Wichtige Sätze und Definitionen zu
§3: Gruppen, Ringe und Körper
aus der Vorlesung:

LV-NR	150 239
Veranstaltung	Diskrete Mathematik II, 4.0 std
Dozent	Holtkamp, R.

3.1

a) $(A, \circ)$ *sei Monoid mit neutralem Element* e*. Dann heißt ein Element* $a \in A$ **invertierbar** *(in* A*) falls ein Element* $a' \in A$ *existiert mit* $a \circ a' = e$ *und* $a' \circ a = e$.
Bezeichnung: $(-a)$ *falls* $\circ = +$ *bzw.* a^{-1} *falls* $\circ = \cdot$, $A^* := \{a \in A : a \text{ invertierbar}\}$

b) Ein Monoid, in dem jedes Element invertierbar ist, heißt **Gruppe**. $(A^* = A)$

c) $(A, +)$ *heißt* **abelsche Gruppe** $\iff$ $(A, +)$ *ist Gruppe (d.h.:* $\forall\, a \in A\ \exists\ (-a) \in A : (-a) + a = 0$*) und* $+$ *ist kommutativ.*

Man schreibt auch $a - b$ *statt* $a + (-b)$.

Beispiel
$A = \{0, 1, 2, 3\}$ *als abelsche Gruppe*

3.2

a) Ist R *zusammen mit* $+$ *eine abelsche Gruppe,* $\cdot$ *eine assoziative Verküpfung auf* R*, so heißt* R *(mit* $+$ *und* $\cdot$*)* **Ring** $\iff$ *es gilt Distributivität, d.h.* $(a + b) \cdot c = a \cdot c + b \cdot c$ *und* $a \cdot (b + c) = a \cdot b + a \cdot c$

b) Ist R *bzgl.* $\cdot$ *ein Monoid mit neutralem Element* 1_R*, so heißt der Ring* $(R, +, \cdot)$ **unitärer Ring** *oder* **Ring mit Eins** 1_R*. Unter* R^* *versteht man die bzgl.* $\cdot$ *invertierbaren Elemente im Ring mit Eins.*

c) Unter einem kommutativen Ring versteht man einen Ring für den $\cdot$ *kommutativ ist*

d) R *heißt nullteilerfrei* $\iff$ $\forall\ a, b \in R$ *mit* $a \neq 0, b \neq 0$ *ist* $a \cdot b \neq 0$

Beispiel
4-elementiger kommutativer Ring mit Eins, nicht nullteilerfrei.

Satz 1 (Ring $\mathbb{Z}$ der ganzrationalen Zahlen)
Es gibt einen Ring $\mathbb{Z}$ mit Eins $1_{\mathbb{Z}}$ und folgenden Eigenschaften:

i) $(\mathbb{N}_0, +)$ ist Untermonoid von $(\mathbb{Z}, +)$

ii) $(\mathbb{N}, \cdot)$ ist Untermonoid von $(\mathbb{Z}, \cdot)$

iii) $\mathbb{N}_0 \cup (-\mathbb{N}_0) = \mathbb{Z}$ und $\mathbb{N}_0 \cap (-\mathbb{N}_0) = 0_{\mathbb{Z}}$ (wobei $-\mathbb{N}_0 := \{-n : n \in \mathbb{N}_0\}$)

Weiter gilt: $\mathbb{Z}$ ist kommutativ und nullteilerfrei.
$\mathbb{Z}^* = \{+1, -1\}$

3.3
$R_1, R_2, \ldots, R_n$ *seien Ringe. Sei* $R = R_1 \times \cdots \times R_n$*. Man versieht* R *mit den Verküpfungen*

$$a + b := (a_1 +_{R_1} b_1, \ldots, a_n +_{R_n} b_n)$$
$$a \cdot b := (a_1 \cdot_{R_1} b_1, \ldots, a_n \cdot_{R_n} b_n)$$

und nennt R **direktes Produkt** *der Ringe* $R_1, \ldots, R_n$.

3.4
Für $a, b \in \mathbb{Z}$ ist

$$a \leq_{\mathbb{Z}} b \iff \exists\ k \in \mathbb{N}_0 \text{ mit } a + k = b$$

und

$$b \geq_{\mathbb{Z}} a \iff a \leq_{\mathbb{Z}} b$$

Satz 2 (Eigenschaften $\leq_{\mathbb{Z}}$)
Die Relation $\leq_{\mathbb{Z}}$ ist eine totale Ordnungsrelation auf $\mathbb{Z}$ mit

$$\begin{aligned}(a+c) &\leq_{\mathbb{Z}} (b+c) \quad \forall\ a,b,c \in \mathbb{Z}\\ (a \cdot c) &\leq_{\mathbb{Z}} (b \cdot c) \quad \forall\ a,b,c \in \mathbb{Z} \text{ mit } c \geq 0\\ (-b) &\leq_{Z} (-a) \quad \text{falls } a \leq_{\mathbb{Z}} b\end{aligned}$$

