9. Ringhomomorphismen

Definition: Es seien R und S zwei Ringe. Eine Abbildung $\varphi : R \to S$ mit den beiden Eigenschaften $\varphi(a+b) = \varphi(a) + \varphi(b)\ \forall a,b \in R$ und $\varphi(ab) = \varphi(a)\varphi(b)\ \forall a,b \in R$ wird (Ring)Homomorphismus genannt. Ein Homomorphismus φ wird Monomorphismus (bzw. Epimorphismus bzw. Isomorphismus) genannt, wenn φ injektiv (bzw. surjektiv bzw. bijektiv) ist. Gilt $R = S$ (d.h. $\varphi : R \to R$), so wird φ Endomorphismus genannt. Ein bijektiver Endomorphismus wird Automorphismus genannt.

Beispiele: 1) Es seien R und S zwei Ringe. Die Abbildung $\varphi : R \to S$, $\varphi(x) = 0\ \forall x \in R$ ist ein Homomorphismus.
2) Es sei $m \in \mathbb{N} \setminus \{0,1\}$. Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(x) = \overline{x}$, die jeder ganzen Zahl x ihre Restklasse $\overline{x}$ modulo m zuordnet, ist ein Epimorphismus (siehe Zahlentheorie).
3) Ist allgemeiner R ein Ring und I ein Ideal von R, so ist $\pi : R \to R/I$, $\pi(x) = x + I$ ein Epimorphismus, da $\pi(x+y) = (x+y)+I = (x+I)+(y+I) = \pi(x)+\pi(y)$ und $\pi(xy) = xy + I = (x+I)(y+I) = \pi(x)\pi(y)$ für alle $x, y \in R$. (Für $R = \mathbb{Z}$ und $I = (m)$ erhält man das vorangegangene Beispiel.)
4) Ist R ein Ring mit Eins, so ist $\varphi : \mathbb{Z} \to R$, $\varphi(n) = n \cdot 1_R$ ein Homomorphismus, denn

$$\varphi(m+n) = (m+n)\cdot 1_R \overset{\text{Satz 7 (iii)}}{=} m \cdot 1_R + n \cdot 1_R = \varphi(m) + \varphi(n)$$

und

$$\begin{aligned}\varphi(m \cdot n) = (m \cdot n) \cdot 1_R &\overset{\text{Satz 8 (iii)}}{=} m \cdot (n \cdot 1_R) = m \cdot \big(1_R \cdot (n \cdot 1_R)\big) \\ &\overset{\text{Satz 48 (v)}}{=} (m \cdot 1_R)\cdot(n \cdot 1_R) = \varphi(m)\cdot\varphi(n)\end{aligned}$$

für alle $m, n \in \mathbb{Z}$. Diese Abbildung ist im allgemeinen weder injektiv noch surjektiv. Für $R = \mathbb{Z}_2$ ist sie z.B. nicht injektiv und für $R = \mathbb{Q}$ nicht surjektiv.
5) Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ ist ein Automorphismus.
6) Bezeichnet

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

mit der üblichen Addition und Multiplikation von Matrizen, so ist

$$\varphi : \mathbb{C} \to R,\ \varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

(mit $a, b \in \mathbb{R}$) ein Isomorphismus.
7) Es sei $d \in \mathbb{Z}$, $d > 1$ quadratfrei. Dann ist $\varphi : \mathbb{Z}\big[\sqrt{d}\big] \to \mathbb{Z}\big[\sqrt{d}\big]$, $\varphi\big(a + b\sqrt{d}\big) = a - b\sqrt{d}$ ein Automorphismus.
8) Es sei $\mathcal{P}$ der Ring aller reellen Polynomfunktionen (mit punktweiser Addition und Multiplikation) und $\alpha \in \mathbb{R}$. Dann ist $\varphi_\alpha : \mathcal{P} \to \mathbb{R}$, $p \mapsto p(\alpha)$ ein Epimorphismus.

9) Es sei V ein endlichdimensionaler K-Vektorraum mit Dimension $n = \dim_K V$ und $\mathrm{End}(V) = \{\varphi : V \to V \mid \varphi \text{ ist } K\text{-linear}\}$. Die Abbildung $\Phi : \mathrm{End}(V) \to M_n(K)$, die jeder linearen Abbildung $\varphi \in \mathrm{End}(V)$ ihre Matrixdarstellung bezüglich einer fest gewählten Basis von V zuordnet, ist ein Isomorphismus (siehe Lineare Algebra).

