

II. Gruppen, Ringe und Körper

Im vorigen Kapitel I wurden die wichtigsten Zahlenmengen bereits genannt:
die *natürlichen* Zahlen,

$$\mathbb{N} := \{1, 2, 3, \dots\}, \quad (\text{II.1})$$

die *ganzen* Zahlen,

$$\mathbb{Z} := \{0, +1, -1, +2, -2, \dots\}, \quad (\text{II.2})$$

die *rationalen* Zahlen,

$$\mathbb{Q} := \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}, \quad (\text{II.3})$$

sowie die *reellen* und die *komplexen* Zahlen,

$$\mathbb{R} \quad \text{und} \quad \mathbb{C}. \quad (\text{II.4})$$

Wir wenden uns zunächst $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ zu. Für $a, b \in \mathbb{N}$ ist auch $a+b \in \mathbb{N}$. Diese Tatsache bezeichnet man als *Abgeschlossenheit* oder *Stabilität* von $\mathbb{N}$ bezüglich Addition.

I.A. gilt $a-b \in \mathbb{N}$ jedoch nicht. Dafür geht man von $\mathbb{N}$ zu $\mathbb{Z}$ über; für $a, b \in \mathbb{Z}$ sind $a+b$ und $a-b \in \mathbb{Z}$. Insbesondere ist 0 das *neutrale Element* bezüglich Addition in $\mathbb{Z}$: $a+0=0+a=a$. Man sagt, dass $\mathbb{Z}$ bezüglich der Addition $+$ eine *Gruppe* bildet.

Weiterhin ist $\mathbb{Z}$ auch bezüglich Multiplikation abgeschlossen, d.h. für $a, b \in \mathbb{Z}$ ist auch $a \cdot b \in \mathbb{Z}$, und es gilt das Distributivgesetz, $a(b+c) = ab+bc$. Somit ist $\mathbb{Z}$ bezüglich der Addition $+$ und der Multiplikation $(\cdot)$ ein *Ring*.

Schließlich gelangt man von $\mathbb{Z}$ zu $\mathbb{Q}$ durch die Forderung, dass auch Abgeschlossenheit bezüglich Division gelten soll: Für $a, b \in \mathbb{Q}$ sind $a+b, a-b, a \cdot b \in \mathbb{Q}$ und $\frac{a}{b} \in \mathbb{Q}$, falls $b \neq 0$. Diese Eigenschaften von $\mathbb{Q}$ stehen auch exemplarisch für die allgemeine Definition eines *Körpers*.

II.1. Gruppen

Definition II.1. Eine Menge G heißt **Gruppe** $:\Leftrightarrow$

Auf G ist eine Verknüpfung $\circ : G \times G \rightarrow G$ definiert, die die folgenden Eigenschaften besitzt:

$$(G_1) \quad \forall a, b, c \in G : \quad (a \circ b) \circ c = a \circ (b \circ c), \quad (\text{II.5})$$

$$(G_2) \quad \exists e \in G \forall a \in G : \quad a \circ e = e \circ a = a, \quad (\text{II.6})$$

$$(G_3) \quad \forall a \in G \exists a^{-1} \in G : \quad a \circ a^{-1} = a^{-1} \circ a = e. \quad (\text{II.7})$$

Dabei bezeichnet man (G_1) als **Assoziativität**, e als das **neutrale Element** und a^{-1} als das **zu a inverse Element**. Die Anzahl $|G|$ der Elemente in G bezeichnet man als **Ordnung von G** .

Gilt außerdem noch

$$(G_4) \quad \forall a, b \in G: \quad a \circ b = b \circ a \quad (\text{Kommutativität}), \quad (\text{II.8})$$

so nennt man G **kommutativ** oder **abelsch**.

Bemerkungen und Beispiele.

- Häufig wird das Verknüpfungszeichen weg gelassen, und man schreibt

$$a \circ b =: ab. \quad (\text{II.9})$$

- Die Assoziativität erlaubt es uns, Klammern bei der Gruppenverknüpfung einfach wegzulassen oder bei Bedarf einzufügen,

$$(ab)c = a(bc) =: abc. \quad (\text{II.10})$$

- Das neutrale Element e einer Gruppe ist eindeutig. Ist nämlich e' irgendein (möglicherweise von e verschiedenes) Element von G , das die Eigenschaft (G_2) besitzt, so folgt $e' = e e' = e$.
- Sind G eine Gruppe, $a \in G$ und $b \in G$ ein (möglicherweise von a^{-1} verschiedenes) zu a inverses Element, also $ab = ba = e$, so folgt dass $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}$, und das zu a inverse Element, a^{-1} , ist eindeutig.
- Aus der Eindeutigkeit des inversen Elements folgen dann auch

$$(a^{-1})^{-1} = a \quad \text{und} \quad (ab)^{-1} = b^{-1}a^{-1}, \quad (\text{II.11})$$

letzteres wegen $ab b^{-1} a^{-1} = a e a^{-1} = a a^{-1} = e$.

