H24T3A2 geg.: $f = x^3 + x \in \mathbb{Z}[x]$

und $R = \mathbb{Z}[x]/(f)$

In Teil (a) gezeigt: Durch $\alpha : R \to \mathbb{Z} \times \mathbb{Z}[i]$, $g + (f) \mapsto (g(0), g(i))$ ist ein Isomorphismus von Ringen definiert.

(b) Bestimmen Sie alle Einheiten von $\mathbb{Z} \times \mathbb{Z}[i]$.

Laut Vorlesung gilt $\mathbb{Z}^\times = \{\pm 1\}$ und $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$

Dadurch erhält man $(\mathbb{Z} \times \mathbb{Z}[i])^\times = \mathbb{Z}^\times \times (\mathbb{Z}[i])^\times$

$= \{\pm 1\} \times \{\pm 1, \pm i\} = \{(c,d) \mid c \in \{\pm 1\}, d \in \{\pm 1, \pm i\}\}$.

(c) Bestimmen Sie alle Paare $(a, b) \in \mathbb{Z}^2$ mit der Eigenschaft, dass $x^2 + ax + b + (f)$ eine Einheit in R ist.

zu (c) Da α ein Ringisomorphismus ist (der die Einheiten von R bijektiv auf die Einheiten von $\mathbb{Z} \times \mathbb{Z}[i]$ abbildet, gilt die Gleichung $R^\times = \alpha^{-1}((\mathbb{Z} \times \mathbb{Z}[i])^\times)$. Für alle $(a, b) \in \mathbb{Z}^2$ gilt somit die Äquivalenz

$$\begin{gathered}
x^2 + ax + b + (f) \in R^\times \quad \Leftrightarrow \\
\alpha(x^2 + ax + b + (f)) \in (\mathbb{Z} \times \mathbb{Z}[i])^\times \quad \Leftrightarrow \\
(0^2 + a \cdot 0 + b, i^2 + a \cdot i + b) \in \{\pm 1\} \times \{\pm 1, \pm i\} \quad \Leftrightarrow \\
(b, b - 1 + ai) \in \{\pm 1\} \times \{\pm 1, \pm i\} \quad \Leftrightarrow \\
b \in \{\pm 1\} \wedge b - 1 + ai \in \{1, -1, i, -i\} \quad \Leftrightarrow \\
b \in \{\pm 1\} \wedge (a, b) \in \{(0, 2), (0, 0), (1, 1), (-1, 1)\} \quad \Leftrightarrow \\
(a, b) \in \{(1, 1), (-1, 1)\}.
\end{gathered}$$

Also ist $\{(1, 1), (-1, 1)\}$ die Menge der gesuchten Paare.

Quadratische Zahlringe

Erinnerung: Die quadratischen Zahlringe wurden folgendermaßen gebildet: Für jedes $d \in \mathbb{Z}$ betrachten wir $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Im Fall $d \equiv 1 \ (4)$ betrachten wir zu-

$\land a=0)$

die

$\square$

...ischen

...maßen

betrachteten

$\in \mathbb{Z}\}$.

... zu-

sätzlich $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})] = \{\frac{1}{2}a+\frac{1}{2}b\sqrt{d} \mid a,b\in\mathbb{Z}$ und $a\equiv b\ (2)\}$

wichtigste Vertreter:

$d=-1$ Ring der Gauß'schen Zahlen $\mathbb{Z}[i]$

$d=-3$ Ring der Eisenstein-Zahlen $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$

Setze nun voraus, dass $d\in\mathbb{Z}\setminus\{0,1\}$ und quadratfrei ist (d.h. $p^2\nmid d$ für alle Primzahlen p). Dann existiert auf $\mathbb{Q}(\sqrt{d})=\{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\}$ ein Automorphismus σ_d gegeben durch $\sigma(a+b\sqrt{d})=a-b\sqrt{d}$. Die Abbildung $N_d:\mathbb{Q}(\sqrt{d})\to\mathbb{Q}$, $\alpha=a+b\sqrt{d}\mapsto\alpha\cdot\sigma_d(\alpha)=$

$(a+b\sqrt{...}$

als No...

zeichn...

auf $\mathbb{Z}$

Fall d ...

N_d mit

$=0$ nu...

wichtige

N_d ist ...

