Skript zur Algebra II
Teil 1

Vorlesung im Wintersemester 2005
an der Technischen Universität Berlin
Prof. Dr. F. Heß

20. Oktober 2005

Inhaltsverzeichnis

Vereinbarungen

Folgende allgemeine Festlegungen sollen gelten: Ein Ring R ist (wenn nicht anders vermerkt) kommutativ und hat ein Einselement 1_R oder kurz 1. Jeder Homomorphismus $\phi : R \to S$ der Ringe R und S erfüllt $\phi(1_R) = 1_S$. Jeder Teilring eines Rings R enthält 1_R. Der Nullring ist $R = \{0\}$.

Kapitel 1

Algebraische Körpererweiterungen

Die zentralen Objekte dieses Kapitels sind algebraische Körpererweiterungen. Solche Erweiterungen ergeben sich bei der näheren Untersuchung algebraischer Eigenschaften von Nullstellen von Polynomen und treten heute in vielen, auch anwendungsbezogenen Bereichen der Mathematik auf.

Sei zum Beispiel $f \in \mathbb{Q}[t]$ ein irreduzibles Polynom und $a \in \mathbb{C}$ mit $f(a) = 0$. Man kann zeigen, daß alle algebraischen Ausdrücke in a der Form $g_1(a)/g_2(a)$ mit $g_1, g_2 \in \mathbb{Q}[t]$ und $g_2(a) \neq 0$ Nullstellen von Polynomen $h \in \mathbb{Q}[t]$ mit $\deg(h) \leq \deg(f)$ sind und einen Körper $\mathbb{Q}(a)$ bilden, welcher $\mathbb{Q}$ enthält. Wir werden so auf eine algebraische Körpererweiterung $\mathbb{Q}(a)/\mathbb{Q}$ geführt. Man kann dann beispielsweise schließen, daß für ein irreduzibles $h \in \mathbb{Q}[t]$ mit $\deg(h) > \deg(f)$ die Gleichung $h(b) = 0$ keine Lösung $b \in \mathbb{Q}(a)$ haben kann. In ähnlicher Weise läßt sich die Nichtlösbarkeit einiger klassischer Konstruktionsaufgaben mit Zirkel und Lineal nach geeigneter Algebraisierung beweisen.

1.1 Endliche, algebraische und transzendente Körpererweiterungen

Im folgenden bezeichnet E einen Körper und K einen Teilkörper. Wir bemerken, daß also per Definition $K \subseteq E$ gilt und K bezüglich der Addition und Multiplikation und bezüglich der Elemente $0, 1$ von E ein Körper ist. Insbesondere haben E und K den gleichen Primkörper. Ferner kann E auch als K-Vektorraum aufgefaßt werden. Dies ermöglicht, Methoden aus der linearen Algebra anzuwenden.

1.1 Definition. Das Paar (E, K) heißt Körpererweiterung und wird als E/K geschrieben. Der Körper E heißt ein Erweiterungskörper von K. Ein Teilkörper

F von E mit $K \subseteq F$ heißt Zwischenkörper der Erweiterung E/K.

1.2 Definition. Der Grad der Körpererweiterung E/K wird als die Dimension des K-Vektorraums E definiert und mit $[E : K]$ bezeichnet. Die Körpererweiterung E/K heißt endlich, wenn $[E : K]$ endlich ist.

Für $[E : K] = 2, 3$, usw. nennt man E/K quadratisch, kubisch, usw. Es gilt $[E : K] = 1$ genau dann, wenn $E = K$. Für $[E : K] = 1$ ist $1 \in E$ linear unabhängig über K und damit eine Basis von E als K-Vektorraum. Es folgt $E = \{\lambda \cdot 1 \mid \lambda \in K\} = K$.

Als Beispiele betrachte man $\mathbb{C}/\mathbb{R}$ und $\mathbb{R}/\mathbb{Q}$. Da sich jedes Element von $\mathbb{C}$ eindeutig als $\mathbb{R}$-Linearkombination von 1 und i schreiben läßt, folgt $[\mathbb{C} : \mathbb{R}] = 2$. Jeder endlich-dimensionale $\mathbb{Q}$-Vektorraum ist abzählbar. Daher ergibt sich $[\mathbb{R} : \mathbb{Q}] = \infty$.

1.3 Lemma. *Sei V ein E-Vektorraum. Dann ist V auch ein K-Vektorraum und es gilt* $\dim_K(V) = [E : K] \dim_E(V)$.

Beweis. Es ist klar, daß V ein K-Vektorraum ist. Sei $v_i \in V$ eine E-Basis von V und $e_j \in E$ eine K-Basis von E. Die Aussage des Lemmas ergibt sich, wenn wir zeigen, daß $e_j v_i$ eine K-Basis von V ist. Zum Beweis sei $v \in V$. Dann gibt es $\lambda_i \in E$ und $\mu_{i,j} \in K$ fast alle gleich Null mit $v = \sum_i \lambda_i v_i$ und $\lambda_i = \sum_j \mu_{i,j} e_j$. Zusammengenommen ergibt dies $v = \sum_{i,j} \mu_{i,j} e_j v_i$, also sind die $e_j v_i$ ein Erzeugendensystem. Seien nun die $\mu_{i,j} \in K$ fast alle gleich Null mit $\sum_{i,j} \mu_{i,j} e_j v_i = 0$. Mit $\lambda_i = \sum_j \mu_{i,j} e_j \in E$ gilt dann $\sum_i \lambda_i v_i = 0$. Es folgt $\lambda_i = 0$ für alle i und dann $\mu_{i,j} = 0$ für alle i, j wegen der Basiseigenschaft der v_i und e_j. □

1.4 Satz (Gradsatz)**.** *Ist F ein Zwischenkörper von E/K, so gilt*

$$[E : K] = [E : F][F : K].$$

Beweis. Folgt direkt aus Lemma 1.3. □

Sei E/K eine endliche Körpererweiterung und F ein Zwischenkörper von E/K. Gilt $[F : K] = [E : K]$, so folgt $F = E$. Aus $[E : F] = [E : K]$ ergibt sich $[F : K] = 1$ unter Verwendung von Satz 1.4 und damit $F = K$. Ist ferner $[E : K]$ eine Primzahl, so folgt $F = E$ oder $F = K$.

1.5 Definition. Sei R ein Teilring des Rings S und $A \subseteq S$. Dann heißt

$$R[A] = \cap\{T \mid T \text{ Teilring von } S \text{ mit } R \cup A \subseteq T\}$$

der durch Adjunktion von A an R erzeugte Teilring von S. Ist S ein Körper, so heißt

$$R(A) = \cap\{T \mid T \text{ Teilkörper von } S \text{ mit } R \cup A \subseteq T\}$$

der durch Adjunktion von A an R erzeugte Teilkörper von S.

Es ist klar, daß es sich bei $R[A]$ und $R(A)$ um einen Teilring bzw. Teilkörper von S handelt. Außerdem ist $R(A)$ der Quotientenkörper von $R[A]$. Für $A = \{a_1, \dots, a_n\}$ schreiben wir auch $R[a_1, \dots, a_n]$ und $R(a_1, \dots, a_n)$.

Sei $\phi : R[t_1, \dots\ t_n] \to S$ der durch $t_i \mapsto a_i$ definierte Einsetzhomomorphismus. Dann haben wir $\phi(g) = g(a_1, \dots, a_n)$ für $g \in R[t_1, \dots t_n]$ und es ist nicht schwer zu zeigen, daß

$$\begin{aligned} R[a_1, \dots, a_n] &= \{\, g(a_1, \dots, a_n) \mid g \in R[t_1, \dots, t_n] \,\} \\ &= \operatorname{im}(\phi) \;\cong\; R[t_1, \dots, t_n]/\ker(\phi), \\ R(a_1, \dots, a_n) &= \{\, g(a_1, \dots, a_n)/h(a_1, \dots, a_n) \mid g, h \in R[t_1, \dots, t_n] \\ &\qquad\qquad \text{und } h(a_1, \dots, a_n) \neq 0 \,\}. \end{aligned}$$

Für $A \subseteq B$ ist $R[A]$ ein Teilring von $R[B]$ und $R(A)$ ein Teilkörper von $R(B)$. Desweiteren gilt $R[A_1 \cup A_2] = R[A_1][A_2]$ und $R(A_1 \cup A_2) = R(A_1)(A_2)$.

Sei I ein Integritätsring und K ein Körper, welcher ein Teilring von I ist. Es ist klar, daß I auch als K-Vektorraum aufgefaßt werden kann.

1.6 Lemma. *Ist die Dimension von I als K-Vektorraum endlich, so ist I ein Körper.*

Beweis. Sei $a \in I$, $a \neq 0$. Die Abbildung $\phi : I \to I$, $x \mapsto ax$ ist K-linear und injektiv, weil I ein Integritätsring ist. Dann ist ϕ auch surjektiv, weil I endlich dimensionaler K-Vektorraum ist. Also gibt es $b \in I$ mit $ab = 1$. $\square$

Aufgrund von Lemma 1.6 ist es nicht allgemeiner, Integritätsringe anstelle von Körpern als endliche Erweiterungen von Körpern zu betrachten. Ist E/K eine endliche Körpererweiterung und $A \subseteq E$, so folgt mit Hilfe von Lemma 1.6 auch $K[A] = K(A)$.

1.7 Definition. Eine Körpererweiterung E/K heißt endlich erzeugbar, falls es $a_1, \dots, a_r \in E$ mit $E = K(a_1, \dots, a_r)$ gibt. Eine Körpererweiterung E/K heißt einfach, wenn es ein $a \in E$ mit $E = K(a)$ gibt. Das Element a heißt dann primitives Element der Körpererweiterung E/K.

Zum Beispiel gilt $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$, so daß i ein primitives Element der Körpererweiterung $\mathbb{C}/\mathbb{R}$ ist.

1.8 Definition. Ein Element $a \in E$ heißt algebraisch über K, wenn es ein $f \in K[t]$ ungleich Null mit $f(a) = 0$ gibt. Ein Element $a \in E$ heißt transzendent über K, wenn es nicht algebraisch über K ist.

Die über $\mathbb{Q}$ algebraischen Elemente von $\mathbb{C}$ heißen algebraische Zahlen und sind Gegenstand der algebraischen Zahlentheorie. Ohne Beweis merken wir an, daß zum Beispiel e und π transzendent über $\mathbb{Q}$ sind. Da es nur abzählbar viele algebraische Zahlen gibt, enthält $\mathbb{R}$ überabzählbar viele transzendente Zahlen.

1.9 Definition. Eine Körpererweiterung E/K heißt algebraisch, wenn jedes $a \in E$ algebraisch über K ist. Andernfalls heißt E/K transzendent.

Wir wenden uns zunächst den algebraischen oder transzendenten Elementen zu. Zur Untersuchung eines solchen Elements $a \in E$ zieht man den Einsetzhomomorphismus $\phi_a : K[t] \to E$, $t \mapsto a$ heran. Nach dem Homomorphiesatz gilt $k[a] = \mathrm{im}(\phi_a) \cong K[t]/\ker(\phi_a)$, und a ist offensichtlich genau dann algebraisch über K, wenn $\ker(\phi_a) \neq \{0\}$. Eine andere Sichtweise ist, daß $a \in E$ genau dann algebraisch ist, wenn die Potenzen $1, a, a^2, \ldots$ linear abhängig über K sind.

1.10 Satz. *Sei $a \in E$ transzendent über K. Es gilt*

(i) $K[a] \cong K[t]$,

(ii) $K(a) \cong K(t)$, *wobei* $K(t) = \mathrm{Quot}(K[t])$ *der Körper der rationalen Funktionen in t über K ist,*

(iii) $[E : K] = [K(a) : K] = \infty$.

Beweis. Wäre a algebraisch, so wäre $\ker(\phi_a) \neq 0$. Nun gilt $K[a] \cong K[t]/\ker(\phi_a) \cong K[t]$, was *(i)* beweist. *(ii)* ergibt sich aus $K(a) = \mathrm{Quot}(K[a])$. *(iii)* folgt, da die Potenzen $1, a, a^2, \ldots$ linear unabhängig über K sind. □

1.11 Definition. Sei $a \in E$ algebraisch über K und $f \in K[t]$ normiert mit $\ker(\phi_a) = fK[t]$. Dann heißt f das Minimalpolynom von a über K und wird mit $m_{a,K}$ bezeichnet.

1.12 Satz. *Sei $a \in E$ algebraisch über K. Das Minimalpolynom ist das eindeutig bestimmte normierte Polynom kleinsten Grades über K, welches a als Nullstelle in E hat. Es ist irreduzibel in $K[t]$. Weiter gilt*

(i) $K[a] \cong K[t]/m_{a,K}K[t]$,

(ii) $K(a) = K[a]$,

(iii) $[K(a) : K] = \deg(m_{a,K})$.

Die Potenzen $1, a, a^2, \ldots, a^{\deg(m_{a,K})-1}$ bilden eine K-Basis von $K(a)$.

Beweis. Die Isomorphie in (i) gilt nach dem Homomorphiesatz angewendet auf ϕ_a, wegen $\ker(\phi_a) = m_{a,K}K[t]$. Weiter ist $K[a]$ als Teilring des Körpers E ein Integritätsring. Daher ist $\ker(\phi_a)$ ein Primideal. Da $K[t]$ Hauptidealring ist, ist $\ker(\phi_a)$ auch maximal und $K[a] \cong K[t]/\ker(\phi_a)$ ein Körper. Es folgt $K(a) = \mathrm{Quot}(K[a]) = K[a]$, also (ii). Die angegebenen a-Potenzen bilden dann eine K-Basis von $K[a]$, weil die entsprechenden t-Potenzen in $K[t]/m_{a,K}K[t]$ eine K-Basis des Quotientenrings bilden. Daraus und aus (ii) folgt (iii) und die letzte Aussage.

Da $\ker(\phi_a) = m_{a,K}K[t]$ ein Primideal ist, ist $m_{a,K}$ irreduzibel. Weil $\ker(\phi_a)$ aus allen Polynomen über K besteht, die a als Nullstelle in E haben, und $m_{a,K}$ der normierte Erzeuger von $\ker(\phi_a)$ ist, hat $m_{a,K}$ minimalen Grad und ist eindeutig bestimmt. Ein weiteres solches normiertes Polynom g hat nämlich zunächst den gleichen Grad wie $m_{a,K}$, da sich g und $m_{a,K}$ gegenseitig teilen müssen. Die Differenz $g - m_{a,K}$ ist dann ein Element von $\ker(\phi_a)$ echt kleineren Grads als $m_{a,K}$, und muß daher gleich Null sein. Also gilt $g = m_{a,K}$. □

Das Minimalpolynom von i über $\mathbb{R}$ ist zum Beispiel $m_{i,\mathbb{R}} = t^2 + 1$. Minimalpolynome werden auch in anderen Zusammenhängen analog definiert, müssen aber nicht mehr unbedingt irreduzibel sein. Siehe beispielsweise Minimalpolynome von Endomorphismen von endlich dimensionalen Vektorräumen.

Ein zweiter, konstruktiverer Beweis für Lemma 1.6 kann wie folgt geführt werden. Sei $a \in I$, $a \neq 0$. Die Potenzen $1, a, a^2, \ldots$ sind K-linear abhängig, da I ein endlich dimensionaler K-Vektorraum ist. Sei $f \in K[t]$ ein Polynom kleinsten Grads ≥ 1 mit $f(a) = 0$. Da I ein Integritätsring ist, muß f irreduzibel sein und es gilt insbesondere $f(0) \neq 0$. Mit $c = -f(0)$ gibt es ein $g \in K[t]$, so daß $f = gt - c$ und $gt/c = f/c + 1$. Für $b = g(a)/c \in I$ ergibt sich dann $ab = g(a)a/c = f(a)/c + 1 = 1$.

1.13 Satz. *Eine einfache transzendente Erweiterung E/K ist isomorph zu $K(t)$.*

Beweis. Ist $a \in E$ ein primitives Element, so ist a transzendent über K. Andernfalls wäre $[E : K] = [K(a) : K] < \infty$ nach Satz 1.12, im Widerspruch zu $[E : K] = \infty$ nach Satz 1.10. Es gilt daher $E = K(a) \cong K(t)$ nach Satz 1.10. □

Wir betrachten jetzt algebraische und endliche Körpererweiterungen. Ist E/K eine Körpererweiterung und $a \in E$ algebraisch über K, so ist a auch algebraisch über jedem Zwischenkörper F von E/K, da $m_{a,K} \in F[t]$, $m_{a,K} \neq 0$ und $m_{a,K}(a) = 0$ gilt.

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

(i) *E/K ist endlich,*

(ii) *E/K ist algebraisch und endlich erzeugbar,* *(iii) E/K ist endlich erzeugbar mit algebraischen Erzeugern.*

Beweis. $(i) \Rightarrow (ii)$: Sei E/K endlich. Jedes Element $a \in E$ ist algebraisch, weil die Potenzen $1, a, a^2, \dots$ linear abhängig über K sind. Ist $e_1, \dots, e_n \in E$ eine K-Basis von E, so gilt $E = K(e_1, \dots, e_n)$. Daher ist E/K algebraisch und endlich erzeugbar.

$(ii) \Rightarrow (iii)$: Ist klar.

$(iii) \Rightarrow (i)$: Sei nun E/K endlich erzeugbar mit den über K algebraischen Erzeugern $a_1, \dots, a_r \in E$, also $E = K(a_1, \dots, a_r)$. Setze $E_i = K(a_1, \dots, a_i)$, so daß $E_i = E_{i-1}(a_i)$. Weil jedes a_i algebraisch über K und somit nach der Bemerkung vor dem Satz auch algebraisch über E_{i-1} ist, gilt $[E_i : E_{i-1}] < \infty$ nach Satz 1.12. Daraus folgt $[E : K] = \prod_i [E_i : E_{i-1}] < \infty$ nach Satz 1.4. □

1.15 Satz. *Sei E/K eine Körpererweiterung und $A \subseteq E$. Sind die Elemente in A algebraisch über K, so ist $K(A)/K$ algebraisch und es gilt $K[A] = K(A)$.*

Beweis. Wir führen die Situation zunächst auf endliche Erweiterungen zurück. Es gilt $K(A) = \cup_M K(M)$, wobei M die endlichen Teilmengen von A durchläuft. Zunächst ist nämlich $K(M) \subseteq K(A)$ für alle M und somit $\cup_M K(M) \subseteq K(A)$. Es genügt nun zu zeigen, daß $\cup_M K(M)$ ein Körper ist, welcher K und A enthält. Seien dazu $a, b \in \cup_M K(M)$. Es gibt endliche Mengen $M_1, M_2 \subseteq A$ mit $a \in K(M_1)$ und $b \in K(M_2)$. Dann gilt weiter, daß $a, b \in K(M_1 \cup M_2)$, wobei $M_1 \cup M_2$ ebenfalls endlich ist. Somit sind $a + b, a - b, ab, a/b \in K(M_1 \cup M_2) \subseteq \cup_M K(M)$. Wegen $A = \cup_M M$ gilt $K, A \subseteq \cup_M K(M)$. Es folgt $K(A) = \cup_M K(M)$.

Für endliches $M \subseteq A$ ist $K(M)/K$ nach Satz 1.14 endlich und algebraisch. Also besteht $K(A) = \cup_M K(M)$ nur aus über K algebraischen Elementen. Für $a \in K[A]$ gilt $a^{-1} \in K[a]$ nach Satz 1.12, (ii). Wegen $K[a] \subseteq K[A]$ folgt also $a^{-1} \in K[A]$ und damit $K[A] = K(A)$. □

1.16 Satz. *Sei E/K eine Körpererweiterung und F ein Zwischenkörper. Dann ist E/K genau dann algebraisch, wenn E/F und F/K algebraisch sind.*

Beweis. Ist E/K algebraisch, so auch F/K. Außerdem gilt für $a \in E$, daß $m_{a,K} \in F[t]$ und somit a auch algebraisch über F ist. Umgekehrt sei $a \in E$ algebraisch über F und bezeichne L den Zwischenkörper von E/K, der durch Adjunktion der Koeffizienten von $m_{a,F}$ an K entsteht. Dann ist a wegen $m_{a,F} \in L[t]$ algebraisch über L. Weiter sind $L(a)/L$ und L/K endlich wegen Satz 1.14 und weil F/K algebraisch ist. Folglich ist $L(a)/K$ endlich nach Satz 1.4 und damit algebraisch nach Satz 1.14. Es ergibt sich, daß a algebraisch über K ist. □

Die Eigenschaft „algebraisch“ ist also transitiv. Dies gilt nach Satz 1.4 auch für die Eigenschaft „endlich“.

1.17 Definition. Sei E/K eine Körpererweiterung und $A \subseteq E$ die Menge der über K algebraischen Elemente von E. Dann heißt $K(A)$ der algebraische Abschluß von K in E. Gilt $K(A) = K$, so nennt man K algebraisch abgeschlossen in E.

1.18 Satz. *Der algebraische Abschluß von K in E ist ein Teilkörper von E und ist algebraisch abgeschlossen in E.*

Beweis. Die erste Aussage folgt direkt aus Theorem 1.15 und die zweite aus Satz 1.16. □

1.19 Definition. Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper. Dann wird $F_1F_2 = F_1(F_2) = F_2(F_1)$ als das Kompositum von F_1 und F_2 in E bezeichnet. Das Kompositum einer beliebigen Menge $\mathcal{F}$ von Zwischenkörpern von E/K definieren wir als $K(\cup\mathcal{F})$.

Etwas spezieller nennen wir auch F_1F_2/K das Kompositum von F_1/K und F_2/K und F_1F_2/F_2 die Translation von F_1/K um F_2 in E. Typischerweise stellt man solche Körpererweiterungen graphisch dar. Die Abbildung 1.1 enthält eine Zwischenkörpersituation, eine Translation und ein Kompositum.

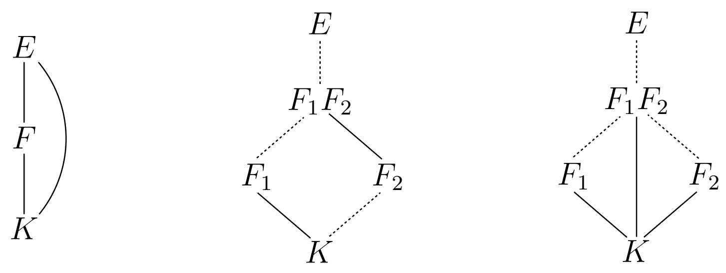

Abbildung 1.1: Zwischenkörper, Translation und Kompositum

Es ist nun natürlich, zu fragen, wie sich die Eigenschaften „endlich“ und „algebraisch“ innerhalb der Diagramme in Abbildung 1.1 fortsetzen. Die relevanten Körpererweiterungen sind hierbei mit durchgezogenen Linien markiert. Für das linke Diagramm haben wir oben bereits die Transitivität von „algebraisch“ und „endlich“ gesehen.

1.20 Satz. *Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper. Für die Translation F_1F_2/F_2 gilt:*

(*i*) *Ist F_1/K algebraisch, so auch F_1F_2/F_2.*

(*ii*) *Ist F_1/K endlich, so auch F_1F_2/F_2 und es gilt $[F_1F_2 : F_2] \leq [F_1 : K]$.*

Für das Kompositum F_1F_2/K gilt:

(*iii*) *Sind F_1/K und F_2/K algebraisch, so auch F_1F_2/K.*

(*iv*) *Sind F_1/K und F_2/K endlich, so auch F_1F_2/K und es gilt $[F_1F_2 : K] \leq [F_1 : K][F_2 : K]$.*

Beweis. (i) folgt aus Satz 1.15 angewendet auf $F_2(F_1)/F_2$, da die Elemente von F_1 auch algebraisch über F_2 sind. (iii) folgt aus (i) und Satz 1.16. (iv) folgt aus (ii) und der Gradformel $[F_1F_2 : K] = [F_1F_2 : F_2][F_2 : K] \leq [F_1 : K][F_2 : K]$. Zum Beweis von ($ii$) betrachte man $F_2[F_1]$. Jedes K-Erzeugendensystem von F_1 wird zu einem F_2-Erzeugendensystem von $F_2[F_1]$. Da F_1 nach Annahme eine endliche K-Basis besitzt, ist auch $F_2[F_1]$ endlich-dimensional über F_2 mit Dimension kleiner gleich $[F_1 : K]$. Nach Lemma 1.6 ist dann $F_2[F_1]$ ein Körper. Es folgt $F_1F_2 = F_2(F_1) = F_2[F_1]$ und (ii). □

Der Beweis zeigt also, daß für $[F_1 : K] < \infty$ jedes K-Erzeugendensystem von F_1 auch ein F_2-Erzeugendensystem von F_1F_2 liefert.

Sind $[F_1 : K]$ und $[F_2 : K]$ teilerfremd, so gilt $[F_1F_2 : K] = [F_1 : K][F_2 : K]$ wegen $[F_1 : K] \,|\, [F_1F_2 : K]$ und $[F_2 : K] \,|\, [F_1F_2 : K]$ nach Satz 1.4 und wegen Satz 1.20, (iv).

1.21 Definition. Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper von E/K. Dann heißen F_1/K und F_2/K linear disjunkt und F_1 und F_2 linear disjunkt über K, wenn jede über K linear unabhängige Menge von Elementen von F_1 über F_2 linear unabhängig bleibt.

Der folgende Satz zeigt unter anderem, daß die Eigenschaft „linear disjunkt" symmetrisch ist.

1.22 Satz. *Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper von E/K. Dann sind äquivalent.*

(*i*) *F_1 und F_2 sind linear disjunkt über K.*

(*ii*) *F_2 und F_1 sind linear disjunkt über K.*

(*iii*) *Sind $\{a_i \,|\, i \in I\}$ und $\{b_j \,|\, j \in J\}$ Mengen über K linear unabhängiger Elemente von F_1 beziehungsweise F_2, so ist $\{a_ib_j \,|\, i \in I, j \in J\}$ eine Menge über K linear unabhängiger Elemente von F_1F_2.*

Beweis. (i) $\Rightarrow$ (iii): Es gelte $\sum_{i,j} \mu_{i,j}a_ib_j = 0$ mit $\mu_{i,j} \in K$. Wir setzen $\lambda_i = \sum_j \mu_{i,j}b_j$, so daß $\lambda_i \in F_2$ und $\sum_{i,j} \mu_{i,j}a_ib_j = \sum_i \lambda_ia_i = 0$ gilt. Nach Voraussetzung ergibt sich $\lambda_i = 0$ für alle $i \in I$, und aus $\lambda_i = \sum_j \mu_{i,j} b_j = 0$ dann auch $\mu_{i,j} = 0$ für alle $j \in J$.

$(iii) \Rightarrow (i)$: Sei $\{a_i \mid i \in I\}$ eine Menge über K linear unabhängiger Elemente von F_1 und $\{b_j \mid j \in J\}$ eine K-Basis von F_2. Es gelte $\sum_i \lambda_i a_i = 0$ mit $\lambda_i \in F_2$. Es gibt $\mu_{i,j} \in K$ mit $\lambda_i = \sum_j \mu_{i,j} b_j$. Dann gilt $\sum_i \lambda_i a_i = \sum_{i,j} \mu_{i,j} a_i b_j = 0$ und nach Voraussetzung $\mu_{i,j} = 0$. Es ergibt sich $\lambda_i = 0$.

$(ii) \Leftrightarrow (iii)$: Aussage (iii) ist symmetrisch in F_1 und F_2, daher folgt der Beweis analog. □

1.23 Satz. *Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper von E/K.*

(i) *Für $[F_1 : K] < \infty$ sind F_1 und F_2 genau dann über K linear disjunkt, wenn $[F_1 : K] = [F_1F_2 : F_2]$ gilt.*

(ii) *Sind F_1 und F_2 linear disjunkt über K, so gilt $F_1 \cap F_2 = K$.*

(iii) *Bleibt eine K-Basis von F_1 über F_2 linear unabhängig, so sind F_1 und F_2 linear disjunkt über K.*

Beweis. (i): Aus $[F_1 : K] < \infty$ ergibt sich zunächst $F_1F_2 = F_2[F_1]$, und jedes K-Erzeugendensystem von F_1 ist auch ein F_2-Erzeugendensystem von F_1F_2.

„$\Rightarrow$“: Da eine K-Basis von F_1 nach Annahme auch eine F_2-Basis von F_1F_2 ist, folgt $[F_1 : K] = [F_1F_2 : F_2]$.

„$\Leftarrow$“: Jede über K linear unabhängige Teilmenge T von F_1 kann zu einer Basis von F_1 über K ergänzt werden. Diese ist ein Erzeugendensystem von F_1F_2 über F_2 und wegen der Gradgleichheit auch eine Basis von F_1F_2 über F_2. Somit ist T ebenfalls über F_2 linear unabhängig.

(ii): Gibt es $a \in F_1 \cap F_2 \backslash K$, so sind $1, a \in F_1$ zwar linear unabhängig über K, aber nicht linear unabhängig über F_2.

(iii): Übung. □

Als Beispiel betrachte man $K = \mathbb{Q}$, $F_1 = \mathbb{Q}(\sqrt{2})$ und $F_2 = \mathbb{Q}(i)$ mit $i^2 = -1$ als Teilkörper von $\mathbb{C}$. Dann gilt $F_1F_2 = \mathbb{Q}(\sqrt{2}, i)$ und $[F_1F_2 : F_1] = 2$. Also sind F_1 und F_2 linear disjunkt über K.

1.24 Lemma. *Sei E/K eine einfache algebraische Erweiterung mit primitivem Element a und F ein Zwischenkörper. Dann entsteht F durch Adjunktion der Koeffizienten von $m_{a,F}$ an K.*

Beweis. Sei L der durch die Adjunktion entstehende Körper. Da $m_{a,F} \in F[t]$ folgt $L \subseteq F$. Es gilt $m_{a,F} \in L[t]$ und $m_{a,F}$ erfüllt die Eigenschaften des Minimalpolynoms $m_{a,L}$. Daher ergibt sich $m_{a,L} = m_{a,F}$ und $[E : L] = [L(a) : L] = \deg(m_{a,L}) = \deg(m_{a,F}) = [F(a) : F] = [E : F]$. Es folgt $L = F$. □

1.25 Satz. *Die Körpererweiterung E/K ist genau dann einfach und algebraisch, wenn E/K nur endlich viele Zwischenkörper hat.*

Beweis. Lassen wir aus. □

Als Anwendung betrachten wir kurz Konstruktionsprobleme mit Zirkel und Lineal. Unter Vorgabe zweier Punkte mit Abstand 1 konstruiert man weitere Punkte als Schnittpunkte von Geraden und Kreisen. Geraden müssen durch zwei verschiedene, bereits konstruierte bzw. die vorgegebenen Punkte gelegt werden. Bei Kreisen muß der Mittelpunkt ein bereits konstruierter bzw. vorgegebener Punkt und der Radius gleich dem Abstand zweier bereits konstruierter bzw. der vorgegebenen Punkte sein. Wir nennen eine Zahl $a \in \mathbb{R}$ konstruierbar, wenn sie als Abstand zweier konstruierter Punkte erhalten werden kann.

Da Kreise quadratischen Gleichungen genügen, werden im Konstruktionsprozeß koordinatenweise gedacht neben dem Lösen von linearen Gleichungen „höchstens“ Quadratwurzeln gezogen. Daher gilt für eine konstruierbare Zahl $a \in \mathbb{R}$ notwendigerweise $a \in \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_n}) \subseteq \mathbb{R}$ mit geeigneten $b_i \in \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_{i-1}})$ und $b_i \geq 0$. Für konstruierbares a ist $[\mathbb{Q}(a) : \mathbb{Q}]$ also eine Potenz von 2. Man kann darüberhinaus zeigen, daß jedes $a \in \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_n}) \subseteq \mathbb{R}$ mit beliebigen $b_i \in \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_{i-1}})$ und $b_i \geq 0$ konstruierbar ist.

Beim Delischen Problem geht es um die Verdoppelung des Volumens eines vorgegebenen Würfels. Nach Normierung soll also zu einem Würfel des Volumens und der Kantenlänge 1 ein Würfel des Volumens 2 mit Kantenlänge $\sqrt[3]{2}$ konstruiert werden. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist dies nach Satz 1.4 nicht möglich.

Bei der Quadratur des Kreises soll ein Quadrat bestimmt werden, dessen Flächeninhalt mit dem eines Kreises vom Radius 1 übereinstimmt. Gesucht ist also eine Kantenlänge a mit $a^2 = \pi$. Da π transzendent ist, muß a nach Satz 1.15 ebenfalls transzendent sein und ist daher nicht konstruierbar.

Die Winkeldreiteilung ist ebenfalls nicht möglich. Das Problem kann mittels Rechenregeln für sin und cos darauf zurückgeführt werden, eine Nullstelle eines irreduziblen Polynoms vom Grad drei über $\mathbb{Q}$ zu konstruieren.

1.2 Zerfällungskörper und algebraischer Abschluß

In diesem Abschnitt zeigen wir, daß es erstens zu jedem Körper K und jedem nicht konstanten Polynom $f \in K[t]$ einen Erweiterungskörper gibt, über dem f in Linearfaktoren zerfällt, und daß es zweitens einen Erweiterungskörper von K gibt, über dem jedes nicht konstante $f \in K[t]$ in Linearfaktoren zerfällt.

1.26 Satz (Kronecker)**.** *Sei K ein Körper und $f \in K[t]$ irreduzibel. Dann gibt es einen Erweiterungskörper E von K und $a \in E$, so daß $f(a) = 0$, $E = K(a)$ und $[E : K] = \deg(f)$.*

Beweis. Wir definieren $E = K[t]/fK[t]$. Nach Korollar **??** kann E als Erweiterungskörper von K aufgefaßt werden. Bezeichnet $a = t + fK[t]$ die Klasse von t in $K[t]/fK[t]$, so gilt $E = K[a]$ und $f(a) = 0$. Ist nämlich $x \in a$, so gilt $x \equiv t \bmod f$ und $f(x) \equiv f(t) \equiv 0 \bmod f$. Die Gradaussage folgt nach Satz 1.12. □

In anderen Worten erzwingt man also durch die Quotientenbildung in $K[t]$ die algebraische Relation $f(t) = 0$. Man kann Satz 1.26 auf auch reduzible Polynome $f \in K[t]$ anwenden, indem man einen irreduziblen Faktor von f betrachtet. So erhält man also stets eine Körpererweiterung von K, indem ein nicht konstantes $f \in K[t]$ eine Nullstelle besitzt.

1.27 Definition. Sei K ein Körper, $M \subseteq K[t]$ eine Menge von nicht konstanten Polynomen und E ein Erweiterungskörper von K. Dann heißt E Zerfällungskörper von M über K, wenn jedes Polynom $f \in M$ über E in Linearfaktoren zerfällt und E durch Adjunktion der Nullstellen der f aus E an K entsteht.

Der Zerfällungskörper ist also der kleinste Erweiterungskörper von K, in dem die $f \in M$ alle ihre Nullstellen haben. Bei einer endlichen Menge $M = \{f_1, \dots, f_n\}$ sprechen wir auch vom Zerfällungskörper der $f_1, \dots, f_n$ über K.

1.28 Satz. *Zu jedem Körper K und nicht konstantem Polynom $f \in K[t]$ gibt es einen Zerfällungskörper E von f über K mit $[E : K] \leq \deg(f)!$.*

Beweis. Sei $E_0 = K$ und $f_0 = f$. Wir gehen nun induktiv vor. Sei $i \geq 0$ und $g_i \in K[t]$ ein irreduzibler Faktor von f_i. Nach Satz 1.26 gibt es einen Erweiterungskörper E_{i+1} von E_i und $a_{i+1} \in E_{i+1}$ mit $E_{i+1} = E_i(a_{i+1})$, $g_i(a_{i+1}) = f_i(a_{i+1}) = f(a_{i+1}) = 0$ und $[E_i(a_{i+1}) : E_i] = \deg(g_i) \leq \deg(f_i)$. Wir setzen $f_{i+1} = f_i/(t - a_{i+1}) \in E_{i+1}[t]$. Nach $n = \deg(f)$ Schritten erhalten wir $E_n = K(a_1, \dots, a_n)$ und mit $c = f_n \in K$ gilt $f = c\prod_i(t - a_i)$ in $E_n[t]$. Die Gradaussage folgt aus $\deg(f_{i+1}) = \deg(f_i) - 1$. □

Die im Beweis durchgeführte Konstruktion eines Zerfällungskörpers von f hängt von der Wahl der irreduziblen Polynome g_i ab. Im nächsten Abschnitt zeigen wir jedoch, daß alle Zerfällungskörper von f über K isomorph sind. Man spricht daher auch manchmal von dem Zerfällungskörper von f über K.

Als Beispiel betrachten wir $f = t^2 - 2 \in \mathbb{Q}[t]$ und $g = t^3 - 2 \in \mathbb{Q}[t]$. In $E = \mathbb{Q}[t]/f\mathbb{Q}[t]$ gibt es eine Nullstelle von f, die wir mit $\sqrt{2}$ bezeichnen. Dann gilt $f = (t - \sqrt{2})(t + \sqrt{2})$ über E, und E ist bereits ein Zerfällungskörper von f über $\mathbb{Q}$, vom Grad 2 über $\mathbb{Q}$.

In $\mathbb{C}$ gilt $g = (t - \sqrt[3]{2})(t - \exp(2\pi i/3)\sqrt[3]{2})(t - \exp(4\pi i/3)\sqrt[3]{2})$. Dann ist $\mathbb{Q}(\sqrt[3]{2}, \exp(2\pi i/3))$ ein in $\mathbb{C}$ gelegener Zerfällungskörper von f über $\mathbb{Q}$, und zwar vom Grad 6 über $\mathbb{Q}$. Alternativ erhalten wir einen Zerfällungskörper von f über $\mathbb{Q}$ mit $\mathbb{Q}[t,s]/(t^3 - 2, s^2 + ts + t^2)$. In $\mathbb{Q}[t]/(t^3 - 2)[s]$ gilt hierbei $s^3 - 2 = (s - t)(s^2 + ts + t^2)$. Dieser Zerfällungskörper hat den Vorteil, daß man in ihm mittels eines Computers exakt rechnen kann, wohingegen dies bei dem anderen Zerfällungskörper nicht möglich ist, wenn die komplexen Zahlen als Fließkommazahlen mit endlicher Präzision dargestellt werden.

1.29 Definition. Ein Körper K heißt algebraisch abgeschlossen, wenn aus E/K algebraisch $E = K$ folgt. Ist E/K algebraisch und E algebraisch abgeschlossen, so heißt E algebraischer Abschluß von K. Wir bezeichnen ein solches E mit $\bar{K}$ oder K^a.

Im Hinblick auf Satz 1.28 faktorisiert jedes nicht konstante Polynom über einem algebraisch abgeschlossenen Körper K in Linearfaktoren, hat also alle seine Nullstellen in K. Iterativ sieht man, daß umgekehrt ein Körper K algebraisch abgeschlossen ist, wenn jedes nicht konstante Polynom $f \in K[t]$ eine Nullstelle in K besitzt. Ist E ein algebraisch abgeschlossener Erweiterungskörper von K, so ist der algebraische Abschluß von K in E nach Satz 1.16 selbst algebraisch abgeschlossen und daher ein algebraischer Abschluß von K.

1.30 Satz. *Jeder Körper besitzt einen algebraischen Abschluß.*

Beweis. Wir gehen im Prinzip wie in Satz 1.28 vor, nur daß wir alle nicht konstanten Polynome aus $K[t]$ simultan betrachten. Wie in Satz 1.28 müssen wir geeignete irreduzible Faktoren wählen. Da wir es nun mit unendlich vielen Polynomen zu tun haben, benötigen wir dazu das Auswahlaxiom. Für die Konstruktion ist es zweckmäßig, Polynomringe in unendlich vielen Variablen zu betrachten und das Auswahlaxiom in der Form der Existenz von maximalen Idealen zu verwenden.

