Grundlagen aus der Algebra

Prof. Dr. Gabriele Nebe

1 Primkörper, Körpererweiterungen und Gradsatz

Definition 1.1. *Sei K ein kommutativer Ring mit 1. K heißt genau dann* **Körper***, wenn $(K \setminus \{0\}, \cdot)$ eine Gruppe ist.*

Definition 1.2. *Seien K, E Körper.*

(i) Das Paar (E/K) heißt **Körpererweiterung***, falls $K \subseteq E$ und $\cdot_K$, $+_K$ durch Einschränkung von $\cdot_E$, $+_E$ entstehen. K heißt dann* **Teilkörper** *von E, und E* **Erweiterungskörper** *von K.*

(ii) Die Körpererweiterung (E/K) heißt **endlich***, falls $[E : K] := dim_K E < \infty$. $[E : K]$ heißt der* **Grad** *von E über K.*

Beispiel. Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann ist $E := K[x]/(f)$ ein Körper und $K \hookrightarrow E, a \mapsto a\overline{1}$ eine Einbettung bezüglich der wir E als Körpererweiterung von K ansehen. Es ist $[E : K] =$Grad(f).

Satz 1.3. *(Gradsatz) Seien E_1, E_2, E_3 Körper mit $E_1 \subseteq E_2 \subseteq E_3$. Dann gilt: $[E_3 : E_1] = [E_3 : E_2] \cdot [E_2 : E_1]$.*

Beweis: Seien $[E_3 : E_2] = n < \infty, [E_2 : E_1] = m < \infty$. Sei weiter $(e_1, \ldots, e_n)$ eine E_2-Basis von E_3 und $(f_1, \ldots, f_m)$ eine E_1-Basis von E_2
Beh.: Dann ist $\mathcal{B} := (e_1 f_1, e_1 f_2, \ldots, e_n f_m)$ eine E_1-Basis von E_2
Bew.:

(i) $\mathcal{B}$ ist Erzeugendensystem: Sei $x \in E_3$. Dann existieren $\alpha_i \in E_2$, so dass $x = \sum_{i=1}^{n} \alpha_i e_i$.

Also existieren $\alpha_{ij} \in E_1$, so dass $\alpha_i = \sum_{j=1}^{m} \alpha_{ij} f_j$. Daraus folgt $x = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} e_i f_j$.

(ii) $\mathcal{B}$ ist linear unabhängig:

$$\text{Sei } \alpha_{ij} \in E_1, \text{ so dass } \sum_{i,j} \alpha_{ij} e_i f_j = 0. \text{ Dann gilt: } \sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha_{ij} f_j) e_i = 0.$$

Da aber nun die e_i über E_2 linear unabhängig sind, muss für alle i gelten:

$$\sum_{j=1}^{m} \alpha_{ij} f_j = 0$$

Da auch die f_j linear unabhängig sind (über E_1), folgt $\alpha_{ij} = 0$ für alle i, j.

Ist nun $[E_3 : E_2]$ oder $[E_2 : E_1]$ unendlich so folgt sofort, dass $[E_3 : E_1] = \infty$. □

Beispiele 1.

a) $[K(x) : K] = \infty$

b) $[K(x) : K(x^2)] = 2$

Bemerkung 1.4. *Sei R ein Integritätsbereich. $\psi : \mathbb{Z} \to R$ definiert durch $n \mapsto n \cdot 1$. Dann ist $Bild(\psi) \leq R$ ein Integritätsbereich, also $ker(\psi)$ ein Primideal in $\mathbb{Z}$. Also $ker(\psi) = (0)$ oder $ker(\psi) = (p)$ für eine Primzahl p.*
p heißt die Charakteristik von R, *$p = Char(R)$. Ist ψ injektiv, so setzen wir $Char(R) = 0$.*

Bemerkung: Man sieht auch leicht "zu Fuß", dass $\ker(\psi)$ entweder 0 oder ein Primideal ist. Denn sei ψ nicht injektiv und $n \in \mathbb{N}$ minimal mit $n \cdot 1 = 0$. Ist n keine Primzahl, dann gibt es $n_1, n_2 \in \mathbb{N}_{>1}$ mit $n = n_1 n_2$. Dann ist aber $0 = n \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1)$. Da R nullteilerfrei ist, gilt $(n_1 \cdot 1) = 0$ oder $(n_2 \cdot 1) = 0$, was ein Widerspruch zur Minimalität von n ist.

Satz 1.5. *Sei K ein Körper. Sei*

$$K_0 := \cap\{L \mid L \text{ ist Teilkörper von } K\}$$

der **Primkörper** *von K. Ist $Char(K) = 0$, so ist $K_0 \cong \mathbb{Q}$ isomorph zum Körper der rationalen Zahlen. Ist $Char(K) = p > 0$ eine Primzahl, so ist $K_0 \cong \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

Beweis: Klar ist K_0 ein Körper und $1 \in K_0$. Dann ist aber auch $1 + 1 = 2 \cdot 1$ in K_0 und also mit den Bezeichnungen aus Bemerkung 1.4 $\psi(\mathbb{Z}) \subset K_0$. Ist $Char(K) = p > 0$, so ist $ker(\psi) = (p) \trianglelefteq \mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$ und $\psi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ ein Körper. Also ist $K_0 = \psi(\mathbb{Z})$. Ist $Char(K) = 0$, dann ist ψ injektiv und $\mathbb{Z} \hookrightarrow K_0$. Da K_0 ein Körper ist, hat ψ eine eindeutig bestimmte Fortsetzung $\tilde{\psi} : \mathbb{Q} = Quot(\mathbb{Z}) \hookrightarrow K_0$. Also ist $K_0 = \mathbb{Q}$ in diesem Fall. □

Definition 1.6. *Sei (E/K) eine Körpererweiterung.*

(i) Für beliebige $a_1, \ldots, a_n \in E$ bezeichnet $K(a_1, \ldots, a_n)$ den kleinsten Teilkörper von E, der $K, a_1, \ldots, a_n$ enthält, und $R := K[a_1, \ldots, a_n]$ den kleinsten Teilring von E, der $K, a_1, \ldots, a_n$ enthält,

(ii) (E/K) heißt **einfache** *Körpererweiterung, falls ein $a \in E$* existiert *mit $E = K(a)$.*

Bemerkung:
$K(a_1, \ldots, a_n) = Quot(K[a_1, \ldots, a_n])$.
Insbesondere ist $K(x) = \{\frac{p(x)}{q(x)} \mid p, q \in K[x], q \neq 0\}$ der Körper der rationalen Funktionen.

