Ringtheorie

Def. Ring = Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt

(i) $(R, +)$ ist abelsche Gruppe
(Neutralelement 0_R = Nullelement)

(ii) $(R, \cdot)$ ist abelsches Monoid
(Neutralelement 1_R = Einselement)

(iii) Distributivgesetz: Für alle $a, b, c \in R$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bem: In einigen Quellen wird für einen Ring nur gefordert, dass $(R, \cdot)$ eine Halbgruppe ist

Unsere Definition entspricht dann einem „kommutativen Ring mit 1".

Def Ein Element a in einem Ring R heißt **Nullteiler**, wenn ein $b \in R \setminus \{0_R\}$ mit $a \cdot b = 0_R$ existiert. Ein Ring, in dem 0_R der einzige Nullteiler ist, heißt Integritätsbereich

Gegenbeispiele:

i) $R = \mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsbereich, weil $\bar{2}$ ein Nullteiler mit $\bar{2} \neq 0_R$ ist.

ii) $R = \mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$ ist kein Integritätsbereich, weil $0_R = \bar{0}$ kein Nullteiler ist.

iii) $R = \mathbb{Z} \times \mathbb{Z}$ ist kein Integritätsbereich, weil

$(1,0) \in R$ Nullteiler mit $(1,0) \neq (0,0) = 0_R$ ist. (Es gilt $(1,0)\cdot(0,1) = 0_R$.)

Def. Die invertierbaren Elemente im Monoid $(R, \cdot)$ heißen Einheiten. Diese Menge wird mit $R^\times$ bezeichnet und bildet eine Gruppe, die sog. Einheitengruppe des Rings

$\forall a \in R: a \in R^\times \iff \exists b \in R$ mit $ab = 1_R$

Ringe R mit der Eigenschaft $R^\times = R \setminus \{0_R\}$ heißen Körper. Jeder Körper ist ein Integritätsbereich.

(a,0) = 0_R
R.)
e im
weiten
kezeichnet
sog.

mit ab = 1_R
R^× = R \ {0_R}
ein Integri-

Beispiele für Einheitengruppen:

(i) $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, ebenso für $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_q$ (q Primzahlpotenz > 1)
(Achtung: $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$)

(ii) $\mathbb{Z}^\times = \{\pm 1\}$

(iii) $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1\}$
z.B. $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$
$(\mathbb{Z}/5\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

(iv) $(\mathbb{Z} \times \mathbb{Z})^\times = \{(\pm 1, \pm 1)\}$ (Allgemein gilt $(R \times S)^\times = R^\times \times S^\times$, für beliebige Ringe R, S.)

(v) Ist R ein Integritätsbereich, dann gilt für die Einheiten des Polynomrings $(R[x])^\times = R^\times$.

Beispiel
($\mathbb{Z}[x]$)
Für Nich
Zum Be
wegen ($\bar{1}$
= T.
F24TZA
1a) Existie
Einheite
endliche
[$z \in R^\times$ da
ein $n \in$
Ja, der Ring

Beispiele: $(\mathbb{R}[x])^\times = \mathbb{R}^\times = \mathbb{R}\setminus\{0\}$,

$(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$.

Für Nicht-Integritätsbereiche ist das falsch.
Zum Beispiel gilt $\bar{1}+\bar{2}x \in (\mathbb{Z}/4\mathbb{Z}[x])^\times$,
wegen $(\bar{1}+\bar{2}x)(\bar{1}+\bar{2}x) = \bar{1} + \bar{4}x + \bar{4}x^2$
$= \bar{1}$.

F24TZA4

1a) Existiert ein Ring mit unendlich vielen Einheiten, die alle in der Einheitengruppe endliche multiplikative Ordnung haben?
[$z \in R^\times$ hat endl. multiplikative Ordnung $\Leftrightarrow$ Es gibt ein $n \in \mathbb{N}$ mit $z^n = 1_R$.]
Ja, der Ring $\mathbb{C}$ hat diese Eigenschaft, denn

das falsch.

