1.3 Ringe

1.3.1 Grundbegriffe und Beispiele

Am Beispiel der Gruppen wird im Abschnitt 1.2 gezeigt, dass bereits wenige Eigenschaften einer inneren Verknüpfung auf einer Menge zu einer reichhaltigen und nützlichen mathematischen Theorie führen. In der Mathematik kommen jedoch viele Situationen vor, in denen eine Menge mehrere innere Verknüpfungen trägt, die außerdem miteinander wechselwirken. Die bekanntesten Beispiele sind die verschiedenen Zahlbereiche:

Beispiel 58 (Zahlbereiche (Forts.)): In den Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ kann man die jeweiligen Zahlen nicht nur addieren, sondern auch multiplizieren. Dabei sind Addition und Multiplikation durch die *Distributivgesetze*

$$a(b+c) = ab + ac,\ (a+b)c = ac + bc$$

miteinander verwoben. Wegen des Kommutativgesetzes der Multiplikation folgt dabei das zweite aus dem ersten Distributivgesetz.

Die Zahlbereiche unterscheiden sich darin, dass $\mathbb{N}$ bezüglich $+$ keine Gruppe bildet, alle anderen Zahlbereiche aber schon.

Weiter bilden alle Zahlbereiche ohne die Zahl 0 eine Gruppe bezüglich der Multiplikation, außer $\mathbb{N}$ und $\mathbb{Z}$. ◇

Die lineare Algebra liefert ein weiteres interessantes Beispiel einer Menge mit zwei inneren Verknüpfungen:

Beispiel 59 (Matrixoperationen (Forts.)): Die quadratischen Matrizen der Menge $\mathbb{K}^{n\times n}$ kann man addieren und multiplizieren. Wie in der linearen Algebra gezeigt wird gelten auch hier die beiden oben genannten Distributivgesetze. Allerdings ist im Fall $n \geq 2$ die Matrixmultiplikation nicht kommutativ, weswegen man aus dem ersten Distributivgesetz *nicht* das zweite folgern kann.

Bezüglich der Matrixaddition bildet $\mathbb{K}^{n\times n}$ eine Gruppe. Die Matrixmultiplikation zeigt allerdings zwei merkwürdige Eigenschaften, die im Fall der Zahlbereiche nicht auftreten:

$$\begin{pmatrix} 2 & 3 \\ -4 & -6 \end{pmatrix} \begin{pmatrix} 3 & -9 \\ -2 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

das heißt ein Produkt AB kann Null sein, obwohl keiner der beiden Faktoren gleich Null ist. Es tritt sogar das extremere Phänomen

$$\begin{pmatrix} 0 & 9 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

auf, das heißt eine Potenz eines Elements kann Null sein, obwohl das Element selbst nicht gleich Null ist. ◇

Wir abstrahieren nun von diesen beiden Beispielen und erhalten eine neue algebraische Struktur:

DEFINITION 60: *Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer nicht leeren Menge R und zwei inneren Verknüpfungen*

$$+ : \ R \times R \to R, \ (r, s) \mapsto r + s,$$

$$\cdot : \ R \times R \to R, \ (r, s) \mapsto r \cdot s,$$

mit folgenden Eigenschaften:

1. *$(R, +)$ ist eine abelsche Gruppe.*
2. *$(R, \cdot)$ ist ein Monoid.*
3. *Die beiden Distributivgesetze*

   $$\forall a, b, c \in R \ a \cdot (b + c) = (a \cdot b) + (a \cdot c), \ (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

   gelten.

Die innere Verknüpfung $+$ nennt man Addition (in R) und bezeichnet ihr neutrales Element entsprechend mit 0 oder 0_R. Das Inverse von $a \in R$ in der Gruppe $(R, +)$ wird mit $-a$ bezeichnet.

Die innere Verknüpfung $\cdot$ nennt man Multiplikation (in R) und bezeichnet ihr neutrales Element entsprechend mit 1 oder 1_R. Das Inverse von $a \in R$ in dem Monoid $(R, \cdot)$ wird, falls es existiert, mit a^{-1} bezeichnet.

Ist die Multiplikation in R kommutativ, so nennt man $(R, +, \cdot)$ einen kommutativen Ring.

KONVENTIONEN: Um das Aufschreiben von Formeln und Gleichungen zu vereinfachen gelten folgende Regeln:

- »Punkt vor Strich«: Ausdrücke der Form $a \cdot b + c$ sind als $(a \cdot b) + c$ zu verstehen.
- Das Multiplikationssymbol $\cdot$ wird oft unterdrückt, das heißt man schreibt ab statt $a \cdot b$. In diesem Skript wird das Unterdrücken von $\cdot$ allerdings nur für das Rechnen mit Zahlen und Matrizen angewendet.

