12. Charakteristik eines Rings

Lemma 85: Es sei R ein Ring mit Eins. Dann gibt es genau einen Ringhomomorphismus $\chi : \mathbb{Z} \to R$ mit der Eigenschaft $\chi(1_\mathbb{Z}) = 1_R$.

Beweis: Eindeutigkeit: Aus der Bedingung $\chi(1_\mathbb{Z}) = 1_R$ folgt

$$\chi(n) = \chi(n \cdot 1_\mathbb{Z}) \overset{\text{Lemma 22 (iii)}}{=} n \cdot \chi(1_\mathbb{Z}) = n \cdot 1_R \quad \forall n \in \mathbb{Z}.$$

Existenz: Dass es sich bei der Abbildung $\chi : \mathbb{Z} \to R$, $\chi(n) = n \cdot 1_R$ um einen Ringhomomorphismus handelt, wurde bereits in Beispiel 4 am Beginn von Kapitel 9 gezeigt.

Definition: Es sei R ein Ring mit Eins und $\chi : \mathbb{Z} \to R$ der eindeutig bestimmte Ringhomomorphismus mit der Eigenschaft $\chi(1_\mathbb{Z}) = 1_R$. Nach Lemma 68 (i) ist $\ker \chi$ ein Ideal von $\mathbb{Z}$ und wegen Satz 59 gibt es ein (ebenfalls eindeutig bestimmtes) $m \in \mathbb{Z}$, $m \geq 0$ mit der Eigenschaft $\ker \chi = (m)$. Dieses m wird die Charakteristik von R genannt und man schreibt dafür $\operatorname{char} R$.

Beispiele: 1) Ist $m \in \mathbb{N} \setminus \{0, 1\}$, so ist $\operatorname{char} \mathbb{Z}_m = m$, denn: Für $R = \mathbb{Z}_m$ hat χ die Form $\chi(n) = n \cdot \overline{1} = \overline{n}$, wobei $\overline{a}$ die Restklasse von a modulo m bezeichnet (für $a \in \mathbb{Z}$). Daher ist

$$n \in \ker \chi \Leftrightarrow \overline{n} = \overline{0} \Leftrightarrow n \equiv 0 \pmod m \Leftrightarrow m \mid n \Leftrightarrow n \in (m).$$

Insbesondere gilt: Ist p eine Primzahl, so ist $\operatorname{char} \mathbb{Z}_p = p$.

2) $\operatorname{char} \mathbb{Z} = 0$, da $n \cdot 1 = 0$ zu $n = 0$ äquivalent ist.

3) Ist $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, so ist $\operatorname{char} \mathbb{Z}\big[\sqrt{d}\big] = 0$. Insbesondere ist $\operatorname{char} \mathbb{Z}[i] = 0$ und $\operatorname{char} \mathbb{Z}\big[\sqrt{2}\big] = 0$.

4) $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

5) Ist $R = \{0\}$, so ist $\operatorname{char} R = 1$, da $1_R = 0_R$ und daher $\chi(n) = n \cdot 1_R = n \cdot 0_R = 0_R$ für alle $n \in \mathbb{Z}$ und somit $\ker \chi = \mathbb{Z} = (1)$. Tatsächlich ist $R = \{0\}$ der einzige Ring mit Eins, dessen Charakteristik $\operatorname{char} R = 1$ ist, da daraus $\ker \chi = (1) = \mathbb{Z}$ folgt. Das impliziert $1_\mathbb{Z} \in \ker \chi$ und daher $1_R = 1_\mathbb{Z} \cdot 1_R = 0_R$. Daraus folgt $R = \{0\}$, wie wir in Beispiel 11 am Beginn von Kapitel 7 gezeigt haben.

Lemma 86: Es sei R ein Ring mit Eins und S ein Unterring von R, der ein Ring mit Eins ist und $1_S = 1_R$ erfüllt. Dann gilt $\operatorname{char} S = \operatorname{char} R$.

