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.

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

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

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 $1 \leq i \leq m$.

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 $p \in P$.

Anwendungsbeispiel für die eindeutige Primfaktor-zerlegung: Berechnung von ggT(-24, 60) und kgV(-24, 60)

eindeutige Primfaktorzerlegung:

$-24 = (-1) \cdot 2^3 \cdot 3^1 \cdot 5^0$, $60 = (+1) \cdot 2^2 \cdot 3^1 \cdot 5^1$

$\Rightarrow ggT(-24, 60) = 2^{\min\{3,2\}} \cdot 3^{\min\{1,1\}} \cdot 5^{\min\{0,1\}}$

$= 2^2 \cdot 3^1 \cdot 5^0 = 12$

$kgV(-24, 60) = 2^{\max\{3,2\}} \cdot 3^{\max\{1,1\}} \cdot 5^{\max\{0,1\}}$

$= 2^3 \cdot 3^1 \cdot 5^1 = 120$

Beweis von Folgerung 12.24:

geg.: faktorieller Ring R, $f \in R$, $f \notin R^\times \cup \{0_R\}$
$P \subseteq R$ Repräsentantensystem der Primelemente

z.zg.: Es gibt eine und bestimmte Familie $(v_p(f))_{p \in P}$ von Elementen $v_p(f) \in \mathbb{N}_0$ mit $v_p(f) = 0$ für alle bis auf endlich viele $p \in P$ und eine eindeutig bestimmte Einheit $\varepsilon \in R^\times$ mit $f = \varepsilon \prod_{p \in P} p^{v_p(f)}$

Eindeutigkeit: Ang., $(u_p)_{p \in P}$, $(v_p)_{p \in P}$ sind zwei solche Familien und $\varepsilon, \varepsilon' \in R^\times$ mit $\varepsilon \prod_{p \in P} p^{u_p} = f = \varepsilon' \prod_{p \in P} p^{v_p}$ (*)

Sei $p_1 \in P$. Das Primelement $p_1 \in P$ kommt im Produkt $\prod_{p \in P} p^{v_p}$ genau m-mal vor, wobei $m = v_{p_1}$.

Aus der Eindeutigkeitsaussage in Satz 12.22 folgt, dass genau m Faktoren im Produkt $\prod_{p \in P} p^{u_p}$ assoziiert zu p_1 sind. Das einzige Element in P, das assoziiert zu p_1 ist, ist p_1 selbst (da P ein Repr.-system der Primelemente von R ist) $\Rightarrow u_{p_1} = m = v_{p_1}$

also: $v_p = u_p \; \forall p \in P \Rightarrow \prod_{p \in P} p^{u_p} = \prod_{p \in P} p^{v_p}$

Kürzungsregel angew. auf (*) $\Rightarrow \varepsilon = \varepsilon'$

<u>Existenz:</u> R faktorieller Ring $\Rightarrow$

$\exists r \in \mathbb{N}_0$ und Primelemente $q_1, \ldots, q_r$ mit

$f = \prod_{i=1}^{r} q_i$ P Repr. der Primelemente $\Rightarrow$

Für $1 \le i \le r$ gilt es jeweils ein $p_i \in P$ und $\varepsilon_i \in R^\times$ mit $p_i \sim q_i$, $q_i = \varepsilon_i p_i$. Setzen wir für jedes $p \in P$ jeweils $\mu_p = |\{i \mid 1 \le i \le r, q_i \sim p\}|$, dann gilt insgesamt $f = \varepsilon \prod_{i=1}^{r} p_i = \varepsilon \prod_{p \in P} p^{\mu_p}$, wobei $\varepsilon = \prod_{i=1}^{r} \varepsilon_i$. $\square$

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 von Lemma 12.5

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

Beh.: $f \mid g \iff v_p(f) \leq v_p(g) \quad \forall p \in P$

Schreibe f, g in der Form $f = \varepsilon \prod_{p \in P} p^{u_p}$,

$g = \varepsilon' \prod_{p \in P} p^{w_p}$, mit $\varepsilon, \varepsilon' \in R^\times$. Dann gilt

$u_p = v_p(f)$, $w_p = v_p(g)$ $\forall p \in P$.

