LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Prof. Dr. Werner Bley
Martin Hofer

Wintersemester 2015/16
18. Februar 2016

Zahlentheorie (Lehramt Gymnasium)

Hauptklausur

Nachname:	Vorname:	Matrikelnummer:

Abschluss: ❍ Lehramt Gymn. (modularisiert) ❍ Lehramt Gymn. (nicht modul.)

❍ Anderes: _____

❑ Ich stimme zu, dass mein Klausurergebnis im Internet nach Angabe meiner Matrikelnummer und meines bei Klausuranmeldung angegebenen Passworts abrufbar sein wird.

Bitte beachten Sie:

- Schalten Sie Ihr Mobiltelefon aus und verstauen Sie es zusammen mit allen weiteren nicht zugelassenen Hilfsmitteln in Ihrer Tasche.
- Legen Sie Ihren Lichtbild- und Studienausweis sichtbar auf den Tisch.
- Überprüfen Sie, ob Sie **fünf Aufgaben** erhalten haben.
- Schreiben Sie mit einem **dokumentenechten** Stift, jedoch nicht in den Farben rot und grün.
- Schreiben Sie auf **jedes Blatt** Ihren **Nach- und Vornamen**. Lösen Sie bitte jede Aufgabe auf den dafür vorgesehenen Blättern. Versehen Sie auch zusätzliche Blätter mit Nach- und Vornamen sowie der Aufgabennummer. Vermerken Sie deutlich, wenn Ihre Lösung auf weiteren Blättern fortgesetzt wird.
- Geben Sie zu jeder Aufgabe nur eine Lösung ab; streichen Sie deutlich durch, was nicht gewertet werden soll.
- Sie haben **120 Minuten** Zeit, die Klausur zu bearbeiten.

Viel Erfolg!

1	2	3	4	5	Summe
/8	/8	/8	/8	/8	/40

Name: _____

Aufgabe 1. (8 Punkte)
Sei $I \subset \mathbb{Z}[X]$ die Menge der Polynome mit geraden Koeffizienten.

a) Zeigen Sie, dass I ein Ideal von $\mathbb{Z}[X]$ ist.

b) Sei $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ die kanonische Projektion.
Zeigen Sie, dass I der Kern des Ringhomomorphismus

$$\varphi : \mathbb{Z}[X] \to (\mathbb{Z}/2\mathbb{Z})[X],$$
$$\sum_i a_i X^i \mapsto \sum_i \pi(a_i) X^i,$$

ist.
Hinweis: Es muss nicht gezeigt werden, dass die Abbildung ein Ringhomomorphismus ist.

c) Zeigen Sie, dass I ein Primideal ist.

d) Ist $\mathbb{Z}[X]/I$ faktoriell? Begründen Sie Ihre Antwort.

Lösung.

a) Seien $f, g \in I$. Dann ist $f + g \in I$, da bei der Addition von Polynomen die Koeffizienten addiert werden und die Summe zweier gerader Zahlen wieder gerade ist. Sei nun

$$f = \sum_i a_i x^i \in I, \quad g = \sum_j b_j x^j \in \mathbb{Z}[x].$$

Dann ist $fg = \sum_k c_k x^k$ mit $c_k = \sum_{i+j=k} a_i b_j$. Da die a_i gerade sind, sind die c_k ebenfalls gerade. Also ist $fg \in I$.

b) Sei wieder $f = \sum_i a_i x^i \in I$. Dann ist $\varphi(f) = \sum_i \pi(a_i) x^i = 0$ in $(\mathbb{Z}/2\mathbb{Z})[x]$, da

$$\pi(a_i) = \bar{0} \iff 2 \mid a_i. \qquad (*)$$

Damit ist $I \subseteq \ker(\varphi)$ gezeigt. Ist umgekehrt $f \in \ker(\varphi)$, so folgt $\sum_i \pi(a_i) x^i = 0$ in $(\mathbb{Z}/2\mathbb{Z})[x]$, d.h. $\pi(a_i) = \bar{0}$ für alle i. Aus $(*)$ folgt, dass also alle a_i gerade sind, also $f \in I$.

c) & d) Nach dem Isomorphiesatz ist $\mathbb{Z}[x]/I \simeq (\mathbb{Z}/2\mathbb{Z})[x]$. Da $\mathbb{Z}/2\mathbb{Z}$ ein Körper ist, ist der Polynomring $(\mathbb{Z}/2\mathbb{Z})[x]$ nullteilerfrei und faktoriell. Also ist auch $\mathbb{Z}[x]/I$ nullteilerfrei und faktoriell. Die Nullteilerfreiheit ist äquivalent dazu, dass I ein Primideal ist.