Sei M die Menge aller nicht konstanten Polynome in $K[t]$. Wir konstruieren zuerst einen Erweiterungskörper von K, in dem jedes $f \in M$ eine Nullstelle besitzt. Für jedes $f \in M$ bezeichne X_f eine eigene Variable und sei $X = \{X_f \mid f \in M\}$. Wir betrachten den Polynomring $K[X]$ und darin das von den $f(X_f)$ erzeugte Ideal $\mathfrak{a}$. Wir nehmen nun an, daß $\mathfrak{a} \neq K[X]$ ist (Beweis folgt gleich). Dann gibt es ein maximales Ideal $\mathfrak{b}$ von $K[X]$ mit $\mathfrak{a} \subseteq \mathfrak{b}$, und $K[X]/\mathfrak{b}$ ist ein Körper. Wegen $K \cap \mathfrak{b} = \{0\}$ kann $K[X]/\mathfrak{b}$ als Erweiterungskörper von K aufgefaßt werden. Die von X_f in $K[X]/\mathfrak{b}$ erzeugte Klasse ist dann eine Nullstelle von f, weil $f(X_f) \in \mathfrak{b}$ gilt. Also ist $K[X]/\mathfrak{b}$ der gesuchte Körper. Der Beweis von $\mathfrak{a} \neq K[X]$ erfolgt durch Widerspruch. Ist nämlich $\mathfrak{a} = K[t]$, dann gibt es endlich viele $g_i \in K[X]$ und $f_i \in M$ mit $1 = \sum_i g_i f_i(X_{f_i})$. Satz 1.28 angewendet auf $\prod_i f_i$ zeigt, daß es einen Erweiterungskörper E von K gibt, in dem jedes f_i eine Nullstelle a_i besitzt. Sei $\phi : K[X] \to E$ der durch $X_{f_i} \mapsto a_i$ und $X_f \mapsto 0$ für $f \neq f_i$ für alle i definierte Einsetzhomomorphismus. Dann gilt in E, daß $\phi(f_i(X_{f_i})) = 0$ und folglich $1 = \sum_i \phi(g_i)\phi(f_i(X_{f_i})) = 0$ ist. Dies ist ein Widerspruch zur Körpereigenschaft von E, und daher kann $\mathfrak{a} = K[X]$ nicht gelten.

Durch Iteration dieses Verfahrens erhalten wir eine aufsteigende Kette $K = E_0 \subseteq E_1 \subseteq \dots$ von Körpern, so daß jedes nicht konstante Polynom in $E_i[t]$ eine Nullstelle in E_{i+1} besitzt. Wir setzen $E = \cup_{i=0}^{\infty} E_i$. Je zwei Elemente $a, b \in E$ liegen bereits in einem E_i. Wir machen E zu einem Körper, indem wir die Summe, Produkt usw. von a, b durch E_i definieren. Wegen der Teilkörpereigenschaft von $E_i \subseteq E_j$ für $j \geq i$ ist dies unabhängig von der Wahl von i.

Ist $f \in E[t]$ ein nicht konstantes Polynom, so gilt bereits $f \in E_i[t]$, da f nur endlich viele Koeffizienten ungleich Null hat. Dann hat f eine Nullstelle in E_i und somit auch in E. Nach den Bemerkungen vor dem Satz ist E algebraisch abgeschlossen und der algebraische Abschluß K^a von K in E ist daher ein algebraischer Abschluß von K. □

Im nächsten Abschnitt zeigen wir, daß je zwei algebraische Abschlüsse von K isomorph sind. Man spricht daher auch manchmal von dem algebraischen Abschluß von K.

Aufgrund des nächsten Satzes befindet sich ein algebraischer Abschluß von $\mathbb{Q}$ in $\mathbb{C}$.

1.31 Satz (Fundamentalsatz der Algebra)**.** *Der Körper der komplexen Zahlen ist algebraisch abgeschlossen.*

Beweis. Erfolgt üblicherweise in der Funktionentheorie I. □

Vom Standpunkt der Computeralgebra aus läßt sich ein algebraischer Abschluß eines Körpers K trotz der impliziten Verwendung des Auswahlaxioms zumindest zum Teil simulieren, wenn man nur Polynome über endlichen Erweiterungen von K faktorisieren kann. Man stellt K^a als abstrakten Datentyp dar, der zu jedem Zeitpunkt durch eine endliche Erweiterung F von K repräsentiert wird. Anfänglich gilt $F = K$. Sollen nun die Nullstellen eines nicht konstanten Polynoms $f \in K^a[t]$ berechnet werden, so gilt zunächst $f \in F[t]$ und man bestimmt einen Zerfällungskörper E von f über F mittels der Vorgehensweise im Beweis von Satz 1.28. Man ersetzt dann F in der Darstellung von K^a durch E und liefert die Nullstellen als Elemente von E zurück. Im Endeffekt wird die unendliche Operation, die mittels des Auswahlaxioms ausgeführt wird, durch einen unbegrenzten dynamischen Prozeß modelliert.

1.32 Korollar. *Sei K ein Körper und $M \subseteq K[t]$ eine Menge nicht konstanter Polynome. Dann gibt es einen Zerfällungskörper von M über K.*

Beweis. Sei K^a ein algebraischer Abschluß von K und $A = \{a \in K^a \mid f(a) = 0 \text{ und } f \in M\}$. Dann leistet $E = K(A)$ das Gewünschte. $\square$

1.3 Homomorphismen und ihre Fortsetzungen

Bei der Untersuchung mathematischer Objekte ist es wesentlich, auch die strukturerhaltenden Abbildungen zwischen ihnen zu betrachten. Für (endliche) Körpererweiterungen ist dies zentraler Bestandteil der Galoistheorie und soll in diesem Abschnitt begonnen werden. Als Anwendung beweisen wir, daß Zerfällungskörper und algebraische Abschlüsse bis auf Isomorphie eindeutig bestimmt sind.

1.33 Definition. Ein Homomorphismus $\sigma : E_1 \to E_2$ der Körper E_1 und E_2 ist ein Ringhomomorphismus der Ringe E_1 und E_2. Die Menge dieser Homomorphismen wird mit $\mathrm{Hom}(E_1, E_2)$ bezeichnet.

Sind E_1/K_1 und E_2/K_2 Körpererweiterungen und $\sigma \in \mathrm{Hom}(K_1, K_2)$, so bezeichnen wir die Menge aller Fortsetzungen $\tau \in \mathrm{Hom}(E_1, E_2)$ von σ mit $\mathrm{Hom}_\sigma(E_1, E_2)$. Gilt $K_1 = K_2$ und $\sigma = \mathrm{id}$, so schreiben wir dafür auch $\mathrm{Hom}_K(E_1, E_2)$, wobei $K = K_1$, und sprechen von K-Homomorphismen der Körper E_1 und E_2 oder von Homomorphismen der Körpererweiterungen E_1/K und E_2/K.

Weiter verwenden wir die Begriffe Isomorphismus, Endomorphismus und Automorphismus wie erwartet und schreiben $\mathrm{End}(E)$, $\mathrm{Aut}(E)$ usw. Zwei Erweiterungskörper E_1 und E_2 von K können dann beispielsweise nur isomorph oder auch isomorph über K sein.

Ist $\sigma \in \mathrm{Hom}_K(E_1, E_2)$, so gilt also $\sigma(x) = x$ für alle $x \in K$ und σ ist K-linear. Ist allgemeiner $\sigma \in \mathrm{Hom}(E_1, E_2)$, so gilt definitionsgemäß $\sigma(1) = 1$. Wegen $1 \neq 0$ in Körpern ist σ nicht die Nullabbildung. Daher muß $\ker(\sigma) = \{0\}$ gelten, da dies das einzige Ideal von E_1 ungleich E_1 ist, und σ ist ein Isomorphismus auf den Teilkörper $\sigma(E_1)$ von E_2. Außerdem ergibt sich, daß E_1 und E_2 isomorphen Primkörper haben. Sind E_1 und E_2 Teilkörper eines gemeinsamen Oberkörpers, so sind die Primkörper gleich und jedes $\sigma \in \mathrm{Hom}(E_1, E_2)$ ist linear bezüglich des Primkörpers.

Für $\sigma \in \mathrm{Hom}(K_1, K_2)$ erhalten wir durch koeffizientenweises Anwenden einen ebenfalls mit σ bezeichneten Ringhomomorphismus $K_1[t] \to K_2[t]$. Es ist praktisch, $f^\sigma = \sigma(f)$ zu schreiben.

1.34 Lemma. *Seien E_1/K_1 und E_2/K_2 Körpererweiterungen, $\sigma \in \mathrm{Hom}(K_1, K_2)$, $f \in K_1[t]$ und a eine Nullstelle von f in E_1.*

(*i*) *Für* $\tau \in \mathrm{Hom}_\sigma(E_1, E_2)$ *ist* $\tau(a)$ *eine Nullstelle von* $f^\sigma \in K_2[t]$ *in* E_2.

(*ii*) *Sei* σ *ein Isomorphismus und* f *irreduzibel in* $K_1[t]$. *Ist dann* $b \in E_2$ *eine beliebige Nullstelle von* f^σ, *so gibt es ein* $\tau \in \mathrm{Hom}_\sigma(K_1(a), K_2(b))$ *mit* $\tau(a) = b$, *und* τ *ist ein Isomorphismus.*

Beweis. (*i*): Es gilt $f^\sigma(\tau(a)) = \tau(f(a)) = 0$. (*ii*): Ohne Einschränkung können wir f und damit f^σ als normiert annehmen. Da σ ein Isomorphismus ist, muß f^σ irreduzibel in $K_2[t]$ sein. Nach Satz 1.12 folgt $m_{a,K_1} = f$, $m_{b,K_2} = f^\sigma$ und $K_1(a) \cong K_1[t]/fK_1[t]$, $K_2(b) \cong K_2[t]/f^\sigma K_2[t]$. Die Faktorringe $K_1[t]/fK_1[t]$ und $K_2[t]/f^\sigma K_2[t]$ sind aber offenbar unter Verwendung von σ isomorph. Die Kombination der Isomorphismen ergibt τ mit $\tau(a) = b$. □

Auf die Voraussetzung der Irreduzibilität von f kann nicht verzichtet werden (Gegenbeispiel: $f = (t-1)(t-2) \in \mathbb{Q}[t]$, $\sigma = \mathrm{id}_\mathbb{Q}$, $a = 1$, $b = 2$ und $1 = \tau(a) = b = 2$).

1.35 Satz. *Sei* $\sigma \in \mathrm{Hom}(K_1, K_2)$ *ein Isomorphismus,* $f \in K_1[t]$ *ein nicht konstantes Polynom,* E_1 *der Zerfällungskörper von* f *über* K_1 *und* E_2 *der Zerfällungskörper von* f^σ *über* K_2. *Dann gibt es einen Isomorphismus* $\tau \in \mathrm{Hom}_\sigma(E_1, E_2)$.

Beweis. Der Satz folgt im Prinzip auch aus den untenstehenden, allgemeineren Überlegungen. Der folgende Beweis dient nur der Konkretheit.

Ausgehend von E_1 und E_2 führen wir die Konstruktion von E_1 und E_2 im Beweis von Satz 1.28 noch einmal simultan für f und f^σ durch, wobei die auftretenden, irreduziblen Faktoren von f^σ die g_i^σ sein sollen. Hierbei wurde E_2 möglicherweise zwar anders konstruiert, aber jedes g_i^σ zerfällt dennoch über E_2 in Linearfaktoren. Wir definieren also induktiv $E_{1,i+1} = E_{1,i}(a_{i+1})$ mit $g_i(a_{i+1}) = 0$ wie gehabt und $E_{2,i+1} = E_{2,i}(b_{i+1})$ mit $g_i^\sigma(b_{i+1}) = 0$ für ein $b_{i+1} \in E_2$. Unter Verwendung von Lemma 1.34 können wir $\sigma_i \in \mathrm{Hom}(E_{1,i}, E_{2,i})$ zu $\sigma_{i+1} \in \mathrm{Hom}_{\sigma_i}(E_{1,i+1}, E_{2,i+1})$ durch $\sigma_{i+1}(a_{i+1}) = b_{i+1}$ fortsetzen. Schließlich erhalten wir $\tau = \sigma_n \in \mathrm{Hom}_\sigma(E_1, E_2)$. □

1.36 Korollar. *Seien* E_1 *und* E_2 *Zerfällungskörper des nicht konstanten Polynoms* $f \in K[t]$ *über* K. *Dann sind* E_1/K *und* E_2/K *isomorph.*

Jeder K-Isomorphismus von E_1 und E_2 bildet die Nullstellen von f in E_1 auf die Nullstellen von f in E_2 ab. Die Untersuchung aller solcher K-Isomorphismen für $E_1 = E_2$ ist Inhalt der Galoistheorie.

Als Beispiel betrachten wir die Zerfällungskörper $\mathbb{Q}(\sqrt{2})$ von $f = t^2 - 2$ und $E = \mathbb{Q}(\sqrt[3]{2}, \exp(2\pi i/3))$ von $g = t^3 - 2$ über $\mathbb{Q}$. Durch $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ bekommen wir einen $\mathbb{Q}$-Automorphismus von $\mathbb{Q}(\sqrt{2})$, der einzig weiter mögliche außer der

Identität. Weil g irreduzibel über $\mathbb{Q}$ ist und drei verschiedene Nullstellen in E hat, gibt es nach Lemma 1.34 genau drei Elemente σ in $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), E)$. Das Minimalpolynom von $\exp(2\pi i/3)$ über $\mathbb{Q}(\sqrt[3]{2})$ ist t^2+t+1. Dies ist also irreduzibel über $\mathbb{Q}(\sqrt[3]{2})$ und hat zwei Nullstellen in E. Folglich gibt es zu jedem σ zwei Elemente τ in $\mathrm{Aut}_\sigma(E)$. Damit besteht $\mathrm{Aut}_{\mathbb{Q}}(E)$ aus genau 6 Elementen.

1.37 Satz. *Sei $\sigma \in \mathrm{Hom}(K_1, K_2)$ ein Isomorphismus, E/K_1 eine algebraische Erweiterung und C ein algebraischer Abschluß von K_2. Dann gibt es ein $\tau \in \mathrm{Hom}_\sigma(E, C)$.*

Beweis. Sei A die Menge der Paare (F, τ), wobei F ein Zwischenkörper von E/K_1 und $\tau \in \mathrm{Hom}_\sigma(F, C)$ ist. Wegen $(K_1, \sigma) \in A$ ist A nicht leer. Wir schreiben $(F_1, \tau_1) \leq (F_2, \tau_2)$, wenn $F_1 \subseteq F_2$ und τ_2 eine Fortsetzung von τ_1 ist. Dies definiert eine Halbordnung auf A. Wir zeigen, daß A durch $\leq$ induktiv geordnet wird. Sei dazu L eine Kette in A. Wir definieren den Körper F' als die Vereinigung der in L vorkommenden Körper. Ist $x \in F'$, so gibt es ein $(F_1, \tau_1) \in A$ mit $x \in F_1$. Wir können durch $\tau'(x) = \tau_1(x)$ ein Element $\tau' \in \mathrm{Hom}_\sigma(F', C)$ definieren. Das Paar $(F', \tau') \in A$ wird damit zur oberen Schranke von L. Nach dem Zornschen Lemma gibt es ein maximales Element $(F, \tau) \in A$ und es bleibt $F = E$ zu zeigen. Ist $F \neq E$, so gibt es ein $a \in E \backslash F$ und nach Voraussetzung eine Nullstelle $b \in C$ von $\tau(m_{a,F})$. Nach Satz 1.34 gibt es ein Element in $\mathrm{Hom}_\tau(F(a), \tau(F)(b))$ bzw. $\mathrm{Hom}_\tau(F(a), C)$. Wegen $F(a) \neq F$ steht dies im Widerspruch zur Maximalität von (F, τ) und es folgt $F = E$. □

1.38 Satz. *Seien C_1 und C_2 algebraische Abschlüsse des Körpers K. Dann sind C_1/K und C_2/K isomorph.*

Beweis. Nach Satz 1.37 angewendet mit $\sigma = \mathrm{id}$ gibt es ein $\tau \in \mathrm{Hom}_K(C_1, C_2)$ und $\tau(C_1)$ ist ein algebraischer Abschluß von K in C_2. Da jedes Element von C_2 auch algebraisch über $\tau(C_1)$ ist, folgt $\tau(C_1) = C_2$. □

1.39 Satz. *Seien $M \subseteq K[t]$ eine Menge nicht konstanter Polynome und E_1, E_2 Zerfällungskörper von M über K. Dann sind E_1/K und E_2/K isomorph.*

Beweis. Sei C ein algebraischer Abschluß von E_2. Dann ist C wegen Satz 1.16 auch ein algebraischer Abschluß von K. Ist E_3 neben E_2 ein weiterer Zerfällungskörper von M über K in C, so gilt $E_3 = E_2$, weil E_2 und E_3 durch Adjunktion derselben Nullstellen an K in C entstehen. Nach Satz 1.37 gibt es ein $\sigma \in \mathrm{Hom}_K(E_1, C)$, und $\sigma(E_1)$ ist ein Zerfällungskörper von M über K in C. Es folgt $\sigma(E_1) = E_2$. □

1.40 Satz. *Sei E/K algebraisch. Dann ist $\mathrm{End}_K(E) = \mathrm{Aut}_K(E)$.*

Beweis. Zu zeigen ist, daß jedes $\sigma \in \mathrm{End}_K(E)$ surjektiv ist. Sei $b \in E$ und N die Menge der Nullstellen von $m_{b,K}$ in E. Dann bewirkt σ eine Permutation von N, da Nullstellen nach Lemma 1.34 durch σ wieder in Nullstellen überführt werden und N endlich und σ injektiv ist. Also gibt es $a \in N$ mit $\sigma(a) = b$. □

1.4 Normale Erweiterungen

Zerfällungskörper sind bezüglich Nullstellen von nicht notwendigerweise in M gelegenen Polynomen und bezüglich von Homomorphismen im folgenden Sinn abgeschlossen.

1.41 Definition. Eine algebraische Erweiterung E/K heißt normal und E normal über K, wenn jedes irreduzible $f \in K[t]$, welches eine Nullstelle in E hat, über E bereits vollständig in Linearfaktoren zerfällt.

Als Beispiel bemerken wir, daß K/K und C/K normal sind, wo C einen algebraischen Abschluß von K bezeichnet. Auch sind quadratische Erweiterungen immer normal. Auf der anderen Seite ist $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ zum Beispiel nicht normal.

1.42 Satz. *Sei E/K eine algebraische Körpererweiterung. Dann sind die folgenden Bedingungen äquivalent.*

(*i*) *E/K ist normal.*

(*ii*) *E ist ein Zerfällungskörper über K.*

(*iii*) *Für jede Körpererweiterung L/K und für jedes $\sigma, \tau \in \mathrm{Hom}_K(E, L)$ gibt es ein eindeutig bestimmtes $\rho \in \mathrm{Aut}_K(E)$ mit $\tau = \sigma \circ \rho$.*

Beweis. Der Homomorphismus ρ in (*iii*) ist zunächst immer eindeutig bestimmt, da σ injektiv ist.

(*i*) $\Rightarrow$ (*ii*): E ist offenbar der Zerfällungskörper der Menge $M = \{m_{a,K} \in K[t] \mid a \in E\}$ über K.

(*ii*) $\Rightarrow$ (*iii*): Seien E Zerfällungskörper der Menge $M \subseteq K[t]$ über K, und L, σ, τ wie in (*iii*). Die Körper $\sigma(E)$ und $\tau(E)$ sind dann ebenfalls Zerfällungskörper von M über K und entstehen durch Adjunktion der gleichen Nullstellen aus L an K, woraus $\sigma(E) = \tau(E)$ folgt. Also ist $\rho = \sigma^{-1} \circ \tau \in \mathrm{End}_K(E) = \mathrm{Aut}_K(E)$ nach Satz 1.40 der gesuchte Homomorphismus.

(*iii*) $\Rightarrow$ (*i*): Es existiert ein algebraischer Abschluß L von K und ein $\sigma \in \mathrm{Hom}_K(E, L)$. Sei $f \in K[t]$ irreduzibel und $a \in E$ mit $f(a) = 0$. In L gilt $f = c\prod_i(t - b_i)$ mit $c \in K$ und $b_i \in L$. Nach Lemma 1.34 und Satz 1.37 gibt es $\tau_i \in \mathrm{Hom}_K(E, L)$ mit $\tau_i(a) = b_i$ für alle i. Nach (*iii*) gibt es dazu $\rho_i \in \mathrm{Aut}_K(E)$

mit $\tau_i = \sigma \circ \rho_i$. Dann ist $\sigma(\rho_i(a)) = \tau_i(a) = b_i$, so daß $f = f^{\sigma^{-1}} = c\prod_i(t - \rho_i(a))$ in E durch Anwendung von σ^{-1} auf $f = c\prod_i(t - b_i)$ folgt. □

In Satz 1.42, (*iii*) ergibt sich ein wichtiger Spezialfall, wenn $\sigma = \mathrm{id}$ und die betrachteten Körper alle in L liegen:

1.43 Korollar. *Sei L/K eine Körpererweiterung und E ein über K normaler Zwischenkörper von L/K. Für $\tau \in \mathrm{Hom}_K(E, L)$ gilt dann bereits $\tau \in \mathrm{Aut}_K(E)$.*

Sei L/K eine Körpererweiterung und seien E_1, E_2 über K normale Zwischenkörper von L/K. Ist $\phi \in \mathrm{Hom}_K(E_1, E_2)$ ein Isomorphismus, so gilt $E_1 = E_2$.

Beweis. Folgt aus Satz 1.42, (*iii*). □

Sei E/K algebraisch und C ein algebraischer Abschluß von E. Jedes Element von $\mathrm{Hom}_K(E, C)$ läßt sich nach Satz 1.37 und Satz 1.40 zu einem Element von $\mathrm{Aut}_K(C)$ fortsetzen. Eine zu Satz 1.42, (*iii*) ähnliche und äquivalente Bedingung ist dann, daß jedes Element von $\mathrm{Aut}_K(C)$ durch Einschränkung ein Element von $\mathrm{Aut}_K(E)$ vermittelt.

Wir wenden uns jetzt wieder der Abbildung 1.1 zu und untersuchen, wie sich die Eigenschaft „normal“ vererbt.

1.44 Satz. *Sei E/K eine Körpererweiterung.*

(*i*) *Für einen Zwischenkörper F von E/K ist E/F normal, wenn E/K normal ist.*

(*ii*) *Sind F_1, F_2 Zwischenkörper von E/K und ist F_1/K normal, so ist F_1F_2/F_2 normal.*

(*iii*) *Ist zusätzlich F_2/K normal, so sind auch F_1F_2/K und $F_1 \cap F_2/K$ normal.*

Beweis. (*i*): Nach Voraussetzung ist E Zerfällungskörper einer Menge $M \subseteq K[t]$ über K. Wegen $M \subseteq F[t]$ ist E auch Zerfällungskörper von M über F.

(*ii*): Dasselbe Argument gilt für F_1F_2/F_2.

(*iii*): Ist F_1 Zerfällungskörper von M_1 über K und F_2 Zerfällungskörper von M_2 über K, so ist F_1F_2 Zerfällungskörper von $M_1 \cup M_2$ über K. Dies gilt, da jedes Polynom in $M_1 \cup M_2$ über F_1F_2 zerfällt und ein Zerfällungskörper von $M_1 \cup M_2$ somit in F_1F_2 enthalten ist. Auf der anderen Seite muß dieser Zerfällungskörper nach Voraussetzung auch F_1 und F_2 enthalten, woraus die Gleichheit folgt. Die Normalität von $F_1 \cap F_2/K$ ergibt sich aus der Definition. □

Wir bemerken, daß Komposita und Schnitte über beliebige Mengen von über K normalen Zwischenkörpern von E/K wieder normal über K sind.

1.45 Definition. Sei E/K normal und F ein Zwischenkörper von E/K. Dann heißt E normale Hülle von F/K, wenn es keinen Zwischenkörper von E/F außer E gibt, der über K normal ist.

In anderen Worten ist E also ein bezüglich Inklusion minimaler Erweiterungskörper von F, der über K normal ist. Bis auf F-Isomorphie ist er aber auch der kleinste, wie der folgende Satz zeigt.

1.46 Satz. *Sei F/K eine algebraische Körpererweiterung, E eine normale Hülle von F/K und L ein über K normaler Erweiterungskörper von F. Dann existiert ein $\sigma \in \mathrm{Hom}_F(E, L)$. Insbesondere ist E/K bis auf F-Isomorphie eindeutig bestimmt.*

Beweis. Sei C ein algebraischer Abschluß von L. Nach Satz 1.37 gibt es dann ein $\sigma \in \mathrm{Hom}_F(E, C)$ und $\sigma(E)$ ist ebenfalls eine normale Hülle von F/K. Weiter ist $\sigma(E) \cap L$ ein Zwischenkörper von $\sigma(E)/F$, der nach Satz 1.44 normal über K ist. Es folgt $\sigma(E) \cap L = \sigma(E)$ und damit $\sigma(E) \subseteq L$.

Sei L eine weitere normale Hülle von F/K. Dann gibt es auch ein $\tau \in \mathrm{Hom}_F(L, E)$ und es gilt $\tau \circ \sigma \in \mathrm{End}_F(E) = \mathrm{Aut}_F(E)$, $\sigma \circ \tau \in \mathrm{End}_F(L) = \mathrm{Aut}_F(L)$ nach Satz 1.40. Folglich sind E und L isomorph über K. □

1.47 Satz. *Sei F/K eine algebraische Körpererweiterung, L ein über K normaler Erweiterungskörper von F und $A \subseteq F$ mit $F = K(A)$. Dann enthält L genau eine normale Hülle E von F/K, und es gilt*

(*i*) *$E = \cap\{\, T \mid T$ Zwischenkörper von L/F und T/K normal$\}$.*

(*ii*) *E ist der Zerfällungskörper von $M = \{m_{a,K} \mid a \in A\}$ über F.*

(*iii*) *$E = K(\cup\{\tau(F) \mid \tau \in \mathrm{Hom}_K(F, L)\})$.*

Ist F/K endlich, so ist auch E/K endlich.

Beweis. Ist E eine normale Hülle von F/K in L, so ist E nach Korollar 1.43 und Satz 1.46 eindeutig bestimmt.

Der Schnitt in (i) ist nicht leer, da mindestens $T = L$ darin vorkommt. Daher wird durch den Schnitt ein Zwischenkörper E von L/F definiert. Es ist klar, daß E dann eine normale Hülle von F/K ist.

Jeder über K normale Erweiterungskörper T von F enthält einen Zerfällungskörper Z von M über K, da jedes $f \in M$ eine Nullstelle in F und damit alle Nullstellen in T hat. Außerdem gilt $Z \supseteq F$ wegen $F = K(A)$ und Z ist nach Satz 1.42 normal über K. Mit (i) folgt $E = Z$ und damit (ii).

Sei $a \in F$. Dann ist a eine Nullstelle von $m_{a,K}$ in L und $m_{a,K}$ zerfällt über L in Linearfaktoren. Sei $b \in L$ eine beliebige Nullstelle von $m_{a,K}$. Es gibt dann ein $\tau \in \mathrm{Hom}_K(F, L)$ mit $\tau(a) = b$. Die Menge $B = \cup\{\tau(F) \,|\, \tau \in \mathrm{Hom}_K(F, L)\}$ enthält also alle Nullstellen von $m_{a,K}$. Da a beliebig war und B nicht von a abhängt, ist $K(B)$ der Zerfällungskörper von M über K in L und es gilt $E = K(B)$ nach (ii). Damit ist (iii) bewiesen.

Ist F/K endlich, so kann auch A endlich gewählt werden. Nach (ii) entsteht E dann durch Adjunktion endlich vieler Nullstellen an K und ist daher endlich über K. $\square$

1.48 Definition. Seien F/K und L/K algebraisch. Die Elemente $\tau(a)$ mit $\tau \in \mathrm{Hom}_K(F, L)$ und $a \in F$ heißen die Konjugierten von a über K in L. Die Körper $\tau(F)$ mit $\tau \in \mathrm{Hom}_K(F, L)$ heißen die zu F über K konjugierten Körper in L.

Die Konjugierten von a über K in L sind also genau die Nullstellen von $m_{a,K}$ in L.

1.5 Separable Erweiterungen

1.49 Definition. Ein Polynom $f \in K[t]$ heißt separabel, wenn es nur einfache, also $\deg(f)$ verschiedene Nullstellen in einem algebraischen Abschluß C von K besitzt.

Die Definition hängt nicht vom gewählten algebraischen Abschluß C ab, da C bis auf K-Isomorphie eindeutig bestimmt ist. Nach Satz **??** sind die mehrfachen Nullstellen von f in C gleich den Nullstellen von $\gcd\{f, f'\}$ in C und f ist genau dann separabel, wenn $\gcd\{f, f'\} = 1$ gilt. Insofern sieht man auch, daß die Separabilitätseigenschaft eines Polynoms nicht vom betrachteten Grundkörper abhängt.

Nach Korollar **??** sind irreduzible Polynome in Charakteristik Null immer separabel, wohingegen dies in positiver Charakteristik p nicht unbedingt der Fall sein muß. Zum Beispiel ist das Polynom $t^p - x$ über $\mathbb{F}_p(x)$ irreduzibel aber nicht separabel.

1.50 Definition. Sei E/K eine algebraische Körpererweiterung. Das Element $a \in E$ heißt separabel über K, wenn $m_{a,K}$ separabel ist. Die Erweiterung E/K heißt separabel und E separabel über K, wenn jedes Element aus E separabel über K ist. Sei C ein algebraischer Abschluß von K. Der Separabilitätsgrad von E/K wird definiert als $[E : K]_s = \#\mathrm{Hom}_K(E, C)$.

Anstelle von „nicht separabel“ benutzen wir „inseparabel“. In Charakteristik Null treten nur separable irreduzible Polynome, Elemente und Körpererweiterungen auf. Ist C algebraisch abgeschlossen und $\sigma \in \mathrm{Hom}(K, C)$, so gilt $\#\mathrm{Hom}_\sigma(E, C) = [E : K]_s$, indem wir K mit $\sigma(K)$ identifizieren. Ein Homomorphismus $\sigma \in \mathrm{Hom}(K, C)$ besitzt also genau $[E : K]_s$ Fortsetzungen auf E.

Bei den Überlegungen dieses Abschnitts könnten wir C auch durch einen Körper ersetzen, welcher E enthält und über K normal ist.

1.51 Lemma. *Sei F ein Zwischenkörper der algebraischen Erweiterung E/K und sei C ein algebraischer Abschluß von E. Dann gibt es eine Bijektion*

$$\mathrm{Hom}_K(F, C) \times \mathrm{Hom}_F(E, C) \to \mathrm{Hom}_K(E, C).$$

Beweis. Durch die Wahl beliebiger, aber fest gewählter Fortsetzungen definieren wir eine injektive Abbildung $\mathrm{Hom}_K(F, C) \to \mathrm{Aut}_K(C)$, $\sigma \mapsto \hat{\sigma}$. Wir erhalten dann die Abbildung $\phi : \mathrm{Hom}_K(F, C) \times \mathrm{Hom}_F(E, C) \to \mathrm{Hom}_K(E, C)$ mit $(\sigma, \tau) \mapsto \hat{\sigma} \circ \tau$.

Zum Beweis der Injektivität von ϕ gelte $\hat{\sigma}_1 \circ \tau_1 = \hat{\sigma}_2 \circ \tau_2$. Durch Einschränkung auf F ergibt sich $\sigma_1 = (\hat{\sigma}_1)_F = (\hat{\sigma}_1 \circ \tau_1)_F = (\hat{\sigma}_2 \circ \tau_2)_F = (\hat{\sigma}_2)_F = \sigma_2$ und somit $\sigma_1 = \sigma_2$. Da $\hat{\sigma}_i$ injektiv ist, folgt schließlich $\tau_1 = \tau_2$.

Zum Beweis der Surjektivität von ϕ sei $\rho \in \mathrm{Hom}_K(E, C)$. Wir definieren $\sigma = (\rho)_F$ und $\tau = \hat{\sigma}^{-1} \circ \rho$. Es gilt $\tau \in \mathrm{Hom}_F(E, C)$, so daß also (σ, τ) das Urbild von ρ unter ϕ ist. □

1.52 Satz. *Sei E/K eine algebraische Körpererweiterung und F ein Zwischenkörper. Dann gilt*

$$[E : K]_s = [E : F]_s [F : K]_s.$$

Beweis. Folgt direkt aus Lemma 1.51. □

1.53 Lemma. *Sei E/K eine einfache algebraische Körpererweiterung mit primitivem Element a und C ein algebraischer Abschluß von K. Dann gilt*

$$[E : K]_s = \#\{b \in C \mid m_{a,K}(b) = 0\} \leq [E : K].$$

Insbesondere ist a genau dann separabel über K, wenn $[E : K]_s = [E : K]$ gilt.

Beweis. Folgt direkt aus Lemma 1.34: Für jede Nullstelle b von $m_{a,K}$ in C gibt es genau ein $\tau \in \mathrm{Hom}_K(E, C)$ mit $\tau(a) = b$. □

1.54 Satz. *Sei E/K eine algebraische Körpererweiterung. Dann gilt $[E : K]_s \leq [E : K]$ und es sind äquivalent:*

(*i*) *E/K ist separabel.*

(*ii*) *Es gibt* $A \subseteq E$ *mit* $E = K(A)$ *und jedes* $a \in A$ *ist separabel über* K.

(*iii*) *Für jeden Zwischenkörper* F *von* E/K *gilt* $[F : K]_s = [F : K]$.

Wird E/K *endlich vorausgesetzt, so kann* (*iii*) *durch folgende Bedingung ersetzt werden:*

$(iii)'$ *Es gilt* $[E : K]_s = [E : K]$.

Beweis. Die Aussage $[E : K]_s \leq [E : K]$ ist für $[E : K] = \infty$ richtig. Für $[E : K] < \infty$ entsteht E als die Vereinigung eines Turms von endlich vielen, einfachen und algebraischen Erweiterungen. Mit anderen Worten gibt es Zwischenkörper E_i von E/K mit $E_0 = K$, $E_n = E$ und $E_i \subseteq E_{i+1}$, so daß E_{i+1}/E_i einfach und algebraisch ist. Nach Lemma 1.53, Satz 1.52 und dem Gradsatz gilt daher $[E : K]_s = \prod_{i=0}^{n-1}[E_{i+1} : E_i]_s \leq \prod_{i=0}^{n-1}[E_{i+1} : E_i] = [E : K]$. Ist jede dieser einfachen Erweiterungen E_{i+1}/E_i separabel, so ergibt sich darüberhinaus die Gleichheit.

Gilt $[E : K]_s = [E : K]$ für eine endliche Erweiterung E/K, so folgt $[F : K]_s = [F : K]$ für alle Zwischenkörper von E/K wegen $[F : K]_s \leq [F : K]$ und der Multiplikativität von $[\,:\,]_s$ und $[\,:\,]$. Dies zeigt $(iii)' \Leftrightarrow (iii)$ für endliche Erweiterungen E/K.

$(i) \Rightarrow (ii)$: Ist klar.

$(iii) \Rightarrow (i)$: Für $a \in E$ gilt $[K(a) : K]_s = [K(a) : K]$, also ist a nach Lemma 1.53 separabel über K.

$(ii) \Rightarrow (iii)$: Wir stellen die Bemerkung voran, daß ein über K separables $a \in E$ auch separabel über Zwischenkörpern F von E/K ist, da $m_{a,F}$ ein Teiler von $m_{a,K}$ ist. Wir nehmen nun zuerst an, daß E/K endlich ist. Durch die sukzessive Adjunktion endlich vieler, geeigneter Elemente aus A erhalten wir damit einen Turm endlich vieler, einfacher und separabler Erweiterungen, deren Vereinigung gleich E ist, und nach der Schlußweise zum Anfang des Beweises gilt $[E : K]_s = [E : K]$. Ist F ein Zwischenkörper, so folgt damit $[F : K]_s = [F : K]$. Dies beweist Satz 1.54 für endliche Erweiterungen.

Sei nun E/K beliebig. Ist F/K endlich, so gibt es $a_1, \ldots, a_n \in A$ mit $F \subseteq K(a_1, \ldots, a_n)$ und es folgt $[F : K]_s = [F : K]$ nach dem bereits Bewiesenen. Ist F/K unendlich, so gilt $[F : K]_s \geq [F_1 : K]_s = [F_1 : K]$ nach Satz 1.52 für alle endlichen Zwischenkörper F_1 von F/K. Da $[F_1 : K]$ beliebig groß wird, folgt $[F : K]_s = \infty = [F : K]$. □

Eine endliche, separable Erweiterung E/K gestattet also nach Satz 1.54 die maximal mögliche Anzahl von $[E : K]$ Fortsetzungen $\tau \in \mathrm{Hom}_\sigma(E, C)$ für $\sigma \in \mathrm{Hom}(K, C)$ und C algebraisch abgeschlossen.

Wir wenden uns wieder der Abbildung 1.1 zu und untersuchen, wie sich die Eigenschaft „separabel“ vererbt.

1.55 Satz. *Sei E/K eine algebraische Körpererweiterung.*

(i) Für einen Zwischenkörper F von E/K ist E/K genau dann separabel, wenn E/F und F/K separabel sind.

(ii) Sind F_1, F_2 Zwischenkörper von E/K und ist F_1/K separabel, so ist auch F_1F_2/F_2 separabel.

(iii) Ist zusätzlich F_2/K separabel, so sind F_1F_2/K und $F_1 \cap F_2/K$ separabel.

Beweis. (i): Ist E/K separabel, so folgt unmittelbar, daß F/K separabel ist. Außerdem gilt für $a \in E$, daß $m_{a,K} \in F[t]$ ist und somit von $m_{a,F}$ geteilt wird. Daher ist $m_{a,F}$ ebenfalls separabel und a separabel über F (dies wurde bereits im Beweis von Satz 1.54 gesehen). Umgekehrt sei $a \in E$ separabel über F und bezeichne L den Zwischenkörper von E/K, der durch Adjunktion der Koeffizienten von $m_{a,F}$ an K entsteht. Dann ist a wegen $m_{a,L} = m_{a,F}$ separabel über L und $L(a)/L$ und L/K sind endlich und separabel. Es folgt $[L(a) : K]_s = [L(a) : L]_s[L : K]_s = [L(a) : L][L : K] = [L(a) : K]$. Daher ist a ist separabel über K und folglich E/K separabel.

(ii): Die Separabilität von F_1F_2/F_2 folgt aus Satz 1.54, (ii) angewendet auf die Körpererweiterung $F_2(F_1)/F_2$, da die Elemente von F_1 auch separabel über F_2 sind.

(iii): Die Separabilität von F_1F_2/K folgt aus der Separabilität von F_1F_2/F_2 und F_2/K und der Transitivität von „separabel". Die Separabilität von $F_1 \cap F_2/K$ ist klar. □

Wir bemerken, daß Komposita und Schnitte über beliebige Mengen von über K separablen Zwischenkörpern von E/K wieder separabel über K sind.

1.56 Definition. Sei E/K eine algebraische Körpererweiterung und $A = \{a \in E \,|\, a \text{ ist separabel über } K\}$. Dann heißt $K(A)$ der separable Abschluß von K in E. Gilt $K(A) = K$, so nennt man K separabel abgeschlossen in E.

Ist E ein algebraischer Abschluß von K, so heißt $K(A)$ ein separabler Abschluß von K und wird mit K^s bezeichnet. Gilt $K^s = K$, so nennt man K separabel abgeschlossen.

