Vorlesung 3

Teilbarkeitslehre und Restklassenarithmetik

3.1 Gruppentheorie

Wie wir in Vorlesung 2 gesehen haben, hat die Menge $\mathbb{Z}$ mit der Addition gewisse Eigenschaften. Wir fassen nun bestimmte Eigenschaften zusammen und führen den fundamentalen Begriff einer *Gruppe* ein.

Definition 3.1.1. Ein Paar $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung

$$\begin{aligned} * : \ & G \times G \to G \\ & (a, b) \mapsto a * b \end{aligned}$$

heißt *Gruppe*, wenn folgendes gilt:

(G1) Für alle $a, b, c \in G$ gilt

$$(a * b) * c = a * (b * c) \qquad \text{(Assoziativität)}.$$

(G2) Es existiert ein neutrales Element $e \in G$, so dass für alle $a \in G$ gilt

$$e * a = a * e = a.$$

(G3) Für jedes $a \in G$ existiert ein inverses Element $a^{-1} \in G$, so dass

$$a^{-1} * a = a * a^{-1} = e$$

gilt.

Bemerkung: Beachte a^{-1} hat *nichts* mit einer negativen Potenz zu tun, dies ist eine reine Bezeichnung für ein Inverses von a.

In der obigen Definition bezeichnet $G \times G$ das *kartesische Produkt* von G mit sich selbst:

Definition 3.1.2. Seien A und B Mengen. Dann definieren wir das *kartesische Produkt* von A mit B durch

$$A \times B := \{(a, b) | a \in A, b \in B\}.$$

Das kartesische Produkt $A \times B$ ist also die Menge aller Tupel (a, b) mit $a \in A$ und $b \in B$.

Die Gruppe heißt *abelsch* bzw. *kommutativ*, falls gilt

$$a * b = b * a.$$

Anstatt $(G, *)$ schreiben wir kurz G, wenn klar ist, welche Gruppe und welche Verknüpfung gemeint ist.

Definition 3.1.3. $(H, *)$ heißt *Halbgruppe*, wenn die Verknüpfung $*$ assoziativ ist.

Eine Halbgruppe ist eine Verallgemeinerung einer Gruppe. Bei einer Halbgruppe fordern wir nicht die Existenz eines neutralen Elements oder die Existenz von Inversen. Eine Gruppe ist stets eine Halbgruppe, umgekehrt gilt das natürlich nicht.

Beispiele.

- Mit diesen Definitionen können wir sagen, dass $(\mathbb{Z}, +)$, d.h. die Menge der ganzen Zahlen mit der gewöhnlichen Addition $+$ als Verknüfung, eine kommutative Gruppe ist: Die Addition ist assoziativ (G1):

  $$(a + b) + c = a + (b + c).$$

  Es gibt ein neutrales Element (G2), nämlich 0, so dass

  $$a + 0 = a.$$

  Zu jedem $n \in \mathbb{Z}$ gibt es ein $n^{-1} \in \mathbb{Z}$ (G3) mit

  $$n^{-1} + n = n + n^{-1} = 0 \qquad (\text{nämlich } n^{-1} = -n).$$

  Überdies gilt

  $$a + b = b + a.$$

- Frage: Ist $(\mathbb{N}, +)$ ist eine Gruppe? Nein! Das neutrale Element ist ebenfalls die 0. Aber zum Beispiel hat das Element $2 \in \mathbb{N}$ kein Inverses: Es gibt kein $n \in \mathbb{N}$ mit

  $$2 + n = 0.$$

  $(\mathbb{N}, +)$ ist eine Halbgruppe.

- Frage: Ist $(\mathbb{Z}, \cdot)$ mit der gewöhnlichen Multiplikation eine Gruppe? Nein! Das neutrale Element bezüglich der Multiplikation ist 1. Aber beispielsweise hat $2 \in \mathbb{Z}$ kein multiplikatives Inverses. $(\mathbb{Z}, \cdot)$ ist eine Halbgruppe.

