Musterlösung 6

Irreduzibilität in Polynomringe, Elementarteiler, Moduln

Erinnerung: ** bedeutet: Geht über den Standardstoff hinaus. Besprechen Sie Ihre Lösung mit Prof. Pink.

1. Zeige, dass die folgenden Polynome irreduzibel sind:
   (a) $\frac{1}{3}X^3 + \frac{5}{2}X^2 + 3X - 1 \in \mathbb{Q}[X]$
   (b) $X^3 + 8iX^2 - 6X - 1 + 3i \in \mathbb{Z}[i][X]$
   Hinweis: Benutze Serie 5, Aufgabe 1. (c).
   (c) $X^\ell + Y^m + Z^n \in \mathbb{C}[X, Y, Z]$ für beliebige $\ell, m, n \geqslant 1$.

   Lösung:

   (a) Sei $f(X) := \frac{1}{3}X^3 + \frac{5}{2}X^2 + 3X - 1$ und sei $g(X) := 6f(X) = 2X^3 + 15X^2 + 18X - 6 \in \mathbb{Z}[X]$, welches die Voraussetzungen an das Eisenstein-Kriterium für das Primelement $3 \in \mathbb{Z}$ erfüllt. Folglich ist g irreduzibel in $\mathbb{Z}[X]$. Nach einem Satz der Vorlesung ist g auch irreduzibel in $\mathbb{Q}[X]$. Da 6 eine Einheit in $\mathbb{Q}[X]$ ist, gilt $f \sim g$. Deshalb ist f irreduzibel.

   (b) Nach Serie 5, Aufgabe 1. (c) ist $-1 + 3i = (1 + i)(1 + 2i)$ eine Zerlegung in Primfaktoren in $\mathbb{Z}[i]$, wobei $1 + i$ und $1 + 2i$ nicht assoziiert sind. Da $\mathbb{Z}[i]$ faktoriell ist, gilt daher $(1 + i) \mid (-1 + 3i)$, aber $(1 + i)^2 \nmid -1 + 3i$. Wegen $2 = (1 + i)(1 - i)$ ist $1 + i$ auch ein Teiler von $8i$ und -6. Somit ist $X^3 + 8iX^2 - 6X - 1 + 3i$ nach dem Eisenstein-Kriterium für $p = 1 + i$ in $\mathbb{Z}[i][X]$ irreduzibel.

   (c) Wir betrachten $X^\ell + Y^m + Z^n$ als Polynom in $\mathbb{C}[Y, Z][X]$ mit konstantem Koeffizienten $Y^m + Z^n \in \mathbb{C}[Y, Z]$. Letzterer ist ein normiertes Polynom in $\mathbb{C}[Z][Y]$; er ist also ein Produkt von normierten irreduziblen Polynomen in $\mathbb{C}[Z][Y]$. Schreibe $Y^m + Z^n = \prod_i P_i(Y, Z)^{\mu_i}$ mit paarweise verschiedenen normierten irreduziblen Polynomen $P_i \in \mathbb{C}[Z][Y]$ mit $\deg_Y(P_i) \geqslant 1$ und Exponenten $\mu_i \geqslant 1$. Einsetzen von $Z = 1$ liefert dann $Y^m + 1 = \prod_i P_i(Y, 1)^{\mu_i}$ mit normierten Polynomen $P_i(Y, 1)$ vom Grad $\geqslant 1$ in $\mathbb{C}[Y]$. Aber das Polynom $Y^m + 1$ hat keine mehrfachen Nullstellen in $\mathbb{C}$. Deshalb müssen alle $\mu_i = 1$ sein.

   Wegen $m \geqslant 1$ besitzt das Polynom $Y^m + Z^n$ also einen irreduziblen Faktor P_i der Multiplizität 1. Mit diesem sind dann die Bedingungen des Eisensteinkriteriums für das Polynom $X^\ell + Y^m + Z^n \in \mathbb{C}[Y, Z][X]$ erfüllt. Daher ist dieses Polynom irreduzibel.

