Definition der irreduziblen Elemente

Definition (12.10)

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 (12.11)

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 (12.12)

In einem Integritätsbereich ist jedes Primelement irreduzibel.

Ideale in Hauptidealringen

Proposition (12.17)

Sei R ein Integritätsbereich und $p \in R$, $p \neq 0_R$. Genau dann ist p ein Primelement in R, wenn das Hauptideal (p) ein Primideal ist.

Satz (12.18)

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 (12.19)

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

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

Irreduzible Elemente in faktoriellen Ringen

Lemma (12.20)

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 selbst eine Einheit.

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

Proposition (12.21)

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

Beweis von Prop. 12.21

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

z.zg.: p ist prim

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

R faktoriell $\Rightarrow p$ ist Produkt $p_1 \cdot \ldots \cdot p_m$ von Primelementen (mit $m \geq 1$) Ang. $m \geq 2 \Rightarrow p = p_1 \cdot q$ mit $q = p_2 \cdot \ldots \cdot p_m$ $p_1 \notin R^\times$ (da Primelement)

q wird vom Primelement p_2 geteilt, ist wegen Lemma 12.20 also ebenfalls keine Einheit $\Rightarrow p = p_1 \cdot q$ steht im Widerspruch zur Irred. $\lightning$ also $m = 1$, $p = p_1$ ist prim. $\square$

Charakterisierung der faktoriellen Ringe

Satz (12.22)

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 ist $m = n$, und nach eventueller Umnummerierung der Elemente ist p_i assoziiert zu q_i für $1 \leq i \leq m$.

Beweis von Satz 12.22 geg.: Integritätsbereich R

z.zg.: Äquivalenz der Aussagen

(i) Existenz einer Darstellung als Produkt von Primelementen für jedes $r \in R$ mit $r \notin R^\times \cup \{0_R\}$

(ii) Existenz und Eindeutigkeit („im Wesentlichen") für jedes solche $r \in R$

„(i) $\Rightarrow$ (ii)" Sei $r \in R$ mit $r \notin R^\times \cup \{0_R\}$

Existenz: Vor (i) $\Rightarrow \exists\, m \in \mathbb{N}$, Primelemente $p_1, \dots, p_m$ mit $r = p_1 \cdot \dots \cdot p_m$ Jedes p_i ist auch ein irred. Element.

Eindeutigkeit: Zeige durch vollst. Ind. über $n \in \mathbb{N}$: Sind $p_1 \cdot \dots \cdot p_m = r = q_1 \cdot \dots \cdot q_n$ zwei Darstellungen von r als Produkt irred. Elemente, dann gilt $n = m$ und $p_i \sim q_i$ für $1 \le i \le m$,

nach evtl. Umnummerierung der Elemente

Ind.-Anf. ($n=1$): geg. $p_1 \cdot \ldots \cdot p_m = q_1$

Da q_1 irred ist, muss $m=1$ sein (sonst wäre $q_1 = p_1 \cdot (p_2 \cdot \ldots \cdot p_m)$ eine Darstellung von q_1 als Produkt von Nicht-Einheiten, denn offenbar ist $p_1 \notin R^\times$, und wäre $p_2 \cdot \ldots \cdot p_m$ eine Einheit, dann nach Lemma 12.20 (ii) auch p_2 ↯)

$\Rightarrow p_1 = q_1$, insb. also auch $p_1 \sim q_1$.

Ind.-schritt $n \mapsto n+1$: geg.:

$p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_{n+1}$ Nach Prop 12.21 sind p_i, q_j alles Primelemente. $q_1 \mid (p_1 \cdot \ldots \cdot p_m)$

$\xrightarrow{q_1 \text{ prim}}$ $q_1 \mid p_j$ für ein $j \in \{1, \ldots, m\}$, nach Umnum-

Nerezug o.B.d.A. $j=1$, d.h. $q_1 | p_1 \Rightarrow \exists c \in R$
mit $p_1 = c q_1$ p_1 irred., $q_1 \notin R^* \Rightarrow c \in R^*$ Also
sind p_1 und q_1 zueinander assoziiert ($p_1 \sim q_1$)

$c q_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_{n+1} \overset{\text{Kürzungs-regel}}{\Rightarrow}$

$(cp_2) \cdot p_3 \cdot \ldots \cdot p_m = q_2 \cdot \ldots \cdot q_{n+1}$, und wegen
$cp_2 \sim p_2$ ist auch cp_2 irreduzibel
Da $q_2 \cdot \ldots \cdot q_{n+1}$ ein Prod. von n Faktoren ist,
kann die Ind.-V. angewendet werden. $\Rightarrow$
$m-1 = n$, nach Umnummerierung $cp_2 \sim q_2$,
$p_j \sim q_j$ für $3 \le j \le n+1 \Rightarrow m = n+1$ und
$p_j \sim q_j$ für $1 \le j \le m$.

