F22T3A3 (Fortsetzung)

geg: $R = \mathbb{Z}[i]$ Ring der Gaußschen Zahlen

in (a) gezeigt: $R^\times = \{\pm 1, \pm i\}$

(b) Seien $z, w \in R$. z.zg.: Genau dann sind z und w assoziiert (Notation: $z \sim w$), wenn $z^4 = w^4$ gilt.

(Nach Def. bedeutet $z \sim w$, dass $z \mid w$ und $w \mid z$ gilt.)

Da R ein Integritätsbereich ist (als Teilring

des Körpers $\mathbb{C}$), ist $w \sim z$ äquivalent zu $w = \varepsilon z$ für ein $\varepsilon \in R^*$. Für alle $\varepsilon \in R^* = \{\pm 1, \pm i\}$ gilt $\varepsilon^4 = 1$. Aus $w = \varepsilon z$ mit $\varepsilon \in R^*$ folgt also $w^4 = \varepsilon^4 \cdot z^4 = 1 \cdot z^4 = z^4$.

Sei nun $z^4 = w^4$ voraus. 1. Fall: $z = 0$

Dann folgt $w^4 = 0^4 = 0 \Rightarrow w = 0 \Rightarrow w \sim z$ da 0 zu sich selbst assoziiert ist

2. Fall $z \neq 0$ $w^4 = z^4 \Rightarrow \left(\frac{w}{z}\right)^4 = 1 \Rightarrow$

$\frac{w}{z}$ ist Nullstelle von $X^4 - 1 = (x^2 - 1)(x^2 + 1) =$

$(x-1)(x+1)(x+i)(x-i) \Rightarrow \frac{w}{z} \in \{\pm 1, \pm i\}$

Setzen wir $\varepsilon = \frac{w}{z}$, dann gilt also $\varepsilon \in R^\times$ und

$w = \varepsilon \cdot z \Rightarrow w \sim z$

(c) Bestimmen Sie einen Erzeuger $a \in \mathbb{Z}$ des Ideals

$I = (1-i) \cap \mathbb{Z}$ (mit Nachweis)

Sei $a = 2$. Beh: $\mathbb{Z}a = (1-i) \cap \mathbb{Z}$

„$\subseteq$" genügt z.zg: $a \in (1-i) \cap \mathbb{Z}$, da $\mathbb{Z}a$ ein Ideal in $\mathbb{Z}$ ist. Offensichtlich gilt $a = 2 \in \mathbb{Z}$, außerdem: $a = 2 = (1+i)(1-i) \in (1-i)$

„$\supseteq$" Sei $b \in (1-i) \cap \mathbb{Z}$ z.zg: $b \in 2\mathbb{Z}$

$b \in (1-i) \Rightarrow \exists \gamma \in \mathbb{Z}[i]$ mit $b = (1-i) \cdot \gamma$

Sei $N: \mathbb{C} \to \mathbb{R}_+$ gegeben durch $N(z) = z\bar{z} = |z|^2$

für alle $z \in \mathbb{C}$ $\Rightarrow N(\beta) = N((1-i)\cdot\gamma) =$

$N(1-i)N(\gamma) \Rightarrow \beta^2 = 2 \cdot N(\gamma) \Rightarrow 2 \mid \beta^2 \overset{2 \text{ Primzahl}}{\Longrightarrow}$

$2 \mid \beta \Rightarrow \beta \in 2\mathbb{Z}$ □

F23T2A3 Sei $R = \{x + y\sqrt{-3i} \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Zeigen Sie, dass R ein Ring ist.

Es genügt zu überprüfen, dass R ein Teilring von $\mathbb{C}$ ist. dafür z.zg.:

$1 \in R$ und $\alpha - \beta, \alpha\beta \in R \quad \forall \alpha, \beta \in R$

lring

Es gilt $1 = 1 + 0\cdot\sqrt{-31} \in R$ (wg. $1, 0 \in \mathbb{Z}$).