3.5

a) R, R' seien Ringe, $\varphi : R \to R'$ Abbildung. φ heißt **Ringhomomorphismus** $\iff \forall\ a, b \in R$:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

b) $\mathrm{Kern}(\varphi) := \{a \in R : \varphi(a) = 0\}$ *heißt* **Kern von** φ

c) Sei $n \in \mathbb{N}$, $n\mathbb{Z} := \{n \cdot a | a \in \mathbb{Z}\}$. Sei $A \subseteq \mathbb{Z} \times \mathbb{Z}$ Relation gegeben durch $\{(a,b) \in \mathbb{Z} \times \mathbb{Z} | a - b \in n\mathbb{Z}\}$. Dann wird A auch mit $\equiv$ bezeichnet, genauer $a \equiv b \mod n$ statt aAb.

d) φ heißt **unitärer Ringhomomorphismus** $\iff$ *φ ist Ringhomomorphismus und $\varphi(1_R) = 1_{R'}$.*

Beispiel
Nullhomomorphismus ist nicht unitär.

Satz 3 (Restklassenringe $\mathbb{Z}/n\mathbb{Z}$)
Für alle $n \in \mathbb{N}_0$ gibt es einen untitären Ring $\mathbb{Z}/n\mathbb{Z}$ mit folgender Eigenschaft:
Es gibt einen surjektiven Ringhomomorphismus π_n mit $\mathrm{Kern}(\pi_n) = n\mathbb{Z}$.
Weiter gilt:

$$\begin{aligned}\forall\ n \neq 0 :\ \#\mathbb{Z}/n\mathbb{Z} &= n\\ \mathbb{Z}/n\mathbb{Z} &= \{\pi_n(a) : 0 \leq a < n\}\end{aligned}$$

und

$$a \equiv b \mod n \iff \pi_n(a) = \pi_n(b)$$

Beispiel
„Quersummenregel“

3.6
K sei kommutativer Ring mit Eins $1_K \neq 0_K$. Dann heißt K **Körper** $\iff K^* = K - \{0\}$

Satz 4 (Körper $\mathbb{Z}/p\mathbb{Z}$)
$\mathbb{Z}/n\mathbb{Z}$ ist Körper $\iff$ n ist Primzahl

Beispiel
Jeder Körper ist nullteilerfrei.

3.7
Es seien $a, n \in \mathbb{N}$, $a \leq n$. Man nennt

$$\varphi(n) := \#\{1 \leq a \leq n : \mathrm{ggT}(a, n) = 1\}$$

die **Eulersche φ-Funktion**.

Beispiel
$\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$

Satz 5 (Fundamentalsatz der Arithmetik)
Jede Zahl $n \in \mathbb{N}$ lässt sich eindeutig als Produkt von Primzahlen darstellen:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \dot{p}_k^{e_k}$$

wobei $p_1 < p_2 < \ldots < p_k$ prim und $e_i \in \mathbb{N}_{\geq 1}$ (Vielfachheit von p_i in n).

Übung 1
$\mathrm{ggT}(a, b)$, $\mathrm{kgV}(a, b)$

Erweiteter Euklidischer Algorithmus
Setze $r_0 = a$, $r_1 = b$, oBdA $r_0 > r_1 > 0$.
Division mit Rest ergibt:

$$\begin{aligned} r_0 &= a_0 r_1 + r_2 \\ r_1 &= a_1 r_2 + r_3 \\ &\vdots \\ r_{j-1} &= a_{j-1} r_j + r_{j+1} \\ r_j &= a_j r_{j+1} + 0 \end{aligned}$$

liefert

$$ggT(a, b) = d = r_{j+1}$$

$d = r_{j+1}$ lässt sich durch r_0, r_1 ausdrücken

$$d = a' r_0 + b' r_1 \quad a', b' \in \mathbb{Z}$$

wegen

$$\begin{aligned} r_{j+1} &= r_{j-1} - a_{j-1} r_j \\ &= r_{j-1} - a_{j-1}(r_{j-2} - a_{j-2} r_{j-1}) \\ &= usw \end{aligned}$$

liefert (a', b') mit

$$d = a'a + b'b$$

Beispiel
Erweiterter euklidischer Algorithmus mit

$$(a, b) = (198, 34)$$

Satz 6 (Chinesischer Restsatz, ringtheoretisch)
Wenn $m_1, \ldots, m_s \in \mathbb{N}$ mit $\text{ggT}(m_i, m_j) = 1 \; \forall \; i \neq j$, $m := m_1 \cdot \ldots \cdot m_s$ und für $1 \leq i \leq s$ die Abbildungen φ_i durch