- Für abelsche Gruppen G schreibt man die Verknüpfung “ $\circ$ ” häufig als Addition $+: G \times G \rightarrow G$, und die Eigenschaften (G_1) – (G_4) nehmen folgende Gestalt an:

$$(\tilde{G}_1) \quad \forall a, b, c \in G: \quad (a + b) + c = a + (b + c), \quad (\text{II.12})$$

$$(\tilde{G}_2) \quad \exists 0 \in G \forall a \in G: \quad a + 0 = 0 + a = a, \quad (\text{II.13})$$

$$(\tilde{G}_3) \quad \forall a \in G \exists -a \in G: \quad a + (-a) = (-a) + a = 0, \quad (\text{II.14})$$

$$(\tilde{G}_4) \quad \forall a, b \in G: \quad a + b = b + a. \quad (\text{II.15})$$

- Die Menge $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ der ganzen Zahlen ist bezüglich der Addition eine abelsche Gruppe mit 0 als neutralem Element und $k^{-1} = -k$ als zu $k \in \mathbb{Z}$ inverses Element.
- Die Menge $\mathbb{Q} \setminus \{0\}$ der rationalen Zahlen ohne Null ist bezüglich der Multiplikation eine abelsche Gruppe mit 1 als neutralem Element und $q^{-1} = 1/q$ als zu $q \in \mathbb{Q} \setminus \{0\}$ inverses Element.
- Die Menge $G := \mathbb{R} \setminus \{1\}$ bildet bezüglich $a \circ b := a + b - ab$ eine Gruppe.

II.1.1. Permutationen

Definition II.2. Zu vorgegebenem $n \in \mathbb{N}$ sei $\mathbb{Z}_1^n := \{1, 2, \dots, n\}$. Die Menge der **Permutationen** von n Elementen ist durch

$$\mathcal{S}_n := \{ \pi : \mathbb{Z}_1^n \rightarrow \mathbb{Z}_1^n \mid \pi \text{ ist bijektiv} \} \quad (\text{II.16})$$

gegeben. Das **Signum** $(-1)^\pi \in \{-1, 1\}$ von π ist definiert durch

$$(-1)^\pi := \frac{\prod_{1 \leq i < j \leq n} \pi(i) - \pi(j)}{\prod_{1 \leq i < j \leq n} i - j}. \quad (\text{II.17})$$

Die Permutationen schreibt man auch häufig als Schema

$$\pi \equiv \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}. \quad (\text{II.18})$$

Die Komposition von Bijektionen ist nach Satz I.4 (iii) stets selbst bijektiv. Somit bildet die Komposition zweier Permutationen eine Verknüpfung $\circ : \mathcal{S}_n \times \mathcal{S}_n \rightarrow \mathcal{S}_n$. Die Komposition von Abbildungen ist stets assoziativ, deshalb gilt auch (G_1) . Weiterhin agiert, wie in (G_2) gefordert,

$$\mathbb{1}_{\mathbb{Z}_1^n} \equiv \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in \mathcal{S}_n \quad (\text{II.19})$$

als neutrales Element bezüglich $\circ$. Schließlich ist mit $\pi \in \mathcal{S}_n$ auch die Umkehrabbildung $\pi^{-1} \in \mathcal{S}_n$ eine Permutation, und es gilt $\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = \mathbb{1}_{\mathbb{Z}_1^n}$, also (G_3) . Zusammenfassend stellen wir fest, dass die Permutationen $\mathcal{S}_n$ bezüglich der Komposition $\circ$ eine Gruppe bilden. Dabei ist die Ordnung gleich $|\mathcal{S}_n| = n!$.

Bemerkungen und Beispiele.

- Beachte, dass

$$\prod_{1 \leq i < j \leq n} F(i, j) = \prod_{i=1}^n \left(\prod_{j=i+1}^n F(i, j) \right). \quad (\text{II.20})$$

- Für $n = 2$ sind $|\mathcal{S}_2| = 2! = 2$ und

$$\mathcal{S}_2 = \left\{ \mathbb{1} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}, \quad (\text{II.21})$$

mit $(-1)^\mathbb{1} = +1$ und $(-1)^\sigma = -1$.

- Für $n = 3$ sind $|\mathcal{S}_3| = 3! = 6$ und

$$\mathcal{S}_3 = \left\{ \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \right. \quad (\text{II.22})$$

$$\left. \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \quad (\text{II.23})$$

mit $(-1)^{\pi_1} = (-1)^{\pi_2} = (-1)^{\pi_3} = +1$ und $(-1)^{\pi_4} = (-1)^{\pi_5} = (-1)^{\pi_6} = -1$.