3.2 Teilbarkeitslehre

Es seien $m, n \in \mathbb{Z}$. Wir sagen m ist durch n teilbar, wenn es ein $k \in \mathbb{Z}$ gibt mit

$$m = k \cdot n.$$

Anders formuliert: n teilt m. Hierfür schreiben wir kurz

$$n|m.$$

Wir bemerken: $0 \in \mathbb{Z}$ ist durch jede Zahl $n \in \mathbb{Z}$ teilbar, denn es gilt

$$0 = 0 \cdot n \qquad \text{(wir wählen } k = 0\text{)}.$$

Welche Teilbarkeitsregeln kennen Sie?

- Jede Zahl $n \in \mathbb{Z}$ ist durch 1 teilbar. Es gilt

$$n = n \cdot 1.$$

- Eine Zahl $n \in \mathbb{Z}$ ist genau dann durch 2 teilbar, wenn sie gerade ist, d.h. ihre letzte Ziffer ist 0, 2, 4, 6 oder 8.
- 100 ist durch 4 teilbar. Somit ist auch jedes Vielfache von 100 durch 4 teilbar. Damit ist eine entsprechend große Zahl genau dann durch 4 teilbar, wenn ihre beiden letzten Ziffern als Zahl aufgefasst durch 4 teilbar ist.
- Eine Zahl ist genau dann durch 5 teilbar, wenn ihre letzte Ziffer 0 oder 5 ist.
- $8|1000 \Rightarrow 8|1000k, k \in \mathbb{Z}$. Somit ist eine entsprechend große Zahl genau dann durchh 8 teilbar, wenn ihre letzten 3 Ziffern als Zahl aufgefasst durch 8 teilbar ist.
- Für die Teilbarkeit durch 3 oder 9 gilt die *Quersummenregel*, siehe unten.
- Eine Zahl ist genau dann durch 6 teilbar, wenn sie durch 2 und 3 teilbar ist.
- Für die Teilbarkeit durch 7 gibt es keine bekannte Regel.

Definition 3.2.1. Es sei $n \in \mathbb{N}$ eine $(m+1)$-stellige Zahl, d.h. wir haben

$$n = \sum_{k=0}^{m} a_k \cdot 10^k \text{ mit } a_j \in \{0, 1, \ldots, 9\}, j = 0, \ldots, m.$$

Die *Quersumme* von n ist dann definiert durch

$$Q(n) = \sum_{k=0}^{m} a_k.$$

Die *alternierende Quersumme* von n ist definiert durch

$$Q^*(n) = \sum_{k=0}^{m} (-1)^k a_k.$$

Beispiel. Wir haben

$$2792 = 2 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0.$$

Es gilt

$$Q(2792) = 2 + 7 + 9 + 2 = 20,$$

und

$$Q^*(2792) = -2 + 7 - 9 + 2 = -2.$$

Satz 3.2.2 (Quersummenregel)**.** Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

Wir werden diese Quersummenregeln nun beweisen. Dazu bedarf es etwas Theorie und wir führen in die Restklassenarithmetik ein.

3.3 Restklassenarithmetik

Sei $n \in \mathbb{Z}$. Bei Division durch 3 gibt es drei mögliche Reste, nämlich 0,1 oder 2. Der Rest 3 entspricht dem Rest 0, usw. Wir bezeichnen die Teilmenge der ganzen Zahlen, die bei Division durch 3 den Rest 0 lassen, als Restklasse $[0]_3$. Entsprechend bezeichnen die Restklassen $[1]_3$ und $[2]_3$ die Teilmengen der ganzen Zahlen, die den Rest 1 bzw. 2 bei Division durch 3 lassen.

Wir haben also

$$[0]_3 = \{a \in \mathbb{Z} | a = 3k + 0, k \in \mathbb{Z}\},$$

dies entspricht genau der Menge aller ganzen Zahlen, die ein Vielfaches von 3 sind. Analog haben wir

$$[1]_3 = \{a \in \mathbb{Z} | a = 3k + 1, k \in \mathbb{Z}\},$$
$$[2]_3 = \{a \in \mathbb{Z} | a = 3k + 2, k \in \mathbb{Z}\}.$$

Wenn klar ist, welche Restklassen wir betrachten, so können wir den Index und die eckigen Klammern weglassen. Im folgenden lassen wir den Index weg, behalten aber die eckigen Klammern bei.

