**Prof. Dr. H. Brenner** **Osnabrück SS 2015**

# Elemente der Algebra

## Vorlesung 17

### Quotientenkörper

Bei der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ betrachtet man die formalen Brüche

$$\frac{a}{b},\ a,b \in \mathbb{Z},\ b \neq 0$$

und identifiziert zwei Brüche $\frac{a}{b}$ und $\frac{c}{d}$, wenn $ad = bc$ ist. Das gleiche Verfahren kann man für jeden Integritätsbereich $R$ anwenden und erhält dadurch einen Körper, in dem $R$ als Unterring enthalten ist.

Definition 17.1. Zu einem Integritätsbereich $R$ ist der *Quotientenkörper* $Q(R)$ definiert als die Menge der formalen Brüche

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

mit natürlichen Identifizierungen und Operationen.

Diese Definition ist etwas vage, gemein ist das folgende: Auf der Menge der Paare aus $R \times (R \setminus \{0\})$ führt man eine Äquivalenzrelation ein, indem man

$$(a,b) \sim (a',b') \text{ setzt, wenn } ab' = a'b \text{ ist}.$$

Die zugehörige Quotientenmenge ist dann der Quotientenkörper, also

$$Q(R) = R \times (R \setminus \{0\}) / \sim$$

Die Äquivalenzklasse zu $(a,b)$ schreibt man als $\frac{a}{b}$. Man definiert dann durch $0 = \frac{0}{1}$, $1 = \frac{1}{1}$, spezielle Elemente in $Q(R)$ und durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

und

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

(wohldefinierte) Verknüpfungen, die $Q(R)$ zu einem kommutativen Ring machen. Bei $a,b \neq 0$ gilt

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1$$

und somit liegt ein Körper vor. Die Abbildung

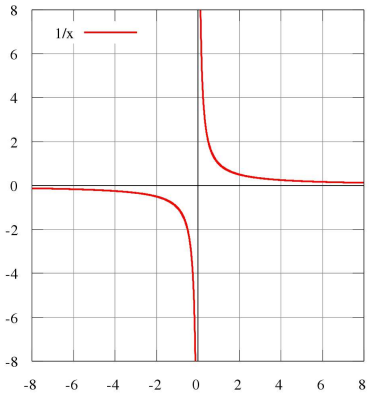
$$R \longrightarrow Q(R),\ r \longmapsto \frac{r}{1},$$

ist ein injektiver Ringhomomorphismus.

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 $K$).




Man kann auch Brüche $P/Q$ von Polynomen als Funktionen auffassen, die außerhalb der Nullstellen des Nenners definiert sind. Das Beispiel zeigt den Graph der rationalen Funktion $1/X$.

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 bei einem endlichen Grundkörper vorsichtig sein und darf nicht die formalen Brüche mit den dadurch definierten Funktionen gleichsetzen.Bei $K = \mathbb{R}$ ist dies aber eine richtige und hilfreiche Vorstellung.

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

Satz 17.2. *Sei $R$ ein Integritätsbereich mit Quotientenkörper $Q(R)$. Es sei*

$$\varphi\colon\ R \longrightarrow K$$

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

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

*mit*

$$\varphi = \tilde{\varphi}\tilde{i},$$

*wobei $i$ die kanonische Einbettung*

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

*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

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

□

Für die vorstehende Aussage ist die Injektivität der Abbildung $R \to K$ wichtig. Beispielsweise gibt es für den Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/(p)$ keine Faktorisierung über $\mathbb{Q}$, da es überhaupt keinen Ringhomomorphismus von $\mathbb{Q}$ in einen endlichen Restklassenring von $\mathbb{Z}$ gibt.