- Für $n = 3$ sind $\pi_5(1) = 3, \pi_5(2) = 2, \pi_5(3) = 1$ und somit

$$\prod_{1 \leq i < j \leq n} (i - j) = (1 - 2) \cdot (1 - 3) \cdot (2 - 3) = (-1) \cdot (-2) \cdot (-1) = (-2) \quad (\text{II.24})$$

und

$$\begin{aligned} \prod_{1 \leq i < j \leq n} (\pi_5(i) - \pi_5(j)) &= (\pi_5(1) - \pi_5(2)) \cdot (\pi_5(1) - \pi_5(3)) \cdot (\pi_5(2) - \pi_5(3)) \\ &= (3 - 2) \cdot (3 - 1) \cdot (2 - 1) = 1 \cdot 2 \cdot 1 = 2. \end{aligned} \quad (\text{II.25})$$

Also ist in der Tat

$$(-1)^{\pi_5} := \frac{\prod_{1 \leq i < j \leq n} (\pi_5(i) - \pi_5(j))}{\prod_{1 \leq i < j \leq n} (i - j)} = \frac{2}{-2} = -1. \quad (\text{II.26})$$

- Für $n = 3$ sind $\pi_6(1) = 2, \pi_6(2) = 1, \pi_6(3) = 3$ sowie $\pi_2(1) = 3, \pi_2(2) = 1, \pi_2(3) = 2$. Also sind

$$[\pi_6 \circ \pi_2](1) = \pi_6[\pi_2(1)] = \pi_6[3] = 3, \quad (\text{II.27})$$

$$[\pi_6 \circ \pi_2](2) = \pi_6[\pi_2(2)] = \pi_6[1] = 2, \quad (\text{II.28})$$

$$[\pi_6 \circ \pi_2](3) = \pi_6[\pi_2(3)] = \pi_6[2] = 1, \quad (\text{II.29})$$

und dementsprechend ist

$$\pi_6 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ [\pi_6 \circ \pi_2](1) & [\pi_6 \circ \pi_2](2) & [\pi_6 \circ \pi_2](3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \pi_5. \quad (\text{II.30})$$

- Analog erhält man für $n = 3$

$$\pi_2 \circ \pi_6 = \pi_4 \neq \pi_5 = \pi_6 \circ \pi_2, \quad (\text{II.31})$$

was zeigt, dass die Gruppe $\mathcal{S}_3$ der Permutationen nicht kommutativ ist. Dies gilt in der Tat ganz allgemein für alle $\mathcal{S}_n$ mit $n \geq 3$. (Trivialerweise ist $\mathcal{S}_2$ kommutativ.)

- Das Signum von Permutationen ist multiplikativ, d.h. für $n \in \mathbb{N}$ und $\pi, \kappa \in \mathcal{S}_n$ gilt

$$(-1)^{\pi \circ \kappa} = (-1)^\pi \cdot (-1)^\kappa. \quad (\text{II.32})$$

Dies wird in Lemma II.12 bewiesen.

- Die Permutationen der Form

$$\sigma = \begin{pmatrix} 1 & \dots & i-1 & \mathbf{i} & i+1 & \dots & j-1 & \mathbf{j} & j+1 & \dots & n \\ 1 & \dots & i-1 & \mathbf{j} & i+1 & \dots & j-1 & \mathbf{i} & j+1 & \dots & n \end{pmatrix} \in \mathcal{S}_n, \quad (\text{II.33})$$

die nur zwei Elemente (hier: $i \leftrightarrow j$) gegeneinander austauschen, heißen **Transpositionen**. Gemäß Lemma II.11 gilt stets $(-1)^\sigma = -1$.

- Jede Permutation $\pi \in \mathcal{S}_n$ lässt sich als Komposition von Transpositionen schreiben, d. h. es gibt Transpositionen $\sigma_1, \dots, \sigma_m \in \mathcal{S}_n$, so dass

$$\pi = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_m. \quad (\text{II.34})$$

Gemäß (II.32) und (II.62) gilt also

$$(-1)^\pi = (-1)^{\sigma_1} \cdot (-1)^{\sigma_2} \dots (-1)^{\sigma_m} = (-1)^m, \quad (\text{II.35})$$

d.h. das Signum der Permutation π ist -1 hoch die Anzahl der Transpositionen, deren Komposition π ergibt.

Weitere Details zu Permutationen findet man in Abschnitt II.4.2.

