Skript zur Algebra II

Vorlesung im Wintersemester 2007

an der Technischen Universität Berlin

Prof. Dr. F. Heß

Inhaltsverzeichnis

Vereinbarungen **V**

1 Algebraische Körpererweiterungen **1**
1.1 Endliche, algebraische und transzendente Körpererweiterungen . . 1
1.2 Zerfällungskörper und algebraischer Abschluß 11
1.3 Homomorphismen und ihre Fortsetzungen 14
1.4 Normale Erweiterungen 17
1.5 Separable Erweiterungen 21
1.6 Rein inseparable Erweiterungen 25
1.7 Weitere Eigenschaften von normalen, separablen und rein inseparablen Erweiterungen 29
1.8 Endliche Körper 32
1.9 Kreisteilungskörper 34
1.10 Charakteristisches Polynom, Spur und Norm 36

2 Galoistheorie **43**
2.1 Galoiserweiterungen 43
2.2 Beziehungen zwischen Galoiserweiterungen 48
2.3 Galoisgruppen spezieller Körpererweiterungen 51
2.4 Permutationsdarstellungen und Galoisgruppen von Polynomen . . 52
2.5 Symmetrische Polynome und das Umkehrproblem der Galoistheorie 56
2.6 Lineare Unabhängigkeit von Charakteren 59
2.7 Normalbasen 61
2.8 Kummertheorie 61
2.9 Auflösbarkeit durch Radikale 71
2.10 Reduktionsprinzip 74

3 Transzendente Körpererweiterungen **77**
3.1 Transzendenzbasen 77
3.2 Separable Erweiterungen 80

3.3 Reguläre Erweiterungen 82
3.4 Beispiele 84

4 Moduln II **85**
4.1 Tensorprodukte 85
4.2 Induzierte und koinduzierte Moduln 92
4.3 Lokalisierungen 94
4.4 Flache Moduln 97
4.5 Freie Moduln 99
4.6 Projektive Moduln 101
4.7 Satz von Cayley-Hamilton und Lemma von Nakayama 103
4.8 Beziehungen zwischen den Moduleigenschaften und lokal-global Aussagen 105

5 Ringe II **111**
5.1 Tensorprodukt von Algebren 111
5.2 Gebrochene und invertierbare Ideale, Primidealfaktorisierung . . . 112
5.3 Lokale Charakterisierungen invertierbarer Ideale 116
5.4 Ganze Ringerweiterungen 124
5.5 Globale Charakterisierung von Dedekindringen 126
5.6 Beispiele 129

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 $A = \{a_1, \ldots, a_n\}$ schreiben wir auch $R[a_1, \ldots, a_n]$ und $R(a_1, \ldots, a_n)$.

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

$$\begin{aligned} R[a_1, \ldots, a_n] &= \{\, g(a_1, \ldots, a_n) \mid g \in R[t_1, \ldots, t_n] \,\} \\ &= \operatorname{im}(\phi) \;\cong\; R[t_1, \ldots, t_n]/\ker(\phi), \end{aligned}$$

$$\begin{aligned} R(a_1, \ldots, a_n) = \{\, g(a_1, \ldots, a_n)/h(a_1, \ldots, a_n) \mid g, h \in R[t_1, \ldots, t_n] \\ \text{und } h(a_1, \ldots, a_n) \neq 0 \,\}. \end{aligned}$$

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 $ab = 1$. □

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 $a_1, \ldots, a_r \in E$ mit $E = K(a_1, \ldots, a_r)$ 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 $k[a] = \operatorname{im}(\phi_a) \cong K[t]/\ker(\phi_a)$, 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* $K(t) = \operatorname{Quot}(K[t])$ *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 $K(a) = \operatorname{Quot}(K[a])$. *(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 über K algebraischen Erzeugern.

Beweis. $(i) \Rightarrow (ii)$: Sei E/K endlich. Jedes Element $a \in E$ ist algebraisch, weil die Potenzen $1, a, a^2, \ldots$ linear abhängig über K sind. Ist $e_1, \ldots, e_n \in E$ eine K-Basis von E, so gilt $E = K(e_1, \ldots, e_n)$. 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 $a_1, \ldots, a_r \in E$, also $E = K(a_1, \ldots, a_r)$. Setze $E_i = K(a_1, \ldots, a_i)$, 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 $a + b, a - b, ab, a/b \in K(M_1 \cup M_2) \subseteq \cup_M K(M)$ (sofern gegebenenfalls $b \neq 0$ ist). 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 $a \in K[A]$ mit $a \neq 0$ 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.

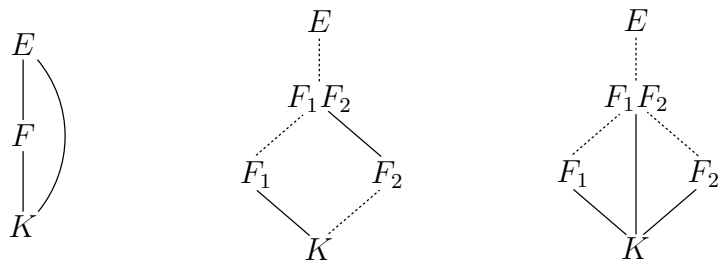

Abbildung 1.1: Zwischenkörper, Translation und Kompositum

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. Ist B_1 ein K-Erzeugendensystem von F_1, so ist B_1 auch ein F_2-Erzeugendensystem von F_1F_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. *Ist* B_1 *ein* K*-Erzeugendensystem von* F_1 *und* B_2 *ein* K*-Erzeugendensystem von* F_2, *so ist* $B_1B_2 = \{b_1b_2 \,|\, b_1 \in B_1, b_2 \in B_2\}$ *ein* K*-Erzeugendensystem von* F_1F_2.

(*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. Die erste Aussage von (*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. Genauer gilt $F_2(F_1) = F_2[F_1]$. Da F_1 multiplikativ abgeschlossen ist, gibt es für jedes $x \in F_2[F_1]$ Elemente $a_i \in F_1$ und $\lambda_i \in F_2$ mit $x = \sum_i \lambda_i a_i$. Die a_i lassen sich wiederum als K-Linearkombinationen von Elementen aus B_1 schreiben. Also ist jedes $x \in F_2[F_1]$ auch eine F_2-Linearkombination von Elementen aus B_1. Dies beweist die zweite Aussage in (*i*).

(*ii*) folgt aus (*i*). (*iii*) folgt aus (*i*) und Satz 1.16, sowie dem Argument im Beweis von Satz 1.4. (*iv*) folgt aus (*ii*) und der Gradformel $[F_1F_2 : K] = [F_1F_2 : F_2][F_2 : K] \leq [F_1 : K][F_2 : K]$. □

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 $\sum_{i,j} \mu_{i,j} a_i b_j = 0$ 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 $\sum_{i,j} \mu_{i,j} a_i b_j = \sum_i \lambda_i a_i = 0$ 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) *Sind F_1 und F_2 linear disjunkt über K, so gilt $[F_1F_2 : F_2] = [F_1 : K]$. Gilt umgekehrt $[F_1F_2 : F_2] = [F_1 : K]$ und $[F_1 : K] < \infty$, so sind F_1 und F_2 linear disjunkt über K.*

(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.*

(iv) *Sei L ein weiterer Zwischenkörper von E/K und gelte $F_1 \subseteq F_2$. Dann sind L/K und F_2/K genau dann linear disjunkt, wenn L/K und F_1/K sowie LF_1/F_1 und F_2/F_1 linear disjunkt sind.*

(v) *F_1 und F_2 sind genau dann linear disjunkt über K, wenn F_1' und F_2 über K linear disjunkt sind für alle Teilkörper F_1' von F_1 mit $[F_1' : K] < \infty$.*

Beweis. (i): „$\Rightarrow$“: Enthält F_1 ein über K transzendentes Element a, so ist a nach Voraussetzung auch über F_2 transzendent. Es folgt $[F_1F_2 : F_2] = [F_1 : K] = \infty$. Andernfalls ist F_1/K algebraisch. Da eine K-Basis von F_1 nach der Voraussetzung und nach Satz 1.20, (i) 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 nach Satz 1.20, (i) 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. (iv): Übung. (v): Übung. □

Aussage (iii) ist eine Verallgemeinerung von Aussage (i). Aussage (iv) kann man auch als Transitivität von „linear disjunkt“ auffassen. Zur Verdeutlichung zeichne man das zugehörige Diagramm analog zu Abbildung 1.1.

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.

Ein einfaches hinreichendes Kriterium für lineare Disjunktheit ist die Teilerfremdheit der Körpergrade: Sind $[F_1 : K]$ und $[F_2 : K]$ teilerfremd, so gilt $[F_1F_2 : K] = [F_1 : K][F_2 : K]$ wegen $[F_1 : K] \mid [F_1F_2 : K]$ und $[F_2 : K] \mid [F_1F_2 : K]$ nach Satz 1.4 und wegen Satz 1.20, (iv). Es gilt dann auch $[F_1F_2 : F_2] = [F_1 : K]$. In Satz 1.20, (i) geht in diesem Fall eine K-Basis B_1 von F_1 also in eine F_2-Basis von F_1F_2 über, und in (iii) ist B_1B_2 eine K-Basis von F_1F_2, wenn B_1 und B_2 jeweils eine K-Basis von F_1 beziehungsweise F_2 sind.

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 dieses Abschnitts 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

$$[\mathbb{Q}(a) : \mathbb{Q}] = 2^r \tag{1.26}$$

für ein $r \in \mathbb{Z}^{\geq 1}$, also $[\mathbb{Q}(a) : \mathbb{Q}]$ gleich einer 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 $a = \sqrt[3]{2}$ konstruiert werden. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist dies nach Satz 1.4 und (1.26) 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.

1.27 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 1.27 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.

1.28 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 $f \in M$ 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 $M = \{f_1, \ldots, f_n\}$ sprechen wir auch vom Zerfällungskörper der $f_1, \ldots, f_n$ über K.

1.29 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 1.27 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 $E_n = K(a_1, \ldots, a_n)$ und mit $c = f_n \in K$ gilt $f = c\prod_i (t - a_i)$ in $E_n[t]$. Die Gradaussage folgt aus $\deg(f_{i+1}) = \deg(f_i) - 1$. $\square$

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.

1.30 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 1.29 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.

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

Beweis. Wir gehen im Prinzip wie in Satz 1.29 vor, nur daß wir alle nicht konstanten Polynome aus $K[t]$ simultan betrachten. Wie in Satz 1.29 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 1.29 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 $K = E_0 \subseteq E_1 \subseteq \ldots$ 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 $\mathbb{C}$.

1.32 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 1.29. 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.

1.33 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. □

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.

1.34 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. Haben E_1 und E_2 den gleichen Primkörper K, so ist jedes $\sigma \in \mathrm{Hom}(E_1, E_2)$ automatisch K-linear, also gilt $\sigma \in \mathrm{Hom}_K(E_1, E_2)$.

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.

1.35 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 $K_1(a) \cong K_1[t]/fK_1[t]$, $K_2(b) \cong K_2[t]/f^\sigma K_2[t]$ mit K_1- bzw. K_2-linearen Isomorphismen. Die Faktorringe $K_1[t]/fK_1[t]$ und $K_2[t]/f^\sigma K_2[t]$ sind aber offenbar unter vertreterweise Anwendung 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 $1 = \tau(a) = b = 2$).

1.36 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 1.29 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 1.35 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 $\tau = \sigma_n \in \mathrm{Hom}_\sigma(E_1, E_2)$. □

1.37 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 $\mathbb{Q}(\sqrt{2})$, nach Lemma 1.35 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 1.35 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.

1.38 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 1.35 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 $F = E$. □

1.39 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 1.38 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 $\tau(C_1) = C_2$. □

1.40 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 1.38 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 $\sigma(E_1) = E_2$. □

1.41 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 1.35 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.

1.42 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.

1.43 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 $\sigma, \tau \in \mathrm{Hom}_K(E, L)$ gilt $\sigma(E) = \tau(E)$, es gibt also auch 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 1.41 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 1.35 und Satz 1.38 gibt es $\tau_i \in \mathrm{Hom}_K(E, L)$ mit $\tau_i(a) = b_i$ für alle i. Nach (*iii*) gilt $b_i \in \tau_i(E) = \sigma(E)$ und es gibt $\rho_i \in \mathrm{Aut}_K(E)$ mit $\tau_i = \sigma \circ \rho_i$. Dann ist $\rho_i(a) = \sigma^{-1}(b_i)$, 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 1.43, (*iii*) ergibt sich ein wichtiger Spezialfall, wenn $\sigma = \mathrm{id}$ und die betrachteten Körper alle in L liegen:

1.44 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 1.43, (*iii*). □

Sei E/K algebraisch und C ein algebraischer Abschluß von E. Jedes Element von $\mathrm{Hom}_K(E, C)$ läßt sich nach Satz 1.38 und Satz 1.41 zu einem Element von $\mathrm{Aut}_K(C)$ fortsetzen. Eine zu Satz 1.43, (*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.

1.45 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 wie folgt: Ist $f \in K[t]$ normiert und irreduzibel, und besitzt f eine Nullstelle in $F_1 \cap F_2$, so zerfällt f nach Voraussetzung über F_1 und über F_2 in Linearfaktoren. Da F_1, F_2 Teilkörper von E sind und $E[t]$ faktoriell ist, stimmen diese beiden Faktorisierungen von f bs auf die Reihenfolge der Linearfaktoren überein und liefern daher bereits eine Faktorisierung von f in Linearfaktoren aus $(F_1 \cap F_2)[t]$. □

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

1.46 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.

1.47 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 1.38 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 1.45 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 1.41. Folglich sind E und L isomorph über K. □

1.48 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 1.44 und Satz 1.47 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 1.43 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 $B = \cup\{\tau(F) \mid \tau \in \mathrm{Hom}_K(F, L)\}$ 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. □

1.49 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

1.50 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 K abhängt, da der größte gemeinsame Teiler von f und f' bezüglich aller Körpererweiterungen von K gleich ist.

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.

1.51 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.

1.52 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 mit Hilfe von Satz 1.38 und Satz 1.41 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. □

1.53 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 1.52. □

1.54 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 1.35: Für jede Nullstelle b von $m_{a,K}$ in C gibt es genau ein $\tau \in \mathrm{Hom}_K(E, C)$ mit $\tau(a) = b$. □

1.55 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. Wir beweisen zuerst $[E : K]_s \leq [E : K]$. Diese Aussage 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 1.54, Satz 1.53 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.

Wir beweisen nun die Äquivalenz $(iii) \Leftrightarrow (iii)'$ für eine endliche Erweiterung E/K. Aus (iii) folgt $(iii)'$ mit $F = E$. Gilt umgekehrt $(iii)'$, also $[E : K]_s = [E : K]$ 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 $[:]$.

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

$(iii) \Rightarrow (i)$: Für $a \in E$ gilt $[K(a) : K]_s = [K(a) : K]$, also ist a nach Lemma 1.54 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 im ersten Abschnitt des Beweises gilt $[E : K]_s = [E : K]$. Ist F ein Zwischenkörper, so folgt $[F : K]_s = [F : K]$ nach der bereits bewiesenen Äquivalenz $(iii) \Leftrightarrow (iii)'$. Dies beweist Satz 1.55 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 1.53 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 1.55 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.

1.56 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 1.55 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 1.55, (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.

1.57 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.

1.58 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 1.67. □

1.59 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

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

1.6 Rein inseparable Erweiterungen

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

1.61 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.

1.62 Definition. Sei E/K eine algebraische Erweiterung. Ein Element $a \in E$ heißt rein inseparabel über K, 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 1.62 im Analogievergleich zu Definition 1.51 und zu den Definitionen für „algebraisch“ behoben wird. Wir fassen ∞ auch als Potenz von $p = \mathrm{char}(K)$ auf.

1.63 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 1.63 ebenfalls richtig.

Ist F ein Zwischenkörper von E/K und $a \in E$, so ist a auch rein inseparabel über F, denn es gilt $m_{a,F} \mid m_{a,K}$ 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. □

1.64 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*): Folgt aus Lemma 1.63, (*i*).

(*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. Nach Lemma 1.54 gilt $[L_{i+1} : L_i]_s = 1$. Nach Satz 1.53 gilt folglich $[L_n : K]_s = \prod_i [L_{i+1} : L_i]_s = 1$ 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 1.64, (*iii*) genügt es, wegen Satz 1.53 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.

1.65 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 1.64 und Satz 1.67 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.

1.66 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.

1.67 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 1.55, Satz 1.64 und Satz 1.53 gilt $[E : F]_s = 1$ und damit $[F : K] = [F : K]_s = [E : F]_s[F : K]_s = [E : K]_s$. Die Aussage über $[E : F]$ folgt aus Lemma 1.63. □

1.68 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 1.67 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 ähnliche Eigenschaften wie der Separabilitätsgrad:

1.69 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 E/K normal und F der rein inseparable Abschluß von K in E, so ist E/F separabel und es gilt $[E : K]_i = [F : K]$.*

Beweis. (*i*): Sei F' der separable Abschluß von K in F, E' der separable Abschluß von F in E und L der separable Abschluß von F' in E'. Nach Satz 1.73 sind F und L über F' linear disjunkt mit $E' = FL$. Weiter ist L/K separabel und E/L rein inseparabel. Daher ist L der separable Abschluß von K in E. Es folgt $[E : K]_i = [E : L] = [E : E'][E' : L] = [E : F]_i[E' : L] = [E : F]_i[F : F'] = [E : F]_i[F : K]_i$.

(*ii*): Folgt aus Satz 1.73. □

Für endliche Erweiterungen E/K kann man die Multiplikativität von $[:]_i$ 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.

1.70 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.

1.71 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 (Aufgabe: f ist sogar irreduzibel). 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.

1.72 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 1.63. □

Im Abschnitt 1.6 haben wir gesehen, daß sich eine algebraische Körpererweiterung E/K in eine separable Erweiterung F_1/K und eine rein inseparable Erweiterung E/F_1 aufteilen läßt. Ist E/K normal, so kann E/K auch in eine rein inseparable Erweiterung F_2/K und eine separable Erweiterung E/F_2 aufgeteilt werden. Hierbei sind F_1 und F_2 der separable bzw. rein inseparable Abschluß von K in E.

1.73 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*) *F_1 und F_2 sind linear disjunkt über K.*

(*ii*) *Ist E separabel über F_2, so gilt $E = F_1F_2$ sowie $[E : K]_s = [F_1 : K] = [E : F_2]$ und $[E : K]_i = [F_2 : K] = [E : F_1]$.*

(*iii*) *Ist E normal über K, so ist E separabel über F_2.*

Beweis. (*i*): Für die lineare Disjunktheit genügt es wegen Satz 1.23, (*v*) und Satz 1.59 zu zeigen, daß für jedes separable $a \in E$ die Erweiterungen $K(a)/K$ und F_2/K linear disjunkt sind. Nach Lemma 1.63 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.

(*ii*): Die Erweiterung E/F_1F_2 ist nach Satz 1.65, (*i*) rein inseparabel und nach Satz 1.56, (*i*) und separabel. Daher gilt $E = F_1F_2$.

(*iii*): Sei $a \in E$ und $m_{a,K} = g(t^{p^r})$ mit $g \in K[t]$ separabel. Da E/K normal ist, gibt es paarweise verschiedene $a_i \in E$ mit $m_{a,K} = \prod_{i=1}^n (t - a_i)^{p^r}$ und $g = \prod_{i=1}^n (t - a_i^{p^r})$. Das Polynom $h = \prod_{i=1}^n (t - a_i)$ erfüllt $h^{p^r} = g$ und daher $h \in F_2[t]$. Schließlich gilt $h(a) = 0$ und h ist separabel, so daß a separabel über F_2 ist. □

1.74 Korollar. *Sei E/K eine einfache Erweiterung mit primitivem Element a und C ein algebraischer Abschluß von E. Sei F_1 der separable Abschluß von K in E und F_2 der rein inseparable Abschluß von K in E. Sei $r \in \mathbb{Z}^{\geq 0}$ maximal, so daß es ein $g \in K[t]$ mit $m_{a,K} = g(t^{p^r})$ gibt. Sei $h \in C[t]$ mit $h^{p^r} = g(t^{p^r}) = m_{a,K}$. Ist E/F_2 separabel, so 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 1.63. Nach Lemma 1.63 gibt es auch ein $s \in \mathbb{Z}^{\geq 0}$ minimal mit ${m_{a,F_2}}^{p^s} \in K[t]$. Dann gilt $m_{a,K} = h^{p^r} \mid {m_{a,F_2}}^{p^s}$. Das Polynom h ist nach Definition separabel. Wegen Satz 1.73, (*i*) ist aber auch m_{a,F_2} separabel. Die Betrachtung der Faktorisierungen dieser Polynome über C zeigt $r = s$ und $h \mid m_{a,F_2}$. Wegen $\deg(m_{a,F_2}) = [K(a) : K]_s = \deg(h)$ folgt $h = m_{a,F_2}$.

(*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 $K(a^{p^r}) \subseteq F_1$. Da $E/K(a^{p^r})$ rein inseparabel ist, folgt $F_1 = K(a^{p^r})$. Weiter gilt $h = \sum_i c_i^{p^{-r}} t^i$ und aus Aussage (*i*) und Lemma 1.24 folgt $F_2 = K(c_0^{p^{-r}}, \ldots, c_n^{p^{-r}})$. □

Für normale Erweiterungen ist das notwendige Kriterium für lineare Disjunktheit aus Satz 1.23, (*ii*) unter gewissen Bedingungen auch hinreichend, wie der folgende Satz zeigt.

1.75 Satz. *Seien E/K eine Körpererweiterung und F_1, F_2 Zwischenkörper von E/K mit F_1/K normal und $F_1 \cap F_2 = K$. Ist F_1/K einfach oder separabel, oder ist F_2/K separabel, so sind F_1 und F_2 linear disjunkt über K.*

Beweis. Sei zuerst F_1/K einfach mit primitivem Element a. Dann ist $m_{a,K}$ irreduzibel in $F_2[t]$: Seien $g, h \in F_2[t]$ normiert mit $m_{a,K} = gh$. Die Koeffizienten von g und h sind Polynomausdrücke in den Nullstellen von $m_{a,K}$, welche wegen der Normalität von F_1/K alle in F_1 liegen. Wegen $F_1 \cap F_2 = K$ folgt $g, h \in K[t]$. Da $m_{a,K}$ irreduzibel in $K[t]$ ist, folgt $g = 1$ oder $h = 1$. Also ist $m_{a,K}$ auch in $F_2[t]$ irreduzibel. Damit folgt $[F_1 : K] = [K(a) : K] = [F_2(a) : F_2] = [F_1F_2 : F_2]$, und die lineare Disjunktheit ergibt sich aus Satz 1.23, (*i*).

Sei nun F_1/K separabel. Die lineare Disjunktheit ergibt sich dann aus dem bereits bewiesenen Fall mit Hilfe von Satz 1.23, (*v*) und Satz 1.59.

Sei schließlich F_2/K separabel. Sei L der separable Abschluß von K in F_1. Dann ist L/K separabel und normal und nach dem bereits bewiesenen Fall sind L/K und F_2/K linear disjunkt. Nach Satz 1.73, (*i*) sind aber auch F_1/L und F_2L/L linear disjunkt, so daß sich die lineare Disjunktheit von F_1/K und F_2/K mit Satz 1.23, (*iv*) ergibt. □

1.76 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 1.67 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 1.76 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 $\#K = p^n$.

1.77 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 $x \in K$. □

1.78 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 1.77 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. □

1.79 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 auf Seite 29 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. □

1.80 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 $\overline{\mathbb{F}}_p$.

1.81 Satz. *Seien $\mathbb{F}_{p^n}$ und $\mathbb{F}_{p^m}$ endliche Körper (in einem gemeinsamen Erweiterungskörper $\overline{\mathbb{F}}_p$). Dann ist $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ genau dann, wenn $m \mid n$ gilt.*

Beweis. Gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, so folgt $\#\mathbb{F}_{p^n} = (\#\mathbb{F}_{p^m})^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]}$, also $p^n = p^{m[\mathbb{F}_{p^n}:\mathbb{F}_{p^n}]}$. Gelte umgekehrt $m \mid n$. Für $x \in \mathbb{F}_{p^m}$ ergibt sich $x^{p^m} = x$, $x^{p^{2m}} = (x^{p^m})^{p^m} = x$ usw. und schließlich $x^{p^n} = x^{(p^m)^{n/m}} = x$ unter Verwendung von $m \mid n$. Dies wiederum bedeutet $x \in \mathbb{F}_{p^n}$. □

1.82 Korollar. *Es gilt $\mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^{\mathrm{lcm}(n,m)}}$ und $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{\gcd(n,m)}}$.*

Beweis. Übung. □

Die explizite Darstellung von endlichen Körpern kann wieder mit irreduziblen Polynomen erfolgen. Ist $\mathbb{F}_q$ endlicher Körper mit q Elementen und $f \in \mathbb{F}_q[t]$ normiert und irreduzibel vom Grad n, so ergibt $\mathbb{F}_q[t]/f\mathbb{F}_q[t]$ eine Erweiterung von $\mathbb{F}_q$ vom Grad n. Wählt man ein anderes irreduzibles Polynom vom Grad n, so erhält man einen $\mathbb{F}_q$-isomorphen Körper. Die Existenz von $\mathbb{F}_{q^n}$ bzw. primitiver Elemente von $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ zeigt auch, daß es für jedes $n \in \mathbb{Z}^{\geq 1}$ mindestens ein irreduzibles Polynom $f \in \mathbb{F}_q[t]$ mit $\deg(f) = n$ gibt.

1.9 Kreisteilungskörper

1.83 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 $\exp(2\pi i r/n)$ 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 $E = K(\mu_{q-1})$.

1.84 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. □

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

Beweis. Sei $p = \mathrm{char}(K)$. Dann ist $K(\mu_n)$ Zerfällungskörper des separablen Polynoms $t^n - 1$ für $p = 0$ beziehungsweise $t^{n/v_p(n)} - 1$ für $p > 0$. □

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

1.86 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.

1.87 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 $\Phi_n = (t^n - 1)/\prod_{d\,|\,n, d\neq n} \Phi_d$. 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.

1.88 Satz. *Die Kreisteilungspolynome sind bereits über $\mathbb{Z}$ bzw. den jeweiligen Primkörpern $\mathbb{F}_p$ definiert. Die Reduktion des Kreisteilungspolynoms über $\mathbb{Z}$ modulo einer Primzahl p liefert das Kreisteilungspolynom über $\mathbb{F}_p$.*

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 (Polynomdivision liefert Quotienten über $\mathbb{Z}$ bzw. $\mathbb{F}_p$ und es bleibt kein Rest übrig). Sei $\bar{\cdot} : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ der kanonische Epimorphismus bezüglich koeffizientenweiser Reduktion modulo p. Gilt $t^n - 1 = \Phi_n \prod_{d\,|\,n, d\neq n} \Phi_d$, so erhalten wir auch $t^n - 1 = \overline{\Phi_n} \prod_{d\,|\,n, d\neq n} \overline{\Phi_d}$. Dies zeigt, daß das n-te Kreisteilungspolynom über $\mathbb{F}_p$ gleich $\overline{\Phi_n}$ ist. □

1.89 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. □

Der vorhergehende Satz ist über endlichen Körpern im allgemeinen falsch.

Wegen $\#\mu_n = n$ aufgrund der Annahmen und da μ_n zyklisch ist, gilt $\mu_m \subseteq \mu_n$ genau dann, wenn $m \,|\, n$. Daraus folgt $\mu_n \cap \mu_m = \mu_{\gcd(n,m)}$ und $\mu_n \mu_m = \mu_{\mathrm{lcm}(n,m)}$.

1.90 Korollar. *Es gilt* $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$ *und* $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ *für eine primitive* n*-te Einheitswurzel* $\zeta \in \mu_n$*. Es gilt* $\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{\mathrm{lcm}(n,m)})$ *und* $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{\gcd(n,m)})$*.*

Beweis. Der erste Teil ist mit Satz 1.89 klar. Der Rest ist eine Übung. □

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). Wir erhalten schließlich einen Ringmonomorphismus $\phi : E \to \mathrm{End}_K(E)$ durch $a \mapsto \phi_a$.

1.91 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.

1.92 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

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

Für die Spur gilt direkt

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

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

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

□

1.93 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 1.92.

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 $K(t)$ (Übungsaufgabe, beachte Satz 1.20, (i) und Satz 3.7).

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 1.92 als der durch koeffizientenweise Anwendung von f erhaltene Monomorphismus definiert. Nach Lemma 1.92 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 1.93) untersuchen. Wir benötigen dies hier aber nicht.

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

1.94 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 $\phi_{\chi_{a,E/K}(a)} = \chi_{a,E/K}(\phi_a) = 0$ nach der Homomorphieeigenschaft von ϕ und dem Satz von Cayley-Hamilton folgt $\chi_{a,E/K}(a) = 0$ aufgrund der Injektivität von ϕ. Gradvergleich zeigt dann $\chi_{a,K(a)/K} = m_{a,K}$, da beide Polynome normiert sind. (*iii*): Folgt direkt aus Satz 1.93. □

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 1.94, (*iii*) kann dann auch nur unter Verwendung von Körperhomomorphismen geführt werden (siehe Lemma 2.36).

1.95 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. Die Aussagen (i) und (ii) folgen direkt aus (iii) durch Ausmultiplizieren. Wenn $[E:K]_i > 1$ ist, gilt außerdem $p = \mathrm{char}(K) > 0$ und $[E:K]_i \equiv 0 \bmod p$. 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 1.63 (oder auch Korollar 1.74) 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 $m_{a^q,K}(b) = 0$ genau ein $\tau \in \mathrm{Hom}_K(K(a^q),C)$ mit $\tau(a^q) = b$ nach Lemma 1.35 gibt (siehe auch Lemma 1.54). 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 1.74). Da jedes $\tau \in \mathrm{Hom}_K(K(a^q),C)$ somit nach Satz 1.64, (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 1.94, (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 1.52 fortgesetzt werden kann. □

Für beliebiges $\tau \in \mathrm{Hom}(E,C)$ 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 normal. Der Fixkörper E^G von $G = \mathrm{Aut}_K(E)$ ist dann rein inseparabel über K. Ist E/K galoissch, so gilt $E^G = K$. Für jeden Zwischenkörper F von E/K ist E/F galoissch.*

Beweis. Sei C ein algebraischer Abschluß von E und $\sigma \in \mathrm{Hom}_K(E^G, C)$ beliebig. Nach Satz 1.38 gibt es eine Fortsetzung $\tau \in \mathrm{Hom}_\sigma(E, C)$. Da E normal über K ist, folgt $\tau(E) = E$ nach Satz 1.43 und somit $\tau \in G$. Sei $a \in E^G$. Dann gilt $\sigma(a) = \tau(a) = a$. Dies zeigt $\#\mathrm{Hom}_K(E^G, C) = 1$, so daß E^G/K nach Satz 1.64, (iii) und Satz 1.53 rein inseparabel ist.

