13 Euklidische Ringe

13.1 Def: Ein **Integritätsring** ist ein kommutativer Ring R, in dem gilt:
Ist $a \cdot b = 0$ für $a, b \in R$, so folgt $a = 0$ oder $b = 0$.

Beispiele:

- $\mathbb{Z}$ ist Integritätsring
- Jeder Körper K ist Integritätsring.
  ($a \cdot b = 0$ mit $a \neq 0 \Rightarrow \underbrace{a^{-1} \cdot a \cdot b}_{b} = \underbrace{a^{-1} \cdot 0}_{0}$)
- $\mathbb{Z}/n\mathbb{Z}$ ist Integritätsring $\Leftrightarrow$ n prim
  (Siehe Satz 3.7 & Beweis.
  $(\Leftarrow)$ Falls n prim, ist $\mathbb{Z}/n\mathbb{Z}$ sogar Körper.
  $(\Rightarrow)$ Falls $n = a \cdot b$ mit $a, b > 1$ ist $[a] \cdot [b] = 0$ in $\mathbb{Z}/n\mathbb{Z}$
  aber $[a] \neq 0$ und $[b] \neq 0$)

  (In diesem Fall heißen $[a]$ und $[b]$ Nullteiler.)

- $Mat_{\mathbb{R}}(2 \times 2)$ ist aus zwei Gründen **kein** Integritätsring:
  1. nicht kommutativ
  2. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Weiteres Beispiel:

13.2 Satz:

① Für jeden Integritätsring R ist auch $R[X]$ ein Integritätsring.

② Für jeden Integritätsring R ist $R[X]^\times = R^\times$.

aufgefasst als konstante Polynome

Beweis:

1: Für $A = \sum_{i=0}^{n} a_i X^i$ und $B = \sum_{i=0}^{m} b_i X^i \in R[X]$ mit $a_n \neq 0$ und $b_m \neq 0$ ist auch $a_n \cdot b_m \neq 0$, da R Integritätsring ist. Also folgt aus Satz 3.15 (Gradformel) auch $A \cdot B \neq 0$.

2: Seien A und B wie oben mit $A \cdot B = 1$. Dann folgt aus der Gradformel

$$\underbrace{\deg A}_{\geq 0} + \underbrace{\deg B}_{\geq 0} = 0,$$

also $\deg A = \deg B = 0$.

Also ist $A = a_0$, $B = b_0$, und $a_0 \cdot b_0 = 1$.

Somit $A = a_0 \in R^\times$ (und $B = b_0 \in R^\times$). $\square$

13.3 Notiz (Kürzungsregel)

Für Elemente a, b, c eines Integritätsrings gilt:

$$\begin{pmatrix} ab = ac \\ \wedge\ a \neq 0 \end{pmatrix} \Rightarrow b = c$$

$$\Big(ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \overset{\text{Integritätsring}}{\Rightarrow} (a = 0 \vee b - c = 0) \Big)$$

13.4 Def: R Integritätsring, $a, b \in R$.

1. a ist **Teiler** von b / b ist **Vielfaches** von a

   $:\Leftrightarrow \quad \exists c \in R: \quad b = c \cdot a$

   Notation: $a \mid b$

2. a und b sind **assoziiert**

   $:\Leftrightarrow \quad \exists c \in R^\times: \quad b = c \cdot a$

   Notation: $a \sim b$

Beispiele in $\mathbb{Z}$:

$5 \mid 10, \quad 10 \nmid 5, \quad 5 \mid 5, \quad 5 \mid -5,$

$5 \not\sim 10, \quad 10 \not\sim 5, \quad 5 \sim 5, \quad 5 \sim -5$

13.5 Notiz: $a \sim b \iff (a \mid b$ und $b \mid a)$

(($\Rightarrow$) Nach Annahme $b = c \cdot a$, also $a \mid b$.

Da $c \in R^\times$, $\quad a = c^{-1} \cdot b$, also $b \mid a$.

($\Leftarrow$) Nach Annahme $b = c \cdot a$ und $a = c' \cdot b$.

Falls $a = 0$ auch $b = 0$, also $a \sim b$.

Falls $b = 0$ auch $a = 0$, also $a \sim b$.

Falls $a \neq 0$ und $b \neq 0$, wende Kürzungsregel 13.3 an auf:

$$\begin{cases} b = cc' \cdot b \\ a = c'c \cdot a \end{cases}$$

Es folgt

$$\begin{cases} 1 = cc' \\ 1 = c'c \end{cases}$$

Also $c, c' \in R^\times$, $c' = c^{-1}$.

