**Prof. Dr. H. Brenner** **Osnabrück SS 2020**

# Diskrete Mathematik

## Vorlesung 12

Heute war es besonders anstrengend, Vorli muss noch mehr schlafen. Ein gesunder Schlaf ist für alle Beteiligten wichtig.

In dieser Vorlesung besprechen wir Restklassenbildung. Dies ist ein wichtiger Spezialfall der Bildung einer Quotientenmenge zu einer Äquivalenzrelation. Ein zusätzlicher Aspekt ist, dass man auf diesen Quotientenmengen Verknüpfungen hat, die sich von der Startmenge her vererben. Unmittelbare Anwendungen sind ein besseres Verständnis der Division mit Rest der ganzen Zahlen, insbesondere der algebraischen Struktur der Reste.

Um die folgenden Aussagen prägnanter formulieren zu können, brauchen wir eigene Begriffe für strukturerhaltende Abbildungen, das sind Abbildungen, die mit den gegebenen Verknüpfungen verträglich sind.

DEFINITION 12.1. Seien $(G, \circ, e_G)$ und $(H, \circ, e_H)$ Gruppen. Eine Abbildung

$$\psi\colon\ G \longrightarrow H$$

heißt *Gruppenhomomorphismus*, wenn die Gleichheit

$$\psi(g \circ g') \ = \ \psi(g) \circ \psi(g')$$

für alle $g, g' \in G$ gilt.

Beispielsweise ist eine lineare Abbildung insbesondere ein Gruppenhomomorphismus.

DEFINITION 12.2. Seien $R$ und $S$ Ringe. Eine Abbildung

$$\varphi\colon\ R \longrightarrow S$$

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a)+\varphi(b)$.
(2) $\varphi(1) = 1$.
(3) $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

## Restklassengruppen

Bei der folgenden Konstruktion denke man an die Gruppe $\mathbb{Z}$ zusammen mit der Untergruppe $\mathbb{Z}n$ aller Vielfachen zu einer fixierten Zahl $n$, also an die Situation $\mathbb{Z}n \subseteq \mathbb{Z}$, oder an die Situation eines Untervektorraumes $U \subseteq K^n$, siehe Aufgabe 10.15.

DEFINITION 12.3. Es sei $(G,0,+)$ eine kommutative Gruppe und $H \subseteq G$ eine Untergruppe. Für Elemente $x,y \in G$ setzen wir $x \sim_H y$ (und sagen, dass $x$ und $y$ äquivalent sind), wenn $x-y \in H$.

In dem eingangs erwähnten Beispiel sind zwei ganze Zahlen äquivalent, wenn ihre Differenz ein Vielfaches von $n$ ist. Diese Äquivalenzrelation wurde schon in Beispiel 10.14 betrachtet. Wir sichern zuerst, dass wirklich in voller Allgemeinheit eine Äquivalenzrelation vorliegt.

LEMMA 12.4. *Es sei $(G,0,+)$ eine kommutative Gruppe, $H \subseteq G$ eine Untergruppe und $\sim_H$ die durch $H$ auf $G$ definierte Relation. Dann liegt eine Äquivalenzrelation vor, und die Äquivalenzklasse zu $0$ ist gerade $H$.*

*Beweis.* Wegen

$$x-x = 0 \in H$$

ist die Relation reflexiv. Mit $x-y \in H$ ist auch $y-x \in H$, da Untergruppen unter dem Negativen abgeschlossen sind, was die Symmetrie der Relation bedeutet. Mit $x \sim_H y$ und $y \sim_H z$, also $x-y, y-z \in H$, ist auch

$$x-z = (x-y)+(y-z) \in H,$$

da Untergruppen unter der Addition abgeschlossen sind, und somit ist auch $x \sim_H z$. Damit ist die Relation auch transitiv. Die Äquivalenz von $x$ mit $0$ bedeutet $x-0 = x \in H$, so dass die letzte Aussage auch klar ist. □

Die Äquivalenzklassen heißen in dieser Situation auch die *Nebenklassen* der Relation. Sie haben die Gestalt

$$[x] = x+H = \{x+h \mid h \in H\},$$

sie bestehen also aus allen Elementen, die man von $x$ aus durch Addition mit einem Element aus $H$ erreichen kann. Man kann sich dabei $H$ als einen

mehr oder weniger restriktiven Vorrat an Sprungmöglichkeiten oder Bewegungsmöglichkeiten vorstellen, und die Äquivalenz zwischen $x$ und $y$ bedeutet, dass man von $x$ nach $y$ mit einem erlaubten Sprung gelangen kann.

