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

Körper- und Galoistheorie

Vorlesung 6

Ringhomomorphismen

Wir besprechen nun die strukturerhaltenden Abbildungen zwischen Ringen (und Körpern).

DEFINITION 6.1. Seien R und S Ringe. Eine Abbildung

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

heißt *Ringhomomorphismus*, wenn folgende Eigenschaften gelten:

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(1) = 1$.
(3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Ein Ringhomomorphismus ist also zugleich ein Gruppenhomomorphismus für die additive Struktur und ein Monoidhomomorphismus für die multiplikative Struktur. Einen bijektiven Ringhomomorphismus nennt man einen *Ringisomorphismus*, und zwei Ringe heißen *isomorph*, wenn es einen Ringisomorphismus zwischen ihnen gibt. Zu einem Unterring $S \subseteq R$ ist die natürliche Inklusion ein Ringhomomorphismus. Die konstante Abbildung $R \to 0$ in den Nullring ist stets ein Ringhomomorphismus, dagegen ist die umgekehrte Abbildung, also $0 \to R$, nur bei $R = 0$ ein Ringhomomorphismus.

Die Charakteristik eines Ringes

SATZ 6.2. *Sei R ein Ring. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\mathbb{Z} \longrightarrow R.$$

Beweis. Ein Ringhomomorphismus muss die 1 auf die 1_R abbilden. Deshalb gibt es nach Lemma 4.4 genau einen Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow (R,+,0),\ n \longmapsto n1_R.$$

Wir müssen zeigen, dass diese Abbildung auch die Multiplikation respektiert, d.h. dass $(mn)1_R = (m1_R) * (n1_R)$. ist, wobei $*$ hier die Multiplikation in R bezeichnet. Dies folgt aber aus dem allgemeinen Distributivgesetz. □

Den in dieser Aussage konstruierten und eindeutig bestimmten Ringhomomorphismus nennt man auch den *kanonischen Ringhomomorphismus* (oder den *charakteristischen Ringhomomorphismus*) von $\mathbb{Z}$ nach R.

Definition 6.3. Die *Charakteristik* eines kommutativen Ringes R ist die kleinste positive natürliche Zahl n mit der Eigenschaft $n \cdot 1_R = 0$. Die Charakteristik ist 0, falls keine solche Zahl existiert.

Die Charakteristik beschreibt genau den Kern des obigen kanonischen (charakteristischen) Ringhomomorphismus.

Der Einsetzungshomomorphismus

Satz 6.4. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei A ein weiterer kommutativer Ring und es sei $\varphi\colon R \to A$ ein Ringhomomorphismus und $a \in A$ ein Element. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus*

$$\psi\colon R[X] \longrightarrow A$$

mit $\psi(X) = a$ und mit $\psi \circ i = \varphi$, wobei $i\colon R \to R[X]$ die kanonische Einbettung ist. Dabei geht das Polynom $P = \sum_{j=0}^{n} c_j X^j$ auf $\sum_{j=0}^{n} \varphi(c_j) a^j$.

Beweis. Bei einem Ringhomomorphismus

$$\psi\colon R[X] \longrightarrow A$$

mit $\psi \circ i = \varphi$. müssen die Konstanten $c \in R$ auf $\varphi(c)$ und X auf a gehen. Daher muss X^j auf a^j gehen. Da Summen respektiert werden, kann es nur einen Ringhomorphismus geben, der die im Zusatz angegebene Gestalt haben muss. Es ist also zu zeigen, dass durch diese Vorschrift wirklich ein Ringhomomorphismus definiert ist. Dies folgt aber direkt aus dem Distributivgesetz. □

Den in diesem Satz konstruierten Ringhomomorphismus nennt man den *Einsetzungshomomorphismus*. Es wird ja für die Variable X das Element a eingesetzt.

Algebren

Ein wichtiges Konzept für das Studium von Körpern und Ringen ist, diese als eine Erweiterung von einfacheren Ringen aufzufassen (Grundring, Grundkörper) und dann mit Hilfe des schon verstandenen einfacheren Objektes das erweiterte Objekt zu untersuchen. Man spricht vom relativen Standpunkt. Diese Idee wird durch den Begriff Algebra präzisiert.

Definition 6.5. 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. Jeder Ring A ist auf eine eindeutige Weise eine $\mathbb{Z}$-Algebra über den kanonischen Ringhomomorphismus $\mathbb{Z} \to A$, $n \mapsto n_A$. Bei einer Körpererweiterung $K \subseteq L$ ist L eine K-Algebra. 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 6.6. Seien A und B kommutative R-Algebren über einem kommutativen Grundring R. Dann nennt man einen Ringhomomorphismus

$$\varphi\colon\ A \longrightarrow B$$

einen R- *Algebrahomomorphismus* , wenn er zusätzlich mit den beiden fixierten Ringhomomorphismen $R \to A$ und $R \to B$ verträglich ist.

Zum Beispiel ist jeder Ringhomomorphismus ein $\mathbb{Z}$-Algebrahomomorphismus, 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-Algebrahomomorphismus $R[X] \to A$ definiert wird.