)

13.6 Notiz: Für $a \sim a'$ und $b \sim b'$ gilt:

$$a \mid b \iff a' \mid b'.$$

(($\Rightarrow$) $b = ca$ für ein $c \in R$
$a = c_1 a'$ für ein $c_1 \in R^\times$
$b = c_2 b'$ für ein $c_2 \in R^\times$ $\Big\} \Rightarrow b' = c_2^{-1} c c_1 \cdot a'$, also $a' \mid b'$.

($\Leftarrow$) folgt aus Symmetriegründen.)

13.7 Def: R Integritätsring, $a, b \in R$.

① c ist ein größten gemeinsamer Teiler von a und b

$:\iff$ (i) $c \mid a$ und $c \mid b$, und
(ii) $\forall c' \in R$:
$(c' \mid a$ und $c' \mid b) \Rightarrow c' \mid c$.

Notation: $c \sim ggT(a,b)$

a und b sind teilerfremd, falls $1 \sim ggT(a,b)$.

② c ist ein kleinstes gemeinsames Vielfache von a und b

$:\iff$ (i) $a \mid c$ und $b \mid c$, und
(ii) $\forall c' \in R$:
$(a \mid c'$ und $b \mid c') \Rightarrow c \mid c'$.

Notation: $c \sim kgV(a,b)$

13.8 Notiz (Rechtfertigung für Notation)

Alle größten gemeinsamen Teiler von a, b sind assoziiert, und jedes zu einem ggT von a, b assoziierte Element ist selbst ein ggT von a, b.

Alle kleinsten gemeinsamen Vielfache von a, b sind assoziiert, und jedes zu einem kgV von a, b assoziierte Element ist selbst ein kgV von a, b.

(ggT: Sind c und c' ggT von a, b, so folgt aus (ii): $c \mid c'$ und $c' \mid c$. Also $c \sim c'$ nach Notiz 13.5.
Zweite Aussage folgt aus Notiz 13.6.
kgV: analog.)

Beispiele in $\mathbb{Z}$:

$6 \sim -6 \sim \mathrm{ggT}(12, 30)$

$60 \sim -60 \sim \mathrm{kgV}(12, 30)$

In allgemeinen Integritätsringen müssen kgV und ggT gar nicht existieren. Wir zeigen Existenz nur in folgendem Spezialfall:

13.9 Def: Ein Integritätsring R ist **euklidisch**, falls eine Abbildung

$$\delta : R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

mit folgender Eigenschaft existiert:

Für alle $a, b \in R$ mit $b \neq 0$ existieren $\overset{\text{Quotient}}{q}, \overset{\text{Rest}}{r} \in R$ mit

$$a = q \cdot b + r$$

und $\left(r = 0 \text{ oder } \underbrace{\delta(r)}_{\text{Grad von } r} < \delta(b) \right)$.

13.10 Beispiel: $\mathbb{Z}$ ist euklidisch mit

$$\delta : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0, \quad a \mapsto |a|$$

13.11 Beispiel: $K[X]$ ist euklidisch für jeden Körper K,

mit $\delta : K[X] \setminus \{0\} \longrightarrow \mathbb{N}_0, \quad A \mapsto \deg(A)$

(siehe Satz 3.16: Division mit Rest)

In beiden Beispielen sind „q“ & „r“ eindeutig bestimmt, aber das ist nicht Teil der Definition.

13.12 Satz: Zu beliebigen Elementen a, b eines euklidischen Rings existiert ein ggT.

Konstruktiver Beweis: euklidischer Algorithmus

Falls $a = 0 \vee b = 0$: $\quad 0 \sim ggT(a, b)$.

Falls $a \neq 0 \wedge b \neq 0$:

Def. $a_0 := a$

$a_1 := b$

Division mit Rest:

$$
\begin{aligned}
a_0 &= q_1 \cdot a_1 + a_2 \\
a_1 &= q_2 \cdot a_2 + a_3 \\
a_2 &= q_3 \cdot a_3 + a_4 \\
&\;\;\vdots \\
a_{k-2} &= q_{k-1} \cdot a_{k-1} + a_k \\
a_{k-1} &= q_k \cdot a_k + 0
\end{aligned}
$$

① $\uparrow$: $a_k \mid a_0$, $a_k \mid a_1$, …, $a_k \mid a_{k-2}$, $a_k \mid a_{k-1}$

② $\downarrow$

$\delta(a_1) > \delta(a_2) > \delta(a_3) \dots \in \mathbb{N}$

solange $a_i \neq 0$

Also $\exists i$ mit $a_i = 0$.

$k :=$ letzten Index mit $a_k \neq 0$.

① Beh.: $a_k \mid a_i \;\; \forall i$, insbesondere $a_k \mid a \wedge a_k \mid b$.

Beweis: Argumentiere von unten nach oben.

