Erinnerung Homomorphiesatz:

Sei $\phi : R \to S$ ein Ringhomomorphismus und $I = \ker(\phi)$. Dann existiert ein (eindeutig bestimmter) Isomorphismus $R/_I \cong \mathrm{im}(\phi)$ von Ringen gegeben durch $\bar{\phi}(a+I) = \phi(a)$ für alle $a \in R$.

F24T1A3

zu (b) Sei $R = \mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ (Ring der Gaußschen Zahlen) und $I = (1+i)$.
Zeigen Sie, dass R/I aus zwei Elementen besteht.

F24T1A3

Beh.: $R/I \cong \mathbb{F}_2$

Betrachte die Abbildung $\phi: R \to \mathbb{F}_2$ geg. durch $\phi(a+ib) = a+b+2\mathbb{Z} = \bar{a}+\bar{b}$ (wobei $\bar{a}, \bar{b}$ die Bilder von a, b in $\mathbb{F}_2$ sind).

Überprüfe die Voraussetzungen des Homomorphiesatzes: (1) ϕ ist Ringhom. (2) ϕ ist surjektiv (3) $\ker(\phi) = (1+i)$

zu (1) Es gilt $\phi(1) = \bar{1} = 1_{\mathbb{F}_2}$. Seien $a, b, c, d \in \mathbb{Z}$ vorgegeben. Dann gilt $\phi((a+ib)+(c+id)) =$

$\phi((a+c)+i(b+d)) = \overline{a+c}+\overline{b+d} = \bar{a}+\bar{b}+\bar{c}+\bar{d} =$

$\phi(a+ib) + \phi(c+id)$. außerdem $\phi((a+ib)\cdot(c+id))$
$= \phi(ac-bd + i(bc+ad)) = \overline{ac} - \overline{bd} + \overline{bc} + \overline{ad} =$
$\bar a\,\bar c + \bar b\,\bar d + \bar b\,\bar c + \bar a\,\bar d$; ebenso $\phi(a+ib)\cdot\phi(c+id) =$
$(\bar a + \bar b)\cdot(\bar c + \bar d) = \bar a\,\bar c + \bar b\,\bar c + \bar a\,\bar d + \bar b\,\bar d$.

<u>zu (2)</u> Es gilt $\phi(0) = \bar 0$, $\phi(1) = \bar 1$.

<u>zu (3)</u> „$\supseteq$" $\phi(1+i) = \bar 1 + \bar 1 = \bar 0 \rightarrow 1+i \in \ker(\phi)$

$\ker(\phi)$ ist Ideal $\Rightarrow (1+i) \subseteq \ker(\phi)$

„$\subseteq$" Sei $a+ib \in \ker(\phi)$ (mit $a, b \in \mathbb{Z}$). $\longrightarrow$

$\phi(a+ib) = \bar 0 \Rightarrow \bar a + \bar b = \bar 0 \Rightarrow \bar a = \bar b$

$\underline{\text{zu (3)}}$ $\overset{\text{"}}{=}$ $\Phi(1+i) = 1+1 = 0 \Rightarrow 1+i \in \ker(\Phi)$

$\ker(\Phi)$

$\Rightarrow a \equiv b \mod 2 \Rightarrow \exists c \in \mathbb{Z} : b = a + 2c$

$\Rightarrow b - a = 2 \cdot c = (1+i)(1-i)c$

$\Rightarrow a + ib = a + ia + i(b-a) = a(1+i) + i \cdot c \cdot (1-i)(1+i) \Rightarrow a + ib \in (1+i)$

Also liefert der Hom.-Satz einen Isom. $R/I \cong \mathbb{F}_2$.

$\Rightarrow |R/I| = |\mathbb{F}_2| = 2.$

Korrektur zu (a): Induktionsschritt

$(a^2)^n = a^{2n} = a^{n+1} \cdot a^{n-1} = 0 \cdot a^{n-1} = 0. \overset{\text{Ind.V.}}{\Longrightarrow}$

$a^2 \in I \overset{I \text{ Primideal}}{\Longrightarrow} a \in I$

(Die Korrektur wurde auf den Bildern von Dienstag ergänzt.)

H25T2A5

Sei $\phi: \mathbb{Z}[x] \to \mathbb{F}_p[x]$ die Abbildung, die jedes Polynom $f \in \mathbb{Z}[x]$ auf seine Reduktion modulo p abbildet, wobei p eine Primzahl bezeichnet. Sei $\bar{h} \in \mathbb{F}_p[x]$ ein irreduzibles Element und $(\bar{h})$ das entsprechende Hauptideal in $\mathbb{F}_p[x]$.