Sei E/K galoissch. Dann ist E^G/K separabel und rein inseparabel, also folgt $E^G = K$.

Sei F ein Zwischenkörper von E/K. Die Erweiterung E/F ist normal nach Satz 1.45 und separabel nach Satz 1.56, weil E/K normal und separabel ist. Also ist E/F galoissch. □

2.4 Korollar. *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 Korollar 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 1.59 gilt dann aber bereits $[E : K] \leq n$ (Übungsaufgabe!). Es ist klar, daß $G \subseteq G(E/K)$ gilt. Dann folgt $n = \#G \leq \#G(E/K) = [E : K]_s = [E : K] \leq n$, 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 $H \subseteq G(E/K)$. Da E/K normal ist, gilt $\#G(E/K) = [E : K]_s \leq [E : K] < \infty$. Also ist auch 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/F algebraisch und E/K normal ist, gilt $\mathrm{Hom}_K(F, E) = \{\sigma|F \mid \sigma \in G\}$ aufgrund von Satz 1.38 und Satz 1.43, (*iii*). 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 $G = \dot{\bigcup}_{\sigma \in R} \sigma H$. Zusammen 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 Korollar 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 Korollar 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 $\mathrm{Aut}_{\lambda K}(\lambda E) = \lambda \mathrm{Aut}_K(E)\lambda^{-1}$ *und* $\mathcal{G}_{\lambda E/\lambda K}(\lambda F) = \lambda \mathcal{G}_{E/K}(F)\lambda^{-1}$ *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 1.43 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 1.38, Satz 1.43 und Satz 1.41 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 1.43 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).

2.13 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. □

2.14 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 1.45 und Satz 1.56 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 1.75 linear disjunkt. Nach Satz 2.13 setzt sich daher jedes $\sigma \in G(E/E \cap L)$ zu einem $\tau \in G(EL/L)$ fort. Dies ergibt $\phi(G(EL/L)) = G(E/E \cap L)$. □

2.15 Satz. *Seien F_i über K galoissche Zwischenkörper von C/K. Dann ist $E = \coprod_i F_i$ 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 1.45 und Satz 1.56 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 2.14 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.

2.16 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.

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

2.18 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 2.14 und Satz 2.15. Ferner sind Untergruppen und Faktorgruppen abelscher bzw. zyklischer Gruppen wieder abelsch bzw. zyklisch. □

2.19 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. Es gilt $K^{ab} = \mathcal{F}_{K^s/K}(G(K)^{ab})$. Nach Satz 2.18 ist $G(K^{ab}/K)$ abelsch.

2.20 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. □

2.21 Satz. *Sei* $\mathrm{char}(K) = 0$ *oder n koprim zu* $\mathrm{char}(K)$*, 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 2.21 auch auf Erweiterungen von endlichen Körpern wie in Satz 2.20 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 2.21 ist die von q in $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^\times$ erzeugte, n-elementige Untergruppe.

2.22 Satz. *Sei* $\mathrm{char}(K) = 0$ *oder* n *koprim zu* $\mathrm{char}(K)$*, 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. □

2.23 Satz. *Sei* $\mathrm{char}(K) = p > 0$ *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 2.22 bzw. Satz 2.23 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.

Als weitere Übungsaufgabe bestimme man die Galoisgruppe des Zerfällungskörpers $\mathbb{Q}(\mu_n, \sqrt{n}a)/\mathbb{Q}$ für irreduzibles $f = t^n - a \in \mathbb{Q}[t]$ als semidirektes Produkt der Galoiserweiterungen $\mathbb{Q}(\mu_n)/\mathbb{Q}$ und $\mathbb{Q}(\mu_n, \sqrt[n]{a})/\mathbb{Q}(\mu_n)$.

2.4 Permutationsdarstellungen und Galoisgruppen von Polynomen

Sei K ein Körper, $f \in K[t]$ ein nicht-konstantes, separables Polynom und E ein Zerfällungskörper 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 $a_1, \ldots, a_n \in E$ 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 $a_1, \ldots, a_n$. Bezeichnet S_n die symmetrische Gruppe (die Gruppe der Permutationen auf den Ziffern $1, \ldots, n$), 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.

2.24 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 $E = K(a_1, \ldots, a_n)$ 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 nichtkonstanten Polynomen f_1 und f_2, so können die Nullstellen von f_1 wegen der Separabilität von f 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.

2.25 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 1.29. 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 2.21 bestimmen wir zunächst $G(K(\zeta)/K)$, und setzen diese Automorphismen mittels Satz 2.22 und Lemma 1.52 zu allen Automorphismen in $G(E/K)$ zusammen. Dies ergibt $G(E/K) = \{\sigma_{i,j} \,|\, 1 \le i \le 2, 1 \le j \le 3\}$ 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 und Satz 1.95 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 $n = 23$ und in Einzelfällen bis $n = 70$. Wir nehmen dieses Thema im folgenden Abschnitt auf. Auf der anderen Seite kann man die Galoisgruppen von Klassen von spezi-

ellen Polynomen bzw. Galoiserweiterungen wie im Abschnitt 2.3 leicht explizit bestimmen.

Wir beenden diesen Abschnitt mit einem Reduktionsprinzip der Galoistheorie (auch Kriterium von van der Waerden oder Frobenius Kriterium genannt). Jede Permutation $\sigma \in S_n$ lässt sich bis auf die Reihenfolge eindeutig als Produkt $\sigma = \prod_{i=1}^{s} \sigma_i$ von disjunkten Zykeln σ_i schreiben. Der Zykeltyp von σ ist dann das ungeordnete Tupel $(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_s))$. Der Zykeltyp einer Permutation σ und jeder ihrer Konjugierten $\tau\sigma\tau^{-1}$ für $\tau \in S_n$ ist gleich. Daher spricht man auch vom Zykeltyp der Konjugationsklasse von σ.

2.26 Satz. *Sei R ein Integritätsring und $K = \mathrm{Quot}(R)$. Sei $f \in R[t]$ ein normiertes irreduzibles Polynom, welches in $K[t]$ irreduzibel ist. Sei $\mathfrak{p}$ ein maximales Ideal von R, so daß $R/\mathfrak{p}$ ein endlicher Körper ist. Sei $\bar{\cdot} : R[t] \to (R/\mathfrak{p})[t]$ der Reduktionshomomorphismus.*

Ist dann $\bar{f}$ separabel und ist $\bar{f} = \prod_{i=i}^{s} \bar{f}_i$ die Faktorisierung von $\bar{f}$ in die irreduziblen Faktoren $\bar{f}_i$, so enthält $G(f, K)$ eine Permutation des Zykeltyps

$$(\deg(\bar{f}_1), \ldots, \deg(\bar{f}_s)).$$

Beweis. Siehe Abschnitt 2.10. □

Sei $f \in \mathbb{Z}[t]$ ein normiertes, irreduzibles Polynom vom Grad n. Anhand der Faktorisierungen von f modulo Primzahlen p kann man mittels des Satzes erkennen, welche Zykeltypen für Permutationen in $G(f, \mathbb{Q})$ vorkommen müssen. Dies liefert einschränkende Bedingungen an die möglichen, transitiven Untergruppen von S_n. Allerdings ist es im allgemeinen nicht möglich, $G(f, \mathbb{Q})$ damit eindeutig zu bestimmen.

Wir betrachten ein Beispiel. Es ist nicht sehr schwer, folgende Aussage zu zeigen: Ist n eine Primzahl und enthält eine transitive Permutationsgruppe G in S_n eine Transposition und ein Element der Ordnung n, so gilt $G = S_n$. Sei $f = t^5 - 5t^3 + 4t + 2$. Man kann nachrechnen, daß f modulo 3 irreduzibel und modulo 61 das Produkt dreier verschiedener Linearfaktoren und eines irreduziblen quadratischen Faktors ist. Nach der Aussage folgt $G(f, \mathbb{Q}) = S_5$. Hierfür hätten wir aber auch wie folgt argumentieren können: Man rechnet leicht nach, daß das Polynom f zwei komplexe Nullstellen und drei reelle Nullstellen besitzt. Daher enthält $G(f, \mathbb{Q})$ eine Transposition (die komplexe Konjugation) und wegen $5 = \deg(f) \mid \#G(f, \mathbb{Q})$ auch ein Element der Ordnung 5.

Betrachten wir $g = f - 3$, so besitzt g nur reelle Nullstellen, so daß die eben durchgeführte Schlußweise mit den komplexen und rellen Nullstellen nicht möglich ist. Hier ist g modulo 2 irreduzibel und modulo 79 das Produkt dreier verschiedener Linearfaktoren und eines irreduziblen quadratischen Faktors, so daß wiederum $G(g, \mathbb{Q}) = S_5$ gilt.

Sei $f \in \mathbb{Z}[t]$ normiert und irreduzibel. Über Satz 2.26 hinausgehend kann man zeigen, daß es für jeden Zykeltyp in $G(f, \mathbb{Q})$ eine Primzahl p gibt, so daß die Faktorisierung von f modulo p diesen Zykeltyp ergibt. Mann kann sogar zeigen, daß die Anzahl solcher $p \leq x$ im Verhältnis zu allen Primzahlen $p \leq x$ für $x \to \infty$ asymptotisch gleich dem Verhältnis der Anzahl der Konjugationsklassen von Permutationen aus $G(f, \mathbb{Q})$ dieses Zykeltyps und der Anzahl aller Konjugationsklassen von Permutationen aus $G(f, \mathbb{Q})$ ist (Satz von Tschebotarev).

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.

2.27 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.

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

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 der Beweis von Satz **??** ein konstruktives Verfahren angibt, mit dem man ein symmetrisches Polynom in den x_i als Polynom in den s_i darstellt.

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

Beweis. Fordern wir statt $h \in k[x_1, \ldots, x_n]$ nur $h \in k(x_1, \ldots, x_n)$, so ergibt sich die Existenz von h direkt aus dem Satz vom primitiven Element. Für jedes $g \in k[x_1, \ldots, x_n]$ ist $f = \mathrm{N}_{E/K}(g) = \prod_{\sigma \in S_n} \sigma(g) \in k[x_1, \ldots, x_n] \cap k(s_1, \ldots, s_n)$ nach Satz 2.27 (genauer $f \in k[s_1, \ldots, s_n]$ nach Satz 2.28). Besitzt $h \in k(x_1, \ldots, x_n)$ einen Nenner g, so können wir wegen $f \in k(s_1, \ldots, s_n)$ anstelle von h daher auch $fh \in k[x_1, \ldots, x_n]$ als primitives Element verwenden. □

Es gelten die Bezeichnungen von Satz 2.29 mit $k = \mathbb{Q}$. Satz 2.29 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 $G(f_0, \mathbb{Q}) \leq G$ muß dann $h(a_1, \ldots, a_n) \in \mathbb{Q}$ folgen, weil h unter G und unter $G(f_0, \mathbb{Q})$ als Permutationsgruppe, und somit $h(a_1, \ldots, a_n)$ unter $G(f_0, \mathbb{Q})$ als Gruppe von Körperautomorphismen invariant ist. Unter einer Zusatzbedingung gilt auch die Umkehrung dieser Implikation, aus $h(a_1, \ldots, a_n) \in \mathbb{Q}$ folgt $h \in \mathcal{F}_{E/K}(G(f_0, \mathbb{Q}))$ und daraus $G(f_0, \mathbb{Q}) \leq G$. Durch systematisches Testen von $h(a_1, \ldots, a_n) \in \mathbb{Q}$ 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 $G(f_0, \mathbb{Q}) \leq G_i$, also $h_j(a_1, \ldots, a_n) \in \mathbb{Q}$

für $1 \leq j \leq i$. Sei $G_{i+1} < G_i$ eine Kandidatengruppe, für die wir herausfinden wollen, ob $G(f_0, \mathbb{Q}) \leq G_{i+1}$ gilt. Wir definieren h_{i+1} als primitives Element von $F_{i+1} = \mathcal{F}_{E/K}(G_{i+1})$ über $F_i = \mathcal{F}_{E/K}(G_i) = K(h_1, \ldots, h_i)$ und testen $h_{i+1}(a_1, \ldots, a_n) \in \mathbb{Q}$ (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 $h(a_1, \ldots, a_n)$ 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. Wir erinnern dazu an die Definition der Diskriminante in Definition **??**.

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 2.28, daß $D(f) = h^2 \in k[s_1, \ldots, s_n]$ 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 2.29, daß $F = \mathcal{F}_{E/K}(G) = K(h)$ und $m_{h,K} = t^2 - D(f)$ ist.

2.30 Satz. *Sei $f_0 \in k[t]$ ein separables Polynom vom Grad n und* $\mathrm{char}(k) = 0$ *oder* $\mathrm{char}(k) > 2$. *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 $G(f_0, k) \not\subseteq A_n$, 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 2.30 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 2.27 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 gegebenenfalls 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 $\chi_1, \ldots, \chi_n$ 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.

2.31 Satz (Artin). *Sei G eine Halbgruppe und K ein Körper. Die Charaktere $\chi_1, \ldots, \chi_n$ 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 2.31 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.

2.32 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*) $\Rightarrow$ (*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 1.95 (*i*), folgt dies aus Satz 2.31.

(*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 1.95, daß $\mathrm{Tr}_{E/K} = 0$ gilt und die Bilinearform ist ausgeartet. □

2.7 Normalbasen

2.33 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.

2.34 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 2.31 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. □

2.35 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 2.34 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 Teilmenge H von G definieren wir $A^H = \{x \in A \,|\, \sigma(x) = x \text{ für alle } \sigma \in H\}$. Ist umgekehrt B eine Teilmenge 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 ein Normalteiler von G, so operieren G/H und G auf A^H in kompatibler Weise und A^H ist sowohl ein G- als auch ein G/H-Modul.

Um eine Verbindung zwischen Zwischenkörpern von E/K und Untergruppen von A herzustellen, 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.

2.36 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 $\mathrm{N}_{F_3/F_1}(x) = \prod_{\sigma,\tau} \sigma(\tau(x)) = \prod_\sigma \sigma(\prod_\tau \tau(x)) = \mathrm{N}_{F_2/F_1}(\mathrm{N}_{F_3/F_2}(x))$. □

Es sei angemerkt, daß die Normabbildung N_{F_2/F_1} nicht von der Galoiserweiterung E/K abhängt. Lemma 2.36 liefert einen zu Satz 1.94 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:

2.37 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 2.36 ist klar, daß die Implikation „$\Leftarrow$“ in Annahme 2.37 immer gilt. Wir verwenden Annahme 2.37 nur für den zweiten Teil des nachfolgenden Satzes 2.38.

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 $\wp^{-1}(\wp(A_K)) = A_K$.

2.38 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 2.37 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 $F'_i = K(b) \subseteq K(\wp^{-1}(\Delta))$. $\square$

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.

2.39 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 $\mathrm{Hom}(C, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(D, \mathbb{Z}/2\mathbb{Z}) \cong D \ncong C$.

2.40 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 $b_1b_2 \in \wp^{-1}(a_1a_2)$ und $(b_1b_2)/\sigma(b_1b_2) = (b_1/\sigma(b_1))(b_2/\sigma(b_2))$, 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 2.39 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 2.38, (ii). $\square$

Die Paarung von Satz 2.40 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 2.14 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 2.37:

2.41 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 2.36. $(i), \Rightarrow$: 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 2.31 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

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

die Bedingung $a = b - \sigma(b)$. $\square$

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

2.42 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 2.40. 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 2.41. $\square$

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 $n = n_1 p^r$ 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 2.40 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 2.39.

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.

2.43 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 2.39 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. □

2.44 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 2.40 existert diese und ist nicht ausgeartet. Außerdem ist die Bedingung von Lemma 2.43 an $D = A_K/\wp(A_K)$ nach dem Beweis von Satz 2.40 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 2.43. Seien $\psi_2 : \Delta/\wp(A_K) \mapsto F$ und $\psi_1 : F \mapsto \Delta/\wp(A_K)$ die Abbildungen wie in Satz 2.40.

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 2.43, (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 2.43, (i) erhalten wir, daß $[K(\wp^{-1}(\Delta)) : K] = (\Delta : \wp(A_K))$ gilt. Nach Satz 2.38, (ii) ist ψ_1 die inverse Abbildung von ψ_2 und ψ_2 ist surjektiv.

Nach Lemma 2.43, (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. □

Wählt man $K = \mathbb{Q}$, p_i die i-te Primzahl und $\Delta = \langle p_1, p_2, \dots\rangle\mathbb{Q}^{\times 2}$, so gilt $\Delta/\mathbb{Q}^{\times 2} \cong \coprod_{i\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ und $G(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots)/\mathbb{Q}) \cong \prod_{i\in\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ nach der ersten Isomorphie in Satz 2.44. In diesem Fall dürfen für die zweite Isomorphie in Satz 2.44 wirklich nur Homomorphismen mit abgeschlossenen Kern betrachtet werden, wie das Beispiel nach Lemma 2.39 zeigt.

2.9 Auflösbarkeit durch Radikale

2.45 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.

2.46 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. □

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 2.42 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.

2.47 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. $\square$

Wegen $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ und Satz 2.47, (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.

2.48 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 2.42 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 Faktorgruppe 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 2.42 ersehen wir, daß jede dieser zyklischen Erweiterungen vom Typ (ii) oder Typ (iii) in Definition 2.45 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. $\square$

2.49 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.

2.50 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.

2.51 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 2.27. Nach Satz 2.47, (iv) wissen wir, daß S_n für $n \leq 4$, aber nicht für $n \geq 5$ auflösbar ist. Der Rest ergibt sich aus Korollar 2.50. □

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.

2.10 Reduktionsprinzip

Wir führen noch einen fast vollständigen Beweis von Satz 2.26 an.

2.52 Satz. *Sei S/R eine Ringerweiterung der Integritätsringe R und S. Seien $E = \mathrm{Quot}(S)$ und $K = \mathrm{Quot}(R)$. Wir nehmen an, daß E/K endlich und galoissch ist, und daß $\sigma(S) = S$ für alle $\sigma \in G(E/K)$ gilt. Weiter sei $\mathfrak{p}$ maximales Ideal von R und $\mathfrak{q}$ ein maximales Ideal von S mit $\mathfrak{q} \cap R = \mathfrak{p}$.*

(i) Für alle $\sigma \in G(E/K)$ ist $\sigma(\mathfrak{q})$ ein maximales Ideal von S mit $\sigma(\mathfrak{q}) \cap R = \mathfrak{p}$ und aus $\sigma(\mathfrak{q}) \subseteq \mathfrak{q}$ folgt $\sigma(\mathfrak{q}) = \mathfrak{q}$.

(ii) Die Gruppe $G(E/K)$ operiert transitiv auf der Menge der maximalen Ideale $\mathfrak{q}'$ von S mit $\mathfrak{q}' \cap R = \mathfrak{p}$. Insbesondere gibt es höchstens $[E : K]$ verschiedene solche Ideale.

(*iii*) *Die Menge* $G_{\mathfrak{q}} = \{\sigma \,|\, \sigma \in G(E/K)$ *und* $\sigma(\mathfrak{q}) \subseteq \mathfrak{q}\}$ *ist eine Untergruppe von* $G(E/K)$. *Sei* $L = S/\mathfrak{q}$, $k = R/\mathfrak{p}$ *und* $\bar{\cdot} : S \to L$ *der kanonische Epimorphismus. Dann ist der Homomorphismus* $\phi : G_{\mathfrak{q}} \to \mathrm{Aut}_k(L)$, $\phi(\sigma)(x + \mathfrak{q}) = \sigma(x) + \mathfrak{q}$ *surjektiv.*

Beweis. (*i*): Weil σ ein Automorphismus von S ist, muß $\sigma(\mathfrak{q})$ ebenfalls ein maximales Ideal sein. Da σ auf R die Identität ist, gilt $\sigma(\mathfrak{p}) = \mathfrak{p}$ und es folgt $\sigma(\mathfrak{q}) \cap R \supseteq \mathfrak{p}$. Zum Beweis von $\subseteq$ sei sei $x \in \mathfrak{q}$ mit $\sigma(x) \in R$. Dann gilt $x \in R$ und $\sigma(x) = x \in \mathfrak{q} \cap R$, also $\sigma(x) \in \mathfrak{p}$. Es gelte $\sigma(\mathfrak{q}) \subseteq \mathfrak{q}$. Da $\mathfrak{q}$ und $\sigma(\mathfrak{q})$ maximale Ideale sind, folgt $\sigma(\mathfrak{q}) = \mathfrak{q}$.

(*ii*): Wir nehmen an, daß $G(E/K)$ nicht transitiv operiert. Dann gibt es ein von $\mathfrak{q}$ verschiedenes maximales Ideal $\mathfrak{q}'$ von S mit $\mathfrak{q}' \cap R = \mathfrak{p}$ und $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ für alle $\sigma \in G(E/K)$. Nach dem chinesischen Restsatz gibt es $a \in S$ mit $a \equiv 0 \bmod \mathfrak{q}$ und $a \equiv 1 \bmod \sigma^{-1}(\mathfrak{q}')$ für alle $\sigma \in G(E/K)$ (nur endlich viele Bedingungen, wobei die $\sigma^{-1}(\mathfrak{q}')$ möglicherweise gleich sein können). Anwenden von σ auf die Kongruenzen liefert $\sigma(a) \equiv 0 \bmod \mathfrak{q}$ für $\sigma = \mathrm{id}$ und $\sigma(a) \equiv 1 \bmod \mathfrak{q}'$ für alle $\sigma \in G(E/K)$. Sei $b = \mathrm{N}_{E/K}(a) = \prod_{\sigma \in G(E/K)} \sigma(a)$. Dann gilt $b \in R$ sowie $b \equiv 0 \bmod \mathfrak{q}$ und $b \equiv 1 \bmod q'$. Wegen $\mathfrak{p} = \mathfrak{q} \cap R = \mathfrak{q}' \cap R$ folgt daraus der Widerspruch $b \in \mathfrak{p}$ und $b \notin \mathfrak{p}$.

Eine endliche Gruppe G kann nicht transitiv auf einer Menge M mit $\#M > \#G$ operieren. Dies liefert die letzte Aussage.

(*iii*): Die Untergruppeneigenschaft folgt nach (*i*). Sei F der separable Abschluß von k in L. Dann ist F/k nach dem Satz vom primitiven Element endlich, denn für $b \in S$ mit $\bar{b}$ separabel über k gilt $m_{\bar{b},k} = \bar{g}$ mit einem normierten $g \in R[t]$, welches modulo $\mathfrak{p}$ irreduzibel und daher in $R[t]$ irreduzibel ist, und es folgt $\deg(m_{\bar{b},k}) = \deg(g) \leq [E : K]$. Da F/k endlich und separabel ist, gibt es ein $b \in S$, so daß $\bar{b}$ ein primitives Element von F über k ist. Wegen $\sigma(S) = S$ gilt $\sigma(b) \in S$ für alle $\sigma \in G(E/K)$. Daher gilt auch $m_{b,K} = \prod_{i=1}^{r}(t - b_i)$ mit geeigneten $b_i \in S$, $\overline{m_{b,K}}(\bar{b}) = \overline{m_{b,K}(b)} = 0$ und $m_{\bar{b},k} \,|\, \overline{m_{b,K}}$. Für $\sigma_0 \in \mathrm{Aut}_k(L)$ gilt $\sigma_0(\bar{b}) = \bar{b}_j$ für ein j, und hierdurch ist σ_0 eindeutig bestimmt (L/F ist rein inseparabel). Da $m_{b,K}$ irreduzibel ist und $m_{b,K}(b_j) = 0$ gilt, gibt es ein $\sigma \in \mathrm{Hom}_K(K(b), K(b_j))$ mit $\sigma(b) = b_j$. Aufgrund der Konstruktion gilt $\sigma(R[b]) = R[b_j]$ und $\sigma(R[b] \cap \mathfrak{q}) = R[b_j] \cap \mathfrak{q}$ (letzteres, da σ ein Lift von σ_0 bezüglich $\bar{\cdot}$ ist bzw. mit Reduktion modulo $\mathfrak{q}$ kommutiert). Wir können σ zu $\sigma \in G(E/K)$ fortsetzen. Dann gilt $\sigma(S) = S$ und $\sigma(\mathfrak{q})$ ist ein maximales Ideal von S mit $\sigma(\mathfrak{q}) \cap R[b_j] = \mathfrak{q} \cap R[b_j]$. Da $G(E/K(b_j))$ auf den maximalen Idealen $\mathfrak{q}'$ mit $\mathfrak{q}' \cap R[b_j] = \mathfrak{q} \cap R[b_j]$ nach Satz 2.52, (*ii*) transitiv operiert, gibt es ein $\tau \in G(E/K(b_j))$ mit $\tau(\sigma(\mathfrak{q})) = \mathfrak{q}$. Zusammenfassend erhalten wir $\tau(\sigma(b)) = b_j$ und $\tau(\sigma(\mathfrak{q})) = \mathfrak{q}$, also $\tau \circ \sigma \in G_{\mathfrak{q}}$ und $\phi(\tau \circ \sigma) = \sigma_0$. $\square$

Aufgrund der transitiven Operation von $G(E/K)$ auf den maximalen Idealen

$\mathfrak{q}'$ von S mit $\mathfrak{q}' \cap R = \mathfrak{p}$ ist $(G(E/K) : G_{\mathfrak{q}})$ gleich der Anzahl dieser verschiedenen maximalen Ideale.

Beweis von Satz 2.26. Seien $a_1, \ldots, a_n$ die Nullstellen von f und $E = K(a_1, \ldots, a_n)$ der Zerfällungskörper von f über K. Sei $S = R[a_1, \ldots, a_n]$ der von R und den a_i in E erzeugte Teilring. Da E ein Körper ist, ist S ein Integritätsring. Jedes $\sigma \in G(E/K)$ permutiert die a_i und ist die Identität auf R, daher gilt $\sigma(S) = S$.

Wir verwenden ohne Beweis, daß S ein maximales Ideal $\mathfrak{q}$ mit $\mathfrak{q} \supseteq \mathfrak{p}$ besitzt (Beweis erfolgt später). Dann gilt $R \neq \mathfrak{q} \cap R \supseteq \mathfrak{p}$ und wegen der Maximalität von $\mathfrak{p}$ folgt $\mathfrak{q} \cap R = \mathfrak{p}$.

Sei $k = R/\mathfrak{p}$ und $L = S/\mathfrak{q}$. Wegen $\mathfrak{q} \cap R = \mathfrak{p}$ ist L/k eine Körpererweiterung und L ist der Zerfällungskörper von $\bar{f}$ über k. Daher ist L/k nach Voraussetzung galoissch. Sei $G_{\mathfrak{q}} = \{\sigma \in G(E/K) \mid \sigma(\mathfrak{q}) \subseteq \mathfrak{q}\}$. Dann ist $G_{\mathfrak{q}}$ eine Untergruppe von $G(E/K)$ und wir erhalten den Homomorphismus $\phi : G_{\mathfrak{q}} \to G(L/k)$. Aufgrund der Separabilität von $\bar{f}$ ist ϕ injektiv. Nach Satz 2.52, (iii) ist ϕ surjektiv. Also ist ϕ ein Isomorphismus.

Mit der Nullstellenzuordnung $a_i \mapsto \bar{a}_i$ und der Separabilität von $\bar{f}$ ergibt sich, daß $G(\bar{f}, k)$ als Permutationsgruppe eine Untergruppe von $G(f, K)$ ist.

Da L/k eine Erweiterung endlicher Körper ist, ist $G(L/k)$ zyklisch. Sei $\sigma \in G(E/K)$ ein Urbild eines Erzeugers σ_0 von $G(L/k)$ unter ϕ. Ist $\bar{N}_i$ die Nullstellenmenge von $\bar{f}_i$ in L, so induziert σ_0 auf $\bar{N}_i$ eine zyklische Permutation der Ordnung $\#\bar{N}_i = \deg(\bar{f}_i)$. Daher induziert σ_0 auf der Nullstellenmenge $\bar{a}_1, \ldots, \bar{a}_n$ von $\bar{f}$ eine Permutation des Zykeltyps $(\deg(\bar{f}_1), \ldots, \deg(\bar{f}_s))$. Da $\bar{f}$ separabel ist, liefert σ genau die gleiche Permutation auf den Nullstellen $a_1, \ldots, a_n$. $\square$

Durch die Verwendung von Lokalisierungen können wir die Aussagen auf Primideale an Stelle von maximalen Idealen (geeignet) verallgemeinern. Wir erhalten dann zusammenfassend folgenden, allgemeinen Satz. Sei R ein Integritätsring und $f \in R[t]$ normiert. Sei $\mathfrak{p}$ ein Primideal von R und g das Bild von f in $(R/\mathfrak{p})[t]$ unter koeffizientenweiser Reduktion modulo $\mathfrak{p}$. Für separables g ist die Galoisgruppe $G(g, \mathrm{Quot}(R/\mathfrak{p}))$ bei geeigneter Nullstellenanordnung eine Untergruppe der Galoisgruppe $G(f, \mathrm{Quot}(R))$.

Kapitel 3

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.

3.1 Transzendenzbasen

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

3.1 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“.

3.2 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 3.2, (i) als Variablen aufgefaßt werden.

3.3 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 und E algebraisch über $K(A)$ ist.