Bemerkung 1.7. *Sei $E = K(a)$ einfache Körpererweiterung über K. Dann gilt entweder $E = K[a]$ oder $E \cong K(x)$. Im 1.Fall heißt a* **algebraisch** *über K. Im 2.Fall heißt a* **transzendent** *über K.*

BEWEIS: Sei $\varphi : K[x] \to K(a)$ der K-Algebrenhomomorphismus definiert durch $x \mapsto a$. Da $K(a)$ nullteilerfrei ist, ist auch $Bild(\varphi)$ ein Integritätsring. Also ist $\ker(\varphi)$ ein Primideal in dem Hauptidealbereich$K[x]$.

(i). $\ker(\varphi) \neq 0$. Dann ist $\ker(\varphi) = (m(x))$ für ein irreduzibles Polynom $m(x) \in K[x]$. (Es gilt $m(a) = 0$ in E und der normierte Erzeuger $\mu_{a,K}(x)$ von $\ker(\varphi)$ heißt das **Minimalpolynom** von a (über K).) Also ist $\ker(\varphi)$ ein maximales Ideal und daher $Bild(\varphi) = K[a]$ ein Körper, d.h. $K[a] = K(a) = E$.

(ii). $\varphi : K[x] \longrightarrow E$ ist injektiv. Also ist $Bild(\varphi) \cong K[x]$ kein Körper, aber $Bild(\varphi) = K[a]$ und $E = Quot(K[a]) \cong K(x)$.

□

Übung: Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann ist $K[a]$ ein endlich dimensionaler K-Vektorraum und $m_a : K]a] \to K[a], z \mapsto az$ eine K-linerare Abbildung. Es gilt $\mu_{a,K} = \mu_{m_a} = \chi_{m_a}$, d.h. das Minimalpolynom von a über K stimmt mit dem Minimalpolynom dieser linearen Abbildung überein. Es ist $(1, a, \ldots, a^{d-1})$ eine K-Basis von $K[a]$, $d = \text{Grad}(\mu_{a,K})$.

2 Zerfällungskörper.

Definition 2.1. *(i) Seien E_1 und E_2 Körper. Ein Ringhomomorphismus $\varphi : E_1 \longrightarrow E_2$ heißt auch* **Körperhomomorphismus**.
Ein Körperisomorphismus $\varphi : E \longrightarrow E$ heißt **Körperautomorphismus**.

(ii) Seien $(E_1/K), (E_2/K)$ Körpererweiterungen. Ein K-Algebrenhomomorphismus $\varphi : E_1 \longrightarrow E_2$ heißt **Körperhomomorphismus über** K.

(iii) $E_1 \overset{\cong}{_K} E_2$, falls K-Algebrenisomorphismus zwischen E_1 und E_2 existiert.

(iv) $\mathcal{A}ut(E) := \{\varphi | \varphi : E \longrightarrow E$ ist Körperautomorphismus$\}$
$\mathcal{A}ut_K(E) = \mathcal{A}ut(E/K) := \{\varphi | \varphi : E \longrightarrow E$ ist Körperautomorphismus über K $\}$

Beachte: Körperhomomorphismen sind immer injektiv. Denn der Kern ist ein Ideal, also $= 0$ oder $= E_1$. Aber 1 wird unter Körperhomomorphismen auf 1 abgebildet, also ist 1 nicht im Kern, also Kern $= 0$.

Bemerkung 2.2. *Sei $\psi : K \to K'$ ein Körperhomomorphismus. Dann gibt es genau einen Ringhomomorphismus $\tilde{\psi} : K[x] \to K'[x]$ der ψ fortsetzt, mit $\tilde{\psi}(x) = x$. Es gilt $\tilde{\psi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \psi(a_i) x^i$.*

Definition 2.3. *Sei K ein Körper und $f(t) \in K[t]$.*

(i) E heißt ein **Wurzelkörper** *von $f(t)$, falls (E/K) eine Körpererweiterung ist und ein $\xi \in E$* existiert *mit $f(\xi) = 0$.*

(ii) *Der Erweiterungskörper E von K heißt ein* **Zerfällungskörper** *von $f(t)$, falls $f(t)$ über E in Linearfaktoren zerfällt und E minimal ist, d.h. $f(t)$ zerfällt nicht in Linearfaktoren in $F[t]$ für $K \subseteq F \subset E$, $F \neq E$.*
(Dann existieren $\xi_i \in E$, so dass $f(t) = \prod(t - \xi_i)$ in $E[t]$.)
Beachte: $f(t)$ hat dann keine weiteren Wurzeln in E.

Satz 2.4. *Sei $f(t) = \sum_{i=0}^{n} a_i t^i \in K[t]$, $a_n \neq 0$ ein Polynom vom Grad $n \geq 1$.*

(i) *Ein Wurzelkörper von $f(t)$* existiert .

(ii) *Jeder minimale Wurzelkörper L von f ist von der Form $L = K[\alpha]$ mit $f(\alpha) = 0$.*

(iii) *Sei $f(t)$ irreduzibel in $K[t]$, $\psi : K \to K_1$ ein Körperisomorphismus, und $\tilde{\psi}$ wie in Bemerkung 2.2. Sei $f_1(t) = \sum_{i=0} \psi(a_i)t^i = \tilde{\psi}(f(t)) \in K_1[t]$. Ist $L = K[\alpha]$ ein minimaler Wurzelkörper von f und $L_1 = K_1[\alpha_1]$ ein minmaler Wurzelkörper von f_1, dann definiert $\psi_1 : L \to L_1, \sum_{i=0}^{m} a_i\alpha^i \mapsto \sum_{i=0}^{m} \psi(a_i)\alpha_1^i$ einen Körperisomorphismus (der ψ fortsetzt).*

(iv) *Insbesondere folgt aus (iii): Ist $f(t)$ irreduzibel in $K[t]$, so sind je zwei minimale Wurzelkörper isomorph über K.*

BEWEIS:

(i) Sei $\tilde{E} = K[t]/(f(t))$ "Wurzelring" mit $f(\bar{t}) = 0$ $(\bar{t} = t + (f(t)))$. Jedes maximale Ideal $I \trianglelefteq \tilde{E}$ liefert einen (sogar minimalen) Wurzelkörper $E = \tilde{E}/I$.
Alternativ sei f_1 ein irreduzibler Teiler von f in $K[t]$ und setze $E := K[t]/(f_1)$.