„(ii) → (i)" Hier ist zu zeigen, dass jedes irreduzible Element unter der Voraussetzung (ii) ein Primelement ist. Sei also $p \in R$ irreduzibel $\rightarrow p \notin R^* \cup \{0_R\}$. noch zu zeigen:

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

Seien also $a, b \in R$ mit $p \mid (ab) \Rightarrow \exists c \in R:$

$ab = pc$ (*)

1. Fall: $a = 0_R$ oder $b = 0_R$

Dann folgt direkt $p \mid a$ oder $p \mid b$ wegen $0_R = p \cdot 0_R$

2. Fall: $a \in R^*$ oder $b \in R^*$

Dann ist ab zu a oder zu b assoziiert, und aus $p \mid ab$ folgt direkt $p \mid a$ oder $p \mid b$, nach Lemma 12.20 i)

3. Fall: $a, b \notin R^\times \cup \{0_R\}$

Wegen Vor. (ii) gibt es $m, n \in \mathbb{N}$ und unred. Elemente $p_1, \dots, p_m, q_1, \dots, q_n$ mit $a = p_1 \cdot \dots \cdot p_m$, $b = q_1 \cdot \dots \cdot q_n$.

Ang. $c = 0_R \Rightarrow ab = 0_R \Rightarrow a = 0_R$ oder $b = 0_R$ ↯

Ist $c \in R^\times$, dann ist $p = (c^{-1}a) \cdot b$. p unred. $\Rightarrow$ $c^{-1}a \in R^\times$ oder $b \in R^\times \Rightarrow a \in R^\times$ oder $b \in R^\times$ ↯

also: $c \notin R^\times \cup \{0_R\}$ Vor. (ii) $\Rightarrow \exists\, t \in \mathbb{N}$ und unred. Elemente $r_1, \dots, r_t$ mit $c = r_1 \cdot \dots \cdot r_t$

Einsetzen der Produktzerlegungen in (*) $\rightarrow$

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

Auf Grund der Eindeutigkeit in (ii) gilt $p \sim p_i$ für ein $i \in \{1, \ldots, m\}$ oder $p \sim q_j$ für ein $j \in \{1, \ldots, m\}$. Wegen $p_i \mid a$ und $q_j \mid b$ folgt daraus $p \mid a$ oder $p \mid b$, nach Lemma 12.20 (i) $\square$

Repräsentantensysteme der Primelemente

Definition (12.23)

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.

Beispiele:

- Die Primzahlen $p \in \mathbb{N}$ bilden ein Repräsentantensystem der Primelmente in $\mathbb{Z}$.
- Ist K ein Körper, dann bilden die normierten irreduziblen Polynome ein Repräsentantensystem in $K[x]$.

Definition einer eindeutigen Primfaktorzerlegung

Folgerung (12.24)

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 12.24:

geg: faktorieller Ring R, $P \subseteq R$ Repr.-system der Primelemente, $f \in R \setminus \{0_R\}$

z.zg: Es gibt ein eindeutig bestimmtes $\varepsilon \in R^\times$ und eine eindeutig bestimmte Familie $(v_p(f))_{p \in P}$ in $\mathbb{N}_0$, so dass

(*) $f = \varepsilon \prod_{p \in P} p^{v_p(f)}$ und $v_p(f) = 0$ für alle bis auf endlich viele $p \in P$

Existenz: 1. Fall: $f \in R^\times$ Setze $v_p(f) = 0$ für alle $p \in P$ und $\varepsilon = f$. Dann ist (*) erfüllt.

2. Fall: $f \notin R^\times$ Da R faktoriell ist, existiert ein $m \in \mathbb{N}$

und Primelemente $q_1, \dots, q_m$ mit $f = q_1 \cdot \dots \cdot q_m$

Da P ein Repr.-system der Primelemente ist, ist jedes q_i assoziiert zu genau einem Element $p_i \in P$. $\longrightarrow$

$\exists \varepsilon_i \in R^\times$ mit $q_i = \varepsilon_i p_i$ Für jedes $p \in P$ definiere

$\nu_p(f) = |\{i \in \{1, \dots, m\} \mid p_i = p\}|$ Setze $\varepsilon = \varepsilon_1 \cdot \dots \cdot \varepsilon_m$

$\Rightarrow \varepsilon \in R^\times$, $\varepsilon \prod_{p \in P} p^{\nu_p(f)} = \varepsilon_1 \cdot \dots \cdot \varepsilon_m \cdot (p_1 \cdot \dots \cdot p_m)$

$= (\varepsilon_1 p_1) \cdot \dots \cdot (\varepsilon_m p_m) = q_1 \cdot \dots \cdot q_m = f$

Eindeutigkeit: Ang., $\varepsilon, \varepsilon' \in R^\times$ und $(\mu_p)_{p \in P}$, $(\nu_p)_{p \in P}$ mit

$\varepsilon \prod_{p \in P} p^{\mu_p} = f = \varepsilon' \prod_{p \in P} p^{\nu_p}$ Für jedes $p \in P$ muss der Faktor p wegen der Eind. in Satz 12.23 bis auf Assoziierte

gleich oft vorkommen (und p ist zu keinem anderen Element aus P assoziiert) $\Rightarrow u_p = v_p$ für alle $p \in P$. $\Rightarrow \prod_{p \in P} p^{u_p} = \prod_{p \in P} p^{v_p}$ $\Rightarrow$ Kürzungsregel

$\varepsilon = \varepsilon'$.

