Serie 3:
Gruppen, Ringe und Körper

1. Im Folgenden sei $n \in \mathbb{N}$ und $\mathbb{Z}/n\mathbb{Z}$ bezeichne die Menge der Äquivalenzklassen von $\mathbb{Z}$ bezüglich der Relation:

$$k \sim_n l \Leftrightarrow n \mid k - l \quad \text{für alle } k, l \in \mathbb{Z}$$

Wir schreiben $k \equiv l \mod n$, wenn $k \sim_n l$, und bezeichnen mit $[k]$ die Äquivalenzklasse von k bezüglich n.

a) Definieren Sie eine Addition "$+$" und eine Multiplikation "$\cdot$" auf $\mathbb{Z}/n\mathbb{Z}$ durch

$$[k] + [l] := [k + l] \text{ und } [k] \cdot [l] := [kl] \quad \text{für alle } [k], [l] \in \mathbb{Z}/n\mathbb{Z}$$

Zeigen Sie, dass Addition und Multiplikation wohldefiniert sind und dass $\mathbb{Z}/n\mathbb{Z}$ mit diesen Verknüpfungen ein Ring ist.

b) Zeigen Sie mithilfe von Division mit Rest und Induktion, dass für ganze Zahlen $a, b, e, f \in \mathbb{Z} \setminus \{0\}$ mit der Eigenschaft $m \mid e \wedge m \mid f \implies m = \pm 1$ gilt:

$$ae = bf \implies e \mid b$$

***c)** Gegeben $k, l \in \mathbb{Z} \setminus \{0\}$, definiere $(k, l) \in \mathbb{Z} \setminus \{0\}$ durch:

1. $(k, l) \mid k$ und $(k, l) \mid l$
2. $\forall a \in \mathbb{Z} : (a \mid k \wedge a \mid l) \Rightarrow a \mid (k, l)$

Zeigen Sie, dass für alle $k, l \in \mathbb{Z} \setminus \{0\}$ ein Element $(k, l) \in \mathbb{Z} \setminus \{0\}$ mit dieser Eigenschaft existiert und dass es bis auf Vorzeichen eindeutig ist, d.h. wenn $a \in \mathbb{Z} \setminus \{0\}$ ein weiteres Element mit denselben Eigenschaften ist, dann gilt $a = \pm(k, l)$. Das (bis auf Vorzeichen eindeutige) Element (k, l) heisst "grösster gemeinsamer Teiler" von k und l, kurz $\mathrm{ggT}(k, l)$.

Bitte wenden!

d) Zeigen Sie das Lemma von Bézout: Seien $k, l, m \in \mathbb{Z}$ mit $k, l \neq 0$, dann sind folgende äquivalent:

1. $\exists s, t \in \mathbb{Z} : m = sk + tl$
2. $(k, l) \mid m$

e) Folgern Sie aus Teilaufgabe d), dass

$$\mathbb{Z}/n\mathbb{Z} \text{ ist ein Körper } \iff n \text{ ist prim}$$

2. Im Folgenden seien $(G, \circ, e_G)$ und $(H, *, e_H)$ Gruppen.

♡**a)** Seien $a, b, c \in G$. Beweisen Sie die folgenden Aussagen:

1. Es gilt
$$\forall a, b, c \in G : b = c \iff a \circ b = a \circ c.$$
2. Das inverse Element $a^{-1} \in G$ mit der Eigenschaft $a^{-1} \circ a = e$ ist eindeutig.
3. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

♡**b)** Eine Abbildung $\varphi : G \to H$ heisst *Gruppenhomomorphismus*, wenn gilt:

$$\forall g_1, g_2 \in G : \varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2).$$

Zeigen Sie

1. $\varphi(e_G) = e_H$ und für alle $g \in G$ ist $\varphi(g^{-1}) = \varphi(g)^{-1}$.
2. Das *Bild* $\{h \in H \mid \exists g \in G : \varphi(g) = h\} \subset H$ von φ mit der von H induzierten Verknüpfung ist eine Gruppe.
3. Der *Kern* $\{g \in G \mid \varphi(g) = e_H\} \subset G$ mit der von G induzierten Veknüpfung ist eine Gruppe.