Zeigen Sie, dass $\mathfrak{m} = \phi^{-1}((\bar{h}))$ ein maximales Ideal in $\mathbb{Z}[x]$ und $\mathbb{Z}[x]/\mathfrak{m}$ ein Kp. der Charakteristik p ist.

Laut Vorlesung existiert für jeden Ringhom $\psi : \mathbb{Z} \to \mathbb{F}_p[x]$ und jedes $\bar{f} \in \mathbb{F}_p[x]$ ein eindeutig bestimmter Hom. $\tilde{\psi} : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ mit $\tilde{\psi}(x) = \bar{f}$ (universelle Eigenschaft des Polynomrings). Wenden wir dies auf die Komposition ψ der beiden Hom. $\mathbb{Z} \to \mathbb{F}_p$, $a \mapsto a + p\mathbb{Z}$ und $\mathbb{F}_p \to \mathbb{F}_p[x]$, $\bar{g} \mapsto \bar{g}$ und auf das Element $\bar{f} = x \in \mathbb{F}_p[x]$ an, so erhalten wir genau die Abb. ϕ. Daraus folgt, dass ϕ ein Ringhom. ist.

Betrachte nun die Abbildung $\phi_1 : \mathbb{Z}[x] \to \mathbb{F}_p[x]/(\bar{h})$, die durch Komposition von $\phi : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ mit dem kanonischen Epimorphismus $\pi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]/(\bar{h})$ zu Stande kommt, d.h. $\phi_1(g) = (\pi \circ \phi)(g) = \pi(\phi(g))$

...n

...un

...$[x]$

...s

...mpos-

...$p\mathbb{Z}$ und

$\bar{f} = x \in \mathbb{F}_p[x]$

folgt, dass ϕ

...$] \to \mathbb{F}_p[x]/(\bar{h})$,

$\mathbb{F}_p[x]$ mit

...$] \to \mathbb{F}_p[x]/(\bar{h})$

...$) = \pi(\phi(g))$

$= \phi(g) + (\bar{h})$ für alle $g \in \mathbb{Z}[x]$.

Wir wenden den Hom.-satz an, um zu zeigen, dass $\mathbb{Z}[x]/\mathfrak{m} \cong \mathbb{F}_p[x]/(\bar{h})$ gilt.

Überprüfe dafür: (1) ϕ_1 ist Ringhom (2) ϕ_1 ist surjektiv (3) $\ker(\phi_1) = \mathfrak{m}$

<u>zu (1)</u> klar, da ϕ_1 Komposition von Ringhom.

<u>zu (2)</u> Sei $\bar{g} + (\bar{h}) \in \mathbb{F}_p[x]/(\bar{h})$, mit $\bar{g} \in \mathbb{F}_p[x]$. Sei $g \in \mathbb{Z}[x]$ ein Urbild von $\bar{g}$ unter ϕ (d.h. wähle für jeden Koeff. von $\bar{g}$ ein Urbild in $\mathbb{Z}$). Dann gilt $\phi_1(g) = (\pi \circ \phi)(g) = \pi(\bar{g}) = \bar{g} + (\bar{h})$

<u>zu (3)</u> Für alle $g \in \mathbb{Z}[x]$ gilt die Äquivalenz $g \in \ker(\phi_1) \iff \phi_1(g) = 0_{\mathbb{F}_p[x]/(\bar{h})}$

...ng.
...e
...ber p
$\in \mathbb{F}_p[x]$
das
...$[x]$
... maxi-
... Krp. des

$$\Leftrightarrow \phi(g) + (\bar{h}) = \bar{0} + (\bar{h}) \Leftrightarrow \phi(g) \in (\bar{h})$$

$$\Leftrightarrow g \in \phi^{-1}((\bar{h})) \Leftrightarrow g \in M$$

Also liefert der Hom.-satz den angeg. Isomorphismus. Da $\mathbb{F}_p[x]$ (als Polynomring über einem Körper) ein Hauptidealring und $\bar{h}$ ein irreduzibles Element ist, ist $(\bar{h})$ in $\mathbb{F}_p[x]$ ein maximales Ideal. Daraus folgt, dass $\mathbb{F}_p[x]/(\bar{h})$ ein Körper ist. Auf Grund des Isom gilt dasselbe für $\mathbb{Z}[x]/M$. Daraus wiederum folgt, dass M ein maximales Ideal in $\mathbb{Z}[x]$ ist. (Als Urbild eines Ideals unter einem Ringhom. ist M auf jeden Fall ein Ideal.)