(ii) Ist L ein minimaler Wurzelkörper von f, so enthält L ein α mit $f(\alpha) = 0$. Da $K(\alpha) \leq L$ ein Wurzelteilkörper von L ist, folgt $L = K(\alpha)$. Weiter ist α algebraisch über K, also $L = K[\alpha]$.

(iii) Da $f(t) \in K[t]$ irreduzibel ist, ist auch sein Bild $f_1 = \tilde{\psi}(f) \in K_1[t]$ irreduzibel. Daher ist $L \cong K[t]/(f(t)) \cong K_1[t]/(f_1(t)) \cong L_1$.

□

Beispiel Das irreduzible Polynom $t^4 - 2 \in \mathbb{Q}[x]$ hat $\mathbb{Q}[\sqrt[4]{2}]$ und $\mathbb{Q}[i\sqrt[4]{2}]$ als minimale Wurzelkörper. Der Wurzelkörper ist also nicht physikalisch eindeutig, sondern nur bis auf Isomorphie.

Satz 2.5. *Sei $f(t) \in K[t] \setminus K$.*

(i) *Es gibt einen Erweiterungskörper von K, über welchem $f(t)$ in Linearfaktoren zerfällt.*

(ii) *Je zwei Zerfällungskörper von f sind isomorph über K.*

BEWEIS:

(i) folgt aus 2.4 durch Iteration.

(ii) Sei L ein Zerfällungskörper von f über K. Durch Induktion über $m := [L : K]$ zeigen wir: Ist $\psi : K \to K'$ ein Körperisomorphismus und L' ein Zerfällungskörper von $\tilde{\psi}(f) \in K'[t]$ über K', so lässt sich ψ zu einem Körperisomorphismus $\psi' : L \to L'$ fortsetzen.
Ist $m = 1$, dann zerfällt f in $K[t]$ in Linearfaktoren und $L' = K' \cong K = L$.
Sei also $m > 1$ und $g(t) \in K[t]$ ein irreduzibler Faktor von f vom Grad $d > 1$. Sei $g_1 := \tilde{\psi}(g)$. Sei $\alpha \in L$ mit $g(\alpha) = 0$ und $\alpha' \in L'$ mit $g_1(\alpha') = 0$. Dann sind die Teilkörper $L_1 = K[\alpha] \leq L$ und $L_2 = K'[\alpha'] \leq L'$ beides minimale Wurzelkörper von g (bzw. g_1) und nach Satz 2.4 (iii) lässt sich ψ zu einem Isomorphismus $\psi_1 : L_1 \to L_2$ fortsetzen. Weiter ist $[L : L_1] = \dim_{L_1}(L) = \frac{\dim_K(L)}{\dim_K(L_1)} = \frac{\dim_K(L)}{d} < [L : K]$ und L (bzw. L') ist ein Zerfällungskörper von $f(t) \in L_1[t]$ (bzw. $\tilde{\psi}_1(f(t)) \in L_2[t]$). Nach Induktionsvoraussetzung lässt sich ψ_1 zu einem Körperisomorphismus von L nach L' fortsetzen, der dann natürlich auch ψ fortsetzt.

□

3 Der algebraische Abschluss.

Bemerkung 3.1. *Sei L/K eine Körpererweiterung. Dann ist*

$$Alg_K(L) := \tilde{K} := \{a \in L \mid a \text{ ist algebraisch über } K\}$$

ein Teilkörper von L. $\tilde{K}$ heißt der **algebraische Abschluss von K in L.** *$\tilde{K}$ ist der größte Teilkörper von L, der algebraisch über K ist.*

Definition 3.2. *Ein Körper K heißt* **algebraisch abgeschlossen**, *falls jedes $f \in K[t]$ eine Nullstelle in K hat.*

Bemerkung 3.3. *Äquivalent sind:*

(i) K is algebraisch abgeschlossen.

(ii) Jedes irreduzible Polynom in $K[t]$ hat Grad 1.

(iii) Ist (L/K) eine algebraische Erweiterung, so gilt $L = K$.

Definition 3.4. *Sei K ein Körper. Ein Erweiterungskörper E von K heißt ein* **algebraischer Abschluss** *von K, falls*

(i) E ist algebraisch abgeschlossen.

(ii) (E/K) ist algebraisch.

Es gilt (ohne Beweis):

Satz 3.5. *(a) Jeder Körper K hat einen algebraischen Abschluss.*
(b) Je zwei algebraische Abschlüsse $\bar{K}$ und $\bar{K}'$ von K sind über K isomorph.

Der Beweis von (b) folgt aus

Lemma 3.6. *Sei $\bar{K}$ ein algebraischer Abschluss von K. Ist $K \subset L \subset F$ eine algebraische Erweiterung und $\varphi : L \to \bar{K}$ ein Ringhomomorphismus mit $\varphi_{|K} = id$, dann gibt es einen Ringhomomorphismus $\psi : F \to \bar{K}$ mit $\psi_{|L} = \varphi$.*

Der Beweis von Lemma 3.6 ist nicht konstruktiv, er benötigt das Lemma von Zorn, kann jedoch für endliche Erweiterungen konstruktiv gemachtwerden.

4 Endliche Körper.

Satz 4.1. *Sei K ein Körper und $U \leq K^*$ endlich. Dann ist U zyklisch, d.h. es gibt ein $z \in K$ mit $U =< z >$.*

Beweis. K^* ist eine abelsche Gruppe, also ist auch U eine endliche abelsche Gruppe. Angenommen U ist nicht zyklisch. Nach dem Hauptsatz über endliche abelsche Gruppen gibt es dann eine Primzahl p und eine Untergruppe $X := C_p \times C_p \cong \langle a, b\rangle \leq U$. Die p^2 Elemente von X erfüllen aber alle $x^p = 1$, sind also Nullstellen des Polynoms $t^p - 1 \in K[t]$. Dieses hat aber (da $K[t]$ faktoriell ist) höchstens p Nullstellen in K, ein Widerspruch. □

Lemma 4.2. *Sie K ein Körper und $f : K \to K$ ein Körperendomorphismus. Dann ist*

$$F := Fix(f) := \{k \in K \mid f(k) = k\}$$

ein Teilkörper von K.

