



Dr. Ralf Gerkmann

Wintersemester 2017/18  
22.02.2018

# Zahlentheorie

(Lehramt Gymnasium)

## Klausur

Nachname: \_\_\_\_\_ Vorname: \_\_\_\_\_

Matrikelnr.: \_\_\_\_\_

Studiengang: ☐ Lehramt Gymnasium ☐ Bachelor Wirtschaftspädagogik

Prüfungsordnung ☐ 2009 ☐ 2011

Ihr Klausurergebnis können Sie auf der Vorlesungshomepage mit Hilfe eines Benutzernamens, eines Passworts und einer vierstelligen Identifikationsnummer abrufen, die Ihnen persönlich zugeordnet ist. Sie erhalten diese Daten während der Klausur.

Aufgabe	1	2	3	4	5	6	7	8	$\Sigma$
Punkte									

### Hinweise:

- (a) Bitte überprüfen Sie, ob Sie **neun Blätter** (Deckblatt + 8 Aufgaben) erhalten haben.
- (b) Für die Klausur sind **keine Hilfsmittel** (z.B. Skripten, handschriftliche Notizen, Taschenrechner) zugelassen.
- (c) Schreiben Sie keine Lösungen zu unterschiedlichen Aufgaben auf dasselbe Blatt.
- (d) Füllen Sie das Deckblatt bitte in BLOCKSCHRIFT aus. Schreiben Sie auf **jedes Blatt** Ihren **Vor- und Nachnamen**.
- (e) Bitte denken Sie daran, jeden Schritt Ihrer Lösung zu begründen und explizit darauf hinzuweisen, wenn Sie Ergebnisse aus der Vorlesung verwenden. Die Verwendung von Ergebnissen aus Übungsaufgaben ist **nicht** zulässig.
- (f) Bitte achten Sie darauf, dass Sie zu jeder Aufgabe nur eine Lösung abgeben; streichen Sie deutlich durch, was nicht gewertet werden soll.
- (g) Bei Bedarf kann zusätzliches Schreibpapier angefordert werden. Bitte verwenden Sie keine eigenen Blätter.

Bearbeitungszeit: 120 Minuten

Viel Erfolg!

Name: \_\_\_\_\_

**Aufgabe 1.** (2+2+3+3 Punkte)

Sei  $R = \mathbb{F}_2 \times \mathbb{F}_3$ , wobei  $\mathbb{F}_2$  den Körper mit zwei und  $\mathbb{F}_3$  den Körper mit drei Elementen bezeichnet.

- (a) Geben Sie alle Einheiten von  $R$  an. Ein Nachweis, dass es sich tatsächlich um Einheiten handelt, ist hier *nicht* erforderlich.
- (b) Entscheiden Sie, ob  $R$  ein Körper ist, und begründen Sie Ihre Entscheidung.
- (c) Geben Sie ein Ideal  $I$  von  $R$  mit  $\{0_R\} \subsetneq I \subsetneq R$  an, indem Sie alle Elemente von  $I$  aufzählen, und begründen Sie, dass die von Ihnen angegebene Teilmenge tatsächlich ein Ideal ist.
- (d) Bestimmen Sie die Charakteristik von  $R$  (mit Nachweis).

Name: \_\_\_\_\_

**Aufgabe 2.** (6+4 Punkte)

Wir betrachten die Teilmenge  $R \subseteq \mathbb{R}$  gegeben durch

$$R = \left\{ \frac{a + b\sqrt{2}}{2^n} \mid a, b \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

- (a) Weisen Sie nach, dass  $R$  ein Teilring von  $\mathbb{R}$  ist.
- (b) Beweisen Sie die Gleichung  $R = \mathbb{Z}[\frac{1}{\sqrt{2}}]$ .

Name: \_\_\_\_\_

**Aufgabe 3.** (2+8 Punkte)

- (a) Geben Sie zwei Beispiele euklidischer Ringe an, jeweils mit zugehöriger Höhenfunktion.
- (b) Bestimmen Sie mit dem Euklidischen Algorithmus das multiplikative Inverse von  $\overline{437}$  im Restklassenring  $\mathbb{Z}/911\mathbb{Z}$ .

Name: \_\_\_\_\_

**Aufgabe 4.** (3+7 Punkte)

- (a) Formulieren Sie den Chinesischen Restsatz für beliebige Ringe.
- (b) Bestimmen Sie ein  $a \in \mathbb{Z}$  mit  $a \equiv 3 \pmod{15}$  und  $a \equiv 47 \pmod{92}$ .

Name: \_\_\_\_\_

**Aufgabe 5.** (4+6 Punkte)

- (a) Geben Sie die Definitionen der Begriffe „Primideal“ und „maximales Ideal“ an.
- (b) Wir betrachten im  $R = \mathbb{Z}[i]$  die Ideale  $I = (3, 2 - i)$  und  $J = (1 + i, 6)$ . Bestimmen Sie ein Element  $\alpha \in R$ , so dass  $IJ = (\alpha)$  erfüllt ist.

Name: \_\_\_\_\_

**Aufgabe 6.** (3+2+5 Punkte)

Sei  $R = \mathbb{F}_2[x]$  und  $f = x^3 + x + \bar{1}$ . Ohne Beweis darf verwendet werden, dass  $f$  in  $R$  ein irreduzibles Element ist.

- (a) Begründen Sie mit Hilfe geeigneter Sätze aus der Vorlesung, dass der Faktorring  $R/(f)$  ein Körper ist.
- (b) Welche Bedingung müssen zwei Polynome  $g, h \in R$  erfüllen, damit in  $R/(f)$  die Gleichung  $g + (f) = h + (f)$  gilt?
- (c) Sei  $\alpha = x + (f)$ . Bestimmen Sie Elemente  $a, b, c \in \mathbb{F}_2$ , so dass  $\alpha^4 = ax^2 + bx + c + (f)$  gilt.

Name: \_\_\_\_\_

**Aufgabe 7.** (6+4 Punkte)

- (a) Geben Sie ein  $r \in \mathbb{N}$  und zyklische Gruppen  $C_1, \dots, C_r$  an, so dass ein Isomorphismus  $(\mathbb{Z}/132\mathbb{Z})^\times \cong C_1 \times \dots \times C_r$  existiert.
- (b) Weisen Sie nach, dass 3 eine Primitivwurzel modulo 17 ist, 2 aber nicht.



Name: \_\_\_\_\_

**Aufgabe 8.** (4+6 Punkte)

- (a) Geben Sie die Definitionen der Begriffe „irreduzibles Element“ und „Primelement“ an.
- (b) Sei  $R$  ein Integritätsbereich,  $p, q$  Primelemente in  $R$  und  $a, b, c$  drei weitere Ringelemente. Zeigen Sie: Gilt  $pq = abc$ , dann ist mindestens eines der drei Elemente  $a, b, c$  eine Einheit im Ring  $R$ .