SATZ 12.5. *Es sei $(G,0,+)$ eine kommutative Gruppe, $H \subseteq G$ eine Untergruppe und $G/H$ die Quotientenmenge zur durch $H$ definierten Äquivalenzrelation auf $G$ mit der kanonischen Projektion*

$$q\colon\ G \longrightarrow G/H,\ g \longmapsto [g].$$

*Dann gibt es eine eindeutig bestimmte Gruppenstruktur auf $G/H$ derart, dass $q$ ein Gruppenhomomorphismus ist.*

*Beweis.* Da die kanonische Projektion zu einem Gruppenhomomorphismus werden soll, muss die Verknüpfung durch

$$[x] + [y] \ = \ [x+y]$$

gegeben sein, was bereits die Eindeutigkeit sichert. Wir müssen also zeigen, dass durch diese Vorschrift eine wohldefinierte Verknüpfung auf $G/H$ definiert ist, die unabhängig von der Wahl der Repräsentanten ist. D.h. wir haben für $[x] = [x']$ und $[y] = [y']$ zu zeigen, dass $[x+y] = [x'+y']$ ist. Nach Voraussetzung können wir $x' = x + h$ und $y' = y + h'$ mit $h, h' \in H$ schreiben. Damit ist

$$x' + y' \ = \ (x+h) + (y+h') \ = \ x + y + (h + h')$$

und somit ist $[x+y] = [x'+y']$. Aus der Wohldefiniertheit der Verknüpfung auf $G/H$ und der Surjektivität der kanonischen Projektion folgen die Gruppeneigenschaften und die Homomorphieeigenschaft der Projektion. □

DEFINITION 12.6. Es sei $(G,0,+)$ eine kommutative Gruppe und $H \subseteq G$ eine Untergruppe. Die Quotientenmenge

$$G/H$$

mit der aufgrund von Satz 12.5 eindeutig bestimmten Gruppenstruktur heißt *Restklassengruppe von $G$ modulo $H$*. Die Elemente $[g] \in G/H$ heißen *Restklassen*. Für eine Restklasse $[g]$ heißt jedes Element $g' \in G$ mit $[g'] = [g]$ ein *Repräsentant* von $[g]$.

BEISPIEL 12.7. Die Untergruppen der ganzen Zahlen sind nach Satz 8.4 von der Form $\mathbb{Z}n$ mit $n \geq 0$. Die Restklassengruppen werden mit

$$\mathbb{Z}/(n)$$

bezeichnet (sprich „$\mathbb{Z}$ modulo $n$“). Bei $n = 0$ ist das einfach $\mathbb{Z}$ selbst, bei $n = 1$ ist das die triviale Gruppe. Im Allgemeinen ist die durch die Untergruppe $\mathbb{Z}n$ definierte Äquivalenzrelation auf $\mathbb{Z}$ dadurch gegeben, dass zwei ganze Zahlen $a$ und $b$ genau dann äquivalent sind, wenn ihre Differenz $a - b$ zu $\mathbb{Z}n$ gehört, also ein Vielfaches von $n$ ist. Daher ist (bei $n \geq 1$) jede ganze Zahl zu genau einer der $n$ Zahlen

$$0, 1, 2, \ldots, n-1$$

äquivalent (oder, wie man auch sagt, *kongruent modulo* $n$), nämlich zum Rest, der sich bei Division durch $n$ ergibt. Diese Reste bilden also ein Repräsentantensystem für die Restklassengruppe, und diese besitzt $n$ Elemente. Diese werden im Allgemeinen mit $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ bezeichnet. Dabei ist $\overline{0}$ das neutrale Element, das negative Element zu $\overline{k}$ ist $\overline{n-k}$ und die Summe $\overline{i}+\overline{k}$ ist $\overline{i+k}$ bzw. $\overline{i+k-n}$, falls $i+k \geq n$ ist. Die Tatsache, dass die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n),\, a \longmapsto [a] = a \mod n,$$

ein Homomorphismus ist, kann man auch so ausdrücken, dass der Rest einer Summe von zwei ganzen Zahlen nur von den beiden Resten, nicht aber von den Zahlen selbst, abhängt.

