G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 9

Aufgabe 36.

Wir zeigen zunächst die Existenz eines solchen Ringmorphismus. Setze

$$\begin{array}{rcl} R_S & \xrightarrow{\hat{f}} & T \\ \frac{r}{s} & \longmapsto & f(r)f(s)^{-1}\,. \end{array}$$

Dies ist wohldefiniert, da aus $\frac{r}{s} = \frac{r'}{s'}$ folgt, daß $f(r)f(s') = f(r')f(s)$, und somit $f(r)f(s)^{-1} = f(r')f(s')^{-1}$.
Dies ist ein Ringmorphismus, da

$$\begin{array}{rcl} \hat{f}(\frac{1}{1}) & = & 1 \\ \hat{f}(\frac{r}{s} + \frac{r'}{s'}) & = & f(rs' + r's)f(ss')^{-1} \;=\; f(r)f(s)^{-1} + f(r')f(s')^{-1} \\ \hat{f}(\frac{r}{s} \cdot \frac{r'}{s'}) & = & f(rr')f(ss')^{-1} \;=\; (f(r)f(s)^{-1}) \cdot (f(r')f(s')^{-1}) \end{array}$$

für $\frac{r}{s},\ \frac{r'}{s'} \in R_S$.

Sei $R_S \xrightarrow{\tilde{f}} T$ ein weiterer Ringmorphismus mit $\tilde{f}|_R = f$. Zunächst ist $1 = f(\frac{1}{1}) = \tilde{f}(\frac{s}{1})\tilde{f}(\frac{1}{s}) = f(s)\tilde{f}(\frac{1}{s})$, und also $\tilde{f}(\frac{1}{s}) = f(s)^{-1}$. Allgemein wird mithin $\tilde{f}(\frac{r}{s}) = \tilde{f}(\frac{r}{1})\tilde{f}(\frac{1}{s}) = f(r)f(s)^{-1} = \hat{f}(\frac{r}{s})$.

Den Fall $S = R \smallsetminus \{0\}$ der vorstehenden Aufgabe kennen Sie als Satz 10.3 (ii) aus der Vorlesung.

Aufgabe 37.

(1) Sei $\mathfrak{p}$ ein Primideal. Es ist $1 \in R \smallsetminus \mathfrak{p}$, da $\mathfrak{p} \neq R$. Ferner, sind $s,\ s' \in R \smallsetminus \mathfrak{p}$, und wäre $ss' \in \mathfrak{p}$, so folgte aus der definierenden Eigenschaft eines Primideals, daß $s \in \mathfrak{p}$ oder $s' \in \mathfrak{p}$, was nicht geht. Also ist $ss' \in R \smallsetminus \mathfrak{p}$.

Umgekehrt, sei $R \smallsetminus \mathfrak{p}$ als multiplikative Teilmenge bekannt. Wegen $1 \in R \smallsetminus \mathfrak{p}$ ist $\mathfrak{p} \neq R$. Sind $s,\ s' \in R$ so gegeben, daß $ss' \in \mathfrak{p}$, so können nicht s und s' in $R \smallsetminus \mathfrak{p}$ gelegen haben, da sonst wegen der Multiplikativität dieser Teilmenge auch ss' darin liegen würde. Also ist $s \in \mathfrak{p}$ oder $s' \in \mathfrak{p}$.

(2) Es ist $\mathfrak{p}_\mathfrak{p}$ ein Ideal von $R_\mathfrak{p}$, da $\mathfrak{p}_\mathfrak{p} \subseteq R_\mathfrak{p}$; da $\frac{0}{1} \in \mathfrak{p}_\mathfrak{p}$; da mit $\frac{a}{s},\ \frac{a'}{s'} \in \mathfrak{p}_\mathfrak{p}$ wegen $\mathfrak{p}$ Ideal und $R \smallsetminus \mathfrak{p}$ multiplikativ auch $\frac{ab'+a'b}{bb'} \in \mathfrak{p}_\mathfrak{p}$; und da schließlich mit $\frac{a}{s} \in \mathfrak{p}_\mathfrak{p}$ und $\frac{r}{t} \in R_\mathfrak{p}$ wegen $\mathfrak{p}$ Ideal und $R \smallsetminus \mathfrak{p}$ multiplikativ auch $\frac{ar}{st} \in \mathfrak{p}_\mathfrak{p}$ liegt.

Sei noch angemerkt, daß wenn *ein* Repräsentant $\frac{a}{s}$ eines Elementes in R_S die definierenden Eigenschaften $a \in \mathfrak{p}$ und $s \in R \smallsetminus \mathfrak{p}$ besitzt, daß dann jeder andere Repräsentant $\frac{a'}{s'}$ desselben Elements auch die erste, nämlich $a' \in \mathfrak{p}$, besitzt. Denn aus $a's = as' \in \mathfrak{p}$ folgt wegen $\mathfrak{p}$ prim und $s \notin \mathfrak{p}$, daß $a' \in \mathfrak{p}$. (Ferner vereinbaren wir, Elemente von $R_\mathfrak{p}$ stets mit Nenner in $R \smallsetminus \mathfrak{p}$ als Elemente von $\mathrm{Quot}(R)$ zu repräsentieren.)