Separable Abschlüsse K^s sind bis auf K-Isomorphie eindeutig bestimmt. Wegen der Transitivität von „separabel" sind separable Abschlüsse separabel abgeschlossen.

1.57 Satz. *Sei E/K eine algebraische Körpererweiterung und F der separable Abschluß von K in E. Dann gilt*

$$[F : K] = [E : K]_s.$$

Beweis. Siehe Satz 1.66. □

1.58 Satz (Primitives Element). *Sei E/K eine algebraische Erweiterung und $a, b \in E$. Ist a separabel über K, so besitzt $K(a, b)$ ein primitives Element.*

Beweis. Da a, b algebraisch über K sind, ist $K(a, b)/K$ endlich. Für einen endlichen Körper K ist dann auch $K(a, b)$ ein endlicher Körper. Nach Satz **??** ist $K(a, b)^\times$ zyklisch und wird von einem Element $c \in K(a, b)$ erzeugt. Dann gilt offenbar $K(a, b) = K(c)$. Für beliebiges K und $a \in K$ gilt außerdem $K(a, b) = K(b)$.

Wir nehmen nun an, daß $\#K$ unendlich ist und a nicht in K liegt. Seien C ein Zerfällungskörper von $m_{a,K} m_{b,K}$ und $a_1, a_2, \ldots, a_r \in C$ die Nullstellen von $m_{a,K}$ und $b_1, b_2, \ldots, b_s$ die Nullstellen von $m_{b,K}$ in C. Wir nehmen ohne Einschränkung $a = a_1$ und $b = b_1$ an. Für $x \in K$ setzen wir $W(x) = \{a_i x + b_j \,|\, 2 \leq i \leq r, 1 \leq j \leq s\}$. Durch Auflösen nach x und unter Verwendung der Separabilität von a sehen wir, daß es nur endlich viele $x \in K$ gibt, für die $ax + b \in W(x)$ gilt. Da $\#K = \infty$ ist, gibt es ein $y \in K$ mit $ay + b \notin W(y)$. Wir zeigen, daß $c = ay + b$ ein primitives Element von $K(a, b)/K$ ist.

Wir setzen $h = \gcd\{m_{a,K}, m_{b,K}(c - yt)\}$ in $K(c)[t]$. Wegen $m_{a,K}(a) = m_{b,K}(c - ya) = 0$ ist $t - a$ ein Teiler von h in $C[t]$. Über C zerfällt $m_{a,K}$ in die paarweise verschiedenen Linearfaktoren $t - a_i$ und $m_{b,K}$ in die Linearfaktoren $t - b_j$. Für $i \geq 2$ gilt $c - ya_i \neq b_j$ für alle j nach Wahl von y. Daher ist $m_{b,K}(c - ya_i) \neq 0$ und $h = t - a$. Wegen $h \in K(c)[t]$ nach Definition von h ergibt sich $a \in K(c)$, dann $b = c - ya \in K(c)$ und schließlich $K(a, b) = K(c)$. □

Induktiv erhalten wir

1.59 Korollar. *Jede endliche, separable Körpererweiterung ist einfach.*

1.6 Rein inseparable Erweiterungen

Wir setzen in diesem Abschnitt voraus, daß K ein Körper positiver Charakteristik $p = \operatorname{char}(K) > 0$ ist.

Sei $f \in K[t]$ ein irreduzibles Polynom. Durch wiederholte Anwendung von Korollar **??** kann f in der Form $f = g(t^{p^r})$ geschrieben werden, wobei $g \in K[t]$ irreduzibel und separabel ist, wenn r maximal gewählt wird. Über einem algebraischen Abschluß C von K gibt es dann ein separables $h \in C[t]$ mit $f = g(t^{p^r}) = h^{p^r}$, indem man p^r-te Wurzeln aus den Koeffizienten von g zieht. Die Nullstellen von f treten daher mit der genauen Vielfachheit p^r auf.

Im vorigen Abschnitt haben wir irreduzible Polynome f betrachtet, für die $g = f$ gilt, die also nur einfache Nullstellen besitzen. Wir betrachten jetzt den Fall, daß g ein Linearfaktor ist, so daß f nur eine einzige Nullstelle besitzt.

1.60 Definition. Ein Polynom $f \in K[t]$ heißt rein inseparabel, wenn es nur eine einzige Nullstelle in einem algebraischen Abschluß C von K besitzt.

Mit der obigen Zerlegung ist es klar, daß ein rein inseparables Polynom eine Potenz eines Polynoms der Form $t^{p^r} - c \in K[t]$ ist.

1.61 Definition. Sei E/K eine algebraische Erweiterung. Ein Element $a \in E$ heißt rein inseparabel, wenn $m_{a,K}$ rein inseparabel ist. Die Erweiterung E/K heißt rein inseparabel und E rein inseparabel über K, wenn jedes $a \in E \backslash K$ inseparabel über K ist.

Die Erweiterung K/K ist die einzige Erweiterung, die separabel und rein inseparabel ist. Eine Erweiterung E/K, in der jedes $a \in E$ rein inseparabel über K ist, ist selbst rein inseparabel. Die Umkehrung dieser Aussage wird im folgenden Lemma bewiesen, wodurch auch die Abweichung der Definition 1.61 im Analogievergleich zu Definition 1.50 und zu den Definitionen für „algebraisch“ behoben wird. Wir fassen ∞ auch als Potenz von $p = \mathrm{char}(K)$ auf.

1.62 Lemma. *Sei E/K eine rein inseparable Körpererweiterung.*

(*i*) *Jedes $a \in E$ ist rein inseparabel über K. Genauer gibt es ein $r \in \mathbb{Z}^{\geq 0}$ mit $a^{p^r} \in K$. Für das kleinste solche r ist $m_{a,K} = t^{p^r} - a^{p^r}$.*

(*ii*) *Der Grad $[E : K]$ ist eine Potenz von p.*

Beweis. (*i*): Ist $f = m_{a,K}$ das Minimalpolynom eines Elements $a \in E$, so ist g mit r wie aus der obigen Zerlegung das Minimalpolynom von a^{p^r} über K und separabel, folglich ist a^{p^r} separabel über K und nach Voraussetzung folgt $a^{p^r} \in K$. Also gilt $g = t - a^{p^r}$ und $f = t^{p^r} - a^{p^r}$. Da f irreduzibel über K ist, muß r bereits minimal mit $a^{p^r} \in K$ sein.

(*ii*): Für $[E : K] = \infty$ ist die Aussage richtig. Gelte nun also $[E : K] < \infty$. Für einfache rein inseparable Erweiterungen ist die Aussage wegen Lemma 1.62 ebenfalls richtig.

Ist F ein Zwischenkörper von E/K und $a \in E$, so ist a auch rein inseparabel über F, denn es gilt $m_{a,F} \,|\, m_{a,K}$ und $m_{a,F}$ ist mit $m_{a,K}$ rein inseparabel. Die Erweiterung E/K entsteht durch einen endlichen Turm von einfachen Erweiterungen, die wegen der vorstehenden Bemerkung alle rein inseparabel sind. Daher folgt die Aussage über $[E : K]$ unter Verwendung des Gradsatz. □

1.63 Satz. *Sei E/K eine algebraische Körpererweiterung. Dann sind äquivalent.*

(*i*) *E/K ist rein inseparabel.*

(*ii*) *Es gibt $A \subseteq E$ mit $E = K(A)$ und jedes $a \in A$ ist rein inseparabel über K.*

(*iii*) *Für jeden Zwischenkörper F von E/K gilt $[F : K]_s = 1$.*

Beweis. $(i) \Rightarrow (ii)$: Ist klar.

$(iii) \Rightarrow (i)$: Wenn es ein über K separables Element $b \in E \backslash K$ gibt, so ist $[K(b) : K]_s \neq 1$.

$(ii) \Rightarrow (iii)$: Seien $\sigma, \tau \in \mathrm{Hom}_K(F, C)$, wo C einen algebraischen Abschluß von K bezeichnet, und $b \in F$ beliebig. Wir wollen $\sigma(b) = \tau(b)$ und somit $\sigma = \tau$ zeigen. Es gibt zunächst $a_1, \ldots, a_n \in A$, so daß $b \in L_n$ mit $L_i = K(a_1, \ldots, a_i)$ ist. Die Elemente $a \in A$ sind rein inseparabel über jedem echten Zwischenkörper von E/K. Daher sind die L_{i+1}/L_i einfach und rein inseparabel, und nach Satz 1.52 und Lemma 1.53 gilt folglich $[L : K]_s = \prod_i [L_{i+1} : L_i]_s = 1$ und somit $[K(b) : K]_s = 1$. Dies ergibt $\sigma(b) = \tau(b)$ und $\sigma = \tau$, da b beliebig war. □

Der Beweis verdeutlicht wieder die allgemeine Strategie, Aussagen zuerst für einfache Körpererweiterungen zu untersuchen und zu beweisen, und dann auf endliche und schließlich auf algebraische Erweiterungen zu verallgemeinern.

In Satz 1.63, (*iii*) genügt es, wegen Satz 1.52 im Grunde nur die Gleichheit $[E : K]_s = 1$ zu fordern. Eine rein inseparable Erweiterung E/K gestattet also nur die minimale Anzahl von genau einer Fortsetzung $\tau \in \mathrm{Hom}_\sigma(E, C)$ für $\sigma \in \mathrm{Hom}(K, C)$ und C algebraisch abgeschlossen.

Wir wenden uns wieder der Abbildung 1.1 zu und untersuchen, wie sich die Eigenschaft „rein inseparabel“ vererbt.

1.64 Satz. *Sei E/K eine algebraische Körpererweiterung.*

(*i*) *Für einen Zwischenkörper F von E/K ist E/K genau dann rein inseparabel, wenn E/F und F/K rein inseparabel sind.*

(*ii*) *Sind F_1, F_2 Zwischenkörper von E/K und ist F_1/K rein inseparabel, so ist auch F_1F_2/F_2 rein inseparabel.*

(*iii*) *Ist zusätzlich F_2/K rein inseparabel, so sind auch F_1F_2/K und $F_1 \cap F_2/K$ rein inseparabel.*

Beweis. Der Beweis erfolgt wegen Satz 1.63 und Satz 1.66 für „rein inseparabel“ analog wie für „separabel“. □

Wir bemerken, daß Komposita und Schnitte über beliebige Mengen von über K rein inseparablen Zwischenkörpern von E/K wieder rein inseparabel über K sind.

1.65 Definition. Sei E/K eine algebraische Körpererweiterung und $A = \{a \in E \mid a \text{ ist rein inseparabel über } K\}$. Dann heißt $K(A)$ der rein inseparable Abschluß von K in E. Gilt $K(A) = K$, so nennt man K rein inseparabel abgeschlossen in E.

Ist E ein algebraischer Abschluß von K, so heißt $K(A)$ ein rein inseparabler Abschluß von K und wird mit $K^{p^{-\infty}}$ bezeichnet. Gilt $K^{p^{-\infty}} = K$, so nennt man K rein inseparabel abgeschlossen.

Die Bezeichnung $K^{p^{-\infty}}$ rührt daher, daß wir sukzessive p-te Wurzeln an K adjungieren, um $K^{p^{-\infty}}$ zu erhalten. Rein inseparable Abschlüsse $K^{p^{-\infty}}$ sind sind bis auf K-Isomorphie eindeutig bestimmt. Wegen der Transitivität von „rein inseparabel“ sind rein inseparable Abschlüsse rein inseparabel abgeschlossen.

1.66 Satz. *Sei E/K algebraisch und F der separable Abschluß von K in E. Dann ist E/F rein inseparabel, $[F : K] = [E : K]_s$ und $[E : F]$ eine Potenz von $p = \mathrm{char}(K)$.*

Beweis. Für jedes $a \in E$ gibt es ein $r \in \mathbb{Z}^{\geq 0}$, so daß a^{p^r} separabel über F ist. Wegen der Transitivität von „separabel“ folgt $a^{p^r} \in F$, also ist a rein inseparabel über F. Daher ist E/K rein inseparabel.

Nach Satz 1.54, Satz 1.63 und Satz 1.52 gilt $[F : K] = [F : K]_s = [E : F]_s[F : K]_s = [E : K]_s$. Die Aussage über $[E : F]$ folgt aus Lemma 1.62. $\square$

1.67 Definition. Sei E/K eine algebraische Körpererweiterung und F der separable Abschluß von K in E. Der Inseparabilitätsgrad von E/K wird als $[E : K]_i = [E : F]$ definiert.

Der Inseparabilitätsgrad ist also nach Satz 1.66 stets eine nicht negative Potenz der Charakteristik p und es gilt $[E : K] = [E : K]_i[E : K]_s$. Zur Vereinheitlichung definieren wir $[E : K]_i = 1$ für Körper in Charakteristik Null.

Der Inseparabilitätsgrad besitzt die gleichen Eigenschaften wie der Separabilitätsgrad:

1.68 Satz. *Sei E/K eine algebraische Körpererweiterung.*

(*i*) *Für jeden Zwischenkörper F von E/K gilt $[E : K]_i = [E : F]_i[F : K]_i$.*

(*ii*) *Ist F der rein inseparable Abschluß von K in E, so gilt $[F : K] = [E : K]_i$.*

Beweis. (*i*): Wir wenden Satz 1.72 mehrfach an. Sei F_1 der separable Abschluß von K in F, F_2 der rein inseparable Abschluß von K in F, E_1 der separable Abschluß von F in E und E_2 der rein inseparable Abschluß von F in E. Sei T der separable Abschluß von F_1 in E_1.

Dann ist F/F_1 rein inseparabel. Da E_1/F separabel ist, muß F/F_1 der rein inseparable Abschluß von F_1 in E_1 sein und es gilt $E_1 = TF$. Folglich ist auch

E_1/T rein inseparabel. Nun gilt $[E_1 : T] = [F : F_1] = [F_2 : K] = [F : K]_i$, $[E : E_1] = [E_2 : F] = [E : F]_i$, T/K ist separabel und E/T ist rein inseparabel. Also ist T/K der separable Abschluß von K in E und es gilt $[E : K]_i = [E : T]$.

Zusammen folgt $[E : K]_i = [E : T] = [E : E_1][E_1 : T] = [E : F]_i[F : K]_i$, was zu zeigen war.

(ii): Folgt aus Satz 1.72. □

Für endliche Erweiterungen E/K kann man den Satz auch mit Hilfe der Multiplikativität von $[:]$, $[:]_s$ und mit $[E : K] = [E : K]_i[E : K]_s$ leicht beweisen.

Der Satz vom primitiven Element gilt für (rein) inseparable Erweiterungen im allgemeinen nicht. Sei zum Beispiel $K = \mathbb{F}_p(x, y)$ und $E = K(x^{1/p}, y^{1/p})$. Dann gilt $[E : K] = p^2$, aber für jedes $a \in E$ ist $m_{a,K} = t^p - a^p$. Also kann E/K nicht einfach sein.

1.7 Weitere Eigenschaften von normalen, separablen und rein inseparablen Erweiterungen

Wir bezeichnen mit K jetzt wieder einen beliebigen Körper. Wird das Symbol p verwendet, so nehmen wir $p = \mathrm{char}(K) > 0$ an.

1.69 Definition. Ein Körper K heißt vollkommen, wenn jede algebraische Körpererweiterung E/K separabel ist.

Für einen Körper K schreiben wir $K^p = \{a^p \mid a \in K\}$. Man kann die Definition offensichtlich auf höhere p-Potenzen und unter Verwendung eines algebraischen Abschluß von K auch auf negative Potenzen erweitern.

1.70 Satz. (i) *Jeder Körper der Charakteristik Null ist vollkommen.*

(ii) *Ein Körper der Charakteristik $p > 0$ ist genau dann vollkommen, wenn $K^p = K$ gilt.*

(iii) *Jeder algebraische Erweiterungskörper eines vollkommenen Körpers ist vollkommen.*

Beweis. (i): Die über K irreduziblen Polynome sind separabel.

(ii): Ist $K^p \neq K$, so gibt es ein $a \in K \backslash K^p$ und $f = t^p - a$ hat keine Nullstelle in K, aber nur eine Nullstelle in einem algebraischen Abschluß von K. Damit besitzt f einen irreduziblen, nicht separablen Faktor vom Grad ≥ 2. Sei nun $K^p = K$ und $f \in K[t]$ irreduzibel. Ist f nicht separabel, so gibt es wegen $K^p = K$ Polynome $g, h \in K[t]$ mit $f = g(t^p) = h^p$, im Widerspruch zur Irreduzibilität von f.

(iii): Sei K vollkommen und L/K algebraisch. Ist dann E/L algebraisch, so ist auch E/K algebraisch und daher nach Voraussetzung separabel. Dann ist auch E/L separabel. □

Sei K ein Körper mit endlichen vielen Elementen, und sei $p = \mathrm{char}(K) > 0$. Da der Frobeniusendomorphismus $x \mapsto x^p$ von K injektiv ist, ist er wegen der Endlichkeit von K auch surjektiv und es gilt $K^p = K$. Körper mit endlich vielen Elementen sind somit vollkommen. Algebraische Abschlüsse und rein inseparable Abschlüsse sind ebenfalls vollkommen. Auf der anderen Seite ist zum Beispiel $\mathbb{F}_p(t)$ nicht vollkommen.

1.71 Lemma. *Die normale Hülle einer separablen Körpererweiterung E/K ist separabel. Der separable Abschluß von K in einer normalen Körpererweiterung E/K ist normal. Eine rein inseparable Körpererweiterung E/K ist normal.*

Beweis. Die ersten zwei Aussagen ergeben sich aus der Tatsache, daß die zu einem über K separablen Element konjugierten Elemente ebenfalls separabel sind, da sie das gleiche Minimalpolynom haben. Die dritte Aussage folgt direkt aus der Definition von „normal“ und Lemma 1.62. □

Im Abschnitt 1.6 haben wir gesehen, daß sich eine algebraische Körpererweiterung E/K in eine separable Erweiterung F/K und eine rein inseparable Erweiterung E/F aufteilen läßt. Hier ist F der separable Abschluß von K in E und es gilt allgemein $[F : K] = [E : K]_s$.

1.72 Satz. *Sei E/K eine algebraische Körpererweiterung. Sei F_1 der separable Abschluß von K in E und F_2 der rein inseparable Abschluß von K in E.*

(i) *Die Erweiterungen F_1/K und E/F_2 sind separabel und die Erweiterungen F_2/K und E/F_1 sind rein inseparabel.*

(ii) *F_1 und F_2 sind linear disjunkt über K und es gilt $E = F_1F_2$.*

(iii) $[F_1 : K] = [E : F_2] = [E : K]_s$ *und* $[F_2 : K] = [E : F_1] = [E : K]_i$.

Beweis. *(i)*: Die Erweiterungen F_1/K und F_2/K sind nach Definition separabel bzw. rein inseparabel. Sei $a \in E$. Dann sind $F_1' = F_1 \cap K(a)$ und $F_2' = F_2 \cap K(a)$ der separable bzw. rein inseparable Abschluß von K in $K(a)$. Nach Satz 1.66 ist die Erweiterung $K(a)/F_1'$ rein inseparabel. Die Erweiterung $K(a)/F_2'$ ist separabel, allerdings benötigt der Beweis dieser Tatsache etwas Galoistheorie und wird verschoben. Nach Satz 1.64, *(ii)* und Satz 1.55, *(ii)* sind dann auch die Erweiterungen $F_1(a)/F_1$ und $F_2(a)/F_2$ rein inseparabel bzw. separabel. Da a beliebig war, sind E/F_1 und E/F_2 insgesamt rein inseparabel bzw. separabel.

(ii): Die Erweiterung E/F_1F_2 ist wegen (i) nach Satz 1.64, (i) rein inseparabel und nach Satz 1.55, (i) und separabel. Daher gilt $E = F_1F_2$.

Für die lineare Disjunktheit genügt es wegen Satz 1.58 zu zeigen, daß für jedes $a \in E$ die Erweiterungen $K(a)/K$ und F_2/K linear disjunkt sind. Nach Lemma 1.62 gibt es $s \in \mathbb{Z}^{\geq 0}$ mit ${m_{a,F_2}}^{p^s} \in K[t]$. Dann gilt $m_{a,K} \mid {m_{a,F_2}}^{p^s}$ in $K[t]$ und folglich auch in $F_2[t]$. Da m_{a,F_2} irreduzibel ist, gibt es also $d \in \mathbb{Z}^{\geq 1}$ mit $m_{a,K} = {m_{a,F_2}}^d$. Weil $m_{a,K}$ aber separabel ist, folgt $d = 1$ und $m_{a,K} = m_{a,F_2}$. Es ergibt sich $[F_2(a) : F_2] = [K(a) : K]$ und nach Satz 1.23, (i) sind $K(a)/K$ und F_2/K linear disjunkt.

(iii): Die Gleichungen folgen unmittelbar aus (ii) und den Definitionen. □

1.73 Korollar. *Sei E/K eine einfache Erweiterung mit primitivem Element a und C ein algebraischer Abschluß von E. Sei $f = m_{a,K}$ und $r \in \mathbb{Z}^{\geq 0}$ maximal, so daß es ein $g \in K[t]$ mit $f = g(t^{p^r})$ gibt. Sei $h \in C[t]$ mit $h^{p^r} = g(t^{p^r}) = f$. Sei F_1 der separable Abschluß von K in E und F_2 der rein inseparable Abschluß von K in E. Dann gilt.*

(i) $m_{a,F_1} = t^{p^r} - a^{p^r}$ *und* $m_{a,F_2} = h$ *(insbesondere ist $h \in F_2[t]$ irreduzibel).*

(ii) $F_1 = K(a^{p^r})$ *und* $m_{a^{p^r},K} = g$. $F_2 = K(c_0^{p^{-r}}, \ldots, c_n^{p^{-r}})$ *mit* $g = \sum_{i=0}^n c_i t^i$.

Beweis. (i): Die Aussage $m_{a,F_1} = t^{p^r} - a^{p^r}$ folgt aus Lemma 1.62. Nach Lemma 1.62 gibt es auch $s \in \mathbb{Z}^{\geq 0}$ mit ${m_{a,F_2}}^{p^s} \in K[t]$. Dann gilt $f \mid {m_{a,F_2}}^{p^s}$. Das Polynom h ist nach Definition separabel. Wegen Satz 1.72, (i) ist aber auch m_{a,F_2} separabel. Daher folgt $r = s$ und $m_{a,F_2} = h$.

(ii): Das Polynom g ist separabel und irreduzibel über K und es gilt $g(a^{p^r}) = 0$. Daher folgt $m_{a^{p^r},K} = g$ und $K(a^{p^r}) \subseteq F_1$. Aus Gradgründen ergibt sich $K(a^{p^r}) = F_1$. Weiter gilt $h = \sum_i c_i^{p^{-r}} t^i$ und aus Aussage (i) und Lemma 1.24 folgt $F_2 = K(c_0^{p^{-r}}, \ldots, c_n^{p^{-r}})$. □

1.74 Satz. *Sei E/K eine algebraische Körpererweiterung und F_1, F_2 Zwischenkörper von E/K. Ist F_1/K normal, F_2/K separabel und gilt $F_1 \cap F_2 = K$, so sind F_1 und F_2 linear disjunkt über K.*

Beweis. Sei T der separable Abschluß von K in F_1. Dann sind T/K und F_2/K linear disjunkt wegen Satz 2.13. Da F_1/T rein inseparabel und TF_2/T separabel ist, sind diese Erweiterungen wegen Satz 1.72 linear disjunkt über T. Aus der Übungsaufgabe über die „Transitivität“ von „linear disjunkt“ in Türmen folgt die Aussage. □

1.75 Satz. *Sei E/K eine endliche Körpererweiterung mit $p = \mathrm{char}(K) > 0$. Dann ist E/K genau dann separabel, wenn $E^pK = E$ gilt. Aus $E^pK = E$ folgt $E^{p^n}K = E$ für alle $n \geq 0$.*

Beweis. Wir beweisen die letzte Aussage zuerst. Es gelte $E^pK = E$. Dann folgt induktiv $E^{p^{n+1}}K = (E^{p^n})^p(K^pK) = (E^{p^n}K)^pK = E^pK = E$.

Sei nun E/K separabel. Dann ist E/E^pK separabel und rein inseparabel, denn für $a \in E$ gilt $a^p \in E^pK$. Es folgt $E = E^pK$. Gelte nun $E^pK = E$ und sei L der separable Abschluß von K in E. Dann ist E/L nach Satz 1.66 rein inseparabel. Es gibt $a_1, \dots a_r \in E$ mit $E = K(a_1, \dots, a_r)$, und für jedes a_i gibt es ein $m_i \geq 0$ mit $a_i^{p^{m_i}} \in L$. Dann folgt mit $m = \max_i m_i$, daß $E^{p^m} \subseteq L$. Wegen $K \subseteq L$ ergibt sich $E = E^{p^m}K \subseteq L$, folglich $E = L$ und E/K ist separabel. □

Satz 1.75 wird falsch, wenn auf die Endlichkeitsvoraussetzung von E/K verzichtet wird. Zum Beispiel gilt $E^p = E$ für einen rein inseparablen Abschluß $E = K^{p^{-\infty}}$ von K, und E/K ist nicht separabel.

1.8 Endliche Körper

Ein endlicher Körper ist ein Körper mit endlich vielen Elementen. Endliche Körper sind in gewisser Weise die „einfachsten“ Körper, die es gibt. Sie spielen eine wichtige Rolle in der Mathematik und in praktischen Anwendungen wie zum Beispiel Kryptographie und Kodierungstheorie.

Ist p eine Primzahl, so ist zum Beispiel der Faktorring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper der Charakteristik p. Ist K ein endlicher Körper, so ist sein Primkörper von der Form $\mathbb{F}_p$ für eine geeignete Primzahl p. Da K ein Vektorraum der Dimension $n = [K : \mathbb{F}_p]$ über $\mathbb{F}_p$ ist, folgt $\#K = p^n$.

1.76 Satz. *Sei K ein endlicher Körper mit q Elementen. Dann ist $K^\times$ eine endliche zyklische Gruppe und für $x \in K$ gilt $x^q = x$.*

Beweis. Folgt direkt aus Satz **??**, da $K^\times$ eine endliche Gruppe ist. Es gilt weiter $\#K^\times = q - 1$, und folglich ist $x^{q-1} = 1$ für $x \in K^\times$. Daraus folgt $x^q = x$ für alle $x \in K$. □

1.77 Satz. *Sei K ein Erweiterungskörper von $\mathbb{F}_p$. Dann sind äquivalent.*

(*i*) *K ist ein endlicher Körper mit $q = p^n$ Elementen.*

(*ii*) *K ist Zerfällungskörper des Polynoms $t^q - t$ über $\mathbb{F}_p$ mit $q = p^n$.*

Insbesondere existiert also für jedes $q = p^n$ ein endlicher Körper K mit q Elementen.

Beweis. (*i*) $\Rightarrow$ (*ii*): Aus Satz 1.76 folgt, daß die Elemente von K genau die Nullstellen von $t^q - t$ sind.

$(ii) \Rightarrow (i)$: Sind $a, b \in K$ und $b \neq 0$ zwei Nullstellen von $t^q - t$, so sind auch $a + b, ab, -a, 1/b$ Nullstellen von $t^q - t$. Aus $a^q = a$ und $b^q = b$ folgt nämlich $a^q + b^q = (a + b)^q = a + b$, $(ab)^q = ab$, $(-a)^q = -a$ und $(1/b)^q = 1/b$ unter Beachtung von Satz **??**. Damit bilden die Nullstellen von $t^q - t$ bereits einen Körper, und K besteht wegen der Zerfällungskörpereigenschaft aus genau diesen Nullstellen. Wegen $\gcd\{t^q - t, qt^{q-1} - 1\} = 1$ ist $t^q - t$ separabel und daher $\#K = q$.

Die Existenz von K folgt aus der Existenz von Zerfällungskörpern. □

1.78 Satz. *Je zwei endliche Körper mit q Elementen sind isomorph. Jede Erweiterung E/K von endlichen Körpern ist normal, separabel und einfach. Endliche Körper sind vollkommen.*

Beweis. Die Isomorphie folgt, weil Zerfällungskörper isomorph sind. Die Normalität folgt, weil E als Zerfällungskörper über $\mathbb{F}_p$ und über K normal ist. Die Separabilität folgt, weil die Polynome $t^q - t$ separabel sind. Nach dem Satz vom primitiven Element ist E/K dann einfach. Ein primitives Element wird zum Beispiel durch einen Erzeuger von $E^\times$ gegeben. Daß endliche Körper vollkommen sind, wurde bereits gezeigt. Man kann auch so argumentieren: Ist a ein über K separables Element, so ist $K(a)$ ein endlicher Körper und $m_{a,K}$ ein Teiler eines Polynoms der Form $t^q - t$ und somit separabel. □

1.79 Definition. Innerhalb eines fest gewählten, algebraischen Abschlußes $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ bezeichnen wir mit $\mathbb{F}_q$ den eindeutig bestimmten endlichen Körper mit q Elementen in $\overline{\mathbb{F}}_p$.

1.80 Satz. *Seien E und K endliche Körper in einem gemeinsamen Erweiterungskörper C. Es gelte $\#E = p^n$ und $\#K = p^m$. Dann gilt $K \subseteq E$ genau dann, wenn $m \mid n$.*

Beweis. Gilt $K \subseteq E$, so folgt $\#E = (\#K)^{[E:K]}$, also $p^n = p^{m[E:K]}$. Gelte umgekehrt $m \mid n$. Für $x \in K$ ergibt sich $x^{p^m} = x$ und somit $x^{p^n} = x$. Dies wiederum bedeutet $x \in E$. □

Die explizite Darstellung von endlichen Körpern kann wieder mit irreduziblen Polynomen erfolgen. Ist K ein endlicher Körper mit q Elementen und $f \in K[t]$ normiert und irreduzibel vom Grad n, so ergibt $K[t]/fK[t]$ eine Erweiterung von K vom Grad n. Wählt man ein anderes irreduzibles Polynom vom Grad n, so erhält man einen K-isomorphen Körper.

1.9 Kreisteilungskörper

1.81 Definition. Sei K ein Körper und $f = t^n - 1$. Die Nullstellen von f in einem algebraischen Abschluß $\bar{K}$ von K heißen n-te Einheitswurzeln und die Menge der

n-ten Einheitswurzeln von f in $\bar{K}$ wird mit μ_n bezeichnet. Der Zerfällungskörper $K(\mu_n)$ von f über K heißt n-ter Kreisteilungskörper.

Offenbar gilt $\#\mu_n \leq n$ und $\mu_m \subseteq \mu_n$ für $m \mid n$. Der Name Kreisteilungskörper ergibt sich daraus, daß die n-ten Einheitswurzeln in $\mathbb{C}$ von der Form $\exp(2\pi ir/n)$ sind, daher auf dem Einheitskreis liegen und ihn in gleiche Teile teilen. Ist E als weiteres Beispiel ein endlicher Körper mit q Elementen, so gilt $E = K(\mu_{q-1})$.

1.82 Satz. *Die Menge μ_n ist eine zyklische Untergruppe von $K(\mu_n)^\times$. Es gilt $\mu_{pn} = \mu_n$ für $p = \mathrm{char}(K) > 0$. Aus $p \nmid n$ oder $\mathrm{char}(K) = 0$ folgt $\#\mu_n = n$.*

Beweis. Die erste Aussage folgt aus Satz **??**. Die zweite folgt, weil $t^{mp} - 1 = (t^m - 1)^p$ ist. Die dritte folgt, weil $\gcd\{t^n - 1, nt^{n-1}\} = 1$ unter den gemachten Voraussetzungen gilt. □

Wir nehmen für den Rest des Abschnitts an, daß n nicht von der Charakteristik geteilt wird bzw. daß die Charakteristik Null ist.

1.83 Definition. Die Erzeuger von μ_n heißen primitive n-te Einheitswurzeln. Für eine primitive n-te Einheitswurzel heißt das Polynom

$$\Phi_n = \prod_{\substack{1 \leq i \leq n \\ \gcd\{i,n\} = 1}} (t - \zeta^i)$$

das n-te Kreisteilungspolynom.

Eine zyklische Gruppe der Ordnung n hat $\phi(n)$ verschiedene Erzeuger. Daher gibt es also genau $\phi(n)$ primitive n-te Einheitswurzeln. Ferner hat Φ_n genau die primitiven n-ten Einheitswurzeln als Nullstellen und es gilt $\deg(\Phi_n) = \phi(n)$. Ist d die Ordnung einer Einheitswurzel $\zeta \in \mu_n$, so ist ζ eine primitive d-te Einheitswurzel. Sind n and m teilerfremd, so gilt $\mu_n\mu_m = \mu_{nm}$ und $\mu_n \cap \mu_m = \{1\}$.

1.84 Satz. *Für die Kreisteilungspolynome gilt die Beziehung $t^n - 1 = \prod_{d \mid n} \Phi_d$.*

Beweis. Ist klar, weil wir alle primitiven Einheitswurzeln erfassen. □

Der Satz liefert ein Rekursionsverfahren zur Berechnung der Kreisteilungspolynome, mittels $\Phi_n = (t^n - 1)/\prod_{d \mid n, d \neq n} \Phi_d$. Ist n zum Beispiel prim, gilt also $\Phi_n = (t^n - 1)/(t - 1) = \sum_{i=0}^{n-1} t^i$. Für eine Reihe weiterer Rekursionsformeln siehe Lang, Algebra, S. 208.

1.85 Satz. *Die Kreisteilungspolynome sind bereits über $\mathbb{Z}$ bzw. den jeweiligen Primkörpern $\mathbb{F}_p$ definiert.*

Beweis. Folgt induktiv aus der Rekursionsformel $\Phi_n = (t^n - 1)/\prod_{d\,|\,n, d\neq n} \Phi_d$. Da Zähler und Nenner der rechten Seite über $\mathbb{Z}$ bzw. über dem jeweiligen Primkörper definiert und die Nenner normiert sind, ist auch Φ_d über $\mathbb{Z}$ bzw. über dem jeweiligen Primkörper definiert. $\square$

1.86 Satz. *Das n-te Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Q}$.*

Beweis. Sei f ein normierter irreduzibler Faktor von Φ_n über $\mathbb{Q}$. Dann gilt bereits $f \in \mathbb{Z}[t]$ nach Korollar **??**. Sei p eine Primzahl mit $p \nmid n$ und ζ eine Nullstelle von f. Dann ist ζ^p ebenfalls eine primitive n-te Einheitswurzel. Wir zeigen gleich, daß ζ^p auch eine Nullstelle von f ist. Durch die Verwendung möglicherweise verschiedener, jedoch zu n teilerfremder Primzahlen p_i können wir dann jede primitive n-te Einheitswurzel ξ in der Form $\xi = \zeta^{\prod_i p_i}$ schreiben. Damit ist jede primitive n-te Einheitswurzel eine Nullstelle von f, es gilt $\Phi_n = f$ und Φ_n ist irreduzibel.

Sei $h \in \mathbb{Z}[t]$ normiert mit $fh = \Phi_n$. Es gilt $f(\zeta^p) = 0$ oder $h(\zeta^p) = 0$. Nehmen wir $f(\zeta^p) \neq 0$ an. Dann ist ζ^p eine Nullstelle von h und ζ eine Nullstelle von $h(t^p)$. Folglich gilt $f \,|\, h(t^p)$ und es gibt $g \in \mathbb{Z}[t]$ normiert mit $fg = h(t^p)$. Sei $\bar{\cdot} : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ der kanonische Epimorphismus bezüglich koeffizientenweiser Reduktion modulo p. Für alle $x \in \mathbb{F}_p$ gilt $x^p = x$. Daher folgt $\overline{h}(t)^p = \overline{h}(t^p) = \overline{f}\overline{g}$. Wegen $\deg(\overline{f}) \geq 1$ haben dann $\overline{h}$ und $\overline{f}$ einen gemeinsamen Faktor vom Grad ≥ 1 und sind nicht teilerfremd. Auf der anderen Seite sind aber die Polynome $t^n - 1 \in \mathbb{F}_p[t]$ und damit $\overline{\phi}_n = \overline{f}\,\overline{h} \in \mathbb{F}_p[t]$ wegen $p \nmid n$ separabel. Daraus ergibt sich ein Widerspruch, und es muß also $f(\zeta^p) = 0$ gelten. $\square$

Der vorhergehende Satz ist über endlichen Körpern im allgemeinen falsch.

1.87 Korollar. *Es gilt $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ für eine primitive n-te Einheitswurzel $\zeta \in \mu_n$. Sind n und m teilerfremd so gilt $\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{nm})$ und $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}$.*

Beweis. Der erste Teil ist klar. Für den zweiten folgt aus $\mu_n\mu_m = \mu_{nm}$, daß $\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{nm})$ gilt. Wegen $\phi(nm) = \phi(n)\phi(m)$ ergibt sich dann aus Gradgründen $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = [\mathbb{Q}(\mu_{nm}) : \mathbb{Q}(\mu_m)]$, so daß $\mathbb{Q}(\mu_n)$ und $\mathbb{Q}(\mu_m)$ über $\mathbb{Q}$ linear disjunkt sind und somit $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}$ folgt. $\square$

1.88 Satz. *Die Körpererweiterungen $K(\mu_n)/K$ sind normal und separabel.*

Beweis. $K(\mu_n)$ ist Zerfällungskörper des separablen Polynoms $t^n - 1$. $\square$

1.10 Charakteristisches Polynom, Spur und Norm

Wir wenden nun eine allgemeine und häufig auftretende Begriffsbildung aus der linearen Algebra auf endliche Körpererweiterungen an.

Das charakteristische Polynom, die Spur und Norm (Determinante) von Vektorraumendomorphismen sind wie folgt definiert. Sei V ein Vektorraum über dem Körper K der Dimension n und $\phi \in \mathrm{End}_K(V)$. Für eine Basis $v_1, \ldots, v_n$ von V sei $M \in K^{n\times n}$ mit $(\phi(v_1), \ldots, \phi(v_n)) = (v_1, \ldots, v_n)M$ die Darstellungsmatrix von ϕ bezüglich der v_i. Dann ist $\chi_{\phi,V/K} = \det(tI_n - M) \in K[t]$ mit $\deg(\chi_{\phi,V/K}) = n$ das charakteristische Polynom von ϕ, und für $\chi_{\phi,V/K} = \sum_{i=0}^{n} a_i t^{n-i}$ ist die Spur von ϕ gleich $\mathrm{Tr}_{V/K}(\phi) = \mathrm{Tr}(M) = -a_1$ und die Norm von ϕ gleich $\mathrm{N}_{V/K}(\phi) = \det(M) = (-1)^n a_n$. Das charakteristische Polynom, die Spur und die Norm von ϕ hängen nicht von der gewählten Basis v_i ab.

Die Notation V/K zusammen mit ϕ soll im Zusammenhang mit charakteristischem Polynom, Spur und Norm bedeuten, daß V ein K-Vektorraum ist und daß $\phi \in \mathrm{End}_K(V)$ gilt.

Sei E/K eine endliche Körpererweiterung und $a \in E$. Dann ist E auch ein endlich dimensionaler Vektorraum über K und die Multiplikation $x \mapsto ax$ mit a liefert einen Vektorraumendomorphismus ϕ_a von E (allgemeiner kann man auch eine endlich dimensionale K-Algebra E betrachten).

1.89 Definition. Das charakteristische Polynom $\chi_{a,E/K} \in K[t]$ von a bezüglich der endlichen Körpererweiterung E/K wird als χ_{ϕ_a} definiert. Die Spur $\mathrm{Tr}_{E/K}(a)$ und die Norm $\mathrm{N}_{E/K}(a)$ von a bezüglich E/K werden als $\mathrm{Tr}_{E/K}(\phi_a)$ beziehungsweise $\mathrm{N}_{E/K}(\phi_a)$ definiert.