2. (a) *Lagrange-Interpolation:* Sei K ein Körper und seien $a_0, \ldots, a_m \in K$ paarweise verschieden. Zeige, dass es für alle $b_0, \ldots, b_m \in K$ genau ein Polynom $f \in K[X]$ vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$ gibt.

   Hinweis: Benutze die Vandermondsche Determinante oder betrachte für $0 \leqslant i \leqslant m$ die Polynome
$$\prod_{\substack{j=0\\ j\neq i}}^{m} \frac{X - a_j}{a_i - a_j}.$$

   (b) Zerlege $X^5 + X^4 + 1 \in \mathbb{Z}[X]$ in Primfaktoren mit folgendem Verfahren.

   Explizite Primfaktorzerlegung nach Kronecker: Sei $f \in \mathbb{Z}[X]$ ein primitives Polynom vom Grad n. Wir nehmen an, f habe eine (noch unbekannte) Faktorisierung $f = g \cdot h$ mit $g, h \in \mathbb{Z}[X]$ und $m := \deg(g) \leqslant \frac{n}{2}$. Um diese zu finden, wählen wir irgendwelche paarweise verschiedene $a_0, \ldots, a_m \in \mathbb{Z}$. Dann muss $g(a_i) | f(a_i)$ in $\mathbb{Z}$ für alle i gelten. Falls $f(a_i) = 0$ für ein i ist, kann $X - a_i$ von f abgespaltet werden und mit $\frac{f}{X-a_i}$ weiter gearbeitet werden. Andernfalls hat $f(a_i)$ für jedes i nur endlich viele Teiler in $\mathbb{Z}$. Für jedes System von Teilern $b_i | f(a_i)$ liefert (a) höchstens einen Kandidaten für g in $\mathbb{Z}[X]$ mit $g(a_i) = b_i$, für den man testet, ob er f teilt.

   *(c) Beschreibe einen analogen Algorithmus für Polynome in beliebig vielen Variablen über $\mathbb{Z}$.

Lösung:

(a) Sei P_m der K-Vektorraum der Polynome $f \in K[X]$ mit $\deg(f) \leqslant m$. Betrachte die K-lineare Abbildung
$$\alpha : \begin{array}{ccc} P_m & \longrightarrow & K^{m+1} \\ f & \longmapsto & (f(a_0), \ldots, f(a_m)) \end{array}.$$

Die Matrix von α bezüglich der Basis $\{1, X, X^2, \ldots, X^m\}$ von P_m und der Standardbasis von K^{m+1} ist
$$A = \begin{pmatrix} 1 & a_0 & \cdots & a_0^m \\ 1 & a_1 & \cdots & a_1^m \\ & & \vdots & \\ 1 & a_m & \cdots & a_m^m \end{pmatrix}.$$

Die Determinante von A ist gleich $\prod_{0 \leqslant i < j \leqslant m}(a_j - a_i)$ (Vandermondsche Determinante, siehe Lineare Algebra) und nach dieser Darstellung verschieden von Null, da $a_0, \ldots, a_m$ paarweise verschieden sind. Somit ist α als Isomorphismus von Vektorräumen bijektiv. Daher gibt es für alle $b_0, \ldots, b_m \in K$ genau ein Polynom $f \in P_m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$.

Variante: Betrachte für $0 \leqslant i \leqslant m$ die Polynome

$$f_i(X) := \prod_{\substack{j=0 \\ j\neq i}}^{m} \frac{X - a_j}{a_i - a_j} \in K[X]$$

vom Grad m. Sie erfüllen $f_i(a_i) = 1$ für alle i und $f_i(a_j) = 0$ für $j \neq i$. Daher ist für beliebige $b_0, \ldots, b_m \in K$

$$f := b_0 f_0 + \cdots b_m f_m \in K[X]$$

ein Polynom vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$.