Wir müssen zeigen, daß

$$\begin{array}{rcl} R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} & \longrightarrow & \mathrm{Quot}(R/\mathfrak{p}) \\ \frac{r}{s} + \mathfrak{p}_\mathfrak{p} & \longmapsto & \frac{r+\mathfrak{p}}{s+\mathfrak{p}} \\ \frac{r}{s} + \mathfrak{p}_\mathfrak{p} & \longleftarrow\!\shortmid & \frac{r+\mathfrak{p}}{s+\mathfrak{p}} \end{array}$$

in beiden Richtungen eine wohldefinierte Abbildung ist. Sodann genügt es zu zeigen, daß in eine Richtung ein Ringmorphismus vorliegt, es folgt dann daraus, daß in inverser Richtung ebenfalls ein Ringmorphismus vorliegt.

Nun ist aber $\frac{r}{s} + \mathfrak{p}_\mathfrak{p} = \frac{r'}{s'} + \mathfrak{p}_\mathfrak{p} \iff \frac{rs'-r's}{ss'} \in \mathfrak{p}_\mathfrak{p} \iff rs' \equiv_\mathfrak{p} r's \iff (r+\mathfrak{p})(s'+\mathfrak{p}) = (r'+\mathfrak{p})(s+\mathfrak{p})$ $\iff \frac{r+\mathfrak{p}}{s+\mathfrak{p}} = \frac{r'+\mathfrak{p}}{s'+\mathfrak{p}}$. Dies zeigt die Wohldefiniertheit von $\longmapsto$, wenn wie die Äquivalenzkette von links nach rechts lesen, und die Wohldefiniertheit von $\longleftarrow\!\!|$, wenn wir sie in umgekehrter Richtung lesen.

Es ist $\longmapsto$ ein Ringmorphismus. Die benötigten Verträglichkeiten mit Einselement, Addition und Multiplikation folgen unmittelbar.

(3) Mit (2) ist $\mathfrak{p}_\mathfrak{p}$ ein maximales Ideal von $R_\mathfrak{p}$, da der Quotient ein Körper ist.

Da jedes Element in $R_\mathfrak{p} \smallsetminus \mathfrak{p}_\mathfrak{p}$ invertierbar ist in $R_\mathfrak{p}$, liegt jedes Ideal ungleich $R_\mathfrak{p}$ von $R_\mathfrak{p}$ in $\mathfrak{p}_\mathfrak{p}$. Also ist $\mathfrak{p}_\mathfrak{p}$ das einzige maximale Ideal von $R_\mathfrak{p}$. (Das Quotientenargument des vorigen Absatzes kann mit diesem Argument auch entfallen, da Maximalität gleich mit folgt; es ist aber dennoch lehrreich.)

Aufgabe 38.

Wir bemerken zunächst, daß v_p wegen $\bigcap_{n\geq 0}(p^n) = 0$ wohldefiniert ist – dies war aber in der Aufgabe nicht verlangt.

(1) (i) Zunächst beobachten wir, daß $\mathrm{v}_p(x) = n$ bedeutet, daß in der Primfaktorzerlegung des Nenners r von $x = \frac{r}{s}$, wobei $s \in \mathbf{Z} \smallsetminus (p)$, der Faktor p^n bei der Primzahl p auftritt. Daher ist $\mathrm{v}_p(xy) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$.

(ii) Sei $n := \mathrm{v}_p(x)$ und $m := \mathrm{v}_p(y)$.
Aus $x \in (p^n)$ und $y \in (p^m)$ folgt $x + y \in (p^{\min(m,n)})$, d.h. die erste Behauptung.
Sei nun o.E. $n < m$. Wäre $x+y \in (p^{n+1})$, so wäre wegen $y \in (p^{n+1})$ auch $x \in (p^{n+1})$. Das ist aber nicht der Fall, und die zweite Behauptung folgt, welche in diesen Bezeichnungen $\mathrm{v}_p(x + y) = n$ besagt.