Wir wiederholen zunächst die für uns interessanten, allgemeinen Eigenschaften charakteristischer Polynome, Spuren und Normen für Vektorraumendomorphismen.

Nach dem Satz von Cayley-Hamilton ist $\chi_{\phi,V/K}(\phi)$ die Nullabbildung auf V. Sind $\phi_1, \phi_2 \in \mathrm{End}_K(V)$ und $\lambda \in K$, so gilt offenbar $\mathrm{Tr}_{V/K}(\phi_1 + \phi_2) = \mathrm{Tr}_{V/K}(\phi_1) + \mathrm{Tr}_{V/K}(\phi_2)$ und $\mathrm{Tr}_{V/K}(\lambda\phi_1) = \lambda \mathrm{Tr}_{V/K}(\phi_1)$. Die Spur ist demnach K-linear. Ferner gilt $\mathrm{N}_{V/K}(\phi_1\phi_2) = \mathrm{N}_{V/K}(\phi_1)\mathrm{N}_{V/K}(\phi_2)$, so daß die Norm multiplikativ ist.

Seien $V_1, V_2 \subseteq V$ Unterräume von V mit $V = V_1 \oplus V_2$ und $\phi(V_i) \subseteq V_i$. Wir setzen $\phi_i = \phi|V_i$. Dann gilt $\chi_{\phi,V/K} = \chi_{\phi_1,V_1/K} \cdot \chi_{\phi_2,V_2/K}$ und folglich $\mathrm{Tr}_{V/K}(\phi) = \mathrm{Tr}_{V_1/K}(\phi_1) + \mathrm{Tr}_{V_2/K}(\phi_2)$ und $\mathrm{N}_{V_1/K}(\phi) = \mathrm{N}_{V_1/K}(\phi_1)\mathrm{N}_{V_2/K}(\phi_2)$.

Das folgende Lemma ist im wesentlichen eine Aussage aus der linearen Algebra.

1.90 Lemma. *Sei F ein Körper und Teilring von $K^{m\times m}$ und sei*

$$h : F^{n\times n} \to K^{nm\times nm},\ ((a_{i,j,\mu,\nu})_{i,j})_{\mu,\nu} \mapsto (a_{i,j,\mu,\nu})_{(\mu-1)n+i,(\nu-1)n+j}.$$

Dann ist h ein Ringmonomorphismus, und für alle $M \in F^{n\times n}$ gilt

$$\mathrm{Tr}(\mathrm{Tr}(M)) = \mathrm{Tr}(h(M)) \text{ und } \det(\det(M)) = \det(h(M)).$$

Beweis. Es ist zunächst offensichtlich, daß h injektiv ist und $h(0) = 0$, $h(1) = 1$ gilt. Seien $M, N \in F^{n\times n}$ und $M = ((a_{i,j,\mu,\nu})_{i,j})_{\mu,\nu}$, $N = ((b_{i,j,\mu,\nu})_{i,j})_{\mu,\nu}$. Dann gilt

$$\begin{aligned}
h(MN) &= h\left(\Big(\sum_{c=1}^{n}(a_{i,j,\mu,c})_{i,j}(b_{i,j,c,\nu})_{i,j}\Big)_{\mu,\nu}\right)\\
&= h\left(\Big(\sum_{c=1}^{n}\big(\sum_{d=1}^{m} a_{i,d,\mu,c}b_{d,j,c,\nu}\big)_{i,j}\Big)_{\mu,\nu}\right)\\
&= h\left(\Big(\big(\sum_{c=1}^{n}\sum_{d=1}^{m} a_{i,d,\mu,c}b_{d,j,c,\nu}\big)_{i,j}\Big)_{\mu,\nu}\right)\\
&= \Big(\sum_{c=1}^{n}\sum_{d=1}^{m} a_{i,d,\mu,c}b_{d,j,c,\nu}\Big)_{(\mu-1)n+i,(\nu-1)n+j}\\
&= \big(a_{i,j,\mu,\nu}\big)_{(\mu-1)n+i,(\nu-1)n+j}\big(b_{i,j,\mu,\nu}\big)_{(\mu-1)n+i,(\nu-1)n+j}\\
&= h(N)h(M).
\end{aligned}$$

Für die Spur gilt direkt

$$\begin{aligned}
\mathrm{Tr}(\mathrm{Tr}(M)) = \mathrm{Tr}\Big(\sum_{c=1}^{n}(a_{i,j,c,c})_{i,j}\Big) &= \mathrm{Tr}\Big(\big(\sum_{c=1}^{n} a_{i,j,c,c}\big)_{i,j}\Big)\\
&= \sum_{d=1}^{m}\sum_{c=1}^{n} a_{d,d,c,c} = \mathrm{Tr}(h(M)).
\end{aligned}$$

Für die Determinante gilt zunächst $\det(\det(M)) = \det(h(M))$, wenn M eine Dreiecksmatrix oder eine elementare Transformationsmatrix der folgenden Form ist: Zeile mit Element aus F multiplizieren, Zeile mit Element aus F multiplizieren und zu einer anderen Zeile addieren, zwei Zeilen vertauschen. Die Aussage für Dreiecksmatrizen ist aus der linearen Algebra bekannt. Die Aussage für die ersten beiden Transformationsmatrixtypen folgt aus der für Dreiecksmatrizen. Ist M eine Transformationsmatrix des dritten Typs, so entsteht $h(M)$ aus I_{nm} durch Vertauschung von m Zeilen und es gilt

$$\det(\det(M)) = \det(-1) = \det(-I_m) = (-1)^m = \det(h(M)).$$

Nach dem Gaußalgorithmus gibt es zu beliebigem $M \in F^{n\times n}$ elementare Transformationsmatrizen $T_i \in F^{n\times n}$ und eine Dreiecksmatrix $N \in F^{n\times n}$ mit $M = N\prod_i T_i$. Dann folgt

$$\begin{aligned}\det(\det(M)) &= \det(\det(N\prod_i T_i)) = \det(\det(N)\prod_i \det(T_i))\\ &= \det(\det(N))\prod_i \det(\det(T_i)) = \det(h(N))\prod_i \det(h(T_i))\\ &= \det(h(N)\prod_i h(T_i)) = \det(h(N\prod_i T_i))\\ &= \det(h(M)).\end{aligned}$$

□

1.91 Satz. *Sei V ein endlich dimensionaler F-Vektorraum und K ein Teilkörper von F mit $[F:K] < \infty$. Für $\phi \in \mathrm{End}_F(V)$ gilt auch $\phi \in \mathrm{End}_K(V)$ und*

(i) $\mathrm{Tr}_{V/K}(\phi) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{V/F}(\phi))$,

(ii) $\mathrm{N}_{V/K}(\phi) = \mathrm{N}_{F/K}(\mathrm{N}_{V/F}(\phi))$,

(iii) $\chi_{\phi,V/K} = \mathrm{N}_{F(t)/K(t)}(\chi_{\phi,V/F})$.

Beweis. Der Beweis beruht auf der „Transitivität" der Spur und der Determinante aus Lemma 1.90.

Sei $n = \dim_F(V)$ und $m = [F:K]$. Es ist günstig, anstelle von F und K mit den rationalen Funktionenkörpern $F(t)$ und $K(t)$ zu arbeiten. Eine Basis von F über K ist auch eine Basis von $F(t)$ über $K(t)$. Wir bezeichnen mit $f: F(t) \to K(t)^{m\times m}$ den Monomorphismus, der jedem $a \in F(t)$ die Darstellungsmatrix der Muliplikation-mit-a-Abbildung bezüglich einer festgewählten Basis $e_1, \ldots, e_m$ von F über K zuordnet. Definitionsgemäß gilt dann $\mathrm{Tr}(f(a)) = \mathrm{Tr}_{F(t)/K(t)}(a)$ und $\det(f(a)) = \mathrm{N}_{F(t)/K(t)}(a)$ für alle $a \in F(t)$ und speziell auch $\mathrm{Tr}(f(a)) = \mathrm{Tr}_{F/K}(a)$ und $\det(f(a)) = \mathrm{N}_{F/K}(a)$ für alle $a \in F$.

Die Abbildung $f_n: F(t)^{n\times n} \to K(t)^{nm\times nm}$ wird analog zu h in Lemma 1.90 als der durch koeffizientenweise Anwendung von f erhaltene Monomorphismus definiert. Nach Lemma 1.90 gilt nun $\mathrm{Tr}(f(\mathrm{Tr}(M))) = \mathrm{Tr}(f_n(M))$ und $\det(f(\det(M))) = \det(f_n(M))$ für jedes $M \in F(t)^{n\times n}$.

Sei $v_1, \ldots, v_n$ eine F-Basis von V. Dann ist $e_j v_\nu$ für $1 \le j \le m$ und $1 \le \nu \le n$ eine K-Basis von V. Sei $M_F = (m_{\mu,\nu})_{\mu,\nu} \in F^{n\times n}$ die Darstellungsmatrix von ϕ bezüglich $(v_\nu)_\nu$ und sei $M_K \in K^{nm\times nm}$ die Darstellungsmatrix von ϕ bezüglich $(e_j v_\nu)_{(\nu-1)n+j}$. Wir wollen $M_K = f_n(M_F)$ zeigen. Sei $f_n(M_F) =$

$(a_{i,j,\mu,\nu})_{(\mu-1)n+i,(\nu-1)n+j}$ mit $a_{i,j,\mu,\nu} \in K$. Dann gilt aufgrund der Definitionen $\phi(v_\nu) = \sum_{c=1}^n m_{c,\nu} v_c$ und $m_{\mu,\nu} e_j = \sum_{d=1}^m a_{d,j,\mu,\nu} e_d$ und zusammen

$$\begin{aligned}\phi(e_j v_\nu) = e_j \phi(v_\nu) = e_j \sum_{c=1}^n m_{c,\nu} v_c = \sum_{c=1}^n (m_{c,\nu} e_j) v_c = \sum_{c=1}^n \Big(\sum_{d=1}^m a_{d,j,c,\nu} e_d \Big) v_c \\ = \sum_{c=1}^n \sum_{d=1}^m a_{d,j,c,\nu} e_d v_c.\end{aligned}$$

Dies heißt aber nichts anderes, als daß $(a_{i,j,\mu,\nu})_{(\mu-1)n+i,(\nu-1)n+j} = f_n(M_F)$ die Darstellungsmatrix von ϕ bezüglich der K-Basis $(e_j v_\nu)_{(\nu-1)n+j}$ ist, daß also $M_K = f_n(M_F)$ gilt.

Mit der Transitivität der Spur ergibt sich nun zusammenfassend

$$\begin{aligned}\mathrm{Tr}_{V/K}(\phi) &= \mathrm{Tr}(M_K) = \mathrm{Tr}(f_n(M_F)) = \mathrm{Tr}(f(\mathrm{Tr}(M_F))) \\ &= \mathrm{Tr}(f(\mathrm{Tr}_{V/F}(\phi))) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{V/F}(\phi)).\end{aligned}$$

Mit der Transitivität der Determinante gilt analog

$$\begin{aligned}\mathrm{N}_{V/K}(\phi) &= \det(M_K) = \det(f_n(M_F)) = \det(f(\det(M_F))) \\ &= \det(f(\mathrm{N}_{V/F}(\phi))) = \mathrm{N}_{F/K}(\mathrm{N}_{V/F}(\phi)),\end{aligned}$$

und abschließend

$$\begin{aligned}\chi_{\phi,V/K} &= \det(tI_{nm} - M_K) = \det(f_n(tI_n - M_F)) = \det(f(\det(tI_n - M_F))) \\ &= \det(f(\chi_{\phi,V/F})) = \mathrm{N}_{F(t)/K(t)}(\chi_{\phi,V/F}).\end{aligned}$$

□

Man kann auch noch das Verhalten von charakteristischen Polynomen, Spuren und Normen auf Tensorprodukten $V_1 \otimes_K V_2$ und bei Konstantenerweiterung $V \otimes_K F$ (die umgekehrte Richtung von Satz 1.91) untersuchen. Wir benötigen dies hier aber nicht.

Durch Anwendung beziehungsweise Spezialisierung der obigen Aussagen auf den Körpererweiterungsfall erhalten wir den folgenden Satz.

1.92 Satz. *Sei E/K eine endliche Körpererweiterung und F ein Zwischenkörper von E/K.*

(i) *Für $a, b \in E$ und $\lambda \in K$ gilt $\mathrm{Tr}_{E/K}(a+b) = \mathrm{Tr}_{E/K}(a) + \mathrm{Tr}_{E/K}(b)$, $\mathrm{Tr}_{E/K}(\lambda a) = \lambda \mathrm{Tr}_{E/K}(a)$ und $\mathrm{N}_{E/K}(ab) = \mathrm{N}_{E/K}(a)\mathrm{N}_{E/K}(b)$.*

(*ii*) *Für* $a \in F$ *gilt* $\mathrm{Tr}_{E/K}(a) = [E:F]\,\mathrm{Tr}_{F/K}(a)$, $\mathrm{N}_{E/K}(a) = \mathrm{N}_{F/K}(a)^{[E:F]}$ *und* $\chi_{a,E/K} = \chi_{a,F/K}{}^{[E:F]}$. *Außerdem ist* $\deg(\chi_{a,E/K}(a)) = [E:K]$, $\chi_{a,E/K}(a) = 0$ *und* $\chi_{a,K(a)/K} = m_{a,K}$.

(*iii*) *Für* $a \in E$ *ist* $\mathrm{Tr}_{E/K}(a) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(a))$, $\mathrm{N}_{E/K}(a) = \mathrm{N}_{F/K}(\mathrm{N}_{E/F}(a))$ *und* $\chi_{a,E/K} = \mathrm{N}_{F(t)/K(t)}(\chi_{a,E/F})$.

Beweis. (*i*): Ist klar. (*ii*): Es gilt $E \cong F^{[E:F]}$ als F-Vektorräume. Damit gilt auch $E \cong F^{[E:F]}$ als K-Vektorräume und die Multiplikation mit a bildet die zu den F unter der Isomorphie gehörigen direkten Summanden von E auf sich selbst ab. Aus der obenstehenden Bemerkung über direkte Summen folgt $\chi_{a,E/K} = \chi_{a,F/K}{}^{[E:F]}$. Die Aussage über die Spuren und Normen ergibt sich aus dieser Aussage über die charakteristischen Polynome. Per Definition gilt $\deg(\chi_{a,E/K}(a)) = [E:K]$. Wegen $\chi_{a,E/K}(\phi_a) = 0$ nach dem Satz von Cayley-Hamilton ist die Multiplikation mit $\chi_{a,E/K}(a)$ die Nullabbildung und daher gilt $\chi_{a,E/K}(a) = 0$. Gradvergleich zeigt dann $\chi_{a,K(a)/K} = m_{a,K}$, da beide Polynome normiert sind. (*iii*): Folgt direkt aus Satz 1.91. □

Für $a \in K$ gilt also insbesondere $\mathrm{Tr}_{E/K}(a) = [E:K]a$, $\mathrm{N}_{E/K}(a) = a^{[E:K]}$ und $\chi_{a,E/K} = (t-a)^{[E:K]}$.

Wir bringen nun Körperhomomorphismen ins Spiel. Dies liefert eine alternative Definitionsmöglichkeit für Spur, Norm und charakteristisches Polynom. Der Beweis von Satz 1.92, (*iii*) kann dann auch nur unter Verwendung von Körperhomomorphismen geführt werden (siehe Lemma 2.39).

1.93 Satz. *Sei* E/K *eine endliche Körpererweiterung,* C *ein algebraischer Abschluß von* K *und sei* $G = \mathrm{Hom}_K(E,C)$. *Für* $a \in E$ *gilt dann*

(*i*) $\mathrm{Tr}_{E/K}(a) = [E:K]_i \sum_{\sigma\in G} \sigma(a)$,

(*ii*) $\mathrm{N}_{E/K}(a) = \left(\prod_{\sigma\in G} \sigma(a)\right)^{[E:K]_i}$,

(*iii*) $\chi_{a,E/K} = \left(\prod_{\sigma\in G}(t-\sigma(a))\right)^{[E:K]_i}$.

Ist $[E:K]_i > 1$, *so gilt also* $\mathrm{Tr}_{E/K}(a) = 0$ *für alle* $a \in E$.

Beweis. Es ist klar, daß (*i*) und (*ii*) aus (*iii*) folgen. Außerdem gilt $p = \mathrm{char}(K) > 0$ und $[E:K]_i \equiv 0 \bmod p$, wenn $[E:K]_i > 1$ ist. Daher folgt $\mathrm{Tr}_{E/K}(a) = 0$ für alle $a \in E$ aus (*i*).

Zum Beweis von (*iii*): Sei F der separable Abschluß von K in E, so daß $[E:F] = [E:K]_i$ ist. Dann ist a^q mit $q = [K(a):K]_i$ nach Lemma 1.62 (oder auch Korollar 1.73) separabel über K und es gilt $m_{a^q,K} = \prod_{\tau\in\mathrm{Hom}_K(K(a^q),C)}(t-\tau(a^q))$, da $m_{a^q,K}$ separabel ist und es für jedes $b \in C$ mit $m_{a^q,K}(b) = 0$ ein $\tau \in$

$\mathrm{Hom}_K(K(a^q),C)$ mit $\tau(a^q)=b$ nach Lemma 1.34 gibt (siehe auch Lemma 1.53). Nach der Zerlegung am Anfang von Abschnitt 1.6 folgt $m_{a,K}=m_{a^q,K}(t^q)$. Wegen $\deg(m_{a^q,K})=[K(a):K]_s$ ist $K(a^q)$ der separable Abschluß von K in $K(a)$ und $K(a)/K(a^q)$ rein inseparabel (vergleiche auch Korollar 1.73). Da jedes $\tau\in\mathrm{Hom}_K(K(a^q),C)$ somit nach Satz 1.63, (iii) genau eine Fortsetzung $\sigma\in\mathrm{Hom}_\tau(K(a),C)$ besitzt, ergibt sich also zusammengenommen die allgemeine Gleichung

$$\begin{aligned} m_{a,K} &= m_{a^q,K}(t^q) \\ &= \textstyle\prod_{\tau\in\mathrm{Hom}_K(K(a^q),C)}(t^q-\tau(a^q)) \\ &= \textstyle\prod_{\sigma\in\mathrm{Hom}_K(K(a),C)}(t^q-\sigma(a^q)) \\ &= \textstyle\prod_{\sigma\in\mathrm{Hom}_K(K(a),C)}(t-\sigma(a))^{[K(a):K]_i}. \end{aligned}$$

Für das charakteristische Polynom gilt $\chi_{a,E/K}={m_{a,K}}^{[E:K(a)]}$ nach Satz 1.92, (ii), und weiter

$$\begin{aligned} \chi_{a,E/K} &= {m_{a,K}}^{[E:K(a)]} \\ &= \textstyle\prod_{\tau\in\mathrm{Hom}_K(K(a),C)}(t-\tau(a))^{[E:K(a)][K(a):K]_i} \\ &= \textstyle\prod_{\tau\in\mathrm{Hom}_K(K(a),C)}(t-\tau(a))^{[E:K(a)]_s[E:K]_i} \\ &= \textstyle\prod_{\sigma\in\mathrm{Hom}_K(E,C)}(t-\sigma(a))^{[E:K]_i}. \end{aligned}$$

Die letzte Gleichung ist gültig, da jedes $\tau\in\mathrm{Hom}_K(K(a),C)$ zu genau $[E:K(a)]_s$ vielen $\sigma\in\mathrm{Hom}_\tau(E,C)$ nach der Bemerkung vor Lemma 1.51 fortgesetzt werden kann. □

Für beliebiges $\tau\in G$ gelten außerdem die Gleichungen $\mathrm{Tr}_{\tau E/\tau K}(\tau(a))=\tau(\mathrm{Tr}_{E/K}(a))$, $\mathrm{N}_{\tau E/\tau K}(\tau(a))=\tau(\mathrm{N}_{E/K}(a))$ und $\chi_{\tau(a),\tau E/\tau K}=\tau(\chi_{a,E/K})$.

Kapitel 2

Galoistheorie

Die Galoistheorie liefert eine „funktorielle“ Beziehung von Zwischenkörpern normaler und separabler Erweiterungen zu Untergruppen von Automorphismengruppen, mittels derer Untersuchungen in Körpern auf Untersuchungen von Gruppen und Automorphismen zurückgeführt werden können. Die Anwendungen erstrecken sich von der Auflösung von Gleichungen durch Radikale bis zu Fragestellungen in der Geometrie.

2.1 Galoiserweiterungen

Sei E/K eine Körpererweiterung und F ein beliebiger Zwischenkörper. Die Zuordnung

$$\mathcal{G}_{E/K} : F \mapsto \mathrm{Aut}_F(E)$$

liefert eine Abbildung der Menge der Zwischenkörper von E/K in die Menge der Untergruppen von $\mathrm{Aut}_K(E)$. Sind F_1 und F_2 zwei Zwischenkörper von E/K mit $F_1 \supseteq F_2$, so gilt $\mathcal{G}_{E/K}(F_1) \subseteq \mathcal{G}_{E/K}(F_2)$.

2.1 Definition. Sei E ein Körper, C ein Erweiterungskörper von E und $G \subseteq \mathrm{Hom}(E, C)$ eine Menge von Homomorphismen. Der Fixkörper E^G von G in E wird als $E^G = \{x \in E \,|\, \sigma(x) = x \text{ für } \sigma \in G\}$ definiert.

Es ist leicht zu sehen, daß E^G ein Teilkörper von E ist. Für eine Untergruppe G von $\mathrm{Aut}_K(E)$ liefert die Zuordnung

$$\mathcal{F}_{E/K} : G \mapsto E^G$$

eine Abbildung der Menge der Untergruppen von $\mathrm{Aut}_K(E)$ in die Menge der Zwischenkörper von E/K. Sind G_1 und G_2 Untergruppen von $\mathrm{Aut}_K(E)$ mit $G_1 \subseteq G_2$, so gilt $\mathcal{F}_{E/K}(G_1) \supseteq \mathcal{F}_{E/K}(G_2)$.

Führen wir $\mathcal{F}_{E/K}$ und $\mathcal{G}_{E/K}$ hintereinander aus, ergibt sich $\mathcal{F}_{E/K}(\mathcal{G}_{E/K}(F)) \supseteq F$ und $G \subseteq \mathcal{G}_{E/K}(\mathcal{F}_{E/K}(G))$. Wir untersuchen als nächstes die Eigenschaften von $\mathcal{G}_{E/K}$ und $\mathcal{F}_{E/K}$ bezüglich Injektivität und Surjektivität.

2.2 Definition. Eine algebraische Körpererweiterung E/K heißt eine Galoiserweiterung oder galoissch und E galoissch über K, wenn E/K normal und separabel ist. Die Automorphismengruppe $\mathrm{Aut}_K(E)$ wird dann Galoisgruppe von E/K genannt und mit $G(E/K)$ oder $G_{E/K}$ bezeichnet.

2.3 Satz. *Sei E/K eine Galoiserweiterung. Für den Fixkörper von $G = G(E/K)$ gilt dann $K = E^G$. Für jeden Zwischenkörper F von E/K ist E/F galoissch.*

Beweis. Sei C ein algebraischer Abschluß von E und $a \in E^G$ beliebig. Für jedes $\sigma \in \mathrm{Hom}_K(K(a), C)$ gibt es nach Satz 1.37 eine Fortsetzung $\tau \in \mathrm{Hom}_\sigma(E, C)$. Da E normal über K ist, folgt $\tau(E) = E$ nach Satz 1.42 und somit $\tau \in G(E/K)$. Wegen $a \in E^G$ gilt $\tau(a) = a$, daher auch $\sigma(a) = a$ und es folgt $[K(a) : K]_s = 1$, da σ beliebig war. Weil a mit E separabel über K ist, ergibt sich $[K(a) : K]_s = [K(a) : K] = 1$ nach Satz 1.54 und weiter $a \in K$. Daher gilt $K = E^G$, weil a beliebig war.

Sei F ein Zwischenkörper von E/K. Die Erweiterung E/F ist normal nach Satz 1.44 und separabel nach Satz 1.55, weil E/K normal und separabel ist. Also ist E/F galoissch. □

2.4 Satz. *Sei E/K eine Galoiserweiterung. Für alle Zwischenkörper F von E/K gilt $\mathcal{F}_{E/K}(\mathcal{G}_{E/K}(F)) = F$. Daher ist $\mathcal{G}_{E/K}$ injektiv und $\mathcal{F}_{E/K}$ surjektiv.*

Beweis. Nach Satz 2.3 ist E/F galoissch und es gilt $F = E^H$ mit $H = G(E/F)$. In anderen Worten $F = \mathcal{F}_{E/K}(H)$ und $H = \mathcal{G}_{E/K}(F)$. □

2.5 Definition. Sei E/K eine Galoiserweiterung. Der Abschluß einer Untergruppe $G \subseteq G(E/K)$ wird als $\bar{G} = \mathcal{G}_{E/K}(\mathcal{F}_{E/K}(G))$ definiert. Ferner heißt G abgeschlossen, wenn $\bar{G} = G$ gilt.

Für den Abschluß gilt $\bar{G} \supseteq G$ und $\bar{\bar{G}} = \bar{G}$. Letzteres ergibt sich aus $\bar{\bar{G}} = \mathcal{G}(\mathcal{F}(\mathcal{G}(\mathcal{F}(G)))) = \mathcal{G}(\mathcal{F}(G)) = \bar{G}$ mit $\mathcal{G} = \mathcal{G}_{E/K}$ und $\mathcal{F} = \mathcal{F}_{E/K}$ unter der Berücksichtigung, daß $\mathcal{F} \circ \mathcal{G}$ nach Satz 2.4 die Identität ist.

Sei E/K eine Galoiserweiterung und F ein Zwischenkörper. Sei H eine Untergruppe von $G(E/F)$. Dann ist H bezüglich E/F genau dann abgeschlossen, wenn H bezüglich E/K abgeschlossen ist. Daher brauchen wir bei „abgeschlossen“ nicht speziell die Körpererweiterung oder Galoisgruppe anzugeben.

2.6 Satz (Hauptsatz der Galoistheorie – Teil 1)**.** *Sei E/K eine Galoiserweiterung. Dann werden durch $\mathcal{G}_{E/K}$ und $\mathcal{F}_{E/K}$ zueinander inverse, inklusionsumkehrende Bijektionen der Menge der Zwischenkörper von E/K und der Menge der abgeschlossenen Untergruppen von $G(E/K)$ definiert.*

Beweis. Das Bild von $\mathcal{G}_{E/K}$ besteht genau aus den abgeschlossenen Untergruppen von $G(E/K)$: Denn mit $\mathcal{G} = \mathcal{G}_{E/K}$, $\mathcal{F} = \mathcal{F}_{E/K}$ und $G = \mathcal{G}(F)$ folgt $\bar{G} = \mathcal{G}(\mathcal{F}(G)) = \mathcal{G}(\mathcal{F}(\mathcal{G}(F))) = \mathcal{G}(F) = G$ wegen $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$, also ist G abgeschlossen. Ist umgekehrt G abgeschlossen, so gilt $G = \mathcal{G}(\mathcal{F}(G))$, also ist G im Bild von $\mathcal{G}$.

Wegen $\mathcal{F}(\mathcal{G}(F) = F$ für alle Zwischenkörper F von E/K und $\mathcal{G}(\mathcal{F}(G)) = G$ für alle abgeschlossenen Untergruppen G sind also $\mathcal{G}$ und $\mathcal{F}$ zueinander inverse Bijektionen, die nach den eingangs gemachten Bemerkungen auch inklusionsumkehrend sind. □

Die Definition von „abgeschlossen“ wurde hier im wesentlichen nur deshalb eingeführt, um bei $\mathcal{F}$ und $\mathcal{G}$ von zueinander inversen Bijektionen sprechen zu können. Die Konstruktion kann abstrakt für beliebige Abbildungen $g : M \to N$ und $f : N \to M$ mit $f \circ g = \mathrm{id}$ durchgefürt werden.

Wir sind jetzt an einer näheren Beschreibung der abgeschlossenen Untergruppen für endliche Galoiserweiterungen E/K interessiert.

2.7 Satz. *Sei E ein Körper, $G \subseteq \mathrm{Aut}(E)$ eine Automorphismengruppe. Ist G endlich, so ist E/E^G galoissch mit $G = G(E/E^G)$ und $[E : E^G] = \#G$. Ist G beliebig und E/E^G algebraisch, so ist E/E^G galoissch mit $G \subseteq G(E/E^G)$ und $[E : E^G] = \#G$.*

Beweis. Wir schreiben $K = E^G$ und $n = \#G$. Sei G endlich oder E/K algebraisch. Sei $a \in E$ beliebig. Die Menge $S = \{\sigma(a) \mid \sigma \in G\}$ ist dann endlich, da G endlich ist oder weil S eine Teilmenge der Nullstellen von $m_{a,K}$ ist. Jedes $\tau \in G$ induziert eine injektive Abbildung $S \to S$, die wegen $\#S < \infty$ auch surjektiv ist. Also gilt $\tau(S) = S$ und das Polynom $f = \prod_{b \in S}(t - b)$ erfüllt $f^\tau = f$. Da dies für alle $\tau \in G$ gilt, ergibt sich $f \in K[t]$. Nun ist $f(a) = 0$, f separabel und alle Nullstellen von f liegen in E. Da $a \in E$ beliebig war, folgt, daß E separabel und Zerfällungskörper aller solcher f über K, also normal und folglich galoissch ist.

Für $n = \infty$ ist die Aussage $[E : K] \leq n$ richtig. Für $n < \infty$ und $a \in E$ beliebig gilt $[K(a) : K] \leq n$, da a nach obiger Schlußweise eine Nullstelle eines $f \in K[t]$ mit $\deg(f) \leq n$ ist. Wegen der Separabilität von E/K und Satz 1.58 gilt dann aber bereits $[E : K] \leq n$. Es ist klar, daß $G \subseteq G(E/K)$ gilt. Dann folgt $n = \#G \leq \#G(E/K) \leq [E : K] \leq n$, also $\#G = \#G(E/K) = [E : K]$. Für $n < \infty$ ergibt sich insbesondere $G = G(E/K)$. □

Die Abgeschlossenheitsaussage im folgenden Satz zeigt, daß $\mathcal{G}_{E/K}$ für eine endliche Galoiserweiterung E/K surjektiv ist, daß also $\mathcal{G}_{E/K}$ und $\mathcal{F}_{E/K}$ in diesem Fall zueinander inverse Bijektionen der Menge aller Zwischenkörper von E/K und der Menge aller Untergruppen von $G(E/K)$ sind.

2.8 Satz (Hauptsatz der Galoistheorie – Teil 2)**.** *Sei E/K eine Galoiserweiterung.*

(*i*) *Ist E/K endlich, so sind alle Untergruppen von $G(E/K)$ abgeschlossen.*

(*ii*) *Sind $F_1 \subseteq F_2$ Zwischenkörper von E/K, so gilt $(\mathcal{G}_{E/K}(F_1) : \mathcal{G}_{E/K}(F_2)) = [F_2 : F_1]$.*

Beweis. (*i*): Sei E/K endlich und $H \subseteq G(E/K)$. Dann ist H endlich und nach Satz 2.7 gilt $H = G(E/E^H) = \mathcal{G}_{E/K}(E^H) = \mathcal{G}_{E/K}(\mathcal{F}_{E/K}(H))$.

(*ii*): Es gelten die Gleichungen $\mathcal{G}_{E/F_1}(F_1) = \mathcal{G}_{E/K}(F_1)$, $\mathcal{G}_{E/F_1}(F_2) = \mathcal{G}_{E/K}(F_2)$ und folglich $(\mathcal{G}_{E/F_1}(F_1) : \mathcal{G}_{E/F_1}(F_2)) = (\mathcal{G}_{E/K}(F_1) : \mathcal{G}_{E/K}(F_2))$. Nach Satz 2.3 ist außerdem E/F_1 galoissch. Wir können daher ohne Einschränkung von einer Galoiserweiterung E/K und einem Zwischenkörper F ausgehen und müssen $(\mathcal{G}_{E/K}(K) : \mathcal{G}_{E/K}(F)) = [F : K]$ zeigen.

Sei $G = \mathcal{G}_{E/K}(K)$ und $H = \mathcal{G}_{E/K}(F)$. Da E/K normal ist, gilt $\mathrm{Hom}_K(F, E) = \{\sigma|F \mid \sigma \in G\}$. Für $\sigma_1, \sigma_2 \in G$ gilt dabei $\sigma_1|F = \sigma_2|F$ genau dann, wenn $\sigma_1/\sigma_2 \in H$ ist. Sei R ein Nebenklassenrepräsentantensystem von H in G mit $G = \dot\bigcup_{\sigma \in R} \sigma H$. Dann folgt, daß die Abbildung $R \to \mathrm{Hom}_K(F, E)$, $\sigma \mapsto \sigma|F$ bijektiv ist und daher $\#\mathrm{Hom}_K(F, E) = \#R = (G : H)$ gilt. Da E/K normal und separabel ist, gilt $[F : K] = \#\mathrm{Hom}_K(F, E)$. Zusammen ergibt sich $[F : K] = (G : H)$, was zu zeigen war. □

Dies schließt die Diskussion der Injektivität bzw. Surjektivität der Abbildungen $\mathcal{G}_{E/K}$ und $\mathcal{F}_{E/K}$ für endliche Galoiserweiterungen E/K ab. Für unendliche Galoiserweiterungen führt man eine geeignete Topologie auf $G(E/K)$ ein, so daß die abgeschlossenen Untergruppen von $G(E/K)$ gerade mit den im Sinn von Definition 2.5 abgeschlossenen Untergruppen übereinstimmen. Außerdem wird gezeigt, daß und wie sich $G(E/K)$ aus den Galoisgruppen $G(F/K)$ zusammensetzt, wobei F die über K galoisschen (und endlichen) Zwischenkörper von E/K durchläuft. Wir gehen hierauf nicht weiter ein.

2.9 Satz. *Sei E/K eine algebraische Körpererweiterung. Dann sind äquivalent.*

(*i*) *E/K ist galoissch,*

(*ii*) *$\mathcal{G}_{E/K}$ ist injektiv,*

(*iii*) *$K = E^{\mathrm{Aut}_K(E)}$.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Wurde in Satz 2.4 bewiesen. (*ii*) $\Rightarrow$ (*iii*): In anderer Notation ist $K = \mathcal{F}_{E/K}(\mathcal{G}_{E/K}(K))$ zu zeigen. Wir kürzen $\mathcal{F} = \mathcal{F}_{E/K}$ und $\mathcal{G} = \mathcal{G}_{E/K}$ ab. Dann kann man leicht allgemein (also ohne (*ii*) vorauszusetzen) zeigen, daß $\mathcal{F} \circ \mathcal{G} \circ \mathcal{F} = \mathcal{F}$ und $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G} = \mathcal{G}$ gilt. Ist $\mathcal{G}$ nun injektiv, so können wir $\mathcal{G}$ links aus $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G} = \mathcal{G}$ kürzen und erhalten $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$, also speziell $K = \mathcal{F}(\mathcal{G}(K))$. (*iii*) $\Rightarrow$ (*i*): Die Erweiterung $E/E^{\mathrm{Aut}_K(E)} = E/K$ ist algebraisch und nach Satz 2.7 daher galoissch. □

Der Satz zeigt also die Äquivalenz zweier weiterer, gebräuchlicher Definitionen von „galoissch“ zu der hier verwendeten Definition.

Wir fahren mit der Untersuchung der Eigenschaften von $\mathcal{G}_{E/K}$ und $\mathcal{F}_{E/K}$ bezüglich Körper- und Gruppenkonstruktionen fort.

2.10 Satz. *Seien F_i Zwischenkörper der Körpererweiterung E/K und G_i Untergruppen von $\mathrm{Aut}_K(E)$. Mit $\coprod_i$ bezeichnen wir das Kompositum von Körpern in E bzw. die von Gruppen in $\mathrm{Aut}_K(E)$ erzeugte Untergruppe. Dann gilt*

(*i*) $\mathcal{G}_{E/K}(\coprod_i F_i) = \cap_i \mathcal{G}_{E/K}(F_i)$, $\mathcal{F}_{E/K}(\coprod_i G_i) = \cap_i \mathcal{F}_{E/K}(G_i)$,

(*ii*) $\mathcal{G}_{E/K}(\cap_i F_i) \supseteq \coprod_i \mathcal{G}_{E/K}(F_i)$, $\mathcal{F}_{E/K}(\cap_i G_i) \supseteq \coprod_i \mathcal{F}_{E/K}(G_i)$.

Ist E/K endlich und galoissch, so gilt in (ii) die Gleichheit.

Beweis. (*i*): Sei $F = \coprod_i F_i$. Für $\sigma \in \mathrm{Aut}_K(E)$ gilt die Äquivalenz $\sigma \in \mathrm{Aut}_F(E) \Leftrightarrow \sigma \in \mathrm{Aut}_{F_i}(E)$ für alle i. Dies bedeutet $\mathcal{G}_{E/K}(F) = \cap_i \mathcal{G}_{E/K}(F_i)$. Sei $G = \coprod_i G_i$. Für $x \in E$ gilt die Äquivalenz $x \in E^G \Leftrightarrow x \in E^{G_i}$ für alle i. Dies bedeutet $\mathcal{F}_{E/K}(G) = \cap_i \mathcal{F}_{E/K}(G_i)$.

(*ii*): Folgt aus $\mathcal{G}_{E/K}(\cap_i F_i) \supseteq \mathcal{G}_{E/K}(F_i)$ und $\mathcal{F}_{E/K}(\cap_i G_i) \supseteq \mathcal{F}_{E/K}(G_i)$ für alle i. Wir zeigen nun die Gleichheit in (*ii*) für E/K endlich und galoissch. Wir lassen die Indizes von $\mathcal{F}_{E/K}$ und $\mathcal{G}_{E/K}$ im folgenden aus. Nach Satz 2.4 ist $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$. Nach Satz 2.6 und Satz 2.8 ist $\mathcal{G} \circ \mathcal{F} = \mathrm{id}$.

Mit dem zweiten Teil von (*i*) ergibt sich $\mathcal{F}(\coprod_i \mathcal{G}(F_i)) = \cap_i \mathcal{F}(\mathcal{G}(F_i)) = \cap_i F_i$ und Anwenden von $\mathcal{G}$ liefert $\mathcal{G}(\cap_i F_i) = \mathcal{G}(\mathcal{F}(\coprod_i \mathcal{G}(F_i))) = \coprod_i \mathcal{G}(F_i)$.

Mit dem ersten Teil von (*i*) ergibt sich $\mathcal{G}(\coprod_i \mathcal{F}(G_i)) = \cap_i \mathcal{G}(\mathcal{F}(G_i)) = \cap_i G_i$ und Anwenden von $\mathcal{F}$ liefert $\mathcal{F}(\cap_i G_i) = \mathcal{F}(\mathcal{G}(\coprod_i \mathcal{F}(G_i))) = \coprod_i \mathcal{F}(G_i)$. □

Der Beweis zeigt, daß die Gleichheit in (*ii*) auch für unendliche Galoiserweiterungen gilt, wenn man im ersten Teil den Abschluß von $\coprod_i \mathcal{G}_{E/K}(F_i)$ verwendet und im zweiten Teil nur abgeschlossene G_i betrachtet.

2.2 Beziehungen zwischen Galoiserweiterungen

Wir sind nun an den Beziehungen der Galoisgruppen interessiert, die unter der Anwendung von Isomorphismen, bei Zwischenkörpersituationen, Translationen und Komposita auftreten.

