Euklidische Ringe und quadr. Zahlringe

Def. euklidischer Ring (oder euklidischer Bereich) = Integritätsbereich, auf dem eine Höhenfunktion existiert

Dabei ist eine Höhenfunktion auf einem Ring R eine Abbildung $h: R \setminus \{0_R\} \to \mathbb{N}_0$ mit folgender Eigenschaft: Für bel. Elemente $a, b \in R$ mit $b \neq 0_R$ gibt es $q, r \in R$ mit $a = qb + r$, wobei entweder $r = 0_R$ oder $h(r) < h(b)$ gilt.

Euklidische Ringe und quadr. Zahlringe

Def.: euklidischer Ring (oder euklidischer Bereich) =

Beispiele für euklidische Ringe:

(1) $R = \mathbb{Z}$, mit $h(a) = |a|$ als Höhenfunktion

(2) $R = K[x]$, wobei K einen Körper bezeichnet

Hier ist $h(f) = \text{grad}(f)$ eine Höhenfunktion.

(Hinweis: $\mathbb{Z}[x]$ ist kein euklidischer Ring, noch nicht einmal ein Hauptidealring, denn z.B. ist $I = (2, x)$ in $\mathbb{Z}[x]$ kein Hauptideal. Nachweis als Übung)

(3) einige (!) quadratische Zahlringe

In der Vorlesung hatten wir die folgenden Ringe als quadratische Zahlringe bezeichnet: einerseits Ringe der Form

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$ mit $d \in \mathbb{Z}$ beliebig, und andererseits Ringe der Form

$$\mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{d})\right] = \left\{\tfrac{1}{2}a + \tfrac{1}{2}b\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \,(2)\right\}$$

wobei $d \in \mathbb{Z}$ mit $d \equiv 1 \,(4)$ ist.

besonders wichtig:

$\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ Ring der Gaußschen Zahlen

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

Def: Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei

Dann bezeichnet man die Funktion

$N: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ gegeben durch

$N(a+b\sqrt{d}) = a^2 - db^2 = (a-b\sqrt{d})(a+b\sqrt{d})$

für alle $a, b \in \mathbb{Q}$ als Normfunktion

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

bekannt:

i) Für folgende Ringe ist die Abb. $x \mapsto N(x)$ eine Höhenfunktion, der Ring also euklidisch:

$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$ und $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})]$.

ii) Die Ringe $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ sind ebenfalls euklidisch, mit der Höhenfkt. jeweils gegeben durch $x \mapsto |N(x)|$

Satz: Sei R ein quadratischer Zahlring und $N : R \to \mathbb{N}_0$ eine Normfunktion der angegebenen Form. Dann gilt für alle $\alpha \in R$

(i) $\alpha \in R^\times \iff |N(\alpha)| = 1$

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

(iii) Ist $|N(\alpha)|$ ein Primzahlquadrat p^2 und existiert in R kein Element γ mit $|N(\gamma)| = p$ ist, dann ist α ebenfalls irreduzibel.

(Im Fall $R \subsetneq \mathbb{R}$ nimmt N nur Werte in $\mathbb{N}_0$

an, und somit kann man die Betragsstriche dann weglassen.)

[Übungen zu heute: F21T1A1, F23T2A3, F24T2A1(a)]

H24T2A4 Sei $R = \mathbb{Z}[i]$ und $N: R \to \mathbb{N}_0$ gegeben 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 $N(\alpha) \leq 5$ (mit Nachweis)

Jedes $\alpha \in R$ hat die Form $\alpha = a + ib$ mit $a, b \in \mathbb{Z}$, und es ist $N(\alpha) = a^2 + b^2$. Es genügt also, alle Paare $(a, b) \in \mathbb{Z}^2$ mit

$a^2+b^2 \in \{0,1,2,3,4,5\}$ } aufzuzählen.

einzige Lösung von $a^2+b^2=0$: $(0,0)$

Lsg von $a^2+b^2=1$:

$(1,0), (0,1), (-1,0), (0,-1)$

Lsg von $a^2+b^2=2$:

$(1,1), (-1,-1), (-1,1), (1,-1)$

Lsg von $a^2+b^2=3$: keine

(Ang $a^2+b^2=3 \Rightarrow a^2 \leq 3 \Rightarrow |a| \leq 1$

$\Rightarrow |a| \in \{0,1\} \Rightarrow b^2 = 3-a^2 \in \{2,3\}$ ↯

da 2,3 beides keine Quadrate in $\mathbb{Z}$ sind.)