Bemerkungen: 1) Jeder Ringhomomorphismus $\varphi : R \to S$ ist ein Gruppenhomomorphismus der abelschen Gruppen $(R, +)$ und $(S, +)$. Daher gelten (laut Lemma 22) $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)\ \forall a \in R$ und $\varphi(na) = n\varphi(a)\ \forall n \in \mathbb{Z}\ \forall a \in R$.
2) Sind R und S zwei Ringe mit Eins und $\varphi : R \to S$ ein Homomorphismus, so muss nicht gelten, dass $\varphi(1_R) = 1_S$. Ist z.B. $R = \mathbb{Z}$, $S = \mathbb{Z} \times \mathbb{Z}$ (mit komponentenweiser Addition und Multiplikation und Einselement $(1, 1)$) und $\varphi(a) = (a, 0)$, so ist φ ein Homomorphismus mit $\varphi(1) = (1, 0) \neq (1, 1)$.
3) Sind R und S zwei Ringe mit Eins und $\varphi : R \to S$ ein Homomorphismus, so muss nicht gelten, dass $\varphi(R^*) \subseteq S^*$, d.h. das Bild einer Einheit in R muss keine Einheit in S sein. Als Gegenbeispiel kann das aus der vorangegangenen Bemerkung dienen. Dabei ist $1 \in R^*$ aber $\varphi(1) = (1, 0) \notin S^*$.

Lemma 62: (i) Ist R ein Ring mit Eins, S ein Ring und $\varphi : R \to S$ ein Homomorphismus, so gilt $b \cdot \varphi(1_R) = \varphi(1_R) \cdot b = b\ \forall b \in \mathrm{Im}\,\varphi$.
(ii) Ist R ein Ring mit Eins, S ein Ring und $\varphi : R \to S$ ein Epimorphismus, so ist auch S ein Ring mit Eins und $1_S = \varphi(1_R)$.
(iii) Sind R und S Ringe mit Eins und $\varphi : R \to S$ ein Epimorphismus, so gilt $\varphi(1_R) = 1_S$.

Beweis: (i) Ist $b \in \mathrm{Im}\,\varphi$, so $\exists a \in R : \varphi(a) = b$ und daher
$$b \cdot \varphi(1_R) = \varphi(a) \cdot \varphi(1_R) = \varphi(a \cdot 1_R) = \varphi(a) = b$$
und analog $\varphi(1_R) \cdot b = b$.
(ii) Aus (i) und der Surjektivität von φ folgt $b \cdot \varphi(1_R) = \varphi(1_R) \cdot b = b\ \forall b \in S$. Daher ist $\varphi(1_R)$ Einselement von S, d.h. S ist ein Ring mit Eins und $1_S = \varphi(1_R)$.
(iii) Folgt sofort aus (ii).

Lemma 63: (i) Es sei R ein Ring mit Eins, S ein Ring, in dem 0_S der einzige Links- bzw. Rechtsnullteiler ist und $\varphi : R \to S$ ein Homomorphismus mit der Eigenschaft, dass $\exists a \in R : \varphi(a) \neq 0$. Dann ist auch S ein Ring mit Eins und $1_S = \varphi(1_R)$.
(ii) Es sei R ein Ring mit Eins, S ein Integritätsbereich und $\varphi : R \to S$ ein Homomorphismus mit der Eigenschaft, dass $\exists a \in R : \varphi(a) \neq 0$. Dann gilt $\varphi(1_R) = 1_S$.

Beweis: (i) Aus $\varphi(1_R) \cdot \varphi(a) = \varphi(1_R \cdot a) = \varphi(a) \neq 0$ folgt $\varphi(1_R) \neq 0$. Für $b \in S$ gilt nun $\varphi(1_R) \cdot b = \varphi(1_R^2) \cdot b = \varphi(1_R)^2 \cdot b$ und daher
$$\varphi(1_R) \cdot \big(\varphi(1_R) \cdot b - b\big) = \varphi(1_R)^2 \cdot b - \varphi(1_R) \cdot b = 0.$$

Da $\varphi(1_R) \neq 0$, ist $\varphi(1_R) \cdot b - b = 0$ und daher $\varphi(1_R) \cdot b = b$. Die Gleichung $b \cdot \varphi(1_R) = b$ kann man analog zeigen. Also ist S ein Ring mit Eins und $\varphi(1_R)$ ist Einselement von S.
(ii) Folgt sofort aus (i).

