(siehe
ing. und
alle Ring
eduziblen

e Ringe:
[i], $\mathbb{Z}[\sqrt{-2}]$
aber z.B.

Def. Ideal = Teilmenge I eines Rings R mit den Eigenschaften (i) $0_R \in I$ (ii) $\forall a, b \in I$: $a+b \in I$ (iii) $\forall r \in R, a \in I$: $ra \in I$

Die Teilmenge $(a) = \{ra \mid r \in R\}$ bestehend aus den Vielfachen eines Ringelements a heißt das von a erzeugte Hauptideal genannt.

Das von einer endlichen Teilmenge $\{a_1, \dots, a_n\} \subseteq R$ erzeugte Ideal ist gegeben durch

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \dots, r_n \in R \right\}.$$

$\sqrt{-2}$]

Das von einer endlichen Teilmenge $\{a_1, \dots, a_n\} \subseteq R$ erzeugte Ideal ist gegeben durch

wichtige Regel: $(a_1, \dots, a_m) = (b_1, \dots, b_n) \iff$

$a_i \in (b_1, \dots, b_n)$ für $1 \le i \le m$ und $b_j \in (a_1, \dots, a_m)$ für $1 \le j \le n$.

Def. ii) Hauptidealring = Integritätsbereich, in dem jedes Ideal ein Hauptideal ist

iii) faktorieller Ring = Integritätsbereich, in dem jedes Element, das weder Einheit noch null ist, als Produkt von Primelementen darstellbar ist (gleichbedeutend: Jedes solche Element ist darstellbar als Produkt irreduzibler Elemente, und diese Darstellung ist eindeutig bis auf Reihenfolge und Einheiten)

$\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, aber z. B.

- faktoriell, aber kein Hauptidealring:
  $\mathbb{Z}[x]$, $K[x,y]$ (wobei K Körper)
  $I = (2, x)$ kein Hauptideal in $\mathbb{Z}[x]$
  $J = (x, y)$ kein Hauptideal in $K[x,y]$
- Hauptidealring, aber nicht euklidisch:
  $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$

Erinnerung: • Jeder euklidische Ring (siehe nächste Woche) ist ein Hauptidealring, und jeder Hauptidealring ist ein faktorieller Ring.

• In faktoriellen Ringen sind die irreduziblen Elemente genau die Primelemente.

• wichtige Beispiele für euklidische Ringe: $\mathbb{Z}$, $K[x]$ (falls K Körper), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, aber z.B. nicht $\mathbb{Z}[\sqrt{-3}]$

H24T1A3 geg. k Körper, $R = \{f \in k[x] \mid$

$\exists n \in \mathbb{N}_0, a_0, \dots, a_n \in k$ mit $f = \sum_{k=0}^{n} a_k x^k$, wobei $a_1 = 0_k\}$

(a) gezeigt: R ist Teilring von $k[x]$

(b) Ist $x^3 \in R$ irreduzibel (bzw. prim) in R?
(mit Begründung)

Das Element ist irreduzibel, denn:
Ansonsten gäbe es eine Zerlegung $x^3 = f \cdot g$
mit $f, g \in R \setminus R^\times \Rightarrow \operatorname{grad}(f) + \operatorname{grad}(g)$
$= \operatorname{grad}(x^3) = 3$, o.B.d.A. (nach evtl Vertauschung von f und g) $\operatorname{grad}(f) \leq \operatorname{grad}(g)$

mit
$x \cdot$
$\Rightarrow$
aber:
Das
denn:
Dann ist
ein Teil
• $x^3 +$
$>$ gr
• $x^3 +$ g
$\exists h \in$

1. Fall: $\operatorname{grad}(f) = 0$, $\operatorname{grad}(g) = 3$

Dann liegt f in $K^\times$ ($f = 0_K$ ist ausgeschlossen, da sonst $x^3 = f \cdot g = 0_K$) $\Rightarrow \exists\, h \in K \subseteq R$ mit $f \cdot h = 1_K \Rightarrow f \in R^\times$ $\lightning$

2. Fall: $\operatorname{grad}(f) = 1$, $\operatorname{grad}(g) = 2$

(Der Fall $\operatorname{grad}(f) \geq 2$ ist ausgeschlossen, da sonst $3 = \operatorname{grad}(f) + \operatorname{grad}(g) \geq 2 \cdot \operatorname{grad}(f) = 4$ $\lightning$.)

Die Zerlegung $x^3 = f \cdot g$ ist auch eine Zerlegung in $K[x]$. Der Ring $K[x]$ ist faktoriell, und $x^3 = x \cdot x \cdot x$ ist die bis auf Reihenfolge und Einheiten einzige Zerlegung von x^3 in irreduzible Faktoren. Aus $x^3 = f \cdot g$ folgt somit, dass f und g bis auf Einheiten

$f \in K[x]$ ||

$\ldots$ der $a_1 = 0_K$?