Bemerkung: Eine *Untergruppe* einer Gruppe $(G, \circ, e_G)$ ist eine Teilmenge $S \subset G$, die versehen mit der Restriktion der Verknüpfung wieder eine Gruppe ist. Insbesondere ist die Verknüpfung auf S wohldefiniert: es gilt $s_1 \circ s_2 \in S$ für alle $s_1, s_2 \in S$. Man sagt, S ist *abgeschlossen* unter $\circ$.

c) Sei $(G, \circ, e)$ eine Gruppe, sei $H \subset G$ eine Teilmenge. Zeigen Sie, dass folgende äquivalent sind:

1. H ist eine Untergruppe von G.
2. H ist nicht leer und für alle $g, h \in H$ gilt $g \circ h^{-1} \in H$.

3. Sei $\mathbb{R}[x]$ der Ring der Polynome mit Koeffizienten in $\mathbb{R}$.

Siehe nächstes Blatt!

a) Seien $p, q \in \mathbb{R}[x]$. Zeigen Sie, dass $p+q$ und $p \cdot q$ Polynome sind und bestimmen Sie Koeffizienten von $p+q$ und $p \cdot q$.

Bemerkung: Sie werden im Verlaufe dieses Semesters lernen, dass *die* Koeffizienten eines Polynoms eindeutig sind. Sie können dies im Folgenden verwenden.

b) Sei p ein Polynom mit Koeffizienten $a_0, \ldots, a_n \in \mathbb{R}$, d.h.

$$p(x) = \sum_{k=0}^{n} a_k x^k \quad \text{für alle } x$$

Der *Grad* von p ist definiert als

$$\deg(p) := \begin{cases} -\infty & \text{falls } a_k = 0 \text{ für alle } 0 \leq k \leq n \\ \max\{k \mid 0 \leq k \leq n \wedge a_k \neq 0\} & \text{sonst} \end{cases}$$

Seien $p, q \in \mathbb{R}[x]$. Bestimmen Sie $\deg(p \cdot q)$.

c) Bestimmen Sie die Elemente $0_R, 1_R \in \mathbb{R}[x]$ definiert durch

$$0_R + p = p \text{ bzw. } 1_R \cdot p = p \quad \text{für alle } p \in \mathbb{R}[x]$$

Sei weiter $p \in \mathbb{R}[x]$. Zeigen Sie, dass das Element $p' \in \mathbb{R}[x]$ mit der Eigenschaft $p + p' = 0_R$ eindeutig bestimmt ist. Wir schreiben $-p$ für dieses durch p vollständig bestimmte Element.

d) Beweisen Sie die folgenden Rechenregeln in $\mathbb{R}[x]$:

1. $\forall p \in \mathbb{R}[x] : 0_R \cdot p = p \cdot 0_R = 0_R$
2. $\forall p, q \in \mathbb{R}[x] : (-p) \cdot q = p \cdot (-q) = -(p \cdot q)$
3. $\forall p, q \in \mathbb{R}[x] : p \cdot q = (-p) \cdot (-q)$
4. $\forall p \in \mathbb{R}[x] : (-1_R) \cdot p = p \cdot (-1_R) = -p$

4. Gegeben eine Gruppe $(G, \circ, e)$ mit endlich vielen Elementen $G = \{g_1, \ldots, g_n\}$ ist die Gruppentafel gegeben durch

$\circ$	$\cdots$	g_j	$\cdots$
$\vdots$		$\vdots$	
g_i	$\cdots$	$g_i \circ g_j$	$\cdots$
$\vdots$		$\vdots$	

Sei zum Beispiel $(G, \circ, e)$ eine Gruppe mit zwei verschiedenen Elementen $G = \{e, a\}$, dann impliziert die Kürzungsregel, dass $a \circ a = e$ und also ist die Gruppentafel notwendigerweise gegeben durch

$\circ$	e	a
e	e	a
a	a	e

Bitte wenden!