$N_d(\alpha\beta)$

$\mathbb{Q}(\sqrt{...})$

$\pm b\sqrt{d}$ |

len $\mathbb{Z}[i]$

ahlen $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$

$\{0,1\}$ und

für alle Prim-

$\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d}$

σ_d gegeben

Die Abbildung

$\alpha \cdot \sigma_d(\alpha) =$

$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2$ wird als <u>Normfunktion</u> auf $\mathbb{Q}(\sqrt{d})$ bezeichnet. Durch Einschränkung auf $\mathbb{Z}[\sqrt{d}]$ oder $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ im Fall $d \equiv 1 \ (4)$ erhält man eine Abb. N_d mit Werten in $\mathbb{Z}$, wobei $N_d(\alpha) = 0$ nur für $\alpha = 0$ gilt.

wichtige Eigenschaft: Die Abbildung N_d ist multiplikativ, d.h. es gilt $N_d(\alpha\beta) = N_d(\alpha) N_d(\beta)$ für alle α, β aus $\mathbb{Q}(\sqrt{d})$.

Erinn

R e

(i) F

ge

(ii) J

α

(iii) Q

und

dann

wird
le-

ung
)] um
e Alle
$N_d(\alpha)$

Abbildung
gilt
e α, β aus

<u>Erinnerung</u>: Sei $d \in \mathbb{Z}$ wie oben und R ein quadratischer Zahlring in $\mathbb{Q}(\sqrt{d})$.

(i) Für alle $\alpha \in R$ gilt $N(\alpha) \in \{\pm 1\}$ genau dann, wenn α in $R^\times$ liegt.

(ii) Ist $|N(\alpha)|$ eine Primzahl, dann ist α im Ring R ein irreduzibles Element.

(iii) Gilt $|N(\alpha)| = p^2$ für eine Primzahl p und existiert kein $\beta \in R$ mit $|N(\beta)| = p$, dann ist α in R irreduzibel.

Bem: (i) In einigen Fällen wird die Abbildung $\alpha \mapsto |N(\alpha)|$ auf R zu einer Höhenfunktion, und R ist dann ein euklidischer Ring. Ist $R = \mathbb{Z}[\sqrt{d}]$, so gilt dies z.B. für $d = -1, -2, 2, 3$. Im Fall $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$, $d \equiv 1 \ (4)$, gilt dies unter anderem für $d = -3, -7, -11$.

(ii) In anderen Fällen gilt dies nicht. Zum Beispiel sind $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-5}]$ keine euklidischen Ringe.

$=1$ genau

und die

$1, \pm i$.

$a^2+b^2=2$

$\in \{\pm 1\} \Longleftrightarrow$

$, -1-i\}$

3 Aus a^2+b^2

$\Longrightarrow a^2+b^2 \leq 2$ ↯

Elemente mit

$4 \overset{|a|,|b|\leq 2}{\Longleftrightarrow}$

$(-2,0), (0,-2)\}$

H24T2A4

Sei $R=\mathbb{Z}[i]$, der Ring der Gaußschen Zahlen, und $N: R \to \mathbb{N}_0$ die Normabbildung geg. durch $N(\alpha) = \alpha\bar{\alpha} = a^2+b^2$ für alle $\alpha = a+ib \in R$ (mit $a, b \in \mathbb{Z}$)

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

Sei $\alpha = a+ib \in R$ mit $a, b \in \mathbb{Z}$.

Es gilt die Äquivalenz $N(\alpha)=0$

$\Longleftrightarrow a^2+b^2=0 \Longleftrightarrow a=b=0 \Longleftrightarrow$

$\alpha = 0$

Bem:

auf

ein ei

dies z

$\mathbb{Z}[\frac{1}{2}($

$d=-3$

(ii) In

$\mathbb{Z}[$

$\overset{|a|,|b| \leq 2}{\Longleftrightarrow}$

$4) \Longleftrightarrow$

$2+i,$

$1+2i \}$

$4+4+0+4+8$

5 in R

$, 5$ als Pro-

elemente aus R dar

$)$, und da $N(1+i) =$

hl ist, sind ± 2

Laut Vorlesung gilt $N(\alpha) = 1$ genau dann, wenn $\alpha \in R^\times$ ist, und die Einheiten in R sind $\pm 1, \pm i$.

