LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2016/17
24.2.2017

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	$\sum$
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. (2+8 Punkte)

(a) Geben Sie die Definition eines Integritätsbereichs an. Was ist über die Charakteristik eines Integritätsbereichs bekannt?

(b) Geben Sie für die folgenden Ringe jeweils die Menge der Einheiten und die Menge der Nullteiler an. Eine Begründung ist hier *nicht* erforderlich.

$$\mathbb{Z}/2\mathbb{Z} \quad , \quad \mathbb{Z}/6\mathbb{Z} \quad , \quad \mathbb{Z}[i] \quad , \quad \mathbb{Q}[x]$$

Lösung:

zu (a) Ein Integritätsbereich ist ein Ring, in dem das Nullelement der einzige Nullteiler ist.

zu (b) Die Ring $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}[i]$ und $\mathbb{Q}[x]$ sind Integritätsbereiche, deshalb ist hier das Nullelement jeweils der einzige Nullteiler. Die Nullteiler in $\mathbb{Z}/6\mathbb{Z}$ sind die Elemente $\bar{0}$, $\bar{2}$, $\bar{3}$ und $\bar{4}$. Die Einheitengruppen der Ringe sind gegeben durch

$$(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\} \quad , \quad (\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\} \quad , \quad (\mathbb{Z}[i])^\times = \{\pm 1, \pm i\} \quad \text{und} \quad (\mathbb{Q}[x])^\times = \mathbb{Q}^\times = \{a \in \mathbb{Q} \mid a \neq 0\}.$$

Name: _____

Aufgabe 2. (3+7 Punkte)

(a) Sei $\tilde{R}|R$ eine Ringerweiterung und $A \subseteq \tilde{R}$ eine beliebige Teilmenge. Welche Bedingungen muss ein Teilring S von $\tilde{R}$ nach Definition erfüllen, damit er mit dem von A über R erzeugten Teilring $R[A]$ übereinstimmt?

(b) Beweisen Sie die Gleichung

$$\mathbb{Z}[\sqrt{3},\sqrt{7}] \quad = \quad \{a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21} \mid a, b, c, d \in \mathbb{Z}\}.$$

Dabei darf ohne Beweis verwendet werden, dass die Menge auf der rechten Seite der Gleichung (die wir mit S bezeichnen) ein Teilring des Körpers $\mathbb{R}$ der reellen Zahlen ist.

Lösung:

zu (a) Es muss $S \supseteq R \cup A$ gelten, und für jeden Teilring T von $\tilde{R}$ mit $T \supseteq R \cup A$ muss $T \supseteq S$ gelten.

zu (b) Wir überprüfen die beiden in Teil (a) genannten Punkte für $R = \mathbb{Z}$, $\tilde{R} = \mathbb{R}$ und $A = \{\sqrt{3}, \sqrt{7}\}$. Jedes $a \in \mathbb{Z}$ ist wegen $a = a+0\cdot\sqrt{3}+0\cdot\sqrt{7}+0\cdot\sqrt{21}$ in S enthalten. Außerdem gilt $\sqrt{3} = 0+1\cdot\sqrt{3}+0\cdot\sqrt{7}+0\cdot\sqrt{21} \in S$ und $\sqrt{3} = 0 + 1 \cdot \sqrt{3} + 0 \cdot \sqrt{7} + 0 \cdot \sqrt{21} \in S$. Insgesamt ist damit $S \supseteq \mathbb{Z} \cup \{\sqrt{3}, \sqrt{7}\}$ erfüllt.

Sei nun T ein beliebiger Teilring von $\mathbb{R}$ mit $T \supseteq \mathbb{Z} \cup \{\sqrt{3}, \sqrt{7}\}$. Zu zeigen ist $T \supseteq S$. Sei dazu $\alpha \in S$ vorgegeben. Nach Definition von S gibt es $a, b, c, d \in S$ mit $\alpha = a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21}$. Wegen $T \supseteq \mathbb{Z}$ gilt $a, b, c, d \in T$, wegen $T \supseteq \{\sqrt{3}, \sqrt{7}\}$ auch $\sqrt{3}, \sqrt{7} \in T$. Weil T als Teilring von $\mathbb{R}$ unter Multiplikation abgeschlossen ist, folgt $\sqrt{21} = \sqrt{3} \cdot \sqrt{7} \in T$ und $b\sqrt{3}, c\sqrt{7}, d\sqrt{21} \in T$. Weil T auch abgeschlossen unter Addition ist, folgt $\alpha = a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21} \in T$. Damit ist $S \subseteq T$ nachgewiesen.