Lemma 64: Es seien R und S zwei Ringe mit Eins und $\varphi : R \to S$ ein Homomorphismus mit der Eigenschaft $\varphi(1_R) = 1_S$. Dann ist $\varphi(R^*) \subseteq S^*$ und $\varphi(a^{-1}) = \varphi(a)^{-1}$ $\forall a \in R^*$.

Beweis: Für $a \in R^*$ ist
$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(1_R) = 1_S$$
und analog $\varphi(a^{-1}) \cdot \varphi(a) = 1_S$. Also ist $\varphi(a) \in S^*$ und $\varphi(a)^{-1} = \varphi(a^{-1})$.

Lemma 65: Es seien R, S und T drei Ringe und $\varphi : R \to S$ und $\psi : S \to T$ zwei Abbildungen. Sind φ und ψ Homomorphismen (bzw. Monomorphismen bzw. Epimorphismen bzw. Isomorphismen), so ist auch $\psi \circ \varphi : R \to T$ ein Homomorphismus (bzw. Monomorphismus bzw. Epimorphismus bzw. Isomorphismus).

Beweis: Sind φ und ψ Homomorphismen, so ist
$$(\psi \circ \varphi)(a \cdot b) = \psi\big(\varphi(a \cdot b)\big) = \psi\big(\varphi(a) \cdot \varphi(b)\big) = \psi\big(\varphi(a)\big) \cdot \psi\big(\varphi(b)\big) = (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)$$
für alle $a, b \in R$. Der Rest der Behauptung folgt aus Lemma 23, da man φ und ψ auch als Gruppenhomomorphismen der drei abelschen Gruppen $(R, +)$, $(S, +)$ und $(T, +)$ auffassen kann.

Lemma 66: Es seien R und S Ringe und $\varphi : R \to S$ ein Homomorphismus.
(i) Ist φ ein Isomorphismus, so ist auch die Umkehrabbildung $\varphi^{-1} : S \to R$ ein Isomorphismus.
(ii) φ ist genau dann ein Isomorphismus, wenn es einen Homomorphismus $\psi : S \to R$ mit den Eigenschaften $\psi \circ \varphi = \mathrm{id}_R$ und $\varphi \circ \psi = \mathrm{id}_S$ gibt.

Beweis: (i) Nach Lemma 24 (i) ist $\varphi^{-1} : S \to R$ ein Gruppenisomorphismus der abelschen Gruppen $(S, +)$ und $(R, +)$. Außerdem gilt: Sind $b_1, b_2 \in S$, so $\exists! a_1, a_2 \in R : \varphi(a_1) = b_1$ und $\varphi(a_2) = b_2$. Daher ist
$$\varphi^{-1}(b_1 \cdot b_2) = \varphi^{-1}\big(\varphi(a_1) \cdot \varphi(a_2)\big) = \varphi^{-1}\big(\varphi(a_1 \cdot a_2)\big) = a_1 \cdot a_2 = \varphi^{-1}(b_1) \cdot \varphi^{-1}(b_2),$$
d.h. $\varphi^{-1} : S \to R$ ist auch ein Ringhomomorphismus.
(ii) Analog zum Beweis von Lemma 24 (ii).

Lemma 67: Es seien R und S zwei Ringe und $\varphi : R \to S$ ein Homomorphismus.

(i) Ist T ein Unterring von R, so ist $\varphi(T)$ ein Unterring von S.
(ii) Ist U ein Unterring von S, so ist $\varphi^{-1}(U)$ ein Unterring von R.
(iii) Ist I ein Ideal von R und φ surjektiv, so ist $\varphi(I)$ ein Ideal von S.
(iv) Ist J ein Ideal von S, so ist $\varphi^{-1}(J)$ ein Ideal von R.

