$(R,+,\circ)$	(assoziativer) Ring	*(associative) ring*
$(R,+)$	kommutative Gruppe	(additiv)
$0 \in R$	Nullelement	(neutral bzgl. $+$)
$(R \setminus \{0\}, \circ)$	Halbgruppe	Nullring $\{0\}$
$r \circ (a+b) = r \circ a + r \circ b$	(links-)distributiv	
$(a+b) \circ r = a \circ r + b \circ r$	(rechts-)distributiv	
es gilt: $0 \circ r = r \circ 0 = 0$		$(\forall r)$
$r \circ s = 0 \;\Rightarrow\; r = 0 \vee s = 0$	nullteilerfrei	
$(\forall r)\ r \circ 1 = 1 \circ r = r$	Ring mit Einselement	
$(\exists r')\ r \circ r' = r' \circ r = 1$	r (*und* r') Einheit	$(r' := r^{-1})$

R Integritätsbereich $:\Leftrightarrow$ R kommutativer nullteilerfreier Ring

R Schiefkörper $:\Leftrightarrow$ *skew field*

$(R \setminus \{0\}, \circ)$ ist *(nichtkommutative)* Gruppe

R Körper $:\Leftrightarrow$ $(R \setminus \{0\}, \circ)$ ist abelsche Gruppe *field*

($\Rightarrow$ Einselement, nur Einheiten)

Charakteristik $\operatorname{char} F$ *((Schief-)Körper F)*

$\operatorname{char} F := \operatorname{ord} 1$ falls $< \infty$

$\operatorname{char} F := 0$ falls $n \cdot 1 = 0 \;\Rightarrow\; n = 0$

Es gilt: $\operatorname{char} F$ ist prim

$(n \in \mathbb{Z})$ $0 \cdot r := 0,\ n \cdot r := (n-1) \cdot r + r$ *(Potenz, abelsch)*

$\operatorname{ord} r = \min\{n > 0 \mid n \cdot r = 0\}$ Ordnung in $(R,+)$

$(\forall r)\ \operatorname{ord} r = \operatorname{ord} 1$ (Ring mit 1)

Restklassenring $(\mathbb{Z}_m, +, \cdot)$ *(Nullteiler r mit $(r,m) \neq 1$)*

Restklassenkörper $(\mathbb{Z}_p, +, \cdot)$ *(p prim)*

F endlicher (Schief-)Körper (Galois-Feld)

$\operatorname{char} F = p$ und $|F| = p^s$ *(p prim)*

ist Vektorraum $(F,+) \cong C_p^s \cong (\mathbb{Z}_p)^s$ *(direktes Produkt)*

und $F \setminus \{0\} = \langle x \rangle$ zyklisch *(also kommutativ)*

Jeder Integritätsbereich (mit Eins) kann *(auf genau eine Art)*
zu einem (kleinsten) Körper
(Quotientenkörper) erweitert werden.

R Integritätsbereich (mit 1) *(notwendig: nullteilerfrei!)*

(F Körper) $R \subset F \Rightarrow Q = \langle R \rangle$

$Q = \bigcap \{G \mid R \subset G \subset F\}$ *(G Unterkörper)*

Unterkörper Q von R in F erzeugt

Konstruktion von Q *(allgemein: nicht Teil eines Körpers!)*

Motivation: $(r,s) \leftrightarrow sx = r \ (s \neq 0)$ *(eindeutige) Lösung*

($s(x - x') = r - r$) $sx = 0 \ (s \neq 0) \Rightarrow x = 0$ $\Leftrightarrow$ *nullteilerfrei*

$sx = r$ und $(ts)x = (tr)$ *gleiche Lösung*

$R \times (R \setminus \{0\})$ $(r,s) + (r',s') := (rs' + r's, ss')$ *(„Brüche“!)*

$(r,s)(r',s') := (rr', ss')$ *(„fast“ Ring)*

Kongruenzrelation auf $R \times (R \setminus \{0\})$ *($N = \{(0,r) \mid r \in R\}$)*

$(r,s) \equiv (r',s') \ :\Leftrightarrow \ rs' = r's$ $(s, s' \neq 0)$

Quotientenkörper $Q := R \times (R \setminus \{0\})/\equiv$ *($R \times (R \setminus \{0\})/N$)*

