__Def.__ Sei R ein Ring.

Ideal in R = Teilmenge $I \subseteq R$ mit den Eigenschaften (i) $0_R \in I$

(ii) $\forall a, b \in I : a + b \in I$

(iii) $\forall \underline{r \in R}\ \forall a \in I : ra \in I$

__Erinnerung:__ Sei R ein Ring.

(i) Sei $S \subseteq R$ eine beliebige. Dann bezeichnen wir das kleinste Ideal I von R mit $I \supseteq S$ mit der Notation (S) und nennen es das von S __erzeugte__ Ideal.

$\subseteq R$ mit

I

I

Dann be-

I von R

n (S) und

r Ideal.

(ii) Ist $n \in \mathbb{N}_0$, $S = \{a_1, \dots, a_n\} \subseteq R$, dann gilt $(S) = \{\sum_{j=1}^{n} r_j a_j \mid r_1, \dots, r_n \in R\}$.

(iii) Ist $n = 1$, also $(S) = (a_1) = \{r_1 a_1 \mid r_1 \in R\}$, dann spricht man von einem Hauptideal. Ein Integritätsbereich, in jedem jedes Ideal ein Hauptideal ist, wird Hauptidealring oder auch Hauptidealbereich genannt.

(iv) Jeder euklidische Ring ist ein Hauptidealring (also z.B. $\mathbb{Z}$, $\mathbb{Z}[i]$, Polynomringe über Körpern). Jeder Hauptidealring ist faktoriell.

Def. Se

(i) Man

$I \neq ($

mit a

gilt.

(ii) Man

wenn

Ideal J

$I = J$ od

Erinnerung:

also die U

Bsp.: Das H

…} $\subseteq R$,
…, $r_n \in R$}.
=
…zieht man
Integritäts-
ein Haupt-
…g oder
…t.
ist ein
…, $\mathbb{Z}[i]$
Jeder Haupt-

Def. Sei R ein Ring, I ein Ideal.

(i) Man nennt I ein <u>Primideal</u>, wenn $I \neq (1)$ gilt und für alle $a, b \in R$ mit $ab \in I$ jeweils $a \in I$ oder $b \in I$ gilt.

(ii) Man nennt I <u>maximales Ideal</u>, wenn $I \neq (1)$ gilt und für jedes Ideal J mit $I \subseteq J \subseteq (1)$ entweder $I = J$ oder $J = (1)$ gilt.

<u>Erinnerung:</u> (i) Jede maximale Ideal ist Primideal, aber die Umkehrung ist im Allg. falsch.

Bsp.: Das Hauptideal (x) in $\mathbb{Z}[x]$ ist ein

Primidea…
gilt auc…
Dagegen
diesem
(ii) Das
genau…
ein M…
(iii) Ein m…
genau
Def. Se…
nennt ma…
mit den b…

Primideal, aber kein maximales Ideal. Dasselbe gilt auch für das Hauptideal (2) in $\mathbb{Z}[x]$. Dagegen ist $(2, x)$ ein maximales Ideal in diesem Ring. (Übung)

(ii) Das Nullideal ist in einem Ring R genau dann ein Primideal, wenn R ein Integritätsbereich ist.

(iii) Ein maximales Ideal ist das Nullideal genau dann, wenn der Ring ein Körper ist.

<u>Def.</u> Sei R ein Ring und ein Ideal. Dann nennt man die Menge $R/I = \{a+I \mid a \in R\}$ mit den beiden Verknüpfungen $+$ und $\circ$ geg. durch

Dasselbe
in $\mathbb{Z}[x]$.
deal in

ing R
enn R

Nullideal
in Körper ist.
deal. Dann
$+I \mid a\in R\}$
$\cdot$ geg. durch

$(a+I)+(b+I)=(a+b)+I$ und
$(a+I)\cdot(b+I)=ab+I$ den Faktorring von R modulo I.

<u>wichtige Regel:</u> Für alle $a,b\in R$ gilt die Äquivalenz $a+I=b+I \iff b\in a+I \iff a\in b+I$.

wichtiges Beispiel für Faktorringe:
$R=\mathbb{Z}$, $I=(n)$ (mit $n\in\mathbb{N}$). Der Faktorring R/I ist dann der Restklassenring $\mathbb{Z}/n\mathbb{Z}$.

