§14 Körper

(14.1) DEF: Ein kommutativer Ring $(K,+,\cdot)$ heißt ein **Körper**, wenn gilt:

1) $1_K \neq 0_K$ **2)** $K^\star = K \setminus \{0_K\}$

(14.2) BEM: **a)** Ist K ein Körper, so ist $(K \setminus \{0_K\},\cdot)$ eine Gruppe.

b) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.

c) $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$ sind (endliche) Körper.

d) Jeder Unterring eines Körpers ist nullteilerfrei. Insbesondere ist jeder Körper nullteilerfrei.

e) Ein **Schiefkörper** ist ein nicht notwendig kommutativer Ring S mit $1_S \neq 0_S$ und $S^\star = S\setminus\{0_S\}$. Ein Beispiel für einen Schiefkörper ist

$$\mathbb{H} := \left\{ \begin{pmatrix} w & z \\ -\overline{z} & \overline{w} \end{pmatrix} \;\middle|\; w, z \in \mathbb{C} \right\} \subseteq \mathrm{M}_2(\mathbb{C}).$$

Dieser sog. Schiefkörper der Hamiltonschen Quaternionen ist nichtkommutativ.

Nach einem Satz von Wedderburn aus dem Jahre 1905 ist jeder endliche Schiefkörper kommutativ.

(14.3) SATZ: Für $n \in \mathbb{N}, n \geq 1$, sind folgende Aussagen äquivalent:

a) Der Ring $\mathbb{Z}_n$ ist ein Körper

b) Der Ring $\mathbb{Z}_n$ ist ein IB

c) n ist eine Primzahl.

(14.4) DEF: Sei K ein Körper. Eine Unterring $U \subseteq K$ heißt ein **Unterkörper** von K, wenn gilt: $\forall\, x \in U \setminus \{0_K\} \,:\, x^{-1} \in U$

BEM: Ein Unterkörper $U \subseteq K$ ist für sich betrachtet wieder ein Körper. Seine Verknüpfungen sind die Einschränkungen der Verknüpfungen von K auf U.

Beispiele: $\mathbb{Q}$ ist ein Unterkörper von $\mathbb{R}$, $\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$.

(14.5) LEMMA: Für einen kommutativen Ring $R \neq 0$ sind folgende Aussagen äquivalent:

a) R ist ein Körper

b) 0 und R sind die einzigen Ideale in R.

Fazit: Faktorringbildungen sind bei Körpern uninteressant! Es gibt nur die Fälle $K/0 \cong K$ und $K/K \cong 0$.

BEM: Auch Produktbildungen sind bei Körpern uninteressant, da das Produkt zweier Körper nie mehr ein Körper sein kann.

(14.6) DEF: Ein Ringhomomorphismus zwischen zwei Körpern heißt ein **Körperhomomorphismus**. Ein bijektiver Körperhomomorphismus heißt ein **Körperisomorphismus**.

(14.7) LEMMA: Jeder Körperhomomorphismus ist injektiv.

Endliche Körper

(14.8) LEMMA: K sei ein endlicher Körper. Dann gibt es eine Primzahl p (die sog. **Charakteristik** von K), für die gilt:

a) $p\,1_K \;=\; 0_K$

b) K enthält einen kleinsten Unterkörper U (den sog. **Primkörper** von K) mit $U \cong \mathbb{Z}_p$.

Bew: Nach Voraussetzung ist $(K,+)$ eine endliche abelsche Gruppe, in der daher jedes Element endliche Ordnung hat. Sei $p := \operatorname{ord}(1_K)$. Dann gilt

$$p1_K = 0_K$$

und p ist die kleinste der positiven Zahlen m mit $m\,1_K = 0_K$. ($m\,1_K$ ist die m–te Potenz von 1_K in der Gruppe $(K,+)$) . Wir betrachten die Abbildung

$$\alpha : \mathbb{Z} \longrightarrow K \quad \text{definiert durch} \quad \alpha(k) := k\,1_K \quad (k \in \mathbb{Z})$$