ebenso: $N(\alpha) = 2 \Longleftrightarrow a^2 + b^2 = 2$

$\overset{|a|,|b| \leq 1}{\Longleftrightarrow} a \in \{\pm 1\}$ und $b \in \{\pm 1\} \Longleftrightarrow$

$\alpha \in \{1+i, 1-i, -1+i, -1-i\}$

$N(\alpha) = 3 \Longleftrightarrow a^2 + b^2 = 3$. Aus $a^2 + b^2 = 3$ folgt $|a|, |b| \leq 1 \Rightarrow a^2 + b^2 \leq 2$ ↯

Also gibt es in R keine Elemente mit Norm 3.

$N(\alpha) = 4 \Longleftrightarrow a^2 + b^2 = 4 \overset{|a|,|b| \leq 2}{\Longleftrightarrow}$

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

H24

Sei R

Gauß'sc

die N

$N(\alpha)$

$\alpha = a +$

(a) Best

de

Sei $\alpha =$

Es gilt d

$\Longleftrightarrow a^2 +$

$\alpha = 0$

…el nach
…t mit
…laut Vl. im

…$-i)^2$, und
…d $1 \pm i$ in R

…$i)$, und weil
…e Primzahl ist
…lemente in R.

$\alpha \in \{\pm 2, \pm 2i\}$.

$N(\alpha) = 5 \Leftrightarrow a^2 + b^2 = 5 \overset{|a|,|b| \leq 2}{\Longleftrightarrow}$

$(a^2 = 4 \wedge b^2 = 1) \vee (a^2 = 1, b^2 = 4) \Leftrightarrow$

$\alpha \in \{2+i, 2-i, -2-i, -2+i,$
$1+2i, 1-2i, -1-2i, -1+2i\}$

Insgesamt gibt es also $1+4+4+0+4+8$
$= 21$ Elemente der Norm ≤ 5 in R.

(b) Stellen Sie 2, 3, 4, 5 als Produkte irreduzibler Elemente aus R dar.

Es gilt $2 = (1+i)(1-i)$, und da $N(1+i) = N(1-i) = 2$ eine Primzahl ist, sind ± 2 irreduzibel.

La…
da…
Ei…
eben…
$|a|, |b|$…
$\Leftrightarrow$
$\alpha \in$…
$N(\alpha)$…
$= 3$
Also…
Norm…
$N(\alpha)$…
(a, b)…

ass

$i, 1+3i)$

$R/(\delta)$

er Ring

Daraus

$(\delta) = I$ gilt,

$= 5+10i$ und

nisse von

$(1-2i)(1+2i)$

reduzible Fak-

Wegen $N(\beta) = 9 = 3^2$, und weil nach Teil (a) in R kein Element mit Norm 3 existiert, ist 3 laut Vl. im Ring R irreduzibel.

Es gilt $4 = 2^2 = (1+i)^2(1-i)^2$, und wie bereits bemerkt, sind $1 \pm i$ in R irreduzibel.

Es gilt $5 = (2+i)(2-i)$, und weil $N(2+i) = N(2-i) = 5$ eine Primzahl ist, sind $2 \pm i$ irreduzible Elemente in R.

$\alpha \in (1\pm$

$N(\alpha) =$

$(a^2 = 4$

$\alpha \in (2$

$1+2$

Insgesa

$= 21$

(b) Ste

duk

Es g

$N(1-i$

irredu

<u>zu (c)</u> Bestimmen Sie ein $\delta \in R$, so dass das Hauptideal (δ) mit $I = (5+10i, 1+3i)$ übereinstimmt. Begründen Sie, dass $R/(\delta)$ ein Körper ist.

Laut Vorlesung ist $\mathbb{Z}[i]$ ein euklidischer Ring und somit auch ein Hauptidealring. Daraus folgt, dass für jedes $\delta \in R$ genau dann $(\delta) = I$ gilt, wenn δ ein größter gem. Teiler (ggT) von $\alpha = 5+10i$ und $\beta = 1+3i$ ist. Auf Grund der Ergebnisse von Teil (b) ist $\alpha = 5(1+2i) = (1+2i)(1-2i)(1+2i)$ $= (1+2i)^2$ eine Zerlegung von α in irreduzible Faktoren. (Alle Faktoren haben Norm 5, dies ist eine Primzahl!)