<u>Erinnerung:</u> Sei R ein Ring, $I\subseteq R$ ein Ideal.
(i) I ist Primideal $\iff$ R/I ist Integritätsber.
(ii) I ist max. Ideal $\iff$ R/I ist Körper

<u>Erin</u>
(i) D
gene
Prima
R d
(ii) D
max
M
<u>F24 T</u>
(a) Sei
Elemen
für ein

... und
... Faktor -

$b \in R$ ggT

$I \Leftrightarrow$

...ringe:

...) Der Faktor -

...ssenring $\mathbb{Z}/n\mathbb{Z}$

...g, $I \subseteq R$ ein Ideal

...I ist Integritätsbereich

.../I ist Körper

<u>Erinnerung:</u> Sei R ein Hauptidealring.

(i) Die maximalen Ideale in R sind genau die Ideale (p), wobei p die Primelemente (oder die irred. Elt.) von R durchläuft.

(ii) Die Primideale sind genau die maximalen Ideale zuzüglich des Nullideals (0_R).

<u>F24T1A3</u> Übung: F21T3A4

(a) Sei R ein Ring. Man nennt ein Element $a \in R$ <u>nilpotent</u>, wenn $a^n = 0_R$ für ein $n \in \mathbb{N}$ gilt. Sei nun I ein Primideal

$= 0_R \in I$

und

(1_R)

folgt $a | c$.

mit

$c \cdot (ra + sb)$

$\exists u \in R$

$sua =$

und $a \in R$ nilpotent. z.zg: $a \in I$

zeige durch vollständige Induktion über $n \in \mathbb{N}$: Ist $a \in R$ mit $a^n = 0_R$, dann folgt $a \in I$.

Ind.-Anf.: $n = 1$ Vor.: $a^1 = 0_R$

Da I ein Ideal ist, gilt $0_R \in I \Rightarrow a \in I$.

Ind-Schritt: Sei $n \in \mathbb{N}$, setze die Aussage für n voraus. Sei $a \in R$ mit $a^{n+1} = 0_R$.

$\overset{I \text{ Ideal}}{\Longrightarrow} a^{n+1} \in I \Rightarrow a \cdot a^n \in I \Rightarrow a \in I$ oder $a^n \in I$. 1. Fall: $a \in I$ Dann ist nichts mehr zu zeigen. 2. Fall: $a^n \in I$.

$$(a^n)^2 = a^{2n} = a^{n+1}\cdot a^{n-1} = 0_R\cdot a^{n-1} = 0_R \in I$$

$$\Rightarrow a^n \in I \Rightarrow a^{n+1} = a\cdot a^n \in I.$$

I Primideal

(c) Sei R ein Integritätsbereich und seien $a, b, c \in R$ mit $(a, b) = (1_R)$. Zeigen Sie: Gilt $a \mid (bc)$, dann folgt $a \mid c$.

Wegen $1_R \in (a, b)$ gibt es $r, s \in R$ mit

$$ra + s\cdot b = 1_R \Rightarrow c = c\cdot 1_R = c\cdot(ra + sb)$$
$$= cra + s\cdot(bc) \qquad a \mid (bc) \Rightarrow \exists u \in R$$

mit $bc = au \Rightarrow c = cra + sua =$

$$(cr + su)a \Rightarrow a \mid c.$$

Korrekturhinweis auf der nächsten Seite

Hier ist mir beim Induktionsschritt ein Fehler unterlaufen. Das Beweisziel war $a \in I$, nicht $a^{n+1} \in I$, und die Fallunterscheidung ist unnötig.

korrekte Ausführung des Induktionsschritts:

Sei $n \in \mathbb{N}$, und setze die Aussage für n voraus. Sei $a \in R$ mit $a^{n+1} = 0_R$. Zu zeigen ist $a \in I$. Es gilt

$$(a^2)^n = a^{2n} = a^{n+1} \cdot a^{n-1} = 0_R \cdot a^{n-1} = 0_R.$$

Die Induktionsvoraussetzung, angewendet auf a^2, liefert $a^2 \in I$. Aus $a \cdot a \in I$ folgt $a \in I$, weil I ein Primideal ist.