Beweis. Mit $a, b \in F$ liegen auch $a + b$ und $a \cdot b$ in F. Weiter gilt $0, 1 \in F$ und für $0 \neq a \in F$ auch $a^{-1} \in F$. □

Lemma 4.3. *Ist K ein Körper der Charakteristik p, dann ist die Abbildung $\Phi_p : K \to K, a \mapsto a^p$ ein Körperendomorphismus von K, der sogenannte* Frobeniusendomorphismus. *Ist K endlich, so ist Φ_p bijektiv also ein Automorphismus von K, der* **Frobeniusautomorphismus**.

Beweis: Φ_p ist ein Ringhomomorphismus, denn $\Phi_p(ab) = \Phi_p(a)\Phi_p(b)$ und

$$\Phi_p(a + b) = (a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p \text{ für alle } a, b \in K.$$

Der Kern eines Ringhomomorphismus ist ein Ideal, also ist Φ_p injektiv und damit auch surjektiv, wenn K endlich ist. □

Satz 4.4. *Sei K ein endlicher Körper. Dann ist $Char(K) = p$ eine Primzahl und $|K| = p^n$ eine Potenz dieser Primzahl. Umgekehrt gibt es zu jeder Primzahlpotenz p^n genau einen Körper mit p^n Elementen. Dieser wird mit $\mathbb{F}_{p^n}$ bezeichnet.*

Beweis. Der Primkörper von K ist auch endlich und daher $\cong \mathbb{F}_p$ für eine Primzahl p. Also ist K ein endlich dimensionaler $\mathbb{F}_p$-Vektorraum und daher $|K| = p^n$ mit $n = [K : K_0]$.
Sei umgekehrt $n \in \mathbb{N}$ und p eine Primzahl.
Existenz: Sei K der Zerfällungskörper des Polynoms $f(t) = t^{p^n} - t \in \mathbb{F}_p[t]$. Dann gilt $f(t) = \prod_{i=1}^{p^n}(t - a_i) \in K[t]$ mit $Z := \{a_1, \ldots, a_{p^n}\} \subseteq K$. Da $ggT(f, f') = 1$ gilt $|Z| = p^n$, die Nullstellen von f sind also paarweise verschieden. Weiter gilt: $f(1) = f(0) = 0$ und $a \in K$ ist Nullstelle von f genau dann wenn $\Phi_p^n(a) = a$. Da die n-te Potenz des Frobeniusautomorphismus von K wieder ein Automorphismus von K ist, bilden die Nullstellen von f in K also einen Teilring von K, und damit $K = Z$.
Eindeutigkeit. Sei L ein Körper mit p^n Elementen. Dann ist der Primkörper $L_0 = \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Weiter ist $L^* = L \setminus \{0\}$ eine Gruppe mit $p^n - 1$ Elementen, also gilt $a^{p^n-1} = 1$ für alle $0 \neq a \in L$. Also enhält L die p^n verschiedenen Nullstellen von $t^{p^n} - t \in \mathbb{F}_p[t]$ und damit ist L der Zerfällungskörper dieses Polynoms. □

Bemerkung 4.5. *Jeder Erzeuger $a \in \mathbb{F}_{p^n}$ mit $\langle a \rangle = \mathbb{F}_{p^n}^*$ heißt* **Primitivwurzel** *von $\mathbb{F}_{p^n}$.*
Jede Primitivwurzel erzeugt den Körper $\mathbb{F}_{p^n} = \mathbb{F}_p[a]$.
Die Teilkörper von $\mathbb{F}_{p^n}$ sind genau die Körper $\mathbb{F}_{p^d}$ für die Teiler d von n.
Für $d \mid n$ ist

$$\mathbb{F}_{p^d} := \{a \in \mathbb{F}_{p^n} \mid a^{p^d} = a\} = Fix(\Phi_p^d).$$

Bemerkung 4.6. *Sei $\mathbb{F} = \mathbb{F}_{p^n}$ ein endlicher Körper und $\alpha \in \mathbb{F}^*$ eine Primitivwurzel. Sei m ein Teiler von n und $\mathbb{F}_{p^m} \cong K \leq \mathbb{F}$. Dann ist $\langle N_{\mathbb{F}/K}(\alpha) \rangle = K^*$.*

Beweis: Sei $n = md$. $Gal(\mathbb{F}/K)$ wird erzeugt von F^m. Also ist

$$\alpha N_{\mathbb{F}/K} = \alpha^{p^m + p^{2m} + \ldots + p^{dm}} \alpha^{1 + p^m + p^{2m} + \ldots + p^{(d-1)m}} = \alpha^{\frac{p^n - 1}{p^m - 1}}.$$

Da α ein Element der Ordnung $p^n - 1$ ist, ist $\alpha N_{\mathbb{F}/K} \in K^*$ ein Element der Ordnung $p^m - 1$, also eine Primitivwurzel. □

5 Separable Erweiterungen

Definition 5.1. *(i) Ein Polynom $f(t) \in K[t]$ heißt* **separabel**, *falls die Wurzeln von $f(t)$ in einem Zerfällungskörper von f paarweise verschieden sind.*

(ii) Sei (E/K) algebraische Körpererweiterung. $a \in E$ heißt **separabel**, *falls das Minimalpolynom über K von a separabel ist. (E/K) heißt* **separabel**, *falls jedes $a \in E$ separabel ist. (Beachte: Das Minimalpolynom ist irreduzibel über K.)*

(iii) Die Abbildung $': K[t] \longrightarrow K[t] :$ $\begin{array}{ccc} f(t) & \mapsto & f'(t) \\ \| & & \| \\ \sum_{i=0}^{n} a_i t^i & & \sum_{i=1}^{n} i a_i t^{i-1} \end{array}$ *heißt* **Ableitung** *von f.*