Man beachte weiter, dass in einem Ring R die im Abschnitt 1.1.2 eingeführte »Potenzrechnung« in zwei Formen auftritt:

- Multiplikative Form: das Symbol r^k steht im Fall $k \in \mathbb{N}$ für das Produkt $r \cdot r \cdot \ldots \cdot r$ mit n gleichen Faktoren r, im Fall $k = 0$ für das Ringelement 1 und im Fall $k < 0$ für das multiplikativ Inverse s^{-1} des Ringelements r^{-k}.
- Additive Form: das Symbol kr steht im Fall $k \in \mathbb{N}$ für die Summe $r + r + \ldots + r$ mit n gleichen Summanden r, im Fall $k = 0$ für das Ringelement 0 und im Fall $k < 0$ für das additiv Inverse $-s$ des Ringelements $-kr$.

Beispielsweise steht das Symbol $(-3r)^{-2}$ also für das Ringelement

$$(-(r + r + r) \cdot -(r + r + r))^{-1}.$$

Einfache für Zahlen bekannte Rechenregeln gelten in jedem Ring:

Feststellung 61: *In einem Ring $(R, +, \cdot)$ gelten:*

1. $\forall r \in R \quad r \cdot 0 = 0 \cdot r = 0.$
2. $\forall r \in R \quad -r = (-1) \cdot r.$
3. $\forall r, s \in R \quad (-r) \cdot s = r \cdot (-s) = -(r \cdot s).$
4. $\forall r, s \in R \quad (-r) \cdot (-s) = r \cdot s.$
5. *Gilt für die Ringelemente $r, s \in R$ die Vertauschbarkeit $a \cdot b = b \cdot a$, so gilt die binomische Formel*

$$\forall n \in \mathbb{N} \quad (a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

BEWEIS: 1. Nach dem zweiten Distributivgesetz und weil 0 neutral in $(R,+)$ ist, gilt

$$0 \cdot r + 0 \cdot r = (0+0) \cdot r = 0 \cdot r,$$

also durch Addieren des Inversen $-(r \cdot 0)$ auf beiden Seiten $r \cdot 0 = 0$.

2. Anwendung des zweiten Distributivgesetzes und des Punkts 1 liefert

$$r + (-1) \cdot r = 1 \cdot r + (-1) \cdot r = (1 + (-1)) \cdot r = 0 \cdot r = 0.$$

Dies beweist die Behauptung, da $(R,+)$ abelsch ist.

3. Genauso wie bei Punkt 2 sieht man

$$r \cdot s + (-r) \cdot s = (r + (-r)) \cdot s = 0 \cdot s = 0,$$

was die Gleichung $(-r) \cdot s = -(r \cdot s)$ beweist. Die verbliebene Behauptung beweist man analog, wobei man anstelle des zweiten das erste Distributivgesetz verwendet.

4. Die zweimalige Anwendung des Punkts 3 liefert

$$(-r) \cdot (-s) = -((-r) \cdot s) = -(-(r \cdot s)) = r \cdot s.$$

5. Die Behauptung wird durch Induktion nach n bewiesen.

Induktionsanfang bei $n = 1$: Es ist nichts zu beweisen, da nach Definition der Binomialkoeffizienten $\binom{1}{0} = \binom{1}{1} = 1$ gilt.

Induktionsschritt:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b) \cdot (a+b)^n \\
&= (a+b) \cdot (\sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k}) \text{ (Induktionsannahme)} \\
&= a \cdot (\sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k}) + b \cdot (\sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k}) \text{ (Distributivgesetz)} \\
&= (\sum_{k=0}^{n} \tbinom{n}{k} a^{k+1} b^{n-k}) + (\sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k+1}) \ (a \cdot b = b \cdot a) \\
&= \tbinom{n}{0} a^0 b^{n+1} + \sum_{k=1}^{n} (\tbinom{n}{k-1} + \tbinom{n}{k}) a^k b^{n-k+1} + \tbinom{n}{n} a^{n+1} b^0 \\
&= \tbinom{n+1}{0} a^0 b^{n+1} + \sum_{k=1}^{n} \tbinom{n+1}{k} a^k b^{n-k+1} + \tbinom{n+1}{n+1} a^{n+1} b^0,
\end{aligned}$$

wobei in der vorletzten Zeile die Identität

$$\begin{array}{rcl}\binom{n}{k-1}+\binom{n}{k} & = & \frac{n!}{(n-k+1)!(k-1)!}+\frac{n!}{(n-k)!k!} \\ & = & \frac{n!k}{(n-k+1)!k!}+\frac{n!(n-k+1)}{(n-k+1)!k!} \\ & = & \frac{n!k+n!(n-k+1)}{(n-k+1)!k!} \\ & = & \frac{n!(n+1)}{(n-k+1)!k!} \\ & = & \binom{n+1}{k}\end{array}$$

genutzt wurde. □

Das Beispiel des Matrixrings $(\mathbb{K}^{n\times n},+,\cdot)$ macht klar, dass man Ringelemente nach ihren Eigenschaften in Klassen einteilen kann. Eine Klasse von Elementen eines Rings $(R,+,\cdot)$ kennen wir bereits, nämlich die invertierbaren Elemente $R^\times$ des Monoids $(R,\cdot)$. Wir wissen, dass diese nach Feststellung 17 eine Gruppe bilden.

