Kapitel 6

Körpertheorie

6.1 Quotientenkörper eines Integritätsbereiches

6.1.A Quotientenhalbgruppe

Sei $\mathfrak{M} = (M, \cdot, 1)$ ein kommutatives Monoid, dann heißt ein Element $a \in M$ *kürzbar* (*regulär*) $:\Leftrightarrow \forall x, y \in M : ax = ay \Rightarrow x = y$. $R(\mathfrak{M})$ sei die Menge aller kürzbaren Elemente von $\mathfrak{M}$. Wegen $1 \in R(\mathfrak{M})$ ist $R(\mathfrak{M}) \neq \emptyset$.

In vielen wichtigen Fällen ist $R(\mathfrak{M}) = M$.

6.1.1 Beispiele. 1) $\mathfrak{M} = (\mathbb{N}_0, +, 0)$.

2) $\mathfrak{M} = (\mathbb{Z} \setminus \{0\}, \cdot, 1)$.

3) $\mathfrak{M} = (I \setminus \{0\}, \cdot, 1)$, I Integritätsbereich.

Sei $S := M \times R(\mathfrak{M}) = \{(a, b) \mid a \in M,\ b \in R(\mathfrak{M})\}$ und $\sim$ auf S definiert durch

$$(a, b) \sim (c, d) :\Leftrightarrow ad = bc, \quad a, c \in M,\ b, d \in R(\mathfrak{M}).$$

Dann ist $\sim$ eine Äquivalenzrelation auf S (reflexiv, symmetrisch: klar; transitiv: $(a, b) \sim (c, d) \sim (e, f) \Rightarrow ad = bc$ und $cf = ed \Rightarrow adf = bcf = bed \Rightarrow af = be \Rightarrow (a, b) \sim (e, f)$).

Wir setzen $S/\sim =: S_1$, $[(a, b)]_\sim =: \frac{a}{b}$, $a \in M$, $b \in R(\mathfrak{M})$, und definieren

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}, \qquad \frac{a}{b}, \frac{c}{d} \in S_1.$$

Die Operation $\cdot$ (auf S_1) ist wohldefiniert, denn: 1) $bd \in R(\mathfrak{M})$, da $b, d \in R(\mathfrak{M})$, 2) $(a, b) \sim (a_1, b_1)$ und $(c, d) \sim (c_1, d_1) \Rightarrow (ac, bd) \sim (a_1c_1, b_1d_1)$ (Übungsbeispiel 97). Weiters sei $1 := \frac{1}{1}$. Damit ist $(S_1, \cdot, 1)$ ein kommutatives Monoid.

Die Abbildung

$$\begin{cases} M \to S_1 \\ a \mapsto \frac{a}{1} \end{cases}$$

ist ein injektiver Homomorphismus (d.h. ein Monomorphismus) von $\mathfrak{M}$ in $(S_1, \cdot, 1)$. Nach dem Prinzip der isomorphen Einbettung erhalten wir damit ein kommutatives Monoid $\mathfrak{T} = (T, \cdot, 1) \cong (S_1, \cdot, 1)$, sodass $\mathfrak{M}$ Unteralgebra von $\mathfrak{T}$ ist. $\mathfrak{T}$ heißt *Quotientenhalbgruppe* von $\mathfrak{M}$ und hat folgende Eigenschaften (Übungsbeispiel 99):

a) Jedes $a \in R(\mathfrak{M})$ ist in $\mathfrak{T}$ invertierbar und hat das Inverse $a^{-1} = \frac{1}{a}$.

b) $E(\mathfrak{T}) = R(\mathfrak{T}) = \{\frac{a}{b} \mid a, b \in R(\mathfrak{M})\}$, und für $a, b \in R(\mathfrak{M})$ gilt: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. Dabei ist — analog zu Abschnitt 5.1 (vgl. auch Übungsbeispiel 18) — $E(\mathfrak{T})$ definiert als die Menge der invertierbaren Elemente des Monoids $\mathfrak{T}$. (Einheitengruppe von $\mathfrak{T}$)

Für $a \in M$ setzen wir dabei $a =: \frac{a}{1} =: \frac{ae}{e}$ mit $e \in R(\mathfrak{M})$ beliebig.

Es gilt nach a):

$$T = \{ab^{-1} \mid a \in M,\ b \in R(\mathfrak{M})\}.$$

6.1.B Quotientenring, Quotientenkörper

Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit Einselement $1 \neq 0$. Ein Element $a \in R$ heißt ein *Nullteiler* von $R :\Leftrightarrow \exists b \in R \setminus \{0\} : ab = 0$. Dann ist $\mathfrak{M} := (R, \cdot, 1)$ ein kommutatives Monoid, und es gilt

$$R(\mathfrak{M}) = \{a \in R \mid a \text{ ist } \textit{kein} \text{ Nullteiler von } R\}.$$

Mit der Bezeichnung von oben haben wir also $S_1 = \{\frac{a}{b} \mid a, b \in R,\ b \text{ kein Nullteiler}\}$ und definieren auf S_1 folgende weiteren Operationen:

$$\begin{aligned}
&\tfrac{a}{b} + \tfrac{c}{d} := \tfrac{ad+bc}{bd} \quad && a, b, c, d \in R,\ b, d \text{ keine Nullteiler},\\
&0 := \tfrac{0}{1},\\
&-\tfrac{a}{b} := \tfrac{-a}{b} && a, b \in R,\ b \text{ kein Nullteiler}.
\end{aligned}$$

Man kann zeigen, dass auch diese Operationen wohldefiniert sind (Übungsbeispiel 98).

Die Abbildung

$$\begin{cases} R \to S_1 \\ a \mapsto \frac{a}{1} \end{cases}$$

ist ein Monomorphismus von $(R, +, 0, -, \cdot, 1)$ in $(S_1, +, 0, -, \cdot, 1)$, und S_1 ist wieder ein kommutativer Ring mit Einselement. Nach dem Prinzip der isomorphen Einbettung erhalten wir damit einen kommutativen Ring mit Einselement $(T, +, 0, -, \cdot, 1) \cong (S_1, +, 0, -, \cdot, 1)$ mit folgenden Eigenschaften:

a) $(R, +, 0, -, \cdot, 1)$ ist Unteralgebra von $(T, +, 0, -, \cdot, 1)$.

b) Jedes $a \in R$, welches kein Nullteiler ist, ist in T invertierbar und hat das Inverse $a^{-1} = \frac{1}{a}$.

c) $T = \{ab^{-1} \mid a, b \in R, b \text{ kein Nullteiler}\}$.

d) In $(T, \cdot, 1)$ sind genau die Elemente $\frac{a}{b}$ invertierbar, bei denen a, b beide keine Nullteiler sind, und es gilt $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Spezialfall: Ist R ein Integritätsbereich, dann ist $(T, +, 0, -, \cdot, 1)$ ein Körper, genannt der *Quotientenkörper* von R.

6.1.2 Beispiele. 1) Die Quotientenhalbgruppe von $(\mathbb{N}_0, +, 0)$ ist isomorph zu $(\mathbb{Z}, +, 0)$.

2) Der Quotientenkörper von $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist isomorph zu $(\mathbb{Q}, +, 0, -, \cdot, 1)$.

3) Ist K ein Körper, so ist der Quotientenkörper von K gleich K.

4) Der Quotientenkörper von $K[x_1, \ldots, x_n]$ (K Körper) heißt *Körper der rationalen Funktionen in $x_1, \ldots, x_n$ über K* und wird mit $K(x_1, \ldots, x_n)$ bezeichnet. Es gilt

$$K(x_1, \ldots, x_n) = \{\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \mid p, q \in K[x_1, \ldots, x_n],\ q \neq 0\},$$

insbesondere

$$K(x) = \{\frac{p(x)}{q(x)} \mid p, q \in K[x],\ q \neq 0\}.$$

6.2 Primkörper

6.2.1 Definition. Ein Körper $(K, +, 0, -, \cdot, 1)$ heißt *Primkörper*, wenn er nur sich selbst als Unterkörper besitzt.

6.2.2 Satz. *Jeder beliebige Körper besitzt stets genau einen Unterkörper, welcher Primkörper ist.*

Beweis. Sei L beliebiger Körper und $K := \bigcap\{M \subseteq L \mid M \text{ ist Unterkörper von } L\}$, d.h., K ist der kleinste Unterkörper von L. Offensichtlich ist K Primkörper. Sind $K_1, K_2 \subseteq L$ zwei Primkörper, so ist $K_1 \cap K_2$ Unterkörper von K_1 und von K_2 und daher $K_1 = K_1 \cap K_2 = K_2$. □

6.2.3 Lemma. *Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann wird durch*

$$\varphi : \mathbb{Z} \to R, \qquad n \mapsto n \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{n \text{ mal}}, & n > 0, \\ 0, & n = 0, \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ mal}}, & n < 0, \end{cases}$$

ein Homomorphismus von $(\mathbb{Z}, +, \cdot)$ nach $(R, +, \cdot)$ definiert.

Beweis. $\varphi(n+m) = (n+m)\cdot 1 = n\cdot 1 + m\cdot 1 = \varphi(n) + \varphi(m)$ (vgl. Potenzrechnung in Gruppen, Abschnitt 1.7); für $n, m > 0$ ist $\varphi(nm) = (nm) \cdot 1 = \underbrace{1 + \cdots + 1}_{nm \text{ mal}} = \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{nm \text{ mal}} = (\underbrace{1 + \cdots + 1}_{n \text{ mal}})(\underbrace{1 + \cdots + 1}_{m \text{ mal}}) = (n \cdot 1)(m \cdot 1) = \varphi(n)\varphi(m)$, alle anderen Fälle werden analog gezeigt. □

6.2.4 Folgerung. $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ ist ein kommutativer Unterring von R mit demselben Einselement 1, nämlich der von 1 erzeugte Unterring.

