Definition R Int-Ring, $a, b \in R$. Nenne a *Teiler* von b (a *teilt* b, $a \mid b$), falls $b = ra$ mit $r \in R$.

Bemerkung R Int-Ring, $a \in R$. Dann:

(i) $a \mid a$, denn $a = 1_R \cdot a$,

(ii) $a \mid 0_R$, denn $0_R = 0_R \cdot a$,

(iii) $c \in R^* \Rightarrow c \mid a$, denn $a = (ac^{-1}) \cdot c$.

Beispiel Die Teiler von $12 \in \mathbb{Z}$ sind:

$$\pm 1, \ \pm 2, \ \pm 3, \ \pm 4, \pm 6, \pm 12.$$

Beispiel Die Teiler von $f = T^2 - 1 \in \mathbb{Q}[T]$ sind:

$$a, \ b(T-1), \ c(T+1), \ d(T^2-1),$$

wobei $a, b, c, d \in \mathbb{Q}^*$. Beachte dazu

$$f = gh \Rightarrow \deg(g) + \deg(h) = 2.$$

Satz Es seien R Int-Ring, $a, b \in R$.

Dann:

$$a \mid b \iff_1 b \in \langle a \rangle$$
$$\iff_2 \langle b \rangle \subseteq \langle a \rangle.$$

Weiter:

$$a \mid b \text{ und } b \mid a \iff_3 \langle a \rangle = \langle b \rangle$$
$$\iff_4 b = ca \text{ mit } c \in R^*.$$

Beweis Klar: "$\iff_1$, $\iff_2$, $\iff_3$".

Zu "$\Rightarrow_4$": Haben

$$a \in \langle b \rangle \Rightarrow a = c'b, \quad b \in \langle a \rangle \Rightarrow b = ca$$

Damit

$$a = c'ca \underset{\text{Int-Ring}}{\overset{R}{\Rightarrow}} 1_R = c'c \Rightarrow c', c \in R^*.$$

Zu "$\Leftarrow_4$": Haben

$$b = ca \Rightarrow b \in \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle.$$

Weiter:

$$a = c^{-1}b \Rightarrow a \in \langle b \rangle \Rightarrow \langle a \rangle \subseteq \langle b \rangle.$$

$\square$

Definition R Int-Ring. Nenne $a, b \in R$ *assoziiert zueinander* ($a \sim b$), falls $b = ca$ mit $c \in R^*$.

Beispiel Für $m, n \in \mathbb{Z}$:

$$m \sim n \iff m = \pm n.$$

Beispiel Für $f, g \in \mathbb{k}[T]$:

$$f \sim g \iff g = af \text{ mit } a \in \mathbb{k}^*.$$

Satz Es sei R Int-Ring.

(i) "$\sim$" ist Äquivalenzrel. auf R.

(ii) Haben $a \sim b \iff a|b$ und $b|a$.

(iii) Falls $a \sim b$: a und b haben dasselbe Teilbarkeitsverhalten, d.h.

$$a|r \iff b|r \quad \text{und} \quad r|a \iff r|b.$$

Umgekehrt: Falls a, b dasselbe Teilbarkeitsverhalten, so gilt $a \sim b$.

Beweis Zu (i). Reflexivität:

$$a = 1_R \cdot a \implies a \sim a$$

Symmetrie:

$$a \sim b \implies b = ca,\ c \in R^*$$
$$\implies a = c^{-1}b,\ c^{-1} \in R^*$$
$$\implies a \sim b.$$

Transitivität:

$$a \sim b,\ b \sim d \implies b = ca,\ d = c'b,\ c, c' \in R^*$$
$$\implies d = \underbrace{c'c}_{\in R^*}a$$
$$\implies a \sim d.$$

Zu (iii). Sei $a \sim b$, d.h. $b = ca$ mit $c \in R^*$. Dann:

$$a|r \iff r = r'a \iff r = r'c^{-1}b \iff b|r,$$
$$r|a \iff a = a'r \iff b = ca'r \iff r|b.$$

Falls a, b selbes Teilbarkeitsverhalten:

$$a|a \implies a|b, \quad a|a \implies b|a$$

Also $a|b$ und $b|a$. Somit $a \sim b$. $\square$

Definition R Int-Ring, $a_1, \dots, a_n \in R$.

(i) Nenne $a \in R$ einen *größten gemeinsamen Teiler* von $a_1, \dots, a_n$, falls

* $a \mid a_i$ für $i = 1, \dots, n$,
* $a' \mid a_i$ für $i = 1, \dots, n \Rightarrow a' \mid a$.

