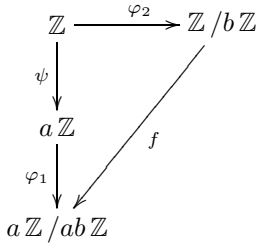
# Lösungen einiger Präsenzaufgaben II

**Aufgabe (P8).** *Sind* $\left(a\mathbb{Z}/ab\mathbb{Z},+\right)$ *und* $\left(\mathbb{Z}/b\mathbb{Z},+\right)$ *isomorph?*

*Lösung.* Da $\mathbb{Z}$ kommutativ ist, sind $ab\mathbb{Z}$ und $b\mathbb{Z}$ Normalteiler und folglich sind $a\mathbb{Z}/ab\mathbb{Z}$ und $\mathbb{Z}/b\mathbb{Z}$ Gruppen und die beiden Abbildungen $\varphi_1 : a\mathbb{Z} \to a\mathbb{Z}/ab\mathbb{Z}$, $z \mapsto [z]$ und $\varphi_2 : \mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, $z \mapsto [z]$ nach §4 Satz 11 a) surjektive Gruppenmorphismen.

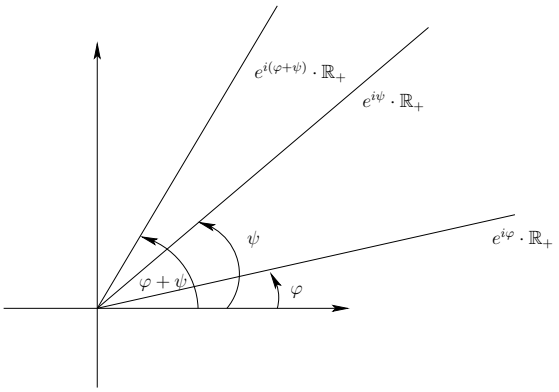



Da $\psi : \mathbb{Z} \to a\mathbb{Z}$, $z \mapsto az$ nach §3 Beobachtung 2 a) ebenfalls ein surjektiver Gruppenmorphismus ist (beachte die additive Schreibweise) ist dies auch $\varphi_1 \circ \psi$.
Es ist nach §4 Satz 11 $\operatorname{Kern}(\varphi_2) = b\mathbb{Z}$ und $\operatorname{Kern}(\varphi_1) = ab\mathbb{Z}$. Da damit $\operatorname{Kern}(\varphi_1 \circ \psi) = \psi^{-1}(ab\mathbb{Z}) = b\mathbb{Z} = \operatorname{Kern}(\varphi_2)$, sind die beiden Gruppen nach dem Homomorphiesatz für Gruppen isomorph.

**Aufgabe (P9).** *Für einen Körper* $K$ *sei* $K^* = K \setminus \{0\}$. *Berechne* $\mathbb{R}^*/\mathbb{R}_+$, $\mathbb{C}^*/\mathbb{R}_+$ *und* $\mathbb{C}^*/\mathcal{K}$ *mit* $\mathcal{K} = \{z \in \mathbb{C} : |z| = 1\}$.

*Lösung.* Es ist $\mathbb{R}^*/\mathbb{R}_+ = \{\mathbb{R}_+, \mathbb{R}_-\}$, mit $[-1][-1] = [1][1] = [1]$, $[-1][1] = [-1][1] = [-1]$, also eine zyklische Gruppe der Ordnung 2.

Es ist $\mathbb{C}^*/\mathbb{R}_+ = \{e^{i\alpha} \cdot \mathbb{R}_+ : \alpha \in [0, 2\pi[\}$, die Menge aller Halbstrahlen, die von 0 ausgehen ohne diese zu enthalten.
Hierbei sieht die Verknüpfung auf $\mathbb{C}^*/\mathbb{R}_+$ wie folgt aus: $\left[re^{i\varphi}\right]\left[r'e^{i\psi}\right] = \left[e^{i(\varphi+\psi)}\right]$ für $r, r', \varphi, \psi \in \mathbb{R}$, d.h. zwei Halbstrahlen ergeben verknüpft den Halbstrahl, den man erhält, wenn man die beiden Winkel zwischen der positiven X-Achse und den Strahlen addiert und wiederum von der positiven X-Achse abträgt.




Die Gruppe $\mathbb{C}^*/\mathcal{K} = \{r \cdot \mathcal{K} : r \in [0, \infty[\}$ ist die Menge aller Kreise mit dem Zentrum in 0. Zwei Kreise ergeben dabei verknüpft den Kreis mit dem Radius, der das Produkt der beiden Radien der ursprünglichen Kreise ist.