3.4 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: Zum Beweis dieser Behauptung sei B eine solche Transzendenzbasis und $x \in C \backslash B$. Dann ist $B \cup \{x\}$ nach Lemma 3.2, (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 3.2, (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 $C = \{c_j \mid j \in J\}$. Für $B \subseteq C$ folgt $B = C$, da C andernfalls wegen $E/K(B)$ algebraisch nicht algebraisch unabhängig über K sein könnte. Dann folgt $n = m$ wie gewünscht. Für $B \not\subseteq C$ behaupten wir: Für jedes j gibt es ein i, so daß $b_i \notin C$ gilt, wir b_i durch c_j austauschen können und die resultierende Menge $\{c_j, b_1, \ldots, \hat{b}_i, \ldots, b_n\}$ eine Transzendenzbasis bleibt. Denn nach Voraussetzung gibt es ein Polynom $f \neq 0$ über K mit $f(c_j, b_1, \ldots, b_n) = 0$. Da C algebraisch unabhängig über K ist, gibt es ein i mit $b_i \notin C$, so daß $f(x_0, x_1, \ldots, x_n) = \sum_\nu g_\nu(x_0, x_1, \ldots, \hat{x}_i, \ldots, x_n) x_i^\nu = 0$ mit $g_\nu(x_0, x_1, \ldots, \hat{x}_i, \ldots, x_n) \neq 0$ für ein $\nu \geq$

1 ist (wäre dies für kein i möglich, so wäre $f(c_j, b_1, \ldots, b_n)$ ein polynomieller Ausdruck in Werten aus C und daher gälte $f = 0$, im Widerspruch zur Wahl von f). 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. Dann ist $E/K(\cup_{a \in C} B_a)$ algebraisch und 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. □

3.5 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 3.2, (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.

3.6 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. □

3.7 Satz. *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 B eine Transzendenzbasis von F über K, so ist B 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.

3.8 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.

3.2 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.

3.9 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.

3.10 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 3.4 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 Satz 3.7 linear unabhängig. Da $F/K(B)$ algebraisch und separabel und da $K(B)K^{p^{-\infty}}/K(B)$ nach Satz 1.65 rein inseparabel ist, sind $F/K(B)$ und $K(B)K^{p^{-\infty}}/K(B)$ nach Satz 1.73 linear disjunkt. Nach dem Satz über lineare Disjunktheit in Türmen 1.23, (*iv*) 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 paarweise verschiedenen 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 unter Berücksichtigung von Korollar **??** 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 $\mu_i \in K$ nicht alle Null gelten. Die g_i sind mit den f_i paarweise verschiedene Monome und daher linear unabhängig über K. Daher gilt $g \neq 0$ und $\deg(g) \leq \deg(f)/p < \deg(f)$. 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 3.10 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.

3.11 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 3.10.

(*ii*): Sei B eine separierende Transzendenzbasis. Dann sind $K(B)/K$ und $K^{p^{-\infty}}/K$ nach Satz 3.7 und $E/K(B)$ und $K(B)K^{p^{-\infty}}/K(B)$ nach Satz 1.75 linear disjunkt. Nach Satz 1.23, (*iv*) ergibt sich die lineare Disjunktheit von E/K und $K^{p^{-\infty}}/K$.

(*iii*): Folgt aus Satz 3.10 wegen $K^{p^{-\infty}} = K$.

(*iv*): Folgt direkt aus der Definition von „separabel“ oder aus Satz 3.10.

(*v*): Folgt aus Satz 3.10 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 und nach Satz 3.7 auch eine separierende Transzendenzbasis von HL/L. Nach (*ii*) ist HL/L separabel und daher G/L separiert erzeugt.

(*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 3.10 linear disjunkt. Da F/K und L/K nach Vorausetzung 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 3.10 separabel ist. □

Die Aussagen (*v*) und (*vi*) implizieren auch, daß ein Kompositum algebraisch disjunkter, separabler Erweiterungen wieder separabel ist.

3.3 Reguläre Erweiterungen

Wir verschärfen nun den Begriff „separabel“ und Satz 3.10.

3.12 Definition. Eine Körpererweiterung E/K heißt regulär, wenn E/K und der algebraische Abschluß K^a/K linear disjunkt sind.

3.13 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 3.10 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 1.73 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 1.75 und der Vorbemerkung $EK^{p^{-\infty}} \cap K^a = K^{p^{-\infty}}$ 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. □

3.14 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 3.13 und Satz 3.11, (iii).

(iii): Folgt aus Satz 3.13 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.

3.4 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 3.11, (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 3.10 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 $\mathbb{F}_p(z^{1/p}, x)/\mathbb{F}_p(z, x)$, 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. Nach der linearen Disjunktheit in Türmen sind auch $K/\mathbb{F}_p(z)$ und $\mathbb{F}_p(z^{1/p})/\mathbb{F}(z)$ nicht linear disjunkt und damit $K/\mathbb{F}_p(z)$ 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 3.13 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.

Kapitel 4

Moduln II

In diesem Kapitel werden das Tensorprodukt und die Begriffe projektiv, flach und lokal frei behandelt.

4.1 Tensorprodukte

Wir wollen auch kurz etwas zum Tensorprodukt sagen. Tensorprodukte bildet man von R-Moduln oder R-Algebren, und sie sind wieder R-Moduln bzw. R-Algebren. Wir betrachten vornehmlich den ersten Fall. Zur Vereinfachung sei R ein kommutativer Ring und M, N Moduln über R (links und rechts). Dies ist für das folgende keine wesentliche Einschränkung, spart aber ein paar Fälle und etwas Notation. Beim Tensorprodukt $M \otimes_R N$ handelt es sich um einen R-Modul, welcher von formalen Produkten $m \otimes n$ für $m \in M$ und $n \in N$ erzeugt wird. Die Elemente sind also von der Form $\sum_i m_i \otimes n_i$ für $m_i \in M$ und $n_i \in N$. Hierbei soll sich $\otimes$ wirklich wie eine Multiplikation verhalten, nur daß sie nicht „ausgeführt“ wird sondern nur generisch ausgeführt wird (also unter Eingabe von m und n eben den „abstrakten Wert“ $m \otimes n$ zurückliefert). Entsprechend wird gefordert $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ und analog für n_1, n_2. Die Angabe von R soll bedeuten, daß $mr \otimes n = m \otimes rn$ ist. Außerdem gelte $r(m \otimes n) = rm \otimes n = m \otimes rn$. Hier muß man im Nichtkommutativen etwas aufpassen, ob man von links oder rechts oder innen oder außen multiplizieren will. Beim Tensorprodukt von R-Algebren M und N soll per Definition auch noch $(m_1 \otimes n_1) \cdot (m_2 \otimes n_2) = (m_1 m_2) \otimes (n_1 n_2)$ gelten, doch dazu später.

4.1 Definition. Der R-Modul P zusammen mit einer R-bilinearen Abbildung $h : M \times N \to P$ heißt Tensorprodukt von M und N über R, wenn folgendes gilt. Ist g eine R-bilineare Abbildung $M \times N \to Q$ für einen beliebigen, weiteren R-Modul Q, so gibt es genau eine R-lineare Abbildung $f : P \to Q$ mit $g = f \circ h$.

4.2 Satz. *Für alle R-Moduln M und N existiert ein Tensorprodukt von M und N über R. Je zwei Tensorprodukte von M und N über R sind isomorph.*

Beweis. Zunächst zur Existenz. Sei V der von den Paaren $(m,n) \in M \times N$ erzeugte, freie R-Modul und I der Untermodul von V, welcher von den Elementen der Form $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, $(rm, n) - (m, rn)$ und $r(m,n) - (rm, n)$ erzeugt wird. Wir definieren die Abbildung $h : M \times N \to V/I$ durch $h(m,n) = (m,n) + I$. Die R-Bilinearität von h folgt unmittelbar aufgrund der Definition von I. Wir behaupten, daß V/I zusammen mit h ein Tensorprodukt von M und N über R ist.

Da V frei ist, können wir eine vorgegebene, bilineare Abbildung $g : M \times N \to Q$ zu einer linearen Abbildung $f' : V \to Q$ durch $f'((m,n)) = g(m,n)$ machen. Nun gilt $I \subseteq \ker(f')$ und durch Abspalten des Restklassenhomomorphismus $V \to V/I$ erhalten wir $f : V/I \to Q$. Damit gilt $f \circ h = g$, und die Existenz von f ist nachgewiesen. Es gibt aber auch nur einen einzigen Homomorphismus $f : V/I \to Q$ mit $f \circ h = g$, denn das Bild von h ist ein Erzeugendensystem von V/I. Damit ist V/I zusammen mit h tatsächlich ein Tensorprodukt von M und N über R.

Jetzt zur Eindeutigkeit bis auf Isomorphie. Sind B und B' zwei Tensorprodukte von M und N über R mit den zugehörigen bilinearen Abbildungen h und h', so gibt es $f \in \mathrm{Hom}_R(B, B')$ und $f' \in \mathrm{Hom}_R(B', B)$ mit $h' = f \circ h$ und $h = f' \circ h'$, also $h = f' \circ f \circ h$. Aufgrund der Eindeutigkeitsaussage für B folgt $f' \circ f = \mathrm{id}_B$, und durch Symmetrie $f \circ f' = \mathrm{id}_{B'}$. Also sind B und B' isomorph. □

4.3 Definition. Für je zwei R-Moduln M und N bezeichne $M \otimes_R N$ ein (festgewähltes) Tensorprodukt von M und N über R mit der bilinaren Abbildung $\cdot \otimes \cdot : M \times N \to M \otimes_R N$, $(x,y) \mapsto x \otimes y$.

Die Menge der bilinearen Abbildungen $M \times N \to Q$ bildet einen R-Modul, welcher in natürlicher Weise isomorph zum R-Modul $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, Q))$ ist. Aufgrund der Eindeutigkeit von f in Definition 4.1 erhalten wir eine Abbildung $\phi : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, Q)) \to \mathrm{Hom}_R(M \otimes_R N, Q)$, $g \mapsto f$ mit $g(x,y) = f(x \otimes y)$. Diese ist bijektiv: Sind g_1 und g_2 bilineare Abbildungen und f_1, f_2 die zugehörigen linearen Abbildungen und gilt $f_1 = f_2$, so ergibt sich auch $g_1 = f_1 \circ (\cdot \otimes \cdot) = f_2 \circ (\cdot \otimes \cdot) = g_2$. Also ist ϕ injektiv. Da für jedes lineare f die Abbildung $g = f \circ (\cdot \otimes \cdot)$ bilinear ist, ist ϕ auch surjektiv. Es gilt also $\mathrm{Hom}_R(M \otimes_R N, Q) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, Q))$ (in natürlicher Weise als R-Moduln). Die Abbildung $\cdot \otimes \cdot$ ist damit „die universelle“, auf $M \times N$ definierte bilineare Abbildung.

Die Elemente von $M \otimes_R N$ wie im Satz konstruiert sind also von der Form $\sum_i m_i \otimes n_i$, wobei $\otimes$ die Axiome einer Multiplikation erfüllt und mit der Multiplikation mit Elementen aus R verträglich ist. Speziell handelt es sich bei der Menge $\{m \otimes n \mid m \in M, n \in N\}$ um ein Erzeugendensystem von $M \otimes_R N$.

Seien nun M_1, M_2, N_1, N_2 Moduln über R und $f_i \in \mathrm{Hom}_R(M_i, N_i)$. Wir erhalten die Produktabbildung $f_1 \times f_2 : M_1 \times M_2 \to N_1 \times N_2$. Durch Komposition mit der bilinearen Abbildung $h_N : N_1 \times N_2 \to N_1 \otimes_R N_2$ ergibt dies eine bilineare Abbildung $M_1 \times M_2 \to N_1 \otimes N_2$, und wir können die bilineare Abbildung $h_M : M_1 \times M_2 \to M_1 \otimes M_2$ abspalten. Dies liefert eine lineare Abbildung $M_1 \otimes M_2 \to N_1 \otimes N_2$, welche mit $T(f_1, f_2)$ und als das Tensorprodukt von f_1 und f_2 bezeichnet wird. Sie ist durch $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ eindeutig bestimmt.

Zusammen erhalten wir eine Abbildung $\mathrm{Hom}_R(M_1, N_1) \times \mathrm{Hom}_R(M_2, N_2) \to \mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2)$, $(f_1, f_2) \mapsto T(f_1, f_2)$. Wegen $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ und $(f + g)(x) = f(x) + g(x)$ für $f, g \in \mathrm{Hom}_R(M_i, N_i)$ ist diese Abbildung bilinear, und somit erhalten wir eine lineare Abbildung

$$\mathrm{Hom}_R(M_1, N_1) \otimes_R \mathrm{Hom}_R(M_2, N_2) \to \mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2),$$

welche durch $f_1 \otimes f_2 \mapsto T(f_1, f_2)$ definiert ist. Mittels dieses Homomorphismus können wir $f_1 \otimes f_2$ also stets auch als Element von $\mathrm{Hom}_R(M_1 \otimes_R M_2, N_1 \otimes_R N_2)$ auffassen. Unter Verwendung von Satz 4.4, (ii) ist es nicht schwer zu beweisen, daß dies ein Isomorphismus ist, wenn die M_i und N_i beispielsweise endlich erzeugt und frei sind.

Die universelle Eigenschaft der Tensorprodukte und etwas „Diagrammjagd“ oder die konkrete Formel $T(f_1, f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ zeigen die folgende, bifunktorielle Eigenschaft von $T(\cdot, \cdot)$: Sind P_1, P_2 weitere R-Moduln und $g_i \in \mathrm{Hom}_R(N_i, P_i)$, so gilt $T(g_1 \circ f_1, g_2 \circ f_2) = T(g_1, g_2) \circ T(f_1, f_2)$.

Ein wichtiger Spezialfall ist $M_2 = N_2 = P_2 = Q$ und $f_2 = g_2 = \mathrm{id}$. Tensorieren mit Q liefert dann einen Funktor in der Kategorie der R-Moduln, ein Homomorphimus $f : M \to N$ wird auf $T(f, \mathrm{id}) : M \otimes_R Q \to N \otimes_R Q$ mit $T(f, \mathrm{id})(m \otimes q) = f(m) \otimes q$ abgebildet. Dieser wird in Satz 4.4, (iii) angewendet.

4.4 Satz. *Seien M, N, P, Q R-Moduln und M_i eine Familie von R-Moduln.*

(i) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$ *unter* $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$.

(ii) $M \otimes_R N \cong N \otimes_R M$ *unter* $x \otimes y \mapsto y \otimes x$.

(iii) $(\coprod_i M_i) \otimes_R N \cong \coprod_i (M_i \otimes_R N)$ *unter* $(\sum_i x_i) \otimes y \mapsto \sum_i (x_i \otimes y)$. *Das Tensorprodukt und die direkte Summenbildung sind also vertauschbar.*

(iv) *Ist* $M \to N \to P \to 0$ *eine exakte Sequenz, dann ist auch die zugehörige, mit Q tensorierte Sequenz* $M \otimes_R Q \to N \otimes_R Q \to P \otimes_R Q \to 0$ *exakt.*

Beweis. (i): Wir zeigen die Existenz eines Homomorphismus $f : (M \otimes_R N) \otimes_R P \to M \otimes_R (N \otimes_R P)$ mit $(x \otimes y) \otimes z \to x \otimes (y \otimes z)$. Wollen wir dies als Definition für f

nehmen, ergibt sich das Problem, daß wir die Wohldefiniertheit von f nachweisen müssen. Denn implizit extrahieren wir aus $(x \otimes y) \otimes z$ das unter Umständen nicht eindeutig bestimmte Paar (x, y, z) und definieren damit das Bild $x \otimes (y \otimes z)$. Um diesem Problem entgegenzutreten, verwendet man standardmäßig die universelle Eigenschaft des Tensorprodukts.

Für $z \in P$ starten wir zunächst mit $g_z : M \times N \to M \otimes_R (N \otimes_R P)$, $g_z(x, y) = x \otimes (y \otimes z)$. Dies ist eine wohldefinierte bilineare Abbildung, so daß es $f_x : M \otimes N \to M \otimes_R (N \otimes_R P)$ mit $f_z(x \otimes y) = x \otimes (y \otimes z)$ gibt. Nun sei $g : (M \otimes_R N) \times P \to M \otimes_R (N \otimes_R P)$, $g(x \otimes y, z) = f_z(x \otimes y) = x \otimes (y \otimes z)$. Dies ist ebenfalls eine wohldefinierte, bilineare Abbildung. Damit erhalten wir schließlich den Homomorphismus $f : (M \otimes_R N) \otimes_R P \to M \otimes_R (N \otimes_R P)$ mit $(x \otimes y) \otimes z \to x \otimes (y \otimes z)$.

Analoge Argumente zeigen die Existenz eines Homomorphismus $f' : M \otimes_R (N \otimes_R P) \to (M \otimes_R N) \otimes_R P$ mit $x \otimes (y \otimes z) \to (x \otimes y) \otimes z$. Da es bei den Elementen um Erzeugende der Tensorprodukte handelt, ergibt sich $f \circ f' = \mathrm{id}$ und $f' \circ f = \mathrm{id}$.

Ein im Prinzip gleicher, aber kompakterer Beweis kann mit Hilfe des Lemmas von Yoneda geführt werden (siehe S. **??**). Das geht wie folgt:

$$\begin{aligned}
\mathrm{Hom}_R((M \otimes_R N) \otimes_R P, \cdot) &\cong \mathrm{Hom}_R(M \otimes_R N, \mathrm{Hom}_R(P, \cdot)) \\
&\cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, \mathrm{Hom}_R(P, \cdot))) \\
&\cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N \otimes_R P, \cdot)) \\
&\cong \mathrm{Hom}_R(M \otimes_R (N \otimes_R P), \cdot).
\end{aligned}$$

Also gilt auch $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$, und zwar unter $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$, was man durch Nachverfolgen der einzelnen Isomorphismen sehen kann.

(ii): Geht analog zu (i) (direkt und mit Lemma von Yoneda).

(iii): Wir definieren die bilineare Abbildung $g : (\coprod_i M_i) \times N \to \coprod_i (M_i \otimes N)$ durch $((\sum_i x_i), y) \mapsto \sum_i (x_i \otimes y)$, wobei wir die direkte Summeneigenschaft von $\coprod_i M_i$ verwenden. Daraus erhalten wir den Homomorphismus $f : (\coprod_i M_i) \otimes N \to \coprod_i (M_i \otimes N)$ mit $(\sum_i x_i) \otimes y \mapsto \sum_i (x_i \otimes y)$. Umgekehrt definieren wir die bilineare Abbildung $g'_i : M_i \times N \to (\coprod_i M_i) \otimes N$ durch $(x_i, y) \mapsto x_i \otimes y$ und erhalten den Homomorphismus $f'_i : M_i \otimes N \to (\coprod_i M_i) \otimes N$ mit $x_i \otimes y \mapsto x_i \otimes y$. Die universelle Eigenschaft der direkten Summe angewendet auf die f'_i liefert jetzt einen Homomorphismus $f' : \coprod_i (M_i \otimes N) \to (\coprod_i M_i) \otimes N$ mit $\sum_i (x_i \otimes y) \mapsto (\sum_i x_i) \otimes y$. Die Abbildungsvorschriften für f und f' schreiben die Bilder von Erzeugendensystemen vor. Es ergibt sich $f \circ f' = \mathrm{id}$ und $f' \circ f = \mathrm{id}$.

Die Aussage (iii) wird in Satz 4.5 noch einmal in allgemeinerer Form bewiesen.

(iv): Seien $f_1 : M \to N$ und $f_2 : N \to P$ die Homomorphismen aus der exakten Sequenz und $g_1 : M \otimes_R Q \to N \otimes_R Q$ und $g_2 : N \otimes_R Q \to P \otimes_R Q$

die zugehörigen, tensorierten Homomorphismen. Die Aussage $0 \otimes_R Q = 0$ wird in Lemma 4.6, (i) bewiesen.

Wir zeigen zuerst, daß g_2 surjektiv ist. Jedes Element aus $P \otimes_R Q$ ist eine endliche Summe von Elementen der Form $p \otimes q$. Daher genügt es zu zeigen, daß jedes dieser Elemente im Bild von g_2 liegt. Zu $p \in P$ gibt es aber $n \in N$ mit $f_2(n) = p$ nach Voraussetzung. Dann gilt $g_2(n \otimes q) = f(n) \otimes q = p \otimes q$, was zu zeigen war. Dies ergibt die Exaktheit bei $P \otimes_R Q$.

Da das Tensorieren der Nullabbildung die Nullabbildung liefert, folgt wegen $f_2 \circ f_1 = 0$ auch $g_2 \circ g_1 = 0$, also $\mathrm{im}(g_1) \subseteq \ker(g_2)$. Sei nun $I = \mathrm{im}(g_1)$ und $g_2' : N \otimes_R Q/I \to P \otimes_R Q$ der nach dem Homomorphiesatz eindeutig bestimmte Homomorphismus mit $g_2'(n \otimes q + I) = g_2(n \otimes q)$. Zum Nachweis der Exaktheit bei $N \otimes_R Q$ müssen wir beweisen, daß g_2' injektiv ist. Dazu konstruieren wir einen Homomorphismus $h : P \otimes_R Q \to N \otimes_R Q/I$ mit $h \circ g_2' = \mathrm{id}$: Für $p \in P$ und $q \in Q$ sei $n \in N$ mit $f_2(n) = p$. Wir definieren $h' : P \times Q \to N \otimes_R Q/I$ durch $h'(p, q) := n \otimes q + I$. Dies ist wohldefiniert: Für $n_1, n_2 \in N$ mit $f_2(n_1) = f_2(n_2) = p$ gilt $f_2(n_1 - n_2) = 0$, also gibt es $m \in M$ mit $n_1 - n_2 = f_1(m)$. Dann folgt $n_1 \otimes q - n_2 \otimes q = (n_1 - n_2) \otimes q = f_1(m) \otimes q \in I$. Außerdem ist h' bilinear, wie leicht zu sehen ist. Es gibt also einen Homomorphismus $h : P \otimes_R Q \to N \otimes_R Q/I$ mit $h(p \otimes q) = n \otimes q + I$. Nach Konstruktion gilt $h \circ g_2' = \mathrm{id}$ auf der Menge der Elemente der Form $n \otimes q + I$ und damit auch auf ganz $N \otimes_R Q/I$.

Man kann (iv) auch kürzer beweisen. Tensorieren mit Q ist nämlich ein linksadjungierter Funktor des Funktors $\mathrm{Hom}_R(Q, \cdot)$, denn es besteht die natürliche Äquivalenz

$$\mathrm{Hom}_R(\cdot \otimes Q, \cdot) \cong \mathrm{Hom}_R(\cdot, \mathrm{Hom}_R(Q, \cdot)).$$

Aufgrund allgemeiner Überlegungen ist dann Tensorieren mit Q rechtsexakt, es gilt also (iv) (siehe Kapitel **??**). □

Bei nicht-kommutativen Ringen macht (ii) wenig Sinn, da man sonst die Multiplikationen von links oder rechts oder innen oder außen umordnen muß und leicht durcheinander kommen kann.

Die Aussage (iii) ist ein Spezialfall der folgenden Aussage für Kolimites von Diagrammen von R-Moduln (siehe Seite **??**ff.).

4.5 Satz. *Sei N ein R-Modul und $\mathcal{D}$ ein Diagramm von R-Moduln. Sei $\mathcal{D} \otimes_R N$ das Diagramm, welches aus $\mathcal{D}$ durch Tensorieren der in $\mathcal{D}$ vorkommenden Moduln mit N entsteht. Dann gilt*

$$(\varinjlim \mathcal{D}) \otimes_R N \cong \varinjlim (\mathcal{D} \otimes_R N).$$

Das Tensorprodukt und die Kolimesbildung sind also vertauschbar.

Beweis. Wir zeigen, daß $\varinjlim(\mathcal{D}\otimes_R N)$ ein Tensorprodukt von $\varinjlim\mathcal{D}$ und N ist. Sei $g : (\varinjlim\mathcal{D}) \times N \to Q$ bilinear. Für jedes D_i in $\mathcal{D}$ sei $\iota_i : D_i \to \varinjlim\mathcal{D}$ die Injektion. Zurückziehen entlang ι_i liefert bilineare Abbildungen $g_i : D_i \times N \to Q$, und lineare Abbildungen $f_i : D_i \otimes_R N \to Q$. Da Tensorieren ein Funktor ist, bilden die $D_i \otimes_R N$ das Diagramm $\mathcal{D} \otimes_R N$. Etwas Diagrammjagd und die universelle Eigenschaft von Tensorprodukten zeigt, daß die f_i einen Morphismus $\mathcal{D} \otimes_R N \to Q$ bilden. Die universelle Eigenschaft vom Kolimes zeigt, daß es eine lineare Abbildung $f : \varinjlim(\mathcal{D} \otimes_R N) \to Q$ gibt. Die Konstruktionsschritte von f sind jeder für sich genommen eindeutig umkehrbar, so daß insbesondere f eindeutig durch g bestimmt ist. Für $Q = \varinjlim(\mathcal{D} \otimes_R N)$ erhalten wir die Strukurabbildung $h : (\varinjlim\mathcal{D}) \times N \to \varinjlim(\mathcal{D} \otimes_R N)$ wie in (i) aus der Identität auf $\varinjlim(\mathcal{D} \otimes_R N)$.

Alternativ kann man auch allgemein argumentieren, daß linksadjungierte Funktoren Kolimites in Kolimites überführen. Das geht unter Verwendung von Satz **??** im wesentlichen so:

$$\begin{aligned}
\mathrm{Hom}_R((\varinjlim\mathcal{D}) \otimes_R N, \cdot) &\cong \mathrm{Hom}_R(\varinjlim\mathcal{D}, \mathrm{Hom}_R(N, \cdot)) \\
&\cong \varinjlim \mathrm{Hom}_R(\mathcal{D}, \mathrm{Hom}_R(N, \cdot)) \\
&\cong \varinjlim \mathrm{Hom}_R(\mathcal{D} \otimes_R N, \cdot) \\
&\cong \mathrm{Hom}_R(\varinjlim(\mathcal{D} \otimes_R N), \cdot).
\end{aligned}$$

Mit dem Lemma von Yoneda schließt man jetzt $(\varinjlim\mathcal{D})\otimes_R N \cong \varinjlim(\mathcal{D}\otimes_R N)$. □

Hier sind ein paar einfache Formeln, die bei der Berechnung von vorgelegten Tensorprodukten hilfreich sind.

4.6 Lemma. *Seien M, N Moduln über R.*

(*i*) *Ist $N = Rn$ frei vom Rang eins, so gilt $M \otimes_R N \cong M$ unter $m \otimes rn \mapsto rm$. Ist $N = \{0\}$, so gilt $M \otimes_R N \cong \{0\}$.*

(*ii*) *Sind die m_i und n_j ein Erzeugendensystem (eine Basis) von M bzw. N, so ist $m_i \otimes n_j$ ein Erzeugendensystem (eine Basis) von $M \otimes_R N$.*

Sind die n_j eine Basis von N, so schreibt sich jedes Element aus $M \otimes_R N$ als Summe $\sum_j x_j \otimes n_j$ mit eindeutig bestimmten $x_j \in M$.

(*iii*) *Es gilt $(M/I) \otimes_R (N/J) \cong M \otimes_R N/(I \otimes N + M \otimes J)$ für Untermoduln $I \subseteq M$ und $J \subseteq N$ unter $(m + I) \otimes (n + J) \mapsto (m \otimes n) + (I \otimes N + M \otimes J)$.*

(*iv*) *Es gelte $\sum_i m_i \otimes n_i = 0$ für $m_i \in M$ und $n_i \in N$, wobei die n_i ein Erzeugendensystem von N bilden. Dann gibt es $a_{i,j} \in R$ und $m'_j \in M$ mit $m_i = \sum_j a_{i,j} m'_j$ und $\sum_i a_{i,j} n_i = 0$ für alle j.*

Beweis. (i): Sei $N = Ry$ und $h : M \times N \to M$ die durch $(x, ry) \mapsto rx$ definierte, bilineare Abbildung. Jede bilineare Abbildung $f : M \times N \to P$ liefert mit $x \mapsto f(x, y)$ eine lineare Abbildung $g : M \to P$ mit $f = g \circ h$, wobei g wegen der Surjektivität von h eindeutig bestimmt ist. Die Eindeutigkeit des Tensorprodukts ergibt $M \cong M \otimes_R N$.

Bilineare Abbildungen auf $M \times \{0\}$ sind alles Nullabbildungen, entsprechen also den linearen Abbildungen auf $\{0\}$. Mit der bilinearen Abbildung $h : M \times \{0\} \to \{0\}$ liefert eine ähnliche Schlußweise wie eben $\{0\} \cong M \otimes_R \{0\}$.

(ii): Für $v = \sum_i \lambda_i m_i$ und $w = \sum_j \mu_j n_j$ gilt $v \otimes w = \sum_{i,j} \lambda_i \mu_j (m_i \otimes n_j)$. Da jedes Element in $M \otimes_R N$ eine Summe von Elementen der Form $v \otimes w$ ist, folgt die Aussage über die Erzeugendensysteme.

Sei N frei mit Basis n_j. Aus $N = \oplus_j Rn_j$ folgt $M \otimes_R N \cong \oplus_j (M \otimes_R Rn_j) \cong \oplus_j M$ nach Satz 4.4, (ii) und nach (i). Unter den Isomorphismen wird $\sum_j x_j \otimes n_j$ mit $x_j \in M$ auf das Element von $\oplus_j M$ abgebildet, welches x_j an der j-ten Koordinate enthält. Die x_j sind also durch das Element $\sum_j x_j \otimes n_j$ eindeutig bestimmt. Dies zeigt die zweite Aussage in (ii).

Ferner bilden hier die $m_i \otimes n_j$ eine Basis des j-ten Komponentenmodul M, so daß $m_i \otimes n_j$ für i, j eine Basis von $M \otimes_R N$ ist.

(iii): Ergibt sich durch dreimalige Anwendung von Satz 4.4, (iii): Im folgenden sind die angegebenen „Untermoduln“ geeignet einzubetten. Es gilt $M/I \otimes N/J \cong (M/I \otimes N)/(M/I \otimes J)$ (tensorieren mit $M/I \otimes -$) und $M/I \otimes N \cong (M \otimes N)/(I \otimes N)$ (tensorieren mit $- \otimes N$) und $M/I \otimes J \cong (M \otimes J)/(I \otimes J)$ (tensorieren mit $- \otimes J$). Wir erhalten $M/I \otimes N/J \cong ((M \otimes N)/(I \otimes N))/((M \otimes J)/(I \otimes J)) \cong (M \otimes N)/(I \otimes N + M \otimes J)$, was zu zeigen war.

