Definition (9.1)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt Addition und Multiplikation, so dass die folgenden Bedingungen erfüllt sind:

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Ergänzungen zur Ringdefinition

- Das Neutralelement von $(R,+)$ heißt <u>Nullelement</u> des Rings (Bezeichnung 0_R).
- Das Neutralelement von $(R,\cdot)$ heißt <u>Einselement</u> des Rings (Bezeichnung 1_R).
- Das Inverse von $a \in R$ in $(R,+)$ heißt <u>Negatives</u> von a (Bezeichnung $-a$).
- Das Inverse eines invertierbaren Elements a im Monoid $(R,\cdot)$ heißt Kehrwert von a

(Bezeichnung a^{-1})

Die Rechenregeln für das Neutralelement und die Inversen invertierbarer Elemente in Monoiden übertragen sich auf $(R,+)$ und $(R,\cdot)$, d.h. es gilt z.B.

$-0_R = 0_R$, $-(a+b) = (-a)+(-b)$, $-(-a) = a$ $\forall a,b \in R$

$1_R^{-1} = 1_R$, $(ab)^{-1} = a^{-1}b^{-1}$, $(a^{-1})^{-1} = a$ falls a invertierbar in $(R,\cdot)$ ist

Hinzu kommen einige Rechenregeln, die Addition und Multiplikation betreffen, z.B. $0_R \cdot a = 0_R$, $(-a)(-b) = ab$ für alle $a,b \in R$.

Beispiele für Ringe:

- $\mathbb{Z}$ (mit der „gewöhnlichen" Addition und Multiplikation, ebenso $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}$)
- Für jeden Ring R gibt es einen Polynomring $R[x]$ über R.
- Sind $(R, +_R, \circ_R)$, $(S, +_S, \circ_S)$ Ringe, dann erhält man einen neuen Ring $(R \times S, +, \circ)$ mit Addition und Multiplikation definiert durch

$$(a, b) + (c, d) = (a +_R c,\ b +_S d)$$
$$(a, b) \cdot (c, d) = (a \cdot_R c,\ b \cdot_S d)$$

für alle $a, c \in R$, $b, d \in S$. Man nennt ihn das **direkte Produkt** der Ringe R und S.

Fra

Antw

$a =$

gilt

werden

__Frage__: Gibt es Ringe R mit $0_R = 1_R$?

__Antwort__: Ja, aber in solchen Ringen gilt $a = a \cdot 1_R = a \cdot 0_R = 0_R \ \forall a \in R$, d.h. es gilt dann $R = \{0_R\} = \{1_R\}$. Solche Ringe werden __Nullringe__ genannt.

Definition der Ringhomomorphismen

Definition (9.2)

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\phi : R \to S$ heißt Ringhomomorphismus von $(R, +_R, \cdot_R)$ nach $(S, +_S, \cdot_S)$, wenn die Gleichung $\phi(1_R) = 1_S$ gilt und außerdem

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{und} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

für alle $a, b \in R$ erfüllt ist.

Satz (9.3)

Für jeden Ring R existiert ein eindeutig bestimmter Ringhomomorphismus $\mathbb{Z} \to R$.

Anmerkung zur Definition der Ring-homomorphismen:

Sind R und S Ringe, dann gibt es im Allgemeinen Abbildungen, die zwar verträglich mit Addition und Multiplikation sind, aber nicht das Einselement 1_R auf 1_S abbilden.

<u>Bsp</u>: $R = \mathbb{Z}$, $S = \mathbb{Z} \times \mathbb{Z}$

Betrachte die Abb. $\phi : R \to S$, $a \mapsto (a, 0)$.

Dann gilt $\phi(a+b) = (a+b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$ und ebenso $\phi(ab) = \phi(a)\,\phi(b)$, aber $\phi(1_R) = \phi(1) = (1, 0) \neq (1, 1) = 1_S$.