Name: _____

Aufgabe 2. (8 Punkte)
Wir betrachten im Polynomring $\mathbb{F}_3[X]$ die Polynome:

$$f = X^5 + X^4 + 2X^3 + X^2 + X + 2 \qquad g = X^4 + X^3 + X + 2.$$

a) Finden Sie ein normiertes Polynom $h \in \mathbb{F}_3[X]$ mit $(h) = (f, g)$ in $\mathbb{F}_3[X]$.

b) Finden Sie $p, q \in \mathbb{F}_3[X]$, so dass $h = pf + qg$, wobei h das Polynom aus a) ist.

c) Finden Sie die Faktorisierung von f in irreduzible Polynome in $\mathbb{F}_3[X]$.

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Lösung.

a) Sukzessive Polynomdivision liefert

$$\begin{aligned} X^5 + X^4 + 2X^3 + X^2 + X + 2 &= X \cdot (X^4 + X^3 + X + 2) + (2X^3 + 2X + 2), \\ X^4 + X^3 + X + 2 &= (2X + 2) \cdot (2X^3 + 2X + 2) + (2X^2 + 2X + 1), \\ 2X^3 + 2X + 2 &= (X + 2) \cdot (2X^2 + 2X + 1) + 0. \end{aligned}$$

Also ist $h = X^2 + X + 2$ (normiert) der ggT von f und g. Dieser erzeugt das Hauptideal (f, g).

b) Nach dem erweiterten euklidischen Algorithmus sind die obigen sukzessiven Polynomdivisionen von unten nach oben nach h aufzulösen. Man erhält:

$$\begin{aligned} -h &= g - (2X + 2)(2X^3 + 2X + 2) \\ &= g - (2X + 2)(f - Xg) \\ &= (X + 1)f + (2X^2 + 2X + 1)g. \end{aligned}$$

Also gilt $h = pf + qg$ mit $p = 2X + 2$ und $q = X^2 + X + 2$.

c) Dividiert man f durch h so erhält man $X^3 + 1$. Es gilt $X^3 + 1 = (X + 1)^3$ in $\mathbb{F}_3[X]$. Da h keine Nullstellen in $\mathbb{F}_3$ hat, ist h irreduzibel und die Zerlegung in irreduzible Faktoren ist gegeben durch $f = (X + 1)^3 h$.

Name: _____

Aufgabe 3. (8 Punkte)

a) Bestimmen Sie die Anzahl der Lösungen $x \in (\mathbb{Z}/120\mathbb{Z})^\times$ für $x^2 = \bar{1}$.

b) Bestimmen Sie alle Lösungen $x \in \mathbb{Z}$ von $x^2 \equiv 1 \bmod 75$ für die gilt: $x \not\equiv 1 \bmod 3$.

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Lösung.

a) Nach dem chinesischen Restsatz ist $(\mathbb{Z}/120\mathbb{Z})^\times \simeq (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. Während $(\mathbb{Z}/8\mathbb{Z})^\times$ bizyklisch von der Ordnung 4 ist, sind $(\mathbb{Z}/3\mathbb{Z})^\times$ bzw. $(\mathbb{Z}/5\mathbb{Z})^\times$ zyklisch von der Ordnung 2 bzw. 4. Explizit:

$$(\mathbb{Z}/120\mathbb{Z})^\times \simeq C_2 \times C_2 \times C_2 \times C_4.$$

In jeder Komponente gibt es genau zwei Elemente z mit $z^2 = 1$. Also gibt es insgesamt $16 = 2^4$ verschiedene Elemente $x \in (\mathbb{Z}/120\mathbb{Z})^\times$ mit $x^2 = \bar{1}$.

b) Nach dem chinesischen Restsatz ist $(\mathbb{Z}/75\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5^2\mathbb{Z})^\times$. In $(\mathbb{Z}/3\mathbb{Z})^\times$ hat $x^2 \equiv 1 \pmod 3$ die beiden Lösungen ± 1. Ebenso hat man in $(\mathbb{Z}/5^2\mathbb{Z})^\times$ die beiden Lösungen ± 1. Da die Lösung $+1$ modulo 3 ausgeschlossen wurde, haben wir die beiden simultanen Kongruenzen

$$\begin{aligned} x &\equiv -1 \pmod 3 \\ x &\equiv +1 \pmod{25} \end{aligned}$$

und

$$\begin{aligned} x &\equiv -1 \pmod 3 \\ x &\equiv -1 \pmod{25} \end{aligned}$$

zu lösen. Das zweite System hat offenbar die Lösung $x = -1$. Die Menge aller Lösungen ist gegeben durch $-1 + 75\mathbb{Z}$.

Das erste System löst man mit dem Algorithmus zum Lösen simultaner Kongruenzen. Schreibe etwa $(-1) - 1 = -2 = 16 \cdot 3 - 2 \cdot 25$. Dann ist $x = -1 - 16 \cdot 3 = 1 - 2 \cdot 25 = -49$ eine Lösung und die Menge aller Lösungen ist durch $-49 + 75\mathbb{Z} = 26 + 75\mathbb{Z}$ gegeben.

