§ 3. Die Charakteristik eines Körpers

Sei $(R, +, \cdot)$ ein Ring. Mit 0_R wird das Nullelement des Ringes und mit 1_R das Einselement des Ringes bezeichnet. Für $m \in \mathbb{Z}$ und $a \in R$ definieren wir das Vielfache $ma \in R$ von a durch die Vorschrift

$$ma := \begin{cases} 0_R & \text{für } m = 0 \\ (m-1)a + a & \text{für } m \geq 1 \\ -((-m)a) & \text{für } m < 0 \end{cases}$$

Dies entspricht die Bildung der Potenz in der abelschen Gruppe $(R, +)$, so daß dann die folgenden Potenzregeln gelten:

$$(m+n)a = ma + na \quad , \quad (mn)a = m(na) \quad , \quad m(a+b) = ma + mb$$

Man erhält speziell für $a = 1_R$, daß die Abbildung

$$f_R : \mathbb{Z} \longrightarrow R \quad , \quad m \longmapsto m1_R$$

ein Ringhomomorphismus ist. Falls f_R injektiv ist, findet man dann die ganzen Zahlen in dem Ring R wieder.

(3.1) DEF: Sei R ein Ring. Gibt es dann ein $m \in \mathbb{N} = \{1, 2, 3, \ldots\}$ mit $m1_R = 0_R$, so sagt man, daß der Ring R eine **endliche Charakteristik** besitzt und nennt

$$\operatorname{char}(R) := \min\{\, k \mid k \in \mathbb{N}\,,\, k1_R = 0_R \,\}$$

die **Charakteristik von** R. Im anderen Fall setzt man

$$\operatorname{char}(R) := 0$$

und nennt R einen Ring der **Charakteristik 0**.

(3.2) BEM: **a)** $\operatorname{char}(\mathbb{Z}_n) = n \;\; (n \in \mathbb{N}) \quad , \quad \operatorname{char}(\mathbb{Z}) = 0$

b) Ist $\operatorname{char}(R) = m$ endlich, so ist m gerade die Ordnung von 1_R in der Gruppe $(R, +)$. Es gilt dann

$$\forall\, k \in \mathbb{Z} : k1_R = 0_R \implies m \mid k$$

$\operatorname{char}(R) = 0$ dagegen ist gleichbedeutend damit, daß 1_R unendliche Ordnung in $(R, +)$ besitzt.

c) Es gilt: $\operatorname{char}(R) = 0 \iff f_R$ ist injektiv und $\operatorname{char}(R) > 0 \iff f_R$ ist nicht injektiv.

(3.3) SATZ: Die Charakteristik eines Integritätsbereiches ist entweder 0 oder eine Primzahl. Dies gilt insbesondere für Körper.

(3.4) LEMMA: Ist $f : R \longrightarrow S$ ein injektiver Ringhomomorphismus, so gilt $\mathrm{char}(R) \;=\; \mathrm{char}(S)$.

(3.5) KOROLLAR: Ist $U \subseteq R$ Unterring eines Ringes R, so gilt $\mathrm{char}(U) \;=\; \mathrm{char}(R)$.

(3.6) SATZ: Sei K ein Körper. Dann gilt:

a) Der Durchschnitt über ein beliebiges System von Unterkörpern von K ist wieder ein Unterkörper von K .

b) Der Durchschnitt $P(K)$ über alle Unterkörper von K ist der kleinste Unterkörper von K, d.h. $P(K)$ ist ein Unterkörper von K, und es gilt: ist $U \subseteq K$ ein beliebiger Unterkörper von K, so folgt $P(K) \subseteq U$.

$P(K)$ heißt der **Primkörper von** K .

BEISPIELE: $P(\mathbb{C}) = P(\mathbb{R}) = P(\mathbb{Q}) = \mathbb{Q}$, $P(\mathbb{Z}_p) = \mathbb{Z}_p$ $(p \in \mathbb{P})$ (s. Übungen)

(3.7) SATZ: Sei K ein Körper und $P(K)$ der Primkörper von K . Dann gilt:

a) $\mathrm{char}(K) = 0 \iff P(K) \cong \mathbb{Q}$

b) $\mathrm{char}(K) = p \iff P(K) \cong \mathbb{Z}_p$ $(p \in \mathbb{P})$.

(3.8) KOROLLAR: Sei K ein endlicher Körper der Charakteristik $p \in \mathbb{P}$. Dann gibt es ein $n \in \mathbb{N}$ mit

$$|K| \;=\; p^n \,.$$