Falls $g \in K[X]$ ein zweites Polynom vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle i ist, hat $f-g$ mindestens die $m+1$ Nullstellen $a_0, \ldots, a_m \in K$. Dies ist wegen $\deg(f-g) \leqslant m$ nur für $f - g = 0$ möglich. Somit ist f eindeutig.

(b) Als normiertes Polynom hat $f(X) := X^5 + X^4 + 1 \in \mathbb{Z}[X]$ eine Primfaktorzerlegung in normierte Polynome. Daher suchen wir nur normierte Teiler von f.

Wir prüfen zuerst nach, ob f einen normierten Teiler $g(X) := X - a$ vom Grad 1 hat, was äquivalent zur Existenz einer Nullstelle $a \in \mathbb{Z}$ von f ist. Für einen solchen Teiler g müsste $a = g(0) \mid f(0) = 1$, also $a = \pm 1$ gelten. Jedoch sind 1 und -1 keine Nullstellen von f. Somit hat f keine Teiler vom Grad 1.

Nun suchen wir normierte Teiler $g(X) := X^2 + aX + b$ vom Grad 2 von f. Wir wählen $a_0 := -1$, $a_1 := 0$ und $a_2 := 1$. Wegen $g(a_i) \mid f(a_i)$ für $i = 0, 1, 2$ muss $g(-1) \in \{\pm 1\}$, $g(1) \in \{\pm 1, \pm 3\}$ und $b = g(0) \in \{\pm 1\}$ gelten. Aus Letzterem und dem Ansatz für g folgt

$$g(-1) + g(1) = 2 + 2b \in \{0, 4\}.$$

Daher bleiben nur die Möglichkeiten

$$(g(-1), g(0), g(1)) = (g(-1), b, g(1)) = (-1, -1, 1), (1, -1, -1), (1, 1, 3).$$

Diese ergeben für g die Kandidaten $X^2 + X - 1$, $X^2 - X - 1$ und $X^2 + X + 1$. Mit Polynomdivision prüft man nach, dass davon nur $X^2 + X + 1$ ein Teiler von f ist und

$$f(X) = (X^2 + X + 1)(X^3 - X + 1)$$

gilt. Da f keine Teiler vom Grad 1 hat, können die in dieser Zerlegung auftretenden Faktoren nicht weiter zerlegt werden. Somit haben wir eine Primfaktorzerlegung von f gefunden.

*(c) Siehe van der Waerden, Algebra I§32.

3. Finde die Elementarteiler und die zugehörigen Matrizen U, V für die Matrix

$$A := \begin{pmatrix} 4 & 7 \\ 5 & 8 \\ 6 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 2}.$$

Lösung: Durch elementare Zeilen- und Spaltenoperationen bringen wir A in Elementarteilerform D:

$$\begin{pmatrix} 4 & 7 \\ 5 & 8 \\ 6 & 9 \end{pmatrix} \to \begin{pmatrix} 4 & 7 \\ 1 & 1 \\ 2 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 4 & 7 \\ 2 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} =: D$$

Wir haben dabei A von links mit

$$U := \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 5 & -4 & 0 \\ 1 & -2 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z})$$

und von rechts mit $V := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ multipliziert. Somit sind 1 und 3 die Elementarteiler von A und es ist

$$UAV = D.$$

4. Für jede natürliche Zahl ℓ und jede $(m \times n)$-Matrix A über einem Hauptidealring R sei $d_\ell(A)$ der grösste gemeinsame Teiler aller $(\ell \times \ell)$-Unterdeterminanten von A. Zeige, dass für alle Matrizen $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$ gilt $d_\ell(UAV) \sim d_\ell(A)$. Folgere, dass die Elementarteiler von A bis auf Assoziiertheit eindeutig bestimmt sind.

