__Beispiel__ Betrachte Int-Ring $\mathbb{Z}$ und die Abb.:

$$\mathbb{Z} \longrightarrow \mathbb{Z}_{\geq 0}, \quad a \mapsto |a|.$$

Haben für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$:

(i) $|a| \leq |a| \cdot |b| = |ab|$.

(ii) Es gibt $q, r \in \mathbb{Z}$, sodass

$$a = qb + r, \qquad 0 \leq r < |b|.$$

__Definition__ Euklidischer Ring: Int-Ring R mit Abbildung $\delta : R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$, sodass

(i) Für alle $a, b \in R \setminus \{0_R\}$: $\delta(a) \leq \delta(ab)$.

(ii) Für alle $a \in R$, $b \in R \setminus \{0_R\}$ hat man Darst.:

$$(*) \quad a = qb + r, \quad q, r \in R, \quad \delta(r) < \delta(b) \text{ oder } r = 0_R.$$

Nennen δ Gradabbildung und $(*)$ Division mit Rest.

__Satz__ $\mathbb{Z}[I] = \{m + In;\ m, n \in \mathbb{Z}\}$ ist ein Euklidischer Ring mit Gradabbildung

$$\delta : \mathbb{Z}[I] \setminus \{0\} \to \mathbb{Z}_{\geq 0}, \quad m + In \mapsto m^2 + n^2.$$

__Beweis__ Haben stets $\delta(a) = a\bar{a}$. Damit, für $a = m + In$ und $b = k + Il \neq 0$:

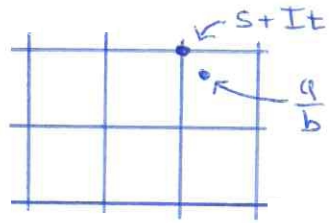
$$\begin{aligned} \delta(a) &\leq \delta(a)(k^2 + l^2) \\ &= \delta(a)\delta(b) \\ &= a\bar{a}\, b\bar{b} = ab\overline{ab} = \delta(ab). \end{aligned}$$

Division mit Rest: Seien $a, b \in \mathbb{Z}[I]$, $b \neq 0$. Schreibe

$$\frac{a}{b} = u + Iv \quad \text{mit } u, v \in \mathbb{R}$$

Wähle $s, t \in \mathbb{Z}$ mit

$$|u - s| \leq \tfrac{1}{2}, \quad |v - t| \leq \tfrac{1}{2}$$



Setze

$$q := s + It \in \mathbb{Z}[I].$$

Dann:

$$a = qb + r, \quad \text{mit } r := a - qb = b\left(\tfrac{a}{b} - q\right)$$

Mit $\delta : \mathbb{C} \to \mathbb{R}_{\geq 0}$, $x + Iy \mapsto x^2 + y^2$:

$$\begin{aligned} \delta(r) = \delta\left(b\left(\tfrac{a}{b} - q\right)\right) &= \delta(b)\,\delta\left(\tfrac{a}{b} - q\right) \\ &= \delta(b)\,\delta(u + Iv - (s + It)) \\ &= \delta(b)\left((u-s)^2 + (v-t)^2\right) \\ &\leq \delta(b)\left(\tfrac{1}{4} + \tfrac{1}{4}\right) < \delta(b). \end{aligned}$$

$\square$

Satz $\Bbbk$ Körper. Betrachte $\Bbbk[T]$ und, für $f = \sum a_\nu T^\nu \in \Bbbk[T]$, Grad:

$$\deg(f) = \begin{cases} \max(\nu \in \mathbb{Z}_{\geq 0} : a_\nu \neq 0_{\Bbbk}), & f \neq 0_{\Bbbk[T]}, \\ -\infty, & f = 0_{\Bbbk[T]}. \end{cases}$$

Dann:

(i) Für alle $f, g \in \Bbbk[T]$ mit $g \neq 0_{\Bbbk[T]}$:

$$\deg(f) \leq \deg(f) + \deg(g) = \deg(fg)$$

(ii) Für alle $f, g \in \Bbbk[T]$ mit $g \neq 0_{\Bbbk[T]}$:

$$f = qg + r, \quad \deg(r) < \deg(g)$$

mit eind. best. $q, r \in \Bbbk[T]$.