(ii) $$\mathrm{ggT}(a_1, \dots, a_n) := \left\{ a \in R;\ \begin{array}{l} a \text{ ist gr. gem.} \\ \text{Teiler von } a_1, \dots, a_n \end{array} \right\}$$

(iii) Nenne $a_1, \dots, a_n$ *teilerfremd*, falls $1_R \in \mathrm{ggT}(a_1, \dots, a_n)$.

(iv) Nenne $b \in R$ ein *kleinstes gemeinsames Vielfaches* von $a_1, \dots, a_n$, falls

* $a_i \mid b$ für $i = 1, \dots, n$,
* $a_i \mid b'$ für $i = 1, \dots, n \Rightarrow b \mid b'$.

(v) $$\mathrm{kgV}(a_1, \dots, a_n) := \left\{ b \in R;\ \begin{array}{l} b \text{ ist kl. gem.} \\ \text{Vielf. von } a_1, \dots, a_n \end{array} \right\}$$

Beispiel In $\mathbb{Z}$ haben wir

$$\mathrm{ggT}(12, 18) = \{\pm 6\},$$

$$\mathrm{kgV}(12, 18) = \{\pm 36\}.$$

Bemerkung R Int-Ring, $a_1, \dots, a_n \in R$.

(i) Für alle $a, a' \in R$:

$$a, a' \in \mathrm{ggT}(a_1, \dots, a_n) \Rightarrow a \sim a'$$

$$a \in \mathrm{ggT}(a_1, \dots, a_n),\ a \sim a' \Rightarrow a' \in \mathrm{ggT}(a_1, \dots, a_n).$$

(ii) Für alle $b, b' \in R$:

$$b, b' \in \mathrm{kgV}(a_1, \dots, a_n) \Rightarrow b \sim b'$$

$$b \in \mathrm{kgV}(a_1, \dots, a_n),\ b \sim b' \Rightarrow b' \in \mathrm{kgV}(a_1, \dots, a_n).$$

<u>Definition</u> Hauptidealring: Int-Ring R, sodass jedes $\mathfrak{a} \leq_R R$ Hauptideal, d.h., $\mathfrak{a} = \langle a \rangle$ mit $a \in R$.

<u>Satz</u> R Hauptidealring, $a_1, \dots, a_n \in R$.
Dann, für jedes $a \in R$:

$$a \in \mathrm{ggT}(a_1, \dots, a_n) \overset{}{\underset{1}{\iff}} \langle a \rangle = \langle a_1, \dots, a_n \rangle,$$

$$a \in \mathrm{kgV}(a_1, \dots, a_n) \underset{2}{\iff} \langle a \rangle = \langle a_1 \rangle \cap \dots \cap \langle a_n \rangle.$$

Insbesondere:

$$\mathrm{ggT}(a_1, \dots, a_n) \neq \emptyset, \quad \mathrm{kgV}(a_1, \dots, a_n) \neq \emptyset.$$

<u>Beweis</u> Zu "$\Rightarrow_1$": Haben

$$a \mid a_i,\ i = 1, \dots, n \implies a_i \in \langle a \rangle,\ i = 1, \dots, n$$
$$\implies \langle a_1, \dots, a_n \rangle \subseteq \langle a \rangle.$$

Wegen R HIR: Es gibt $b \in R$ mit

$$\langle a_1, \dots, a_n \rangle = \langle b \rangle.$$

Damit:

$$a_i \in \langle b \rangle,\ i = 1, \dots, n \implies b \mid a_i,\ i = 1, \dots, n$$
$$\implies b \mid a \quad (a \in \mathrm{ggT}(a_1, \dots, a_n))$$
$$\implies \langle a \rangle \subseteq \langle b \rangle = \langle a_1, \dots, a_n \rangle$$

Zu "$\Leftarrow_1$": Haben

$$a_i \in \langle a \rangle,\ i = 1, \dots, n \implies a \mid a_i,\ i = 1, \dots, n.$$

Sei $a' \in R$ mit $a' \mid a_i$, $i = 1, \dots, n$. Dann:

$$a_i \in \langle a' \rangle,\ i = 1, \dots, n \implies \langle a_1, \dots, a_n \rangle \subseteq \langle a' \rangle$$
$$\implies \langle a \rangle \subseteq \langle a' \rangle$$
$$\implies a' \mid a. \qquad \square$$

<u>Folgerung</u> R Hauptidealring, $a_1, \dots, a_n \in R$.
Dann:

