**Prof. Dr. H. Brenner** **Osnabrück WS 2018/2019**

# Körper- und Galoistheorie

## Vorlesung 28

In dieser Vorlesung standen endliche Körpererweiterungen der rationalen Zahlen $\mathbb{Q}$ im Mittelpunkt. Zum Abschluss werden wir Körper betrachten, die von den rationalen Zahlen aus nicht algebraisch erfasst werden können, sondern transzendente Elemente enthalten. Diese Eigenschaft haben zwar auch die reellen Zahlen, aber diese lassen sich von den rationalen Zahlen aus als Grenzwerte erfassen (was allerdings kein algebraisches Konzept ist). Hier geht es um transzendente Elemente, die eher den Charakter von Funktionen oder einfach von Variablen haben. Es bestehen enge Beziehungen zur Invariantentheorie, Dimensionstheorie für kommutative Ringe, Funktionenkörper von algebraischen Varietäten.

## Algebraische Unabhängigkeit

Wir haben schon öfters den Körper der rationalen Funktionen $K(X)$, also den Quotientenkörper des Polynomringes in einer Variablen über einem Körper erwähnt. Dort gibt es das Phänomen, dass dieser Körper echte Unterkörper enthält, die zu diesem Körper selbst isomorph sind, und zwar als $K$-Algebra. Beispielsweise ist der von $X^2$ erzeugte Unterkörper $K(X^2) \subseteq K(X)$ selbst isomorph zu $K(Y)$ (und damit zu $K(X)$). Der Grad der angegebenen Erweiterung ist 2. In der Tat ist sogar für jedes Polynom $P \in K[X]$, $P \notin K$, der davon erzeugte Unterkörper isomorph zum Körper der rationalen Funktionen in einer Variablen. Wir fragen uns, wie zu Polynomen $P, Q \in K[X]$, $P, Q \notin K$, der erzeugte Unterkörper $K(P, Q) \subseteq K(X)$ aussieht. Es wird sich herausstellen, dass hierbei stets eine algebraische Abhängigkeit zwischen diesen Polynomen besteht. Es gibt also zwar viele verschiedene, aber isomorphe, Unterkörper von $K(X)$, aber kein Unterkörper, der zum Quotientenkörper von $K[X, Y]$ isomorph wäre. Für solche Quotientenkörper führen wir eine eigene Bezeichnung ein.

Definition 28.1. Es sei $K$ ein Körper. Den Quotientenkörper des Polynomringes $K[X_1, \ldots, X_n]$ nennt man *Körper der rationalen Funktionen in $n$ Variablen*. Er wird mit $K(X_1, \ldots, X_n)$ bezeichnet.

Die Elemente dieses Körpers sind rationale Funktionen in mehreren Variablen, also Quotienten aus Polynomen in mehreren Variablen (wie schon bei Polynomen muss man aber bei einem endlichen Grundkörper vorsichtig sein bei der Identifizierung zwischen Elementen dieses Körpers und Funktionen auf gewissen Punktmengen).

Definition 28.2. Es sei $R$ ein kommutativer Ring und $A$ eine kommutative $R$-Algebra. Die Elemente $f_1, \ldots, f_n \in A$ heißen *algebraisch unabhängig* (über $R$), wenn für jedes vom Nullpolynom verschiedene Polynom $P \in R[X_1, \ldots, X_n]$ bei der Einsetzung

$$P(f_1, \ldots, f_n) \neq 0$$

gilt.

Ein einzelnes algebraisch unabhängiges Element ist einfach ein transzendentes Element. Von daher ist die Vorstellung, dass es sich bei einer algebraisch unabhängigen Familie um eine „transzendente Familie“ handelt, sinnvoll. Das Urbeispiel einer algebraisch unabhängigen Familie ist die Variablenfamilie in einem Polynomring $K[X_1, \ldots, X_n]$ bzw. im Körper der rationalen Funktionen $K(X_1, \ldots, X_n)$.