II.2. Ringe

Definition II.3. Eine Menge R heißt **Ring** $:\Leftrightarrow$

Auf R sind zwei Verknüpfungen *Addition* $+: R \times R \rightarrow R$ und *Multiplikation* $(\cdot): R \times R \rightarrow R$ definiert, die die folgenden Eigenschaften besitzen:

$$(R_1) \quad R \text{ ist bezüglich der Addition } + \text{ eine abelsche Gruppe,} \quad (\text{II.36})$$

$$(R_2) \quad \forall a, b, c \in R: \quad (a \cdot b) \cdot c = a \cdot (b \cdot c), \quad (\text{II.37})$$

$$(R_3) \quad \forall a, b, c \in R: \quad a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a. \quad (\text{II.38})$$

Dabei bezeichnet man (R_3) als **Distributivität** und vereinbart, dass Multiplikation vor Addition ausgeführt wird (Punktrechnung vor Strichrechnung).

Bemerkungen und Beispiele.

- Die Menge $\mathbb{N} := \{1, 2, 3, \dots\}$ der natürlichen Zahlen ist kein Ring.
- Die Menge $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ der ganzen Zahlen bildet einen Ring.
- Die Menge $2\mathbb{Z} := \{\dots, -4, -2, 0, 2, 4, \dots\}$ der geraden Zahlen bildet einen Ring.
- Die Menge $2\mathbb{Z} + 1 := \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ der ungeraden Zahlen ist gegenüber Addition nicht abgeschlossen und deswegen auch kein Ring.
- $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Ringe.

II.2.1. Die Restklassenringe $\mathbb{Z}_p$ von $\mathbb{Z}$ modulo p

Für $p \in \mathbb{N}$ definieren wir die **Restklassen modulo p** durch

$$\forall k \in \mathbb{Z}: \quad [k]_p := k + p\mathbb{Z} = \{k + pn \mid n \in \mathbb{Z}\}. \quad (\text{II.39})$$

Wir beobachten, dass $[k]_p = [\ell]_p$ gleichwertig mit $(k - \ell) \in p\mathbb{Z} = \{pn \mid n \in \mathbb{Z}\}$ ist. Offensichtlich gibt es genau p solcher Restklassen modulo p . Ihre Menge bezeichnen wir mit

$$\mathbb{Z}_p := \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}, \quad (\text{II.40})$$

sie bilden eine paarweise disjunkte Zerlegung der ganzen Zahlen, $\mathbb{Z} = \bigcup_{K \in \mathbb{Z}_p} K$. Definieren wir Addition und Multiplikation auf $\mathbb{Z}_p$ durch

$$[k]_p + [\ell]_p := [k + \ell]_p \quad \text{und} \quad [k]_p \cdot [\ell]_p := [k \cdot \ell]_p, \quad (\text{II.41})$$

so bilden die Restklassen $\mathbb{Z}_p$ modulo p mit den Verknüpfungen in (II.41) einen Ring, den **Restklassenring modulo p** .

Um einzusehen, dass $\mathbb{Z}_p$ einen Ring bildet, braucht man natürlich nur die Ringaxiome nachzuprüfen, was eine reine Fleißaufgabe ist. Eine Subtilität liegt allerdings im Beweis der *Wohldefiniertheit* der Verknüpfungen in (II.41): Damit (II.41) überhaupt Verknüpfungen $+: \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ und $(\cdot): \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ definiert, ist zu zeigen, dass die Gleichungen in (II.41) unabhängig von den gewählten Repräsentanten $k, \ell \in \mathbb{Z}$ sind. Seien dazu $k, k', \ell, \ell' \in \mathbb{Z}$ und $[k]_p = [k']_p$ sowie $[\ell]_p = [\ell']_p$, es gibt also $m, n \in \mathbb{Z}$, sodass

$$k' = k + mp \quad \text{und} \quad \ell' = \ell + np. \quad (\text{II.42})$$

Dann sind aber auch

$$[k + \ell]_p = [k' + \ell']_p \quad \text{und} \quad [k \cdot \ell]_p = [k' \cdot \ell']_p, \quad (\text{II.43})$$

denn

$$k' + \ell' = (k + \ell) + (m + n)p \quad \text{und} \quad k' \cdot \ell' = k \cdot \ell + (kn + \ell m + mn)p, \quad (\text{II.44})$$

also sind die Verknüpfungen in (II.41) unabhängig von den gewählten Repräsentanten.