6.2.5 Definition. Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann ist die *Charakteristik* von R (in Zeichen: $\operatorname{char} R$) definiert durch

$$\operatorname{char} R := \begin{cases} |\{n \cdot 1 \mid n \in \mathbb{Z}\}|, & \text{falls diese Mächtigkeit endlich ist,} \\ 0 & \text{sonst.} \end{cases}$$

Sei $\mathrm{o}(1)$ die Ordnung von 1 in der abelschen Gruppe $(R, +)$ (siehe Abschnitt 1.7), dann gilt:

$$\operatorname{char} R = \begin{cases} \mathrm{o}(1), & \text{falls } \mathrm{o}(1) \in \mathbb{N}, \\ 0, & \text{falls } \mathrm{o}(1) = \infty. \end{cases}$$

6.2.6 Beispiele. 1) Für den Restklassenring $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ gilt $\operatorname{char}\mathbb{Z}_n = n$ $(n \in \mathbb{N}_0)$.

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

6.2.7 Lemma. *Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement. Dann gilt:*

a) $\forall n \in \mathbb{Z} : \Big(n \cdot 1 = 0 \Leftrightarrow \operatorname{char} R | n \Leftrightarrow n \in (\operatorname{char} R) \lhd \mathbb{Z}\Big)$.

b) $\forall a \in R : \Big(\operatorname{char} R \cdot a = 0,$ *d.h.,* $\operatorname{o}(a) | \operatorname{char} R\Big)$.

c) $\{n \cdot 1 \mid n \in \mathbb{Z}\} \cong \mathbb{Z}_m$, *wobei* $m := \operatorname{char} R$.

Beweis. a) Folgt aus 1.7.17 und 5.3.1.
b) Sei $m = \operatorname{char} R$. Für $m = 0$ ist die Aussage trivial. Für $m > 0$ gilt: $m \cdot a = \underbrace{a + \cdots + a}_{m \text{ mal}} = \underbrace{a \cdot 1 + \cdots + a \cdot 1}_{m \text{ mal}} = a \cdot (\underbrace{1 + \cdots + 1}_{m \text{ mal}}) = a \cdot 0 = 0$.
c) Wir betrachten den Homomorphismus $\varphi : \mathbb{Z} \to R$, $n \mapsto n \cdot 1$. Aus dem Homomorphiesatz 2.2.38 (in Verbindung mit 2.2.45) folgt $\varphi(\mathbb{Z}) = \{n \cdot 1 \mid n \in \mathbb{Z}\} \cong \mathbb{Z}/\ker\varphi$ und $\ker\varphi = \{n \in \mathbb{Z} \mid \varphi(n) = 0\} \overset{\text{a)}}{=} (\operatorname{char} R)$. Setzen wir $m = \operatorname{char} R$, so ist also $\varphi(\mathbb{Z}) \cong \mathbb{Z}/(m) = \mathbb{Z}_m$. □

6.2.8 Lemma. 1) *Ist R Integritätsbereich, dann ist auch $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ und damit $\mathbb{Z}_m$ mit $m = \operatorname{char} R$ Integritätsbereich, und es gilt $m = 0$ oder $m \in \mathbb{P}$ (d.h., m ist Primzahl).*

2) *Ist R Integritätsbereich und $\operatorname{char} R \in \mathbb{P}$, dann ist $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ ein Körper.*

Beweis. Nach Abschnitt 5.3 gilt: $\mathbb{Z}_m = \mathbb{Z}/(m)$ Integritätsbereich $\Leftrightarrow m = 0$ oder $m \in \mathbb{P}$; $\mathbb{Z}_m$ Körper $\Leftrightarrow m \in \mathbb{P}$. □

6.2.9 Satz. *Sei $(K, +, 0, -, \cdot, 1)$ ein Körper mit $\operatorname{char} K \in \mathbb{P}$. Dann ist $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ der Primkörper von K. In diesem Fall gilt also: Der Primkörper von K ist isomorph zu $\mathbb{Z}_m$ mit $m = \operatorname{char} K$.*

Beweis. Folgt unmittelbar aus 6.2.8. □

6.2.10 Satz. *Sei $(K, +, 0, -, \cdot, 1)$ ein Körper mit $\operatorname{char} K = 0$. Dann ist $\{\frac{n \cdot 1}{m \cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\}$ der kleinste Unterkörper und damit der Primkörper von K. Dieser Primkörper ist isomorph zu $\mathbb{Q}$. Dabei haben wir $\frac{n \cdot 1}{m \cdot 1} := (n \cdot 1)(m \cdot 1)^{-1}$ gesetzt.*

Beweis. Sei L ein Unterkörper von K. Dann gilt: $1 \in L \Rightarrow \forall n \in \mathbb{Z} : n \cdot 1 \in L \Rightarrow \forall n, m \in \mathbb{Z},\ m \neq 0 : \frac{n \cdot 1}{m \cdot 1} \in L \Rightarrow P := \{\frac{n \cdot 1}{m \cdot 1} \mid n \in \mathbb{Z},\ m \in \mathbb{Z} \setminus \{0\}\} \subseteq L$.
Wir zeigen nun, dass die Abbildung $\varphi : \mathbb{Q} \to P$, $\frac{n}{m} \mapsto \frac{n \cdot 1}{m \cdot 1}$, wohldefiniert und ein Isomorphismus ist:
φ ist wohldefiniert und bijektiv: $\frac{n \cdot 1}{m \cdot 1} = \frac{p \cdot 1}{q \cdot 1} \Leftrightarrow (n \cdot 1)(m \cdot 1)^{-1} = (p \cdot 1)(q \cdot 1)^{-1} \Leftrightarrow (n \cdot 1)(q \cdot 1) = (m \cdot 1)(p \cdot 1) \Leftrightarrow (nq) \cdot 1 = (mp) \cdot 1 \Leftrightarrow nq = mp \Leftrightarrow \frac{n}{m} = \frac{p}{q}$.
φ ist ein Homomorphismus: $\varphi(\frac{n}{m} \cdot \frac{p}{q}) = \varphi(\frac{np}{mq}) = \frac{(np) \cdot 1}{(mq) \cdot 1} = \frac{(n \cdot 1)(p \cdot 1)}{(m \cdot 1)(q \cdot 1)} = \frac{(n \cdot 1)}{(m \cdot 1)} \cdot \frac{(p \cdot 1)}{(q \cdot 1)} = \varphi(\frac{n}{m})\varphi(\frac{p}{q})$; analog folgt $\varphi(\frac{n}{m} + \frac{p}{q}) = \varphi(\frac{n}{m}) + \varphi(\frac{p}{q})$. □

6.2.11 Folgerung. Bis auf Isomorphie sind alle Primkörper gegeben durch $\mathbb{Z}_p$ $(p \in \mathbb{P})$ und $\mathbb{Q}$.

6.2.12 Schreibweise. Statt $n \cdot 1$ schreiben wir meistens nur n. Der Kontext[1] entscheidet, ob etwa mit „3“ die natürliche Zahl 3 gemeint ist, oder das Ringelement $1 + 1 + 1$. Man beachte, dass die natürliche Zahl 3 verschieden von der Zahl 0 ist, aber das Ringelement $1 + 1 + 1$ durchaus gleich dem neutralen Element 0 sein kann.

6.2.13 Satz. *Sei* $(K, +, 0, -, \cdot, 1)$ *ein Körper mit* $\operatorname{char} K = p \in \mathbb{P}$. *Dann gilt für alle* $a, b \in K$: $(a + b)^p = a^p + b^p$.

Beweis. Es gilt:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + a^p.$$

Für $i = 1, \ldots, p-1$ gilt $p \mid \binom{p}{i}$ (wegen $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} \in \mathbb{Z}$). Daher ist $\binom{p}{i} a^i b^{p-i} = 0$ für $1 \leq i \leq p-1$. □

6.2.14 Folgerung. Für alle $a, b \in K$ und $k \in \mathbb{N}$ gilt

$$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}.$$

6.3 Nullstellenkörper

6.3.1 Definition. Seien K, L Körper und K Unterkörper von L. Dann heißt L ein *Oberkörper* oder *Erweiterungskörper* von K.

Problem.

> Gegeben: K Körper, $f(x) \in K[x]$, $f(x) \neq 0$, $\operatorname{grad} f(x) = n$.
> Gesucht: Erweiterungskörper L von K, in dem $f(x)$ genau n Nullstellen (gezählt mit ihren Vielfachheiten) besitzt, d.h., in dem gilt: $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ mit $\alpha_i \in L$. Anders ausgedrückt: $f(x)$ zerfällt ganz in Linearfaktoren.

Ein solcher Körper L heißt ein *Nullstellenkörper* von $f(x)$ bezüglich K.

Sei L so ein Nullstellenkörper von $f(x)$ bezüglich K. Dann ist

$$K(\alpha_1, \ldots, \alpha_n) := \bigcap \{M \subseteq L \mid M \text{ Unterkörper von } L,\ K \subseteq M,\ \alpha_1, \ldots, \alpha_n \in M\}$$

der kleinste Unterkörper von L, der K und $\alpha_1, \ldots, \alpha_n$ enthält. $K(\alpha_1, \ldots, \alpha_n)$ heißt ein *Zerfällungskörper* von $f(x)$ bezüglich K.

Es gilt: Ist M Unterkörper von L und $K \subseteq M \subseteq K(\alpha_1, \ldots, \alpha_n)$, so ist entweder $M = K(\alpha_1, \ldots, \alpha_n)$, oder M ist — da $f(x)$ in L genau die Nullstellen $\alpha_1, \ldots, \alpha_n$ besitzt — *kein* Nullstellenkörper von $f(x)$ bezüglich K. Die Zerfällungskörper sind somit genau die minimalen Nullstellenkörper.

6.3.2 Satz (von Kronecker). *Zu jedem* $f(x) \in K[x]$, $f(x) \neq 0$, *gibt es einen Nullstellenkörper, also auch einen Zerfällungskörper von* $f(x)$ *bezüglich* K.

