Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 20

Multiplikative Systeme

Wir wollen zeigen, dass es zu jedem Integritätsbereich R einen Körper K gibt derart, dass R ein Unterring von K wird. Diesen Körper werden wir dann den *Quotientenkörper* von R nennen. Die Konstruktion ist dieselbe, mit der man aus den ganzen Zahlen $\mathbb{Z}$ die rationalen Zahlen $\mathbb{Q}$ gewinnt.

Definition 20.1. Sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

(1) $1 \in S$
(2) Wenn $f, g \in S$, dann ist auch $fg \in S$

gelten.

Wir erwähnen einige Beispiele von multiplikativen Systemen. Zunächst ist natürlich der Gesamtring, die Menge $\{1\}$ und die Einheitengruppe $R^\times$ ein multiplikatives System. Darüber hinaus erwähnen wir die folgenden Beispiele.

Beispiel 20.2. Sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n, $n \in \mathbb{N}$, ein multiplikatives System.

Beispiel 20.3. Die Nichtnullteiler bilden ein multiplikatives System in einem kommutativen Ring. Die 1 ist wie jede Einheit ein Nichtnullteiler, und wenn f und g Nichtnullteiler sind, so ist auch deren Produkt ein Nichtnullteiler, da aus $f(gh) = 0$ zunächst $gh = 0$ und daraus $h = 0$ folgt.

Beispiel 20.4. Sei R ein Integritätsbereich. Dann bilden alle von null verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R - \{0\}$ bezeichnet wird.

Definition 20.5. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Beispiel 20.6. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R - \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

Beispiel 20.7. Sei R ein faktorieller Bereich und sei M eine Menge von Primelementen. Dann ist die Menge aller Elemente aus R, in deren Primfaktorzerlegung ausschließlich Primelemente aus M vorkommen, ein multiplikatives System S. Es ist also

$$S = \{up_1^{r_1} \cdots p_k^{r_k} \mid u \in R^\times, \, p_i \in M\} .$$

LEMMA 20.8. *Seien R und A kommutative Ringe und sei*

$$\varphi : R \longrightarrow A$$

ein Ringhomomorphismus. Dann ist das Urbild $\varphi^{-1}(A^\times)$ der Einheitengruppe ein multiplikatives System.

Beweis. Das ist trivial. □

Nenneraufnahme

Unser nächstes Ziel ist es, zu einem multiplikativen System S einen Ring zu konstruieren mit der Eigenschaft, dass die Elemente aus S dort zu Einheiten werden, und dieser Ring minimal mit dieser Eigenschaft ist.

DEFINITION 20.9. Sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$. Dann heißt die Menge der *formalen Brüche*

$$R_S := \left\{ \frac{f}{g} : f \in R, g \in S \right\}$$

die *Nenneraufnahme* zu S. Dabei werden zwei Brüche $\frac{f}{g}$ und $\frac{s}{t}$ identifiziert, wenn $ft = gs$ gilt. Die Nenneraufnahme ist ein kommutativer Ring mit der Addition

$$\frac{f}{g} + \frac{s}{t} = \frac{ft + gs}{tg}$$

und der Multiplikation

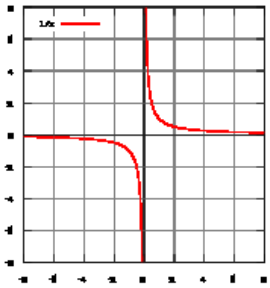
$$\frac{f}{g} \cdot \frac{s}{t} = \frac{fs}{tg}.$$

Für die Nenneraufnahme an einem Element f schreibt man einfach R_f statt $R_{\{f^n : n \in \mathbb{N}\}}$. Die Elemente $s \in S$ aus dem multiplikativen System werden in R_S zu Einheiten, und zwar ist $1/s$ das Inverse zu s. Die Nenneraufnahme an $R^* = R \setminus \{0\}$ in einem Integritätsbereich spielt für uns eine besondere Rolle. Dort werden sämtliche Elemente $\neq 0$ zu Einheiten und es entsteht somit ein Körper.

DEFINITION 20.10. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

$$Q(R) = \{ \frac{r}{s} : r, s \in R, s \neq 0 \}$$

mit natürlichen Identifizierungen und Operationen.



Die einfachste rationale Funktion (von den Polynomen abgesehen)ist $1/X$.

Die wichtigsten Beispiele für einen Quotientenkörper sind die rationalen Zahlen $Q(\mathbb{Z}) = \mathbb{Q}$ und der Quotientenkörper des Polynomrings in einer Variablen über einem (Grund-)körper K. Man bezeichnet ihn mit $K(X) = Q(K[X])$ und nennt ihn den *Körper der rationalen Funktionen* (über K). In der Tat definiert ein Bruch P/Q aus zwei Polynomen $P, Q \in K[X]$, $Q \neq 0$, eine Funktion

$$U \longrightarrow K,\, x \longmapsto \frac{P(x)}{Q(x)},$$

wobei $U \subseteq K$ das Komplement der Nullstellenmenge von Q bezeichnet. Wie schon im Fall von Polynomen und den dadurch definierten polynomialen Funktionen muss man auch hier vorsichtig sein und darf nicht die formalen Brüche mit den dadurch definierten Funktionen gleichsetzen, auch wenn dies bei $K = \mathbb{R}$ die Vorstellung unterstützt.