Eine Anwendung der Restklassenringe ist die Regel, dass eine Zahl $n \in \mathbb{N}$ genau dann durch 9 teilbar ist, wenn ihre Quersumme durch 9 teilbar ist, denn es gilt

$$\begin{aligned} & [a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \dots + a_m \cdot 10^m]_9 \\ &= [a_0]_9 + [a_1]_9 \cdot [10]_9 + \dots + [a_m]_9 \cdot [10]_9^m \\ &= [a_0]_9 + [a_1]_9 + [a_2]_9 + \dots + [a_m]_9 \\ &= [a_0 + a_1 + a_2 + \dots + a_m]_9. \end{aligned} \quad (\text{II.45})$$

II.3. Körper

Definition II.4. Ein Ring $\mathbb{F}$ heißt **Körper**¹ $\Leftrightarrow$

$\mathbb{F}$ besitzt zu (R_1) – (R_3) zusätzlich die folgenden Eigenschaften:

$$(K_1) \quad \forall a, b \in \mathbb{F} : \quad a \cdot b = b \cdot a, \quad (\text{II.46})$$

$$(K_2) \quad \exists 1 \in \mathbb{F} \setminus \{0\} \quad \forall a \in \mathbb{F} : \quad 1 \cdot a = a \cdot 1 = a, \quad (\text{II.47})$$

$$(K_3) \quad \forall a \in \mathbb{F} \setminus \{0\} \quad \exists \frac{1}{a} \in \mathbb{F} \setminus \{0\} : \quad a \cdot \frac{1}{a} = 1. \quad (\text{II.48})$$

Bemerkungen und Beispiele.

¹engl.: Field

- Ist F ein Ring, der die Eigenschaften (K_2) und (K_3) , aber nicht (K_1) besitzt, so bezeichnet man F als Schiefkörper.
- Die Eigenschaften (R_1) – (R_3) sowie (K_1) – (K_3) eines Körpers F implizieren, dass $F \setminus \{0\}$ bezüglich der Multiplikation eine abelsche Gruppe mit neutralem Element 1 ist. Man bezeichnet $F^\times := F \setminus \{0\}$ als multiplikative Gruppe von F .
- Der Ring $\mathbb{Z}$ der ganzen Zahlen ist kein Körper.
- Die Menge $\mathbb{Q} := \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}\}$ der *rationalen Zahlen* bilden einen Körper.
- Weitere Körper sind die Menge der *reellen Zahlen* $\mathbb{R}$ und die Menge der *komplexen Zahlen* $\mathbb{C}$. Diese Körper sind für diese Vorlesung am wichtigsten. Deshalb schreiben wir $\mathbb{K}$ statt F , falls $F = \mathbb{R}$ oder $F = \mathbb{C}$.
- Ist p eine Primzahl, so bilden die Restklassen $\mathbb{Z}_p$ modulo p einen Körper (s. Abschnitt II.2.1).

II.4. Ergänzungen

II.4.1. Untergruppen

Definition II.5. Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ heißt **Untergruppe**

$$:\Leftrightarrow U \text{ ist bezüglich der Verknüpfung } \circ \text{ in } G \text{ selbst eine Gruppe.} \quad (\text{II.49})$$

Lemma II.6 (Untergruppenkriterium). *Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ ist eine Untergruppe, falls folgende drei Kriterien erfüllt sind:*

$$(i) \quad e \in U, \quad (\text{II.50})$$

$$(ii) \quad \forall a, b \in U : \quad a \circ b \in U, \quad (\text{II.51})$$

$$(iii) \quad \forall a \in U : \quad a^{-1} \in U. \quad (\text{II.52})$$

Beweis. Wegen (i) gilt $\circ : U \times U \rightarrow U$, d.h. U ist bezüglich $\circ$ abgeschlossen. Da die Verknüpfung auf G assoziativ ist, ist sie (erst recht) auch auf $U \subseteq G$ assoziativ. (i) sichert (G_2) und (iii) sichert (G_3) . $\square$

Bemerkungen und Beispiele.

- $\{e\}, G \subseteq G$ sind stets Untergruppen – die trivialen Untergruppen.
- Die geraden Zahlen $2\mathbb{Z} \subseteq \mathbb{Z}$ bilden bezüglich Addition eine Untergruppe.
- Die ungeraden Zahlen $2\mathbb{Z} + 1 \subseteq \mathbb{Z}$ sind bezüglich Addition keine Untergruppe, denn $0 \notin 2\mathbb{Z} + 1$.

Definition II.7. Sei $(G, \circ)$ eine Gruppe. Das **Zentrum** $Z(G) \subseteq G$ von G ist definiert durch

$$Z(G) := \{a \in G \mid \forall x \in G : ax = xa\}. \quad (\text{II.53})$$

Lemma II.8. $Z(G)$ ist eine abelsche Untergruppe von G .

Beweis. Zunächst weisen wir mit Hilfe des Untergruppenkriteriums, Lemma II.6, nach, dass $Z(G)$ eine Untergruppe von G ist.

- (i) Wegen $ex = x = xe$ ist $e \in Z(G)$.
- (ii) Für $a, b \in Z(G)$ und $x \in G$ ist $abx = axb = xab$, also ist $ab \in Z(G)$.
- (iii) Für $a \in Z(G)$ und $x \in G$ ist $x^{-1}a = ax^{-1}$ und daher $a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}$. Also ist mit a auch $a^{-1} \in Z(G)$.

