

Einführung in die Algebra

Vorlesung 21

Algebren

DEFINITION 1. Seien R und A kommutative Ringe und sei $R \longrightarrow A$ ein fixierter Ringhomomorphismus. Dann nennt man A auch 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 $\mathbb{Z} \longrightarrow R, n \longmapsto n_R$. Der Begriff der Algebra ist auch für nicht-kommutative Ringe A (bei kommutativem Grundring R) sinnvoll, wobei dann in aller Regel die Voraussetzung gemacht wird, dass die Elemente aus R mit allen Elementen aus A vertauschen.

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 2. Seien A und B zwei kommutative R -Algebren über einem kommutativen Grundring R . Dann nennt man einen Ringhomomorphismus

$$\varphi : A \longrightarrow B$$

einen R -Algebra-Homomorphismus, wenn er zusätzlich mit den beiden fixierten Homomorphismen $R \longrightarrow A$ und $R \longrightarrow B$ verträglich ist.

Zum Beispiel ist jeder Ringhomomorphismus ein \mathbb{Z} -Algebra-Homomorphismus, da es zu jedem Ring A überhaupt nur den kanonischen Ringhomomorphismus $\mathbb{Z} \longrightarrow A$ gibt. Mit dieser Terminologie kann man den Einsetzungshomomorphismus (siehe Vorlesung 16) 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 $R[X] \longrightarrow A$ definiert wird.

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 3. *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 $x^0 = 1, x^1, \dots, x^{n-1}$ 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 $(P) = (\frac{P}{a_n})$, 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 , $i = 0, \dots, n-1$, 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 null 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 4. Wir betrachten den Restklassenring

$$L = \mathbb{Q}[X]/(X^3 + 2X^2 - 5)$$

und bezeichnen die Restklasse von X mit x . Aufgrund von Proposition 21.3 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 null 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

$$\begin{aligned} (3x^2 - 2x + 4)(2x^2 + x - 1) &= 6x^4 + 3x^3 - 3x^2 - 4x^3 - 2x^2 + 2x + 8x^2 + 4x - 4 \\ &= 6x^4 - x^3 + 3x^2 + 6x - 4 \\ &= 6(4x^2 + 5x - 10) - (2x^2 - 5) + 3x^2 + 6x - 4 \\ &= 25x^2 + 36x - 59. \end{aligned}$$

Endliche Körpererweiterungen

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

$$K \subseteq K[X]/(P) = L$$

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

DEFINITION 5. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlich-dimensionaler Vektorraum über K ist.

DEFINITION 6. 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 Satz 21.3(5) der Grad der Körpererweiterung gleich dem Grad von P .

DEFINITION 7. 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 null verschiedenes Polynom $P \in K[X]$ gibt mit $P(f) = 0$.

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

BEISPIEL 9. Bei einer Körpererweiterung $K \subseteq L$ sind die Elemente $a \in K$ trivialerweise algebraisch, und zwar ist $X - a \in K[X]$ 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 bspw. $X - \sqrt{2}$ zwar ein annullierendes Polynom für $\sqrt{2}$ ist, dessen Koeffizienten aber nicht zu \mathbb{Q} gehören.

LEMMA 10. 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 Ringhomomorphismus

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

Dessen Kern ist nach Satz 16.11 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. \square

DEFINITION 11. 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 . Gelegentlich werden wir auch den kleinsten Unterkörper von L betrachten, der sowohl K als auch f enthält. Dieser wird mit $K(f)$ bezeichnet. Es ist also $K[f] \subseteq K(f)$.

SATZ 12. Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Es sei P das Minimalpolynom von f . Dann gibt es eine kanonische

K-Algebra-Isomorphie

$$K[X]/(P) \longrightarrow K[f], X \longmapsto f.$$

Beweis. Die Einsetzung $X \mapsto f$ ergibt nach Korollar 14.4 den kanonischen K -Algebra-Homomorphismus

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

Das Bild davon ist genau $K[f]$, so dass ein surjektiver K -Algebra-Homomorphismus

$$K[X] \longrightarrow K[f]$$

vorliegt. Daher gibt es nach Satz 16.3 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 21.10 das vom Minimalpolynom erzeugte Hauptideal. \square

LEMMA 13. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann gelten folgende Aussagen.*

- (1) *Das Minimalpolynom P von f über K ist irreduzibel.*
- (2) *Wenn $Q \in K[X]$ ein normiertes, irreduzibles Polynom mit $Q(f) = 0$ ist, so handelt es sich um das Minimalpolynom.*

Beweis. (1) Es sei $P = P_1 P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(f) = P_1(f) P_2(f).$$

Da L ein Körper ist, muss ein Faktor null sein, sagen wir $P_1(f) = 0$. Da aber P unter allen Polynomen $\neq 0$, die f annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant ($\neq 0$), also eine Einheit sein.

(2) Wegen $Q(f) = 0$ ist Q aufgrund von Lemma 21.10 ein Vielfaches des Minimalpolynoms P , sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad eins besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$. \square