Eine bilineare Abbildung auf $(M/I) \times (N/J)$ entspricht den bilinearen Abbildungen auf $M \times N$, welche auf $I \times N$ und $M \times J$ Null sind, und diese wiederum entsprechen den linearen Abbildungen auf $M \otimes N$, deren Kern $I \otimes N + M \otimes J$ enthält. Dies verdeutlicht ebenfalls $M/I \otimes N/J \cong M \otimes N/(I \otimes N + M \otimes J)$.

(iv): Gibt es solche Elemente $a_{i,j}$ und m'_i, so folgt $\sum_i m_i \otimes n_i = \sum_i \big(\sum_j a_{i,j} m'_j\big) \otimes n_i = \sum_j m'_j \otimes \big(\sum_i a_{i,j} n_i\big) = 0$.

Für die Rückrichtung sei V frei und $f : V \to N$ surjektiv, so daß $n_i = f(g_i)$ für eine Basis g_i von V gilt. Die Sequenz $U \to V \to N \to 0$ mit $U = \ker(f)$ ist exakt. Aufgrund von Theorem 4.4, (iii) ist damit auch die Sequenz $M \otimes_R U \to M \otimes_R V \to M \otimes_R N \to 0$ exakt. Weil das Element $\sum_i m_i \otimes g_i$ auf Null abgebildet wird, gibt es aufgrund der Exaktheit bei V Elemente $m'_j \in M$ und $y_j \in U$ mit $\sum_i m_i \otimes g_i = \sum_j m'_j \otimes y_j$. Seien $a_{i,j} \in R$ mit $y_j = \sum_i a_{i,j} g_i$. Nach dem Beweis von (ii) folgt aus $\sum_i m_i \otimes g_i = \sum_j m'_j \otimes \big(\sum_i a_{i,j} g_i\big) = \sum_i \big(\sum_j a_{i,j} m'_j\big) \otimes g_i$ durch Koeffizientenvergleich, daß $\sum_j a_{i,j} m'_j = m_j$ ist. Schließlich gilt $0 = f(y_j) = \sum_i a_{i,j} n_i$ für alle j. $\square$

Die Aussage (iv) führt das Rechnen in Tensorprodukten auf lineare Algebra zurück. Die Definition des Tensorprodukts ist dafür nicht besonders geeignet. Die $a_{i,j}$ können nach dem Beweis als „Strukturkonstanten“ gewählt werden.

Ist R ein Ring und I ein Ideal, so gilt $I \otimes_R R \cong I$ nach (i), denn wegen $1 \in R$ ist R ein freier R-Modul vom Rang eins. Nach (iii) ergibt sich damit speziell $(R/I) \otimes_R (R/J) \cong R/(I+J)$ für Ideale I, J von R.

Ein paar Beispiele: $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$, $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^3 \cong \mathbb{Z}^6$. Weiter $\mathbb{Z}/6\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ nach der eben gemachten Bemerkung. Ähnlich $\mathbb{Z}/3\mathbb{Z} \otimes 7\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$. Es gilt auch $1 \otimes 3 = 3 \otimes 1 = 0 \otimes 1 = 0$. Mit diesen Beispielen und Satz 4.4, (ii) kann man Tensorprodukte von endlich erzeugten Moduln über Hauptidealringen nach Satz **??** leicht berechnen.

4.7 Satz. *Sei M ein R-Modul und $I \subseteq R$ ein Ideal. Dann gilt*

$$(R/I) \otimes_R M \cong M/IM$$

unter der Abbildung $(r+I) \otimes m \mapsto rm + IM$.

Beweis. Wir tensorieren die exakte Sequenz $0 \to I \to R \to R/I \to 0$ über R mit M und erhalten nach Lemma 4.4, (iii) und Lemma 4.6, (i) die exakte Sequenz $I \otimes_R M \to M \to (R/I) \otimes_R M \to 0$. Das Bild von $I \otimes M$ in M ist hierbei IM. Die Aussage über die Abbildung ergibt sich durch Nachverfolgen der einzelnen Abbildungen in den exakten Sequenzen. □

4.2 Induzierte und koinduzierte Moduln

Ist M ein R-Modul und $f : R \to S$ ein Ringhomomorphismus (also S eine R-Algebra), dann ist S auch ein R-Modul und wir können $S \otimes_R M$ als R-Modul definieren. Durch $s(x \otimes m) = (sx) \otimes m$ können wir $S \otimes_R M$ zu einem S-Modul machen. Dies erlaubt es, den Ring eines Moduls zu wechseln. Eine formalere Begründung dieser Konstruktion lautet wie folgt. Durch $(s_1, s_2, m) \mapsto (s_1 s_2) \otimes m$ wird eine 3-lineare Abbildung $S \times S \times M \to S \otimes_R M$ definiert. Dies liefert eine lineare Abbildung $S \otimes_R (S \otimes_R M) \to S \otimes_R M$ und damit eine bilineare Abbildung $S \times (S \otimes_R M) \to S \otimes_R M$, $(s_1, s_2 \otimes m) \mapsto (s_1 s_2) \otimes m$.

Eine alternative Konstruktion, welche aus M einen S-Modul macht, geht wie folgt: Wir betrachten die abelsche Gruppe $\mathrm{Hom}_R(S, M)$ und machen diese für $f \in \mathrm{Hom}_R(S, M)$ durch $(s \cdot f)(x) := f(sx)$ in einen S-Modul.

Wir bezeichnen $S \otimes_R M$ als den entlang f induzierten Modul von M und $\mathrm{Hom}_R(S, M)$ als den entlang f koinduzierten Modul von M. Die Zuordnungen $M \mapsto S \otimes_R M$ und $M \mapsto \mathrm{Hom}_R(S, M)$ liefern Funktoren der Kategorie der R-Moduln in die Kategorie der S-Moduln.

Wir können beide Prozesse in gewissem Sinne auch wieder rückgängig machen. Ist N ein S-Modul, so können wir N auch als R-Modul mittels $r \cdot x := f(r)x$ für $x \in N$ auffassen. Diesen Modul bezeichnen wir mit $N|_R$. Die Zuordnung $N \mapsto N|_R$ liefert einen Funktor der Kategorie der S-Moduln in die Kategorie der R-Moduln.

4.8 Satz. *Sei $f : R \to S$ ein Ringhomomorphismus, M ein R-Modul und N ein S-Modul. Dann gibt es in M und N funktorielle Isomorphieen abelscher Gruppen*

$$\mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, N|_R)$$

$$\mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) \cong \mathrm{Hom}_R(N|_R, M).$$

Beweis. (Skizze) Die Menge $\mathrm{Hom}_S(S \otimes_R M, N)$ kann als Menge von R-bilinearen Abbildungen $\phi : S \times M \to N$ angesehen werden, für die zusätzlich $\phi(s \times m) = s\phi(1 \times m)$ gilt. So ein ϕ wird allerdings durch die R-lineare Abbildung $\psi(m) = \phi(1 \times m)$ definiert, welche ein Element in $\mathrm{Hom}_R(M, N|_R)$ ist. Diese Zuordung ist auch umkehrbar. Daraus ergibt sich die erste Isomorphie.

Die zweite Isomorphie ist wie folgt gegeben. Sei $f \in \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M))$. Dann ist das isomorphe Bild $g \in \mathrm{Hom}_R(N|_R, M)$ von f durch $g(x) = f(x, 1)$ gegeben. Ist $g \in \mathrm{Hom}_R(N|_R, M)$, so erhalten wir das isomorphe Urbild $f \in \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M))$ von g durch $f(x, s) = g(sx)$. Man prüft leicht nach, daß hierdurch ein Isomorphismus gegeben wird. □

(Der Satz besagt, daß $M \mapsto S \otimes_R M$ linksadjungierter Funktor zum rechtsadjungierten Funktor $N \mapsto N|_R$ ist, und daß $M \mapsto \mathrm{Hom}_R(S, M)$ rechtsadjungierter Funktor zum linksadjungierten Funktor $N \mapsto N|_R$ ist. Speziell ist $M \mapsto S \otimes_R M$ damit rechtsexakt, $M \mapsto \mathrm{Hom}_R(S, M)$ linksexakt und $N \to N|_R$ exakt.)

Sei S eine R-Algebra, M ein S-Modul und N ein R-Modul. Dann wird $M|_R \otimes_R N$ vermöge $s(m \otimes n) := (sm \otimes n)$ zu einem S-Modul, den wir mit $M \otimes_R N$ bezeichnen. Dies ist im allgemeinen ein von $S \otimes_R (M|_R \otimes_R N)$ verschiedener S-Modul.

4.9 Satz. *Sei S eine R-Algebra, M ein S-Modul und N ein R-Modul. Dann gilt*

$$M \otimes_S (S \otimes_R N) \cong M \otimes_R N$$

als S-Moduln unter $m \otimes (s \otimes n) \mapsto (sm) \otimes n$. Die Isomorphie ist zudem funktoriell in M und N.

Beweis. Ähnlich wie bei der Assoziativität des Tensorprodukts. Die Abbildung $(m, s, n) \mapsto (sm) \otimes n$ ist R-bilinear in s und n und S-bilinear in m und s. Daher gibt es den S-Homomorphismus $m \otimes (s \otimes n) \mapsto (sm) \otimes n$. Umgekehrt ist $(m, n) \mapsto$

$m \otimes (1 \otimes n)$ in m und n R-bilinear und in m S-linear. Daher gibt es den S-Homomorphismus $m \otimes n \mapsto m \otimes (1 \otimes n)$. Die beiden S-Homomorphismen sind invers zueinander, was die Isomorphie beweist.

Die Funktorialität in M und N ergibt sich aus der konkreten Form der Isomorphie zusammen mit den funktoriellen Eigenschaften des Tensorprodukt. □

Die Funktoren „Tensorieren“ und „Induzieren“ vertauschen also in dem im Satz angegebenen Sinn.

Hier ist noch ein Vergleich induzierter und koinduzierter Moduln für R-Algebren S, welche als R-Modul frei von endlichem Rang sind.

4.10 Satz. *Ist die R-Algebra S als R-Modul frei von endlichem Rang und M ein R-Modul, so gibt es eine Isomorphie von S-Moduln*

$$S \otimes_R M \cong \mathrm{Hom}_R(S, M).$$

Beweis. Übung. □

4.3 Lokalisierungen

Sei M ein R-Modul und U eine multiplikativ abgeschlossene Teilmenge mit $1 \in U$ von R. Wir definieren die Lokalisierung $M[U^{-1}]$ genau wie $R[U^{-1}]$ als die Menge der formalen Brüche m/u für $m \in M$ und $u \in U$, wobei $m_1/u_1 = m_2/u_2$ genau dann gelten soll, wenn es ein $v \in U$ mit $vu_2m_1 = vu_1m_2$ gibt. Unter Verwendung der üblichen Bruchrechentechnik wird $M[U^{-1}]$ ein $R[U^{-1}]$-Modul. Die Elemente $u/1$ mit $u \in U$ sind Einheiten in $R[U^{-1}]$, da $(u/1)(1/u) = 1$ gilt. Wir erhalten auch eine R-lineare Abbildung $h : M \to M[U^{-1}]$, $m \mapsto m/1$. Der Kern von h besteht genau aus allen denjenigen $m \in M$, für die es ein $u \in U$ mit $um = 0$ gibt.

4.11 Satz. *Sei M ein R-Modul und $U \subseteq R$ multiplikativ abgeschlossen. Dann gilt*

$$R[U^{-1}] \otimes_R M \cong M[U^{-1}]$$

unter der Abbildung $(r/u) \otimes m \mapsto (rm)/u$.

Beweis. Sei $h : R[U^{-1}] \times M \to M[U^{-1}]$ die Multiplikationsabbildung $r/u \times m \mapsto (rm)/u$ und $f : R[U^{-1}] \otimes_R M \to M[U^{-1}]$ der zugehörige R-lineare Homomorphismus (ist auch $R[U^{-1}]$-linear). Es ist offensichtlich, daß h und f surjektiv sind. Zum Beweis der Injektivität von f sei $f(\sum_i (r_i/u_i) \otimes m_i) = 0$ mit $r_i \in R$, $u_i \in U$ und $m_i \in M$ beliebig. Es gibt $u \in U$ und $m \in M$ mit $\sum_i (r_i/u_i) \otimes m_i = (1/u) \otimes m$ ($(r_i/u_i) \otimes m_i = (1/u_i)(1 \otimes r_i m_i)$ schreiben, ausklammern und auf „Hauptnenner“ bringen). Da u in $R[U^{-1}]$ eine Einheit ist, folgt aus $f((1/u) \otimes m) = 0$

durch Multiplikation mit u bereits $uf((1/u)(1 \otimes m)) = f(u(1/u)(1 \otimes m)) = f(1 \otimes m) = m/1 = 0$ in $M[U^{-1}]$. Es gibt also $v \in U$ mit $vm = 0$ und daher $v(1 \otimes m) = 1 \otimes (vm) = 1 \otimes 0 = 0$. Da v in $R[U^{-1}]$ eine Einheit ist, gilt $1 \otimes m = 0$ und auch $(1/u) \otimes m = 0$ in $R[U^{-1}] \otimes_R M$. □

Lokalisieren entspricht also dem Tensorieren mit $R[U^{-1}]$ über R und ist damit ein Funktor. Zu einem Homomorphismus $f : M \to N$ gibt es also einen Homomorphismus $g : M[U^{-1}] \to N[U^{-1}]$ mit $m/u \mapsto f(m)/u$.

4.12 Satz. *Sei $0 \to I \to M \to N$ eine exakte Sequenz. Dann ist auch die zugehörige, lokalisierte Sequenz $0 \to I[U^{-1}] \to M[U^{-1}] \to N[U^{-1}]$ exakt.*

Beweis. Seien $f_1 : I \to M$ und $f_2 : M \to N$ die Homomorphismen aus der exakten Sequenz und seien $g_1 : I[U^{-1}] \to M[U^{-1}]$ und $g_2 : M[U^{-1}] \to N[U^{-1}]$ die zugehörigen lokalisierten Homomorphismen.

Wir zeigen zuerst, daß g_1 injektiv und die Sequenz somit bei $I[U^{-1}]$ exakt ist. Ist $m/u \in \ker(g_1)$, so gilt $g_1(m/u) = f_1(m)/u = 0$ und daher gibt es ein $v \in U$ mit $vf_1(m) = 0$. Es folgt $f_1(vm) = 0$ und wegen der Injektivität von f_1 auch $vm = 0$. Somit gilt $m/u = 0$ und die Sequenz ist bei $I[U^{-1}]$ exakt.

Für jeden Monomorphismus $\phi : I \to M$ ist die Sequenz $0 \to I \to M \to M/\phi(M)$ mit der Nullabbildung, ϕ und dem kanonischen Epimorphismus exakt. Nach dem vorhergehenden Absatz überführt Lokalisieren also Monomorphismen in Monomorphismen.

Die Exaktheit bei $M[U^{-1}]$ ergibt sich durch konkretes Nachrechnen wie oben oder allgemein aus der Rechtsexaktheit des Lokalisierens bzw. des Tensorprodukts wie folgt. Wir können f_2 in der Form $i \circ f_2'$ mit $f_2' : M \to f_2(M)$ und $i : f_2(M) \to N$ schreiben. Seien $g_2' : M[U^{-1}] \to f_2(M)[U^{-1}]$ und $j : f_2(M)[U^{-1}] \to N[U^{-1}]$ die lokalisierten Homomorphismen. Dann gilt wegen der Funktoreigenschaft des Lokalisierens bzw. des Tensorprodukts $g_2 = j \circ g_2'$. Mit i ist auch j nach dem bereits Bewiesenen ein Monomorphismus. Also folgt $\ker(g_2') = \ker(g_2)$. Die exakte Sequenz $I \to M \to f_2(M) \to 0$ mit f_1, f_2' und der Nullabbildung geht wegen der Rechtsexaktheit des Tensorprodukts in die exakte Sequenz $I[U^{-1}] \to M[U^{-1}] \to f_2(M)[U^{-1}] \to 0$ mit g_1, g_2' und der Nullabbildung über. Also gilt $\ker(g_2) = \ker(g_2') = \mathrm{im}(g_1)$ und wir erhalten die Exaktheit unserer Ausgangssequenz bei M. □

Satz 4.12 und Satz 4.4, (iv) bedeuten, daß Lokalisieren ein exakter Funktor ist. Ein exakter Funktor erhält Kerne und Kokerne.

Hier ist eine Anwendung des Lokalisierens: Nach der obigen Aussage über den Kern der Lokalisierungsabbildung h kann ein torsionsfreier Modul M über einem Integritätsring R in den Vektorraum $\mathrm{Quot}(R) \otimes_R M$ eingebettet werden.

Bei der Untersuchung von solchen Moduln M können wir also bei Bedarf auf einen umgebenden Vektorraum zurückgreifen.

Sei M ein R-Modul und $\mathfrak{p}$ ein Primideal von R. Sei $U = R\backslash\mathfrak{p}$. Wir definieren dann die Lokalisierung von M bei $\mathfrak{p}$ als $M_\mathfrak{p} = M[U^{-1}]$. Dies ist ein $R_\mathfrak{p}$-Modul. Ist N ein weiterer R-Modul und $\phi : M \to N$ ein Homomorphismus, so erhalten wir durch Lokalisieren den Homomorphismus $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$.

Für $f \in R$ sei $U = \{f^i \mid i \in \mathbb{Z}^{\geq 0}\}$. Wir definieren die Lokalisierung von M an f als $M_f = M[U^{-1}]$. Dies ist ein R_f-Modul, wobei $R_f = R[U^{-1}]$. Ist N ein weiterer R-Modul und $\phi : M \to N$ ein Homomorphismus, so erhalten wir durch Lokalisieren den Homomorphismus $\phi_f : M_f \to N_f$.

4.13 Satz. *Sei M ein R-Modul.*

(*i*) *Für $m \in M$ ist $m = 0$ genau dann, wenn $m/1 = 0$ in $M_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$ von R gilt.*

(*ii*) *Es ist $M = 0$ genau dann, wenn $M_\mathfrak{m} = 0$ für jedes maximale Ideal $\mathfrak{m}$ von R gilt.*

Sei $\phi : M \to N$ ein Homomorphismus der R-Moduln M und N und sei E eine der Eigenschaften „Isomorphismus“, „Monomorphismus“, „Epimorphismus“. Seien $f_i, g_i \in R$ mit $1 = \sum_i f_i g_i$. Dann sind äquivalent:

(*iii*) *Der Homomorphismus ϕ besitzt die Eigenschaft E.*

(*iv*) *Die Homomorphismen ϕ_{f_i} besitzen die Eigenschaft E.*

(*v*) *Die Homomorphismen $\phi_\mathfrak{m}$ besitzen die Eigenschaft E für alle maximalen Ideale $\mathfrak{m}$ von R.*

Beweis. (*i*): Das Element $m/1$ ist genau dann Null in $M_\mathfrak{m}$, wenn es ein $u \in R\backslash\mathfrak{m}$ mit $um = 0$ gibt, und dies ist äquivalent zur Bedingung $\mathrm{Ann}_R(m) \not\subseteq \mathfrak{m}$. Nun gilt $m = 0$ genau dann, wenn $\mathrm{Ann}_R(m) = R$ ist, und dieses gilt genau dann, wenn $\mathrm{Ann}_R(m) \not\subseteq \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m}$ gilt.

(*ii*): Folgt aus (*i*).

(*iii*) $\Rightarrow$ (*iv*): Klar, da Lokalisieren an f_i ein exakter Funktor ist.

(*iv*) $\Rightarrow$ (*v*): Für jedes $\mathfrak{m}$ gibt es ein f_i mit $f_i \in R\backslash\mathfrak{m}$, da das von den f_i erzeugte Ideal ganz R ist. Sei $\mathfrak{m}'$ das von $\mathfrak{m}$ in R_{f_i} erzeugte, maximale Ideal. Dann gilt $\phi_\mathfrak{m} = (\phi_{f_i})_{\mathfrak{m}'}$ und die Aussage folgt, da Lokalisieren bei $\mathfrak{m}'$ ein exakter Funktor ist.

(*v*) $\Rightarrow$ (*iii*): Sei $E =$ „Monomorphismus“. Der Homomorphimus ϕ ist genau dann ein Monomorphismus, wenn $\ker(\phi) = 0$ gilt. Da Lokalisieren Kerne in Kerne

überführt, gilt $0 = \ker(\phi_{\mathfrak{m}}) = \ker(\phi)_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m}$, also $\ker(\phi) = 0$ nach (ii).

Sei $E =$ „Epimorphismus“. Der Homomorphimus ϕ ist genau dann ein Epimorphismus, wenn $\operatorname{coker}(\phi) = 0$ gilt. Da Lokalisieren Kokerne in Kokerne überführt, gilt $0 = \operatorname{coker}(\phi_{\mathfrak{m}}) = \operatorname{coker}(\phi)_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m}$, also $\operatorname{coker}(\phi) = 0$ nach (ii).

Die Aussage für $E =$ „Isomorphismus“ folgt aus der für „Monomorphismus“ und „Epimorphismus“. □

4.4 Flache Moduln

Ist $I \subseteq R$ ein Ideal, so motivieren Satz 4.7 und Satz 4.11 auch die Formel $I \otimes_R M \cong IM$, wobei der Isomorphismus durch die Multiplikationsabbildung $i \otimes m \mapsto im$ gegeben sein sollte. Dies ist jedoch im allgemeinen falsch, die Abbildung ist zwar immer surjektiv (wegen der Rechtsexaktheit des Tensorprodukts, oder auch direkt einsichtig), aber nicht unbedingt injektiv. Für $I = Ra$ gilt zum Beispiel $I \otimes_R (R/I) \cong R \otimes_R (R/I) \cong R/I$, aber $I(R/I) = \{0\}$. Insbesondere ist das Bild von $I \otimes_R (R/I)$ in $R \otimes_R (R/I)$ gleich Null, denn in $R \otimes_R (R/I)$ gilt $ra \otimes x = r \otimes ax = r \otimes 0 = 0$. Man mache sich klar, daß man in $I \otimes_R (R/I)$ so nicht rechnen kann und vergleiche mit dem Kriterium in Lemma 4.6, (iv). Die injektive Abbildung $I \to R$ wurde also durch Tensorierung mit R/I in eine nicht injektive Abbildung überführt (nach Satz 4.4, (iii) kann dies mit surjektiven Abbildungen nicht passieren). Dieses Verhalten wird zum Anlaß der folgenden Definition genommen.

4.14 Definition. Sei M ein R-Modul. Dann heißt M flach, wenn injektive Abbildungen zwischen beliebigen R-Moduln durch Tensorieren mit M wieder in injektive Abbildungen überführt werden.

Anders ausgedrückt: M heißt flach, wenn Tensorieren mit M ein exakter Funktor ist.

Die Äquivalenz der beiden Definitionsvarianten in Definition 4.14 folgt aus der Rechtsexaktheit des Tensorprodukts.

4.15 Satz. *Ein R-Modul M ist genau dann flach, wenn die Multiplikationsabbildung $i \otimes m \mapsto im$ einen Isomorphismus $I \otimes_R M \cong IM$ für alle Ideale I von R ergibt.*

Beweis. Wird ausgelassen. □

Ein Ausdruck $\sum_i \lambda_i m_i$ in IM mit $\lambda_i \in I$ und $m_i \in M$ soll also genau dann Null sein, wenn dies aufgrund R-bilinearer Relationen der Fall ist. Der Modul IM

soll in diesem Sinn also keine Relationen außer den Relationen der Bilinearität zwischen I und M enthalten. Wir verwenden diesen Satz aber nicht weiter.

Ist U ein Untermodul und direkter Summand des R-Moduls M, so erhalten wir durch Tensorieren der Inklusion $U \to M$ mit einem R-Modul N stets eine Inklusion $U \otimes_R N \to M \otimes_R N$. Denn nach Lemma 4.4, (ii) erhalten wir für V mit $M \cong U \oplus V$ einen Isomorphismus $(U \otimes_R N) \oplus (V \otimes_R N) \to M \otimes_R N$, dessen Einschränkung auf $U \otimes_R N$ gerade unsere Abbildung $U \otimes_R N \to M \otimes_R N$ ergibt.

Grob gesagt verlieren beliebige Monomorphismen $U \to M$ durch Tensorieren mit N ihre Injektivität genau dann, wenn Elemente $x \in U$ durch Einbetten nach M zu Vielfachen $x = ry$ mit $y \in M$ und $r \in R$ werden, wobei y nicht im Bild von U in M und r im Annulator von Elementen n aus N liegt. Genauer sind x, y durch x_i, y_i und r durch eine Matrix $(r_{i,j})_{i,j}$ und n durch n_j zu ersetzen. Vergleiche mit dem Kriterium aus Lemma 4.6, (iv).

4.16 Definition. Ist S eine R-Algebra und ist S als R-Modul flach, so nennen wir S eine flache R-Algebra. Ist $f : R \to S$ ein Ringhomomorphismus, so nennen wir f flach, wenn die zugehörige R-Algebra S flach ist.

4.17 Satz. *Es gelten die folgenden Aussagen:*

(i) *Für die R-Moduln M_i ist $M = \coprod_i M_i$ genau dann flach, wenn jedes M_i flach ist.*

(ii) *Sind M und N flache R-Moduln, dann ist auch $M \otimes_R N$ ein flacher R-Modul.*

(iii) *Ist S eine R-Algebra und N ein flacher R-Modul, so ist $S \otimes_R N$ ein flacher S-Modul.*

(iv) *Ist S eine flache R-Algebra und N ein flacher S-Modul, so ist $N|_R$ ein flacher R-Modul.*

Beweis. (i): Sei $h : N \to P$ ein Homomorphismus. Durch Tensorieren erhalten wir $f : N \otimes_R M \to P \otimes_R M$ und $f_i : N \otimes_R M_i \to P \otimes_R M_i$. Nach Lemma 4.4, (ii) gilt $N \otimes_R M \cong \coprod_i (N \otimes_R M_i)$ und $P \otimes_R M \cong \coprod_i (P \otimes_R M_i)$. Fassen wir damit die $N \otimes_R M_i$ und $P \otimes_R M_i$ als Untermoduln von $N \otimes_R M$ und $P \otimes_R M$ auf, so stimmen f eingeschränkt auf $N \otimes_R M_i$ und f_i überein. Dann ist f genau dann injektiv, wenn alle f_i injektiv sind, und dies beweist die Aussage.

(ii): Tensorieren mit $M \otimes_R N$ entspricht Tensorieren mit M und anschließend Tensorieren mit N. Da $\cdot \otimes_R M$ und $\cdot \otimes_R N$ exakt sind, ist auch $\cdot \otimes_R (M \otimes_R N)$ exakt.

(iii): Tensorieren über S mit $S \otimes_R N$ ist nach Satz 4.9 das gleiche wie Tensorieren über R mit N. Da N flach ist, ist Tensorieren über R mit N exakt. Also ist Tensorieren über S mit $S \otimes_R N$ ebenfalls exakt.

(iv): Sei M ein R-Modul. Nach Satz 4.9 gilt dann (mit M und N vertauscht) die in M funktorielle Isomorphie $M \otimes_R N \cong (M \otimes_R S) \otimes_S N$ als S-Moduln und somit auch als R-Moduln. Nach Voraussetzung sind $\cdot \otimes_R S$ und $\cdot \otimes_S N$ exakt, also ist auch $\cdot \otimes_R N$ exakt. □

Als Beispiel zu (i) sind alle freien R-Moduln flach, da R als R-Modul flach ist. Ein endlich erzeugter Modul über einem Hauptidealring ist damit nach Satz **??**, (ii) genau dann flach, wenn er torsionsfrei ist. Nach Satz 4.12 ist eine Lokalisierung $R[U^{-1}]$ als R-Modul stets flach.

Ein R-Modul M heißt endlich präsentiert, wenn es einen Epimorphismus $R^n \to M$ mit $n < \infty$ und endlich erzeugtem Kern gibt.

Sei $f : R \to S$ ein Ringhomomorphismus, so daß S eine R-Algebra wird, und seien M, N zwei R-Moduln. Tensorieren mit S über R liefert einen R-Homomorphismus $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ mit $f \mapsto \mathrm{id} \otimes f$. Da der Wertebereich ein S-Modul ist, faktorisiert dieser Homomorphismus nach Satz 4.8 eindeutig durch den S-Homomorphismus $\phi : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ mit $s \otimes f \mapsto s(\mathrm{id} \otimes f)$.

4.18 Satz. *Sei S als R-Modul flach und M endlich präsentiert. Dann liefert ϕ einen Isomorphismus*

$$S \otimes_R \mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N).$$

Beweis. Soll noch eingegeben werden. □

Eine spezielle Anwendung des Satzes ergibt sich für $S = R[U^{-1}]$, so daß wir mit ϕ einen Isomorphismus $\mathrm{Hom}_R(M, N)[U^{-1}] \cong \mathrm{Hom}_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}])$ erhalten. Beispielsweise gibt es damit für jeden Homomorphismus $f : M[U^{-1}] \to N[U^{-1}]$ ein $u \in U$ und $g : M \to N$ mit $uf(m) = g(m)$ in $N[U^{-1}]$ für alle $m \in M$. Es kann also aus der Existenz von Homomorphismen lokalisierter Moduln in gewisser Weise auf die Existenz dazu passender Homomorphismen der Ausgangsmoduln geschlossen werden.

4.5 Freie Moduln

In diesem Abschnitt diskutieren wir ein paar weitere Aspekte und Eigenschaften freier Moduln.

Satz **??**, (ii) hatte zum Inhalt, daß die Kardinalitäten beliebiger Basen eines R-Moduls für einen kommutativen Ring R übereinstimmen. Für nicht kommutative Ringe ist dies im allgemeinen nicht richtig. Sei zum Beispiel V ein unendlich dimensionaler K-Vektorraum. Dann gibt es einen Isomorphismus $f : V \oplus V \to V$. Wir bezeichnen mit $\iota_1, \iota_2 : V \to V \oplus V$ die Einbettung in den ersten bzw. zweiten Summand. Wir erhalten Vektorraumisomomorphismen $\mathrm{End}_K(V) \cong \mathrm{Hom}_K(V \oplus V, V)$ durch $g \mapsto g \circ f$ und $\mathrm{Hom}_K(V \oplus V, V) \cong \mathrm{End}_K(V) \times \mathrm{End}_K(V)$ durch $h \mapsto (h \circ \iota_1, h \circ \iota_2)$. Mit $R = \mathrm{End}_K(V)$ liefert dies zusammen einen Vektorraumisomorphismus $\psi : R \to R \times R$. Werden R und $R \times R$ in der natürlichen Weise als R-Moduln aufgefaßt, so ist ψ sogar R-linear: Für $r, g \in R$ gilt $r\psi(g) = (r \circ g \circ f \circ \iota_1, r \circ g \circ f \circ \iota_2) = \psi(rg)$. Somit besitzt R als R-Modul eine einelementige und eine zweielementige Basis („Eilenberg Schwindel“).