Das Beispiel der Matrizen legt zwei weitere Elementklassen nahe:

Definition 62: *Es sei $(R,+,\cdot)$ ein Ring.*

- *Die Elemente $r\in R^\times$ werden als Einheiten von R bezeichnet.*
- *Das Element $r\in R$ heißt Nullteiler (von R), falls $r\neq 0$ gilt und Elemente $s,t\in R\setminus\{0\}$ mit der Eigenschaft $r\cdot s=0$ und $t\cdot r=0$ existieren.*
- *Das Element $r\in R$ heißt nilpotent, falls $r^e=0$ für ein $e\in\mathbb{N}$ gilt.*

Welche Elementklassen in einem Ring auftreten und welchen Umfang sie haben, hängt sehr stark vom Ring selbst ab. Beispielsweise besitzt der Ring $\mathbb{Z}$ keine Nullteiler und nur 0 als nilpotentes Element. Weiter sind nur die Elemente $-1,1$ invertierbar. Fast alle Elemente von $\mathbb{Z}$ gehören also keiner der genannten Klassen an. Wir wollen zwei weitere Beispielklassen diskutieren:

Beispiel 63 (Quadratische Zahlringe): Es sei $n\in\mathbb{Z}$ eine ganze Zahl, die keine Quadratzahl ist. Dann definiert man

$$\mathbb{Z}[\sqrt{n}]:=\{z+w\sqrt{n}:z,w\in\mathbb{Z}\}\subset\mathbb{C}.$$

Eine einfache Rechnung zeigt, dass $\mathbb{Z}[\sqrt{n}]$ zusammen mit der Addition und Multiplikation komplexer Zahlen zu einem kommutativen Ring wird. Dieser

Ring besitzt keine Nullteiler und außer 0 keine nilpotenten Elemente, da es solche in $\mathbb{C}$ nicht gibt.

Die Einheiten lassen sich nicht in einfacher Weise für alle n angeben. Tatsächlich macht hierüber der Dirichlet'sche Einheitensatz der Zahlentheorie eine Aussage, der nicht einfach zu beweisen ist. Immerhin lässt sich mit Hilfe der Betragsfunktion

$$|a + bi| = \sqrt{a^2 + b^2}$$

Folgendes über die Einheiten sagen: Ist $u \in \mathbb{Z}[\sqrt{n}]^\times$, so gibt es ein $v \in \mathbb{Z}[\sqrt{n}]$ mit der Eigenschaft $uv = 1$. Da die Betragsfunktion multiplikativ ist, folgt $1 = |uv| = |u||v|$. Ist nun $n < 0$ und $u = z + w\sqrt{n}$, so gilt $u = z + |n|wi$ und daher

$$|u|^2 = z^2 + |n|w^2 \in \mathbb{N}_0.$$

Die Gleichung $1 = |u||v|$ liefert also $|u| = 1$, was im Fall $|n| > 1$ nur für $z \in \{-1, 1\}$ und $w = 0$ möglich ist. Im verbleibenden Fall ist $n = -1$ und dann auch $w \in \{-1, 1\}$ und $z = 0$ eine Option. Wir haben gezeigt:

- $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$,
- $\mathbb{Z}[\sqrt{n}]^\times = \{-1, 1\}$ im Fall $n < -1$.

Die Ringe $\mathbb{Z}[\sqrt{n}]$ werden als quadratische Zahlringe bezeichnet, der Ring $\mathbb{Z}[i]$ speziell als Ring der ganzen gaußschen Zahlen.

Rechnen mit Restklassen modulo n

Es sei $n \in \mathbb{N}$ eine natürliche Zahl mit $n \geq 2$. Das Rechnen mit Restklassen beruht auf der folgenden einfachen Tatsache:

Feststellung 64: *Jede ganze Zahl $z \in \mathbb{Z}$ kann in der Form*

$$z = qn + r, \quad q \in \mathbb{Z},\ r \in \{0, \ldots, n-1\} \tag{17}$$

geschrieben werden, wobei q und r durch z und n eindeutig bestimmt sind.