Lösung: We begin with the following lemma:

Lemma 1. *Consider matrices $A \in \mathrm{Mat}_{m\times n}(R)$ and $V \in \mathrm{Mat}_{n\times n'}(R)$ and an integer $1 \leqslant \ell \leqslant \min\{m, n'\}$. Then any $\ell \times \ell$-minor (i.e. subdeterminant) of AV is an R-linear combination of the $\ell \times \ell$-minors of A.*

Beweis. Consider the $\ell \times \ell$-submatrix M of AV obtained by selecting the rows $1 \leqslant i_1 < \ldots < i_\ell \leqslant m$ and the columns $1 \leqslant j_1 < \ldots < j_\ell \leqslant n'$. Then $M = A'V'$, where A' is obtained from A by selecting the rows $i_1, \ldots, i_\ell$, and V' is obtained from V by selecting the columns $j_1, \ldots, j_\ell$.

Let $\vec{x}_1, \ldots, \vec{x}_n$ denote the column vectors of A', and write $V' = (v'_{jk})_{j,k}$. Then for each $1 \leqslant k \leqslant \ell$ the k-th column vector of $A'V'$ is equal to $\sum_{j=1}^{n} v'_{jk}\vec{x}_j$. Using the multilinearity of the determinant with respect to column vectors, we obtain:

$$\det(A'V') = \sum_{j_1,\ldots,j_\ell=1}^{n} \left(\prod_{k=1}^{\ell} v'_{j_k k}\right) \cdot \det(\vec{x}_{j_1}, \ldots, \vec{x}_{j_\ell}).$$

Here $(\vec{x}_{j_1}, \ldots, \vec{x}_{j_\ell})$ has determinant zero if some of the indices $j_1, \ldots, j_\ell$ are equal. Otherwise it is obtained by interchanging columns in an $\ell \times \ell$-submatrix of A', and hence of A, and its determinant is $\pm$ an $\ell \times \ell$-minor of A. Thus $\det(M)$ is an R-linear combination of $\ell \times \ell$-minors of A, as desired. $\square$

Lemma 2. *Consider matrices $U \in \mathrm{Mat}_{m' \times m}(R)$ and $A \in \mathrm{Mat}_{m \times n}(R)$ and $V \in \mathrm{Mat}_{n \times n'}(R)$ and an integer $1 \leqslant \ell \leqslant \min\{m', n'\}$. Then any $\ell \times \ell$-minor of UAV is an R-linear combination of the $\ell \times \ell$-minors of A.*

Beweis. By Lemma 1 each $\ell \times \ell$-minor of UAV is an R-linear combination of the $\ell \times \ell$-minors of UA. Applying Lemma 1 to the matrices A^t and U^t shows that each of these is an R-linear combination of the $\ell \times \ell$-minors of A. $\square$

Now assume that $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$. Since $d_\ell(A)$ divides every linear combination of $\ell \times \ell$-minors of A, Lemma 2 implies that $d_\ell(A) \,|\, d_\ell(UAV)$. The same argument for (U^{-1}, UAV, V^{-1}) in place of (U, A, V) shows that $d_\ell(UAV) \,|\, d_\ell(A)$. Thus $d_\ell(UAV) \sim d_\ell(A)$, as desired.

Finally let U and V be as provided by the elementary divisor theorem, and let $e_1|e_2|...|e_k$ be the elementary divisors of A. Then for any $1 \leqslant \ell \leqslant k$ the top left $\ell \times \ell$-minor of UAV is $e_1 \cdots e_\ell$, and all others are zero. Thus $d_\ell(A) \sim d_\ell(UAV) \sim e_1 \cdots e_\ell$, and so $e_1 \cdots e_\ell$ is uniquely determined up to $\sim$ by A. Since $e_1, \ldots, e_k$ are non-zero, it follows that each e_ℓ is unique up to $\sim$.

5. Zeige: Für alle $n \geqslant 1$ und $a_1, \ldots, a_n$ in einem Hauptidealring R sind äquivalent:

   (a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$.

   (b) Es existiert eine Matrix in $\mathrm{GL}_n(R)$ mit erster Spalte $(a_1, \ldots, a_n)^T$.