Beweis: (i) Sind $b_1, b_2 \in \varphi(T)$, so $\exists a_1, a_2 \in T : \varphi(a_1) = b_1$ und $\varphi(a_2) = b_2$. Daraus folgt $a_1 - a_2, a_1 \cdot a_2 \in T$ und daher $b_1 - b_2 = \varphi(a_1) - \varphi(a_2) = \varphi(a_1 - a_2) \in \varphi(T)$ und $b_1 \cdot b_2 = \varphi(a_1) \cdot \varphi(a_2) = \varphi(a_1 \cdot a_2) \in \varphi(T)$. Die Behauptung folgt aus Satz 52.
(ii) Sind $a_1, a_2 \in \varphi^{-1}(U)$, so $\varphi(a_1), \varphi(a_2) \in U$. Daher $\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) \in U$ und $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2) \in U$ und somit $a_1 - a_2, a_1 \cdot a_2 \in \varphi^{-1}(U)$.
(iii) Nach (i) ist $\varphi(I)$ ein Unterring von S. Ist $y \in S$ und $b \in \varphi(I)$, so $\exists x \in R : \varphi(x) = y$ (da φ surjektiv ist) und $\exists a \in I : \varphi(a) = b$. Da I ein Ideal ist, folgt $x \cdot a, a \cdot x \in I$ und daher $y \cdot b = \varphi(x) \cdot \varphi(a) = \varphi(x \cdot a) \in \varphi(I)$ und $b \cdot y = \varphi(a) \cdot \varphi(x) = \varphi(a \cdot x) \in \varphi(I)$.
(iv) Nach (ii) ist $\varphi^{-1}(J)$ ein Unterring von R. Ist $x \in R$ und $a \in \varphi^{-1}(J)$, so ist $\varphi(x) \in S$ und $\varphi(a) \in J$ und daher $\varphi(x \cdot a) = \varphi(x) \cdot \varphi(a) \in J$ und $\varphi(a \cdot x) = \varphi(a) \cdot \varphi(x) \in J$, d.h. $x \cdot a, a \cdot x \in \varphi^{-1}(J)$.

Definition: Es seien R und S zwei Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann werden $\ker \varphi := \{x \in R \mid \varphi(x) = 0\} = \varphi^{-1}\big(\{0\}\big)$ der Kern von φ und $\operatorname{Im} \varphi = \varphi(R)$ das Bild von φ genannt. (D.h. der Kern von φ ist der Kern von φ aufgefasst als Gruppenhomomorphismus der abelschen Gruppen $(R, +)$ und $(S, +)$.)

Lemma 68: Es seien R und S zwei Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann gelten

(i) $\ker \varphi$ ist ein Ideal von R und $\operatorname{Im} \varphi$ ein Unterring von S,
(ii) φ ist ein Monomorphismus $\Leftrightarrow \ker \varphi = \{0\}$.

Beweis: (i) Die erste Behauptung folgt aus $\ker \varphi = \varphi^{-1}\big(\{0\}\big)$ und Lemma 67 (iv), die zweite aus Lemma 67 (i).
(ii) Folgt sofort aus Lemma 26 (ii), da man φ als Gruppenhomomorphismus der abelschen Gruppen $(R, +)$ und $(S, +)$ auffassen kann.

Beispiele: 1) Es sei $m \in \mathbb{N} \setminus \{0, 1\}$. Der Kern der Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(x) = \overline{x}$, die jeder ganzen Zahl x ihre Restklasse $\overline{x}$ modulo m zuordnet, ist $\ker \varphi = m\mathbb{Z} = (m)$.
2) Ist allgemeiner R ein Ring und I ein Ideal von R, so ist der Kern der Abbildung $\pi : R \to R/I$, $\pi(x) = x + I$ das Ideal $\ker \pi = I$ (denn $x \in \ker \varphi \Leftrightarrow \pi(x) = I \Leftrightarrow x + I = I \Leftrightarrow x \in I$).
3) Es sei $\mathcal{P}$ der Ring aller reellen Polynomfunktionen (mit punktweiser Addition und Multiplikation) und $\alpha \in \mathbb{R}$. Der Kern des Homomorphismus $\varphi_\alpha : \mathcal{P} \to \mathbb{R}$, $p \mapsto p(\alpha)$ ist das Ideal $I_\alpha = \{p \in \mathcal{P} \mid p(\alpha) = 0\}$ aller Polynome, die im Punkt α eine Nullstelle besitzen.

Definition: Zwei Ringe R und S heißen isomorph, wenn es einen (Ring)Isomorphismus $\varphi : R \to S$ gibt. Man schreibt dafür $R \cong S$.

Bemerkung: Auch Isomorphie von Ringen besitzt alle Eigenschaften einer Äquivalenzrelation. Das kann völlig analog wie im Fall von Gruppen begründet werden.

Beispiele: 1) Bezeichnet
$$R = \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right) \,\middle|\, a, b \in \mathbb{R} \right\}$$
mit der üblichen Addition und Multiplikation von Matrizen, so ist $R \cong \mathbb{C}$. (Ein Isomorphismus wurde in Bsp. 6 am Beginn des Abschnitts angegeben.)
2) Es sei V ein endlichdimensionaler K-Vektorraum mit Dimension $n = \dim_K V$ und $\operatorname{End}(V) = \{\varphi : V \to V \mid \varphi \text{ ist } K\text{-linear}\}$. Dann ist $\operatorname{End}(V) \cong M_n(K)$. (Ein Isomorphismus wurde in der Linearen Algebra bzw. in Bsp. 9 am Beginn des Abschnitts angegeben.)