Sei $m \in \mathbb{Z}$. Die Restklasse von m sei mit $[m]$ bezeichnet. m gehört genau einer Restklasse bezüglich der Division durch 3 an, denn für m gilt genau eine der folgenden Darstellungen

(i) $m = 3k \Leftrightarrow m \in [0]$

(ii) $m = 3k + 1 \Leftrightarrow m \in [1]$

(iii) $m = 3k + 2 \Leftrightarrow m \in [2]$

Je nachdem in welcher Restklasse [0],[1] oder [2] m liegt, setzen wir $[m]$ entsprechend: (i) $[m] := [0]$ (ii) $[m] := [1]$ (iii) $[m] := [2]$.
So gilt z. B. $[15] = [0]$ oder $[100] = [1]$. Nun erklären wir, was wir unter der Summe von zwei Restklassen verstehen: Seien $m, n \in \mathbb{Z}$. Dann setzen wir

$$[m] + [n] := [m + n]. \tag{3.1}$$

Links definieren wir eine neue Addition unter Bezugnahme der gewöhliche Addition auf der rechten Seite.

Bemerkung. Die Menge aller Restklassen bei der Division durch 3 bezeichnen wir mit $\mathbb{Z}_3$, d.h.

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

Bemerkung. $\mathbb{Z}_3$ zusammen mit der in (3.1) erklären Addition ist eine kommutative Gruppe.

Das neutrale Element ist [0]. Zu jedem Element gibt es ein Inverses: Das Inverse zu [1] ist [2] und das Inverse zu [0] ist [0], wie wir der folgenden Additionstabelle entnehmen können:

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

Die Assoziativität und Kommutativität ergeben sich aus der gewöhnlichen Addition in $\mathbb{Z}$.

Analog definieren wir das Produkt von zwei Restklassen: Seien $m, n \in \mathbb{Z}$. Wir setzen

$$[m] \cdot [n] := [m \cdot n]. \tag{3.2}$$

Das neutrale Element bezüglich dieser neuen Multiplikation in $\mathbb{Z}_3$ ist [1]. Somit ist [1] zu sich selbst invers, ebenso ist [2] zu sich selbst invers. $(\mathbb{Z}_3, \cdot)$ ist jedoch keine Gruppe, denn die [0] hat kein multiplikatives Inverses.

Bemerkung. Das neutrale Element [0] der Addition kann kein multiplikatives Inverses haben. Gäbe es ein multiplikatives Inverses n, so erhielten wir

$$[0] \cdot n = [1].$$

Wir betrachten daher $\mathbb{Z}_3$ ohne das Element [0] und setzen

$$(\mathbb{Z}/3\mathbb{Z})^\times := \mathbb{Z}_3 \backslash \{0\}.$$

Dann ist $((\mathbb{Z}/3\mathbb{Z})^\times, \cdot)$ eine abelsche Gruppe.

Wir kombinieren nun die zwei Verknüpfungen der Addition und Multiplikation und führen den wichtigen Begriff eines *Ringes* ein.

Definition 3.3.1. Sei R eine Menge mit zwei Verknüpfungen

$$+ : R \times R \to R$$
$$\cdot : R \times R \to R.$$

$R = (R, +, \cdot)$ heißt *Ring*, wenn

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $(R, \cdot)$ ist eine Halbgruppe.

(R3) Es gelten die Distributivgesetze, d.h.

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

für alle $a, b, c \in R$.