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

$$\frac{1}{5}(7+i) = \frac{7}{5} + \frac{1}{5}i \notin R$$

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

liegt in $R \Rightarrow \beta = (-1+i)(1-2i)$

Weil $N(-1+i) = 2$ und $N(-1-2i) = 5$ Primzahlen sind, ist dies ebenfalls eine Zerlegung in irreduzible Faktoren. Die Zerlegungen von α und β (und die Tatsache, dass $-1+i$ kein Teiler von $1 \pm 2i$ ist, wegen $2 \nmid 5$) zeigen, dass $\delta = 1-2i$ ein ggT von α und β ist, also $I = (\delta)$ für dieses Element erfüllt ist.

=

$-1+i$

zahlen

reduzible

die Tat-

gen $2+5$)

Laut Vorlesung ist $R/(\delta)$ genau dann ein Körper, wenn (δ) in R ein maximales Ideal ist. Da R ein Hauptidealring ist, ist die Maximalität von (δ) äquivalent zur Irreduzibilität des Elements δ. Da $N(\delta) = 5$ eine Primzahl ist, ist δ tatsächlich ein irreduzibles Element. $\square$

Übung: F24T2A1(a), F24T3A1(d), F21T1A1

F22T

(a) B

R

Sei N

$N(a+$

Diese

d.h. N

$N(\alpha)N$

$\alpha\bar{\alpha}$, N

insgesamt

$\alpha\bar{\alpha}\beta\bar{\beta}$

genau dann
ein maxima-
Hauptideal-
alität von
zibilität
$(\delta) = 5$ eine
sächlich ein
$\square$

F24T3A1(d),

<u>F22T3A3</u> Sei $R = \mathbb{Z}[i]$.

(a) Bestimmen Sie die Einheitengruppe $R^\times$ (mit Nachweis der Korrektheit).

Sei $N : R \to \mathbb{N}_0$ definiert durch
$N(a+ib) = a^2 + b^2 \;\forall\, a, b \in \mathbb{Z}$.
Diese Abbildung ist multiplikativ, d.h. für alle $\alpha, \beta \in R$ gilt $N(\alpha\beta) = N(\alpha)N(\beta)$, denn: Nach Def. gilt $N(\alpha) = \alpha\bar{\alpha}$, $N(\beta) = \beta\bar{\beta}$ und $N(\alpha\beta) = \alpha\beta\overline{(\alpha\beta)}$, insgesamt also $N(\alpha\beta) = \alpha\beta\overline{(\alpha\beta)} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$.

Sei n
$\alpha\beta =$
$= N$
Schrei
dann f
(a, b)
$\Rightarrow \alpha$
Andere
wegen
Einheit
<u>Übung</u>:
Ring $\mathbb{Z}$

ngsgruppe

ektheit).

h

$\in \mathbb{Z}$.

kahir,

$N(\alpha\beta) =$

gilt $N(\alpha) =$

$= \alpha\beta\,\overline{(\alpha\beta)}$

$= \alpha\beta\,\bar{\alpha}\,\bar{\beta} =$

Sei nun $\alpha \in R^\times$. $\Rightarrow \exists\, \beta \in R$ mit $\alpha\beta = 1$. $\Rightarrow N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1 \overset{N(\alpha),\,N(\beta)}{\underset{\in \mathbb{N}_0}{\Longrightarrow}} N(\alpha) = 1$

Schreiben wir $\alpha = a + ib$ mit $a, b \in \mathbb{Z}$, dann folgt $a^2 + b^2 = N(\alpha) = 1$. $\Rightarrow$
$(a,b) \in \{(1,0), (-1,0), (0,1), (0,-1)\}$
$\Rightarrow \alpha \in \{\pm 1, \pm i\}$, also: $R^\times \subseteq \{\pm 1, \pm i\}$

Andererseits sind die vier Elemente wegen $1 \cdot 1 = (-1)\cdot(-1) = i \cdot (-i) = 1$ alles Einheiten in R. $\Rightarrow R^\times = \{\pm 1, \pm i\}$.

Übung: Bestimmen Sie die Einheiten im Ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, mit Nachweis der Korrektheit.