**Prof. Dr. H. Brenner** **Osnabrück SS 2015**

# Elemente der Algebra

## Vorlesung 22

In den verbleibenden Vorlesungen werden wir uns mit Körpererweiterungen $K \subseteq L$ beschäftigen. Wir betrachten beispielsweise in $\mathbb{R}$ den von $\mathbb{Q}$ und $\sqrt{7}$ erzeugten Unterring

$$L = \mathbb{Q}[\sqrt{7}].$$

Er besteht aus allen reellen Zahlen der Form

$$a + b\sqrt{7}$$

mit $a, b \in \mathbb{Q}$. Dabei kann man direkt nachprüfen, dass die Summe und das Produkt von zwei solchen Ausdrücken wieder von dieser Form ist, und somit liegt ein Unterring vor. Es handelt sich aber sogar um einen Körper. Es ist nämlich

$$\left(a + b\sqrt{7}\right)\left(a - b\sqrt{7}\right) = a^2 - 7b^2$$

und somit ist für $a + b\sqrt{7} \neq 0$

$$\left(a + b\sqrt{7}\right)\left(\frac{a}{a^2 - 7b^2} - \frac{b\sqrt{7}}{a^2 - 7b^2}\right) = 1,$$

also ist jedes von 0 verschiedene Element eine Einheit. Da $\sqrt{7}$ irrational ist, ist $a^2 - 7b^2 \neq 0$. Es liegt also eine Körpererweiterung

$$\mathbb{Q} = \mathbb{Q}[\sqrt{7}]$$

vor. Den Körper $\mathbb{Q}[\sqrt{7}]$ kann man auch einfach als Restklassenkörper von $\mathbb{Q}[X]$ beschreiben. Der Einsetzungshomomorphismus

$$\mathbb{Q}[X] \longrightarrow \mathbb{R},\ X \longmapsto \sqrt{7},$$

liefert eine surjektiven Ringhomomorphismus auf das Bild, also

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt{7}],\ X \longmapsto \sqrt{7}.$$

Unter dieser Abbildung geht $X^2 - 7$ auf 0, und in der Tat ist der Kern gleich dem Hauptideal $(X^2 - 7)$. Nach dem Isomorphiesatz gilt daher

$$\mathbb{Q}[X]/(X^2 - 7) \cong \mathbb{Q}[\sqrt{7}].$$

## Rechnen in $K[X]/(P)$

Körper werden häufig ausgehend von einem schon bekannten Körper als Restklassenkörper des Polynomrings konstruiert. Die Arithmetik in einem solchen Erweiterungskörper wird in der folgenden Aussage beschrieben.

Proposition 22.1. *Sei $K$ ein Körper und sei $K[X]$ der Polynomring über $K$. Es sei $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein Polynom vom Grad $n$ und $R = K[X]/(P)$ der zugehörige Restklassenring. Dann gelten folgende Rechenregeln (wir bezeichnen die Restklasse von $X$ in $R$ mit $x$).*

(1) *Man kann stets $P$ als normiert annehmen (also $a_n = 1$; das werden wir im Folgenden tun).*
(2) *In $R$ ist*
$$x^n = -\sum_{i=0}^{n-1} a_i x^i \, .$$
(3) *Höhere Potenzen $x^k$, $k \geq n$, kann man mit den Potenzen $x^i$, $i \leq n-1$, ausdrücken, indem man mittels Vielfachen von (2) sukzessive den Grad um eins reduziert.*
(4) *Die Potenzen $x^0 = 1$, $x^1$ , $\ldots$ , $x^{n-1}$ bilden eine $K$-Basis von $R$.*
(5) *$R$ ist ein $K$-Vektorraum der Dimension $n$.*
(6) *In $R$ werden zwei Elemente $P = \sum_{i=0}^{n-1} b_i x^i$ und $Q = \sum_{i=0}^{n-1} c_i x^i$ komponentenweise addiert, und multipliziert, indem sie als Polynome multipliziert werden und dann die Restklasse berechnet wird.*

*Beweis.* (1) Es ist $(P) = \left(\frac{P}{a_n}\right)$, da es bei einem Hauptideal nicht auf eine Einheit ankommt.
(2) Dies folgt direkt durch Umstellung der definierenden Gleichung.
(3) Dies folgt durch Multiplikation der Gleichung in (2) mit Potenzen von $x$.
(4) Dass die Potenzen $x^i$, $i = 0, \ldots, n-1$, ein Erzeugendensystem bildet, folgt aus Teil (2) und (3). Zum Beweis der linearen Unabhängigkeit sei angenommen, es gebe eine lineare Abhängigkeit, sagen wir $\sum_{i=0}^{n-1} c_i x^i = 0$. D.h., dass das Polynom $Q = \sum_{i=0}^{n-1} c_i X^i$ unter der Restklassenabbildung auf 0 geht, also zum Kern gehört. Dann muss es aber ein Vielfaches von $P$ sein, was aber aus Gradgründen erzwingt, dass $Q$ das Nullpolynom sein muss. Also sind alle $c_i = 0$.
(5) Dies folgt direkt aus (4).
(6) Dies ist klar.