Insbes.: $\Bbbk[T]$ eukl. Ring mit Gradabb.:

$$\delta(f) := \deg(f).$$

Beweis Wissen schon: (i) und Existenz von q, r wie in (ii).

Nur noch zu zeigen: q, r aus (ii) sind eindeutig. Sei

$$f = qg + r = q'g + r', \quad \deg(r), \deg(r') < \deg(g).$$

Dann:

$$0_{\Bbbk[T]} = (q - q')g + r - r'$$

Wegen $\deg(r - r') < \deg(g)$: $q - q' = 0_{\Bbbk[T]}$

Somit $q = q'$, $r = r'$. $\square$

Polynomdivision (mit Rest) Betrachte $f = T^3 + 2T + 1$ und $g = T - 1$ in $\mathbb{Q}[T]$:

$$T^3 + 2T + 1 = (T-1)\underbrace{(T^2 + T + 3)}_{q} + \underbrace{4}_{r}$$

$$\begin{array}{l} T^3 + 2T + 1 \\ \underline{-(T^3 - T^2)} \\ T^2 + 2T + 1 \\ \underline{-(T^2 - T)} \\ 3T + 1 \\ \underline{-(3T - 3)} \\ 4 \end{array}$$

__Satz__ Jeder euklidische Ring ist ein Hauptidealring.

__Beweis__ Sei R euklidischer Ring mit Gradabb.

$$\delta : R \setminus \{0_R\} \longrightarrow \mathbb{Z}_{\geq 0}.$$

Zu zeigen: Jedes $\mathfrak{a} \leq_R R$ ist von der Gestalt

$$\mathfrak{a} = \langle b \rangle \quad \text{mit } b \in R.$$

Falls $\mathfrak{a} = \{0_R\}$: ✓ Sei $\mathfrak{a} \neq \{0_R\}$.

Wähle ein $0_R \neq b \in \mathfrak{a}$ mit

$\delta(b) \leq \delta(a)$ für alle $0_R \neq a \in \mathfrak{a}$.

Dann, für jedes $a \in \mathfrak{a}$:

$$a = qb + r$$

mit $q, r \in R$ sodass $\delta(r) < \delta(b)$ oder $r = 0_R$.

Zeigen $r = 0_R$. Sonst:

$$r = a - qb \in \mathfrak{a}$$

mit $\delta(r) < \delta(b)$ ↯ Somit $\mathfrak{a} = \langle b \rangle$. □

__Folgerung__ $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind HIR

Weiter ist $\mathbb{k}[T]$ ein HIR für jeden Körper $\mathbb{k}$.

__Folgerung__ Haben für $\mathbb{Z}$:

(i) Für jedes $p \in \mathbb{Z}_{\geq 0}$ gilt:

p Primzahl $\Leftrightarrow$ p prim.

(ii) $H \leq \mathbb{Z} \Rightarrow H = n\mathbb{Z}$ mit $n \in \mathbb{Z}$.

__Beweis__ Zu (i). Haben:

p Primzahl $\overset{\text{Def}}{\Longleftrightarrow}$ p irreduz. in $\mathbb{Z}$

$\overset{\mathbb{Z}\text{ HIR}}{\Longleftrightarrow}$ p prim in $\mathbb{Z}$.

Zu (ii). Sei $H \subseteq \mathbb{Z}$ Untergruppe. Dann:

$$a \in H, m \in \mathbb{Z} \Rightarrow \begin{array}{l} ma = \underbrace{a + \dots + a}_{m\text{-mal}} \in H \text{ für } m \geq 0 \\ ma = -\underbrace{(a + \dots + a)}_{-m\text{-mal}} \in H \text{ für } m \leq 0 \end{array}$$

Somit: $H \leq_{\mathbb{Z}} \mathbb{Z}$. Wegen $\mathbb{Z}$ HIR:

$H = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. □

Euklidischer Algorithmus R eukl. Ring mit Gradabb. $\delta: R\setminus\{0_R\} \to \mathbb{Z}_{\geq 0}$, $a, b \in R$, $b \neq 0_R$.

Schritt 0: $c_{-1} := a$, $c_0 := b$.

Schritt 1: Wähle $c_1, q_1 \in R$ mit

$c_{-1} = q_1 c_0 + c_1$, wobei $\delta(c_1) < \delta(c_0)$ oder $c_1 = 0_R$.