□

Die Teilerrelation in faktoriellen Ringen

Durch direktes Nachrechnen sieht man leicht, dass für alle $a, b \in R \setminus \{0_R\}$ jeweils

$$v_p(ab) = v_p(a) + v_p(b) \qquad \text{gilt.}$$

Lemma (12.25)

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.

Folgerung (12.26)

Sei R ein faktorieller Ring, und seien $a, b \in R \setminus \{0_R\}$ teilerfremd. Ist $0_R \neq c \in R$ ein Element mit $a|(bc)$, dann folgt $a|c$.

Beweis der Gleichung $v_p(ab) = v_p(a) + v_p(b)$
für alle $a, b \in R \setminus \{0_R\}$

Folgerung 12.24 $\Rightarrow \exists \varepsilon, \varepsilon' \in R^*$ und
Familien $(u_p)_{p \in P}, (v_p)_{p \in P}$ in $\mathbb{N}_0$ mit

$$a = \varepsilon \prod_{p \in P} p^{u_p}, \quad b = \varepsilon' \prod_{p \in P} p^{v_p} \Rightarrow$$

$$ab = \varepsilon\varepsilon' \prod_{p \in P} p^{u_p + v_p}$$ Für jedes $p \in P$

gilt somit $v_p(ab) = u_p + v_p = v_p(a) + v_p(b)$.

Beweis von Folgerung 12.26:

geg R faktorieller Ring, $P \subseteq R$ Repr.-system der Primelemente, $a, b, c \in R \setminus \{0_R\}$, wobei a und b teilerfremd. Vor.: $a \mid (b \cdot c)$ z.Zg: $a \mid c$

Ang $a \nmid c$. Lemma 12.25 $\Rightarrow$ $v_p(a) > v_p(c)$ für ein $p \in P$ andererseits: $a \mid (b \cdot c) \rightarrow v_p(a) \leq v_p(b) + v_p(c) \overset{v_p(a) > v_p(c)}{\Rightarrow} v_p(b) > 0$

also: $v_p(b) > 0$, $v_p(a) > 0$ $\Rightarrow$ p ist gemeinsamer Primteiler von a und b $\lightning$ zur Teilerfremdheit. $\square$

Der ggT und das kgV in Hauptidealringen

Satz (12.27)

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

$$u_p = \min\{v_p(f_i) \mid 1 \leq i \leq m\}$$

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 $f_1, ..., f_m$.

Beweis von Satz 12.27 (nur für den ggT)

R faktorieller Ring, $P \subseteq R$ Repr.-system der Primelemente, $m \in \mathbb{N}$, $f_1, \dots, f_m \in R \setminus \{0_R\}$, $u_p = \min\{v_p(f_j) \mid 1 \le j \le m\}$ für jedes $p \in P$, $f = \prod_{p \in P} p^{u_p}$

Beh: f ist ein ggT von $f_1, \dots, f_m$, dafür zu überprüfen

(i) $f \mid f_j$ für $1 \le j \le m$ (ii) $\forall g \in R: g \mid f_j$ für $1 \le j \le m \Rightarrow g \mid f$

zu (i) Sei $j \in \{1, \dots, m\}$. Für jedes $p \in P$ gilt $v_p(f) = u_p = \min\{v_p(f_1), \dots, v_p(f_m)\} \Rightarrow v_p(f) \le v_p(f_j)$. Aus $v_p(f) \le v_p(f_j)$ $\forall p \in P$ folgt $f \mid f_j$, mit Lemma 12.25.

zu (ii) Sei $g \in R$ mit $g \mid f_j$ für $1 \le j \le m$ $\overset{f_j \neq 0_R}{\Rightarrow}$ $g \neq 0_R$

Sei $p \in \mathbb{P}$ $g \mid f_j$ für $1 \le j \le m$ $\Rightarrow v_p(g) \le v_p(f_j)$ für $1 \le j \le m$

$u_p = \min\{v_p(f_1), \dots, v_p(f_m)\}$ $\Rightarrow$ $v_p(g) \le u_p = v_p(f)$ also:

$v_p(g) \le v_p(f)$ $\forall p \in \mathbb{P}$ $\overset{\text{Lemma 12.2}}{\Rightarrow}$ $g \mid f$ $\square$