Übung zu primen bzw. irreduziblen Elementen in quadratischen Zahlringen:

F19T1A3, F17T1A1

Erinnerung Homomorphiesatz

(i) Sei R ein Ring, I ein Ideal von R und $\phi: R \to S$ ein Hom. in einen anderen Ring S. Gilt $I \subseteq \ker(\phi)$, dann existiert ein eind. bestimmter Hom. $\bar{\phi}: R/I \to S$ mit $\bar{\phi}(a+I) = \phi(a)$ $\forall a \in R$. Dies ist

der sog. durch ϕ induzierte Homomorphismus.

(ii) Ist $I = \ker(\phi)$, dann liefert der induzierte Hom. $\bar{\phi}$ einen Isomorphismus $\boxed{R/I \cong \mathrm{im}(\phi)}$

H22T3A4 Übung: F19T2A4, F18T3A4

Sei $K = \mathbb{Z}[x]/I$ mit $I = (f, g)$, wobei $f = x^5 + 2$, $g = x^4 + x^3 + x^2 + x + 1$ ($\Rightarrow g = \Phi_5$, das fünfte Kreisteilungspolynom)

Zeigen Sie: (a) $3 \in I$ (b) K ist Körper

zu (a) Es gilt $x^5 - 1 = (x-1) \cdot g \in I$ und

$3 = (x^5+2) - (x^5-1) = f - (x-1)\cdot g \Rightarrow 3 \in I$

zu (b) Erinnerung: Laut Vorlesung gilt für einen Hauptidealring R, der kein Körper ist, und jedes $f \in R$ die Äquivalenz der folgenden Aussagen:

(i) f ist prim (ii) f ist irreduzibel

(iii) (f) ist maximales Ideal

(iv) (f) ist Primideal, und $f \neq 0_R$

[Übrigens: Um diesen Satz anwenden zu können, müssen wir $\mathbb{Z}[x]/I$ mit einem Hauptidealring, z.B. einem Polynomring über einem Körper in Ver-

Bindung bringen. Die Aussage aus Teil (a), $3 \in I$, deutet darauf hin, dass $\mathbb{Z}[x]/I$ einen zu $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ isomorphen Teilring enthält. $\rightsquigarrow$ Versuche, $\mathbb{Z}[x]/I$ mit einem Faktorring des Polynomrings $\mathbb{F}_3[x]$ in Verbindung zu bringen. Seien $\bar{f}, \bar{g}$ die Bilder von f, g in $\mathbb{F}_3[x]$. Dann ist $\bar{I} = (\bar{f}, \bar{g})$ das Bild von I in $\mathbb{F}_3[x]$ s.o. $\bar{3} = \bar{f} - (x - \bar{1})\bar{g}$, $\bar{3} = \bar{0} \rightarrow \bar{f} = (x - \bar{1})\bar{g} \Rightarrow$ $\bar{f} \in (\bar{g}) \Rightarrow \bar{I} = (\bar{g})$.]

Beh. (1) $\mathbb{Z}[x]/I \cong \mathbb{F}_3[x]/(\bar{g})$, wobei $\bar{g} \in \mathbb{F}_3[x]$ das Bild von g bezeichnet (ebenso $\bar{f}$ sei das Bild von f)

(2) $\mathbb{F}_3[x]/(\bar{g})$ ist ein Körper

Aus (1) und (2) folgt insgesamt, dass k ein Körper ist.

zu (1) Betrachte die Abbildung $\phi: \mathbb{Z}[x] \to \mathbb{F}_3[x]/(\bar{g})$ gegeben durch $\phi(h) = \bar{h} + (\bar{g})$, wobei $\bar{h} \in \mathbb{F}_3[x]$ jeweils das Bild von $h \in \mathbb{Z}[x]$ bezeichnet. Um den Homomorphiesatz anwenden zu können, müssen wir überprüfen (i) ϕ ist ein Ringhom. (✓)
(ii) ϕ ist surjektiv (✓)
(iii) $\ker(\phi) = I$

zu (iii)