$+2(x])^x$,

$\overline{4}x + \overline{4}x^2$

ch vielen

ibengruppe

haben $\subseteq$

ng $\Leftrightarrow$ Es gibt

eiatt, denn

$\{ e^{2\pi i/n} \mid n \in \mathbb{N} \}$ ist eine unendliche Teilmenge von $\mathbb{C}^\times$, und $e^{2\pi i/n}$ ist jeweils ein Element der genauen multiplikativen Ordnung n, d.h. es gilt $(e^{2\pi i/n})^k \neq 1$ für $1 \leq k < n$ und $(e^{2\pi i/n})^n = e^{2\pi i} = 1$.

(b) Existiert ein Ring mit unendlich vielen Einheiten, die alle endliche additive Ordnung haben? (bedeutet: endliche Ordnung in der Gruppe $(R,+)$)

Ja. Sei p eine beliebige Primzahl und $\mathbb{F}_p(x)$ der rationale Funktionenkörper über $\mathbb{F}_p$, also der Quotientenkörper des Polynom-

Element
$\rangle = \{u^n \mid$
von $R^\times$,
dann nicht
□

ist ein Teiler
ein $c \in R$
$a \mid b$ und $b \mid a$,
ls assoziiert
, dann ist dies
$\in R^\times$ mit $b = \varepsilon a$

rings $\mathbb{F}_p[x]$. (Es gilt $\mathbb{F}_p(x) = \{\frac{f}{g} \mid f, g \in \mathbb{F}_p[x],\ g \neq \bar{0}\}$.) Weil $\mathbb{F}_p(x)$ ein Körper ist, gilt $\mathbb{F}_p(x)^\times = \mathbb{F}_p(x) \setminus \{\bar{0}\}$, z.B. sind x^n mit $n \in \mathbb{N}_0$ lauter verschiedene Einheiten. Für jedes Element $u \in \mathbb{F}_p(x)$ gilt aber $pu = \bar{0}$, d.h. u hat endliche Ordnung in $(\mathbb{F}_p(x), +)$.

(alternativ: Der algebraische Abschluss $\mathbb{F}_p^{alg} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$ hat ebenfalls die gewünschten Eigenschaften.)

(c) Gibt es einen Ring R mit endlich vielen Einheiten, wobei ein $u \in R^\times$ unendliche multiplikative Ordnung hat?

...reduzibel,
...t, und
... $p = ab$
... $R^\times$ folgt.
...rim (oder
... $R^\times \cup \{0_R\}$
...aus $p \mid ab$
...gt.
...h R ist jedes
... Element, aber
...alsch. Zum
... $+b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$
...ber nicht prim.

Nein. Denn ang., $u \in R^\times$ ist ein Element unendlicher Ordnung. Dann ist $\langle u \rangle = \{u^n \mid n \in \mathbb{Z}\}$ eine unendliche Teilmenge von $R^\times$, d.h. die Menge der Einheiten kann dann nicht endlich sein. □

Def. Sei R ein Ring.

(i) Seien $a, b \in R$. Man sagt, a ist ein Teiler von b (Notation $a \mid b$), wenn ein $c \in R$ mit $ac = b$ existiert. Gilt $a \mid b$ und $b \mid a$, dann bezeichnet man a und b als assoziiert. Wenn R ein Integritätsbereich, dann ist dies gleichbedeutend damit, dass ein $\varepsilon \in R^\times$ mit $b = \varepsilon a$ existiert.

...ein
...z.
...sch
...u ∈
...end
...(alt
...=
...sch
...(c) ...
...hei
...tue

ein Integri-
nde beiden
gelten:

$a \notin R^\times \cup \{0_R\}$.
lementen dar-

$a \notin R^\times \cup \{0_R\}$
ibles Elemente
rstellung ist im
d. bis auf Assozii
ren).

(ii) Ein Element $p \in R$ heißt <u>irreduzibel</u>, wenn $p \neq 0_R$ und $p \notin R^\times$ gilt, und wenn für alle $a, b \in R$ aus $p = ab$ jeweils $a \in R^\times$ oder $b \in R^\times$ folgt.

(iii) Ein Element $p \in R$ heißt <u>prim</u> (oder Primelement), wenn $p \notin R^\times \cup \{0_R\}$ gilt und für alle $a, b \in R$ aus $p \mid ab$ jeweils $p \mid a$ oder $p \mid b$ folgt.