   Lösung: Applying the elementary divisor theorem to the $n \times 1$-matrix $v := (a_1, \ldots, a_n)^T$ yields matrices $U \in \mathrm{GL}_n(R)$ and $V \in \mathrm{GL}_1(R) = R^\times$ such that $UvV = (e, 0 \ldots, 0)^T$ for some $e \in R$. Since v is not the zero vector, we have $e \neq 0$. By the preceding exercise we therefore have $e \sim \mathrm{ggT}(a_1, \ldots, a_n)$. (Alternatively apply Lemma 2 of the preceding exercise directly.)

   In the situation of (a) we therefore have $e \sim 1$. After replacing U by $Ue^{-1}V$ we then have $Uv = (1, 0 \ldots, 0)^T$. This is equivalent to $U^{-1}(1, 0, \ldots, 0)^T = (a_1, \ldots, a_n)^T$. But $U^{-1}(1, 0, \ldots, 0)^T$ is just the first column of U^{-1}, so (b) follows.

   Conversely, consider a matrix $W \in \mathrm{GL}_n(R)$ with first column $(a_1, \ldots, a_n)^T$. Write $W^{-1} = (u_{ij})_{i,j}$. Then the upper left entry of $W^{-1}W = I_n$ is $\sum_{j=1}^n u_{1j} a_j = 1$. This sum is divisible by $\mathrm{ggT}(a_1, \ldots, a_n)$, from which it follows that $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$.

**6. Zeige oder widerlege für jedes n: Jede Matrix in $\mathrm{GL}_n(\mathbb{Z})$ ist ein Produkt von Matrizen der Form

(a) Diagonalmatrizen mit Diagonaleinträgen ± 1,

(b) Permutationsmatrizen, oder

(c) Dreiecksmatrizen mit Diagonaleinträgen 1, einem weiteren Eintrag ± 1, und allen übrigen Einträgen 0.

7. Beweise: Für jeden Homomorphismus $\varphi\colon M \to N$ von Moduln über einem Ring R gilt:

(a) $\mathrm{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ist ein Untermodul von M.

(b) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von N.

(c) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 0$ ist.

(d) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = N$ ist.

(e) Beweise den Homomorphiesatz für Moduln: Jeder Homomorphismus $\varphi\colon M \to N$ von R-Moduln induziert einen Isomorphismus von R-Moduln

$$M/\mathrm{Kern}(\varphi) \xrightarrow{\sim} \mathrm{Bild}(\varphi),\ m + \mathrm{Kern}(\varphi) \mapsto \varphi(m).$$

Lösung:

(a) Since $0 \in \mathrm{Kern}(\varphi)$, it follows that $\mathrm{Kern}(\varphi) \neq \varnothing$. For all $m, m' \in \mathrm{Kern}(\varphi)$, we have $\varphi(m + m') = \varphi(m) + \varphi(m') = 0 + 0 = 0$, so $m + m' \in \mathrm{Kern}(\varphi)$. Lastly, for all $x \in R$ and $m \in \mathrm{Kern}(\varphi)$, we have $\varphi(xm) = x\varphi(m) = x \cdot 0 = 0$. Thus $xm \in \mathrm{Kern}(\varphi)$, and so $\mathrm{Kern}(\varphi) \subset M$ is a submodule.

(b) Since $0 = \varphi(0) \in \mathrm{Bild}(\varphi)$, we have $\mathrm{Bild}(\varphi) \neq \varnothing$. For $n, n' \in \mathrm{Bild}(\varphi)$, there exist $m, m' \in M$ such that $\varphi(m) = n$ and $\varphi(m') = n'$. Then $n + n' = \varphi(m) + \varphi(m') = \varphi(m + m') \in \mathrm{Bild}(\varphi)$ and $xn = x\varphi(m) = \varphi(xm) \in \mathrm{Bild}(\varphi)$. Thus $\mathrm{Bild}(\varphi) \subset N$ is a submodule.