2.11 Satz. *Sei E/K eine Körpererweiterung, C ein Körper und $\lambda \in \mathrm{Hom}(E, C)$ ein Isomorphismus. Die Abbildung*

$$\phi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_{\lambda K}(\lambda E),\ \sigma \mapsto \lambda \circ \sigma \circ \lambda^{-1}$$

ist ein Isomorphismus. Daher gilt $\mathrm{Aut}_{\lambda K}(\lambda E) \cong \lambda \mathrm{Aut}_K(E)\lambda^{-1}$ *und* $\mathcal{G}_{\lambda E/\lambda K}(\lambda F) \cong \lambda \mathcal{G}_{E/K}(F)\lambda^{-1}$ *unter* ϕ *für beliebige Zwischenkörper* F *von* E/K*.*

Beweis. Die Homomorphieeigenschaft von ϕ ist klar. Außerdem wird durch $\tau \mapsto \lambda^{-1} \circ \tau \circ \lambda$ ein zu ϕ inverser Homomorphismus gegeben, so daß ϕ also bijektiv ist. □

Es wird häufig der Fall betrachtet, daß $\lambda E = E$, also zum Beispiel $\lambda \in \mathrm{Aut}_K(E)$ ist. Dann gilt insbesondere $\mathcal{G}_{E/K}(\lambda F) = \lambda \mathcal{G}_{E/K}(F)\lambda^{-1}$.

2.12 Satz (Hauptsatz der Galoistheorie – Teil 3)**.** *Sei* E/K *algebraisch und* F *ein Zwischenkörper von* E/K*.*

(*i*) *Ist* F/K *normal, so liefert die Einschränkung von Automorphismen von* E *auf* F *einen Homomorphismus*

$$\phi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(F)$$

mit $\ker(\phi) = \mathrm{Aut}_F(E)$*. Ist zusätzlich* E/K *normal, so ist* ϕ *surjektiv und ergibt eine Isomorphie* $\mathrm{Aut}_K(E)/\mathrm{Aut}_F(E) \cong \mathrm{Aut}_K(F)$.

(*ii*) *Ist* E/K *galoissch und* F *ein beliebiger Zwischenkörper, so ist* E/F *galoissch und* F/K *genau dann galoissch, wenn* $\mathcal{G}_{E/K}(F)$ *normal in* $G(E/K)$ *ist.*

Beweis. (*i*): Die Einschränkung von Automorphismen liefert wegen Satz 1.42 in der Tat einen Homomorphismus $\phi : \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(F)$. Für $\sigma \in \mathrm{Aut}_K(E)$ gilt $\sigma \in \ker(\phi)$ genau dann, wenn σ auf F die Identität ist, also $\sigma \in \mathrm{Aut}_F(E)$ gilt. Daher ist $\ker(\phi) = \mathrm{Aut}_F(E)$. Ist E/K normal, so läßt sich jedes $\sigma \in \mathrm{Aut}_K(F)$ zu einem $\tau \in \mathrm{Aut}_\sigma(E)$ nach Satz 1.37, Satz 1.42 und Satz 1.40 fortsetzen.

(*ii*): Sei E/K galoissch. Daß E/F galoissch ist, wurde bereits in Satz 2.3 gezeigt. Außerdem ist F/K separabel, so daß wir nur F/K normal zu betrachten haben. Ist F/K normal, so ist $\mathcal{G}_{E/K}(F) = \mathrm{Aut}_F(E)$ als Kern von ϕ normal in $G(E/K)$. Ist umgekehrt $\mathcal{G}_{E/K}(F)$ normal in $G(E/K)$, so gilt $\mathcal{G}_{E/K}(F) = \sigma\mathcal{G}_{E/K}(F)\sigma^{-1} = \mathcal{G}_{\sigma E/\sigma K}(\sigma F) = \mathcal{G}_{E/K}(\sigma F)$ für alle $\sigma \in G(E/K)$ nach Satz 2.11. Die Injektivität von $\mathcal{G}_{E/K}$ ergibt $F = \sigma F$ für alle $\sigma \in G(E/K)$, also ist F/K nach Satz 1.42 normal. □

Für E/K und F/K normal sagt man auch, daß die durch die Inklusion und die Einschränkung ϕ gegebene Sequenz

$$1 \to \mathrm{Aut}_F(E) \to \mathrm{Aut}_K(E) \to \mathrm{Aut}_K(F) \to 1$$

exakt ist. Links und rechts außen stehen die nur aus dem Einselement bestehenden Gruppen. Exakt bedeutet, daß für jede Gruppe zwischen den Abbildungspfeilen der Kern der rechten Abbildung gleich dem Bild der linken Abbildung ist.

Dies ist äquivalent zur Isomorphieaussage $\mathrm{Aut}_K(F) \cong \mathrm{Aut}_K(E)/\mathrm{Aut}_F(E)$ von Satz 2.12, (*ii*).

Bevor wir uns Translationen und Komposita zuwenden, benötigen wir einen auch anderweitig nützlichen Einschub über linear disjunkte Körper.

2.13 Satz. *Seien C/K eine Körpererweiterung und E und L Zwischenkörper von C/K, so daß E/K galoissch ist und $E \cap L = K$ gilt. Dann sind E und L linear disjunkt über K.*

Beweis. Wir zeigen, daß aus E/K galoissch und E/K und L/K nicht linear disjunkt folgt, daß $E \cap L \neq K$ ist. Seien $a_1, \ldots, a_n$ endlich viele, über K linear unabhängige Elemente von E, welche über L linear abhängig sind. Da E/K separabel ist, gibt es ein $a \in E$ mit $K(a_1, \ldots, a_n) = K(a)$, und die Potenzen von a bilden eine K-Basis von $K(a)$. Nun ist $K(a)/K$ nicht linear disjunkt zu L/K, folglich ist $m_{a,L}$ ein echter Teiler von $m_{a,K}$ eines kleineren Grads. Es gibt daher Koeffizienten von $m_{a,L}$, welche in L, aber nicht in K liegen. Da E/K normal ist, liegen alle Nullstellen von $m_{a,K}$ und somit auch die von $m_{a,L}$ in E. Daher sind die Koeffizienten von $m_{a,L}$ als algebraische Ausdrücke in den Nullstellen auch Elemente von E. Zusammengenommen ergibt dies $E \cap L \neq K$. □

2.14 Satz. *Seien C/K eine Körpererweiterung und E und L über K linear disjunkte Zwischenkörper von C/K. Für jedes $\sigma \in \mathrm{Hom}_K(E, C)$ gibt es dann genau eine Fortsetzung $\tau \in \mathrm{Hom}_L(EL, C)$.*

Beweis. Seien die a_i eine K-Basis von E. Da E und L über K linear disjunkt sind, sind die a_i auch eine L-Basis von EL. Sei $\sigma \in \mathrm{Hom}_K(E, C)$. Für eine Fortsetzung $\tau \in \mathrm{Hom}_L(EL, C)$ von σ muß dann $\tau(\sum_i \lambda_i a_i) = \sum_i \lambda_i \sigma(a_i)$ mit $\lambda_i \in L$ gelten. Daher kann es höchstens eine Fortsetzung geben.

Um die Existenz nachzuweisen, nehmen wir dies nun als Definition von τ. Da die Darstellung $\sum_i \lambda_i a_i$ eindeutig ist, ist τ zunächst wohldefiniert und L-linear. Seien $a, b \in EL$ mit $a = \sum_i \lambda_i a_i$ und $b = \sum_j \mu_j a_j$. Dann gilt

$$\begin{aligned}
\tau(ab) &= \tau\Big(\sum_{i,j} \lambda_i \mu_j a_i a_j\Big) = \sum_{i,j} \lambda_i \mu_j \sigma(a_i a_j) \\
&= \sum_{i,j} \lambda_i \mu_j \sigma(a_i)\sigma(a_j) = \Big(\sum_i \lambda_i \sigma(a_i)\Big)\Big(\sum_j \mu_j \sigma(a_j)\Big) \\
&= \tau(a)\tau(b).
\end{aligned}$$

Damit ist τ auch multiplikativ. □

2.15 Satz. *Seien C/K eine Körpererweiterung und E und L Zwischenkörper von C/K, so daß E/K galoissch ist. Dann ist EL/L galoissch und die Einschränkung von Automorphismen von EL auf E ergibt einen Monomorphimus*

$$\phi : G(EL/L) \to G(E/K)$$

mit $\phi(G(EL/L)) = G(E/E \cap L)$.

Beweis. Es ist klar, daß $E/E \cap L$ galoissch ist. Nach Satz 1.44 und Satz 1.55 ist auch EL/L galoissch. Wir bekommen dann offensichtlich einen Monomorphismus $\phi : G(EL/L) \to G(E/K)$ mit $\phi(G(EL/L)) \subseteq G(E/E \cap L)$. Nun sind $E/E \cap L$ und $L/E \cap L$ nach Satz 2.13 linear disjunkt. Nach Satz 2.14 setzt sich daher jedes $\sigma \in G(E/E \cap L)$ zu einem $\tau \in G(EL/L)$ fort. Dies ergibt $\phi(G(EL/L)) = G(E/E \cap L)$. □

2.16 Satz. *Seien F_i über K galoissche Zwischenkörper von C/K. Dann ist $E = \prod_i F_i$ galoissch über K und das Produkt der Einschränkungen von Automorphismen von E auf die F_i liefert einen Monomorphismus*

$$\psi : G(E/K) \to \prod_i G(F_i/K).$$

Für $F_1 \cap F_2 = K$ liefert ψ die Isomorphie

$$G(F_1F_2/K) \cong G(F_1/K) \times G(F_2/K).$$

Beweis. Die Erweiterung E/K ist nach Satz 1.44 und Satz 1.55 galoissch. Außerdem ist klar, daß $\psi : G(E/K) \to \prod_i G(E_i/K)$ ein Monomorphismus ist. Gilt $F_1 \cap F_2 = K$, so gibt es für $\sigma_i \in G(F_i/K)$ nach Satz 2.15 ein $\tau_i \in G(E/F_j)$ mit $j \neq i$, so daß τ_i auf F_i mit σ_i übereinstimmt. Da τ_i die Identität auf F_j ist, gilt $\psi(\tau_1\tau_2) = (\sigma_1, \sigma_2)$ und die Isomorphieaussage folgt. □

Im allgemeinen liefert die Einschränkung wirklich nur einen Monomorphismus. Dies liegt daran, daß vorgegebene $\sigma_i \in G(F_i/K)$ nicht unbedingt zueinander passen müssen und es daher nicht notwendigerweise eine gemeinsame Fortsetzung $\sigma \in G(E/K)$ gibt. Zum Beispiel sind für die Kompatibilität der σ_i neben den Schnitten $F_i \cap F_j$ auch Überschneidungen von F_iF_j mit F_k etc. und das Verhalten von σ_i, σ_j und σ_k darauf zu berücksichtigen.

2.17 Beispiel. Konkret betrachte man $K = \mathbb{Q}$, $F_1 = \mathbb{Q}(\sqrt{2})$, $F_2 = \mathbb{Q}(\sqrt{3})$ und $F_1F_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Es gilt $G(F_1/\mathbb{Q}) \cong G(F_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ und nach dem Satz folgt $G(F_1F_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gibt es aber drei Untergruppen der Ordnung 2, und entsprechend ist $\mathbb{Q}(\sqrt{6})$ der dritte quadratische Teilkörper von

$F_1F_2/\mathbb{Q}$. Jedes $\sigma \in G(F_1F_2/\mathbb{Q})$ wird nach dem Satz durch seine Einschränkungen $\sigma_1 = \sigma|F_1$ und $\sigma_2 = \sigma|F_2$ eindeutig bestimmt. Daher ist $\sigma_3 = \sigma|F_3$ durch σ_1 und σ_2 bereits eindeutig bestimmt. Wir können also σ_3 bei gegebenem σ_1 und σ_2 nicht beliebig vorgeben, wenn es ein σ geben soll, so daß die σ_i als Einschränkungen von σ erhalten werden. Entsprechend ist ψ im allgemeinen nicht surjektiv.

Sind allerdings die F_i/K alle in E/K enthaltenen endlichen Galoiserweiterungen und stimmen σ_i und σ_j auf $F_i \cap F_j$ für alle i, j überein, so gibt es eine gemeinsame Fortsetzung $\sigma \in G(E/K)$. Man definiert einfach $\sigma(a) = \sigma_i(a)$, wobei i so gewählt ist, daß $a \in F_i$ gilt.

2.3 Galoisgruppen spezieller Körpererweiterungen

Wir betrachten zunächst die Galoisgruppen einiger spezieller, häufig auftretender Körpererweiterungen.

2.18 Definition. Eine Galoiserweiterung E/K heißt abelsch bzw. zyklisch, wenn $G(E/K)$ abelsch bzw. zyklisch ist.

2.19 Satz. *Sei E/K abelsch (zyklisch) und F ein Zwischenkörper. Dann sind E/F und F/K abelsch (zyklisch). Ist C ein Erweiterungskörper von E und L ein Zwischenkörper von C/K, so ist EL/L abelsch (zyklisch). Für Zwischenkörper F_i von C/K mit F_i/K abelsch ist $\coprod_i F_i/K$ abelsch.*

Beweis. Folgt direkt durch die Betrachtung der Homomorphismen in Satz 2.12, Satz 2.15 und Satz 2.16. Ferner sind Untergruppen und Faktorgruppen abelscher bzw. zyklischer Gruppen wieder abelsch bzw. zyklisch. □

2.20 Definition. Die absolute Galoisgruppe $G(K)$ eines Körpers K ist definiert als $G(K^s/K)$, wo K^s ein separabler Abschluß von K ist. Der abelsche Abschluß K^{ab} von K ist das Kompositum aller abelscher Erweiterungen von K in K^s.

Man nennt K^{ab} auch maximale abelsche Erweiterung von K, da jeder abelsche Erweiterungskörper von K in K^{ab} eingebettet werden kann. Nach Satz 2.19 ist $G(K^{ab}/K)$ abelsch.

2.21 Satz. *Sei E/K eine Erweiterung von endlichen Körpern. Dann ist E/K galoissch mit zyklischer Galoisgruppe $G(E/K)$. Für $q = \#K$ wird $G(E/K)$ vom Frobeniusautomorphismus $x \mapsto x^q$ erzeugt.*

Beweis. Übung. □

2.22 Satz. *Sei* char$(K) = 0$ *oder* n *koprim zu* char(K)*, und sei* $\zeta \in \mu_n$ *eine primitive* n*-te Einheitswurzel. Dann wird durch*

$$\phi : G(K(\mu_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times,\ \sigma \mapsto \phi(\sigma) \text{ mit } \sigma(\zeta) = \zeta^{\phi(\sigma)}$$

ein Monomorphismus definiert. Für $K = \mathbb{Q}$ *ist* ϕ *auch surjektiv.*

Beweis. Übung. □

Man kann Satz 2.22 auch auf Erweiterungen von endlichen Körpern wie in Satz 2.21 anwenden, denn mit $n = [E : K]$ gilt $E = K(\mu_{q^n-1})$. Ist $\zeta \in \mu_{q^n-1}$ eine primitive $(q^n - 1)$-te Einheitswurzel, so hat ζ genau n verschiedene Konjugierte ζ^{q^j} über K und das Bild von ϕ aus Satz 2.22 ist die von q in $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^\times$ erzeugte, n-elementige Untergruppe.

2.23 Satz. *Sei* char$(K) = 0$ *oder* n *koprim zu* char(K)*, und sei* $\zeta \in \mu_n \subseteq K$ *eine primitive* n*-te Einheitswurzel. Sei* $f = t^n - a \in K[t]$ *irreduzibel. Der Zerfällungskörper* E *von* f *über* K *ist galoissch über* K *und es gilt* $E = K(b)$ *mit* $f(b) = 0$*. Durch*

$$\phi : G(E/K) \to \mathbb{Z}/n\mathbb{Z},\ \sigma \mapsto \phi(\sigma) \text{ mit } \sigma(b) = \zeta^{\phi(\sigma)}b$$

wird ein Isomorphismus definiert. Die Erweiterung E/K *ist also zyklisch von der Ordnung* n*.*

Beweis. Übung. □

2.24 Satz. *Sei* char$(K) = p > 0$ *und* $f = t^p - t - a \in K[t]$ *irreduzibel. Der Zerfällungskörper* E *von* f *über* K *ist galoissch über* K *und es gilt* $E = K(b)$ *mit* $f(b) = 0$*. Durch*

$$\phi : G(E/K) \to \mathbb{Z}/p\mathbb{Z},\ \sigma \mapsto \phi(\sigma) \text{ mit } \sigma(b) = b + \phi(\sigma)$$

wird ein Isomorphismus definiert. Die Erweiterung E/K *ist also zyklisch von der Ordnung* p*.*

Beweis. Übung. □

Die Erweiterungen E/K aus Satz 2.23 bzw. Satz 2.24 heißen einfache Kummererweiterungen bzw. einfache Artin-Schreier-Erweiterungen. Sie spielen bei weitergehenden Körperkonstruktionen als einfachste Bausteine eine wichtige Rolle. Kummererweiterungen sind ihrer Natur nach multiplikativ, während Artin-Schreier-Erweiterungen einen additiven Charakter aufweisen. Abgesehen davon sind sie sich aber recht ähnlich.

2.4 Permutationsdarstellungen und Galoisgruppen von Polynomen

Sei K ein Körper, $f \in K[t]$ ein nicht-konstantes, separables Polynom und E ein Zerfällungskörper E von f über K. Dann ist E/K galoisch. Für die Galoisgruppe von E/K erhalten wir eine Permutationsdarstellung $\phi : G(E/K) \to S_n$ wie folgt. Seien $a_1, \dots, a_n \in E$ die paarweise verschiedenen Nullstellen von f, wobei $n = \deg(f)$ ist. Für $\sigma \in G(E/K)$ gilt $f^\sigma = f$, daher bewirkt σ eine Permutation der Nullstellen $a_1, \dots, a_n$. Bezeichnet S_n die symmetrische Gruppe (die Gruppe der Permutationen auf den Ziffern $1, \dots, n$), so gibt es also ein $\phi(\sigma) \in S_n$ mit $\sigma(a_i) = a_{\phi(\sigma)(i)}$. Für die Definition von $\phi(\sigma)$ verwenden wir somit eine festgewählte Anordnung der Nullstellen a_i.

2.25 Satz. *Die Abbildung $\phi : G(E/K) \to S_n$, $\sigma \mapsto \phi(\sigma)$ ist ein Monomorphismus und ϕ bzw. $\phi(G(E/K))$ sind ohne Angabe einer Nullstellenanordnung nur bis auf Konjugation in S_n eindeutig bestimmt. Die Permutationsgruppe $\phi(G(E/K))$ ist genau dann transitiv, wenn f irreduzibel ist.*

Beweis. Die Homomorphieeigenschaft ist klar. Wegen $E = K(a_1, \dots, a_n)$ ist σ durch die Operation auf den a_i bereits eindeutig bestimmt, daher ist ϕ injektiv.

Sei b_i eine andere Anordnung der Nullstellen von f und ϕ_a, ϕ_b die entsprechenden Permutationsdarstellungen. Es gibt ein $\tau \in S_n$ mit $b_i = a_{\tau(i)}$. Sei $\sigma \in G(E/K)$. Dann gilt $\phi_b(\sigma)(i) = j$ genau dann, wenn $\phi_a(\sigma)(\tau(i)) = \tau(j)$. Letzteres heißt $(\tau^{-1}\phi_a(\sigma)\tau)(i) = j$, so daß wir $\phi_b(\sigma) = \tau^{-1}\phi_a(\sigma)\tau$ erhalten. Folglich gilt auch $\phi_b(G(E/K)) = \tau^{-1}\phi_a(G(E/K))\tau$.

Sei f irreduzibel und $1 \leq i, j \leq n$. Zu a_i, a_j gibt es ein $\sigma \in \mathrm{Hom}_K(K(a_i), K(a_j))$ mit $\sigma(a_i) = a_j$, und σ läßt sich auf E fortsetzen. Dann gilt $\sigma \in G(E/K)$ und $\phi(\sigma)(i) = j$. Also ist $\phi(G(E/K))$ transitiv. Ist umgekehrt $f = f_1 f_2$ mit nicht-konstanten Polynomen f_1 und f_2, so können die Nullstellen von f_1 nicht auf die Nullstellen von f_2 abgebildet werden und $\phi(G(E/K))$ ist daher nicht transitiv. □

Der Satz gibt Anlaß zu folgender Definition, die historisch vor der Definition der Galoisgruppe einer Körpererweiterung steht.

2.26 Definition. Sei K ein Körper, $f \in K[t]$ ein nicht-konstantes, separables Polynom und E ein Zerfällungskörper von f über K. Die Galoisgruppe $G(f, K)$ von f über K wird als Bild der Permutationsdarstellung von $G(E/K)$ auf einer fest gewählten Anordnung der Nullstellen von f in E definiert.

Die Galoisgruppe $G(f, K)$ eines Polynoms ist also ohne Angabe einer Nullstellenanordnung nur bis auf Konjugation in S_n mit $n = \deg(f)$ eindeutig bestimmt.

Für jede Galoiserweiterung E/K gilt $G(E/K) \cong G(m_{a,K}, K)$, wobei a ein primitives Element von E/K bezeichnet.

Die Berechnung von $G(f, K)$ kann auf die Berechnung des Zerfällungskörpers von f über K zurückgeführt werden. Seien die E_i eine aufsteigende Kette von Zwischenkörpern von E/K mit $E_{i+1} = E_i(a_i)$ und $f(a_i) = 0$ wie im Beweis von Satz 1.28. Für $\sigma_i \in \mathrm{Hom}_K(E_i, E)$ sind alle Fortsetzungen auf E_{i+1} durch $a_i \mapsto a_j$ gegeben, wobei a_j über die Nullstellen von ${m_{a_i,E_i}}^{\sigma_i}$ läuft. Man erhält daher alle Elemente von $G(f, K)$, indem man Polynome über den E_i faktorisiert und induktiv alle Fortsetzungen der Identität auf K nach E bestimmt.

Als Beispiel für dieses Vorgehen betrachten wir $f = t^3 - 2 \in \mathbb{Q}[t]$. Wir setzen $E_0 = K = \mathbb{Q}$, $a_1 = \sqrt[3]{2}$, $a_2 = \zeta\sqrt[3]{2}$ mit $\zeta = \exp(2\pi i/3) \in \mu_3$ und $E_{i+1} = E_i(a_i)$. Damit gilt $[E_1 : K] = 3$, $[E_2 : E_1] = 2$ und $E = E_2$. Die Identität auf K hat drei Fortsetzungen auf E_1, und diese drei Fortsetzungen haben jeweils zwei Fortsetzungen auf E_2. Damit besteht $G(f, K)$ aus 6 Elementen. Die Bestimmung dieser 6 Elemente ist allerdings etwas leichter, wenn wir $E = K(\zeta, \sqrt[3]{2})$ beachten. Mit Satz 2.22 bestimmen wir zunächst $G(K(\zeta)/K)$, und setzen diese Automorphismen mittels Satz 2.23 und Lemma 1.51 zu allen Automorphismen in $G(E/K)$ zusammen. Dies ergibt $G(E/K) = \{\sigma_{i,j} \mid 1 \le i \le 2, 1 \le j \le 3\}$ mit $\sigma_{i,j}$ definiert durch $\sigma_{i,j}(\zeta) = \zeta^i$, $\sigma_{i,j}(\sqrt[3]{2}) = \zeta^j\sqrt[3]{2}$.

Wir betrachten nun die allgemeinen Fälle $n = 1, 2, 3$. Für $n = 1$ ist f linear und $G(f, K) = \{(1)\}$ als Untergruppe von S_1. Für $n = 2$ hat f zwei Nullstellen a_1 und a_2. Gilt $a_i \in K$, so folgt $G(f, K) = \{(1)\}$ als Untergruppe von S_2. Ansonsten gilt $G(f, K) = \{(1), (1, 2)\} = S_2$.

Der erste nicht völlig triviale Fall ergibt sich für $n = 3$. Ist f nicht irreduzibel, so sind wir auf die Fälle $n = 1$ und $n = 2$ zurückgeführt. Wir nehmen also an, daß f irreduzibel ist. Sei E der Zerfällungskörper von f über K. Dann gilt $[E : K] = 3$ oder $[E : K] = 6$. Im ersten Fall ist $G(f, K) = A_3$ zyklisch und wird beispielsweise von $(1, 2, 3)$ erzeugt. Hier gibt es keine nicht-trivialen Zwischenkörper. Im letzteren Fall $[E : K] = 6$ gilt $G(f, K) = S_3$ wegen $\#S_3 = 6$, und $G(f, K)$ ist nicht abelsch. Die S_3 wird von $(1, 2, 3)$ und $(1, 2)$ erzeugt. Man rechnet leicht nach, daß es genau drei (zueinander konjugierte) Untergruppen der Ordnung zwei gibt, nämlich $G_1 = \langle(1, 2)\rangle$, $G_2 = \langle(1, 3)\rangle$ und $G_3 = \langle(2, 3)\rangle$, und genau eine normale Untergruppe der Ordnung drei, nämlich $H = \langle(1, 2, 3)\rangle$. Daher gibt es genau drei (zueinander konjugierte) Zwischenkörper $F_i = \mathcal{F}_{E/K}(G_i)$ von E/K mit $[F_i : K] = 3$ und einen über K galoisschen Zwischenkörper $L = \mathcal{F}_{E/K}(H)$ mit $[L : K] = 2$. Man setze diese allgemeinen Betrachtungen in Beziehung zum obigen Beispiel $f = t^3 - 2$. Wie lautet der Isomorphismus zwischen den Permutationen und den $\sigma_{i,j}$, und welchen Zwischenkörpern entsprechen die F_i und L? Ein allgemeiner Ansatz zur Konstruktion von Erzeugern von Fixkörpern von Automorphismengruppen wird übrigens durch Lemma 1.24 gegeben.

Für höhere Polynomgrade n wird die Diskussion schnell schwieriger. Mit Spezialbetrachtungen kann man aber trotzdem einiges über $G(f,K)$ herausfinden. Ein systematisches Vorgehen und der Einsatz von Computern erlauben die explizite Bestimmung von $G(f,K)$ für geeignete Grundkörper K zur Zeit bis $n = 23$. Wir nehmen dieses Thema im folgenden Abschnitt auf. Auf der anderen Seite kann man die Galoisgruppen von Klassen von speziellen Polynomen bzw. Galoiserweiterungen wie im Abschnitt 2.3 leicht explizit bestimmen.

Der folgende Satz zeigt, daß wir für eine Permutationsdarstellung einer Galoisgruppe in gewissen Fällen immer ein Polynom finden können, welches diese Permutationsdarstellung realisiert.

2.27 Satz. *Sei E/K eine Galoiserweiterung und $\phi : G(E/K) \to S_n$ ein Homomorphismus. Mit den Bezeichnungen $G = \phi(G(E/K))$ und $H_i = \mathrm{Stab}_G(i)$ gelte $N_G(H_i) = H_i$ für ein i mit $1 \le i \le n$. Ist G transitiv oder gilt $\#K \ge n$, so gibt es ein normiertes, separables Polynom $f \in K[t]$ mit den folgenden Eigenschaften.*

(i) Der Zerfällungskörper F von f über K ist in E enthalten und erfüllt $[E : F] = \#\ker(\phi)$.

(ii) Es gilt $G(f,K) = G$ für eine Nullstellenanordnung.

Beweis. Wir schicken ein paar Betrachtungen für transitive Permutationsgruppen G voraus. Da G transitiv ist, gibt es für alle i,j ein $\sigma \in G$ mit

$$H_j = \mathrm{Stab}_G(j) = \mathrm{Stab}_G(\sigma(i)) = \sigma \mathrm{Stab}_G(i)\sigma^{-1} = \sigma H_i \sigma^{-1},$$

also sind die H_i alle konjugiert. Wir wählen ein festes ν und setzen $H = H_\nu$. Desweiteren gilt dann $G \cdot \nu = \{1, \dots n\}$ und daher $(G : H) = \#(G \cdot \nu) = n$. Bezeichnet $G \cdot H$ die Bahn von H unter der Operation von G durch Konjugation, so gilt $G \cdot H = \{H_i \,|\, 1 \le i \le n\}$ und $\#(G \cdot H) = (G : N_G(H))$. Wegen $H \subseteq N_G(H)$ ergibt sich also $\#(G \cdot H) \le n$, und $\#(G \cdot H) = n$ gilt genau dann, wenn $N_G(H) = H$ ist. Für $N_G(H) = H$ seien die $\sigma_i \in G$ ein Nebenklassenrepräsentantensystem mit $G = \dot\cup\{\sigma_i H \,|\, 1 \le i \le n\}$. Dann gilt $\sigma_i H \sigma_i^{-1} = \sigma_j H \sigma_j^{-1}$ genau dann, wenn $(\sigma_j^{-1}\sigma_i)H(\sigma_j^{-1}\sigma_i)^{-1} = H$, also $\sigma_j^{-1}\sigma_i \in H$ und damit $\sigma_i = \sigma_j$ ist. Es folgt $G \cdot H = \{\sigma_i H \sigma_i^{-1} \,|\, 1 \le i \le n\}$. Die σ_i können so numeriert werden, daß $\sigma_i(\nu) = i$ gilt. Dann ergibt sich genauer $\sigma_i H \sigma_i^{-1} = H_i$ für $1 \le i \le n$.

Sei nun $F = \mathcal{F}_{E/K}(\ker(\phi))$. Dann ist F/K galoissch und $\phi|F$ erfüllt ebenfalls die Voraussetzungen des Satzes. Außerdem gilt $[E : F] = \#\ker(\phi)$, so daß wir mit den Bezeichnungen des Satzes ohne Einschränkung annehmen können, daß ϕ injektiv ist. Im folgenden identifizieren wir $G(E/K)$ mit G und verwenden die Bezeichnungen des vorigen Absatzes.

Wir behandeln zuerst den Fall, daß G transitiv ist. Dann operiert G durch Konjugation auf der n-elementigen Menge $\{H_i \mid 1 \leq i \leq n\}$. Wir setzen $F_i = \mathcal{F}_{E/K}(H_i)$ und $F = \mathcal{F}_{E/K}(H)$. Dann operiert G durch $\sigma \cdot F_i = \sigma(F_i)$ ebenfalls auf der n-elementigen Menge $\{F_i \mid 1 \leq i \leq n\}$, denn es gilt $\sigma(F_i) = \mathcal{F}_{E/K}(\sigma H_i \sigma^{-1}) = \mathcal{F}_{E/K}(H_j) = F_j$ für ein j. Sei $a \in E$ ein primitives Element von F/K und $a_i = \sigma_i(a) \in F_i$. Da die F_i paarweise verschieden sind (oder auch die σ_i ein Nebenklassenrepräsentantensystem von G/H bilden), sind die a_i paarweise verschieden. Dann operiert G durch $\sigma \cdot a_i = \sigma(a_i)$ auch auf der n-elementigen Menge $\{a_i \mid 1 \leq i \leq n\}$, denn $\sigma(a_i) = \sigma(\sigma_i(a)) = \sigma_j(a)$ für ein j wegen $a \in \mathcal{F}_{E/K}(H)$. Vermöge der Bijektionen $i \mapsto H_i$, $i \mapsto F_i$, $i \mapsto a_i$ und wegen $\sigma(F_i) = \mathcal{F}_{E/K}(\sigma H_i \sigma^{-1})$ für $\sigma \in G$ sind alle diese Operationen von G äquivalent und transitiv, da G transitiv vorausgesetzt wurde. Wir definieren $f = \prod_{i=1}^{n}(t - a_i)$. Dann ist f normiert und separabel. Weil G auf $\{a_i \mid 1 \leq i \leq n\}$ operiert, gilt $f^\sigma = f$ für alle $\sigma \in G$ und es folgt $f \in K[t]$. Wegen der Transitivität von G auf $\{a_i \mid 1 \leq i \leq n\}$ ist f irreduzibel über K. Nach Konstruktion gilt $G(f, K) = G$ mit der gewählten Nullstellenanordnung. Schließlich folgt aus $\sigma(a_i) = a_i$ auch $\sigma(i) = i$ für alle i (wir identifizieren $G(E/K)$ und G), und daraus $\sigma = \mathrm{id}$. Also gilt für den Zerfällungskörper F von f über K wie gewünscht $F = K(a_1, \ldots, a_n) = E$.

Für nicht unbedingt transitives G, aber $\#K \geq n$, seien nun $D_i = \{d_{i,j} \mid 1 \leq i \leq r, 1 \leq j \leq s_i\}$ die Bahnen von G in $\{1, \ldots, n\}$. Durch Einschränkung auf D_i erhalten wir Homomorphismen $\psi_i : G \to S(D_i)$. Sei $G_i = \psi_i(G)$. Es gilt

$$\begin{aligned}
N_{G_i}(\mathrm{Stab}_{G_i}(d_{i,j})) &= \psi_i(\psi_i^{-1}(N_{G_i}(\mathrm{Stab}_{G_i}(d_{i,j})))) \\
&= \psi_i(N_G(\psi_i^{-1}(\mathrm{Stab}_{G_i}(d_{i,j})))) \\
&= \psi_i(N_G(\mathrm{Stab}_G(d_{i,j}))) \\
&= \psi_i(\mathrm{Stab}_G(d_{i,j})) \\
&= \mathrm{Stab}_{G_i}(d_{i,j}).
\end{aligned}$$

Wir können daher den bereits bewiesenen, transitiven Fall des Satzes auf G_i anwenden. Für jedes i mit $1 \leq i \leq r$ gibt es separable und irreduzible $f_i \in K[t]$ mit $f_i = \prod_{j=1}^{s_i}(t - a_{i,j})$ und $a_{i,j} \in E$. Die Gruppe G operiert äquivalenterweise auf D_i und $\{a_{i,j} \mid 1 \leq j \leq s_i\}$. Wegen $\#K \geq n$ gibt es $c_i \in K$, so daß die Polynome $f_i(t + c_i)$ für $1 \leq i \leq r$ paarweise teilerfremd sind. Mit $f = \prod_i f_i(t + c_i)$ erhalten wir dann ein separables Polynom mit $G(f, K) = G$ bezüglich der gewählten Nullstellenanordnung. Für den Zerfällungskörper F von K gilt wieder wie gewünscht $F = K(\{a_{i,j} \mid i, j\}) = E$. □

Sei E/K galoissch, a ein primitives Element von E/K und $G = G(m_{a,K}, K)$. Dann gilt $\mathrm{Stab}_G(i) = \{\mathrm{id}\}$ und $N_G(\mathrm{Stab}_G(i)) = G$. Dieses Beispiel zeigt, daß die Bedingung des Satzes nur hinreichend für die Existenz eines Polynoms f mit $G = G(f, K)$ ist.

2.5 Symmetrische Polynome und das Umkehrproblem der Galoistheorie

Wir wollen an die Situation des vorhergehenden Abschnitts anknüpfen und für allgemeines f kurz „allgemeine" Betrachtungen anstellen. Sei k ein Körper und $E = k(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen in $x_1, \ldots, x_n$. Für $\sigma \in S_n$ definieren wir ein $\psi(\sigma) \in \mathrm{Aut}_k(E)$ durch $\psi(\sigma)(x_i) = x_{\sigma(i)}$. Dies liefert einen Monomorphismus $\psi : S_n \to \mathrm{Aut}_k(E)$, $\sigma \mapsto \psi(\sigma)$. Wir setzen $K = E^{\psi(S_n)}$. Die Elemente aus K bleiben unverändert, wenn man die x_i permutiert. Es handelt sich also dabei um genau die symmetrischen Funktionen in E. Da $\psi(S_n)$ endlich ist, ist E/K nach Satz 2.7 galoissch mit $G(E/K) = \psi(S_n)$. Aufgrund der Isomorphie $\psi(S_n) \cong S_n$ identifizieren wir $G(E/K)$ und S_n im folgenden.

Wir setzen nun $f = \prod_{i=1}^n (t - x_i) = \sum_{i=0}^n (-1)^i s_i t^{n-i}$, wobei die s_i die elementarsymmetrischen Polynome in den x_i sind. Offenbar gilt $f \in k(s_1, \ldots, s_n)[t]$, und E ist Zerfällungskörper von f über $k(s_1, \ldots, s_n)$. Wegen $[E : k(s_1, \ldots, s_n)] \leq n!$, $[E : K] = n!$ und $k(s_1, \ldots, s_n) \subseteq K$ ergibt sich $K = k(s_1, \ldots, s_n)$. Dies zeigt, daß sich jede symmetrische Funktion als rationale Funktion in den s_i erhalten läßt. Darüberhinaus gibt es zu i, j ein $\sigma \in S_n$ mit $\sigma(x_i) = x_j$. Die x_i sind damit alle konjugiert und f ist irreduzibel über K. Zusammenfassend erhalten wir folgenden Satz.

2.28 Satz. *Sei $E = k(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen in x_i und K der Teilkörper der symmetrischen Funktionen in E. Dann ist E/K galoissch mit $G(E/K) = S_n$ und es gilt $K = k(s_1, \ldots, s_n)$, wobei s_i die elementarsymmetrischen Polynome in den x_i sind. Der Körper E ist Zerfällungskörper des irreduziblen Polynoms $f = \sum_{i=0}^n (-1)^i s_i t^{n-i} \in K[t]$.*

Die folgende Aussage ist an dieser Stelle noch von grundsätzlichem Interesse.

2.29 Satz. *Die elementarsymmetrischen Polynome $s_i \in k[x_1, \ldots, x_n]$ sind algebraisch unabhängig. Daher kann $k[s_1, \ldots, s_n]$ auch als Polynomring in den Variablen s_i aufgefaßt werden. Sei K der Körper der symmetrischen Funktionen und $R = k[x_1, \ldots, x_n] \cap K$ der Ring der symmetrischen Polynome. Dann gilt $R = k[s_1, \ldots, s_n]$.*

Beweis. Wurde in Algebra 1 bewiesen. Mit Theorie, die später behandelt wird, kann man wie folgt argumentieren: Die Körpererweiterung $k(x_1, \ldots, x_n)/k$ hat

Transzendenzgrad n, und $k(x_1,\dots,x_n)/k(s_1,\dots,s_n)$ ist endlich. Daher hat auch $k(s_1,\dots,s_n)/k$ Transzendenzgrad n, und die s_i sind algebraisch unabhängig. Die Ringerweiterung $k[x_1,\dots,x_n]/k[s_1,\dots,s_n]$ ist ganz. Daher ist auch die Ringerweiterung $R/k[s_1,\dots,s_n]$ ganz. Da $k[s_1,\dots,s_n]$ wegen der algebraischen Unabhängigkeit ein Polynomring und damit faktoriell ist, ist $k[s_1,\dots,s_n]$ in seinem Quotientenkörper K ganz abgeschlossen. Es folgt $R = k[s_1,\dots,s_n]$. □

Das oben verwendete Polynom $f = \sum_{i=0}^{n}(-1)^i s_i t^{n-i} \in R[t]$ heißt aufgrund der ersten Aussage des Satzes allgemeines Polynom n-ten Grads, da f nicht nur „allgemeine“ Nullstellen, sondern auch „allgemeine“ Koeffizienten hat. Wir merken an, daß es einen konstruktiven Beweis der zweiten Aussage von Satz 2.29 gibt, der ein Verfahren angibt, mit dem man ein symmetrisches Polynom in den x_i als Polynom in den s_i darstellt.

