LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2018/19
14.02.2019

Zahlentheorie

(Lehramt Gymnasium)

Klausur

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									

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. (3+2+2+3 Punkte)

Wir betrachten den Ring $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mit der komponentenweisen Addition und Multiplikation.

(a) Ist R ein Körper? Ist R ein Integritätsbereich? Bitte begründen Sie Ihre Antworten.

(b) Geben Sie alle Einheiten von R an (ohne Nachweis).

(c) Geben Sie einen Teilring $S \subsetneq R$ von R an. Auch hier ist kein Nachweis erforderlich.

(d) Zeigen Sie, dass die Abbildung $\phi : R \to R$, $(\bar{a}, \bar{b}) \mapsto (\bar{b}, \bar{a})$ ein Ringautomorphismus ist.

Lösung:

zu (a) Das Element $(\bar{1}, \bar{0})$ ist ein von Null verschiedener Nullteiler in R, denn es gilt $(\bar{0}, \bar{1}) \cdot (\bar{1}, \bar{0}) = (\bar{0} \cdot \bar{1}, \bar{1} \cdot \bar{0}) = (\bar{0}, \bar{0}) = 0_R$ und $(\bar{0}, \bar{1}) \neq 0_R$. Dies zeigt, dass R kein Integritätsbereich ist. Erst recht ist R kein Körper (da laut Vorlesung alle Körper auch Integritätsbereiche sind).

zu (b) Die einzige Einheit in R ist das Element $1_R = (\bar{1}, \bar{1})$. (Wie man leicht überprüft, sind die anderen drei Elemente $(\bar{0}, \bar{0})$, $(\bar{1}, \bar{0})$ und $(\bar{0}, \bar{1})$ Nullteiler in R, und laut Vorlesung kann ein Ringelement nicht zugleich Einheit und Nullteiler sein. Das Einselement ist dagegen in jedem Ring eine Einheit.)

zu (c) $S = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$. (Jeder Teilring von R muss zumindest 1_R und auf Grund der Abgeschlossenheit unter Subtraktion auch $1_R - 1_R = 0_R$ enthalten.)

zu (d) Um zu zeigen, dass ϕ ein *Endomorphismus* von R ist, müssen wir $\phi(1_R) = 1_R$ sowie $\phi(\alpha+\beta) = \phi(\alpha)+\phi(\beta)$ und $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ für alle $\alpha, \beta \in R$ überprüfen. Nach Definition von ϕ gilt $\phi(1_R) = \phi((\bar{1}, \bar{1})) = (\bar{1}, \bar{1}) = 1_R$. Seien nun $\alpha, \beta \in R$ vorgegeben, $\alpha = (\bar{a}, \bar{b})$, $\beta = (\bar{c}, \bar{d})$ mit $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}/2\mathbb{Z}$. Dann gilt

$$\begin{aligned} \phi(\alpha + \beta) &= \phi((\bar{a}, \bar{b}) + (\bar{c}, \bar{d})) = \phi(\bar{a} + \bar{c}, \bar{b} + \bar{d}) = (\bar{b} + \bar{d}, \bar{a} + \bar{c}) \\ &= (\bar{b}, \bar{a}) + (\bar{d}, \bar{c}) = \phi((\bar{a}, \bar{b})) + \phi((\bar{c}, \bar{d})) = \phi(\alpha) + \phi(\beta) \end{aligned}$$

und

$$\begin{aligned} \phi(\alpha\beta) &= \phi((\bar{a}, \bar{b}) \cdot (\bar{c}, \bar{d})) = \phi(\bar{a}\bar{c}, \bar{b}\bar{d}) = (\bar{b}\bar{d}, \bar{a}\bar{c}) \\ &= (\bar{b}, \bar{a}) \cdot (\bar{d}, \bar{c}) = \phi((\bar{a}, \bar{b})) \cdot \phi((\bar{c}, \bar{d})) = \phi(\alpha)\phi(\beta). \end{aligned}$$

Für jedes $\alpha \in R$, $\alpha = (\bar{a}, \bar{b})$ mit $\bar{a}, \bar{b} \in \mathbb{Z}$ gilt auch

$$(\phi \circ \phi)((\bar{a}, \bar{b})) = \phi(\phi(\bar{a}, \bar{b})) = \phi(\bar{b}, \bar{a}) = (\bar{a}, \bar{b}) = \mathrm{id}_R(\bar{a}, \bar{b})$$

und somit $\phi \circ \phi = \mathrm{id}_R$. Dies zeigt, dass die Abbildung ϕ mit ihrer eigenen Umkehrabbildung übereinstimmt. Also ist ϕ auch bijektiv, insgesamt ein Automorphismus von R.

