

FIGURA 1 $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b \right\}$

wobei p eine Primzahl ist

in Teil (a) durch Anwendung des Homomorphismesatzes gezeigt: $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$

Erinnerung: Nachweis der Surjektivität von

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}, a \mapsto a + p\mathbb{Z}_{(p)}$$

geg. $\frac{a}{b} + p\mathbb{Z}_{(p)}$ mit $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z}$,

wähle $c \in \mathbb{Z}$ mit $bc \equiv 1 \pmod{p}$

gezeigt: Dann gilt $\phi(ac) = \frac{a}{b} + p\mathbb{Z}_{(p)}$

Def.

R

Für

$a =$

zu (b) gesucht: $y \in \{0, 1, 2, 3, 4\}$ mit

$$y + 5\mathbb{Z}_{(5)} \stackrel{(*)}{=} \left(\frac{2}{3} + 5\mathbb{Z}_{(5)}\right) + \left(\frac{1}{7} + 5\mathbb{Z}_{(5)}\right)$$

$$\frac{2}{3} + \frac{1}{7} = \frac{14}{21} + \frac{3}{21} = \frac{17}{21} \quad \text{Bestimme das Inverse}$$

$$\text{von } \overline{21} \in \mathbb{Z}/5\mathbb{Z}. \quad \overline{21} = \overline{1} \Rightarrow \overline{21}^{-1} = \overline{1}^{-1} = \overline{1}$$

$$\text{außerdem: } \overline{17} = \overline{2} \text{ in } \mathbb{Z}/5\mathbb{Z} \Rightarrow$$

$$\overline{17} \cdot \overline{21}^{-1} = \overline{2} \cdot \overline{1} = \overline{2}$$

Bew. $y = 2$ löst die Gleichung (*)

$$\begin{aligned} \left(\frac{2}{3} + 5\mathbb{Z}_{(5)}\right) + \left(\frac{1}{7} + 5\mathbb{Z}_{(5)}\right) &= \frac{2}{3} + \frac{1}{7} + 5\mathbb{Z}_{(5)} \\ &= \frac{17}{21} + 5\mathbb{Z}_{(5)} \quad \text{z.z.g. also: } \frac{17}{21} + 5\mathbb{Z}_{(5)} = 2 + 5\mathbb{Z}_{(5)} \end{aligned}$$

$$\leftarrow \frac{17}{21} - 2 \in 5\mathbb{Z}(5) \iff \frac{17}{21} - \frac{42}{21} \in 5\mathbb{Z}(5) \iff$$

$$-\frac{25}{21} \in 5\mathbb{Z}(5), \text{ Dies ist erfüllt, da } -\frac{5}{21} \in \mathbb{Z}(5)$$

$$(\text{wg. } 5+21) \text{ und somit } -\frac{25}{21} = 5 \cdot \left(-\frac{5}{21}\right) \in 5\mathbb{Z}(5). \quad \square$$

Euklidische Ringe

Def. 1) Höhenfkt. auf einem Int.-Bereich $R = \text{Abk.}$

$R: R \setminus \{0\} \rightarrow \mathbb{N}_0$ mit der Eigenschaft:

Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit
 $a = qb + r$ und ($r = 0$ oder $h(r) < h(b)$)

ii) euklidischer Ring = Integritätsbereich auf dem eine Höhenfunktion existiert

Beispiele: (i) $\mathbb{Z}$ mit $h: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$, $a \mapsto |a|$

(ii) $K[x]$ (K Körper) mit $h: K[x] \setminus \{0\} \rightarrow \mathbb{N}_0$, $f \mapsto \deg(f)$

(iii) $\mathbb{Z}[i]$ mit $h: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$, $\alpha \mapsto N(\alpha)$, wobei

$N: \mathbb{C} \rightarrow \mathbb{R}_+$ die Normfkt. geg. durch $N(z) = z\bar{z} = |z|^2$

$\forall z \in \mathbb{C}$ bezeichnet.

In euklidischen Ringen kann für je zwei Elemente mit dem euklidischen Algorithmus ein ggT berechnet werden

$\mathbb{Z}(5)$

$-2+5\mathbb{Z}$
(5)

H24T2A4 Sei $R = \mathbb{Z}[i]$ und N die Normfunktion auf R .

(a) Bestimmen Sie alle $\alpha \in R$ mit der Eigenschaft $N(\alpha) \leq 5$.