Lsg von $a^2+b^2=4$:

$(2,0), (-2,0), (0,2), (0,-2)$

Lsg von $a^2+b^2=5$:

$(2,1), (-2,-1), (-2,1), (2,-1), (1,2), (-1,-2), (-1,2), (1,-2)$

Die gesuchte Menge der Einheiten ist also

$\{0, \pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2, \pm 2i, \pm(2+i), \pm(2-i), \pm(1+2i), \pm(1-2i)\}$

(b) Stellen Sie die Einheiten 2, 3, 4, 5, 6 als Produkte irreduzibler Elemente des Rings R dar.

bekannt: $\alpha \in R$, $N(\alpha)$ Primzahl $\Rightarrow \alpha$ irred. in R

$N(1\pm i) = 2$ (Primzahl) Also ist $2 = (1+i)(1-i)$ eine Darstellung als Produkt irred. Elemente.

Lsg von $a^2+b^2=5$.

$N(3)=9$ Primzahlquadrat. Teil (a) $\Rightarrow$ Es gibt in R kein Element der Norm 3. Laut VL folgt daraus, dass 3 selbst in R ein irreduzibles Element ist.

Da $1\pm i$ irred ist, erhalten wir durch $4 = 2\cdot 2 = (1+i)(1-i)(1+i)(1-i)$ eine Darstellung der gewünschten Norm.

$N(2\pm i) = 5$ Primzahl $\Rightarrow 2\pm i$ sind irreduzible Elemente in R.

Also ist $5 = (2+i)(2-i)$ eine Dast. der gew. Form

$6 = 2\cdot 3 = (1+i)(1-i)\cdot 3$, s.o. $\Rightarrow 1\pm i, 3$ sind irred. Elemente in R. Also erfüllt auch diese Prod.-darstellung die Bedingung.

(c) Bestimmen Sie ein $\gamma \in R$, so dass das Ideal $(5+10i, 1+3i)$ mit dem Hauptideal (γ) übereinstimmt, und zeigen Sie, dass $R/(\gamma)$ ein Körper ist.

Da R ein Hauptidealring ist, gilt LL.
Vl. $(5+10i, 1+3i) = (\gamma)$ genau dann, wenn γ in R ein ggT von $5+10i$ und $1+3i$ ist. Da R euklidisch ist, kann ein ggT mit dem euklidischen Algorithmus berechnet werden.

q	a_k	x_k	y_k
	$5+10i$	1	0
	$1+3i$	0	1
3	$2+i$	1	-3
$1+i$	0		

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

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

$= \frac{1}{2}(1+2i)(1-3i) = \frac{1}{2}(7 - i)$

$= 7/2 - \frac{1}{2}i \approx 3$

$5 + 10i - 3 \cdot (1+3i) = 5 + 10i - 3 - 9i$

$= 2 + i$

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

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

Also ist $\gamma = 2+i$ ein Element mit der Eigenschaft $(\gamma) = (5+10i, 1+3i)$

noch zu zeigen: $R/(\gamma)$ ist ein Körper

Teil (b) $\Rightarrow \gamma = 2+i$ ist irreduzibel

Da R faktoriell ist, ist γ damit auch in R ein Primelement. Da R ein Hauptidealring ist, folgt daraus wiederum, dass das Hauptideal (γ) ein maximales Ideal ist. Weil (γ) in R ein max. Ideal ist, ist der Faktorring $R/(\gamma)$ ein Körper. □

...ch auch
...Hauptideal-
...dass das Haupt-
...Wert (r) in
...Faktorring
□

F25T3A5 (übrig: F14T3A3)

geg. $R = \mathbb{Z}[\sqrt{3}]$, $K = \mathbb{Q}(\sqrt{3})$ und $N: K \to \mathbb{Q}$ geg. durch $N(a+b\sqrt{3}) = (a+b\sqrt{3})(a-b\sqrt{3}) = a^2 - 3b^2$ $\forall a, b \in \mathbb{Q}$.

(a) Zeigen Sie, dass für bel. $\alpha, \beta \in R$ mit $\beta \neq 0$ jeweils ein Element $\gamma \in R$ mit $|N(\frac{\alpha}{\beta} - \gamma)| < 1$ existiert.

(Hinweis: Zeigen Sie zunächst, dass $\frac{\alpha}{\beta}$ in der Form $r + s\sqrt{3}$ mit $r, s \in \mathbb{Q}$ dargestellt werden kann.)

