LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2024/25
10.04.2025

Zahlentheorie

(Wiederholungsklausur alte Studienordnung)

Nachholklausur

Nachname: ______________________ Vorname: ______________________

Matrikelnr.: ____

Studiengang:
- ❑ Lehramt Gymnasium
- ❑ Master Wirtschaftspädagogik

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	$\sum$
Punkte									

Lösungen sind nur angedeutet, unvollst.

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. (5+3+2 Punkte)

Wir betrachten im Körper $\mathbb{R}$ der reellen Zahlen die Teilmenge

$$S = \left\{ a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} \mid a, b, c, d \in \mathbb{Z} \right\}.$$

(a) Zeigen Sie, dass S ein Teilring von $\mathbb{R}$ mit $S \supseteq \mathbb{Z} \cup \{\sqrt{2}, \sqrt{5}\}$ ist.

(b) Zeigen Sie, dass S mit dem Teilring $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$ von $\mathbb{R}$ übereinstimmt.

(c) Weisen Sie nach, dass $1 + \sqrt{2}$ in S eine Einheit ist.

zu (a) zu zeigen: (i) $1 \in S$

(ii) $\forall \alpha, \beta \in S$: $\alpha - \beta, \alpha\beta \in S$

(iii) $\forall a \in \mathbb{Z}$: $a \in S$ (iv) $\sqrt{2}, \sqrt{5} \in S$

zu (b) Sei T ein Teilring von $\mathbb{R}$ mit $T \supseteq \mathbb{Z} \cup \{\sqrt{2}, \sqrt{5}\}$.

zu zeigen: $S \subseteq T$

zu (c) $(1+\sqrt{2})(-1+\sqrt{2}) = 1$, und $-1+\sqrt{2} \in S$

(nur Lösungsskizze)

Name: ____

Aufgabe 2. (4+3+3 Punkte)

Wir betrachten die Menge $R = \mathbb{F}_3 \times \mathbb{F}_5$ mit den durch komponentenweise Addition und Multiplikation gegebenen Verknüpfungen, d.h. wir definieren die Verknüpfungen $+$ und $\cdot$ auf R durch

$$(a,b) + (c,d) = (a+c, b+d) \quad \text{und} \quad (a,b)\cdot(c,d) = (ac, bd)$$

für alle $a, c \in \mathbb{F}_3$ und $b, d \in \mathbb{F}_5$. Ohne Beweis darf verwendet werden, dass $(R, +, \cdot)$ ein Ring ist.

(a) Bestimmen Sie die Menge der Nullteiler von R.

(b) Bestimmen Sie die Menge der Einheiten von R.

(c) Geben Sie die Definition der Charakteristik eines Rings an, und bestimmen Sie die Charakteristik von R.

Bitte begründen Sie in jedem Aufgabenteil jeweils Ihre Antwort.

zu (a) Nullteiler $\{(a,b) \mid a = 0_{\mathbb{F}_3} \vee b = 0_{\mathbb{F}_5}\}$

z.zg.: (i) Alle Elemente der Menge sind Nullteiler.

(ii) Jeder Nullteiler ist in der Menge enthalten.

zu (b) $R^\times = \mathbb{F}_3^\times \times \mathbb{F}_5^\times = \{\bar{1}, \bar{2}\} \times \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

(Laut Vorlesung gilt $(R \times S)^\times = R^\times \times S^\times$ für beliebige Ringe R, S.)

zu (c) Ergebnis: $\operatorname{char} R = 15$

(nur Lösungsskizze)

Name: ____________________

Aufgabe 3. (2+6+2 Punkte)

Sei $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ der Ring der Gauß'schen Zahlen.

(a) Geben Sie die Einheiten von $\mathbb{Z}[i]$ an. Ein Nachweis ist hier nicht erforderlich.

(b) Entscheiden Sie, welche der Elemente

$$-1, \quad 6, \quad 2+3i, \quad 3+3i, \quad 7, \quad 13$$

Primelemente in $\mathbb{Z}[i]$ sind, und begründen Sie jeweils Ihre Entscheidung.

