

Sei A ein kommutativer Ring und seien $I, J \subset A$ Ideale. Dann sind auch

$$\begin{aligned} I + J &= \{i + j \mid i \in I, j \in J\}, \\ I \cdot J &= \{\sum_{\alpha} i_{\alpha} j_{\alpha} \mid i_{\alpha} \in I, j_{\alpha} \in J\}, \\ I \cap J & \end{aligned}$$

Ideale in A . Es gilt $I \cdot J \subset I \cap J$ (Warum?).

I, J heißen *teilerfremd*, falls $I + J = A$. Z.B. für $A = \mathbb{Z}$ sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ teilerfremd (also $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$), genau dann, wenn $\text{ggT}(m, n) = 1$.

Lemma. Sind I, J teilerfremd, so gilt $I \cdot J = I \cap J$.

Beweis. Es bleibt zu zeigen, dass $I \cdot J \supset I \cap J$. Da $I + J = A$, können wir $i \in I$ und $j \in J$ finden, so dass $i + j = 1$. Für $x \in I \cap J$ gilt $x = x1 = x(i + j) = xi + xj \in I \cdot J$. \square

Satz. Sei A ein kommutativer Ring und seien I_1, \dots, I_n paarweise teilerfremde Ideale in A . Dann induziert der Ringhomomorphismus

$$\varphi : A \longrightarrow A/I_1 \times \dots \times A/I_n \quad , \quad a \mapsto (a + I_1, \dots, a + I_n)$$

einen Ringisomorphismus

$$\bar{\varphi} : A / \prod_{i=1}^n I_i \longrightarrow A/I_1 \times \dots \times A/I_n .$$

Beweis.

1. I_i und $\prod_{j \neq i} I_j$ sind teilerfremd:

Per Annahme sind I_j und I_i teilerfremd für $j \neq i$. Somit gibt es $x_j \in I_j$ und $y_j \in I_i$ mit $x_j + y_j = 1$. Damit folgt

$$1 = \prod_{j \neq i} (x_j + y_j) = \prod_{j \neq i} x_j + (\text{Terme mit mindestens einem Faktor } y_j) .$$

Der erste Summand liegt in $\prod_{j \neq i} I_j$ und jeder Summand in der restlichen Summe liegt in I_i (da $y_j \in I_i$). Daher $1 \in (\prod_{j \neq i} I_j) + I_i$.

2. $\prod_{i=1}^n I_i = \bigcap_{i=1}^n I_i$:

Per Induktion über n . Für $n = 2$ ist dies die Aussage von Lemma 2. Die Aussage gelte nun für $n - 1$. Nach Teil 1 sind I_n und $\prod_{j \neq n} I_j$ teilerfremd. Nach dem Lemma gilt daher $I_n \cdot \prod_{j \neq n} I_j = I_n \cap \prod_{j \neq n} I_j$. Nach Induktionsvoraussetzung ist ferner $\prod_{j \neq n} I_j = \bigcap_{j \neq n} I_j$.

3. $\ker \varphi = \prod_{i=1}^n I_i$:

Per Definition von φ gilt $\ker \varphi = \bigcap_{i=1}^n I_i$. Damit folgt die Behauptung aus Teil 2.

4. φ ist surjektiv:

Seien $a_1, \dots, a_n \in A$ gegeben. Wir zeigen, dass es $x \in A / \prod_i I_i$ gibt, mit $\varphi(x) = (a_1 + I_1, \dots, a_n + I_n)$. Für jedes $i = 1, \dots, n$ gibt es nach Teil 1 $u_i \in I_i$ und $v_i \in \prod_{j \neq i} I_j$ mit $u_i + v_i = 1$. Setze $x = \sum_{i=1}^n v_i a_i$. Für jedes $k = 1, \dots, n$ gilt

$$x + I_k = v_k a_k + I_k = (1 - u_k) a_k + I_k = a_k + I_k,$$

da $v_i \in I_k$ für $i \neq k$, und da $u_k \in I_k$.

Da $A / \ker \varphi \cong \text{im } \varphi$ als Ringe (2.1, Kor. 2), mit Isomorphismus $\bar{\varphi}$, folgt der Satz aus Teil 3 und 4. \square

Korollar. (Chinesischer Restsatz)

Seien $m_1, \dots, m_n \in \mathbb{Z}_{>0}$ paarweise teilerfremd (d.h. $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$). Dann ist

$$\begin{aligned} \mathbb{Z} / (m_1 \cdots m_n \mathbb{Z}) &\longrightarrow \mathbb{Z} / m_1 \mathbb{Z} \times \cdots \times \mathbb{Z} / m_n \mathbb{Z} \\ x + m_1 \cdots m_n \mathbb{Z} &\longmapsto (x + m_1 \mathbb{Z}, \dots, x + m_n \mathbb{Z}) \end{aligned}$$

wohldefiniert und ein Ringisomorphismus.