Definition der irreduziblen Elemente

Definition (11.16)

Sei R ein Ring. Ein Element $p \in R$ wird irreduzibel genannt, wenn p weder eine Einheit noch Null ist und die Implikation

$$p = ab \quad \Rightarrow \quad a \in R^\times \text{ oder } b \in R^\times$$

für alle $a, b \in R$ erfüllt ist. Nichteinheiten ungleich Null, die nicht irreduzibel sind, bezeichnen wir als reduzible Ringelemente.

Definition der Primelemente

Definition (11.17)

Sei R ein Ring. Ein Element $p \in R$ heißt Primelement, wenn p weder eine Einheit noch Null ist und außerdem die Implikation

$$p \mid (ab) \quad \Rightarrow \quad p \mid a \quad \text{oder} \quad p \mid b \qquad \text{für alle } a, b \in R \text{ erfüllt ist.}$$

Satz (11.18)

In einem Integritätsbereich ist jedes Primelement irreduzibel.

Primelemente in Hauptidealringen

Satz (11.24)

Sei R ein Hauptidealring, aber kein Körper, und $p \in R$. Dann sind die folgenden Aussagen äquvialent.

(i) Das Element p ist prim.

(ii) Das Element p ist irreduzibel.

(iii) Das Ideal (p) ist maximal.

(iv) Das Ideal (p) ist ein Primideal, und es gilt $p \neq 0_R$.

Definition der faktoriellen Ringe

Definition (11.25)

Ein faktorieller Ring ist ein Integritätsbereich R mit der Eigenschaft, dass jedes Element $r \in R$, das weder gleich Null noch eine Einheit ist, als Produkt von Primelementen dargestellt werden kann. Dies bedeutet: Es gibt ein $n \in \mathbb{N}$ und Primelemente $p_1, ..., p_n \in R$, so dass

$$r = p_1 \cdot p_2 \cdot ... \cdot p_n \quad \text{gilt.}$$

Charakterisierung der faktoriellen Ringe (Vorb.)

Lemma (11.26)

Sei R ein Integritätsbereich.

(i) Seien $a, a', b, b' \in R$, wobei $a \sim a'$, $b \sim b'$ und $a|b$ gilt. Dann gilt auch $a'|b'$.

(ii) Jedes Element in R, das eine Einheit teilt, ist eine Einheit.

(iii) Ein Element, das von einem Primelement geteilt wird, ist keine Einheit.

Proposition (11.27)

In einem faktoriellen Ring R ist jedes irreduzible Element ein Primelement.

Beweis von Lemma 11.26 geg: R Integritätsber.

zu (i) siehe Skript

zu (ii) Sei $\varepsilon \in R^\times$ und $a \in R$ mit $a \mid \varepsilon$

z.zg.: $a \in R^\times$ $\quad a \mid \varepsilon \Rightarrow \exists c \in R$ mit

$\varepsilon = a \cdot c \Rightarrow 1 = \varepsilon^{-1} a \cdot c = a(\varepsilon^{-1} c)$

$\Rightarrow a$ ist in R invertierbar (mit $a^{-1} = \varepsilon^{-1} c$)

$\Rightarrow a \in R^\times$

zu (iii) Sei $a \in R$ und $p \in R$ ein Primelement mit $p \mid a$. Beh.: $a \notin R^\times$ Ang. $a \in R^\times$ $p \mid a \overset{(ii)}{\Rightarrow}$

$p \in R^\times$ ↯ zu p Primelement $\square$

Beweis von Proposition 11.27

geg: faktorieller Ring R, $p \in R$ irreduzibel

Beh.: p ist Primelement

$p \neq 0$, $p \notin R^\times$ (da p irreduzibel), R faktoriell $\Rightarrow$
$\exists m \in \mathbb{N}$ und Primelemente $p_1, \dots, p_m \in R$ mit
$p = p_1 \cdot (p_2 \cdot \dots \cdot p_m)$ 1. Fall: $m = 1 \Rightarrow p = p_1$ prim

2 Fall: $m \geq 2$ Als Primelement ist p_1 keine Einheit
$p_2 \cdot \dots \cdot p_m$ wird vom Primelement p_2 geteilt $\overset{\text{Lemma 11.26 (ii)}}{\Rightarrow}$
$p_2 \cdot \dots \cdot p_m \notin R^\times \Rightarrow p$ ist Produkt zweier Nicht-
Einheiten $\lightning$ zu p irreduzibel $\square$

Charakterisierung der faktoriellen Ringe

Satz (11.28)

Sei R ein Integritätsbereich. Dann sind äquivalent

(i) R ist ein faktorieller Ring.