(c) Gibt es in $\mathbb{Z}[i]$ ein Element, das zwar irreduzibel, aber nicht prim ist?
Bitte begründen Sie auch hier Ihre Antwort.

Lösungsskizze:

zu (a) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

zu (b) -1 Einheit $\Rightarrow$ kein Primelt.

$6 = 2 \cdot 3$, $2, 3 \notin \mathbb{Z}[i]^\times$ $\Rightarrow$ nicht irred. $\Rightarrow$ nicht prim

$N(2+3i) = 13$ Primzahl $\Rightarrow$ Primelement

$3 = 3 \cdot (1+i)$, $3, 1+i \notin \mathbb{Z}[i]^\times$ $\Rightarrow$ nicht prim

$N(7)$ Primzahlquadrat, $a^2 + b^2 = 7$ nicht lösbar $\Rightarrow$ Primelt.

$13 = (2+3i)(2-3i)$, $2 \pm 3i \notin \mathbb{Z}[i]^\times$ $\Rightarrow$ nicht prim

zu (c) nein, weil $\mathbb{Z}[i]$ euklidisch und somit auch faktoriell ist

Name: ____

Aufgabe 4. (4+6 Punkte)

(a) Zeigen Sie, dass der Körper $\mathbb{Q}(\sqrt{-3})$ ein Quotientenkörper des Rings $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ ist. Geben Sie zu Beginn die Definition des Quotientenkörpers eines Integritätsbereichs an.

(b) Beweisen Sie, dass ein Isomorphismus $\mathbb{Z}[x]/(3,x) \cong \mathbb{F}_3$ von Ringen existiert, indem Sie den Homomorphiesatz für Ringe auf die Abbildung $\mathbb{Z}[x] \to \mathbb{F}_3$, $f \mapsto f(0) + 3\mathbb{Z}$ anwenden.

Lösungsskizze:

Zu (a) zeige: (i) $\alpha \in \mathbb{Q}(\sqrt{-3}) \Rightarrow \exists\, a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $\alpha = \frac{1}{c}(a + b\sqrt{-3})$

(ii) $\mathbb{Z} \subseteq \mathbb{Q}(\sqrt{-3})$ und $\frac{1}{2}(1+\sqrt{-3}) \in \mathbb{Q}(\sqrt{-3})$

Zu (b) Zu überprüfen: Die angeg. Abbildung ϕ ist (i) ein Ringhom. (ii) surjektiv und (iii) $\ker \phi = (3, x)$

Name: ______________________________

Aufgabe 5. (4+6 Punkte)

(a) Zeigen Sie, dass das Polynom $x^3 + x + 1$ in $\mathbb{Q}[x]$ irreduzibel ist.

(b) Bestimmen Sie alle $a \in \mathbb{Z}$ mit der Eigenschaft, dass das Polynom $x^4 + ax + 2 \in \mathbb{Z}[x]$ in $\mathbb{Q}$ eine Nullstelle besitzt (mit Nachweis).

Lösungsskizze:

zu (a) einzige mögliche Nullst. in $\mathbb{Q}$ sind ± 1

keine Nullst. in $\mathbb{Q}$, Pol. vom Grad 3 $\Rightarrow$ irred.

zu (b) einzige mögl. Nullst. sind $\pm 1, \pm 2$

betrachte die Gleichungen $1 + a + 2 = 0$, $1 - a + 2 = 0$,

$16 + 2a + 2 = 0$, $16 - 2a + 2 = 0$

Ergebnis: $a \in \{\pm 3, \pm 9\}$

Name: ____________________

Aufgabe 6. (5+2+3 Punkte)

(a) Bestimmen Sie ein $r \in \mathbb{N}$ und zyklische Gruppen $C_1, ..., C_r$, so dass die prime Restklassengruppe $(\mathbb{Z}/1120\mathbb{Z})^\times$ isomorph zu $C_1 \times ... \times C_r$ ist. (Es ist $1120 = 32 \cdot 5 \cdot 7$.)

