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

Invariantentheorie

Vorlesung 8

Monoidringe

DEFINITION 8.1. Sei M ein kommutatives (additiv geschriebenes) Monoid und R ein kommutativer Ring. Dann wird der *Monoidring* $R[M]$ wie folgt konstruiert. Als R-Modul ist

$$R[M] = \bigoplus_{m \in M} Re_m,$$

d.h. $R[M]$ ist der freie Modul mit Basis e_m, $m \in M$. Die Multiplikation wird auf den Basiselementen durch

$$e_m \cdot e_k := e_{m+k}$$

definiert und auf ganz $R[M]$ distributiv fortgesetzt. Dabei definiert das neutrale Element $0 \in M$ das neutrale Element $1 = e_0$ der Multiplikation.

BEMERKUNG 8.2. Ein Element in einem Monoidring lässt sich eindeutig schreiben als

$$f = \sum_{m \in \tilde{M}} a_m e_m \, ,$$

wobei $\tilde{M} \subseteq M$ eine endliche Teilmenge ist und $a_m \in R$. Addiert wird komponentenweise und die Multiplikation ist explizit gegeben durch

$$f \cdot g = \left(\sum_{m \in \tilde{M}} a_m e_m \right) \left(\sum_{k \in \tilde{M}} b_k e_k \right) = \sum_{\ell \in M} \left(\sum_{m+k=\ell, m \in \tilde{M}, k \in \tilde{M}} a_m b_k \right) e_\ell .$$

Dies ist gemeint mit distributiver Fortsetzung. Die Menge der ℓ, über die hier summiert wird, ist endlich, und auch die inneren Summen sind jeweils endlich.

Es ist üblich, statt e_m suggestiver X^m zu schreiben, wobei X ein Symbol ist, das an eine Variable erinnern soll. Die Multiplikationsregel $X^m X^k = X^{m+k}$ erinnert dann an die entsprechende Regel für Polynomringe. In der Tat sind Polynomringe Spezialfälle von Monoidringen, und diese Notation stammt von dort. Auch ein exakter Beweis, dass in der Tat ein Ring mit assoziativer und distributiver Multiplikation vorliegt, funktioniert wie im Fall von Polynomringen. Meistens schreibt man ein Element einfach als $\sum_{m \in M} a_m X^m$, wobei fast alle $a_m = 0$ sind. Elemente der Form X^m nennt man *Monome*. Die Abbildung $M \to R[M]$, $m \mapsto X^m$, ist ein Monoidhomomorphismus, wobei rechts die multiplikative Monoidstruktur des Monoidringes genommen wird.

Ein Monoidring ist in natürlicher Weise eine R-Algebra, und zwar sind die Elemente f aus R aufgefasst in $R[M]$ gleich

$$f = f \cdot 1 = fX^0.$$

Man nennt daher auch R den *Grundring* des Monoidringes. Monoidringe sind bereits für Grundkörper interessant.

Beispiel 8.3. Sei n eine natürliche Zahl und $M = \mathbb{N}^n$ das n-fache direkte Produkt der natürlichen Zahlen. Ein Element $k \in \mathbb{N}^n$ ist also ein n-Tupel $(k_1, \ldots, k_n)$ mit $k_i \in \mathbb{N}$. Dies kann man auch als

$$(k_1, \ldots, k_n) = k_1(1, 0, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \ldots + k_n(0, 0, 0, \ldots, 1)$$

schreiben. Damit lässt sich das zugehörige Monom X^k eindeutig als

$$X^k = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$$

schreiben, wobei wir $X_i = X^{e_i} = X^{(0,\ldots,0,1,0,\ldots,0)}$ für das Monom zum i-ten Basiselement geschrieben haben. Das bedeutet aber, dass der Monoidring zum Monoid $\mathbb{N}^n$ über R genau der Polynomring in n Variablen ist. Insbesondere ist $R[\mathbb{N}] = R[X]$. Der Monoidring zum trivialen Monoid ist der Grundring selbst.

