Def. Sei R ein Ring und I ein Ideal von R.

(i) I ist ein Primideal $\Leftrightarrow$ $I \neq (1_R)$ und für alle $a, b \in R$ folgt aus $ab \in I$ jeweils $a \in I$ oder $b \in I$.

(ii) I ist ein maximales Ideal $\Leftrightarrow$ $I \neq (1_R)$ und für jedes Ideal J von R mit $I \subseteq J \subseteq (1_R)$ gilt jeweils $I = J$ oder $J = (1_R)$.

Erinnerung:

(i) I ist Primideal $\Leftrightarrow$ R/I ist Integritätsbereich

(ii) I ist ein maximales Ideal $\Leftrightarrow$ $I \neq (1_R)$

(iii) I ist maximales Ideal $\Leftrightarrow$ R/I ist Körper

Aus (i) und (iii) folgt, dass jedes maximale Ideal von R ein Primideal ist. (Die Umkehrung ist falsch. Das Nullideal (0) ist in $\mathbb{Z}$ zwar ein Primideal, aber kein maximales Ideal.)

F26T1A3 (Forts.) geg: Primzahl p

bereits gezeigt: Die Abbildung $\varphi: \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$, $h \mapsto \overline{h(0)} = h(0) + p\mathbb{Z}$ ist ein surjektiver Ringhomomorphismus mit $\ker(\varphi) = (p, x)$.

(c) Zeigen Sie, dass $I = (p, x)$ ein maximales Ideal in $\mathbb{Z}[x]$ ist.

... weil $\ker(\varphi)$ ein Ideal in $\mathbb{Z}[x]$ ist, folgt daraus $(0) \subseteq \ker(\varphi)$. „$\subseteq$" Sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ mit $k \in \mathbb{N}_0$ ...

Nach Teil (a) und (b) sind die Voraussetzungen des Homomorphiesatzes für Ringe für φ erfüllt. Dieser liefert einen Isom. $\mathbb{Z}[x]/I \cong \mathbb{Z}/p\mathbb{Z}$. Weil p eine Primzahl ist, ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Auf Grund des Isom. gilt dasselbe für den Faktorring $\mathbb{Z}[x]/I$. Aus der Körpereig. von $\mathbb{Z}[x]/I$ folgt, dass I in $\mathbb{Z}[x]$ ein maximales Ideal ist.

(d) Entscheiden Sie, ob (x) ein Primideal in $\mathbb{Z}[x]$ ist, und begründen Sie Ihre Entscheidung.

Beh.: $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ — Betrachte den Einsetzungs-

Homomorphismus $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, $h \mapsto h(0)$. Dieser ist surjektiv, denn für vorgeg. $a \in \mathbb{Z}$ gilt $\varphi(a) = a$.
Zeige noch: $\ker(\varphi) = (0)$ „$\supseteq$" Wegen $\varphi(0) = 0$ gilt $0 \in \ker(\varphi)$, und weil $\ker(\varphi)$ ein Ideal in $\mathbb{Z}[x]$ ist, folgt daraus $(0) \subseteq \ker(\varphi)$ „$\subseteq$" Sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ mit $k \in \mathbb{N}_0$, $a_0, \dots, a_n \in \mathbb{Z}$ und $f \in \ker(\varphi)$ $\Rightarrow \varphi(f) = 0 \Rightarrow$
$f(0) = 0 \Rightarrow a_0 = 0 \Rightarrow f = x \cdot \sum_{k=1}^{n} a_k x^{k-1} \Rightarrow f \in (x)$
Also kann der Hom.-satz für Ringe auf φ angewendet werden. Dieser liefert einen Isom. $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ ($\Rightarrow$ Beh.)
Weil $\mathbb{Z}$ ein Int.-Ber. ist, gilt dasselbe für $\mathbb{Z}[x]/(x)$
Daraus folgt, dass (x) in $\mathbb{Z}[x]$ ein Primideal ist. □

Def Sei R ein Ring und $p \in R$.

i) p ist irreduzibel in $R \Leftrightarrow$ Es gilt $p \neq 0_R$, $p \notin R^\times$ und für alle $a, b \in R$ folgt aus $p = ab$ jeweils $a \in R^\times$ oder $b \in R^\times$

ii) p ist prim (oder Primelement) in $R \Leftrightarrow$ Es gilt $p \neq 0_R$, $p \notin R^\times$, und für alle $a, b \in R$ folgt aus $p \mid (ab)$ jeweils $p \mid a$ oder $p \mid b$.

Ist R ein Integritätsbereich, dann ist jedes Primelement in R ein irreduzibles Element, aber die Umkehrung ist im Allg.

falsch.