Falls $c_1 = 0_R$: STOP

Schritt 2: Wähle $c_2, q_2 \in R$ mit

$c_0 = q_2 c_1 + c_2$, wobei $\delta(c_2) < \delta(c_1)$ oder $c_2 = 0_R$

Falls $c_2 = 0_R$: STOP

⋮

Das Verfahren bricht bei einem $n \in \mathbb{Z}_{\geq 0}$ mit $c_n = 0_R$ ab. Dann:

* $c_{n-1} \in \mathrm{ggT}(a,b)$
* $c_{n-1} = ua + vb$, wobei $u, v \in \mathbb{Z}$ explizit durch $q_1, \dots, q_{n-1}$ darstellbar.

Beispiel Betrachten $R = \mathbb{Z}$ mit $\delta(r) = |r|$ sowie $a = 60$ und $b = 42$

Schritt 0: $c_{-1} := 60$, $c_0 := 42$

Schritt 1: $q_1 := 1$, $c_1 := 18$:

$$60 = 1 \cdot 42 + 18$$

Schritt 2: $q_2 := 2$, $c_2 := 6$:

$$42 = 2 \cdot 18 + 6$$

Schritt 3: $q_2 := 3$, $c_3 := 0$:

$$18 = 3 \cdot 6 + 0$$

Damit: $6 \in \mathrm{ggT}(60, 42)$. Weiter:

$$\begin{aligned} 6 &= 42 - \underbrace{2}_{q_2} \cdot 18 && \text{(Schritt 2)} \\ &= 42 - \underbrace{2}_{q_2} \cdot (60 - \underbrace{1}_{q_1} \cdot 42) && \text{(Schritt 1)} \\ &= \underset{u = -q_2}{-2} \cdot 60 + \underset{v = 1 + q_2 q_1}{3} \cdot 42. \end{aligned}$$

__Beweis Eukl. Alg.__ Wegen $0 \le \delta(c_{i+1}) < \delta(c_i)$ bricht das Verfahren bei einem $n \in \mathbb{Z}_{\ge 0}$ ab. Haben dann:

$$
(*) \quad
\begin{aligned}
c_{n-2} &= q_n c_{n-1} \\
c_{n-3} &= q_{n-1} c_{n-2} + c_{n-1} \\
c_{n-4} &= q_{n-2} c_{n-3} + c_{n-2} \\
&\vdots \\
c_1 &= q_3 c_2 + c_3 \\
b = c_0 &= q_2 c_1 + c_2 \\
a = c_{-1} &= q_1 c_0 + c_1
\end{aligned}
$$

Zeigen: $c_{n-1} | a$ und $c_{n-1} | b$. Mit $(*)$:

c_{n-2} Vielfaches von c_{n-1}

$\Rightarrow$ c_{n-3} " " "

$\vdots$

c_1 " " "

Also: c_{n-1} Teiler von $c_{-1} = a$ und $c_0 = b$.

Zeigen: c_{n-1} __größter__ gem. Teiler von a, b.

Schreiben $(*)$ um:

$$
(**) \quad
\begin{aligned}
c_{n-1} &= c_{n-3} - q_{n-1} c_{n-2} && (S_{n-1}) \\
c_{n-2} &= c_{n-4} - q_{n-2} c_{n-3} && (S_{n-2}) \\
&\vdots \\
c_2 &= c_0 - q_2 c_1 && (S2) \\
c_1 &= c_{-1} - q_1 c_0 = a - q_1 b && (S1)
\end{aligned}
$$

Falls $c|a$ und $c|b$ für ein $c \in R$:

$$
\begin{aligned}
c|c_{-1},\ c|c_0 &\Rightarrow c | c_1 \\
&\Rightarrow c | c_2 \\
&\vdots \\
&\Rightarrow c | c_{n-1}.
\end{aligned}
$$

Ebenso mit $(**)$: Schrittweises Einsetzen:

(S1) in (S2), (S2) in (S3), ..., (S_{n-2}) in (S_{n-1})

eliminiert $c_1, \dots, c_{n-2}$ und liefert die gewünschte Darstellung $c_{n-1} = ua + bv$. $\square$