Name: _____

Aufgabe 3. (3+7 Punkte)

Sei $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ der Ring der Gaußschen Zahlen und $\mathfrak{p} = (1 + i)$ das von $1 + i$ erzeugte Hauptideal.

(a) Zeigen Sie, dass im Faktorring $R/\mathfrak{p}$ die Gleichungen $2 + \mathfrak{p} = 0 + \mathfrak{p}$ und $1 + \mathfrak{p} = i + \mathfrak{p}$ erfüllt sind, und dass $0 + \mathfrak{p} \neq 1 + \mathfrak{p}$ gilt.

(b) Beweisen Sie mit Hilfe des Homomorphiesatzes, dass ein Isomorphismus $\mathbb{Z}/2\mathbb{Z} \cong R/\mathfrak{p}$ von Ringen existiert. Dabei darf ohne Beweis verwendet werden, dass durch $\phi : \mathbb{Z} \to R/\mathfrak{p}$, $a \mapsto a + \mathfrak{p}$ ein Ringhomomorphismus gegeben ist.

Lösung:

zu (a) Die Gleichung $2 + \mathfrak{p} = 0 + \mathfrak{p}$ ist äquivalent zu $2 = 2 - 0 \in \mathfrak{p}$. Dies ist erfüllt, denn wegen $2 = (1 - i)(1 + i)$ ist 2 ein Vielfaches von $1 + i$, liegt also im von $1 + i$ erzeugten Hauptideal $\mathfrak{p} = (1 + i)$. Ebenso ist $1 + \mathfrak{p} = i + \mathfrak{p}$ äquivalent zu $1 - i \in \mathfrak{p}$. Wegen $1 - i = (-i)(1 + i)$ ist $1 - i$ ein Vielfaches von $1 + i$, also gilt tatsächlich $1 - i \in \mathfrak{p}$.

Würde $0 + \mathfrak{p} = 1 + \mathfrak{p}$ gelten, dann wäre $1 = 1 - 0 \in \mathfrak{p}$, also 1 ein Vielfaches von $1 + i$. Es gäbe also ein $\alpha = a + ib \in \mathbb{Z}[i]$ mit $a, b \in \mathbb{Z}$, so dass $1 = \alpha(1 + i) = (a + ib)(1 + i) = a + ib + ia + i^2 b = (a - b) + i(a + b)$ gilt. Der Vergleich von Real- und Imaginärteil liefert $a + b = 0$ und $a - b = 1$, also $b = -a$ und $1 = a - (-a) = 2a$ im Widerspruch dazu, dass 1 ungerade ist.

zu (b) Um den Homomorphiesatz anwenden zu können, müssen wir nachweisen, dass ϕ surjektiv ist und $\ker(\phi) = 2\mathbb{Z}$ gilt. Zum Nachweis der Surjektivität sei $\alpha + \mathfrak{p} \in R/\mathfrak{p}$ vorgegeben, wobei $\alpha = a + ib \in R$ mit $a, b \in \mathbb{Z}$ ist. Nach Teil (a) gilt $1 + \mathfrak{p} = i + \mathfrak{p}$. Daraus folgt

$$\begin{aligned} \phi(a + b) &= \phi(a) + \phi(b) = (a + \mathfrak{p}) + (b + \mathfrak{p}) = (a + \mathfrak{p}) + (1 + \mathfrak{p})(b + \mathfrak{p}) = \\ (a + \mathfrak{p}) + (i + \mathfrak{p})(b + \mathfrak{p}) &= (a + \mathfrak{p}) + (ib + \mathfrak{p}) = (a + ib) + \mathfrak{p} = \alpha + \mathfrak{p}. \end{aligned}$$

