Lösungen und zusätzliche Bemerkungen

zu Übungsblatt 1

Jendrik Stelzner

8. Mai 2017

Aufgabe 2

Es sei R ein Integritätsbereich.

Bemerkung 1. Der Quotientenkörpers des Integritätsbereichs der ganzen Zahlen $\mathbb{Z}$ ist der Körper der rationalen Zahlen $\mathbb{Q}$, d.h. $Q(\mathbb{Z}) = \mathbb{Q}$.

Bemerkung 2. Die Abbildung $i \colon R \to Q(R)$, $r \mapsto r/1$ ist ein injektiver Ringhomomorphismus: Es handelt sich um einen Ringhomomorphismus, denn für alle $r_1, r_2 \in R$ gilt

$$i(r_1) + i(r_2) = \frac{r_1}{1} + \frac{r_2}{1} = \frac{r_1 + r_2}{1} = i(r_1 + r_2)$$

und

$$i(r_1) \cdot i(r_2) = \frac{r_1}{1} \cdot \frac{r_2}{1} = \frac{r_1 r_2}{1} = i(r_1 r_2),$$

und es gilt $i(1_R) = 1_R/1_R = 1_{Q(R)}$. Ist $r \in \ker i$, so gilt $r/0 = 0/1$ und somit $r \cdot 1 = 0 \cdot 0$, also $r = 0$. Deshalb ist $\ker i = \{0\}$ und i somit injektiv.

Da i ein injektiver Ringhomomorphismus ist, lässt sich i durch Einschränkung als ein Ringisomorphismus $R \to \operatorname{im} i$ auffassen, d.h. $\operatorname{im} i$ ist ein zu R isomorpher Unterring von $Q(R)$, und ein entsprechender Isomorphismus ist durch $r \mapsto r/1$ gegeben.

Anschaulich gesehen ist $Q(R)$ der „kleinstmögliche" Körper, der R enthält. Dies lässt sich durch die *universelle Eigenschaft des Quotientenkörpers* formalisieren:

Ist K ein beliebiger Körper und $j \colon R \to K$ ein injektiver Ringhomomorphismus, so gibt es einen eindeutigen Ringhomomorphismus $\overline{j} \colon Q(R) \to K$, der das folgende Diagramm zum Kommutieren bringt:

$$\begin{tikzcd} & R \arrow[dl, "i"'] \arrow[dr, "j"] & \\ Q(R) \arrow[rr, "\overline{j}"] & & K \end{tikzcd} \tag{1}$$

Beweis. Für alle $r/s \in Q(R)$ muss

$$\overline{j}\left(\frac{r}{s}\right) = \overline{j}\left(\frac{r}{1}\left(\frac{s}{1}\right)^{-1}\right) = \overline{j}(i(r)i(s)^{-1}) = \overline{j}(i(r))\overline{j}(i(s))^{-1} = j(r)j(s)^{-1} = \frac{j(r)}{j(s)}$$

gelten, was die eindeutig von $\overline{j}$ zeigt. (Hier nutzen wir, dass $\overline{j}(x^{-1}) = \overline{j}(x)^{-1}$ für alle $x \in Q(R)$ mit $x \neq 0$ gelten muss, da $1_K = \overline{j}(1_{Q(R)}) = \overline{j}(xx^{-1}) = \overline{j}(x)\overline{j}(x^{-1})$ gilt.)

Andererseits definiert

$$\overline{j} \colon Q(R) \to K, \quad \frac{r}{s} \mapsto \frac{j(r)}{j(s)}$$

einen wohldefinierten Ringhomomorphismus:

Für $r/s = r'/s' \in Q(R)$ gilt $rs' = r's$ und somit auch

$$j(r)j(s') = j(rs') = j(r's) = j(r')j(s). \tag{2}$$

Wegen der Injektivität von j folgt aus $s, s' \neq 0$, dass auch $j(s), j(s') \neq 0$ gilt. Die Gleichung (2) lässt sich deshalb durch $j(s)$ und durch $j(s')$ teilen, wodurch sich $j(r)/j(s) = j(r')/j(s')$ ergibt. Dies zeigt die Wohldefiniertheit von $\overline{j}$.