Lemma 28.3. *Es sei $A$ eine kommutative $R$-Algebra über einem kommutativen Ring $R$ und seien $f_1, \ldots, f_n \in A$ eine Elementfamilie. Dann sind folgende Aussagen äquivalent.*

(1) *Die Elemente $f_1, \ldots, f_n$ sind algebraisch unabhängig.*
(2) *Der Einsetzungshomomorphismus*

$$R[X_1, \ldots, X_n] \longrightarrow A,\ X_i \longmapsto f_i,$$

*ist injektiv.*
(3) *Der Einsetzungshomomorphismus*

$$R[X_1, \ldots, X_n] \longrightarrow R[f_1, \ldots, f_n],\ X_i \longmapsto f_i,$$

*ist bijektiv.*

*Beweis.* Siehe Aufgabe 28.6. □

Eine algebraisch unabhängige Familie ist also dadurch gekennzeichnet, das der Einsetzungshomomorphismus eine $R$-Algebraisomorphie

$$R[X_1, \ldots, X_n] \longrightarrow R[f_1, \ldots, f_n] \subseteq A$$

definiert. Wenn $R = K$ ein Körper ist, was wir zumeist annehmen werden, so führt dies auch zu einem Körperisomorphismus

$$K(X_1, \ldots, X_n) \longrightarrow K[X_1, \ldots, X_n].$$

## Transzendenzbasen

Definition 28.4. Es sei $K$ ein Grundkörper und $K \subseteq L$ eine Körpererweiterung. Man sagt, dass $f_1, \ldots, f_n \in L$ eine *Transzendenzbasis* von $L$ über $K$ ist, wenn die $f_1, \ldots, f_n$ algebraisch unabhängig sind und $K(f_1, \ldots, f_n) \subseteq L$ eine algebraische Körpererweiterung ist.

Beispiel 28.5. Zum Polynomring $K[X_1, \ldots, X_n]$ über einem Körper $K$ in $n$ Variablen besitzt der Quotientenkörper

$$K(X_1, \ldots, X_n) = Q(K[X_1, \ldots, X_n]),$$

also der rationale Funktionenkörper in $n$ Variablen, die Transzendenzbasis $X_1, \ldots, X_n$, da die Variablen algebraisch unabhängig sind.

Beispiel 28.6. Es sei $K$ ein Körper und $F \in K(X_1, \ldots, X_n)[T]$ ein irreduzibles Polynom, die Koeffizienten des Polynoms sind also rationale Funktionen in den $n$ Variablen $X_1, \ldots, X_n$. Nach Korollar 7.7 ist der Restklassenring

$$L := K(X_1, \ldots, X_n)[T]/(F)$$

ein Körper, und zwar eine endliche Körpererweiterung von $K(X_1, \ldots, X_n)$, deren Grad durch den Grad des Polynoms gegeben ist. Insbesondere bilden die Variablen $X_1, \ldots, X_n$ eine Transzendenzbasis von $L$.

Wenn eine algebraische Körpererweiterung

$$K(X_1, \ldots, X_n) \subset L$$

vorliegt, so kann es natürlich trotzdem sein, dass $L$ die Form

$$L = K(Y_1, \ldots, Y_n)$$

besitzt, also isomorph zum Körper der rationalen Funktionen ist. Das einfachste Beispiel ergibt sich für $X = Y^2$.

Definition 28.7. Eine Körpererweiterung $K \subseteq L$ heißt *rein transzendent*, wenn es algebraisch unabhängige Elemente $f_1, \ldots, f_n \in L$ mit $L = K(f_1, \ldots, f_n)$ gibt.

Rein transzendent bedeutet also einfach, dass es eine $K$-Isomorphie zum Körper der rationalen Funktionen gibt. Es ist im Allgemeinen schwierig zu entscheiden, ob ein gegebener Körper rein transzendent ist. Der Quotientenkörper von $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ ist rein transzendent (über $\mathbb{C}$), der Quotientenkörper von $\mathbb{C}[X, Y]/(X^3 + Y^3 - 1)$ ist hingegen nicht rein transzendent.

Wir wollen zeigen, dass die Anzahl der Elemente in einer Transzendenzbasis wohlbestimmt ist. Die Argumentation orientiert sich am Beweis des Satzes der linearen Algebra, dass die Anzahl der Elemente in einer Vektorraumbasis, also die Dimension des Vektorraumes, wohlbestimmt ist.