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m_i\mathbb{Z} \\ a \bmod m_1 \cdot \ldots \cdot m_s &\longmapsto a \bmod m_i \end{aligned}$$

gegeben sind, so ist

$$\begin{aligned} \varphi \; : \; \mathbb{Z}/m\mathbb{Z} &\xrightarrow{\cong} \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_s\mathbb{Z} \\ x \bmod m &\longmapsto (\varphi_1(x), \ldots, \varphi_s(x)) \end{aligned}$$

ein Isomorphismus von Ringen.
Sind $d_1 \in \mathbb{Z}/m_1\mathbb{Z}, \ldots, d_s \in \mathbb{Z}/m_s\mathbb{Z}$ so existiert insbesondere genau ein $x \in \mathbb{Z}/m\mathbb{Z}$ mit

$$\varphi_i(x) = d_i \qquad \forall \; i = 1, \ldots, s$$

Weiter gilt:

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/m_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/m_s\mathbb{Z})^*$$

Beispiel
$s = 2$, $(m_1, m_2) = (99, 17)$

Satz 7 (Brüche)
Sei R kommutativer Ring mit Eins 1_R, $S \subseteq R$, und bezeichne $\bar{S} = \{1_R\} \cup \{s_1 \cdot \ldots \cdot s_r \mid r \geq 1, \; s_i \in S\}$ das von S erzeugte Untermonoid $(\mathbb{R}, \cdot)$. Dann wird eine Äquivalenzrelation $\sim$ auf $\mathbb{R} \times \bar{S}$ definiert durch

$$(a, s) \sim (a', s') \; :\Longleftrightarrow \; \text{es gibt } t \in \bar{S}, \text{ so dass } t \cdot (a \cdot s' - a' \cdot s) = 0$$

Bezeichnet man mit $\frac{a}{s}$ die Äquivalenzklasse von (a, s) bzgl $\sim$ und mit $S^{-1}R$ die Menge aller Äquivalenzklassen, so gilt:

$$S^{-1}R \text{ ist Ring mit } \tfrac{a}{s} + \tfrac{a'}{s'} = \tfrac{a \cdot s' + a' \cdot s}{s \cdot s'}, \; \tfrac{a}{s} \cdot \tfrac{a'}{s'} = \tfrac{a \cdot a'}{s \cdot s'} \text{ und mit Eins } \tfrac{1_R}{1_R}.$$

Des Weiteren gilt:

$$\text{Die Abbildung } j_s : R \to S^{-1}R, \; a \mapsto \tfrac{a}{1_R} \text{ ist ein Ringhomomorphismus und es gilt:}$$

$$a \in \text{Kern}(j_s) \Longleftrightarrow \text{ es gibt } t \in \bar{S} \text{ mit } a \cdot t = 0.$$

Beispiel
Sei R nullteilerfrei, $S = R - \{0\}$. Dann ist $S^{-1}R$ Körper und j_s ist injektiv. Speziell ist $(\mathbb{Z} - \{0\})^{-1}\mathbb{Z} = \mathbb{Q}$.

3.8
Der Ring $S^{-1}R$ heißt **Ring der Brüche** *mit Nennern aus S. Ist R nullteilerfrei, so heißt der Körper* $\text{Quot}(R) := (R - \{0\})^{-1} R$ *auch* **Quotientenkörper von R**.

Satz 8 (Anordnung von $\mathbb{Q}$)
Sei $P = \left\{x \in \mathbb{Q} \mid x = \frac{a}{s} \text{ mit } a \in \mathbb{N}_0,\ s \in \mathbb{N}\right\}$. Durch $x \leq y :\Longleftrightarrow y - x \in P$ wird eine totale Ordnungsrelation $\leq$ auf $\mathbb{Q}$ gegeben. Es gilt für alle $x, y, z \in \mathbb{Q}$:

a) Ist $x \leq y$, so ist $x + z \leq y + z$.

b) Ist $z > 0$, so ist $x \cdot z \leq y \cdot z$.

c) Ist $x \leq y$ so ist $(-y) \leq (-x)$.

Satz 9 (Charakterisierung des Körpers $\mathbb{R}$ der rellen Zahlen)
Es gibt genau einen Körper $\mathbb{R}$ mit Anordnung $\leq$ und den folgenden Eigenschaften:

a) $\mathbb{Q} \subseteq \mathbb{R}$ (Teilkörper)

b) Jede monoton steigende beschränkte Folge $(a_n)_{n\geq 0}$ in $\mathbb{R}$ hat einen Grenzwert in $\mathbb{R}$.

c) Zu jedem $w \in \mathbb{R}$ und jedem $n \in \mathbb{N}$ existiert ein $x_n \in \mathbb{Q}$ mit $0 < w - x_n < \frac{1}{n}$ (Approximationseigenschaft).

Beispiele
$\lim_{n\to\infty} \left(\sum_{k=0}^{n} \frac{1}{k!}\right) \to e^1$ *und* $\sqrt[3]{\frac{5}{19}}$ *ist irrational.*