**Aufgabe (P10).** *In Beispiel 3 des §5 wurde gezeigt:*

$$FG(x,y)/K \cong S_3 = \langle \tau, \sigma \rangle \text{ mit } \tau = (12), \sigma = (123), K = K(R) = \bigcap_{\substack{N \text{ Normalteiler} \\ R \subseteq N}} N, R = \{x^2, y^3, (xy)^2 = 1\}.$$

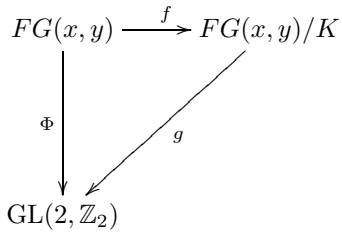
*Benutze dieses Vorwissen, um zu zeigen* $GL(2, \mathbb{Z}_2) \cong S_3$.

*Lösung.* Es wird $\mathrm{GL}(2, \mathbb{Z}_2)$ von den $(2 \times 2)$-Elementarmatrizen über $\mathbb{Z}_2$ erzeugt. Diese sind

$$S_1(1) = S_2(1) = E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ Q_2^1(1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},\ Q_1^2(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ P_1^2 = P_2^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Mit $u := P_1^2$ und $v := \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ gilt sogar $\mathrm{GL}(2, \mathbb{Z}_2) = \langle u, v \rangle$, da $uv = Q_1^2(1)$, $vu = Q_2^1$ und $u^2 = E_2$.

Es ist $u^2 = v^3 = (uv)^2 = E_2$.




Wir setzen $\varphi : \{x,y\} \to \{u,v\}$ durch $\varphi(x) = u$ und $\varphi(y) = v$ fest. Nach Definition 10 der Freiheit in §4 gibt es nun einen Morphismus $\Phi : F(x,y) \to \mathrm{GL}(2,\mathbb{Z}_2)$ mit $\Phi|_{\{x,y\}} = \varphi$. Dass $\Phi$ surjektiv ist, ist klar.
Da $\Phi(x^2) = (\Phi(x))^2 = (\varphi(x))^2 = u^2 = E_2$, genauso $\Phi(y^3) = v^3 = E_2$ und $\Phi\big((xy)^2\big) = (uv)^2 = E_2$, liegt $R$ in Kern $\Phi$ und damit auch $K \subset$ Kern $\Phi$, da Kern $\Phi$ selbst ein Normalteiler ist. Also gibt es nach Satz 9 in §4 einen surjektiven Gruppenmorphismus $g$ von $FG(x,y)/K$ auf $\mathrm{GL}(2,\mathbb{Z}_2)$.

Da $|\mathrm{Gl}(2,\mathbb{Z}_2)| = 6 = |S_3|$, also $g$ injektiv ist, folgt die Behauptung.

**Aufgabe (P11).** *Sei $f : R \to S$ ein surjektiver Ringmorphismus, $I$ Ideal in $R$, $J$ Ideal in $S$.*

*(a) Zeige: Ist $I$ ein maximales Ideal oder Primideal, so muss dieses nicht für $f(I)$ gelten.*

*(b) Zeige: Ist $I$ ein maximales Ideal oder Primideal mit* Kern $f \subset I$*, so ist auch $f(I)$ maximales Ideal bzw. Primideal.*

*(c) Zeige: Ist $J$ ein maximales Ideal oder Primideal, so ist dieses auch $f^{-1}(J)$.*

*Lösung.* Als erstes wiederholen wir noch einmal, dass $f(I)$ ein Ideal ist, wenn $I$ ein Ideal ist und $f$ ein surjektiver Ringmorphismus: Seien $a, b \in f(I)$, d.h. es gibt $a', b' \in I$ mit $f(a') = a$, $f(b') = b$. Da auch $a'+b' \in I$ liegt, gilt $f(a'+b') = f(a')+f(b') = a+b \in f(I)$. Sind $s, t \in S$ gegeben, so gibt es, da $f$ surjektiv ist, $s', t' \in R$ mit $f(s') = s$, $f(t') = t$. Da damit nun $s \cdot f(I) \cdot t = f(s') \cdot f(I) \cdot f(t') = f(s' \cdot I \cdot t) = f(I)$ für beliebiges $s \in S$ gilt, ist $f(I)$ ein Ideal in $S$.

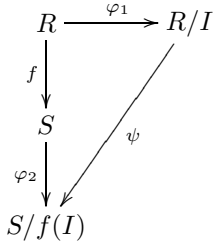
Ebenso ist $f^{-1}(J)$ ein Ideal, wenn $J$ ein Ideal ist: Für $a, b \in f^{-1}(J)$ liegen $f(a)$ und $f(b)$ in $J$, also auch $f(a)+f(b) = f(a+b) \in J$. Da damit $a+b \in f^{-1}(J)$, ist gezeigt, dass $f^{-1}(J)$ eine Untergruppe von $(R,+,0)$ ist. Da für alle $r, s \in R$ die Gleichung $r \cdot f^{-1}(J) \cdot s \subseteq f^{-1}(f(r)) \cdot f^{-1}(J) \cdot f^{-1}(f(s)) = f^{-1}(f(r) \cdot J \cdot f(s)) = f^{-1}(J)$ gilt, ist $f^{-1}(J)$ ein Ideal.

