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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst prime und irreduzible Elemente in einem integer Ring einführen und studieren. Im Abschnitt 9 werden wir dann unsere Untersuchung über Faktorielle Ringe beginnen.

§ 8 Primelemente, Irreduzible Elemente

Sei R stets ein integer Ring.

Definition 6.1.

(1) Sei $0 \neq p \in R$, p ist *Primelement*, wenn $< p >$ *Primideal* in R ist
(für alle $a, b \in R : p|ab \Rightarrow p|a$ oder $p|b$).

(2) Sei $0 \neq r \in R$; $r \notin R^{\times}$, p 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 6.2.
Sei $p \in R$, p ist Primelement $\Rightarrow p$ ist irreduzible.

Beweis:
Sei $< p > \neq \{0\}$ Primideal. Also ist $p \notin R^{\times}$.
Wenn $p = ab$ dann folgt: $ab \in < p > \Rightarrow a \in < p >$ 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 6.3.
Sei R Hauptidealbereich, $p \in R$ irreduzible $\Rightarrow p$ ist Primelement.

Beweis:
Sei $p \notin R^{\times}; p \neq 0$, p irreduzible.
Sei $M \triangleleft R$ ein Ideal so dass $< p > \subseteq M$. Nun existiert ein $m \in R$ mit $M =< m >$.
Also $\exists r : p = rm$ und p irreduzible, also

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

Wir haben gezeigt dass $< p >$ maximal, und insbesondere Primideal ist. □

§ 9 Faktorielle Ringe

Definition 6.4.
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 $u_i \in R^\times$ so dass: $u_i p_i = q_j$.

(3) Also R ist faktoriell wenn für jedes $r \in R$, $r \neq 0$ beliebiges Element, gibt es für r eine Darstellung
$$r = u p_1^{e_1} \cdots p_n^{e_n}$$
mit $u \in R^\times, e_i \in \mathbb{N}_0$, p_i irreduzible, mit $p_i \neq p_j$ für $i \neq j$. (†)

Für faktorielle Ringe gilt auch die Umkehraussage von Proposition 6.2:

Proposition 6.5.
Sei R faktoriell und $p \in R$, es gilt: p 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 $p|ab \Rightarrow ab = pc$ für ein $c \in R$ (∗)
Schreibe a und b wie in (†).
Da p irreduzibel ist, folgt aus (∗) und der Eindeutigkeit in (†): p ist assoziiert mit einem der irreduziblen Faktoren in der Darstellung von a oder von b.
Ohne Einschränkung sei es a, und schreibe $a = (up)p_2 \cdots p_n$; $u \in R^\times$, $p_i \in R$. Somit haben wir bewiesen dass $p|a$. □

Auch für faktorielle Ringe gilt die Existenz eines $ggTs$ (vgl. Satz 5.9):

Proposition 6.6.
Sei R faktoriell, a und $b \in R$. Schreibe:
$a = u p_1^{e_1} \cdots p_n^{e_n}$ (†)
$b = v p_1^{f_1} \cdots p_n^{f_n}$ (‡)
wobei $u, v \in R^\times$, p_i irreduzible, $p_i \neq p_j$ 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 $d' \in R$ so dass, $d'|a$ und $d'|b$. Schreibe in der (†) Darstellung, mit q_i irreduzibel:
$$d' = v q_1^{g_1} \cdots q_n^{g_n} .$$
Nun für alle $i :$ $q_i | d' \Rightarrow q_i | a$ und $q_i | b$.
Also für alle $i :$ $q_i | a \Rightarrow$ existiert ein j und $u_i \in R^\times$ so dass $p_j = u_i q_i$.
Also $g_\ell \leq e_\ell$. Analog zeigt man dass $g_\ell \leq f_\ell$. Also $g_\ell \leq min(e_\ell, f_\ell)$. Somit haben wir gezeigt: $d'|d$. □

Satz 6.7.
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.

Diese Prozedur muss nach endlich vielen Schritten anhalten, da wir sonst eine unendliche (**strikte**) für die Inklusion ansteigende Folge von Idealen bekommen:

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

Wir behaupten nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann:

Sei also $I_i \lhd R$ mit $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$.
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, Skript 5 Seite 3, Beweis vom Satz 5.15). □