□

Beispiel 22.2. Wir betrachten den Restklassenring
$$L \, = \, \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$
und bezeichnen die Restklasse von $X$ mit $x$. Aufgrund von Proposition 22.1 besitzt jedes Element $f$ aus $L$ eine eindeutige Darstellung $f = ax^2 + bx + c$ mit $a, b, c \in \mathbb{Q}$, so dass also ein dreidimensionaler $\mathbb{Q}$-Vektorraum vorliegt. Da $X^3 + 2X^2 - 5$ in $L$ zu 0 gemacht wird, gilt
$$x^3 \, = \, -2x^2 + 5.$$

Daraus ergeben sich die Gleichungen

$$x^4 \;=\; -2x^3+5x \;=\; -2(-2x^2+5)+5x \;=\; 4x^2+5x-10,$$

$$x^5 \;=\; -2x^4+5x^2 \;=\; -2(4x^2+5x-10)+5x^2 \;=\; -3x^2-10x+20,$$

etc. Man kann hierbei auf verschiedene Arten zu dem eindeutig bestimmten kanonischen Repräsentanten reduzieren.

Berechnen wir nun das Produkt

$$(3x^2-2x+4)(2x^2+x-1)\,.$$

Dabei wird distributiv ausmultipliziert und anschließend werden die Potenzen reduziert. Es ist

$$\begin{array}{ll} & (3x^2-2x+4)(2x^2+x-1) \\ = & 6x^4+3x^3-3x^2-4x^3-2x^2+2x+8x^2+4x-4 \\ = & 6x^4-x^3+3x^2+6x-4 \\ = & 6(4x^2+5x-10)+2x^2-5+3x^2+6x-4{=}29x^2+36x-69. \end{array}$$

## Endliche Körpererweiterungen

Wenn $P$ in der vorstehenden Proposition irreduzibel ist, so ist $K[X]/(P)$ nach Satz 15.1 ein Körper und damit liegt eine Körpererweiterung

$$K \;\subseteq\; K[X]/P \;=\; L$$

vor. Bei einer $K$-Algebra (siehe unten) und insbesondere einer Körpererweiterung hat man durch den Vektorraumbegriff sofort die folgenden Begriffe zur Verfügung.

Definition 22.3. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn $L$ ein endlichdimensionaler Vektorraum über $K$ ist.

Definition 22.4. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die $K$-(Vektorraum-)Dimension von $L$ den *Grad* der Körpererweiterung.

Bei $L = K[X]/(P)$ mit einem irreduziblen Polynom $P$ ist nach Proposition 22.1 (5) der Grad der Körpererweiterung gleich dem Grad von $P$.

## Algebren

Definition 22.5. Seien $R$ und $A$ kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man $A$ eine *$R$-Algebra*.

Häufig ist der Ringhomomorphismus, der zum Begriff der Algebra gehört, vom Kontext her klar und wird nicht explizit aufgeführt. Z.B. ist der Polynomring $R[X]$ eine $R$-Algebra, indem man die Elemente aus $R$ als konstante Polynome auffasst, oder jeder Ring ist auf eine eindeutige Weise eine $\mathbb{Z}$-Algebra über den kanonischen Ringhomomorphismus $\mathbb{Z} \to R$, $n \mapsto n_R$.

Wir werden den Begriff der Algebra vor allem in dem Fall verwenden, wo der Grundring $R$ ein Körper $K$ ist. Eine $K$-Algebra $A$ kann man stets in natürlicher Weise als Vektorraum über dem Körper $K$ auffassen. Die Skalarmultiplikation wird dabei einfach über den Strukturhomomorphismus erklärt. Eine typische Situation ist dabei, dass $\mathbb{Q}$ der Grundkörper ist und ein Zwischenring $L$, $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$, gegeben ist. Dann ist $L$ über die Inklusion direkt eine $\mathbb{Q}$-Algebra.

Wenn man zwei Algebren über einem gemeinsamen Grundring hat, so sind vor allem diejenigen Ringhomomorphismen interessant, die den Grundring mitberücksichtigen. Dies führt zu folgendem Begriff.

Definition 22.6. Seien $R$ und $S$ zwei kommutative $K$-Algebren über einem kommutativen Grundring $K$. Dann nennt man einen Ringhomomorphismus

$$\varphi\colon\ R \longrightarrow S$$

einen *$K$-Algebra-Homomorphismus*, wenn er zusätzlich mit den beiden fixierten Ringhomomorphismen $K \to R$ und $K \to S$ verträglich ist.

