Erinnerung *kommutativer Ring mit Eins* (*k1-Ring*): Menge R mit Verknüpfungen

$$R \times R \to R, \quad (a,b) \mapsto a+b \quad \text{„Addition"}$$

$$R \times R \to R, \quad (a,b) \mapsto ab \quad \text{„Multiplikation"}$$

sodass

* $(R,+)$ abelsche Gruppe (neutrales El.: 0_R)
* $(R,\cdot)$ abelsches Monoid, d.h.
  - stets $a(bc) = (ab)c$
  - stets $ab = ba$
  - es gibt $1_R \in R$ mit $1_R a = a$ für alle $a \in R$

Die neutralen Elemente 0_R bez. „+" und 1_R bez. „·" sind eindeutig.

Nenne $a \in R$ *Einheit*, falls es $b \in R$ gibt mit

$$ab = 1_R.$$

Dabei ist b eindeutig. Schreiben:

$$b = a^{-1}.$$

Die Menge aller Einheiten,

$$R^* := \{a \in R;\ a \text{ Einheit}\},$$

ist eine abelsche Gruppe bez. „·" mit neutralem El. 1_R.

Integritätsring: k1-Ring R mit $1_R \neq 0_R$ und stets

$$ab = 0_R \implies a = 0_R \text{ oder } b = 0_R.$$

In jedem Integritätsring gilt die *Kürzungsregel*:

$$ab = ac,\ a \neq 0_R \implies b = c$$

Körper: k1-Ring $\mathbb{K}$ mit $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ und $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$.

Beispiel $(\mathbb{Z},+,\cdot)$ ist Integritätsring. Einheitengruppe:

$$\mathbb{Z}^* = \{\pm 1\}.$$

<u>Beispiel</u> $\mathbb{k}$ Körper. Polynom über $\mathbb{k}$ in der Variablen T:

$$\sum_{\nu \in \mathbb{Z}_{\geq 0}} a_\nu T^\nu \qquad a_\nu \in \mathbb{k},\ a_\nu \neq 0_{\mathbb{k}} \text{ für nur endl. viele } \nu \in \mathbb{Z}_{\geq 0}$$

$\mathbb{k}[T] :=$ Menge aller Pol. über $\mathbb{k}$ in T.

Verknüpfungen:

$$\left(\sum a_\nu T^\nu\right) + \left(\sum b_\nu T^\nu\right) := \sum (a_\nu + b_\nu) T^\nu$$

$$\left(\sum a_\nu T^\nu\right)\left(\sum b_\nu T^\nu\right) := \sum_\nu \left(\sum_{\varkappa+\mu=\nu} a_\varkappa b_\mu\right) T^\nu$$

$(\mathbb{k}[T], +, \cdot)$ ist k1-Ring, der Polynomring in T über $\mathbb{k}$. Haben

$$0_{\mathbb{k}[T]} = 0_{\mathbb{k}} \cdot T^0, \quad 1_{\mathbb{k}[T]} = 1_{\mathbb{k}} \cdot T^0$$

Grad von $f = \sum a_\nu T^\nu \in \mathbb{k}[T]$:

$$\deg(f) := \begin{cases} \max(\nu \in \mathbb{Z}_{\geq 0};\ a_\nu \neq 0_{\mathbb{k}}), & f \neq 0_{\mathbb{k}[T]}, \\ -\infty, & f = 0_{\mathbb{k}[T]}. \end{cases}$$

Falls $\deg(f) = n \geq 0$: Nenne a_n den Leitkoeffizienten von f.

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

$$\deg(f+g) \leq \max(\deg(f), \deg(g))$$

$$\deg(fg) = \deg(f) + \deg(g).$$

Insbesondere

$$\deg(f), \deg(g) \geq 0 \Rightarrow \deg(fg) \geq 0$$

Somit: $\mathbb{k}[T]$ Integritätsring. Weiter

$$fg = 1_{\mathbb{k}[T]} \Rightarrow \deg(f) = \deg(g) = 0$$
$$\Rightarrow f, g \in \mathbb{k}^* \cdot T^0$$

Somit: $\mathbb{k}[T]^* = \mathbb{k}^* \cdot T^0$.

<u>Beispiel</u> $C_n = \{\bar{0}, \ldots, \overline{n-1}\}$ k1-Ring durch

$$\bar{a} + \bar{b} := \overline{r(a+b;n)}, \quad \bar{a}\,\bar{b} := \overline{r(ab;n)}.$$

Einheitengruppe:

$$C_n^* = \{\bar{a};\ \mathrm{ggT}(a,n) = 1\}.$$

Insbes.: C_n Körper $\Leftrightarrow$ n Primzahl.

__Definition__ R k1-Ring. Unterring: Teilmenge $S \subseteq R$ mit

$$0_R, 1_R \in S, \quad a,b \in S \Rightarrow a \pm b, ab \in S$$

und den induzierten Verknüpfungen

$$(a,b) \mapsto a+b, \quad (a,b) \mapsto ab.$$

Nenne $S \subseteq R$ dann Ringerweiterung.