α ist ein Ringhomomorphismus mit $\operatorname{Bild}(\alpha) = \langle 1_K \rangle \subseteq K$. Wir bestimmen den Kern von α:

$\alpha(p) = p\,1_K = 0_K \quad \Longrightarrow \quad p \in \operatorname{Kern}(\alpha) \quad \Longrightarrow \quad \mathbb{Z}p \subseteq \operatorname{Kern}(\alpha)$

$k \in \operatorname{Kern}(\alpha) \quad \Longrightarrow \quad k\,1_K = 0_K \quad \overset{(4.20d)}{\Longrightarrow} \quad p|k \quad \Longrightarrow \quad k \in \mathbb{Z}p$. Also

$$\operatorname{Kern}(\alpha) = \mathbb{Z}p \quad \text{mit} \quad p = \operatorname{ord}(1_K)$$

Nach dem Homomorphiesatz für Ringe (13.14) gibt es eine Ringisomorphie

$$\mathbb{Z}_p = \mathbb{Z}/\operatorname{Kern}(\alpha) \;\cong\; \operatorname{Bild}(\alpha) \subseteq K$$

Als Unterring eines Körpers ist $\operatorname{Bild}(\alpha)$ nullteilerfrei, so daß auch der dazu isomorphe Ring $\mathbb{Z}_p$ nullteilerfrei, also ein IB ist. Nach (14.3) ist dann p eine Primzahl. Sei $U := \operatorname{Bild}(\alpha) = \langle 1_K \rangle$. Wegen $U \cong \mathbb{Z}_p$ (Ringisomorphie) ist dann U ein Unterkörper von K. Ist nun V ein beliebiger Unterkörper von K, so gilt $1_K \in V$ und damit $\langle 1_K \rangle \subseteq V$, da insbesondere $V \leq (K,+)$. Damit ist alles bewiesen. •

(14.9) SATZ: Ist K ein endlicher Körper, so gibt es eine Primzahl p und ein $n \in \mathbb{N}$ mit

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

Bew: Nach (14.8) gibt es eine Primzahl p, so daß K einen Unterkörper U mit p Elementen enthält. (U ist ein Körper!) K läßt sich als Vektorraum über U auffassen. Als solcher ist K endlich erzeugbar (K ist eine endliche Menge!) und damit endlich–dimensional. Sei $n := \dim_U(K)$. Dann folgt

$$K \cong U^n \quad\Longrightarrow\quad |K| = |U^n| = |U|^n = p^n\,.$$

Polynomringe über Körpern

Wir konstruieren endliche Körper als Faktorringe geeigneter Polynomringe über Körpern. Ist K ein Körper, so besitzt der Polynomring in einer Unbestimmten über K zusätzliche Eigenschaften. Zunächst sei erwähnt, daß $K[T]$ durch die in 10.) zum Beweis von (13.20) definierte skalare Multiplikation zu einem unendlich–dimensionalen K–Vektorraum mit $\{T^0, T^1, T^2, \ldots\}$ als Basis wird.

(14.10) SATZ: Ist K ein Körper, so ist $K[T]$ ein HIB .

Bew: Ist $I \neq 0$ ein Ideal von $K[T]$, so ist die Menge der Grade aller Polynome aus $I \setminus \{0\}$ eine nichtleere Teilmenge von $\mathbb{N}_0$, die ein kleinstes Element m enthält. Sei $g \in I \setminus \{0\}$ ein Polynom vom Grade m. Dann gilt $K[T]g = (g) \subseteq I$ wegen der Idealeigenschaft von I. Ist umgekehrt $h \in I$ beliebig, so ergibt Division mit Rest $h = qg + r$ mit $r = 0$ oder $\mathrm{grad}(r) < \mathrm{grad}(g) = m$. Wäre $r \neq 0$, so hätte man mit $r = h - qg \in I \setminus \{0\}$ (I ist ein Ideal!) ein Polynom vom Grade $< m$ in I, was der Wahl von m widerspricht. Also folgt $r = 0$ und daraus $h = qg \in (g)$, womit $I \subseteq (g)$ gezeigt ist. Insgesamt gilt also $I = (g)$, wobei g ein Polynom kleinsten Grades in $I \setminus \{0\}$ ist. •

BEM: Dieser Beweis verläuft analog zum Nachweis von (2.11), wo gezeigt wird, daß jede Untergruppe von $(\mathbb{Z}, +)$ zyklisch ist.