Lemma 5.2. *Seien $f, g \in K[x]$ und (E/K) eine Körpererweiterung. Sei weiter $h = ggT(f, g)$ in $K[x]$. Dann gilt: $h = ggT(f, g)$ in $E[x]$.*

BEWEIS: $*:$ $h = \alpha f + \beta g$ mit geeigneter Wahl von $\alpha, \beta \in K[x]$. Sei nun $s \in E[x]$ mit $s|f$ und $s|g$. Dann folgt mit $*$: $s|h$ (in $E[x]$). Da $h|f$ und $h|g$ in $K[x]$, also auch in $E[x]$ folgt $h = \mathrm{ggT}(f,g)$ in $E[x]$. □

Satz 5.3. *Sei $f \in K[t]$ vom Grad ≥ 1. f ist genau dann inseparabel, wenn $ggT(f,f') \neq 1$ in $K[t]$.*

BEWEIS: Wegen 5.2 sei O.B.d.A. K Zerfällungskörper von f.

"⇒" f ist genau dann inseparabel, wenn ein $a \in K$ existiert mit $(t-a)^2 | f(t)$. Das impliziert $f(t) = (t-a)^2 \cdot g(t)$ mit $g(t) \in K[t]$; $f' = 2(t-a)\cdot g(t) + (t-a)^2 g'(t) = (t-a)\underbrace{[2g(t) + (t-a)g'(t)]}_{\in K[t]}$. Also $(t-a)|ggT(f,f')$.

"⇐" $(t-a)|ggT(f,f')$ impliziert $f(t) = (t-a)h(t)$ und $f'(t) = h(t) + (t-a)h'(t)$, daraus folgt $(t-a)|h(t)$, also $f(t) = (t-a)^2\tilde{h}(t)$.

□

BEISPIELE 2.

a) Jedes irreduzible Polynom über $\mathbb{Q}$ ist separabel.

b) $t^p - x \in \mathbb{F}_p(x)[t]$ ist irreduzibel aber inseparabel, denn es gilt: $(t^p - x)' = pt^{p-1} \equiv 0 \pmod p$. Dann gilt $ggT(0, t^p - x) = t^p - x$.

Definition 5.4. *K heißt* **perfekt** *(vollkommen), falls jede endliche Erweiterung von K separabel ist. (d.h. jedes irreduzible Polynom in $K[t]$ ist separabel)*

Satz 5.5. *(i) Falls $Char(K) = 0$, so ist K perfekt.*

(ii) Falls $|K| < \infty$, so ist K perfekt.

BEWEIS:

(i) Sei $f(t) \in K[t]$ irreduzibel und $grad(f) \geq 1$. Dann ist $f'(t) \neq 0$ und $grad(f') < grad(f)$. Also gilt $ggT(f,f') = 1$.

(ii) Sei $f \in K[t]$ irreduzibel. Es sind nun 2 Fälle zu unterscheiden :

(i). $f' \neq 0$, dann gilt $ggT(f,f') = 1$ (wie oben).

(ii). $f' = 0$. Sei $f(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_0$. Dann ist $f'(t) = na_n t^{n-1} + (n-1)a_{n-1}t^{n-2} + \ldots + a_1 = 0$. $ia_i = 0$ für alle $i = 1 \ldots n$, falls $a_i \neq 0$, dann $p|i$.
Beh.: $f = g^p$ für ein $g \in K[t]$.
Da $a \mapsto a^p$ eine bijektive Abbildung von K ist, gibt es $b_i \in K$ mit $b_i^p = a_i$ $(0 \leq i \leq n)$. Sei $g := \sum_i b_i t^{i/p}$.

Dann gilt $g^p = \sum_i b_i^p t^i = f$.

□

Erinnerung: Eine Körpererweiterung L/K heißt einfach, falls ein $x \in L$ existiert mit $L = K(x)$. In dem Fall nennt man x auch ein **primitives Element** von L/K.

Satz 5.6. *(Satz vom primitiven Element) Sei $L = K(y, z)$ eine endliche Körpererweiterung von K so dass z separabel über K ist. Dann gibt es ein $x \in L$ mit $L = K(x)$.*

Beweis. Für endliche Körper ist dies aus dem Struktursatz ersichtlich. Sei also Œ K unendlich. Seien μ_y und μ_z die Minimalpolynome von y bzw. z über K und E ein Zerfällungskörper von $\mu_y\mu_z$ über L. Dann ist

$$\mu_y = \prod_{i=1}^{n}(t - y_i), \mu_z = \prod_{i=1}^{m}(t - z_i) \in E[t]$$

mit $z_i \neq z_j$ für alle $i \neq j$. Sei Œ $z = z_1, y = y_1$. Da K unendlich ist, gibt es ein $a \in K$ mit

$$y_i + az_j \neq y + az \text{ für alle } 1 \leq i \leq n, 2 \leq j \leq m.$$

Setze $x := y + az$.
Behauptung. $K(x) = L$:
Weil $\mu_y(x - az) = \mu_y(y) = 0$ gilt, ist z Nullstelle von $h := \mu_y(x - at) \in K(x)[t]$. Also ist z auch Nullstelle von $f := \mathrm{ggT}(h, \mu_z)$ in $K(x)[t]$. Ist $j \neq 1$, so gilt $h(z_j) = \mu_y(y + az - az_j) \neq 0$ nach Konstruktion von a. Also ist $(t - z)$ der einzige gemeinsame Teiler von h und μ_z und somit $f = t - z \in K(x)[t]$, woraus sich $z \in K(x)$ ergibt. □

Folgerung 5.7. *Jede endliche separable Körpererweiterung ist einfach. Sei $E = K[\alpha] \cong K[X]/(\mu_\alpha(X))$ endlich und separabel und $n := [L : K]$ der Grad von μ_α. Über einem algebraischen Abschluss $\overline{K}$ von K zerfällt $\mu_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i)$ in ein Produkt von n paarweise verschiedenen Linearfaktoren. Es gibt genau n verschiedene K-lineare Körperhomomorphismen $\sigma_i : E \to \overline{K}$. Diese sind gegeben durch $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, n$.*

6 Normale Erweiterungen

Definition 6.1. *Sei K ein Körper und $\bar{K}$ sein algebraischer Abschluss. Eine algebraische Erweiterung $K \subset E \subset \bar{K}$ heißt* **normal** *über K, falls für jeden K-Algebrenhomomorphismus $\varphi : E \to \bar{K}$ gilt $\varphi(E) = E$.*

Beispiel. $E := \mathbb{Q}[\sqrt[4]{2}]$ ist nicht normal über $\mathbb{Q}$, da z.B. der durch $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ definierte $\mathbb{Q}$-Algebrenhomomorphismus von E in $Alg_{\mathbb{Q}}(\mathbb{C}) \cong \bar{\mathbb{Q}}$ den Körper E nicht in sich selbst abbildet.