Dass $\overline{j}$ ein Ringhomomorphismus ist, ergibt sich durch direktes Nachrechnen, denn für alle $r_1/s_1, r_2/s_2 \in Q(R)$ gilt

$$\begin{aligned}\overline{j}\left(\frac{r_1}{s_1}\right) + \overline{j}\left(\frac{r_2}{s_2}\right) &= \frac{j(r_1)}{j(s_1)} + \frac{j(r_2)}{j(s_2)} = \frac{j(r_1)j(s_2) + j(r_2)j(s_1)}{j(s_1)j(s_2)} \\ &= \frac{j(r_1 s_2 + r_2 s_1)}{j(s_1 s_2)} = \overline{j}\left(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right) = \overline{j}\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right).\end{aligned}$$

sowie

$$\begin{aligned}\overline{j}\left(\frac{r_1}{s_1}\right) \cdot \overline{j}\left(\frac{r_2}{s_2}\right) = \frac{j(r_1)}{j(s_1)} \cdot \frac{j(r_2)}{j(s_2)} = \frac{j(r_1)j(r_2)}{j(s_1)j(s_2)} = \frac{j(r_1 r_2)}{j(s_1 s_2)} &= \overline{j}\left(\frac{r_1 r_2}{s_1 s_2}\right) \\ &= \overline{j}\left(\frac{r_1}{s_1} \cdot \frac{r_2}{s_2}\right),\end{aligned}$$

und es gilt $\overline{j}(1_{Q(R)}) = \overline{j}(1_R/1_R) = j(1_R)/j(1_R) = 1_K/1_K = 1_K$. □

Bemerkung 3. Ringhomomorphismen zwischen zwei Körpern sind stets injektiv: Es seien K und L zwei Körper. Gebe es einen nicht-injektiven Ringhomomorphismus $\varphi \colon K \to L$, so würde $\ker \varphi \neq 0$ gelten. Dann gebe es ein $x \in K$ mit $x \neq 0$ und $\varphi(x) = 0$. Dann würde auch

$$0 = 0 \cdot \varphi(x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(1) = 1,$$

gelten, was aber in Körpern per Definition nicht gilt. Folglich muss $\ker \varphi = 0$ gelten, und φ somit injektiv sein.

Inbesondere erhalten wir in dem kommutativen Diagram (1), dass auch der Ringhomomorphismus $\overline{j}$ injektiv ist, und somit einen Isomorphismus von Körpern $Q(R) \to \operatorname{im} \overline{j}$ induziert. Dies entspricht der Anschauung, dass jeder Körper, der den Integritätsbereich R enthält, auch schon den Quotientenkörper $Q(R)$ enthalten muss.

So muss etwa jeder Körper, der die ganzen Zahlen $\mathbb{Z}$ enthält, auch schon die rationalen Zahlen $Q(\mathbb{Z}) = \mathbb{Q}$ enthalten.

Bemerkung 4. Auf die übliche Weise ergibt sich, dass das Paar $(Q(R), i)$ durch die obige universelle Eigenschaft bis auf eindeutigen Isomorphismus eindeutig bestimmt ist:

Es sei (Q', i') ein weiteres Paar, bestehend aus einem Körper Q' und einem injektiven Ringhomomorphismus $i' \colon R \to Q'$, so dass es für jeden Körper K und jeden injektiven Ringhomomorphismus $j \colon R \to K$ einen eindeutigen Ringhomomorphismus $\overline{j} \colon Q' \to K$ gibt, so dass das folgende Diagramm kommutiert:

$$\begin{tikzcd} & R \arrow[dl, "i'"'] \arrow[dr, "j"] & \\ Q' \arrow[rr, "\overline{j}"] & & K \end{tikzcd} \tag{3}$$

Dann gibt es einen eindeutigen Ringhomomorphismus $\varphi \colon Q(R) \to Q'$, der das Diagramm

$$\begin{tikzcd} & R \arrow[dl, "i"'] \arrow[dr, "i'"] & \\ Q(R) \arrow[rr, "\varphi"] & & Q' \end{tikzcd} \tag{4}$$

zum Kommutieren bringt, und φ ist ein Isomorphismus:

Die Existenz und Eindeutigkeit von φ ergeben sich dadurch, dass man die universelle Eigenschaft des Paars $(Q(R), i)$ auf den injektiven Ringhomomorphismus $i' \colon R \to Q'$ anwendet. Analog ergibt sich Anwenden der analogen Eigenschaft von (Q', i') auf den injektiven Ringhomomorphismus $i \colon R \to Q(Q)$, dass es einen eindeutigen Ringhomomorphismus $\psi \colon Q' \to Q(R)$ gibt, so dass das Diagramm

$$\begin{tikzcd} & R \arrow[dl, "i"'] \arrow[dr, "i'"] & \\ Q(R) & & Q' \arrow[ll, "\psi"] \end{tikzcd} \tag{5}$$

kommutiert. Durch Zusammenfügen von (4) und (5) ergibt sich das folgende kommutative Diagramm:

$$\begin{tikzcd} & R \arrow[dl, "i"'] \arrow[d, "i'"] \arrow[dr, "i"] & \\ Q(R) \arrow[r, "\varphi"] & Q' \arrow[r, "\psi"] & Q(R) \end{tikzcd} \tag{6}$$

Hieraus ergibt sich durch Vergessen des mittleren vertikalen Pfeils das folgende kommutative Diagramm:

$$\begin{tikzcd} & R \arrow[dl, "i"'] \arrow[dr, "i"] & \\ Q(R) \arrow[rr, "\psi \circ \varphi"] & & Q(R) \end{tikzcd} \tag{7}$$

Nach der universellen Eigenschaft von $(Q(R), i)$ ist $\psi \circ \varphi$ dabei bereits der *eindeutige* Ringhomomorphismus $Q(R) \to Q(R)$, der das Diagramm (7) zum Kommutieren bringt. Andererseits bringt auch $\mathrm{id}_{Q(R)} \colon Q(R) \to Q(R)$ das Diagramm zum Kommutieren. Somit muss bereits $\psi \circ \varphi = \mathrm{id}_{Q(R)}$ gelten. Analog ergibt sich, dass auch $\varphi \circ \psi = \mathrm{id}_{Q'}$ gilt. Also ist φ ein Isomorphismus mit $\varphi^{-1} = \psi$.

Aufgabe 3

(a)

Da I eine Untergruppe der unterliegenden additiven Gruppe von R ist, ist aus der Linearen Algebra I bekannt, dass

- $\sim$ eine Äquivalenzrelation auf R definiert,
- durch $\overline{x} + \overline{y} := \overline{x+y}$ eine wohldefinierte binäre Verknüpfung von R/I definiert wird,
- R/I durch $+$ zu einer abelschen Gruppe wird.

Es bleibt zu zeigen, dass

- durch $\overline{x} \cdot \overline{y} := \overline{xy}$ eine wohldefinierte binäre Verknüpfüng auf R/I definiert wird,
- diese Multiplikation assoziativ ist,
- diese Multiplikation kommutativ ist,
- es für diese Multiplikation ein Einselement gibt,
- die Distributivgesetze für die Addition $+$ und Multiplikation $\cdot$ auf R/I gelten.

Für die Wohldefiniertheit der Multiplikation seien $x, x, y, y' \in R$ with $\overline{x} = \overline{x'}$ und $\overline{y} = \overline{y'}$. Dann gilt $x - x', y - y' \in I$ und somit auch

$$xy - x'y' = xy - xy' + xy' - x'y' = x\underbrace{(y - y')}_{\in I} + \underbrace{(x - x')}_{\in I}y' \in I,$$

also $\overline{xy} = \overline{x'y'}$. Das zeigt die Wohldefiniertheit der Multiplikation. Für alle $\overline{x}, \overline{y}, \overline{z} \in R/I$ gilt

$$\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{yz} = \overline{xyz} = \overline{xy} \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z},$$

was die Assoziativität der Multiplikation zeigt. Für alle $\overline{x}, \overline{y} \in R/I$ gilt

$$\overline{x} \cdot \overline{y} = \overline{xy} = \overline{yx} = \overline{y} \cdot \overline{x},$$