(a) Gegenbeispiel 1: Das Ideal $3\,\mathbb{Z}$ ist ein maximales Ideal in $\mathbb{Z}$, wird jedoch unter dem kanonischen Morphismus $f : \mathbb{Z} \to \mathbb{Z}/2\,\mathbb{Z}$ auf ganz $Z/2\,\mathbb{Z}$ abgebildet.

Gegenbeispiel 2: Da $\mathbb{Z}$ nullteilerfrei ist, ist $\{0\}$ ein Primideal. Betrachten wir den kanonischen Morphismus $f : \mathbb{Z} \to \mathbb{Z}/6\,\mathbb{Z}$, so ist das Bild $f(\{0\}) = \{0\}$ hier jedoch kein Primideal mehr, da $Z/6\,\mathbb{Z}$ nicht mehr nullteilerfrei ist. (Z.B. gilt $2 \cdot 3 = 0 \in \{0\}$, aber weder $2 \in \{0\}$ noch $3 \in \{0\}$).

(b) Sei $I$ maximal und $J \supsetneq f(I)$ ein Ideal in $S$. Da $f$ surjektiv ist, ist auch $f^{-1}(J) \supsetneq f^{-1}(f(I)) = I$. Dabei folgt das letzte Gleichheitszeichen aus Satz 7.3 a) und der Voraussetzung Kern $f \subset I$. Also ist $f^{-1}(J) = R$, da $I$ maximal ist und damit $f(J) = S$, da $f$ surjektiv.

Sei $I$ ein Primideal. Wir betrachten das folgende kommutative Diagramm:




Dabei seien $\varphi_1$, $\varphi_2$ die entsprechenden kanonischen Ringmorphismen. Es ist Kern $(\varphi_2 \circ f) = f^{-1}(f(I))$. Mit dem selben Satz 7.3 a) folgt wie eben $f^{-1}(f(I)) = I$.
Da also $\varphi_2 \circ f$ ein surjektiver Ringmorphismus ist mit Kern $(\varphi_2 \circ f) =$ Kern $(\varphi_1)$, gilt nach Satz 7.4 b) $S/f(I) \cong R/I$. Da $I$ Primideal ist, ist $R/I$ nach 7.14 a) nullteilerfrei. Da damit auch $S/f(I)$ nullteilerfrei ist, liefert der selbe Satz nun, dass $f(I)$ ein Primideal ist.

(c) Sei $J$ ein Primideal. Dann gilt für $a, b \in R$ mit $ab \in f^{-1}(J)$, dass $f(a)f(b) = f(ab) \in J$ liegt, also entweder $f(a) \in J$ oder $f(b) \in J$, d.h. $a \in f^{-1}(J)$ oder $b \in f^{-1}(J)$.

Sei nun $J$ maximal. Ist nun $I$ ein Ideal in $R$ mit $I \supsetneq f^{-1}(J)$, so ist auch $f(I) \supsetneq J$. Da $J$ ein maximales Ideal ist folgt $f(I) = S$. Da $I \supsetneq f^{-1}(J) \supset$ Kern $f$ und es nach Satz 7.3 a) eine durch $f$ induzierte Bijektion zwischen den Idealen in $R$, die Kern $f$ enthalten, und den Idealen in $S$ gibt, folgt $I = S$.

**Aufgabe (P12).**

*(a) Für eine Primzahl $p$ ist $\mathbb{Q}_{(p)} = \{\frac{z}{n} \ : \ z \in \mathbb{Z}, n \in \mathbb{N}_+, p \nmid n\}$ ein Ring mit genau einem maximalen Ideal $M$. Betrachte $\mathbb{Q}_{(p)}/M$.*

*(b) Konstruiere einen Unterring von $\mathbb{Q}$ mit genau zwei maximalen Idealen.*

*Lösung.*

(a) $M := \left\{\frac{pz}{n} \ : \ z \in \mathbb{Z}, n \in \mathbb{N}_+, p \nmid n\right\}$ ist ein Ideal in $\mathbb{Q}_{(p)}$, da für $z, z' \in \mathbb{Z}$, $n, n' \mathbb{N}_+$, $p \nmid n$, $p \nmid n'$ gilt:

$$\frac{pz}{n} + \frac{pz'}{n'} = \frac{p(zn' + z'n)}{nn'} \in M \quad \text{und} \quad \frac{pz}{n} \cdot \frac{z'}{n'} = \frac{pzz'}{nn'}.$$

$M$ ist ein maximales Ideal. Gilt nämlich $I \supsetneq M$, dann enthält $I$ eine Einheit, da jedes Element in $Q_{(p)} \setminus M$ invertierbar ist. Also ist $I$ schon gleich dem ganzen Ring $Q_{(p)}$.