## Restklassenringe

Definition 12.8. Eine Teilmenge $\mathfrak{a}$ eines kommutativen Ringes $R$ heißt *Ideal*, wenn die folgenden Bedingungen erfüllt sind:

(1) $0 \in \mathfrak{a}$.
(2) Für alle $a, b \in \mathfrak{a}$ ist auch $a+b \in \mathfrak{a}$.
(3) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Eine Ideal ist insbesondere eine Untergruppe der kommutativen Gruppe $(R, +, 0)$. Somit ist die Restklassengruppe $R/\mathfrak{a}$ in kanonischer Weise eine kommutative Gruppe und die kanonische Abbildung

$$R \longrightarrow R/\mathfrak{a}$$

ist mit der Addition verträglich. Wir werden sehen, dass man in $R/\mathfrak{a}$ zusätzlich eine Multiplikation und ein Einselement definieren kann derart, dass $R/\mathfrak{a}$ zu einem kommutativen Ring wird und dass die kanonische Abbildung auch die Multiplikation respektiert, also ein Ringhomomorphismus ist. Bei $R = \mathbb{Z}$ ist jede Untergruppe bereits ein Ideal.

Die Nebenklassen $a+\mathfrak{a}$ sind gerade die Nebenklassen zur Untergruppe $\mathfrak{a} \subseteq R$. Zwei Elemente $a, b \in R$ definieren genau dann die gleiche Nebenklasse, also $a+\mathfrak{a} = b+\mathfrak{a}$, wenn ihre Differenz $a-b$ zum Ideal gehört.

Lemma 12.9. *Es sei $R$ ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $R/\mathfrak{a}$ die Quotientenmenge zur durch $\mathfrak{a}$ definierten Äquivalenzrelation auf $R$ mit der kanonischen Projektion*

$$q\colon\ R \longrightarrow R/\mathfrak{a},\, g \longmapsto [g].$$

*Dann gibt es eine eindeutig bestimmte Ringstruktur auf $R/\mathfrak{a}$ derart, dass $q$ ein Ringhomomorphismus ist.*

*Beweis.* Nach Satz 12.5 gibt es nur eine Gruppenstruktur auf $R/\mathfrak{a}$ derart, dass die kanonische Abbildung ein Gruppenhomomorphismus ist. Da ein Ringhomomorphismus insbesondere ein Gruppenhomomorphismus bezüglich der Addition ist, ist dies die einzige additive Struktur, die in Frage kommt.

Da die kanonische Abbildung die Multiplikation respektieren soll, kommt nur $\overline{1}$ als neutrales Element der Multiplikation und

$$\overline{a}\,\overline{b} \;=\; \overline{ab}$$

als Multiplikation in Frage. Wir müssen zeigen, dass diese Multiplikation wohldefiniert ist. Seien zwei Restklassen mit unterschiedlichen Repräsentanten gegeben, also $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$. Dann ist $a - a' \in \mathfrak{a}$ und $b - b' \in \mathfrak{a}$ bzw. $a' = a + x$ und $b' = b + y$ mit $x, y \in \mathfrak{a}$. Daraus ergibt sich

$$a'b' \;=\; (a+x)(b+y) \;=\; ab + ay + xb + xy.$$

Die drei hinteren Summanden gehören zum Ideal, so dass die Differenz $a'b' - ab \in \mathfrak{a}$ ist.