Somit ist $(\mathbb{Z}_3, +, \cdot)$ ein Ring. Er heißt *Restklassenring* (*modulo* 3). Wir beweisen nun die Quersummenregel (Satz 3.2.2): Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Beweis. Es bezeichne $[a]$ die Restklasse von a bei Division durch 3. Es gilt

$$[10] = [1].$$

Damit ist jede Zehnerpotenz in der Restklasse [1], d.h.

$$[10^k] = [1] \text{ für alle } k \in \mathbb{N}. \tag{3.3}$$

Es sei

$$a = \sum_{k=0}^{N} a_k \cdot 10^k, a_k \in \{0, 1, \ldots, 9\}$$

eine $(N + 1)$-stellige natürliche Zahl, $N \in \mathbb{N}$. Wir haben zu zeigen, dass

$$a \text{ ist durch 3 teilbar} \Leftrightarrow Q(a) = \sum_{k=0}^{N} a_k \text{ ist durch 3 teilbar.}$$

Aus (3.1) folgt

$$\sum_{k=1}^{N} [a_k] = \left[\sum_{k=1}^{N} a_k \right] \text{ für } a_1, \ldots, a_N \in \mathbb{Z} \tag{3.4}$$

und aus (3.2) folgt

$$\sum_{k=1}^{N} [a_k \cdot b_k] = \sum_{k=1}^{N} [a_k] \cdot [b_k] \text{ für } a_1, \ldots, a_N \in \mathbb{Z}. \tag{3.5}$$

Wir haben dann

$$\begin{aligned} [a] = \left[\sum_{k=0}^{N} a_k \cdot 10^k \right] &\overset{(3.4)}{=} \sum_{k=0}^{N} [a_k \cdot 10^k] \overset{(3.5)}{=} \sum_{k=0}^{N} [a_k] \cdot [10^k] \\ &\overset{(3.3)}{=} \sum_{k=0}^{N} [a_k] \overset{(3.4)}{=} \left[\sum_{k=0}^{N} a_k \right] = [Q(a)] . \end{aligned}$$

Mithin liegen a und $Q(a)$ bezüglich der Division durch 3 stets in derselben Restklasse. Daraus folgt sofort die Behauptung. □

Bemerkung. Der Beweis für die Quersummenregel bei Division durch 9 läuft analog.
Es gilt ferner: Eine Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist. Beweis als Übungsaufgabe unter Ausnutzung, dass $[10]_{11} = [-1]_{11}$ gilt.

3.4 Modulo Notation

Wir führen noch eine übliche Notation in der Restklassenarithmetik ein. Für $m, n, p \in \mathbb{Z}$ schreiben wir

$$m \equiv n \pmod{p},$$

wenn m und n bei Division durch p in der gleichen Restklasse liegen bzw. den gleichen Rest lassen. Lies „m ist kongruent n modulo p“, so gilt z. B.

$$8 \equiv 1 \pmod{7}.$$

Beispiel. In der Aufgabe 2 vom Blatt 1 haben wir: Finden Sie $m, n \in \mathbb{Z}$ mit

$$\frac{m}{3} + \frac{n}{5} = \frac{1}{15}.$$

Mit der modulo Schreibweise bestimmen wir nun *alle* Lösungen. Wir haben

$$\frac{5m + 3n}{15} = \frac{1}{15}.$$

Das impliziert

$$3n = 1 - 5m \Rightarrow n = \frac{1 - 5m}{3}.$$

Es muss gelten

$$1 - 5m \equiv 0 \pmod{3} \Rightarrow 1 \equiv 5m \pmod{3}.$$

Es gilt

$$5 \equiv 2 \pmod{3}.$$

Also folgt

$$1 \equiv 2m \pmod{3}.$$

Damit folgt

$$m \equiv 2 \pmod{3}.$$

Wir können also schreiben

$$m = 3k + 2, k \in \mathbb{Z}.$$

Somit

$$n = \frac{1 - 5(3k + 2)}{3} = \frac{1 - 10 - 15k}{3} = \frac{-9 - 15k}{3} = -3 - 5k.$$

Ergo: Alle Lösungen sind gegeben durch

$$m = 3k + 2 \text{ und } n = -3 - 5k \text{ mit } k \in \mathbb{Z}.$$