valenz

$\Leftrightarrow \bar{h} +$

$\exists \bar{u} \in \mathbb{F}_3$

$\exists u \in \mathbb{Z}$

$\exists u \in \mathbb{Z}$

$\exists u, v \in \mathbb{Z}$

zu i) Bekanntlich ist die Abbildung
$\tilde{\pi}_3 : \mathbb{Z}[x] \to \mathbb{F}_3[x]$, $h \mapsto \bar{h}$ ein Ringhomomorphismus (die eindeutig bestimmte Abb. auf dem Polynomring $\mathbb{Z}[x]$, die auf $\mathbb{Z} \subseteq \mathbb{Z}[x]$ mit der Reduktion $\mathbb{Z} \to \mathbb{F}_3$ modulo 3 übereinstimmt und $x \in \mathbb{Z}[x]$ auf $x \in \mathbb{F}_3[x]$ abbildet.
Sei $\pi_{(\bar{g})} : \mathbb{F}_3[x] \to \mathbb{F}_3[x]/(\bar{g})$ der kanonische Epimorphismus. Dann gilt offenbar $\phi = \pi_{(\bar{g})} \circ \tilde{\pi}_3$, und als Komposition von zwei Ringhom. ist auch ϕ ein Ringhom.

zu (ii) Bekanntlich ist der kan. Epimorphismus $\pi_{(\bar{g})}$ surjektiv. Wegen $\phi = \pi_{(\bar{g})} \circ \tilde{\pi}_3$ folgt die Surjektivität von ϕ also aus der Surjektivität von $\tilde{\pi}_3$

dass

g

durch

$\mathbb{F}_3[x]$ je-

$x]$ bezeich-

satz an-

wir über-

om (✓)

v (✓)

I

Zum Nachweis der Surjektivität von $\tilde{\pi}_3$ sei $\bar{h} \in \mathbb{F}_3[x]$, $\bar{h} = \sum_{j=0}^{n} \bar{a}_j x^j$ mit $n \in \mathbb{N}_0$, $\bar{a}_0, \ldots, \bar{a}_n \in \mathbb{F}_3$.

Für $0 \leq j \leq n$ sei $a_j \in \mathbb{Z}$ ein Urbild von $\bar{a}_j$. Sei $h = \sum_{j=0}^{n} a_j x^j$. Dann gilt $\tilde{\pi}_3(h) = \bar{h}$.

zu (iii) Sei $h \in \mathbb{Z}[x]$. Dann gilt die Äquivalenz $h \in \ker(\phi) \iff \phi(h) = 0_{\mathbb{F}_3[x]/(\bar{g})}$

$\iff \bar{h} + (\bar{g}) = (\bar{g}) \iff \bar{h} \in (\bar{g}) \iff$

$\exists\, \bar{u} \in \mathbb{F}_3[x]$ mit $\bar{h} = \bar{u}\bar{g} \iff$

$\exists\, u \in \mathbb{Z}[x]$ mit $h \equiv ug \bmod (3) \iff$

$\exists\, u \in \mathbb{Z}[x]$ mit $h - ug \in (3) \iff$

$\exists\, u, v \in \mathbb{Z}[x]$ mit $h - ug = 3v \iff$

$\exists u, v \in \mathbb{Z}[x] : h = ug + v \cdot 3 \iff$

$h \in (g, 3)$ noch zu überprüfen: $I = (g, 3)$

Wegen $I = (f, g)$, genügt es z.zg:

(4) $f, g \in (g, 3)$ (5) $g, 3 \in (f, g)$

zu (4) $g \in (g, 3)$ offensichtlich erfüllt

$f = (x-1) \cdot g + 1 \cdot 3 \in (g, 3)$

zu (5) $g \in (f, g)$ offensichtlich

$3 = 1 \cdot f + (1-x) \cdot g \in (f, g)$

zu (2) Da $\mathbb{F}_3[x]$ ein Hauptidealring ist, folgt aus der Irreduzibilität von $\bar{g}$ die Maximalität des Hauptideals $(\bar{g})$. Daraus wiederum folgt, dass $\mathbb{F}_3[x]/(\bar{g})$ ein Körper ist. z.zg. also: $\bar{g}$ ist irreduzibel

ist

Das Polynom $\bar{g} = x^4 + x^3 + x^2 + x + \bar{1} \in \mathbb{F}_3[x]$ hat in $\mathbb{F}_3$ keine Nullstellen wegen $\bar{g}(\bar{0}) = \bar{1} \neq \bar{0}$, $\bar{g}(\bar{1}) = \bar{5} = \bar{2} \neq \bar{0}$ und $\bar{g}(\bar{2}) = \bar{16} + \bar{8} + \bar{4} + \bar{2} + \bar{1} = \bar{31} = \bar{1} \neq \bar{0}$.