Freie Moduln besitzen die folgende Eigenschaft, wie in Satz **??**, (i) gezeigt wurde: Sei B eine Basis des R-Moduls M und N irgendein weiterer R-Modul. Für jede Abbildung von Mengen $f : B \to N$ gibt es genau ein Element in $\mathrm{Hom}_R(M, N)$, welches f fortsetzt. Ähnlich verhält es sich übrigens auch bei Polynomringen (die „frei“ erzeugten Ringen entsprechen) und dem Einsetzhomomorphismus. Hier sind zwei weitere Eigenschaften, die darauf aufbauen.

4.19 Satz. *Sei N ein R-Modul.*

(i) *Es gibt einen freien R-Modul M und einen Epimorphimus $f : M \to N$, so daß $N \cong M/\ker(f)$.*

(ii) *Ist M ein freier R-Modul und $f : N \to M$ ein Epimorphismus, so gibt es ein $g : M \to N$ mit $f \circ g = \mathrm{id}_M$.*

Beweis. (i) : Sei B ein Erzeugendensystem von N und $M = \coprod_{b \in B} R$. Wir definieren f durch $f((\lambda_b)_{b \in B}) = \sum_{b \in B} \lambda_b b$. Dies Isomorphie folgt aus dem ersten Isomorphiesatz.

(ii): Für jedes Basiselement $b \in B$ wählen wir ein Urbild $c \in f^{-1}(b)$ und definieren $g_0(b) = c$. Dies liefert $g_0 : B \to N$ und dann $g : M \to N$. □

Hier sind die zu Satz 4.17 analogen Aussagen für „frei“ statt „flach“.

4.20 Satz. *Es gelten die folgenden Aussagen:*

(i) *Für die R-Moduln M_i ist $M = \coprod_i M_i$ frei, wenn jedes M_i frei ist.*

(ii) *Sind M und N freie R-Moduln, dann ist auch $M \otimes_R N$ ein freier R-Modul.*

(iii) *Ist S eine R-Algebra und N ein freier R-Modul, so ist $S \otimes_R N$ ein freier S-Modul.*

(*iv*) *Ist S eine freie R-Algebra und N ein freier S-Modul, so ist $N|_R$ ein freier R-Modul.*

Beweis. (*i*): Die Vereinigung der Basen der M_i liefert eine Basis von M.

(*ii*) und (*iii*): Folgen aus Satz 4.4, (*iii*) und Lemma 4.6, (*ii*).

(*iv*): Analog wie im Gradsatz: Sind die n_j eine S-Basis von N und die s_i eine R-Basis von S, so sind die $s_i n_j$ eine R-Basis von N. □

Die Umkehrung der Aussage (*i*) ist im allgemeinen falsch. Es gibt Ringe R und Ideale I, J von R, so daß $R \oplus R \cong I \oplus J$ gilt, aber I und J nicht frei sind. Speziell dürfen I, J hier keine Hauptideale sein. Konkrete Beispiele kommen später.

4.6 Projektive Moduln

Die Definition von „frei“ benötigt explizit Elemente von M. Auf der anderen Seite wird in Satz 4.19, (*ii*) eine nützliche, „elementfreie“ Eigenschaft angegeben. Diese macht somit auch in allgemeinerem kategoriellen Rahmen Sinn und man macht sie zur Grundlage einer weiteren Definition. Wie sich herausstellt, ist diese Eigenschaft echt schwächer als „frei“.

4.21 Definition. Sei M ein R-Modul. Dann heißt M projektiv, wenn es für jeden R-Modul N und Epimorphismus $f : N \to M$ einen Homomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$ gibt.

Der Homomorphismus g ist wegen $f \circ g = \mathrm{id}_M$ injektiv.

4.22 Satz. *Sei M ein R-Modul. Dann sind äquivalent.*

(*i*) *M ist projektiv.*

(*ii*) *Es gibt einen R-Modul U und einen freien R-Modul N mit $M \oplus U \cong N$.*

(*iii*) *Es gibt ein Erzeugendensystem B von M und „Koordinatenfunktionale“ $\lambda_b \in \mathrm{Hom}_R(M, R)$ mit $x = \sum_{b \in B} \lambda_b(x) b$.*

(*iv*) *Seien N_1, N_2 beliebige R-Moduln und $f \in \mathrm{Hom}_R(N_1, N_2)$ ein Epimorphismus. Für jedes $g \in \mathrm{Hom}_R(M, N_2)$ gibt es ein $h \in \mathrm{Hom}_R(M, N_1)$ mit $g = f \circ h$.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Nach Satz 4.19, (*ii*) gibt es einen freien R-Modul N und einen Epimorphismus $f : N \to M$. Wegen (*i*) gibt es einen Monomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$. Für den Untermodul $U = \{x - g(f(x)) \,|\, x \in N\} \subseteq$

$\ker(f)$ gilt dann $g(M) + U = N$ und $g(M) \cap U \subseteq g(M) \cap \ker(f) = \{0\}$, also $N = g(M) \oplus U \cong M \oplus U$.

$(ii) \Rightarrow (iii)$: Nach (ii) gibt es einen freien R-Modul N, einen Epimorphismus $f : N \to M$ mit $\ker(f) = U$ und einen Monomorphismus $g : M \to N$ mit $f \circ g = \mathrm{id}_M$. Seien die a_i eine Basis von N. Dann sind die $b_i = f(a_i)$ ein Erzeugendensystem von M, weil f surjektiv ist. Da die a_i eine Basis bilden, gibt es Koordinatenfunktionale $\mu_i \in \mathrm{Hom}_R(N, R)$ mit $y = \sum_i \mu_i(y)a_i$ für alle $y \in N$. Wir definieren $\lambda_i \in \mathrm{Hom}_R(M, R)$ durch $\lambda_i(x) = \mu_i(g(x))$. Wegen $g(b_i) - a_i \in \ker(f)$ gilt dann $g(x - \sum_i \lambda_i(x)b_i) \in g(x) - \sum_i \mu_i(g(x))a_i + \ker(f) = \ker(f)$. Wegen $g(M) \cap \ker(f) = \{0\}$ folgt $g(x - \sum_i \lambda_i(x)b_i) = 0$. Da g injektiv ist, ergibt sich $x - \sum_i \lambda_i(x)b_i = 0$ und damit (iii).

$(iii) \Rightarrow (iv)$: Sei B ein Erzeugendensystem mit Koordinatenfunktionalen λ_b für $b \in B$ wie in (iii). Wir wählen für jedes $b \in B$ ein $y_b \in f^{-1}(g(b))$. Dies ist möglich, da f surjektiv ist. Wir definieren dann $h \in \mathrm{Hom}_R(M, N_1)$ durch $h(x) = \sum_b \lambda_b(x)y_b$. Nach Definition sind die λ_b R-linear und für fast alle $b \in B$ gilt $\lambda_b(x) = 0$. Daher ist h wohldefiniert und ein Element von $\mathrm{Hom}_R(M, N_1)$. Weiter gilt $f(h(x)) = \sum_b \lambda_b(x)f(y_b) = \sum_b \lambda_b(x)g(b) = g(\sum_b \lambda_b(x)b) = g(x)$, also wie gewünscht $f \circ h = g$.

$(iv) \Rightarrow (i)$: Sei $f : N \to M$ der Epimorphismus aus (i) bzw. der Definition 4.21. Wir wenden (iv) mit $N_1 = N$, $N_2 = M$ und $g = \mathrm{id}_M$ an und erhalten direkt Aussage (i). □

Satz 4.22, (iii) ist eine Verallgemeinerung der Aussage für freie Moduln M, daß man einen Homomorphismus $f : M \to N$ durch seine Werte auf einer Basis von M definieren kann.

Ist M ein R-Modul, so ist der Funktor $\mathrm{Hom}_R(M, \cdot)$ linksexakt. Satz 4.22, (iv) läßt sich damit folgendermaßen umformulieren:

4.23 Korollar. *Ein R-Modul M ist genau dann projektiv, wenn der Funktor $\mathrm{Hom}_R(M, \cdot)$ exakt ist.*

Beweis. Da $\mathrm{Hom}_R(M, \cdot)$ linksexakt ist, muß für Exaktheit nur noch nachgewiesen werden, daß surjektive Abildungen in surjektive Abbildungen überführt werden. Das ist aber genau die Aussage von (iv). □

Hier sind die zu Satz 4.17 analogen Aussagen für „projektiv“ statt „flach“.

4.24 Satz. *Es gelten die folgenden Aussagen:*

(i) *Für die R-Moduln M_i ist $M = \coprod_i M_i$ genau dann projektiv, wenn jedes M_i projektiv ist.*

(*ii*) *Sind M und N projektive R-Moduln, dann ist auch $M \otimes_R N$ ein projektiver R-Modul.*

(*iii*) *Ist S eine R-Algebra und N ein projektiver R-Modul, so ist $S \otimes_R N$ ein projektiver S-Modul.*

(*iv*) *Ist S eine projektive R-Algebra und N ein projektiver S-Modul, so ist $N|_R$ ein projektiver R-Modul.*

Beweis. (*i*): Folgt direkt aus Satz 4.22, (*ii*) und Satz 4.20, (*i*).

(*ii*) und (*iii*): Folgen aus Satz 4.22, (*ii*), Satz 4.4, (*iii*) und Satz 4.20, (*ii*) und (*iii*).

(*iv*): Ähnlich wie im Gradsatz: Seien die n_j ein Erzeugendensystem von N mit den Koordinatenfunktionalen $\lambda_j \in \mathrm{Hom}_S(N, S)$ und die s_i ein Erzeugendensystem von S mit den Koordinatenfunktionalen $\mu_i \in \mathrm{Hom}_R(S, R)$. Dann sind die $s_i m_j$ ein Erzeugendensystem mit den Koodinatenfunktionalen $\mu_i \circ \lambda_j \in \mathrm{Hom}_R(N, R)$. Nach Satz 4.22, (*iii*) ist N als R-Modul also projektiv. □

4.7 Satz von Cayley-Hamilton und Lemma von Nakayama

Im folgenden bezeichnet R wieder einen kommutativen Ring mit 1.

4.25 Satz (Cayley-Hamilton)**.** *Sei M ein von n Elementen erzeugter R-Modul und I ein Ideal von R. Sei $\phi \in \mathrm{End}_R(M)$ ein Endomorphismus von M. Gilt $\phi(M) \subseteq IM$, so gibt es ein $f = \sum_{i=0}^{n} \lambda_{n-i} x^i \in R[x]$ mit $\lambda_0 = 1$, $\lambda_i \in I^i$ für $0 \leq i \leq n$ und $f(\phi) = 0$ in $\mathrm{End}_R(M)$.*

Beweis. Seien $m_1, \ldots, m_n$ Erzeuger von M. Nach Voraussetzung existiert ein $A = (a_{i,j})_{i,j} \in I^{n \times n}$ mit $\phi(m_i) = \sum_{j=1}^{n} a_{i,j} m_j$ für alle $1 \leq i \leq n$. Vermöge $g(x)m := g(\phi)(m)$ wird M zu einem $R[x]$-Modul. Dann gilt $x(m_1, \ldots, m_n)^t = A(m_1, \ldots, m_n)^t$ und $(xI_n - A)(m_1, \ldots, m_n)^t = 0$. Durch Multiplikation dieser Gleichung von links mit der Pseudoinversen von $xI_n - A$ (siehe Satz **??**, (*ii*)) erhalten wir $\det(xI_n - A)(m_1, \ldots, m_n)^t = 0$. Setze $f = \sum_{i=0}^{n} \lambda_{n-i} x^i = \det(xI_n - A) \in R[x]$. Die m_i sind ein Erzeugendensystem von M, es folgt also $fM = 0$ und damit $f(\phi) = 0$ in $\mathrm{End}_R(M)$. Durch direktes Ausrechnen der Koeffizienten λ_i von f mittels der Leibnizregel ergibt sich, daß f in der Tat normiert vom Grad n ist und daß $\lambda_i \in I^i$ gilt. □

Ist M ein freier Modul vom Rang n und sind die y_j für $j \in J$ ein Erzeugendensystem von M, so gilt $\#J \geq n$ (vgl. Satz **??**). Das folgende Korollar zeigt, daß die y_j für $\#J = n$ bereits eine Basis von M bilden.

4.26 Korollar. *Sei M ein endlich erzeugter R-Modul. Dann gilt:*

(*i*) *Ist $\psi \in \mathrm{End}_R(M)$ ein Epimorphismus, so ist ψ bereits ein Isomorphismus.*

(*ii*) *Ist M frei vom Rang n, so ist jedes Erzeugendensystem von M bestehend aus n Elementen eine Basis von M.*

Beweis. Übungsaufgabe. □

Ist R ein Körper, so ist M ein Vektorraum und ist daher stets frei. Hier gelten die folgenden beiden Aussagen: Jedes Erzeugendensystem enthält eine Basis, und jeder Monomorphismus in $\mathrm{End}_R(M)$ eines endlich erzeugten M ist ein Isomorphismus. Für beliebige R-Modul gelten diese Aussagen nicht mehr. Zum Beispiel ist $\{2, 3\}$ ein Erzeugendensystem des $\mathbb{Z}$-Moduls $\mathbb{Z}$, enthält aber keine Basis. Auch liefert $x \mapsto 2x$ einen Monomorphismus aus $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$, welcher kein Isomorphismus ist.

4.27 Definition. Das Jacobsonradikal J von R ist der Schnitt aller maximalen Ideale von R. Das Radikal $\mathrm{Rad}(R)$ von R ist der Schnitt aller Primideale von R.

Das Radikal von R wird manchmal auch Nilradikal genannt. Das Jacobsonradikal J und das Radikal $\mathrm{Rad}(R)$ von R sind Ideale von R. Es gilt $J = \{r \in R \,|\, 1 + rs \in R^\times \text{ für alle } s \in R\}$ und $\mathrm{Rad}(R) = \{r \in R \,|\, r^n = 0 \text{ für ein } n \in \mathbb{Z}^{\geq 1}\}$.

4.28 Lemma (Nakayama)**.** *Sei M ein endlich erzeugter Modul und I ein Ideal, welches im Jacobsonradikal von R enthalten ist. Gilt $M = N + IM$ für einen Untermodul N von M, dann folgt $M = N$.*

Beweis. Wir beweisen die Aussage zunächst für $N = 0$, es gelte also $IM = M$. Wir wenden Satz 4.25 auf $\phi = \mathrm{id}_M$ an und erhalten $f(x) = x^n - g(x) \in R[x]$ mit $g \in I[x]$ und $f(1)M = 0$. Für $r = g(1)$ gilt also $r \in I$ und $f(1)M = (1-r)M = 0$. Da r nach Voraussetzung in jedem maximalen Ideal von R enthalten ist, gilt $1 - r \in R^\times$. Es folgt $M = (1 - r)M = 0$.

Sei nun $M = N + IM$. Faktorisieren nach N liefert $M/N = I(M/N)$, also $M/N = 0$ und daher $M = N$. □

Eine mögliche Anwendung von Lemma 4.28 ist die folgende: Sind die Klassen von $n_1, \ldots, n_m \in M$ ein Erzeugendensystem von M/IM, so sind die $n_1, \ldots, n_m$ ein Erzeugendensystem von M. Allerdings darf man bei dieser Schlußweise nicht vergessen, daß M als endlich erzeugt vorauszusetzen ist.

4.8 Beziehungen zwischen den Moduleigenschaften und lokal-global Aussagen

Sei M ein R-Modul. Für $a \in R$ sei $I_a = \{b \in R \mid ab = 0\}$. Dann ist I_a ein Ideal von R und I_aM ist ein Untermodul von M, der durch a annulliert wird. Wir nennen M im wesentlichen torsionsfrei, wenn für jedes $a \in R\backslash\{0\}$ und jedes $x \in M$ aus $ax = 0$ bereits $x \in I_aM$ folgt. Für einen Integritätsring R ist M genau dann im wesentlichen torsionsfrei, wenn M torsionsfrei ist.

4.29 Satz. *Sei M ein R-Modul. Dann gilt*

$$M \text{ frei } \Rightarrow M \text{ projektiv } \Rightarrow M \text{ flach } .$$

Ein projektiver Modul ist torsionsfrei. Ein flacher R-Modul M ist im wesentlichen torsionsfrei.

Beweis. Die erste Implikation folgt direkt aus Satz 4.22, (ii) mit $U = \{0\}$.

Die zweite Implikation folgt aus Satz 4.22, (ii) und Satz 4.17, (i). Damit ist M als direkter Summand eines freien und damit flachen Moduls selbst flach.

Ein freier Modul ist torsionsfrei. Ein projektiver Modul ist als Unternmodul eines freien Moduls daher dann auch torsionsfrei.

Wir beweisen schließlich, daß flache Moduln im wesentlichen torsionsfrei sind. Sei $a \in R$. Dann ist I_a der Kern von $R \to Ra$, $x \mapsto ax$, und es gilt $Ra \cong R/I_a$ und $Ra \otimes_R M \cong R/I_a \otimes_R M \cong M/I_aM$. Tensorieren der exakten Inklusionssequenz $0 \to Ra \to R$ mit M liefert damit die exakte Sequenz $0 \to M/I_aM \to M$ nach Lemma 4.6, (i), wobei der rechte Monomorphismus durch $x + I_aM \mapsto ax$ gegeben ist. Also folgt aus $ax = 0$ bereits $x \in I_aM$, so daß M im wesentlichen torsionsfrei ist. □

Wir wollen im folgenden die Eigenschaften „frei“, „projektiv“ und „flach“ global und lokal vergleichen, und zwar hauptsächlich unter der Voraussetzung, daß die Moduln endlich erzeugt oder endlich präsentiert sind.

4.30 Definition. Ein R-Modul M heißt lokal frei, wenn $M_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul für alle Primideale $\mathfrak{p}$ von R ist. Analog definieren wir lokal projektiv und lokal flach.

4.31 Lemma. *Sei M ein R-Modul.*

(i) *Ein Modul M ist genau dann lokal frei (projektiv, flach), wenn $M_\mathfrak{m}$ frei (projektiv, flach) für alle maximalen Ideale von R ist.*

(ii) *Ein freier (projektiver, flacher) Modul M ist lokal frei (projektiv, flach).*

Beweis. Wir machen eine Vorbemerkung: Die Aussage (iii) der Sätze 4.20, 4.24 und 4.17 impliziert, daß die Eigenschaften frei, projektiv und flach unter Lokalisieren erhalten bleiben.

(i): Für jedes Primideal gibt es ein maximales Ideal $\mathfrak{m}$, so daß $M_\mathfrak{p}$ nur eine weitere Lokalisierung von $M_\mathfrak{m}$ ist. Aus der Vorbemerkung folgt damit die Aussage.

(ii): Ergibt sich unmittelbar aus der Vorbemerkung. □

4.32 Satz. *Sei R ein lokaler Ring und M ein endlich erzeugter R-Modul. Dann gilt*

$$M \text{ ist frei} \Leftrightarrow M \text{ ist projektiv} \Leftrightarrow M \text{ ist flach.}$$

Beweis. Wegen Satz 4.29 ist nur zu zeigen, daß aus M flach bereits M frei folgt.

Sei $\mathfrak{m}$ das maximale Ideal von R und seien $x_1, \ldots, x_n \in M$, so daß die Klassen $\bar{x}_i = x_i + \mathfrak{m}M$ eine Basis des mit M endlich erzeugten $R/\mathfrak{m}$-Vektorraums $M/\mathfrak{m}M$ bilden. Wir zeigen, daß die x_i eine Basis von M sind.

Sei $N = \sum_i Rx_i$. Dann gilt $M = N + \mathfrak{m}M$, und nach dem Lemma 4.28 folgt $M = N$, also sind die x_i ein Erzeugendensystem von M.

Zum Beweis der Basiseigenschaft zeigen wir jetzt, daß für in $M/\mathfrak{m}M$ linear unabhängige, nicht notwendig erzeugende $\bar{x}_i$ die x_i linear unabhängig in M sind.

Wir schicken wir eine Bemerkung voraus. Seien $\lambda_i \in R$ mit $\sum_{i=1}^n \lambda_i x_i = 0$. Sei $I = \sum_{i=1}^n R\lambda_i$. Dann ist das Bild von $\sum_{i=1}^n \lambda_i \otimes x_i$ unter dem Homomorphismus $I \otimes_R M \to R \otimes_R M = M$ gleich $\sum_{i=1}^n \lambda_i x_i = 0$. Da die Inklusion $I \to R$ injektiv und M flach ist, ist dieser Homomorphismus ebenfalls injektiv und es muß bereits $\sum_{i=1}^n \lambda_i \otimes x_i = 0$ gelten. Nach Lemma 4.6, (iv) angewendet für $N = I$ gibt es $a_{i,j} \in R$ und $y_j \in M$ mit $x_i = \sum_{j=1}^m a_{i,j} y_j$ und $\sum_{i=1}^n a_{i,j}\lambda_i = 0$ für alle j.

Um aus dieser Vorbemerkung auf die lineare Unabhängigkeit der x_i zu schließen, verwenden wir Induktion über ihre Anzahl n. Für $n = 1$ gelte $\lambda_1 x_1 = 0$. Nach der Vorbemerkung gilt dann $x_1 = \sum_{j=1}^m a_{1,j} y_j$ und $a_{1,j}\lambda_1 = 0$ für alle j. Wegen $x_1 \notin \mathfrak{m}M$ gibt es ein j mit $a_{1,j} \notin \mathfrak{m}$. Dann gilt $a_{1,j} \in R^\times$ und aus $a_{1,j}\lambda_1 = 0$ folgt $\lambda_1 = 0$.

Sei nun $n > 1$. Nach der Vorbemerkung gilt $x_i = \sum_{j=1}^m a_{i,j} y_j$ und $\sum_{i=1}^n a_{i,j}\lambda_i = 0$ für alle j und mit $y_i \in M$, $a_{i,j} \in R$. Da $x_n \notin \mathfrak{m}M$ ist, gibt es j mit $a_{n,j} \notin \mathfrak{m}$. Also ist $a_{n,j} \in R^\times$ und es gilt $\lambda_n = \sum_{i=1}^{n-1}(-a_{i,j}/a_{n,j})\lambda_i = \sum_{i=1}^{n-1} b_i\lambda_i$ mit $b_i = -a_{i,j}/a_{n,j}$. Dann folgt $0 = \sum_{i=1}^n \lambda_i x_i = \sum_{i=1}^{n-1} \lambda_i(x_i + b_i x_n)$. Die $\bar{x}_1 + b_1\bar{x}_n, \ldots, \bar{x}_{n-1} + b_{n-1}\bar{x}_n$ sind linear unabhängig in $M/\mathfrak{m}M$. Nach Induktionsvoraussetzung sind $x_1, \ldots, x_{n-1}$ also linear unabhängig in M. Daraus folgt $\lambda_i = 0$ für $1 \le i \le n-1$ und $\lambda_n = \sum_{i=1}^{n-1} b_i\lambda_i = 0$. Damit sind die $x_1, \ldots, x_n$ linear unabhängig. □

Die Voraussetzung an die endliche Erzeugung ist notwendig: Für $R = \mathbb{Z}_{(p)}$ ist R zwar lokal und $M = \mathbb{Q}$ als R-Modul flach, aber M ist nicht frei.

Der folgende Satz enthält den lokal-global Vergleich für die Eigenschaft „flach“.

4.33 Satz. *Sei M ein R-Modul.*

(*i*) *M ist genau dann flach, wenn M lokal flach ist.*

(*ii*) *Ist M endlich erzeugt, so ist M genau dann flach, wenn M lokal frei ist.*

Beweis. (*i*): Die Implikation $\Rightarrow$ folgt aus Lemma 4.31. Für die Implikation $\Leftarrow$ sei M lokal flach. Sei $\phi : N \to P$ ein Monomorphismus und $\mathfrak{p}$ ein Primideal. Sei $\phi_1 : N \otimes_R M \to P \otimes_R M$. Nach Voraussetzung ist $M_\mathfrak{p}$ flach über $R_\mathfrak{p}$. Da $R_\mathfrak{p}$ flach über R ist, ist $M_\mathfrak{p}$ nach Satz 4.17, (*ii*) auch flach über R. Daher ist $\phi_2 : N \otimes_R M_\mathfrak{p} \to P \otimes_R M_\mathfrak{p}$ ein Monomorphismus. Mit Satz 4.4, (*i*) und (*ii*) erhalten wir daraus den Monomorphismus $\phi_3 : (N \otimes_R M) \otimes_R R_\mathfrak{p} \to (P \otimes_R M) \otimes_R R_\mathfrak{p}$, welcher durch Tensorieren von ϕ_1 mit $R_\mathfrak{p}$ entsteht. Da $\mathfrak{p}$ beliebig war, ist ϕ_1 nach Satz 4.13 ein Monomorphismus. Also ist M flach.

(*ii*): Ergibt sich aus (*i*) und Satz 4.32. □

Wir wollen noch einen lokal-global Vergleich der Eigenschaft „projektiv“ angeben und eine Verbindung zwischen „projektiv“ und „lokal frei“ herstellen. Dazu müssen wir voraussetzen, daß M nicht nur endlich erzeugt, sondern sogar endlich präsentiert ist.

Zur Erinnerung: Ein R-Modul M heißt endlich präsentiert, wenn es ein $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $\phi : R^n \to M$ mit endlich erzeugtem Kern gibt.

4.34 Lemma. *Sei M ein endlich präsentierter R-Modul. Für jedes $m \in \mathbb{Z}^{\geq 1}$ und jeden Epimorphismus $\psi : R^m \to M$ ist dann* $\ker(\psi)$ *endlich erzeugt.*

Ist R noethersch und M endlich erzeugt, so ist M endlich präsentiert.

Ist M endlich präsentiert und U eine multiplikativ abgeschlossene Teilmenge von R mit $1 \in U$, so ist auch $M[U^{-1}]$ als $R[U^{-1}]$-Modul endlich präsentiert.

Beweis. Sei $\phi : R^n \to M$ ein Epimorphismus mit $\ker(\phi)$ endlich erzeugt und sei $\psi : R^m \to M$ ein weiterer Epimorphismus. Seien $(\lambda_{i,j})_j \in R^m$ mit $\phi(e_i) = \psi((\lambda_{i,j})_j)$ und $(\mu_{j,i})_i \in R^n$ mit $\phi((\mu_{j,i})_i) = \psi(e_j)$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$. Seien $(u_{s,i})_i \in R^n$ für endlich viele s ein Erzeugendensystem von $\ker(\phi)$. Dann bilden die $((u_{s,i})_i, 0) \in R^n \times R^m$ zusammen mit den $((\mu_{j,i})_i, e_j) \in R^n \times R^m$ ein endliches Erzeugendensystem U von $K = \{(x, y) \in R^n \times R^m \mid \phi(x) = \psi(y)\}$. Für jeden Erzeuger $u \in U$ gibt es ein $v_u \in \ker(\psi)$, so daß sich u als R-Linearkombination der $(e_i, (\lambda_{i,j})_j) \in K$ und von $(0, v_u) \in K$ schreiben läßt. Die $(e_i, (\lambda_{i,j})_j)$ zusammen mit den $(0, v_u)$ für jedes u liefern damit ein anderes, endliches Erzeugendensystem V von K. Für $y \in \ker(\psi)$ können keine $(e_i, (\lambda_{i,j})_j)$ in den Darstellungen von $(0, y) \in K$ in V auftreten. Also bilden die v_u ein endliches Erzeugendensystem von $\ker(\psi)$.

Sei R noethersch und M endlich erzeugt. Da M endlich erzeugt ist, gibt es einen Epimorphismus $\psi : R^n \to M$. Da R noethersch ist, muß $\ker(\psi)$ nach Satz **??**, (*iii*) und Satz **??** endlich erzeugt sein. Also ist M endlich präsentiert.

Ist M endlich präsentiert, so haben wir eine exakte Sequenz $R^s \to R^n \to M \to 0$. Durch Lokalisieren geht diese in die exakte Sequenz $R[U^{-1}]^s \to R[U^{-1}]^n \to M[U^{-1}] \to 0$ über, also ist $M[U^{-1}]$ endlich präsentiert. □

4.35 Lemma. *Sei M ein endlich präsentierter R-Modul. Dann ist M ist genau dann lokal frei, wenn es für jedes Primideal $\mathfrak{p}$ von R ein $f \in R\backslash\mathfrak{p}$ gibt, so daß $M[f^{-1}]$ bereits ein freier $R[f^{-1}]$-Modul ist.*

Beweis. Das Lemma ist für $M = \{0\}$ richtig, da M frei ist und dies auch für alle Lokalisierungen gilt. Es gelte also $M \neq \{0\}$.

„$\Leftarrow$“: Ist klar, da nur weiter lokalisiert werden muß.

„$\Rightarrow$“: Mit M ist $M_\mathfrak{p}$ endlich erzeugt, so daß $M_\mathfrak{p}$ eine endliche Basis besitzt (vgl. Satz **??**). Seien $m_1, \ldots, m_k \in M$, so daß die m_i in $M_\mathfrak{p}$ eine Basis bilden. Jeder Erzeuger v_j von M kann aufgrund der Annahme in der Form $u_j v_j = \sum_{i=1}^k \lambda_{i,j} m_i$ mit $u_j \in R\backslash\mathfrak{p}$ und $\lambda_{i,j} \in R$ geschrieben werden. Sei $f = \prod_j u_j$. Dann gilt $f \in R\backslash\mathfrak{p}$ und $v_j = \sum_{i=1}^k (\lambda'_{i,j}/f) m_i$ in $M[f^{-1}]$ mit geeigneten $\lambda'_{i,j} \in R$. Die m_i bilden also ein Erzeugendensystem von $M[f^{-1}]$.