Bsp.: i) Im Ring $R = \mathbb{Z}$ sind die Primelemente genau die Elemente der Form $\pm p$, wobei p die Primzahlen durchläuft, und dies sind zugleich die irreduziblen Elemente

(ii) Ist allgemein R ein Hauptidealring (z.B. ein Polynomring über einem Körper), dann sind die Primelemente genau die irred. Elemente. Die maximalen Ideale in R sind genau die Ideale der Form (p), wobei $p \in R$ die Primelemente durchläuft. Das einzige nicht-maximale Primideal in R ist das Nullideal (0_R).

iii) Sei $d \in \mathbb{N}$ quadratfrei (d.h. $p^2 \nmid d$ für alle Primzahlen p) und $d > 1$. Sei $R = \mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$ und $N : R \to \mathbb{N}_0$ die sog. Normfunktion gegeben durch $\alpha = a + b\sqrt{-d} \mapsto \alpha\bar{\alpha} = a^2 + db^2$. Es gilt:

(1) $\forall \alpha \in R : \alpha \in R^\times \iff N(\alpha) = 1$

(2) p Primzahl, $N(\alpha) = p \Rightarrow \alpha$ irreduzibel in R

(3) p Primzahl, $N(\alpha) = p^2$, es gibt keine $a, b \in \mathbb{Z}$ mit $a^2 + db^2 = p \Rightarrow \alpha$ irred. in R

Übungen dazu: F16T1A4, F17T1A1, F19T1A3

Bem.: Das Element 2 ist in $\mathbb{Z}[\sqrt{-3}]$ irreduzibel (wegen Kriterium (3), denn $N(2) = 4$ ist Primzahlquadrat, aber die Gleichung $a^2 + 3b^2 = 2$ ist mit $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$

weils $p \mid q$

Primelement
$\pm p$, wobei
dies sind
he
alring
n Körper).
n die irred.
R sind genau
$p \in R$ die
inzige nicht-
s Nullideal (0_R).

$a, b \in \mathbb{Z}$ nicht (lösbar). Andererseits ist 2 in $\mathbb{Z}[\sqrt{-3}]$ kein Primelement, denn: Wegen $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ ist 2 ein Teiler von $(1+\sqrt{-3})(1-\sqrt{-3})$. Es gilt (aber) $2 \nmid (1+\sqrt{-3})$ (sonst: $1+\sqrt{-3} = 2\gamma$ für ein $\gamma \in R \rightsquigarrow \gamma = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$ ↯, da $\frac{1}{2} + \frac{1}{2}\sqrt{-3} \notin R$), und ebenso $2 \nmid (1-\sqrt{-3})$.

Def. Ein <u>faktorieller Ring</u> ist ein Integritätsbereich, in dem jedes Element $x \in R$ mit $x \notin R^* \cup \{0_R\}$ als Produkt von Primelementen darstellbar ist (äquivalent: darstellbar als Prod. irred. Elemente, wobei die Darstellung eindeutig bis auf Reihenfolge und Einheiten ist).

Bem.
- Jeder Hauptidealring ist ein faktorieller Ring.
- Die Ringe $\mathbb{Z}[x]$ und $\mathbb{Q}[x,y]$ sind faktoriell, aber keine Hauptidealringe.

H24T1A3

Sei K ein Körper und $R \subseteq K[x]$ geg. durch

$$R = \left\{ \sum_{i=0}^{n} a_i x^i \in K[x] \mid a_1 = 0_K \right\}$$

(a) Zeigen Sie, dass R ein Teilring von $K[x]$ ist

zu überprüfen: (1) $1_K \in R$ (2) $\forall f, g \in R$:
$f - g \in R$ und $f \cdot g \in R$

zu (1) Es gilt $1_K = a_1 \cdot x + a_0$ mit $a_1 = 0_K$ und
$a_0 = 1_K \Rightarrow 1_K \in R$

zu (2) Seien $f, g \in R \Rightarrow \exists\, n \in \mathbb{N}_0$, $b_0, \dots, b_n$, $c_0, \dots, c_n \in R$ mit $f = \sum_{i=0}^{n} b_i x^i$, $g = \sum_{i=0}^{n} c_i x^i$ und $b_n = c_n = 0_K \Rightarrow f - g = \sum_{i=0}^{n} (b_i - c_i) x^i$ und $b_n - c_n = 0_K - 0_K = 0_K \Rightarrow f - g \in R$

$fg = \sum_{j=0}^{2n} u_j x^j$ mit $u_j = \sum_{k=0}^{j} b_{j-k} c_k$ für $0 \leq j \leq 2n$, insb. $u_1 = b_0 c_1 + b_1 c_0 = b_0 0_K + 0_K c_0 = 0_K \Rightarrow fg \in R$

(6) Entscheiden Sie, ob x^3 in R ein irreduzibles Element bzw. ein Primelement ist.