2.30 Satz. *Sei $E = k(x_1,\dots,x_n)$, $K = k(s_1,\dots,s_n)$, G eine Untergruppe von S_n und $F = \mathcal{F}_{E/K}(G)$. Dann gilt $G(E/F) = G$ und es gibt ein $h \in k[x_1,\dots,x_n]$ mit $F = K(h)$.*

Beweis. Fordern wir statt $h \in k[x_1,\dots,x_n]$ nur $h \in k(x_1,\dots,x_n)$, so ergibt sich die Existenz von h direkt aus dem Satz vom primitiven Element. Für jedes $g \in k[x_1,\dots,x_n]$ ist $f = \mathrm{N}_{E/K}(g) = \prod_{\sigma\in S_n}\sigma(g) \in k[x_1,\dots,x_n] \cap k(s_1,\dots,s_n)$ nach Satz 2.28 (genauer $f \in k[s_1,\dots,s_n]$ nach Satz 2.29). Besitzt $h \in k(x_1,\dots,x_n)$ einen Nenner g, so können wir wegen $f \in k(s_1,\dots,s_n)$ anstelle von h daher auch $fh \in k[x_1,\dots,x_n]$ als primitives Element verwenden. □

Es gelten die Bezeichnungen von Satz 2.30 mit $k = \mathbb{Q}$. Satz 2.30 kann folgendermaßen genutzt werden, um Informationen über die Galoisgruppe eines Polynoms $f_0 \in \mathbb{Q}[t]$ zu erhalten. Wir wählen eine Anordnung der Nullstellen $a_i \in \mathbb{C}$ von f_0 und betrachten $G(f_0,\mathbb{Q})$ als Untergruppe der S_n. Aus $G(f_0,\mathbb{Q}) \le G$ muß dann $h(a_1,\dots,a_n) \in \mathbb{Q}$ folgen, weil h unter G und unter $G(f_0,\mathbb{Q})$ als Permutationsgruppe, und somit $h(a_1,\dots,a_n)$ unter $G(f_0,\mathbb{Q})$ als Gruppe von Körperautomorphismen invariant ist. Unter einer Zusatzbedingung gilt auch die Umkehrung dieser Implikation, aus $h(a_1,\dots,a_n) \in \mathbb{Q}$ folgt $h \in \mathcal{F}_{E/K}(G(f_0,\mathbb{Q}))$ und daraus $G(f_0,\mathbb{Q}) \le G$. Durch systematisches Testen von $h(a_1,\dots,a_n) \in \mathbb{Q}$ für die möglichen Kandidatengruppen G kann man so die Galoisgruppe $G(f_0,\mathbb{Q})$ genau bestimmen. Man kann dabei auch induktiv vorgehen, indem man die G absteigend durchläuft. Im i-ten Schritt wissen wir $G(f_0,\mathbb{Q}) \le G_i$, also $h_j(a_1,\dots,a_n) \in \mathbb{Q}$ für $1 \le j \le i$. Sei $G_{i+1} < G_i$ eine Kandidatengruppe, für die wir herausfinden wollen, ob $G(f_0,\mathbb{Q}) \le G_{i+1}$ gilt. Wir definieren h_{i+1} als primitives Element von $F_{i+1} = \mathcal{F}_{E/K}(G_{i+1})$ über $F_i = \mathcal{F}_{E/K}(G_i) = K(h_1,\dots,h_i)$ und testen $h_{i+1}(a_1,\dots,a_n) \in \mathbb{Q}$ (und dazu die oben erwähnte Zusatzbedingung). Für die

Berechnungen kann man Fließkommazahlen in $\mathbb{C}$ benutzen, und die Tests „$\in \mathbb{Q}$“ kann man bei geeignetem Vorgehen auch durch Tests „$\in \mathbb{Z}$“ ersetzen. Die Möglichkeit von Rundungsfehlern in den Berechnungen muß berücksichtigt werden.

Ein anderer Ansatz geht wie folgt. Für jede Kandidatengruppe G bestimmen wir $m_{h,K} \in K[t]$. Die Koeffizienten von $m_{h,K}$ sind Ausdrücke in den s_i und wir können folglich für die s_i die Koeffizienten von f_0 (unter Beachtung der Vorzeichen $(-1)^i$) substituieren. Das resultierende Polynom $m_0 \in \mathbb{Q}[t]$ muß dann mindestens eine Nullstelle in $\mathbb{Q}$ haben, welche $h(a_1, \dots, a_n)$ entsprechen würde. Hat es eine einfache Nullstelle in $\mathbb{Q}$, so folgt $G(f_0, \mathbb{Q}) \leq G$. Hier brauchen wir nur mit den Koeffizienten von f_0, nicht aber mit seinen Nullstellen zu arbeiten.

Normalerweise verwendet man für diese Strategien einen Computer, da die h und $m_{h,K}$ sehr große Ausdrücke werden können und es sehr viele Kandidaten G geben kann (301 Kandidaten für $n = 12$, 1954 Kandidaten für $n = 16$, 25000 Kandidaten für $n = 23$). In Spezialfällen ist es aber möglich, relativ einfache Formeln anzugeben.

Wir wollen als Beispiel $G = A_n$ in Charakteristik Null oder > 2 betrachten. Die folgende, allgemeine Definition ist dafür und auch anderweitig nützlich.

2.31 Definition. Sei $f \in K[t]$ mit $n = \deg(f) \geq 1$ ein Polynom mit Leitkoeffizient $c \in K$ und den Nullstellen $a_1, \dots, a_n$ in einem Zerfällungskörper von f über K. Die Diskriminante $d(f)$ von f wird dann als $d(f) = c^{2n-2} \prod_{1 \leq i < j \leq n} (a_i - a_j)^2$ definiert.

2.32 Satz. *Die Diskriminante liefert eine Abbildung der Menge der Polynome vom Grad ≥ 1 in $K[t]$ nach K.*

Beweis. Es ist unmittelbar einsichtig, daß $d(f)$ nicht von der gewählten Reihenfolge der a_i abhängt. Dies zeigt, daß $d(f)$ invariant unter $G(f, K)$ ist und folglich $d(f) \in K$ gilt. Damit ist $d(f)$ auch unabhängig von den gewählten Nullstellen. □

Mit $h = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ gilt für die Diskriminante $d(f)$ des allgemeinen Polynoms f nach Satz 2.32 und Satz 2.29, daß $d(f) = h^2 \in k[s_1, \dots, s_n]$ ist. Für konkret gegebene Polynome f_0 gibt es also eine Formel für $d(f_0)$ in den Koeffizienten von f_0. Im Hinblick auf den Unterschied von S_n und A_n bemerken wir, daß für $\sigma \in S_n$ entweder $\sigma(h) = h$ oder $\sigma(h) = -h$ gilt, und der zweite Fall tritt wirklich auf. Für $\sigma \in A_n$ gilt auf der anderen Seite stets $\sigma(h) = h$. Aus $(S_n : A_n) = 2$ ergibt sich daher mit den Bezeichnungen von Satz 2.30, daß $F = \mathcal{F}_{E/K}(G) = K(h)$ und $m_{h,K} = t^2 - d(f)$ ist.

2.33 Satz. *Sei $f_0 \in k[t]$ ein separables Polynom vom Grad n und* $\operatorname{char}(k) = 0$ *oder* $\operatorname{char}(k) > 2$. *Die Diskriminante $d(f_0)$ ist ein Quadrat im Zerfällungskörper von f_0 über k und es gilt $G(f_0, k) \subseteq A_n$ genau dann, wenn $d(f_0)$ ein Quadrat in k ist.*

Beweis. Seien a_i die Nullstellen von f_0 und $h_0 = \prod_{1\leq i<j\leq n}(a_i - a_j)$. Die erste Aussage ist wegen $d(f_0) = h_0^2$ klar. Zur zweiten Aussage: Aus $G(f_0, k) \subseteq A_n$ folgt $h_0 \in k$ und somit ist $d(f_0) = h_0^2$ ein Quadrat in k. Gilt $G(f_0, k) \nsubseteq A_n$, so gibt es ein $\sigma \in G(f_0, k)$ mit $\sigma(h_0) = -h_0$. Wegen $h_0 \neq 0$ wegen der Separabilität von f_0 und $-1 \neq 1$ wegen $\mathrm{char}(k) = 0$ oder $\mathrm{char}(k) > 2$ folgt $\sigma(h_0) \neq h_0$. Dann gilt $h_0, -h_0 \notin k$ und $d(f_0)$ ist kein Quadrat in k. $\square$

Für den Fall $n = 3$ betrachten wir das separable Polynom $f = x^3+ax^2+bx+c$ in Charakteristik ungleich 3. Durch die Transformation $x \mapsto x - a/3$ erhalten wir ein Polynom mit gleicher Galoisgruppe wie f, aber ohne den x^2-Term. Wir nehmen daher ohne Einschränkung $a = 0$ an. Man kann nachrechnen, daß dann $d(f) = -4b^3 - 27c^2$ gilt, und wir können Satz 2.33 anwenden, um zwischen $G(f, K) = A_3$ und $G(f, K) = S_3$ zu unterscheiden.

Das Umkehrproblem der Galoistheorie für einen Körper K ist, zu einer endlichen Gruppe G ein Polynom $f \in K[t]$ mit $G(f, K) \cong G$ zu finden. Es hat für endliche Körper K im allgemeinen keine Lösung, da hier nur zyklische Galoisgruppen auftreten. Auf der anderen Seite haben wir mit Satz 2.28 eine Erweiterung E/K mit Galoisgruppe S_n konstruiert. Da jede endliche Gruppe G isomorph zu einer Untergruppe von S_n für geeignetes n ist, erhalten wir durch Fixkörperbildung eine Erweiterung E/F mit Galoisgruppe isomorph zu G. Indem man für die x_i geeignete Werte einsetzt, erhält man Erweiterungen E_0/F_0 und kann das Umkehrproblem so auch für F_0 und G lösen. Ein wesentliches Problem stellt sich hier aber, wenn die Bedingung $F_0 = k$ für $E = k(x_1, \ldots, x_n)$ fest vorgeben ist. Die Körper F sind nach einem Satz von Swan (1969) im allgemeinen keine rationalen Funktionenkörper mehr, ein Gegenbeispiel ist $k = \mathbb{Q}$, $n = 47$ und $G = \langle(1, \ldots, n)\rangle$. Daher fällt F_0 im allgemeinen echt größer als $\mathbb{Q}$ aus. Das Umkehrproblem der Galoistheorie ist damit für $\mathbb{Q}$ zur Zeit nur für spezielle Klassen von Gruppen gelöst. Nach einem Satz von Shafarevich (1954) sind beispielsweise alle auflösbaren Gruppen als Galoisgruppen realisierbar. Schreibt man ein „zufälliges“ Polynom $f \in \mathbb{Q}[t]$ hin, so gilt mit „großer“ Wahrscheinlichkeit $G(f, \mathbb{Q}) = S_n$.

2.6 Lineare Unabhängigkeit von Charakteren

Sei G eine Halbgruppe und K ein Körper. Unter einem Charakter von G in K verstehen wir in diesem Abschnitt einen Homomorphismus $\chi : G \to K^\times$. Der triviale Charakter $\chi = 1$ ist der durch $\chi(a) = 1$ für alle $a \in G$ gegebene Charakter.

Charaktere treten in vielen Zusammenhängen auf (zum Beispiel Fourieranalysis, Darstellungstheorie endlicher Gruppen). Im Rahmen der Vorlesung werden sie aber nur eine geringe Rolle spielen.

Sind χ_1, χ_2 Charaktere und $\lambda \in K$, so definieren wir wie üblich $(\chi_1 + \chi_2)(a) = \chi_1(a) + \chi_2(a)$ und $(\lambda\chi_1)(a) = \lambda\chi_1(a)$. Die Charaktere von G in K spannen damit einen K-Vektorraum von Abbildungen $G \to K$ auf. Die Charaktere $\chi_1, \dots, \chi_n$ von G in K sind linear unabhängig über K, wenn für $\lambda_i \in K$ aus $\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0$ folgt, daß alle $\lambda_i = 0$ sind. Wir haben folgenden, grundlegenden Satz.

2.34 Satz (Artin)**.** *Sei G eine Halbgruppe und K ein Körper. Die Charaktere $\chi_1, \dots, \chi_n$ von G in K sind genau dann linear unabhängig über K, wenn sie paarweise verschieden sind.*

Beweis. Sind die Charaktere linear unabhängig, so sind sie notwendigerweise verschieden. Wir nehmen nun an, daß die χ_i verschieden sind. Ein einzelner Charakter ist offenbar linear unabhängig über K, weil er nicht die Nullabbildung sein kann. Wir betrachten jetzt eine Relation $\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0$ mit minimalem $n \geq 2$. Dann sind alle $\lambda_i \neq 0$. Da $\chi_1 \neq \chi_2$ gibt es $a \in G$ mit $\chi_1(a) \neq \chi_2(a)$. Wegen $\chi_1 : G \to K^\times$ gilt $\chi_1(a) \neq 0$. Für alle $b \in G$ gilt dann $\sum_i \lambda_i\chi_i(ab) = \sum_i \lambda_i\chi_i(a)\chi_i(b) = 0$, folglich $\sum_i \lambda_i\chi_i(a)\chi_i = 0$. Wir dividieren diese Relation durch $\chi_1(a)$ und subtrahieren die ursprüngliche Relation $\sum_i \lambda_i\chi_i = 0$. Dies liefert $\sum_i(\lambda_i\chi_i(a)/\chi_1(a) - \lambda_i)\chi_i = 0$. Der Koeffizient von χ_1 ist Null und der von χ_2 nach Wahl von a ungleich Null. Wir erhalten eine Relation mit weniger als n Summanden, im Widerspruch zur Wahl von n. □

Als Spezialfall können wir Körperhomomorphismen eingeschränkt auf die multiplikativen Gruppen als Charaktere ansehen. Ein anderer, aufwendigerer Beweis für die lineare Unabhängigkeit in diesem Fall wurde von Dedekind gegeben.

Man kann Satz 2.34 nach Artin übrigens zum Ausgangspunkt eines anderen Aufbaus der Galoistheorie als wie behandelt machen (siehe zum Beispiel die Bücher von Fischer/Sacher und Meyberg).

Als erste Anwendung notieren wir den folgenden Satz über die Spurabbildung.

2.35 Satz. *Sei E/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(*i*) *E/K ist separabel.*

(*ii*) *Die Spurabbildung $\mathrm{Tr}_{E/K} : E \to K$ ist surjektiv.*

(*iii*) *Die symmetrische Bilinearform $E \times E \to K$, $(a, b) \mapsto \mathrm{Tr}_{E/K}(ab)$ ist nicht ausgeartet.*

Beweis. (*i*) ⇒ (*ii*): Da $\mathrm{Tr}_{E/K}$ eine Linearform des K-Vektorraums E ist, genügt es, $\mathrm{Tr}_{E/K} \neq 0$ zu zeigen. Sei C ein algebraischer Abschluß von K. Wegen $\mathrm{Tr}_{E/K} = \sum_{\sigma \in \mathrm{Hom}_K(E,C)} \sigma$ nach Satz 1.93 (*i*), folgt dies aus Satz 2.34.

(ii) $\Rightarrow$ *(iii)*: Sei $a \neq 0$. Nach *(ii)* gibt es ein $c \in E$ mit $\mathrm{Tr}_{E/K}(c) \neq 0$. Mit $b = c/a$ folgt $\mathrm{Tr}_{E/K}(ab) \neq 0$.

(iii) $\Rightarrow$ *(i)*: Ist E/K nicht separabel, so folgt aus Satz 1.93, daß $\mathrm{Tr}_{E/K} = 0$ gilt und die Bilinearform ist ausgeartet. □

2.7 Normalbasen

2.36 Definition. Sei E/K eine endliche Galoiserweiterung und $G = G(E/K)$. Eine K-Basis B von E heißt eine Normalbasis von E/K, wenn B von der Form $B = \{\sigma(a) \mid \sigma \in G\}$ für ein $a \in E$ ist.

2.37 Satz. *Jede endliche Galoiserweiterung E/K besitzt eine Normalbasis.*

Beweis. Für ein Element $a \in E$ mit $\sum_{\sigma\in G} \lambda_\sigma \sigma(a) = 0$ und $\lambda_\sigma \in K$ folgt $\sum_{\sigma\in G} \lambda_\sigma(\tau^{-1}\sigma)(a) = 0$ für alle $\tau \in G$. Es genügt also, ein Element a in E mit $\det(((\tau^{-1}\sigma)(a))_{\tau,\sigma}) \neq 0$ zu finden. Sei $g(t) = m_{b,K}(t)/(t-b) = \prod_{\tau\neq 1}(t - \tau(b))$ für ein primitives Element b von E/K. Genau dann ist $g^\sigma(b) \neq 0$, wenn $\sigma = 1$ ist. Denn für $\sigma = 1$ ist $g^\sigma(b) = g(b) \neq 0$ aufgrund der Separabilität von $m_{b,K}(t)$. Umgekehrt folgt aus $g^\sigma(b) \neq 0$, daß $b \neq \sigma(\tau(b))$ für alle $\tau \neq 1$ gilt, und daraus ergibt sich $\sigma = 1$ wegen $E = K(b)$. Wir betrachten die über $E[t]$ definierte Matrix $M(t) = (g^{\tau^{-1}\sigma}(t))_{\tau,\sigma}$ und $d(t) = \det(M)$. Für $t = b$ ist $M(b)$ eine Diagonalmatrix mit $g(b) \neq 0$ auf der Diagonalen. Daher gilt $d(b) \neq 0$ und folglich $d(t) \neq 0$. Enthält K unendlich viele Elemente, so gibt es ein $c \in K$ mit $d(c) \neq 0$. Wegen $g^{\tau^{-1}\sigma}(c) = (\tau^{-1}\sigma)(g(c))$ erhalten wir mit $a = g(c)$ das gesuchte Element a. Es bleibt der Fall zu behandeln, daß K ein endlicher Körper ist. Dann ist E/K zyklisch. Sei σ ein Erzeuger von $G(E/K)$. Wir betrachten σ als lineare Abbildung des Vektorraums E/K. Es gilt $\sigma^{[E:K]} - 1 = 0$.

Außerdem sind $1, \sigma, \ldots, \sigma^{[E:K]-1}$ nach Satz 2.34 über K linear unabhängig. Daher gilt für das Minimalpolynom $m_{\sigma,K}(t) = t^{[E:K]} - 1$ und wegen $\deg(m_{\sigma,K}(t)) = [E : K]$ ist es auch gleich dem charakteristischen Polynom von σ. Aus der linearen Algebra folgt damit, daß E/K ein σ-zyklischer Vektorraum ist und von einem Element $a \in E$ erzeugt wird. Per Definition liefert a dann eine Normalbasis von E/K. □

2.38 Bemerkung. Die Galoisgruppe operiert auf E, so daß E neben der Struktur eines K-Vektorraums auch die Struktur eines $K[G]$-Moduls besitzt ($(\sum_\sigma \lambda_\sigma\sigma)a = \sum_\sigma \lambda_\sigma\sigma(a)$ für $\lambda_\sigma \in K$ und $a \in E$). Die Aussage von Satz 2.37 besitzt dann die folgende, äquivalente Formulierung: Der $K[G]$-Modul E ist zyklisch.

Neben der theoretischen Bedeutung spielen Normalbasen zum Beispiel in der effizienten Computerarithmetik von endlichen Körpern eine wichtige Rolle.

2.8 Kummertheorie

Im Abschnitt 2.3 haben wir gesehen, daß die Galoisgruppen von einfachen Kummer- und Artin-Schreier-Erweiterungen zyklisch sind. In diesem Abschnitt zeigen wir umgekehrt, daß eine zyklische Erweiterung unter geeigneten Voraussetzungen wie in Abschnitt 2.3 eine einfache Kummer- oder Artin-Schreier-Erweiterung ist. Wir betrachten dafür aber allgemeiner gleich „mehrfache" Kummer- bzw. Artin-Schreier-Erweiterungen.

Um Kummer- und Artin-Schreier-Erweiterungen gemeinsam behandeln zu können, verwenden wir folgende Abstraktion. Für eine Galoiserweiterung E/K mit Galoisgruppe $G = G(E/K)$ betrachten wir eine Teilmenge $A \subseteq E^m$ mit $m \in \mathbb{Z}^{\geq 1}$, die eine mit der koordinatenweise Operation von G auf A verträgliche abelsche Gruppenstruktur haben soll. Es soll also $\sigma(ab) = \sigma(a)\sigma(b)$ für alle $\sigma \in G$ und $a, b \in A$ gelten, wobei das Gruppengesetz von A multiplikativ geschrieben wird. Wir nennen ein solches A einen G-Modul. Die uns hier im wesentlichen interessierenden Beispiele für A sind $A = E^\times$ und $A = E^+$.

Bezüglich G und A haben wir galoistheoretische Operationen und Normabbildungen. Zu einer Untergruppe H von G definieren wir $A^H = \{x \in A \,|\, \sigma(x) = x \text{ für alle } \sigma \in H\}$. Ist umgekehrt B eine Untergruppe von A, so sei $G_B = \{\sigma \in G \,|\, \sigma(x) = x \text{ für alle } x \in B\}$. Diese Definitionen sind ganz analog zu den Definitionen der Abbildungen $\mathcal{F}_{E/K}$ und $\mathcal{G}_{E/K}$ aus Abschnitt 2.1. Es hängt jedoch von der Wahl von A ab, ob $H \mapsto A^H$ und $B \mapsto G_B$ zueinander invers sind oder nicht. Zumindest gilt beispielsweise immer $G_{\sigma B} = \sigma G_B \sigma^{-1}$. Ist ferner H normal in G, so operieren G/H und G auf A^H in kompatibler Weise und A^H ist ein G/H-Modul.

Um Zwischenkörper von E/K und Untergruppen von A logisch zu verbinden, definieren wir zu einem Zwischenkörper F von E/K die Untergruppe $A_F = A^{\mathcal{G}_{E/K}(F)}$ und umgekehrt zu einer Untergruppe B von A den Zwischenkörper $K(B) = \mathcal{F}_{E/K}(G_B)$. Wegen der Regel $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$ gilt offenbar einerseits $A_F = A \cap F^m$, und andererseits entsteht $K(B)$ durch Adjunktion der in den Koordinaten der Elemente von B vorkommenden Elemente aus E an K. Ist F ein Zwischenkörper von E/K und normal über K, so wird A_F in natürlicher Weise ein $G(F/K)$-Modul.

Für eine Zwischenkörpererweiterung F_2/F_1 von E/K und $x \in A_{F_2}$ definieren wir schließlich $\mathrm{N}_{F_2/F_1}(x) = \prod_{\sigma \in R} \sigma(x)$, wobei R ein Nebenklassenrepräsentantensystem von $\mathcal{G}_{E/K}(F_2)$ in $\mathcal{G}_{E/K}(F_1)$ mit $\mathcal{G}_{E/K}(F_1) = \dot{\bigcup}_{\sigma \in R} \sigma \mathcal{G}_{E/K}(F_2)$ ist. Die Definition hängt nicht von der Wahl von R ab, da A_{F_2} von $\mathcal{G}_{E/K}(F_2)$ fixiert wird. Wir könnten die Norm übrigens auch nur für Untergruppen H_2, H_1 von G ohne einen Bezug zu Körpern definieren. Wegen der galoistheoretischen Äquivalenz von Zwischenkörpern und Untergruppen sind diese Varianten im Endeffekt gleichbedeutend.

2.39 Lemma. *Sei F_2/F_1 eine Zwischenkörpererweiterung der Galoiserweiterung E/K. Dann gilt $\mathrm{N}_{F_2/F_1}(x) \in A_{F_1}$ und die resultierende Abbildung $\mathrm{N}_{F_2/F_1} : A_{F_2} \to A_{F_1}$ ist ein Homomorphismus.*

Ferner gilt $\mathrm{N}_{\tau F_2/\tau F_1}(\tau(x)) = \tau(\mathrm{N}_{F_2/F_1}(x))$ für alle $\tau \in G$ und $x \in F_2$, und $\mathrm{N}_{F_3/F_1} = \mathrm{N}_{F_2/F_1} \circ \mathrm{N}_{F_3/F_2}$ für einen weiteren Zwischenkörper F_3 von E/K mit $F_2 \subseteq F_3$.

Beweis. Wir kürzen $\mathcal{G} = \mathcal{G}_{E/K}$ ab. Mit R ist auch $R' = \{\tau\sigma \,|\, \sigma \in R\}$ für jedes $\tau \in \mathcal{G}(F_1)$ ein Nebenklassenrepräsentantensystem von $\mathcal{G}(F_2)$ in $\mathcal{G}(F_1)$. Folglich gilt $\tau(\mathrm{N}_{F_2/F_1}(x)) = \prod_{\sigma \in R} \tau\sigma(x) = \prod_{\sigma \in R'} \sigma(x) = \mathrm{N}_{F_2/F_1}(x)$ und daher $\mathrm{N}_{F_2/F_1}(x) \in A_{F_1}$. Die Homomorphieeigenschaft folgt, da die σ als Endomorphismen auf A_{F_2} operieren.

Für jedes $\tau \in G$ ist das System $R' = \{\tau\sigma\tau^{-1} \,|\, \sigma \in R\}$ ein Nebenklassenrepräsentantensystem von $\tau\mathcal{G}(F_2)\tau^{-1} = \mathcal{G}(\tau F_2)$ in $\tau\mathcal{G}(F_1)\tau^{-1} = \mathcal{G}(\tau F_1)$. Daraus folgt direkt die Behauptung $\mathrm{N}_{\tau F_2/\tau F_1}(\tau(x)) = \tau(\mathrm{N}_{F_2/F_1}(x))$.

Schließlich seien R_{F_2/F_1} und R_{F_3/F_2} Nebenklassenrepräsentantensysteme von $\mathcal{G}(F_2)$ in $\mathcal{G}(F_1)$ bzw. von $\mathcal{G}(F_3)$ in $\mathcal{G}(F_2)$ wie oben. Dann ist $R_{F_3/F_1} = \{\sigma\tau \,|\, \sigma \in R_{F_2/F_1}, \tau \in R_{F_3/F_2}\}$ ein Nebenklassenrepräsentantensystem von $\mathcal{G}(F_3)$ in $\mathcal{G}(F_1)$ und es gilt $\mathrm{N}_{F_3/F_1}(x) = \prod_{\sigma,\tau} \sigma(\tau(x)) = \prod_\sigma \sigma(\prod_\tau \tau(x)) = \mathrm{N}_{F_2/F_1}(\mathrm{N}_{F_3/F_2}(x))$. $\square$

Es sei angemerkt, daß die Normabbildung N_{F_2/F_1} nicht von der Galoiserweiterung E/K abhängt. Lemma 2.39 liefert einen zu Satz 1.92 alternativen Beweis für die Transitivität von Spur und Norm.

Sei E/K galoissch, $G = G(E/K)$ und A wie oben ein G-Modul. Durch Untergruppen B von A können wir Zwischenkörper $K(B)$ von E/K definieren und umgekehrt. Wir wollen diesen Prozeß genauer untersuchen, wenn es einen surjektiven G-Homomorphismus $\wp : A \to A$ mit endlichem, zyklischem Kern $\mu_\wp \subseteq A_K$ gibt. G-Homomorphismus bedeutet, daß $\sigma(\wp(a)) = \wp(\sigma(a))$ für alle $\sigma \in G$ und $a \in A$ gilt. Wir setzen $n = \#\mu_\wp$ und machen folgende, axiomatische Annahme:

2.40 Annahme. *Sei F/K eine endliche, zyklische Erweiterung mit $F \subseteq E$ und σ ein Erzeuger von $G(F/K)$. Für $a \in A_F$ gilt $\mathrm{N}_{F/K}(a) = 1$ genau dann, wenn es ein $b \in A_F$ mit $a = b \cdot \sigma(b)^{-1}$ gibt.*

Mit Lemma 2.39 ist klar, daß die Implikation „$\Leftarrow$" in Annahme 2.40 immer gilt. Wir verwenden Annahme 2.40 nur für den zweiten Teil des nachfolgenden Satzes 2.41.

Für eine Untergruppe $\Delta \subseteq A$ mit $\wp(A_K) \subseteq \Delta$ bezeichnet $\wp^{-1}(\Delta)$ die Menge aller Urbilder der Elemente von Δ unter $\wp$. Wir können daher den Körper $K(\wp^{-1}(\Delta))$ bilden. Ist $B \subseteq \wp^{-1}(\Delta)$ derart, daß $\{\wp(b)\wp(A_K) \,|\, b \in B\}$ ein Erzeugendensystem von $\Delta/\wp(A_K)$ bildet, so gilt $K(\wp^{-1}(\Delta)) = K(B)$ wegen der Homomorphieeigenschaft von $\wp$ und $\wp^{-1}(\wp(A_K)) = A_K$.

2.41 Satz. *Im folgenden bezeichnet F einen Zwischenkörper von E/K.*

(*i*) *Sei Δ eine Untergruppe von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$ und $F = K(\wp^{-1}(\Delta))$. Dann ist F/K galoissch und $G(F/K)$ abelsch vom Exponenten n.*

(*ii*) *Ist umgekehrt F/K eine galoissche Erweiterung mit $G(F/K)$ abelsch vom Exponenten n, so ist $\Delta = \wp(A_F) \cap A_K$ eine Untergruppe von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$ und es gilt $F = K(\wp^{-1}(\Delta))$.*

Beweis. (*i*): Sei $a \in A_K$ und $b \in A$ mit $\wp(b) = a$. Das Element b ist modulo $\mu_\wp$ definiert und die Erweiterung $K(b)/K$ ist wegen $\mu_\wp \subseteq A_K$ nach Voraussetzung eindeutig durch a bestimmt. Wir nennen $K(b)/K$ eine einfache Kummererweiterung bezüglich $\wp$ und a. Wegen $\wp(\sigma(b)) = \sigma(\wp(b)) = \sigma(a) = a = \wp(b)$ für $\sigma \in G$ gibt es daher für jedes σ ein $\zeta_\sigma \in \mu_\wp$ mit $\sigma(b) = \zeta_\sigma b \in A_{K(b)}$, so daß $K(b)/K$ galoissch ist und $G(K(b)/K)$ durch $\sigma \mapsto \zeta_\sigma$ nach $\mu_\wp$ eingebettet wird. Insbesondere ist $K(b)/K$ demzufolge zyklisch vom Exponenten n.

Sei nun Δ eine Untergruppe von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$ und $F = K(\wp^{-1}(\Delta))$. Wegen $F = \coprod_{b\in\wp^{-1}(\Delta)} K(b)$ ist F/K galoissch mit einer Galoisgruppe, die sich nach $\prod_{b\in\wp^{-1}(\Delta)} \mu_\wp$ einbettet. Diese ist daher abelsch vom Exponenten n.

(*ii*): Sei umgekehrt F/K abelsch vom Exponenten n. Aufgrund der Definition ist Δ eine Untergruppe von A_K. Da $\wp$ G-linear ist, gilt $\wp(A_K) \subseteq A_K$ und damit $\Delta = \wp(A_F) \cap A_K \supseteq \wp(A_K) \cap A_K = \wp(A_K)$. Außerdem gilt $\wp^{-1}(\Delta) \subseteq \wp^{-1}(\wp(A_F)) = A_F$ wegen $\mu_\wp \subseteq A_K$, woraus sich $K(\wp^{-1}(\Delta)) \subseteq F$ ergibt.

Wir wollen nun $F \subseteq K(\wp^{-1}(\Delta))$ zeigen. Jeder endliche Teilkörper F' von F/K ist ebenfalls abelsch vom Exponenten n über K. Da F das Kompositum solcher endlicher Teilerweiterungen ist, genügt es zu zeigen, daß $F' \subseteq K(\wp^{-1}(\Delta))$ gilt.

Die Galoisgruppe $G(F'/K)$ läßt sich in ein Produkt $\prod_{i\in I} \mu_\wp$ für eine endliche Indexmenge I einbetten. Wir definieren den Kern der Komposition dieser Einbettung mit der i-ten Projektion $\prod_{i\in I} \mu_\wp \to \mu_\wp$ als H_i und setzen $F'_i = \mathcal{F}_{F'/K}(H_i)$. Wegen $\cap_i H_i = \{1\}$ und $[F' : K] < \infty$ gilt $F' = \coprod_i F'_i$ nach Satz 2.10, (*ii*), so daß wir nun nur noch $F'_i \subseteq K(\wp^{-1}(\Delta))$ für alle $i \in I$ zeigen müssen.

Sei $i \in I$ beliebig. Die Erweiterung F'_i/K ist galoissch und $G(F'_i/K) \cong G(F'/K)/H_i$ bettet sich nach $\mu_\wp$ ein, so daß F'_i/K insbesondere zyklisch ist. Sei σ ein Erzeuger von $G(F'_i/K)$ und $\zeta_\sigma \in \mu_\wp$ ein Element der Ordnung $[F'_i : K]$. Dann gilt $\mathrm{N}_{F'_i/K}(\zeta_\sigma) = \zeta_\sigma^{[F'_i:K]} = 1$ und aufgrund der Annahme 2.40 gibt es ein $b \in A_{F'_i}$ mit $\sigma(b) = \zeta_\sigma b$. Da ζ_σ die Ordnung $[F'_i : K]$ besitzt, gilt $\mathcal{G}_{F'_i/K}(K(b)) = \{1\}$ und somit $F'_i = K(b)$. Außerdem ist $\sigma(\wp(b)) = \wp(\sigma(b)) = \wp(\zeta_\sigma b) = \wp(b)$ und folglich $\wp(b) \in \wp(A_F) \cap A_K = \Delta$. Daraus ergibt sich $b \in \wp^{-1}(\Delta)$ und $F'_i = K(b) \subseteq K(\wp^{-1}(\Delta))$. □

Für den Hauptsatz dieses Abschnitts benötigen wir noch eine allgemeine Aussage. Seien C und D abelsche Gruppen. Eine Paarung von C und D in die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist eine in beiden Argumenten homomorphe Abbildung $\langle\cdot,\cdot\rangle : C \times D \to \mathbb{Z}/n\mathbb{Z}$. Eine Paarung definiert (und wird definiert durch) Homomorphismen $\iota_1 : C \to \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z})$ bzw. $\iota_2 : D \to \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ und heißt nicht ausgeartet, wenn ι_1 und ι_2 injektiv sind.

2.42 Lemma. *Sei $\langle\cdot,\cdot\rangle : C \times D \to \mathbb{Z}/n\mathbb{Z}$ eine nicht ausgeartete Paarung. Dann besitzen C und D den Exponenten n und es gilt $\#C = \#D$. Gilt zusätzlich $\#C < \infty$, so sind die Monomorphismen $\iota_1 : C \to \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z})$ und $\iota_2 : D \to \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ Isomorphismen und es gibt eine (nicht kanonische) Isomorphie $C \cong D$.*

Beweis. Übung. □

Für $C = \coprod_{i\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ und $D = \prod_{i\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ liefert $((a_i)_i, (b_i)_i) \mapsto \sum_i a_i b_i$ eine nicht ausgeartete Paarung $C \times D \to \mathbb{Z}/2\mathbb{Z}$. Hier gilt $\mathrm{Hom}(C, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(D, \mathbb{Z}/2\mathbb{Z}) \cong D \not\cong C$.

2.43 Satz. *Die Zuordnung*

$$\Delta \mapsto F = K(\wp^{-1}(\Delta))$$

ist eine inklusionserhaltende Bijektion zwischen den Untergruppen Δ von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$ und den abelschen Erweiterungen F/K vom Exponenten n in E mit der inversen Bijektion

$$F \mapsto \Delta = \wp(A_F) \cap A_K.$$

Weiter gilt $[F : K] = (\Delta : \wp(A_K))$ und $\Delta/\wp(A_K)$ besitzt den Exponenten n.

Sind Δ und F einander zugeordnet, gibt es eine kanonische, nicht ausgeartete Paarung

$$G(F/K) \times \Delta/\wp(A_K) \to \mu_\wp,$$

welche $(\sigma, a\wp(A_K))$ auf $b/\sigma(b)$ für $b \in \wp^{-1}(a)$ abbildet. Für $[F : K] = (\Delta : \wp(A_K)) < \infty$ liefert die Paarung die Isomorphismen

$$G(F/K) \cong \mathrm{Hom}(\Delta/\wp(A_K), \mu_\wp), \quad \Delta/\wp(A_K) \cong \mathrm{Hom}(G(F/K), \mu_\wp).$$

Beweis. Die Wohldefiniertheit und Homomorphieeigenschaft der Paarung in beiden Argumenten folgen im wesentlichen aus der Definition von $\wp$: Sei Δ eine Untergruppe von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$, $F = K(\wp^{-1}(\Delta))$, $a \in \Delta$ und

$\sigma \in G(F/K)$. Da $\wp : A \to A$ surjektiv ist, gibt es zunächst einmal überhaupt ein $b \in \wp^{-1}(a) \subseteq A_F$, mit dem die Paarung definiert werden kann. Außdem gilt $\wp(b/\sigma(b)) = \wp(b)/\sigma(\wp(b)) = a/\sigma(a) = 1$, also $b/\sigma(b) \in \mu_\wp$. Zu $b' \in \wp^{-1}(a\wp(c)) = \wp^{-1}(a)c$ mit $c \in A_K$ gibt es $\zeta \in \mu_\wp \subseteq A_K$ mit $b' = \zeta bc$. Daraus folgt $b'/\sigma(b') = (\zeta bc)/(\zeta\sigma(b)c) = b/\sigma(b)$ und die Paarung ist wohldefiniert. Zu $a_1, a_2 \in \Delta$ gibt es $b_i \in \wp^{-1}(a_i)$. Dann gilt $b_1 b_2 \in \wp^{-1}(a_1 a_2)$ und $(b_1 b_2)/\sigma(b_1 b_2) = (b_1/\sigma(b_1))(b_2/\sigma(b_2))$, also die Homomorphieeigenschaft im rechten Argument der Paarung. Für $\sigma_1, \sigma_2 \in G(F/K)$ gilt $b/\sigma_1(\sigma_2(b)) = (b/\sigma_2(b))(\sigma_2(b)/\sigma_1(\sigma_2(b))) = (b/\sigma_2(b))\sigma_2(b/\sigma_1(b)) = (b/\sigma_2(b))(b/\sigma_1(b))$, weil die Galoisgruppe $G(F/K)$ abelsch ist und $b/\sigma_1(b) \in \mu_\wp \subseteq A_K$ gilt. Dies ergibt die Homomorphieeigenschaft im linken Argument.

Wir zeigen nun, daß die Paarung nicht ausgeartet ist. Gilt $b/\sigma(b) = 1$ für alle $\sigma \in G(F/K)$, so folgt $b \in A_K$. Damit ist $a \in \wp(A_K)$ und die Paarung ist im rechten Argument nicht ausgeartet. Sei $\sigma \in G$. Gilt dann $b/\sigma(b) = 1$ für $b \in \wp^{-1}(a)$ und alle $a \in \Delta$, so folgt $\sigma \in G_{\wp^{-1}(\Delta)} = \mathcal{G}_{E/K}(F)$. Somit ist σ auf F die Identität und die Paarung im linken Argument nicht ausgeartet.

Da die Paarung nicht ausgeartet ist, können wir Lemma 2.42 anwenden. Es ergibt sich, daß $[F : K] = \#G(F/K) = \#(\Delta/\wp(A_K)) = (\Delta : \wp(A_K))$ gilt und $\Delta/\wp(A_K)$ den Exponenten n besitzt. Für $(\Delta : \wp(A_K)) < \infty$ ergeben sich außerdem die Isomorphieen $G(F/K) \cong \mathrm{Hom}(\Delta/\wp(A_K), \mu_\wp)$ und $\Delta/\wp(A_K) \cong \mathrm{Hom}(G(F/K), \mu_\wp)$.

