# Definition der euklidischen Ringe

**Definition (12.3)**

Eine Höhenfunktion auf einem Integritätsbereich $R$ ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung

$$a = qb + r$$

erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt. Ein euklidischer Ring ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

# Beispiele für euklidische Ringe

## Proposition (12.4)

(i) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, denn die Abbildung $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ gegeben durch $h(a) = |a|$ ist eine Höhenfunktion auf diesem Ring.

(ii) Sei $K$ ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Höhenfunktion gegeben durch die Gradabbildung, also $h(f) = \mathrm{grad}(f)$ für alle $f \in K[x] \setminus \{0_K\}$.

(iii) Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, wobei eine Höhenfunktion durch die auf $\mathbb{Z}[i] \setminus \{0\}$ eingeschränkte Normfunktion gegeben ist.

wichtiger Hinweis:

Die meisten quadratischen Zahlringe sind keine euklidischen Ringe, zum Beispiel $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\sqrt{-5}]$ nicht.

# Anwendung: Nullstellen von Polynomen

**Folgerung (12.5)**

Sei $K$ ein Körper und $0 \neq f \in K[x]$.

(i) Ist $a \in K$ eine Nullstelle von $f$, dann gilt $f = (x - a)g$ für ein Polynom $g \in K[x]$.

(ii) Ist $\mathrm{grad}(f) = n$ mit $n \in \mathbb{N}_0$, dann hat $f$ höchstens $n$ Nullstellen in $K$.

Beweis von Folgerung 12.5

geg: Körper $K$, $f \in K[x]$, $f \neq 0_K$

zu (i) Sei $a \in K$ mit $f(a) = 0_K$. z.zg: $\exists\, g \in K[x]$ mit
$f = (x-a)\, g$

$K[x]$ eukl. Ring, mit $g \mapsto \mathrm{grad}(g)$ als Höhenfkt. $\Rightarrow$
$\exists\, g, r \in K[x]$ mit $f = g\cdot(x-a) + r$, wobei $r = 0_K$ oder
$\mathrm{grad}(r) < \mathrm{grad}(x-a)$. Ang. $r \neq 0_K$. $\mathrm{grad}(r) < 1$
$\Rightarrow r \in K^\times \Rightarrow f(a) = g(a)\cdot(a-a) + r = r \neq 0_K$
↯ zur Vor. $f(a) = 0_K$. also: $f = g\cdot(x-a)$

zu (ii) Zeige durch vollst. Induktion über $n \in \mathbb{N}_0$

$\exists\, g, r \in K[x]$ mit $f = g\,(x-a) + r$, wobei $r = 0_K$ oder

$\mathrm{grad}(r) < \mathrm{grad}(x-a)$. Ang. $r \neq 0_K$: $\mathrm{grad}(r) < 1$

Ist $f \in K[x]$, $f \neq 0_K$ mit $\mathrm{grad}(f) = n$, dann hat $f$ höchstens $n$ Nullstellen in $K$.

__Ind.-Anf.__ $n = 0$. Dann liegt $f$ in $K^*$ $\Rightarrow$ $f$ hat keine Nullst. in $K$

__Ind.-Schritt__: $n \to n+1$. Sei $f \in K[x]$ vom Grad $n+1$.

1. __Fall__: $f$ hat keine Nullst. in $K$. Dann ist nichts zu zeigen.

2. __Fall__: $\exists\, a \in K$ mit $f(a) = 0_K$. Teil (i) $\Rightarrow$ $\exists\, g \in K[x]$ mit

(*) $f = (x-a) \cdot g$. Dann ist $g$ vom Grad $n$. Ind.-V. $\Rightarrow$ $g$ hat in $K$ genau $r$ Nullstellen $a_1, \dots, a_r$, mit $r \leq n$.

Wegen (*) ist die Nullstellenmenge von $f$ in $\{a_1, \dots, a_r, a\}$ enthalten. Diese enthält $\leq r+1 \leq n+1$ Elemente. $\square$

# Wichtige Rechenregel für den $\mathrm{ggT}$

**Lemma (12.6)**

Sei $R$ ein Ring, und seien $a, b, q \in R$ mit $b \neq 0$. Dann gilt die Gleichung $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - qb, b)$. Genauer ausformuliert bedeutet das: Ein Ringelement $d$ ist genau dann ein größter gemeinsamer Teiler von $a$ und $b$, wenn $d$ ein größter gemeinsamer Teiler von $a - qb$ und $b$ ist.