Lemma 28.8. *Es sei $K$ ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit endlichen Transzendenzbasen $f_1, \ldots, f_m$ und $g_1, \ldots, g_n$. Dann gibt es zu jedem Element $f_i$ der ersten Transzendenzbasis ein Element $g_j$ der zweiten Transzendenzbasis derart, dass $f_1, \ldots, f_{i-1}, g_j, f_{i+1}, \ldots, f_m$ ebenfalls eine Transzendenzbasis ist.*

*Beweis.* Wir zeigen, dass man $f_m$ durch eines der $g_j$ ersetzen kann. Da die Körpererweiterung $K(f_1, \ldots, f_m) \subseteq L$ algebraisch ist, gibt es zu jedem $g_j$ ein irreduzibles Polynom $P_j \in K(f_1, \ldots, f_m)[T]$ mit $P_j(g_j) = 0$. Wir multiplizieren mit dem Hauptnenner sämtlicher Koeffizienten der $P_j$ und können dann annehmen, dass $P_j \in K[f_1, \ldots, f_m][T]$ gilt. Nehmen wir an, dass sämtliche $P_j$ sogar zu $K[f_1, \ldots, f_{m-1}][T]$ gehören. Dann wäre die Körperkette

$$K(f_1, \ldots, f_{m-1}) \subseteq K(g_1, \ldots, g_n) \subseteq L$$

eine nach Aufgabe 10.4 algebraische Erweiterung und insbesondere wäre $f_m$ algebraisch über $K(f_1, \ldots, f_{m-1})$ im Widerspruch zur Voraussetzung, dass die $f_i$ algebraisch unabhängig sind. Es gibt also ein $P_j$ mit $P_j \notin K[f_1, \ldots, f_{m-1}][T]$. Wir schreiben

$$P_j = \sum_{k=0}^{r} \alpha_k T^k$$

mit

$$\alpha_k = \sum_{\ell=0}^{s} \beta_{k,\ell} f_m^\ell$$

und $\beta_{k,\ell} \in K[f_1, \ldots, f_{m-1}]$. Dabei ist zumindest ein $\beta_{k,\ell} \neq 0$ für ein $\ell \geq 1$. Daher können wir die Gleichung $P_j(g_j) = 0$ als eine algebraische Gleichung für $f_m$ über $K[f_1, \ldots, f_{m-1}, g_j]$ lesen. Dies bedeutet, dass $f_m$ algebraisch über $K(f_1, \ldots, f_{m-1}, g_j)$ ist.

Wir behaupten, dass $f_1, \ldots, f_{m-1}, g_j$ eine Transzendenzbasis von $L$ über $K$ ist, wobei wir gerade gezeigt haben, dass $L$ darüber algebraisch ist. Es ist zu zeigen, dass diese Elemente algebraisch unabhängig sind. Wären sie algebraisch abhängig, so müsste $g_j$ algebraisch über $K(f_1, \ldots, f_{m-1})$ sein. Doch dann wäre, wieder wegen der Transitivität von algebraisch, auch $f_m$ algebraisch über $K(f_1, \ldots, f_{m-1})$ im Widerspruch zur Voraussetzung. □

Satz 28.9. *Es sei $K$ ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit einer endlichen Transzendenzbasis. Dann besitzt jede Transzendenzbasis von $L$ über $K$ gleich viele Elemente.*

*Beweis.* Es sei $m$ die minimale Zahl derart, dass es eine Transzendenzbasis mit $m$ Elementen gibt. Es sei $f_1, \ldots, f_m$ eine Transzendenzbasis und $g_1, \ldots, g_n$ eine weitere Transzendenzbasis mit

$$n \geq m$$

Elementen. Wir wenden Lemma 28.8 sukzessive an und erhalten Transzendenzbasen

$$g_{j_1}, f_2, \ldots, f_m\,,$$

$$g_{j_1}, g_{j_2}, f_3, \ldots, f_m\,,$$

...

$$g_{j_1}, g_{j_2}, g_{j_3}, \ldots, g_{j_{m-1}}, f_m ,$$

$$g_{j_1}, g_{j_2}, g_{j_3}, \ldots, g_{j_{m-1}}, g_{j_m} ,$$

wobei die $g_{j_i}$ Elemente der zweiten Familie sind. Die letzte Familie ist eine Transzendenzbasis mit $m$ Elementen (es kann keine Elementwiederholungen geben wegen der vorausgesetzen Minimalität von $m$). Bei $n > m$ würde sich ein Widerspruch ergeben, da eine echte Teilfamilie einer Transzendenzbasis keine Transzendenzbasis sein kann, also ist $n = m$. □

## Der Transzendenzgrad

DEFINITION 28.10. Es sei $K$ ein Grundkörper und $K \subseteq L$ eine Körpererweiterung mit einer endlichen Transzendenzbasis. Dann nennt man die Anzahl der Elemente in einer jeden Transzendenzbasis von $L$ über $K$ den *Transzendenzgrad* von $L$ über $K$. Dafür schreibt man $\operatorname{trdeg}(L/K)$.