Name: _____

Aufgabe 2. (6+4 Punkte)

(a) Zeigen Sie, dass die Teilmenge $R \subseteq \mathbb{R}$ gegeben durch

$$R \quad = \quad \left\{ \frac{a}{6^n} \;\middle|\; a \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$$

ein Teilring von $\mathbb{R}$ ist.

(b) Beweisen Sie die Gleichung $R = \mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$.

Lösung:

zu (a) Zunächst gilt $1 \in R$, denn setzen wir $a = 1$ und $n = 0$, dann gilt $a \in \mathbb{Z}$, $n \in \mathbb{N}_0$ und $1 = \frac{a}{6^n}$. Seien nun $\alpha, \beta \in R$ vorgegeben. Zu zeigen ist $\alpha - \beta \in R$ und $\alpha\beta \in R$. Wegen $\alpha, \beta \in R$ gibt es $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}_0$ mit $\alpha = \frac{a}{6^m}$ und $\beta = \frac{b}{6^n}$. Dann liegt das Element

$$\alpha + \beta \quad = \quad \frac{a}{6^m} + \frac{b}{6^n} \quad = \quad \frac{6^n a + 6^m b}{6^{m+n}}$$

in R wegen $6^n a + 6^m b \in \mathbb{Z}$ und $m + n \in \mathbb{N}_0$. Ebenso gilt $\alpha\beta = \frac{a}{6^m} \cdot \frac{b}{6^n} = \frac{ab}{6^{m+n}} \in R$ wegen $ab \in \mathbb{Z}$ und $m + n \in \mathbb{N}_0$.

zu (b) (Zu überprüfen sind die charakteristischen Eigenschaften des Rings $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$, wie sie in Satz (3.4) der Vorlesung angegeben sind.) Aus Teil (a) wissen wir bereits, dass R ein Teilring von $\mathbb{R}$ ist. Wir überprüfen nun $\mathbb{Z} \cup \{\frac{1}{2}, \frac{1}{3}\} \subseteq \mathbb{R}$. Für jedes $a \in \mathbb{Z}$ gilt $a = \frac{a}{6^0} \in R$ (nach Definition von R, wegen $a \in \mathbb{Z}$ und $0 \in \mathbb{N}_0$). Außerdem gilt $\frac{1}{2} = \frac{3}{6^1} \in R$ und $\frac{1}{3} = \frac{2}{6^1} \in R$.

Sei nun S ein weiterer Teilring von $\mathbb{R}$ mit $S \supseteq \mathbb{Z} \cup \{\frac{1}{2}, \frac{1}{3}\}$. Zu zeigen ist $S \supseteq R$. Sei dazu $\alpha \in R$ vorgegeben, $\alpha = \frac{a}{6^n}$ mit $a \in \mathbb{Z}$ und $n \in \mathbb{N}_0$. Wegen $\mathbb{Z} \subseteq S$ gilt $a \in S$. Mit $\frac{1}{2}$ und $\frac{1}{3}$ ist auch $\frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$ in S enthalten, auf Grund der Abgeschlossenheit von S unter Multiplikation. Damit liegen auch $(\frac{1}{6})^n = \frac{1}{6^n}$ und $a \cdot \frac{1}{6^n} = \frac{a}{6^n} = \alpha$ im Teilring S von $\mathbb{R}$.

Name: _____

Aufgabe 3. (6+4 Punkte)

(a) Bestimmen Sie mit dem Euklidischen Algorithmus $x, y \in \mathbb{Z}$, so dass $64x + 137y = 1$ gilt.

