Eigenschaften von Elementen in (Euklidischen) Ringen, ggT

R kommutativer Ring mit 1

Satz: K Körper $\Rightarrow K^* = K \setminus \{0\}$

R^* Menge der Einheiten
$R^* = \{a \in R \mid a \text{ Einheit}\}$

$x \in R$ Einheit
$\exists y \in R: xy = 1$

„invertierbare Elemente im Ring, verhalten sich wie 1"

Satz: $x \in R \setminus \{0\}$ Nullteiler (d.h. $\exists y \in R \setminus \{0\}: xy = 0$) $\Rightarrow$ x keine Einheit

Satz: $a \triangleq b \Leftrightarrow (a) = (b) \Leftrightarrow a \mid b$ und $b \mid a$

$a, b \in R$ assoziiert, $a \triangleq b$
$\exists x \in R^*: a = x \cdot b$

„R Integritätsring"

R nullteilerfrei
$\forall a, b \in R:$
$a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$

b Teiler von a, $b \mid a$
$\exists q \in R: a = q \cdot b$

p irreduzibel
$p \in R \setminus (R^* \cup \{0\})$, und
$\forall a, b \in R:$
$p = a \cdot b \Rightarrow a \in R^*$ oder $b \in R^*$

R nullteilerfrei

R faktoriell

p prim
$p \in R \setminus (R^* \cup \{0\})$, und
$\forall a, b \in R:$
$p \mid a \cdot b \Rightarrow p \mid a$ oder $p \mid b$

R faktoriell
R nullteilerfrei, und $\forall a \in R \setminus (R^* \cup \{0\})$ existieren irreduzible $p_1, \dots, p_r \in R$ mit $a = p_1 \cdot \dots \cdot p_r$, und die Darstellung ist bis auf Reihenfolge und Assoziiertheit eindeutig.
(d.h.: Sind $q_1, \dots, q_s \in R$ irred mit $a = q_1 \cdot \dots \cdot q_s \Rightarrow r = s$ und nach Umnumm. $q_i \triangleq p_i$)

Satz: Rekursive Berechnung ggT:
$ggT(a_1, \dots, a_n) = ggT(ggT(a_1, \dots, a_{n-1}), a_n)$

$ggT(a_1, \dots, a_n)$
$= \{d \in R: d \text{ ggT von } a_1, \dots, a_n\}$

$d \in R$ ist größter gemeinsamer Teiler (ggT) von $a_1, \dots, a_n \in R$
(ggT1) $d \mid a_1, \dots, d \mid a_n$
(ggT2) $\forall c \in R: c \mid a_1, \dots, c \mid a_n \Rightarrow c \mid d$

R Hauptidealring (HIR)
R nullteilerfrei und jedes Ideal in R ist Hauptideal

$\mathbb{Z}[t]$ kein HIR

Satz: Bestimmung von Hauptidealen mit ggT:
R HIR, $a, b \in R \Rightarrow$
$d \in ggT(a, b) \Leftrightarrow (d) = (a, b)$

„Eindeutigkeit des ggT":
$d \in ggT(a_1, \dots, a_n)$. Dann gilt:
- $d_2 \in ggT(a_1, \dots, a_n) \Leftrightarrow d \triangleq d_2$
- $ggT(a_1, \dots, a_n) = \{d \cdot u \mid u \in R^*\}$

Berechnung in euklidischen Ringen

R Euklidischer Ring
R nullteilerfrei und es gibt $\delta: R \setminus \{0\} \to \mathbb{N}_0$ („Gradabbildung"), so dass: $\forall f, g \in R, g \neq 0: \exists r, q \in R:$
$f = q \cdot g + r$ mit $[\delta(r) < \delta(g)$ oder $r = 0]$

- $R = \mathbb{Z}$ mit $\delta(z) := |z|$
- $R = K[t]$ mit $\delta(p) = \text{grad}(p)$, K Körper

R Körper
Zu jedem $r \in R \setminus \{0\}$ existiert r^{-1}

$\delta(r) := 1$

Euklidischer Algorithmus
Für $a, b \in R \setminus \{0\}$.
- Setze $a_0 := a$, $a_1 := b$, und für $n \in \mathbb{N}, n \geq 2$ sei a_n bestimmt durch
- $a_{n-2} = q_{n-2} \cdot a_{n-1} + a_n$ (Def. Eukl. Ring) mit $[\delta(a_n) < \delta(a_{n-1})$ oder $a_n = 0]$.

$\Rightarrow \exists$ kleinstes $m \in \mathbb{N}$ mit $a_{m+1} = 0$.
$\Rightarrow a_m \in ggT(a, b)$.

Erweiterter Euklidischer Algorithmus
Rückwärtseinsetzen gibt Darstellung
$a_m = a_{m-2} - q_{m-2} a_{m-1}$
$= \dots$
$= u \cdot a + v \cdot b$
mit $u, v \in R$