Die folgende Aussage kann man so verstehen, dass der Quotientenkörper der minimale Körper ist, in dem man einen Integritätsbereich als Unterring realisieren kann.

Satz 20.11. *Sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Es sei*

$$\varphi : R \longrightarrow K$$

ein injektiver Ringhomomorphismus in einen Körper K Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi} : Q(R) \longrightarrow K$$

mit $\varphi = \tilde{\varphi} \circ i$, wobei i die kanonische Einbettung

$$i : R \longrightarrow Q(R)$$

bezeichnet.

Beweis. Damit die Ringhomomorphismen kommutieren muss $\tilde{\varphi}(1/b) = (\varphi(b))^{-1}$ und damit $\tilde{\varphi}(a/b) = \varphi(a)(\varphi(b))^{-1}$ sein. Es kann also maximal einen solchen Ringhomomorphismus geben, der durch die letzte Gleichung definiert sein muss. Da für $b \neq 0$ auch $\varphi(b) \neq 0$ ist und K ein Körper ist, gibt es $\varphi(b)^{-1} \in K$. Es ist zu zeigen, dass dadurch ein wohldefinierter Ringhomomorphismus gegeben ist. Zur Wohldefiniertheit sei $\frac{a}{b} = \frac{c}{d}$, also $ad = bc$.

Dann ist auch $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$ und durch Multiplizieren mit der Einheit $\varphi(b)^{-1}\varphi(d)^{-1}$ folgt

$$\varphi(a)(\varphi(b))^{-1} = \varphi(c)(\varphi(d))^{-1}.$$

Wir zeigen exemplarisch für die Addition, dass ein Ringhomomorphismus vorliegt. Es ist

$$\begin{aligned}
\tilde{\varphi}(\frac{a}{b}+\frac{c}{d}) &= \tilde{\varphi}(\frac{ad+cb}{bd}) \\
&= \varphi(ad+bc)\varphi(bd)^{-1} \\
&= (\varphi(a)\varphi(d)+\varphi(b)\varphi(c))\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1}+\varphi(c)\varphi(d)^{-1} \\
&= \tilde{\varphi}(\frac{a}{b})+\tilde{\varphi}(\frac{c}{d}).
\end{aligned}$$

□

Der Satz von Gauß

Wir wollen nun für einen faktoriellen Integritätsbereich R zeigen, dass auch der Polynomring $R[X]$ faktoriell ist. Speziell ergibt sich daraus induktiv, dass für einen Körper die Polynomringe in beliebig vielen Variablen faktoriell sind, obwohl sie nur bei einer Variablen Hauptidealbereiche sind. Es liegt nahe, dabei mit dem Quotientenkörper $Q(R)$ zu arbeiten und Teilbarkeitseigenschaften in $R[X]$ mit denen in $Q(R)[X]$ zu vergleichen. Da letzteres ein Hauptidealbereich ist, ist darüber viel bekannt.

In den folgenden Beweisen werden zwei einfache Beobachtungen wiederholt zur Anwendung kommen. Ein konstantes Polynom $c \in R$ teilt ein Polynom $P = \sum_{i=0}^{n} a_i X^i \in R[X]$ genau dann, wenn c jeden Koeffizienten a_i teilt. Und zu einem Polynom $F = \sum_{i=0}^{n} q_i X^i \in Q(R)[X]$ gibt es stets ein $a \in R$ (nämlich einen *Hauptnenner* der q_i) derart, dass aF zu $R[X]$ gehört.

Lemma 20.12. *Sei R ein kommutativer Ring und sei $R[X]$ der Polynomring über R. Es sei $p \in R$ ein Primelement. Dann ist p auch in $R[X]$ prim.*

Beweis. Sei $ph = fg$. Wir nehmen an, dass p weder f noch g teilt. Dann teilt p nicht alle Koeffizienten von f und von g. Es sei $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ und es seien i_0 bzw. j_0 die kleinsten Indizes derart, dass a_{i_0} (bzw. b_{j_0}) kein Vielfaches von p ist (für alle kleineren Indizes sind die Koeffizienten also Vielfache von p). Wir betrachten den (i_0+j_0)-ten Koeffizienten von fg, dieser ist

$$c_{i_0+j_0} = a_0 b_{i_0+j_0} + \ldots + a_{i_0-1} b_{j_0+1} + a_{i_0} b_{j_0} + a_{i_0+1} b_{j_0-1} + \ldots + a_{i_0+j_0} b_0$$

Die Summanden links sind Vielfache von p aufgrund der Wahl von i_0 und die Summanden rechts sind ebenso Vielfache von p. Da auch der Gesamtkoeffizient nach Voraussetzung ein Vielfaches von p ist, muss auch der mittlere

Summand $a_{i_0}b_{j_0}$ ein Vielfaches von p sein. Da p prim ist, ist dies ein Widerspruch. □

LEMMA 20.13. *(Lemma von Gauß)*

Es sei R ein faktorieller Bereich und $K = Q(R)$ der zugehörige Quotientenkörper. Es sei $f \in R[X]$ ein nicht-konstantes Polynom derart, dass in $R[X]$ nur Faktorzerlegungen $f = gh$ mit $g \in R$ oder $h \in R$ möglich sind. Dann ist f irreduzibel in $K[X]$.