$\ldots$

$\ldots$ m) in R?

$\ldots$

$x^3 = f \cdot g$

$\ldots$ + grad(g)

$\ldots$ ach evtl Ver-

$\ldots$ f) $\leq$ grad(g)

mit Potenzen des einzigen (wed. Faktors x. übereinstimmen. grad(f) = 1, grad(g) = 2

$\Rightarrow \exists c \in K^\times$ mit $f = c \cdot x$, $g = c^{-1} \cdot x^2$

aber: $f \notin R$ ↯

Das Element x^3 ist nicht prim, denn: Sei $a = x^2$ und $b = x^4$.

Dann ist x^3 wegen $a \cdot b = x^6 = x^3 \cdot x^3$ ein Teiler von $a \cdot b$, aber:

- $x^3 \nmid a$ wegen grad(x^3) = 3 > grad(a) = 2
- $x^3 \nmid b$, denn: Ang. $x^3 \mid b$ $\Rightarrow$ $\exists h \in R$ mit $x^4 = b = h \cdot x^3$

geschlossen.

$K \subseteq R$

en, da

$d(f) = 4 \not< 4.$

Zerlegung in

und $x^3 = x \cdot x \cdot x$

en einzige Zer-

ren. Aus $x^3 =$

auf Einheiten

$K[x]$ Teil-G.

$\Longrightarrow$

Kürzungsregel

$h = x \not\mid$ da $x \notin R$

(c) Entscheiden Sie, ob R ein faktorieller Ring ist.

Wäre R faktoriell, dann müsste jedes irreduzible Element in R ein Primelement sein. Teil (b) $\Rightarrow x^3$ ist irreduzibel, aber nicht prim. Also ist R kein faktorieller Ring.

(d) Finden Sie ein $a \in R$ mit der Eigenschaft, dass $I = (x^3, a)$ kein Hauptideal ist (mit Nachweis).

Beh.: $I = (x^3, x^2)$ ist kein Hauptideal

in R, d.h. $a = x^2$ hat die gewünschte Eigenschaft

Ang. $f \in R$ ist ein Element mit $(f) = (x^2, x^3) \Rightarrow$

$x^2, x^3 \in (f) \Rightarrow f \mid x^2$ und $f \mid x^3 \Rightarrow \exists\, g \in R$ mit $x^2 = f \cdot g$ Das Element x^2 hat im faktoriellen Ring $K[x]$ die Zerlegung $x^2 = x \cdot x$ in irreduzible Faktoren. f setzt sich bis auf Einheiten aus diesen Faktoren zusammen $\Rightarrow \exists\, c \in K^\times, m \in \{0, 1, 2\}$ mit $f = c x^m$

1. Fall: $m = 0$ Dann wäre $(x^2, x^3) = (c)$ und somit $(x^2, x^3) = (1_K)$, da c in $K[x]$ eine Einheit ist

$\Rightarrow \exists\, u, v \in k[x]$ mit $u \cdot x^2 + v \cdot x^3 = 1_k \Rightarrow x^2 \mid 1_k$ in $k[x]$ ↯ da $\operatorname{grad}(x^3) = 2 > 0 = \operatorname{grad}(1_k)$

2. Fall: $m = 1$ Dann wäre $f = c \cdot x \notin R$ ↯

3. Fall: $m = 2$ s.o. $\Rightarrow f \mid x^3$ in $R \Rightarrow c \cdot x^2 \mid x^3$ in R

$\Rightarrow \exists\, u \in R$ mit $x^3 = c \cdot x^2 u \overset{\text{Kürzungsregel}}{\Rightarrow} u = c^{-1} x$ ↯

da $c^{-1} x \notin R$ □

Erinnerung: Sei $d \in \mathbb{N}$ und

$R = \mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$

Definition der Normfunktion $N : R \to \mathbb{N}_0$:

$\alpha = a + b\sqrt{-d}$ (mit $a, b \in \mathbb{Z}$) $\Rightarrow N(\alpha) = \alpha\overline{\alpha} = a^2 + db^2$

wichtige Eigenschaft: Multiplikativität

$N(\alpha\beta) = N(\alpha)N(\beta) \quad \forall \alpha, \beta \in R$

Sei $\alpha \in R$. Laut Vorlesung gilt

(i) $N(\alpha) = 1 \iff \alpha \in R^*$

(ii) $N(\alpha)$ Primzahl $\Rightarrow \alpha$ in R irreduzibel

(iii) $N(\alpha) = p^2$ für eine Primzahl p und es gibt keine $a, b \in \mathbb{Z}$ mit $a^2 + db^2 = p$
$\Rightarrow \alpha$ ist irreduzibel in R

F24T3A1 (c) Bestimmen Sie ein $f \in \mathbb{R}[x]$ mit $(f) = (x^2 - 1, x^3 - 1)$.