② Beh.: $(c \mid \underset{a_0}{\underset{\shortparallel}{a}} \wedge c \mid \underset{a_1}{\underset{\shortparallel}{b}}) \Rightarrow c \mid a_k$

Beweis: Argumentiere von oben nach unten.

$\square$

Beispiel: $a = 19$, $b = 7$:

$$19 = 2\cdot 7 + 5$$
$$7 = 1\cdot 5 + 2$$
$$5 = 2\cdot 2 + 1$$
$$2 = 2\cdot 1$$

Also $ggT(19,7) \sim 1$ ✓.

13.13 Lemma von Bézout

In jedem euklidischen Ring gilt:
Ist $c \sim ggT(a,b)$, so existieren x, y mit
$c = x\cdot a + y\cdot b$.

(Umkehrung falsch. I.A. folgt aus $c = x\cdot a + y\cdot b$ noch nicht einmal, dass c a und b teilt.
$5 = 1\cdot 1 + 1\cdot 4$)

13.14 Korollar:

In jedem euklidischen Ring gilt:
a, b sind teilerfremd $\Leftrightarrow$ $\exists x,y$: $1 = x\cdot a + y\cdot b$

Beweis zu 13.14:

($\Rightarrow$) Lemma 13.13

($\Leftarrow$) $1 | a$ und $1 | b$, und

$$\left.\begin{array}{l} c | a \\ \wedge\ c | b \\ \wedge\ 1 = x\cdot a + y\cdot b \end{array}\right\} \Rightarrow c | 1.$$

$\square$

(Alternativer (nicht-konstruktiver) Beweis zu ($\Rightarrow$) für $\mathbb{Z}$:
Lineare Algebra I, Blatt 5, Aufgabe 4 „Millimeterarbeit")

Beispiel: Da 19, 7 teilerfremd $\exists x, y \in \mathbb{Z}$:

$$1 = x \cdot 19 + y \cdot 7$$

$$x = ? \qquad y = ?$$

Gute Nachrichten:

konstruktiver **Beweis von 13.13:**

Falls $a = 0 \vee b = 0$: $\quad 0 \sim ggT(a, b)$, daher $c = 0$.
Wähle $x = y = 0$.

Falls $a \neq 0 \wedge b \neq 0$:

Führe euklidischen Algorithmus wie im vorherigen Beweis aus:

$$\begin{aligned}
a_0 &= q_1 \cdot a_1 + a_2 \\
a_1 &= q_2 \cdot a_2 + a_3 \\
a_2 &= q_3 \cdot a_3 + a_4 \\
&\;\;\vdots \\
a_{k-2} &= q_{k-1} \cdot a_{k-1} + a_k \\
a_{k-1} &= q_{k-1} \cdot a_k + 0
\end{aligned}$$

Beh: $\exists x_i, y_i$ mit $a_i = x_i a_0 + y_i a_1$

Beweis: IA: $i = 0$: $\quad a_0 = 1 \cdot a_0 + 0 \cdot a_1$

$i = 1$: $\quad a_1 = 0 \cdot a_0 + 1 \cdot a_1$

IV: Seien $x_i, x_{i-1}, y_i, y_{i-1}$ bereits konstruiert.

IS: Aus $a_{i-1} = q_i \cdot a_i + a_{i+1}$ folgt

$$\begin{aligned}
a_{i+1} &= a_{i-1} - q_i \cdot a_i \\
&= (x_{i-1} a_0 + y_{i-1} a_1) - q_i (x_i a_0 + y_i a_1) \\
&= \underbrace{(x_{i-1} - q_i x_i)}_{=: x_{i+1}} a_0 + \underbrace{(y_{i-1} - q_i y_i)}_{=: y_{i+1}} a_1
\end{aligned}$$

Insbesondere also $a_k = x_k a_0 + y_k a_k$.

Nach Notiz 13.8 $c \sim a_k$, also folgt Aussage für c. $\square$

Beispiel (fortgesetzt): $a = 19$, $b = 7$ teilerfremd

1. EUKLID: (s.o.)

$$19 = 2 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

2. BEZOUT:

$$\begin{pmatrix} 19 = 1 \cdot 19 + 0 \cdot 7 \\ 7 = 0 \cdot 19 + 1 \cdot 7 \end{pmatrix}$$

$$5 = 19 - 2 \cdot 7 \quad \checkmark$$

$$\begin{aligned} 2 &= 7 - 1 \cdot 5 \\ &= 7 - 1 \cdot (19 - 2 \cdot 7) \\ &= 3 \cdot 7 - 19 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= (19 - 2 \cdot 7) - 2 \cdot (3 \cdot 7 - 19) \\ &= 3 \cdot 19 - 8 \cdot 7 . \end{aligned}$$

Also $1 = \underbrace{3 \cdot 19}_{57} - \underbrace{8 \cdot 7}_{56}$.