[1] Der Exponenten der Unbestimmten in einem Polynom wird immer als natürliche Zahl interpretiert. So ist etwa im Polynom $2x^3$ die Zahl 2 Abkürzung für $1+1$ („+“ ist hier die Ringaddition), während die Zahl 3 tatsächlich die natürliche Zahl 3 ist. Formal ist dieses Polynom ja eine Potenzreihe $0+0x+0x^2+2x^3+0x^4+\cdots$, also ganz formal die Folge $(0, 0, 0, 1+1, 0, \ldots)$; die Zahl 3 kommt hier nur als Index des Elements $1+1$ vor.

Den Beweis dieses Satzes führen wir in 4 Schritten (6.3.3 – 6.3.7) durch:

6.3.3 Lemma. *Sei $p(x) \in K[x]$, $p(x)$ irreduzibel,* $\operatorname{grad} p(x) = k$, *$I := (p(x)) = \{p(x)q(x) \mid q(x) \in K[x]\}$, dann ist der Restklassenring $K[x]/I$ ein Körper, und es gilt:*

$$K[x]/I = \{b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + I \mid b_i \in K\} = \\ = \{g(x) + I \mid g(x) = 0 \vee \operatorname{grad} g(x) < k\}.$$

Weiters gilt: $g_1(x) + I = g_2(x) + I$ mit $g_i(x) = 0 \vee \operatorname{grad} g_i(x) < k \Rightarrow g_1(x) = g_2(x)$.

Beweis. Wir wissen aus 5.3.10, dass $K[x]/I$ ein Körper ist.
$h(x) + I \in K[x]/I \Rightarrow h(x) = q(x)p(x) + r(x)$ mit $r(x) = 0$ oder $\operatorname{grad} r(x) < \operatorname{grad} p(x) = k$ $\Rightarrow h(x) + I = r(x) + I$. Ist $g_1(x) + I = g_2(x) + I$ mit $g_i(x) = 0$ oder $\operatorname{grad} g_i(x) < k$, so gilt $g_1(x) - g_2(x) \in I$ und damit $g_1(x) = g_2(x)$. □

6.3.4 Lemma. *Sei $p(x) \in K[x]$, $p(x)$ irreduzibel mit $k := \operatorname{grad}(p) \geq 1$. Dann gibt es einen Erweiterungskörper $L \supseteq K$, sodass ein $\alpha \in L$ mit $p(\alpha) = 0$ existiert.*

Beweis. Sei y eine neue Variable. Wegen 6.3.3 ist $K[y]/(p(y))$ Körper, und die Abbildung $\varphi : K \to K[y]/(p(y))$, $a \mapsto a + (p(y))$ ist ein injektiver Homomorphismus. Nach dem Prinzip der isomorphen Einbettung identifizieren wir K mit seinem Bild $\varphi(K) \subseteq K[y]/(p(y))$, somit ist $L := K[y]/(p(y))$ ein Oberkörper von K.
Sei $k := \operatorname{grad} p(x)$.
Fall 1: Sei $k = 1$. Dann gilt $L = K$, und in K gibt es schon eine Nullstelle von $p(x)$.
Fall 2: Sei $k > 1$ und $(p(y)) =: I$. Dann ist $\alpha := y + I$ Nullstelle des Polynoms $p(x) \in K[x] \subseteq L[x]$, denn:
Sei $p(x) = a_0 + a_1 x + \cdots + a_k x^k$. In $K[y]/I$ gilt: $p(y+I) = (a_0 + I) + (a_1 + I)(y + I) + \cdots + (a_k + I)(y + I)^k = a_0 + a_1 y + \cdots + a_k y^k + I = p(y) + I = I$, also $p(\alpha) = a_0 + a_1\alpha + \cdots + a_k\alpha^k = 0$. □

6.3.5 Anmerkung. Nach 6.3.3 ist $L = \{b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} \mid b_i \in K\}$.

6.3.6 Lemma. *Zu jedem $f(x) \in K[x]$, $f(x) \neq 0$,* $\operatorname{grad} f(x) = n \in \mathbb{N}$, *gibt es einen Oberkörper $L \supseteq K$, sodass ein $\alpha \in L$ mit $f(\alpha) = 0$ existiert.*

Beweis. Sei $f(x) = p(x)q(x)$, wobei $p(x)$ irreduzibel ist. Nach 6.3.4 gibt es dann einen Oberkörper L von K, sodass ein $\alpha \in L$ mit $p(\alpha) = 0$ existiert. Für dieses α gilt dann auch $f(\alpha) = p(\alpha)q(\alpha) = 0$. □

6.3.7 Lemma. *Zu jedem $f(x) \in K[x]$, $f(x) \neq 0$,* $\operatorname{grad} f(x) = n \in \mathbb{N}$, *gibt es einen Oberkörper $L \supseteq K$, sodass in $L[x]$ gilt: $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ mit $\alpha_1, \ldots, \alpha_n \in L$.*

Beweis. Induktion nach n: Für $n = 1$ kann $L = K$ gewählt werden.
Sei $\operatorname{grad} f(x) = n + 1$. Nach 6.3.6 gibt es $L^* \supseteq K$ und $\alpha \in L^*$ mit $f(\alpha) = 0$. In $L^*[x]$ gilt daher $f(x) = (x - \alpha)f_1(x)$ mit $\operatorname{grad} f_1(x) = n$. Nach Induktionsvoraussetzung gibt es $L \supseteq L^*$, sodass in $L[x]$ gilt: $f_1(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ mit $\alpha_1, \ldots, \alpha_n \in L$. Dann gilt in $L[x]$ auch $f(x) = (x - \alpha)f_1(x) = c(x - \alpha)(x - \alpha_1) \cdots (x - \alpha_n)$. □

6.4 Erweiterungskörper

Ist L Oberkörper von K, dann ist L auch Vektorraum über K mit den Operationen

$$a + b \ \ldots \text{ Summe in } L \ (a, b \in L),$$
$$\lambda a \ \ \ldots \text{ Produkt in } L \ (a \in L, \lambda \in K).$$

Es existiert daher eine Vektorraumbasis von L über K. Diese bestimmt die Dimension $\dim_K L =: [L : K]$, den so genannten *Grad der Körpererweiterung L von K*. Ist $[L : K] < \infty$, so heißt L eine *endliche Erweiterung von K*.

6.4.1 Anmerkungen. 1) $[L : K] = 1 \Leftrightarrow L = K$.

2) In 6.3.4 und 6.3.5 gilt $L = \{b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} \mid b_i \in K\}$, und $\{1, \alpha, \ldots, \alpha^{k-1}\}$ ist eine Basis von L über K. Also gilt $[L : K] = k$.

3) Wenn $K \leq E \leq L$, dann ist $[L : K] \leq [L : E]$, weil jedes Erzeugendensystem des K-Vektorraums L auch den E-Vektorraum L erzeugt. Überdies ist $[E : K] \leq [L : K]$, weil E Untervektoraum des K-Vektorraums L ist.

6.4.2 Satz (Gradsatz). *Ist L Oberkörper von K, E Oberkörper von L und $[E : K] < \infty$, so gilt:*

$$[E : K] = [E : L] \cdot [L : K].$$

Beweis. Übungsbeispiel 100. (Man zeigt: Ist $\{a_1, \ldots, a_m\}$ eine Basis des Vektorraumes L über K und $\{b_1, \ldots, b_n\}$ eine Basis des Vektorraumes E über L, so ist $\{a_i b_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ eine Basis des Vektorraumes E über K.) □

6.4.3 Definition. Seien $K \leq L$ Körper, und sei $\alpha \in L$. Sei $\varphi_\alpha : K[x] \to L$ der in 4.2.1, 4.2.2 definierte Einsetzungshomomorphismus, der jedem Polynom $a_0 + a_1 x + \cdots + a_n x^n$ das Körperelement $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ zuordnet. Die Wertemenge von φ_α bezeichnen wir mit $K[\alpha]$.

Offenbar ist $K[\alpha]$ der kleinste Unterring von L, der $K \cup \{\alpha\}$ enthält.
Aus dem Homomorphiesatz 2.2.38 (in Verbindung mit 2.2.45) wissen wir, dass der Kern des Einsetzungshomomorphismus ein Ideal von $K[x]$ ist, und dass $K[\alpha] \cong K[x]/\ker(\varphi_\alpha)$. Wir untersuchen also den Kern von φ_α:

6.4.4 Definition. Sei L Oberkörper von K und $\alpha \in L$.

- α heißt *algebraisch* über $K :\Leftrightarrow \exists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$.
- α heißt *transzendent* über $K :\Leftrightarrow \nexists f(x) \in K[x] \setminus \{0\} : f(\alpha) = 0$.

Mit anderen Worten: α ist transzendent über K, wenn $\ker(\varphi_\alpha) = \{0\}$, und algebraisch, wenn $\ker(\varphi_\alpha) \neq \{0\}$.

6.4.5 Beispiele. 1) $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$ ($f(x) = x^2 - 2$, $L = \mathbb{R}$).

2) $\sqrt[3]{3}$ ist algebraisch über $\mathbb{Q}$ ($f(x) = x^3 - 3$, $L = \mathbb{R}$).

3) i ist algebraisch über $\mathbb{R}$ ($f(x) = x^2 + 1$, $L = \mathbb{C}$).

4) e, π sind transzendent über $\mathbb{Q}$ (ohne Beweis).

6.4.6 Definition. Ist L Oberkörper von K und $S \subseteq L$, so definieren wir den Erweiterungskörper $K(S)$ von K durch

$$K(S) := \bigcap \{E \subseteq L \mid E \text{ ist Unterkörper von } L, \text{ der } K \cup S \text{ enthält}\}.$$

Ist $S = \{u_1, \ldots, u_r\}$ endlich, so schreiben wir $K(S) =: K(u_1, \ldots, u_r)$. Ist insbesondere $S = \{\alpha\}$ einelementig, so schreiben wir $K(S) =: K(\alpha)$ („einfache Erweiterung von K“).