(ii) Jedes Element $r \in R$, dass weder gleich Null noch eine Einheit ist, kann als Produkt von irreduziblen Elementen dargestellt werden, und diese Darstellung ist im wesentlichen eindeutig. Dies bedeutet genau: Sind $m, n \in \mathbb{N}$ und

$$p_1 \cdot \ldots \cdot p_m \;=\; r \;=\; q_1 \cdot \ldots \cdot q_n$$

zwei Darstellungen von r als Produkt irreduzibler Elemente p_i, q_j, dann gilt $m = n$, und nach eventueller Umnummerierung $p_i \sim q_i$ für $1 \leq i \leq m$.

Beweis von Satz 11.28

geg.: R Integritätsbereich

z.zg.: Äquivalenz der Aussagen

(i) R ist faktoriell

(ii) Jedes $c \in R \setminus (R^\times \cup \{0_R\})$ hat eine im Wesentlichen eindeutige Darstellung als Produkt irreduzibler Elemente

„(ii) $\Rightarrow$ (i)" Es genügt z.zg., dass unter der Vor. (ii) jedes irreduzible Element in R ein Primelement ist.

der Vor. (iii) jedes irreduzible Element

Sei $p \in R$ irreduzibel $\Rightarrow p \neq 0_R,\ p \notin R^\times$

Seien $a, b \in R$ mit $p \mid (ab)$. z.zg.: $p \mid a$ oder $p \mid b$. Ist $a = 0_R$ oder $b = 0_R$, dann folgt sofort $p \mid a$ oder $p \mid b$. Setze also $a, b \neq 0_R$ voraus. Ang. $a \in R^\times$. $\overset{p \mid a}{\underset{\text{Lemma 11.26}}{\Longrightarrow}}$ $p \in R^\times$ $\lightning$ zu p irreduzibel also: $a \notin R^\times$, zeige ebenso $b \notin R^\times$

$a, b \notin R^\times \cup \{0_R\} \overset{(ii)}{\Rightarrow} \exists\, m, n \in \mathbb{N}$ und irreduzible Elemente $p_i, q_j \in R$ mit

$a = p_1 \cdot \ldots \cdot p_m, \quad b = q_1 \cdot \ldots \cdot q_n$

$p \mid ab \Rightarrow \exists c \in R$ mit $ab = pc$

Ang. $c = 0_R \Rightarrow ab = 0_R \overset{R \text{ Int.-b}}{\Rightarrow} a = 0_R$ oder $b = 0_R$ ↯

Ang. $c \in R^\times$. $p = (c^{-1}a) \cdot b \overset{p \text{ irred}}{\Rightarrow}$

$\Rightarrow c^{-1}a \in R^\times$ oder $b \in R^\times \Rightarrow a \in R^\times$ oder $b \in R^\times$ ↯

<u>also</u>: $c \notin R^\times \cup \{0_R\} \overset{(ii)}{\Rightarrow} \exists t \in \mathbb{N}$ und irreduzible Elemente $r_1, \dots, r_t \in R$ mit

$c = r_1 \cdot \dots \cdot r_t$

$a \cdot b = p c \Rightarrow$

$p_1 \circ \dots \circ p_m \circ q_1 \circ \dots \circ q_n = p \cdot r_1 \circ \dots \circ r_t$

Eindeutigkeit in (ii) $\Rightarrow$ $p \sim p_i$ für ein $i \in \{1, \dots, m\}$ oder $p \sim q_j$ für ein $j \in \{1, \dots, n\}$

$\Rightarrow p \mid a$ oder $p \mid b$.