Es folgt, dass $Z(G)$ eine Untergruppe ist. Weiterhin ist für $a, b \in Z(G)$ insbesondere $b \in G$ und deshalb ist $ab = ba$. Also ist $Z(G)$ abelsch. $\square$

II.4.2. Permutationen, Transpositionen, Zyklen und Signum

Definition II.9. Sei $\pi \in \mathcal{S}_n$ eine Permutation. Sind $k_1, k_2, \dots, k_r \in \mathbb{Z}_1^n$ mit $\pi(k_1) = k_2$, $\pi(k_2) = k_3, \dots, \pi(k_r) = k_1$, also

$$k_1 \xrightarrow{\pi} k_2 \xrightarrow{\pi} k_3 \xrightarrow{\pi} \dots \xrightarrow{\pi} k_r \xrightarrow{\pi} k_1, \quad (\text{II.54})$$

so heißt $(k_1, k_2, \dots, k_r)$ **Zyklus** von π der Länge r .

Bemerkungen und Beispiele.

- Die Permutation $\pi \in \mathcal{S}_9$,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 9 & 3 & 8 & 7 & 6 & 2 \end{pmatrix}, \quad (\text{II.55})$$

besitzt die Zyklen

$$(1, 5, 3), \quad (2, 4, 9), \quad (6, 8), \quad (7) \quad (\text{II.56})$$

(etwa $1 \mapsto 5 \mapsto 3 \mapsto 1$). Jede Permutation ist offensichtlich durch ihre Zyklen eindeutig bestimmt, und man schreibt

$$\pi := (1, 5, 3) (2, 4, 9) (6, 8). \quad (\text{II.57})$$

(Zur Vereinfachung lässt man Zyklen der Länge 1 weg.)

- Umgekehrt kann für $n \geq r$ jeder Zyklus $(k_1, k_2, \dots, k_r)$ als Permutation in $\mathcal{S}_n$ gelesen werden: $(k_1, k_2, \dots, k_r)$ lässt alle Elemente in $\mathbb{Z}_1^n \setminus \{k_1, k_2, \dots, k_r\}$ invariant. Mit dieser Lesart wird (II.57) zu

$$\pi = (1, 5, 3) \circ (2, 4, 9) \circ (6, 8). \quad (\text{II.58})$$

- Außerdem kommutieren disjunkte Zyklen miteinander, deshalb ist $\pi = (1, 5, 3) \circ (2, 4, 9) \circ (6, 8) = (2, 4, 9) \circ (6, 8) \circ (1, 5, 3)$.
- Ein Vergleich mit (II.33) zeigt, dass Transpositionen genau die Zyklen der Länge 2 sind, nämlich

$$\sigma = \begin{pmatrix} 1 & \dots & i-1 & \mathbf{i} & i+1 & \dots & j-1 & \mathbf{j} & j+1 & \dots & n \\ 1 & \dots & i-1 & \mathbf{j} & i+1 & \dots & j-1 & \mathbf{i} & j+1 & \dots & n \end{pmatrix} = (i, j). \quad (\text{II.59})$$

Satz II.10. Sei $n \geq 2$. Jede Permutation $\pi \in \mathcal{S}_n$ kann als Komposition von Transpositionen geschrieben werden, d.h. es gibt $a_1, b_1, a_2, b_2, \dots, a_m, b_m \in \mathbb{Z}_1^n$, mit $a_i \neq b_i$, so dass

$$\pi = (a_1, b_1) \circ (a_2, b_2) \circ \dots \circ (a_m, b_m). \quad (\text{II.60})$$

Beweis. Zunächst stellen wir fest, dass es genügt, für einen beliebigen Zyklus $(a_1, \dots, a_r)$ der Länge $2 \leq r \leq n$ Glg. (II.60) zu zeigen. Es ist aber

$$(a_1, a_2, \dots, a_r) = (a_1, a_r) \circ (a_1, a_{r-1}) \circ \dots \circ (a_1, a_2). \quad (\text{II.61})$$

□

Lemma II.11. Sind $n \in \mathbb{N}$, $n \geq 2$, $1 \leq i < j \leq n$ und $\sigma = (i, j) \in \mathcal{S}_n$ eine Transposition, so ist