(b) Begründen Sie, dass $\overline{64}$ im Restklassenring $\mathbb{Z}/137\mathbb{Z}$ eine Einheit ist, und bestimmen Sie ein $a \in \mathbb{Z}$ mit $\overline{64}^{-2} = \bar{a}$.

(Hierbei bezeichnet $\bar{c}$ für jedes $c \in \mathbb{Z}$ jeweils das Bild von c unter dem kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{Z}/137\mathbb{Z}$, $c \mapsto c + 137\mathbb{Z}$.)

Lösung:

zu (a) Durch Anwendung des Euklidischen Algorithmus erhalten wir die Tabelle

q	a_n	x_n	y_n
–	137	1	0
–	64	0	1
2	9	1	-2
7	1	-7	15
9	0	–	–

Es gilt also $\mathrm{ggT}(137, 64) = 1$, und die Gleichung $64x + 137y = 1$ wird durch $x = 15$ und $y = -7$ gelöst.

zu (b) Nach Teil (a) gilt $64 \cdot 15 + 137 \cdot (-7) = 1$, im Restklassenring $\mathbb{Z}/137\mathbb{Z}$ also $\overline{64} \cdot \overline{15} + \overline{137} \cdot \overline{-7} = \bar{1}$. Wegen $\overline{137} = \bar{0}$ folgt $\overline{64} \cdot \overline{15} = \bar{1}$. Dies zeigt, dass das Element $\overline{64}$ im Ring $\mathbb{Z}/137\mathbb{Z}$ invertierbar ist und $\overline{64}^{-1} = \overline{15}$ gilt. (Alternativ kann die Invertierbarkeit des Elements auch mit dem Ergebnis $\mathrm{ggT}(137, 64) = 1$ begründet werden aus Teil (a) begründet werden.) Aus der Gleichung $\overline{64}^{-1} = \overline{15}$ wiederum folgt

$$\overline{64}^{-2} \quad = \quad (\overline{64}^{-1})^2 \quad = \quad \overline{15}^2 \quad = \quad \overline{15} \cdot \overline{15} \quad = \quad \overline{225} \quad = \quad \overline{88}$$

wobei im letzten Schritt $225 = 137 + 88 \equiv 88 \mod 137$ verwendet wurde. Die Gleichung $\overline{64}^{-2} = \bar{a}$ wird also durch $a = 88$ erfüllt.

Name: _____

Aufgabe 4. (2+4+4 Punkte)

(a) Begründen Sie, dass $x^2 + 2$ ein irreduzibles Element im Polynomring $\mathbb{Q}[x]$ ist.

(b) Zeigen Sie mit Hilfe geeigneter Sätze aus der Vorlesung, dass es sich bei dem Faktorring $R = \mathbb{Q}[x]/(x^2 + 2)$ um einen Körper handelt.

(c) Sei $\alpha = x + (x^2 + 2) \in R$. Bestimmen Sie ein $c \in \mathbb{Z}$, so dass die Gleichung $\alpha^6 = c + (x^2 + 2)$ in R erfüllt ist (mit Nachweis).

Lösung:

zu (a) Wäre das Polynom x^2+2 über $\mathbb{Q}[x]$ reduzibel, dann müsste es wegen $\text{grad}(x^2+2)$ in zwei Linearfaktoren zerfallen. Dies würde bedeuten, dass die beiden Nullstellen von x^2+2 in $\mathbb{Q}$ liegen. Aber die Nullstellen $\pm i\sqrt{2}$ des Polynoms sind nicht in $\mathbb{R}$, erst recht nicht in $\mathbb{Q}$ enthalten. (Alternativ könnte man hier das Eisenstein-Kriterium verwenden.)

zu (b) Laut Vorlesung ist $\mathbb{Q}[x]$ als Polynomring über einem Körper ein Hauptidealring. In einem solchen Ring ist für jedes irreduzible Element $a \in R$ das Hauptideal (a) maximal. Also ist nach Teil (a) das Ideal $(x^2 + 2)$ in $\mathbb{Q}[x]$ ein maximales Ideal. Daraus folgt laut Vorlesung, dass der Faktorring $R = \mathbb{Q}[x]/(x^2 + 2)$ ein Körper ist.