Beweis: Es genügt die Existenz von q und r für $z \geq 0$ zu beweisen: Ist nämlich $z < 0$ und gilt für $-z > 0$ die Gleichung $-z = qn + r$, so folgt

$$z = -qn - r = -qn - n + (n - r) = -(q + 1)n + s,$$

wobei $s \in \{0, \ldots, n-1\}$ gilt.

Den Fall $z \geq 0$ beweist man durch Induktion nach z, wobei der Induktionsanfang bei $z = 0$ trivial ist: $0 = 0n + 0$.

Induktionsschritt: Für $z + 1 \in \mathbb{N}$ gilt nach Induktionsannahme

$$z + 1 = (qn + r) + 1.$$

Ist $r < n - 1$, so ist $z = qn + (r + 1)$ die behauptete Darstellung von z. Sonst gilt $r + 1 = n$ und $z = (q + 1)n$ ist die behauptete Darstellung.

Zur Eindeutigkeit: Aus der Gleichung $qn + r = q'n + r'$ folgt $(q - q')n = r' - r$, womit $r' - r$ durch n teilbar ist. Ohne Einschränkung kann man andererseits $r' - r \geq 0$ annehmen. Dann ist $r' - r \in \{0, \ldots, n - 1\}$, womit $r' - r = 0$ gelten muss. Hieraus folgt dann auch $q = q'$. □

Mit Hilfe der Feststellung 64 kann man auf der Menge $\{0, \ldots, n - 1\}$ der möglichen Reste bei Division durch n zwei innere Verknüpfungen definieren, die diese Menge zu einem Ring machen. Dies soll nun geschehen, allerdings werden die Reste im Folgenden mit den Symbolen $\overline{0}, \overline{1}, \ldots, \overline{n - 1}$ bezeichnet, um mit den Standardbezeichnungen in der gängigen Literatur im Einklang zu bleiben. Dort wird das Rechnen modulo n in einer begrifflich etwas schwierigeren Weise eingeführt, die diese Bezeichnung erforderlich macht.

Satz 65: *Es sei $n \in \mathbb{N}$, $n \geq 2$. Die Menge*

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \ldots, \overline{n - 1}\}$$

bildet zusammen mit den beiden inneren Verknüpfungen

$$\overline{a} + \overline{b} := \overline{r}, \text{ wobei } a + b = qn + r,$$

und

$$\overline{a} \cdot \overline{b} := \overline{r}, \text{ wobei } ab = qn + r,$$

einen kommutativen Ring.

Beweis: Beide Verknüpfungen sind wohldefiniert, da die Zahl r, die auf der rechten Seite der Definition erscheint, nach Definition in der Menge $\{0, \ldots, n - 1\}$ liegt und nach Feststellung 64 durch n und $a + b$ bzw. ab eindeutig bestimmt ist.

Es ist weiter zu zeigen, das $(\mathbb{Z}/n, +)$ eine abelsche Gruppe ist.

Assoziativgesetz: Es seien $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n$. Das Element $(\overline{a} + \overline{b}) + \overline{c}$ berechnet sich dann nach Definition wie folgt:

- $\overline{a} + \overline{b} = \overline{r}$, wobei $a + b = qn + r$.
- $(\overline{a} + \overline{b}) + \overline{c} = \overline{r} + \overline{c} = \overline{s}$, wobei $r + c = q'n + s$.

Durch Einsetzen folgt:

$$a + b + c = qn + r + q'n + s - r = (q + q')n + s,$$

das heißt s ist der eindeutig bestimmte Rest von $a+b+c$ bei Division durch n.

Das Element $\overline{a} + (\overline{b} + \overline{c})$ berechnet sich andererseits nach Definition wie folgt:

- $\overline{b} + \overline{c} = \overline{u}$, wobei $b + c = \hat{q}n + u$.
- $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{u} = \overline{v}$, wobei $a + u = \hat{q}'n + v$.

Durch Einsetzen folgt:

$$a + b + c = \hat{q}'n + v - u + \hat{q}n + u - r = (\hat{q}' + \hat{q})n + v,$$

das heißt v ist der eindeutig bestimmte Rest von $a+b+c$ bei Division durch n.

Insgesamt folgt $s = v$, womit das Assoziativgesetz bewiesen ist.

Neutrales Element: $\overline{0}$ ist ein neutrales Element für die Verknüpfung $+$, denn aus $a = 0 \cdot n + a$ für jedes $a \in \{0, \ldots, n-1\}$ folgt $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$.

Inverse Elemente: Für jedes $a \in \{0, \ldots, n-1\}$ gilt $n - a \in \{0, \ldots, n-1\}$ und $a + (n - a) = 1 \cdot n + 0$, woraus $\overline{a} + \overline{n-a} = \overline{n-a} + \overline{a} = \overline{0}$ folgt. Also ist $\overline{n-a}$ das Inverse zu $\overline{a}$.