Seien $\alpha, \beta \in R$. $\Rightarrow \exists\, a, b, c, d \in \mathbb{Z}$ mit

$\alpha = a + b\sqrt{-31}$, $\beta = c + d\sqrt{-31}$. $\Rightarrow \alpha - \beta$

$= (a-c) + (b-d)\sqrt{-31} \in R$ (wg. $a-c, b-d \in \mathbb{Z}$) und $\alpha\beta = (a+b\sqrt{-31})(c+d\sqrt{-31})$

$= (ac - 31bd) + (bc+ad)\sqrt{-31} \in R$

wegen $ac - 31bd,\ bc + ad \in \mathbb{Z}$

(b) Zeigen Sie, dass R nicht faktoriell ist. (Hinweis: $32 = (1+\sqrt{-31})(1-\sqrt{-31})$)

Beh.: Das Element 2 ist in R

(i) irreduzibel (ii) kein Primelement.

Daraus folgt die Aussage, weil in

wegen $ac - 31bd,\ bc + ad \in \mathbb{Z}$

Faktorzellen Ringen die Primelemente genau die irreduziblen Elemente sind.

zu (ii) Sei N die Normfunktion auf R gegeben durch $N(\alpha) = \alpha\bar{\alpha}\ \forall \alpha \in R$. Diese ist multiplikativ, d.h. $N(\alpha\beta) = N(\alpha)N(\beta)$ $\forall \alpha, \beta \in R$. Für alle $a, b \in \mathbb{Z}$ gilt

$N(a + b\sqrt{-31}) = (a + b\sqrt{-31})(a - b\sqrt{-31}) =$

$a^2 + 31b^2 \in \mathbb{N}_0$

Sei $\alpha, \beta \in R$ mit $\alpha\beta = 2$. z.zg.:

$\alpha \in R^\times$ oder $\beta \in R^\times$ $\quad N(\alpha\beta) = N(2)$

$\Rightarrow N(\alpha)N(\beta) = 4 \overset{N(\alpha), N(\beta) \in \mathbb{N}_0}{\Longrightarrow}$

$N(\alpha) = 1$ oder $N(\beta) = 1$ oder $N(\alpha) = N(\beta) = 2$

1. Fall: $N(\alpha) = 1$ oder $N(\beta) = 1$

O.B.d.A. setze $N(\alpha) = 1$ voraus. Schreibe

zu (ii)

E
Re
Al

F25

und
$\forall a,$
N in

(a) Ze
ex

(b) Be

zu (a)

$\alpha = a + b\sqrt{-31}$ mit $a, b \in \mathbb{Z}$ $\Rightarrow a^2 + 31b^2 = 1$

$\Rightarrow b = 0,\ a^2 = 1 \rightarrow b = 0,\ a \in \{\pm 1\} \rightarrow \alpha \in \{\pm 1\}$

Daraus folgt $\alpha \in R^\times$, denn ± 1 sind offenbar Einh. in R.

2. Fall: $N(\alpha) = N(\beta) = 2$

Seien $a, b \in \mathbb{Z}$ mit $\alpha = a + b\sqrt{-31}$ $\Rightarrow$

$a^2 + 31b^2 = 2 \Rightarrow b = 0,\ a^2 = 2$ $\lightning$ da 2 kein Quadrat in $\mathbb{Z}$ ist.

zu (ii) Aus $2 \mid 32$ folgt $2 \mid (1+\sqrt{-31})(1-\sqrt{-31})$

Angenommen, 2 ist Primelement in R. Dann folgt $2 \mid (1+\sqrt{-31})$ oder $2 \mid (1-\sqrt{-31})$ $\Rightarrow$