Beispiel 8.4. Sei n eine natürliche Zahl und $M = \mathbb{Z}^n$ das n-fache direkte Produkt der ganzen Zahlen. M ist also die freie Gruppe vom Rang n. Jedes Element $k \in \mathbb{Z}^n$ ist ein n-Tupel $(k_1, \ldots, k_n)$ mit $k_i \in \mathbb{Z}$. Dies kann man auch als

$$(k_1, \ldots, k_n) = k_1(1, 0, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \ldots + k_n(0, 0, 0, \ldots, 1)$$

schreiben und das zugehörige Monom X^k kann man eindeutig als

$$X^k = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$$

mit $k_i \in \mathbb{Z}$ schreiben, wobei wir wieder $X_i = X^{e_i}$ geschrieben haben. Für diesen Monoidring schreibt man auch

$$R[M] = R[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}],$$

und dieser ist isomorph zur Nenneraufnahme des Polynomringes am Produkt der Variablen, also

$$R[M] = R[X_1, \ldots, X_n, X_1^{-1}, \ldots, X_n^{-1}] = R[X_1, \ldots, X_n]_{X_1 \cdots X_n},$$

Diesen Ring nennt man auch den *Laurent-Ring* in n Variablen über R.

Universelle Eigenschaft der Monoidringe

Satz 8.5. *Sei R ein kommutativer Ring und sei M ein kommutatives Monoid. Sei B eine kommutative R-Algebra und*

$$\varphi\colon M \longrightarrow B$$

ein Monoidhomomorphismus (bezüglich der multiplikativen Struktur von B). Dann gibt es einen eindeutig bestimmten R-Algebrahomomorphismus

$$\tilde{\varphi}\colon\ R[M] \longrightarrow B$$

derart, dass das Diagramm

$$\begin{array}{ccc} M & \longrightarrow & R[M] \\ & \searrow & \downarrow \\ & & B \end{array}$$

kommutiert.

Beweis. Ein R-Modul-Homomorphismus $\tilde{\varphi}\colon\ R[M] \to B$ ist festgelegt durch die Bilder der Basiselemente X^m, $m \in M$. Das Diagramm kommutiert genau dann, wenn $\tilde{\varphi}(X^m) = \varphi(m)$ ist. Durch diese Bedingung ist die Abbildung also eindeutig festgelegt und ist bereits ein R-Modul-Homomorphismus. Es ist zu zeigen, dass dieser Homomorphismus auch die Multiplikation respektiert. Es ist $\tilde{\varphi}(1) = \tilde{\varphi}(X^0) = \varphi(0) = 1$. Ferner ist

$$\tilde{\varphi}(X^m X^k) = \tilde{\varphi}(X^{m+k}) = \varphi(m+k) = \varphi(m)\cdot\varphi(k) = \tilde{\varphi}(X^m)\cdot\tilde{\varphi}(X^k).$$

Auf der Ebene der Monome respektiert die Abbildung also die Multiplikation. Daraus folgen für zwei Elemente $f = \sum_{m\in M} a_m X^m$ und $g = \sum_{k\in M} b_k X^k$ die Identitäten

$$\begin{aligned} \tilde{\varphi}\left(\left(\sum_{m\in M} a_m X^m\right)\left(\sum_{k\in M} b_k X^k\right)\right) &= \tilde{\varphi}\left(\sum_{\ell\in M}\left(\sum_{m+k=\ell} a_m b_k\right) X^\ell\right) \\ &= \sum_{\ell\in M}\left(\sum_{m+k=\ell} a_m b_k\right)\varphi(\ell) \\ &= \sum_{m,k\in M} a_m b_k \varphi(m)\varphi(k) \\ &= \left(\sum_{m\in M} a_m\varphi(m)\right)\left(\sum_{k\in M} b_k\varphi(k)\right) \\ &= \tilde{\varphi}\left(\sum_{m\in M} a_m X^m\right)\tilde{\varphi}\left(\sum_{k\in M} b_k X^k\right), \end{aligned}$$

so dass die Abbildung ein Ringhomomorphismus ist. □

Korollar 8.6. *Sei R ein kommutativer Ring. Seien M und N kommutative Monoide und sei*

$$\varphi\colon\ M \longrightarrow N$$

ein Monoidhomomorphismus. Dann induziert dies einen R-Algebrahomomorphismus zwischen den zugehörigen Monoidringen

$$\tilde{\varphi}\colon\ R[M] \longrightarrow R[N],\ X^m \longmapsto X^{\varphi(m)}.$$

Beweis. Dies folgt aus Satz 17.5 (Algebraische Kurven (Osnabrück 2012)) angewandt auf die R-Algebra $B = R[N]$ und den zusammengesetzten Monoidhomomorphismus $M \stackrel{\varphi}{\to} N \to R[N]$. □