<u>Bem.:</u> In einem Integritätsbereich R ist jedes Primelement auch ein irreduzibles Element, aber die Umkehrung ist im Allgemeinen falsch. Zum Beispiel ist in $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ die Zahl 2 zwar irreduzibel, aber nicht prim.

Neun. D
unendli
$n \in \mathbb{Z}$ f
d.h. die
endlich

<u>Def.</u> Se
(i) Seien
von 6 (
mit a
dann be
Wenn R
gleichbed
existiert

d damit
aktorieller
-3)].
re Körpern
dann
ein Beispiel
eine
genschaften:
R und ab ∈ R.

Def: Ein **faktorieller Ring** ist ein Integritätsbereich R, für den folgende beiden äquivalenten Bedingungen gelten:

(i) Jedes Element $a \in R$ mit $a \notin R^\times \cup \{0_R\}$ ist als Produkt von Primelementen darstellbar.

(ii) Jedes Element $a \in R$ mit $a \notin R^\times \cup \{0_R\}$ ist als Produkt irreduzibler Elemente darstellbar, und diese Darstellung ist im Wesentlichen eindeutig (d.h. bis auf Assoziiertheit und Reihenfolge der Faktoren).

(iii) Ein
wenn
wenn
jeweils
(iii) Ein E
Primele
gilt und
jeweils

Bem. J ein
Primelement
die Umkehr
Beispiel is
die Zahl 2

Beispiele:

(1) Jeder Hauptidealring (s.u.), und damit jeder euklidische Ring, ist ein faktorieller Ring, z.B. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, Polynomringe über Körpern.

(2) Ist R ein faktorieller Ring, dann auch der Polynomring $R[x]$. (Zum Beispiel ist $\mathbb{Z}[x]$ faktoriell.)

Def.: Ein Teilring eines Rings R ist eine Teilmenge $S \subseteq R$ mit folgenden Eigenschaften:

(1) $1_R \in S$ (2) $\forall a, b \in R: a-b \in R$ und $ab \in R$.

H24T1A3 Sei K ein Körper und

$$R = \left\{ \sum_{k=0}^{n} a_k x^k \mid n \in \mathbb{N},\ a_0, \dots, a_n \in R,\ a_1 = 0_K \right\}.$$

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

zu überprüfen: (1) $1_{K[x]} \in R$

(2) $\forall f, g \in R$: $f - g \in R$ und $fg \in R$

zu (1) Es gilt $1_{K[x]} = \sum_{k=0}^{n} a_k x^k$ mit $n = 1$ und $a_0 = 1_K$, $a_1 = 0_K$ $\Rightarrow 1_{K[x]} \in R$

zu (2) Seien $f, g \in R$ $\Rightarrow \exists m, n \in \mathbb{N}$ und $a_0, \dots, a_m, b_0, \dots, b_n$, so dass

$$f = \sum_{k=0}^{m} a_k x^k, \quad g = \sum_{l=0}^{n} b_l x^l \text{ und } a_1 = b_1 = 0_K$$

VOGEL ♡
(THE GOAT)

erfüllt ist. O.B.d.A. können wir $m = n$ annehmen.
(Gilt $m < n$, dann definiere $a_k = 0_K$ für $m < k \leq n$,
erhalte dadurch $f = \sum_{k=0}^{n} a_k x^k$. Verfahre entsprechend
mit g im Fall $m > n$.)

Es gilt $f - g = \sum_{k=0}^{n} c_k x^k$ mit $c_k = a_k - b_k$,
wobei $c_1 = a_1 - b_1 = 0_K - 0_K = 0_K$. $\Rightarrow f - g \in R$

Weiter gilt $f \cdot g = \sum_{l=0}^{2n} d_l x^l$ mit $d_l = \sum_{k=0}^{l} a_{l-k} b_k$.

Insb gilt $d_1 = a_1 b_0 + a_0 b_1 = 0_K b_0 + a_0 \cdot 0_K = 0_K$.
$\Rightarrow fg \in R$