Beweis: Es seien $\chi_R : \mathbb{Z} \to R$, $\chi_R(n) = n \cdot 1_R$ und $\chi_S : \mathbb{Z} \to S$, $\chi_S(n) = n \cdot 1_S$. Wegen $\chi_R(n) = n \cdot 1_R = n \cdot 1_S = \chi_S(n)$ (und $0_R = 0_S$) ist

$$n \in \ker \chi_R \Leftrightarrow n \cdot 1_R = 0_R \Leftrightarrow n \cdot 1_S = 0_S \Leftrightarrow n \in \ker \chi_S$$

und daher $\ker \chi_R = \ker \chi_S$, woraus sofort $\operatorname{char} R = \operatorname{char} S$ folgt.

Bemerkung: Die Aussage des letzten Lemmas ist ohne die Voraussetzung $1_R = 1_S$ falsch. Das sieht man z.B. am Ring $R = \mathbb{Z}_2 \times \mathbb{Z}_3$ der Charakteristik $\operatorname{char} R = 6$ besitzt, denn

$$n \in \ker \chi \Leftrightarrow n \cdot 1_R = 0_R \Leftrightarrow 2 \mid n \wedge 3 \mid n \Leftrightarrow 6 \mid n \Leftrightarrow n \in (6).$$

Der Ring R enthält die beiden Unterringe $S_1 = \{(x, 0) \mid x \in \mathbb{Z}_2\}$ und $S_2 = \{(0, y) \mid y \in \mathbb{Z}_3\}$, die offenbar $S_1 \cong \mathbb{Z}_2$ und $S_2 \cong \mathbb{Z}_3$ erfüllen und daher Charakteristik $\operatorname{char} S_1 = 2$ und $\operatorname{char} S_2 = 3$ besitzen.

Definition: Es seien K und L Körper und K ein Unterring von L. Dann sagt man stattdessen, K sei ein Teilkörper von L.

Korollar 87: Sind K und L Körper und K ein Teilkörper von L, so ist $\operatorname{char} K = \operatorname{char} L$.

Beweis: Nach Lemma 53 gilt $1_K = 1_L$. Die Behauptung folgt sofort aus Lemma 86.

Satz 88: Es sei R ein Ring mit Eins. Dann sind äquivalent:

(i) $\operatorname{char} R = 0$,
(ii) $n \cdot 1_R = 0_R \Leftrightarrow n = 0_{\mathbb{Z}}$ (für $n \in \mathbb{Z}$).

Beweis: $\operatorname{char} R = 0 \Leftrightarrow \ker \chi = (0) \Leftrightarrow \{n \in \mathbb{Z} \mid n \cdot 1_R = 0_R\} = \{0_{\mathbb{Z}}\}$.

Satz 89: Es sei R ein Ring mit Eins und $\operatorname{char} R > 0$. Dann gelten:

(i) $\operatorname{char} R = \min\{k \in \mathbb{Z} \mid k \geq 1, k \cdot 1_R = 0_R\}$,
(ii) Ist R ein Integritätsbereich, so ist $\operatorname{char} R$ eine Primzahl.

Beweis: (i) Ist $m := \operatorname{char} R \geq 1$, so ist $m \in \ker \chi$ und daher $m \cdot 1_R = \chi(m) = 0_R$. Ist $k \in \mathbb{Z}$, $k \geq 1$ mit $k \cdot 1_R = 0_R$, so ist $\chi(k) = 0_R \Rightarrow k \in \ker \chi = (m) \Rightarrow m \mid k \Rightarrow m \leq k$.

(ii) Da R ein Integritätsbereich ist, ist $R \neq \{0\}$ und daher $\operatorname{char} R \geq 2$. Angenommen, $\operatorname{char} R$ wäre keine Primzahl. Dann gäbe es $k, \ell \in \mathbb{N}$ mit $1 < k, \ell < \operatorname{char} R$ und $\operatorname{char} R = k\ell$. Dann wäre

$$0_R = \operatorname{char} R \cdot 1_R = (k \cdot \ell) \cdot 1_R = (k \cdot 1_R) \cdot (\ell \cdot 1_R)$$

und daher $k \cdot 1_R = 0_R$ oder $\ell \cdot 1_R = 0_R$, was der in (i) bewiesenen Minimalität widersprechen würde.