Zum Beispiel ist jeder Ringhomomorphismus ein $\mathbb{Z}$-Algebra-Homomorphismus, da es zu jedem Ring $A$ überhaupt nur den kanonischen Ringhomomorphismus $\mathbb{Z} \to A$ gibt. Mit dieser Terminologie kann man den Einsetzungshomomorphismus jetzt so verstehen, dass der Polynomring $R[X]$ mit seiner natürlichen Algebrastruktur und eine weitere $R$-Algebra $A$ mit einem fixierten Element $a \in A$ vorliegt und dass dann durch $X \mapsto a$ ein $R$-Algebra-Homomorphismus $R[X] \to A$ definiert wird.

Definition 22.7. Sei $A$ eine $R$-Algebra und sei $f_i \in A$, $i \in I$, eine Familie von Elementen aus $A$. Dann heißt die kleinste $R$-Unteralgebra von $A$, die alle $f_i$ enthält, die von diesen Elementen *erzeugte $R$-Algebra*. Sie wird mit $R[f_i,\, i \in I]$ bezeichnet.

Man kann diese $R$-Algebra auch als den kleinsten Unterring von $A$ charakterisieren, der sowohl $R$ als auch die $f_i$ enthält. Wir werden hauptsächlich von erzeugten $K$-Algebren in einer Körpererweiterung $K \subseteq L$ sprechen, wobei nur ein einziger Erzeuger vorgegeben ist. Man schreibt dafür dann einfach $K[f]$, und diese $K$-Algebra besteht aus allen $K$-Linearkombinationen von Potenzen von $f$. Dies ist das Bild unter dem durch $X \mapsto f$ gegebenen Einsetzungshomomorphismus.

Gelegentlich werden wir auch den kleinsten Unterkörper von $L$ betrachten, der sowohl $K$ als auch eine Elementfamilie $f_i$, $i \in I$, enthält. Dieser

wird mit $K(f_i, i \in I)$ bezeichnet, und man sagt, dass die $f_i$ ein *Körper-Erzeugendensystem* von diesem Körper bilden. Es ist $K[f_i, i \in I] \subseteq K(f_i, i \in I)$ und insbesondere $K[f] \subseteq K(f)$.

## Minimalpolynom

Definition 22.8. Sei $K$ ein Körper und $A$ eine kommutative $K$-Algebra. Es sei $f \in A$ ein Element. Dann heißt $f$ *algebraisch* über $K$, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Wenn ein Polynom $P \neq 0$ das algebraische Element $f \in A$ annulliert (also $P(f) = 0$ ist), so kann man durch den Leitkoeffizienten dividieren und erhält dann auch ein normiertes annullierendes Polynom.

Definition 22.9. Sei $K$ ein Körper und $A$ eine $K$-Algebra. Es sei $f \in A$ ein über $K$ algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von $f$.

Wenn $f$ nicht algebraisch ist, so wird das Nullpolynom als Minimalpolynom betrachtet.

Beispiel 22.10. Bei einer Körpererweiterung $K \subseteq L$ sind die Elemente $a \in K$ trivialerweise algebraisch, und zwar ist jeweils $X - a \in K[X]$ das Minimalpolynom. Weitere Beispiele liefern über $K = \mathbb{Q}$ die komplexen Zahlen $\sqrt{2}, i, 3^{1/5}$, etc. Annullierende Polynome aus $\mathbb{Q}[X]$ sind dafür $X^2 - 2$, $X^2 + 1$, $X^5 - 3$ (es handelt sich dabei übrigens um die Minimalpolynome, was in den ersten zwei Fällen einfach und im dritten Fall etwas schwieriger zu zeigen ist). Man beachte, dass beispielsweise $X - \sqrt{2}$ zwar ein annullierendes Polynom für $\sqrt{2}$ ist, dessen Koeffizienten aber nicht zu $\mathbb{Q}$ gehören.

Lemma 22.11. *Sei $K$ ein Körper, $A$ eine $K$-Algebra und $f \in A$ ein Element. Es sei $P$ das Minimalpolynom von $f$ über $K$. Dann ist der Kern des kanonischen $K$-Algebra-Homomorphismus*

$$K[X] \longrightarrow A,\ X \longmapsto f,$$

*das von $P$ erzeugte Hauptideal.*

*Beweis.* Wir betrachten den kanonischen Einsetzungshomorphismus

$$K[X] \longrightarrow A,\ X \longmapsto f.$$

Dessen Kern ist nach Satz 13.10 und nach Satz 8.3 ein Hauptideal, sagen wir $\mathfrak{a} = (F)$, wobei wir $F$ als normiert annehmen dürfen (im nicht-algebraischen Fall liegt das Nullideal vor und die Aussage ist trivialerweise richtig). Das Minimalpolynom $P$ gehört zu $\mathfrak{a}$. Andererseits ist der Grad von $F$ größer oder gleich dem Grad von $P$, da ja dessen Grad minimal gewählt ist. Daher muss der Grad gleich sein und somit ist $P = F$, da beide normiert sind. □