Als Körper hat $\mathbb{F}_p[x]/(\bar{h})$ entweder Charakteristik 0, oder die Char. ist eine Primzahl. Es gilt $p \cdot 1_{\mathbb{F}_p[x]/(\bar{h})} = p \cdot (\bar{1} + (\bar{h})) = \bar{p} + (\bar{h}) = \bar{0} + (\bar{h}) = 0_{\mathbb{F}_p[x]/(\bar{h})} \Rightarrow$

$\Rightarrow \operatorname{ord}(1_{\mathbb{F}_p[x]/(\bar{h})})$ teilt p. Da die Ordnung nicht 1 sein kann, folgt $\operatorname{char}(\mathbb{F}_p[x]/(\bar{h})) = \operatorname{ord}(1_{\mathbb{F}_p[x]/(\bar{h})}) = p$.

Auf des ~~Isom~~ ist auch $\mathbb{Z}[x]/M$ ein Ring der Char. p. $\square$

<u>Übung</u>: H22T3A4, H23T1A1 (Hinweis: Zeigen Sie zunächst $\mathbb{Z}[x]/(2, x^3+x^2+x) \cong \mathbb{F}_2[x]/(x^3+x^2+x)$. Mit dem Chin. Restsatz erhält man $\mathbb{F}_2[x]/(x^3+x^2+x) \cong \mathbb{F}_2 \times \mathbb{F}_2[x]/(x^2+x+\bar{1})$.)

also: $(\bar{a}+\bar{b}x+I)^{-1} = \dfrac{\bar{a}+(-\bar{b})x}{\bar{a}^2+\bar{b}^2}+I \quad (*)$

2. Fall: $\bar{a}=\bar{0}$ erhalte $-\bar{b}\bar{d}=\bar{1}$, $\bar{b}\bar{c}=\bar{0}$

H20T3A4 Sei $I = (x^2+\bar{1}) \subseteq \mathbb{F}_3[x]$.

zu (a) z.zg: $\mathbb{F}_3[x]/I$ ist ein Körper

Bestimmen Sie die Anzahl der Elemente des Rings.

Da $\mathbb{F}_3[x]$ als Polynomring über einem Körper ein Hauptidealring ist, ist das Ideal $I=(\bar{f})$ mit $\bar{f}=x^2+\bar{1}$ genau dann maximal, wenn $\bar{f}$ irreduzibel ist. Wegen $\operatorname{grad}(\bar{f})=2$ ist dies gleichbedeutend damit, dass $\bar{f}$ in $\mathbb{F}_3$ keine Nullst. hat

$\bar{f}(\bar{0})=\bar{1}\neq\bar{0}$, $\bar{f}(\bar{1})=\bar{2}\neq\bar{0}$, $\bar{f}(\bar{2})=\bar{2}^2+\bar{1}=\bar{5}=\bar{2}\neq\bar{0}$

$\Rightarrow \bar{f}$ ist irreduzibel $\Rightarrow I$ ist maximal $\Rightarrow \mathbb{F}_3[x]/I$ ist ein Körper

Allgemein gilt: Ist K ein Körper und $f \in K[x] \setminus K$, dann bilden die Polynome vom Grad $< n$, $n = \text{grad}(f)$, zusammen mit 0_K ein Repräsentantensystem von $K[x]/(f)$.

$\Rightarrow R = \{\bar{a} + \bar{b}x \mid \bar{a}, \bar{b} \in \mathbb{F}_3\}$ ist ein Repräsentantensystem von $\mathbb{F}_3[x]/I$. Offenbar ist $\mathbb{F}_3 \times \mathbb{F}_3 \to R$, $(\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b}x$ eine Bijektion.

$\Rightarrow |\mathbb{F}_3[x]/I| = |R| = |\mathbb{F}_3 \times \mathbb{F}_3| = 3 \cdot 3 = 9$

zu (b) Geben Sie für alle $\bar{a}, \bar{b} \in \mathbb{F}_3$ jeweils eine Formel für $(\bar{a} + \bar{b}x + I)^{-1}$ an, sofern das Inverse existiert.