## Der euklidische Algorithmus

*Eingabe:* ein euklidischer Ring $R$ mit Höhenfunktion $h$
Elemente $a, b \in R$ mit $b \neq 0$

*Ausgabe:* Elemente $d, x, y \in R$ mit $d = \mathrm{ggT}(a, b)$ und $d = xa + yb$

*Ablauf:* (1) definiere $(a_1, x_1, y_1) = (a, 1, 0)$ und $(a_2, x_2, y_2) = (b, 0, 1)$

(2) Sei das Tupel $(a_n, x_n, y_n)$ bereits definiert.

Wenn $a_n = 0$ ist,
dann setze $d = a_{n-1}$, $x = x_{n-1}$, $y = y_{n-1}$ und gib $d, x, y$ als Ergebnis aus. (Stop)

Ansonsten bestimme $q, r \in R$ mit
$a_{n-1} = qa_n + r$, $r = 0$ oder $h(r) < h(a_n)$.
Definere $(a_{n+1}, x_{n+1}, y_{n+1}) = (r, x_{n-1} - qx_n, y_{n-1} - qy_n)$.
Wiederhole Schritt 2.

# Korrektheit des euklidischen Algorithmus

**Satz (12.7)**

Sei $R$ ein euklidischer Ring mit Höhenfunktion $h$. Der euklidische Algorithmus hält für jedes Paar $(a, b)$ mit $a, b \in R$ und $b \neq 0$ nach einer endlichen Zahl von Wiederholungen. Er liefert als Ausgabe tatsächlich $d = \mathrm{ggT}(a, b)$ und Ringelemente $x, y \in R$ mit $d = xa + yb$.

- Wenn die Schleife im Algorithmus unendlich oft durchlaufen würde, dann wäre $h(a_1) > h(a_2) > h(a_3) > ...$ eine unendliche absteigende Folge in $\mathbb{N}$. Aber eine solche Folge gibt es nicht.

# Anwendungen des Euklidischen Algorithmus

## (1) Berechnung von $\overline{42}^{-1}$ in $\mathbb{F}_{59}$

| $q$ | $a_n$ | $x_n$ | $y_n$ |
|---|---|---|---|
| – | 42 | 1 | 0 |
| – | 59 | 0 | 1 |
| 0 | 42 | 1 | 0 |
| 1 | 17 | −1 | 1 |
| 2 | 8 | 3 | −2 |
| 2 | $\underline{1}$ | $\underline{-7}$ | $\underline{5}$ |
| 8 | 0 | – | – |

Berechne $d = ggT(42, 59)$ und $x, y \in \mathbb{Z}$ mit $42x + 59y = d$.

Ergebnis:

$ggT(42, 59) = 1$
$= \underbrace{(-7)\cdot 42}_{-294} + \underbrace{5 \cdot 59}_{295}$

In $\mathbb{F}_{59}$ gilt $\overline{1} = (\overline{-7})\,\overline{42} + \overline{5}\;\overline{59} = (\overline{-7})\cdot\overline{42} + \overline{5}\;\overline{0} = (\overline{-7})\cdot\overline{42} \Rightarrow \overline{42}^{-1} = -\overline{7} = \overline{52}$

(2) $R = \mathbb{Z}[i]$, $\alpha = 12+14i$, $\beta = 32-6i$

<u>Ziel</u>: Bestimmung von $\delta = \mathrm{ggT}(\alpha, \beta)$ sowie von Elementen $\sigma, \tau \in R$ mit $\sigma \cdot \alpha + \tau \cdot \beta = \delta$

| $q$ | $a_n$ | $x_n$ | $y_n$ |
|---|---|---|---|
| – | $12+14i$ | $1$ | $0$ |
| – | $32-6i$ | $0$ | $1$ |
| $0$ | $12+14i$ | $1$ | $0$ |
| $1-2i$ | $-8+4i$ | $-1+2i$ | $1$ |
| $-1-2i$ | $-4+2i$ | $-4$ | $1+2i$ |
| $2$ | $0$ | | |

Ergebnis:

$\delta = -4+2i$

$\sigma = -4$

$\tau = 1+2i$

Nebenrechnung: $\frac{12+14i}{32-6i} = \frac{(12+14i)(32+6i)}{(32-6i)(32+6i)} = \frac{15}{53} + \frac{26}{53} i \approx 0$

