2. Übungsblatt

1. Wiederholen Sie die Begriffe „Gruppe“, „Ring“ und „Körper“. Verwenden Sie die Definitionen dieser algebraischen Strukturen, um die folgenden Aufgaben zu lösen:

   a) Sei $n \in \mathbb{N}$. Mit E_n wird die Menge der n-ten *Einheitswurzeln* aus $\mathbb{C}$ bezeichnet, d.h. $E_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

      i) Geben Sie alle n-ten Einheitswurzeln an. Dabei ist es hilfreich, die Polardarstellung von komplexen Zahlen zu verwenden.

      ii) Zeigen Sie, dass $(E_n, \cdot)$ eine Gruppe bildet.

   b) Zeigen Sie, dass in $\mathbb{Z}$ für jedes $a \in Z$ gilt, dass $a \cdot 0 = 0$. Welche Eigenschaften von $\mathbb{Z}$ verwenden Sie?

   c) Zeigen Sie, dass in $\mathbb{Q}$ keine Zahlen $a, b \neq 0$ gibt, so dass $a \cdot b = 0$. Welche Eigenschaften von $\mathbb{Q}$ verwenden Sie für Ihren Beweis?

2. Modulare Arithmetik

   Definition 1: *Es seien $a, b \in \mathbb{Z}$. Wir nennen a einen Teiler von b (oder b ein Vielfaches von a, oder man sagt auch a teilt b), wenn es ein Element $c \in \mathbb{Z}$ gibt mit $b = a \cdot c$. Ist a ein Teiler von b, dann schreiben wir $a \mid b$, sonst $a \nmid b$ (a teilt nicht b).*

   Sei n eine feste natürliche Zahl. Wir definieren eine binäre Relation $\equiv_n$ auf $\mathbb{Z} \times \mathbb{Z}$ wie folgt:

   $$a \equiv_n b \text{ gdw. } n \mid (b - a)$$

   Statt $a \equiv_n b$ schreiben wir meist $a \equiv b \bmod n$. Zeigen Sie für eine feste natürliche Zahl n:

   - Für alle $a \in \mathbb{Z}$ gilt $a \equiv_n a$
   - Seien $a, b \in \mathbb{Z}$ und $a \equiv_n b$, dann auch $b \equiv_n a$
   - Seien $a, b, c \in \mathbb{Z}$, $a \equiv_n b$ und $b \equiv_n c$, dann auch gilt auch $a \equiv_n c$.

   Die Relation $\equiv_n$ teilt $\mathbb{Z}$ in n verschiedene Klassen auf, die wir wie folgt beschreiben können:

   $$\overline{a} =_{\text{def}} \{b \in \mathbb{Z} \mid b \equiv a \bmod n\}$$

   Damit ergibt sich $\overline{a} = \{a + k \cdot n \mid k \in \mathbb{Z}\}$ und deshalb ist $\overline{a}$ die Menge aller ganzen Zahlen, die beim teilen durch n den gleichen Rest lassen wie a. Die Menge $\overline{a}$ nennt man auch *Restklasse (mod n)*.

   Geben Sie alle Restklassen $\bmod 8$ an.

   Wir legen fest:

   $$\mathbb{Z}_n =_{\text{def}} \{\overline{a} \mid \ \overline{a} \text{ ist Restklasse } \bmod n\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

   und definieren zwei binäre Operationen wie folgt:

Restklassenaddition: $\overline{a} + \overline{b} =_{\text{def}} \overline{a+b}$
Restklassenmultiplikation: $\overline{a} \cdot \overline{b} =_{\text{def}} \overline{a \cdot b}$

Beweisen Sie: Die Struktur $(\mathbb{Z}_n, +, \cdot)$ ist ein kommutativer Ring mit Einselement.

Geben Sie die Verknüpfungstabellen des Rings $(\mathbb{Z}_6, +, \cdot)$ an. Gibt es Elemente $\overline{a}, \overline{b} \in \mathbb{Z}_6$ mit $\overline{a}, \overline{b} \neq \overline{0}$ und $\overline{a} \cdot \overline{b} = \overline{0}$? Wie verhält sich das bei $(\mathbb{Z}_7, +, \cdot)$?

Besprechnung in der Übung am 30. Oktober 2013