was die Kommutativität der Multiplikation zeigt. Das Element $\overline{1} \in R/I$ ist ein Einselement für die Multiplikation, denn für alle $\overline{x} \in R/I$ gilt

$$\overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}.$$

Die Distributivität der Multiplikation im ersten Argument ergibt sich darus, dass für alle $\overline{x}, \overline{y}, \overline{z} \in R/I$ die Gleichheit

$$(\overline{x} + \overline{y}) \cdot \overline{z} = \overline{x+y} \cdot \overline{z} = \overline{(x+y)z} = \overline{xz + yz} = \overline{xz} + \overline{yz} = \overline{x} \cdot \overline{z} + \overline{y} \cdot \overline{z}$$

gilt. Da die Multiplikation auf R/I kommutativ ist, ergibt sich hieraus auch die Distributivität im zweiten Argument.

Ingesamt zeigt dies, dass R/I mit der gegeben Addition und Multiplikation ein kommutativer Ring ist.

Bemerkung 5. Im Falle $R = \mathbb{Z}$ und $I = (n) = n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$ ist die Konstruktion von $R/I = \mathbb{Z}/n\mathbb{Z}$ bereits aus der Linearen Algebra I bekannt.

Bemerkung 6. Die Konstruktion des Quotientenringes R/I funktioniert auch für einen nicht-kommutativen Ring, sofern man fordert, dass I ein beidseitiges Ideal ist, d.h. dass $rx, xr \in I$ für alle $x \in I$ und $r \in R$ gilt.

(b)

Als Ringhomomorphismus ist φ insbesondere ein Gruppenhomomorphismus zwischen den unterliegenden additiven Gruppen von R und S; deshalb gilt

$$\varphi(0) = 0$$

und somit $0 \in \ker \varphi$, und für jedes $x \in \ker \varphi$ gilt

$$\varphi(-x) = -\varphi(x) = -0 = 0$$

und somit auch $-x \in \ker \varphi$. Für alle $x, y \in \ker \varphi$ gilt außerdem

$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0,$$

und somit auch $x + y \in \ker \varphi$. Das zeigt, dass $\ker \varphi$ eine Untergruppe der additiven Gruppe von R ist. (Eventuell wurde dies auch schon in der Linearen Algebra I gezeigt.) Für alle $r \in R$ und $x \in \ker \varphi$ gilt

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0,$$

und somit auch $rx \in \ker \varphi$. Somit ist $\ker \varphi$ bereits ein Ideal in R.

Beispiel 7. Ist K ein Körper, so sind $\{0\}, K \subseteq K$ die einzigen beiden Ideale in K: Ist nämlich $I \subseteq K$ ein Ideal mit $I \neq \{0\}$, so gibt es ein $x \in I$ mit $x \neq 0$. Dann gilt auch $1 = x^{-1}x \in I$, und für jedes $y \in K$ somit auch $y = y \cdot 1 \in I$. Deshalb gilt dann bereits $I = K$.

Ist nun R ein Ring und $\varphi\colon K \to R$ ein Ringhomomorphismus, so ist $\ker \varphi \subseteq K$ ein Ideal. Ist $R \neq 0$, so gilt $0_R \neq 1_R$ und deshalb $1_K \notin \ker \varphi$. Somit muss nach der obigen Beobachtung bereits $\ker \varphi = 0$ gelten, und φ deshalb injektiv sein.

Ringhomomorphismen aus Körpern heraus sind also injektiv, sofern sie nicht ausgerechnet in den Nullring gehen.

(c)

Wir betrachten den kommutativen Ring R/I und die Abbildung $\pi\colon R \to R/I$, $x \mapsto \overline{x}$. Dies ist ein Ringhomomorphismus, denn für alle $x, y \in R$ gilt

$$\pi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \pi(x) + \pi(y)$$

sowie

$$\pi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \pi(x) \cdot \pi(y),$$

und es gilt $\pi(1_R) = \overline{1_R} = 1_{R/I}$. Für den Ringhomomorphismus π gilt

$$\begin{aligned} \ker \pi &= \{x \in R \mid \pi(x) = 0\} = \{x \in R \mid \overline{x} = \overline{0}\} \\ &= \{x \in R \mid x - 0 \in I\} = \{x \in R \mid x \in I\} = I, \end{aligned}$$

was die gegebene Behauptung zeigt.