zu (c) Wegen $x^2+2 \in (x^2+2)$ gilt in R die Gleichung $(x^2+(x^2+2))+(2+(x^2+2)) = x^2+2+(x^2+2) = 0+(x^2+2)$, was zu $x^2+(x^2+2) = (-2)+(x^2+2)$ umgestellt werden kann. Es folgt $\alpha^2 = \alpha \cdot \alpha = (x+(x^2+2))(x+(x^2+2)) = x^2 + (x^2 + 2) = -2 + (x^2 + 2)$. Daraus wiederum folgt $\alpha^6 = (\alpha^2)^3 = ((-2) + (x^2 + 2))^3 = (-2)^3 + (x^2 + 2) = (-8) + (x^2 + 2)$. Also ist $c = -8$ eine ganze Zahl mit der gewünschten Eigenschaft.

Name: _____

Aufgabe 5. (6+4 Punkte)

(a) Bestimmen Sie ein $r \in \mathbb{N}$ und zyklische Gruppen $C_1, ..., C_r$, so dass die prime Restklassengruppe $(\mathbb{Z}/48\mathbb{Z})^\times$ zu $C_1 \times ... \times C_r$ isomorph ist. Geben Sie dabei an, durch welche Sätze aus der Vorlesung die Isomorphie gewährleistet ist.

(b) Ist $(\mathbb{Z}/48\mathbb{Z})^\times$ selbst zyklisch? Bitte begründen Sie Ihre Antwort.

Lösung:

zu (a) Weil die Faktoren 16 und 3 in der Zerlegung $48 = 16 \cdot 3$ teilerfremd sind, kann der Chinesische Restsatz angwendet werden und liefert $(\mathbb{Z}/48\mathbb{Z})^\times \cong (\mathbb{Z}/16\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$. Für jede ungerade Primzahl p gilt laut Vorlesung $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, also insbesondere $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. Für alle $r \in \mathbb{N}$ mit $r \geq 3$ gilt außerdem $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$. Wenden wir dies auf $r = 4$ an, so erhalten wir $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Insgesamt gilt also $(\mathbb{Z}/48\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Setzen wir also $r = 3$, $C_1 = C_2 = \mathbb{Z}/2\mathbb{Z}$ und $C_3 = \mathbb{Z}/4\mathbb{Z}$, dann ist $(\mathbb{Z}/48\mathbb{Z})^\times \cong C_1 \times C_2 \times C_3$ erfüllt.

zu (b) Wäre $(\mathbb{Z}/48\mathbb{Z})^\times$ zyklisch, dann müsste dies auch für die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ mit $2 \cdot 2 \cdot 4 = 16$ Elementen gelten. Es gäbe in dieser Gruppe also ein Element der Ordnung 16. Aber für alle Gruppenelemente $(\bar{a}, \bar{b}, \bar{c})$ mit $\bar{a}, \bar{b} \in \mathbb{Z}/2\mathbb{Z}$ und $\bar{c} \in \mathbb{Z}/4\mathbb{Z}$ gilt $4 \cdot (\bar{a}, \bar{b}, \bar{c}) = (\overline{4a}, \overline{4b}, \overline{4c}) = (\bar{0}, \bar{0}, \bar{0})$. Die Ordnung jedes Elements ist also ein Teiler von 4 und damit ungleich 16. Dies zeigt, dass weder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ noch $(\mathbb{Z}/48\mathbb{Z})^\times$ zyklisch ist.

Name: _____

Aufgabe 6. (2+4+4 Punkte)

(a) Geben Sie die Definitionen der Begriffe „Primideal“ und „maximales Ideal“ an.

(b) Zeigen Sie direkt anhand der Definition, dass im Ring $R = \mathbb{Z}[i]$ der Gaußschen Zahlen das Hauptideal (5) kein Primideal ist.

(c) Begründen Sie (unter anderem mit Hilfe geeigneter Sätze), dass das Hauptideal (3) in R ein Primideal ist.