6.4.7 Anmerkung. Für einen Körper K und eine Unbestimmte x haben wir den Körper der rationalen Funktionen mit $K(x)$ bezeichnet. $K(x)$ ist der Quotientenkörper des Polynomrings $K[x]$. Wir verwenden also die Schreibweise $K(\cdot)$ für zwei scheinbar verschiedene Operationen. Tatsächlich ergibt sich aber, dass die eine ein Spezialfall der anderen ist:

> Schreiben wir etwa $K(\alpha)$ (wenn $\alpha \in L \geq K$) für den kleinsten Unterkörper von L, der $K \cup \{\alpha\}$ enthält, und $K\langle x\rangle$ für den Quotientenkörper von $K[x]$; jedes Element aus $K\langle x\rangle$ lässt sich als Quotient $p(x)/q(x)$ mit $p(x) \in K[x]$, $q(x) \in K[x]$, $q(x) \neq 0$ schreiben.
> Offenbar enthält $K\langle x\rangle$ den gesamten Ring $K[x]$ und ist daher insbesondere eine Obermenge von $K \cup \{x\} \subseteq K[x]$. Sei umgekehrt $E \leq K\langle x\rangle$ ein beliebiger Unterkörper, der $K \cup \{x\}$ enthält, dann muss E zunächst ganz $K[x]$, aber dann auch ganz $K\langle x\rangle$ enthalten.
> Somit ist $K\langle x\rangle$ der kleinste Unterkörper von $K\langle x\rangle$, der $K \cup \{x\}$ enthält.

Daher ist die Schreibweise $K(x)$ an Stelle von $K\langle x\rangle$ gerechtfertigt.

6.4.8 Satz (Einfache transzendente Erweiterungen). *Sei $K \leq L$, $\alpha \in L$ transzendent über K. Dann ist $K(\alpha) \cong K(x)$ (wobei $K(x)$ wieder der Quotientenkörper des Polynomrings $K[x]$ ist). Es gibt einen (einzigen) Isomorphismus $\varphi : K(x) \to K(\alpha)$, der auf K die Identität ist und x auf α abbildet.*
Insbesondere gilt: Seien α, β beide transzendent über K, dann ist $K(\alpha) \cong K(\beta)$, mit einem Isomorphismus, der α auf β abbildet.

Beweis. Da α transzendent über K ist, ist der Einsetzungshomomorphismus $\varphi_\alpha : K[x] \to K[\alpha]$ ein Ringisomorphismus. Dieser lässt sich durch $\frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$ zu einem Körperisomorphismus $\bar{\varphi} : K(x) \to K(\alpha)$ fortsetzen (Übungsbeispiel 101). □

6.4.9 Anmerkung. Sei α transzendent über K. Dann ist der Körpergrad $[K(\alpha) : K]$ unendlich, denn die Potenzen α^n sind linear unabhängig über K.

Jedes Ideal in $K[x]$ ist Hauptideal, also von der Form $(p(x))$ mit einem „Erzeuger“ $p(x) \in K[x]$. Offenbar gibt es (wenn $I \neq \{0\}$) genau einen normierten Erzeuger.

6.4.10 Definition. Sei α algebraisch über K, und sei $I \subseteq K[x]$ der Kern des Einsetzungshomomorphismus, also $I := \{p(x) \in K[x] \mid p(\alpha) = 0\}$. Sei $m(x)$ normierter Erzeuger von I, dann heißt $m(x)$ *Minimalpolynom* von α über K.

6.4.11 Beispiele. 1) Für $\alpha \in K$ ist $x - \alpha$ Minimalpolynom von α bezüglich K.

2) $x^2 - 2$ ist Minimalpolynom von $\sqrt{2}$ bezüglich $\mathbb{Q}$.

3) $x^3 - 3$ ist Minimalpolynom von $\sqrt[3]{3}$ bezüglich $\mathbb{Q}$.

4) $x^2 + 1$ ist Minimalpolynom von i bezüglich $\mathbb{R}$.

5) Sei $\alpha := \frac{\sqrt{2}}{2}(1 + i)$. Dann ist $\alpha^2 = i$, $\alpha^4 = -1$. Das Minimalpolynom von α über $\mathbb{R}$ ist $x^2 - \sqrt{2}x + 1$, über $\mathbb{Q}$ ist es $x^4 + 1$.

6) Das Minimalpolynom von π über $\mathbb{Q}(\pi^2)$ ist $x^2 - \pi^2$, über $\mathbb{Q}(\pi)$ ist es $x - \pi$, und über $\mathbb{Q}$ hat π kein Minimalpolynom.

Es gilt: $[K(\alpha) : K] = \operatorname{grad} p(x)$, wobei $p(x)$ das Minimalpolynom von α bezüglich K ist. Eine Basis von $K(\alpha)$ (als Vektorraum über K gesehen) ist dann gegeben durch $\{1, \alpha, \ldots, \alpha^{k-1}\}$ mit $k = \operatorname{grad} p(x)$.

6.4.12 Lemma. *Sei α algebraisch über K, $m(x) \in K[x]$ das Minimalpolynom von α über K. Dann ist $m(x)$ in $K[x]$ irreduzibel.*
Sei umgekehrt $p(x) \in K[x]$ ein irreduzibles normiertes Polynom mit $p(\alpha) = 0$, dann muss $p(x) = m(x)$ sein.

Beweis. Nach dem Homomorphiesatz 2.2.38 ist $K[\alpha] \cong K[x]/(m(x))$. Da $K[\alpha]$ Integritätsbereich ist, ist das Ideal $(m(x))$ ein Primideal, daher ist $m(x)$ prim und irreduzibel.
Wenn $p(\alpha) = 0$ ist, dann gilt $m(x)|p(x)$. Wenn aber p irreduzibel ist, muss $m(x) \sim p(x)$ gelten. Da $m(x)$ und $p(x)$ beide normiert sind, schließen wir $m(x) = p(x)$. □

6.4.13 Satz (Einfache algebraische Erweiterungen). *Sei $K \leq L$, $\alpha \in L$ algebraisch über K. Sei $m(x)$ das Minimalpolynom von α über K, $k = \operatorname{grad} m(x)$. Dann gilt:*

(a) *$K[\alpha] \simeq K[x]/I$, wobei I das von $m(x)$ erzeugte Ideal in $K[x]$ ist. Es gibt einen Isomorphismus, der auf K die Identität ist, und der α auf die Nebenklasse $x + I$ abbildet.*

(b) *$K(\alpha) = K[\alpha]$.*

(c) *Jedes Element $\beta \in K(\alpha)$ lässt sich eindeutig in der Form $\beta = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$ mit $a_0, \ldots, a_{k-1} \in K$ darstellen.*

(d) *$[K(\alpha) : K] = n$.*

Insbesondere gilt:

(e) *Wenn $\alpha, \beta \in L$ dasselbe Minimalpolynom $m(x)$ über K haben, dann gibt es einen Isomorphismus $\varphi : K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$, $\varphi{\restriction}K = id$.*

Beweis. (a) Sei $\varphi_\alpha : K[x] \to K[\alpha]$ der Einsetzungshomomorphismus, $j : K[x] \to K[x]/I$ die kanonische Abbildung $p \mapsto p + I$. Der Homomorphiesatz liefert einen Isomorphismus $h : K[\alpha] \to K[x]/I$ mit $k \circ \varphi_\alpha = j$. Insbesondere ist $x + I = j(x) = k(\varphi_\alpha(x)) = k(\alpha)$. Die Abbildung j ist injektiv auf $K \subseteq K[x]$; wir identifizieren alle $b \in K$ mit $j(b)$. Dann gilt $b = j(b) = k(\varphi_\alpha(b)) = k(b)$.

(b) $K[x]/I$ ist ein Körper wegen 6.3.3. Wegen (a) ist also auch $K[\alpha]$ ein Körper. Also $K[\alpha] = K(\alpha)$.

(c) Siehe 6.3.3.

(d) Aus (c) folgt, dass $1, \alpha, \ldots, \alpha^{k-1}$ eine Basis von des K-Vektorraums $K[\alpha]$ ist.

□

6.4.14 Satz. *Sei $K \leq L$, und seien $\alpha_1, \ldots, \alpha_n, \beta \in L$. Wenn $\alpha_1, \ldots, \alpha_n$ algebraisch über K sind, und β algebraisch über $K(\alpha_1, \ldots, \alpha_n)$, dann ist β algebraisch über K.*

Beweis. Die Erweiterungsgrade

$$[K(\alpha_1, \ldots, \alpha_n, \beta) : K(\alpha_1, \ldots, \alpha_n)],\ [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})],\ \ldots,\ [K(\alpha_1) : K]$$

sind alle endlich. Durch wiederholte Anwendung des Gradsatzes schließen wir, dass der K-Vektorraum $K(\alpha_1, \ldots, \alpha_n, \beta)$ und sein Unterraum $K(\beta)$ endliche Dimension haben. Wenn nun $[K(\beta) : K] = n$ ist, dann sind $\{1, \beta, \ldots, \beta^n\}$ über K linear abhängig, und wir erhalten ein Polynom $p(x) \in K[x] \setminus \{0\}$ mit Nullstelle β. □

6.4.15 Lemma. *Sei K ein Körper mit $\operatorname{char} K = 0$ und $f(x) \in K[x]$ irreduzibel, L ein Erweiterungskörper von K und α Nullstelle von $f(x)$ in L, dann ist α eine einfache Nullstelle.*

Beweis. Wäre α eine mehrfache Nullstelle, so wäre α auch Nullstelle von $f'(x)$ (siehe Übungen), also wäre in $L[x]$

$$\operatorname{grad} \operatorname{ggT}(f(x), f'(x)) \geq 1.$$

Nun ist aber — nach dem Euklidischen Algorithmus — der ggT von $f(x)$ und $f'(x)$ in $K[x]$ derselbe wie in $L[x]$. Da $f(x)$ in $K[x]$ irreduzibel ist, muss daher $\operatorname{ggT}(f(x), f'(x)) = f(x)$ gelten. Also muss $f'(x) = 0$ sein (sonst wäre ja $\operatorname{grad} f'(x) \geq \operatorname{grad} f(x)$). Ist $f(x) = \sum_{i=0}^{n} a_i x^i$, so gilt $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$, also muss $i a_i = 0$ sein für $i = 1, \ldots, n$. Wegen $\operatorname{char} K = 0$ folgt daraus $a_i = 0$ für $i = 1, \ldots, n$, also $f(x) = a_0$, Widerspruch! □

