

Übungsaufgaben zur Vorlesung
Algebra / Zahlentheorie

Prof. Dr. J. Kramer

Abgabetermin: 15.06.2015 in der Vorlesung

Bitte beachten:

JEDE Aufgabe auf einem neuen Blatt abgeben.

JEDES Blatt mit Namen, Matrikelnummer und Übungsgruppe versehen.

Serie 9 (30 Punkte)

Aufgabe 1 (10 Punkte)

Zeigen Sie, dass die Ordnungsrelation „ $<$ “ auf der Menge der ganzen Zahlen \mathbb{Z} die beiden folgenden Regeln erfüllt:

- (a) Für alle $a, b, c \in \mathbb{Z}$ gilt mit $a < b$ auch $a + c < b + c$.
- (b) Für alle $a, b, c \in \mathbb{Z}$ gilt mit $a < b$ die Ungleichung

$$a \cdot c < b \cdot c, \text{ falls } c > 0, \quad \text{bzw.} \quad a \cdot c > b \cdot c, \text{ falls } c < 0.$$

Hinweis: Man beweise zuerst, dass für zwei Zahlen $a, b \in \mathbb{Z}$ die Relation $a < b$ äquivalent zur Relation $b - a > 0$ ist.

Aufgabe 2 (10 Punkte)

Beweisen Sie die Gültigkeit der Division mit Rest im Bereich der ganzen Zahlen, d.h. gegeben $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann existieren eindeutig bestimmte ganze Zahlen q, r mit $0 \leq r < |b|$, so dass die Gleichheit

$$a = q \cdot b + r$$

besteht.

Hinweis: Es darf die Gültigkeit der Division mit Rest im Bereich der natürlichen Zahlen vorausgesetzt werden.

Aufgabe 3 (10 Punkte)

Es seien $n \in \mathbb{N}$ mit $n > 0$ und $\mathbb{Z}/n\mathbb{Z}$ die Menge der Linksnebenklassen von \mathbb{Z} nach $n\mathbb{Z}$. Mit der Schreibweise $\bar{a} := a + n\mathbb{Z}$ ($a \in \mathbb{Z}$) wird durch

$$\bar{a} \circ \bar{b} := \overline{a \cdot b} \quad (a, b \in \mathbb{Z})$$

eine assoziative und kommutative Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$ definiert.

Bitte wenden!

- (a) Beweisen Sie, dass $(\mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}, \circ)$ genau dann eine Gruppe ist, wenn n eine Primzahl ist.
- (b) Es sei p eine Primzahl. Zeigen Sie, dass $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \circ)$ zu $(\mathcal{R}_p \setminus \{0\}, \odot)$ isomorph ist.
- (c) Es sei p eine Primzahl und $a \in \mathbb{Z}$. Beweisen Sie mit Hilfe des Satzes von Lagrange, dass die Teilbarkeitsbeziehung

$$p \mid (a^p - a)$$

besteht.

Hinweis: Betrachten Sie für $p \nmid a$ die Ordnung von \bar{a} in der Gruppe $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \circ)$.