Satz 69: Es seien R und S zwei Ringe, $\varphi : R \to S$ ein Homomorphismus und I ein Ideal von R mit der Eigenschaft $I \subseteq \ker \varphi$. Dann gibt es genau einen Homomorphismus $\overline{\varphi} : R/I \to S$, sodass $\overline{\varphi} \circ \pi = \varphi$, wobei $\pi : R \to R/I$, $\pi(a) = a + I$ (d.h. $\overline{\varphi}(a + I) = \varphi(a)\ \forall a \in R$). Dabei gelten $\operatorname{Im} \overline{\varphi} = \operatorname{Im} \varphi$ und $\ker \overline{\varphi} = (\ker \varphi)/I$. Weiters ist $\overline{\varphi}$ ein Isomorphismus genau dann wenn φ ein Epimorphismus ist und $I = \ker \varphi$.

Beweis: Nach dem Beweis von Satz 27 ist $\overline{\varphi} : R/I \to S$, $\overline{\varphi}(a + I) = \varphi(a)$ wohldefiniert und der eindeutig bestimmte Gruppenhomomorphismus von $(R/I, +)$ nach $(S, +)$ mit der Eigenschaft $\overline{\varphi} \circ \pi = \varphi$. Wegen
$$\overline{\varphi}\big((a + I)(b + I)\big) = \overline{\varphi}(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a + I)\overline{\varphi}(b + I)\ \forall a, b \in R$$
ist $\overline{\varphi}$ auch ein Ringhomomorphismus. Die übrigen Behauptungen folgen aus Satz 27.

Korollar 70 (Homomorphiesatz): Es seien R und S zwei Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann gilt $R/\ker \varphi \cong \operatorname{Im} \varphi$. Ist φ ein Epimorphismus, so gilt $R/\ker \varphi \cong S$.

Beweis: Das folgt durch Anwendung von Satz 69 mit $I = \ker \varphi$.

Beispiele: 1) Ist R ein Ring, so gilt $R/R \cong \{0\}$, da $\varphi : R \to \{0\}$, $\varphi(x) = 0\ \forall x \in R$ ein Epimorphismus mit $\ker \varphi = R$ ist.
2) Ist R ein Ring, so ist $R/\{0\} \cong R$, da $\varphi : R \to R$, $\varphi(x) = x$ ein Epimorphismus mit $\ker \varphi = \{0\}$ ist.
3) Es sei $m \in \mathbb{N} \setminus \{0, 1\}$. Dann ist $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(a) = \overline{a}$ (wobei $\overline{a}$ die Restklasse von a modulo m bezeichnet) ein Epimorphismus mit $\ker \varphi = m\mathbb{Z} = (m)$ und daher $\mathbb{Z}/(m) \cong \mathbb{Z}_m$.
4) Es sei $\mathcal{P}$ der Ring aller reellen Polynomfunktionen (mit punktweiser Addition und Multiplikation) und $\alpha \in \mathbb{R}$. Dann ist $\varphi_\alpha : \mathcal{P} \to \mathbb{R}$, $p \mapsto p(\alpha)$ ein Epimorphismus mit Kern $\ker \varphi_\alpha = I_\alpha = \{p \in \mathcal{P} \mid p(\alpha) = 0\}$ und daher $\mathcal{P}/I_\alpha \cong \mathbb{R}$.

Lemma 71: Es sei R ein Ring und I und J zwei Ideale von R. Dann ist

$$I + J = \{a + b \mid a \in I, b \in J\}$$

ebenfalls ein Ideal von R.

Beweis: Nach Satz 29 (iii) ist $(I + J, +)$ eine Untergruppe von $(R, +)$. Ist $a \in I$, $b \in J$ und $x \in R$, so gelten $xa, ax \in I$ und $xb, bx \in J$ und daher $x(a + b) = xa + xb \in I + J$ und $(a + b)x = ax + bx \in I + J$.