Bemerkung 8.7. Eine Familie von Elementen $m_i \in M$, $i \in I$, in einem Monoid M ergibt einen Monoidhomomorphismus $\mathbb{N}^{(I)} \to M$, indem das i-te Basiselement e_i auf m_i geschickt wird. Dies ist insbesondere für endliche Indexmengen $I = \{1, \ldots, n\}$ relevant. Der Monoidhomomorphismus induziert dann nach Korollar 8.6 einen R-Algebra-Homomorphismus $R[\mathbb{N}^n] = R[X_1, \ldots, X_n] \to R[M]$ von der Polynomalgebra in den Monoidring. Diese Abbildung ist der Einsetzungshomomorphismus, der durch $X_i \mapsto X^{m_i}$ gegeben ist.

Definition 8.8. Zu einem kommutativen Monoid M und einem kommutativen Ring R nennt man einen Monoidhomorphismus

$$M \longrightarrow (R, \cdot, 1)$$

auch einen *R-wertigen Punkt* von M.

Lemma 8.9. *Sei R ein von null verschiedener kommutativer Ring. Seien M und N kommutative Monoide und sei $\varphi\colon M \to N$ ein Monoidhomomorphismus. Dann ist φ genau dann injektiv (surjektiv), wenn der zugehörige R-Algebra-Homomorphismus $\tilde{\varphi}\colon R[M] \to R[N]$ injektiv (surjektiv) ist.*

Beweis. Sei φ injektiv, und angenommen, dass

$$\tilde{\varphi}\left(\sum_{m \in M} a_m X^m\right) = \sum_{m \in M} a_m X^{\varphi(m)} = 0.$$

Da die $\varphi(m)$, $m \in M$, alle verschieden sind, folgt daraus $a_m = 0$. Ist umgekehrt φ nicht injektiv, sagen wir $\varphi(m) = \varphi(k)$, $m \neq k$, so ist auch $\tilde{\varphi}(X^m) = \tilde{\varphi}(X^k)$, obwohl $X^m \neq X^k$ ist.

Ist φ surjektiv, so kann man für ein beliebiges Element $\sum_{n \in N} a_n X^n$ aus $R[N]$ sofort ein Urbild angeben, nämlich $\sum_{n \in N} a_n X^{m_n}$, wobei m_n ein beliebiges Urbild von n sei. Ist hingegen φ nicht surjektiv, so sei $n \in N$ ein Element, das nicht zum Bild gehört. Dann ist das Monom X^n von null verschieden und kann nicht im Bild des Algebra-Homomorphismus liegen. □

Korollar 8.10. *Sei R ein von null verschiedener kommutativer Ring. Sei M ein kommutatives Monoid und $m_i \in M$, $i \in I$, eine Familie von Elementen aus M. Dann bilden die m_i genau dann ein Monoid-Erzeugendensystem für M, wenn die X^{m_i}, $i \in I$, ein R-Algebra-Erzeugendensystem für den Monoidring $R[M]$ bilden.*

Beweis. Die m_i, $i \in I$, bilden genau dann ein Monoid-Erzeugendensystem für M, wenn der Monoidhomomorphismus $\mathbb{N}^{(I)} \to M$ surjektiv ist. Dies ist nach Lemma 8.9 genau dann der Fall, wenn der zugehörige Homomorphismus

$$R[X_i, i \in I] \longrightarrow R[M],\ X_i \longmapsto X^{m_i},$$

surjektiv ist. Dies ist aber genau dann der Fall, wenn die X^{m_i} ein R-Algebra-Erzeugendensystem bilden. □

KOROLLAR 8.11. *Sei R ein kommutativer Ring und S eine R-Algebra. Es sei M ein kommutatives Monoid. Dann gibt es einen natürlichen R-Algebra-Homomorphismus*

$$R[M] \longrightarrow S[M], \sum_{m\in M} a_m X^m \longmapsto \sum_{m\in M} a_m X^m \,,$$

(die Koeffizienten aus R werden also einfach in S aufgefasst).