Bemerkung 8. Analog zu den letzten beiden Aufgabenteilen ergibt sich für einen nicht-kommutativen Ring R, dass $I \subseteq R$ genau dann beidseitiges Ideal ist, wenn es einen Ring S und einen Ringhomomorphismus $\varphi\colon R \to S$ mit $\ker \varphi = I$ gibt.

Aufgabe 4

(a)

Die Kommutativität des Diagrams

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

ist äquivalent dazu, dass $\overline{\varphi}(\overline{x}) = \varphi(x)$ für alle $x \in R/I$ gilt. Dies zeigt bereits die Eindeutigkeit von $\overline{\varphi}$.

Zum Beweis der Existenz von $\overline{\varphi}$ gilt es zu zeigen, dass durch

$$\overline{\varphi}\colon R/I \to S, \quad \overline{x} \mapsto \varphi(x)$$

ein wohldefinierter Ringhomomorphismus gegeben ist:

Für $x, y \in R$ mit $\overline{x} = \overline{y}$ gilt $x - y \in \ker \varphi$ und somit $0 = \varphi(x - y) = \varphi(x) - \varphi(y)$, also $\varphi(x) = \varphi(y)$. Dies zeigt die Wohldefiniertheit von $\overline{\varphi}$. Durch direktes Nachrechnen ergibt sich, dass $\overline{\varphi}$ ein Ringhomomorphismus ist, denn für alle $\overline{x}, \overline{y} \in R/I$ gilt

$$\overline{\varphi}(\overline{x} + \overline{y}) = \overline{\varphi}(\overline{x + y}) = \varphi(x + y) = \varphi(x) + \varphi(y) = \overline{\varphi}(\overline{x}) + \overline{\varphi}(\overline{y}).$$

und

$$\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{x \cdot y}) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\overline{x}) \cdot \overline{\varphi}(\overline{y}),$$

und es gilt $\overline{\varphi}(1_{R/I}) = \overline{\varphi}(\overline{1_R}) = \varphi(1_R) = 1_S$.

Bemerkung 9. Ist R ein nicht-kommutativer Ring und $I \subseteq R$ ein beidseitiges Ideal, so gilt der Homomorphiesatz in gleicher Form und mit unveränderten Beweis.

(b)

Es gilt

$$\operatorname{im}\overline{\varphi} = \{\overline{\varphi}(\overline{x}) \mid \overline{x} \in R/I\} = \{\varphi(x) \mid x \in R\} = \operatorname{im}\varphi.$$

Insbesondere ist $\overline{\varphi}$ genau dann surjektiv, wenn φ surjektiv ist. Außerdem gilt

$$\begin{aligned}\ker\overline{\varphi} &= \{\overline{x} \in R/I \mid \overline{\varphi}(\overline{x}) = 0\} = \{\overline{x} \in R/I \mid \varphi(x) = 0\} \\ &= \{\overline{x} \in R/I \mid x \in \ker\varphi\} = \{\overline{x} \mid x \in \ker\varphi\} = \{x + I \mid x \in \ker\varphi\} = (\ker\varphi)/I.\end{aligned}$$

Deshalb gilt

$$\overline{\varphi} \text{ ist injektiv} \iff \ker\overline{\varphi} = \{0\} \iff (\ker\varphi)/I = \{0\} \iff \ker\varphi = I.$$

Behauptung 10. Das Bild $\operatorname{im}\varphi$ ist ein kommutativer Unterring von S.

Beweis. Es gilt

$$0 = \varphi(0) \in \operatorname{im}\varphi.$$

Für $y \in \operatorname{im}\varphi$ gibt es $x \in R$ mit $y = \varphi(x)$, weshalb auch

$$-y = -\varphi(x) = \varphi(-x) \in \operatorname{im}\varphi$$

gilt Für $y_1, y_2 \in \operatorname{im}\varphi$ gibt es $x_1, x_2 \in R$ mit $y_1 = \varphi(x_1)$ und $y_2 = \varphi(x_2)$, weshalb auch

$$y_1 + y_2 = \varphi(x_1) + \varphi(x_2) = \varphi(x_1 + x_2) \in \operatorname{im}\varphi$$

gilt. Das zeigt, dass $\operatorname{im}\varphi$ eine Untergruppe der additiven Gruppe von S ist.