$\exists \gamma \in R$ mit $2\gamma \in \{1 \pm \sqrt{-31}\}$ $\Rightarrow$

$\gamma \in \{\frac{1}{2} \pm \frac{1}{2}\sqrt{-31}\}$ Aber $\frac{1}{2} \pm \frac{1}{2}\sqrt{-31}$ sind keine

zu (ii) Aus $2 \mid 32$ folgt $2 \mid (1+\sqrt{-31})(1-\sqrt{-31})$

Elemente aus R, weil alle Elemente aus R einen Realteil in $\mathbb{Z}$ besitzen. $\lightning$

Also ist 2 kein Primelement. $\square$

F25T3A5 Sei $R = \mathbb{Z}[\sqrt{3}]$, $K = \mathbb{Q}(\sqrt{3})$ und $N : K \to \mathbb{Q}$ gegeben durch $N(a+b\sqrt{3}) = a^2 - 3b^2$ $\forall a, b \in \mathbb{Q}$. Es darf verwendet werden, dass N multiplikativ ist.

(a) Zeigen Sie: Sind $\alpha, \beta \in R$ mit $\beta \neq 0$, dann existiert ein $\gamma \in R$ mit $|N(\frac{\alpha}{\beta} - \gamma)| < 1$

(b) Beweisen Sie, dass R ein euklidischer Ring ist.

zu (a) Seien $\alpha, \beta \in R$ mit $\beta \neq 0$

und $\rho \in R$ mit $\alpha = \gamma\beta + \rho$, wobei $\rho = 0$ oder $h(\rho) < h(\beta)$, wobei $h: R \setminus \{0\} \to \mathbb{N}$ durch $h(x)$

Wegen $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{3})$ gibt es $r, s \in \mathbb{Q}$ mit $\frac{\alpha}{\beta} = r + s\sqrt{3}$

Wähle $r_0, s_0 \in \mathbb{Z}$ mit $|r - r_0| \leq \frac{1}{2}$, $|s - s_0| \leq \frac{1}{2}$.

Setze $\gamma = r_0 + s_0\sqrt{3}$. Dann gilt $N\left(\frac{\alpha}{\beta} - \gamma\right) =$

$N\left((r + s\sqrt{3}) - (r_0 + s_0\sqrt{3})\right) = N\left((r - r_0) + (s - s_0)\sqrt{3})\right)$

$= (r - r_0)^2 - 3(s - s_0)^2 \Rightarrow \left|N\left(\frac{\alpha}{\beta}\right) - \gamma\right| =$

$\left|(r - r_0)^2 - 3(s - s_0)^2\right| \leq \max\{(r - r_0)^2, 3(s - s_0)^2\}$

$\leq \max\left\{\frac{1}{4}, \frac{3}{4}\right\} = \frac{3}{4} < 1$ $\quad \uparrow (r - r_0)^2 \geq 0,\ (s - s_0)^2 \geq 0$

zu (6) Beh.: Die Funktion $\alpha \mapsto |N(\alpha)|$ ist eine Höhenfunktion auf R.

Seien $\alpha, \beta \in R$ mit $\beta \neq 0$. z.zg: $\exists \gamma \in R$ und $\rho \in R$ mit $\alpha = \gamma\beta + \rho$, wobei $\rho = 0$ oder $h(\rho) < h(\beta)$, wobei $h: R \setminus \{0\} \to \mathbb{N}$ durch $h(\alpha) = |N(\alpha)|$ definiert ist. (Ist $a + b\sqrt{3} \in R$ mit $a, b \in \mathbb{Z}$ $(a, b) \neq (0, 0)$, dann folgt $N(a + b\sqrt{3}) = a^2 - 3b^2 \neq 0$, weil $\sqrt{3}$ irrational ist. Also erfüllt h tatsächlich nicht nur nach N_0, sondern nach N ab.)

Teil (a) $\Rightarrow \exists \gamma \in R$ mit $|N(\frac{\alpha}{\beta} - \gamma)| < 1$.

Setze $\rho = \alpha - \gamma\beta$, dann gilt $\alpha = \gamma\beta + \rho$.