(b) Geben Sie die Ordnung von $(\mathbb{Z}/1120\mathbb{Z})^\times$ an und begründen Sie, dass die Gruppe nicht zyklisch ist.

(c) Geben Sie die Anzahl der Elemente der Ordnung 2 in $(\mathbb{Z}/1120\mathbb{Z})^\times$ an.
Ein Nachweis ist *nicht* erforderlich.

Lösungsskizze:

zu (a) $r = 4$, $C_1 = \mathbb{Z}/2\mathbb{Z}$, $C_2 = \mathbb{Z}/8\mathbb{Z}$, $C_3 = \mathbb{Z}/4\mathbb{Z}$
$C_4 = \mathbb{Z}/6\mathbb{Z}$

zu (b) $|(\mathbb{Z}/1120\mathbb{Z})^\times| = \varphi(1120) = \varphi(32) \cdot \varphi(5) \cdot \varphi(7)$
$= 16 \cdot 4 \cdot 6 = 96 \cdot 4 = 384$

zu (c) Anzahl 15

Name: ______________________________

Aufgabe 7. (5+5 Punkte)

(a) Weisen Sie nach, dass im Ring $\mathbb{Z}[\sqrt{-6}]$ das Produkt $\mathfrak{p}_1\mathfrak{p}_2$ der beiden Ideale $\mathfrak{p}_1 = (5, 11 - 2\sqrt{-6})$ und $\mathfrak{p}_2 = (5, 11 + 2\sqrt{-6})$ mit dem Hauptideal (5) übereinstimmt.

(b) Seien R und S Ringe, $I \subseteq R$ ein Ideal in R und $J \subseteq S$ ein Ideal in S. Weisen Sie nach, dass $I \times J$ ein Ideal in $R \times S$ ist.

Lösungsskizze:

Zu (a) $\mathfrak{p}_1 \mathfrak{p}_2 = (25, 55 - 10\sqrt{-6}, 55 + 10\sqrt{-6}, 121 + 24)$

$\overset{(*)}{=} (5)$ (*) überprüfe $5 \in (25, \ldots)$ und

$25, 55 - 10\sqrt{-6}, \ldots \in (5)$

Zu (b) Seien $\alpha, \beta \in I \times J$, $\alpha = (a, b)$, $\beta = (c, d)$ mit

$a, c \in I$ und $b, d \in J$. überprüfe:

(0) $(0_R, 0_S) \in I \times J$

(i) $\alpha + \beta \in I \times J$

(ii) $\forall (r, s) \in R \times S : (r, s) \cdot \alpha \in I \times J$

Name: ______________________________

Aufgabe 8. (6+2+2 Punkte)

(a) Bestimmen Sie $u, v \in \mathbb{Z}$ mit $1007u + 561v = 1$.

(b) Bestimmen Sie die Lösungsmenge des Kongruenzsystems

$$x \equiv 0 \bmod 1007\ ,\ \ x \equiv 1 \bmod 561.$$

(c) Bestimmen Sie die Lösungsmenge des Kongruenzsystems

$$x \equiv 1 \bmod 1007\ ,\ \ x \equiv 1 \bmod 561.$$

Geben Sie jeweils entweder einen Rechenweg oder eine kurze Begründung für Ihr Ergebnis an. (Es ist $1007 \cdot 561 = 564927$.)

Lösungsskizze:

zu (a) Der euklidische Algorithmus liefert $u = 200$, $v = -359$.

zu (b) $1007u + 561v = 1 \Rightarrow 1007u = 1 - 561v$

$\Rightarrow 1007u = 201400$ ist Lösung

$\Rightarrow \mathcal{L} = 201400 + 564927\mathbb{Z}$

zu (c) $\mathcal{L} = 1 + 564927\mathbb{Z}$