Es gilt

$$1_S = \varphi(1_R) \in \operatorname{im}\varphi.$$

Für alle $y_1, y_2 \in \operatorname{im}\varphi$ gibt es $x_1, x_2 \in R$ mit $y_1 = \varphi(x_1)$ und $y_2 = \varphi(x_2)$, weshalb auch

$$y_1 y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1 x_2) \in \operatorname{im}\varphi$$

gilt Das zeigt, dass $\operatorname{im}\varphi$ bereits ein Unterring von S ist.

Für $y_1, y_2 \in \operatorname{im}\varphi$ gibt es $x_1, x_2 \in R$ mit $y_1 = \varphi(x_1)$ und $y_2 = \varphi(x_2)$. Aus der Kommutativität von φ ergibt sich dann, dass

$$y_1 y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1 x_2) = \varphi(x_2 x_1) = \varphi(x_2)\varphi(x_1) = y_2 y_1.$$

Also ist auch $\operatorname{im}\varphi$ kommutativ. □

Wir können nun φ als einen surjektiven Ringhomorphismus $R \to \operatorname{im}\varphi$, $r \mapsto \varphi(r)$ auffassen. Aus den bereits gezeigten Aussagen erhalten wir, dass φ einen bijektiven Ringhomomorphismus, also einen Ringisomorphismus $\overline{\varphi}\colon R/I \to \operatorname{im}\varphi$, $\overline{x} \mapsto \varphi(x)$ induziert. Somit gilt $R/I \cong \operatorname{im}\varphi$.

Bemerkung 11. Ist R ein nicht-kommutativer Ring und $I \subseteq R$ ein Ideal, bzw. $\varphi\colon R \to S$ ein Ringhomomorphismus, so gelten die Aussagen unverändert mit gleichen Beweis. (Der einzige Unterschied besteht darin, dass $\operatorname{im}\varphi$ nicht mehr notwendigerweise kommutativ ist.)

Beispiel 12. 1. Nach der universellen Eigenschaft des Polynomrings gibt es einen eindeutigen Homomorphismus von $\mathbb{R}$-Algebren $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$ mit $\varphi(X) = i$; konkret ist φ durch $\varphi(p) = p(i)$ für alle $p \in \mathbb{R}[X]$ gegeben. Für alle $a, b \in \mathbb{R}$ gilt $a + ib = \varphi(a + bX) \in \operatorname{im}\varphi$, weshalb φ surjektiv ist.

Behauptung 13. Es gilt $\ker\varphi = (X^2+1) = \{f \cdot (X^2+1) \mid f \in \mathbb{R}[X]\}$.

Beweis. Für $p \in (X^2+1)$ gibt es $f \in \mathbb{R}[X]$ mit $p = f \cdot (X^2+1)$. Dann gilt

$$\varphi(p) = p(i) = f(i) \cdot (i^2+1) = f(i) \cdot 0 = 0,$$

und somit $p \in \ker\varphi$.

Gilt andererseits $p \in \ker\varphi$, so ist $p(i) = \varphi(p) = 0$. Durch Polynomdivison ergeben sich $f, r \in K[X]$ mit $p = f \cdot (X^2+1) + r$ und $\deg r < \deg(X^2+1) = 2$. Also ist r von der Form $r = a + bX$ mit $a, b \in \mathbb{R}$. Wir erhalten, dass

$$0 = p(i) = f(i) \cdot \underbrace{(i^2+1)}_{=0} + r(i) = r(i) = a + bi.$$

Es folgt, dass $a = b = 0$ gilt, und somit $r = 0$. Also ist bereits $p = f \cdot (X^2+1) \in (X^2+1)$. □

Damit ergibt sich, dass φ einen Ringisomorphismus

$$\overline{\varphi}\colon \mathbb{R}[X]/(X^2+1) \to \mathbb{C}, \quad p \mapsto p(i)$$

induziert. Dieser Isomorphismus kann so verstanden werden, dass $\mathbb{C}$ aus $\mathbb{R}$ durch hinzufügen eines Elements $\overline{X}$ mit $\overline{X}^2 + 1 = 0$ entsteht, wobei $\overline{X}$ der üblichen komplexen Zahl i entspricht.