Nach Satz 28.9 ist dieser Transzendenzgrad wohldefiniert.

KOROLLAR 28.11. *Es sei $K$ ein Körper. und $K(X_1, \ldots, X_n) \subseteq L$ eine algebraische Körpererweiterung des Körpers der rationalen Funktionen in $n$ Variablen. Dann ist der Transzendenzgrad von $L$ über $K$ gleich $n$. Insbesondere besitzt der Körper der rationalen Funktionen $K(X_1, \ldots, X_n)$ den Transzendenzgrad $n$.*

*Beweis.* Dies folgt direkt daraus, dass die Variablen $X_1, \ldots, X_n$ eine Transzendenzbasis von $K(X_1, \ldots, X_n)$ und von $L$ bilden und dass man nach Satz 28.9 den Transzendenzgrad mit jeder Basis bestimmen kann. □

KOROLLAR 28.12. *Es sei $K \subseteq L$ eine Körpererweiterung und seien $f_1, \ldots, f_n \in L$ Elemente. Dann sind folgende Aussagen äquivalent.*

(1) *Die Elemente $f_1, \ldots, f_n$ sind algebraisch unabhängig.*
(2) *Der Einsetzungshomomorphismus induziert eine $K$-Algebraisomorphie*

$$K(X_1, \ldots, X_n) \longrightarrow K(f_1, \ldots, f_n),\ X_i \longmapsto f_i,$$

(3) *Es gibt eine $K$-Algebraisomorphie*

$$K(X_1, \ldots, X_n) \longrightarrow K(f_1, \ldots, f_n).$$

*Beweis.* Die Äquivalenz von (1) und (2) folgt direkt aus Lemma 28.3. Von (2) nach (3) ist klar, sei also (3) erfüllt. Da eine Isomorphie vorliegt, und der Transzendenzgrad eine (wohldefinierte) invariante einer Körpererweiterung ist, besitzt der Körper $K(f_1, \ldots, f_n)$ den Transzendenzgrad $n$. Von diesem Körper ist $f_1, \ldots, f_n$ eine Transzendenzbasis und insbesondere algebraisch unabhängig. □

KOROLLAR 28.13. *Es sei $K \subseteq L \subseteq M$ eine Kette von Körpererweiterungen. Dann ist*

$$\operatorname{trdeg}(M/K) = \operatorname{trdeg}(L/K) + \operatorname{trdeg}(M/L).$$

*Beweis.* Es sei $x_1, \ldots, x_n \in L$ eine Transzendenzbasis von $L$ über $K$ und $y_1, \ldots, y_m \in M$ eine Transzendenzbasis von $M$ über $L$. Nach Aufgabe 28.13 ist $x_1, \ldots, x_n, y_1, \ldots, y_m$ algebraisch unabhängig über $K$. Nach Voraussetzung ist $K(x_1, \ldots, x_n) \subseteq L$ algebraisch. Daher ist auch

$$K(x_1, \ldots, x_n, y_1, \ldots, y_m) \subseteq L(y_1, \ldots, y_m)$$

algebraisch. Da auch $L(y_1, \ldots, y_m) \subseteq M$ algebraisch ist, folgt mit Aufgabe 10.4, dass $K(x_1, \ldots, x_n, y_1, \ldots, y_m) \subseteq M$ algebraisch ist. □

KOROLLAR 28.14. *Es sei $K \subseteq L \subseteq M$ eine Kette von Körpererweiterungen. Dann ist*

$$\operatorname{trdeg}(L/K) \leq \operatorname{trdeg}(M/K).$$

*Beweis.* Dies folgt unmittelbar aus Korollar 28.13. □

# Abbildungsverzeichnis