„$\Rightarrow$" $f \mid g \Rightarrow \exists h \in R$ mit $f \cdot h = g$

$g \neq 0_R \Rightarrow h \neq 0_R \Rightarrow \exists \varepsilon'' \in R^\times$ und eine Darstellung $h = \varepsilon'' \prod_{p \in P} p^{z_p} \Rightarrow \varepsilon' \prod_{p \in P} p^{w_p} =$

($\varepsilon'' \in R^\times$)

$$g = fh = \varepsilon \prod_{p \in P} p^{u_p} \cdot \varepsilon'' \prod_{p \in P} p^{z_p} = \varepsilon\varepsilon'' \prod_{p \in P} p^{u_p + z_p}$$

Eind.
$\Rightarrow \forall p \in P : v_p(g) = w_p = u_p + z_p = v_p(f) + z_p$, und

Folgerung 12.24
$z_p \in \mathbb{N}_0 \Rightarrow \forall p \in P : v_p(g) \geq v_p(f)$

„$\Leftarrow$" $\forall p \in P : v_p(g) \geq v_p(f) \Rightarrow$ Für jedes $p \in P$ gibt es ein $z_p \in \mathbb{N}_0$ mit $v_p(g) = v_p(f) + z_p$

$$\rightarrow g = \varepsilon' \prod_{p \in P} p^{w_p} = \varepsilon' \prod_{p \in P} p^{u_p + z_p} = \varepsilon \prod_{p \in P} p^{u_p} \cdot (\varepsilon' \varepsilon^{-1}) \cdot \prod_{p \in P} p^{z_p} = f \cdot h \text{ mit } h = \varepsilon' \varepsilon^{-1} \prod_{p \in P} p^{z_p}$$

$\Rightarrow f \mid g$. □

Beweis von Folgerung 12.26:

geg: faktorieller Ring R und einem Repr.-system $P \subseteq R$ der Primelemente, $a, b, c \in R$ mit $a, b, c \neq 0_R$
a und b teilerfremd, $a \mid bc$

zzg: $a \mid c$ Ang. a ist kein Teiler von c.

Lemma 12.25 $\Rightarrow$ Es gibt ein $p \in P$ mit $v_p(a) > v_p(c)$

$a \mid bc \overset{\text{Lemma 12.25}}{\Rightarrow} v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$

$v_p(a) > v_p(c)$, $v_p(a) \leq v_p(b) + v_p(c) \Rightarrow v_p(b) > 0$

$v_p(a), v_p(b) > 0 \Rightarrow p$ ist gem. Primteiler von a und b

↯ da a und b teilerfremd sind. □

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 $f_1, ..., f_m$.

Hauptidealring $\Rightarrow$ faktorieller Ring

Satz (12.28)

Jeder Hauptidealring R ist faktoriell.

Ergänzungen:

- Der Polynomring $\mathbb{Z}[x]$ ist faktoriell (als Polynomring über einem faktoriellen Ring, siehe nächstes Kapitel), aber kein Hauptidealring, denn das Ideal $I = (2, x)$ in $\mathbb{Z}[x]$ ist kein Hauptideal.
- Es gibt Hauptidealringe, die keine euklidischen Ringe sind (zum Beispiel den Ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$, siehe Anhang).

Beweis von Satz 12.28.

Sei R ein Hauptidealring zzg. R ist faktoriell

Weil in Hauptidealringen die Primelemente genau die irred. Elemente sind, genügt es zzg.: Jedes Element $a \in R$ mit $a \notin R^\times$, $a \neq 0_R$ ist Produkt irreduzibler Elemente.

