdot q(x)$ das Nullpolynom. In diesem Fall ist die Behauptung richtig, da das Nullpolynom den Grad $-\infty$ hat.

Andernfalls sei $\operatorname{grad} p(x) = n$, $\operatorname{grad} q(x) = m$ und $p(x) = a_0 + \cdots + a_nx^n$, $q(x) = b_0 + \cdot + b_mx^m$, wobei $a_n \neq 0$, $b_m \neq 0$. Dann ist der Koeffizient der größten Potenz von x in $p(x) \cdot q(x)$ gleich a_nb_m. Es gilt aber $a_nb_m \neq 0$, da R keine Nullteiler besitzt. Also gilt $\operatorname{grad}(p(x) \cdot q(x)) = m + n$. □

Korollar 6.1 *Es sei R ein kommutativer Ring mit 1. Der Polynomring $R[x]$ ist genau dann ein Integritätsbereich, wenn R ein Integritätsbereich ist.*

Beweis. Indem wir einem $a \in R$ das konstante Polynom $a \in R[x]$ zuordnen, sehen wir, dass $R \subset R[x]$. Wenn also $R[x]$ keine Nullteiler enthält, dann enthält erst recht R keine Nullteiler. Es sei umgekehrt R ein Integritätsbereich. Sind nun $p(x)$ und $q(x)$ Polynome aus $R[x]$, die verschieden vom Nullpolynom sind, so ist nach der Gradformel auch $p(x) \cdot q(x)$ von Null verschieden. Also enthält $R[x]$ keine Nullteiler. □

Wenn a und b ganze Zahlen mit $b \neq 0$ sind, so gibt es eindeutig bestimmte ganze Zahlen q und r, so dass gilt

$$a = qb + r \quad \text{und} \quad 0 \leq r < |b|.$$

Die Zahl q heißt der *Quotient* bei Division von a durch b und r heißt der *Rest*. Wir betrachten nun Ringe, in denen eine solche *Division mit Rest* möglich ist.

Definition Ein Integritätsbereich R heißt ein *euklidischer Ring*, wenn es eine Abbildung $d : R \setminus \{0\} \to \mathbb{N}$ in die Menge der natürlichen Zahlen gibt, so dass gilt:

(a) Für alle $a, b \in R$ mit $a \neq 0$ und $b \neq 0$ gilt $d(a) \leq d(ab)$.

(b) Für alle $a, b \in R$ mit $b \neq 0$ gibt es Elemente $q, r \in R$ mit

$$a = qb + r, \quad \text{wobei entweder } r = 0 \text{ oder } d(r) < d(b).$$

Beispiel 6.1 $\mathbb{Z}$ ist ein euklidischer Ring, wenn wir $d(a) := |a|$ für $a \in \mathbb{Z}$, $a \neq 0$, setzen. Ein Körper K ist trivialerweise ein euklidischer Ring, wenn wir $d(a) = 1$ für alle $a \in K \setminus \{0\}$ setzen.

Satz 6.2 *Es sei K ein Körper. Dann ist der Polynomring $K[x]$ mit der Abbildung $d = \operatorname{grad}$ ein euklidischer Ring.*

Beweis. Die Eigenschaft (a) folgt aus der Gradformel.

Der Beweis von (b) folgt aus dem *Divisionsalgorithmus für Polynome*:

Behauptung Es seien $f(x), g(x) \in K[x]$ und $g(x)$ sei nicht das Nullpolynom. Dann gibt es eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$, so dass

$$f(x) = q(x) \cdot g(x) + r(x),$$

wobei $\operatorname{grad} r(x) < \operatorname{grad} g(x)$.

Beweis. (a) Wir zeigen zunächst die Existenz der Polynome $q(x)$ und $r(x)$.

Ist $f(x)$ das Nullpolynom oder $\operatorname{grad} f(x) < \operatorname{grad} g(x)$, dann können wir $f(x) = 0 \cdot g(x) + f(x)$ schreiben. Es sei also $f(x) \neq 0$ und $n := \operatorname{grad} f(x) \geq \operatorname{grad} g(x)$. Wir beweisen die Behauptung durch Induktion nach n.

Induktionsanfang: Es sei $n = 0$. Dann gilt $\operatorname{grad} f(x) = \operatorname{grad} g(x) = 0$, also $f(x) = a_0$, $g(x) = b_0$. Dann ist $f(x) = (a_0 b_0^{-1}) g(x)$.

Es sei nun $g(x)$ fest. Wir nehmen an, dass die Behauptung für alle Polynome $f(x)$ mit $\operatorname{grad} f(x) < n$ gilt. Es sei $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$ mit $a_n \neq 0$, $b_m \neq 0$, $n \geq m$. Dann setze

$$\tilde{f}(x) := f(x) - a_n b_m^{-1} x^{n-m} g(x).$$

Dann gilt $\operatorname{grad} \tilde{f}(x) < n$. Nach Induktionsannahme gibt es $\tilde{q}(x)$, $r(x)$ mit

$$\tilde{f}(x) = \tilde{q}(x) \cdot g(x) + r(x), \quad \text{wobei} \quad \operatorname{grad} r(x) < \operatorname{grad} g(x).$$

Also gilt

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + \tilde{f}(x) = (a_n b_m^{-1} x^{n-m} g(x) + \tilde{q}(x)) \cdot g(x) + r(x).$$

Dies ist eine Darstellung der gewünschten Form.

(b) Wir zeigen nun die Eindeutigkeit von $q(x)$ und $r(x)$. Es sei $f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x)$ mit $\operatorname{grad} r_2(x) \leq \operatorname{grad} r_1(x) < \operatorname{grad} g(x)$. Dann gilt

$$(q_2(x) - q_1(x)) \cdot g(x) = r_1(x) - r_2(x).$$

Ist $q_2(x) - q_1(x)$ nicht das Nullpolynom, so folgt aus der Gradformel

$$\operatorname{grad}(r_1(x) - r_2(x)) = \operatorname{grad}((q_2(x) - q_1(x)) \cdot g(x) \geq \operatorname{grad} g(x)),$$

im Widerspruch zu $\operatorname{grad}(r_1(x) - r_2(x)) < \operatorname{grad} g(x)$. Also gilt $q_1(x) = q_2(x)$ und damit auch $r_1(x) = r_2(x)$. □

□

Beispiel 6.2 In $\mathbb{Z}_3[x]$ gilt

$$\begin{array}{rcrcrcl|c|rcl}
x^3 & + & 2x^2 & + & & & 1 & : & x^2+2 & = & x+2 \\
\cline{1-7}\cline{9-11}
x^3 & + & & & 2x & & & & & & \\
\cline{1-5}
 & & 2x^2 & + & x & + & 1 & & & & \\
 & & 2x^2 & + & & & 1 & & & & \\
\cline{2-5}
 & & & & x & & & & & &
\end{array}$$

Es ist also $x^3 + 2x^2 + 1 = (x+2)(x^2+2) + x$.

Korollar 6.2 *Teilt man das Polynom $f(x) \in K[x]$ durch $(x - \alpha)$, dann ergibt sich als Rest $f(\alpha)$.*

Beweis. Nach dem Divisionsalgorithmus existieren $q(x), r(x) \in K[x]$ mit $f(x) = q(x)(x - \alpha) + r(x)$, wobei $\operatorname{grad} r(x) < 1$. Also ist $r(x) = r_0 \in K$ und $f(x) = q(x)(x - \alpha) + r_0$. Setzen wir hier $x = \alpha$ ein, so erhalten wir $f(\alpha) = r_0$. □

Korollar 6.3 *Das Polynom $f(x) \in K[x]$ ist genau dann durch $(x - a)$ teilbar, wenn $f(\alpha) = 0$.*

Beweis. Nach dem vorherigen Korollar gilt $f(x) = q(x)(x - \alpha) + f(\alpha)$. Also gilt $f(x) = q(x)(x - \alpha)$ genau dann, wenn $f(\alpha) = 0$. □

Definition Es sei $f(x) \in K[x]$. Ein Element $\alpha \in K$ mit $f(\alpha) = 0$ heißt *Nullstelle* oder *Wurzel* des Polynoms $f(x)$.

Satz 6.3 *Ein Polynom vom Grad $n \geq 0$ über einem Körper K hat höchstens n Wurzeln in K.*

Beweis. Wir beweisen den Satz durch Induktion nach n. Ein Polynom vom Grad 0 ist von der Form $f(x) = a_0$ mit $a_0 \neq 0$. Ein solches Polynom hat keine Nullstellen.

Wir nehmen nun an, dass der Satz für Polynome vom Grad $n-1$ gilt. Es sei $f(x) \in K[x]$ ein Polynom vom Grad n. Hat $f(x)$ keine Nullstellen, so ist der Satz richtig. Andernfalls sei α eine Nullstelle von $f(x)$. Nach dem vorhergehenden Korollar können wir dann schreiben:

$$f(x) = (x - \alpha)g(x).$$

Nach der Gradformel gilt $\operatorname{grad} g(x) = n-1$. Da K als Körper keine Nullteiler besitzt, gilt $f(\beta) = 0$ genau dann, wenn $(\beta - \alpha) = 0$ oder $g(\beta) = 0$. Also ist eine Nullstelle von $f(x)$ entweder gleich α oder eine Nullstelle von $g(x)$. Nach Induktionsannahme hat $g(x)$ höchstens $n-1$ Wurzeln in K. Also hat $f(x)$ höchstens n Wurzeln in K. □

Beispiel 6.3 Der Ring $\mathbb{Z}[i] := \{a + ib \,|\, a, b \in \mathbb{Z}\}$ (der Ring der *Gaußschen ganzen Zahlen*) ist ein euklidischer Ring mit $d(a + ib) = a^2 + b^2$.

Wegen $\mathbb{Z}[i] \subset \mathbb{C}$ sieht man leicht, dass $\mathbb{Z}[i]$ ein Integritätsbereich ist. Es sei $z \in \mathbb{Z}[i]$. Dann gilt $d(z) = z\overline{z}$, wobei $\overline{z}$ die komplex konjugierte Zahl von z ist. Also gilt $d(z) > 0$ für jede komplexe Zahl z mit $z \neq 0$, und für $z, w \in \mathbb{Z}[i]$ gilt $d(zw) = d(z)d(w)$.

Es seien $z, w \in \mathbb{Z}[i]$ mit $w \neq 0$. Dann gilt

$$\frac{z}{w} = c + id \quad \text{mit } c, d \in \mathbb{Q},$$

Es seien $a, b \in \mathbb{Z}$ mit $|c - a| \leq \frac{1}{2}$ und $|d - b| \leq \frac{1}{2}$. Dann gilt

$$\frac{z}{w} = a + ib + ((c - a) + i(d - b)).$$

Daraus folgt

$$z = (a + ib)w + ((c - a) + i(d - b))w$$

mit

$$\begin{aligned} d(((c - a) + i(d - b))w) &= d(((c - a) + i(d - b)))d(w) \\ &= ((c - a)^2 + (d - b)^2)d(w) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) d(w) < d(w). \end{aligned}$$

Also ist in $\mathbb{Z}[i]$ Division mit Rest möglich.

7 Der euklidische Algorithmus

Der Name "euklidischer Ring" rührt daher, dass in einem solchen Ring der euklidische Algorithmus funktioniert.

Definition Es sei R ein Ring mit 1, $a, b \in R$. Wir sagen a *teilt* b oder a ist ein *Teiler* von b, in Zeichen $a|b$, falls es ein $q \in R$ gibt mit $b = qa$.