2. Es sei

$$\mathcal{C} \coloneqq \{(a_n)_{n\in\mathbb{N}} \mid a_n \in \mathbb{Q} \text{ für alle } n \in \mathbb{N}, (a_n)_{n\in\mathbb{N}} \text{ ist eine Cauchyfolge}\}$$

der Raum der rationalen Cauchyfolgen. Sind $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$ zwei rationale Cauchyfolgen, so sind auch $(a_n+b_n)_{n\in\mathbb{N}}$ und $(a_n \cdot b_n)_{n\in\mathbb{N}}$ rationale Cauchyfolgen. Zusammen mit dieser Addition und Multiplikation bildet $\mathcal{C}$ einen kommutativen Ring; das Einselement ist durch die konstante 1-Folge $(1)_{n\in\mathbb{N}}$ gegeben ($\mathcal{C}$ enthält alle konstanten Folgen, da diese insbesondere konvergent und somit Cauchy sind).

Da jede rationale Cauchyfolge in $\mathbb{R}$ kovergiert, ergibt sich eine wohldefinierte Abbildung

$$\lim\colon \mathcal{C} \to \mathbb{R}, \quad (a_n)_{n\in\mathbb{N}} \mapsto \lim_{n\to\infty} a_n.$$

Die Abbildung lim ist ein Ringhomomorphismus, denn für alle $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$ gilt

$$\begin{aligned}\lim((a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}}) &= \lim((a_n+b_n)_{n\in\mathbb{N}}) = \lim_{n\to\infty}(a_n+b_n) \\ &= \Big(\lim_{n\to\infty} a_n\Big) + \Big(\lim_{n\to\infty} b_n\Big) = \lim((a_n)_{n\in\mathbb{N}}) + \lim((b_n)_{n\in\mathbb{N}}).\end{aligned}$$

und

$$\begin{aligned}\lim((a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}}) &= \lim((a_n b_n)_{n\in\mathbb{N}}) = \lim_{n\to\infty}(a_n b_n)\\ &= \left(\lim_{n\to\infty} a_n\right) \cdot \left(\lim_{n\to\infty} b_n\right) = \lim((a_n)_{n\in\mathbb{N}}) \cdot \lim((b_n)_{n\in\mathbb{N}}).\end{aligned}$$

Da jede reelle Zahl als Grenzwert einer rationalen Cauchyfolge geschrieben werden kann (dies ist gerade die Dichtheit von $\mathbb{Q}$ in $\mathbb{R}$), ist lim surjektiv. Außerdem gilt

$$\ker \lim = \{(a_n)_{n\in\mathbb{N}} \in \mathcal{C} \mid \lim((a_n)_{n\in\mathbb{N}}) = 0\} = \left\{(a_n)_{n\in\mathbb{N}} \in \mathcal{C} \,\middle|\, \lim_{n\to\infty} a_n = 0\right\},$$

d.h. der Kern von lim besteht aus genau den rationalen Cauchyfolgen, die auch Nullfolgen sind. Da aber jede Nullfolge bereits eine Cauchyfolge ist, ist der Kern von lim durch

$$N \coloneqq \{(a_n)_{n\in\mathbb{N}} \mid a_n \in \mathbb{Q} \text{ für alle } n \in \mathbb{N}, a_n \to 0 \text{ für } n \to \infty\}$$

gegeben. Somit ist N ein Ideal in $\mathcal{C}$, und lim induziert einen Isomorphismus von Ringen

$$\mathcal{C}/N \to \mathbb{R}, \quad \overline{(a_n)_{n\in\mathbb{N}}} \mapsto \lim_{n\to\infty} a_n.$$

Dies führt dazu, dass sich die reellen Zahlen als Äquivalenzklassen von rationalen Cauchyfolgen konstruieren lassen, wobei zwei rationale Cauchyfolgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ genau dann äquivalent sind, wenn $(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}}$ eine Nullfolge ist.