$)\cdot(x+(x^2 1))$

$[x]/(x^2)$

da ansonsten

$) \Rightarrow$

↯ da

)

gleich null

per

) genau dann

maximales Ideal

Hauptidealring

örper $\mathbb{F}_2$)

H2OT1A2

(a) Welche der folgenden Ringe sind Körper? $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_2[x]/(x^2)$, $\mathbb{F}_2[x]/(x^2+x+\bar{1})$

(i) In $\mathbb{Z}/4\mathbb{Z}$ gilt $\bar{2}\cdot\bar{2} = \bar{0}$, aber $\bar{2} \neq \bar{0}$ $\Rightarrow$ $\bar{2}$ ist Nullteiler $\neq \bar{0}$

$\Rightarrow$ $\mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsbereich und damit auch kein Körper.

(ii) In $\mathbb{F}_2 \times \mathbb{F}_2$ gilt $(\bar{1},\bar{0})\cdot(\bar{0},\bar{1}) = (\bar{0},\bar{0}) = 0_{\mathbb{F}_2\times\mathbb{F}_2}$, aber $(\bar{1},\bar{0}), (\bar{0},\bar{1}) \neq 0_{\mathbb{F}_2\times\mathbb{F}_2}$

$\Rightarrow$ Die Elemente sind Nullteiler ungleich null.

$\Rightarrow$ $\mathbb{F}_2 \times \mathbb{F}_2$ ist kein Körper

(a

$\Rightarrow$ a

I Reminde

(c) S

seien

Zeigen

Wegen

ra+

= cr

mit

(cr+s

dass
duzibel ist.
gleichbedeuten-
keine Null-
$= \bar{1} \neq \bar{0}$ und
es der Fall
Körper.
paarweise

gensatz zu den
ist, ist dieser
gebenen Ringe

(iii) In $\mathbb{F}_2[x]/(x^2)$ gilt $(x+(x^2))\cdot(x+(x^2))$

$$= x^2 + (x^2) \underset{\uparrow\, x^2 \in (x^2)}{=} (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$$

aber $x+(x^2) \neq 0_{\mathbb{F}_2[x]/(x^2)}$, da ansonsten

$x+(x^2) = (x^2) \Rightarrow x \in (x^2) \Rightarrow$

$\exists f \in \mathbb{F}_2[x]$ mit $x = f \cdot x^2$ ↯ da

$\mathrm{grad}(x) = 1 < 2 = \mathrm{grad}(x^2)$

also: $x+(x^2)$ ist Nullteiler ungleich null

$\Longrightarrow \mathbb{F}_2[x]/(x^2)$ ist kein Körper.

(iv) Lt. Vl. ist $\mathbb{F}_2[x]/(x^2+x+\bar{1})$ genau dann ein Körper, wenn $(x^2+x+\bar{1})$ ein maximales Ideal in $\mathbb{F}_2[x]$ ist. Da $\mathbb{F}_2[x]$ ein Hauptidealring ist (als Pol.-ring über dem Körper $\mathbb{F}_2$)

H2

(a)

sind

$\mathbb{F}_2($

(i) In

$\bar{2}+$

$\Rightarrow 2$

und d

(ii) In

$= ($

$\Rightarrow$ Die

$\Rightarrow \mathbb{F}_2$

e R, S
selbe
R → S ein
s. Da ϕ inst.
(S,+) ist, folgt
selbe Ordnung
Bekanntlich
ng der Char. n.

$\mathbb{F}_2\times\mathbb{F}_2 = (\bar{2},\bar{2}) =$
$\times\,\mathbb{F}_2) = 2$
$0_{\mathbb{F}_2[x]/(x^2)}$, da
$x]$ mit $f\cdot x^2 = \bar{1}$ ↯

ist, ist dies äquivalent dazu, dass $f = x^2+x+\bar{1}$ in $\mathbb{F}_2[x]$ irreduzibel ist. Wegen grad$(f) = 2$ ist das gleichbedeutend damit, dass f in $\mathbb{F}_2$ keine Nullstellen hat. Wegen $f(\bar{0}) = \bar{1} \neq \bar{0}$ und $f(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$ ist dies der Fall

$\Rightarrow \mathbb{F}_2[x]/(x^2+x+\bar{1})$ ist ein Körper.