## Quotientenkörper zu faktoriellen Ringen

Lemma 17.3. *Zu einem Primelement $p \in R$ in einem faktoriellen Bereich $R$ mit Quotientenkörper $Q(R)$ ist die Zuordnung*

$$Q(R)^\times \longrightarrow \mathbb{Z},\ \frac{f}{g} \longmapsto \exp_p(f) - \exp_p(g),$$

*ein (wohldefinierter) Gruppenhomomorphismus.*

*Beweis.* Zum Nachweis der Wohldefiniertheit sei

$$\frac{f}{g} = \frac{h}{q}$$

eine weitere Darstellung, also

$$fq = hg.$$

Dann ist nach Lemma 9.8

$$\exp_p(f) + \exp_p(q) = \exp_p(fq) = \exp_p(hg) = \exp_p(h) + \exp_p(g),$$

woraus sich

$$\exp_p(f) - \exp_p(g) = \exp_p(h) - \exp_p(q)$$

ergibt. Die Gruppenhomomorphie ergibt sich ebenfalls aus Lemma 9.8. □

Satz 17.4. *Sei $R$ ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Dann besitzt jedes Element $f \in K$, $f \neq 0$, eine im Wesentlichen eindeutige Produktzerlegung*

$$f = up_1^{r_1} \cdots p_n^{r_n}$$

*mit einer Einheit $u \in R$ und ganzzahligen Exponenten $r_i$.*

*Beweis.* Wir schreiben

$$f = \frac{a}{b}$$

mit von 0 verschiedenen Elementen $a, b \in R$. Die Primfaktorzerlegungen dieser Elemente seien $a = u_1 p_1^{m_1} \cdots p_n^{m_n}$ und $b = u_2 p_1^{k_1} \cdots p_n^{k_n}$, wobei die $p_i$ nicht untereinander assoziiert seien, $m_i, k_i \in \mathbb{N}_{\geq 0}$ und $u_1, u_2$ Einheiten sind. Dann ist

$$\frac{a}{b} = \frac{u_1 p_1^{m_1} \cdots p_n^{m_n}}{u_2 p_1^{k_1} \cdots p_n^{k_n}} = u_1 u_2^{-1} p_1^{m_1 - k_1} \cdots p_n^{m_n - k_n}$$

eine Darstellung der gewünschten Art. Wenn zwei Dastellungen

$$up_1^{r_1} \cdots p_n^{r_n} = f = vp_1^{s_1} \cdots p_n^{s_n}$$

gegeben sind, so erhält man durch Multiplikation mit $(p_1 \cdots p_n)^t$ für hinreichend großes $t$, dass links und rechts alle Exponenten positiv werden. Aus der Faktorialität folgt daraus $r_i = s_i$ für alle $i$ und damit auch $u = v$. □

Man kann also beispielsweise jede rationale Zahl $q = a/b$ eindeutig schreiben als

$$q = \pm p_1^{r_1} \cdots p_n^{r_n}$$

mit Primzahlen $p_1, \ldots, p_n$ und Exponenten $r_1, \ldots, r_n \in \mathbb{Z}$. Der multiplikative Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ enspricht also auf der Ebene der Exponenten dem additiven Übergang von $\mathbb{N}$ nach $\mathbb{Z}$.

Die eben angeführte eindeutige Darstellung ist mit der Multiplikation verträglich. In der nächsten Aussage bedeutet die Schreibweise $\mathbb{Z}^{(I)}$ die Menge aller $I$-Tupel mit Werten in $\mathbb{Z}$, wobei aber jeweils nur endlich viele Einträge von 0 verschieden sein dürfen.

Satz 17.5. *Sei $R$ ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Es sei $p_i$, $i \in I$, ein System von paarweise nicht assoziierten Primelementen von $R$ und sei $U$ die Einheitengruppe von $R$ Dann ist (wobei $u(q)$ die nach Satz 17.4 eindeutige Einheit bezeichnet)*

$$Q(R)^\times \longrightarrow U \times \mathbb{Z}^{(I)},\ q \longmapsto (u(q), \exp_{p_i}(q)),$$

*ein Gruppenisomorphismus mit der Umkehrabbildung*

$$U \times \mathbb{Z}^{(I)} \longrightarrow Q(R)^\times,\ (u, e_{p_i}) \longmapsto u \prod_{i \in I} p^{e_{p_i}}.$$

*Beweis.* Dies folgt aus Lemma 17.3 und Satz 17.4. □

# Abbildungsverzeichnis