$\frac{32-6i}{12+14i} = \frac{15}{17} - \frac{26}{17} i \approx 1-2i$

$32-6i - (1-2i)(12+14i) = 32-6i - (40-10i) = -8+4i$

$\frac{12+14i}{-8+4i} = \frac{(12+14i)(-8-4i)}{(-8+4i)(-8-4i)} = \frac{1}{80}(-40-160i) = -\frac{1}{2} - 2i \approx -1-2i$

# Korrektheit des euklidischen Algorithmus (Forts.)

- Mit Hilfe von Lemma 12.6 ist leicht zu sehen, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_2, a_3) = \ldots = \mathrm{ggT}(a_{n-1}, a_n) = \mathrm{ggT}(a_{n-1}, 0_R) = a_{n-1}$ gilt, dass im $n$-ten Schritt die Abbruchbedingung $a_n = 0_R$ erfüllt ist. Dies zeigt, dass der korrekte $\mathrm{ggT}$ ausgegeben wird.

- Durch vollständige Induktion zeigt man leicht, dass $a_k = x_k a + y_k b$ für $1 \leq k \leq n-1$ gilt. Insbesondere ist damit $d = a_{n-1} = x_{n-1}a + y_{n-1}b = xa + yb$ erfüllt.

# Euklidische Ringe sind Hauptidealringe

Erinnerung:
Ein Hauptidealring ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

**Satz (12.8)**

Jeder euklidische Ring $R$ ist ein Hauptidealring.

Also sind insbesondere $\mathbb{Z}$, $\mathbb{Z}[i]$ und Polynomringe über Körpern Hauptidealringe.

Beweis von Proposition 12.8

geg: euklidischer Ring $R$, $h: R \setminus \{0_R\} \to \mathbb{N}$
Höhenfunktion auf $R$

Sei $I$ ein Ideal in $R$. z.zg: $\exists\, a \in I$ mit $I = (a)$

O.B.d.A. setze $I \neq (0_R)$ voraus.

Wähle $a \in I \setminus \{0_R\}$ so, dass $h(a)$ minimal ist.

Beh: $I = (a)$ „$\supseteq$" offensichtlich, wegen $a \in I$

„$\subseteq$" Sei $b \in I$, ang. $b \notin (a)$. Division mit Rest liefert $q, r \in R$ mit $b = qa + r$, wobei $r = 0_R$ oder $h(r) < h(a)$.

Rest liefert $q, r \in R$ mit $b = qa + r$, wobei $r = 0_K$ oder $h(r) < h(a)$

1. Fall: $r = 0_K \Rightarrow b = qa \Rightarrow b \in (a)$ ↯ zur Annahme

2. Fall: $r \neq 0_K$ Dann ist $h(r) < h(a)$.

$r = b - qa$, $b \in I$, $a \in I \Rightarrow r \in I \setminus \{0_R\}$

Dann steht $h(r) < h(a)$ im Widerspruch zur Minimalität von $h(a)$.

Also war die Annahme falsch, es gilt $b \in (a)$. $\square$

# Beispiel für einen Nicht-Hauptidealring

Nicht jeder Integritätsbereich ist ein Hauptidealring.

**Proposition (12.9)**

Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring, denn beispielsweise ist das Ideal $\mathfrak{p} = (3, 1 + 2\sqrt{-5})$ kein Hauptideal.

Beweis von Proposition 12.9.

geg.: Ring $R = \mathbb{Z}[\sqrt{-5}]$, Ideal $\mathfrak{p} = (3, 1+2\sqrt{-5})$

z.zg.: $\mathfrak{p}$ ist kein Hauptideal

Es ist $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Die Norm-funktion $N : R \to \mathbb{N}_0$ ist geg. durch

$N(a+b\sqrt{-5}) = a^2 + 5b^2 \quad \forall a, b \in \mathbb{Z}$.

<u>Annahme</u>: Es gibt ein $\gamma \in R$ mit $(\gamma) = \mathfrak{p}$.

$(\gamma) = (3, 1+2\sqrt{-5}) \Rightarrow 3, 1+2\sqrt{-5} \in (\gamma)$

$\Rightarrow \gamma \mid 3$ und $\gamma \mid (1+2\sqrt{-5})$. Allgemein gilt: Sind $\alpha, \beta \in R$ mit $\alpha \mid \beta$, dann

A

e

$\Rightarrow$

folgt $N(\alpha) \mid N(\beta)$. Also ist $N(\gamma)$ ein gemeinsamer Teiler von $N(3) = 9$ und $N(1+2\sqrt{-5}) = 21$. $\Rightarrow N(\gamma)$ ist Teiler von $ggT(9, 21) = 3$