Satz 6.2. *Äquivalent sind:*

(i) (E/K) normal.

(ii) Jedes irreduzible Polynom in $K[t]$, das eine Nullstelle in E hat, zerfällt in $E[t]$ in Linearfaktoren.

(iii) Das Minimalpolynom jedes Elements von E über K zerfällt in $E[t]$ in Linearfaktoren.

(iv) Das Minimalpolynom jedes Erzeugers von E über K zerfällt in $E[t]$ in Linearfaktoren.

BEWEIS: (i) $\Rightarrow$ (ii) Sei $f \in K[t]$ irreduzibel, $\alpha \in E$ eine Nullstelle von f. Sei $\beta \in \bar{K}$ eine weitere Nullstelle von f. Zu zeigen: $\beta \in E$. Es gilt $K[\alpha] \cong K[\beta]$. Dieser Isomorphismus lässt sich nach Lemma 3.6 zu einem Körperhomomorphismus $\varphi : E \to \bar{K}$ fortsetzen. Da E normal ist, gilt $\varphi(E) = E$. Also gilt $\beta \in E$.
(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) Klar.
(iv) $\Rightarrow$ (i) Sei $\varphi : E \to \bar{K}$ ein Körperhomomorphismus mit $\varphi_{|K} = id$. Sei α ein Erzeuger von E über K, $\beta = \varphi(\alpha) \in \text{Bild}(\varphi)$ und sei $f(t) \in K[t]$ das Minimalpolynom von β. Dann ist $f(t)$ auch das Minimalpolynom von $\alpha \in E$. Nach Voraussetzung zerfällt f in Linearfaktoren in $E[t]$, d.h. E enthält alle Nullstellen von f in $\bar{K}$ und damit auch β. □

Beispiel Die Eigenschaft, normal zu sein, ist nicht transitiv. Sei $L = \mathbb{Q}[\sqrt{2}]$ und $E = \mathbb{Q}[\sqrt[4]{2}]$. Dann sind $(L/\mathbb{Q})$ und (E/L) normale Erweiterungen, als Erweiterungen vom Grad 2, aber $(E/\mathbb{Q})$ ist nicht normal.

Satz 6.3. *Eine endliche Erweiterung (E/K) ist normal, genau dann wenn E der Zerfällungskörper eines Polynoms in $K[t]$ ist.*

BEWEIS: $\Rightarrow$: Sei (E/K) normal. Da E endlich ist, gibt es $a_1, \ldots, a_n \in E$ mit $E = K[a_1, \ldots, a_n]$. Ist p_i das Minimalpolynom von a_i über K, so ist E der Zerfällungskörper von $\prod_{i=1}^{n} p_i$.
$\Leftarrow$: Sei E der Zerfällungskörper eines Polynoms p in $K[t]$. Dann ist E von den Nullstellen $a_1, \ldots, a_n$ von p über K erzeugt und das Minimalpolynom jedes dieser a_i über K teilt p und zerfällt daher in $E[t]$ in Linearfaktoren. Also ist E normal über K. □

Satz 6.4. *Sei E/K eine algebraische Körpererweiterung. Dann gibt es eine eindeutig bestimmte minimale normale Körpererweiterung $\tilde{E}/K$, mit $E \subseteq \tilde{E}$. $\tilde{E}$ heißt die* **normale Hülle** *von E über K.*
Ist E/K endlich, so auch $\tilde{E}/K$.

BEWEIS: Setze $\tilde{E}$ gleich dem Zerfällungskörper aller Minimalpolynome (über K) von Elementen von E. Dann ist $\tilde{E}/K$ normal und $\tilde{E}$ minimal. Ist $E = K[a_1, \ldots, a_n]$ endlich über K, so ist $\tilde{E}$ der Zerfällungskörper des Produkts der Minimalpolynome der a_i und damit endlich über K. □

7 Galoiserweiterungen

Wiederholung: Eine algebraische Körpererweiterung E/K heißt **normal**, falls für jeden K-Algebrenhomomorphismus $\varphi : E \to \overline{E} \cong \overline{K}$ in einen algebraischen Abschluss von E gilt, dass $\varphi(E) = E$ ist. Da man K-Automorphismen von E zu K-Automorphismen von $\overline{K}$ fortsetzen kann (Lemma 3.6) liefert also die Einschränkung einen Gruppenepimorphismus

$$\text{Aut}_K(\overline{K}) \to \text{Aut}_K(E), \varphi \mapsto \varphi_{|E}.$$

Der Kern dieses Epimorphismus ist $\mathrm{Aut}_E(\overline{E})$ ein Normalteiler in $\mathrm{Aut}_K(\overline{K})$ und es gilt

$$\mathrm{Aut}_K(E) \cong \mathrm{Aut}_K(\overline{K})/\,\mathrm{Aut}_E(\overline{K}).$$

Eine Erweiterung E/K ist genau dann normal, wenn jedes Minimalpolynom eines Elements von E in $E[t]$ in Linearfaktoren zerfällt.

Eine algebraische Körpererweiterung E/K heißt **separabel**, falls das Minimalpolynom eines jeden Elements von E in $\overline{K}[t]$ in paarweise verschiedene Linearfaktoren zerfällt. Für jedes $a \in E$ gilt also $\mathrm{ggT}(\mu_a, \mu_a') = 1$.