6.4.16 Satz (Satz vom primitiven Element). *Ist L Oberkörper von K mit* $\operatorname{char} K = 0$ *(also auch* $\operatorname{char} L = 0$*), und sind $u_1, \ldots, u_r \in L$ alle algebraisch über K, so gibt es ein $\alpha \in L$ mit $K(u_1, \ldots, u_r) = K(\alpha)$.*

Beweis. Induktion nach r. Für $r = 1$ ist die Aussage trivial.
Annahme: Die Aussage stimmt für $r - 1$ $(r > 1)$. Wir haben dann: $K(u_1, \ldots, u_r) = K(u_1, \ldots, u_{r-1})(u_r) = K(\alpha)(u_r) = K(\alpha, \beta)$ für ein geeignetes $\alpha \in L$ und für $\beta = u_r$. Wegen $[K(\alpha, \beta) : K] < \infty$ sind α, β algebraisch über K. Wir zeigen: $\exists \delta \in L$ mit $K(\alpha, \beta) = K(\delta)$.
Seien $f(x)$ bzw. $g(x)$ die Minimalpolynome von α bzw. β. Wir betrachten einen Erweiterungskörper M von K, der zugleich Nullstellenkörper von $f(x)$ und $g(x)$ ist, d.h., $\exists \alpha_1, \ldots, \alpha_s$, $\beta_1, \ldots, \beta_t \in M$ mit $f(x) = (x - \alpha_1) \cdots (x - \alpha_s)$ und $g(x) = (x - \beta_1) \cdots (x - \beta_t)$. Dabei sei o.B.d.A.: $\alpha_1 = \alpha$ und $\beta_1 = \beta$. Nach 6.4.15 ist $\beta \neq \beta_k$ für $k = 2, \ldots, t$, daher hat die Gleichung $\alpha_i + x\beta_k = \alpha + x\beta$ für jedes $i = 1, \ldots, s$ und $k = 2, \ldots, t$ höchstens eine Lösung in K. Da K unendlich ist (wegen $\operatorname{char} K = 0$), haben wir also für fast alle $c \in K$ (d.h. für alle $c \in K$ bis auf endlich viele) $\alpha_i + c\beta_k \neq \alpha + c\beta$ für alle $i = 1, \ldots, s$ und $k = 2, \ldots, t$. Wir wählen ein solches c, halten es fest und behaupten

$$K(\alpha, \beta) = K(\delta) \text{ mit } \delta := \alpha + c\beta.$$

Trivialerweise ist $K(\delta) \subseteq K(\alpha, \beta)$. Für die umgekehrte Inklusion genügt es zu zeigen, dass $\alpha, \beta \in K(\delta)$. Dazu betrachten wir das Polynom $\bar{f}(x) := f(\delta - cx) \in K(\delta)[x]$. Es ist dann $\bar{f}(\beta) = f(\delta - c\beta) = f(\alpha) = 0$, aber für $k = 2, \ldots, t$ gilt: $\bar{f}(\beta_k) = f(\delta - c\beta_k) = f(\alpha + c\beta - c\beta_k) \neq 0$, da ja $\alpha + c\beta - c\beta_k \neq \alpha_i$ für $i = 1, \ldots, s$ nach Wahl von c. Also haben $g(x)$ und $\bar{f}(x)$ genau die eine Nullstelle β gemeinsam. Daher ist in $K(\delta)[x]$: $\operatorname{ggT}(g(x), \bar{f}(x)) = x - \beta$, insbesondere also $\beta \in K(\delta)$ und somit auch $\alpha = \delta - c\beta \in K(\delta)$. □

6.5 Zerfällungskörper

Gemäß 6.3.1 ist ein minimaler Nullstellenkörper von $f(x) \in K[x]$ mit $f(x) \neq 0$ ein Zerfällungskörper von $f(x)$ bezüglich K.

Die Existenz wurde bereits in Abschnitt 6.3 gezeigt: Ist L Nullstellenkörper von $f(x)$ bezüglich K, dann gilt $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ mit $c \in K$, $\alpha_1, \ldots, \alpha_n \in L$, und $K(\alpha_1, \ldots, \alpha_n)$ ist ein Zerfällungskörper von $f(x)$ bezüglich K.

6.5.1 Definition. Sei $K_1 \cong K_2$ (K_1, K_2 Körper), $\varphi : K_1 \to K_2$ Isomorphismus und L_i Erweiterungskörper von K_i, $i = 1, 2$. Dann heißen L_1, L_2 *äquivalent* bezüglich $\varphi :\Leftrightarrow$ Es gibt einen Isomorphismus $\bar{\varphi} : L_1 \to L_2$ mit $\bar{\varphi} \restriction K_1 = \varphi$.
Spezialfall: $K_1 = K_2 = K$, $\varphi = \mathrm{id}_K$. In diesem Fall sind L_1, L_2 äquivalent bezüglich $\varphi \Leftrightarrow$ es gibt einen Isomorphismus $\psi : L_1 \to L_2$ mit $\psi(a) = a$ für alle $a \in K$. Solche Erweiterungskörper L_1, L_2 heißen *äquivalent* bezüglich K.

6.5.2 Anmerkung. „äquivalent bezüglich K“ ist eine Äquivalenzrelation.

6.5.3 Lemma. *Sind R, S kommutative Ringe mit Einselement und ist $\varphi : R \to S$ Homomorphismus, so gibt es* genau einen *Homomorphismus von $R[x] \to S[x]$, der φ fortsetzt und x auf x abbildet. Wir bezeichnen diesen Homomorphismus mit $\varphi_{[x]}$ und nennen $\varphi_{[x]}$ die „natürliche Fortsetzung“ von φ.*
Ist φ Isomorphismus, so auch $\varphi_{[x]}$.

Beweis. $\varphi_{[x]}$ ist gegeben durch die Zuordnung

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \mapsto \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Die angegebenen Eigenschaften von $\varphi_{[x]}$ rechnet man leicht nach. □

6.5.4 Satz. *Sei Z ein Zerfällungskörper von $f(x) \in K[x]$ bezüglich K und Z_1 äquivalent zu Z bezüglich K. Dann ist auch Z_1 ein Zerfällungskörper von $f(x) \in K[x]$ bezüglich K.*

Beweis. In $Z[x]$ gilt: $f(x) = c(x-\alpha_1)^{k_1} \cdots (x-\alpha_r)^{k_r}$ mit $c \in K$, $\alpha_1, \ldots, \alpha_r \in Z$. Sei $\varphi : Z \to Z_1$ ein Isomorphismus mit $\varphi(a) = a$ für alle $a \in K$ und $\varphi_{[x]} : Z[x] \to Z_1[x]$ die Fortsetzung von φ nach 6.5.3. Dann ist $\varphi_{[x]}$ Isomorphismus und $\varphi_{[x]}(f(x)) = c(x - \varphi(\alpha_1))^{k_1} \cdots (x - \varphi(\alpha_r))^{k_r} = f(x)$, da ja $\varphi_{[x]}{\restriction}K[x] = \mathrm{id}$. Somit ist Z_1 Nullstellenkörper.

Ist U Unterkörper von Z_1 mit $U \supseteq K \cup \{\varphi(\alpha_1), \ldots, \varphi(\alpha_r)\}$, so ist $\varphi^{-1}(U) \supseteq K \cup \{\alpha_1, \ldots, \alpha_r\}$, $\varphi^{-1}(U) \subseteq Z$ und $\varphi^{-1}(U)$ Unterkörper von Z. Wegen $Z = K(\alpha_1, \ldots, \alpha_r)$ ist $Z = \varphi^{-1}(U)$ und damit $Z_1 = U$. □

Wir wollen nun zeigen (siehe 6.5.12), dass je zwei Zerfällungskörper Z_1, Z_2 desselben Polynoms (oder derselben Menge von Polynomen) in $K[x]$ äquivalent bezüglich K sind.
Das folgende Lemma ist eine Verallgemeinerung von 6.4.13(e):

6.5.5 Lemma. *Sei $\varphi : K \to \tilde{K}$ Isomorphismus. Sei α algebraisch über K mit Minimalpolynom $m(x)$, und sei $\tilde{\alpha}$ algebraisch über $\tilde{K}$ mit Minimalpolynom $\tilde{m}(x)$, wobei $\tilde{m}(x) = \varphi_{[x]}(m(x))$ (vergleiche* 6.5.3*). Wenn $\varphi_{[x]}(m(x)) = \tilde{m}(x)$, dann gibt es einen Isomorphismus $\bar{\varphi} : K(\alpha) \cong K(\tilde{\alpha})$, der φ fortsetzt und $\bar{\varphi}(\alpha) = \tilde{\alpha}$ erfüllt.*

Beweis. Nach 6.4.13 wissen wir, dass es einen Isomorphismus $\iota : K(\alpha) \to K[x]/I$ gibt (wobei I das von $m(x)$ erzeugte Ideal in $K[x]$ ist), der K fest lässt und α auf die Nebenklasse $x + I$ abbildet.
Ebenso gibt es einen Isomorphismus $\tilde{\iota} : \tilde{K}(\tilde{\alpha}) \to \tilde{K}[x]/\tilde{I}$, wobei $\tilde{I}$ das von $\tilde{m}(x)$ erzeugte Ideal in $\tilde{K}[x]$ ist, und $\tilde{\iota}(\tilde{\alpha}) = x + \tilde{I}$.
Der Isomorphismus $\varphi_{[x]}$ bildet $K[x]$ auf $K^*[x]$ und I auf I^* ab (wobei $\varphi_{[x]}(x) = x$ gilt) und vermittelt daher einen Isomorphismus von $K[x]/I$ nach $\tilde{K}[x]/\tilde{I}$.
Insgesamt erhalten wir die folgenden Kette von Isomorphismen:

$$K(\alpha) \xrightarrow{\ \iota\ } K[x]/I \xrightarrow{\ \varphi_{[x]}\ } \tilde{K}[x]/\tilde{I} \xrightarrow{\ \tilde{\iota}^{-1}\ } \tilde{K}(\tilde{\alpha}),$$

wobei der erste und der dritte Isomorphismus die Identität auf K bzw $\tilde{K}$ induzieren, und der mittlere Isomorphismus den Isomorphismus φ fortsetzt. □

6.5.6 Lemma. *Sei $\varphi : K \to \tilde{K}$ ein Körperisomorphismus; seien $E, \tilde{E}$ Körper mit $K \leq E$, $\tilde{K} \leq \tilde{E}$. Sei $p(x) \in K[x]$, $\alpha \in E$, $p(\alpha) = 0$. Mit $\tilde{p}(x)$ bezeichnen wir das Bild von $p(x)$ unter der natürlichen Fortsetzung von $\varphi : K \to \tilde{K}$ zu $\varphi_{[x]} : K[x] \to \tilde{K}[x]$.*
Wenn $\tilde{p}(x)$ in $\tilde{E}$ in Linearfaktoren zerfällt, dann gibt es ein $\tilde{\alpha} \in \tilde{E}$, sodass sich φ zu einem Isomorphismus $\bar{\varphi} : K(\alpha) \to \tilde{K}(\tilde{\alpha})$ fortsetzen lässt.