Definition Es sei R ein Integritätsbereich und $a, b \in R$. Ein Element $g \in R$ heißt ein *größter gemeinsamer Teiler* von a und b, in Zeichen $g = \mathrm{ggT}(a, b)$, falls

(i) $g|a$ und $g|b$,

(ii) Für alle $c \in R$ gilt: Aus $c|a$ und $c|b$ folgt $c|g$.

Ein Element $k \in R$ heißt *kleinstes gemeinsames Vielfaches* von a und b, in Zeichen $k = \mathrm{kgV}(a, b)$, falls

(i) $a|k$ und $b|k$,

(ii) Für alle $c \in R$ gilt: Aus $a|c$ und $b|c$ folgt $k|c$.

Es sei R ein euklidischer Ring. Wir wollen einen g.g.T. zweier von Null verschiedener Elemente $a, b \in R$ bestimmen. Dies geschieht mit dem *euklidischen Algorithmus*, den wir nun beschreiben. Wir setzen zunächst $a_1 := a$, $a_2 := b$. Nun dividieren wir a_1 durch a_2. Dann erhalten wir eine Darstellung $a_1 = q_1 a_2 + a_3$ mit $d(a_3) < d(a_2)$. Ist nun $a_3 \neq 0$, so können wir im nächsten Schritt a_2 durch a_3 mit einem Rest a_4 teilen, usw. Da $d(a_2) > d(a_3) > d(a_4) > \dots$ gilt, kommt dieser Prozeß nach endlich vielen Schritten zum Stillstand, nämlich dann, wenn der anfallende Rest Null wird. Wir erhalten also ein Schema wie folgt:

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3, \quad d(a_2) > d(a_3), \\
a_2 &= q_2 a_3 + a_4, \quad d(a_3) > d(a_4), \\
&\vdots \quad \vdots \quad \vdots \\
a_{m-1} &= q_{m-1} a_m + a_{m+1}, \quad d(a_m) > d(a_{m+1}), \\
a_m &= q_m a_{m+1}
\end{aligned}$$

Hierbei gilt $a_i \neq 0$, $i = 1, \dots, m+1$.

Behauptung a_{m+1} ist ein g.g.T. von a_1 und a_2.

Beweis. (i) Aus der letzten Zeile folgt $a_{m+1}|a_m$, aus der vorletzten $a_{m+1}|a_{m-1}$, usw. Aus der zweiten und ersten Zeile folgt schließlich $a_{m+1}|a_2$ und $a_{m+1}|a_1$. Also ist a_{m+1} ein Teiler von a und b.

(ii) Es sei c ein Teiler von a und b. Aus der ersten Zeile folgt, dass $c|a_3$, aus der zweiten $c|a_4$ usw. Aus der letzten Zeile folgt schließlich $c|a_{m+1}$. Also ist a_{m+1} ein größter gemeinsamer Teiler von a und b. □

Darüberhinaus kann man mit Hilfe dieses Algorithmus Elemente $s, t \in R$ finden, so dass

$$a_{m+1} = \mathrm{ggT}(a, b) = sa + tb$$

gilt. Dazu beginnt man mit der vorletzten Gleichung

$$a_{m+1} = a_{m-1} - q_{m-1}a_m$$

und setzt rückwirkend die vorherigen Gleichungen ein, wobei jedesmal a_i durch einen Ausdruck mit a_{i-1} und a_{i-2} ersetzt wird.

Damit haben wir bewiesen

Satz 7.1 *Es sei R ein euklidischer Ring. Dann haben je zwei Elemente a und b in R einen größten gemeinsamen Teiler g. Ferner gibt es $s, t \in R$, so dass*

$$g = sa + tb.$$

Beispiel 7.1 Wir bestimmen einen größten gemeinsamen Teiler von $x^3 + 2x^2 + 1$ und $x^2 + 2$ in $\mathbb{Z}_3[x]$. Nach Beispiel 6.2 gilt

$$\begin{aligned} x^3 + 2x^2 + 1 &= (x + 2)(x^2 + 2) + x \\ x^2 + 2 &= x \cdot x + 2 \\ x &= 2x \cdot 2 \end{aligned}$$

Daraus folgt $\mathrm{ggT}(x^3 + 2x^2 + 1, x^2 + 2) = 2$ und

$$\begin{aligned} 2 &= (x^2 + 2) - x \cdot x \\ &= (x^2 + 2) - (x^3 + 2x^2 + 1 - (x + 2)(x^2 + 2))x \\ &= 2x(x^3 + 2x^2 + 1) + (x^2 + 2x + 1)(x^2 + 2) \end{aligned}$$

Wir wenden diese Resultate nun auf diophantische Gleichungen an.

Satz 7.2 *Die Gleichung*

$$ax + by = c, \quad a, b, c \in \mathbb{Z},$$

hat genau dann ganzzahlige Lösungen x, y, wenn $\mathrm{ggT}(a, b)|c$.

Beweis. Wenn $ax + by = c$ eine Lösung besitzt, dann teilt $\mathrm{ggT}(a, b)$ die Zahlen a und b, also auch c.

Gilt umgekehrt $\mathrm{ggT}(a, b)|c$, so folgt $c = m \cdot \mathrm{ggT}(a, b)$. Nach Satz 7.1 existieren $s, t \in \mathbb{Z}$ mit

$$as + bt = \mathrm{ggT}(a, b).$$

Also gilt

$$asm + btm = m \cdot \mathrm{ggT}(a, b)$$

und $x := sm$, $y := tm$ ist eine Lösung von $ax + by = c$. □

Der euklidische Algorithmus liefert eine praktische Methode, um die Zahlen s und t aus dem Beweis des vorherigen Satzes zu bestimmen.

8 Zerlegung in irreduzible Faktoren

Eine wichtige Eigenschaft der ganzen Zahlen ist die Tatsache, dass sich jede ganze Zahl > 1 in Primfaktoren zerlegen lässt. Wir wollen nun Ringe betrachten, in denen eine ähnliche Zerlegung möglich ist.

Definition Es sei R ein kommutativer Ring mit 1. Ein Element $a \in R$ heißt *Einheit*, falls es ein Element $b \in R$ mit $ab = 1$ gibt. Die Menge aller Einheiten in einem kommutativen Ring R wird mit R^* bezeichnet.

Beispiel 8.1 (a) In einem Körper K sind alle von Null verschiedenen Elemente Einheiten und es gilt $K^* = K \setminus \{0\}$.

(b) Die Einheiten in $\mathbb{Z}$ sind ± 1.

(c) Es sei K ein Körper. Die Einheiten in $K[x]$ sind die vom Nullpolynom verschiedenen konstanten Polynome, d.h. die Polynome vom Grad 0.

Satz 8.1 *In einem kommutativen Ring R mit 1 bilden die Einheiten mit der Multiplikation als Verknüpfung eine abelsche Gruppe.*

Beweis. Es seien $a_1, a_2 \in R^*$ und $b_1, b_2 \in R$ mit $a_1 b_1 = a_2 b_2 = 1$. Dann gilt $(a_1 a_2)(b_1 b_2) = 1$. Also ist $a_1 a_2$ eine Einheit in R. Die Gruppenaxiome folgen sofort. □

Lemma 8.1 *Es sei R ein Integritätsbereich. Dann gilt $a|b$ und $b|a$ genau dann, wenn $a = eb$ ist, wobei e eine Einheit in R ist. (a und b heißen dann* assoziiert*.)*

Beweis. "⇒": Aus $a|b$ folgt $b = ac$ für ein $c \in R$ und aus $b|a$ folgt $a = bd$ für ein $d \in R$. Dann gilt $a = bd = acd$, also $a(cd - 1) = 0$. Daraus folgt $a = 0$ oder $cd = 1$. Ist $a = 0$, so ist auch $b = 0$. Im anderen Fall ist d eine Einheit.

"⇐": Aus $a = eb$ folgt $b|a$. Ist $c \in R$ mit $ec = 1$, so folgt $b = ca$, also $a|b$. □

Definition Es sei R ein Integritätsbereich. Ein Element $p \in R$ heißt *irreduzibel*, wenn p weder das Nullelement noch eine Einheit ist und wenn gilt: Aus $p = ab$ mit $a, b \in R$ folgt a ist eine Einheit oder b ist eine Einheit.

Ein Element $p \in R$ heißt *Primelement*, wenn p weder das Nullelement noch eine Einheit ist und wenn gilt: Aus $p|ab$ für $a, b \in R$ folgt $p|a$ oder $p|b$.

Satz 8.2 *Jedes Primelement ist irreduzibel.*

Beweis. Es sei p ein Primelement in einem Integritätsbereich R. Wir betrachten eine Zerlegung $p = ab$ mit $a, b \in R$. Dann folgt $a|p$ und $b|p$. Da p ein Primelement ist, folgt $p|a$ oder $p|b$. Angenommen, $p|a$. Nach dem vorherigen Lemma gilt dann $a = ep$, wobei $e \in R$ eine Einheit ist. Daraus folgt $p = ebp$. Da $p \neq 0$ folgt daraus $eb = 1$. Also ist b eine Einheit. □

Die Umkehrung gilt im Allgemeinen nicht:

Beispiel 8.2 In $\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ gilt

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Die Elemente $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ sind irreduzibel und es gilt $(1+\sqrt{-3})|2\cdot 2$, aber $1 + \sqrt{-3}$ teilt nicht 2.

Definition Ein Integritätsbereich R heißt *faktoriell* oder ein *ZPE-Ring*, wenn sich jede von Null verschiedene Nichteinheit aus R als Produkt von Primelementen schreiben lässt.

Satz 8.3 *In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement.*

Beweis. Es sei R ein faktorieller Ring, $a \in R$ ein irreduzibles Element. Da a keine Einheit ist, lässt sich a als Produkt von Primelementen

$$a = p_1 \cdots p_n, \quad p_1, \ldots, p_n \in R,$$

schreiben. Da a irreduzibel ist, muss hierbei $n = 1$ sein. Also ist a ein Primelement. □

Beispiel 8.3 $\mathbb{Z}[\sqrt{-3}]$ ist kein faktorieller Ring, da $1+\sqrt{-3}$ irreduzibel, aber kein Primelement ist.

Satz 8.4 *In einem faktoriellen Ring R ist die Zerlegung in Primfaktoren eindeutig, d.h. jede von Null verschiedene Nichteinheit aus R lässt sich als Produkt von Primelementen schreiben, wobei die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt sind.*

Beweis. Es sei $a \in R$ eine von Null verschiedene Nichteinheit. Angenommen,

$$a = p_1 \cdots p_n = q_1 \cdots q_m,$$

wobei jedes p_i und jedes q_j ein Primelement ist. Dann gilt $p_1|a$ und damit $p_1|q_1 \cdots q_m$. Da p_1 ein Primelement ist, muss p_1 eins der q_j teilen. Nach

eventueller Umnummerierung können wir annehmen, dass $p_1|q_1$. Das bedeutet, $q_1 = u_1 p_1$ für ein $u_1 \in R$. Da p_1 und q_1 auch irreduzibel sind, folgt, dass u_1 eine Einheit ist. Also gilt

$$a = p_1 p_2 \cdots p_n = u_1 p_1 q_2 \cdots q_m$$

und daraus folgt $p_2 \cdots p_n = u_1 q_2 \cdots q_m$. Durch Induktion folgt $q_i = u_i p_i$ für $i = 1, \ldots, \min(m, n)$, wobei u_i eine Einheit ist.

