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.

Irreduzibilität als Eigenschaft der Assoziiertenklasse

Notation:

Die Schreibweise $p \sim q$ bedeutet, dass zwei Ringelemente p und q zueinander assoziiert sind.

Proposition (12.13)

Sei R ein Integritätsbereich, und seien $p, q \in R$ mit $p \sim q$.

(i) Ist p irreduzibel, dann gilt dasselbe für q.

(ii) Ist p ein Primelement, dann ist auch q ein Primelement.

Proposition (12.14)

Im Ring $\mathbb{Z}$ der ganzen Zahlen sind die irreduziblen Elemente genau die Zahlen der Form $\pm p$, wobei p die Primzahlen durchläuft.

Irreduzible Elemente in $\mathbb{Z}[\sqrt{-d}]$

Proposition (12.15)

Sei $d \in \mathbb{N}$, $R = \mathbb{Z}[\sqrt{-d}]$ und $\alpha \in R$ beliebig.

(i) Das Element α ist genau dann eine Einheit in R, wenn $N(\alpha) = 1$ ist.

(ii) Ist $N(\alpha)$ eine Primzahl, dann ist α in R irreduzibel.

(iii) Gilt $N(\alpha) = p^2$ mit einer Primzahl p, und besitzt die Gleichung $a^2 + db^2 = p$ keine Lösung mit $a, b \in \mathbb{Z}$, dann ist α ebenfalls ein irreduzibles Element.

Folgerung (12.16)

Sei $d \in \mathbb{N}$. Für die Einheitengruppe von $R = \mathbb{Z}[\sqrt{-d}]$ gilt $R^\times = \{\pm 1, \pm\sqrt{-1}\}$, falls $d = 1$ ist, ansonsten $R^\times = \{\pm 1\}$.

Anwendung:

Das Element $2 \in \mathbb{Z}[\sqrt{-3}]$ ist irreduzibel, aber nicht prim.

Anwendung von Proposition 12.15:

zeige: Die Zahl 2 ist als Element des Rings $R = \mathbb{Z}[\sqrt{-3}]$ irreduzibel.

Sei $N : R \to \mathbb{N}_0$ die Normfkt. auf R geg. durch $N(a+b\sqrt{-3}) = a^2+3b^2 \ \forall a, b \in \mathbb{Z}$. Dann ist $N(2) = 4 = 2^2$, und die Gleichung $a^2+3b^2 = 2$ hat für $a, b \in \mathbb{Z}$ keine Lösung (denn: Ang. $a^2+3b^2 = 2$ mit $a, b \in \mathbb{Z}$. $\overset{3>2}{\Longrightarrow} b = 0, a^2 = 2$ $\lightning$ da 2 kein Quadrat in $\mathbb{Z}$ ist)

Nach Prop. 12.15 (iii) ist 2 in R also irreduzibel keine Lösung (denn: Ang. $a^2+3b^2=2$ mit $a,b\in\mathbb{Z}$.

$3>2$ ...

Beweis von Proposition 12.15:

geg: $R=\mathbb{Z}[\sqrt{-d}]$ mit $d\in\mathbb{N}$. $N: R\to\mathbb{N}_0$ Normfunktion

zu (i) Sei $\alpha\in R$. z.zg.: $\alpha\in R^\times \Leftrightarrow N(\alpha)=1$

„$\Rightarrow$" $\alpha\in R^\times \Rightarrow \exists\beta\in R$ mit $\alpha\beta=1 \Rightarrow N(\alpha\beta)=N(1)$

$\Rightarrow N(\alpha)N(\beta)=1 \xRightarrow{N(\alpha),N(\beta)\in\mathbb{N}_0} N(\alpha)=N(\beta)=1$

„$\Leftarrow$" $N(\alpha)=1 \Rightarrow \alpha\bar{\alpha}=1$ Seien $a,b\in\mathbb{Z}$ geg durch

$\alpha=a+b\sqrt{-d} \Rightarrow \bar{\alpha}=a-b\sqrt{-d} \Rightarrow \bar{\alpha}\in R$

Also ist das $\bar{\alpha}$ das multiplikative Inverse von α in R.