Erinnerung: Notation für additive Potenzen in Gruppen

$n \cdot 1_R$ bezeichnet die n-te Potenz von 1_R in der Gruppe $(R,+)$

d.h. $n \cdot 1_R = \underbrace{1_R + 1_R + \dots + 1_R}_{n\text{-mal}}$, falls $n \in \mathbb{N}$, und

$(-n) \cdot 1_R = -(\underbrace{1_R + 1_R + \dots + 1_R}_{n\text{-mal}})$. In Ringen schreibt man

an Stelle von $n \cdot 1_R$ auch n_R, d.h. $2_R = 1_R + 1_R$, $3_R = 1_R + 1_R + 1_R$.

Beweis von Satz 9.3

Sei R ein Ring. z.zg.: Es gibt einen eindeutig bestimmten Ringhom $\phi: \mathbb{Z} \to R$.

<u>Existenz</u>: bekannt: $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, und 1 ist ein erzeugendes Element unendlicher Ordnung. Laut Gruppentheorie (§4) existiert somit für jedes $r \in R$ ein eindeutig bestimmter Gruppenhom. $(\mathbb{Z}, +) \to (R, +)$ mit $1 \mapsto r$. Insb. existiert also ein eindeutig bestimmter Gruppenhom. $\phi: (\mathbb{Z}, +) \to (R, +)$ mit $\phi(1) = 1_R$.

<u>Beh</u>.: Diese Abbildung ϕ ist auch ein Ringhom.

Für alle $n \in \mathbb{Z}$ gilt $\phi(n) = \phi(n \cdot 1) = n\,\phi(1) =$ ↑ additive Potenz
$n \cdot 1_R = n_R$.

<u>Beh.</u> $\forall n \in \mathbb{N}_0 \ \forall m \in \mathbb{Z}: \phi(mn) = \phi(m)\,\phi(n)$

Beweis durch vollst. Induktion über n.

Ind-Anf.: Sei $m \in \mathbb{Z}$. $\phi(m \cdot 0) = \phi(0) = 0_R = m_R \cdot 0_R = \phi(m)\phi(0)$

Ind-schritt: Sei $n \in \mathbb{N}_0$, setze $\phi(mn) = \phi(m)\phi(n)$ $\forall m \in \mathbb{Z}$ voraus. Sei $m \in \mathbb{Z}$. Dann gilt $\phi(m(n+1)) = \phi(mn + m) =$
$\phi(mn) + \phi(m) \underset{\uparrow \text{Ind-V.}}{=} \phi(m) \cdot \phi(n) + \phi(m) = m_R\, n_R + m_R =$
$m_R\,(n_R + 1_R) = m_R\,(n+1)_R = \phi(m) \cdot \phi(n+1)$ ($\Rightarrow$ Beh.)

Für bel. $m \in \mathbb{Z}$, $n \in \mathbb{N}$ gilt außerdem: $\phi(m \cdot (-n)) = \phi(-mn)$
$= -\phi(mn) \overset{\text{s.o.}}{=} -\phi(m)\,\phi(n) = \phi(m)\,(-\phi(n)) = \phi(m)\,\phi(-n)$

Also ist $\phi(mn) = \phi(m)\phi(n)$ für alle $m, n \in \mathbb{Z}$ erfüllt.

Die Eindeutigkeit ist offensichtlich, da bereits ein Gruppenhom. $(\mathbb{Z}, +) \to (R, +)$, der 1 auf 1_R abbildet, eindeutig bestimmt ist (siehe oben).

$\square$

Einheiten und Nullteiler

Definition (9.4)

Sei R ein Ring.

(i) Ein Element $a \in R$ heißt Einheit, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von R bezeichnen wir mit $R^\times$.

(ii) Man nennt es Nullteiler, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten eines Rings R bilden eine Gruppe $R^\times$, die sogenannte Einheitengruppe.

Integritätsbereiche und Körper

Definition (9.5)

Ein Ring R mit 0_R als einzigem Nullteiler heißt Integritätsbereich. Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein Körper.

Eigenschaften von Nullteilern und Einheiten

Lemma (9.6)

(i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.

(ii) Jeder Körper ist ein Integritätsbereich.

(iii) In jedem Integritätsbereich R gilt die Kürzungsregel: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

d

or -

smus.