Aus $\sum_i (\mu_i/u_i) m_i = 0$ in $M_\mathfrak{p}$ für beliebige $\mu_i \in R$ und $u_i \in R\backslash\mathfrak{p}$ folgt $\mu_i/u_i = 0$ für alle i nach Voraussetzung, also gibt es für jedes i ein $v_i \in R\backslash\mathfrak{p}$ mit $v_i \mu_i = 0$ in R. Der $R_\mathfrak{p}$-Modul T aller solcher Tupel $(\mu_i/u_i)_i \in R_\mathfrak{p}^k$ mit $\sum_i (\mu_i/u_i) m_i = 0$ in $M[f^{-1}]$ ist nach Lemma 4.34 endlich erzeugt, da $M_\mathfrak{p}$ mit M endlich präsentiert ist. Wir multiplizieren an f die endlich vielen, auftretenden v_i (für jeden Erzeuger des Tupelraums T sind das k Elemente v_i). Jedes Tupel $(\mu_i)_i$ wird dann also durch koordinatenweise Multiplikation mit f annulliert, ist also Null in $R[f^{-1}]^k$. Die m_i sind daher auch linear unabhängig in $M[f^{-1}]$. □

Der Satz ist falsch, wenn auf die Voraussetzung der endlichen Erzeugung verzichtet wird. Sei zum Beispiel $R = \mathbb{Z}$ und M der von $\{a/p \mid a \in \mathbb{Z}, p \text{ Primzahl}\}$ erzeugte $\mathbb{Z}$-Untermodul von $\mathbb{Q}$. Dann sind die $M_\mathfrak{p}$ für $\mathfrak{p} = \mathbb{Z}p$ isomorph zu den von $1/p$ erzeugten $R_\mathfrak{p}$-Untermoduln von $\mathbb{Q}$, also frei. Wegen der unbeschränkten Nenner kann es aber kein einziges f wie im Lemma geben.

Torsion bleibt lokal nicht unbedingt erhalten. Siehe $R = K \times K$ und $M = R$. Dann ist M nicht torsionsfrei, aber alle Lokalisierungen an Primidealen sind isomorph zu K, also torsionsfrei.

Der folgende Satz enthält den angestrebten lokal-global Vergleich für „projektiv“.

4.36 Satz. *Sei M ein endlich präsentierter R-Modul. Dann sind äquivalent:*

(*i*) *M ist projektiv.*

(*ii*) *M ist flach.*

(*iii*) *M ist lokal frei.*

(*iv*) *Es gibt $f_1, \ldots, f_n \in R$ mit $R = \sum_{i=1}^n Rf_i$, so daß $M[f_i^{-1}]$ frei über $R[f_i^{-1}]$ für alle $1 \leq i \leq n$ ist.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Folgt aus Satz 4.29. (*ii*) $\Rightarrow$ (*iii*): Folgt aus Satz 4.33.

(*iii*) $\Rightarrow$ (*iv*): Nach Lemma 4.35 gibt es für jedes maximale Ideal $\mathfrak{m}$ ein $f_\mathfrak{m} \in R\backslash\mathfrak{m}$, so daß $M[f_\mathfrak{m}^{-1}]$ ein freier $R[f_\mathfrak{m}^{-1}]$-Modul ist. Sei $I = \sum_\mathfrak{m} Rf_\mathfrak{m}$ das von den $f_\mathfrak{m}$ erzeugte Ideal von R. Dann ist I wegen $f_\mathfrak{m} \in I$ und $f_\mathfrak{m} \notin \mathfrak{m}$ in keinem maximalen Ideal enthalten, also folgt $I = R$. Wegen $1 \in I$ gibt es daher endlich viele f_i unter den $f_\mathfrak{m}$ und $g_i \in R$ mit $1 = \sum_i g_i f_i$. Dann gilt bereits $R = \sum_i Rf_i$. Es ergibt sich (*iv*).

(*iv*) $\Rightarrow$ (*i*): Mit M ist jedes $M[f_i^{-1}]$ endlich erzeugt, besitzt also eine endliche Basis (vgl. Satz **??**). Für jedes i seien $m_{i,j} \in M$ für endlich viele j, so daß die Bilder der $m_{i,j}$ in $M[f_i^{-1}]$ eine Basis von $M[f_i^{-1}]$ bilden. Seien $\mu_{i,j} \in \mathrm{Hom}_{R[f_i^{-1}]}(M[f_i^{-1}], R[f_i^{-1}])$ die Koordinatenfunktionale bezüglich der $m_{i,j}$, so daß $m/f_i^r = \sum_j \mu_{i,j}(m/f_i^r)m_{i,j}$ in $M[f_i^{-1}]$ für alle $m \in M$, $r \in \mathbb{Z}^{\geq 0}$ und i gilt.

Nach Satz 4.18 gibt es $\lambda_{i,j} \in \mathrm{Hom}_R(M, R)$ und $k_{i,j} \in \mathbb{Z}^{\geq 1}$ mit $f_i^{k_{i,j}}\mu_{i,j}(m/f_i^r) = \lambda_{i,j}(m)/f_i^r$ in $R[f_i^{-1}]$ für alle $m \in M$ und $r \in \mathbb{Z}^{\geq 0}$. Sei $k = \max_{i,j} k_{i,j}$. Wir ersetzen $\lambda_{i,j}$ durch $f_i^{k-k_{i,j}}\lambda_{i,j}$, so daß nun speziell $f_i^k\mu_{i,j}(m) = \lambda_{i,j}(m)$ in $R[f_i^{-1}]$ mit $\lambda_{i,j} \in \mathrm{Hom}_R(M, R)$ und $f_i^k m = \sum_j \lambda_{i,j}(m)m_{i,j}$ in $M[f_i^{-1}]$ für alle $m \in M$ gilt. Da M endlich erzeugt ist, gilt $f_i^k m = \sum_j \lambda_{i,j}(m)m_{i,j}$ auch in M, wenn wir zuvor k groß genug wählen.

Potenzieren wir beide Seiten der Gleichung $1 = \sum_i g_i f_i$ mit einer ausreichend großen ganzen Zahl, erhalten wir einen Ausdruck $1 = \sum_i h_i f_i^k$ mit $h_i \in R$.

Es ergibt sich $m = (\sum_i h_i f_i^k)m = \sum_{i,j}(h_i\lambda_{i,j}(m))m_{i,j}$ in M für alle $m \in M$. Wir erhalten also Erzeuger $m_{i,j}$ und Koordinatenfunktionale $m \mapsto h_i\lambda_{i,j}(m)$ aus $\mathrm{Hom}_R(M, R)$, so daß M nach Satz 4.22 projektiv ist. $\square$

Kapitel 5

Ringe II

In diesem Kapitel werden das Tensorprodukt von Algebren, ganze Ringerweiterungen, gebrochene und invertierbare Ideale, Dedekindringe und die Faktorisierung in Dimension 1 und Kodimension 1 behandelt.

5.1 Tensorprodukt von Algebren

Wir kommen nun auf das Tensorprodukt von (kommutativen) R-Algebren S_1, S_2 zu sprechen. Die Multiplikation in $S_1 \otimes_R S_2$ wird durch $(x_1 \otimes_R y_1) \cdot (x_2 \otimes_R y_2) = (x_1x_2) \otimes (y_1y_2)$ definiert. Formal bekommen wir durch $(x_1, y_1, x_2, y_2) \mapsto S_1 \otimes_R S_2$, $(x_1, y_1, x_2, y_2) \mapsto (x_1x_2) \otimes_R (y_1y_2)$ eine 4-lineare Abbildung. Diese faktorisiert durch $S_1 \otimes_R S_2 \otimes_R S_1 \otimes_R S_2$ und zieht sich zu einer bilinearen Abbildung auf $(S_1 \otimes_R S_2) \times (S_1 \otimes_R S_2)$ zurück, welche die Multiplikation definiert.

Sei T eine R-Algebra und $g_i : S_i \to T$ zwei R-lineare Ringhomomorphismen. Dann definieren wir eine bilineare Abbildung $g : S_1 \times S_2 \to T$ durch $g(x, y) = xy$, und diese faktorisiert eindeutig durch eine R-lineare Abbildung $f : S_1 \otimes_R S_2 \to T$, welche aufgrund der Definitionen ebenfalls ein Ringhomomorphismus ist. Daher erfüllt $S_1 \otimes_R S_2$ die universelle Eigenschaft einer direkten Summe in der Kategorie der R-Algebren (deren Morphismen R-lineare Ringhomomorphismen sind).

Der vollständigkeit halber noch der folgende Satz.

5.1 Satz. *Für ein Diagramm $\mathcal{D}$ von R-Algebren existieren $\varprojlim \mathcal{D}$ und $\varinjlim \mathcal{D}$ als R-Algebren.*

Beweis. Die Aussage für $\varprojlim \mathcal{D}$ wird ganz analog zu der für Moduln wie in Satz **??** gezeigt. Für $\varinjlim \mathcal{D}$ verwendet man eine ring- statt modultheoretische Konstruktion wie in Satz 4.2. Insbesondere betrachtet man eingeschränkte Tensorprodukte, deren Elemente $\cdots \otimes 1 \otimes a_i \otimes \cdots \otimes a_j \otimes 1 \otimes \cdots$ an fast allen Stellen eine 1 haben. Die Prinzipien sind ähnlich wie in Satz **??** und wir lassen die Details aus. $\square$

Sind S_1 und S_2 R-Algebren und X ein Menge von Variablen, so gilt $S_1[X] \otimes_R \mathcal{S}_2 \cong (S_1 \otimes_R S_2)[X]$. Ist $S_1 = R[X]/J$ für eine Menge von Variablen X und ein Ideal J, so gilt $S_1 \otimes_R S_2 = S_2[X]/J$. Speziell ergibt sich $R[X] \otimes_R R[Y] \cong R[X \cup Y]$ und $(R[X]/I) \otimes_R (R[Y]/J) \cong R[X \cup Y]/\langle I, J\rangle$ für Y eine weitere Menge von Variablen mit $X \cap Y = \{\}$. Diese Aussagen sind analog zu denen für Moduln.

Die Charakterisierung linear disjunkter Körpererweiterungen E_1/K und E_2/K in einem Erweiterungskörper C zeigt, daß $E_1 \otimes_K E_2 \cong E_1E_2$ unter Verwendung der Multiplikationsabbildung genau dann gilt, wenn E_1 und E_2 linear disjunkt über K sind.

5.2 Gebrochene und invertierbare Ideale, Primidealfaktorisierung

Sei R ein kommutativer Ring und $\mathrm{Quot}(R)$ der volle Quotientenring von R, also $\mathrm{Quot}(R) = R[U^{-1}]$, wobei U die multiplikativ abgeschlossene Menge der regulären Elemente von R (Elemente $\neq 0$ die keine Nullteiler sind) bezeichnet. Der Homomorphismus $R \to \mathrm{Quot}(R)$, $r \mapsto r/1$ ist injektiv. Daher fassen wir R im folgenden als Teilring von $\mathrm{Quot}(R)$ auf. Die Elemente $\neq 0$ von $\mathrm{Quot}(R)$ sind entweder Einheiten oder Nullteiler.

5.2 Definition. Seien I, J zwei R-Untermoduln von $\mathrm{Quot}(R)$. Wir definieren

$$\begin{aligned} IJ &= \{\textstyle\sum_i x_i y_i \mid x_i \in I, y_i \in J\}, \\ (I : J) &= \{x \in \mathrm{Quot}(R) \mid xI \subseteq J\}, \\ I^{-1} &= (I : R). \end{aligned}$$

Ein R-Untermodul I von $\mathrm{Quot}(R)$ heißt invertierbares Ideal, wenn es einen R-Untermodul J von $\mathrm{Quot}(R)$ mit $IJ = R$ gibt.

Ein R-Untermodul I von $\mathrm{Quot}(R)$ heißt gebrochenes Ideal von R, wenn es ein $a \in U$ mit $aI = \{ax \mid x \in I\} \subseteq R$ gibt. Ein Ideal von R heißt ganzes Ideal.

Seien I, K gebrochene Ideale von R und J ein ganzes Ideal von R. Gilt $IJ = K$, so sagen wir, daß K durch I teilbar und daß I ein Teiler von K ist. Wir schreiben dann $I \mid K$.

Die ganzen Ideale von R sind auch gebrochene Ideale von R. Das folgende Lemma enthält im wesentlichen die Grundrechenregeln für gebrochene und invertierbare Ideale.

5.3 Lemma. *Seien I, J, K drei R-Untermoduln von* $\mathrm{Quot}(R)$. *Dann gelten die folgenden Aussagen.*

(*i*) *IJ und $(I : J)$ sind R-Untermoduln von* $\mathrm{Quot}(R)$. *Sind I, J gebrochene Ideale von R, so ist IJ ein gebrochenes Ideal von R und $(I : J)$ für $I \neq 0$ ein gebrochenes Ideal von R.*

(*ii*) *$(IJ)K = I(JK)$, $IJ = JI$ und $RI = IR = I$. Die R-Untermoduln von* $\mathrm{Quot}(R)$ *bilden einen abelschen Monoid mit Einselement R, und die gebrochenen Ideale bilden einen Untermonoid davon.*

(*iii*) *Ist I invertierbar, so ist I endlich erzeugt und ein gebrochenes Ideal von R. Die invertierbaren Ideale bilden die Untergruppe der im Monoid der gebrochenen Ideale von R invertierbaren Elemente.*

(*iv*) *Gilt $IJ = K$ und ist K invertierbar, so sind auch I und J invertierbar.*

(*v*) *Aus $J \subseteq K$ folgt $IJ \subseteq IK$. Ist I*

invertierbar und gilt $IJ \subseteq IK$, so folgt auch $J \subseteq K$.

(*vi*) *Ist I invertierbar, so gilt $I \neq 0$, $II^{-1} = R$ und $(I : J) = I^{-1}J$.*

(*vii*) *Aus $I \mid K$ folgt $I \supseteq K$. Ist I invertierbar und gilt $I \supseteq K$, so folgt auch $I \mid K$.*

(*viii*) *Sind I, J gebrochene Ideale von R, so sind auch $I + J$ und $I \cap J$ gebrochene Ideale von R.*

(*ix*) *Ein gebrochenes Hauptideal Ra mit $a \in$* $\mathrm{Quot}(R)$ *ist genau dann invertierbar, wenn $a \in$* $\mathrm{Quot}(R)^\times$ *gilt.*

(*x*) *Jedes gebrochene Ideal I ist von der Form $K^{-1}J$ mit einem ganzen Ideal J und einem ganzen, invertierbaren (Haupt)Ideal K.*

Beweis. (*i*): Die erste Aussage ist direkt zu sehen, und die zweite wie folgt: Aus $aI \subseteq R$ und $bJ \subseteq R$ folgt $(ab)IJ \subseteq R$. Für $c \in I \backslash \{0\}$ gilt $bc(I : J) \subseteq bJ \subseteq R$.

(*ii*): Klar unter Verwendung der Definitionen und von (*i*).

(*iii*): Sei J der R-Untermodul von $\mathrm{Quot}(R)$ mit $IJ = R$. Es gibt endlich viele $x_i \in I$ und $y_i \in J$ mit $1 = \sum_{i=1}^n x_i y_i$. Sei $x \in I$ beliebig. Dann gilt $x = x \sum_{i=1}^n x_i y_i = \sum_{i=1}^n (xy_i) x_i$, wobei $xy_i \in R$ für alle $1 \leq i \leq n$ ist. Also sind die x_i ein Erzeugendensystem von I. Weiter gibt es ein $a \in R \backslash \{0\}$ mit $ax_i \in R$ für alle $1 \leq i \leq n$. Dann gilt auch $aI \subseteq R$, und I ist ein gebrochenes Ideal von R. Der Rest der Aussage ist klar mit (*i*) und (*ii*).

(*iv*): Aus $IJ = K$ folgt $I(JK^{-1}) = J(IK^{-1}) = R$, also sind I und J invertierbar (allgemein sind in einem Monoid Teiler von Einheiten wieder Einheiten).

(*v*): Die erste Implikation folgt direkt aus den Definitionen. Gilt $IJ \subseteq IK$, so erhalten wir aus der ersten Implikation $J = I^{-1}IJ \subseteq I^{-1}IK = K$.

(vi): Für invertierbare Ideale gilt notwendigerweise $I \neq 0$. Aufgrund der Definition von I^{-1} gilt $II^{-1} \subseteq R$. Ist I invertierbar und J der R-Untermodul von $\mathrm{Quot}(R)$ mit $IJ = R$, so gilt $J \subseteq I^{-1}$. Daraus ergibt sich $R = IJ \subseteq II^{-1} \subseteq R$, also $II^{-1} = R$. Da Inverse in Monoiden eindeutig bestimmt sind, folgt $I^{-1} = J$.

Ist I invertierbar, so gilt $(I : J) = I^{-1}J$. Die Inklusion $\supseteq$ ist klar und gilt auch für nicht-invertierbares I. Auf der anderen Seite gilt $(I : J)I \subseteq J$, also folgt durch Multiplikation mit I^{-1} wie gewünscht $(I : J) \subseteq I^{-1}J$.

(vii): Für $I \,|\, K$ gibt es ein ganzes Ideal J von R mit $IJ = K$. Dann gilt $I \supseteq IJ = K$, also $I \supseteq K$. Sind umgekehrt I und K gebrochene Ideale mit $I \supseteq K$ und ist I invertierbar, so folgt $R = II^{-1} \supseteq KI^{-1}$. Mit $J = KI^{-1}$ gilt also $IJ = IKI^{-1} = II^{-1}K = K$, und K wird von I geteilt.

$(viii)$: Gilt $aI \subseteq R$ und $bJ \subseteq R$ mit $a, b \in R\backslash\{0\}$, so folgt $a(I \cap J) \subseteq R$ und $(ab)(I + J) \subseteq R$ mit $ab \in R\backslash\{0\}$.

(ix): Gilt $a \in \mathrm{Quot}(R)^\times$, so folgt $(Ra)(Ra^{-1}) = R$, also ist Ra invertierbar. Sei J ein R-Untermodul von $\mathrm{Quot}(R)$ mit $(Ra)J = R$. Dann gibt es $b \in J$ mit $ab = 1$. Also folgt $a \in \mathrm{Quot}(R)^\times$.

(x): Folgt direkt aus den Definitionen und aus (ix). □

Ist I ein invertierbares Ideal von R, so nennen wir I^{-1} das inverse Ideal von I. Ist M ein R-Modul, so nennen wir $x \in M\backslash\{0\}$ regulär, wenn $\mathrm{Ann}_R(x) = \{0\}$ gilt. Andernfalls heißt x ein Nullteiler von M. Ein torsionsfreier R-Modul M enthält neben 0 nur reguläre Elemente.

5.4 Lemma. *Seien I, J zwei R-Untermoduln von $\mathrm{Quot}(R)$, und I enthalte mindestens ein reguläres Element. Dann ist $\phi : (I : J) \to \mathrm{Hom}_R(I, J)$, $c \mapsto (x \mapsto cx)$ ein Isomorphismus. Hierbei ist $\phi(c)$ genau dann ein Isomorphismus, wenn $c \in \mathrm{Quot}(R)^\times$ gilt.*

Beweis. Es ist klar, daß ϕ einen Homomorphismus definiert. Gilt $\phi(c) = 0$, so folgt $cI = 0$ und, da I ein reguläres Element enthält, auch $c = 0$. Also ist ϕ ein Monomorphismus.

Zum Beweis der Surjektivität sei $f \in \mathrm{Hom}_R(I, J)$. Sei $x \in I$ ein reguläres Element von I. Dann ist x von der Form v/u mit $u, v \in U$. Wir können daher $c = f(x)/x \in \mathrm{Quot}(R)$ definieren. Nun ist f auch $\mathrm{Quot}(R)$-linear ($R[U^{-1}]$-Linearität gilt allgemein für einen R-Homomorphismus $\phi : M \to N$ von $R[U^{-1}]$-Moduln M, N). Daher erhalten wir, daß c unabhängig von der Wahl von x definiert ist und $f(y) = f((y/x)x) = (y/x)f(x) = (y/x)(cx) = cy$ für alle $y \in I$ gilt. Daher ist $\phi(c) = f$ und ϕ ist surjektiv.

Allgemein gilt: In einem Ring ist $x \mapsto cx$ genau dann bijektiv, wenn $c \in R^\times$ gilt („$\Leftarrow$“ ist klar, für „$\Rightarrow$“ gibt es $x \in R$ mit $cx = 1$, also ist $c \in \mathbb{R}^\times$). Daraus folgt die letzte Aussage. □

5.5 Lemma. *Seien $\mathfrak{p}$ und $\mathfrak{q}$ invertierbare Primideale mit $\mathfrak{q} \supseteq \mathfrak{p}$. Dann gilt $\mathfrak{q} = \mathfrak{p}$.*

Beweis. Wir nehmen $\mathfrak{p} \neq 0$ an. Dann gibt es ein ganzes Ideal I mit $\mathfrak{q}I = \mathfrak{p}$. Gilt $\mathfrak{q} \supsetneq \mathfrak{p}$, so folgt $I \subseteq \mathfrak{p}$, da $\mathfrak{p}$ Primideal ist. Dann folgt $\mathfrak{p} = \mathfrak{q}I \subseteq \mathfrak{q}\mathfrak{p} \subseteq \mathfrak{p}$, also $\mathfrak{p} = \mathfrak{q}\mathfrak{p}$. Da $\mathfrak{p}$ invertierbar ist, folgt $R = \mathfrak{q}$ im Widerspruch zur Annahme. Also gilt $\mathfrak{q} = \mathfrak{p}$. □

5.6 Satz. *Sei I ein invertierbares Ideal von R und seien die $\mathfrak{p}_i$ paarweise verschiedene invertierbare Primideale von R mit $I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$ für $e_i \in \mathbb{Z}\backslash\{0\}$. Dann sind n und die Paare $(\mathfrak{p}_i, e_i)$ bis auf die Reihenfolge eindeutig bestimmt.*

Sei S eine Menge von invertierbaren Primidealen. Dann ist die Menge $\mathcal{I}_S = \{\prod_{\mathfrak{p}\in S} \mathfrak{p}^{e_\mathfrak{p}} \mid e_\mathfrak{p} \in \mathbb{Z}$ fast alle Null$\}$ eine freie abelsche Gruppe von invertierbaren Primidealen von R mit Basis S.

Beweis. Seien $\mathfrak{q}_j$ paarweise verschiedene invertierbare Primideale von R mit $I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{m} \mathfrak{q}_j^{f_j}$ für $f_j \in \mathbb{Z}\backslash\{0\}$. Wir müssen zeigen, daß $n = m$ gilt und die $(\mathfrak{p}_i, e_i)$ mit den $(\mathfrak{q}_j, f_j)$ bis auf die Reihenfolge übereinstimmen. Indem wir beide Seiten der Gleichung mit allen $\mathfrak{p}_i^{e_i}$ und $\mathfrak{q}_j^{f_j}$ mit $e_i < 0$ und $f_j < 0$ multiplizieren und die $\mathfrak{p}_i$, $\mathfrak{q}_j$, n, m geeignet neu definieren, können wir uns auf das folgende Problem reduzieren: Es gelte $J = \prod_{i=1}^{n} \mathfrak{p}_i = \prod_{j=1}^{m} \mathfrak{q}_j$ mit nicht notwendigerweise paarweise verschiedenen invertierbaren Primidealen $\mathfrak{p}_i$ und $\mathfrak{q}_j$. Zu zeigen ist $n = m$, und daß die $\mathfrak{p}_i$ mit den $\mathfrak{q}_j$ bis auf die Reihenfolge übereinstimmen.

Nach Umordnung erhalten wir $\mathfrak{p}_n \supseteq \mathfrak{q}_m$ aus der Primidealeigenschaft von $\mathfrak{p}_n$ und $\mathfrak{p}_n = \mathfrak{q}_m$ nach Lemma 5.5. Multiplikation mit $\mathfrak{p}_n^{-1}$ liefert $\prod_{i=1}^{n-1} \mathfrak{p}_i = \prod_{j=1}^{m-1} \mathfrak{q}_j$. Induktiv gelangen wir zu $R = \prod_{j=1}^{m'} \mathfrak{q}_j$. Wegen $R \supsetneq \mathfrak{q}_1 \supseteq \prod_{j=1}^{m'} \mathfrak{q}_j$ für $m' \geq 1$ folgt schließlich $m' = 0$.

Die letzte Aussage folgt unmittelbar aus der ersten Aussage und aus Lemma 5.3, (*iii*). □

5.7 Definition. Sei R ein Ring und $\mathcal{I}$ eine Menge von invertierbaren Idealen von R. Läßt sich jedes $I \in \mathcal{I}$ in Primideale aus $\mathcal{I}$ faktorisieren, so sagen wir, daß $\mathcal{I}$ die Primidealfaktorisierungseigenschaft besitzt.

Zum Beispiel besitzt die Menge $\mathcal{I}_S$ aus Satz 5.6 die Primidealfaktorisierungseigenschaft. Wir wollen jedoch Mengen $\mathcal{I}$ mit Primidealfaktorisierungseigenschaft auch auf andere Weise charakterisieren. Dabei ist die folgende Beobachtung hilfreich.

5.8 Satz. *Sei R ein noetherscher Ring und $\mathcal{I}$ eine Menge von ganzen, invertierbaren Idealen von R, die bezüglich der Idealmultiplikation abgeschlossen ist und für die $R \in \mathcal{I}$ gilt. Dann besitzt $\mathcal{I}$ genau dann die Primidealfaktorisierungseigenschaft, wenn es für jedes $I \in \mathcal{I}$ mit $I \neq R$ ein Primideal $\mathfrak{p} \in \mathcal{I}$ mit $\mathfrak{p} \supseteq I$ und $\mathfrak{p}^{-1}I \in \mathcal{I}$ gibt.*

Beweis. „$\Rightarrow$“: Sei $I \in \mathcal{I}$ mit $I \neq R$. Es gilt $I = \prod_{i=1}^{n} \mathfrak{p}_i$ mit invertierbaren Primidealen $\mathfrak{p}_i \in \mathcal{I}$ und $n \geq 1$. Wegen $\mathfrak{p}_1 \supseteq \prod_{i=1}^{n} \mathfrak{p}_i = I$ und $\mathfrak{p}_1^{-1} I = \prod_{i=2}^{n} \mathfrak{p}_i \in \mathcal{I}$ aufgrund der multiplikativen Abgeschlossenheit besitzt $\mathcal{I}$ die besagte Eigenschaft.

„$\Leftarrow$“: Falls nicht alle Ideale aus $\mathcal{I}$ in Primideale aus $\mathcal{I}$ faktorisiert werden können, gibt es ein bezüglich Inklusion maximales Ideal $I \in \mathcal{I}$ mit dieser Eigenschaft, da R nach Voraussetzung noethersch ist. Es gilt $I \neq R$, weil R das leere Produkt ist. Nach Voraussetzung existiert ein invertierbares Primideal $\mathfrak{p} \in \mathcal{I}$ mit $\mathfrak{p} \supseteq I$ und $\mathfrak{p}^{-1} I \in \mathcal{I}$. Da I invertierbar ist, gilt $I \supsetneq \mathfrak{p} I$, denn sonst hätten wir $R = \mathfrak{p}$ nach Multiplikation mit I^{-1}. Multiplikation mit $\mathfrak{p}^{-1}$ liefert nun $R \supseteq \mathfrak{p}^{-1} I \supsetneq I$. Nach Konstruktion gibt es invertierbare Primideale $\mathfrak{p}_i \in \mathcal{I}$ mit $\mathfrak{p}^{-1} I = \prod_i \mathfrak{p}_i$. Daraus folgt $I = \mathfrak{p} \prod_i \mathfrak{p}_i$, also läßt sich I doch in Primideale faktorisieren. □

5.9 Definition. Ein kommutativer Ring mit $1 \neq 0$, für den jedes Ideal $\neq 0$ invertierbar ist, heißt Dedekindring.

Die Eigenschaften invertierbarer Ideale aus Lemma 5.3, (*iii*) und (*ix*) zeigen, daß R ein noetherscher Integritätsring ist (ein Element $a \in R \backslash \{0\}$ erfüllt genau dann $a \in \mathrm{Quot}(R)^\times$, wenn a kein Nullteiler von R ist).

5.10 Korollar. *In einem Dedekindring läßt sich jedes gebrochene Ideal $\neq 0$ eindeutig in Primideale faktorisieren.*

Beweis. Die Menge aller ganzen Ideale $\neq 0$ besitzt nach Satz 5.8 die Primidealfaktorisierungseigenschaft, so daß die Behauptung aus Lemma 5.3, (x) und Satz 5.6 folgt. □

Beim einem Dedekindring handelt es sich also um einen bestmöglichen Ring, was die Primidealfaktorisierung in invertierbare Primideale angeht. Zum Beispiel sind Hauptidealringe auch Dedekindringe, aber die Umkehrung hiervon gilt nicht. Es ist jetzt interessant, nach anderen Kriterien für Ringe und Ideale zu suchen, mit denen die Eigenschaft in Satz 5.8 und speziell die Dedekindringeigenschaft überprüft werden kann.

5.3 Lokale Charakterisierungen invertierbarer Ideale

Wir untersuchen zunächst das Verhalten unter Lokalisierung und machen dazu eine Vorbemerkung.

Sei V die Menge der regulären Elemente von R und W das Urbild der Menge der regulären Elemente von $R[U^{-1}]$ unter dem Lokalisierungshomomorphismus $R \to R[U^{-1}]$. Dann gilt $\mathrm{Quot}(R) = R[V^{-1}]$ und $\mathrm{Quot}(R)[U^{-1}] = R[(UV)^{-1}]$. Da

reguläre Elemente unter Lokalisierungshomomorphismen nach Satz **??** wieder auf reguläre Elemente abgebildet werden, gilt auch $\mathrm{Quot}(R[U^{-1}]) = R[(UVW)^{-1}]$. Wir erhalten $R[U^{-1}] \subseteq \mathrm{Quot}(R)[U^{-1}] \subseteq \mathrm{Quot}(R[U^{-1}])$ und den Lokalisierungshomomorphismus $\iota : \mathrm{Quot}(R) \to \mathrm{Quot}(R)[U^{-1}]$, welcher den Lokalisierungshomomorphismus $R \to R[U^{-1}]$ fortsetzt.

Ist I ein R-Untermodul von $\mathrm{Quot}(R)$, so sei $I[U^{-1}] = R[U^{-1}]\iota(I)$ der zugehörige $R[U^{-1}]$-Untermodul von $\mathrm{Quot}(R[U^{-1}])$.