$$(-1)^\sigma = -1. \quad (\text{II.62})$$

Beweis. Der Beweis ist eine kleine Rechnung,

$$\begin{aligned} (-1)^\sigma &= \prod_{p < q} \frac{\sigma(q) - \sigma(p)}{q - p} = \prod_{p < q; \{p=i \vee q=j\}} \frac{\sigma(q) - \sigma(p)}{q - p} \\ &= \left(\prod_{p=i; i < q < j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \cdot \left(\prod_{p=i; q=j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \cdot \left(\prod_{p=i; q > j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \\ &\quad \cdot \left(\prod_{p=j; q > j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \cdot \left(\prod_{p < i; q=i} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \cdot \left(\prod_{p < i; q=j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \\ &\quad \cdot \left(\prod_{i < p < j; q=j} \frac{\sigma(q) - \sigma(p)}{q - p} \right) \\ &= \left(\prod_{p=i; i < q < j} \frac{q - j}{q - i} \right) \cdot \left(\frac{i - j}{j - i} \right) \cdot \left(\prod_{p=i; q > j} \frac{q - j}{q - i} \right) \cdot \left(\prod_{p=j; q > j} \frac{q - i}{q - j} \right) \\ &\quad \cdot \left(\prod_{p < i; q=i} \frac{j - p}{i - p} \right) \cdot \left(\prod_{p < i; q=j} \frac{i - p}{j - p} \right) \cdot \left(\prod_{i < p < j; q=j} \frac{i - p}{j - p} \right) \\ &= -1. \end{aligned} \quad (\text{II.63})$$

□

Lemma II.12. Sind $n \in \mathbb{N}$, $n \geq 2$, und $\pi, \kappa \in \mathcal{S}_n$ zwei Permutationen, so gilt

$$(-1)^{\pi \circ \kappa} = (-1)^\pi \cdot (-1)^\kappa. \quad (\text{II.64})$$

Beweis.

$$\begin{aligned} (-1)^{\pi \circ \kappa} &= \prod_{1 \leq i < j \leq n} \frac{\pi(\kappa(i)) - \pi(\kappa(j))}{i - j} = \prod_{1 \leq i < j \leq n} \frac{[\pi(\kappa(i)) - \pi(\kappa(j))] \cdot [\kappa(i) - \kappa(j)]}{[\kappa(i) - \kappa(j)] \cdot [i - j]} \\ &= \left(\prod_{1 \leq i < j \leq n} \frac{\pi(\kappa(i)) - \pi(\kappa(j))}{\kappa(i) - \kappa(j)} \right) \cdot \left(\prod_{1 \leq i < j \leq n} \frac{\kappa(i) - \kappa(j)}{i - j} \right) \\ &= \left(\prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j} \right) \cdot \left(\prod_{1 \leq i < j \leq n} \frac{\kappa(i) - \kappa(j)}{i - j} \right) \\ &= (-1)^\pi \cdot (-1)^\kappa. \end{aligned} \quad (\text{II.65})$$

□

Aus Lemmata II.11 und II.12 folgt nun Glg. (II.35), die wir nochmal als Korollar formulieren.

Korollar II.13. *Sind $n \in \mathbb{N}$ und $\pi = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_m \in \mathcal{S}_n$ eine Permutation, die als Komposition von m Transpositionen $\sigma_1, \sigma_2, \dots, \sigma_m \in \mathcal{S}_n$ dargestellt werden kann, so ist*

$$(-1)^\pi = (-1)^m. \quad (\text{II.66})$$

Beweis. Nach Lemmata II.11 und II.12 ist

$$(-1)^\pi = (-1)^{\sigma_1} \cdot (-1)^{\sigma_2} \dots (-1)^{\sigma_m} = (-1)^m. \quad (\text{II.67})$$

□

II.4.3. Der Polynomring $R[x]$ über einem kommutativen Ring R

Sei R ein kommutativer Ring. Wir betrachten Folgen $\underline{a} = (a_n)_{n=0}^\infty \in R^{\mathbb{N}_0}$, wobei nur endlich viele Folgenglieder von 0 verschieden sind. D.h. es gibt ein $m = m(\underline{a}) \in \mathbb{N}$, so dass

$$\underline{a} = (a_0, a_1, a_2, \dots, a_m, 0, 0, \dots). \quad (\text{II.68})$$

(Dabei hängt $m(\underline{a})$ im Allgemeinen von der betrachteten Folge $\underline{a}$ ab und ist nicht für alle Folgen gleich.) Wir sammeln diese Folgen in

$$R[x] := \left\{ \underline{a} = (a_n)_{n=0}^\infty \in R^{\mathbb{N}_0} \mid \exists m \in \mathbb{N} \forall n > m : a_n = 0 \right\}. \quad (\text{II.69})$$

$R[x]$ wird zu einem kommutativen Ring bezüglich der Verknüpfungen

$$\underline{a} + \underline{b} := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \quad (\text{II.70})$$

und

$$\underline{a} \cdot \underline{b} = \underline{c}, \quad \text{wobei} \quad c_n := a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0. \quad (\text{II.71})$$

Dies prüft man durch Nachrechnen der Ringaxiome leicht nach.