Ist nun $m < n$, so folgt

$$p_{m+1} \cdots p_n = u_1 \cdots u_m.$$

Dies ist aber unmöglich, da irreduzible Elemente keine Einheit teilen können. Ist $m > n$, so folgt

$$1 = u_1 \cdots u_n q_{m+1} \cdots q_m.$$

Daraus folgt, dass q_m eine Einheit ist, ein erneuter Widerspruch. Also ist $m = n$ und die Primelemente $p_1, \ldots, p_n$ sind die gleichen wie die Primelemente $q_1, \ldots, q_m$ bis auf ihre Reihenfolge und die Multiplikation mit Einheiten. □

Satz 8.5 *Ein Integritätsbereich R ist genau dann faktoriell, wenn sich jede von Null verschiedene Nichteinheit als Produkt von irreduziblen Elementen schrieben lässt, wobei die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt sind.*

Beweis. "⇒": Es sei R faktoriell. Dann lässt sich jede von Null verschiedene Nichteinheit aus R als Produkt von Primelementen schreiben. Nach Satz 8.4 sind die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt. Nach Satz 8.2 ist jedes Primelement irreduzibel.

"⇐": Hier reicht es zu zeigen, dass jedes irreduzible Element von R ein Primelement ist. Es sei also $u \in R$ ein irreduzibles Element. Angenommen, $u|ab$ mit $a, b \in R$. Dann gilt $ab = cu$ mit einem $c \in R$. Die Elemente a, b und c zerlegen wir jedes für sich in ein Produkt irreduzibler Elemente und setzen die Produkte in $ab = cu$ ein. Nach Voraussetzung sind die Faktoren der Produkte auf beiden Seiten der Gleichung die gleichen bis auf Einheiten und Reihenfolge. Also muss u zu einem Teiler von a oder b assoziiert sein und somit selbst ein Teiler von a oder b sein. □

Wir wollen nun zeigen, dass jeder euklidische Ring faktoriell ist. Dazu brauchen wir einige Hilfssätze.

Lemma 8.2 *Es sei R ein euklidischer Ring, $a, b \in R$ und g_2 ein größter gemeinsamer Teiler von a und b. Dann ist g_1 genau dann ebenfalls ein größter gemeinsamer Teiler von a und b, wenn $g_1 = e g_2$ für eine Einheit $e \in R$ gilt.*

Beweis. Wenn $g_1 = eg_2$ und $eu = 1$, dann folgt $g_2 = ug_1$. Also gilt $g_2|g_1$ und $g_1|g_2$ genau dann, wenn $g_1 = eg_2$. □

Lemma 8.3 *Es sei R ein euklidischer Ring und $a, b \in R$. Dann gilt $d(a) = d(ab)$ genau dann, wenn b eine Einheit ist. Andernfalls gilt $d(a) < d(ab)$.*

Beweis. Ist b eine Einheit und $bc = 1$, so gilt

$$d(a) \leq d(ab) \leq d(abc) = d(a),$$

also $d(a) = d(ab)$.

Ist b keine Einheit, dann teilt ab nicht a und es gilt

$$a = qab + r \quad \text{mit } d(r) < d(ab).$$

Daraus folgt $r = a(1 - qb)$, also $d(a) \leq d(r)$. Also gilt $d(a) < d(ab)$. □

Lemma 8.4 *Es sei R ein euklidischer Ring, $a, b, c \in R$. Gilt $\mathrm{ggT}(a, b) = 1$ und $a|bc$, so folgt $a|c$.*

Beweis. Nach Satz 7.1 können wir $1 = sa+tb$ mit $s, t \in R$ schreiben. Daraus folgt $c = sac + tbc$, also $a|c$. □

Satz 8.6 *Jeder euklidische Ring ist faktoriell.*

Beweis. Wir zeigen zunächst, dass in einem euklidischen Ring R jedes irreduzible Element ein Primelement ist. Es sei $u \in R$ ein irreduzibles Element. Angenommen, $u|ab$ mit $a, b \in R$. Dann gilt $\mathrm{ggT}(a, u)|u$, also $u = \mathrm{ggT}(a, u)\cdot c$ für ein $c \in R$. Da u irreduzibel ist, ist entweder $\mathrm{ggT}(a, u)$ oder c eine Einheit. Daraus folgt $\mathrm{ggT}(a, u) = 1$ oder $\mathrm{ggT}(a, u) = u$. Teilt u nun a nicht, so folgt $\mathrm{ggT}(a, u) = 1$ und aus Lemma 8.4 folgt $u|b$.

Es reicht damit zu zeigen, dass sich in R jede von Null verschiedene Nichteinheit als Produkt von irreduziblen Elementen schreiben lässt. Dies beweisen wir durch Induktion nach $d(a)$ für $a \in R$. Der kleinste Wert von $d(a)$ für $a \neq 0$ ist $d(1)$, denn 1 teilt jedes andere Element. Angenommen, $d(a) = d(1)$. Dann gilt $d(1\cdot a) = d(1)$ und nach Lemma 8.3 ist a eine Einheit.

Als Induktionsannahme nehmen wir an, dass alle Elemente $x \in R$ mit $d(x) < d(a)$ entweder Einheiten sind oder als Produkt von irreduziblen Elementen geschrieben werden können.

Wir zeigen nun, dass dies auch für das Element a gilt. Wenn a irreduzibel ist, dann ist nichts zu beweisen. Andernfalls können wir $a = bc$ schreiben, wobei weder b noch c eine Einheit ist. Nach Lemma 8.3 gilt $d(b) < d(bc) = d(a)$ und $d(c) < d(bc) = d(a)$. Nach Induktionsannahme können b und c als Produkt von irreduziblen Elementen geschrieben werden, also auch a. □

9 Irreduzible Polynome

Die Frage, ob ein Polynom irreduzibel ist oder nicht, wird im Folgenden sehr wichtig sein. Deswegen wollen wir nun Methoden betrachten, mit denen man diese Frage untersuchen kann. Dabei spielt es eine Rolle, über welchem Koeffizientenring wir das Polynom zerlegen wollen.

Definition Es sei R ein Integritätsbereich. Ein Polynom $f(x) \in R[x]$ von positivem Grad heißt *reduzibel über* R, wenn man es in $R[x]$ in ein Produkt von zwei Polynomen von positivem Grad zerlegen kann. Andernfalls heißt $f(x)$ *irreduzibel über* R. Das Polynom $f(x)$ ist dann ein irreduzibles Element in $R[x]$

Bemerkung 9.1 Man beachte, dass die Reduzibilität von R abhängt: Das Polynom $x^2 + 1$ ist irreduzibel über $\mathbb{R}$, aber reduzibel über $\mathbb{C}$.

In $\mathbb{C}$ gilt der berühmte Fundamentalsatz der Algebra:

Satz 9.1 (Fundamentalsatz der Algebra) *Ist $f(x)$ ein Polynom in $\mathbb{C}[x]$ von positivem Grad, dann hat $f(x)$ eine Nullstelle in $\mathbb{C}$.*

Zu diesem Satz existieren viele Beweise. Allein Gauß, der diesen Satz in seiner Doktorarbeit im Jahre 1799 als erster bewiesen hat, hat 7 Beweise gegeben. Der eleganteste Beweis benutzt Resultate aus der Funktionentheorie und soll hier nicht gegeben werden.

Satz 9.2 (i) *Die irreduziblen Polynome in $\mathbb{C}[x]$ sind die Polynome vom Grad 1.*

(ii) *Die irreduziblen Polynome in $\mathbb{R}[x]$ sind die Polynome vom Grad 1 und die Polynome vom Grad 2 der Form $ax^2 + bx + c$, wobei $b^2 < 4ac$.*

Beweis. (i) folgt aus dem Fundamentalsatz der Algebra.

(ii) Es sei $f(x)$ ein Polynom mit reellen Koeffizienten. Ist z eine komplexe Nullstelle von $f(x)$ mit nicht verschwindendem Imaginärteil, so ist auch die konjugiert komplexe Zahl $\overline{z}$ eine Nullstelle von $f(x)$, denn es gilt $f(\overline{z}) = \overline{f(z)} = 0$. Nun sind aber z und $\overline{z}$ Nullstellen eines Polynoms vom Grad 2 des angegebenen Typs. □

Nun betrachten wir Polynome mit ganzzahligen Koeffizienten. Wir untersuchen, wann ein solches Polynom irreduzibel über $\mathbb{Q}$ ist oder rationale Wurzeln besitzt.

Satz 9.3 (Satz über rationale Wurzeln) *Es sei $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Ist $\frac{r}{s}$ eine rationale Nullstelle von $p(x)$ und $\mathrm{ggT}(r, s) = 1$, dann gilt $r|a_0$ und $s|a_n$.*

Beweis. Aus $p(\frac{r}{s}) = 0$ folgt

$$a_0 + a_1\left(\frac{r}{s}\right) + \cdots + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + a_n\left(\frac{r}{s}\right)^n = 0.$$

Multiplizieren wir diese Gleichung mit s^n, so erhalten wir

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

Daraus folgt

$$a_s^n = -r(a_1 s^{n-1} + \cdots + a_{n-1} r^{n-2} s + a_n r^{n-1}),$$

also $r|a_0 s^n$. Da $\mathrm{ggT}(r, s) = 1$, folgt aus Lemma 8.4 $r|a_0$. Ähnlich zeigt man $s|a_n$. □

Satz 9.4 (Lemma von Gauß) *Es sei $P(x) \in \mathbb{Z}[x]$. Ist $P(x)$ reduzibel über $\mathbb{Q}$, so ist $P(x)$ auch reduzibel über $\mathbb{Z}$.*

Beweis. Es sei $P(x) = q(x)r(x)$ mit $q(x), r(x) \in \mathbb{Q}[x]$. Wir stellen die rationalen Koeffizienten von $q(x)$ als gekürzte Brüche dar. Es sei u der Hauptnenner dieser Brüche. Dann gilt $q(x) = \frac{1}{u}\tilde{Q}(x)$, wobei $\tilde{Q}(x) \in \mathbb{Z}[x]$. Es sei s der größte gemeinsame Teiler aller Koeffizienten von $\tilde{Q}(x)$. Wir schreiben $q(x) = \frac{s}{u}Q(x)$, wobei $Q(x) \in \mathbb{Z}[x]$ und die Koeffizienten von $Q(x)$ teilerfremd sind. In analoger Weise schreiben wir $r(x) = \frac{t}{v}R(x)$. Dann gilt

$$P(x) = q(x)r(x) = \frac{s}{u}Q(x)\frac{t}{v}R(x) = \frac{st}{uv}Q(x)R(x).$$

Um den Satz zu beweisen, bleibt zu zeigen, dass $uv|st$. Dazu zeigen wir, dass kein Primfaktor p von uv alle Koeffizienten von $Q(x)R(x)$ teilt.