(14.11) DEF: **a)** Sei K ein Körper. Sind $f, g \in K[T]$, so heißt f ein Teiler von g (in Zeichen: $f|g$) , wenn es ein Polynom $h \in K[T]$ gibt mit $g = fh$.

b) Seien $f_1, f_2 \in K[T]$. Ein Polynom $g \in K[T]$ heißt ein **größter gemeinsamer Teiler (ggT)** von f_1 und f_2, wenn gilt:

i) $g|\,f_1$ und $g|\,f_2$ **ii)** $\forall\, h \in K[T] \;:\; h|\,f_1 \wedge h|\,f_2 \;\Longrightarrow\; h|\,g$

(14.12) SATZ: K sei ein Körper. Zu je zwei Polynomen $f_1, f_2 \in K[T]$ existiert ein ggT g, der bis auf Multiplikation mit einer Einheit eindeutig bestimmt ist. Außerdem gibt es Polynome $h_1, h_2 \in K[T]$ mit

$$g \;=\; h_1 \cdot f_1 + h_2 \cdot f_2$$

(14.13) BEM: Da in $K[T]$ Division mit Rest möglich ist, läßt sich ein ggT zweier Polynome mit Hilfe des euklidischen Algorithmus berechnen.

Primzahlen sind ganze Zahlen ≥ 2, die keine echten Teiler haben. Wichtig ist der Satz über die PFZ. Wir werden sehen, daß wir diese Ergebnisse auf Polynomringe übertragen können .

(14.14) DEF: Sei K ein Körper. Ein Polynom $f \in K[T]$ vom Grade ≥ 1 heißt **irreduzibel (über K)**, wenn gilt

$$\forall\, g \in K[T] \,:\, g|f \quad \Longrightarrow \quad \operatorname{grad}(g) = 0 \;\text{ oder }\; \operatorname{grad}(g) = \operatorname{grad}(f)\,.$$

BEM: **a)** $g|f$ und $\operatorname{grad}(g) = \operatorname{grad}(f)$ bedeutet: es gibt ein $a \in K^\star$ mit $f = ag$.

b) Jedes lineare Polynom ist irreduzibel.

c) Ein Polynom $f \in K[T]$ vom Grade 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in K besitzt.

d) Das Polynom $T^2 + 1$ ist irreduzibel über $\mathbb{R}$, aber reduzibel über $\mathbb{C}$.

(14.15) SATZ: Sei K ein Körper. Dann läßt sich jedes Polynom aus $K[T]$ vom Grade ≥ 1 als Produkt von (endlich vielen) irreduziblen Polynomen darstellen. Diese Darstellung ist eindeutig bis auf die Reihenfolge und Multiplikation mit Einheiten.

Bew: Die Existenz läßt sich leicht durch Induktion nach $m := \operatorname{grad}(f) \geq 1$ zeigen:

(IA) Im Falle $m = 1$ ist f irreduzibel, also Produkt aus einem Faktor.

(IV) Sei $m > 1$ beliebig und die Behauptung richtig für alle Polynome vom Grade $< m$

(IB) Jedes Polymom $f \in K[T]$ vom Grade m ist Produkt von irreduziblen Polynomen:

1. Fall: f ist irreduzibel. Dann sind wir wieder fertig.

2. Fall: f ist reduzibel. Dann ist $f = g \cdot h$ Produkt zweier Polynome vom Grade $< m$. Nach (IV) sind dann aber g und h jeweils Produkte von irreduziblen Polynomen, was damit auch für $f = g \cdot h$ gilt. •

(14.16) SATZ: K sei ein Körper, $f \in K[T]$ ein irreduzibles Polynom vom Grade n und

$$L := K[T]/(f)\,.$$

Dann gilt:

a) L ist ein Körper.

b) $L = \{\, [r] \mid r \in K[T]\,,\, r = 0 \text{ oder } \operatorname{grad}(r) < n \,\}$.

