Prof. Dr. H. Brenner **Osnabrück WS 2012/2013**

Invariantentheorie

Vorlesung 11

Ganzheit

In der nächsten Vorlesung werden wir sehen, dass bei einer endlichen Gruppe, die auf einem kommutativen Ring als Gruppe von Ringautomorphismen operiert, der Ring ganz über seinem Invariantenring ist, wodurch eine enge Beziehung zwischen diesen beiden Ringen gestiftet wird. Hier führen wir die Ganzheit und verwandte Begriffe ein.

DEFINITION 11.1. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

DEFINITION 11.2. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz*, wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

DEFINITION 11.3. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S.

DEFINITION 11.4. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

LEMMA 11.5. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.*

(1) *x ist ganz über R.*
(2) *Es gibt eine R-Unteralgebra T von S mit $x \in T$ und die ein endlicher R-Modul ist.*
(3) *Es gibt einen endlichen R-Untermodul M von S, der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.*

Beweis. (1) $\Rightarrow$ (2). Wir betrachten die von den Potenzen von x erzeugte R-Unteralgebra $R[x]$ von S, die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \ldots + r_1 x + r_0 = 0$$

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \ldots - r_1 x - r_0\,.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] = R + Rx + Rx^2 + \ldots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \ldots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) $\Rightarrow$ (3). Sei $x \in T \subseteq S$, T eine R-Unteralgebra, die als R-Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) $\Rightarrow$ (1). Sei $M \subseteq S$ ein endlich erzeugter R-Untermodul mit $xM \subseteq M$. Seien $y_1, \ldots, y_n$ erzeugende Elemente von M. Dann ist insbesondere xy_i für jedes i eine R-Linearkombination der y_j, $j = 1, \ldots, n$. Dies bedeutet

$$xy_i = \sum_{j=1}^{n} r_{ij} y_j$$

mit $r_{ij} \in R$ oder als Matrix geschrieben

$$x \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} & . & . & r_{1,n} \\ r_{2,1} & r_{2,2} & . & . & r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ r_{n,1} & r_{n,2} & . & . & r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix}.$$

Dies schreiben wir als

$$0 = \begin{pmatrix} x - r_{1,1} & -r_{1,2} & . & . & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & . & . & -r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ -r_{n,1} & -r_{n,2} & . & . & x - r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix}.$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{adj}Ay = 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist $A^{adj}A = (\det A)E_n$, also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j = 0$ für alle j und damit $(\det A)z = 0$ für alle $z \in M$. Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein.

Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n, sodass eine Ganzheitsgleichung vorliegt. □

KOROLLAR 11.6. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann ist der ganze Abschluss von R in S eine R-Unteralgebra von S.*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei $y_1, \ldots, y_n$ ein R-Erzeugendensystem von T_1 und $z_1, \ldots, z_m$ ein R-Erzeugendensystem von T_2. Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R-Modul

$$T \;=\; T_1 \cdot T_2 \;=\; \langle y_i z_j,\, i = 1, \ldots, n,\, j = 1, \ldots, m \rangle,$$

der offensichtlich $x_1 + x_2$ und $x_1 x_2$ (und 1) enthält. Dieser R-Modul T ist auch wieder eine R-Algebra, da für zwei beliebige Elemente gilt

$$\Big(\sum r_{ij} y_i z_j\Big)\Big(\sum s_{kl} y_k z_l\Big) = \sum r_{ij} s_{kl} y_i y_k z_j z_l\,,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$, sodass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S, der R enthält. Also liegt eine R-Unteralgebra vor. □

DEFINITION 11.7. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S, wenn der ganze Abschluss von R in S gleich R ist.

Ganzheit und Endlichkeit

ENg verwandt mit der Ganzheit $A \subseteq B$ ist die Endlichkeit der Algebra B über A, die einfach bedeutet, dass B ein endlich erzeugter A-Modul ist.

LEMMA 11.8. *Es sei S eine endliche R-Algebra und M ein endlich erzeugter S-Modul. Dann ist M auch ein endlich erzeugter R-Modul.*

Beweis. Es sei $s_1, \ldots, s_k$ ein R-Modul-Erzeugendensystem von S und $v_1, \ldots, v_n$ ein S-Modul-Erzeugendensystem von M. Dann bilden die Produkte $s_i v_j$, $1 \leq i \leq k$, $1 \leq j \leq n$, ein R-Modul-Erzeugendensystem von M. □

KOROLLAR 11.9. *Es sei S eine endliche R-Algebra und T eine endliche S-Algebra. Dann ist T eine endliche R-Algebra.*

Beweis. Dies folgt direkt aus Lemma 11.8. □

SATZ 11.10. *Es sei $\varphi\colon R \to S$ ein ganzer Ringhomomorphismus von endlichem Typ. Dann ist S endlich über R.*

Beweis. Es sei $S = R[x_1, \ldots, x_n]$. Wir betrachten die Kette

$$R \longrightarrow R[x_1] \longrightarrow R[x_1, x_2] \longrightarrow \ldots \longrightarrow R[x_1, \ldots, x_n] = S$$

von ganzen Ringhomomorphismen, die jeweils durch ein Element erzeugt werden. Nach Korollar 11.9 genügt es zu zeigen, dass

$$R \longrightarrow R[x]$$

endlich ist, wenn x eine Ganzheitsgleichung über R erfüllt. Mit der Ganzheitsgleichung lässt sich aber eine Potenz (und damit alle höheren Potenzen) von x als R-Linearkombination der kleineren Potenzen ausdrücken, so dass ein endlich erzeugter R-Modul vorliegt. □

Normale und faktorielle Integritätsbereiche

Definition 11.11. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Wichtige Beispiele für normale Ringe werden durch faktorielle Ringe geliefert.

Definition 11.12. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Lemma 11.13. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*
(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und

wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein assoziiertes Element ergibt. Das gekürzte Element hat eine Faktorzerlegung mit $r-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg\,.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. □

Der Polynomring über einem Körper ist faktoriell, was wir aber nicht beweisen werden.

Satz 11.14. *Sei R ein faktorieller Integritätsbereich. Dann ist R normal.*

Beweis. Sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1}q^{n-1} + r_{n-2}q^{n-2} + \ldots + r_1 q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir haben zu zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1}b)a^{n-1} + (r_{n-2}b^2)a^{n-2} + \ldots + (r_1 b^{n-1})a + (r_0 b^n) = 0\,.$$

Wenn b keine Einheit ist, dann gibt es einen Primteiler p von b. Dieser teilt alle Summanden $(r_{n-i}b^i)a^{n-i}$ für $i \geq 1$ und daher auch den ersten, also a^n. Das bedeutet aber, dass a selbst ein Vielfaches von p ist im Widerspruch zur vorausgesetzten Teilerfremdheit. □

Definition 11.15. Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R.