Algebra B III

- Kuhlmann -

6. Vorlesung
am 12. 11. 2012.

Definition: Sei R integer.

(1) $0 \neq p \in R$ ist Primelement wenn $\langle p \rangle$ Primideal ist.

($\forall a, b \in R$: $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$

(2) $0 \neq r \in R$; $r \notin R^\times$ ist irreduzible in R wenn

$\forall a, b \in R$: $r = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$

Sonst ist r reduzible.

Proposition 1. Sei R integer, $p \in R$
p Primelement $\Rightarrow p$ 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. $\blacksquare$

Proposition 2 Sei R H.I.R ; $p \in R$ irreduzible
$\Rightarrow p$ ist Primelement.

Beweis. Sei $p \notin R^{\times}$, $p \neq 0$,
p irreduzible

Sei $M \lhd R$ mit $\langle p \rangle \subseteq M$.
Nun $\exists\, m \in R$ mit $M = \langle m \rangle$
$\exists\, r : p = rm$ und p irreduzible, also

Fall 1. $r \in R^{\times}$ oder **Fall 2.** $m \in R^{\times}$

1. Fall $\Rightarrow \langle p \rangle = \langle m \rangle$ 2. Fall $\Rightarrow \langle m \rangle = R$.

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

Definition Sei R entéger. R ist factoriell wenn

(1) $\forall\, 0 \neq r \in R \setminus R^{\times}$, $\exists\, p_1, \dots, p_n \in R$
irreduzible: $r = p_1 \cdots p_n$ (#)

(2) Diese Darstellung ist eindeutig bis auf 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 factoriell und $r \neq 0$ beliebiges Element, so hat r also eine Darstellung

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

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

Proposition 3. Sei R faktoriell, $p \in R$ irreduzibel $\Rightarrow$ p Primelement.

Beweis. Sei $0 \neq p$, $p \in R \setminus R^\times$ irreduzibel, $a, b \in R$ mit: $p \mid ab$. Nun:
$p \mid ab \Rightarrow$

$$ab = pc \quad \text{für ein } c \in R \qquad (*)$$

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.

OE Sei es a. Also

$$a = (u\,p)\, p_2 \cdots p_m \qquad u \in R^\times,\ p_i \in R$$

und damit $p \mid a$. $\blacksquare$

Proposition 4. Sei R faktoriell

$0 \neq a, b \in R$

$$a = u\, p_1^{e_1} \cdots p_n^{e_n} \quad (\dagger)$$

$$b = v\, p_1^{f_1} \cdots p_n^{f_n} \quad (\ddagger)$$

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

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

Dann ist d ein ggT von a und b.

Beweis: Aus $\left\{\begin{array}{l}(\ddagger\!\!\!\ddagger)\\ (\ddagger)\\ (\dagger)\end{array}\right.$ ist es klar daß $d \mid a$ und $d \mid b$.

Sei $d' \in R$; $d' \mid a$ und $d' \mid b$. Schreibe

$$d' = v\, q_1^{g_1} \cdots q_m^{g_m}$$

$\forall i$: $q_i \mid d' \Rightarrow q_i \mid a$ und $q_i \mid b$

also $\forall i\ \exists j$: $q_i \mid p_j$; so $p_j = u_i q_i$ $\quad u_i \in R^\times$

also $\{p_1, \dots, p_n\} \supseteq \{u_1 q_1, \dots, u_m q_m\}$. Analog zeigt man $g_\ell \leq \min(e_\ell, f_\ell)$; also $d' \mid d$. $\blacksquare$

Satz: Sei R H.I.R, dann ist R faktoriell.

Beweis. sei $0 \neq r \in R \setminus R^{\times}$. Wir wollen eine Darstellung (+) erreichen.

Ist r irreduzibel, dann ist der Ziel erreicht.

Sonst zerlege $r = r_1 r_2$ $\quad r_1 \notin R^{\times}$ und $r_2 \notin R^{\times}$

Sind r_1, r_2 irreduzibel, so ist der 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 (strikt) für die Inklusion ansteigende Folge von Idealen.

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \ldots \subset R$$

Beh. Wir zeigen nun daß dieses in einem H.I.R nicht der Fall sein kann.

Sei also $I_i \trianglelefteq R$ mit $I_1 \subseteq I_2 \subseteq \ldots \subseteq R$

Setze $I := \bigcup_{i=1}^{\infty} I_i \quad \triangleleft \quad R.$

Da R H. I. R $\exists\, a \in R$ 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 $I = I_n$. $\blacksquare$ Beh.

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 der 5. Vorlesung LA II
30.04.2012
Seite 6. $\blacksquare$