Wir führen nun x als formale Variable ein und identifizieren $\underline{a}$ mit dem Polynom

$$\underline{a}(x) := a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m. \quad (\text{II.72})$$

Dann sieht man sofort, dass die Addition und Multiplikation in $R[x]$ gerade der Addition und Multiplikation der zugehörigen Polynome entspricht:

$$\begin{aligned} (\underline{a} + \underline{b})(x) &= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_N + b_N)x^N \\ &= \underline{a}(x) + \underline{b}(x), \end{aligned} \quad (\text{II.73})$$

$$\begin{aligned} (\underline{a} \cdot \underline{b})(x) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots + (a_0 b_N + a_1 b_{N-1} + \dots + a_N b_0)x^N \\ &= \underline{a}(x) \cdot \underline{b}(x), \end{aligned} \quad (\text{II.74})$$

wobei $N := m(\underline{a}) + m(\underline{b})$. Daher bezeichnet man $R[x]$ als Ring der Polynome (in x) über R .

II.4.4. Restklassenringe $\mathbb{Z}_p$ modulo Primzahlen p sind Körper

Definition II.14. Seien $a, b \in \mathbb{Z}$.

- (i) Eine Zahl $g \in \mathbb{Z}$ heißt **Teiler von a** , falls es ein $h \in \mathbb{Z}$ so gibt, dass $a = gh$ gilt.
- (ii) Für $|a| + |b| > 0$ ist der **größte gemeinsame Teiler $\text{ggT}(a, b) \in \mathbb{Z}$** von a und b die größte ganze Zahl, die ein Teiler sowohl von a als auch von b ist.

Bemerkungen und Beispiele.

- Da $0 = g \cdot 0$ für alle $g \in \mathbb{Z}$ gilt, sind alle ganzen Zahlen Teiler von 0. Deshalb müssen wir $a = b = 0$ bei der Definition des größten gemeinsamen Teiler ausschließen.
- Sind $a, b \in \mathbb{Z}$, so ist 1 stets ein Teiler sowohl von a als auch von b . Daher ist $\text{ggT}(a, b) \geq 1$, d.h. der größte gemeinsame Teiler von $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$, $|a| + |b| > 0$, ist stets eine natürliche Zahl.

Lemma II.15. Sind $a, b \in \mathbb{Z}$ mit $|a| + |b| > 0$, so gibt es $k, \ell \in \mathbb{Z}$ so, dass

$$\text{ggT}(a, b) = ka + \ell b. \quad (\text{II.75})$$

Beweis. Sei

$$M := \{n \in \mathbb{N} \mid \exists k, \ell \in \mathbb{Z} : n = ka + \ell b\}. \quad (\text{II.76})$$

Dann ist $|a| + |b| \in M$, also $M \neq \emptyset$. Seien $m \in \mathbb{N}$ die kleinste Zahl in M , $m := \min M$, und $k, \ell \in \mathbb{Z}$ so, dass $m = ka + \ell b$. Da $d := \text{ggT}(a, b)$ sowohl a als auch b teilt, teilt d auch m , also ist $d \leq m$.

Seien nun $a = qm + r$, mit $q \in \mathbb{Z}$ und $0 \leq r < m$. Wäre $r \geq 1$, so wäre

$$r = a - qm = (1 - qk)a - q\ell b \in M. \quad (\text{II.77})$$

Da m die kleinste natürliche Zahl in M ist, kann dies nicht richtig sein, und es folgt $r = 0$, d.h. $a = qm$. Genauso erhält man $b = pm$. Also teilt m sowohl a als auch b . Damit ist $m \leq \text{ggT}(a, b) = d$.

Insgesamt folgt, dass

$$\text{ggT}(a, b) = m \in M. \quad (\text{II.78})$$

□

Satz II.16. $\mathbb{Z}_p$ ist ein Körper genau dann, wenn $p \in \mathbb{N}$ eine Primzahl ist.

Beweis.

Ist $p \in \mathbb{N}$ keine Primzahl, so gibt es $1 < a \leq b < p$ mit $p = ab$. Dann sind $[a]_p, [b]_p \neq [0]_p$, aber

$$[a]_p \cdot [b]_p = [ab]_p = [0]_p. \quad (\text{II.79})$$

Also ist $\mathbb{Z}_p$ kein Körper.

Sind p eine Primzahl und $1 < a < p$, so ist $\text{ggT}(a, p) = 1$. Nach Lemma II.15 gibt es $k, \ell \in \mathbb{Z}$ so, dass $1 = ka + \ell b$. Also ist

$$[1]_p = [k]_p \cdot [a]_p + [\ell]_p \cdot [p]_p = [k]_p \cdot [a]_p, \quad (\text{II.80})$$

d.h. $[k]_p$ ist das Inverse zu $[a]_p$ bezüglich Multiplikation in $\mathbb{Z}_p$. □