(iii) Zunächst bemerken wir, daß $u \in \mathbf{Z}_{(p)}$ genau dann eine Einheit ist, wenn $\mathrm{v}_p(u) = 0$. Denn ist $\mathrm{v}_p(u) > 1$, so liegt u in dem Ideal $(p) \neq \mathbf{Z}_{(p)}$, und ist damit keine Einheit. Umgekehrt, ist $\mathrm{v}_p(u) = 0$, so ist $u \notin (p)$, und damit invertierbar in $\mathbf{Z}_{(p)}$.
Seien nun $x,\, y \in \mathbf{Z}_{(p)}$ assoziiert. Dann ist $xu = y$ für ein $u \in (\mathbf{Z}_{(p)})^*$, also $\mathrm{v}_p(y) = \mathrm{v}_p(xu) = \mathrm{v}_p(x) + \mathrm{v}_p(u) = \mathrm{v}_p(x)$.
Sei umgekehrt $n := \mathrm{v}_p(x) = \mathrm{v}_p(y)$. Schreibe $x = p^n u$ und $y = p^n v$ mit $u,\, v \in (\mathbf{Z}_{(p)})^*$. Es wird $xu^{-1}v = y$, und auch $u^{-1}v$ ist eine Einheit in $\mathbf{Z}_{(p)}$.

(2) Sei $\mathfrak{a} \subseteq \mathbf{Z}_{(p)}$ ein Ideal ungleich 0. Sei $x \in \mathfrak{a} \smallsetminus \{0\}$ ein Element mit $n := \mathrm{v}_p(x)$ minimal. Wir behaupten, daß

$$\mathfrak{a} \;=\; (x) \;=\; (p^n)\,.$$

Letztere Gleichheit folgt mit (1 iii), da $\mathrm{v}_p(p^n) = n$.

In ersterer Gleichheit folgt die Inklusion $\supseteq$ nach Konstruktion. Zeigen wir die Inklusion $\subseteq$. Sei $y \in \mathfrak{a}$. O.E. sei $y \neq 0$. Nach Wahl von x ist $\mathrm{v}_p(y) \geq n$, d.h. $y \in (p^n) = (x)$.

Aufgabe 39.

(1) Die Aussage ist richtig. Denn seien $x,\, y \in R$ mit $xy \in f^{-1}(\mathfrak{p})$, so ist $f(xy) = f(x)f(y) \in \mathfrak{p}$ und also wegen $\mathfrak{p}$ prim $f(x) \in \mathfrak{p}$ oder $f(y) \in \mathfrak{p}$, d.h. $x \in f^{-1}(\mathfrak{p})$ oder $y \in f^{-1}(\mathfrak{p})$.

Alternative Begründung. Es ist $R/f^{-1}(\mathfrak{p}) \longrightarrow S/\mathfrak{p}$, $r + f^{-1}(\mathfrak{p}) \longmapsto f(r) + \mathfrak{p}$ ein injektiver Ringmorphismus. Ferner ist $S/\mathfrak{p}$ ein Integritätsbereich. Also ist auch $R/f^{-1}(\mathfrak{p})$ ein Integritätsbereich.

(2) Die Aussage ist falsch. Denn es ist $0 \subseteq \mathbf{Q}$ ein maximales Ideal, nicht aber sein Urbild 0 unter $\mathbf{Z} \hookrightarrow \mathbf{Q}$.

(3) Die Aussage ist richtig. Denn es ist

$$\begin{aligned} \mathrm{F}(1) &= 1^p = 1 \\ \mathrm{F}(x+y) &= (x+y)^p = x^p + \left(\textstyle\sum_{i\in[1,p-1]} \binom{p}{i} x^i y^{p-i}\right) + y^p = x^p + y^p = \mathrm{F}(x) + \mathrm{F}(y) \\ \mathrm{F}(x\cdot y) &= (xy)^p = x^p y^p = \mathrm{F}(x)\cdot\mathrm{F}(y) \end{aligned}$$

für $x, y \in R$, da $\binom{p}{i} = 0$ für $i \in [1, p-1]$ in einer $\mathbf{F}_p$-Algebra.

(4) Die Aussage ist falsch. Sei etwa $R = \mathbf{F}_p(X)$. Es ist X nicht im Bild von F, da der Ansatz $\mathrm{F}\left(\frac{f(X)}{g(X)}\right) = X$ mit $f(X), g(X) \in \mathbf{F}_p[X] \smallsetminus \{0\}$ zu $f(X)^p = Xg(X)^p$ und damit zu

$$0 \equiv_p p\cdot\deg(f(X)) = \deg(f(X)^p) = \deg(Xg(X)^p) = 1 + p\cdot\deg(g(X)) \equiv_p 1$$

führt, was nicht geht. Mithin ist F nicht surjektiv, und also kein Automorphismus.

Hingegen ist F auf einem Körper ein *injektiver* Endomorphismus – wie gemäß 35 (3) jeder Ringmorphismus von einem Körper in einen Ring $\neq 0$.

Körper, die entweder Charakteristik 0 haben, oder die Charakteristik $p > 0$ haben und auf denen F ein Automorphismus darstellt, heißen *perfekt*. Endliche Körper sind perfekt. Algebraisch abgeschlossene Körper sind perfekt.