Korollar 90: Ist K ein Körper, so ist entweder $\operatorname{char} K = 0$ oder $\operatorname{char} K$ ist eine Primzahl.

Beweis: Folgt sofort aus Satz 89 (ii).

Satz 91: Sind R ein Integritätsbereich, K ein Körper und $\varphi : R \to K$ ein Ringmonomorphismus, so existiert ein eindeutig bestimmter Ringmonomorphismus $\overline{\varphi} : Q(R) \to K$, der φ auf den Quotientenkörper $Q(R)$ von R fortsetzt, d.h. $\overline{\varphi}\left(\frac{a}{1}\right) = \varphi(a) \, \forall a \in R$.

Beweis: Eindeutigkeit: Wegen Lemma 63 (ii) gilt $\varphi(1_R) = 1_K$. Erfüllt $\overline{\varphi} : Q(R) \to K$ alle gestellten Bedingungen, so folgt für $b \in R \setminus \{0\}$, dass

$$1_K = \varphi(1_R) = \overline{\varphi}\Big(\frac{1_R}{1_R}\Big) = \overline{\varphi}\Big(\frac{b}{b}\Big) = \overline{\varphi}\Big(\frac{b}{1}\cdot\frac{1}{b}\Big) = \overline{\varphi}\Big(\frac{b}{1}\Big)\cdot\overline{\varphi}\Big(\frac{1}{b}\Big) = \varphi(b)\cdot\overline{\varphi}\Big(\frac{1}{b}\Big),$$

woraus $\overline{\varphi}\big(\frac{1}{b}\big) = \varphi(b)^{-1}$ folgt. Für $a, b \in R$, $b \neq 0$ muss daher

$$\overline{\varphi}\Big(\frac{a}{b}\Big) = \overline{\varphi}\Big(\frac{a}{1}\cdot\frac{1}{b}\Big) = \overline{\varphi}\Big(\frac{a}{1}\Big)\cdot\overline{\varphi}\Big(\frac{1}{b}\Big) = \varphi(a)\varphi(b)^{-1}$$

gelten.

Existenz: Wir überprüfen, dass $\overline{\varphi} : Q(R) \to K$, $\overline{\varphi}\big(\frac{a}{b}\big) = \varphi(a)\varphi(b)^{-1}$ ein Ringhomomorphismus ist, der alle gestellten Bedingungen erfüllt. Zunächst ist $\overline{\varphi}$ wohldefiniert, da

$$\frac{a}{b} = \frac{c}{d} \;\Rightarrow\; ad = bc \;\Rightarrow\; \varphi(a)\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\varphi(c)$$

und daher

$$\overline{\varphi}\Big(\frac{a}{b}\Big) = \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1} = \overline{\varphi}\Big(\frac{c}{d}\Big).$$

Die Abbildung $\overline{\varphi}$ ist ein Ringhomomorphismus, da

$$\begin{aligned}\overline{\varphi}\Big(\frac{a}{b}+\frac{c}{d}\Big) &= \overline{\varphi}\Big(\frac{ad+bc}{bd}\Big) = \varphi(ad+bc)\varphi(bd)^{-1} = \big(\varphi(a)\varphi(d)+\varphi(b)\varphi(c)\big)\big(\varphi(b)\varphi(d)\big)^{-1}\\ &= \big(\varphi(a)\varphi(d)+\varphi(b)\varphi(c)\big)\varphi(b)^{-1}\varphi(d)^{-1} = \varphi(a)\varphi(b)^{-1}+\varphi(c)\varphi(d)^{-1} = \overline{\varphi}\Big(\frac{a}{b}\Big)+\overline{\varphi}\Big(\frac{c}{d}\Big)\end{aligned}$$

und

$$\overline{\varphi}\Big(\frac{a}{b}\cdot\frac{c}{d}\Big) = \overline{\varphi}\Big(\frac{ac}{bd}\Big) = \varphi(ac)\varphi(bd)^{-1} = \varphi(a)\varphi(b)^{-1}\cdot\varphi(c)\varphi(d)^{-1} = \overline{\varphi}\Big(\frac{a}{b}\Big)\cdot\overline{\varphi}\Big(\frac{c}{d}\Big)$$