__Bemerkung__ R k1-Ring, $S \subseteq R$ Unterring. Dann: S k1-Ring mit

$$0_S = 0_R, \quad 1_S = 1_R, \quad a \in S \Rightarrow -a = 0_R - a \in S.$$

__Bemerkung__ R k1-Ring, $S \subseteq R$ Unterring. Dann: R Int-Ring $\Rightarrow$ S Int-Ring.

__Beispiel__ Haben Ringerweiterung $\mathbb{Z} \subseteq \mathbb{Q}$.

__Konstruktion__ R k1-Ring, $S \subseteq R$ Unterring, $A \subseteq S$. Haben Unterring:

$$S[A] := \left\{ \sum_{i=1}^{n} s_{i_1} \cdots s_{i_{m_i}} ;\ n, m_i \in \mathbb{Z}_{\geq 1},\ s_{i_j} \in S \cup A \right\},$$

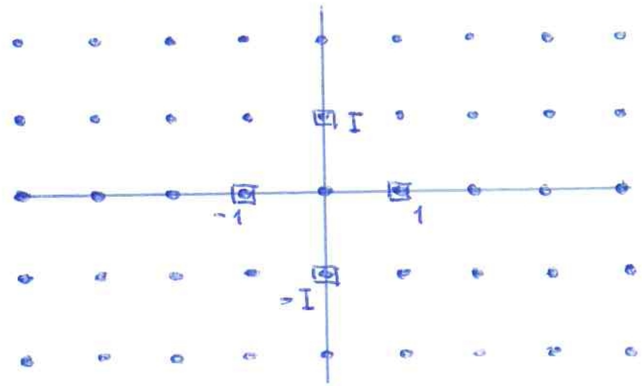
den von A über S erzeugten Unterring.

__Beweis__ Klar: $0_R = \sum_{i=1}^{1} 0_R$, $1_R = \sum_{i=1}^{1} 1_R \in S[A]$.

Weiter: $a, b \in S[A] \Leftrightarrow a, b$ Summen von Produkten von El. aus $S \cup A \Rightarrow a \pm b, ab \in S[A]$. $\square$

__Ring der ganzen Gaußschen Zahlen__ Betrachte Ringerweiterung $\mathbb{Z} \subseteq \mathbb{C}$ und $I \in \mathbb{C}$. Dann:

$$\mathbb{Z}[I] = \{ m + In;\ m, n \in \mathbb{Z} \} \subseteq \mathbb{C}$$



Haben $\mathbb{C}$ Int-Ring $\Rightarrow$ $\mathbb{Z}[I]$ Intring. Weiter:

$$\mathbb{Z}[I]^* = \{ \pm 1, \pm I \}$$

Klar: $\pm 1, \pm I \in \mathbb{Z}[I]^*$. Sei $m + In \in \mathbb{Z}[I]^*$.

Dann: $(m+In)^{-1} = l + Ik$. Somit:

$$1 = (m+In)(l+Ik) = |(m+In)(l+Ik)|^2$$
$$= |m+In|^2 \, |l+Ik|^2 = (m^2+n^2)(l^2+k^2)$$

$$\Rightarrow m^2 + n^2 = 1 \Rightarrow m = \pm 1, n = 0 \text{ oder } m = 0, n = \pm 1.$$

Definition *Homomorphismus* von k1-Ringen R und S: Abbildung $\varphi: R \to S$ mit

$$\varphi(1_R) = 1_S, \qquad \begin{aligned} \varphi(a+b) &= \varphi(a)+\varphi(b), \\ \varphi(ab) &= \varphi(a)\varphi(b). \end{aligned}$$

Ein Hom. $\varphi: R \to S$ heisst *Isomorphismus*, falls es Hom. $\psi: S \to R$ gibt mit

$$\psi \circ \varphi = \mathrm{id}_R, \qquad \varphi \circ \psi = \mathrm{id}_S.$$

Weiter, für Hom. $\varphi: R \to S$ von k1-Ringen:

$$\mathrm{kern}(\varphi) := \{a \in R;\ \varphi(a) = 0_S\},$$

$$\mathrm{Bild}(\varphi) := \{\varphi(a);\ a \in R\}.$$

Beispiel Haben surjektiven Hom. von k1-Ringen

$$\pi: \mathbb{Z} \to C_n, \quad a \mapsto \overline{r(a;n)}$$

Dabei $\mathrm{Bild}(\pi) = C_n$, $\mathrm{kern}(\pi) = n\mathbb{Z}$.

Beachte: $\mathrm{kern}(\pi) \subseteq \mathbb{Z}$ für $n \geq 2$ kein Unterring wegen $1 \notin \mathrm{kern}(\pi)$.

Satz $\varphi: R \to S$ Hom. von k1-Ringen.

Dann:

(i) $\varphi(0_R) = 0_S$.

(ii) $R' \subseteq R$ Unterring $\Rightarrow \varphi(R') \subseteq S$ Unterring.

(iii) $S' \subseteq S$ Unterring $\Rightarrow \varphi^{-1}(S') \subseteq R$ Unterring.

(iv) $\varphi: R \to S$ injektiv $\Leftrightarrow \mathrm{kern}(\varphi) = \{0_R\}$.

(v) $\varphi: R \to S$ Iso $\Leftrightarrow \varphi$ bijektiv.

Konstruktion Seien $R_1, \dots, R_s$ k1-Ringe.

Direktes Produkt: $R_1 \times \dots \times R_s$ mit

$$(a_1, \dots, a_s) + (b_1, \dots, b_s) := (a_1+b_1, \dots, a_s+b_s),$$
$$(a_1, \dots, a_s) \cdot (b_1, \dots, b_s) := (a_1 b_1, \dots, a_s b_s).$$

$R_1 \times \dots \times R_s$ ist k1-Ring mit

$$0_{R_1 \times \dots \times R_s} = (0_{R_1}, \dots, 0_{R_1}), \qquad 1_{R_1 \times \dots \times R_s} = (1_{R_1}, \dots, 1_{R_s})$$

Haben surjektive Ringhomomorphismen

$$\pi_i: R_1 \times \dots \times R_s \to R_i, \quad (a_1, \dots, a_s) \mapsto a_i.$$