

# Übungsaufgaben zur Vorlesung Algebra und Zahlentheorie und ihre Didaktik Serie 8

Dr. Daniel Skodlerack

Abgabe am **Montag den 19.06.2017** vor dem Beginn der Vorlesung.

Bitte beachten Sie Folgendes:

1. Beginnen Sie **jede** Aufgabe auf einem neuen Blatt.
2. Beschriften Sie **jedes** abzugebende Blatt mit Namen, Matrikelnummer und Übungsgruppe.
3. Begründen Sie Ihre Lösungen, wenn nicht anders lautend, **nur** mit der Vorlesung, der Übung und vorhergehender Übungsaufgaben.

**Aufgabe 1.** (5+5+5 Punkte)(RSA-Verfahren, Spionage) In dieser Aufgabe betätigen Sie sich als Spion. Sie wissen, dass Person A an Person B eine Nachricht schreiben möchte. Sie fangen den öffentlichen Schlüssel  $T := (n, e) = (85, 5)$  von Person B ab.

1.  $n$  wurde leider nicht besonders gut gewählt, und daher kann man aus ihm leicht den geheimen Schlüssel  $S = (d)$  ausrechnen. Berechnen Sie  $d$ .
2. Person A verschickt gerade Nachrichten an B. Sie fangen 1, 27 und 55 ab. Dies sind Reste modulo 85. Entschlüsseln Sie diese, d.h. finden Sie  $N_1, N_2, N_3 \in \mathbb{N}_0^{\leq 84}$ , so dass  $N_1 \equiv 1^d$ ,  $N_2 \equiv 27^d$  und  $N_3 \equiv 55^d$  modulo 85 gelten.
3. Wir haben die Zahl  $(N_1, N_2, N_3)_{85}$  in 85-adischer Darstellung. Schreiben Sie diese in 26-adischer Darstellung und finden Sie das Wort. Null entspricht dem ersten Buchstaben im Alphabet.

**Aufgabe 2.** (5+5 Punkte)(Ringe von Abbildungen)

1. Es seien  $S$  ein unitärer Ring und  $X$  eine nichtleere Menge. Zeigen Sie, dass  $(\text{Abb}(X, S), +, \cdot)$  mit den durch  $(f + g)(x) := f(x) + g(x)$  und  $(f \cdot g)(x) := f(x)g(x)$  definierten Strukturen ein unitärer Ring ist.
2. Ist für alle unitären Ringe  $S$  das Tripel  $(\text{Abb}(S, S), +, \circ)$  ein unitärer Ring? Beweisen Sie Ihre Antwort.

**Aufgabe 3.** (5+5+5\* Punkte)(Monoidringe und Gruppenringe) Wir betrachten einen Monoiden  $(M, *)$  und einen kommutativen unitären Ring  $R$ . Wir bezeichnen für eine Abbildung  $f : M \rightarrow R$  die Menge

$$\text{supp}(f) := \{x \in M \mid f(x) \neq 0\}$$

als den *Träger* von  $f$ .

1. Zeigen Sie, dass

$$(RM := \{f \in \text{Abb}(M, R) \mid \text{supp}(f) \text{ ist endlich.}\}, +, \odot)$$

mit den durch

$$(f + g)(x) := f(x) + g(x) \text{ und } (f \odot g)(x) := \sum_{y, z \in M \text{ mit } y * z = x} f(y)g(z)$$

definierten Strukturen ein unitärer Ring ist. Man bezeichnet ihn als den *Monoidring* von  $M$  über  $R$ .

2. Zeigen Sie, dass ein Monoidmonomorphismus von  $M$  nach  $(RM, \odot)$  existiert.
3. Zeigen Sie, dass  $M$  eine abelsche Gruppe sein muss, wenn  $RM$  ein Körper ist. Im Fall, dass  $M$  eine Gruppe ist, nennt man  $RM$  den *Gruppenring* von  $M$  über  $R$ .

**Aufgabe 4.** (10 Punkte)(Polynome und endliche Körper) Es sei  $P$  ein nichtkonstantes ganzzahliges Polynom, d.h. ein Element aus  $\mathbb{Z}[X] \setminus \mathbb{Z}$ . Zeigen Sie, dass ein endlicher Körper existiert, in dem  $P$  eine Nullstelle hat.