Ideale unter einem Ringhomomorphismus

Der Zusammenhang zwischen Ringhomomorphismen und Idealen wird durch folgenden Satz hergestellt.

Satz 6.7. *Seien R und S kommutative Ringe und sei*

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

ein Ringhomomorphismus. Dann ist der Kern

$$\operatorname{kern} \varphi\ =\ \{f \in R |\, \varphi(f) = 0\}$$

ein Ideal in R.

Beweis. Sei

$$I := \varphi^{-1}(0).$$

Wegen $\varphi(0) = 0.$ ist $0 \in I$. Seien $a, b \in I$. Das bedeutet $\varphi(a) = 0$ und $\varphi(b) = 0$. Dann ist

$$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$$

und daher $a + b \in I$.

Sei nun $a \in I$ und $r \in R$ beliebig. Dann ist

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0,$$

also ist $ra \in I$. □

Da ein Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der zugrunde liegenden additiven Gruppe ist, gilt wieder das Kernkriterium für die Injektivität. Eine Anwendung davon ist das folgende Korollar.

Korollar 6.8. *Es sei K ein Körper und S ein vom Nullring verschiedener Ring. Es sei*

$$\varphi\colon K \longrightarrow S$$

ein Ringhomomorphismus. Dann ist φ injektiv.

Beweis. Es genügt nach Lemma 4.9 zu zeigen, dass der Kern der Abbildung gleich 0 ist. Nach Satz 6.7 ist der Kern ein Ideal. Da die 1 auf $1 \neq 0$ geht, ist der Kern nicht ganz K. Da es nach Lemma 20.9 (Lineare Algebra (Osnabrück 2017-2018)) in einem Körper überhaupt nur zwei Ideale gibt, muss der Kern das Nullideal sein. □

Algebraische Elemente und Minimalpolynom

Definition 6.9. 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 6.10. 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 6.11. 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 $\sqrt{2}, \mathrm{i}, 3^{1/5}$, 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 beiden 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 6.12. *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-Algebrahomomorphismus*

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

das von P erzeugte Hauptideal.

Beweis. Wir betrachten den kanonischen Einsetzungshomorphismus

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

Dessen Kern ist nach Satz 6.7 und nach Satz 3.15 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. □

Definition 6.13. Eine Körpererweiterung $K \subseteq L$, heißt *algebraisch*, wenn jedes Element $f \in L$ algebraisch über K ist.

Erzeugendensysteme

Definition 6.14. 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 $K[f] \subseteq K(f)$.

Definition 6.15. Es sei K ein Körper. Der *Primkörper* von K ist der kleinste Unterkörper von K.

Definition 6.16. Eine Körpererweiterung $K \subseteq L$, heißt *einfach*, wenn es ein Element $x \in L$ mit

$$L = K(x)$$

gibt.

Definition 6.17. Eine Körpererweiterung $K \subseteq L$ heißt eine *einfache Radikalerweiterung*, wenn es ein $b \in L$ gibt mit $L = K(b)$ und ein $n \in \mathbb{N}$ mit $b^n \in K$.

Definition 6.18. Eine Körpererweiterung $K \subseteq L$ heißt eine *Radikalerweiterung*, wenn es Zwischenkörper

$$K \subseteq L_1 \subseteq \ldots \subseteq L_{n-1} \subseteq L_n = L$$

derart gibt, dass $L_i \subseteq L_{i+1}$ für jedes i eine einfache Radikalerweiterung ist.

Bemerkung 6.19. Bei einer Radikalerweiterung entstehen die einzelnen einfachen Radikalerweiterungen durch die Hinzunahme von reinen Wurzelausdrücken. Dies gilt aber im Allgemeinen nicht für die Gesamterweiterung. Beispielsweise kann man eine Situation der Form

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}] \subseteq (\mathbb{Q}[\sqrt[3]{7}]) \left[\sqrt[5]{2 + 9\sqrt[3]{7} - 4\sqrt[3]{7}^2}\right]$$

haben (alles spiele sich innerhalb von $\mathbb{C}$ ab). In den Einzelschritten kommt eine reine Wurzel aus dem Vorgängerkörper hinzu, insgesamt entstehen dabei aber beliebig verschachtelte Wurzelausdrücke. Radikalerweiterungen sind dafür da, solche verschachtelten Wurzelausdrücke systematisch zu erfassen.

Wenn eine komplexe Zahl $z \in \mathbb{C}$ als Nullstelle eines normierten Polynoms mit Koeffizienten aus $\mathbb{Q}$ auftritt, so ist es eine wichtige Frage, ob man sie innerhalb einer Radikalerweiterung beschreiben kann. Die Formel von Cardano besagt insbesondere, dass man die Nullstellen einer kubischen Gleichung $x^3 + px + q = 0$ innerhalb einer Radikalerweiterung realisieren kann, und zwar braucht man dazu die dritten Einheitswurzeln, die Quadratwurzel $\sqrt{3\,(4p^3 + 27q^2)}$ und noch dritte Wurzeln von zuvor erzeugten Ausdrücken. Siehe auch Aufgabe 2.8.

Abbildungsverzeichnis