Es sei

$$\begin{aligned} Q(x) &= b_0 + b_1 x + \cdots + b_k x^k, \\ R(x) &= c_0 + c_1 x + \cdots + c_l x^l. \end{aligned}$$

Es sei p eine beliebige Primzahl. Da die Koeffizienten von $Q(x)$ teilerfremd sind, gibt es einen Koeffizienten von $Q(x)$, der nicht von p geteilt wird. Es sei b_i der erste solche Koeffizient. Entsprechend sei c_j der erste Koeffizient von $R(x)$, der nicht von p geteilt wird. Dann lautet der Koeffizient von x^{i+j} in $Q(x)R(x)$

$$b_{i+j}c_0 + \cdots + b_{i+1}c_{j-1} + b_i c_j + b_{i-1}c_{j+1} + \cdots + b_0 c_{i+j}.$$

Nun gilt $p|c_0, \ldots, p|c_{j-1}$, $p|b_{i-1}, \ldots, p|b_0$, aber p teilt nicht $b_i c_j$. Daher ist dieser Koeffizient nicht durch p teilbar. Daher sind alle Koeffizienten von $Q(x)R(x)$ teilerfremd. Also gilt $uv|st$. □

Beispiel 9.1 Wir zerlegen das Polynom $P(x) = x^4 - 3x^2 + 2x + 1$ in $\mathbb{Q}[x]$ in irreduzible Faktoren. Nach Satz 9.3 sind die einzigen möglichen rationalen Wurzeln von $P(x)$ die Zahlen ± 1. Einsetzen ergibt, dass dies aber keine Wurzeln sind. Also hat $P(x)$ keine linearen Faktoren.

Wenn sich also $P(x)$ in ein Produkt irreduzibler Faktoren zerlegen lässt, so müssen diese Faktoren beide den Grad 2 haben. Nach dem Lemma von Gauß kann man diese Faktoren so wählen, dass sie ganzzahlige Koeffizienten haben. Wir nehmen also an:

$$\begin{aligned} x^4 - 3x^2 + 2x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a+c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd. \end{aligned}$$

Durch Koeffizientenvergleich erhalten wir die folgenden Gleichungen:

$$a + c = 0, \quad b + d + ac = -3, \quad bc + ad = 2, \quad bd = 1.$$

Diese Gleichungen haben aber keine gemeinsamen ganzzahligen Lösungen, denn aus $bd = 1$ folgt $b = d = \pm 1$ und damit $b(a + c) = \pm 2$ im Widerspruch zu $a + c = 0$.

Also ist das Polynom $P(x)$ irreduzibel über $\mathbb{Q}$ und damit erst recht über $\mathbb{Z}$.

Satz 9.5 (Kriterium von Eisenstein) *Es sei $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Für eine Primzahl p gelte*

(i) $p | a_0$, $p | a_1$, $\ldots$, $p | a_{n-1}$,

(ii) $p \nmid a_n$ *und*

(iii) $p^2 \nmid a_0$.

Dann ist $f(x)$ irreduzibel über $\mathbb{Q}$.

Beweis. Angenommen, $f(x)$ ist reduzibel. Nach dem Lemma von Gauß lässt sich $f(x)$ dann in $\mathbb{Z}[x]$ als Produkt

$$f(x) = (b_0 + \cdots + b_r x^r)(c_0 + \cdots + c_s x^s)$$

schreiben, wobei $b_i, c_j \in \mathbb{Z}$, $r, s > 0$ und $r + s = n$.

Durch Koeffizientenvergleich folgt

$$a_0 = b_0 c_0.$$

Da $p | a_0$, aber $p^2 \nmid a_0$, muss p entweder b_0 oder c_0 teilen. O.B.d.A. nehmen wir an, dass $p | b_0$ und $p \nmid c_0$. Nun kann p nicht alle Koeffizienten $b_0, b_1, \ldots, b_r$ teilen, denn sonst würde $p | a_n$ gelten. Es sei t die kleinste ganze Zahl, für die $p \nmid b_t$ gilt, also $1 \leq t \leq r < n$. Nun gilt

$$a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_1 c_{t-1} + b_0 c_t$$

und p teilt die Koeffizienten a_t, b_0, b_1, $\ldots$, b_{t-1}. Also muss p auch $b_t c_0$ teilen, ein Widerspruch. □

Beispiel 9.2 Es sei p eine Primzahl und

$$\varphi(x) = 1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Dieses Polynom heißt das *p-te Kreisteilungspolynom*. Wir zeigen, dass dieses Polynom irreduzibel über $\mathbb{Q}$ ist.

Beweis. Wir können das Kriterium von Eisenstein nicht direkt auf $\varphi(x)$ anwenden. Wir machen zuerst eine Variablentransformation $x = y + 1$. Damit erhalten wir

$$\begin{aligned}
\varphi(y+1) &= \frac{(y+1)^p - 1}{y} \\
&= \sum_{i=1}^{p} \binom{p}{i} y^{i-1} \\
&= p + \binom{p}{2} y + \cdots + \binom{p}{p-2} y^{p-3} + p y^{p-2} + y^{p-1}.
\end{aligned}$$

Es gilt $p | \binom{p}{i}$ für $i = 1, \ldots, p-1$, $p \nmid \binom{p}{p}$, $p^2 \nmid \binom{p}{1}$, also ist $\varphi(y+1)$ nach dem Kriterium von Eisenstein irreduzibel. Da $\varphi(x)$ genau dann irreduzibel ist, wenn $\varphi(y+1)$ irreduzibel ist, ist auch $\varphi(x)$ irreduzibel. □

Nun betrachten wir die Zerlegung von Polynomen über endlichen Körpern.

Um die Wurzeln eines Polynoms in $\mathbb{Z}_p[x]$ zu finden, kann man einfach alle p möglichen Werte für x ausprobieren.

Beispiel 9.3 Wir betrachten das Polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Wir stellen eine Wertetabelle auf:

x	0	1	2
x^2	0	1	1
$x^2 + 1$	1	2	2

Aus dieser Tabelle ist ersichtlich, dass $x^2 + 1$ keine Wurzeln in $\mathbb{Z}_3$ hat, also irreduzibel in $\mathbb{Z}_3[x]$ ist.

Satz 9.6 *Ein Polynom in $\mathbb{Z}_2[x]$ hat genau dann einen Faktor $(x+1)$, wenn es eine gerade Anzahl von von Null verschiedenen Koeffizienten hat.*

Beweis. Es sei $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}_2[x]$. Nach Korollar 6.3 ist $(x+1)$ genau dann ein Faktor von $p(x)$, wenn $p(1) = 0$. (Man beachte, dass in $\mathbb{Z}_2[x]$ gilt: $x - 1 = x + 1$.) Nun gilt

$$p(1) = a_0 + a_1 + \cdots + a_n.$$

Also ist $p(1) = 0$ genau dann, wenn $p(x)$ eine gerade Anzahl von Koeffizienten, die von Null verschieden sind, hat. □

Beispiel 9.4 Wir bestimmen alle irreduziblen Polynome vom Grad ≤ 4 über $\mathbb{Z}_2$.

Jedes Polynom vom Grad 1 ist irreduzibel. Die Polynome vom Grad 1 in $\mathbb{Z}_2[x]$ sind x und $x+1$.

Es sei $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}_2[x]$ mit $\text{grad}(p(x)) = n$. Dann gilt $a_n \neq 0$, also $a_n = 1$. Die möglichen Wurzeln sind 0 und 1. Das Element 0 ist genau dann eine Wurzel, wenn $a_0 = 0$ gilt, 1 ist genau dann eine Wurzel, wenn die Anzahl der a_i mit $a_i = 1$, $i = 0, \ldots, n$, gerade ist. Damit haben wir die folgende Liste von Polynomen vom Grad 2,3 und 4 in $\mathbb{Z}_2[x]$ ohne Linearfaktoren:

$$\begin{array}{ll} \text{Grad } 2: & x^2+x+1 \\ \text{Grad } 3: & x^3+x+1, x^3+x^2+1 \\ \text{Grad } 4: & x^4+x+1, x^4+x^2+1, x^4+x^3+1, x^4+x^3+x^2+x+1 \end{array}$$

Wenn ein Polynom vom Grad 2 oder 3 reduzibel ist, so muss es einen Linearfaktor haben. Daher sind die obigen Polynome vom Grad 2 oder 3 irreduzibel. Wenn ein Polynom vom Grad 4 reduzibel ist, so hat es entweder einen Linearfaktor oder es ist das Produkt von zwei irreduziblen Polynomen vom Grad 2. Es gibt aber nur ein irreduzibles Polynom vom Grad 2 in $\mathbb{Z}_2[x]$, nämlich x^2+x+1, und es gilt

$$(x^2+x+1)^2 = x^4+x^2+1.$$

Also sind die irreduziblen Polynome vom Grad ≤ 4 über $\mathbb{Z}_2$ die Polynome:

$$\begin{array}{ll} \text{Grad } 1: & x, x+1 \\ \text{Grad } 2: & x^2+x+1 \\ \text{Grad } 3: & x^3+x+1, x^3+x^2+1 \\ \text{Grad } 4: & x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1 \end{array}$$

10 Unterringe und Ideale

Wir betrachten nun Teilmengen von Ringen mit 1, die unter den Ringoperationen abgeschlossen sind.

Definition Es sei R ein Ring mit Einselement 1. Eine nichtleere Teilmenge $S \subset R$ heißt *Unterring* von R, wenn gilt:

(UR1) Für alle $a, b \in S$ gilt $a + b \in S$.

(UR2) Für alle $a \in S$ gilt $-a \in S$.

(UR3) Für alle $a, b \in S$ gilt $a \cdot b \in S$.

(UR4) $1 \in S$.

Satz 10.1 *Ein Unterring S eines Rings R mit 1 ist ebenfalls ein Ring mit 1.*

Beweis. Aus (UR1) und (UR2) folgt, dass S bezüglich der Addition eine Untergruppe von R ist. Aus Satz 2.2 folgt, dass $(S, +)$ eine abelsche Gruppe ist. Die Bedingungen (UR3) und (UR4) zeigen, dass S abgeschlossen bezüglich der Multiplikation ist und $1 \in S$ gilt. Die übrigen Axiome gelten in S, da sie in R gelten. □

Beispiel 10.1 $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, $\mathbb{Q}$ ist ein Unterring von $\mathbb{R}$ und $\mathbb{R}$ ist ein Unterring von $\mathbb{C}$.

Es stellt sich heraus, dass wichtiger als Unterringe eine andere Art von Untergruppen sind, nämlich die Ideale, die den Normalteilern von Gruppen entsprechen.

Definition Es sei R ein Ring mit 1. Eine nichtleere Teilmenge $I \subset R$ heißt *Ideal* von R, wenn gilt:

(I1) Für alle $x, y \in I$ gilt $x - y \in I$.

(I2) Für alle $x \in I$ und $r \in R$ gilt $r \cdot x \in I$ und $x \cdot r \in I$.

Aus (I1) folgt, dass $(I, +)$ eine Untergruppe von $(R, +)$ ist.

Beispiel 10.2 In jedem Ring mit Einselement R sind R und $\{0\}$ Ideale.

Satz 10.2 *Es sei R ein kommutativer Ring mit 1, $a \in R$. Die Menge $\{ra \mid r \in R\}$ ist ein Ideal in R.*

Definition Die Menge $\{ra \mid r \in R\}$ bezeichnen wir mit (a) und nennen sie das von a erzeugte *Hauptideal*.

Beweis. Es sei $ra, sa \in (a)$ und $t \in R$. Dann gilt

$$\begin{aligned} ra - sa &= (r - s)a \in (a), \\ t(ra) &= (tr)a \in (a). \end{aligned}$$

Also ist (a) ein Ideal von R. □

Beispiel 10.3 (1) $(n) = n\mathbb{Z}$ ist das von n erzeugte Hauptideal in $\mathbb{Z}$.

(2) Die Menge aller Polynome in $\mathbb{Z}_2[x]$, die $x + 1$ als Faktor haben ist das Hauptideal

$$(x + 1) = \{p(x)(x + 1) \mid p(x) \in \mathbb{Z}_2[x]\}$$

in $\mathbb{Z}_2[x]$, das von $x+1$ erzeugt wird. Es enthält alle Polynome, die 1 als Nullstelle haben.