Eine endliche Erweiterung E/K ist genau dann separabel, wenn

$$[E:K] = [E:K]_s = |\,\mathrm{Hom}_K(E, \overline{K})|.$$

Folgerung 7.1. *Eine endliche Körpererweiterung E/K ist genau dann normal und separabel wenn $|\,\mathrm{Aut}_K(E)| = [E:K]$.*

Definition 7.2. *Sei M ein Monoid und K ein Körper. Ein Homomorphismus $\lambda : M \longrightarrow K^*$ heißt* **Charakter** *(von M über K).*

Satz 7.3. (Artin) *Sei M ein Monoid und K ein Körper. Je n verschiedene Charaktere über K sind linear unabhängig (als Elemente von K^M).*

Beweis: Induktion über n: $n = 1$: klar
$n-1 \to n$: Seien $\sigma_1, \ldots, \sigma_n$ Charaktere. Ann.: $\sigma_1, \ldots, \sigma_n$ sind linear abhängig. Dann existieren $a_i \in K$ mit nicht alle $a_i = 0$, so dass gilt:

$$*: \; a_1\sigma_1(m) + \ldots + a_n\sigma_n(m) = 0 \text{ für alle } m \in M.$$

Mit der Induktionsannahme folgt $a_i \neq 0$ für alle i . Sei nun $m_0 \in M$. Setzt man nun $m_0 m$ für m in $*$ ein und bildet zum anderen $\sigma_1(m_0)*$, so erhält man nach Bildung der Differenz:

$$-\left\{\begin{array}{l} a_1\sigma_1(m_0)\sigma_1(m) + \quad \ldots \quad \ldots\ldots + a_n\sigma_n(m_0)\sigma_n(m) = 0 \\ a_1\sigma_1(m_0)\sigma_1(m) + a_2\sigma_1(m_0)\sigma_2(m)) + \ldots + a_n\sigma_1(m_0)\sigma_n(m) = 0 \end{array}\right.$$

$$\underbrace{a_1(\sigma_1(m_0) - \sigma_1(m_0))\sigma_1(m)}_{=0} + \ldots\ldots\ldots + \underbrace{a_n(\sigma_n(m_0) - \sigma_1(m_0))}_{\text{neueKoeff.}}\sigma_n(m) = 0 \qquad \text{für alle } m \in M$$

Nun sind $\sigma_2, \ldots, \sigma_n$ linear unabhängig (nach Ind.Ann). Damit gilt: $a_i(\sigma_i(m_0) - \sigma_1(m_0)) = 0$ für alle $i = 1, \ldots, n$. Da die a_i alle ungleich 0 sind, folgt $\sigma_i(m_0) = \sigma_1(m_0)$ für alle $i = 1, \ldots, n$. $m_0 \in M$ war beliebig gewählt, also gilt: $\sigma_i = \sigma_1$. Dies ist ein Widerspruch. □

Folgerung 7.4. *Sei L/K eine separable Körpererweiterung vom Grad n und* $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ *Für $(v_1, \ldots, v_n) \in L^n$ gilt:*

$$(v_1, \ldots, v_n) \text{ ist } K\text{-Basis von } L \Leftrightarrow \det((\sigma_i(v_j))_{i,j=1}^n) \neq 0.$$

Beweis. als Übung. □

Hauptsatz 7.5. *Sei E ein Körper und $G \leq \mathrm{Aut}(E)$.*
Sei $K = Fix_G(E) := \{k \in E | gk = k \text{ für alle } g \in G\}$ der Fixkörper von G.
Dann gilt: $[E:K] = |G|$.

BEWEIS: Sei $r := [E : K]$ und $n := |G|$.
Sei zunächst $r < \infty$. Dann ist $E = K[a_1, \ldots, a_d]$ für gewisse $a_i \in E$. Jeder K-Automorphismus von E ist durch die Bilder der a_i eindeutig bestimmt. Ist m_i der Grad des Minimalpolynoms von a_i über K, so gibt es höchstens m_i mögliche Bilder von a_i in E. Also gilt $n = |G| \leq |\operatorname{Aut}_K(E)| \leq m_1 \cdot \ldots \cdot m_d < \infty$.
(i) Zeige $r \geq n$.
Annahme: $r < n$. Dann ist $n < \infty$. Nun fasst man $g \in G$ als Charakter auf $g : E^* \longrightarrow E^*,\ x \mapsto gx$. Sei $(a_1, \ldots, a_r)$ eine K-Basis von E. Dann ist

$$\sum_{g \in G} x_g(ga_i) = 0 \text{ für } i = 1, \ldots, r \tag{7.1}$$

ein lineares homogenes Gleichungssystem in x_g über E mit r Gleichungen und $n = |G| > r$ Unbekannten. Damit existiert eine nichttriviale Lösung $(x_g)_{g \in G}$. Da alle Elemente in E K-Linearkombinationen der a_i sind und G aus K-linearen Abbildungen besteht, gilt $\sum_{g \in G} x_g g = 0$ (als lineare Abbildung von E nach E). Also ist G linear abhängig, was einen Widerspruch zu Satz 7.3 impliziert.
(ii) Zeige $n \geq r$. Sei nun o.B.d.A. n endlich (d.h., $|G| < \infty$).

$$S : E \longrightarrow K : a \mapsto \sum_{g \in G} ga \text{ ist eine K-lineare Abbildung. Nach 7.3 ist } S \neq 0.$$

Zeige nun: Sind $a_1, \ldots, a_{n+1} \in E$, so sind $(a_1, \ldots, a_{n+1})$ linear abhängig über K.
Bew.:$* : \sum_{i=1}^{n+1} x_i(g^{-1}a_i) = 0$ mit $g \in G$ ist ein homogenes lineares Gleichungssystem in x_i über E mit $|G| = n$ Gleichungen und $n + 1$ Unbekannten. Also existiert eine nichtriviale Lösung von $* : (x_1, \ldots, x_{n+1})$. O.B.d.A. sei $S(x_1) \neq 0$ (durch eine Permutation der Indizes wird erreicht, dass $x_1 \neq 0$ und durch Multiplikation mit einem geeigneten Element aus E wird erreicht, dass $S(x_1) \neq 0$) Nun bildet man $g *$und summiert anschließend über alle $g \in G$. Man erhält:

$$\sum_{g \in G} \sum_{i=1}^{n+1} a_i g(x_i) = \sum_{i=1}^{n+1} a_i \underbrace{S(x_i)}_{\in K} = 0 \text{ mit } S(x_1) \neq 0$$

Also sind $(a_1, \ldots, a_{n+1})$ linear abängig über K . □

Folgerung 7.6. *Seien die Voraussetzungen wie bei 7.5 mit $|G| < \infty$. Dann gilt:*
$G = \operatorname{Aut}_K(E)$.