Für alle $\bar a, \bar b \in \mathbb{F}_3$ gilt die Äquivalenz

$\bar a + \bar b x + I = 0_{\mathbb{F}_3[x]/I} \Longleftrightarrow \bar a + \bar b x + I = I$

$\Longleftrightarrow \bar a + \bar b x \in I \Longleftrightarrow \bar a + \bar b x$ ist Vielfaches von $\bar f \underset{\mathrm{grad}(\bar f) = 2}{\Longleftrightarrow} \bar a = \bar b = \bar 0$.

Da $\mathbb{F}_3[x]/I$ ein Körper ist, ist jedes Element $\neq 0_{\mathbb{F}_3[x]/I}$ invertierbar. Also existiert $(\bar a + \bar b x + I)^{-1}$ für alle $(\bar a, \bar b) \neq (\bar 0, \bar 0)$.

Für alle $\bar a, \bar b, \bar c, \bar d \in \mathbb{F}_3$ mit $(\bar a, \bar b) \neq (\bar 0, \bar 0)$ gilt die Äquivalenz $(\bar a + \bar b x + I) \cdot (\bar c + \bar d x + I) = \bar 1 + I$

$\mathrm{grad}(\bar f) = 2$

$\Longleftrightarrow (\bar a + \bar b x)\cdot(\bar c + \bar d x) + I = \bar 1 + I$

$\Longleftrightarrow \bar a\bar c + \bar b\bar c x + \bar a\bar d x + \bar b\bar d x^2 + I = \bar 1 + I$

$x^2 + \bar 1 + (\bar f) = (\bar f)$

$\Longleftrightarrow$

$x^2 + (\bar f) = -1 + (\bar f)$

$(\bar a\bar c - \bar b\bar d) + (\bar b\bar c + \bar a\bar d)\cdot x + I = \bar 1 + I$

R Repr.-system

$\Longleftrightarrow \bar a\bar c - \bar b\bar d + (\bar b\bar c + \bar a\bar d)x = \bar 1$

$\Longleftrightarrow \bar a\bar c - \bar b\bar d = 1,\ \bar b\bar c + \bar a\bar d = \bar 0$

1. Fall: $\bar a \neq \bar 0$ Dann ist das Gleichungssystem äquivalent zu $\bar d = -\bar a^{-1}\bar b\bar c,\ \bar a\bar c + \bar b(\bar a^{-1}\bar b\bar c) = \bar 1$

$\Longleftrightarrow \bar d = -\bar a^{-1}\bar b\bar c,\ \bar c(\bar a + \bar a^{-1}\bar b^2) = \bar 1$

$\Longleftrightarrow \bar c = (\bar a + \bar a^{-1}\bar b^2)^{-1},\ \bar d = -\bar a^{-1}\bar b(\bar a^{-1} - \bar a^{-1}\bar b^{-2})^{-1}$

$$\Longleftrightarrow \bar{c} = \frac{\bar{a}}{\bar{a}^2 + \bar{b}^2}, \quad \bar{d} = \frac{(-\bar{b})}{\bar{a}^2 + \bar{b}^2}$$

also: $(\bar{a} + bx + I)^{-1} = \frac{\bar{a} + (-\bar{b})x}{\bar{a}^2 + \bar{b}^2} + I \quad (*)$

2. Fall: $\bar{a} = \bar{0}$ erhalte $-\bar{b}\bar{d} = \bar{1}, \ \bar{b}\bar{c} = \bar{0}$

$$\Longrightarrow \bar{d} = (-\bar{b})^{-1}, \ \bar{c} = \bar{0}$$

$$\Longleftrightarrow \bar{c} = \bar{0} = \frac{\bar{a}}{\bar{a}^2 + \bar{b}^2}, \quad \bar{d} = \frac{(-\bar{b})}{\bar{0}^2 + \bar{b}^2} = \frac{(-\bar{b})}{\bar{a}^2 + \bar{b}^2}$$

Also gilt $(*)$ auch in diesem Fall. $\square$

Bem. In $\mathbb{C}$ gilt $\forall (x,y) \neq (0,0),\ x,y \in \mathbb{R}$ jeweils $(x+iy)^{-1} = \frac{x - iy}{x^2 + y^2}$ in $\mathbb{F}_3[x]/I$: $(x+I)^2 = -\bar{1}_{\mathbb{F}_3[x]/I}$

$\bar{0})$

$I) = \bar{1} + I$