Beweis von Satz 11.28

geg.: R Integritätsbereich

z.zg.: Äquivalenz der Aussagen

(i) R ist faktoriell

(ii) Jedes $c \in R \setminus (R^\times \cup \{0_R\})$ hat eine im Wesentlichen eindeutige Darstellung als Produkt irreduzibler Elemente

„(i) $\Rightarrow$ (ii)" Es genügt zu zeigen, dass jede Darstellung eines Elements $c \in R \setminus (R^\times \cup \{0_R\})$ als Produkt von Primelementen im Wesent-

lichen eindeutig ist (bereits bekannt nach Prop 11.27: In R sind die irreduziblen Elemente genau die Primelemente)

Sei also c ein solches Element, und seien $m, n \in \mathbb{N}$ und $p_1, \dots, p_m, q_1, \dots, q_n \in R$ Primelemente mit

$$p_1 \cdot \dots \cdot p_m = c = q_1 \cdot \dots \cdot q_n$$

zu zeigen: $m = n$, und nach evtl. Umnummerierung gilt $p_i \sim q_i$ für $1 \leq i \leq n$.

Beweis durch vollst. Ind. über n

Ind.-Anf. $n = 1$ $p_1 \circ \dots \circ p_m = q_1$

Da q_1 als Primelement irreduzibel ist muss $m = 1$ sein (Grund: Für $m \geq 2$ sind p_1 und $p_2 \circ \dots \circ p_m$ Nicht-Einheiten, vgl. Rop. 11.27.) $\Rightarrow p_1 = q_1 \Rightarrow p_1 \sim q_1$

Ind.-Schritt $n \mapsto n+1$.

Es gilt $p_1 \circ \dots \circ p_m = q_1 \circ \dots \circ q_{n+1}$, z.Zg. $m = n+1$, $p_i \sim q_i$ für $1 \leq i \leq n+1$ nach evtl. Umnummerierung.

Auf Grund der Gleichung gilt $p_1 \mid q_j$ für ein $j \in \{1, \dots, n+1\}$, o.B.d.A. (nach Umnummerierung) $p_1 \mid q_1 \Rightarrow \exists c \in R$ mit $q_1 = p_1 c$ $\overset{q_1 \text{ irreduzibel}}{\Rightarrow}$ $p_1 \notin R^\times$ $c \in R^\times \Rightarrow q_1 \sim p_1$

einsetzen $\Rightarrow p_1 \cdot \dots \cdot p_m = (p_1 c) \cdot \dots \cdot q_{n+1}$

R Int.-B.
$\Rightarrow$
Kürzungsregel $p_2 \cdot \dots \cdot p_m = (c q_2) \cdot \dots \cdot q_{n+1}$

Rechts steht ein Produkt von n, links ein Produkt von $m-1$ Faktoren $\overset{\text{Ind-V}}{\Rightarrow}$ $n = m-1$ und nach Umnummerierung $p_2 \sim c q_2$, $p_i \sim q_i$ für $3 \le i \le n+1$

$\Rightarrow n+1 = m$ und $p_2 \sim q_2$, $p_i \sim q_i$ für $3 \leq i \leq n+1$ $\square$

Repräsentantensysteme der Primelemente

Definition (11.29)

Sei R ein Integritätsbereich und $P \subseteq R$ eine Teilmenge bestehend aus Primelementen. Wir nennen P ein Repräsentantensystem der Primelemente in R, wenn jedes Primelement $q \in R$ zu genau einem $p \in P$ assoziiert ist.

Eindeutige Darstellung als Produkt von Primelementen

Folgerung (11.30)

Sei R ein faktorieller Ring und $P \subseteq R$ ein Repräsentantensystem der Primelemente. Dann gibt es für jedes Element $0_R \neq f \in R$ eine eindeutig bestimmte Familie $(v_p(f))_{p \in P}$ von Zahlen $v_p(f) \in \mathbb{N}_0$ und eine eindeutig bestimmte Einheit $\varepsilon \in R^\times$, so dass

$$f \quad = \quad \varepsilon \prod_{p \in P} p^{v_p(f)} \qquad \text{erfüllt ist.}$$

Dabei gilt $v_p(f) = 0$ für alle bis auf endlich viele Elemente $p \in P$.