Beweis. Nehmen wir an, es gebe eine nicht-triviale Faktorzerlegung $f = gh$ mit nicht-konstanten Polynomen $g, h \in K[X]$. Sowohl in g als auch in h kommen nur endlich viele Nenner aus R vor, so dass man mit einem gemeinsamen Hauptnenner $r \in R$ multiplizieren kann und somit eine Darstellung $rf = \tilde{g}\tilde{h}$ mit $\tilde{g}, \tilde{h} \in R[X]$ erhält. Dabei haben sich die Grade der beteiligten Polynome nicht geändert. Es sei $r = p_1 \cdots p_n$ die Primfaktorzerlegung von r. Nach Lemma 20.12 ist p_1 auch im Polynomring $R[X]$ prim. Da es das Produkt $\tilde{g}\tilde{h}$ teilt, muss es einen der Faktoren teilen, sagen wir $\tilde{h}$. Dann kann man mit p_1 kürzen und erhält eine Gleichung der Form

$$r'f = \tilde{g}\tilde{h}' .$$

Dabei ändern sich wieder die Grade nicht. So kann man sukzessive alle Primfaktoren wegkürzen und erhält schließlich eine Zerlegung

$$f = g'h'$$

mit nicht konstanten Polynomen $h', g' \in R[X]$ im Widerspruch zur Voraussetzung. □

SATZ 20.14. *Sei R ein faktorieller Bereich. Dann ist auch der Polynomring $R[X]$ faktoriell.*

Beweis. Wir zeigen, dass jedes irreduzible Element prim ist und dass jedes Polynom eine Zerlegung in irreduzible Polynome besitzt. Sei also $f \in R[X]$ irreduzibel und

$$fq = hg .$$

Bei $f \in R$ ist f prim nach Lemma 20.12, so dass wir $\operatorname{grad}(f) \geq 1$ annehmen können. Die Teilbarkeitsbeziehung gilt erst recht in $Q(R)[X]$. Nach Lemma 20.13 ist das Polynom f auch irreduzibel in $Q(R)[X]$ und damit darin prim nach Satz 17.15. Daher teilt dieses Element in $Q(R)[X]$ einen der Faktoren, sagen wir h. Es ist also $fu = h$ mit $u \in Q(R)[X]$. Wir können mit einem Hauptnenner a von u multiplizieren und erhalten die Beziehung

$$fv = ha = hp_1 \cdots p_n$$

mit $v \in R[X]$, wobei a durch seine Primfaktorzerlegung ersetzt wurde. Da f irreduzibel ist, sind die Koeffizienten von f teilerfremd. Insbesondere ist p_1 kein Teiler von allen Koeffizienten von f. Da p_1 nach Lemma 20.12 auch in $R[X]$ prim ist, folgt, dass v ein Vielfaches von p ist. Man kann also durch p_1

kürzen. So kann man sukzessive die Primfaktorzerlegung von a abarbeiten und erhält schließlich, dass h ein Vielfaches von f ist.

Dass jedes Polynom $f \in R$ ein Produkt von irreduziblen Polynomen ist, beweisen wir durch Induktion über den Grad von f. Bei Grad null liefert die Primfaktorzerlegung in P sofort die gewünschte Zerlegung in $R[X]$. Sei also der Grad von f positiv. Wenn es eine Produktzerlegung in Polynome von kleinerem Grad gibt, so sind wir fertig aufgrund der Induktionsvoraussetzung. Andernfalls sei a der größte gemeinsame Teiler der Koeffizienten von f. Dann ist $f = a\tilde{f}$ mit $\tilde{f} \in R[X]$ und die Koeffizienten von $\tilde{f}$ sind teilerfremd. Dann ist aber $\tilde{f}$ irreduzibel, da es weder eine Zerlegung in Polynome mit kleinerem Grad noch eine nicht-triviale Zerlegung mit Konstanten geben kann. □

KOROLLAR 20.15. *Der Polynomring $\mathbb{Z}[X]$ ist faktoriell.*

Beweis. Dies folgt aus Satz 14.9, Satz 18.3 und Satz 20.14. □

KOROLLAR 20.16. *Es sei K ein Körper. Dann sind die Polynomringe $K[X_1, \ldots, X_n]$ faktoriell.*

Beweis. Dies folgt durch induktive Anwendung von Satz 20.14 auf die Kette

$$K \subset K[X_1] \subset (K[X_1])[X_2] \subset (K[X_1, X_2])[X_3] \subset \ldots$$

□

Abbildungsverzeichnis