$a_1, \dots, a_n$ teilerfremd $\iff$ Es gibt $r_1, \dots, r_n \in R$ mit $1_R = r_1 a_1 + \dots + r_n a_n$

<u>Beweis</u> Haben

$a_1, \dots, a_n$ teilerfremd $\overset{\text{Def.}}{\iff} 1_R \in \mathrm{ggT}(a_1, \dots, a_n) \overset{\text{Satz}}{\iff} \langle 1_R \rangle = \langle a_1, \dots, a_n \rangle.$

$\square$

__Definition__ R Int-Ring.

(i) Nenne $q \in R$ *irreduzibel*, falls

* $q \neq 0_R$, $q \notin R^*$,
* $q = ab$ mit $a, b \in R \Rightarrow a \in R^*$ oder $b \in R^*$.

(ii) Nenne $p \in R$ *prim*, falls

* $p \neq 0_R$, $p \notin R^*$,
* $p \mid ab$ mit $a, b \in R \Rightarrow p \mid a$ oder $p \mid b$.

__Bemerkung__ R Int-Ring, $0_R \neq q \in R \setminus R^*$.

Dann:

q irreduz. $\Longleftrightarrow$ q hat keine "echten" Teiler, d.h., $a \mid q \Rightarrow a \in R^*$ oder $a \sim q$.

__Beispiel__ Üblich: $p \in \mathbb{Z}_{\geq 1}$ *Primzahl*, falls 1 und p einzige Teiler von p in $\mathbb{Z}_{\geq 1}$.

D.h.: Primzahlen sind irreduzibel.

__Beispiel__ $\mathbb{k}$ Körper. Wissen: $\mathbb{k}[T]^* = \mathbb{k}^*$.

Haben:

$f \in \mathbb{k}[T]$, $\deg(f) = 1 \Rightarrow f$ irreduzibel.

Denn:

$$f = gh \Rightarrow \deg(g) = 0,\ \deg(h) = 1 \text{ oder } \deg(g) = 1,\ \deg(h) = 0$$

$$\Rightarrow g \in \mathbb{k}^* \text{ oder } h \in \mathbb{k}^*.$$

__Satz__ R Int-Ring, $p \in R$ prim. Dann ist p irreduzibel.

__Beweis__ Sei $p = ab$ mit $a, b \in R$.

Dann: $p \mid ab$. Somit

$p \mid a$ oder $p \mid b$.

Etwa $p \mid a$. Dann $a = rp$ mit $r \in R$.

Damit:

$$p = ab = rpb$$

$$\xrightarrow[\text{Int-Ring}]{R} 1_R = rb$$

$$\Longrightarrow b \in R^*.$$

$\square$

<u>Satz</u> R Hauptidealring. Dann für jedes $q \in R$ äquivalent:

(i) q ist prim.

(ii) q ist irreduzibel.

<u>Beweis</u> Wissen schon: "(i) $\Rightarrow$ (ii)".

Zu "(ii) $\Rightarrow$ (i)". Zeigen zunächst:

Für jedes $\mathfrak{a} \trianglelefteq_R R$ gilt

$$(*) \quad \langle q \rangle \subsetneq \mathfrak{a} \Rightarrow \mathfrak{a} = R.$$

Wegen R HIR: $\mathfrak{a} = \langle a \rangle$ mit $a \in R$.

Damit:

$$\langle q \rangle \subsetneq \langle a \rangle$$

Folglich $q = ab$ mit $b \in R \setminus R^*$. Wegen q irred: $a \in R^*$. Also

$$\mathfrak{a} = \langle a \rangle = R.$$

Zeigen jetzt: q prim. Seien $a, b \in R$ mit $q \mid ab$. Zu zeigen:

$$q \mid a \text{ oder } q \mid b.$$

Angenommen $q \nmid a$ und $q \nmid b$. Dann:

$$a \notin \langle q \rangle \text{ und } b \notin \langle q \rangle.$$

Mit $(*)$:

$$\begin{aligned} \langle q \rangle &\subsetneq \langle a, q \rangle \\ &= R \\ &= \langle b, q \rangle \supsetneq \langle q \rangle. \end{aligned}$$

Also

$$\begin{aligned} R &= \langle a, q \rangle \langle b, q \rangle \\ &= \langle ab, aq, bq, q^2 \rangle \subseteq \langle q \rangle. \end{aligned}$$

Folglich

$$R = \langle q \rangle \Rightarrow 1_R \in \langle q \rangle \;\lightning. \qquad \square$$