(f) Zeigen Sie, dass 2 in $\mathbb{Z}[\sqrt{-13}]$ ein irreduzibles Element ist.

[Überlegung: Ist f ein solches Element, dann sind $x^2 - 1$ und $x^3 - 1$ wegen $x^2 - 1 \in (f)$ und $x^3 - 1 \in (f)$ beides Vielfache von f.
$x^2 - 1 = (x+1)(x-1)$, $x^3 - 1 = (x-1)(x^2 + x + 1)$]

Beh.: $(x-1) = (x^2-1, x^3-1)$

„$\supseteq$" $x^2-1 = (x+1)(x-1) \Rightarrow x^2-1 \in (x-1)$

$x^3-1 = (x^2+x+1)(x-1) \Rightarrow x^3-1 \in (x-1)$

Daraus folgt $(x^2-1, x^3-1) \subseteq (x-1)$.

„$\subseteq$" s.o. $\Rightarrow x-1$ ist gemeinsamer Teiler von x^2-1 und x^3-1. Darüber hinaus ist $x-1$ größter gem. Teiler dieser Elemente, denn ansonsten wäre der ggT ein echtes Vielfaches von $x-1$ (d.h. ein Vielfaches, aber nicht zu $x-1$ assoziiert) und zugleich ein Teiler von x^2-1. Damit wäre dann x^2-1 ein ggT der Elemente, und $\ldots$

ein Teiler von x^3-1. Wegen $x^2-1=(x-1)(x+1)$,
$x^3-1=(x^2+x+1)(x-1)$ wäre $x+1$ dann Teiler
von x^2+x+1 und -1 somit Nullstelle von x^2+x+1 ↯

also: $ggT(x^2-1, x^3-1) = x-1$ $(u=-x, v=1)$

Lemma von Bézout $\Rightarrow \exists u, v \in \mathbb{R}[x]$ mit
$x-1 = u\cdot(x^2-1) + v\cdot(x^3-1) \Rightarrow x-1 \in (x^2-1, x^3-1)$

zu (b) Sei $N: R \to \mathbb{N}_0$ die Normfunktion auf
$R = \mathbb{Z}[\sqrt{-13}]$ gegeben durch $N(a+b\sqrt{-13}) =$
a^2+13b^2 für alle $a, b \in \mathbb{N}_0$. Es ist $N(2)$
$= 4$ ein Quadrat der Primzahl 2, aber die Glei-
chung $a^2+13b^2 = 2$ ist mit $a, b \in \mathbb{Z}$ nicht
lösbar. (Es kommt wegen $13 > 2$ nur $b=0$ in Frage,

aber 2 ist kein Quadrat in $\mathbb{Z}$.)
Daraus folgt, dass 2 in R irreduzibel ist. (Übung: Zeigen Sie, dass 2 in R kein Primelement ist.)

$[2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})]$

Def: Sei R ein Ring und I ein Ideal in R. Faktorring von R modulo I $= (R/I, +, \cdot)$, wobei

$R/I = \{a+I \mid a \in R\}$ Menge der Nebenklassen

und die Verknüpfungen + und · auf

$x+1)$,
an Terlo
von x^2+x+1 |
$(u=-x, v=1)$
$x]$ mit
$1 \in (x^2-1, x^3-1)$.
tion auf
$+b\sqrt{-13}) =$
Es ist $N(2)$
2, aber die Glei-
$a, b \in \mathbb{Z}$ nicht
aus $b=0$ in Frage.

R/I gelten sind durch

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)\cdot(b+I) = ab+I$$

wichtigste Beispiele: die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$. (Hier ist $R = \mathbb{Z}$ und $I = (n)$.)

(Es ist $\mathbb{Z}/0\cdot\mathbb{Z} = \mathbb{Z}/(0) \cong \mathbb{Z}$,
$\mathbb{Z}/(-2)\mathbb{Z} = \mathbb{Z}/(-2) = \mathbb{Z}/2\mathbb{Z}$
wegen $(2) = (-2)$ in $\mathbb{Z}$.)

Erinnerung: Sei R ein Ring, I ein Ideal in R. Dann gelten die Äquivalenzen

(i) I Primideal $\Leftrightarrow$ R/I Int.-bereich (ii) I max. Ideal $\Leftrightarrow$ R/I Körper