$\Rightarrow \alpha\in R^\times$

zu (ii) Sei $\alpha\in R$, so dass $p=N(\alpha)$ eine Primzahl ist.

z.zg.: p ist irreduzibel Ang. $\alpha=0 \Rightarrow p=N(\alpha)=0$ ↯

Ang. $\alpha \in R^\times$ $\overset{(i)}{\Longrightarrow}$ $p = N(\alpha) = 1$ $\lightning$

Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma$. z. zg.: $\beta \in R^\times$ oder $\gamma \in R^\times$. Es gilt $p = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. $N(\beta), N(\gamma) \in \mathbb{N}_0$ und p ist Primzahl $\Rightarrow N(\beta) = 1$ oder $N(\gamma) = 1$ $\overset{(i)}{\Longrightarrow}$ $\beta \in R^\times$ oder $\gamma \in R^\times$

zu (iii) Sei $\alpha \in R$ und p eine Primzahl mit $N(\alpha) = p^2$. Setze voraus, dass keine $a, b \in \mathbb{Z}$ mit $p = a^2 + db^2$ existieren. z. zg.: α ist irred.

Zeige wie unter (ii), dass $\alpha \neq 0_R$ und $\alpha \notin R^\times$ gilt.

„$\Rightarrow$

$\exists$

Sei

$\exists\, c \in$

$p \mid a$

$b = p$

Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma$. Angenommen, es gilt $\beta \notin R^\times$ und $\gamma \notin R^\times \overset{(i)}{\Longrightarrow} N(\beta), N(\gamma) > 1$

außerdem: $p^2 = N(\alpha) = N(\beta)N(\gamma)$

$\xrightarrow[N(\beta), N(\gamma) > 1]{p \text{ Primzahl}}$ $N(\beta) = N(\gamma) = p$ Schreiben wir $\beta = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann folgt $p = N(\beta) = a^2 + db^2$. $\lightning$ zur Voraussetzung $\square$

"

(

p

(p)

$\Rightarrow$

$a =$

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 äquivalent.

(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 $p \neq 0_R$.

(α)

$\in \mathbb{N}_0$

$\gamma) = 1$

mit

$b \in \mathbb{Z}$

red.

R^* gilt!

Beweis von Proposition 12.17

geg: Integritätsbereich R, $p \in R \setminus \{0_R\}$

Beh.: p ist Primelement $\Longleftrightarrow$ (p) ist Primideal

„$\Longrightarrow$“ Ang. $(p) = (1_R) \Rightarrow 1_R \in (p) \Rightarrow$

$\exists c \in R$ mit $1_R = pc \Rightarrow p \in R^*$ ↯

Seien $a, b \in R$ mit $ab \in (p) \Rightarrow$

$\exists c \in R$ mit $ab = pc \Rightarrow p \mid (ab) \xRightarrow{p \text{ ist prim}}$

$p \mid a$ oder $p \mid b \Rightarrow \exists c \in R$ mit $a = pc$ oder

$b = pc \Rightarrow a \in (p)$ oder $b \in (p)$

„$\Leftarrow$" Vor. $\Rightarrow p \neq 0_R$ Ang. $p \in R^\times \Rightarrow$
$\exists c \in R$ mit $pc = 1_R \Rightarrow 1_R \in (p) \Rightarrow (p) = (1_R)$ $\lightning$
(zu (p) Primideal) Seien $a, b \in R$ mit
$p \mid (ab) \Rightarrow \exists c \in R$ mit $pc = ab \Rightarrow ab \in (p)$
$\xRightarrow{(p) \text{ Primideal}}$ $a \in (p)$ oder $b \in (p) \Rightarrow \exists c \in R$ mit
$a = pc$ oder $b = pc \Rightarrow p \mid a$ oder $p \mid b$. $\square$

Beweis von Satz 12.18

geg.: Hauptidealring R, R kein Körper, $p \in R$

z.zg.: Äquivalenz der vier Aussagen

(i) p ist prim (ii) p ist irred. (iii) (p) ist max. (iv) (p) ist Primideal und $p \neq 0_R$

„(i) $\Rightarrow$ (ii)" Jedes Primelement ist irreduzibel. (Das gilt sogar in beliebigen Integritätsbereichen.)