(Einbettung von R) *(Isomorphismus $R \to \iota(R)$)*

$$\begin{array}{rccc} \iota & : & R & \to & Q \\ & & r & \mapsto & (r,1) \end{array}$$

(Charakterisierung)

Jede Einbettung $\varphi : R \to F$ *(φ injektiv, F Körper)*

kann zu einer Einbettung $\overline{\varphi} : Q \to F$ *(eindeutig)*

erweitert werden: $\overline{\varphi} \circ \iota / R = \varphi, \ \overline{\varphi}(Q) = \langle R \rangle$

Beispiele: $\mathbb{Z} \to \mathbb{Q}$ rationale Zahlen

($a \in \mathbb{N}$) $\mathbb{Z}(\sqrt{a}) \to \mathbb{Q}(\sqrt{a})$ *(quadratische Zahlkörper)*

speziell: $\mathbb{Z}(\sqrt{-1}) \subset \mathbb{Q}(\sqrt{-1}) \subset \mathbb{C}$

Polynomfunktionen $\to$ rationale Funktionen

Unterring (eines Rings $(R,+,\circ)$) *subring*

$H \subset R$ ist Unterring von R $(H < R)$

$:\Leftrightarrow$ $(H,+,\circ)$ ist Ring

$\Leftrightarrow H - H \subset H$ und $H \circ H \subset H$

(Links-)Ideal $H :\Leftrightarrow H - H \subset H,\ R \circ H \subset H$ *ideal*

(R kommutativ, mit 1)

Einheitengruppe $R^* := \{e \in R \mid (\exists e')\ e'e = 1\}$ *(invertierbar)*

$r \in R^* \ \Leftrightarrow\ R = rR\ (= \langle r \rangle)$

Klasseneinteilung $r \sim s :\Leftrightarrow\ s \in rR^*$ assoziiert

Hauptideal (monogen) $I = aR = \langle a \rangle$ *(von a erzeugt)*

$(a \sim b \ \Leftrightarrow\ a/b \wedge b/a)$ $a/b \ \Leftrightarrow\ bR \subset aR$ *(Teilbarkeit)*

Hauptidealring $R :\Leftrightarrow$ Jedes Ideal ist Hauptideal *(in $\mathbb{Z}$: ggT!)*

π Primideal $:\Leftrightarrow$ R/π Integritätsbereich

S maximales Ideal $:\Leftrightarrow$ $\Leftrightarrow\ R/S$ Körper

$S \neq R$ und $S \subset H \subset R\ \Rightarrow\ (H = S) \vee (H = R)$ *(H Ideal)*

p Primelement $:\Leftrightarrow$ $p/ab\ \Rightarrow\ p/a \vee p/b$ $\Leftrightarrow\ pR$ Primideal

q irreduzibel $:\Leftrightarrow$ $q = rr'\ \Rightarrow\ r \in R^* \vee r' \in R^*$ $\Leftrightarrow\ pR$ *maximal*

(prim $\Rightarrow$ irreduzibel) *als Hauptideal*

Ring-Homomorphismus $\varphi : R \mapsto S$

Kern von φ $\ker\varphi := \varphi^{-1}\{0\} \lhd R$ *(beidseitiges) Ideal*

Kongruenz $a \equiv b \pmod{\ker\varphi}\ \Leftrightarrow\ \varphi(a-b) = 0$ $\ker\varphi \lhd (R,+)$

Projektion $\varphi_1 : R \to R/\ker\varphi,\ r \mapsto r + \ker\varphi$ surjektiv

$\varphi_2 : R/\ker\varphi \to S,\ r + \ker\varphi \mapsto \varphi(r + \ker\varphi) = \varphi(r)$ injektiv

Einbettung $R/\ker\varphi \cong \varphi(R) < S$

Homomorphiesatz (für Ringe) (kanonische Zerlegung)

$$\begin{array}{ccc} R & & \\ \downarrow & \searrow & \varphi = \varphi_1 \circ \varphi_2 \\ R/\ker\varphi & \to & S \end{array}$$

Homomorphismus $\varphi : R \to R/I,\ r \mapsto r + I \Leftrightarrow I$ *beidseitiges Ideal*