Beweis. Sei $p(x) = p_1(x) \cdot p_2(x) \cdots$ Produkt von irreduziblen Faktoren $p_i(x) \in K[x]$, dann ist α Nullstelle eines Faktors, sagen wir $p_1(\alpha) = 0$. Sei $\tilde{p}_i := \varphi_{[x]}(p_i)$, dann sind die Polynome $\tilde{p}_i(x) \in \tilde{K}[x]$ irreduzibel (siehe 6.5.3), und es gilt $\tilde{p}(x) = \tilde{p}_1(x) \cdot \tilde{p}_2(x) \cdots$.
Da E Nullstellenkörper von $\tilde{p}(x)$ ist, zerfällt $\tilde{p}_1(x)$ in E in Linearfaktoren. Sei nun $\tilde{\alpha} \in \tilde{E}$ eine beliebige Nullstelle des irreduziblen Polynoms $\tilde{p}_1(x)$. Dann können wir nach 6.5.5 einen Isomorphismus $\bar{\varphi} : K(\alpha) \to \tilde{K}(\tilde{\alpha})$ mit $\bar{\varphi}(\alpha) = \tilde{\alpha}$ finden, der φ fortsetzt. □

6.5.7 Lemma. *Seien $K \leq E$, $\tilde{K} \leq \tilde{E}$ Körper, $\varphi : K \to \tilde{K}$ ein Isomorphismus. Sei $p(x) \in K[x]$, $\tilde{p}(x) := \varphi_{[x]}(p(x))$ das entsprechende Polynom in $\tilde{K}[x]$. Dann gilt:*

(a) *Wenn E ein Zerfällungskörper von $p(x)$ über K ist, und $\tilde{E}$ ein Nullstellenkörper von $\tilde{p}(x)$, dann lässt sich φ zu einem Monomorphismus $\bar{\varphi} : E \to \tilde{E}$ fortsetzen.*

(b) *Wenn überdies $\tilde{E}$ Zerfällungskörper von $\tilde{p}(x)$ über $\tilde{K}$ ist, dann ist $\bar{\varphi}$ ein Isomorphismus zwischen E und $\tilde{E}$.*

Beweis von (a). Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $p(x)$ in E, dann ist $E = K(\alpha_1, \ldots, \alpha_n)$. Wir werden Elemente $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n \in \tilde{E}$ sowie eine aufsteigende Kette $\varphi = \varphi_0 \subseteq \varphi_1 \subseteq \cdots \subseteq \varphi_n$ finden, sodass $\varphi_k : K(\alpha_1, \ldots, \alpha_k) \to \tilde{K}(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k)$ ein Isomorphismus mit $\varphi_k(\alpha_i) = \tilde{\alpha}_i$ für $1 \leq i \leq k$ ist. Die Abbildung φ_n ist dann der gewünschte Monomorphismus $\bar{\varphi}$, der $E = K(\alpha_1, \ldots, \alpha_n)$ auf $K(\bar{\alpha}_1, \ldots, \bar{\alpha}_n) \subseteq \tilde{E}$ abbildet.
$\varphi = \varphi_0$ ist bereits gegeben. Wenn wir φ_k bereits kennen, können wir 6.5.6 auf das Polynom $p(x)$ mit der Nullstelle α_{k+1} (und den Körper $K(\alpha_1, \ldots, \alpha_k)$) anwenden und erhalten $\tilde{\alpha}_{k+1}$ und φ_{k+1}. □

Beweis von (b). Da $p(x)$ in E bereits in Linearfaktoren zerfällt, zerfällt auch $\tilde{p}(x)$ in $\bar{\varphi}(E) \subseteq \tilde{E}$ in Linearfaktoren. Daher ist $\bar{\varphi}(E)$ bereits Nullstellenkörper für $\tilde{p}(x)$, also muss $\bar{\varphi}(E) = \tilde{E}$ sein. □

6.5.8 Anmerkung. Im Beweis von 6.5.6 bzw. 6.5.7(a) sieht man, dass die Fortsetzung $\bar{\varphi}$ von φ im Allgemeinen nicht eindeutig ist, denn als Bild $\tilde{\alpha} = \varphi(\alpha)$ kann man eine beliebige Nullstelle des irreduziblen Polynoms $\tilde{p}_1(x)$ wählen.

6.5.9 Anmerkung. Sei $p(x)$ in $K(x)$ irreduzibel ist, und seien α, β, γ Nullstellen von $p(x)$ in einem Nullstellenkörper E (wobei wir hier nicht annehmen, dass α, β, γ verschieden sind). Es gibt einen Monomorphismus $\varphi : K(\alpha) \to E$ mit $\varphi \restriction K = id$, $\varphi(\alpha) = \beta$; φ ist Isomorphismus zwischen $K(\alpha)$ und $K(\beta)$.
Nach dem bereits Bewiesenen gibt es eine Fortsetzung $\varphi' : K(\alpha, \gamma) \to E$. Um eine solche Fortsetzung zu finden, muss man $p(x)$ in $K(\alpha)[x]$ in irreduzible Faktoren zerlegen; einer dieser Faktoren hat dann die Nullstelle γ, und γ kann dann auf eine beliebige andere Nullstelle dieses Faktors abgebildet werden. Über den Grad dieses Faktors, und somit über die Anzahl der möglichen Fortsetzungen, wissen wir nur, dass er kleiner als der Grad von $p(x)$ sein muss. Es kann durchaus der Fall eintreten, dass γ bereits in $K(\alpha)$ liegt, dann ist $\varphi(\gamma)$ bereits definiert und es muss $\varphi' = \varphi$ gelten.

6.5.10 Anmerkung. Die Definition des Nullstellenkörpers und des Zerfällungskörpers einer Menge $\mathscr{P}$ von Polynomen ist völlig analog der für ein Polynom in 6.3.1 gegebenen. Die Existenz kann mit Hilfe des Lemmas von Zorn bewiesen werden.

6.5.11 Lemma. *Seien $K \leq E$, $\tilde{K} \leq \tilde{E}$ Körper, $\varphi : K \to \tilde{K}$ ein Isomorphismus. Sei $\mathscr{P} \subseteq K[x]$ eine Menge von Polynomen, $\tilde{\mathscr{P}} := \varphi_{[x]}(\mathscr{P})$. Dann gilt:*
Wenn $E, \tilde{E}$ Zerfällungskörper von $\mathscr{P}$ bzw. $\tilde{\mathscr{P}}$ über K bzw $\tilde{K}$ sind, dann lässt sich φ zu einem Isomorphismus $\bar{\varphi} : E \to \tilde{E}$ fortsetzen.

Beweis. Betrachten wir zunächst den Fall, dass $\mathscr{P} = \{p_0(x), p_1(x), \ldots\}$ abzählbar ist. Sei $K_0 := K$, und sei K_{n+1} der Zerfällungskörper von $p_n(x)$ über K_n. Mit Hilfe von 6.5.7 erhalten wir eine Folge von Monomorphismen $\varphi_n : K_n \to \tilde{E}$ mit $\varphi = \varphi_0 \subseteq \varphi_1 \subseteq \cdots$.
Die Abbildung $\bar{\varphi} := \varphi_0 \cup \varphi_1 \cup \cdots$ ist dann ein Monomorphismus von E nach $\tilde{E}$, und ähnlich wie vorhin können wir schließen, dass $\bar{\varphi}(E) = \tilde{E}$ sein muss.
Wenn $\mathscr{P}$ überabzählbar ist, verwenden wir eine Wohlordnung von $\mathscr{P}$ und konstruieren durch transfinite Induktion eine transfinite Folge von Approximationen an $\bar{\varphi}$, deren Vereinigung schließlich $\bar{\varphi}$ ergibt. □

6.5.12 Satz. *Sei $\mathscr{P} \subseteq K[x]$. Seien Z_1 und Z_2 Zerfällungskörper von $\mathscr{P}$ (bezüglich K). Dann sind Z_1 und Z_2 bezüglich K äquivalent.*

6.6 Endliche Körper (Galois-Felder)

Sei K ein endlicher Körper. Dann ist $\operatorname{char} K = p \in \mathbb{P}$, und der Primkörper P von K ist isomorph zu $\mathbb{Z}_p$. Da K Vektorraum über dem Unterkörper P ist, gibt es eine Basis $\{a_1, \ldots, a_n\}$ von K über P ($[K : P] = n \in \mathbb{N}$). Daher ist $K = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in P\}$ und $|K| = p^n$, da jeder Koeffizient λ_i auf $|P| = p$ Arten gewählt werden kann.

Frage: Gegeben $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Gibt es einen Körper K mit $|K| = p^n$?