Beweis. Dies folgt aus Satz 17.5 (Algebraische Kurven (Osnabrück 2012)), angewandt auf die R-Algebra $S[M]$ und den Monoidhomomorphismus $M \to S[M]$. □

Differenzengruppe zu einem Monoid

Wir interessieren uns nun für die Frage, wann ein Monoidring ein Integritätsbereich ist (was nur bei integrem Grundring sein kann) und wie man dann den Quotientenkörper beschreiben kann. Da im Quotientenkörper jedes von null verschiedene Element invertierbar sein muss, gilt das insbesondere für die Monome T^m, $m \in M$, und es liegt nahe, nach einer additiven Gruppe zu suchen, die M umfasst.

DEFINITION 8.12. Sei M ein kommutatives Monoid. Dann nennt man die Menge der *formalen Differenzen*

$$\Gamma(M) \;=\; \{m-n|\, m,n \in M\}$$

mit der Addition

$$(m_1-n_1)+(m_2-n_2) \;:=\; (m_1+m_2)-(n_1+n_2)$$

und der Identifikation

$$m_1-n_1 = m_2-n_2 \text{ falls es } m\in M \text{ gibt mit } m+m_1+n_2 = m+m_2+n_1\,.$$

die *Differenzengruppe* zu M.

Wir überlassen es dem Leser als Aufgabe, zu zeigen, dass die Differenzengruppe wirklich eine Gruppe ist. Die vorstehende Konstruktion ist natürlich der Konstruktion von Quotientenkörpern bzw. Quotientenringen nachempfunden, man muss nur die multiplikative Schreibweise dort additiv umdeuten. Die Konstruktion der Differenzengruppe ist eigentlich elementarer. Die Differenzengruppe zum additiven Monoid $\mathbb{N}$ ist natürlich $\mathbb{Z}$. Die Elemente in einem Monoid kann man direkt im Differenzenmonoid auffassen, und zwar durch den Monoidhomomorphismus

$$M \longrightarrow \Gamma(M),\, m \longmapsto m-0\,,$$

wobei wir statt $m-0$ einfach m schreiben. Völlig unproblematisch ist dieser Übergang aber doch nicht, da diese Abbildung im Allgemeinen nicht injektiv sein muss. Das hat damit zu tun, dass in der obigen Definition bei der Identifizierung links und rechts ein m auftreten darf (und das lässt sich auch nicht vermeiden). Natürlich will man auch diejenigen Monoide charakterisieren, für die man dieses Extra-m nicht braucht.

DEFINITION 8.13. Man sagt, dass in einem kommutativen Monoid M die *Kürzungsregel* gilt (oder dass M ein *Monoid mit Kürzungsregel* ist), wenn aus einer Gleichung

$$m+n=m+k \text{ mit } m,n,k\in M\,,$$

stets folgt, dass $n=k$ ist.

Für ein solches Monoid ist die Abbildung in die Differenzengruppe injektiv, siehe Aufgabe 8.4.

Weitere Begriffe für Monoide

DEFINITION 8.14. Ein kommutatives Monoid M heißt *endlich erzeugt*, wenn es Elemente $m_1,\ldots,m_n\in M$ gibt derart, dass man jedes $m\in M$ als

$$m\ =\ \sum_{j=1}^{n} a_j m_j$$

mit $a_j\in\mathbb{N}$ schreiben kann.

DEFINITION 8.15. Ein kommutatives Monoid M heißt *spitz*, wenn 0 das einzige invertierbare Element in M ist.

DEFINITION 8.16. Ein kommutatives Monoid M heißt *torsionsfrei*, wenn für $m,n\in M$ aus $rm=rn$ für eine positive Zahl $r\in\mathbb{N}_+$ stets $m=n$ folgt.

Wenn M ein endlich erzeugtes, torsionsfreies Monoid mit Kürzungsregel ist, so ist die zugehörige Differenzengruppe isomorph zu $\mathbb{Z}^n$ und wird auch das *Differenzengitter* zu M genannt.

DEFINITION 8.17. Sei M ein torsionsfreies kommutatives Monoid mit Kürzungsregel und mit zugehöriger Differenzengruppe $\Gamma(M)$. Dann heißt das Untermonoid

$$\tilde{M}=\{m\in\Gamma(M)|\ \text{es gibt } r\in\mathbb{N}_+ \text{ mit } rm\in M\}$$

die *Normalisierung* von M.

Ein Monoid heißt *normal*, wenn es ein torsionsfreies Monoid mit Kürzungsregel ist und mit seiner Normalisierung übereinstimmt.