Kommutativgesetz: ... folgt direkt aus der Definition zusammen mit der Kommutativität der Addition ganzer Zahlen.

Es ist nun zu zeigen, das $(\mathbb{Z}/n, \cdot)$ ein kommutatives Monoid ist.

Assoziativgesetz: Es seien $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n$. Das Element $(\overline{a} \cdot \overline{b}) \cdot \overline{c}$ berechnet sich dann nach Definition wie folgt:

- $\overline{a} \cdot \overline{b} = \overline{r}$, wobei $ab = qn + r$.
- $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{r} \cdot \overline{c} = \overline{s}$, wobei $rc = q'n + s$.

Durch Einsetzen folgt:

$$abc = (qn + r)c = qcn + rc = qcn + q'n + s = (qc + q')n + s,$$

das heißt s ist der eindeutig bestimmte Rest von abc bei Division durch n.

Das Element $\overline{a} \cdot (\overline{b} \cdot \overline{c})$ berechnet sich andererseits nach Definition wie folgt:

- $\overline{b} \cdot \overline{c} = \overline{u}$, wobei $bc = \hat{q}n + u$.
- $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{u} = \overline{v}$, wobei $au = \hat{q}'n + v$.

Durch Einsetzen folgt:

$$abc = a(\hat{q}'n + u) = a\hat{q}'n + au = a\hat{q}'n + \hat{q}'n + v = (a\hat{q}' + \hat{q}')n + v,$$

das heißt v ist der eindeutig bestimmte Rest von abc bei Division durch n.

Insgesamt folgt $s = v$, womit das Assoziativgesetz bewiesen ist.

Neutrales Element: $\overline{1}$ ist ein neutrales Element für die Verknüpfung $\cdot$, denn aus $a = 0 \cdot n + a$ für jedes $a \in \{0, \ldots, n-1\}$ folgt $\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$.

Kommutativgesetz: ... folgt direkt aus der Definition zusammen mit der Kommutativität der Multiplikation ganzer Zahlen.

Schließlich sind die Distributivgesetze zu zeigen. Wegen der Kommutativität der Multiplikation $\cdot$ genügt es eines der beiden zu beweisen: Es seien $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n$. Das Element $(\overline{a} + \overline{b}) \cdot \overline{c}$ berechnet sich dann nach Definition wie folgt:

- $\overline{a} + \overline{b} = \overline{r}$, wobei $a + b = qn + r$.
- $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{r} \cdot \overline{c} = \overline{s}$, wobei $rc = q'n + s$.

Durch Einsetzen folgt:

$$(a + b)c = (qn + r)c = qcn + rc = qcn + q'n + s = (qc + q')n + s,$$

das heißt s ist der eindeutig bestimmte Rest von $(a + b)c$ bei Division durch n.

Das Element $\overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$ berechnet sich andererseits nach Definition wie folgt:

- $\overline{a} \cdot \overline{c} = \overline{u_a}$, wobei $ac = q_a n + u_a$.
- $\overline{b} \cdot \overline{c} = \overline{u_b}$, wobei $bc = q_b n + u_b$.

- $\overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c} = \overline{u_a} + \overline{u_b} = \overline{v}$, wobei $u_a + u_b = qn + v$.

Durch Einsetzen folgt:

$$ac + bc = q_a n + u_a + q_b n + u_b = (q_a + q_b)n + qn + v = (q_a + q_b + q)n + v,$$

das heißt v ist der eindeutig bestimmte Rest von $(a + b)c = ac + bc$ bei Division durch n.

Insgesamt folgt $s = v$, womit das Distributivgesetz bewiesen ist. □

Wir wollen als Nächstes die verschiedenen Ringelementtypen in $\mathbb{Z}/n$ untersuchen. Deren Vorkommen bei konkretem n hängt eng mit elementaren zahlentheoretischen Sachverhalten zusammen.

Im Folgenden bezeichne $\mathrm{ggT}\,(a, b)$ den größten gemeinsamen Teiler der Zahlen $a, b \in \mathbb{Z}$. Für diesen gilt das grundlegende

LEMMA 66 (Etienne Bezout, 1730 – 1783):

$$\forall a, b \in \mathbb{Z} \setminus \{0\}\ \exists u, v \in \mathbb{Z} \quad ua + vb = \mathrm{ggT}\,(a, b).$$

BEWEIS: Man betrachtet die Menge

$$I := \{sa + tb : s, t \in \mathbb{Z}\}.$$

Sie besitzt die beiden Eigenschaften

$$z, w \in I \Rightarrow z + w \in I, \tag{18}$$

und

$$z \in \mathbb{Z}, w \in I \Rightarrow zw \in I, \tag{19}$$

wie man direkt nachrechnet.

