Theorem 10.8 (Chinesischer Restsatz)

Sei R ein Ring, $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$, und seien $b_1, \dots, b_n \in R$. Dann ex. $b \in R$ mit $b \equiv b_i \pmod{\mathfrak{a}_i}$ für alle $1 \leq i \leq n$. Zudem ist b modulo $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$ eindeutig bestimmt.

[Thm. formulieren für $R = \mathbb{Z}$]

Beweis: Wir zeigen zuerst folgende

Beh. $R = \mathfrak{a}_k + \bigcap_{j \neq k} \mathfrak{a}_j$ für alle $1 \leq k \leq n$.

Bew. Mit Induktion nach n.

Vorraussetzung: $n = 2$ ✓

Annahme: $R = \mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1})$

Es ist $R = R \cdot R = \underbrace{(\mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1}))}_{=R} \cdot \overbrace{(\mathfrak{a}_1 + \mathfrak{a}_n)}^{=R}$

$$= \underbrace{R \cdot \mathfrak{a}_1}_{=\mathfrak{a}_1} + \underbrace{\mathfrak{a}_1 \cdot \mathfrak{a}_n}_{\subseteq \mathfrak{a}_1 \cap \mathfrak{a}_n} + \underbrace{(\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_{n-1}) \cdot \mathfrak{a}_n}_{\text{Lem. 10.4.(2')}\ \subseteq \mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n}$$

Also $R = \mathfrak{a}_1 + (\mathfrak{a}_2 \cap \dots \cap \mathfrak{a}_n)$. ⊣ Beh.

- Seien nun $b_1, \dots, b_n \in R$. Dann ex. für jedes k mit $1 \leq k \leq n$ ein $a_k \in \mathfrak{a}_k$ und ein $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j$ mit $b_k = a_k + r_k$.
  Definiere $b := r_1 + \dots + r_n$.
  Dann ist $b - b_i = b - a_i - r_i = \sum_{k \neq i} r_k - a_i$. $(*)$
  Weil $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j$ gilt für $k \neq i$: $r_k \in \bigcap_{j \neq k} \mathfrak{a}_j \subseteq \mathfrak{a}_i$.
  D.h. $\sum_{k \neq i} r_k \in \mathfrak{a}_i$ und somit $b - b_i \in \mathfrak{a}_i$ (folgt aus $(*)$)
  also $b \equiv b_i \pmod{\mathfrak{a}_i}$.

- Seien $b, c \in R$ mit $b \equiv b_i \pmod{\mathfrak{a}_i}$ und $c \equiv b_i \pmod{\mathfrak{a}_i}$.
  Für $1 \leq i \leq n$ gilt: $b - b_i, c - b_i \in \mathfrak{a}_i$, d.h. $(b - b_i) - (c - b_i) \in \mathfrak{a}_i$
  und somit ist $b - c = (b - b_i) - (c - b_i) \in \mathfrak{a}_1 \cap \dots \mathfrak{a}_n$. ⊣

Korollar 10.9 Seien R und $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ wie in Thm. 10.8.
Dann ist $R/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \cong R/\mathfrak{a}_1 \oplus \dots \oplus R/\mathfrak{a}_n$.

[Kor. formulieren für $R = \mathbb{Z}$]

Beweis: Betrachte $\varphi: R \to R/\mathfrak{a}_1 \oplus \dots \oplus R/\mathfrak{a}_n$
$$r \longmapsto (r+\mathfrak{a}_1, \dots, r+\mathfrak{a}_n)$$

- $\ker(\varphi) = \{r \in R : \forall i\, (r \equiv 0 \pmod{\mathfrak{a}_i})\} = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$.
- Mit Lemma 10.5 bzw. der Folgerung gilt $R/\ker(\varphi) \cong \varphi[R]$.
- Ist $\bar{b} = (b_1 + \mathfrak{a}_1, \dots, b_n + \mathfrak{a}) \in R/\mathfrak{a}_1 \oplus \dots \oplus R/\mathfrak{a}_n$, so ex. mit Chin. Restsatz 10.8 ein $b \in R$ mit $\varphi(b) = \bar{b}$, d.h. φ ist surjektiv. ⊣

Def. Sei R ein Ring.
- Der <u>Primring</u> von R ist der kleinste nicht-triviale Unterring von R.
- Für $n \in \mathbb{N}$ und $a \in R$ sei $n \cdot a = \underbrace{(a + \dots + a)}_{n\text{-mal}}$ und $(-n) \cdot a := -(n \cdot a)$.