Nun zeigen wir, dass $\ker(\phi) = 2\mathbb{Z}$ gilt. Wegen Teil (a) gilt $\phi(2) = 2 + \mathfrak{p} = 0 + \mathfrak{p}$ und $2 \in \ker(\phi)$. Weil $\ker(\phi)$ ein Ideal in $\mathbb{Z}$ ist, folgt $2\mathbb{Z} = (2) \subseteq \ker(\phi)$. Da es sich bei $\mathbb{Z}$ um einen Hauptidealring handelt, gilt $\ker(\phi) = (d)$ für ein $d \in \mathbb{Z}$, und wegen $(2) \subseteq \ker(\phi) = (d)$ muss d ein Teiler von 2 sein. Es ist also nur $d \in \{\pm 1, \pm 2\}$ möglich. Wäre $d \in \{\pm 1\}$, dann würde $1 \in \ker(\phi)$, also $1 + \mathfrak{p} = \phi(1) = 0 + \mathfrak{p}$ folgen, was dem Ergebnis aus Teil (a) widerspricht. Also gilt $d \in \{\pm 2\}$, und daraus folgt $\ker(\phi) = (d) = 2\mathbb{Z}$.

Name: _____

Aufgabe 4. (6+4 Punkte)

Sei $R = \mathbb{Q}[x]$ der Polynomring über $\mathbb{Q}$ und $\mathfrak{p} = \{f \in \mathbb{Q}[x] \mid f(\sqrt{3}) = 0\}$.

(a) Weisen Sie nach, dass $\mathfrak{p}$ ein Ideal in R ist.

(b) Zeigen Sie, dass $\mathfrak{p}$ darüber hinaus ein Primideal ist.

Lösung:

zu (a) Sei $0_{\mathbb{Q}[x]} \in \mathbb{Q}[x]$ das Nullpolynom. Wegen $0_{\mathbb{Q}[x]}(\sqrt{3}) = 0$ gilt $0_{\mathbb{Q}[x]} \in \mathfrak{p}$. Seien nun $f, g \in \mathfrak{p}$ und $r \in \mathbb{Q}[x]$ vorgegeben. Wegen $f, g \in \mathfrak{p}$ gilt $f(\sqrt{3}) = 0$ und $g(\sqrt{3}) = 0$. Daraus folgt $(f+g)(\sqrt{3}) = f(\sqrt{3})+g(\sqrt{3}) = 0+0 = 0$ und somit $f + g \in \mathfrak{p}$. Ebenso gilt $(rf)(\sqrt{3}) = r(\sqrt{3}) \cdot f(\sqrt{3}) = r(\sqrt{3}) \cdot 0 = 0$ und somit $rf \in \mathfrak{p}$.

zu (b) Sei $1_{\mathbb{Q}[x]} \in Q[x]$ das konstante Polynom zum Wert 1. Wäre $\mathfrak{p}$ das Einheitsideal, dann würde insbesondere $1_{\mathbb{Q}[x]} \in \mathfrak{p}$ gelten. Aber dann wäre $1_{\mathbb{Q}[x]}(\sqrt{3}) = 0$, was wegen $1_{\mathbb{Q}[x]}(\sqrt{3}) = 1$ offensichtlich nicht der Fall ist. Wir müssen noch überprüfen, dass für vorgegebene $f, g \in \mathbb{Q}[x]$ aus $fg \in \mathfrak{p}$ jeweils $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$ folgt. Wegen $fg \in \mathfrak{p}$ ist $f(\sqrt{3})g(\sqrt{3}) = (fg)(\sqrt{3}) = 0$. Weil das Produkt zweier reeller Zahlen nur dann Null ist, wenn einer der Faktoren Null ist, folgt $f(\sqrt{3}) = 0$ oder $g(\sqrt{3}) = 0$ und somit $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$.

Name: _____

Aufgabe 5. (2+8 Punkte)

(a) Geben Sie den Chinesischen Restsatz an.

(b) Bestimmen Sie ein $a \in \mathbb{Z}$ mit $a \equiv 2 \mod 41$ und $a \equiv 3 \mod 43$.

Lösung:

zu (a) Sei R ein Ring, $I_1, ..., I_m$ paarweise teilerfremde Ideale in R und $I = I_1 \cdot ... \cdot I_m$. Dann gibt es einen eindeutig bestimmten Isomorphismus $\phi : R/I \to (R/I_1) \times ... \times (R/I_m)$ mit $\phi(r+i) = (r+I_1, ..., r+I_m)$ für alle $r \in R$.