$(L,+)$

ses Hom.

egt im

$= \phi(a\cdot a^{-1})$

L Körper $\square$

Beweis von Lemma 9.6

Sei R ein Ring.

zu (i) Angenommen, $a \in R$ ist Einheit und Nullteiler

a Nullteiler $\Rightarrow \exists\, b \in R \setminus \{0_R\}$ mit $b \cdot a = 0_R$

a Einheit $\Rightarrow \exists\, c \in R$ mit $a \cdot c = 1_R$

$\Rightarrow b = b \cdot 1_R = b \cdot a \cdot c = 0_R \cdot c = 0_R$ ↯

zu (ii) Voraussetzung: R ist Körper,

d.h. $R^\times = R \setminus \{0_R\}$ z.zg. 0_R ist der einzige Nullteiler von R. $1_R \in R^\times$ (da $1_R \cdot 1_R = 1_R$)

$\Rightarrow 1_R \neq 0_R$, außerdem $0_R \cdot 1_R = 0_R$

Also ist 0_R ein Nullteiler.

Ang. $a \in R$ mit $a \neq 0_R$ ist ebenfalls Nullteiler. $\Rightarrow a \in R \setminus \{0_R\} \Rightarrow a \in R^\times$

↯ da nach (i) kein Element Einheit und Nullteiler ist

zu (iii) Seien $a, b, c \in R$ mit $c \neq 0_R$ und $ac = bc$. $\Rightarrow ac - bc = 0_R \Rightarrow$

$(a-b)c = 0_R \xrightarrow[\text{bereich},\ c \neq 0_R]{R \text{ Integritäts-}} a - b = 0_R$

$\Rightarrow a = b$. $\square$

D

b

d

ist

Die Injektivität der Körperhomomorphismen

Proposition (9.7)

Ein Körperhomomorphismus $\phi : K \to L$ ist stets injektiv.

<u>Bem</u>: Sind K und L Körper, dann wird ein Ringhom. $K \to L$ auch <u>Körperhomomorphismus</u> genannt

Beweis von Proposition 9.7:

Sei $\phi: K \to L$ ein Körperhomomorphismus.

z.zg.: ϕ ist injektiv

Da ϕ insb. ein Gruppenhom. $(K,+) \to (L,+)$ ist, genügt es z.zg., dass der Kern dieses Hom. in $\{0_K\}$ enthalten ist. Ang. $a \in K$ liegt im Kern, aber $a \neq 0_K$. $\Rightarrow 1_L = \phi(1_K) = \phi(a \cdot a^{-1})$
$= \phi(a) \cdot \phi(a^{-1}) = 0_L \cdot \phi(a^{-1}) = 0_L$ ↯ da L Körper $\square$

Die Charakteristik eines Rings

Definition (9.8)

Sei R ein Ring. Die Charakteristik eines Rings R ist definiert durch

$$\mathrm{char}(R) \quad = \quad \begin{cases} n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1_R = 0_R \text{ ist,} \\ 0 & \text{falls } n \cdot 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \text{ gilt.} \end{cases}$$

Proposition (9.9)

Sei R ein Integritätsbereich. Dann ist die Charakteristik $\mathrm{char}(R)$ entweder gleich Null oder eine Primzahl.

Beweis von Proposition 9.9

Sei R ein Integritätsbereich, $n = \mathrm{char}(R)$.

Ang. $n \neq 0$ und n ist auch keine Primzahl

1. Fall: $n = 1$ Dann gilt $1_R = 1 \cdot 1_R = 0_R$. $\Rightarrow$

$R = \{0_R\}$, d.h. R ist Nullring $\Rightarrow$ R ist kein Integritätsb. $\lightning$

2. Fall. Es gibt $n = r \cdot s$ mit $1 < r, s < n$, $r, s \in \mathbb{N}$.

Nach Def der Charakteristik gilt dann $r_R = r \cdot 1_R \neq 0_R$ wegen $r < n$, ebenso $s_R \neq 0_R$, aber $r_R \cdot s_R \underset{\text{Homomorphismus-Eigenschaft von } \phi:\, \mathbb{Z} \to R,\ m \mapsto m_R}{=} (rs)_R = n_R = n \cdot 1_R = 0_R$ $\Rightarrow$ r_R, s_R sind Nullteiler ungleich 0_R im Ring R. $\lightning$ da R Integritätsbereich

$\square$