Es kann kein weitere maximales Ideal geben, da $Q_{(p)} \setminus M$ nur aus Einheiten besteht, d.h. für jedes Ideal $I$ liegt entweder in $M$ oder ist gleich $Q_{(p)}$.

Der Faktorring $\mathbb{Q}_{(p)}/M$ ist isomorph zu $\mathbb{Z}_p$, denn:

In $\mathbb{Q}_{(p)}/M$ ist $p \cdot 1 = 0$, womit die 1 in der Gruppe $\left(\mathbb{Q}_{(p)}/M, +\right)$ nur die Ordnungen $p$ oder 1 haben kann (denn mehr Teiler hat $p$ als Primzahl nicht). Da jedoch $1 \notin M$ ist, muss die Ordnung $p$ sein. Damit enthält $\mathbb{Q}_{(p)}/M$ mindestens die $p$ verschiedenen Elemente $0 + M$, $1 + M$, $\ldots$, $(p-1) + M$.

Sei $\frac{z}{n} \in \mathbb{Q}_{(p)}$. Dann gilt $k + M = \frac{z}{n} + M \Leftrightarrow \frac{z-kn}{n} = \frac{z}{n} - k \in M \Leftrightarrow p \mid (z - kn)$ für beliebige $k \in \mathbb{Z}$. Diese Gleichung ist gerade äquivalent zu $\varrho_p(z) = \varrho_p(k) \odot \varrho_p(n)$ in $\mathbb{Z}_p$. Nun ist $\varrho_p(n) \neq 0$, womit es ein $x \in \mathbb{Z}_p$ gibt ($\mathbb{Z}_p$ ist ein Körper!) mit $\varrho_p(z) = x \odot \varrho_p(n)$. Mit $k = x$ gilt dann also $k + M = \frac{z}{n} + M$, womit $k$ und $\frac{z}{n}$ die gleiche Restklasse bezüglich $M$ haben.

Also enthält $\mathbb{Q}_{(p)}/M$ gerade die (paarweise verschiedenen) Elemente $0 + M$, $1 + M$, $\ldots$, $(p-1) + M$. Insbesondere ist damit $\left(\mathbb{Q}_{(p)}/M, +\right)$ zyklisch von der Primordnung $p$, und somit isomorph zum $(\mathbb{Z}_p, \oplus)$. Der Isomorphismus ist durch $\varphi : \mathbb{Z}_d \to \mathbb{Q}_{(p)}/M$, $x \mapsto x + M$ gegeben.

Man kann nun leicht nachrechnen, dass $\varphi$ ebenfalls ein Ringhomomorphismus ist (und somit ein Ringisomorphismus): Es ist

$$\varphi(ab) = \varrho_p(ab) + M = ab + M = (a + M)(b + M) = \varphi(a)\varphi(b)$$

und $\varphi(1) = 1 + M$.

(b) Seien $q, p$ zwei Primzahlen. Dann ist $\mathbb{Q}_{(p,q)} = \{\frac{z}{n} \ : \ z \in \mathbb{Z}, n \in \mathbb{N}_+, p \nmid n, q \nmid n\}$ ein Ring mit genau zwei maximalen Idealen.

Wie eben folgt, dass

$$M_p := \left\{\frac{pz}{n} \ : \ z \in \mathbb{Z}, n \in \mathbb{N}_+, p \nmid n, q \nmid n\right\} \text{ und } M_q := \left\{\frac{qz}{n} \ : \ z \in \mathbb{Z}, n \in \mathbb{N}_+, p \nmid n, q \nmid n\right\}$$

Ideale in $\mathbb{Q}_{(p,q)}$ sind.

Sei nun $I \supsetneq M_p$. Dann gibt es ein $\frac{z}{n} \in I$ mit $p \nmid z$. Gilt $q \nmid z$, so ist dies eine Einheit und somit $I = Q_{(p,q)}$. Gilt $q \mid z$ gibt es $a, b \in \mathbb{Z}$ mit $az + np = 1$ mit $p \nmid a$ und $q \nmid a$, da sonst $p \mid 1$ oder $q \mid 1$ folgen würde. Dann ist also $\frac{p}{a} \in M_p$, also auch $\frac{z}{n} + \frac{p}{a} = \frac{az+pn}{an} \in M_p$. Dies ist jedoch eine Einheit. Also ist auch in diesem Fall $I = Q_{(p,q)}$, d.h. $M_p$ ist ein maximales Ideal. Genauso folgt, dass $M_q$ ein maximales Ideal ist.