zu (b) Die Anwendung des Euklidischen Algorithmus auf den Ring $R = \mathbb{Z}$ und die Elemente $41, 43 \in \mathbb{Z}$ liefert

q	a_n	x_n	y_n
–	43	1	0
–	41	0	1
1	2	1	-1
20	1	-20	21
2	0	–	––

An der vorletzten Zeile kann $\mathrm{ggT}(41, 43) = 1$ und $21 \cdot 41 + (-20) \cdot 43 = 1$ abgelesen werden. Sei ϕ der Homomorphismus von $\mathbb{Z}/(41 \cdot 43)\mathbb{Z} = \mathbb{Z}/1763\mathbb{Z}$ nach $\mathbb{Z}/41\mathbb{Z} \times \mathbb{Z}/43\mathbb{Z}$ gegeben durch $\phi(a + \mathbb{Z}/1763\mathbb{Z}) = (a + 41\mathbb{Z}, a + 43\mathbb{Z})$ für alle $a \in \mathbb{Z}$. Die Gleichung $1 + (-21) \cdot 41 = (-20) \cdot 43 = -860$ zeigt $\phi(-860 + 1763\mathbb{Z}) = (1 + 41\mathbb{Z}, 0 + 43\mathbb{Z})$, und die Gleichung $1 + 20 \cdot 43 = 21 \cdot 41 = 861$ liefert $\phi(861 + 1763\mathbb{Z}) = (0 + 41\mathbb{Z}, 1 + 43\mathbb{Z})$. Folglich wird das Element $2 \cdot (-860) + 3 \cdot 861 + 1763\mathbb{Z} = 863 + 1763\mathbb{Z}$ auf $(2 + 41\mathbb{Z}, 3 + 43\mathbb{Z})$ abgebildet. Also ist $a = 863$ eine ganze Zahl mit $a \equiv 2 \mod 41$ und $a \equiv 3 \mod 43$.

Name: _____

Aufgabe 6. (3+7 Punkte)

(a) Entscheiden Sie, ob die Zahl 2 eine Primitivwurzel modulo 7 ist, und begründen Sie Ihre Entscheidung.

(b) Geben Sie ein $r \in \mathbb{N}$ und endliche zyklische Gruppen $C_1, ..., C_r$ an, so dass $(\mathbb{Z}/120\mathbb{Z})^\times \cong C_1 \times ... \times C_r$ erfüllt ist.

Lösung:

zu (a) Wäre 2 eine Primitivwurzel modulo 7, dann müsste das Element $\bar{2} \in (\mathbb{Z}/7\mathbb{Z})^\times$ die gesamte Gruppe $(\mathbb{Z}/7\mathbb{Z})^\times$ erzeugen, also von Ordnung $\varphi(7) = 6$ sein. Aber die Gleichung $\bar{2}^3 = \bar{8} = \bar{1}$ zeigt, dass die Ordnung von $\bar{2}$ in $(\mathbb{Z}/7\mathbb{Z})^\times$ höchstens 3 ist.

zu (b) Die Primfaktorzerlegung von 120 ist gegeben durch $2^3 \cdot 3 \cdot 5$. Der Chinesische Restsatz liefert $\mathbb{Z}/120\mathbb{Z} \cong \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, und laut Vorlesung folgt daraus für die Einheitengruppen

$$(\mathbb{Z}/120\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/2^3\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times.$$

Weil 3 und 5 ungerade Primzahlen sind, handelt es sich bei $(\mathbb{Z}/3\mathbb{Z})^\times$ und $(\mathbb{Z}/5\mathbb{Z})^\times$ um zyklische Gruppen, es gilt also $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$. Außerdem gilt laut Vorlesung $(\mathbb{Z}/2^s\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$ für alle $s \geq 3$, also $(\mathbb{Z}/2^3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insgesamt gilt also $(\mathbb{Z}/120\mathbb{Z})^\times \cong C_1 \times ... \times C_r$ mit $r = 4$, $C_1 = C_2 = C_3 = \mathbb{Z}/2\mathbb{Z}$ und $C_4 = \mathbb{Z}/4\mathbb{Z}$.

Name: _____

Aufgabe 7. (2+5+3 Punkte)

Sei $R = \mathbb{Z}[i]$ der Ring der Gaußschen Zahlen.

(a) Begründen Sie mit Hilfe geeigneter Sätze aus der Vorlesung, dass die irreduziblen Elemente in R genau die Primelemente sind.

(b) Untersuchen Sie mit Hilfe der Normfunktion $N : R \to \mathbb{N}_0$, $a + ib \mapsto a^2 + b^2$, welche der folgenden drei Elemente Primelemente in R sind.

$$3 + 2i \quad , \quad 11 \quad , \quad 17$$

(c) Geben Sie eine Zerlegung des Elements $6 + 2i$ in irreduzible Faktoren an, und begründen Sie, dass die angegebenen Faktoren tatsächlich irreduzibel sind.