„(ii) $\Rightarrow$ (iii)" Ang. p ist irred., aber (p) ist kein maximales Ideal. Dann ist entweder $(p) = (1_R)$ oder es gibt ein Ideal I in R mit $(p) \subsetneq I \subsetneq (1_R)$

<u>1. Fall:</u> $(p) = (1_R)$. Dann gilt $1_R \in (p) \Rightarrow \exists c \in R$ mit

$pc = 1_R \Rightarrow p \in R^\times$ ↯ zu p irred.

2. Fall: Es gibt ein Ideal I mit $(p) \subsetneq I \subsetneq (1_R)$

R Hauptidealring $\Rightarrow \exists m \in R$ mit $I = (m)$ $\quad p \in (m) \Rightarrow$
$\exists c \in R$ mit $p = mc \overset{p \text{ irred.}}{\Longrightarrow} m \in R^\times$ oder $c \in R^\times$

Fall 2.1: $m \in R^\times \Rightarrow \exists n \in R$ mit $nm = 1_R \Rightarrow 1_R \in (m) \Rightarrow$
$I = (m) = (1_R)$ ↯ zu $I \subsetneq (1_R)$

Fall 2.2: $c \in R^\times \Rightarrow pc^{-1} = m \Rightarrow m \in (p) \Rightarrow (m) \subseteq (p)$
$\Rightarrow I \subseteq (p) \overset{(p) \subseteq I}{\Longrightarrow} (p) = I$ ↯ zu $(p) \subsetneq I$

„(iii) ⇒ (iv)" Jedes maximale Ideal ist ein Primideal
(gilt in beliebigen Ringen). Ang. $p = 0_R$. Dann wäre

das Nullideal (0_R) ein maximales Ideal.

Dann gäbe es in R genau zwei Ideale nämlich (0_R) und (1_R). Daraus würde folgen, dass R ein Körper ist. $\lightning$

„(iv) $\Rightarrow$ (i)" Vor. $\Rightarrow$ (p) ist Primideal, $p \neq 0_R$

$\overset{\text{Prop. 12.17}}{\Longrightarrow}$ p ist Primelement. $\square$

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

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

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 Proposition 12.21

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

z.zg.: p ist Primelement

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

$\exists n \in \mathbb{N}$, Primelemente $p_1, \dots, p_n$ mit $p = p_1 \cdot \ldots \cdot p_n$.

Ang. $n \geq 2$. p_1 ist prim $\Rightarrow p_1 \notin R^\times$

Lemma 12.20 $\Rightarrow q = p_2 \cdot \ldots \cdot p_n \notin R^\times$

$\Rightarrow p = p_1 \cdot q$, $p_1, q \in R^\times$ ↯ zur Irred. von r

Also gilt $p = p_1 \Rightarrow p$ ist Primelement. $\square$

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) Jedes $r \in R \setminus (R^\times \cup \{0_R\})$ ist Produkt von Primelementen.

(ii) Jedes solche r hat eine im Wesentlichen eindeutige Darstellung als Produkt irreduzibler Elemente.

„(ii) $\Rightarrow$ (i)" z.zg.: Unter der Voraussetzung (ii) ist jedes irreduzible Element in R ein Primelement.