Wir beweisen nun die Injektivität der Abbildung $\Delta \mapsto F$. Seien Δ_1, Δ_2 mit $F = K(\wp^{-1}(\Delta_1)) = K(\wp^{-1}(\Delta_2))$ und sei $a \in \Delta_1$. Wir wollen $a \in \Delta_2$ zeigen. Wegen $K(\wp^{-1}(a)) \subseteq K(\wp^{-1}(\Delta_1)) = K(\wp^{-1}(\Delta_2))$ und $\#\wp^{-1}(a) < \infty$ gibt es eine endliche Menge $S \subseteq \wp^{-1}(\Delta_2)$ mit $K(\wp^{-1}(a)) \subseteq K(S)$. Sei $\Delta_a = \langle \wp(S) \rangle \wp(A_K)$ die von $\wp(S)$ und $\wp(A_K)$ erzeugte Untergruppe von Δ_2. Wegen der Homomorphieeigenschaft von $\wp$ und $\mu_\wp \subseteq A_K$ gilt dann auch $K(\wp^{-1}(a)) \subseteq K(\wp^{-1}(\Delta_a)) = K(S)$. Da $\#\wp(S) < \infty$ und $\Delta_2/\wp(A_K)$ den Exponenten n besitzt, gilt $\#(\Delta_a/\wp(A_K)) < \infty$. Aus $K(\wp^{-1}(a)) \subseteq K(\wp^{-1}(\Delta_a))$ ergibt sich $K(\wp^{-1}(\langle a \rangle \Delta_a)) = K(\wp^{-1}(\Delta_a))$, wobei $\langle a \rangle \Delta_a$ die von a und Δ_a erzeugte Untergruppe von A_K bezeichnet. Nach der bereits bewiesenen Gleicheit von Körpergrad und Gruppenindex ergibt sich $(\langle a \rangle \Delta_a : \wp(A_K)) = [K(\wp^{-1}(\langle a \rangle \Delta_a)) : K] = [K(\wp^{-1}(\Delta_a)) : K] = (\Delta_a : \wp(A_K))$. Wegen $(\Delta_a : \wp(A_K)) < \infty$ und $\Delta_a \subseteq \langle a \rangle \Delta_a$ folgt $\Delta_a = \langle a \rangle \Delta_a$, also $a \in \Delta_a \subseteq \Delta_2$. Da a beliebig war, folgt $\Delta_1 \subseteq \Delta_2$. Analog ergibt sich $\Delta_2 \subseteq \Delta_1$, so daß $\Delta_1 = \Delta_2$ folgt und die Abbildung $\Delta \mapsto F$ injektiv ist.

Die Surjektivität der Abbildung $\Delta \mapsto F$ und die Ausssage über die inverse Abbildung folgt direkt aus Satz 2.41, *(ii)*. □

Die Paarung von Satz 2.43 wird Kummerpaarung genannt. Ist L/K eine Erweiterung von K, so können wir die Translation $L(\wp^{-1}(\Delta))/L$ der Erweiterung

$K(\wp^{-1}(\Delta))/K$ betrachten. Diese ist nach Satz 2.15 wieder abelsch vom Exponenten n und gehört zur von Δ in $A_L/\wp(A_L)$ erzeugten Untergruppe $\Delta_L = \Delta\wp(A_L)/\wp(A_L) \cong \Delta/(\Delta \cap \wp(A_L))$. Ähnlich gilt für Komposita und Schnitte, daß $K(\wp^{-1}(\Delta_1))K(\wp^{-1}(\Delta_2))/K$ zu $\Delta_1\Delta_2$ und $K(\wp^{-1}(\Delta_1)) \cap K(\wp^{-1}(\Delta_2))/K$ zu $\Delta_1 \cap \Delta_2$ gehören.

Wir spezialisieren obige Theorie nun auf die Fälle $A = E^\times$ und $A = E^+$, wo E den separablen Abschluß von K bezeichnet. Im ersten Fall betrachten wir $\wp : A \mapsto A, x \mapsto x^n$, wobei $\mathrm{char}(K) = 0$ oder $\gcd(\mathrm{char}(K), n) = 1$ gelte. Wir müssen $\mu_\wp \subseteq A_K$, also $\mu_n \subseteq K^\times$ voraussetzen. Die Erweiterungen $K(\wp^{-1}(\Delta))/K$ entstehen dann also durch Adjunktion aller n-ter Wurzeln der Elemente in Δ an K und werden Kummererweiterungen genannt. Im zweiten Fall betrachten wir den Artin-Schreier Operator $\wp : A \mapsto A, x \mapsto x^p - x$, wobei $p = \mathrm{char}(K) > 0$ gelte. Hier ist $\mu_\wp \subseteq A_K$, also $\mathbb{F}_p^+ \subseteq K^+$ automatisch erfüllt. Die Erweiterungen $K(\wp^{-1}(\Delta))/K$ enstehen also durch Adjunktion aller Nullstellen der Polynome $t^p - t - a$ für $a \in \Delta$ an K und werden Artin-Schreier Erweiterungen genannt. Für diese beiden Fälle gilt die Annahme 2.40:

2.44 Satz (Hilbert 90)**.** *Sei F/K eine endliche, zyklische Erweiterung und σ ein Erzeuger von $G(F/K)$.*

(i) *Für $a \in F^\times$ gilt $\mathrm{N}_{F/K}(a) = 1$ genau dann, wenn es ein $b \in F^\times$ mit $a = b \cdot \sigma(b)^{-1}$ gibt.*

(ii) *Für $a \in F^+$ gilt $\mathrm{Tr}_{F/K}(a) = 0$ genau dann, wenn es ein $b \in F^+$ mit $a = b - \sigma(b)$ gibt.*

Beweis. $(i), \Leftarrow$: Es gilt $\mathrm{N}_{F/K}(a) = \mathrm{N}_{F/K}(b)/\mathrm{N}_{F/K}(\sigma(b)) = 1$ nach Lemma 2.39. $(i), \Rightarrow$: Wir setzen $n = [F : K]$. Die durch

$$\sigma^0 + a\sigma^1 + a\sigma(a)\sigma^2 + \cdots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}$$

definierte Abbildung $F^\times \to F$ ist nach Satz 2.34 nicht die Nullabbildung. Daher gibt es ein $c \in F$, so daß

$$b := \sigma^0(c) + a\sigma^1(c) + a\sigma(a)\sigma^2(c) + \cdots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(c) \neq 0$$

ist. Anwenden von σ und Multiplikation mit a ergibt

$$a\sigma(b) = a\sigma^1(c) + a\sigma(a)\sigma^2(c) + \cdots + a\sigma(a)\cdots\sigma^{n-1}(a)\sigma^n(c) = b,$$

da $\sigma^n = 1$ und $a\sigma(a)\cdots\sigma^{n-1}(a) = \mathrm{N}_{F/K}(a) = 1$ nach Voraussetzung gilt.

(ii): Kann ähnlich wie (i) bewiesen werden. Ist $c \in F$ mit $\mathrm{Tr}_{F/K}(c) \neq 0$ so erfüllt

$$b = \frac{1}{\mathrm{Tr}_{F/K}(c)}\big(a\sigma^1(c) + (a+\sigma(a))\sigma^2(c) + \dots \\ + (a+\sigma(a)+\dots+\sigma^{n-2}(a))\sigma^{n-1}(c)\big)$$

die Bedingung $a = b - \sigma(b)$. □

Genauer bezeichnet man eigentlich nur Teil (i) als Satz Hilbert 90. Als Beispiel betrachten wir die aufsteigende Folge von Primzahlen $p_1, \dots, p_m$, $K = \mathbb{Q}$, $A_K = \mathbb{Q}^\times$, $\wp(x) = x^2$, $n = 2$, $\mu_2 = \{-1, 1\}$ und die von den p_i und den Quadraten $\mathbb{Q}^{\times 2}$ erzeugte Untergruppe Δ von $\mathbb{Q}^\times$. Da die p_i die Gruppe $\Delta/\mathbb{Q}^{\times 2}$ erzeugen, gilt $F = K(\wp^{-1}(\Delta)) = K(\sqrt{p_1}, \dots, \sqrt{p_m})$. Da die p_i multiplikativ unabhängig sind, gilt $\Delta/\mathbb{Q}^{\times 2} \cong \langle p_1, \dots, p_m\rangle/(\langle p_1, \dots, p_m\rangle \cap \mathbb{Q}^{\times 2}) \cong (\mathbb{Z}/2\mathbb{Z})^m$. Daraus folgt $G(F/K) \cong \mathrm{Hom}(\Delta/\mathbb{Q}^{\times 2}, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^m$.

2.45 Korollar. *Sei F/K eine algebraische Körpererweiterung und $p = \mathrm{char}(K)$.*

- (i) *Es gelte $p = 0$ oder $\gcd(p, n) = 1$, und K enthalte die n-ten Einheitswurzeln. Dann ist F/K genau dann zyklisch vom Exponenten n, wenn $F = K(b)$ mit $b^n \in K$ gilt.*

- (ii) *Es gelte $p > 0$. Dann ist F/K genau dann zyklisch vom Exponenten p, wenn $F = K(b)$ mit $b^p - b \in K$ gilt.*

Beweis. Ist der einfachste Fall in Satz 2.43. Für die Richtung „$\Leftarrow$“ setzen wir $a = \wp(b)$ und $\Delta = \langle a\rangle\wp(A_K)$ und erhalten $F = K(b) = K(\wp^{-1}(\Delta))$. Da $\Delta/\wp(A_K)$ zyklisch ist, muß auch $G(F/K) \cong \mathrm{Hom}(\Delta/\wp(A_K), \mu_\wp)$ zyklisch sein. Für die Richtung „$\Rightarrow$“ sei F/K zyklisch und $\Delta = \wp(A_F) \cap A_K$. Dann ist $\Delta/\wp(A_K) \cong \mathrm{Hom}(G(F/K), \mu_\wp)$ zyklisch. Also gibt es $a \in A_K$ mit $\Delta = \langle a\rangle\wp(A_K)$ und mit $b \in \wp^{-1}(a)$ gilt $F = K(\wp^{-1}(\Delta)) = K(b)$.

Ist ζ eine Einheitswurzel der genauen Ordnung $[F : K]$, so ist das gesuchte Element b im übrigen das Element b zu $a = \zeta$ aus Satz 2.44. □

Abschließend sei bemerkt, daß man für die Betrachtung von abelschen Erweiterungen vom Exponenten p^r in Charakteristik $p > 0$ den G-Modul A als die additive Gruppe des Rings der Wittvektoren der Länge r über K wählt. Eine abelsche Erweiterung F/K eines beliebigen Exponenten $n = n_1p^r$ mit $\gcd(n_1, p^r) = 1$ und $p = \mathrm{char}(K)$ kann damit auf eine abelsche Erweiterung F_1/K vom Exponenten n_1 und eine dazu linear disjunkte abelsche Erweiterung F_2/K vom Exponenten p^r mit $F = F_1F_2$ zurückgeführt werden.

Ergänzung

Die Isomorphieen in Satz 2.43 gelten zum Teil auch ohne die Voraussetzung $(\Delta : \wp(A_K)) < \infty$. Dies soll hier noch nachgetragen werden. Wir benötigen dazu eine Verschärfung von Lemma 2.42.

Seien C und D abelsche Gruppen und $\langle\cdot,\cdot\rangle : C \times D \to \mathbb{Z}/n\mathbb{Z}$ eine Paarung. Für Untergruppen U von C und V von D definieren wir Abbildungen $\phi_1 : U \mapsto V = \{d \in D \mid \langle U, d\rangle = \{0\}\}$ und $\phi_2 : V \mapsto U = \{c \in C \mid \langle c, V\rangle = \{0\}\}$. Die Abbildungen ϕ_1 und ϕ_2 erfüllen analoge Eigenschaften wie $\mathcal{F}$ und $\mathcal{G}$ in Abschnitt 2.1. Das folgende Lemma kann als eine Art „Galoistheorie" aufgefaßt werden.

2.46 Lemma. *Sei $\langle\cdot,\cdot\rangle : D \times C \to \mathbb{Z}/n\mathbb{Z}$ eine nicht ausgeartete Paarung.*

(i) Es gilt $\#U = \#D/\phi_1(U)$ und $\#V = \#C/\phi_2(V)$ für alle Untergruppen U von C und V von D.

(ii) Der Homomorphismus $\iota_2 : D \to \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ ist ein Monomorphismus, dessen Bild aus allen $h \in \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ besteht, für die es eine Untergruppe V von D mit $\ker(h) = \phi_2(V)$ gibt. Analoges gilt für ι_1.

Für jede Untergruppe V von D und $d \in D$ mit $\phi_2(V) \subseteq \phi_2(\langle d\rangle)$ gebe es nun eine endliche Untergruppe $V_0 \subseteq V$ mit $\phi_2(V_0) \subseteq \phi_2(\langle d\rangle)$. Dann gilt weiter:

(iii) Die Abbildung $\phi_1 \circ \phi_2$ ist die Identität auf der Menge der Untergruppen von D.

(iv) Der Homomorphismus $\iota_1 : C \to \mathrm{Hom}(D, \mathbb{Z}/n\mathbb{Z})$ ist ein Isomorphismus.

Beweis. (i): Ist U eine Untergruppe von C so erhalten wir aus $\langle\cdot,\cdot\rangle$ eine Paarung $U \times D/\phi_1(U) \to \mathbb{Z}/n\mathbb{Z}$. Nach Vorausetzung ist die linke zugehörige Abbildung $U \to \mathrm{Hom}(D/\phi_1(U), \mathbb{Z}/n\mathbb{Z})$ injektiv. Außerdem hat die rechte Abbildung $D \to \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z})$ den Kern $\phi_1(U)$, so daß $D/\phi_1(U) \to \mathrm{Hom}(U, \mathbb{Z}/n\mathbb{Z})$ ebenfalls injektiv ist. Die Paarung ist also nicht entartet. Nach Lemma 2.42 gilt also $\#U = \#D/\phi_1(U)$. Analoges gilt für Untergruppen V von D und $C/\phi_2(V)$.

(ii): Für $d \in D$ gilt $\ker(\iota_2(d)) = \phi_2(\langle d\rangle)$. Daher besteht das Bild von ι_2 nur aus Elementen der angegebenen Form. Sei umgekehrt $h \in \mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ beliebig und $\ker(h) = \phi_2(V)$. Fassen wir die Gruppe $\mathrm{Hom}(C/\phi_2(V), \mathbb{Z}/n\mathbb{Z})$ mittels Zurückziehung als Untergruppe von $\mathrm{Hom}(C, \mathbb{Z}/n\mathbb{Z})$ auf, so gilt $h \in \mathrm{Hom}(C/\phi_2(V), \mathbb{Z}/n\mathbb{Z})$. Da die eingeschränkte Paarung $C/\phi_2(V) \times V \to \mathbb{Z}/n\mathbb{Z}$ nach (i) nicht ausgeartet ist und $\#V = \#C/\phi_2(V) < \infty$ gilt, liefert die Einschränkung von ι_2 auf V eine Isomorphie $V \cong \mathrm{Hom}(C/\phi_2(V), \mathbb{Z}/n\mathbb{Z})$. Also gibt es ein Urbild $d \in V$ von h unter ι_2 in D.

(*iii*): Man sieht wie bei $\mathcal{G}$ und $\mathcal{F}$ leicht, daß $\phi_2 \circ \phi_1 \circ \phi_2 = \phi_2$ gilt. Ist ϕ_2 injektiv, ergibt sich daraus $\phi_1 \circ \phi_2 = \mathrm{id}$. Zum Beweis der Injektivität von ϕ_2 seien V und V' Untergruppen von D mit $\phi_2(V) = \phi_2(V')$. Sei $d \in V'$. Wir wollen $d \in V$ zeigen.

Es gilt $\phi_2(V) = \phi_2(V') \subseteq \phi_2(\langle d \rangle)$. Nach Voraussetzung gibt es eine endliche Untergruppe V_0 von V mit $\phi_2(V_0) \subseteq \phi_2(\langle d \rangle)$. Dann gilt $\phi_2(V_0) = \phi_2(V_0 + \langle d \rangle)$. Wir wenden (*i*) für $V = V_0$ und $V = V_0 + \langle d \rangle$ an und erhalten $\#V_0 = \#C/\phi_2(V_0) = \#C/\phi_2(V_0 + \langle d \rangle) = \#(V_0 + \langle d \rangle)$. Wegen $\#V_0 < \infty$ und $V_0 \subseteq V_0 + \langle d \rangle$ ergibt sich daraus $V_0 = V_0 + \langle d \rangle$ und $d \in V_0 \subseteq V$. Da d beliebig war, folgt $V' \subseteq V$. Analog ergibt sich $V \subseteq V'$ und damit $V = V'$.

(*iv*). Die Aussage in (*ii*) gilt analog auch für ι_1. Jede Untergruppe V von D ist aber von der Form $\phi_1(U)$ für eine Untergruppe U von C. Definiere nämlich $U = \phi_2(V)$. Nach (*iii*) gilt dann $\phi_1(U) = \phi_1(\phi_2(V)) = V$. Also ist ι_1 surjektiv. □

2.47 Satz. *Sei Δ eine Untergruppe von A_K mit $\wp(A_K) \subseteq \Delta \subseteq A_K$ und $F = K(\wp^{-1}(\Delta))$. Die Kummerpaarung liefert Isomorphismen*

$$G(F/K) \cong \mathrm{Hom}(\Delta/\wp(A_K), \mu_\wp), \quad \Delta/\wp(A_K) \cong \mathrm{Hom}_a(G(F/K), \mu_\wp),$$

wobei $\mathrm{Hom}_a(G(F/K), \mu_\wp)$ *die Gruppe der Homomorphismen mit abgeschlossenem Kern bezeichnet.*

Beweis. Sei $E = K(\wp^{-1}(A_K))$. Wir bezeichnen die zugehörige Kummerpaarung mit $\langle \cdot, \cdot \rangle : G(E/K) \times A_K/\wp(A_K) \to \mu_\wp$. Nach Satz 2.43 existert diese und ist nicht ausgeartet. Außerdem ist die Bedingung von Lemma 2.46 an $D = A_K/\wp(A_K)$ nach dem Beweis von Satz 2.43 erfüllt.

Seien $\phi_1 : H \mapsto \Delta/\wp(A_K)$ und $\phi_2 : \Delta/\wp(A_K) \mapsto H$ die Abbildungen der Untergruppen wie in Lemma 2.46. Seien $\psi_2 : \Delta/\wp(A_K) \mapsto F$ und $\psi_1 : F \mapsto \Delta/\wp(A_K)$ die Abbildungen wie in Satz 2.43.

Sei $B \subseteq A$ beliebig. Wegen $K(B) = \mathcal{F}_{E/K}(G_B)$ gilt $\psi_2 = \mathcal{F}_{E/K} \circ \phi_2$. Wegen $G_B = \mathcal{G}_{L/K}(K(B))$ gilt $\phi_2 = \mathcal{G}_{E/K} \circ \psi_2$. Damit sind die Bilder von ϕ_2 abgeschlossene Untergruppen von $G(E/K)$. Aus Lemma 2.46, (*iii*) erhalten wir daher, daß $\psi_2 = \mathcal{F}_{E/K} \circ \phi_2$ die inverse Abbildung $\phi_1 \circ \mathcal{G}_{L/K}$ besitzt, also injektiv ist. Aus Lemma 2.46, (*i*) erhalten wir, daß $[K(\wp^{-1}(\Delta)) : K] = (\Delta : \wp(A_K))$ gilt. Nach Satz 2.41, (*ii*) ist ψ_1 die inverse Abbildung von ψ_2 und ψ_2 ist surjektiv.

Nach Lemma 2.46, (*iv*) und (*ii*) gilt $G(F/K) \cong \mathrm{Hom}(\Delta/\wp(A_K), \mu_\wp)$ und $\Delta/\wp(A_K) \cong \mathrm{Hom}_a(G(F/K), \mu_\wp)$. Für die zweite Isomorphie muß man noch beachten, daß der Kern H eines Elements in $\mathrm{Hom}_a(G(F/K), \mu_\wp)$ abgeschlossen ist und somit eine endliche, abelsche Erweiterung $L = \mathcal{F}_{F/K}(M)$ vom Exponenten n von K definiert. Da $\psi_2 = \mathcal{F}_{L/K} \circ \phi_2$ surjektiv und $\mathcal{F}_{F/K}$ auf der Menge der abgeschlossenen Untergruppen von $G(F/K)$ injektiv ist, gehört L zu einem Δ mit

$\phi_2(\Delta/\wp(A_K)) = H$. Außerdem ergibt sich, daß $\mathrm{Hom}_a(G(F/K), \mu_\wp)$ tatsächlich eine Gruppe ist. $\square$

Wählt man $K = \mathbb{Q}$, p_i die i-te Primzahl und $\Delta = \langle p_1, p_2, \ldots \rangle \mathbb{Q}^{\times 2}$, so gilt $\Delta/\mathbb{Q}^{\times 2} \cong \coprod_{i \in \mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ und $G(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots)/\mathbb{Q}) \cong \prod_{i \in \mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ nach der ersten Isomorphie in Satz 2.47. In diesem Fall dürfen für die zweite Isomorphie in Satz 2.47 wirklich nur Homomorphismen mit abgeschlossenen Kern betrachtet werden, wie das Beispiel nach Lemma 2.42 zeigt.

2.9 Auflösbarkeit durch Radikale

2.48 Definition. Eine endliche Körpererweiterung E/K heißt eine Radikalerweiterung, wenn es Körper E_i mit $K = E_0 \subseteq \cdots \subseteq E_m = E$ gibt, so daß E_{i+1}/E_i von der folgenden Gestalt ist.

(*i*) E_{i+1} entsteht aus E_i durch Adjunktion einer Einheitswurzel.

(*ii*) E_{i+1} entsteht aus E_i durch Adjunktion einer Nullstelle von $t^n - a$ für $a \in E_i$ und n teilerfremd zur Charakteristik.

(*iii*) E_{i+1} entsteht aus E_i durch Adjunktion einer Nullstelle von $t^p - t - a$ für $a \in E_i$ und $p = \mathrm{char}(K) > 0$.

Eine endliche Körpererweiterung F/K heißt durch Radikale auflösbar, wenn F ein Zwischenkörper einer Radikalerweiterung E/K ist.

In einer durch Radikale auflösbaren Erweiterung E/K läßt sich jedes Element als „Wurzelausdruck“ schreiben. Eine durch Radikale auflösbare Erweiterung E/K ist separabel. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß n in (*ii*) eine Primzahl ist.

Das folgende Lemma zeigt, daß sich die Eigenschaft „durch Radikale auflösbar“ analog zu den Eigenschaften „algebraisch“, „normal“ usw. verhält.

2.49 Lemma. *Die Erweiterung E/K ist genau dann durch Radikale auflösbar, wenn E/F und F/K für jeden Zwischenkörper F von E/K durch Radikale auflösbar ist.*

Sind E, L Zwischenkörper einer Erweiterung C/K und E/K durch Radikale auflösbar, so ist auch EL/L durch Radikale auflösbar.

Sind E_1, E_2 Zwischenkörper in C/K und über K durch Radikale auflösbar, so ist E_1E_2/K durch Radikale auflösbar.

Beweis. Folgt ziemlich direkt aus der Definition. $\square$

Sei E/K eine galoissche Radikalerweiterung mit $G = G(E(K), \mu_{\#G}(K^a) \subseteq K$, den Zwischenkörpern E_i wie oben und $G_i = \mathcal{G}_{E/K}(E_i)$. Dann gilt $G = G_0 \geq \cdots \geq G_m = \{1\}$. Die Erweiterungen E_{i+1}/E_i sind nach Korollar 2.45 zyklisch von Primzahlgrad, daher sind auch die G_{i+1} normal in G_i und $G_i/G_{i+1} \cong G(E_{i+1}/E_i)$ ist zyklisch mit Primzahlordnung $[E_{i+1} : E_i]$. Diese Eigenschaft nimmt man zum Anlaß der folgenden Definition.

Eine endliche Gruppe G heißt auflösbar, wenn es Untergruppen G_i gibt, so daß $G = G_0 \geq \cdots \geq G_m = \{1\}$, G_{i+1} normal in G_i und G_i/G_{i+1} zyklisch von Primzahlordnung ist. Die G_i heißen eine Kompositionsreihe von G.

2.50 Satz. *Sei G eine endliche Gruppe.*

(*i*) *Ist G auflösbar, so ist auch jede Untergruppen und jede Faktorgruppe von G auflösbar.*

(*ii*) *Ist $N \leq G$ ein Normalteiler und sind N und G/N auflösbar, so ist G auflösbar.*

(*iii*) *Abelsche Gruppen G und p-Gruppen G sind auflösbar.*

(*iv*) *Die alternierende Gruppe A_n ist auflösbar für $n \leq 4$ und ist nicht auflösbar für $n \geq 5$.*

Beweis. (*i*): Ist G_i eine Kompositionsreihe von G, so liefern $G_i \cap U$ und G_iN/N nach Auslassung von Wiederholungen Kompositionsreihen von U und G/N: Für $G_i \cap U$ gilt $G_0 \cap U = U$, $G_m \cap U = \{1\}$ und nach dem Homomorphiesatz gibt es einen Monomorphismus $(G_i \cap U)/(G_{i+1} \cap U) \to G_i/G_{i+1}$, so daß $(G_i \cap U)/(G_{i+1} \cap U)$ zyklisch von Primzahlordnung oder trivial ist. Für G_iN/N gilt $G_0N/N = G/N$, $G_mN/N = \{1\}$ und es gibt einen Epimorphismus $G_i/G_{i+1} \to (G_iN/N)/(G_{i+1}N/N)$, so daß $(G_iN/N)/(G_{i+1}N/N)$ abermals zyklisch von Primzahlordnung oder trivial ist. Den Epimorphimus erhalten wir wie folgt: Wir starten mit dem kanonischen Epimorphismus $G_i \to G_i/(G_i \cap N)$ und verlängern mit dem Isomorphismus aus dem ersten Isomorphiesatz zum Epimorphismus $G_i \to G_iN/N$. Diesen verlängern wir mit dem kanonischen Epimorphismus $G_iN/N \to (G_iN/N)/(G_{i+1}N/N)$ zum Epimorphismus $G_i \to (G_iN/N)/(G_{i+1}N/N)$. Der Kern umfaßt G_{i+1}, so daß wir nach dem Homomorphiesatz den Epimorphismus $G_i/G_{i+1} \to (G_iN/N)/(G_{i+1}N/N)$ erhalten.

(*ii*): Wir liften die Kompositionsreihe von G/N durch Urbildbildung unter dem kanonischen Epimorphimus $G \to G/N$ nach G und hängen die Kompositionsreihe von N an. Dies liefert eine Kompositionsreihe von G.

(*iii*): Die Aussage für abelsche Gruppen ist nach dem Hauptsatz für endlich erzeugte abelsche Gruppen klar. Für die Aussage für p-Gruppen G beachten wir, daß das Zentrum $Z(G)$ nicht-trivial ist. Induktiv ist dann $G/Z(G)$ als echt kleinere p-Gruppe und $Z(G)$ als abelsche Gruppe auflösbar. Nach (ii) ist damit G auflösbar.

(iv): Die Gruppen A_1, A_2 und A_3 sind zyklisch und daher auflösbar. Die Gruppe A_4 ist nach den Sylowsätzen semidirektes Produkt einer abelschen Gruppe der Ordnung 4 und einer abelschen Gruppe der Ordnung 3 und somit auflösbar (vgl. die Aufgabe aus der Algebra 1, es gilt $A_4 \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z})$. Die Gruppe A_5 ist nach einer Übung in der Algebra 1 einfach, aber nicht abelsch, und daher nicht auflösbar. □

Wegen $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ und Satz 2.50, (i) und (ii) gilt (iv) auch für S_n anstelle von A_n.

Nach dem Satz von Burnside sind alle endlichen Gruppen der Ordnung $p^a q^b$ mit Primzahlen p, q und $a, b \in \mathbb{Z}^{\geq 0}$ auflösbar. Nach dem Satz von Feit-Thompson sind alle endlichen Gruppen ungerader Ordnung auflösbar.

Durch Radikale auflösbare Erweiterungen lassen sich galoistheoretisch wie folgt klassifizieren.

2.51 Satz. *Eine endliche, separable Körpererweiterung F/K ist genau dann durch Radikale auflösbar, wenn die Galoisgruppe $G(F'/K)$ der normalen Hülle F' von F/K auflösbar ist.*

Beweis. „$\Rightarrow$“: Wir können F/K und F'/K in eine normale Radikalerweiterung E'/K wie folgt einbetten. Wir betrachten die beteiligten Körper als Teilkörper eines algebraischen Abschluß C. Sei E/K eine Radikalerweiterung mit $F \subseteq E$. Für die normale Hülle E' von E gilt $E' = \coprod_{\sigma \in \mathrm{Hom}_K(E,C)} \sigma(E)$, und mit jedem $\sigma(E)/K$ ist auch E'/K eine Radikalerweiterung. Also ist E'/K eine galoissche Radikalerweiterung mit $F' \subseteq E'$. Wir werden zeigen, daß $G(E'/K)$ auflösbar ist. Da $G(F'/K) \cong G(E'/K)/G(E'/F')$ gilt, ist $G(F'/K)$ als Faktorgruppe einer auflösbaren Gruppe auflösbar.

Sei n der zu $\mathrm{char}(K)$ teilerfremde Faktor von $[E' : K]$ und $L = K(\mu_n)$. Dann ist $E'L/L$ ebenfalls eine normale Radikalerweiterung. Durch mehrfache Anwendung von Korollar 2.45 ersehen wir, daß $E'L/L$ durch einen Turm von zyklischen Erweiterungen mit Primzahlgraden entsteht. Also ist $G(E'L/L)$ auflösbar. Weiter ist L/K zyklisch und $E'L/K$ als Kompositum der Galoiserweiterungen L/K und E'/K selbst galoissch, so daß $G(E'L/K)$ den auflösbaren Normalteiler $G(E'L/L)$ und auflösbaren Quotienten $G(L/K) \cong G(E'L/K)/G(E'L/L)$ besitzt. Daher ist auch $G(E'L/K)$ auflösbar und es folgt, daß $G(E'/K)$ als Untergruppe auflösbar ist.

„$\Leftarrow$“: Sei n der zu $\mathrm{char}(K)$ teilerfremde Faktor von $[F' : K]$ und $L = K(\mu_n)$. Dann sind $G(F'/K)$ und $G(F'L/L)$ auflösbar. Daher entsteht $F'L/L$ durch einen

Turm von zyklischen Erweiterungen mit Primzahlgraden. Durch mehrfache Anwendung von Korollar 2.45 ersehen wir, daß jede dieser zyklischen Erweiterungen vom Typ (*ii*) oder Typ (*iii*) in Definition 2.48 ist und daß $F'L/L$ somit eine Radikalerweiterung ist. Weiter ist L/K eine Radikalerweiterung. Es folgt, daß $F'L/K$ eine Radikalerweiterung und F/K somit durch Radikale auflösbar ist. □

2.52 Definition. Sei $f \in K[t]$ normiert und separabel. Dann heißt f durch Radikale auflösbar, wenn der Zerfällungskörper von f über K durch Radikale auflösbar ist.

2.53 Korollar. *Ein normiertes und separables Polynom $f \in K[t]$ ist genau dann durch Radikale auflösbar, wenn $G(f, K)$ auflösbar ist.*

Ist f durch Radikale auflösbar und gilt bei positiver Charakteristik $\mathrm{char}(K) \nmid \#G(f, K)$, so können die Nullstellen von f als echte, geschachtelte Wurzelausdrücke dargestellt werden.

Für quadratische Polynome $t^2 + pt + q$ erhält man die Nullstellen in der Form $-p/2 \pm \sqrt{p^2/4 - q}$. Gibt es solche Formeln in den Koeffizienten von f auch für höhere Polynomgrade? Hierzu betrachten wir die Auflösbarkeit des allgemeinen Polynoms n-ten Grads durch Radikale.

2.54 Satz. *Sei k ein Körper und $K = k(a_1, \ldots, a_n)$ rationaler Funktionenkörper in den Variablen a_i über K. Das allgemeine Polynom $f = \sum_{i=0}^{n} a_i t^i \in K[t]$ vom Grad n ist für $n \geq 5$ nicht durch Radikale auflösbar.*

Sei K ein beliebiger Körper. Jedes normierte und separable Polynom $f \in K[t]$ vom Grad $n \leq 4$ ist durch Radikale auflösbar.

Beweis. Es gilt $G(f, K) \cong S_n$ nach Satz 2.28. Nach Satz 2.50, (*iv*) wissen wir, daß S_n für $n \leq 4$, aber nicht für $n \geq 5$ auflösbar ist. Der Rest ergibt sich aus Korollar 2.53. □

Die Formeln für $n = 3$ und $n = 4$ sind für Rechnungen mit der Hand im übrigen verhältnismäßig unangenehm.

Die Auflösung von Polynomen durch Radikale spielt in der Robotik eine Rolle. Hier wird versucht, die Lösungen von Bewegungsgleichungen zur Robotersteuerung durch Radikale schneller als mit allgemeinen Methoden zu berechnen.

Kapitel 3

Anwendungen in der Kryptographie

Wir wollen kurz auf ein paar einfache Anwendungen der bisher behandelten Theorie in der Kryptographie eingehen.

3.1 Zielsetzung der Kryptographie

Die Kryptographie beschäftigt sich mit der sicheren Informationsübertragung im weiteren Sinne zwischen logischen Einheiten. Solche logischen Einheiten können zum Beispiel Personen oder Computer sein. Eine der grundlegenden und namensgebenden Fragestellungen ist, wie zwei Personen Informationen austauschen können, ohne das eine mithörende dritte Person diese Informationen erhalten kann. Dabei geht es nicht darum, wie man das Mithören der dritten Person verhindern kann, sondern wie sich die kommunizierenden Personen zu verhalten haben, so daß das Mithören ergebnislos bleibt.

Die zwei wichtigsten Fragestellungen der Kryptographie sind etwa

1. Verschlüsselung. Nur der rechtmäßige Empfänger soll das Verschlüsselte entschlüsseln bzw. überhaupt nur irgendwelche Informationen erhalten können.

2. Unterschriften. Alle Personen sollen die Unterschrift einer Person verifizieren, aber niemand soll sie fälschen können.

Darüberhinaus gibt es eine ganze Reihe weiterer Fragestellungen wie zum Beispiel den Austausch von Geheimnissen (Schlüsselaustausch), Authentifizierung, Datenintegrität, Unleugbarkeit usw.

Die Kryptographie befaßt sich heute im wesentlichen mit Algorithmen, Computern und der digitalen Kommunikation und ist ein eigenständiges, interdisziplinäres Gebiet mit Verbindungen zur theoretischen Informatik, Mathematik, Software Engineering, Elektrotechnik, Quantenphysik.

3.2 Fachliche Unterteilung

Die Gebiete der Kryptographie unterteilen sich grob wie folgt.

Theoretische Grundlagen aus der Informatik Hierzu gehören neben anderem Informationstheorie und Fragen nach der Existenz von Einwegfunktionen und Zero-Knowledge Beweisen.

Symmetrische Kryptoverfahren Dies sind spezielle Verfahren zur Verschlüsselung (Block- und Stromchiffren), bei denen man davon ausgeht, daß die kommunizierenden Personen sich einen geheimen Schlüssel teilen. Ein Schlüssel ist einfach eine digitale Information. Die Untersuchung der Sicherheit dieser Verfahren basiert mehr oder weniger auf statistischen Methoden und ist im wesentlichen heuristisch. Symmetrische Kryptoverfahren sind im allgemeinen effizienter als die asymmetrischen Kryptoverfahren.

Asymmetrische Kryptoverfahren Hier sind jeder Person ein öffentlicher (allen Personen bekannter) und ein geheimer Schlüssel zugeordnet. Darauf aufbauend betreibt man dann Verfahren zur Verschlüsselung, zum Unterschreiben und zum Schlüsselaustausch geheimer Schlüssel für symmetrische Kryptoverfahren. Die Untersuchung der Sicherheit dieser Verfahren basiert im wesentlichen auf der Reduktion zu algorithmischen Problemen aus der Mathematik mit hoher Komplexität. Entsprechend geht bei asymmetrischen Kryptoverfahren die meiste Mathematik und besonders die algebraische Zahlentheorie ein. Die asymmetrische Kryptographie wurde 1976 von Diffie und Hellman erfunden.

Technische Fragestellungen Hier untersucht man, inwieweit die verwendeten Geräte auch physikalisch sicher sind. Zum Beispiel kann man aus Stromverbrauch, elektromagnetischer Abstrahlung oder Öffnen der Geräte unauthorisierten Zugang zu Informationen erhalten. Eine andere Disziplin ist die Untersuchung biometrischer Verfahren (z.B. Identifikation durch Fingerabdruck oder Iris).

3.3 Asymmetrische Kryptoverfahren

Die grundlegende Vorgehensweise bei den asymmetrischen Kryptosystemen ist wie folgt. Wir betrachten die Personen Alice und Bob. Alice hat einen öffentlichen und einen geheimen Schlüssel. Wenn Bob Alice eine geheime Nachricht schicken möchte, verwendet er einen geeigneten Algorithmus $\mathcal{E}$, der als Eingabe die Nachricht und den öffentlichen Schlüssel von Alice erwartet und als Ausgabe die verschlüsselte Nachricht liefert. Bob schickt diese Nachricht an Alice. Mithilfe eines zu $\mathcal{E}$ passenden Entschlüsselungsalgorithmus $\mathcal{D}$ kann Alice unter Eingabe der verschlüsselten Nachricht und ihres geheimen Schlüssels die ursprüngliche Nachricht berechnen.

Beim Unterschreiben wird wie folgt vorgegangen. Alice verwendet einen Signaturalgorithmus $\mathcal{S}$, welcher nach Eingabe des zu unterschreibenden Texts und des geheimen Schlüssels von Alice eine Unterschrift zurückliefert. Mithilfe eines passenden Verifikationsalgorithmus $\mathcal{V}$ und nach Eingabe der Unterschrift und des öffentlichen Schlüssels von Alice verifiziert Bob dann die Unterschrift.

Zum Schlüsselaustausch schließlich benötigt Bob ebenfalls einen öffentlichen und geheimen Schlüssel. Man verwendet dann einen Algorithmus $\mathcal{K}$, welcher denselben Wert nach Eingabe von Alice's geheimen Schlüssel und Bob's öffentlichem Schlüssel und nach Eingabe von Alice's öffentlichem Schlüssel und Bob's geheimen Schlüssel zurückliefert. Alice und Bob tauschen ihre öffentlichen Schlüssel aus und benutzen $\mathcal{K}$, um ein gemeinsames Geheimnis zu berechnen.

Im allen Fällen soll die Kenntnis des geheimen Schlüssels unbedingt erforderlich sein, um Nachrichten zu entschlüsseln, Unterschriften zu fälschen bzw. das gemeinsame Geheimnis zu berechnen (dies ist nicht ganz richtig, zumindest soll es möglich sein, einen erfolgreichen Angreifer zur Lösung eines schwierigen mathematischen Problems zu verwenden). Es wird nicht angenommen, daß die verwendeten Algorithmen $\mathcal{E}$, $\mathcal{D}$, $\mathcal{S}$, $\mathcal{V}$ und $\mathcal{K}$ geheim sind.

Nun stellt sich die Frage, ob solche Algorithmen überhaupt realisiert werden können. Dies ist in der Tat der Fall, wenn verschiedene plausible Annahmen gemacht werden bzw. gewisse mathematische Berechnungsprobleme nur mit hohem algorithmischen Aufwand gelöst werden können. Ein solches Problem ist die Faktorisierung ganzer Zahlen. Das bekannteste, darauf beruhende asymmetrische Kryptoverfahren heißt RSA-Verfahren (nach den Entdeckern Rivest, Adleman, Shamir). Eine andere Klasse von asymmetrischen Kryptoverfahren beruht auf geeigneten endlichen, zyklischen Gruppen und dem diskreten Logarithmusproblem, auf die wir im folgenden eingehen.