Sei $\alpha \in R$ mit $N(\alpha) \leq 5$, $\alpha = a + ib$ mit $a, b \in \mathbb{Z}$. Die Normfkt. nimmt auf R nur Werte in $\mathbb{N}_0$ an. $\Rightarrow$
 $N(\alpha) \in \{0, 1, \dots, 5\}$

Aus $\alpha = a + ib$ folgt $N(\alpha) = a^2 + b^2$

1. Fall: $N(\alpha) = 0 \rightarrow a^2 + b^2 = 0$
 $\xrightarrow{a^2, b^2 \geq 0} a = b = 0 \Rightarrow \alpha = 0$

2. Fall: $N(x) = 1 \rightarrow a^2 + b^2 = 1 \quad a^2, b^2 \in \{0, 1\} \Rightarrow$

$(a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\} \rightarrow$
 $x \in \{1, i, -1, -i\}$

3. Fall: $N(x) = 2 \Rightarrow a^2 + b^2 = 2$

$a=0$ oder $b=0$ unmöglich, da 2 kein Quadrat in $\mathbb{Z} \Rightarrow a^2 = b^2 = 1 \Rightarrow a, b \in \{\pm 1\}$

$\Rightarrow (a, b) \in \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}$

$\Rightarrow x \in \{1+i, -1+i, 1-i, -1-i\}$

4. Fall: $N(x) = 3 \Rightarrow a^2 + b^2 = 3$

Der Fall $a^2 = 0$ oder $b^2 = 0$ ist ausgeschlossen, da 3 in $\mathbb{Z}$ kein Quadrat, ebenso $a^2 = 1$ oder $b^2 = 1$, da 2 kein Quadrat in $\mathbb{Z}$ ist.

ges
 $\{0$
 also
 (b) St
 irred
 Land
 in einem
 Einheits
 Produkt da

die $\Rightarrow |a| \geq 2 \Rightarrow a^2 + b^2 \geq 4$ ∇

5. Fall: $N(x) = 4 \Rightarrow a^2 + b^2 = 4$

$|a| = 1$ oder $|b| = 1$ unmöglich, da 3 kein Quadrat

Andererseits muss $|a|, |b| \leq 2$ gelten,
da ansonsten $a^2 + b^2 > 4 \Rightarrow$ einzige

Mögl. $(a, b) \in \{(2, 0), (-2, 0), (0, 2), (0, -2)\}$

$\Rightarrow x \in \{\pm 2, \pm 2i\}$

6. Fall: $N(x) = 5 \Rightarrow a^2 + b^2 = 5$

Dann muss $|a|, |b| \leq 2$ gelten.

$|a| = 0$ oder $|b| = 0$ unmöglich, da 5 kein

Quadrat. $\Rightarrow (a^2, b^2) \in \{(1, 4), (4, 1)\}$

$$\Rightarrow (a, b) \in \{ (1, 2), (-1, 2), (1, -2), (-1, -2), \\ (2, 1), (-2, 1), (2, -1), (-2, -1) \} \Rightarrow$$

$\alpha \in \{ \pm 1 \pm 2i, \pm 2 \pm i \}$ (jeweils alle vier
Vorzeichenkombinationen)

gesuchte Menge insgesamt:

$$\{ 0, \pm 1, \pm i, \pm 1 \pm i, \pm 2, \pm 2i, \pm 1 \pm 2i, \pm 2 \pm i \}$$

also 21 Elemente

(b) Stellen Sie all diese Elemente als Produkte
irreduzibler Elemente dar.

laut Vorlesung sind Produkte irreduzibler Elemente
in einem Integritätsbereich weder gleich null noch
Einheiten. Für 0 existiert also keine solche
Produktzerlegung.

Die Elemente $\pm 1, \pm i$ haben Norm 1 und sind somit Einheiten. Für sie existiert also ebenfalls keine Darstellung als Produkt irred. Elemente.

bekannt: Ist $\alpha \in \mathbb{R}$ und $N(\alpha)$ eine Primzahl, dann ist α irreduzibel (also ein Produkt irred. Elemente der Länge 1). Dies gilt hier für die Elemente mit Norm 2 oder 5, also für $\pm 1 \pm i$, $\pm 2 \pm i$ und $\pm 1 \pm 2i$.

Es ist $2 = (1+i)(1-i)$, und wg. $N(1+i) = N(1-i) = 2$ (Primzahl)

sind diese beiden Faktoren irreduzibel.

$$-2 = (-1) \cdot 2 = (-1)(1+i)(1-i) = (-1-i)(1-i)$$

$$2i = i \cdot 2 = i(1+i)(1-i) = (-1+i)(1-i)$$

$$-2i = (-i) \cdot 2 = (-i)(1+i)(1-i) = (1-i)(1-i)$$

Auch hier überprüft man, dass alle Faktoren vom Grad 2 und somit irreduzibel sind.

(c) Sei $d \in R$ mit $(d) = (5+10i, 1+3i) (*_2)$

Zeigen Sie, dass $R/(d)$ ein Körper ist.