Korollar 72 (1. Isomorphiesatz): Es sei R ein Ring und I und J zwei Ideale von R. Dann gilt

$$I/(I \cap J) \cong (I + J)/J.$$

Beweis: Die Abbildung $\varphi : I \to (I + J)/J$, $\varphi(a) = a + J$ ist ein Ringhomomorphismus, da sie Zusammensetzung der Einbettung $I \to I + J$, $a \mapsto a$ und des Epimorphismus $I + J \to (I + J)/J$, $a \mapsto a + J$ ist. Offenbar ist $\ker \varphi = I \cap J$. Ist $a \in I$ und $b \in J$, so ist $(a + b) + J = a + J = \varphi(a)$ und φ daher ein Epimorphismus. Die Behauptung folgt aus Korollar 70.

Satz 73: Es sei R ein Ring und I ein Ideal von R.
(i) Ist S ein Unterring von R mit der Eigenschaft $I \subseteq S$, so ist S/I ein Unterring von R/I.
(ii) Ist J ein Ideal von R mit der Eigenschaft $I \subseteq J$, so ist J/I ein Ideal von R/I.
(iii) Ist $\overline{S}$ ein Unterring von R/I, so gibt es einen Unterring S von R mit der Eigenschaft $I \subseteq S$, derart dass $S/I = \overline{S}$.
(iv) Ist $\overline{J}$ ein Ideal von R/I, so gibt es ein Ideal J von R mit der Eigenschaft $I \subseteq J$, derart dass $J/I = \overline{J}$.

Beweis: Die Abbildung $\pi : R \to R/I$, $\pi(a) = a + I$ ist ein Epimorphismus.
(i) Folgt durch Anwendung von Lemma 67 (i), da $S/I = \pi(S)$.
(ii) Folgt durch Anwendung von Lemma 67 (iii), da π surjektiv ist und $J/I = \pi(J)$.
(iii) Nach Lemma 67 (ii) ist $S = \pi^{-1}\big(\overline{S}\big)$ ein Unterring von R, der offenbar $I \subseteq S$ erfüllt. Da π surjektiv ist, gilt $S/I = \pi(S) = \pi\big(\pi^{-1}\big(\overline{S}\big)\big) = \overline{S}$.
(iv) Nach Lemma 67 (iv) ist $J = \pi^{-1}\big(\overline{J}\big)$ ein Ideal von R, das offenbar $I \subseteq J$ erfüllt. Da π surjektiv ist, gilt $J/I = \pi(J) = \pi\big(\pi^{-1}\big(\overline{J}\big)\big) = \overline{J}$.

Beispiel: Da $\mathbb{Z}$ ein Hauptidealring ist, haben die Ideale des Rings $\mathbb{Z}/(12)$ nach Satz 73 (iv) die Gestalt $(m)/(12)$, wobei $(12) \subseteq (m)$ gelten muss. Da die letzte Bedingung offenbar zu $m \mid 12$ äquivalent ist und 12 genau die nichttrivialen positiven Teiler $2, 3, 4$ und 6 besitzt, sind die (nichttrivialen) Ideale von $\mathbb{Z}/(12)$ gerade $(2)/(12)$, $(3)/(12)$, $(4)/(12)$ und $(6)/(12)$.

Korollar 74 (2. Isomorphiesatz): Es sei R ein Ring und I und J zwei Ideale von R mit der Eigenschaft $I \subseteq J$. Dann gilt

$$(R/I)\big/(J/I) \cong R/J.$$

Beweis: Betrachte den Epimorphismus $\varphi : R \to R/J$, $\varphi(a) = a + J$. Da $I \subseteq J = \ker \varphi$, gibt es nach Satz 69 einen Homomorphismus $\overline{\varphi} : R/I \to R/J$, $\overline{\varphi}(a + I) = a + J$. Da $\operatorname{Im} \overline{\varphi} = \operatorname{Im} \varphi = R/J$, ist $\overline{\varphi}$ surjektiv und $\ker \overline{\varphi} = (\ker \varphi)/I = J/I$. Die Behauptung folgt aus Korollar 70.

Beispiel: Es seien $m, n \in \mathbb{N} \setminus \{0, 1\}$, sowie $d = \mathrm{ggT}(m, n)$ und $\ell = \mathrm{kgV}(m, n)$. Verwendet man die Identitäten $(m) \cap (n) = (\ell)$ und $(m) + (n) = (d)$ aus der Zahlentheorie, so folgt aus Korollar 72

$$(m)/(\ell) = (m)\big/\big((m) \cap (n)\big) \cong \big((m) + (n)\big)\big/(n) = (d)/(n).$$

Gilt zusätzlich $m \mid n$ (und daher $(n) \subseteq (m)$), so folgt aus Korollar 74

$$\big(\mathbb{Z}/(n)\big)\big/\big((m)/(n)\big) \cong \mathbb{Z}/(m).$$