Wenn es einen solchen Körper gibt, dann mit $\operatorname{char} K = p$. Wir gehen daher von $\mathbb{Z}_p$ aus und betrachten das Polynom $f(x) = x^{p^n} - x = x(x^{p^n-1} - 1) \in \mathbb{Z}_p[x]$. Sei K ein Zerfällungskörper von $f(x)$ über $\mathbb{Z}_p$. Dann hat $f(x)$ in K genau p^n Nullstellen $\alpha_1, \ldots, \alpha_{p^n}$, welche alle einfach sind, denn: $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$ ($p^n x^{p^n-1} = 0$ wegen $\operatorname{char} \mathbb{Z}_p[x] = p$). Wir behaupten nun, dass $K = \{\alpha_1, \ldots, \alpha_{p^n}\} =: N$ gilt. Dazu müssen wir nur zeigen, dass N Unterkörper von K ist:
$0, 1 \in N$, denn $f(0) = f(1) = 0$.
$\alpha, \beta \in N \Rightarrow f(\alpha+\beta) = (\alpha+\beta)^{p^n} - (\alpha+\beta) = (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = f(\alpha) + f(\beta) = 0 + 0 = 0$
$\Rightarrow \alpha + \beta \in N$.
$\alpha \in N \Rightarrow f(-\alpha) = (-1)^{p^n}\alpha^{p^n} - (-1)\alpha = (-1)f(\alpha) = (-1)0 = 0 \Rightarrow -\alpha \in N$. (Beachte, dass für $p = 2$ die Gleichung $1 = -1$ gilt.)
$\alpha, \beta \in N \Rightarrow f(\alpha\beta) = (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0 \Rightarrow \alpha\beta \in N$.
$\alpha \in N$, $\alpha \neq 0 \Rightarrow f(\alpha) = 0 \Rightarrow \alpha^{p^n} = \alpha \Rightarrow (\alpha^{p^n})^{-1} = \alpha^{-1} \Rightarrow (\alpha^{-1})^{p^n} = \alpha^{-1} \Rightarrow f(\alpha^{-1}) = 0$
$\Rightarrow \alpha^{-1} \in N$.

Sind K_1, K_2 endliche Körper mit $|K_1| = |K_2| = p^n$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$) und P_1, P_2 die Primkörper von K_1, K_2, so gilt: $P_1 \cong P_2 \cong \mathbb{Z}_p$.

Wir zeigen nun, dass K_i Zerfällungskörper von $f(x) = x^{p^n} - x \in P_i[x]$ über P_i, $i = 1, 2$ ist: Es gilt $|K_1 \setminus \{0\}| = p^n - 1$ und $(K_1 \setminus \{0\}, \cdot)$ ist eine Gruppe. Sei $\alpha \in K_1 \setminus \{0\}$. Dann ist $\alpha^{p^n-1} = 1$ und damit $\alpha^{p^n} - \alpha = f(\alpha) = 0$, wobei letzteres auch für $\alpha = 0$ gilt. Somit sind die Elemente von K_1 genau die p^n Nullstellen von $f(x)$. Die Aussage für K_2 folgt analog. Wegen der Eindeutigkeit des Zerfällungskörpers (siehe 6.5.7) gilt dann $K_1 \cong K_2$.

6.6.1 Satz. *Die Ordnung jedes endlichen Körpers ist eine Primzahlpotenz p^n ($p \in \mathbb{P}$, $n \in \mathbb{N}$). Umgekehrt gibt es zu jeder Primzahlpotenz p^n bis auf Isomorphie genau einen Körper K mit $|K| = p^n$.* □

Schreibweise für K mit $|K| = p^n$: $K = \mathrm{GF}(p^n)$ (*Galois-Feld*).

6.6.2 Satz. *Ist K endlicher Körper, so ist die Gruppe $(K \setminus \{0\}, \cdot)$ zyklisch.*

Beweis. Sei $a \in K \setminus \{0\}$ mit maximaler Ordnung r. Zu zeigen: $r = p^n - 1$ (wobei $|K| = p^n$). Sei $b \in K \setminus \{0\}$ beliebig, $\mathrm{o}(b) = s$. Wir betrachten die Primfaktorzerlegungen von r und s: $r = p_1^{e_1} \cdots p_k^{e_k}$, $s = p_1^{f_1} \cdots p_k^{f_k}$. Es gilt:

$$\mathrm{kgV}(r,s) \quad = \quad \prod_{i=1}^{k} p_i^{\max(e_i,f_i)} \quad \overset{\text{o.B.d.A.}}{=} \quad \underbrace{p_1^{e_1} \cdots p_j^{e_j}}_{=:\,\tilde{r}} \underbrace{p_{j+1}^{f_{j+1}} \cdots p_k^{f_k}}_{=:\,\tilde{s}}, \qquad 1 \le j \le k.$$

Es gilt: $\mathrm{ggT}(\tilde{r},\tilde{s}) = 1$ und $\mathrm{kgV}(\tilde{r},\tilde{s}) = \tilde{r}\tilde{s} = \mathrm{kgV}(r,s)$. Sei $\tilde{a} := a^{r/\tilde{r}}$ und $\tilde{b} := b^{s/\tilde{s}}$. Dann gilt $\mathrm{o}(\tilde{a}) = \tilde{r}$ (denn: $\tilde{a}^{\tilde{r}} = a^r = 1$ und $\mathrm{o}(a) = r$) und $\mathrm{o}(\tilde{b}) = \tilde{s}$ (analog).

Wir behaupten nun: $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{o}(\tilde{a})\mathrm{o}(\tilde{b})$. Wegen $(\tilde{a}\tilde{b})^{\tilde{r}\tilde{s}} = (\tilde{a}^{\tilde{r}})^{\tilde{s}}(\tilde{b}^{\tilde{s}})^{\tilde{r}} = 1 \cdot 1 = 1$ gilt $\mathrm{o}(\tilde{a}\tilde{b}) | \tilde{r}\tilde{s}$. Weiters gilt: $(\tilde{a}\tilde{b})^m = 1$ für ein $m \in \mathbb{N} \Rightarrow \tilde{a}^m = \tilde{b}^{-m} \Rightarrow 1 = \tilde{a}^{m\tilde{r}} = \tilde{b}^{-m\tilde{r}} \Rightarrow \mathrm{o}(\tilde{b}) = \tilde{s} | -m\tilde{r} \Rightarrow \tilde{s} | m$. Analog: $\tilde{r} | m$. Aus $\mathrm{ggT}(\tilde{r},\tilde{s}) = 1$ folgt somit $\tilde{r}\tilde{s} | m$.

Also haben wir: $\mathrm{o}(\tilde{a}\tilde{b}) = \tilde{r}\tilde{s} = \mathrm{kgV}(r,s) = \frac{rs}{\mathrm{ggT}(r,s)} \le r$, da r maximal. Daraus erhält man: $s \le \mathrm{ggT}(r,s) \Rightarrow s = \mathrm{ggT}(r,s) \Rightarrow s | r$. Da b beliebig war, gilt also $b^r = 1$ für alle $b \in K \setminus \{0\}$.

$f(x) = x^r - 1 \in K[x]$ hat $p^n - 1$ Nullstellen, somit gilt $p^n - 1 \le r$. Klarerweise gilt $r | p^n - 1$, also $r \le p^n - 1$. Daraus folgt: $r = p^n - 1$. □

Jedes erzeugende Element von $(K \setminus \{0\}, \cdot)$ heißt ein *primitives Element* von K (für $K = \mathbb{Z}_p$: *Primitivwurzel* $\mathrm{mod} p$). Ist a primitives Element von K, so gilt $K = \{0, 1, a, a^2, \ldots, a^{|K|-2}\}$ und $K \setminus \{0\} = \langle a \rangle = \langle a^t \rangle$ mit $\mathrm{ggT}(t, |K| - 1) = 1$ (vgl. Übungsbeispiel 38).

Weiters gilt $K \cong \mathbb{Z}_p(a)$ für ein beliebiges primitives Element a von K. Sei $q(x)$ das Minimalpolynom von a über $\mathbb{Z}_p$. Dann ist $q(x)$ irreduzibel, und es gilt

$$\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/(q(x)) = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{m-1}x^{m-1} + (q(x)) \mid \alpha_i \in \mathbb{Z}_p\}$$

mit $m = \mathrm{grad}\, q(x)$. Aus $|K| = p^n$ folgt dann $n = m = \mathrm{grad}\, q(x)$, also: zu beliebigem $n \in \mathbb{N}$ gibt es ein irreduzibles Polynom $q(x) \in \mathbb{Z}_p[x]$ mit $\mathrm{grad}\, q(x) = n$.

Um einen endlichen Körper K mit $|K| = p^n$ ($p \in \mathbb{P}$, $n \in \mathbb{N}$) zu bestimmen, d.h., seine Operationstafeln zu ermitteln, kann man daher so vorgehen:

1) Der Primkörper von K wird als $\mathbb{Z}_p$ angenommen.

2) Bestimme ein Polynom $q(x) \in \mathbb{Z}_p[x]$ mit $q(x)$ normiert, irreduzibel und $\mathrm{grad}\, q(x) = n$ (in endlich vielen Schritten möglich).

3) Bilde $\mathbb{Z}_p[x]/(q(x))$ — dies ist der gesuchte Körper K.

Es gilt: $\alpha := x + (q(x))$ ist (nach Einbettung von $\mathbb{Z}_p$) Nullstelle von $q(x)$. Aber nicht immer muss dieses α ein primitives Element von K sein.

α ist primitives Element $\Leftrightarrow \alpha^r \neq 1$ für $0 < r < |K| - 1 = p^n - 1 \Leftrightarrow \alpha$ ist nicht Nullstelle von $x^r - 1$ für $0 < r < p^n - 1 \;\Leftrightarrow\; q(x) \nmid x^r - 1$ für $0 < r < p^n - 1$.

Irreduzible Polynome $q(x)$ mit dieser Eigenschaft heißen *primitive Polynome*.