und $\overline{\varphi}$ ist injektiv, da

$$\overline{\varphi}\Big(\frac{a}{b}\Big) = \overline{\varphi}\Big(\frac{c}{d}\Big) \;\Rightarrow\; \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1} \;\Rightarrow\; \varphi(ad) = \varphi(a)\varphi(d) = \varphi(b)\varphi(c) = \varphi(bc),$$

woraus $ad = bc$ und daher $\frac{a}{b} = \frac{c}{d}$ folgt. Schließlich gilt

$$\overline{\varphi}\Big(\frac{a}{1}\Big) = \varphi(a)\varphi(1_R)^{-1} = \varphi(a)\cdot 1_K^{-1} = \varphi(a)\;\forall a \in R,$$

d.h. $\overline{\varphi}$ setzt φ auf $Q(R)$ fort.

Korollar 92: Es sei K ein Körper.
(i) Ist $\operatorname{char} K = 0$, so enthält K einen zu $(\mathbb{Q}, +, \cdot)$ isomorphen Teilköper.
(ii) Ist $\operatorname{char} K = p > 0$, so enthält K einen zu $(\mathbb{Z}_p, +, \cdot)$ isomorphen Teilkörper.

Beweis: Betrachte den Ringhomomorphismus $\chi : \mathbb{Z} \to K$, $\chi(n) = n \cdot 1_K$.
(i) Ist $\operatorname{char} K = 0$, so ist nach Definition $\ker \chi = (0)$ und χ daher nach Lemma 68 (ii) injektiv. Also enthält K (nach Lemma 67 (i)) den Unterring $\operatorname{Im} \chi \cong \mathbb{Z}$ und nach Satz 91 daher einen zu $\operatorname{Im} \overline{\chi} \cong Q(\mathbb{Z}) = \mathbb{Q}$ isomorphen Teilkörper (wobei $\overline{\chi} : \mathbb{Q} \to K$ die eindeutig bestimmte Fortsetzung von χ bezeichnen soll, deren Existenz in Satz 91 bewiesen wurde).
(ii) Ist $\operatorname{char} K = p > 0$, so ist nach Korollar 90 $\ker \chi = (p)$ ein maximales Ideal von $\mathbb{Z}$ und wegen Korollar 70 und Satz 77 enthält K den Teilkörper $\operatorname{Im} \chi \cong \mathbb{Z}/\ker \chi = \mathbb{Z}/(p) = \mathbb{Z}_p$.

Definition: Es sei K ein Körper. Der zu $\mathbb{Q}$ (im Fall $\operatorname{char} K = 0$) bzw. $\mathbb{Z}_p$ (im Fall $\operatorname{char} K = p > 0$) isomorphe Teilkörper von K, dessen Existenz in Korollar 92 bewiesen wurde, wird als Primkörper von K bezeichnet.

Bemerkung: Der Primkörper eines Körpers K ist der kleinste in K enthaltenen Teilkörper. Jeder Teilkörper eines Körpers K muss offenbar die Menge

$$\{n \cdot 1_K \mid n \in \mathbb{Z}\} = \{\chi(n) \mid n \in \mathbb{Z}\} = \operatorname{Im} \chi$$

enthalten. Im Fall $\operatorname{char} K > 0$ handelt sich dabei nach Korollar 92 (ii) bereits um den Primkörper von K. Ist $\operatorname{char} K = 0$, muss jeder Teilkörper von K die Menge

$$\{(n \cdot 1_K) \cdot (\ell \cdot 1_K)^{-1} \mid n, \ell \in \mathbb{Z}, \ell \neq 0\} = \{\chi(n) \cdot \chi(\ell)^{-1} \mid n, \ell \in \mathbb{Z}, \ell \neq 0\}$$

enthalten, die in diesem Fall nach dem Beweis von Satz 91 und Korollar 92 (i) der Primkörper von K ist.