5. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller

WS 2016/2017: 11. November 2016

Euklidische Bereiche

Definition

(1) Eine Abbildung $N : R \to \mathbb{N}_0$ 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.

Proposition

Sei R ein euklidischer Integritätswbereich, $I \lhd R$, dann ist I ein Hauptideal.

Beweis

Sei $I \neq \{0\}$ und $0 \neq d \in I$ mit $N(d)$ minimal. Es ist klar, dass $< d > \subseteq I$ (siehe (i) unten bei Definition).
Umgekehrt: Sei $a \in I$ und $q, r \in R$ mit $a = qd + r \qquad r = 0$ oder $N(r) < N(d)$.
Nun ist aber $r = a - qd \in I$, also $N(r) < N(d)$ unmöglich.
Also $r = 0$ und somit $a = qd \in < d >$. □

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 $a \in < b >$ genau dann, wenn $< a > \subseteq < b >$

(*ii*) d ist ggT von a, b genau dann, wenn $< a, b > \subseteq < d >$ und aus $< a, b > \subseteq < d' >$ folgt $< d > \subseteq < d' >$ (für alle $d' \in R$).

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

Proposition 2
Ist $< a, b >$ ein Hauptideal, i.e. $< a, b > = < d >$, dann ist d ein ggT von a und b.

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

Proposition (Eindeutigkeit bis auf Einheiten)
Sei R integer, $d, d' \in R$ und $a, b \in R$.
Es gilt: $< d > = < d' >$ 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 $d' = ud \Rightarrow d' \in < d > \Rightarrow < d' > \subseteq < d >$
und umgekehrt aus $d = d'u^{-1}$ folgt auch $< d > \subseteq < d' >$.

"$\Rightarrow$" Seien $d, d' \neq 0$ und $< d > = < d' >$. Also

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

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

$$\begin{array}{lllll} a & = & q_0 b & + & r_o \\ b & = & q_1 r_0 & + & r_1 \\ r_0 & = & q_2 r_1 & + & r_2 \\ \vdots & & & & \\ r_{n-2} & = & q_n r_{n-1} & + & r_n \quad r_n \neq 0 \\ r_{n-1} & = & q_{n+1} r_n & & \end{array}$$

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

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 $< a, b >$. 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 $< p > \neq \{0\}$ Primideal und $M \supseteq < p > M$ maximal (wir wissen M existiert!). Nun ist auch $M =< m >$ ein Hauptideal; $p \in < m >$ also existiert $r \in R$ mit $p = rm$.
Aber $< p >$ prim $\Rightarrow r \in < p >$ oder $m \in < p >$.
1. Fall: $m \in < p > \Rightarrow < m > \subseteq < p > \Rightarrow < p > = M$
2. Fall: $r \in < p > \Rightarrow r = ps \Rightarrow p = rm = psm$ oder $sm = 1$.
Somit ist aber $m \in R^{\times}$. Das widerspricht, dass M maximal (also echt) ist. □

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 $< x >$ 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.
"$\Rightarrow$" $R[x]/ < x > \backsimeq R, < x >$ Primideal.
Nun $R[x]$ Hauptidealbereich $\Rightarrow < x >$ maximales Ideal $\Rightarrow R[x]/ < x >$ ist ein Körper. □