In I gibt es eine natürliche Zahl, nämlich je nach Vorzeichen von a entweder a selbst oder $-a$. Folglich gibt es auch eine kleinste natürliche Zahl $m \in I$. Wegen Eigenschaft (23) ist dann $\mathbb{Z}m \subseteq I$. Ist andererseits $c \in I$, so gilt $c = qm + r$ mit $r \in \{0, \ldots, m - 1\}$. Wegen der Eigenschaften (22) und (23) folgt $r \in I$ und damit $r = 0$, da $r < m$. Man hat also bewiesen:

$$I = \{zm : z \in \mathbb{Z}\}$$

und damit auch $ua + vb = m$ für gewisse $u, v \in \mathbb{Z}$.

Sei nun $d \in \mathbb{Z}$ ein gemeinsamer Teiler von a und b. Dann folgt aus der letzten Gleichung, dass d auch m teilt. Folglich teilt $\mathrm{ggT}\,(a, b)$ die Zahl m. Andererseits gilt $a, b \in I$, womit $a = q_a m$ und $b = q_b m$, m ist also ein Teiler von a und b. Insgesamt folgt $m = \mathrm{ggT}\,(a, b)$ und damit die Behauptung. □

SATZ 67: *Es sei $n \in \mathbb{N}$, $n \geq 2$.*

1. $(\mathbb{Z}/n)^\times = \{\overline{a} : \mathrm{ggT}\,(a,n) = 1\}$,
2. $\mathrm{Nullteiler}(\mathbb{Z}/n) = \{\overline{a} : \mathrm{ggT}\,(a,n) \neq 1\}$,
3. $\mathrm{Nilpotente}(\mathbb{Z}/n) = \{\overline{a} : a$ *und* n *besitzen dieselben Primteiler*$\}$.

BEWEIS: Es sei $a \in \{1, \ldots, n-1\}$ und $d \in \mathbb{N}$, $d \neq 1$, ein gemeinsamer Teiler von a und n. Dann gilt $a = db$ und $n = dm$, woraus $am = nb + 0$ folgt. Nach Definition gilt also $\overline{a} \cdot \overline{m} = \overline{0}$ und $\overline{a}$ ist ein Nullteiler.

Gilt andererseits $\overline{a} \cdot \overline{b} = \overline{0}$ für ein $b \in \{1, \ldots, n-1\}$, so folgt $ab = qn$. Wegen $b < n$ kann nicht jeder Teiler von n ein Teiler von b sein, folglich besitzen a und n einen gemeinsamen Teiler. Insgesamt ist Punkt 2 des Satzes damit bewiesen.

Da eine Einheit $\overline{a}$ von $\mathbb{Z}/n$ kein Nullteiler ist (allgemeiner Beweis folgt in der nächsten Feststellung), muss für eine solche $\mathrm{ggT}\,(a,n) = 1$ sein. Gilt andererseits $\mathrm{ggT}\,(a,n) = 1$, so folgt nach dem Lemma von Bezout

$$ua + vn = 1$$

also $ua = -vn + 1$ und damit nach Definition $\overline{u} \cdot \overline{a} = \overline{1}$, womit $\overline{a}$ eine Einheit ist. Punkt 1 ist damit gezeigt.

Es gelte schließlich $a^e = 0$ für ein $e \in \mathbb{N}$, also $a^e = qn$. Dann ist jede Primzahl, die n teilt, auch ein Teiler von a. Besitzen andererseits a und n dieselben Primteiler $p_1, \ldots, p_r$, so gilt $n = p_1^{v_1} \cdot \ldots \cdot p_r^{v_r}$ und $a = p_1^{u_1} \cdot \ldots \cdot p_r^{u_r}$. Also ist $a^{v_1 + \cdots + v_r}$ durch n teilbar und $\overline{a}$ damit nilpotent. □

Die »gegenseitige Lage« der verschiedenen Typen von Ringelementen wird durch das nächste Resultat geklärt. Mit diesem gewinnt man einen ersten Überblick über den allgemeinen Aufbau eines Rings.

FESTSTELLUNG 68: *In einem Ring $(R, +, \cdot)$ gelten die folgenden Aussagen:*

1. *Jedes nilpotente Element $r \neq 0$ ist ein Nullteiler; die Umkehrung dieser Implikation gilt im Allgemeinen nicht.*
2. *Eine Einheit ist kein Nullteiler.*
3. *Kürzungsregel: Gilt für ein $r \in R \setminus \{0\}$, das kein Nullteiler ist, die Gleichung $r \cdot a = r \cdot b$ oder $a \cdot r = b \cdot r$, so folgt $a = b$.*

BEWEIS: Ist $r \in R$ nilpotent, so gilt $r^e = 0$ für ein $e \in \mathbb{N}$, das man zusätzlich minimal wählen kann. Da $r \neq 0$ vorausgesetzt ist, gilt $e > 1$, also $r \cdot r^{e-1} = r^{e-1} \cdot r = 0$ mit $r^{e-1} \neq 0$ wegen der Minimalität von e. Diese Gleichungen zeigen, dass r ein Nullteiler ist.