BEWEIS: Falls $G < \operatorname{Aut}_K(E)$, so wendet man 7.5 auf $\tilde{G} = \operatorname{Aut}_K(E)$ an. Sei nun $\tilde{K}$ der $\tilde{G}$-Fixkörper: $|G| = [E : K] \overset{K \subseteq \tilde{K}}{\geq} [E : \tilde{K}] \overset{7.5}{=} |\tilde{G}| > |G|$. Dies ist ein Widerspruch, also gilt: $\tilde{G} = G$. □

Folgerung 7.7. *Sei E/K eine endliche Körpererweiterung und $G = \operatorname{Aut}_K(E)$, so gilt:*

(i) $|G| \leq [E : K]$

(ii) $|G| = [E : K]$ *genau dann, wenn* $K = Fix_G(E)$.

BEWEIS: $\tilde{K} := Fix_G(E) \supseteq K$, also gilt $[E:K] \geq [E:\tilde{K}] \overset{7.5}{=} |G|$. □

Definition 7.8. *Eine endliche Körpererweiterung (E/K) heißt* **galoissch**, *falls* $|\operatorname{Aut}_K(E)| = [E:K]$. *Dann heißt* $G = Gal(E/K) := \operatorname{Aut}_K(E)$ *die* **Galoisgruppe** *von E über K.*

Satz 7.9. *Für eine endliche Körpererweiterung E/K sind äquivalent:*

(1) E/K ist Galoiserweiterung.

(2) E/K ist normal und separabel, also Zerfällungskörper eines separablen Polynoms.

(3) $K = \operatorname{Fix}_G(E)$ für eine endliche Untergruppe G von $\operatorname{Aut}(E)$.

BEWEIS: (1) $\Leftrightarrow$ (2) ist Folgerung 7.1.
(3) $\Rightarrow$ (2): Sei $a \in E$. Betrachte die Bahn von a unter G.

$$Ga = \{a = a_1, \ldots, a_n\}.$$

Das Polynom $p_a(x) := \prod_{i=1}^{n}(x - a_i) \in E[x]$ ist invariant unter der Operation von G auf $E[x]$ vermöge $g(\sum b_i x^i) := \sum g(b_i)x^i$ liegt also im Fixring $K[x]$ (da $\operatorname{Fix}_G(E) = K$). Insbesondere zerfällt das Minimalpolynom von a über K (welches ja p_a teilt) in paarweise verschiedene Linearfaktoren in $E[x]$. Damit ist E normal und separabel.
(1) $\Rightarrow$ (3): Folgt aus Folgerung 7.7 □

Folgerung 7.10. *Sei E/K galoissch mit Galoisgruppe G. Ist $a \in E$, so operiert G transitiv auf den Nullstellen des Minimalpolynoms von a über K. Der Stabilisator ist die Galoisgruppe von E über $K[a]$,*

$$\operatorname{Stab}_G(a) = Gal(E/K[a])$$

.

Hauptsatz 7.11. Fundamentalsatz der Galois-Theorie: *Sei (E/K) Galoiserweiterung und $G = \operatorname{Aut}_K(E)$. Dann gilt:*

(i) $|G| = [E:K]$

(ii)
$$\begin{array}{ccccc} \Phi : \mathcal{U}(G) = \{U | U \leq G\} & \longrightarrow & \mathcal{Z}(K,E) = \{F | F \text{ ist ein Körper und } K \leq F \leq E\} \\ U & \mapsto & Fix_U(E) \end{array}$$
ist eine inklusionsumkehrende Ähnlichkeit, wobei G auf $\mathcal{U}$ durch Konjugation und auf $\mathcal{Z}(K,E)$ durch Anwenden operiert.

BEWEIS:

(i) Dies ist sofort klar.

(ii) Zeige: Φ ist injektiv.
Sei $U_i \leq G$ mit $\Phi(U_1) = \Phi(U_2)$. Ersetzt man U_2 durch $\langle U_1, U_2\rangle$ (beachte $\Phi(\langle U_1, U_2\rangle) = \Phi(U_2)$), so kann man o.B.d.A. annehmen, dass $U_1 \leq U_2$. Außerdem gilt: $|U_1| = [E : \Phi(U_1)] = [E : \Phi(U_2)] = |U_2|$. Also gilt: $U_1 = U_2$.
Zeige: Φ ist surjektiv.

Ist $F \in \mathcal{Z}$, so ist E/F galoissch, denn E ist Zerfällungskörper eines separablen Polynoms $f(t) \in K[t] \subset F[t]$. Setze $U := \mathrm{Aut}_F(E) \leq \mathrm{Aut}_K(E)$. Dann ist $F = \Phi(U)$.
Dass Φ G-verträglich ist, folgt wegen $\mathrm{Fix}_{gUg^{-1}}(E) = g(\mathrm{Fix}_U(E))$.
Die inklusionsionsumkehrende Eigenschaft folgt sofort.

□

Folgerung 7.12. *Mit den Bezeichnungen aus 7.11 gilt:*
$U \leq G$ genau dann ein Normalteiler von G, wenn $(\Phi(U)/K)$ galoissch ist. Dann ist $Gal_K(\Phi(U)) \cong G/U$ vermöge Einschränken.
(E/F) ist galoissch für alle $F \in \mathcal{Z}(K, E)$.

Folgerung 7.13. *(Satz vom primitiven Element) Sei (E/K) endlich und separabel. Dann existiert ein $a \in E$ mit $E = K[a]$. (a heißt ein* **primitives Element***.)*

Beweis: Ist $|K| < \infty$, so folgt dies aus dem Struktursatz für endliche Körper (jeder Erzeuger von K^* ist ein solches primitives Element). Sei also $|K| = \infty$. Zwischen E und K liegen nur endlich viele Zwischenkörper, also wird die Behauptung für jedes $a \in E \backslash \{$endlich viele Zwischenkörper$\}$ erfüllt. □