Definition der euklidischen Ringe

Definition (11.9)

- Eine Höhenfunktion auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung $a = qb + r$ erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt.
- Ein euklidischer Ring ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

euklidischer Ring $\Rightarrow$ Hauptidealring

Satz (11.14)

Jeder euklidische Ring R ist ein Hauptidealring.

Quadratischer Zahlring, der kein Hauptidealring ist

Proposition (11.15)

Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring, denn beispielsweise ist das Ideal $\mathfrak{p} = (3, 1 + 2\sqrt{-5})$ kein Hauptideal.

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

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

Zusammenhänge zwischen den Begriffen

Satz (11.18)

In einem Integritätsbereich ist jedes Primelement irreduzibel.

Proposition (11.19)

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

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

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

Beweis von Satz 11.18

geg: Ring R, Primelement p in R

z.zg.: p ist irreduzibel in R

Da p Primelement ist, gilt $p \neq 0$ und $p \notin R^*$.

Seien nun $a, b \in R$ mit $p = ab$, z.zg.:

$a \in R^*$ oder $b \in R^*$

$p = ab \Rightarrow p \mid (ab) \overset{p \text{ prim}}{\Longrightarrow} p \mid a$ oder $p \mid b$,

o.B.d.A. $p \mid a$, $\Rightarrow \exists c \in R$ mit $a = pc$

$\Rightarrow p = (pc)b = p(cb) \overset{p \neq 0}{\underset{\text{Kürzungsregel}}{\Longrightarrow}}$

$1_R = cb \Rightarrow b \in R^\times$ $\square$

Beweis von Prop. 11.19:

geg. Integritätsbereich R
zueinander assoziierte Elemente $p, q \in R$, d.h. $\exists \varepsilon \in R^\times$ mit $q = \varepsilon p$

zu ii) Vor: p ist irred., z.zg.: q ist irreduzibel

Ang. $q = 0_R \Rightarrow p = \varepsilon^{-1} q = \varepsilon^{-1} \cdot 0_R = 0_R$
↯ zu p irreduzibel

Ang. $q \in R^\times \Rightarrow p = \varepsilon^{-1} q \in R^\times$ ↯

also: $q \neq 0_R$, $q \notin R^\times$

Seien $a, b \in R$ mit $q = ab$ z.Zg:

$a \in R^\times$ oder $b \in R^\times$ $\quad q = ab \Longrightarrow$

$p = (\varepsilon^{-1} a) b \overset{p \text{ irred.}}{\Longrightarrow} \varepsilon^{-1} a \in R^\times$ oder

$b \in R^\times \Longrightarrow a = \varepsilon(\varepsilon^{-1} a) \in R^\times$ oder $b \in R^\times$

zu (ii) Vor. p ist Primelement z.Zg.: q ist Primelement s.o. $\Rightarrow$ Aus $p \neq 0_R$, $p \notin R^\times$ folgt dasselbe für q. Seien $a, b \in R$ mit $q \mid (ab)$

z.Zg.: $q \mid a$ oder $q \mid b$ $\quad q \mid (ab) \Rightarrow \exists c \in R$ mit

$ab = cq = c\varepsilon p \Rightarrow p \mid (ab) \overset{p \text{ Prim}}{\Longrightarrow} p \mid a$

oder $p \mid b$, o.B.d.A. $p \mid a$. $\Rightarrow \exists d \in R$ mit

$a = dp = d\varepsilon^{-1} q \Rightarrow q \mid a$. $\square$

Primelemente und irreduzible Elemente in $\mathbb{Z}$

Proposition (11.20)

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 quadratischen Zahlringen

Proposition (11.21)

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 (11.22)

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 $R^\times = \{\pm 1\}$.