Sei nun $r \in R^\times$ und $rs = 0$. Dann folgt $0 = r^{-1} \cdot 0 = r^{-1} \cdot r \cdot s = 1 \cdot s = s$, womit r kein Nullteiler sein kann.

Sei schließlich $r \in R \setminus \{0\}$ kein Nullteiler und gelte $r \cdot a = r \cdot b$. Unter Verwendung des Distributivgesetzes folgt hieraus $r \cdot (a-b) = 0$, also $a-b = 0$, da r kein Nullteiler ist. Die zweite Behauptung beweist man analog. □

LINEARE GLEICHUNGSSYSTEME IN RINGEN

In der Numerik treten häufig Situationen auf, in denen man Matrizen $X \in \mathbb{R}^{n \times n}$ sucht, die bestimmten Anforderungen genügen, die sich als lineare Gleichungen formulieren lassen, etwa:

$$AX + C = D,$$

wobei $A, B, C, D \in \mathbb{R}^{n \times n}$ bekannte Matrizen sind. Diese Gleichung lässt sich im Ring der Matrizen $(\mathbb{R}^{n \times n}, +, \cdot)$ leicht lösen, wenn A eine Einheit in diesem Ring ist, also eine invertierbare Matrix:

$$X = A^{-1}(D - C).$$

Ganz allgemein kann man versuchen lineare Gleichungssystem mit Koeffizienten in einem Ring $(R, +, \cdot)$ zu lösen. Sind $x_1, \ldots, x_m$ die zu bestimmenden Ringelemente, so können, da R nicht kommutativ sein muss, in einem linearen Gleichungssystem Terme der Form $r \cdot x_i$, $x_i \cdot s$ und $r \cdot x_i \cdot s$ mit Koeffizienten $r, s \in R$ auftreten. Das allgemeine lineare Gleichungssystem von m Gleichungen und n Unbekannten mit Koeffizienten in R sieht also so aus:

$$\begin{array}{rcl}
a_{11} \cdot x_1 + b_{11} \cdot x_1 \cdot c_{11} + x_1 \cdot d_{11} + \ldots + a_{1n} \cdot x_n + b_{1n} \cdot x_n \cdot c_{1n} + x_n \cdot d_{1n} & = & e_{11} \\
a_{21} \cdot x_1 + b_{21} \cdot x_1 \cdot c_{21} + x_1 \cdot d_{21} + \ldots + a_{2n} \cdot x_n + b_{2n} \cdot x_n \cdot c_{2n} + x_n \cdot d_{2n} & = & e_{21} \\
\vdots \quad \vdots \quad \vdots & & \\
a_{n1} \cdot x_1 + b_{n1} \cdot x_1 \cdot c_{n1} + x_1 \cdot d_{n1} + \ldots + a_{nn} \cdot x_n + b_{nn} \cdot x_n \cdot c_{nn} + x_n \cdot d_{nn} & = & e_{nn}
\end{array}$$

Wie in der linearen Algebra zeigt man, dass die folgenden Umformungen eines solchen Gleichungssystems seine Lösungsmenge nicht verändern:

1. Ersetzen einer Gleichung G, durch die von links mit einem Nichtnullteiler $r \in R$ multiplizierte Gleichung $r \cdot G$.

2. Ersetzen einer Gleichung G, durch die von rechts mit einem Nichtnullteiler $r \in R$ multiplizierte Gleichung $G \cdot r$.

3. Ersetzen einer Gleichung G durch die Summe $G + H$ zweier Gleichungen.

Natürlich können diese Umformungen kombiniert werden: Führt man etwa Umformungen vom Typ 1 und 2 nacheinander aus, so kann man eine Gleichung G durch eine Gleichung $r \cdot G \cdot s$ mit Nichtnullteilern $r, s \in R$ ersetzen.

Die Forderung, dass man nur mit Nichtnullteilern multiplizieren darf, geht auf die Kürzungsregel aus Feststellung 68 zurück, die man für den Nachweis benötigt, dass sich die Lösungsmenge nicht ändert.

Da in einem Ring im Allgemeinen nicht alle Elemente Einheiten sind, lässt sich der Gaußalgorithmus *nicht* auf beliebige Ringe übertragen: Die Tatsache, dass man nur mit Nichtnullteilern multiplizieren darf, und Gleichungen der Form

$$r \cdot x = s$$

im Allgemeinen nur lösen kann, wenn r eine Einheit ist, stellen gegebenenfalls starke Einschränkungen dar.

