6. Script zur Vorlesung: Algebra (B III)

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

WS 2012/2013: 12. November 2012

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

Definition

Sei R integer.

(1) $0 \neq p \in R$ ist *Primelement*, wenn $< p >$ *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 $< p > \neq \{0\}$ Primideal. Also ist $p \notin R^\times$.

Sei $p = ab; ab \in < p > \Rightarrow a \in < p >$ oder $b \in < p >$.

1. Fall: $a \in < p > \Rightarrow a = pr \Rightarrow p = prb$ 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 $M \lhd R$ mit $< p > \subseteq M$. Nun existiert ein $m \in R$ mit $M = < m >$.

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

1. Fall		2. Fall
$r \in R^\times$	oder	$m \in R^\times$
$\Downarrow$		$\Downarrow$
$< p > = < m >$		$< m > = R$

Also $< p >$ ist maximal, insbesondere Primideal. □

Definition

Sei R integer. R ist *faktoriell*, wenn

(1) Für alle $0 \neq r \in R \setminus R^\times$ existiert $p_1, \ldots, p_n \in R$ 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 $q_1, \ldots, q_m$ 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

$$r = u p_1^{e_1} \cdots p_n^{e_n}$$

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 $b \in R$.
$a = u p_1^{e_1} \cdots p_n^{e_n}$ (†)

$b = v p_1^{f_1} \cdots p_n^{f_n}$ (‡)

$u, v \in R^\times, p_i$ 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

$$d' = v q_1^{g_1} \cdots q_n^{g_n}.$$

für alle $iq_i|d' \Rightarrow q_i'|a$ 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 $\{p_1, \ldots, p_n\} \supseteq \{u_1 q_1, \ldots, u_n q_n\}$. Analog zeigt man $g_\ell \leq min(e_\ell f_\ell)$. Also $d'|d$. □

Satz

Sei R ein Hauptidealbereich, dann is R faktoriell.

Beweis

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

$$< r > \subsetneq < r_1 > \subsetneq < r_{11} > \subsetneq \cdots \subseteq R$$

Behauptung

Wir zeigen nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann.
Sei also $I_i \lhd R$ mit $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq R$.
Setze $I := \bigcup_{i=1}^{\infty} I_i \lhd R$. Da R ein Hauptidealbereich, existiert $a \in R$ mit $I =< a >$.
Nun $a \in I \Rightarrow \exists n \in \mathbb{N} : a \in I_n$. Also $I_n \subseteq I =< a > \subseteq I_n$ und somit $I = I_n$.
Damit ist die Behauptung bewiesen.

Wir haben also die $\exists^Z$ einer Darstellung (†) 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). □