(3) Die Menge aller Polynome in zwei Variablen x und y mit reellen Koeffizienten bezeichnen wir mit $\mathbb{R}[x,y]$. Die Menge aller solchen Polynome mit konstanten Glied $a_0 = 0$ ist ein Ideal von $\mathbb{R}[x,y]$. Dieses Ideal ist aber kein Hauptideal.

Definition Ein kommutativer Ring R mit 1 heißt *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist.

Satz 10.3 *Ein euklidischer Ring ist ein Hauptidealring.*

Beweis. Es sei R ein euklidischer Ring und I ein Ideal von R. Ist $I = \{0\}$, so ist $I = (0)$, das von 0 erzeugte Hauptideal von R. Andernfalls enthält I mindestens ein von 0 verschiedenes Element. Es sei $b \in I$, $b \neq 0$, mit $d(b)$ minimal. Ist nun $a \in I$, so gibt es $q, r \in R$ mit

$$a = qb + r \quad \text{wobei } r = 0 \text{ oder } d(r) < d(b).$$

Nun ist $r = a - qb \in I$. Da b ein Element aus I mit $d(b)$ minimal ist, muss $r = 0$ und $a = qb$ gelten. Also gilt $a \in (b)$ und $I \subset (b)$.

Umgekehrt ist jedes Element von (b) von der Form qb für ein $q \in R$. Dann ist aber $qb \in I$, da I ein Ideal ist. Also folgt $(b) \subset I$ und $I = (b)$. Also ist R ein Hauptidealring. □

Korollar 10.1 *Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptidealring. Ist K ein Körper, so ist $K[x]$ ein Hauptidealring.*

Beweis. $\mathbb{Z}$ und $K[x]$ sind euklidische Ringe. □

Satz 10.4 *Es sei R ein Ring mit 1 und I ein Ideal in R. Enthält I eine Einheit von R, so ist I der ganze Ring R.*

Beweis. Es sei $e \in I$ eine Einheit von R. Dann gibt es ein $u \in R$ mit $eu = 1$. Da I ein Ideal ist, ist dann auch $1 \in I$. Ist nun $r \in R$, so ist auch $r \cdot 1 = r \in I$, also $I = R$. □

Bemerkung 10.1 Ein Ideal ist also genau dann ein Unterring von R, wenn $I = R$ ist.

11 Quotientenringe

Es sei R ein Ring mit 1 und I ein Ideal in R. Dann ist I insbesondere ein Normalteiler von R. Wir erinnern an die Kongruenzrelation modulo I

$$r_1 \equiv r_2 \bmod I \Leftrightarrow r_1 - r_2 \in I.$$

Die Äquivalenzklasse, die $r \in R$ enthält, also die Rechtsnebenklasse von I in R, die r enthält, bezeichnen wir mit $I + r$. Also

$$I + r := \{x + r \mid x \in I\}.$$

Die Menge der Rechtsnebenklassen

$$R/I = \{I + r \mid r \in R\}$$

mit der Verknüpfung

$$(I + r_1) + (I + r_2) := I + (r_1 + r_2)$$

bildet eine abelsche Gruppe nach Satz 3.5.

Satz 11.1 *Es sei I ein Ideal im Ring R mit 1. Dann bildet die Menge der Rechtsnebenklassen R/I zusammen mit den Verknüpfungen*

$$(I + r_1) + (I + r_2) := I + (r_1 + r_2) \text{ und } (I + r_1) \cdot (I + r_2) := I + (r_1 r_2)$$

einen Ring mit Einselement $I + 1$.

Definition Dieser Ring heißt der *Quotientenring* oder der *Faktorring* von R nach I.

Beweis. Wir müssen nur noch die Axiome der Multiplikation nachweisen.

Zunächst zeigen wir, dass die Multiplikation wohl definiert ist. Es sei $r_1' \in I + r_1$ und $r_2' \in I + r_2$. Dann ist $r_1' - r_1 = x_1 \in I$ und $r_2' - r_2 = x_2 \in I$. Dann gilt

$$r_1' r_2' = (x_1 + r_1)(x_2 + r_2) = x_1 x_2 + r_1 x_2 + x_1 r_2 + r_1 r_2.$$

Da I ein Ideal ist, gilt $x_1 x_2, r_1 x_2, x_1 r_2 \in I$. Also gilt $r_1' r_2' - r_1 r_2 \in I$, also

$$I + r_1' r_2' = I + r_1 r_2.$$

Daraus folgt, dass die Multiplikation auf R/I wohl definiert ist.

Die Axiome können nun leicht bewiesen werden. □

Beispiel 11.1

$$\mathbb{Z}/(n) = \mathbb{Z}_n.$$

Es sei nun K ein Körper und $p(x) \in K[x]$ ein Polynom. Wir betrachten den Quotientenring $K[x]/(p(x))$.

Lemma 11.1 *Es sei $f(x), g(x) \in K[x]$, $f(x) = q(x)p(x) + r(x)$, $g(x) = s(x)p(x) + t(x)$, $\operatorname{grad} r(x) < \operatorname{grad} p(x)$, $\operatorname{grad} t(x) < \operatorname{grad} p(x)$. Dann gilt*

$$f(x) \equiv g(x) \bmod (p(x)) \Leftrightarrow r(x) = t(x).$$

Beweis.

$$\begin{aligned} & f(x) \equiv g(x) \bmod (p(x)) \\ \Leftrightarrow \quad & f(x) - g(x) \in (p(x)) \\ \Leftrightarrow \quad & p(x) | (f(x) - g(x)) \\ \Leftrightarrow \quad & p(x) | [(q(x) - s(x))p(x) + (r(x) - t(x))] \\ \Leftrightarrow \quad & p(x) | (r(x) - t(x)) \\ \Leftrightarrow \quad & r(x) = t(x). \end{aligned}$$

□

Satz 11.2 *Es sei $P = (p(x))$, wobei $p(x)$ ein Polynom vom Grad $n > 0$ ist. Dann gilt*

$$K[x]/(p(x)) = \{P + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}.$$

Beweis. Es sei $P + f(x) \in K[x]/(p(x))$. Schreibe $f(x) = q(x)p(x) + r(x)$ mit $\operatorname{grad} r(x) < n$. Dann gilt nach dem vorhergehenden Lemma $P + f(x) = P + r(x)$.

Angenommen, $P + r(x) = P + t(x)$ wobei $\operatorname{grad} r(x), \operatorname{grad} t(x) < n$. Dann gilt $r(x) \equiv t(x) \bmod P$. Nach dem vorhergehenden Lemma gilt $r(x) = t(x)$. □

Notation Wir schreiben $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ anstelle von $P + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Also

$$K[x]/(p(x)) = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}.$$

Beispiel 11.2 Wir betrachten $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Es gilt

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}.$$

Was ist z.B. $(x + 1)(x + 1)$ in $\mathbb{Z}_2[x]/(x^2 + x + 1)$? Es gilt

$$(x + 1)(x + 1) = x^2 + 1 = (x^2 + x + 1) + x.$$

Also gilt $(x + 1)(x + 1) = x$ in $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Auf diese Weise erhalten wir die folgende Multiplikationstafel:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Wir untersuchen nun, unter welchen Voraussetzungen der Quotientenring ein Integritätsbereich oder ein Körper ist.

Definition Es sei R ein kommutativer Ring mit 1. Ein Ideal $I \neq R$ von R heißt *Primideal*, wenn für alle $x, y \in R$ gilt: Aus $xy \in I$ folgt $x \in I$ oder $y \in I$.

Satz 11.3 *Es sei R ein kommutativer Ring mit 1, $a \in R$. Dann ist (a) genau dann ein vom Nullideal verschiedenes Primideal, wenn a ein Primelement ist.*

Beweis. "$\Rightarrow$": Es sei (a) ein Primideal. Da $(a) \neq R$, ist a keine Einheit. Wegen $(a) \neq (0)$ gilt $a \neq 0$. Es seien $x, y \in R$ und es gelte $a|xy$. Dann folgt $xy \in (a)$. Da (a) ein Primideal ist, folgt $x \in (a)$ oder $y \in (a)$. Also gilt $a|x$ oder $a|y$.

"$\Leftarrow$": Es sei a ein Primelement. Da $a \neq 0$ und a keine Einheit ist, gilt $(a) \neq (0), R$. Es sei $xy \in (a)$ für $x, y \in R$. Dann folgt $a|xy$. Da a ein Primelement ist, folgt $a|x$ oder $a|y$, also $x \in (a)$ oder $y \in (a)$. □

Satz 11.4 *Es sei I ein Ideal des kommutativen Rings R mit 1. Dann ist I genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.*

Beweis. Übungsaufgabe. □

Definition Es sei R ein kommutativer Ring mit 1. Ein Ideal I von R heißt *maximales Ideal* in R, wenn $I \neq R$ und für alle Ideale J von R mit $I \subset J \subset R$ gilt: $J = I$ oder $J = R$.

Satz 11.5 *Es sei R ein euklidischer Ring, $a \in R$, $a \neq 0$. Dann ist (a) genau dann ein maximales Ideal von R, wenn a irreduzibel ist.*

Beweis. "$\Leftarrow$": Es sei a irreduzibel. Es sei $J \subset R$ ein Ideal mit $(a) \subset J \subset R$, $(a) \neq J$. Es ist zu zeigen: $J = R$. Da $(a) \neq J$, gibt es ein $b \in J$ mit $b \notin (a)$. Das bedeutet $b \neq ra$ für alle $r \in R$. Also $\mathrm{ggT}(a, b) = 1$, da a irreduzibel ist. Nach Satz 7.1 gibt es $s, t \in R$ mit

$$sa + tb = 1.$$

Nun gilt aber $sa \in (a) \subset J$ und $tb \in J$, also $1 \in J$. Aus Satz 10.4 folgt dann $J = R$.

"$\Rightarrow$": Es sei (a) ein maximales Ideal. Angenommen, $a = st$ für $s, t \in R$. Wegen $a \neq 0$ ist $s, t \neq 0$. Dann gilt $(a) \subset (s)$. Da (a) ein maximales Ideal ist, folgt $(a) = (s)$ oder $(s) = R$. Gilt $(s) = R$, dann ist $1 \in (s)$, also ist s eine Einheit. Wenn $(a) = (s)$ gilt, dann gibt es ein $b \in R$ mit $s = ab$, also $a = st = abt$. Daraus folgt $bt = 1$, also ist t eine Einheit. □

Satz 11.6 *Ein nichttrivialer kommutativer Ring R mit 1 ist genau dann ein Körper, wenn (0) und R die einzigen Ideale sind.*

Beweis. "$\Rightarrow$": Es sei R ein Körper und $I \subset R$ ein Ideal mit $I \neq (0)$. Dann gibt es ein $a \in I$ mit $a \neq 0$. Dann ist aber auch $aa^{-1} = 1 \in I$, also $I = R$ nach Satz 10.4.

"$\Leftarrow$": Es seien (0) und R die einzigen Ideale von R. Es sei $a \in R$, $a \neq 0$. Wir betrachten das Ideal (a). Es gilt $(a) \neq (0)$, da $1 \cdot a \in (a)$. Also folgt $(a) = R$. Dann gilt aber $1 \in (a)$ und es gibt ein $b \in R$ mit $ab = 1$. Also besitzt a ein inverses Element b und R ist ein Körper. □

Satz 11.7 *Es sei R ein Ring mit 1, I ein Ideal in R. Ist J ein Ideal von R mit $I \subset J$, so ist J/I ein Ideal von R/I. Ist umgekehrt U ein Ideal von R/I, so gibt es ein Ideal J von R mit $I \subset J$ und $U = J/I$.*

Beweis. (a) Es sei $I + r \in R/I$, $I + a \in J/I$. Dann gilt $(I + r)(I + a) = I + ra \in J/I$, da $ra \in J$.