Proposition 10.10 Der Primring eines nicht-trivialen Rings ist eindeutig bestimmt und isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n > 0$ ($n \in \mathbb{N}$).

Beweis: Sei R ein nicht-trivialer Ring. Definiere $\varphi: \mathbb{Z} \to R$
$$n \longmapsto n \cdot 1_R$$

- Dann ist φ ein Ringhom. und $\varphi[\mathbb{Z}]$ ist Unterring von R.
- Sei $S := \varphi[\mathbb{Z}]$, dann ist $S \cong \mathbb{Z}/\ker(\varphi)$ und S ist der Primring von R. [$S \neq \{0\}$ und $S \subseteq S'$ für alle Unterringe $S' \subseteq R$]
- Weil $\mathbb{Z}$ ein Hauptidealring ist und $\ker(\varphi)$ ein Ideal in $\mathbb{Z}$ ist, ist $\ker(\varphi) = (n)$ für ein $n \in \mathbb{N}$.
- D.h. $\underbrace{S \cong \mathbb{Z} \text{ (für } n=0)}_{\mathrm{char}(R)=0}$ oder $\underbrace{S \cong \mathbb{Z}/n\mathbb{Z}}_{\mathrm{char}(R)=n}$ (für $n > 0$). ⊣

Def. <u>Charakteristik</u> von R: $\mathrm{char}(R) = 0$ $\qquad$ $\mathrm{char}(R) = n$

II. Kommutative Ringe

In diesem Kapitel sei R stets ein nicht-trivialer komm. Ring.

<u>Def.</u> Ein Ideal $\mathfrak{p} \subseteq R$ heisst <u>Primideal</u>, falls $R/\mathfrak{p}$ ein Integritätsring ist. [Fall $R = \mathbb{Z}$]

<u>Proposition II.1</u> Ist $\mathfrak{p} \subseteq R$ ein Ideal, dann gilt:

$\mathfrak{p}$ ist Primideal $\Leftrightarrow$ $\mathfrak{p} \neq R$ und für alle $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$ gilt: $\boxed{a \in \mathfrak{p} \vee b \in \mathfrak{p}.}$

<u>Beweis:</u> ($\Rightarrow$) Ist $\mathfrak{p}$ Primideal, dann ist $R/\mathfrak{p}$ Integritätsring, also $R/\mathfrak{p} \neq \{0\}$ und somit $\mathfrak{p} \neq R$.

Seien $a, b \in R$ mit $a \cdot b \in \mathfrak{p}$.

Betrachte $R \to R/\mathfrak{p}$

$a \cdot b \mapsto \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{0}$ (weil $a \cdot b \in \mathfrak{p}$)

Weil $R/\mathfrak{p}$ als Integritätsring nullteilerfrei ist, ist also $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$, d.h. $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

($\Leftarrow$) zu zeigen: $R/\mathfrak{p}$ ist Integritätsring.

Betrachte wieder $R \to R/\mathfrak{p}$

$a \mapsto \bar{a}$

Ist $\overline{a \cdot b} = \bar{a} \cdot \bar{b} = \bar{0}$, so ist $a \cdot b \in \mathfrak{p}$ und mit der Voraussetzung ist dann $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, d.h. $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$, d.h. $R/\mathfrak{p}$ ist Integritätsring. $\dashv$

<u>Def.</u> Ein Ideal $\mathfrak{m} \subseteq R$ heisst <u>maximal</u>, falls gilt:

$\mathfrak{m} \neq R$ und es ex. kein Ideal $\mathfrak{a} \neq R$ mit $\mathfrak{m} \subsetneq \mathfrak{a}$.