Angenommen, a ist ein Element in $R \setminus (R^\times \cup \{0_R\})$, dass keine solche Produktdarstellung hat. Dann gibt es eine Folge $(a_n)_{n \in \mathbb{N}}$ in R, so dass gilt

(i) $a_n \notin R^\times$, $a_n \neq 0_R$

(ii) a_n hat keine Darstellung als Produkt irred. El.

(iii) $a_{n+1} \mid a_n$ und $a_n \not\sim a_{n+1}$

Setze $a_1 = a$. Dann sind (i) und (ii) für a_1 erfüllt.

Sei nun $n \in \mathbb{N}$. Arg., wir haben bereits die Existenz eines a_n nachgewiesen, das (i) und (ii) erfüllt. zeige: Es gibt ein a_{n+1}, das (iii) erfüllt ist, und (i) und (ii) für das Element a_{n+1}.

Eig. (ii) für $a_n \Rightarrow a_n$ ist nicht irreduzibel

$\Rightarrow \exists\, b, c \in R$ mit $a_n = b \cdot c$, $b, c \notin R^\times$

Eines der Elemente ist nicht als Prod. irred. Elemente darstellbar (weil sonst a_n eine solche Darstellung hätte), o.B.d.A. sei dies b.

Setze $a_{n+1} := b$. Es ist $b \neq 0_R$ (da sonst $a_n = 0_R$) $\Rightarrow a_{n+1}$ erfüllt insg. (i) und (ii)

Es gilt $a_{n+1} \mid a_n$ wg. $a_n = b \cdot c$ Ang. $a_n \mid a_{n+1}$

$\rightsquigarrow a_n \mid b \Rightarrow \exists d \in R$ mit $b = d a_n$ einsetzen

$\Rightarrow a_n = d a_n c \underset{\text{kürzungsr.}}{\Rightarrow} 1_R = dc \Rightarrow c \in R^* \lightning$

Insgesamt ist damit die Existenz einer Folge $(a_n)_{n \in \mathbb{N}}$ mit den angeg. Eigenschaften nachgewiesen.

Betrachte nun die Folge der Hauptideale (a_n), $n \in \mathbb{N}$.

$a_{n+1} \mid a_n$, $a_n \neq a_{n+1} \Rightarrow (a_n) \subseteq (a_{n+1})$, $(a_{n+1}) \nsubseteq (a_n)$

$\Rightarrow (a_n) \subsetneq (a_{n+1})$

Betrachte nun $I = \bigcup_{n \in \mathbb{N}} (a_n)$. Beh.: I ist Ideal in R.

$0_R \in (a_1)$ (da (a_1) Ideal), $(a_1) \subseteq I \Rightarrow 0_R \in I$

Seien nun $u, v \in I$ und $r \in R$. zu zeigen:

$u + v \in I$, $ru \in I$

$u, v \in I \Rightarrow \exists\, m, n \in \mathbb{N}$ mit $u \in (a_m)$, $v \in (a_n)$

O.B.d.A. $m \leq n$ (sonst vertausche u und v)

$\Rightarrow (a_m) \subseteq (a_n) \Rightarrow u, v \in (a_n) \overset{(a_n) \text{ ist Ideal}}{\Longrightarrow}$

$u+v \in (a_n)$, $ru \in (a_n) \overset{(a_n) \subseteq I}{\Longrightarrow} u+v, ru \in I$

($\Rightarrow$ Beh.) Da R ein Hauptidealring und I ein Ideal ist, existiert ein $a_0 \in I$ mit $I = (a_0)$

$\Rightarrow a_0 \in I \Rightarrow \exists\, n \in \mathbb{N}$ mit $a_0 \in (a_n)$

$(a_{n+1}) \subseteq I = (a_0)$, $a_0 \in (a_n) \Rightarrow (a_{n+1}) \subseteq (a_n)$

↯ da $(a_n) \subsetneq (a_{n+1})$ $\square$