Insbesondere existiert bis auf Umbenennung der Elemente genau eine Gruppe mit zwei Elementen.

a) Verwenden Sie die Gruppentafel, um zu zeigen, dass es, bis auf Umbenennung der Elemente, genau eine Gruppe mit drei Elementen gibt.

b) Verwenden Sie die Gruppentafel, um bis auf Umbenennung alle (zwei) Gruppen mit vier Elementen zu bestimmen.

c) Eine Gruppe $(G, \circ, e)$ heisst abelsch genau dann, wenn

$$\forall a, b \in G : a \circ b = b \circ a$$

Geben Sie eine Charakterisierung endlicher, abelscher Gruppen unter Verwendung der Gruppentafel.

*__d)__ Sei D_4 die Gruppe erzeugt durch Komposition von Rotationen um den Mittelpunkt sowie Spiegelungen entlang der Symmetrieachsen eines Quadrats, die das Quadrat auf sich selber abbilden (vgl. Bild 1). Zeigen Sie, dass zwei Elemente $r, s \in D_4$ existieren, so dass sich jedes Element in D_4 als Komposition von s mit einer Potenz von r schreiben lässt.

e) Zeigen Sie, dass D_4 nicht-abelsch ist.

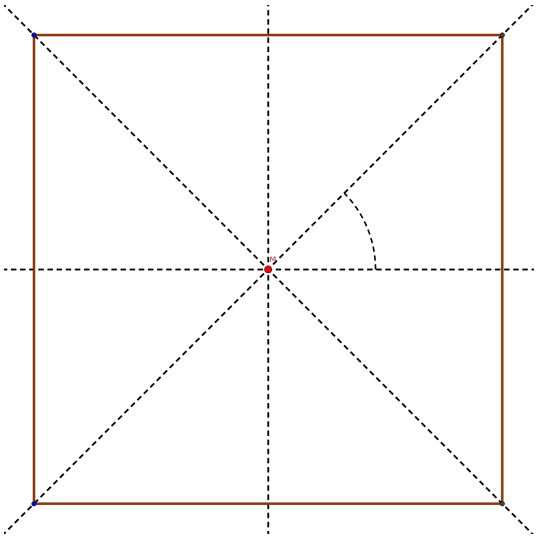

Abbildung 1: Ein Quadrat mit Mittelpunkt M und seinen Symmetrieachsen.

5. Online-Abgabe

Siehe nächstes Blatt!

1. Für welche der folgenden Verknüpfungen können wir eine abelsche Gruppe $(G, \circ, e)$ definieren?

(a) $G = \mathbb{N}$, $a \circ b := \max\{a, b\}$.

(b) $G = \mathbb{N}$, $a \circ b := \mathrm{kgV}(a, b)$.

(c) $G = \{x \in \mathbb{R} \mid x > 0\}$, $a \circ b := a^b$.

(d) $G := \{x \in \mathbb{R} \mid 0 < x < 1\}$, $a \circ b := \frac{ab}{1-(a+b)+2ab}$

2. *Prüfung HS 2016:* Die Vorschrift $G = \mathbb{N}, a * b := \min\{a, b\}$ definiert eine Gruppe $(G, *)$.

(a) Wahr.

(b) Falsch.

3. *Prüfung HS 2016:* Seien $f, g \in \mathbb{R}[X]$ mit $\deg(f) = \deg(g) = n$, dann ist $\deg(f + g) = n$.

(a) Wahr.

(b) Falsch.

4. Betrachten Sie die Verknüpfungen $+, \cdot$ auf $\mathbb{Q} \times \mathbb{Q}$ gegeben durch

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2)\\ (a_1, a_2) \cdot (b_1, b_2) &:= (a_1 b_1 + 3a_2 b_2, a_1 b_2 + a_2 b_1)\end{aligned}$$

für alle $(a_1, a_2), (b_1, b_2) \in \mathbb{Q} \times \mathbb{Q}$.

(a) $\mathbb{Q} \times \mathbb{Q}$ mit den Verknüpfungen $+$ und $\cdot$ ist ein Ring.

(b) $\mathbb{Q} \times \mathbb{Q}$ mit den Verknüpfungen $+$ und $\cdot$ ist ein Körper.

Abgabe der schriftlichen Aufgaben: Vor Donnerstag, den 12. Oktober 10:00 Uhr vormittags im Raum HG J 68, in einem der Fächer beschriftet mit *Abgabe*.