Angenommen, es ist $\rho \neq 0$. z.zg.: $h(\rho) < h(\beta)$

Sei $\alpha + I \in R/I$, mit $\alpha \in R$. $\rightarrow \exists c, d \in \mathbb{Z}$

Es gilt $h(\rho) = |N(\alpha - \gamma\beta)| =$

$|N((\frac{\alpha}{\beta} - \gamma) \cdot \beta)| = |N(\frac{\alpha}{\beta} - \gamma)| \cdot |N(\beta)|$

$< 1 \cdot |N(\beta)| = |N(\beta)| = h(\beta)$ □

$N(\beta) \neq 0$ Übung: F14T3A3

F16T2A2 Sei $R = \mathbb{Z}[i]$ und $I = 25\mathbb{Z} + (7+i)\mathbb{Z}$ Ohne Beweis darf verwendet werden, dass I ein Ideal in R ist.

(a) Zeigen Sie, dass die Abbildung

$\phi: \mathbb{Z} \rightarrow R/I$, $a \mapsto a + I$ surjektiv ist, und

bestimmen See den Kern.

Nachweis der Surjektivität:

Sei $\alpha + I \in R/I$, mit $\alpha \in R$. $\Rightarrow \exists c, d \in \mathbb{Z}$ mit $\alpha = c + id$. z.zg: $\exists a \in \mathbb{Z}$ mit $\phi(a) = \alpha + I$

gleichbedeutend: $\exists a \in \mathbb{Z}$ mit $a + I = c + id + I$

Es gilt $7 + i \in I \Rightarrow i - (-7) \in I \Rightarrow$

$i + I = -7 + I \Rightarrow c + id + I =$

$(c + I) + (i + I) \cdot (d + I) = (c + I) + (-7 + I) \cdot (d + I)$

$= (c - 7d) + I$ Also gilt $\phi(c - 7d) = \alpha + I$.

Bestimmung des Kerns:

Für alle $a \in \mathbb{Z}$ gilt die Äquivalenz

$a \in \ker(\phi) \iff \phi(a) = 0_{R/I} \iff$

$a + I = I \iff a \in I \iff \exists\, b, c \in \mathbb{Z}$ mit

$a = 25b + (7+i)c = 25b + 7c + ic$

$a \in R \iff \exists\, b \in \mathbb{Z} : a = 25b \iff a \in 25\mathbb{Z}$

$c = 0$

Also ist $\ker(\phi) = 25\mathbb{Z}$

(b) Zeigen Sie, dass $(R/I)^\times$ zyklisch von Ordnung 20 ist

Aus Teil (a) folgt mit dem Homomorphiesatz für Ringe, dass $\mathbb{Z}/\ker(\phi) = \mathbb{Z}/25\mathbb{Z}$ isomorph zu R/I ist (als Ring).

Aus $R/I \cong \mathbb{Z}/25\mathbb{Z}$ folgt $(R/I)^\times \cong (\mathbb{Z}/25\mathbb{Z})^\times$

Da 25 Potenz einer ungeraden Primzahl ist, ist $(\mathbb{Z}/25\mathbb{Z})^\times$ zyklisch, damit auch $(R/I)^\times$, und die Ordnung ist gegeben durch $\varphi(25) = \varphi(5^2) = 5^1 \cdot (5-1) = 5 \cdot 4 = 20$.

(c) Bestimmen Sie die Anzahl der erzeugenden Elemente der zyklischen Gruppe $(R/I)^\times$.

Allgemein gilt: Ist G zyklisch von Ordnung n, $n \in \mathbb{N}$ und $g \in G$ mit $G = \langle g \rangle$, dann gibt es in G genau $\varphi(n)$ erzeugende Elemente (nämlich g^a mit $0 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$). Hier ist gesuchte Anzahl also $\varphi(20) = \varphi(4) \cdot \varphi(5) = 2 \cdot 4 = 8$. □