Beh x^3 ist in R irreduzibel

Es ist $x^3 \neq 0_K = 0_R$. Ang. $x^3 \in R^\times$ $\Rightarrow \exists f \in R$ mit $x^3 \cdot f = 1_K \Rightarrow 3 + \text{grad}(f) = \text{grad}(x^3) + \text{grad}(f) = \text{grad}(1_K) = 0$ ↯ da $\text{grad}(f) \geq 0$ $\rightarrow x^3$ ist keine Einheit

Ang. x^3 ist reduzibel in R. $\Rightarrow \exists f, g \in R \setminus R^\times$ mit $x^3 = f g$ $f, g, x^3 \in K[x]$. $K[x]$ ist faktoriell. x ist irreduzibel in $K[x] \Rightarrow f, g$ stimmen bzs auf eine Einheit in $K[x]$ (also bzs auf einen Faktor in $K^\times$) mit einer Potenz von x überein) $\Rightarrow \exists c, d \in K^\times$ und $m, n \in \mathbb{N}_0$ mit $f = c x^m$, $g = d x^n$, $m + n = \text{grad}(x^3) = 3$

Ang. $m=0$ oder $n=0$. $\Rightarrow f \in K^\times$ oder $g \in K^\times$.

$\Rightarrow f \in R^\times$ oder $g \in R^\times$ (denn jedes $c \in K^\times$ ist wg. $c^{-1} \in R$ und $c \cdot c^{-1} = 1_K$ auch Einheit in R.) $\lightning$ zur Vor.

Also ist nur $(m,n) \in \{(1,2), (2,1)\}$ möglich.

$\Rightarrow f = cx$ für ein $c \in K^\times$ oder $g = dx$ für ein $d \in K^\times$

$\lightning$ da $cx, dx \notin R$ ($\Rightarrow$ Beh.)

Beh. x^3 ist kein Primelement in R

$x^3 \cdot x^3 = x^6 = x^2 \cdot x^4 \Rightarrow x^3 \mid (x^2 \cdot x^4)$ Ang. x^3 ist

prim. Dann folgt $x^3 \mid x^2$ oder $x^3 \mid x^4$.

1. Fall: $x^3 \mid x^2 \Rightarrow \exists f \in R : x^2 = f x^3 \Rightarrow$

$2 = \text{grad}(x^2) = \text{grad}(f) + \text{grad}(x^3) =$
$\text{grad}(f) + 3 \quad \lightning$ da $\text{grad}(f) \geq 0$

2. Fall. $x^3 \mid x^4 \Rightarrow \exists f \in R$ mit $x^4 = f \cdot x^3$.

$K[x]$ Int. ber. $x = f \quad \lightning$ da $x \notin R$
$\Longrightarrow$
Kürzungsregel

(c) Ist R faktoriell? (Antwort mit Begr.)
Nein; denn in faktoriellen Ringen sind alle irreduziblen Elemente auch prim, und x^3 ist nach (6) ein Gegenbeispiel.

(d) Geben Sie ein $a \in R$ an, so dass (x^3, a) kein Hauptideal ist (mit Nachweis).
Es ist $a = x^2 \in R$. Beh. (x^3, x^2) ist kein Hauptideal

im Ring R

Ang., es gilt $(f) = (x^2, x^3)$ für ein $f \in R$.

$\Rightarrow x^2, x^3 \in (f) \Rightarrow \exists\, u, v \in R$ mit

$x^2 = u \cdot f$, $x^3 = v \cdot f$. Da $K[x]$ faktoriell ist, folgt aus $x^2 = u f$, dass $f = c x^m$ für ein $c \in K^\times$ und ein $m \in \{0, 1, 2\}$ gilt.

Ang. $m = 0 \Rightarrow f = c \Rightarrow c \in (x^2, x^3) \Rightarrow$

$\exists\, g, h \in K[x]$ mit $c = g \cdot x^2 + h \cdot x^3$ ↯

da $c \neq 0_K$ und $g \cdot x^2 + h \cdot x^3$ den Konstantenterm 0_K hat.

Ang. $m = 1 \Rightarrow f = c \cdot x$ ↯ da $c \cdot x \notin R$.

Als letzte Möglichkeit betrachten wir den Fall $m = 2$. Dann gilt $f = cx^2$, und durch Einsetzen erhalten wir $x^3 = vf = vcx^2$. Die Anwendung der Kürzungsregel liefert $x = vc$ und $v = c^{-1}x$. Aber v in ein Element von R, während $c^{-1}x$ nicht in R enthalten ist. Also erhalten wir auch in diesem Fall einen Widerspruch.