5.11 Lemma. *Sei R ein kommutativer Ring und U eine multiplikativ abgeschlossene Teilmenge von R mit $1 \in U$.*

(*i*) *Für R-Untermoduln I, J von $\mathrm{Quot}(R)$ gilt $(IJ)[U^{-1}] = I[U^{-1}] \cdot J[U^{-1}]$.*

(*ii*) *Für jedes ganze (gebrochene, invertierbare) Ideal I von R ist $I[U^{-1}]$ ein ganzes (gebrochenes, invertierbares) Ideal von $R[U^{-1}]$.*

(*iii*) *Ist $\mathcal{I}$ eine Menge von Idealen mit Primfaktorisierungseigenschaft und ist $\mathcal{I}[U^{-1}] := \{I[U^{-1}] \mid I \in \mathcal{I}\}$, so besitzt $\mathcal{I}[U^{-1}]$ ebenfalls die Primidealfaktorisierungseigenschaft.*

(*iv*) *Für einen Dedekindring R ist $R[U^{-1}]$ ebenfalls ein Dedekindring.*

(*v*) *Seien I, J zwei R-Untermoduln von $\mathrm{Quot}(R)$. Ist I invertierbar oder gilt $\mathrm{Quot}(R)[U^{-1}] = \mathrm{Quot}(R[U^{-1}])$ (zum Beispiel wenn R ein Integritätsring ist) und ist I endlich erzeugt, so gilt $(I : J)[U^{-1}] = (I[U^{-1}] : J[U^{-1}])$.*

Beweis. (*i*): Es gilt $(IJ)[U^{-1}] = R[U^{-1}]\iota(IJ) = R[U^{-1}]\iota(I)\iota(J) = R[U^{-1}]\iota(I) \cdot R[U^{-1}]\iota(J) = I[U^{-1}]J[U^{-1}]$.

(*ii*): Sei $I \subseteq R$ ein ganzes Ideal von R. Dann folgt $\iota(I) \subseteq R[U^{-1}]$ und $I[U^{-1}] = R[U^{-1}]\iota(I) \subseteq R[U^{-1}]$, also ist $I[U^{-1}]$ ein ganzes Ideal von $R[U^{-1}]$.

Sei $I \subseteq \mathrm{Quot}(R)$ ein gebrochenes Ideal von R. Ist $a \in V$ mit $aI \subseteq R$, so folgt $aI[U^{-1}] = aR[U^{-1}]\iota(I) = R[U^{-1}]\iota(aI) \subseteq R[U^{-1}]$, also ist $I[U^{-1}]$ ein gebrochenes Ideal von $R[U^{-1}]$.

Sei $I \subseteq \mathrm{Quot}(R)$ ein invertierbares Ideal von R. Aus $IJ = R$ folgt $I[U^{-1}] \cdot J[U^{-1}] = R[U^{-1}]$ nach (*i*), also ist $I[U^{-1}]$ ein invertierbares Ideal von $R[U^{-1}]$.

(*iii*): Folgt aus (*i*), (*ii*) und Satz **??**, da Lokalisieren einer Primidealfaktorisierung wie in Satz 5.8, (*i*) wieder eine solche liefert (unter Umständen mit weniger Primidealen, falls Primideale zu $R[U^{-1}]$ lokalisieren).

(*iv*): Die Ideale von $R[U^{-1}]$ sind nach Satz **??** von der Form $I[U^{-1}]$ für ein Ideal I von R. Für $I \neq 0$ ist nach Voraussetzung $II^{-1} = R$ und $I[U^{-1}]$ nach (*ii*) invertierbar.

(*v*): Für I invertierbar gilt $(I[U^{-1}] : J[U^{-1}]) = I[U^{-1}]^{-1}J[U^{-1}] = (I^{-1})[U^{-1}] \cdot J[U^{-1}] = (I^{-1}J)[U^{-1}] = (I : J)[U^{-1}]$ wegen (*i*) und (*ii*).

Es gelte $\mathrm{Quot}(R)[U^{-1}] = \mathrm{Quot}(R[U^{-1}])$. Allgemein folgt zunächst aus $(I : J)I \subseteq J$ auch $(I : J)[U^{-1}]I[U^{-1}] \subseteq J[U^{-1}]$ durch Anwendung von (i), also $(I : J)[U^{-1}] \subseteq (I[U^{-1}] : J[U^{-1}])$. Aufgrund der Annahme sind die Elemente aus $(I[U^{-1}] : J[U^{-1}])$ von der Form a/u mit $a \in \mathrm{Quot}(R)$ und $u \in U$ (und nicht etwa noch Nenner aus W). Für ein solches a/u gilt auch $a \in (I[U^{-1}] : J[U^{-1}])$. Seien die b_i ein endliches Erzeugendensystem von I. Für jedes b_i gibt es dann ein $c_i \in J$ und $v_i \in U$ mit $ab_i = c_i/v_i$ in $\mathrm{Quot}(R)[U^{-1}]$. Also gibt es $w_i \in U$ mit $w_i v_i a b_i \in J$ in $\mathrm{Quot}(R)$. Sei $d = \prod_i w_i v_i \in U$. Es folgt $dab_i \in J$ für alle i und daher $da \in (I : J)$. Wir erhalten $a \in (I : J)[U^{-1}]$ und schließlich $a/u \in (I : J)[U^{-1}]$.

Ist R ein Integritätsring, so gilt $UW \subseteq V$ und $\mathrm{Quot}(R) = \mathrm{Quot}(R)[U^{-1}] = \mathrm{Quot}(R[U^{-1}])$. □

Für $R = \mathbb{Q}[x, y, z]/(xy, zy)$ und $U = \langle x \rangle$ gilt $\mathrm{Quot}(R)[U^{-1}] \subsetneq \mathrm{Quot}(R[U^{-1}])$, da $z \in \mathrm{Quot}(R)[U^{-1}]$ weder eine Einheit noch ein Nullteiler ist, aber in $\mathrm{Quot}(R[U^{-1}])$ invertierbar ist.

5.12 Satz. *Sei R ein kommutativer Ring. Für einen R-Untermodul $I \neq 0$ von $\mathrm{Quot}(R)$ sind äquivalent:*

(i) I ist invertierbar.

(ii) I ist projektiv.

(iii) I ist lokal frei vom Rang 1.

Beweis. $(i) \Rightarrow (ii)$: Sei I invertierbar und die x_i, y_i wie im Beweis von Lemma 5.3, (iii). Wir definieren $\lambda_i \in \mathrm{Hom}_R(I, R)$ durch $x \mapsto xy_i$. Dann sind die λ_i Koordinatenfunktionale bezüglich der Erzeuger x_i und I ist nach Satz 4.22 projektiv.

$(ii) \Rightarrow (iii)$: Sei nun I projektiv. Dann gibt es nach Satz 4.22 ein Erzeugendensystem x_i (vielleicht unendlich) und Koordinatenfunktionale $\lambda_i \in \mathrm{Hom}_R(I, R)$. Nach Lemma 5.4 gibt es $y_i \in \mathrm{Quot}(R)$ mit $\lambda_i(x) = xy_i$ für alle $x \in I$. Da $I \neq 0$ und nach Satz 4.29 torsionsfrei ist, gibt es $x \in I$ mit $x \in \mathrm{Quot}(R)^\times$. Dann gilt $x = \sum_i \lambda_i(x)x_i = \sum_i xy_ix_i$, wobei die Summe endlich ist und daher $y_ix_i = 0$ für fast alle i wegen $x \in \mathrm{Quot}(R)^\times$ gilt. Also sind die endlich vielen x_i mit $x_iy_i \neq 0$ ein endliches Erzeugendensystem von I. Nach Satz 4.29 und Satz 4.33 ist damit I lokal frei. Sei $\mathfrak{m}$ ein maximales Ideal von R. Dann ist $I_\mathfrak{m}$ also frei. Da $I_\mathfrak{m}$ ein $R_\mathfrak{m}$-Untermodul von $\mathrm{Quot}(R_\mathfrak{m})$ ist und daher keine zwei Elemente $R_\mathfrak{m}$-linear unabhängig sein können, folgt, daß $I_\mathfrak{m}$ frei vom Rang 1 ist.

$(iii) \Rightarrow (i)$: Wir betrachten den Inklusionshomomorphismus $\phi : II^{-1} \to R$. Für jedes maximale Ideal $\mathfrak{m}$ von R bekommen wir unter Verwendung von Lemma 5.11 den lokalisierten Monomorphismus $\phi_\mathfrak{m} : I_\mathfrak{m}I_\mathfrak{m}^{-1} \to R_\mathfrak{m}$. Da $I_\mathfrak{m}$ frei vom Rang 1 ist, gibt es $a \in \mathrm{Quot}(R_\mathfrak{m})$ mit $I_\mathfrak{m} = aR_\mathfrak{m}$. Aus der Definition von $I_\mathfrak{m}^{-1}$ folgt

$I_\mathfrak{m}^{-1} = a^{-1}R_\mathfrak{m}$. Es ergibt sich $I_\mathfrak{m}I_\mathfrak{m}^{-1} = R_\mathfrak{m}$, also ist $\phi_\mathfrak{m}$ surjektiv und nach Satz 4.13 ist ϕ ein Isomorphismus und daher $II^{-1} = R$.

Zusatz: Um den Gebrauch der allgemeinen Sätze Satz 4.29 und Satz 4.33 zu vermeiden, beweisen wir noch $(ii) \Rightarrow (i)$ und $(i) \Rightarrow (iii)$ auf direktem Weg.

$(ii) \Rightarrow (i)$: Sei I projektiv. Dann gibt es nach Satz 4.22 ein Erzeugendensystem x_i (vielleicht unendlich) und Koordinatenfunktionale $\lambda_i \in \mathrm{Hom}_R(I, R)$. Nach Lemma 5.4 gibt es $y_i \in \mathrm{Quot}(R)$ mit $\lambda_i(x) = xy_i$ für alle $x \in I$. Da $I \neq 0$ und nach Satz 4.29 torsionsfrei ist, gibt es $x \in I$ mit $x \in \mathrm{Quot}(R)^\times$. Dann gilt $x = \sum_i \lambda_i(x)x_i = \sum_i xy_ix_i$, wobei die Summe endlich ist. Division durch x ergibt $1 = \sum_i y_ix_i$. Wegen $xy_i \in R$ für alle $x \in I$ gilt $y_i \in I^{-1}$. Also folgt $1 \in II^{-1}$ und somit $II^{-1} = R$.

$(i) \Rightarrow (iii)$: Sei I invertierbar. Wegen $II^{-1} = R$ gibt es $x_i \in I$ und $y_i \in I^{-1}$ mit $1 = \sum_i x_iy_i$. Sei $\mathfrak{m}$ ein maximales Ideal von R. Wir fassen $I_\mathfrak{m}$ und $I_\mathfrak{m}^{-1}$ als Untermoduln von $\mathrm{Quot}(R_\mathfrak{m})$ auf. Dann gibt es ein i mit $x_iy_i \in R_\mathfrak{m}\backslash\mathfrak{m}R_\mathfrak{m}$, also $x_iy_i \in R_\mathfrak{m}^\times$. Es folgt $(x_iy_i)^{-1}x_i \in I_\mathfrak{m}$ und $y_i((x_iy_i)^{-1}x_i) = 1$, also $y_iI_\mathfrak{m} = R_\mathfrak{m}$. Daraus ergibt sich $y_i \in \mathrm{Quot}(R_\mathfrak{m})^\times$ und $I_\mathfrak{m} = R_\mathfrak{m}y_i^{-1}$, also ist $I_\mathfrak{m}$ frei vom Rang 1. □

5.13 Satz. *Ein Integritätsring R ist genau dann ein Dedekindring, wenn $R_\mathfrak{p}$ für jedes Primideal $\mathfrak{p}$ ein Hauptidealring ist.*

Beweis. „$\Rightarrow$“: Sei R ein Dedekindring. Sei $J \neq 0$ ein Ideal von $R_\mathfrak{p}$ und $\iota_\mathfrak{p} : R \to R_\mathfrak{p}$ der Lokalisierungshomomorphismus. Wir setzen $I = \iota_\mathfrak{p}^{-1}(J)$. Dann gilt $I \neq 0$ und $I_\mathfrak{p} = \iota_\mathfrak{p}(I) = J$. Da R ein Dedekindring ist, ist I invertierbar. Nach Satz 5.12 ist dann $J = I_\mathfrak{p}$ ein Hauptideal.

„$\Leftarrow$“: Sei $I \neq 0$ ein Ideal von R. Für jedes Primideal $\mathfrak{p}$ von R ist $I_\mathfrak{p}$ ein Hauptideal, da $R_\mathfrak{p}$ ein Hauptidealring ist, und es gilt $I_\mathfrak{p} \neq 0$, da R ein Integritätsring ist. Daher ist $I_\mathfrak{p}$ lokal frei vom Rang 1. Nach Satz 5.12 ist I invertierbar. □

Da jedes $R_\mathfrak{p}$ eine Lokalisierung von $R_\mathfrak{m}$ für ein maximales Ideal $\mathfrak{m}$ von R ist und Lokalisierung von Hauptidealringen wieder Hauptidealringe liefert (Satz **??**), genügt es in Satz 5.13 zu fordern, daß $R_\mathfrak{m}$ für jedes maximale Ideal von R ein Hauptidealring ist.

Sei R ein kommutativer Ring mit 1. Die Länge der echt aufsteigenden Kette $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ von Primidealen $\mathfrak{p}_i$ von R ist n. Die Dimension $\dim(R)$ von R ist das Supremum über die Länge aller echt aufsteigenden Ketten von Primidealen von R.

Zum Beispiel ist die Dimension des Polynomrings $k[x_1, \ldots, x_n]$ über dem Körper k gleich n.

Ist $\mathfrak{p}$ ein Primideal, so nennen wir $\dim(R/\mathfrak{p})$ die Dimension und $\dim(R_\mathfrak{p})$ die Kodimension von R.

Ist R ein Integritätsring mit $\dim(R) = 0$, so ist R ein Körper. Denn $\{0\}$ ist ein Primideal, und wegen $\dim(R) = 0$ ist es das einzige Primideal von R. Daher ist es maximal und jedes Element $\neq 0$ eine Einheit.

Ist R ein Integritätsring mit $\dim(R) = 1$, so ist $\{0\}$ ein Primideal und jedes weitere Primideal ist $\neq 0$ und maximal.

Für einen Integritätsring R ist Bedingung $\dim(R) \leq 1$ also äquivalent dazu, daß jedes Primideal $\neq 0$ von R maximal ist.

5.14 Satz. *Für einen Dedekindring R ist $\dim(R) \leq 1$, wobei R genau dann ein Körper ist, wenn $\dim(R) = 0$ gilt.*

Beweis. Jeder Körper K ist ein Dedekindring, denn K ist das einzige Ideal $\neq 0$ und K ist invertierbar. Für einen Dedekindring R gilt $\dim(R) \leq 1$. Denn entweder ist $\{0\}$ maximales Ideal und R ein Körper, oder jedes Primideal $\mathfrak{p} \neq 0$ ist invertierbar und wegen Lemma 5.5 maximal. □

5.15 Definition. Ein diskreter Bewertungsring ist ein lokaler Hauptidealring der Dimension 1.

Ist R ein diskreter Bewertungsring, so gibt genau ein maximales Ideal $\mathfrak{m} = \pi R \neq 0$ von R. Dann ist $\mathfrak{m}$ das einzige Primideal $\neq 0$, und π ist ein Primelement. Da R auch faktoriell ist, gibt es zu jedem $a \in R\backslash\{0\}$ genau ein $u \in R^\times$ und $e \in \mathbb{Z}^{\geq 0}$ mit $a = u\pi^e$. Die Zuordnung $v : R \to \mathbb{Z} \cup \{\infty\}$ mit $v(a) = e$ und $v(0) = \infty$ liefert eine surjektive, diskrete Bewertung (siehe Algebra 1).

5.16 Lemma. *Sei R ein Ring und $\mathfrak{p} \neq 0$ ein Primideal von R, welches mindestens ein reguläres Element enthält. Dann gilt $1 \leq \dim(R_\mathfrak{p}) \leq \dim(R)$.*

Beweis. Zunächst ist klar, daß $\dim(R_\mathfrak{p}) \leq \dim(R)$ gilt, da ineinander enthaltende Primideale von $R_\mathfrak{p}$ eindeutig ineinander enthaltenen (bezüglich $U = R\backslash\mathfrak{p}$ abgeschlossenen) Primidealen von R entsprechen.

Sei $d \in \mathfrak{p}$ das reguläre Element. Dann ist auch $d/1 \in R_\mathfrak{p}$ ein reguläres Element und keine Einheit, da es sonst $u, v \in U = R\backslash\mathfrak{p}$ mit $ud = v$ geben müßte und sich wegen $v \notin \mathfrak{p}$ und $v = ud \in \mathfrak{p}$ ein Widerspruch ergibt. Also ist $R_\mathfrak{p}$ kein Körper und es folgt $\dim(R_\mathfrak{p}) \geq 1$. □

5.17 Lemma. *Sei R ein Ring und $I \neq 0$ ein invertierbares ganzes Ideal von R. Dann enthält I mindestens ein reguläres Element von R.*

Beweis. Seien die $x_i \in I$ und die $y_i \in I^{-1}$ mit $1 = \sum_{i=1}^n x_i y_i$. Nach Definition von $\mathrm{Quot}(R)$ gibt es $z_i \in R$ und $u_i \in U$ (U die multiplikativ abgeschlossene Menge der regulären Elemente von R) mit $y_i = z_i/u_i$. Nach Multiplikation mit $u = \prod_{i=1} u_i$ erhalten wir $u = \sum_{i=1} x_i z_i$ in R und $u \in I$. Also enthält I das reguläre Element u. □

5.18 Satz. *Ein Integritätsring R ist genau dann ein Dedekindring, wenn $R_\mathfrak{p}$ für jedes Primideal $\mathfrak{p} \neq 0$ ein diskreter Bewertungsring ist.*

Beweis. Folgt aus Satz 5.13, Satz 5.14, Lemma 5.16 und Lemma 5.17. □

Dedekindringe treten beispielsweise als Maximalordnungen von Zahlkörpern und als Koordinatenringe nicht-singulärer algebraischer Kurven auf. Wir wollen die Aussage von Satz 5.18 noch etwas detaillierter und allgemeiner untersuchen. Der Satz 5.23 kann zum Beispiel auf beliebige Ordnungen von Zahlkörpern und auf die Koordinatenringe algebraischer Varietäten angewendet werden.

5.19 Lemma. *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Ist R noethersch, so gilt $\cap_{i\in\mathbb{Z}^{\geq 0}} \mathfrak{m}^i = 0$.*

Beweis. Sei $I = \cap_{i\in\mathbb{Z}^{\geq 0}} \mathfrak{m}^i$. Dann gilt $\mathfrak{m}I \subseteq I$. Außerdem haben wir $\mathfrak{m}^i \supseteq I$ und $\mathfrak{m}^{i+1} \supseteq \mathfrak{m}I$ für alle $i \in \mathbb{Z}^{\geq 0}$. Es folgt $I = \cap_{i\in\mathbb{Z}^{\geq 0}} \mathfrak{m}^{i+1} \supseteq \mathfrak{m}I$, zusammen also $I = \mathfrak{m}I$. Da R noethersch ist, ist ein I endlich erzeugter R-Modul mit $\mathfrak{m}I = I$. Nach Lemma 4.28 folgt $I = 0$. □

5.20 Lemma. *Sei R ein lokaler Ring der Dimension 1. Dann sind äquivalent:*

(i) R ist ein diskreter Bewertungsring.

(ii) R ist ein noetherscher Ring, dessen maximales Ideal ein Hauptideal ist und ein reguläres Element enthält.

(iii) R ist ein faktorieller Ring.

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

(ii) $\Rightarrow$ *(iii)*: Sei $\mathfrak{m} = \pi R$ das maximale Ideal von R mit $\pi \neq 0$ wegen $\dim(R) = 1$. Dann ist π ein Primelement von R. Für $x \in R\backslash\{0\}$ gibt es nach Lemma 5.19 ein ein maximales $e \in \mathbb{Z}^{\geq 0}$ mit $x \in \mathfrak{m}^e$, also $\pi^e \mid x$. Sei $u \in R$ mit $x = u\pi^e$. Wegen der Maximalität von e folgt $u \in R\backslash\pi R = R^\times$. Es bleibt zu zeigen, daß R ein Integritätsring ist. Da $\mathfrak{m}$ ein reguläres Element enthält, muß bereits π regulär sein. Jedes Element $\neq 0$ von R läßt sich wie gezeigt als Produkt einer Einheit und einer Potenz des regulären Elements π schreiben, und ist damit selbst regulär. Also enthält R keine Nullteiler und ist ein Integritätsring.

(iii) $\Rightarrow$ *(i)*: Sei π ein Primelement von R, welches wegen $\dim(R) \geq 1$ existiert. Dann ist $R\pi$ ein Primideal und wegen $\dim(R) = 1$ ist $R\pi$ das maximale Ideal von R. Sei v_π die Exponentenbewertung bezüglich π. Für jedes $x \in R\backslash\{0\}$ gilt dann $x = u\pi^{v_\pi(x)}$ mit einem $u \in R\backslash\pi R = R^\times$. Sei $I \neq 0$ ein Ideal von R und $e = \min\{v_\pi(x) \mid x \in I\backslash\{0\}\} \in \mathbb{Z}^{\geq 0}$. Dann gilt $I = R\pi^e$, und I ist ein Hauptideal. □

Lemma 5.20, (ii) trifft für die Ringe $R_\mathfrak{p}$ für alle Primideale $\mathfrak{p} \neq 0$ eines Dedekindrings zu. Unter Beachtung von Lemma 4.28 heißt das nichts anderes, als daß $\dim(R_\mathfrak{m}) \cong \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ für alle maximalen Primideale von R gilt. Man sagt, daß die lokalen Ringe $R_\mathfrak{m}$ regulär seien.

5.21 Satz. *Ein Ring R ist genau dann faktoriell, wenn jedes Primideal der Kodimension* 1 *ein Hauptideal ist.*

Beweis. „$\Leftarrow$“: Beweisen und brauchen wir nicht, aber siehe Matsumura ...

„$\Rightarrow$“: Wir machen eine allgemeine Vorbemerkung. Ist R ein faktorieller Ring und U eine multiplikativ abgeschlossene Teilmenge, so ist $R[U^{-1}]$ ebenfalls faktoriell. Sind die π_i ein vollständiges Vertretersystem von Primelementen modulo Assoziation, so liefern die π_i, die nicht zu Einheiten in $R[U^{-1}]$ werden, ein vollständiges Vertretersystem von Primelementen von $R[U^{-1}]$ modulo Assoziation. Hier ist die Begründung: Für $x \in R$ ist $x \in R[U^{-1}]^\times$ genau dann, wenn es $y \in R$ und $u \in U$ mit $x(y/u) = 1$ gibt, also wenn $xy = u$ und $x \mid u$ gilt. Ist π_i ein Primelement, welches kein Element aus U teilt, so ist π_i ein Primelement in $R[U^{-1}]$. Denn aus $\pi_i(c/w) = (a/u)(b/v)$ mit $a, b, c \in R$ und $u, v, w \in U$ folgt $\pi_i cuv = abw$, und daraus folgt $\pi_i \mid a$ oder $\pi_i \mid b$ nach Voraussetzung. Also teilt π_i auch a/u oder b/v und ist damit ein Primelement von $R[U^{-1}]$. Jedes Element aus $R[U^{-1}]$ kann als Potenzprodukt der π_i geschrieben werden, da dies bereits in R möglich ist. Sind π_i und π_j assoziiert in $R[U^{-1}]$, so gibt es $u, v \in U$ mit $u\pi_i = \pi_j v$. Da π_i und π_j weder u noch v teilen, folgt $\pi_i = \pi_j$ nach Voraussetzung.

Zum Beweis von „$\Rightarrow$“. Sei $\mathfrak{p}$ ein Primideal von R der Kodimension 1. Wegen $\dim(R_\mathfrak{p}) = 1$ ist $R_\mathfrak{p}$ ein lokaler faktorieller Ring der Dimension 1 und nach Lemma 5.20 ein diskreter Bewertungsring. Nach der obigen Vorbemerkung gibt es ein Primelement π von R, welches kein Element von $U = R \backslash \mathfrak{p}$ teilt und für welches $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p}$ gilt. Aus $x = (y/u)\pi \in R$ beziehunsgweise $ux = y\pi$ für $x, y \in R$ mit $x \neq 0$ und $u \in U$ folgt $\pi \mid x$. Daher ergibt sich $\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} \cap R = \pi R$ mit Satz **??**. $\square$

5.22 Satz. *Sei R ein noetherscher Ring und $\mathfrak{p}$ ein Primideal von R.*

(i) *Ist $\mathfrak{p}$ invertierbar, so ist $R_\mathfrak{p}$ ein diskreter Bewertungsring und $\mathfrak{p}$ hat Kodimension 1.*

(ii) *Hat $\mathfrak{p}$ Kodimension* 1 *und ist $R_\mathfrak{m}$ faktoriell für jedes maximale Ideal $\mathfrak{m}$ von R mit $\mathfrak{m} \supseteq \mathfrak{p}$, so ist $\mathfrak{p}$ invertierbar.*

Beweis. (i): Ist $\mathfrak{p}$ invertierbar, so gilt $\mathfrak{p} \neq 0$ und $R_\mathfrak{p}$ ist nach Lemma 5.16 und Lemma 5.17 ein lokaler Ring mit maximalem, invertierbarem Ideal $\mathfrak{p}R_\mathfrak{p}$ und $\dim(R_\mathfrak{p}) \geq 1$. Wegen Lemma 5.5 gilt auch $\dim(R_\mathfrak{p}) \leq 1$. Folglich hat $\mathfrak{p}$ Kodimension 1. Weiter ist $\mathfrak{p}R_\mathfrak{p}$ nach Satz 5.12 ein Hauptideal und enthält mit $\mathfrak{p}$ ein reguläres Element. Nach Lemma 5.20 ist $R_\mathfrak{p}$ dann ein diskreter Bewertungsring.

(ii): Nach Satz 5.12 genügt es zu beweisen, daß $\mathfrak{p}$ lokal ein Hauptideal $\neq 0$ ist. Dazu können wir uns auf Lokalisierungen für maximale Ideale beschränken. Ist $\mathfrak{m}$ ein maximales Ideal von R mit $\mathfrak{m} \not\supseteq \mathfrak{p}$, so gilt $\mathfrak{p}R_\mathfrak{m} = R_\mathfrak{m}$, also ist $\mathfrak{p}$ hier frei. Sei $\mathfrak{m}$ also ein maximales Ideal mit $\mathfrak{m} \supseteq \mathfrak{p}$. Dann ist $R_\mathfrak{m}$ nach Voraussetzung faktoriell und wir wollen zeigen, daß $\mathfrak{p}R_\mathfrak{m}$ ein Hauptideal $\neq 0$ ist. Zur Vereinfachung der Notation und da $R_\mathfrak{p}$ nur eine weitere Lokalisierung von $R_\mathfrak{m}$ ist, können wir annehmen: R ist faktoriell und $\mathfrak{p}$ ist ein Primideal von R der Kodimension 1. Aus Satz 5.21 folgt, daß $\mathfrak{p}$ wie gewünscht ein Hauptideal ist. Wegen $\dim(R_\mathfrak{p}) = 1$ folgt $\mathfrak{p} \neq 0$. □

5.23 Satz. *Sei R ein noetherscher Ring mit $1 \neq 0$ und $\mathcal{S}$ die Menge der maximalen Ideale von R, für die $R_\mathfrak{m}$ nicht faktoriell ist. Sei $\mathcal{I}$ die Menge der ganzen invertierbaren Ideale I von R, für die $I_\mathfrak{m} = R_\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m} \in \mathcal{S}$ gilt. Dann besitzt $\mathcal{I}$ die Primidealfaktorisierungseigenschaft.*

Beweis. Zunächst gilt $R \in \mathcal{I}$ und $\mathcal{I}$ ist nach Lemma 5.11 multiplikativ abgeschlossen. Damit sind die Voraussetzungen von Satz 5.8 erfüllt.

Wir wollen nun die zur Primidealfaktorisierungseigenschaft äquivalente Eigenschaft aus Satz 5.8 für $\mathcal{I}$ verifizieren. Sei $I \in \mathcal{I}$ mit $I \neq R$. Dann gibt es ein maximales Ideal $\mathfrak{n} \notin \mathcal{S}$ mit $I_\mathfrak{n} \neq R_\mathfrak{n}$, wobei $R_\mathfrak{n}$ faktoriell ist.

Da $I_\mathfrak{n}$ wegen der Invertierbarkeit von I ein Hauptideal ist, gibt es ein $x \in R$ mit $I_\mathfrak{n} = xR_\mathfrak{n}$. Wegen $I_\mathfrak{n} \neq R_\mathfrak{n}$ ist x keine Einheit in $R_\mathfrak{n}$ und es gibt ein Element $\pi \in R$, welches in $R_\mathfrak{n}$ ein Primelement mit $\pi \mid x$ ist. Sei $\mathfrak{p} = \iota_\mathfrak{n}^{-1}(\pi R_\mathfrak{n})$. Dann ist $\mathfrak{p}$ ein Primideal von R mit $\mathfrak{p} \supseteq I$.

Nach Konstruktion gilt $\mathfrak{p}R_\mathfrak{n} = \pi R_\mathfrak{n}$ und $R_\mathfrak{p}$ ist ein diskreter Bewertungsring. Für jedes maximale Ideal $\mathfrak{m} \supseteq \mathfrak{p}$ gilt $\mathfrak{m} \notin \mathcal{S}$ wegen $I_\mathfrak{p} \neq R_\mathfrak{p}$ und $R_\mathfrak{m}$ ist ein faktorieller Ring aufgrund der Definition von S und $\mathcal{I}$ (denn für $\mathfrak{m} \in \mathcal{S}$ gilt $I_\mathfrak{m} = R_\mathfrak{m}$, und daraus folgt $I_\mathfrak{p} = R_\mathfrak{p}$, was hier nicht der Fall ist). Nach Satz 5.22, (ii) ist $\mathfrak{p}$ daher invertierbar. Schließlich sind $\mathfrak{p}^{-1}$ und $\mathfrak{p}^{-1}I$ invertierbare Ideale, deren Lokalisierung bei $\mathfrak{m} \in \mathcal{S}$ nach Lemma 5.11 gleich $R_\mathfrak{m}$ ist. Also gilt $\mathfrak{p}^{-1}I \in \mathcal{I}$. Damit erfüllt $\mathcal{I}$ die Primidealfaktorisierungseigenschaft. □

Die Menge $\mathcal{S}$ kann als Menge singulärer Punkte von R aufgefaßt werden. Ist $\mathfrak{m}$ ein maximales Ideal (oder ein Primideal) und gilt $I_\mathfrak{m} \neq R_\mathfrak{m}$, so sagen wir, $\mathfrak{m}$ sei im Träger von I. Im Satz 5.23 wird also gefordert, daß die Ideale aus $\mathcal{I}$ keine singulären Punkte in ihren Trägern haben sollen.