Name: _____

Aufgabe 4. (8 Punkte)

a) Entscheiden Sie, ob $x^2 \equiv 667 \bmod 919$ eine Lösung hat.
Hinweis: 919 *ist eine Primzahl, aber* 667 *ist keine Primzahl.*

b) Sei $n, m \in \mathbb{N}$. Zeigen Sie: Falls es ein $b \in \mathbb{Z}$ gibt mit $b^2 \equiv n \bmod m$, so ist n ein Quadrat modulo p für alle Primteiler p von m.

c) Sei $n, m \in \mathbb{N}$ und $m \geq 3$ ungerade. Für das Jacobi-Symbol $\left(\frac{n}{m}\right)$ gelte $\left(\frac{n}{m}\right) = -1$.
Zeigen Sie: $x^2 \equiv n \bmod m$ hat keine Lösungen mit $x \in \mathbb{Z}$.

Natürlich müssen auch hier die Antworten vollständig begründet und die aufgestellten Behauptungen bewiesen werden.

Lösung.

a) Wir berechnen das Legendre-Symbol $\left(\frac{667}{919}\right)$, wobei wir für die Zwischenschritte die Rechenregeln für das Jacobi-Symbol verwenden.

$$\begin{aligned}
\left(\frac{667}{919}\right) &\overset{(1)}{=} -\left(\frac{919}{667}\right) = -\left(\frac{252}{667}\right) = \\
&= -\left(\frac{2^2}{667}\right)\left(\frac{3^2}{667}\right)\left(\frac{7}{667}\right) = -\left(\frac{7}{667}\right) = \\
&\overset{(1)}{=} \left(\frac{667}{7}\right) = \left(\frac{2}{7}\right) \overset{(2)}{=} 1.
\end{aligned}$$

Hierbei gilt (1) jeweils aufgrund des quadratischen Reziprozitätsgesetzes (man beachte $667 \equiv 919 \equiv 7 \equiv 3 \pmod 4$), und (2) aufgrund des zweiten Ergänzungssatzes (beachte $7 \equiv -1 \pmod 8$).

Da das Legendre-Symbol (919 ist eine Primzahl) gleich $+1$ ist, ist also 667 ein Quadrat modulo 919.

b) Es gilt: $m \mid (b^2 - n)$. Also gilt auch für jeden Teiler p von m die Teilbarkeitsrelation $p \mid (b^2 - n)$. Dies ist äquivalent zu $b^2 \equiv n \pmod p$.

c) Sei $m = p_1 \cdots p_s$ mit (nicht notwendig paarweise verschiedenen) Primzahlen p_i. Dann gilt:

$$\left(\frac{n}{m}\right) = \prod_i \left(\frac{n}{p_i}\right) = -1. \qquad (*)$$

Hätte nun $b^2 \equiv n \pmod m$ eine Lösung, so hätte nach b) auch $b^2 \equiv n \pmod{p_i}$ für alle i eine Lösung, d.h. die Legendre-Symbole $\left(\frac{n}{p_i}\right)$ wären alle gleich $+1$. Dies ist ein Widerspruch zu $(*)$.

Name: _____

Aufgabe 5. (8 Punkte)
Beweisen Sie oder widerlegen Sie folgende Aussagen:

a) Sei R ein kommutativer Ring und $I \subset R$ ein Ideal. Wenn $R \setminus I := \{\alpha \in R \mid \alpha \notin I\}$ eine multiplikative Menge ist, dann ist I ein Primideal.

b) Sei $d \in \mathbb{Z}$ quadratfrei und $d < 0$. Es gilt $|\mathbb{Z}[\sqrt{d}]^\times| = 2$.

c) Sei $n \in \mathbb{N}$ und ζ_n eine primitive n-te Einheitswurzel. Dann gilt stets $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] < n$.

d) Der Ring $(\mathbb{Z}/4\mathbb{Z})[X]$ ist nullteilerfrei.

Lösung.

a) Wahr. Begründung: Sei $ab \in I$ und $a \notin I$. Zu zeigen: $b \in I$. Wäre aber $b \notin I$, so wäre $ab \notin I$, da $R \setminus I$ eine multiplikative Menge ist. Widerspruch!.

b) Falsch, denn $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, wobei wie üblich $i^2 = -1$ ist.

c) Wahr. Begründung: Sei $n = \prod_i p_i^{e_i}$ die Primzahlzerlegung von n mit paarweise verschiedenen Primzahlen p_i. Dann ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \prod_i \varphi(p_i^{e_i}) = \prod_i (p_i - 1) p_i^{e_i - 1} < \prod_i p_i^{e_i} = n$.

d) Falsch, da zum Beispiel $2 \cdot 2 = 0$ in $(\mathbb{Z}/4\mathbb{Z})[X]$ gilt.