Algebra BIII

Kuhlmann

5. Vorlesung am 8.11.2012.

Euklidische Bereiche.

Definition (1) Eine Abbildung $N: R \longrightarrow \mathbb{N}_0$ heißt **Norm**.

(2) Der Integritätsbereich R (mit der Norm N versehen) heißt **euklidisch** wenn:

$\forall\ a, b \in R$ mit $b \neq 0$ $\exists\ q, r \in R$ s.d.

$$a = qb + r$$

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 ist,

mit $N(p(x)) := \deg p(x)$.

weitere Beispiele: siehe ÜB 3. ∎

Proposition 1. Sei R Euklidesch Integritätsbereich, $I \lhd R$, dann ist I Hauptideal.

Beweis. Sei $I \neq \{0\}$ und $0 \neq d \in I$ mit $N(d)$ minimal. Es ist klar daß $\langle d \rangle \subseteq I$ (Bem. (i) unten) ↓

Umgekehrt sei $a \in I$ und $q, r \in R$ mit

$$a = qd + r \qquad r = 0 \text{ oder } N(r) < N(d).$$

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: $a, b \in R \quad b \neq 0$

(i) b teilt a; $b \mid a$, wenn ← Bezeichnung
$\exists x \in R$ mit $a = bx$

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

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

(2) $d' \mid a$ und $d' \mid b$ impliziert $d' \mid d$.

Bemerkungen: (i) $b \mid a$ gdw $a \in \langle b \rangle$ gdw $\langle a \rangle \subseteq \langle b \rangle$

(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 $\exists^{\mathbb{Z}}$ eines ggT:

Proposition 2: Ist $\langle a,b\rangle$ Hauptideal, i.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 $\exists\, u \in R^\times$ mit $xu = y$.

Proposition 3 (Eindeutigkeit bis auf Einheiten).

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

Es gelt: $\langle d\rangle = \langle d'\rangle$ gdw $d' = ud$ mit $u \in R^\times$,
Insbesondere alle ggT von a, b sind zueinander assoziiert.

Beweis: "$\Leftarrow$" $d' = ud \iff d = d'u^{-1}$ 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 $\langle d \rangle \subseteq \langle d' \rangle$.

auch

"$\Rightarrow$" Seien $d, d' \neq 0$ und $\langle d \rangle = \langle d' \rangle$

also $\exists\, x \in R : d = xd'$
$\exists\, y \in R : d' = yd$
$\Rightarrow$ $d = xyd$

i.e.

$d(1 - xy) = 0$

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

$$a = q_0 b + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n \qquad r_n \neq 0$$
$$r_{n-1} = q_{n+1} r_n$$

$N(b) > N(r_0) > \dots > N(r_{n-1}) > N(r_n) > 0$

endlich viele Schritten im Abstieg!

Wir fassen zusammen:

Satz: Sei R ED, $a, b \in R \neq 0$

und $d = r_n$ (wie oben). So ist ① d ein ggT von a und b im Algorithmus ② $d = ax + by$ für geeignete $x, y \in R$. ∎

Hauptidealbereiche.

Definition: Ein Hauptidealbereich ist ein Integritätsbereich in dem jedes Ideal Hauptideal ist.

Abkürzung. H. I. R

Proposition 4. Sei R H.I.R, $a, b \neq 0$ $a, b \in R$

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 H. I. R ist auch maximal.

Beweis. Sei $\langle p \rangle \neq \{0\}$ Primideal und $M \supseteq \langle p \rangle$

M maximal (wir wissen M existiert!).

Nun ist auch $M = \langle m \rangle$ Hauptideal.

$p \in \langle m \rangle$ also $\exists r \in R$ 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: $r \in \langle p \rangle \Rightarrow r = ps \Rightarrow$

$$p = rm = psm \quad \text{oder} \quad sm = 1.$$

Somit ist aber $m \in R^\times$, widerspricht daß

M maximal (also echt) ist. ∎

Beispiele.

① Alle Ideale in $\mathbb{Z}$ sind Hauptideale $n\mathbb{Z}$ und $n\mathbb{Z}$ ist maximal gdw $n = p$ eine Primzahl ist.

② $\mathbb{Z}[x]$ ist kein H.I.R weil $\langle x \rangle$ prim aber nicht maximal ist. Wir verallgemeinern:

Sei R integer. Es gilt:

Korollar: $R[x]$ ist H.I.R gdw R ein Körper ist

Beweis: $\Leftarrow$ R 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 $R[x]$ H.I.R $\Rightarrow \langle x \rangle$ maximal Ideal

$\Rightarrow R[x]/_{\langle x \rangle}$ ist ein Körper. ∎