5 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir einige Begriffe (die wir schon in der LA I für den Ring $\mathbb{Z}$ und in der LA II für den Ring $K[x]$ kennengelernt hatten) allgemeiner für kommutative Ringe einführen. Wir werden im Abschnitt 6 Ringe erhalten, die einen Divisionsalgorithmus und Euklidische Algorithmus (zum Berechnen von ggT) besitzen. Im Abschnitt 7 werden wir eine strikt größere Klasse studieren.

§ 5 Teilbarkeit

Sei R stets ein kommutativer Ring mit Eins.

Definition 5.1.
Seien $a, b \in R; b \neq 0$

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

(*ii*) $d \in R$ ist ein *gemeinsamer Teiler von a und b* (Bezeichnung: gT von a, b) falls $d|a$ und $d|b$

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

  (a) d ist ein gT von a und b, und für alle $d' \in R$ gilt:

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

Bemerkung 5.2.

(*i*) $b|a$ genau dann, wenn $a \in< b >$ (genau dann, wenn $< a >\subseteq< b >$)

(*ii*) d ist gT von a, b genau dann, wenn $< a, b >\subseteq< d >$

(*iii*) d ist ggT von a, b genau dann, wenn d ist gT von a, b und für alle $d' \in R$ gilt: $< a, b >\subseteq< d' >$ impliziert $< d >\subseteq< d' >$.

Aus Bemerkung 5.2 bekommen wir eine hinreichende Bedingung für die $\exists^Z$ eines ggT:

Proposition 5.3.

Seien $a, b \in R$ so dass $< a, b >$ ein Hauptideal ist, i.e. $< a, b >=< d >$, dann ist d ein ggT von a und b.

Die Bedingung ist jedoch nicht notwendig, siehe ÜB.

Definition 5.4.
$x, y \in R$ sind *assoziiert*, falls ein $u \in R^\times$ exisitert mit $xu = y$.

Proposition 5.5. (Eindeutigkeit bis auf Einheiten)

Sei R integer, $d, d' \in R$ und $a, b \in R$.
Es gilt: $< d >=< d' >$ genau dann, wenn d, d' assoziiert sind.
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

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

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

Die letzte Aussage folgt aus Bemerkung 5.2. □

§ 6 Euklidische Bereiche

Definition 5.6.

(1) Eine Abbildung $N : R \setminus \{0\} \to \mathbb{N}_0$ heißt *Norm*.

(2) Der Integritätsbereich R, versehen mit der Norm N, heißt *euklidisch* (R ist E.R.), wenn er einen Divisionsalgorithmus bezüglich N erlaubt, das heißt:
für $\forall a, b \in R$ mit $b \neq 0$ $\exists q, r \in R$, so dass $a = qb + r$, wobei $r = 0$ oder $N(r) < N(b)$.

Beispiel 5.7.

(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 ÜB.

Proposition 5.8.
Sei R ein euklidischer Integritätsbereich, $I \lhd R$, dann ist I ein Hauptideal.

Beweis:
Sei $I \neq \{0\}$ und $0 \neq d \in I$, also $< d > \subseteq I$. Wähle d so dass $N(d)$ minimal ist. Sei nun $a \in I$ und $q, r \in R$ mit $a = qd + r$ wobei $r = 0$ oder $N(r) < N(d)$. Da $r = a - qd \in I$, ist $N(r) < N(d)$ nicht möglich. Also $r = 0$ und somit $a = qd \in < d >$. □

Eine wichtige Eigenschaft von E.R. ist die $\exists^Z$ eines ggT sowie eines Algorithmus zum Berechnen von ggT . Die Aussage und Beweis vom Satz 5.9 haben wir im LA I (Rückwärts EA; Skript 3 Seiten 2 und 3) für $R = \mathbb{Z}$ (und in LA II Skripte 3 und 5 für $R = K[x]$) detailliert studiert. Wir wiederholen hier die Beweisschritte nicht ausführlich.

Satz 5.9.
Sei R E.R; $a, b \in R \neq 0$ und $d = r_n$ der letzte ungleich Null Rest in **(DA)**. Dann ist

(1) d ein ggT von a und b

(2) $d = ax + by$ für geeignete $x, y \in R$.

Beweis: Wiederholter Anwendung des Divisionsalgorithmus (DA)
Seien $a, b \in R, b \neq 0$

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

$r_{n-1} = q_{n+1} r_n \qquad (*)$

(Da

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

kann der Abstieg nur endlich viele Schritte n haben, das Verfahren muss also zwangläufig mit einer Gleichung $(*)$ anhalten). □

§ 7 Hauptidealbereiche

Definition 5.10.
Ein *Hauptidealbereich* (H.I.R.) ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Proposition 5.11.
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:
Folgt aus Proposition 5.2, Bemerkung 2.3 (3) und Proposition 5.5. □

Proposition 5.12.
Jedes Primideal in einem Hauptidealbereich ist auch maximal.

Beweis:
Sei $< p > \neq \{0\}$ Primideal und $M \supseteq < p >$, M maximal (M existiert vgl. Proposition 2.9).
Nun ist auch $M = < m >$ ein Hauptideal und $p \in < m >$. 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: $r \in < p > \Rightarrow r = ps \Rightarrow p = psm$, kürzen ergibt: $sm = 1$. Somit ist aber $m \in R^\times$. Das widerspricht, dass M maximal, also echt, ist (vgl. Proposition 2.6(1)). □

Beispiel 5.13.

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

(2) $\mathbb{Z}[x]$ ist kein Hauptidealbereich, weil $< x >$ prim, aber nicht maximal ist (Beispiel 4.11).

Wir verallgemeinern Beispiel 5.13 (2):

Korollar 5.14.
Sei R integer, $R[x]$ ist ein Hauptidealbereich genau dann, wenn R ein Körper ist.

Beweis:
"$\Leftarrow$" R ist ein Körper $\Rightarrow R[x]$ ist E.R. (s. Beispiel 5.7 (ii)) $\Rightarrow R[x]$ ist H.I.R. (s. Prop. 5.8).

"$\Rightarrow$" $R[x]/ < x > \simeq R$ (vgl. Bemerkung 4.10), also ist $< x >$ Primideal (s. Proposition 3.5).

Nun $R[x]$ Hauptidealbereich $\Rightarrow < x >$ ist ein maximales Ideal (s. Proposition 5.12) $\Rightarrow R[x]/ < x >$ ist ein Körper (s. Proposition 3.1) . □