Da R ein euklidischer Ring, und somit auch ein Hauptidealring ist, folgt aus der Gleichung $(*_2)$, dass d ein ggT der $\text{BD } \alpha = 5+10i, \beta = 1+3i$ ist. Ein ggT kann auch mit dem euklidischen Algorithmus berechnet werden.

$$\frac{5+10i}{1+3i} = \frac{(5+10i)(1-3i)}{(1+3i)(1-3i)} = \frac{1}{10} (35 - 5i) = \frac{7}{2} - \frac{1}{2}i \approx 3$$

$$5+10i - 3 \cdot (1+3i) = 2+i \quad \frac{1+3i}{2+i} = \frac{(1+3i)(2-i)}{(2+i)(2-i)} = \frac{1}{5} (5+5i) = 1+i$$

ente
rg

Euclidischer Algorithmus

a_{n-2}/a_n	q	a_n	x_n	y_n
—	—	$5+10i$	1	0
—	—	$1+3i$	0	1
$7/2 - \frac{1}{2}i$	3	$2+i$	1	-3
$1+i$	$1+i$	0	—	—

Ergebnis der Rechnung:

$$\text{ggT}(\alpha, \beta) = 2+i = 1 \cdot \alpha + (-3) \cdot \beta$$

Da der größte gemeinsame Teiler zweier Elemente in einem Ring bis auf Assoziierte eindeutig

ist, gilt also $d = \varepsilon \cdot (2+i)$ für eine Einheit ε des Rings R . $\Rightarrow N(\varepsilon) = 1 \Rightarrow N(d) = N(\varepsilon) N(2+i) = 1 \cdot 5 = 5$. Da 5 eine Primzahl ist, ist d in R ein irreduzibles Element. Da R ein Hauptidealring, aber kein Körper ist, folgt daraus, dass das Hauptideal (d) ein maximales Ideal ist. Daraus folgt wiederum dass $R/(d)$ ein Körper ist. $\square$

Chinesischer Restsatz:

Sei R ein Ring und I, J teilerfremde Ideale von R (d.h. $I+J=(1)$.)

Dann existiert ein Isomorphismus von Ringen

$$\bar{\Phi}: R/IJ \rightarrow R/I \times R/J \text{ mit}$$

$$\boxed{\bar{\Phi}(a+IJ) = (a+I, a+J)}$$

für alle $a \in R$

wichtiger Spezialfall: Setze voraus, dass R ein euklidischer Ring ist. Dann sind I, J Hauptideale $I=(r), J=(s)$ mit

$r, s \in R. (\Rightarrow IJ = (rs))$ Aus der Teiler-
Freiheit von I, J folgt $\text{ggT}(r, s) = 1_R$. (3)

Für jedes Paar (b, c) mit $b, c \in R$ kann
durch folgende Schritte ein Element $a \in R$
mit $\bar{\phi}(a + IJ) = (b + I, c + J)$ berechnet
werden:

(1) Berechne mit dem Euklidischen Algo-
rithmus Elemente $u, v \in R$ mit
 $ur + vs = \text{ggT}(r, s) = 1_R$

(2) Setze $x = \frac{1}{r} \cdot ur = vs$ und
 $y = \frac{1}{s} \cdot vs = ur$. Dann gilt

$$\bar{\phi}(x + IJ) = (\frac{1}{r}I, 0_R + J) \text{ und}$$

$$\bar{\phi}(y + IJ) = (0_R + I, \frac{1}{s}J)$$

Teiler -
IR
kann
 $a \in R$
ist
Algo -

(3) Setze $a = bx + cy$. Dann gilt

$$\Phi(a + I) = (b + I, c + I)$$

Beispiel: $R = \mathbb{Z}$, $r = 5$, $s = 7$

$$1 = \text{ggT}(5, 7) = \underline{3} \cdot 5 + \underline{(-2)} \cdot 7$$

$$\Rightarrow u = 3, v = -2$$

$$\Rightarrow x = v \cdot s = -14, y = u \cdot r = 15$$

Bestimme nun ein $a \in \mathbb{Z}$ mit

$$\Phi(a + 35\mathbb{Z}) = (2 + 5\mathbb{Z}, 6 + 7\mathbb{Z}), \text{ wobei}$$

$\Phi: \mathbb{Z}/35\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ den Isom aus dem Chin. Restsatz bezeichnet.

$$\text{Setze } a = 2 \cdot x + 6 \cdot y = 2 \cdot (-14) + 6 \cdot 15 = 62$$

$$62 + 35\mathbb{Z} = 27 + 35\mathbb{Z} \Rightarrow \boxed{\Phi(27 + 35\mathbb{Z}) = (2 + 5\mathbb{Z}, 6 + 7\mathbb{Z})}$$