Bew: **a) Bew:** L ist ein kommutativer Ring. Es ist $K[T]f = (f) \neq K[T]$, da sonst aus $1 \in (f)$ die Existenz von $g \in K[T]$ mit $1 = gf$ folgen würde, woraus sich der Widerspruch $\operatorname{grad}(f) = 0$ ergeben würde. Aus $L \neq 0$ folgt dann $1_L \neq 0_L$. Bleibt zu zeigen, daß jedes Element aus $L \backslash \{0_L\}$ invertierbar bzgl. der Multiplikation ist. Sei also $g \in K[T]$ beliebig mit $[g] = g + (f) \neq [0]$. Dann folgt $g \notin (f)$, also $f \nmid g$.
Sei h ein ggT von f und g. Da f irreduzibel ist, folgt $h \in K^\star$. Nach (14.12) existieren Polynome r, s mit $h = rf + sg \implies 1 = (h^{-1}r)f + (h^{-1}s)g = r_1 f + s_1 g$. Der Übergang zu den Nebenklassen nach (f) liefert

$$[1] = [r_1 f + s_1 g] = \underbrace{[r_1 f]}_{=[0]} + [s_1 g] = [s_1] \cdot [g]$$

d.h. $[s_1]$ ist Inverses zu $[g]$.

b) Setze $V := \{ r \mid r \in K[T] \, , \, r = 0 \text{ oder } \operatorname{grad}(r) < n \} \subseteq K[T]$. Sei h ein beliebiges Polynom aus $K[T]$. Nach (13.24) gibt es dann $q, r \in K[T]$ mit $h = qf + r$, wobei $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(f) = n$ gilt, d.h. $r \in V$. In L folgt dann

$$[h] \; = \; [qf + r] \; = \; \underbrace{[qf]}_{=[0]} + [r] \; = \; [r] \;\; \text{mit} \;\; r \in V$$

Damit ist gezeigt: $\forall \, h \in K[T] \, \exists \, r \in V : [h] = [r]$. Außerdem folgt leicht:
$\forall \, g_1, g_2 \in V : [g_1] = [g_2] \implies g_1 = g_2$. Damit ist dann die Behauptung bewiesen.
V enthält also aus jeder Nebenklasse nach (f) genau ein Element. Man nennt V daher auch ein **vollständiges Vertretersystem für** L . •

(14.17) BEISPIEL: $\mathbb{R}[T]/(T^2+1)$ ist ein Körper, in dem $[T]^2 = -[1]$ gilt.

Das Polynom $f := T^2+1$ ist irreduzibel über $\mathbb{R}$, so daß $L := \mathbb{R}[T]/(f)$ nach (14.16a) ein Körper ist. Nach (14.16b) ist $V = \{0\} \cup \{g | g \in \mathbb{R}[T], \operatorname{grad}(g) < 2\} \; = \; \{a + bT | a, b \in \mathbb{R}\}$ ein vollständiges Vertretersystem für L. Dies erinnert stark an die arithmetische Darstellung von komplexen Zahlen, und es gilt in L

$$[0] \; = \; [T^2+1] \; = [T^2] + [1] \; = \; [T]^2 + [1] \;\; \Longrightarrow \;\; [T]^2 = -[1]$$

In der Tat gilt $\mathbb{R}[T]/(T^2+1) \cong \mathbb{C}$, was man leicht mit Hilfe des Ringhomomorphiesatzes beweisen kann.

(14.18) SATZ: Sei p eine Primzahl und $f \in \mathbb{Z}_p[T]$ ein irreduzibles Polynom vom Grade n . Dann ist der Faktorring

$$L := \mathbb{Z}_p[T]/(f)$$

ein Körper mit p^n Elementen.