Beweis von Folgerung 11.30

geg.: Integritätsbereich R
$P \subseteq R$ Repräsentantensystem der Primelemente

Sei $f \in R \setminus \{0_R\}$. Ist $f \in R^*$, dann gilt $f = \varepsilon \prod_{p \in P} p^{v_p(f)}$ mit $\varepsilon = f$ und $v_p(f) = 0 \ \forall p \in P$. Ansonsten gibt es nach Satz 11.28 ein $n \in \mathbb{N}$ und Primelemente $q_1, \dots, q_n$ in R mit $f = q_1 \cdot \dots \cdot q_n$. P Repräsentantensystem der Primelemente $\Rightarrow$ Für $1 \leq i \leq n$ gibt es jeweils ein $p_i \in P$ und ein $\varepsilon_i \in R^*$ mit $q_i = \varepsilon_i p_i$.

Definiere nun für jedes $p \in P$ jeweils

$v_p(f) = |\{i \in \{1, \dots, n\} \mid p_i = p\}|$ und außerdem

$\varepsilon = \varepsilon_1 \cdot \dots \cdot \varepsilon_n \in R^\times$. Dann gilt $f = \varepsilon \prod_{p \in P} p^{v_p(f)}$

Nachweis der Eindeutigkeit:

Sei $(u_p)_{p \in P}$ eine Familie in $\mathbb{N}_0$ mit $u_p = 0$ für alle bis auf endlich viele $p \in P$ und $\varepsilon' \in R^\times$ mit

$$\varepsilon' \prod_{p \in P} p^{u_p} = f = \varepsilon \prod_{p \in P} p^{v_p(f)}$$

Aus der Eindeutigkeit in Satz 11.28 folgt $v_p(f) = u_p \; \forall p \in P$. $\Rightarrow \prod_{p \in P} p^{u_p} = \prod_{p \in P} p^{v_p(f)}$

$\Rightarrow$ Kürzungsregel $\varepsilon' = \varepsilon$.

□

Teilerrelation und Exponenten der Produktdarstellung

Lemma (11.31)

Sei R ein faktorieller Ring, $P \subseteq R$ ein Repräsentantensystem der Primelemente, und seien $f, g \in R$ mit $f, g \neq 0_R$. Dann gilt $f|g$ genau dann, wenn $v_p(f) \leq v_p(g)$ für alle $p \in P$ erfüllt ist.

Darstellung von ggT und kgV durch die Exponenten

Satz (11.33)

Sei R ein faktorieller Ring, und sei $P \subseteq R$ ein Repräsentantensystem der Primelemente in R. Seien $f_1, ..., f_n \in R$ beliebige Elemente ungleich Null. Für jedes $p \in P$ definieren wir

$$u_p = \min\{v_p(f_i) \mid 1 \leq i \leq m\} \text{ und } w_p = \max\{v_p(f_i) \mid 1 \leq i \leq m\}.$$

Dann ist $f = \prod_{p \in P} p^{u_p}$ ein ggT und $g = \prod_{p \in P} p^{w_p}$ ein kgV der Elemente $f_1, ..., f_m$.

Dies zeigt also insbesondere, dass in einem faktoriellen Ring für beliebige endliche Mengen von Elementen jeweils ein kgV und ein ggT existieren.

Beispiel: Berechnung von $ggT(48, 92)$ und $kgV(48, 92)$

$48 = 16 \cdot 3 = 2^4 \cdot 3^1$, $92 = 4 \cdot 23 = 2^2 \cdot 23^1$

$\Rightarrow ggT(48, 92) = 2^{\min(4,2)} \cdot 3^{\min(1,0)} \cdot 23^{\min(0,1)}$

$= 2^2 \cdot 3^0 \cdot 23^0 = 4$

$kgV(48, 92) = 2^{\max(4,2)} \cdot 3^{\max(1,0)} \cdot 23^{\max(0,1)}$

$= 2^4 \cdot 3^1 \cdot 23^1 = 48 \cdot 23 = 1104$