Anwendung in der Kryptographie: Affine Blockchiffren

Endliche Ringe werden in der Kryptographie genutzt, in der es unter anderem darum geht Informationen so zu verschlüsseln, dass Unbefugte diese Informationen nicht »lesen« können. Mit einem einfachen Beispiel soll hier erklärt werden, in welcher Form bei diesem Problem Ringe ins Spiel kommen.

Wir betrachten Texte wie zum Beispiel den Text eines eMails. Ein solcher Text besteht aus einzelnen Zeichen, die aus einem bestimmten Zeichenvorrat $\mathbf{A}$ stammen, dem sogenannten Alphabet. Ein Alphabet ist also eine endliche Menge von Zeichen wie etwa $A, B, C, D, \ldots, a, b, c, d, \ldots, ., !, ?, +, \ldots$. Ein Text ist mathematisch ausgedrückt eine Abbildung

$$T : \{1, 2, 3, \ldots, \ell\} \to \mathbf{A},$$

wobei $T(k)$ jeweils der k-te Buchstabe des Texts und $\ell \in \mathbb{N}$ seine Länge ist.

Eine einfache Art Texte zu verschlüsseln besteht in der Festlegung einer bijektiven Abbildung

$$\sigma : \mathbf{A} \to \mathbf{A},$$

also mit den Begriffen des Abschnitts 1.2 einer Permutation von $\mathbf{A}$.

Einen Text T kann man dann verschlüsseln, indem man zu dem Text $\sigma \circ T$ übergeht. Die Verschlüsselung sieht anschaulich so aus: An allen Stellen,

an denen im Text T der Buchstabe $b \in \mathbf{A}$ erscheint, wird er durch den Buchstaben $\sigma(b)$ ersetzt. Gilt nämlich zum Beispiel $T(k) = b$, das heißt ist der k-te Buchstabe von T der Buchstabe b, so gilt für den Text $\sigma \circ T$ nach Definition der Verkettung von Abbildungen $(\sigma \circ T)(k) = \sigma(T(k)) = \sigma(b)$.

Um diese Form der Verschlüsselung von zum Beispiel eMails zu nutzen, müssen sich die beiden Parteien, die verschlüsselte eMails austauschen wollen, auf eine Permutation σ einigen, die beiden bekannt sein muss. Um eine eMail T sicher zu verschicken, bestimmt man $S = \sigma \circ T$ und verschickt diesen Text, den jemand ohne Kenntnis von σ (zunächst) nicht lesen kann. Der Empfänger bestimmt dann den Text $\sigma^{-1} \circ S$, wobei σ^{-1} die Umkehrabbildung von σ ist. Es gilt also

$$\sigma^{-1} \circ S = \sigma^{-1} \circ \sigma \circ T = \mathrm{id}_{\mathbf{A}} \circ T = T,$$

das heißt der unverschlsselte Text liegt dem Empfänger vor.

Das direkte Verwenden von Permutationen zum Verschlüsseln ist aufwendig und unpraktisch. Besser wäre es die Verschlüsselung über Rechenoperationen bzw. eine Formel durchzuführen. Hierzu muss man allerdings mit den Buchstaben des Alphabets »rechnen« können, das heißt man benötigt mindestens eine innere Verknüpfung auf $\mathbf{A}$. Tatsächlich geht man etwas anders vor: Besitzt das Alphabet $\mathbf{A}$ n verschiedene Zeichen, so kann man eine Bijektion

$$w : \mathbf{A} \to \mathbb{Z}/n$$

festlegen, indem man jedem Buchstaben b ein Element $\overline{k} \in \mathbb{Z}/n$ zuordnet. Eine solche Bijektion nennt man Alphabetwechsel; sie muss nicht geheim gehalten werden.

In $\mathbb{Z}/n$ liegen die früher definierte Addition und Multiplikation vor, mit deren Hilfe man eine Bijektion

$$\sigma : \mathbb{Z}/n \to \mathbb{Z}/n$$

zum Verschlüsseln von T festlegen kann. Zum Beispiel ist die Abbildung

$$\sigma(\overline{k}) = \overline{u} \cdot \overline{k} + \overline{c}$$

bijektiv, wenn man für $\overline{u}$ eine Einheit und für $\overline{c}$ ein beliebiges Element wählt. Es gilt nämlich

$$\sigma^{-1}(\overline{k}) = \overline{u}^{-1} \cdot (\overline{k} - \overline{c})$$

wie man direkt nachrechnet.

Den Text T verschlüsselt man nun zu $S := \sigma \circ w \circ T$. Kennt der Empfänger den Alphabetwechsel w sowie die Einheit $\overline{u}$ und die Konstante $\overline{c}$, so kann er S mittels der Formel

$$T = w^{-1} \circ \sigma^{-1} \circ S$$

wieder entschlüsseln.