HU Berlin Sommersemester 2018

Übungsaufgaben zur Vorlesung
Algebra / Zahlentheorie

Prof. Dr. J. Kramer

Abgabetermin: 25.06.2018 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 $\overline{a} := a + n\mathbb{Z}$ $(a \in \mathbb{Z})$ wird durch

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

eine Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ definiert, die assoziativ und kommutativ ist.

Bitte wenden!

(a) Beweisen Sie, dass $(\mathbb{Z}/n\mathbb{Z}\setminus\{\overline{0}\},\cdot)$ genau dann eine Gruppe ist, wenn n eine Primzahl ist.

(b) Berechnen Sie das Inverse von $\overline{16}$ in der Gruppe $(\mathbb{Z}/97\mathbb{Z}\setminus\{\overline{0}\},\cdot)$.

(c) Es sei p eine Primzahl und $a\in\mathbb{Z}$. Beweisen Sie mit Hilfe des Satzes von Lagrange, dass die Teilbarkeitsbeziehung

$$p\,|\,(a^p-a)$$

besteht.

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