Bew: Nach (14.16) ist $L := \mathbb{Z}_p[T]/(f)$ ein Körper, und es ist

$$V := \{0\} \cup \{g \mid g \in \mathbb{Z}_p[T], \operatorname{grad}(g) < n\}$$

ein vollständiges Vertretersystem für L, so daß $|L| = |V|$ gilt. Wir müssen also die Elemente von V abzählen.
Für beliebiges $k \in \mathbb{N}_0$ bezeichne $a(k, p)$ die Anzahl der Polynome aus $\mathbb{Z}_p[T]$, die den Grad k haben. Ein solches Polynom f ist von der Form

$$f \; = \; a_0 + a_1 T + a_2 T^2 + \ldots + a_{k-1} T^{k-1} + a_k T^k \quad (a_k \neq 0)$$

wobei a_l für $l \in \{0, 1, \ldots, k-1\}$ ein beliebiges Element aus $\mathbb{Z}_p$ ist und $a_k \in \mathbb{Z}_p^\star$. f ist also eindeutig durch das $(k+1)$–Tupel

$$(a_0, a_1, a_2, \ldots, a_{k-1}, a_k) \in \mathbb{Z}_p^k \times \mathbb{Z}_p^\star$$

bestimmt, d.h.

$$a(k, p) \; = \; |\mathbb{Z}_p^k \times \mathbb{Z}_p^\star| \; = \; p^k(p-1).$$

Damit gilt für die Anzahl A aller Polynome $\neq 0$ vom Grade $< n$

$$A = \sum_{k=0}^{n-1} a(k,p) = \sum_{k=0}^{n-1} p^k(p-1) = (p-1)\sum_{k=0}^{n-1} p^k = (p-1)\frac{p^n-1}{p-1} = p^n - 1$$

Berücksichtigt man noch das Nullpolynom, so folgt

$$\underline{\underline{|L|}} = |V| = A+1 = (p^n-1)+1 = \underline{\underline{p^n}}.$$

•

(14.19) BEM: **a)** Man kann beweisen, daß es zu jedem $n \in \mathbb{N}$ ein in $\mathbb{Z}_p[T]$ ein irreduzibles Polynom vom Grade n gibt .

b) Zu jeder Primzahl p und jeder natürlichen Zahl $n \geq 1$ gibt es einen Körper mit p^n Elementen.

c) Man kann zeigen, daß je zwei endliche Körper mit gleichviel Elementen isomorph zueinander sind.

(14.20) BEISPIEL: $K := \mathbb{Z}_2[T]/(T^2+T+1)$ ist ein Körper mit $2^2 = 4$ Elementen.

Das Polynom $f = T^2+T+1 \in \mathbb{Z}_2[T]$ ist irreduzibel, da f den Grad 2 hat und keine Nullstelle in $\mathbb{Z}_2$ besitzt ($f(0) = 0+0+1 = 1 \neq 0$, $f(1) = 1+1+1 = 1 \neq 0$). Also ist K nach (14.18) ein Körper mit $2^2 = 4$ Elementen. Ein vollständiges Vertretersystem V von K wird nach (14.16) gebildet aus 0 und allen Polynomen aus $\mathbb{Z}_2[T]$ vom Grade < 2, das sind $1, T, T+1$. Folglich $V := \{0, 1, T, T+1\}$. Da K die Charakteristik 2 besitzt, gilt $2\,(=1+1) = 0$ in K und $x = -x \;\forall\, x \in K$. Außerdem ist $[T^2+T+1] = [0]$, d.h. $[T^2] = -[T+1] = [T+1]$. In den folgenden Verknüpfungstafeln sind jeweils nur die Elemente aus V angegeben, genaugenommen sind natürlich die Restklassen dieser Elemente nach (f) zu bilden.

Additionstafel

Beispiel: $(T+1)+T = 2T+1 = 0+1 = 1$

$+$	0	1	T	$T+1$
0	0	1	T	$T+1$
1	1	0	$T+1$	T
T	T	$T+1$	0	1
$T+1$	$T+1$	T	1	0

Multiplikationstafel

Beispiel: $(T+1)(T+1) = T^2+2T+1 = (T^2+T+1)+T = 0+T = T$

$\cdot$	0	1	T	$T+1$
0	0	0	0	0
1	0	1	T	$T+1$
T	0	T	$T+1$	1
$T+1$	0	$T+1$	1	T