Lösung:

zu (a) Sei R ein Ring und I ein Ideal in R. Man nennt I ein *Primideal*, wenn $I \neq (1)$ gilt und für alle $a, b \in R$ mit $ab \in I$ jeweils $a \in I$ oder $b \in I$ erfüllt ist. Ein Ideal I wird *maximales Ideal* genannt, wenn $I \neq (1)$ gilt und kein Ideal J mit $I \subsetneq J \subsetneq (1)$ existiert.

zu (b) Setzen wir $\alpha = 2 + i$ und $\beta = 2 - i$, dann gilt $\alpha\beta = (2 + i)(2 - i) = 5 \in (5)$. Wäre (5) ein Primideal, dann müsste $\alpha \in (5)$ oder $\beta \in (5)$ gelten. Betrachten wir zunächst den Fall $\alpha \in (5)$. Dann gibt es ein $\gamma \in R$ mit $\alpha = 5\gamma$, $\gamma = c + di$ mit $c, d \in \mathbb{Z}$. Es folgt $2 + i = 5(c + di) = 5c + 5di$, und der Vergleich von Real- und Imaginärteil liefert $2 = 5c$ und $1 = 5d$, also $c = \frac{2}{5}$ und $d = \frac{1}{5}$, im Widerspruch zu $c, d \in \mathbb{Z}$. Also ist $\alpha \in (5)$ ausgeschlossen. Nehmen wir nun $\beta = 2 - i \in (5)$ an. Dann gibt es $c, d \in \mathbb{Z}$ mit $\beta = 5(c + id)$, was zu $2 = 5c$ und $-1 = 5d$ führt, also $c = \frac{2}{5}$ und $d = -\frac{1}{5}$, im Widerspruch zu $c, d \in \mathbb{Z}$. Es gilt also weder $\alpha \in (5)$ noch $\beta \in (5)$. Dies zeigt, dass (5) kein Primideal ist.

zu (c) Wir zeigen zunächst, dass 3 in R irreduzibel ist. Laut Vorlesung ist dies der Fall, wenn $N(3)$ Quadrat einer Primzahl p und die Gleichung $a^2 + b^2 = p$ mit $a, b \in \mathbb{Z}$ nicht lösbar ist. Tatsächlich gilt $N(3) = 9 = 3^2$, und $a^2 + b^2 = 3$ besitzt keine ganzzahlige Lösung. Denn aus $b^2 \leq 3$ folgt $|b| \leq 1$, also $b \in \{-1, 0, 1\}$ und somit $b^2 \in \{0, 1\}$; aber keine der Gleichungen $a^2 + 1 = 3$ oder $a^2 + 0 = 3$ ist mit $a \in \mathbb{Z}$ lösbar.

Laut Vorlesung ist $R = \mathbb{Z}[i]$ ein euklidischer Ring, damit insbesondere faktoriell und ein Integritätsbereich. In einem faktoriellen Ring sind die irreduziblen Elemente genau die Primelemente, also ist 3 in R ein Primelement. Daraüber hinaus ist bekannt, dass in jedem Integritätsbereich das Hauptideal eines Primelements ein Primideal ist. Dies zeigt, dass (3) in R ein Primideal ist.

Name: _____

Aufgabe 7. (2+4+4 Punkte)

(a) Formulieren Sie den Chinesischen Restsatz für beliebige Ringe.

(b) Weisen Sie nach, dass die Ideale $I = (3)$ und $J = (2 + i)$ im $R = \mathbb{Z}[i]$ teilerfremd sind. *Hinweis:* Eventuell sind die Gleichungen $(-3) \cdot 3 + 2 \cdot 5 = 1$ und $5 = (2 - i)(2 + i)$ dabei hilfreich.

(c) Bestimmen Sie ein $\alpha \in R$ mit $\alpha \equiv 2 \mod I$ und $\alpha \equiv 3 \mod J$.