Aus der VL ist bekannt, dass die Körpererw. $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ vom Grad 2 ist

(weil 3 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist).
Daraus wiederum folgt, dass $\{1, \sqrt{3}\}$ eine Basis von $K = \mathbb{Q}(\sqrt{3})$ als $\mathbb{Q}$-Vektorraum ist.
Jedes Element aus K, also auch $\frac{\alpha}{\beta}$, kann somit als $\mathbb{Q}$-Linearkombination von $\{1, \sqrt{3}\}$ dargestellt werden $\Rightarrow \exists\, r, s \in \mathbb{Q}$ mit $\frac{\alpha}{\beta} = r + s\sqrt{3}$. Seien $r_0, s_0 \in \mathbb{Z}$ so gewählt, dass $|r - r_0| \leq \frac{1}{2}$ und $|s - s_0| \leq \frac{1}{2}$ gilt. Setze $\gamma = r_0 + s_0\sqrt{3} \in R$

$$\Rightarrow |N(\tfrac{\alpha}{\beta} - \gamma)| = |N((r - r_0) + (s - s_0)\sqrt{3})|$$

$$= |\underbrace{(r - r_0)^2}_{\geq 0} - 3\underbrace{(s - s_0)^2}_{\leq 0}| \leq \max\{(r - r_0)^2, 3(s - s_0)^2\}$$

$$\leq \max\{\tfrac{1}{4}, \tfrac{3}{4}\} = \tfrac{3}{4} < 1$$

3)

(b) Zeigen Sie, dass $R = \mathbb{Z}[\sqrt{3}]$ ein euklidischer Ring ist mit $\alpha \mapsto |N(\alpha)|$ als Höhenfkt., dass also für bel. $\alpha, \beta \in R$ mit $\beta \neq 0$ jeweils $\gamma, \rho \in R$ mit $\alpha = \gamma\beta + \rho$ und $|N(\rho)| < |N(\beta)|$ existieren.

Bem.: Die Abb. $R \to \mathbb{R}_+$, $\alpha \mapsto |N(\alpha)|$ ist multiplikativ

Überprüfe zunächst, dass $\sigma: K \to K$, $a + b\sqrt{3} \mapsto a - b\sqrt{3}$ multiplikativ ist. Seien $a, b, c, d \in \mathbb{Q}$. $(a+b\sqrt{3})(c+d\sqrt{3})$
$= (ac + 3bd) + \sqrt{3}(bc + ad)$. $\Rightarrow$ einerseits $\sigma((a+b\sqrt{3})(c-d\sqrt{3}))$
$= (ac + 3bd) - \sqrt{3}(bc + ad)$, andererseits auch

$b \in \mathbb{Z}$

$\sigma(a+b\sqrt{3})\,\sigma(c+d\sqrt{3}) = (a-b\sqrt{3})(c-d\sqrt{3})$

$= ac + 3bd + \sqrt{3}(-bc - ad) =$

$ac + 3bd - \sqrt{3}(bc + ad)$

Seien $\alpha, \beta \in R \Rightarrow |N(\alpha\beta)| =$

$|\alpha\beta\,\sigma(\alpha\beta)| = |\alpha\beta\,\sigma(\alpha)\sigma(\beta)| =$

$|\alpha\,\sigma(\alpha)| \cdot |\beta\,\sigma(\beta)| = |N(\alpha)| \cdot |N(\beta)|$

$(\Rightarrow$ Beh.$)$

Für jedes $\alpha \in R$, $\alpha = a+b\sqrt{3}$ mit $a, b \in \mathbb{Z}$

gilt $|N(\alpha)| = |\underbrace{a^2 - 3b^2}_{\in \mathbb{Z}}| \in \mathbb{N}_0$

Seien nun $\alpha, \beta \in R$ mit $\beta \neq 0$

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

Setze $\rho = \alpha - \gamma\beta \in \rho$. Dann gilt $\alpha = \gamma\beta + \rho$.

außerdem $|N(\rho)| = |N(\alpha - \gamma\beta)| =$

$|N((\frac{\alpha}{\beta} - \gamma) \cdot \beta)| \overset{s.o.}{=} |N(\frac{\alpha}{\beta} - \gamma)| \cdot |N(\beta)|$

$\overset{(*)}{<} 1 \cdot |N(\beta)| = |N(\beta)|$ □