Hinweis: Ein Element $\alpha \in R$ mit $N(\alpha) = 10$ kann nur Faktoren der Norm $1, 2, 5$ oder 10 besitzen.

Lösung:

zu (a) Laut Vorlesung ist $\mathbb{Z}[i]$ ein euklidischer Ring, und euklidische Ringe sind Hauptidealringe. In der Vorlesung wurde gezeigt, dass in Hauptidealringen die Primelemente genau die irreduziblen Elemente sind (Satz 5.11).

zu (b) Es ist $N(3 + 2i) = 3^2 + 2^2 = 9 + 4 = 13$ eine Primzahl; daraus folgt, dass das Element $3 + 2i$ in R irreduzibel ist. Weiter ist $N(11) = 11^2$ ein Primzahlquadrat, und die Gleichung $a^2+b^2 = 11$ besitzt keine Lösung mit $a, b \in \mathbb{Z}$, wie man durch Einsetzen von $b = 0, 1, 2, 3$ unmittelbar überprüft. Daraus folgt die Irreduzibilität von 11 in R. Die Gleichung $4^2+1^2 = 17$ liefert die Zerlegung $17 = (4+i)(4-i)$. Wegen $N(4+i) = N(4-i) = 17$ sind die Elemente $4 \pm i$ in R beides keine Einheiten. Also ist 17 in R reduzibel.

zu (c) Zunächst können wir $6 + 2i$ in das Produkt $2 \cdot (3 + i) = (1 - i)(1 + i)(3 + i)$ zerlegen. Ist $3 + i = \alpha\beta$ eine Zerlegung in zwei Nicht-Einheiten α, β, dann gilt $N(\alpha)N(\beta) = N(\alpha\beta) = N(3 + i) = 3^2 + 1^2 = 10$ und $N(\alpha), N(\beta) \in \{2, 5\}$. Das Element $1 + i$ hat Norm 2. Wegen

$$\frac{3+i}{1+i} \quad = \quad \frac{(3+i)(1-i)}{(1+i)(1-i)} \quad = \quad \tfrac{1}{2}(3+i-3i+1) \quad = \quad \tfrac{1}{2}(4-2i) \quad = \quad 2-i$$

gilt $3+i = (1+i)(2-i)$ und $6+2i = (1-i)(1+i)(3+i) = (1-i)(1+i)(1+i)(2-i) = (1-i)(1+i)^2(2-i)$. Die Normen $N(1-i) = N(1+i) = 2$ und $N(2-i) = 5$ sind Primzahlen, also sind alle Faktoren in der Zerlegung tatsächlich irreduzibel.

Name: _____

Aufgabe 8. (2+8 Punkte)

(a) Geben Sie die Definition eines faktoriellen Rings an (oder eine Charakterisierung, die zur Definition äquivalent ist).

(b) Sei nun R ein (nicht notwendigerweise faktorieller) Integritätsbereich. Seien $p, q \in R$ Primelemente und $a, b \in R$ zwei weitere Ringelemente. Zeigen Sie: Gilt $pq = ab$, dann ist eines der beiden Elemente a, b eine Einheit oder ein Primelement.

Lösung:

zu (a) Ein faktorieller Ring ist ein Integritätsbereich R mit der Eigenschaft, dass jedes Element in R, dass weder Null noch Einheit ist, als Produkt von Primelementen dargestellt werden kann.

zu (b) Wegen $pq = ab$ gilt $p \mid ab$. Weil p ein Primelement ist, folgt daraus $p \mid a$ oder $p \mid b$. Nach eventueller Vertauschung von a und b können wir $p \mid a$ annehmen. Es existiert dann ein $c \in R$ mit $a = pc$. Einsetzen in die Gleichung liefert $pq = (pc)b$, und Anwendung der Kürzungsregel liefert $q = cb$. Weil q als Primelement auch irreduzibel ist, folgt daraus $c \in R^\times$ oder $b \in R^\times$.

Ist b eine Einheit, dann sind wir fertig. Ansonsten gilt $c \in R^\times$. Wegen $q = cb$ ist b dann zum Primelement q assoziiert und damit selbst ein Primelement. Insgesamt ist damit gezeigt, dass b entweder eine Einheit oder ein Primelement ist.