

5. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 8. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

Euklidische Bereiche

Definition

- (1) Eine Abbildung $N : R \rightarrow \mathbb{N}_0$ heißt *Norm*.
- (2) Der Integritätsbereich R (mit der Norm N versehen) heißt *euklidisch*, wenn für alle $a, b \in R$ mit $b \neq 0$ $q, r \in R$ existieren, so dass $a = qb + r$, wobei $r = 0$ oder $N(r) < N(b)$.

Abkürzung: R ist E.R.

Beispiele

- (i) \mathbb{Z} mit $N(a) := |a|$
- (ii) $K[x]$, wenn K ein Körper mit $N(p(x)) := \deg p(x)$ ist.

Weitere Beispiele: Siehe Übungsblatt 3.

Proposition

Sei R ein euklidischer Integritätsbereich, $I \triangleleft R$, dann ist I ein Hauptideal.

Beweis

Sei $I \neq \{0\}$ und $0 \neq d \in I$ mit $N(d)$ minimal. Es ist klar, dass $\langle d \rangle \subseteq I$ (siehe (i) unten bei Definition).

Umgekehrt: Sei $a \in I$ und $q, r \in R$ mit $a = qd + r$ $r = 0$ oder $N(r) < N(d)$.

Nun ist aber $r = a - qd \in I$, also $N(r) < N(d)$ unmöglich.

Also $r = 0$ und somit $a = qd \in \langle d \rangle$. □

Teilbarkeit**Definition**

$a, b \in R; b \neq 0$

(i) b teilt a ; $b|a$ (Bezeichnung), wenn ein $x \in R$ existiert mit $a = bx$.

(ii) $d \in R$ ist ein ggT von a und b , falls

(a) $d|a$ und $d|b$, und für $d' \in R$ gilt:

(b) $d'|a$ und $d'|b$ impliziert $d'|d$.

Bemerkungen

(i) $b|a$ genau dann, wenn $a \in \langle b \rangle$ genau dann, wenn $\langle a \rangle \subseteq \langle b \rangle$

(ii) d ist ggT von a, b , falls $\langle a, b \rangle \subseteq \langle d \rangle$ und aus $\langle a, b \rangle \subseteq \langle d' \rangle$ folgt $\langle d \rangle \subseteq \langle d' \rangle$ (für alle $d' \in R$).

Wir bekommen damit eine hinreichende Bedingung für die \exists^Z eines ggT:

Proposition 2

Ist $\langle a, b \rangle$ ein Hauptideal, u.e. $\langle a, b \rangle = \langle d \rangle$, dann ist d ein ggT von a und b .

Definition

$x, y \in R$ sind *assoziiert*, falls ein $u \in R^\times$ existiert mit $xu = y$.

Proposition (Eindeutigkeit bis auf Einheiten)

Sei R integer, $d, d' \in R$ und $a, b \in R$.

Es gilt: $\langle d \rangle = \langle d' \rangle$ genau dann, wenn $d' = ud$ mit $u \in R^\times$.

Insbesondere alle ggT von a, b sind zueinander assoziiert.

Beweis

“ \Leftarrow ” $d' = ud \Leftrightarrow d = d'u^{-1}$ mit $u \in R^\times$. Also $d' = ud \Rightarrow d' \in \langle d \rangle \Rightarrow \langle d' \rangle \subseteq \langle d \rangle$ und umgekehrt aus $d = d'u^{-1}$ folgt auch $\langle d \rangle \subseteq \langle d' \rangle$.

“ \Rightarrow ” Seien $d, d' \neq 0$ und $\langle d \rangle = \langle d' \rangle$. Also

$$\begin{array}{l} \exists x \in R : d = xd' \\ \exists y \in R : d' = yd \end{array} \left\| \Rightarrow d = xyd \text{ i.e. } d(1 - xy) = 0 \right.$$

R integer und $d \neq 0$ impliziert $1 - xy = 0$, also $xy = 1$. □

Eine wichtige Eigenschaft von E.R. ist der
Algorithmus zum Berechnen von ggT:

Seien $a, b \in R, b \neq 0$

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

\vdots

$$r_{n-2} = q_n r_{n-1} + r_n \quad r_n \neq 0$$

$$r_{n-1} = q_{n+1} r_n$$

$$\underbrace{N(b) > N(r_0) > \dots > N(r_{n-1}) > N(r_n) > 0}_{\text{endlich viele Schritte im Abstieg !}}$$

Wir fassen zusammen:

Satz

Sei $R \in D; a, b \in R \neq 0$ und $d = r_n$ (wie oben), so ist

- (1) d ein ggT von a und b
- (2) $d = ax + by$ für geeignete $x, y \in R$.

Hauptidealbereiche

Definition

Ein *Hauptidealbereich* ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Abkürzung: H.I.R.

Proposition 4

Sei R ein Hauptidealbereich, $a, b \neq 0, a, b \in R$ und d ein Erzeuger von $\langle a, b \rangle$. Es gelten:

- (1) d ist ggT von a, b
- (2) $\exists x, y \in R$ mit $d = ax + by$
- (3) d ist (bis auf Einheiten) eindeutig.

Beweis

Siehe Proposition 2

□

Proposition 5

Jedes Primideal in einem Hauptidealbereich ist auch maximal.

Beweis

Sei $\langle p \rangle \neq \{0\}$ Primideal und $M \supseteq \langle p \rangle$ maximal (wir wissen M existiert!). Nun ist auch $M = \langle m \rangle$ ein Hauptideal; $p \in \langle m \rangle$ also existiert $r \in R$ mit $p = rm$.

Aber $\langle p \rangle$ prim $\Rightarrow r \in \langle p \rangle$ oder $m \in \langle p \rangle$.

1. Fall: $m \in \langle p \rangle \Rightarrow \langle m \rangle \subseteq \langle p \rangle \Rightarrow \langle p \rangle = M$

2. Fall: $r \in \langle p \rangle \Rightarrow r = ps \Rightarrow p = rm = psm$ oder $sm = 1$.

Somit ist aber $m \in R^\times$. Das widerspricht, dass M maximal (also echt) ist. \square

Beispiele

(1) Alle Ideale in \mathbb{Z} sind Hauptideale $n\mathbb{Z}$ und $n\mathbb{Z}$ ist maximal genau dann, wenn $n = p$ eine Primzahl ist.

(2) $\mathbb{Z}[x]$ ist kein Hauptidealbereich, weil $\langle x \rangle$ prim, aber nicht maximal ist.

Wir verallgemeinern: Sei R integer. Es gilt:

Korollar

$R[x]$ ist ein Hauptidealbereich genau dann, wenn R ein Körper ist.

Beweis

“ \Leftarrow ” R ist ein Körper $\Rightarrow R[x]$ ist E.R. $\Rightarrow R[x]$ ist H.I.R.

“ \Rightarrow ” $R[x]/\langle x \rangle \cong R$, $\langle x \rangle$ Primideal.

Nun $R[x]$ Hauptidealbereich $\Rightarrow \langle x \rangle$ maximales Ideal $\Rightarrow R[x]/\langle x \rangle$ ist ein Körper. \square