3.4 Das diskrete Logarithmus Problem

3.1 Definition. Sei G eine endliche, abelsche Gruppe und $g, h \in G$. Eine Zahl $r \in \mathbb{Z}$ mit $h = g^r$ heißt diskreter Logarithmus von h zur Basis g. Das diskrete Logarithmus Problem (DLP) ist, zu vorgegebenen g, h den diskreten Logarithmus r berechnen, falls er existiert.

Es ist klar, daß r modulo der Ordnung von g bestimmt ist. Auch gibt es beispielsweise in der Gruppe $C_3 \times C_3$ keinen diskreten Logarithmus von $h = (1, 0)$ zur Basis $g = (0, 1)$.

Wir fassen die Komplexität des diskreten Logarithmus Problems als eine Funktion von $\log(\#G)$ auf, welche geeignete Grundoperationen (Gruppenoperationen, Bitoperationen) zählt. Diese Komplexität hängt wesentlich von der Gruppe G ab. Zum Beispiel nimmt das diskrete Logarithmus Problem in $G = \mathbb{F}_p^+$ die Form $h = rg$ an, und man muß nur $r = h/g$ berechnen. Das diskrete Logarithmus Problem in $G = \mathbb{F}_p^\times$ ist hingegen viel schwieriger. Wir sind daran interessiert, daß das diskrete Logarithmus Problem möglichst schwierig zu lösen ist.

Eine Black-Box Gruppe G ist eine Gruppe, die man sich als abstrakten Datentyp implementiert vorstellen kann. Es sollen speziell nur die Gruppenoperationen, der Zugriff auf das Einselement und die Auswahl unabhängig und gleichverteilt zufälliger Elemente aus G möglich bzw. zulässig sein. Ein Algorithmus für eine solche Gruppe darf bzw. kann also nur diese Funktionen verwenden.

3.2 Satz. *Sei G eine Black-Box Gruppe, p der größte Primteiler von $\#G$ und $g, h \in G$ unabhängig und gleichverteilt zufällig gewählte Elemente. Die Wahrscheinlichkeit, den diskreten Logarithmus von h zur Basis g mit m Gruppenoperationen zu lösen, ist $\tilde{\Theta}(m^2/p)$.*

Für Black-Box Gruppen von Primzahlordnung n ist die Komplexität des diskreten Logarithmus Problems $\Theta(\sqrt{n})$ und damit exponentiell in $\log(n)$. Wie gesehen, kann dies für speziell gegebene Gruppen auch polynomiell in $\log(n)$ sein. Die kryptographische Qualität einer Gruppe wird einerseits durch die Komplexität der Gruppenoperationen (soll möglichst niedrig sein) und die Komplexität des diskreten Logarithmus Problems (soll möglichst hoch sein) gegeben. Wir merken an, daß die Komplexität des diskreten Logarithmus Problems für die multiplikativen Gruppen von endlichen Körpern $\mathbb{F}_q^\times$ obere, subexponentielle Schranken der (ungefähren) Form $\exp(\log(n)^{1/2})$ und $\exp(\log(n)^{1/3})$ mit $n = q - 1$ existieren. Die Punktgruppen elliptischer Kurven über $\mathbb{F}_q$ sind komplexitätsweise im allgemeinen den Black-Box Gruppen gleichgestellt. Untere Schranken sind in beiden Fällen nicht bekannt.

Das diskrete Logarithmus Problem in nicht zyklischen Gruppen kann offensichtlich auf mehrere diskrete Logarithmus Probleme in den einzelnen zyklischen Faktoren zurückgeführt werden. Da das Verhältnis von Komplexität zu Gruppenordnung hier ungünstiger als bei zyklischen Gruppen ähnlich großer, primer Gruppenordnung ist, beschränken wir uns deshalb nur auf zyklische Gruppen mit Primzahlordnung.

3.5 DLP basierte Kryptoverfahren

Wir legen den Betrachtungen eine endliche, zyklische Gruppe G von Primzahlordnung n zugrunde. Mit g bezeichnen wir Erzeuger von G.

Die Teilnehmer Alice und Bob haben jeweils ein Schlüsselpaar (r_A, g_A) und (r_B, g_B), wobei $r_A, r_B \in \mathbb{Z}/n\mathbb{Z}$ die geheimen Schlüssel und $g_A = g^{r_A}$, $g_B = g^{r_B}$ die öffentlichen Schlüssel sind.

Die geheimen Schlüssel sind eindeutig durch die öffentlichen Schlüssel bestimmt und durch die (hohe) Komplexität des diskreten Logarithmus Problems geschützt.

Diffie-Hellman Schlüsselaustausch Alice und Bob tauschen ihre öffentlichen Schlüssel aus und berechnen unabhängig das gemeinsame Geheimnis $g_B^{r_A} = g^{r_B r_A}$ bzw. $g_A^{r_B} = g^{r_A r_B}$. Dies kann nun als Schlüssel für ein symmetrisches Kryptoverfahren benutzt werden. Der oben erwähnte Algorithmus $\mathcal{K}$ ist daher einfach $\mathcal{K}(x, y) = x^y$.

Will eine dritte Person Oscar das Geheimnis lüften, so muß sie im wesentlichen aus $g, g_A = g^{r_A}, g_B = g^{r_B}$ den Wert $g^{r_A r_B}$ berechnen.

3.3 Definition. Das Computational Diffie-Hellman Problem (CDH) ist, für g, g^a, g^b den Wert g^{ab} zu berechnen. Das Decision Diffie-Hellman Problem (DDH) ist, für g, g^a, g^b, h zu entscheiden, ob $h = g^{ab}$ gilt.

Können wir das DLP lösen, so auch das CDP. Können wir das CDP lösen, so auch das DDH. Über die Umkehrungen weiß man nur etwas in speziellen Fällen. Ist das CDP leicht, so muß der beschriebene Schlüsselaustausch als unsicher angesehen werden.

ElGamal Verschlüsselung Bob will eine Nachricht m an Alice schicken. Dabei wird m als geeignetes Gruppenelement von G aufgefaßt. Der Verschlüsselungsalgorithmus $\mathcal{E}$ berechnet dann für m und den öffentlichen Schlüssel g_A ein gleichverteilt zufälliges $r \in \mathbb{Z}/n\mathbb{Z}$ und liefert die verschlüsselte Nachricht (g^r, mg_A^r) zurück. Alice verwendet den Entschlüsselungsalgorithmus $\mathcal{D}$, welcher für die verschlüsselte Nachricht (u, v) und den geheimen Schlüssel r_A den Wert $v/u^{r_A} = m(g^{r_A})^r/(g^r)^{r_A} = m$ berechnet.

Schnorr Signatur Alice will einen Text $m \in G$ unterschreiben. Hier benötigt man noch eine geeignete Hilfsfunktion $H : G \times G \to \mathbb{Z}/n\mathbb{Z}$. Der Signaturalgorithmus $\mathcal{S}$ wählt ein gleichverteilt zufälliges $k \in \mathbb{Z}/n\mathbb{Z}$ und berechnet $r = g^k$, $u = r_A H(m, r) + k$. Die Unterschrift ist $(u, H(m, r))$. Bob verwendet zur Verifikation der Unterschrift (s, t) den Algorithmus $\mathcal{V}$. Dieser berechnet $r = g^u/g_A^t$

und akzeptiert genau dann, wenn $t = H(m,r)$. Annahmen an H sind, daß keine verschiedenen Argumente mit gleichem Bild und keine Urbilder berechnet werden können.

In einem geeigneten Sicherheitsmodell und unter gewissen Annahmen wird die Sicherheit von ElGamal Verschlüsselung und Schnorr Signaturen auf das DDH bzw. DLP zurückgeführt. Der Begriff der Sicherheit ist jedoch recht delikat und insbesondere stark vom betrachteten Sicherheitsmodell abhängig. Die Theorie ist im übrigen nicht sehr „stetig“, kleine Änderungen oder Fehler bewirken häufig, daß ein Verfahren vollkommen unbrauchbar wird.

3.6 XTR Kryptosystem

Das Akronym „XTR“ steht für „ECSTR“ beziehungsweise „Efficient and Compact Subgroup Trace Representation“. Die Hauptmotivation hinter XTR ist, $G = \mathbb{F}_q^\times$ auf möglichst effiziente und trickreiche Weise zu verwenden. Genauer betrachtet man eine besonders geeignete Untergruppe G von $\mathbb{F}_{p^6}^\times$ für eine Primzahl p. Im folgenden verwenden wir die Bezeichnungen $E = \mathbb{F}_{p^6}$, $F = \mathbb{F}_{p^2}$ und $K = \mathbb{F}_p$.

3.4 Lemma. *Die Gruppe $E^\times$ enthält genau eine Untergruppe G der Ordnung p^2-p+1. Die Gruppe G stimmt mit der Gruppe all derjeningen Elemente $x \in E^\times$ überein, für die $\mathrm{N}_{E/F}(x) = 1$ für alle echten Teilkörper F von E gilt.*

Beweis. Es gilt $p^6 - 1 = (p-1)(p+1)(p^2-p+1)(p^2+p+1)$. Daher existiert genau eine Untergruppe G von $E^\times$ mit Ordnung $p^2 - p + 1$. Es gilt $\mathrm{N}_{E/F}(x) = x^{(p^6-1)/(p^{[F:K]}-1)}$, wobei der Exponent eine ganze Zahl ist, die durch $p^2 - p + 1$ teilbar ist. Genauer ist p^2-p+1 gleich dem ggT dieser Exponenten für alle echten Teilkörper F von E. Daraus folgt die behauptete Charakterisierung von G. $\square$

Ein diskretes Logarithmus Problem in G kann mit der Norm nicht auf ein äquivalentes diskretes Logarithmus Problem in der multiplikativen Gruppe eines der echten Teilkörper von E abgebildet werden. Darüberhinaus wählt man p so, daß $p^2 - p + 1$ einen großen Primfaktor q enthält. Dieser tritt nicht in $p^3 - 1$ und $p^2 - 1$ auf. Daher kann ein diskretes Logarithmusproblem auch nicht auf irgendeine andere Weise in die multiplikative Gruppe eines der echten Teilkörper von E abgebildet werden.

3.5 Lemma. *Für jedes $x \in G$ sind die Konjugierten von x über F gleich x, x^{p-1}, x^{-p} und es gilt $m_{x,F}(t) = t^3 - \mathrm{Tr}_{E/K}(x)t^2 + \mathrm{Tr}_{E/K}(x)^p t - 1$. Es gibt also eine Bijektion der Konjugationsklassen $\{x, x^{p^2}, x^{p^4}\}$ und der Spuren $\mathrm{Tr}_{E/K}(x)$.*

Beweis. Die Konjugierten von $x \in G$ sind $x^{p^2} = x^{p-1}$ und $x^{p^4} = 1/(xx^{p-1}) = x^{-p}$. Der negierte Koeffizient von t in $m_{x,F}(t)$ ist damit gleich $xx^{p-1}+xx^{-p}+x^{p-1}x^{-p} = x^p + x^{-p^2} + x^{p^2-p} = \mathrm{Tr}_{E/K}(x)^p$. □

Kommt es uns nur auf die Konjugationsklasse eines Elements aus G an, so können wir diese durch die Spur des Elements darstellen. Wir können also $(p^2 - p+1)/3$ Konjugationsklassen durch ein Drittel des Speicherbedarfs darstellen, den die $p^2 - p + 1$ Elemente aus G benötigen. Dies ist sehr vorteilhaft. Ein Problem jedoch ist, wie Konjugationsklassen multipliziert oder potenziert werden sollen. Wir bemerken, daß durch elementweise Multiplikation keine eindeutig bestimmte Konjugationsklasse erhalten werden kann. Dies ist aber beim Potenzieren möglich. Wir entwickeln nun Formeln, so daß man nur mit den Spuren selbst zu rechnen braucht.

3.6 Lemma. *Für $x \in G$ gilt.*

(*i*) $\mathrm{Tr}_{E/F}(x^{n+m}) = \mathrm{Tr}_{E/F}(x^n)\mathrm{Tr}_{E/F}(x^m) - \mathrm{Tr}_{E/F}(x^n)^p\mathrm{Tr}_{E/F}(x^{m-n})+ \mathrm{Tr}_{E/F}(x^{m-2n})$.

(*ii*) $\mathrm{Tr}_{E/F}(x^{2n}) = \mathrm{Tr}_{E/F}(x^n)^2 - 2\mathrm{Tr}_{E/F}(x^n)^p$.

(*iii*) $\mathrm{Tr}_{E/F}(x^{n+2}) = \mathrm{Tr}_{E/F}(x)\mathrm{Tr}_{E/F}(x^{n+1}) + \mathrm{Tr}_{E/F}(x)^p\mathrm{Tr}_{E/F}(x^n) + \mathrm{Tr}_{E/F}(x^{n-1})$.

(*iv*) $\mathrm{Tr}_{E/F}(x^{2n-1}) = \mathrm{Tr}_{E/F}(x^n)\mathrm{Tr}_{E/F}(x^{n-1})+\mathrm{Tr}_{E/F}(x^n)^p\mathrm{Tr}_{E/F}(x)^p+\mathrm{Tr}_{E/F}(x^{n+1})^p$.

(*iv*) $\mathrm{Tr}_{E/F}(x^{2n+1}) = \mathrm{Tr}_{E/F}(x^n)\mathrm{Tr}_{E/F}(x^{n+1})+\mathrm{Tr}_{E/F}(x^n)^p\mathrm{Tr}_{E/F}(x)+\mathrm{Tr}_{E/F}(x^{n-1})^p$.

Beweis. (*i*): Aus $m_{x^n,F}(x^n) = 0$ folgt $x^{3n} = \mathrm{Tr}_{E/F}(x^n)x^{2n} - \mathrm{Tr}_{E/F}(x^n)x^n + 1$. Muliplizieren mit x^{m-2n} ergibt $x^{n+m} = \mathrm{Tr}_{E/F}(x^n)x^m - \mathrm{Tr}_{E/F}(x^n)^p x^{m-n} + x^{m-2n}$. Durch Anwenden von $\mathrm{Tr}_{E/F}$ folgt die Aussage.

(*ii*) – (*iv*): Folgen aus (*i*) und $\mathrm{Tr}_{E/F}(x^{-1}) = \mathrm{Tr}_{E/F}(x)^p$. □

Ohne Beweis merken wir an, daß $\mathrm{Tr}_{E/F}(x^n)$ mit Hilfe des Lemmas effizient und nur durch Rechnungen in $F = \mathbb{F}_{p^2}$ aus $\mathrm{Tr}_{E/F}(x)$ bestimmt werden kann. Dabei verwendet man im übrigen auch eine Normalbasis von F/K. Etwas komplizierter, aber trotzdem möglich ist die Berechnung von Ausdrücken der Form $\mathrm{Tr}(x^m x^{kn})$ ausgehend von n, m, $\mathrm{Tr}_{E/F}(x)$ und $\mathrm{Tr}_{E/F}(x^k)$ für ein geheimes k.

Anstelle mit $x \in G$ zu rechnen, benutzt XTR nur die Elemente $\mathrm{Tr}_{E/K}(x)$, wodurch G wie oben bemerkt in Dreierklassen zusammengefaßt wird. Dies bewirkt eine Speicherersparnis vom Faktor 3 und zusätzlich eine höhere Rechengeschwindigkeit.

Der Diffie-Hellman Schlüsselaustausch kann dann wie beschrieben durchgeführt werden. Für die ElGamal Verschlüsselung ist eine Adaption notwendig, da aus

$\mathrm{Tr}(g)$ und $\mathrm{Tr}(h)$ nicht ohne weiteres $\mathrm{Tr}(gh)$ ausgerechnet werden kann. Der Wert $v = mg_A^r$ wird einfach durch den Wert $v = \mathcal{E}'(k, g_A^r)$ ersetzt, wobei $\mathcal{E}'$ ein symmetrisches Verschlüsselungsverfahren bezeichnet. Die Entschlüsselung findet dann durch $m = \mathcal{D}'(v, u^{r_A})$ statt. Unterschriften können in einem ähnlichen Hybridverfahren erzeugt werden, jedoch geht hier kein Weg daran vorbei, Ausdrücke der Form $\mathrm{Tr}(x^m x^{kn})$ wie oben auszurechnen.

Um ein gegenwärtig sicheres System zu bekommen, müssen die Primzahl p und der große Primfaktor q von $\#G = p^2 - p + 1$ mindestens 170 Bit bzw. 52 Dezimalstellen haben (entspricht grob einem RSA 1024 Bit Modul). Das XTR Kryptosystem ist patentiert (Citibank).

Kapitel 4

Transzendente Körpererweiterungen

In diesem Kapitel betrachten wir Körpererweiterungen E/K, in denen nicht alle Elemente algebraisch über K sind, welche also transzendente Elemente enthalten. Nach der Diskussion von Transzendenzbasen besprechen wir die Eigenschaften „separabel“ und „regulär“ für beliebige Körpererweiterungen nur sehr knapp.

4.1 Transzendenzbasen

Die Begriffe dieses Abschnitts verhalten sich ganz analog zu den Begriffen „linear unabhängig“ und „Basis“ aus der linearen Algebra.

4.1 Definition. Sei E/K eine Körpererweiterung. Eine Menge $A \subseteq E$ heißt algebraisch unabhängig über K, wenn für alle endlichen Teilmengen $\{a_1, \ldots, a_n\}$ von A und alle $f \in K[x_1, \ldots, x_n]$ aus $f(a_1, \ldots, a_n) = 0$ bereits $f = 0$ folgt.

Wir fassen die leere Menge $A = \{\}$ als algebraisch unabhängig über K auf. „Algebraisch abhängig“ bedeutet „nicht algebraisch unabhängig“.

4.2 Lemma. *Sei E/K eine Körpererweiterung und $A \subseteq E$.*

(i) *Sei $X_A = \{x_a \,|\, a \in A\}$ eine Menge von Unbekannten und $K[X_A]$ der zugehörige Polynomring. Die Menge A ist genau dann algebraisch unabhängig über K, wenn der Einsetzhomomorphismus $\phi_A : K[X_A] \to K[A]$, $x_a \mapsto a$ injektiv ist.*

(ii) *Ist $A \subseteq E$ algebraisch unabhängig über K und $b \in E \backslash A$, so ist $A \cup \{b\}$ genau dann algebraisch abhängig über K, wenn b im algebraischen Abschluß von $K(A)$ in E liegt.*

Beweis. Teil (i) ist nur eine Umformulierung der Definition. Für Teil (ii) betrachtet man das Minimalpolynom von x über $K(A)$ und multipliziert Nenner heraus, um eine algebraische Relation in $K[A, x]$ zu erhalten. □

Die Elemente einer algebraisch unabhängigen Menge können also nach Lemma 4.2, (i) als Variablen aufgefaßt werden.

4.3 Definition. Sei E/K eine Körpererweiterung. Eine Menge $A \subseteq E$ heißt Transzendenzbasis von E über K bzw. von E/K, wenn A algebraisch unabhängig über K ist und E gleich dem algebraischen Abschluß von $K(A)$ in E ist.

4.4 Satz. *Sei E/K eine Körpererweiterung, $A \subseteq E$ algebraisch unabhängig über K und $C \subseteq E$ mit $E/K(C)$ algebraisch. Dann gibt es eine Transzendenzbasis B von E/K mit $A \subseteq B \subseteq C$.*

Alle Transzendenzbasen von E/K haben die gleiche Kardinalität.

Beweis. Eine über K algebraisch unabhängige Teilmenge B von E mit $A \subseteq B \subseteq C$ ist genau dann eine Transzendenzbasis von E über K, wenn für jedes $x \in C \backslash B$ die Menge $B \cup \{x\}$ algebraisch abhängig über K ist, also wenn B maximal in C bezüglich Inklusion mit der Eigenschaft „algebraisch unabhängig über K“ ist: Sei B eine solche Transzendenzbasis und $x \in C \backslash B$. Dann ist $B \cup \{x\}$ nach Lemma 4.2, (ii) algebraisch abhängig über K. Sei umgekehrt B maximal algebraisch unabhängig über K in C und $x \in C \backslash B$. Dann ist $B \cup \{x\}$ algebraisch abhängig über K und nach Lemma 4.2, (ii) ist x algebraisch über $K(B)$. Daher ist die Erweiterung $K(C)/K(B)$ algebraisch. Mit $E/K(C)$ ist dann auch $E/K(B)$ algebraisch und B eine Transzendenzbasis von E über K.

Die Menge der über K algebraisch unabhängigen Teilmengen B von E mit $A \subseteq B \subseteq C$ ist bezüglich Inklusion induktiv geordnet. Nach dem Zornschen Lemma existiert eine maximale solche Teilmenge B, die nach der Vorbemerkung eine Transzendenzbasis bildet.

Zum Beweis über die Gleichheit der Kardinalität nehmen wir zunächst an, daß B eine endliche Transzendenzbasis von E/K ist und setzen $n = \#B$. Sei C eine weitere Transzendenzbasis von E/K mit $m = \#C$ und $m \geq n$. Wir schreiben $B = \{b_1, \ldots, b_n\}$ und $C = \{c_j \,|\, j \in J\}$. Für beliebiges j gibt es ein i, so daß wir b_i durch c_j austauschen können und die resultierende Menge B' eine Transzendenzbasis bleibt: Nach Voraussetzung gibt es ein Polynom $f \neq 0$ über K mit $f(c_j, b_1, \ldots, b_n) = 0$. Da c_j algebraisch unabhängig über K ist, gibt ein i, so daß $f(c_j, b_1, \ldots, b_n) = \sum_\nu g_\nu(c_j, b_1, \ldots, \hat{b_i}, \ldots, b_n) b_i^\nu = 0$ mit $g_\nu(c_j, b_1, \ldots, \hat{b_i}, \ldots, b_n) \neq 0$ für ein $\nu \geq 1$ ist. Damit ist b_i algebraisch über $K(B')$ für $B' = \{c_j, b_1, \ldots, \hat{b_i}, \ldots, b_n\}$. Mit b_i ist dann auch c_j nicht algebraisch über $K(b_1, \ldots, \hat{b_i}, \ldots, b_n)$ und B' somit eine Transzendenzbasis von E/K.

Durch mehrfache Anwendung der Austauschprozedur erhalten wir, daß C eine Transzendenzbasis B' der Kardinalität n enthält. Es folgt $C = B'$ und $n = m$.

Sind nun B und C unendliche Transzendenzbasen von E/K, so gibt es für jedes $a \in C$ eine endliche Teilmenge $B_a \subseteq B$, so daß a algebraisch über $K(B_a)$ ist. Es folgt $B = \cup_{a \in C} B_a$. Damit ist die Mächtigkeit von B kleiner gleich der Mächtigkeit von C. Dies gilt auch umgekehrt, und B und C besitzen damit die gleiche Mächtigkeit. □

4.5 Definition. Der Transzendenzgrad $\operatorname{trdeg}(E/K)$ einer Körpererweiterung E/K ist die Kardinalität $\#B$ einer Transzendenzbasis B von E/K.

Eine Körpererweiterung E/K heißt rein transzendent, wenn $E = K(B)$ für eine Transzendenzbasis B von E/K gilt.

Eine rein transzendente Erweiterung E/K kann nach Lemma 4.2, (i) als rationaler Funktionenkörper aufgefaßt werden. Wir halten nochmal fest, daß sich jede Körpererweiterung E/K schreiben läßt als eine algebraische Erweiterung E/F eines Zwischenkörpers F von E/K, welcher rein transzendent über K ist.

4.6 Satz. *Sei E/K eine Körpererweiterung und F ein Zwischenkörper. Für Transzendenzbasen B von F/K und B' von E/F gilt $B \cap B' = \{\}$ und $B \cup B'$ ist eine Transzendenzbasis von E/K. Ferner gilt* $\operatorname{trdeg}(E/K) = \operatorname{trdeg}(E/F) + \operatorname{trdeg}(F/K)$.

Beweis. Übung. □

4.7 Korollar. *Sei E/K eine Körpererweiterung, F ein über K rein transzendenter Zwischenkörper von E/K und L ein über K algebraischer Zwischenkörper von E/K. Dann sind F/K und L/K linear disjunkt und FL ist rein transzendent über L. Ist X eine Transzendenzbasis von F über K, so ist X auch eine Transzendenzbasis von FL über L.*

Beweis. Übung. □

Die folgende Definition verwendet algebraische Unabhängigkeit analog wie die Definition von „linear disjunkt“ die lineare Unabhängigkeit benutzt.

4.8 Definition. Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper von E/K. Dann heißen F_1/K und F_2/K algebraisch disjunkt (frei) und F_1 und F_2 algebraisch disjunkt (frei) über K, wenn jede über K algebraisch unabhängige Menge von Elementen von F_1 über F_2 algebraisch unabhängig bleibt.

Es gilt der zu Satz 1.22 analoge Satz. Insbesondere ist die Definition eigentlich symmetrisch. Linear disjunkte Erweiterungen sind auch algebraisch disjunkt. Algebraisch disjunkte Erweiterungen müssen jedoch nicht unbedingt linear disjunkt sein.

4.2 Separable Erweiterungen

In diesem Abschnitt wird die Eigenschaft „separabel“ von algebraischen auf beliebige Körpererweiterungen verallgemeinert. Wir gehen jedoch nur kurz auf die Eigenschaften ein und lassen die Behandlung von Derivationen aus.

4.9 Definition. Eine Transzendenzbasis A der Körpererweiterung E/K heißt separierend, wenn $E/K(A)$ separabel ist. Eine Körpererweiterung E/K heißt separabel erzeugt, wenn sie eine separierende Transzendenzbasis besitzt. Eine Körpererweiterung E/K heißt separabel, wenn für jeden über K endlich erzeugten Zwischenkörper F von E/K die Erweiterung F/K separabel erzeugt ist.

Es ist klar, daß diese Definition für algebraische Erweiterungen E/K mit der bisherigen Definition übereinstimmt. Wir werden dann wieder für verschiedene Körperkonstruktionen zeigen, wie sich die Eigenschaft separabel fortpflanzt. Die Verhältnisse sind aber nicht ganz analog zum Fall algebraischer Erweiterungen.

Mit $K^{p^{-\infty}}$ wird wieder der rein inseparable Abschluß von K für $p = \mathrm{char}(K)$ bezeichnet. Hat K die Charakteristik Null, so soll $K^{p^{-\infty}} = K$ gelten.

4.10 Satz. *Sei E/K eine Körpererweiterung. Dann sind äquivalent.*

(*i*) *E/K ist separabel.*

(*ii*) *E/K und $K^{p^{-\infty}}/K$ sind linear disjunkt.*

Beweis. Für den Fall $p = 0$ ist die Aussage klar. Es gelte also $p > 0$.

$(i) \Rightarrow (ii)$: Aussage (ii) gilt genau dann, wenn für alle endlich erzeugten Zwischenkörper F von E/K die Erweiterungen F/K und $K^{p^{-\infty}}/K$ linear disjunkt sind. Sei also F ein endlich erzeugter Zwischenkörper von E/K. Da E/K separabel ist, besitzt F/K nach Satz 4.4 eine endliche Transzendenzbasis B, so daß die Erweiterung $F/K(B)$ algebraisch und separabel ist. Da $K^{p^{-\infty}}/K$ algebraisch ist, sind $K(B)/K$ und $K^{p^{-\infty}}/K$ nach Korollar 4.7 linear unabhängig. Da $F/K(B)$ algebraisch und separabel und da $K(B)K^{p^{-\infty}}/K(B)$ nach Satz 1.64 rein inseparabel ist, sind $F/K(B)$ und $K(B)K^{p^{-\infty}}/K(B)$ nach Satz 1.72 linear disjunkt. Nach dem Satz über lineare Disjunktheit in Türmen (Übung) ergibt sich, daß F/K und $K^{p^{-\infty}}/K$ linear disjunkt sind.

$(ii) \Rightarrow (i)$: Sei F ein über K endlich erzeugter Zwischenkörper von E/K und $B = \{b_1, \ldots, b_n\}$ ein endliches Erzeugendensystem von F über K. Es gilt also $F = K(B)$. Wir zeigen, daß es eine Teilmenge von B gibt, die eine separierende Transzendenzbasis von F/K bildet. Falls die b_i algebraisch unabhängig über K sind, ist B bereits eine separierende Transzendenzbasis. Andernfalls gibt es ein $f \in K[x_1, \ldots, x_n]$ von minimalem Grad ≥ 1 mit $f(b_1, \ldots, b_n) = 0$. Wegen der Minimalität des Grads ist f irreduzibel.

Wir behaupten, daß f in mindestens einer Variablen x_i separabel ist. Sei dazu $f = \sum_i \lambda_i f_i$ mit Monomen $f_i \in K[x_1, \ldots, x_n]$ und $\lambda_i \in K$. Ist f in keiner Variablen separabel, gibt es wegen der Irreduzibilität von f Monome $g_i \in K[x_1, \ldots, x_n]$ mit $f_i = g_i^p$. Dann gilt $f(b_1, \ldots, b_n)^{1/p} = \sum_i \lambda_i^{1/p} g_i(b_1, \ldots, b_n) = 0$ und die $g_i(b_1, \ldots, b_n)$ sind linear abhängig über $K^{p^{-\infty}}$. Wegen (ii) müssen die $g_i(b_1, \ldots, b_n)$ dann auch linear abhängig über K sein, also muß $g(b_1, \ldots, b_n) = 0$ mit einem $g = \sum_i \mu_i g_i$ und $\mu_i \in K$ gelten. Dies führt zu einem Widerspruch zur Gradminimalität von f. Also gilt die Behauptung.

Sei f ohne Einschränkung in der Variablen x_n separabel. Dann ist die Erweiterung $F/K(b_1, \ldots, b_{n-1})$ algebraisch und separabel. Induktiv erhalten wir eine separierende Transzendenzbasis $B' = \{x_1, \ldots, x_r\}$ mit $r \geq 0$. □

Nach Satz 4.10 können wir (ii) auch als Definition von „separabel" nehmen. Dies hat den hübschen Aspekt, daß es die beiden, nun etwas technisch anmutenden Definitionen von „separabel" vereinheitlicht.

4.11 Satz. *Sei E/K eine Körpererweiterung.*

(i) *Ist E/K separabel und B ein endliches Erzeugendensystem von E/K, so gibt es eine separierende Transzendenzbasis A mit $A \subseteq B$.*

(ii) *Ist E/K separabel erzeugt, so ist E/K separabel.*

(iii) *Ist K vollkommen, so ist E/K separabel.*

(iv) *Ist E/K separabel und F ein Zwischenkörper von E/K, so ist F/K separabel.*

(v) *Ist F ein Zwischenkörper von E/K und sind E/F und F/K separabel, so ist E/K separabel.*

(vi) *Sind F und L über K algebraisch disjunkte Zwischenkörper von E/K und ist F/K separabel, so ist auch FL/L separabel.*

(vii) *Sind F und L über K linear disjunkte Zwischenkörper von E/K und ist FL/L separabel, so ist auch F/K separabel.*

Beweis. (i): Folgt aus dem Beweis von Satz 4.10.

(ii): Aussage (ii) aus Satz 4.10 folgt aus der Annahme analog wie „$\Rightarrow$" im Beweis von Satz 4.10.

(iii): Folgt aus Satz 4.10 wegen $K^{p^{-\infty}} = K$.

(iv): Folgt direkt aus der Definition von „separabel" oder aus Satz 4.10.

(v): Folgt aus Satz 4.10 und der Transitivität von „linear disjunkt" in Körpertürmen.

(vi): Sei G ein endlich erzeugter Zwischenkörper von FL/L. Dann gibt es einen endlich erzeugten Zwischenköper H von F/K mit $G \subseteq HL$. Sei B eine separierende Transzendenzbasis von H/K. Dann ist B wegen der Voraussetzung auch eine separierende Transzendenzbasis von HL/L. Nach (ii) ist HL/L separabel und nach (i) ist G/L separabel.

(vii): Da FL/L separabel ist, sind FL/L und $L^{p^{-\infty}}/L$ und speziell FL/L und $LK^{p^{-\infty}}/L$ nach Satz 4.10 linear disjunkt. Da F/K und L/K nach Voraussetzung linear disjunkt sind, müssen auch FL/K und $LK^{p^{-\infty}}/K$ aufgrund der Transitivität von „linear disjunkt“ in Körpertürmen linear disjunkt sein. Dann sind speziell auch F/K und $K^{p^{-\infty}}/K$ linear disjunkt, so daß F/K nach Satz 4.10 separabel ist. $\square$

Die Aussagen (v) und (vi) implizieren auch, daß ein Kompositum algebraisch disjunkter, separabler Erweiterungen wieder separabel ist.

4.3 Reguläre Erweiterungen

Wir verschärfen nun den Begriff „separabel“ und Satz 4.10.

4.12 Definition. Eine Körpererweiterung E/K heißt regulär, wenn E/K und der algebraische Abschluß K^a/K linear disjunkt sind.

4.13 Satz. *Sei E/K eine Körpererweiterung. Dann sind äquivalent.*

(i) *E/K ist regulär.*

(ii) *K ist algebraisch abgeschlossen in E und E/K ist separabel.*

Beweis. $(i) \Rightarrow (ii)$: Da E/K und K^a/K linear disjunkt sind, gilt $E \cap K^a = K$ und K ist algebraisch abgeschlossen in E. Außerdem sind dann auch E/K und $K^{p^{-\infty}}/K$ wegen $K^{p^{-\infty}} \subseteq K^a$ linear disjunkt und E/K nach Satz 4.10 somit separabel.

$(ii) \Rightarrow (i)$: Aus der Voraussetzung folgt $EK^{p^{-\infty}} \cap K^a = K^{p^{-\infty}}$: Die Erweiterung $EK^{p^{-\infty}} \cap K^a / E \cap K^a$ ist mit $K^{p^{-\infty}}/K$ und $EK^{p^{-\infty}}/E$ rein inseparabel. Wegen $E \cap K^a = K$ und der Transitivität von „rein inseparabel“ ist dann $EK^{p^{-\infty}} \cap K^a / K^{p^{-\infty}}$ rein inseparabel. Diese Erweiterung ist nach Satz 1.72 aber auch separabel. Also folgt $EK^{p^{-\infty}} \cap K^a = K^{p^{-\infty}}$.

Die Erweiterung $K^a/K^{p^{-\infty}}$ ist galoissch. Nach Satz 2.13 und der Vorbemerkung sind nun $EK^{p^{-\infty}}/K^{p^{-\infty}}$ und $K^a/K^{p^{-\infty}}$ linear disjunkt. Außerdem sind E/K und $K^{p^{-\infty}}/K$ nach Voraussetzung linear disjunkt. Wegen der Transitivität von „linear disjunkt“ in Türmen ergibt sich damit, daß E/K und K^a/K linear disjkunkt sind, E/K also regulär ist. $\square$

4.14 Satz. *Sei E/K eine Körpererweiterung.*

(*i*) *Ist K algebraisch abgeschlossen, so ist E/K regulär.*

(*ii*) *Ist E/K regulär und F ein Zwischenkörper von E/K, so ist F/K regulär.*

(*iii*) *Ist F ein Zwischenkörper von E/K und sind E/F und F/K regulär, so ist E/K regulär.*

(*iv*) *Sind F und L über K algebraisch disjunkte Zwischenkörper von E/K und ist F/K regulär, so sind F/K und L/K linear disjunkt.*

(*v*) *Sind F und L über K algebraisch disjunkte Zwischenkörper von E/K und ist F/K regulär, so ist auch FL/L regulär.*

Beweis. (*i*) und (*ii*): Folgen direkt aus Satz 4.13.

(*iii*): Folgt aus Satz 4.13 und der Transitivität von „linear disjunkt" in Körpertürmen.

(*iv*): Wird ausgelassen.

(*v*): Mit F/K und L/K sind auch F/K und L^a/K algebraisch disjunkt. Nach (*iv*) sind F/K und L^a/K dann auch linear disjunkt. Wegen der Transitivität von „linear disjunkt" in Türmen sind dann auch FL/L und L^a/L linear disjunkt. Also ist FL/L regulär. □

Die Aussagen (*iii*) und (*v*) implizieren auch, daß ein Kompositum algebraisch disjunkter, regulärer Erweiterungen wieder regulär ist.

4.4 Beispiele

Wir betrachten nun Beispiele verschiedener Körper. Jeder Körper fällt unter einen der folgenden Typen.

1. Die Primkörper sind gleich $\mathbb{Q}$ oder $\mathbb{F}_p$ für eine Primzahl p.

2. Endliche Erweiterungen der Primkörper $\mathbb{Q}$ und $\mathbb{F}_p$ liefern Zahlkörper und endliche Körper.

3. Alle weiteren algebraischen Erweiterungskörper der Primkörper sind in den algebraischen Abschlüssen $\mathbb{Q}^a$ und $\mathbb{F}_p^a$ enthalten.

4. Rein transzendente Erweiterungen von Körpern K aus 1-3, also Körper der Form $K(X)$, wobei X eine Menge von Variablen bezeichnet.

5. Endliche und algebraische Erweiterungen E der Körper $K(X)$ in 4, wobei man K je nach Sichtweise beispielsweise als Primkörper von E oder als algebraischen Abschluß des Primkörpers von E in E wählen kann.

Sei $f = t^2 - x^3 - 1 \in \mathbb{Q}(x)[t]$. Durch Adjunktion einer Nullstelle y von f an $\mathbb{Q}(t)$ erhalten wir eine separable Erweiterung $K = \mathbb{Q}(x, y)$ vom Grad zwei von $\mathbb{Q}(x)$. Daher ist x ein separierendes Element (das heißt, $\{x\}$ ist eine separierende Transzendenzbasis). Die Erweiterung $K/\mathbb{Q}$ ist separabel.

In $\mathbb{F}_p(x)$ ist x^p zwar transzendent und $\{x^p\}$ eine Transzendenzbasis, aber x^p ist nicht separierend. Nach Satz 4.11, (iii) muß es ein separierendes Element geben. Man kann beispielsweise x oder $1/(x+1)$ wählen. Die Erweiterung $\mathbb{F}_p(x)/\mathbb{F}_p$ ist daher ebenfalls separabel.

Eine nicht separable Erweiterung erhält man unter Benutzung von Satz 4.10 wie folgt. Sei $K = \mathbb{F}_p(z, x, y)$ der durch $x^p + y^p + z = 0$ definierte Körper. Da $x^p + y^p + z$ als Polynom über $\mathbb{F}_p(z)$ irreduzibel ist, hat $K/\mathbb{F}_p(z, x)$ den Grad p. Diese Erweiterung ist jedoch nicht linear disjunkt zu $\mathbb{F}_p(z^{1/p})$, da hier wegen $y + x + z^{1/p} = 0$ gilt, daß $K\mathbb{F}_p(z^{1/p})/\mathbb{F}_p(z^{1/p}, x)$ den Grad eins hat. Folglich ist $K/\mathbb{F}_p(z)$ nicht separabel.

Die Erweiterungen $\mathbb{Q}(x)/\mathbb{Q}$ und $K/\mathbb{Q}$ für $K = \mathbb{Q}(x, y)$ wie oben sind Beispiele für reguläre Erweiterungen. Endliche und algebraische Erweiterungen eines Körpers in Charakteristik Null und zum Beispiel die Erweiterung $\mathbb{Q}(x, \sqrt{2})/\mathbb{Q}$ sind separabel aber nach Satz 4.13 nicht regulär, da der Grundkörper nicht algebraisch abgeschlossen ist. Auf der anderen Seite ist $\mathbb{F}_p(z)$ im obigen Beispiel in $K = \mathbb{F}_p(z, x, y)$ zwar algebraisch abgeschlossen, aber die Erweiterung $K/\mathbb{F}_p(z)$ trotzdem nicht regulär, weil sie nicht separabel ist.