Definition Ring: Menge R mit Verknüpfungen

$$\text{add}: R \times R \longrightarrow R, \quad (a,b) \mapsto a+b,$$

$$\text{mult}: R \times R \longrightarrow R, \quad (a,b) \mapsto a \cdot b,$$

sodass:

(R1) $(R,+)$ ist abelsche Gruppe,

(R2) "$\cdot$" ist assoziativ, d.h., stets

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

(R3) "$+$" und "$\cdot$" sind distributiv, d.h., stets

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

$$(b+c) \cdot a = (b \cdot a) + (c \cdot a)$$

Ein Ring $(R,+,\cdot)$ heisst kommutativ, falls neben (R1), (R2), (R3) auch

(kR) "$\cdot$" ist kommutativ, d.h., stets

$$a \cdot b = b \cdot a.$$

$(R,+,\cdot)$ heisst Ring mit Einselement, falls neben (R1), (R2), (R3) auch

(RE) "$\cdot$" besitzt neutrales Element, d.h., es gibt $1_R \in R$ sodass stets

$$1_R \cdot a = a = a \cdot 1_R.$$

Beispiel kommutative Ringe mit Einselement:

$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$

Lemma Es sei $(R,+,\cdot)$ Ring mit Einselement. Dann:

(i) Die neutralen El. 0_R bez. "+" und 1_R bez. "$\cdot$" sind eindeutig bestimmt.

(ii) Für jedes $r \in R$ gilt:

$$0_R \cdot r = 0_R = r \cdot 0_R .$$

Insbes.: $1_R = 0_R$ nur bei $R = \{0_R\}$.

(iii) Für jedes $r \in R$ gilt:

$$(-1_R)\cdot r = -r = r\cdot(-1_R).$$

Für je zwei $a, b \in R$ gilt:

$$(-a)\cdot b = a\cdot(-b) = -(a\cdot b),$$

$$(-a)\cdot(-b) = a\cdot b.$$

Beweis. Zu (i). Wegen $(R,+)$ Gruppe: 0_R eindeutig.

Eindeutigkeit von 1_R: Es sei $1'_R \in R$ ebenfalls neutral bez. "$\cdot$".

Dann:

$$1'_R = 1_R \cdot 1'_R = 1_R .$$

Zu (ii): Vorüberlegung: Für jedes $r \in R$ gilt:

$$0_R \cdot r = (0_R + 0_R)\cdot r = 0_R \cdot r + 0_R \cdot r$$

Setzt $-0_R \cdot r$ hinzuaddieren:

$$0_R = 0_R \cdot r .$$

Analog: $0_R = r \cdot 0_R$. □

Bemerkung. Es seien $(R,+)$ ab. Gruppe und $a_1,\dots,a_n \in R$. Schreibweisen:

$$\sum_{i=1}^{n} a_i := a_1 + \dots + a_n$$
$$:= a_1 + (a_2 + (\dots (a_{n-1} + a_n) \dots))$$

Für $n \in \mathbb{N}$ und $a \in R$:

$$na := \sum_{i=1}^{n} a, \qquad 0a := 0_R.$$

Bemerkung. Es seien $(R,+,\cdot)$ Ring, $a_1,\dots,a_n \in R$. Schreibweisen:

$$\prod_{i=1}^{n} a_i := a_1 \cdot \dots \cdot a_n$$
$$:= a_1 \cdot (a_2 \cdot (\dots (a_{n-1} \cdot a_n) \dots))$$

Für $n \in \mathbb{N}$ und $a \in R$:

$$a^n := \prod_{i=1}^{n} a, \qquad a^0 := 1_R$$

Sind weiter $b_1,\dots,b_m \in R$ gegeben, so gilt:

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_i b_j\right)$$
$$= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_i b_j\right)$$

Man kann also in einem Ring wie gewohnt ausmultiplizieren.

Definition Es seien R, S Ringe. Eine Abb. $\varphi: R \to S$ heisst Ringhomomorphismus, falls für alle $a, b \in R$ gilt:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Beispiel Es sei R Ring. Dann ist $\mathrm{id}_R: R \to R$ Ringhom.