6.6.3 Beispiel. Bestimmung von GF(9) = GF(3^2): Wir nehmen $\mathbb{Z}_3 = \{0, 1, 2\}$ als Primkörper. Das Polynom $x^2 - x - 1 \in \mathbb{Z}_3[x]$ ist irreduzibel, da es in $\mathbb{Z}_3$ keine Nullstelle hat. Somit ist $\mathbb{Z}_3[x]/(x^2-x-1) \cong \mathbb{Z}_3(\alpha) = \mathrm{GF}(9)$, wobei $\alpha^2 = \alpha+1$ gilt. Es ist $[\mathrm{GF}(9) : \mathbb{Z}_3] = 2$, und eine Basis ist gegeben durch $\{1, \alpha\}$. Wir berechnen nun die Elemente von GF(9) sowie deren Koordinatendarstellung in der Basis $\{1, \alpha\}$:

Elemente	Koordinatendarstellung
0	$(0,0)$
$\alpha^0 = 1$	$(1,0)$
$\alpha^1 = \alpha$	$(0,1)$
$\alpha^2 = 1 + \alpha$	$(1,1)$
$\alpha^3 = 1 + 2\alpha$	$(1,2)$
$\alpha^4 = 2$	$(2,0)$
$\alpha^5 = 2\alpha$	$(0,2)$
$\alpha^6 = 2 + 2\alpha$	$(2,2)$
$\alpha^7 = 2 + \alpha$	$(2,1)$
$\alpha^8 = 1$	$(1,0)$

Die Potenzen α^j, $0 \le j < 8$, sind somit alle verschieden, α ist ein primitives Element von GF(9) und $x^2 - x - 1$ ein primitives Polynom in $\mathbb{Z}_3[x]$. Damit können die Operationstafeln angegeben werden.

Multiplikation: $0 \cdot \alpha^i = 0$, $\alpha^i\alpha^j = \alpha^{(i+j) \bmod 8}$ ($(\mathrm{GF}(9) \setminus \{0\}, \cdot)$ ist eine zyklische Gruppe).
Addition: z.B.:

$$\begin{array}{ccccc} \alpha^2 & + & \alpha^4 & = & \alpha \\ \downarrow & & \downarrow & & \uparrow \\ (1,1) & + & (2,0) & = & (0,1) \end{array}$$

Praktische Vorgangsweise: 1) Wähle normiertes, irreduzibles Polynom $q(x) \in \mathbb{Z}_p[x]$ vom Grad n. Sei etwa $q(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0$ mit $a_i \in \mathbb{Z}_p$.

2) Setze $q(\alpha) = 0$ und betrachte die Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ von GF(p^n) über $\mathbb{Z}_p$. Berechne unter Verwendung von $q(\alpha) = 0$ (d.h., $\alpha^n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$) die Potenzen von α. Gilt erstmals $\alpha^{p^n-1} = 1$ (d.h., $\alpha^j \neq 1$ für $1 \le j < p^n - 1$), so ist das gewählte $q(x)$ primitiv. Andernfalls versuche es mit einem neuen $q(x)$.

6.6.A Unterkörper von endlichen Körpern

Sei p eine feste Primzahl.

6.6.4 Satz. *Für jeden Teiler k von n hat $GF(p^n)$ genau einen Unterkörper der Kardinalität p^k.*
Umgekehrt: Wenn $GF(p^k)$ ein Unterkörper von $GF(p^n)$ ist, dann muss k ein Teiler von n sein.

Beweis. Wir überlegen zuerst, dass $x^{p^k} - x$ in $GF(p^n)$ in Linearfaktoren zerfällt:

- Wenn $a, b \in \mathbb{Z}$, $a|b$, dann gilt in $\mathbb{Z}[x]$ (und auch in $\mathbb{Z}_p[x]$): $x^a - 1|x^b - 1$, denn $x^b - 1 = (x^a - 1)(x^{b-a} + x^{b-2a} + \cdots + x^a + 1)$.
- Sei $n = km$. Dann gilt $x^k - 1|x^n - 1$ in $\mathbb{Z}[x]$, also $p^k - 1|p^n - 1$ in $\mathbb{Z}$.
- Daher $x^{p^k-1} - 1|x^{p^n-1} - 1$ in $\mathbb{Z}[x]$ (und auch in $\mathbb{Z}_p[x]$), daher $x^{p^k} - x|x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

- $x^{p^n} - x$ zerfällt in $GF(p^n)$ in Linearfaktoren, also auch $x^{p^k} - x$.

Sei $K \leq GF(p^n)$ der kleinste Körper, der alle Nullstellen von $x^{p^k} - x$ enthält; K ist Zerfällungskörper von $x^{p^k} - x$ über $\mathbb{Z}_p$, hat also p^k Elemente, und zwar alle Nullstellen von $x^{p^k} - x$.
Damit ist der erste Teil des Satzes bewiesen.
Wenn nun $GF(p^k)$ Unterkörper von $GF(p^n)$ ist, dann ist $GF(p^n)$ Vektorraum über $GF(p^k)$; sei $d := [GF(p^n) : GF(p^k)]$. Dann ist $p^n = (p^k)^d$, also $k|n$. □

6.7 Algebraisch abgeschlossene Körper

6.7.1 Satz. *Sei K Körper. Dann sind die folgenden Aussagen äquivalent:*

1) *Jedes nichtkonstante Polynom $p(x) \in K[x]$ hat eine Nullstelle in K.*
2) *Jedes nichtkonstante irreduzible Polynom in $K[x]$ hat eine Nullstelle in K.*
3) *Jedes nichtkonstante irreduzible Polynom in $K[x]$ hat einen linearen Faktor $x - \alpha \in K[x]$ (ist also linear).*
4) *Jedes nichtkonstante Polynom $p(x) \in K[x]$ zerfällt in Linearfaktoren.*
5) *Für jede algebraische Erweiterung $L \geq K$ gilt $L = K$.*

Jede der obigen Eigenschaften lässt sich also als Definition für den Begriff „K ist algebraisch abgeschlossen“ verwenden. (Vgl. auch 4.2.17.)

Beweis. $4 \Rightarrow 1 \Rightarrow 2$: trivial.
$2 \Leftrightarrow 3$: $p(\alpha) = 0$ genau dann, wenn $x - \alpha$ Teiler von p ist.
$3 \Rightarrow 4$: Jedes Polynom zerfällt in irreduzible Faktoren, diese müssen laut 3 alle linear sein.
$1 \Rightarrow 5$: Sei $\alpha \in L$. Da α algebraisch ist, hat α ein Minimalpolynom in $K[x]$. Dieses muss linear sein, also $\alpha \in K$.
$5 \Rightarrow 2$: Sei $p(x)$ irreduzibel und nicht konstant. Dann ist das von $p(x)$ in $K[x]$ erzeugte Ideal $(p(x))$ maximal, und $L := K[x]/(p(x))$ ist eine algebraische Körpererweiterung von K, in der $p(x)$ eine Nullstelle hat. Wegen $L = K$ hat p auch schon in K eine Nullstelle. □

6.7.2 Satz. *Sei K Körper, und sei L der Zerfällungskörper von ganz $K[x]$ über K. Dann ist L algebraisch abgeschlossen.*

Bemerkung: Jedes Polynom $p(x) \in K[x]$ hat eine Nullstelle in L; wir wollen zeigen, dass auch jedes Polynom aus $L[x]$ eine Nullstelle hat.

Beweis. Sei $L \leq L(\beta)$, β algebraisch über L. Zu zeigen ist $\beta \in L$.
β ist Nullstelle eines Polynoms $a_0 + \ldots + a_n x^n \in L[x]$. Alle Koeffizienten a_i sind in L, daher algebraisch über K.
Es ist also β algebraisch über $K(a_0, \ldots, a_n)$, und jedes a_i algebraisch über K. Nach einem bereits bewiesenen Satz ist dann auch β algebraisch über K. Sei $q(x)$ Minimalpolynom von β über K, dann zerfällt q in $L[x]$ in Linearfaktoren, einer davon muss $x - \beta$ sein, also $\beta \in L$. □

6.7.3 Folgerung. Zu jedem Körper K gibt es eine algebraisch abgeschlossene Erweiterung L. Insbesondere gilt: Der Zerfällungskörper von $K[x]$ ist der „algebraische Abschluss“ von K, das ist der (bis auf Isomorphie eindeutige) kleinste algebraisch abgeschlossene Körper $L \geq K$.

6.7.A Beispiele

Sei p eine Primzahl. Die Körper $GF(p^{n!})$ $(n = 1, 2, \ldots)$ bilden eine aufsteigende Kette:

$$GF(p) \leq GF(p^2) \leq GF(p^6) \leq GF(p^{24}) \leq GF(p^{120}) \leq \cdots$$

Die Vereinigung aller dieser Körper bezeichnen wir mit $GF(p^\infty)$. Offenbar ist $GF(p^\infty)$ Körper. Für jede Zahl $k \geq 1$ gilt $GF(p^k) \leq GF(p^{k!}) \leq GF(p^\infty)$, also enthält $GF(p^\infty)$ alle endlichen Körper der Charakteristik p.

6.7.4 Satz. *$GF(p^\infty)$ ist algebraisch abgeschlossen. $GF(p^\infty)$ ist sogar der kleinste algebraisch abgeschlossene Körper der Charakteristik p.*

Beweis. Sei $q(x) \in GF(p^\infty)[x]$ Polynom. Dann liegen alle Koeffizienten von q in einem geeigneten $GF(p^{k!})$, daher gibt es ein gemeinsames k mit $q(x) \in GF(p^{k!})[x]$.
Sei nun K der Zerfällungskörper von q über $GF(p^{k!})$. K ist eine endliche Erweiterung von $GF(p^{k!})$, ist also isomorph zu einem geeigneten $GF(p^n)$, $n \geq k$. In $GF(p^n)$ (und erst recht in $GF(p^{n!})$ und in $GF(p^\infty)$) zerfällt $q(x)$ in Linearfaktoren.
Für die Umkehrung: Sei L ein algebraisch abgeschlossener Körper der Charakteristik p. Dann zerfällt $x^{p^n} - x$ in $L[x]$ in Linearfaktoren, also enthält L den Körper $GF(p^n)$. □