$\Rightarrow N(\gamma) \in \{1, 3\}$

1. Fall: $N(\gamma) = 3 \Rightarrow \exists a, b \in \mathbb{Z}: a^2 + 5b^2 = 3$

$\Rightarrow b = 0, a^2 = 3$ $\lightning$ da 3 kein Quadrat in $\mathbb{Z}$

2. Fall: $N(\gamma) = 1$. Schreibt man $\gamma = a + b\sqrt{-5}$, dann folgt $a^2 + 5b^2 = 1 \Rightarrow a \in \{\pm 1\}, b = 0$

$\Rightarrow \gamma \in \{\pm 1\} \Rightarrow p = (\gamma) = (1) \Rightarrow 1 \in p$

$\Rightarrow \exists \alpha, \beta \in R$ mit $3\alpha + (1+2\sqrt{-5}) \cdot \beta = 1$

Schreibe $\alpha = r + s\sqrt{-5}$, $\beta = t + u\sqrt{-5}$ mit

$r$

$3$

$(3$

$3r$

$3r$

$r,s,t,u \in \mathbb{Z}$ einsetzen $\Rightarrow 3\cdot(r+s\sqrt{-5}) +$

$(1+2\sqrt{-5})\cdot(t+u\sqrt{-5}) = 1 \Rightarrow$

$3r+3s\sqrt{-5}+t-10u+(2t+u)\sqrt{-5}=1 \Rightarrow$

$(3r+t-10u)+(3s+2t+u)\sqrt{-5}=1 \Rightarrow$

$3r+t-10u=1,\ 3s+2t+u=0 \Rightarrow$

$3r+3s+3t-9u=1$ ↯ da $3\nmid 1$ $\square$

# Definition der irreduziblen Elemente

**Definition (12.10)**

Sei $R$ ein Ring. Ein Element $p \in R$ wird irreduzibel genannt, wenn $p$ weder eine Einheit noch Null ist und die Implikation

$$p = ab \quad \Rightarrow \quad a \in R^{\times} \text{ oder } b \in R^{\times}$$

für alle $a, b \in R$ erfüllt ist. Nichteinheiten ungleich Null, die nicht irreduzibel sind, bezeichnen wir als reduzible Ringelemente.

# Definition der Primelemente

**Definition (12.11)**

Sei $R$ ein Ring. Ein Element $p \in R$ heißt Primelement, wenn $p$ weder eine Einheit noch Null ist und außerdem die Implikation

$$p \mid (ab) \quad \Rightarrow \quad p \mid a \quad \text{oder} \quad p \mid b \qquad \text{für alle } a, b \in R \text{ erfüllt ist.}$$

**Satz (12.12)**

In einem Integritätsbereich ist jedes Primelement irreduzibel.

Beweis von Satz 12.12

geg: Integritätsbereich $R$, Primelement $p$

zzg: $p$ ist irreduzibel

$p$ Primelement $\Rightarrow p \neq 0_R$ und $p \notin R^\times$

Seien $a, b \in R$ mit $p = a \cdot b$

z.zg.: $a \in R^\times$ oder $b \in R^\times$

$$p \mid p \Rightarrow p \mid ab \xRightarrow{p \text{ Primelement}} p \mid a \text{ oder } p \mid b$$

O.B.d.A. gelte $p \mid a \Rightarrow \exists\, c \in R$ mit $a = cp$

einsetzen $\Rightarrow p = cp \cdot b \xRightarrow[\text{Kürzungsregel}]{p \neq 0_R} 1_R = c \cdot b$

$\Rightarrow b \in R^\times$ $\square$

Anmerkung: Im Allgemeinen sind irreduzible Elemente nicht notwendigerweise Primelemente

Bsp: $R = \mathbb{Z}[\sqrt{-3}]$ Dann ist 2 in R irreduzibel (Nachweis morgen), aber nicht prim, denn:

$$2 \cdot 2 = 4 = (1+\sqrt{-3})\cdot(1-\sqrt{-3}) \Rightarrow 2 \mid (1+\sqrt{-3})\cdot(1-\sqrt{-3})$$

Wenn 2 prim wäre, dann würde $2 \mid (1+\sqrt{-3})$ oder $2 \mid (1-\sqrt{-3}) \Rightarrow \exists\, \gamma \in R$ mit $2\gamma \in \{1 \pm \sqrt{-3}\}$

$\Rightarrow \gamma \in \{\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}\}$ ↯ da $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3} \notin \mathbb{Z}[\sqrt{-3}]$