[$\mathfrak{m} \neq R$ ist in keinem echten Ideal von R echt enthalten.]

<u>Proposition II.2</u> Sei $\mathfrak{m} \subseteq R$ ein Ideal; dann gilt:

$\mathfrak{m}$ ist maximal $\Leftrightarrow$ $R/\mathfrak{m}$ ist Körper

<u>Beweis:</u> $\pi : R \to R/\mathfrak{m}$ sei die nat. Projektion.
$a \mapsto \bar{a}$

($\Rightarrow$) $\mathfrak{m} \subseteq R$ sei maximal und $\mathfrak{b} \subseteq R/\mathfrak{m}$ sei Ideal.
Dann ist $\pi^{-1}[\mathfrak{b}]$ ein Ideal in R [Übung 62.(a)]
mit $\mathfrak{m} \subseteq \pi^{-1}[\mathfrak{b}]$. Weil $\mathfrak{m}$ maximal ist, gilt
$\pi^{-1}[\mathfrak{b}] = \mathfrak{m}$ oder $\pi^{-1}[\mathfrak{b}] = R$, d.h.
$\mathfrak{b} = \pi[\pi^{-1}[\mathfrak{b}]] = \pi[\mathfrak{m}] = (\bar{0})$ oder $\mathfrak{b} = \pi[R] = R/\mathfrak{m}$.
Somit hat $R/\mathfrak{m}$ genau zwei Ideale, nämlich $(\bar{0})$
und $R/\mathfrak{m}$, also ist $R/\mathfrak{m}$ mit Prp. 10.3 ein Körper.

($\Leftarrow$) Sei $R/\mathfrak{m}$ ein Körper und sei $\mathfrak{a} \subseteq R$ ein Ideal
mit $\mathfrak{m} \subseteq \mathfrak{a}$. Dann ist $\pi[\mathfrak{a}] \subseteq R/\mathfrak{m}$ ein Ideal. [Üb. 62.(b)]
Mit Proposition 10.3 gilt somit $\pi[\mathfrak{a}] = (\bar{0})$ oder
$\pi[\mathfrak{a}] = R/\mathfrak{m}$, d.h. $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$, also ist
$\mathfrak{m}$ ein maximales Ideal in R. $\dashv$

<u>Bem.</u> Jedes maximale Ideal ist Primideal. [Übung]

<u>Proposition 11.3</u> Seien R, S komm. Ringe, $\varphi : R \to S$ ein
Ringhomom., und $\mathfrak{p} \subseteq S$ ein Primideal in S.
Dann ist $\varphi^{-1}[\mathfrak{p}] \subseteq R$ ein Primideal in R.

<u>Beweis:</u> • $\varphi^{-1}[\mathfrak{p}] \neq R$: [Kontraposition]
$\varphi^{-1}[\mathfrak{p}] = R \Rightarrow 1_R \in \varphi^{-1}[\mathfrak{p}] \Rightarrow \varphi(1_R) = 1_S \in \mathfrak{p}$
$\Rightarrow \mathfrak{p} = S \Rightarrow \mathfrak{p}$ nicht Primideal in S.

• $a, b \in R$ mit $a \cdot b \in \varphi^{-1}[\mathfrak{p}]$, dann $a \in \varphi^{-1}[\mathfrak{p}] \vee b \in \varphi^{-1}[\mathfrak{p}]$:
$a \cdot b \in \varphi^{-1}[\mathfrak{p}] \Rightarrow \varphi(a \cdot b) \in \mathfrak{p} \Leftrightarrow \varphi(a) \cdot \varphi(b) \in \mathfrak{p}$,
und weil $\mathfrak{p} \subseteq S$ Primideal ist, gilt $\varphi(a) \in \mathfrak{p} \vee \varphi(b) \in \mathfrak{p}$,
d.h. $a \in \varphi^{-1}[\mathfrak{p}] \vee b \in \varphi^{-1}[\mathfrak{p}]$. $\dashv$