Wir wollen die beiden voranstehenden Sätze hauptsächlich für $\dim(R) = 1$ anwenden. Hier ist ein $\dim(R) = 2$ Beispiel: Der Polynomring $k[x, y]$ über einem Körper ist faktoriell. Das maximale Ideal $\mathfrak{m} = Rx + Ry$ ist wegen $\dim(R_\mathfrak{m}) = 0$ nicht invertierbar. Jedes Primideal $\mathfrak{p}$ von R mit $\dim(R_\mathfrak{p}) = 1$ ist ein Hauptideal und invertierbar.

5.4 Ganze Ringerweiterungen

Seien S ein Ring und R ein Teilring von S. Dann nennen wir S auch einen Erweiterungsring von R und S/R eine Ringerweiterung. Gemäß unseren Konventionen gilt $1_R = 1_S$.

Ist S/R eine Ringerweiterung, können wir S auch als R-Algebra und R-Modul auffassen. Dann heißt S von endlichem Typ über R, wenn S als R-Algebra endlich erzeugt ist, wenn es also $x_1, \ldots, x_n \in S$ mit $S = R[x_1, \ldots, x_n]$ gibt. Weiter heißt S endlich über R, wenn S als R-Modul endlich erzeugt ist, wenn es also $y_1, \ldots, y_m \in S$ mit $S = Ry_1 + \cdots + Ry_m$ gibt.

Ein Element $x \in S$ heißt ganz über R, wenn es ein normiertes Polynom $f \in R[t]$ mit $f(x) = 0$ gibt. Die Ringerweiterung S/R heißt ganz, wenn jedes $x \in S$ ganz über R ist. Der ganze Abschluß von R in S ist $\mathrm{Cl}(R, S) = \{x \in S \mid x \text{ ganz über } R\}$. Der Ring R heißt ganz abgeschlossen (normal) in S, wenn $\mathrm{Cl}(R, S) = R$ gilt. Ferner heißt R ganz abgeschlossen (normal), wenn R ganz abgeschlossen in $S = \mathrm{Quot}(R)$ ist.

5.24 Lemma. *Sei S/R eine Ringerweiterung und $x \in S$. Dann sind äquivalent:*

(*i*) *x ist ganz über R.*

(*ii*) *$R[x]$ ist endlich über R.*

(*iii*) *Es gibt einen über R endlich erzeugten $R[x]$-Modul M mit $\mathrm{Ann}_{R[x]}(M) = \{0\}$.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Sei $f(x) = 0$ mit $f = \sum_{i=0}^{n} \lambda_i t^i$ und $\lambda_i \in R$, $\lambda_n = 1$. Dann gilt $0 = f(x) = x^n + \sum_{i=1}^{n-1} \lambda_i x^i$, also $x^n = \sum_{i=0}^{n-1} (-\lambda_i) x^i$. Daher bilden $1, x, \ldots, x^{n-1}$ ein endliches Erzeugendensystem von $R[x]$.

(*ii*) $\Rightarrow$ (*iii*): Sei $M = R[x]$. Nach Voraussetzung ist M endlich erzeugt über R und wegen $1 \in M$ folgt aus $zM = \{0\}$ für $z \in R[x]$ bereits $z \cdot 1 = z = 0$. Also gilt $\mathrm{Ann}_{R[x]}(M) = \{0\}$.

(*iii*) $\Rightarrow$ (*i*): Sei $\phi \in \mathrm{End}_{R[x]}(M)$ mit $\phi(m) = xm$. Nach Satz 4.25 angewendet auf M, $I = R$ und ϕ gibt es ein normiertes $f \in R[t]$ mit $f(\phi) = 0$, also $f(x)M = \{0\}$. Wegen $\mathrm{Ann}_{R[x]}(M) = \{0\}$ folgt $f(x) = 0$. $\square$

5.25 Satz. *Seien S/R und T/S Ringerweiterungen.*

(*i*) *Ist S endlich über R, so ist S ganz über R.*

(*ii*) *Wenn T endlich über S und S endlich über R ist, so ist T endlich über R. Ist T endlich über R, so ist T endlich über S.*

(*iii*) *Sind die $x_1, \ldots, x_n \in S$ ganz über R, so ist $R[x_1, \ldots, x_n]$ endlich über R.*

(*iv*) *T ist genau dann ganz über R, wenn T ganz über S und S ganz über R ist.*

(*v*) $\mathrm{Cl}(R,S)$ *ist ein Erweiterungsring von R.*

(*vi*) $\mathrm{Cl}(R,S)$ *ist ganz abgeschlossen in S.*

Beweis. (*i*): Folgt aus Lemma 5.24, (*iii*) mit $M = S$.

(*ii*): Sind die x_i ein Erzeugendensystem von T über S und die y_j ein Erzeugendensystem von S über R, so sind die $x_i y_j$ ein Erzeugendensystem von T über R, was die erste Aussage beweist.

Sind die x_i ein Erzeugendensystem von T über R, so sind die x_i auch ein Erzeugendensystem von T über S, was die zweite Aussage beweist.

(*iii*): Aus Lemma 5.24, (*ii*) und der zweiten Aussage in (*ii*) folgt, daß $R[x_1, \ldots, x_i]$ endlich über $R[x_1, \ldots, x_{i-1}]$ ist. Aus der ersten Aussage in (*ii*) mehrfach angewendet ergibt sich damit, daß $R[x_1, \ldots, x_n]$ endlich über R ist.

(*iv*): „$\Rightarrow$“ folgt direkt aus der Definition von „ganz“. Für „$\Leftarrow$“ sei $x \in T$ und $f = \sum_{i=0}^{n} \lambda_i t^i \in S[t]$ mit $\lambda_n = 1$ und $f(x) = 0$. Nach (*iii*) und (*ii*) ist $R[\lambda_1, \ldots, \lambda_n, x]$ endlich über R und wegen (*i*) dann auch ganz über R. Also ist speziell x ganz über R.

(*v*): Es gilt $R \subseteq \mathrm{Cl}(R,S)$, da R ganz über R ist. Für $x, y \in \mathrm{Cl}(R,S)$ ist $R[x,y]$ nach (*iii*) und (*i*) ganz über R. Wegen $x+y, xy \in R[x,y]$ sind dann auch $x+y$ und xy ganz über R, also gilt $x+y, xy \in \mathrm{Cl}(R,S)$.

(*vi*) $\mathrm{Cl}(R,S)$ ist nach (*iv*) ganz abgeschlossen in S. □

5.26 Satz. *Jeder faktorielle Ring R ist ganz abgeschlossen.*

Beweis. Seien $x/u \in \mathrm{Quot}(R)$ mit $x, u \in R$ teilerfremd und $\lambda_i \in R$ mit $(x/u)^n + \sum_{i=0}^{n-1} \lambda_i (x/u)^i = 0$. Multiplikation mit u^n liefert $x^n + \sum_{i=0}^{n-1} \lambda_i u^{n-i} x^i = 0$. Wegen $i \leq n-1$ ist x^n durch u teilbar, im Widerspruch zur Annahme. □

5.27 Satz. *Sei S/R eine Ringerweiterung und U eine multiplikativ abgeschlossene Teilmenge von R mit $1 \in U$.*

(*i*) *Ist S/R ganz, so ist auch $S[U^{-1}]/R[U^{-1}]$ ganz.*

(*ii*) *Es gilt* $\mathrm{Cl}(R,S)[U^{-1}] = \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$.

(*iii*) *R ist genau dann ganz abgeschlossen in S, wenn $R_{\mathfrak{m}}$ für jedes maximale Ideal $\mathfrak{m}$ von R ganz abgeschlossen in $S_{\mathfrak{m}} = S[(R \backslash \mathfrak{m})^{-1}]$ ist.*

Beweis. (*i*): Sei $x/u \in S[U^{-1}]$ mit $x \in S$ und $u \in U$. Dann ist x ganz über R, es gibt also $\lambda_i \in R$ mit $x^n + \sum_{i=0}^{n-1} \lambda_i x^i = 0$. Division durch u^n liefert $(x/u)^n + \sum_{i=0}^{n-1} (\lambda_i / u^{n-i})(x/u)^i = 0$ in $S[U^{-1}]$ mit $\lambda_i / u^{n-i} \in R[U^{-1}]$. Also ist x/u ganz über $R[U^{-1}]$.

(ii): $\mathrm{Cl}(R,S)$ ist ganz über R, also ist auch $\mathrm{Cl}(R,S)[U^{-1}]$ ganz über $R[U^{-1}]$ nach (i). Es folgt $\mathrm{Cl}(R,S)[U^{-1}] \subseteq \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$.

Sei $x/u \in \mathrm{Cl}(R[U^{-1}], S[U^{-1}])$ mit $x \in S$ und $u \in U$. Zum Nachweis von $x/u \in \mathrm{Cl}(R,S)[U^{-1}]$ müssen wir zeigen, daß es ein $v \in U$ mit xv ganz über R gibt. Sei $(x/u)^n + \sum_{i=0}^{n-1}(\lambda_i/u_i)(x/u)^i = 0$ mit $\lambda_i \in R$ und $u_i \in U$. Sei $v = \prod_{i=0}^{n-1} u_i$. Multiplikation mit $(uv)^n$ liefert $(xv)^n + \sum_{i=0}^{n-1}(\lambda_i u^{n-i}v^{n-i}/u_i)(xv)^i = 0$ in $S[U^{-1}]$, wobei $\lambda_i u^{n-i}v^{n-i}/u_i \in R$ wegen $i \leq n-1$ gilt. Also gibt es $w \in U$ mit $w((xv)^n + \sum_{i=0}^{n-1}(\lambda_i u^{n-i}v^{n-i}/u_i)(xv)^i) = 0$ in S. Durch Multiplikation der Gleichung in $S[U^{-1}]$ mit w^n erhalten wir $(xvw)^n + \sum_{i=0}^{n-1}(\lambda_i u^{n-i}v^{n-i}w^{n-i}/u_i)(xvw)^i = 0$ in S. Also ist xvw ganz über R und es folgt $x/u = (xvw)/(uvw) \in \mathrm{Cl}(R,S)[U^{-1}]$, das heißt $\mathrm{Cl}(R[U^{-1}], S[U^{-1}]) \subseteq \mathrm{Cl}(R,S)[U^{-1}]$.

(iii): Wir betrachten den Inklusionshomomorphismus $\phi : R \to \mathrm{Cl}(R,S)$ und die Lokalisierungen $\phi_{\mathfrak{m}} : R_{\mathfrak{m}} \to \mathrm{Cl}(R,S)_{\mathfrak{m}}$. Wegen $\mathrm{Cl}(R,S)_{\mathfrak{m}} = \mathrm{Cl}(R_{\mathfrak{m}}, S_{\mathfrak{m}})$ nach (ii) sind die $\phi_{\mathfrak{m}}$ genau dann Isomorphismen, wenn $R_{\mathfrak{m}}$ für alle $\mathfrak{m}$ ganz abgeschlossen in $S_{\mathfrak{m}}$ ist. Ebenso ist ϕ genau dann ein Isomorphismus, wenn R ganz abgeschlossen in S ist. Die Äquivalenz dieser Aussagen folgt nun aus Satz 4.13. □

Die Aussage (iii) gilt dann natürlich auch wieder für alle Primideale $\mathfrak{p}$ von R anstelle der maximalen Ideale $\mathfrak{m}$ von R.

5.5 Globale Charakterisierung von Dedekindringen

Sei M ein R-Modul. Ist $\mathfrak{p}$ ein Primideal von R mit $\mathfrak{p} = \mathrm{Ann}_R(m)$ für ein $m \in M$, so heißt $\mathfrak{p}$ ein assoziiertes Primideal von M. Wegen $\mathfrak{p} \neq R$ folgt hier $m \neq 0$. Es gilt $\mathfrak{p} \supseteq \mathrm{Ann}_R(M)$.

5.28 Satz. *Sei M ein R-Modul.*

(i) *Sei J ein maximales Ideal in der Menge $\mathcal{I} = \{\mathrm{Ann}_R(m) \,|\, m \in M\backslash\{0\}\}$. Dann ist J ein Primideal.*

(ii) *Jeder R-Modul $M \neq 0$ mit R noethersch besitzt ein assoziiertes Primideal.*

Beweis. (i): Sei $m \in M\backslash\{0\}$ mit $J = \mathrm{Ann}_R(m)$. Zunächst gilt $J \neq R$, da $m \neq 0$. Seien $x, y \in R$ mit $xy \in J$ und $x \notin J$. Dann ist $xm \neq 0$ und $(Ry + J)(xm) = \{0\}$. Wegen der Maximalität von J folgt $J = Ry + J$, also $y \in J$. Daher ist J ein Primideal.

(ii): Wegen $M \neq 0$ gilt $\mathcal{I} \neq \emptyset$. Da R noethersch ist, gibt es in $\mathcal{I}$ ein maximales Ideal J, welches nach (i) ein Primideal ist. □

5.29 Lemma. *Sei R ein lokaler noetherscher Integritätsring R der Dimension* 1. *Dann sind äquivalent:*

(*i*) *R ist ganz abgeschlossen.*

(*ii*) *$(I : I) = R$ für jedes Ideal $I \neq 0$ von R.*

(*iii*) *R ist ein diskreter Bewertungsring.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Wegen $RI = I$ gilt $(I : I) \supseteq R$. Damit ist $(I : I)$ ist ein Erweiterungsring von R und I sowohl ein R- als auch ein $(I : I)$-Modul. Da R noethersch ist, ist I in beiden Fällen endlich erzeugt. Da $(I : I)$ ein Integritätsring und $I \neq 0$ ist, folgt $\mathrm{Ann}_{(I:I)}(I) = \{0\}$. Nach Satz 5.24, (*iii*) sind daher die Elemente aus $(I : I)$ ganz über R. Da R ganz abgeschlossen ist, folgt $(I : I) \subseteq R$, also $(I : I) = R$.

(*ii*) $\Rightarrow$ (*iii*): Sei $\mathfrak{p}$ das maximale Ideal von R. Es gilt $R \subseteq \mathfrak{p}^{-1}$ und daher ist $\mathfrak{p}^{-1}\mathfrak{p}$ ein Ideal von R mit $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Da $\mathfrak{p}$ maximal ist, gilt $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ oder $\mathfrak{p}^{-1}\mathfrak{p} = R$.

Wir nehmen $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ an. Da R Dimension 1 hat, ist $\mathfrak{p} \neq 0$. Nach (*ii*) gilt dann $\mathfrak{p}^{-1} \subseteq R$, mit oben also $\mathfrak{p}^{-1} = R$. Nach Satz 5.28 gibt es zu $x \in \mathfrak{p}\backslash\{0\}$ ein assoziiertes Primideal $\mathfrak{q} \subseteq R$ von R/Rx. Wegen $\mathfrak{q} \supseteq \mathrm{Ann}_R(R/Rx) = Rx \neq 0$ und da R Dimension 1 hat, folgt $\mathfrak{p} = \mathfrak{q}$. Nach der Definition von assoziiertem Primideal gibt es also $y \in R\backslash Rx$ mit $\mathfrak{p}y \subseteq Rx$. Es gilt also $(y/x)\mathfrak{p} \subseteq R$ und $y/x \notin R$. Daraus folgt $\mathfrak{p}^{-1} \not\subseteq R$. Also ist $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ nicht möglich, es gilt $\mathfrak{p}^{-1}\mathfrak{p} = R$. Damit ist $\mathfrak{p}$ invertierbar, und nach Satz 5.22, (*i*) ist R ein diskreter Bewertungsring.

(*iii*) $\Rightarrow$ (*i*): Jeder diskrete Bewertungsring ist auch ein faktorieller Ring. Nach Satz 5.26 ist R ganz abgeschlossen. □

5.30 Satz. *Sei R ein noetherscher Integritätsring R der Dimension* 1. *Dann sind äquivalent:*

(*i*) *R ist ganz abgeschlossen.*

(*ii*) *$(I : I) = R$ für jedes Ideal $I \neq 0$ von R.*

(*iii*) *R ist ein Dedekindring.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Nach Satz 5.27, (*iii*) ist $R_\mathfrak{p}$ ganz abgeschlossen für jedes Primideal $\mathfrak{p}$ von R. Nach Lemma 5.29 gilt damit $(I_\mathfrak{p} : I_\mathfrak{p}) = R_\mathfrak{p}$ für alle $\mathfrak{p}$. Nach Satz 4.13 und Lemma 5.11 folgt $(I : I) = R$.

(*ii*) $\Rightarrow$ (*iii*): Für jedes Primideal $\mathfrak{p}$ von R und jedes Ideal J von $R_\mathfrak{p}$ ist $I = J \cap R$ ein Ideal von R mit $I_\mathfrak{p} = J$. Wegen $(I : I) = R$ gilt $(J : J) = (I_\mathfrak{p} : I_\mathfrak{p}) = R_\mathfrak{p}$

nach Lemma 5.11. Nach Lemma 5.29 ist $R_\mathfrak{p}$ ein diskreter Bewertungsring für alle $\mathfrak{p}$. Nach Satz 5.18 ist R dann ein Dedekindring.

$(iii) \Rightarrow (i)$: Nach Satz 5.18 ist $R_\mathfrak{p}$ ein diskreter Bewertungsring für alle Primideale $\mathfrak{p}$ von R. Nach Lemma 5.29 ist $R_\mathfrak{p}$ ganz abgeschlossen für alle $\mathfrak{p}$. Nach Satz 5.27, (iii) ist damit R ganz abgeschlossen. □

Der Satz 5.30 enthält Lemma 5.29 als Spezialfall, wenn man R lokalisiert. Die Äquivalenz von (i) und (ii) gilt auch ohne die Voraussetzung $\dim(R) = 1$, und (iii) wird durch die Aussage ersetzt, daß für jedes zu R/Rx mit $x \neq 0$ assoziierte Primideal $\mathfrak{p}$ der lokale Ring $R_\mathfrak{p}$ ein diskreter Bewertungsring ist. Dazu beweist man eine Version von Satz 4.13 unter der Voraussetzung R noethersch, in der nur für solche assoziierte Primideale lokalisiert werden muß. Dann tauchen im Beweis von Satz 5.30 nur noch zu R/Rx mit $x \neq 0$ assoziierte Primideale $\mathfrak{p}$ auf. Speziell wird Lemma 5.29 im Beweis von Satz 5.30 nur für $R_\mathfrak{p}$ mit zu $R_\mathfrak{p}/xR_\mathfrak{p}$ assoziierten Primidealen $\mathfrak{p}R_\mathfrak{p}$ angewendet. Der Beweis von Lemma 5.29 basiert dann direkt auf dieser Eigenschaft und benötigt die Voraussetzung $\dim(R) = 1$ nicht mehr.

Für einen ganz abgeschlossenen, noetherschen Integritätsring R und ein Primideal $\mathfrak{p}$ von R mit $\dim(R_\mathfrak{p}) = 1$ ist $R_\mathfrak{p}$ nach Satz 5.27, (iii) ganz abgeschlossen und daher nach Lemma 5.29 ein diskreter Bewertungsring. Ist dann noch $R_\mathfrak{m}$ faktoriell für alle maximalen Ideale $\mathfrak{m} \supseteq \mathfrak{p}$, so ist $\mathfrak{p}$ nach Satz 5.22 invertierbar. Damit R nicht singulär im Sinn der Bemerkung nach Satz 5.23 ist ($R_\mathfrak{m}$ faktoriell für jedes maximale Ideal $\mathfrak{m}$ von R), muß R also notwendigerweise ganz abgeschlossen sein. Für $\dim(R) = 1$ ist dies nach Satz 5.30 auch hinreichend, weil jedes Primideal $\mathfrak{p}$ mit $\dim(R_\mathfrak{p}) = 1$ maximal ist. Für $\dim(R) \geq 2$ gibt es Beispiele, in denen R ganz abgeschlossen ist und es dennoch singuläre maximale Ideale $\mathfrak{m}$ von R gibt (also $R_\mathfrak{m}$ nicht faktoriell).

Die Aussage (ii) von Satz 5.30 kann für die Berechnung von $\mathrm{Cl}(R, \mathrm{Quot}(R))$ genutzt werden. Für invertierbare Ideale I gilt stets $(I : I) = I^{-1}I = R$. Durch das Aufspüren geeigneter, nicht invertierbarer Ideale I und die Bestimmung der Erweiterungsringe $(I : I)$ von R können wir R sukzessive zu $\mathrm{Cl}(R, \mathrm{Quot}(R))$ erweitern. Ist zum Beispiel $\mathfrak{p}$ ein Primideal $\neq 0$ mit $R_\mathfrak{p}$ nicht ganz abgeschlossen, so gilt $\mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p} \cap R = \mathfrak{p}$ und $\mathfrak{p}^{-1} \not\subseteq R$ nach dem Beweis von Lemma 5.29. Daraus folgt, daß $(\mathfrak{p} : \mathfrak{p})$ ein über R ganzer Erweiterungsring von R mit $(\mathfrak{p} : \mathfrak{p}) \neq R$ ist.

Im folgenden Satz wird das leere Produkt für $I = R$ mit eingerechnet.

5.31 Satz. *Sei R ein Integritätsring mit der Eigenschaft, daß jedes Ideal ein Produkt von Primidealen ist. Dann ist R ein Dedekindring.*

Beweis. Ist zwar nicht so schwer und lang, lassen wir aber aus. □

Die klassische Zusammenfassung der äquivalenten Eigenschaften eines Dedekindrings liefert nun der folgende Satz.

5.32 Satz. *Für einen Integritätsring R sind äquivalent:*

(*i*) *R ist ein Dedekindring.*

(*ii*) *Jedes Ideal $\neq 0$ läßt sich bis auf die Reihenfolge auf genau eine Weise als Produkt von Primidealen von R schreiben.*

(*iii*) *R ist noethersch und $R_{\mathfrak{p}}$ ist ein diskreter Bewertungsring für jedes maximale Ideal $\mathfrak{m} \neq 0$ von R.*

(*iv*) *R ist ganz abgeschlossen und noethersch, und jedes Primideal $\neq 0$ von R ist maximal.*

Beweis. (*i*) $\Rightarrow$ (*ii*): Satz 5.8.
(*ii*) $\Rightarrow$ (*i*): Satz 5.31.
(*i*) $\Leftrightarrow$ (*iii*): Satz 5.18.
(*i*) $\Leftrightarrow$ (*iv*): Satz 5.30. □

Hier ist eine weitere Eigenschaft von Dedekindringen (vgl. das Diagramm auf Seite **??**).

5.33 Satz. *Ein noetherscher Integritätsbereich R ist genau dann ein Hauptidealring, wenn R ein Dedekindring und faktoriell ist.*

Beweis. „$\Rightarrow$“: Da Hauptideale $\neq 0$ invertierbar sind, ist diese Aussage klar.

„$\Leftarrow$“: Sei $\mathfrak{p} \neq 0$ ein Primideal von R und $x \in \mathfrak{p}\backslash\{0\}$. Sei $Rx = \prod_i \mathfrak{p}_i$ die Faktorisierung in Primideale mit $\mathfrak{p}_1 = \mathfrak{p}$. Sei $x = \prod_j \pi_j$ eine Faktorisierung in Primelemente. Die Ideale $R\pi_j$ sind dann Primideale und es gilt $Rx = \prod_j R\pi_j$. Wegen der Eindeutigkeit der Faktorisierung folgt $\mathfrak{p} = R\pi_j$ für ein j. Also ist $\mathfrak{p}$ ein Hauptideal. Da $\mathfrak{p}$ beliebig war, sind alle Primideale und damit alle Ideale von R Hauptideale. □

5.6 Beispiele

Beispiele für freie Moduln sind die R-Moduln R^n.

Ein Beispiel für einen projektiven, aber nicht freien Modul ist $R = \mathbb{Z}[\sqrt{-5}]$ und das Ideal $M = 2R + (1 + \sqrt{-5})R$. Der Beweis dieser Tatsache fällt in die algebraische Zahlentheorie (R ist ganzalgebraisch abgeschlossen, also ein Dedekindring, und M ist kein Hauptideal. Die Klassenzahl von R ist 2).

Hier sind weitere Details zu diesem Beispiel. Sei $\rho = \sqrt{-5}$. Dann gilt $6 = 2 \cdot 3 = (1+\rho)(1-\rho)$. Man kann zeigen, daß 2, 3, $1+\rho$ und $1-\rho$ irreduzible Elemente in R sind. Also ist R ein Ring, in dem es keine eindeutige Faktorisierung in Primelemente mehr gibt. Zur Abhilfe wurden von Kummer in der zweiten Hälfte des 19. Jahrhunderts „ideale Zahlen“ eingeführt, mit denen dann eine eindeutige Faktorisierung möglich sein sollte (vergleichbar mit dem Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$, so daß jede Zahl in $\mathbb{Z}$ invertierbar wird). Bei diesen handelt es sich schlicht um (invertierbare) Ideale von R. Das geht dann wie folgt: Sei $\mathfrak{p} = 2R + (1+\rho)R$, $\mathfrak{q}_1 = 3R + (1+\rho)R$ und $\mathfrak{q}_2 = 3R + (1-\rho)R$. Dann sind $\mathfrak{p}$, $\mathfrak{q}_1$ und $\mathfrak{q}_1$ Primideale. (Ein Beweis dieser Tatsache kann im Prinzip wie folgt gehen: Sei p eine Primzahl und $f = t^2 + 5 \in \mathbb{Z}[t]$ Dann gilt $R \cong \mathbb{Z}[t]/(f)$. Wir betrachten die natürlichen Homomorphismen $\phi : R \mapsto R \otimes_{\mathbb{Z}} \mathbb{F}_p$ und $\psi : R \otimes_{\mathbb{Z}} \mathbb{F}_p \to \mathbb{F}_p[t]/(g)$, wobei $g \in \mathbb{F}_p[t]$ die Reduktion von $f \in \mathbb{Z}[t]$ ist. Nach einer Übungsaufgabe wissen wir, daß ψ ein Isomorphismus ist. Der Homomorphismus ϕ ist surjektiv und hat den Kern pR. Die Verknüpfung $\psi \circ \phi$ ist gerade der kanonische Epimorphismus. Damit entsprechen sich die Primideale $\mathfrak{p}$ von R mit $p \in \mathfrak{p}$ und die Primideale von $R \otimes_{\mathbb{Z}} \mathbb{F}_p$ eineindeutig. Mit Hilfe des chinesischen Restsatzes können wir die Primideale von $\mathbb{F}_p[t]/(g)$ bestimmen, dann ihre Urbilder unter ψ und ihre Urbilder unter ϕ. Die Primideale von $\mathbb{F}_p[t]/(g)$ werden von den irreduziblen Faktoren von g erzeugt.) Weiter gilt

$$\begin{aligned} \mathfrak{p}^2 = 2R, \quad \mathfrak{q}_1\mathfrak{q}_2 = 3R \\ \mathfrak{p}\mathfrak{q}_1 = (1+\rho)R, \quad \mathfrak{p}\mathfrak{q}_2 = (1-\rho)R. \end{aligned}$$

Daraus folgt für die Faktorisierung von 6:

$$\begin{aligned} 6R &= 2R \cdot 3R = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2 \\ 6R &= (1+\rho)R \cdot (1-\rho)R = \mathfrak{p}\mathfrak{q}_1\mathfrak{p}\mathfrak{q}_2 = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2. \end{aligned}$$

Man sieht hier schön, wie durch die Hinzunahme der Primideale die Elementsituation ergänzt wird. Speziell sind $\mathfrak{p}$, $\mathfrak{q}_1$ und $\mathfrak{q}_2$ keine Hauptideale, denn sonst gäbe es ja Primelemente, welche 2, 3, $1+\rho$ und $1-\rho$ teilen würden und 2, 3, $1+\rho$ und $1-\rho$ könnten nicht irreduzibel sein.

Wegen $\mathfrak{p}^2 = 2R$ und $\mathfrak{q}_1\mathfrak{q}_2 = 3R$ sind diese Ideale invertierbare Ideale, da $2R$ und $3R$ invertierbar sind. Damit sind sie auch projektiv. Sie sind aber nicht frei, denn sonst müßten sie ja Hauptideale sein.

Typische Beispiele für flache, aber nicht projektive R-Moduln kann man aus den Moduln $M[U^{-1}]$, aufgefaßt als R-Moduln, erhalten. Sei $R = M = \mathbb{Z}$, $U = \langle 3 \rangle$ und $M[U^{-1}] = \mathbb{Z}[1/3]$. Der $\mathbb{Z}$-Modul $\mathbb{Z}[1/3]$ ist einerseits nicht endlich erzeugt, denn sonst wären die auftretenden Nenner in $\mathbb{Z}[1/3]$ beschränkt, andererseits sind

aber je zwei Elemente aus $\mathbb{Z}[1/3]$ über $\mathbb{Z}$ linear abhängig. Insbesondere kann es keine Einbettung von $\mathbb{Z}[1/3]$ in einen freien $\mathbb{Z}$-Model geben, da in einem freien $\mathbb{Z}$-Modul Elemente nicht beliebig durch Potenzen von 3 teilbar sind, was aber in $\mathbb{Z}[1/3]$ der Fall ist. Nach Satz 4.22, (ii) ist $\mathbb{Z}[1/3]$ daher nicht projektiv. Ein weiteres Beispiel für diesen Effekt ist $\mathbb{Q}$ als $\mathbb{Z}$-Modul.

Torsionsfreie, aber nicht flache Moduln sind zum Beispiel das maximale Ideal M von $R = k[[x_1, x_2]]$ als R-Modul, oder $M = \mathbb{Z}[(1+\sqrt{5})/2]$ als $R = \mathbb{Z}[\sqrt{5}]$-Modul.