Lösung:

zu (a) Sei R ein Ring, $r \in \mathbb{N}$ mit $r \geq 2$, und seien $I_1, ..., I_r$ paarweise teilerfremde Ideale in R. Sei $I = I_1 \cdot ... \cdot I_r$. Dann gibt es einen Isomorphismus $\bar{\phi} : R/I \to R/I_1 \times ... \times R/I_r$ mit $\bar{\phi}(a + I) = (a + I_1, ..., a + I_r)$ für alle $a \in R$.

zu (b) Es gilt $-9 = (-3) \cdot 3 \in (3)$ und $10 = 2 \cdot 5 = 2 \cdot (2 - i) \cdot (2 + i) \in (2 + i)$, also $-9 \in I$ und $10 \in J$. Daraus folgt $1 = (-9) + 10 \in I + J$ und damit $I + J = (1)$. Diese Gleichung wiederum bedeutet nach Definition, dass I und J teilerfremd sind.

zu (c) Die Gleichung $1 = (-9) + 10$ kann zu $1 + 9 = 10$ umgestellt werden. Wegen $9 \in I$ und $10 \in J$ zeigt die Gleichung, dass $10 \equiv 1 \mod I$ und $10 \equiv 0 \mod J$ gilt. Ebenso gilt $1 + (-10) = -9$. Wegen $-9 \in I$ und $-10 \in J$ zeigt dies $-9 \equiv 0 \mod I$ und $-9 \equiv 1 \mod J$. Setzen wir nun $\alpha = 2 \cdot 10 + 3 \cdot (-9) = 20 - 27 = -7$, dann gilt $\alpha \equiv 2 \cdot 1 + 3 \cdot 0 \equiv 2 \mod I$ und $\alpha \equiv 2 \cdot 0 + 3 \cdot 1 \equiv 3 \mod J$.

Name: _____

Aufgabe 8. (2+3+5 Punkte)

(a) Wie sind in einem Integritätsbereich R die *irreduziblen Elemente* und die *Primelemente* definiert?

(b) Begründen Sie: Sind p und q Primelemente in einem Integritätsbereich R, dann ist das Element pq kein Primelement.

(c) Stellen Sie das Element 100 im Ring $R = \mathbb{Z}[i]$ der Gaußschen Zahlen als Produkt von Primelementen dar, und weisen Sie nach, dass es sich bei den Faktoren tatsächlich um Primelemente des Rings R handelt.

Lösung:

zu (a) Ein Element $p \in R$ heißt *irreduzibel*, wenn $p \neq 0$ und $p \notin R^\times$ gilt, und wenn für alle $a, b \in R$ mit $p = ab$ jeweils $a \in R^\times$ oder $b \in R^\times$ gilt. Man nennt $p \in R$ ein *Primelement*, wenn $p \neq 0$, $p \notin R^\times$ gilt, und wenn für alle $a, b \in R$ aus $p \mid (ab)$ jeweils $p \mid a$ oder $p \mid b$ folgt.

zu (b) Seien $p, q \in R$ Primelemente, und nehmen wir an, dass auch pq ein Primelement ist. Dann wäre pq insbesondere irreduzibel (denn in einem Integritätsbereich sind Primelemente immer irreduzibel). Daraus wiederum würde $p \in R^\times$ oder $q \in R^\times$ folgen. Aber als Primelement kann weder p noch q eine Einheit in R sein.

zu (c) Es gilt $100 = 2^2 \cdot 5^2 = (1+i)^2(1-i)^2(2+i)^2(2-i)^2$. Bezeichnen wir mit N die Normfunktion auf R gegeben durch $R \to \mathbb{N}_0$, $\alpha \mapsto \alpha\bar{\alpha}$, dann gilt $N(1+i) = N(1-i) = 2$ und $N(2+i) = N(2-i) = 5$. Laut Vorlesung ist ein Element in einem Ring der Form $\mathbb{Z}[\sqrt{-d}]$ mit $d \in \mathbb{N}$, dessen Norm eine Primzahl ist, ein irreduzibles Element. Also sind $1 \pm i$ und $2 \pm i$ irreduzible Elemente in $\mathbb{Z}[i]$. Außerdem ist $\mathbb{Z}[i]$ laut Vorlesung euklidisch und damit auch faktoriell, und in einem solchen Ring sind die irreduziblen Elemente genau die Primelemente. Dies zeigt, dass die Faktoren $1 \pm i$ und $2 \pm i$ in der Zerlegung von oben alles Primelemente in $\mathbb{Z}[i]$ sind.