Konstruktion Es sei $n \in \mathbb{N}_{\geq 1}$. Haben 2 Verknüpfungen auf $C_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$:

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

Satz $(C_n, +, \cdot)$ ist kommut. Ring mit Einsel. $\overline{1}$. Weiter:

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

ist surjektiver Ringhom. mit $\pi(1) = \overline{1}$ und

$$\pi(a) = \pi(b) \iff n \text{ teilt } (a-b)$$

Bemerkung π hilft beim Rechnen, z.B. in C_6:

$$\begin{aligned}(\overline{4} + \overline{4}) \cdot \overline{5} &= (\pi(4) + \pi(4)) \cdot \pi(5) \\ &= (\pi(4+4)) \cdot \pi(5) \\ &= \pi((4+4) \cdot 5) \\ &= \pi(40) \\ &= \overline{4}.\end{aligned}$$

Definition Es sei R Ring mit Einselement. Nenne $a \in R$ Einheit, falls es $a' \in R$ gibt mit

$$a' \cdot a = 1_R = a \cdot a'.$$

Setzen

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

Beispiel Einheitenmengen von $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$:

$$\mathbb{Z}^* = \{\pm 1\}, \quad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}.$$

Satz Es sei $(R, +, \cdot)$ Ring mit Einselement. Dann:

(i) $(R^*, \cdot)$ ist Gruppe mit neutr. Element 1_R.

(ii) Ist R kommutativ, so ist $(R^*, \cdot)$ abelsch.

Beweis Wir zeigen zunächst

$$a, b \in R^* \Rightarrow a \cdot b \in R^*$$

Wähle $a', b' \in R$ mit

$$a'a = 1_R = a \cdot a', \quad b' \cdot b = 1_R = b \cdot b'$$

Dann:

$$(a \cdot b) \cdot (b' \cdot a') = a \cdot (b \cdot b') \cdot a' = a \cdot a' = 1_R,$$

$$(b' \cdot a') \cdot (a \cdot b) = b' \cdot (a' \cdot a) \cdot b = b' \cdot b = 1_R.$$

Also ist $a \cdot b$ Einheit. Somit

$$R^* \times R^* \to R^*, \quad (a, b) \mapsto a \cdot b$$

wohldefiniert. Rest: klar. □

Schreibweise Es sei R Ring mit Einselement, $a \in R^*$. Wir schreiben a^{-1} für das multiplikative Inverse von a.

Satz Es sei $n \in \mathbb{N}_{\geq 1}$. Für jedes $\bar{a} \in C_n$ sind äquivalent:

(i) $\bar{a} \in C_n^*$.

(ii) $ggT(a,n) = 1$.

Weiter gilt:

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

Beweis Zu "(i) $\Rightarrow$ (ii)". Wähle $\bar{b} \in C_n$ mit $\bar{a} \cdot \bar{b} = \bar{1}$. Dann:

$$\pi(a \cdot b) = \bar{a} \cdot \bar{b} = \bar{1} = \pi(1)$$

für $\pi : \mathbb{Z} \to C_n$, $a \mapsto \bar{a}$. Somit:

$$a \cdot b = 1 + \ell n \quad \text{mit } \ell \in \mathbb{Z}.$$

Zeigen: $ggT(a,n) = 1$. Sei $c \in \mathbb{N}_{\geq 1}$ mit $c \mid a$ und $c \mid n$. Dann:

$$a = a' \cdot c, \quad n = n' \cdot c \quad \text{mit } a', n' \in \mathbb{Z}.$$

Somit

$$1 = ab - \ell n = a'cb - \ell n'c = c(a'b - \ell n')$$

($c \in \mathbb{Z}_{\geq 1}$, $a'b - \ell n' \in \mathbb{Z}$)

$\Rightarrow c = 1$.

Zu "(ii) $\Rightarrow$ (i)". Wähle $b, \ell \in \mathbb{Z}$, sodass

$$c := ab - \ell n \text{ minimal mit } c > 0$$

Zeigen: $c \mid a$. Sonst: Division mit Rest:

$$a = k_a c + c', \quad 0 < c' < c.$$

Damit:

$$c' = a - k_a c = a - k_a(ab - \ell n)$$
$$= a \cdot \underbrace{(1 - k_a b)}_{=:b'} - \underbrace{(-k_a \ell)}_{=:n'} n$$

Widerspruch zu c minimal!

Zeigen: $c \mid n$. Sonst: Division mit Rest:

$$n = k_n c + c'', \quad 0 < c'' < c.$$

Damit:

$$c'' = n - k_n c = n - k_n(ab - \ell n)$$
$$= a \cdot \underbrace{(-k_n b)}_{=:b''} - \underbrace{(-1 - k_n \ell)}_{=:\ell''} n$$

Widerspruch zu c minimal. Wegen $ggT(a,n) = 1$:

$c = 1$. Damit:

$$\bar{a} \cdot \bar{b} = \pi(a)\pi(b) = \pi(ab) \overset{\text{Def von } c}{=} \pi(1 + \ell n)$$
$$= \pi(1) = \bar{1}. \quad \square$$