(b) Zeigen Sie, dass die Ringe paarweise nicht isomorph sind.

Da $\mathbb{F}_2[x]/(x^2+x+\bar{1})$ im Gegensatz zu den anderen drei Ringen ein Körper ist, ist dieser zu keinem der drei angegebenen Ringe isomorph.

(iii) In
$= x^2$
aber x
$x + (x^2$
$\exists f \in$
grad $(x$
also: x
$\Rightarrow \mathbb{F}_2[$
(iv) Lt. V
ein Kö
in $\mathbb{F}_2[x$
ist (alg

Allgemein gilt: Sind zwei Ringe R, S isomorph, dann haben sie dieselbe Charakteristik (denn: Ist $\phi: R \to S$ ein Isom., dann muss $\phi(1_R) = 1_S$. Da ϕ insb. ein Isom. zwischen $(R,+)$ und $(S,+)$ ist, folgt daraus, dass 1_R in $(R,+)$ dieselbe Ordnung hat wie 1_S in $(S,+)$.) Bekanntlich ist $\mathbb{Z}/n\mathbb{Z}$ für jedes $n \in \mathbb{N}$ ein Ring der Char. n.

$\Rightarrow \operatorname{char}(\mathbb{Z}/4\mathbb{Z}) = 4$

$1_{\mathbb{F}_2 \times \mathbb{F}_2} = (\bar{1},\bar{1}) \neq (\bar{0},\bar{0})$, $2 \cdot 1_{\mathbb{F}_2 \times \mathbb{F}_2} = (\bar{2},\bar{2}) = (\bar{0},\bar{0}) = 0_{\mathbb{F}_2 \times \mathbb{F}_2} \Rightarrow \operatorname{char}(\mathbb{F}_2 \times \mathbb{F}_2) = 2$

$1_{\mathbb{F}_2[x]/(x^2)} = \bar{1} + (x^2) \neq (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$, da ansonsten $\bar{1} \in (x^2) \Rightarrow \exists f \in \mathbb{F}_2[x]$ mit $f \cdot x^2 = \bar{1}$ ↯

ist

$f = x$

Wege

tend

stell

$f(\bar{1})$

$\Rightarrow \mathbb{F}$

(b) Z

mehr

Da $\mathbb{F}$

andere

zu kenn

isomor

$$2 \cdot 1_{\mathbb{F}_2[x]/(x^2)} = \bar{2} + (x^2) = \bar{0} + (x^2) = 0_{\mathbb{F}_2[x]/(x^2)}$$

$$\Rightarrow \operatorname{char}(\mathbb{F}_2[x]/(x^2)) = 2$$

Also ist $\mathbb{Z}/4\mathbb{Z}$ weder zu $\mathbb{F}_2 \times \mathbb{F}_2$ noch zu $\mathbb{F}_2[x]/(x^2)$ isomorph.

Ang., es gilt $\mathbb{F}_2 \times \mathbb{F}_2 \cong \mathbb{F}_2[x]/(x^2)$. Sei $\phi : \mathbb{F}_2[x]/(x^2) \to \mathbb{F}_2 \times \mathbb{F}_2$ ein Ringisomorphismus und $(a, b) = \phi(x + (x^2))$ (mit $a, b \in \mathbb{F}_2$).

$x + (x^2) \neq 0_{\mathbb{F}_2[x]/(x^2)}$, ϕ injektiv $\Rightarrow (a, b) \neq (\bar{0}, \bar{0})$

andererseits: $(a^2, b^2) = (a, b)^2 = \phi(x + (x^2))^2 = \phi((x + (x^2))^2)$
$= \phi(x^2 + (x^2)) = \phi(0_{\mathbb{F}_2[x]/(x^2)}) = 0_{\mathbb{F}_2 \times \mathbb{F}_2} = (\bar{0}, \bar{0}) \Rightarrow$
$a^2 = b^2 = \bar{0} \overset{\mathbb{F}_2 \text{ Körper}}{\Longrightarrow} a = b = \bar{0} \Rightarrow (a, b) = (\bar{0}, \bar{0})$ $\lightning$ $\square$