Ang. $\bar{g}$ ist dennoch reduzibel. Dann ist $\bar{g}$ (da $\bar{g}$ normiert und vom Grad 4) Produkt zweier irred. normierter Polynome $\bar{u}, \bar{v}$ vom Grad 2 $\Rightarrow$

$\exists a, b, c, d \in \mathbb{F}_3$ mit $x^4 + \dots + \bar{1} = (x^2 + ax + b)(x^2 + cx + d) =$

$x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$

$\Rightarrow a + c = b + d + ac = ad + bc = bd = 1$

$\Rightarrow d = b^{-1}$, $c = \bar{1} - a$ $\overset{\forall r \in \mathbb{F}_3^\times: r = r^{-1}}{\Longrightarrow}$ $d = b$, $c = \bar{1} - a$

$\Rightarrow \bar{2}b + a(\bar{1} - a) = \bar{1}$, $ab + b(\bar{1} - a) = \bar{1}$

$\mathbb{Z}_{(p)}$

$\mathbb{Z} \setminus p\mathbb{Z}$

$\Rightarrow a = b$, $c = 1 - a$ $\Rightarrow$ $a = b$, $c = 1 - a$

$\forall r \in \mathbb{F}_3^\times$: $r = r^{-1}$

$\Rightarrow \bar{2}b + a(\bar{1} - a) = \bar{1}$, $ab + b(\bar{1} - a) = \bar{1}$

$\Rightarrow \bar{2}b + a - a^2 = \bar{1}$, $b = \bar{1}$

$\Rightarrow \bar{2} + a - a^2 = \bar{1} \Rightarrow a - a^2 = -\bar{1} \Rightarrow a^2 - a = \bar{1}$

$\Rightarrow a(a - \bar{1}) = \bar{1}$ Diese Gleichung ist für $a \in \{\bar{0}, \bar{1}, \bar{2}\}$ jeweils nicht erfüllt. $\lightning$ Also ist $\bar{g}$ irreduzibel.

alternativ: Ang. $\bar{g} = \bar{u}\,\bar{v}$ mit irreduziblen, normierten Polynomen vom Grad 2. Sei $\mathbb{F}_3^{alg}$ ein alg. Abschluss von $\mathbb{F}_3$ und $\alpha \in \mathbb{F}_3^{alg}$ eine Nullstelle von $\bar{g}$. $\Rightarrow \bar{u}(\alpha) \cdot \bar{v}(\alpha) = \bar{0} \Rightarrow$ o.B.d.A. $\bar{u}(\alpha) = \bar{0}$ (nach Vertauschung von $\bar{u}$ und $\bar{v}$) $\bar{u}$ normiert, irred., $\bar{u}(\alpha) = \bar{0} \Rightarrow \bar{u}$ ist Minpol von α über $\mathbb{F}_3 \Rightarrow [\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 2 \Rightarrow \mathbb{F}_3(\alpha) = \mathbb{F}_9$

$\bar{g}(\bar{0}) \neq \bar{0} \Rightarrow \alpha \neq \bar{0} \rightarrow \alpha \in \mathbb{F}_g^\times$ Dies ist eine Gruppe der Ordnung 8 andererseits:

$(x-\bar{1}) \cdot g = x^5 - \bar{1}$, $\bar{g}(\alpha) = \bar{0} \Rightarrow \alpha^5 = \bar{1}$

$g(\bar{1}) \neq \bar{0}$ $\Rightarrow \alpha \neq \bar{1}$ $\operatorname{ord}(\alpha) = 5$ Aber eine Gruppe der Ordnung 8 enthält kein Element der Ordnung 5. ↯ □

F19T3A1 Übung: F16T2A2

Sei p eine Primzahl und der Ring $\mathbb{Z}_{(p)}$ gegeben durch $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$

(Dies ist ein Fortsetzung von (4).)