Beweis von Prop. 11.21

geg. $R = \mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$
mit $d \in \mathbb{N}$, $\alpha \in R$, $N : R \to \mathbb{N}_0$ Norm-
funktion

zu (i) Beh. $\alpha \in R^\times \iff N(\alpha) = 1$

„$\Leftarrow$" $N(\alpha) = 1 \Rightarrow \alpha\bar{\alpha} = 1$ (und $\bar{\alpha} \in R$)
$\Rightarrow \alpha \in R^\times$

„$\Rightarrow$" Sei $\alpha \in R^\times \Rightarrow \exists\, \beta \in R$ mit $\alpha\beta = 1$.
$\Rightarrow N(\alpha\beta) = N(1) = 1 \Rightarrow N(\alpha)N(\beta) = 1$
$\overset{N(\alpha), N(\beta) \in \mathbb{N}_0}{\Longrightarrow}$ $N(\alpha) = 1$

zu ii) Vor.: $p = N(\alpha)$ ist Primzahl

z.zg.: α ist irreduzibel

Ang. $\alpha = 0 \Rightarrow N(\alpha) = 0$ ↯

Ang. $\alpha \in R^\times \overset{(i)}{\Rightarrow} N(\alpha) = 1$ ↯ also: $\alpha \neq 0, \alpha \notin R^\times$

Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma$. z.zg.:

$\beta \in R^\times$ oder $\gamma \in R^\times$

$\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta\gamma) \Rightarrow p = N(\beta)N(\gamma)$

$N(\beta), N(\gamma) \in \mathbb{N}_0$

$\Rightarrow$ p Primzahl $N(\beta) = 1$ oder $N(\gamma) = 1$

$\overset{(i)}{\Rightarrow} \beta \in R^\times$ oder $\gamma \in R^\times$

□

zu (ii) Vor: $N(\alpha) = p^2$, p Primzahl. es gibt keine $a, b \in \mathbb{Z}$ mit $a^2 + db^2 = p$ z.zg: α ist irreduzibel

Ang $\alpha = 0 \Rightarrow N(\alpha) = 0$ ↯ Ang. $\alpha \in R^\times \overset{(i)}{\Rightarrow} N(\alpha) = 1$ ↯

also: $\alpha \notin R^\times$ und $\alpha \neq 0$.

Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma$. z.zg: $\beta \in R^\times$ oder $\gamma \in R^\times$

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

Ang $\beta \notin R^\times$ und $\gamma \notin R^\times$ $\overset{(i)}{\Rightarrow} N(\beta), N(\gamma) \neq 1$

$p^2 = N(\beta)N(\gamma)$, $N(\beta), N(\gamma) \in \mathbb{N} \setminus \{1\} \Rightarrow$

$N(\beta) = N(\gamma) = p$ Seien $a, b \in \mathbb{Z}$ mit $\beta = a + b\sqrt{-d}$

$\Rightarrow p = N(\beta) = a^2 + db^2$ ↯ zur Unlösbarkeit □

Bsp Sei $R = \mathbb{Z}[\sqrt{-3}]$. Dann ist 2 in R irreduzibel, aber kein Primelement.

(i) Irreduzibilität: folgt aus Prop. 11.21, denn $N(2) = 4 = 2^2$ ist Primzahlquadrat, aber $2 = a^2 + 3b^2$ ist unlösbar mit $a, b \in \mathbb{Z}$

(ii) kein Primelement Es gilt $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

$\Rightarrow 2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$ Ang 2 ist Primelement.

Dann würde $2 \mid (1+\sqrt{-3})$ oder $2 \mid (1-\sqrt{-3})$ folgen

Ang $2 \mid (1+\sqrt{-3}) \Rightarrow \exists \gamma \in R : 1+\sqrt{-3} = 2\gamma \Rightarrow$

$\gamma = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$ ↯ da $\frac{1}{2} + \frac{1}{2}\sqrt{-3} \notin R$ $(\sqrt{-3} = i\sqrt{3})$

genauso. $2 \nmid (1-\sqrt{-3})$ Also ist 2 kein Primelement. □

Primelemente und Primideale

Proposition (11.23)

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.

Beweis von Prop. 11.23

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

Erinnerung: Ein Ideal I in R ist ein Primideal, wenn $I \neq (1_R)$ gilt und aus $ab \in I$ jeweils $a \in I$ oder $b \in I$ folgt, für alle $a, b \in R$.