(b) Es sei U ein Ideal von R/I. Setze

$$J := \{r \in R \,|\, I + r \in U\}.$$

Dann ist J ein Ideal mit $I \subset J$ und $U = J/I$. □

Satz 11.8 *Es sei I ein Ideal des kommutativen Rings R mit 1. Dann ist I genau dann ein maximales Ideal von R, wenn R/I ein Körper ist.*

Beweis. "$\Rightarrow$": Es sei I ein maximales Ideal. Es sei $U \subset R/I$ ein Ideal mit $U \neq (0)$. Dann gibt es nach Satz 11.7 ein Ideal $J \subset R$ mit $I \subset J$, $I \neq J$ und $J/I = U$. Da I ein maximales Ideal ist, folgt $J = R$, also $U = R/I$. Nach Satz 11.6 ist R/I ein Körper.

"$\Leftarrow$": Es sei R/I ein Körper. Es sei $J \subset R$ ein Ideal in R mit $I \subset J$, aber $I \neq J$. Dann ist J/I ein Ideal von R/I mit $J/I \neq (0)$. Da R/I ein Körper ist, gilt nach Satz 11.6 $J/I = R/I$. Daraus folgt $J = R$. Also ist I ein maximales Ideal von R. □

Korollar 11.1 *In einem nichttrivialen kommutativen Ring mit 1 ist jedes maximale Ideal auch ein Primideal.*

In euklidischen Ringen gilt auch die Umkehrung.

Korollar 11.2 *Es sei R ein euklidischer Ring, $a \in R$. Dann ist $R/(a)$ genau dann ein Körper, wenn a irreduzibel in R ist.*

12 Ringhomomorphismen

Analog zu Gruppenhomomorphismen betrachten wir nun Abbildungen zwischen Ringen, die die Addition und Multiplikation erhalten.

Definition Es seien R und S zwei Ringe mit 1. Eine Abbildung $f : R \to S$ heißt *Ringhomomorphismus*, wenn für alle $a, b \in R$ gilt:

(i) $f(a + b) = f(a) + f(b)$,

(ii) $f(a \cdot b) = f(a) \cdot f(b)$,

(iii) $f(1) = 1$.

Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus. Wenn es einen Ringisomorphismus zwischen den Ringen mit Einselement R und S gibt, dann sagen wir, R und S sind *isomorph* und wir schreiben $R \cong S$.

Ein Ringhomomorphismus $f : R \to S$ ist insbesondere ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$. Deswegen gilt nach Satz 2.5 $f(0) = 0$ und $f(-a) = -f(a)$ für alle $a \in R$.

Beispiel 12.1 Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}_n$ mit $f(x) = [x]$ ist ein Ringhomomorphismus.

Analog zu Satz 3.6 gilt:

Satz 12.1 *Ist $f : R \to S$ ein Ringhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Ideal von R.*

Beweis. Ist $x \in \operatorname{Ker} f$ und $r \in R$, so gilt

$$f(xr) = f(x)f(r) = 0 \cdot f(r) = 0,$$

also $xr \in \operatorname{Ker} f$. Analog $rx \in \operatorname{Ker} f$. Der Rest folgt aus Satz 3.6. □

Das Bild $\operatorname{Im} f$ eines Ringhomomorphismus $f : R \to S$ ist ein Unterring von S.

Analog zu Satz 3.7 gilt:

Satz 12.2 (Homomorphiesatz für Ringe) *Für einen Ringhomomorphismus $f : R \to S$ gilt:*

$$R/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Beweis. Es sei $K = \operatorname{Ker} f$. Im Beweis des Homomorphiesatzes für Gruppen (Satz 3.7) hatten wir gesehen, dass $\psi : R/K \to \operatorname{Im} f$ mit $\psi(K + r) = f(r)$ ein Gruppenisomorphismus ist. Wir müssen also nur noch zeigen, dass ψ ein Ringhomomorphismus ist. Es gilt

$$\psi((K + r)(K + s)) = \psi(K + rs) = f(rs) = f(r)f(s) = \psi(K + r)\psi(K + s).$$

□

13 Körpererweiterungen

Ist $p(x)$ ein irreduzibles Polynom über dem Körper K, dann ist der Quotientenring $E = K[x]/(p(x))$ ein Körper. Dieser Körper enthält einen Unterring, der isomorph zum Körper K ist. Wir können daher E als Körpererweiterung von K auffassen.

Definition Ein *Unterkörper* eines Körpers E ist ein Unterring K, der auch ein Körper ist. In diesem Fall nennen wir E eine *Körpererweiterung* von K.

Satz 13.1 *Es sei $p(x)$ ein irreduzibles Polynom über dem Körper K. Dann ist $E = K[x]/(p(x))$ ein Erweiterungskörper von K.*

Beweis. Es sei

$$\widetilde{K} := \{(p(x)) + a_0 \,|\, a_0 \in K\} \subset E.$$

Dann ist $\widetilde{K}$ ein Unterkörper von E, der isomorph zu K ist. □

Satz 13.2 *Es sei E ein Erweiterungskörper des Körpers K. Dann ist E ein Vektorraum über K.*

Beweis. Der Körper E ist eine abelsche Gruppe unter der Addition. Man kann Elemente von E mit Elementen von K multiplizieren. Diese skalare Multiplikation genügt den Vektorraumaxiomen. □

Definition Der *Grad* der Körpererweiterung E über K ist die Dimension von E als Vektorraum über K, in Zeichen

$$[E : K] := \dim_K E.$$

Ist $[E : K] < \infty$, dann heißt E eine *endliche* Körpererweiterung von K.

Beispiel 13.1 $[\mathbb{C} : \mathbb{R}] = 2$. Denn: $\mathbb{C} = \{a + ib \,|\, a, b \in \mathbb{R}\}$ und $\{1, i\}$ ist eine Basis von $\mathbb{C}$ über $\mathbb{R}$.

Satz 13.3 *Es sei $p(x)$ ein irreduzibles Polynom vom Grade n über dem Körper K und $E = K[x]/(p(x))$. Dann gilt $[E : K] = n$.*

Beweis. Nach Satz 11.2 gilt

$$E = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \,|\, a_0, \ldots, a_{n-1} \in K\}$$

und jedes Element von E kann auf eindeutige Weise so geschrieben werden. Also ist

$$\{1, x, x^2, \ldots, x^{n-1}\}$$

eine Basis von E über K. □

Satz 13.4 *Es sei F eine endliche Körpererweiterung von E und E eine endliche Körpererweiterung von K. Dann ist F eine endliche Körpererweiterung von K und*

$$[F : K] = [F : E][E : K].$$

Beweis. Es gilt $K \subset E \subset F$. Es sei $[F : E] = m$ und $\{u_1, \dots, u_m\}$ eine Basis von F über E, $[E : K] = n$ und $\{v_1, \dots, v_n\}$ eine Basis von E über K. Wir zeigen, dass

$$\mathcal{B} := \{v_j u_i \,|\, i = 1, \dots, m,\ j = 1, \dots, n\}$$

eine Basis von F über K ist.

Es sei $x \in F$. Dann ist $x = \sum_{i=1}^{m} \lambda_i u_i$ für $\lambda_i \in E$. Jedes λ_i kann nun als $\lambda_i = \sum_{j=1}^{n} \mu_{ij} v_j$ mit $\mu_{ij} \in K$ geschrieben werden. Also gilt

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i.$$

Also ist $\mathcal{B}$ ein Erzeugendensystem von F über K.

Es sei nun

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i = 0, \quad \mu_{ij} \in K.$$

Da $u_1, \dots, u_m$ linear unabhängig über E sind, folgt, dass für jedes fest gewählte $i = 1, \dots, m$ gilt: $\sum_{j=1}^{n} \mu_{ij} v_j = 0$. Da $v_1, \dots, v_n$ linear unabhängig über K sind, folgt $\mu_{ij} = 0$ für jedes i und jedes j. Also ist $\mathcal{B}$ linear unabhängig. □

Definition Es sei E eine Körpererweiterung von K und $\alpha \in E$. Es sei $K(\alpha)$ (K *adjungiert* α) der kleinste Unterkörper von E, der K und α enthält, d.h. der Durchschnitt aller Unterkörper von E, die K und α enthalten. Der Körper $K(\alpha)$ heißt der durch *Adjunktion* von α zu K entstandene Körper.

Beispiel 13.2 (a) Es gilt $\mathbb{R}(i) = \mathbb{C}$, da jeder Unterkörper von $\mathbb{C}$, der $\mathbb{R}$ und i enthält, auch alle Elemente der Form $a + ib$, $a, b \in \mathbb{R}$, enthalten muss.

(b) Es gilt $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$.

Definition Es sei E eine Körpererweiterung von K. Ein Element $\alpha \in E$ heißt *algebraisch* über K, wenn es Elemente $a_0, a_1, \dots, a_n \in K$ gibt, die nicht alle gleich Null sind, so dass

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Mit anderen Worten ist α Wurzel eines vom Nullpolynom verschiedenen Polynoms in $K[x]$. Ein Element $\alpha \in E$ heißt *transzendent*, wenn es nicht algebraisch über K ist.

Beispiel 13.3 Die Zahlen $\sqrt{2}$ und i sind algebraisch über $\mathbb{Q}$. (Sie sind Wurzeln von $x^2 - 2$ und $x^2 + 1$.) F. v. Lindemann ($\star$ 1852 Hannover, † 1939) hat 1882 bewiesen, dass π transzendent ist. (Die Transzendenz von π bedeutet, dass die Quadratur des Kreises unmöglich ist.)

Satz 13.5 *Es sei E eine Körpererweiterung von K und $\alpha \in E$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes Polynom $m_\alpha(x) \in K[x]$ mit den folgenden Eigenschaften:*

(i) *$m_\alpha(x)$ ist ein vom Nullpolynom verschiedenes Polynom minimalen Grades mit α als Wurzel.*

(ii) *$m_\alpha(x)$ ist Teiler jedes Polynoms aus $K[x]$, das α als Wurzel besitzt.*

(iii) *$m_\alpha(x)$ ist* normiert*, d.h. der Leitkoeffizient von $m_\alpha(x)$ ist 1.*

Definition Das Polynom $m_\alpha(x)$ heißt das *Minimalpolynom* von α.

Beweis. Es sei $m_\alpha(x)$ ein Polynom mit der Eigenschaft (i). Es sei $f(x) \in K[x]$ ein beliebiges Polynom mit $f(\alpha) = 0$. Division mit Rest ergibt

$$f(x) = q(x)m_\alpha(x) + r(x), \quad \operatorname{grad} r(x) < \operatorname{grad} m_\alpha(x).$$

Wegen $f(\alpha) = 0$ gilt auch $r(\alpha) = 0$, also ist $r(x)$ das Nullpolynom. Daraus folgt (ii) und $m_\alpha(x)$ ist bis auf eine Konstante $q(x) = a_0$ eindeutig bestimmt. Das normierte Polynom ist daher eindeutig bestimmt. □

Satz 13.6 *Es sei E eine Körpererweiterung von K und $\alpha \in E$ algebraisch über K. Ein Polynom $f(x) \in K[x]$ ist genau dann das Minimalpolynom von α, wenn $f(\alpha) = 0$ und $f(x)$ irreduzibel und normiert ist.*

Beweis. "⇒": Es sei $f(x)$ das Minimalpolynom von α. Angenommen, $f(x) = p(x)q(x)$. Aus $f(\alpha) = 0$ folgt dann $p(\alpha) = 0$ oder $q(\alpha) = 0$. Da der Grad von $f(x)$ minimal ist, folgt $\operatorname{grad} p(x) = \operatorname{grad} f(x)$ oder $\operatorname{grad} q(x) = \operatorname{grad} f(x)$. Das bedeutet aber, dass $q(x)$ oder $p(x)$ eine Einheit ist.