(a) Zeigen Sie, dass ein Isomorphismus

$\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ mit $\varphi(a+p\mathbb{Z}) = a + p\mathbb{Z}_{(p)}$ $\forall a \in \mathbb{Z}$ existiert.

Wir wenden auf die Abb. $\phi : \mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, $a \mapsto a + p\mathbb{Z}_{(p)}$ den Homomorphiesatz an.

Zu überprüfen: (1) ϕ ist Ringhom.

(2) ϕ ist surjektiv

(3) $\ker(\phi) = p\mathbb{Z}$

Ist dies erfüllt, dann ist φ der durch ϕ induzierte Hom., und lt. Homomorphiesatz ist dies ein Isom.

zu (1) Die Abb. ϕ ist die Komposition des Einbettungshom. $\mathbb{Z} \to \mathbb{Z}_{(p)}$, $a \mapsto a$ und des kan. Epimorphismus $\pi_{(p)}$: $\mathbb{Z}_{(p)} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, und somit ebenfalls ein Hom.

zu (2) Sei $\frac{a}{b} + p\mathbb{Z}_{(p)} \in \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ vorgeg.; mit $a \in \mathbb{Z}$ und $b \in \mathbb{Z} \setminus p\mathbb{Z}$.
zu zeigen: Es gibt ein $c \in \mathbb{Z}$ mit
$\phi(c) = \frac{a}{b} + p\mathbb{Z}_{(p)}$ [Überlegung:

$\phi(c) = \frac{a}{b} + p\mathbb{Z}_{(p)} \iff c + p\mathbb{Z}_{(p)} = \frac{a}{b} + p\mathbb{Z}_{(p)}$

$\overset{\cdot 2}{\iff} bc + p\mathbb{Z}_{(p)} = a + p\mathbb{Z}_{(p)}$

$\overset{\cdot 2}{\iff} bc + p\mathbb{Z} = a + p\mathbb{Z} \iff bc \equiv a \bmod p$

$\Leftrightarrow \bar{c} = \bar{a} \cdot \bar{b}^{-1}$ in $\mathbb{F}_p$, wobei $\bar{a}, \bar{b}, \bar{c} \in \mathbb{F}_p$ Bilder von a, b, c]

Sei $c \in \mathbb{Z}$ so gewählt, dass $c + p\mathbb{Z} = (a+p\mathbb{Z}) \cdot (b+p\mathbb{Z})^{-1}$ in $\mathbb{Z}/p\mathbb{Z}$ gilt; wegen $b \notin p\mathbb{Z}$ ist $b+p\mathbb{Z}$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ invertierbar. $\Rightarrow (c+p\mathbb{Z}) \cdot (b+p\mathbb{Z}) = a + p\mathbb{Z}$

$\Rightarrow cb \equiv a \bmod p \Rightarrow \exists u \in \mathbb{Z}$ mit $cb = a + pu \Rightarrow c = \frac{a}{b} + p\underbrace{\frac{u}{b}}$

$\Rightarrow c + p\mathbb{Z}_{(p)} = \frac{a}{b} + p\mathbb{Z}_{(p)}$ $\in \mathbb{Z}_{(p)}$

$\Rightarrow \phi(c) = c + p\mathbb{Z}_{(p)} = \frac{a}{b} + p\mathbb{Z}_{(p)}$.

zu (3) siehe nächste Seite

zu (3) Für jedes $c \in \mathbb{Z}$ gilt die Äquivalenz

$$c \in \ker(\phi) \quad \Leftrightarrow \quad \phi(c) = 0_{\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}} \quad \Leftrightarrow$$

$$c + p\mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)} \quad \Leftrightarrow \quad c \in p\mathbb{Z}_{(p)} \quad \Leftrightarrow$$

$$\exists\, a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus p\mathbb{Z} : c = p \cdot \tfrac{a}{b} \quad \Leftrightarrow$$

$$\exists\, a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus p\mathbb{Z} : bc = pa \quad \Leftrightarrow \quad p \mid c \quad \Leftrightarrow \quad c \in p\mathbb{Z}.$$

Damit ist $\ker(\phi) = p\mathbb{Z}$ nachgewiesen.