Beh. p ist Primelement $\Leftrightarrow$ (p) ist Primideal

„$\Rightarrow$" Ang. $(p) = (1_R)$. $\Rightarrow 1_R \in (p) \Rightarrow \exists c \in R$:

$1_R = cp \Rightarrow p \in R^\times$ ↯ zu p Primelement

Seien $a, b \in R$ mit $ab \in (p)$. $\Rightarrow p \mid (ab)$ $\overset{p \text{ Primelement}}{\Rightarrow}$

$p \mid a$ oder $p \mid b \Rightarrow a \in (p)$ oder $b \in (p)$

„$\Leftarrow$" $p \neq 0$ gilt lt. Voraussetzung Ang. $p \in R^\times \Rightarrow$
$\exists c \in R$ mit $cp = 1_R \Rightarrow 1_R \in (p) \Rightarrow (p) = (1_R)$ ↯
zu (p) Primideal

Seien $a, b \in R$ mit $p \mid (ab)$ z.zg.: $p \mid a$ oder $p \mid b$

$p \mid (ab) \Rightarrow ab \in (p) \overset{(p) \text{ Primideal}}{\Rightarrow} a \in (p)$ oder $b \in (p)$
$\Rightarrow p \mid a$ oder $p \mid b$. □

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 $p \neq 0_R$.

Beweis von Satz 11.24

geg: Hauptidealring R, der kein Körper ist
$p \in R$ z.zg: Äquivalenz der Aussagen

(i) p ist prim (ii) p ist irreduzibel

(iii) (p) ist max. Ideal (iv) (p) ist Primideal, $p \neq 0$

[R Ring, I max. Ideal $\Leftrightarrow$ $I \neq (1_R)$ und es gibt kein Ideal J mit $I \subsetneq J \subsetneq (1_R)$]

„(i) $\Rightarrow$ (ii)" gilt in beliebigen Integritätsbereichen

„(ii) $\Rightarrow$ (iii)" z.zg.: (1) $(p) \neq (1_R)$

(2) Es gibt kein Ideal J mit $(p) \subsetneq J \subsetneq (1_R)$

zu (1) Ang. $(p) = (1_R) \Rightarrow 1_R \in (p) \Rightarrow \exists c \in R$:
$1_R = pc \Rightarrow p \in R^\times$ ↯ zu p irreduzibel

zu (2) Ang. es existiert ein J wie angegeben.
R Hauptidealring $\Rightarrow \exists a \in J$ mit $J = (a)$
$(p) \subseteq (a) \Rightarrow p \in (a) \Rightarrow a \mid p \Rightarrow \exists c \in R$
mit $p = ac$. Da p irreduzibel ist, folgt
$a \in R^\times$ oder $c \in R^\times$
1. Fall: $a \in R^\times$ s.o. $\Rightarrow J = (a) = (1_R)$ ↯
2. Fall: $c \in R^\times \Rightarrow a = c^{-1} p \Rightarrow a \in (p) \Rightarrow$

$J = (a) \subseteq (p) \overset{(p) \subseteq J}{\Longrightarrow} \Rightarrow (p) = J$ ↯

„(iii) ⇒ (iv)" bekannt: Jedes maximale Ideal ist ein Primideal. Ang. $p = 0_R$

$\Rightarrow (0_R)$ ist max. Ideal

Beh.: Dann ist R ein Körper, im Widerspruch zur Voraussetzung

Sei $c \in R \setminus \{0_R\}$. $\Rightarrow (0_R) \subsetneq (c)$

$\overset{(0_R) \text{ ist max. Ideal}}{\Longrightarrow} (c) = (1_R) \Rightarrow 1_R \in (c)$

$\Rightarrow \exists\, r \in R : rc = 1_R \Rightarrow c \in R^*$

Ein Integritätsbereich, in dem jedes Element $\neq 0_R$ Einheit ist, ist ein Körper.

„(iv) $\Rightarrow$ (i)" folgt aus Prop. 11.23