

6. Script zur Vorlesung: Algebra (B III)

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

WS 2016/2017: 15. November 2016

Definition

Sei R integer.

- (1) $0 \neq p \in R$ ist *Primelement*, wenn $\langle p \rangle$ *Primideal* ist
(für alle $a, b \in R : p|ab \Rightarrow p|a$ oder $p|b$).
- (2) $0 \neq r \in R; r \notin R^\times$ ist *irreduzible* in R , wenn für alle $a, b \in R : r = ab \Rightarrow a \in R^\times$
oder $b \in R^\times$. Sonst ist r *reduzible*.

Proposition 1

Sei R integer und $p \in R$. p ist Primelement $\Rightarrow p$ ist irreduzible.

Beweis

Sei $\langle p \rangle \neq \{0\}$ Primideal. Also ist $p \notin R^\times$.

Sei $p = ab; ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ oder $b \in \langle p \rangle$.

1. Fall: $a \in \langle p \rangle \Rightarrow a = pr \Rightarrow p = prb$ oder $p(1 - rb) = 0 \Rightarrow 1 = rb$; also $b \in R^\times$.
2. Fall: Analog. □

Proposition 2

Sei R Hauptidealbereich, $p \in R$ irreduzible $\Rightarrow p$ ist Primelement.

Beweis

Sei $p \notin R^\times; p \neq 0$, p irreduzible.

Sei $M \triangleleft R$ mit $\langle p \rangle \subseteq M$. Nun existiert ein $m \in R$ mit $M = \langle m \rangle$.

$\exists r : p = rm$ und p irreduzible, also

$$\begin{array}{ccc}
 \text{1. Fall} & & \text{2. Fall} \\
 r \in R^\times & \text{oder} & m \in R^\times \\
 \Downarrow & & \Downarrow \\
 \langle p \rangle = \langle m \rangle & & \langle m \rangle = R
 \end{array}$$

Also $\langle p \rangle$ ist maximal, insbesondere Primideal. □

Definition

Sei R integer. R ist *faktoriell*, wenn

- (1) Für alle $0 \neq r \in R \setminus R^\times$ existiert $p_1, \dots, p_n \in R$ irreduzibel: $r = p_1 \cdots p_n$ (†)
- (2) Diese Darstellung ist eindeutig bis auf die Reihenfolge und Assoziiertheit.
(D.h. wenn auch $r = q_1 \cdots q_m$ mit q_1, \dots, q_m irreduzible, dann ist $m = n$
und $\forall i \exists j$ und $u_i \in R^\times : u_i p_i = q_j$.)

Ist R faktoriell und $r \neq 0$ beliebiges Element, so hat r also eine Darstellung

$$r = up_1^{e_1} \cdots p_n^{e_n}$$

mit $u \in R^\times, e_i \in \mathbb{N}_0$ und p_i irreduzible. mit $p_i \neq p_j$ für $i \neq j$.

Proposition 3

Sei R faktoriell und $p \in R$ irreduzible $\Rightarrow p$ ist Primelement.

Beweis

Sei $0 \neq p, p \in R \setminus R^\times$ irreduzible und $a, b \in R$ mit $p|ab$.

Nun ist $p|ab \Rightarrow ab = pc$ für ein $c \in R$ (*)

Schreibe a und b wie in (†).

Aus (*) und Eindeutigkeit in (†) folgt: p ist assoziiert mit einem der irreduziblen Faktoren in der Darstellung von a oder von b .

Ohne Einschränkung sei es a . Also $a = (up)p_2 \cdots p_n; u \in R^\times, p_i \in R$ und damit $p|a$. □

Proposition 4

Sei R faktoriell, $0 \neq a$ und $b \in R$.

$$a = up_1^{e_1} \cdots p_n^{e_n} \quad (\dagger)$$

$$b = vp_1^{f_1} \cdots p_n^{f_n} \quad (\ddagger)$$

$u, v \in R^\times, p_i$ irreduzible (Prim), $p_i \neq p_j$ für $i \neq j, e_i, f_i \in \mathbb{N}_0$.

Setze $d := p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$ (††)

Dann ist d ein ggT von a und b .

Beweis

Aus (††), (‡) und (†) ist klar, dass $d|a$ und $d|b$. Sei $d' \in R, d'|a$ und $d'|b$. Schreibe

$$d' = vq_1^{g_1} \cdots q_n^{g_n}.$$

für alle i $q_i|d' \Rightarrow q_i|a$ und $q_i|b$. Also für alle i existiert ein $j: q_i|p_j$, so dass $p_j = u_i q_i$ mit $u_i \in R^\times$.

Also $\{p_1, \dots, p_n\} \supseteq \{u_1 q_1, \dots, u_n q_n\}$. Analog zeigt man $g_\ell \leq \min(e_\ell, f_\ell)$. Also $d'|d$. □

Satz

Sei R ein Hauptidealbereich, dann ist R faktoriell.

Beweis

Sei $0 \neq r \in R \setminus R^\times$. Wir wollen eine Darstellung (\dagger) erreichen.

Ist r irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r = r_1 r_2$, $r_1 \notin R^\times$ und $r_2 \notin R^\times$.

Sind r_1, r_2 irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r_1 = r_{11} r_{12}$, usw.

Wir wollen zeigen, dass diese Prozedur nach endlich vielen Schritten anhält, sonst bekommen wir eine unendliche (**strikte**) für die Inklusion ansteigende Folge von Idealen:

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \cdots \subseteq R$$

Behauptung

Wir zeigen nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann.

Sei also $I_i \triangleleft R$ mit $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$.

Setze $I := \bigcup_{i=1}^{\infty} I_i \triangleleft R$. Da R ein Hauptidealbereich, existiert $a \in R$ mit $I = \langle a \rangle$.

Nun $a \in I \Rightarrow \exists n \in \mathbb{N} : a \in I_n$. Also $I_n \subseteq I = \langle a \rangle \subseteq I_n$ und somit $I = I_n$.

Damit ist die Behauptung bewiesen.

Wir haben also die \exists^Z einer Darstellung (\dagger) gezeigt. Die Aussage über die Eindeutigkeit erfolgt per Induktion über n in der Darstellung $r = p_1 \cdots p_n$ (genau so wie in Lineare Algebra II, Vorlesung 5 vom 30.04.2012). \square