Aus der Wohldefiniertheit folgen die anderen Eigenschaften und insbesondere, dass ein Ringhomomorphismus in den Restklassenring vorliegt. □

Die kanonische Projektion nennt man wieder die *Restklassenabbildung* oder den *Restklassenhomomorphismus*. Das Bild von $a \in R$ in $R/\mathfrak{a}$ wird mit $[a]$, häufig aber auch mit $\overline{a}$ oder einfach mit $a$ selbst bezeichnet und heißt die *Restklasse* von $a$. Bei dieser Abbildung gehen genau die Elemente aus dem Ideal auf 0, d.h. der Kern dieser Restklassenabbildung ist das vorgegebene Ideal.

## Die Restklassenringe von $\mathbb{Z}$

Für uns sind die Restklassenringe zum Ring $\mathbb{Z}$ und zu den Idealen $\mathbb{Z}n$ die wichtigsten Beispiele. Die praktische Bedeutung von Satz 12.9 liegt darin, dass man mit Resten nahezu gedankenlos rechnen darf, wenn man sich für das Restergebnis interessiert. Es ist egal, wann und wie oft man Zahlen durch ihre Reste oder durch andere Zahlen mit dem gleichen Rest ersetzt. In Aufgabe 6.11 und Aufgabe 6.12 hatten wir dies teilweise schon direkt nachgewiesen.

Durch die Konstruktion erhalten wir für jede natürliche Zahl $n \in \mathbb{N}_+$ einen kommutativen Ring mit $n$ Elementen. Der folgende Satz charakterisiert, wann es sich um Körper handelt.

Satz 12.10. *Sei $n \in \mathbb{N}$. Der Restklassenring $\mathbb{Z}/(n)$ ist genau dann ein Körper, wenn $n$ eine Primzahl ist.*

*Beweis.* Bei $n = 0$ ist der Restklassenring gleich $\mathbb{Z}$ selbst und kein Körper. Bei $n = 1$ besteht der Restklassenring aus nur einem Element und es ist $\overline{0} = \overline{1}$. Dies ist bei einem Körper explizit ausgeschlossen, und 1 ist keine

Primzahl. Sei also von nun an $n \geq 2$. Wenn $n$ keine Primzahl ist, so gibt es eine Darstellung

$$n = rs$$

mit kleineren Zahlen

$$1 < r, s < n.$$

Im Restklassenring $\mathbb{Z}/(n)$ bedeutet dies, dass die Restklassen $\overline{r}$ und $\overline{s}$ nicht 0 sind, dass aber ihr Produkt

$$\overline{r}\,\overline{s} = \overline{rs} = \overline{n} = 0$$

ist. Das kann nach Lemma 5.14 in einem Körper nicht sein.

Sei nun $n$ eine Primzahl. Wir müssen zeigen, dass jede von 0 verschiedene Restklasse $\overline{r}$, $0 < r < n$, ein inverses Element besitzt. Da $n$ prim ist, sind $r$ und $n$ teilerfremd. Nach dem Lemma von Bezout gibt es ganze Zahlen $a, b$ mit

$$ar + bn = 1.$$

Dies führt im Restklassenring zur Identität

$$\begin{aligned} \overline{1} &= \overline{ar + bn} \\ &= \overline{a}\,\overline{r} + \overline{b}\,\overline{n} \\ &= \overline{a}\,\overline{r}\,, \end{aligned}$$

die besagt, dass $\overline{r}$ und $\overline{a}$ invers zueinander sind. □

Der Beweis zeigt auch, wie man zu einem Element $r$ zwischen 1 und der Primzahl $p$ das Inverse in $\mathbb{Z}/(p)$ findet. Man muss mit Hilfe des euklidischen Algorithmus in $\mathbb{Z}$ eine Darstellung der 1 finden. Aus

$$ar + bp = 1$$

lässt sich dann ablesen, dass die Restklasse von $a$ das inverse Element zu $r$ ist.

Beispiel 12.11. Der Restklassenkörper $\mathbb{Z}/(7) = \{0, 1, 2, 3, 4, 5, 6\}$ hat die folgenden Verknüpfungstabellen:

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

# Abbildungsverzeichnis