"⇐": Es sei $f(x)$ ein normiertes irreduzibles Polynom mit $f(\alpha) = 0$. Dann muss der Grad von $f(x)$ minimal unter den Polynomen mit α als Wurzel sein. In dem Beweis des letzten Satzes haben wir gesehen, dass ein Polynom minimalen Grades mit α als Wurzel Teiler jedes Polynoms von $K[x]$, das α als Wurzel hat, ist. Also ist $f(x)$ das Minimalpolynom von α. □

Satz 13.7 *Es sei E eine Körpererweiterung von K, $\alpha \in E$ algebraisch über K und $p(x)$ ein irreduzibles Polynom vom Grad n über K mit α als Wurzel. Dann gilt*

$$K(\alpha) \cong K[x]/(p(x))$$

und die Elemente von $K(\alpha)$ können in eindeutiger Weise in der folgenden Form geschrieben werden:

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in K.$$

Beweis. Wir definieren eine Abbildung $f : K[x] \to K(\alpha)$ durch $q(x) \mapsto q(\alpha)$. Dann ist f ein Ringhomomorphismus, also ist Ker f ein Ideal von $K[x]$. Nach Korollar 10.1 sind alle Ideale in $K[x]$ Hauptideale. Daher gilt

$$\operatorname{Ker} f = (r(x)), \quad r(x) \in K[x].$$

Da $p(\alpha) = 0$, gilt $p(x) \in \operatorname{Ker} f$ und $r(x)|p(x)$. Da $p(x)$ irreduzibel ist, folgt $p(x) = kr(x)$ für ein $k \in K$ mit $k \neq 0$. Also gilt

$$\operatorname{Ker} f = (p(x)).$$

Nach dem Homomorphiesatz für Ringe folgt

$$K[x]/(p(x)) \cong \operatorname{Im} f \subset K(\alpha).$$

Nach Satz 11.2 ist $K[x]/(p(x))$ ein Körper. Daher ist Im f ein Unterkörper von $K(\alpha)$, der K und α enthält. Da aber $K(\alpha)$ nach Definition der kleinste Körper ist, der K und α enthält, folgt

$$K[x]/(p(x)) \cong K(\alpha).$$

Die Darstellung der Elemente von $K(\alpha)$ folgt aus diesem Isomorphismus und Satz 11.2. □

Korollar 13.1 *Ist n der Grad des Minimalpolynoms von α über K, so gilt:*

$$[K(\alpha) : K] = n.$$

Beweis. Aus den Sätzen 13.7 und 13.3 folgt:

$$[K(\alpha) : K] = [K[x]/(m_\alpha(x)) : K] = n.$$

□

Beispiel 13.4 Es gilt $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Lemma 13.1 *Es sei $p(x)$ ein irreduzibles Polynom über K. Dann besitzt K eine endliche Körpererweiterung E, in der $p(x)$ eine Wurzel besitzt.*

Beweis. Es sei

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad P := (p(x)).$$

Betrachte $E := K[x]/P$. Nach Korollar 11.2 ist E ein Körper, der K enthält. Die Elemente von E sind Rechtsnebenklassen der Form $P + f(x)$. Das Element $P + x \in E$ ist eine Wurzel von $p(x)$, da

$$\begin{aligned} & a_0 + a_1(P + x) + \cdots + a_n(P + x)^n \\ &= a_0 + (P + a_1 x) + \cdots + (P + a_n x^n) \\ &= P + (a_0 + a_1 x + \cdots + a_n x^n) \\ &= P + p(x) \\ &= P + 0 \end{aligned}$$

und $P + 0$ ist das Nullelement von E. □

Satz 13.8 *Ist $f(x)$ ein Polynom über dem Körper K, dann gibt es eine endliche Körpererweiterung E von K, in der $f(x)$ in Linearfaktoren zerfällt.*

Bemerkung 13.1 Man kann zeigen, dass der kleinste solche Körper bis auf Isomorphie eindeutig bestimmt ist. Dieser Körper wird der *Zerfällungskörper* von $f(x)$ genannt.

Beweis. Wir beweisen die Behauptung durch Induktion über den Grad von $f(x)$.

Induktionsanfang: $\operatorname{grad} f(x) \leq 1$. Dieser Fall ist klar.

Induktionsannahme: Die Behauptung gelte für Polynome vom Grad $n - 1$.

Induktionsschritt: Es sei $f(x)$ ein Polynom vom Grad n. Dann gilt

$$f(x) = p(x)q(x), \quad \text{wobei } p(x) \text{ irreduzibel ist.}$$

Nach Lemma 13.1 hat $p(x)$ eine Wurzel α in einem Erweiterungsköper E' von K. Also gilt über E':

$$f(x) = (x - \alpha)g(x), \quad \operatorname{grad} g(x) = n - 1.$$

Nach Induktionsannahme besitzt E' eine endliche Körpererweiterung E, in der $g(x)$ in Linearfaktoren zerfällt. Also zerfällt auch $f(x)$ über E in Linearfaktoren. Nach Satz 13.4 ist E eine endliche Körpererweiterung von K. □

Beispiel 13.5 Der Zerfällungskörper des Polynoms $x^2 + 1$ über $\mathbb{R}$ ist der Körper $\mathbb{C}$ der komplexen Zahlen.

14 Endliche Körper

Wir betrachten nun die Struktur von endlichen Körpern.

Definition Es sei R ein Ring mit 1. Die *Charakteristik* von R, in Zeichen $\operatorname{char} R$, ist die kleinste natürliche Zahl $q > 0$, so dass

$$\underbrace{1 + \cdots + 1}_{q} = 0$$

in R gilt. Wenn es kein solches q gibt, dann definieren wir die Charakteristik von R als 0.

Beispiel 14.1 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik 0, $\mathbb{Z}_n$ hat die Charakteristik n.

Satz 14.1 *Die Charakteristik eines Integritätsbereichs ist* 0 *oder eine Primzahl.*

Beweis. Es sei R ein Ring mit 1. Wir betrachten den Ringhomomorphismus $f : \mathbb{Z} \to R$, der wie folgt definiert ist:

$$f(n) = \begin{cases} 1 + \cdots + 1 \quad (n \text{ mal}) & \text{falls } n > 0, \\ 0 & \text{falls } n = 0, \\ -1 - \cdots - 1 \quad (|n| \text{ mal}) & \text{falls } n < 0. \end{cases}$$

Der Kern von f ist ein Ideal in dem Hauptidealring $\mathbb{Z}$, also gilt $\operatorname{Ker} f = (q)$ für ein $q \geq 0$. Diese Zahl q ist die Charakteristik von R. Nach dem Homomorphiesatz gilt

$$\operatorname{Im} f \cong \begin{cases} \mathbb{Z}_q & \text{falls } q \neq 0, \\ \mathbb{Z} & \text{falls } q = 0. \end{cases}$$

Es sei nun R ein Integritätsbereich. Dann ist auch $\operatorname{Im} f$ ein Integritätsbereich, da $\operatorname{Im} f$ ein Unterring von R ist. Nach Satz 11.4 ist $\operatorname{Im} f \cong \mathbb{Z}/(q)$ genau dann ein Integritätsbereich, wenn (q) ein Primideal in $\mathbb{Z}$ ist. Nach Satz 11.3 ist aber (q) genau dann ein Primideal in $\mathbb{Z}$, wenn q eine Primzahl ist oder $q = 0$ gilt. □

Satz 14.2 *Ist die Charakteristik eines Körpers K eine Primzahl p, so enthält K einen Unterkörper, der isomorph zu $\mathbb{Z}_p$ ist.*

Beweis. Der Körper K enthält den Unterring $\operatorname{Im} f$ (siehe den Beweis des vorhergehenden Satzes). Ist die Charakteristik von K eine Primzahl p, so ist dieser Unterkörper isomorph zu $\mathbb{Z}_p$. □

Satz 14.3 *Die Charakteristik eines endlichen Körpers ist von Null verschieden.*

Beweis. Ist die Charakteristik des Körpers K gleich Null, so ist der Unterring $\operatorname{Im} f$ isomorph zu $\mathbb{Z}$, enthält also unendlich viele Elemente. □

Satz 14.4 *Ein endlicher Körper K hat p^m Elemente, wobei p eine Primzahl und m eine natürliche Zahl ist.*

Beweis. Nach den vorherigen Resultaten hat K Primzahlcharakteristik p und enthält einen Unterkörper, der isomorph zu $\mathbb{Z}_p$ ist. Wir identifizieren diesen Unterkörper mit $\mathbb{Z}_p$. Das bedeutet, dass wir K als Körpererweiterung von $\mathbb{Z}_p$ auffassen. Der Grad dieser Körpererweiterung muss endlich sein, da K endlich ist. Es sei

$$[K : \mathbb{Z}_p] = m.$$

Es sei $\{e_1, \dots, e_m\}$ eine Basis von K über $\mathbb{Z}_p$, derart dass

$$K = \{\lambda_1 e_1 + \cdots + \lambda_m e_m \mid \lambda_i \in \mathbb{Z}_p\}.$$

Da es für jedes λ_i genau p Möglichkeiten gibt, enthält K genau p^m Elemente. □

Definition Ein endlicher Körper mit p^m Elementen wird auch ein *Galoiskörper* genannt und mit $\mathbb{F}_{p^m}$ oder $\mathrm{GF}(p^m)$ bezeichnet.

Man kann zeigen, dass zu jeder Primzahl p und jeder natürlichen Zahl m ein Galoiskörper $\mathbb{F}_{p^m}$ existiert und je zwei Körper mit p^m Elementen zueinander isomorph sind.

Wir haben gesehen, dass $\mathbb{F}_{p^m}$ eine Körpererweiterung von $\mathbb{Z}_p$ vom Grad m ist. Wenn wir ein irreduzibles Polynom $q(x)$ vom Grad m in $\mathbb{Z}_p[x]$ finden können, dann gilt nach Satz 11.2

$$\mathbb{F}_{p^m} \cong \mathbb{Z}_p[x]/(q(x)).$$

Nach Lemma 13.1 gibt es ein Element $\alpha \in \mathbb{F}_{p^m}$ mit $q(\alpha) = 0$ und

$$\mathbb{F}_{p^m} \cong \mathbb{Z}_p(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbb{Z}_p\}.$$

Beispiel 14.2 Wir betrachten

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1) = \mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}.$$

Verknüpfungstabellen:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

In $\mathbb{F}_4$ gilt $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$. Daher können wir $\mathbb{F}_4$ auch so repräsentieren:

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}.$$

Mit dieser Darstellung lauten die Verknüpfungstabellen:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Tatsächlich gibt es immer ein Element $\alpha \in \mathbb{F}_{p^m}$, so dass

$$\mathbb{F}_{p^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}, \quad \alpha^{p^m-1} = 1.$$

Der Grund ist der folgende Satz, den wir ohne Beweis angeben.