Sei also p ein irreduzibles Element $\Rightarrow p \neq 0_R,\ p \notin R^*$. Seien $a, b \in R$ mit $p \mid ab$. z.zg.: $p \mid a$ oder $p \mid b$

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

Ang. $a = 0_R$ oder $b = 0_R \Rightarrow p \mid a$ oder $p \mid b$ (da 0_R von jedem Element aus R geteilt wird)

Ang. $a \in R^*$. $\Rightarrow ab \sim b \underset{p \mid ab}{\overset{\text{Lemma 12.20}}{\Longrightarrow}} p \mid b$

Ebenso behandelt man den Fall $b \in R^*$.

Wir können also $a, b \notin R^* \cup \{0_R\}$ voraussetzen. Voraussetzung (ii) $\Rightarrow$

Es gibt $m, n \in \mathbb{N}$ und irreduzible Elemente $p_1, \dots, p_m \in R$ und $q_1, \dots, q_n \in R$ mit $a = p_1 \cdot \ldots \cdot p_m$, $b = q_1 \cdot \ldots \cdot q_n$

Ang. $c = 0_R \overset{pc = ab}{\Longrightarrow} ab = 0_R \overset{R \text{ Int. B.}}{\Longrightarrow} a = 0_R \vee b = 0_R$

Das wurde schon ausgeschlossen

Ang. $c \in R^\times \Rightarrow ab \sim p \Rightarrow ab$ ist irred $\Rightarrow a \in R^\times$ oder $b \in R^\times$ (wurde bereits ausgeschlossen)

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

$pc = ab$ einsetzen $\Rightarrow p \cdot r_1 \cdot \ldots \cdot r_t =$
$p_1 \cdot \ldots \cdot p_m \cdot q_1 \cdot \ldots \cdot q_n$ Eindeutigkeit in (ii)

$\Rightarrow p \sim p_i$ für ein $i \in \{1, \dots, m\}$ oder $p \sim q_j$ für ein
$j \in \{1, \dots, n\}$. Im ersten Fall gilt $p \mid a$, im zweiten $p \mid b$.
„(ii) $\Rightarrow$ (i)" Sei $a \in R^\times \cup \{0_R\}$. Nach Vor. hat a eine
Darstellung als Produkt von Primelementen, also auch als
Produkt von irred. Elementen. Für die Eindeutigkeit zeige
durch vollst. Ind. über n: Ist $m \in \mathbb{N}$ und sind $p_1, \dots, p_m, q_1, \dots, q_n$
irred. Elemente mit $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$, dann gilt $m = n$
und $p_i \sim q_i$ nach Umnummerierung. Nach Prop. 12.21 sind die p_i, q_j
prim. Ind.-Anf.: Vor. $p_1 \cdot \ldots \cdot p_m = q_1$, q_1 irred., $p_i \notin R^\times$ $(1 \le i \le m)$
$\Rightarrow m = 1, p_1 = q_1$. Ind.-Schritt: $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_{n+1}$. q_1 ist
prim, teilt $p_1 \cdot \ldots \cdot p_m \Rightarrow q_1 \mid p_j$ für ein j, nach Umnummerierung
o.B.d.A. $j = 1$. p_1 irred., $q_1 \mid p_1 \Rightarrow q_1 \sim p_1 \Rightarrow \exists \varepsilon \in R^\times: \varepsilon p_1 = q_1$

Setzen wir dies ein, so erhalten wir die Gleichung

$$p_1 \cdot p_2 \cdot \ldots \cdot p_m \;=\; \varepsilon p_1 \cdot q_2 \cdot \ldots \cdot q_{n+1}.$$

Die Anwendung der Kürzungsregel liefert

$$p_2 \cdot \ldots \cdot p_m \;=\; \varepsilon q_2 \cdot \ldots \cdot q_{n+1}.$$

Die Induktionsvoraussetzung liefert $m-1=n$ und nach Umsortierung $p_2 \sim \varepsilon q_2$ und $p_j \sim q_j$ für $3 \le j \le m$. Es folgt $m = n+1$, und insgesamt $p_j \sim q_j$ für $1 \le j \le n+1$.