Theorem 14.1 *Es sei $\mathbb{F}_q^*$ die Menge der invertierbaren Elemente von $\mathbb{F}_q$. Dann ist $(\mathbb{F}_q^*, \cdot)$ eine zyklische Gruppe der Ordnung $q - 1$.*

Definition Ein erzeugendes Element der zyklischen Gruppe $(\mathbb{F}_q^*, \cdot)$ wird *primitives Element* von $\mathbb{F}_q$ genannt.

Beispiel 14.3 Die primitiven Elemente von $\mathbb{F}_4 = \mathbb{Z}_2(\alpha)$ sind α und $\alpha^2 = \alpha + 1$.

Definition Ein irreduzibles Polynom $g(x)$ vom Grad m über $\mathbb{Z}_p$ heißt ein *primitives Polynom*, falls $g(x)|(x^k - 1)$ für $k = p^m - 1$ und für kein kleineres k.

Satz 14.5 *Das irreduzible Polynom $g(x) \in \mathbb{Z}_p[x]$ vom Grad m ist genau dann primitiv, wenn x ein primitives Element von $\mathbb{Z}_p[x]/(g(x)) = \mathbb{F}_{p^m}$ ist.*

Beweis.

x ist ein primitives Element von $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/(g(x))$

$\Leftrightarrow$ $x^k = 1$ in $\mathbb{F}_{p^m}$ für $k = p^m - 1$ und kein kleineres k

$\Leftrightarrow$ $x^k - 1 \equiv 0 \bmod g(x)$ für $k = p^m - 1$ und kein kleineres k

$\Leftrightarrow$ $g(x)|(x^k - 1)$ für $k = p^m - 1$ und kein kleineres k.

□

Beispiel 14.4 Das Polynom $x^2 + x + 1$ ist ein primitives Polynom in $\mathbb{Z}_2[x]$.

15 Fehlerkorrigierende Codes

Zum Abschluss betrachten wir Anwendungen auf fehlerkorrigierende Codes. Es sei $\mathbb{F}_q$ der Galoiskörper mit q Elementen.

Definition Ein (q-*ärer*) *Code* C ist eine Teilmenge von $\mathbb{F}_q^n$. Ein *linearer Code* C ist ein Untervektorraum von $\mathbb{F}_q^n$. Wenn dieser Untervektorraum die Dimension k hat, so nennt man den Code C einen $[n, k]$-Code.

Beispiel 15.1 Es sei C die Teilmenge von $\mathbb{F}_2^n$, die aus allen n-Tupeln mit einer geraden Anzahl von Einsen besteht. Dann ist C ein binärer $[n, n-1]$-Code. Dieser Code heißt der $[n, n-1]$-*Parity-Check-Code*.

Wir repräsentieren nun die n-Tupel von $\mathbb{F}_q^n$ durch Polynome. Das Polynom $x^n - 1 \in \mathbb{F}_q[x]$ erzeugt ein Hauptideal $(x^n - 1)$ in $\mathbb{F}_q[x]$. Nach Satz 11.2 wird der Quotientenring $\mathbb{F}_q[x]/(x^n - 1)$ durch die Menge der Polynome

$$\{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_q\}$$

repräsentiert. Die Zuordnung

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

definiert einen Vektorraumisomorphismus zwischen $\mathbb{F}_q^n$ und $\mathbb{F}_q[x]/(x^n - 1)$. Wir identifizieren diese beiden Vektorräume über $\mathbb{F}_q$ unter diesem Isomorphismus.

Definition Ein linearer Code C in $\mathbb{F}_q^n$ heißt *polynomial*, wenn C ein Ideal in $\mathbb{F}_q[x]/(x^n - 1)$ ist.

Definition Ein linearer Code C heißt *zyklisch*, wenn gilt:

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Satz 15.1 *Ein linearer Code ist genau dann polynomial, wenn er zyklisch ist.*

Beweis. "⇒": Es sei C ein Ideal in $\mathbb{F}_q[x]/(x^n - 1)$ und $c(x) = c_0 + c_1 x + \cdots c_{n-1} x^{n-1}$ ein Kodewort in C. Dann ist auch

$$xc(x) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} \in C.$$

"⇐": Es sei C zyklisch. Die Bedingung

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$$

bedeutet, dass mit $c(x) \in C$ auch $xc(x) \in C$ gilt. Also ist mit $c(x)$ auch $x^i c(x)$ in C für jedes i. Da C linear ist, ist auch $a(x)c(x)$ in C für jedes Polynom $a(x) \in \mathbb{F}_q[x]/(x^n - 1)$. Also ist C ein Ideal in $\mathbb{F}_q[x]/(x^n - 1)$. □

Satz 15.2 *Es sei C ein zyklischer $[n,k]$-Code über $\mathbb{F}_q$. Dann gilt*

(i) *Es gibt ein eindeutig bestimmtes normiertes Polynom $g(x) \in \mathbb{F}_q[x]$ vom Grad $n-k$ mit $g(x)|(x^n-1)$, so dass $C = (g(x))$ ist.*

(ii) *$\{g(x), g(x)x, \ldots, g(x)x^{k-1}\}$ ist eine Basis von C.*

Beweis. (i) Da $\mathbb{F}_q[x]/(x^n-1)$ ein Hauptidealring ist, entspricht jeder zyklische Code C einem Hauptideal $(g(x))$ in $\mathbb{F}_q[x]/(x^n-1)$. Dabei ist $g(x)$ ein Polynom kleinsten Grades, das in C enthalten ist. Wählen wir $g(x)$ normiert, so ist $g(x)$ eindeutig. Das Polynom $g(x)$ muss ein Teiler von x^n-1 sein, denn sonst wäre $\mathrm{ggT}(g(x), x^n-1)$ ein Polynom kleineren Grades als $g(x)$, das das gleiche Ideal in $\mathbb{F}_q[x]/(x^n-1)$ erzeugt. Nach Satz 11.2 gilt

$$\operatorname{grad} g(x) = \dim \mathbb{F}_q[x]/(g(x)) = \dim(\mathbb{F}_q[x]/(x^n-1))/C) = n-k.$$

(ii) Es ist klar, dass die angegebenen Polynome linear unabhängig sind. Da C die Dimension k hat, folgt die Behauptung. □

Definition Es sei C ein zyklischer Code. Das eindeutig bestimmte Polynom $g(x)$ im vorherigen Satz heißt das *Erzeugerpolynom* von C. Das Polynom $h(x) = (x^n-1)/g(x)$ heißt das *Kontrollpolynom* von C.

Beispiel 15.2 Der $[n, n-1]$-Parity-Check-Code C über $\mathbb{F}_2$ ist ein zyklischer Code, der durch das Polynom $1+x$ erzeugt wird. Denn nach Satz 9.6 ist ein Polynom in $\mathbb{F}_2[x]$ genau dann durch $1+x$ teilbar, wenn es eine gerade Anzahl von von Null verschiedenen Koeffizienten hat.

Beispiel 15.3 Wir betrachten zyklische Codes der Länge 7 über $\mathbb{F}_2$. Über $\mathbb{F}_2$ gilt

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1).$$

Es gibt also insgesamt 8 zyklische Codes der Länge 7 über $\mathbb{F}_2$:

$$\begin{aligned}
C_1 &= (0) = \{0\} \\
C_2 &= (1) = \mathbb{F}_2^7 \\
C_3 &= (x-1): \quad [7,6]\text{-Parity-Check-Code} \\
C_4 &= (x^3+x+1) \\
C_5 &= (x^3+x^2+1) \\
C_6 &= ((x-1)(x^3+x+1)) \\
C_7 &= ((x-1)(x^3+x^2+1)) \\
C_8 &= ((x^3+x+1)(x^3+x^2+1))
\end{aligned}$$

Die Codes C_4 und C_5 sind sogenannte $[7,4]$-*Hamming-Codes*. Sie sind *maximale zyklische Codes*, da sie maximalen Idealen entsprechen.

In der Praxis sieht die Codierung mit zyklischen Codes wie folgt aus: Es sei C ein zyklischer $[n,k]$-Code mit Erzeugerpolynom $g(x)$. Eine Nachricht $a(x) \in \mathbb{F}_q[x]/(x^n-1)$ wird in der Form

$$c(x) = x^{n-k}a(x) - r(x) \in C$$

kodiert, wobei $x^{n-k}a(x) = q(x)g(x) + r(x)$ mit $\operatorname{grad} r(x) < n-k$ ist. Um zu erkennen, ob bei dem empfangenen Wort $v(x)$ ein Fehler vorliegt oder nicht, muss man testen, ob $v(x)$ durch $g(x)$ teilbar ist oder nicht. Dies ist technisch einfach zu realisieren, da die Division durch ein festes Polynom durch ein einfaches Schieberegister realisiert werden kann. Ist $v(x)$ durch $g(x)$ teilbar, so gilt $v(x) = x^{n-k}a(x) - r(x)$ und wegen $\operatorname{grad} r(x) < n-k$ kann daran die gesendete Nachricht $a(x)$ unmittelbar abgelesen werden.

Beispiel 15.4 Es sei $q = 2$ und $C \subset \mathbb{F}_2^n$ ein zyklischer Code, der von einem primitiven Polynom $g(x)$ vom Grad m über $\mathbb{F}_2$ erzeugt wird. Es gelte $n \leq 2^m - 1$. Dann können alle einfachen und alle doppelten Fehler aufgedeckt werden.

Beweis. Es sei $c(x)$ das übermittelte Kodewort und $v(x) = c(x) + e(x)$ das empfangene Wort. Man nennt $e(x)$ auch das *Fehlerpolynom*. Ein Fehler ist genau dann feststellbar, wenn $g(x)$ das Wort $v(x)$ nicht teilt. Da $g(x)|c(x)$, lässt sich ein Fehler genau dann entdecken, wenn $g(x)$ das Polynom $e(x)$ nicht teilt.

Angenommen, ein einziger Fehler ist bei der Übertragung aufgetreten. Dann enthält das Fehlerpolynom einen einzigen Term, also $e(x) = x^i$ für ein i mit $0 \leq i < n$. Da $g(x)$ irreduzibel ist, hat es 0 nicht als Wurzel. Daher teilt $g(x)$ das Polynom x^i nicht und der Fehler x^i wird aufgedeckt.

Wenn ein doppelter Fehler auftritt, dann gilt

$$e(x) = x^i + x^j = x^i(1 + x^{j-i}) \text{ mit } 0 \leq i < j < n.$$

Nun teilt $g(x)$ nicht x^i und da $g(x)$ primitiv ist, teilt $g(x)$ auch nicht das Polynom $1 + x^{j-i}$, falls $j - i < 2^m - 1$ gilt. Da $g(x)$ irreduzibel ist und $n \leq 2^m - 1$, teilt $g(x)$ das Polynom $e(x) = x^i(1 + x^{j-i})$ nicht und alle doppelten Fehler werden entdeckt. □

Literatur

[1] S. Bosch: Algebra. 4. überarb. Aufl., Springer-Verlag, 2001. ISBN 3-540-41852-0

[2] W. J. Gilbert: Modern Algebra with Applications. John Wiley and Sons, 1976. ISBN 0-471-29891-3

[3] H.-J. Reiffen, G. Scheja, U. Vetter: Algebra. B.I.-Wissenschaftsverlag, 1969. ISBN 3-411-00110-0

Inhaltsverzeichnis