(c) $\Rightarrow$: If there exists a non-zero $m \in \mathrm{Kern}(\varphi)$ then $\varphi(m) = \varphi(0) = 0$, contradicting the injectivity of φ. Thus $\mathrm{Kern}(\varphi) = 0$.
$\Leftarrow$: Let $m, m' \in M$ be such that $\varphi(m) = \varphi(m')$. Then $\varphi(m) - \varphi(m') = \varphi(m - m') = 0$. Since $\mathrm{Kern}(\varphi) = 0$, this implies $m - m' = 0$. Thus $m = m'$, and φ is injective.

(d) This follows from the definition of surjectivity.

(e) Abbreviate $L := \mathrm{Kern}(\varphi)$.
For any $m, m' \in M$ with $m + L = m' + L$ we have $m - m' \in L$ and therefore $\varphi(m) = \varphi(m - m' + m') = \varphi(m - m') + \varphi(m') = 0 + \varphi(m') = \varphi(m')$. Also we have $\varphi(m) \in \mathrm{Bild}(\varphi)$. Thus the map $\bar{\varphi}$ is well-defined.

For any $m, m' \in M$ we have $\bar{\varphi}((m+L)+(m'+L)) = \bar{\varphi}((m+m')+L) = \varphi(m+m') = \varphi(m)+\varphi(m') = \bar{\varphi}(m+L)+\bar{\varphi}(m'+L)$. Also, for any $m \in M$ and $x \in R$ we have $\bar{\varphi}(x(m+L)) = \bar{\varphi}(xm+L) = \varphi(xm) = x\varphi(m) = x\bar{\varphi}(m+L)$. Thus $\bar{\varphi}$ is an R-module homomorphism.

For any $m+L \in \mathrm{Kern}(\bar{\varphi})$ we have $\varphi(m) = \bar{\varphi}(m+L) = 0$ and hence $m \in \mathrm{Kern}(\varphi) = L$. Thus $m+L = 0$, and so $\mathrm{Kern}(\bar{\varphi})$ is the zero submodule. By part (c) it follows that $\bar{\varphi}$ is injective. On the other hand $\mathrm{Bild}(\bar{\varphi})$ is the set of $\bar{\varphi}(m+L) = \varphi(m)$ for all $m \in M$ and thus equal to $\mathrm{Bild}(\varphi)$. Thus $\bar{\varphi}$ is surjective.

Altogether $\bar{\varphi}$ is thus a bijective homomorphism and therefore an isomorphism.

Aliter: Use the universal property of the factor module:

Proposition. *Let R be a ring and let M an R-module. Then for every R-module L, every homomorphism $\varphi : M \to L$ and each submodule $N \subset M$ contained in* $\mathrm{Kern}(\varphi)$*, there exists a unique homomorphism $\bar{\varphi} : M/N \to L$ such that $\bar{\varphi} \circ \pi = \varphi$. In other words, the following diagram commutes:*

$$\begin{tikzcd} M \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & L \\ & M/N \arrow[ur, dotted, "\bar{\varphi}"'] & \end{tikzcd}$$

Beweis. Define $\bar{\varphi}(m+N) := \varphi(m)$. If $m'+N = m+N$, then $m' = m+n$ for some element $n \in N$. Since $N \subset \mathrm{Kern}(\varphi)$, we have $\varphi(m') = \varphi(m+n) = \varphi(m)+\varphi(n) = \varphi(m)$. Thus $\bar{\varphi}$ is well-defined with $\bar{\varphi}\circ\pi = \varphi$, and one can check by a similar calculation as above that $\bar{\varphi}$ is a homomorphism of R-modules.

If $\bar{\psi}$ also satisfies $\bar{\psi} \circ \pi = \varphi$, then for all $m+N \in M/N$ we have $\bar{\psi}(m+N) = \bar{\psi}(\pi(m)) = \varphi(m)$ so that $\bar{\psi} = \bar{\varphi}$, thereby proving uniqueness.

$\square$

**8. Sei R ein Ring. Zeige:

(a) $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/\operatorname{ggT}(m,n)\mathbb{Z})$ für alle $m, n \in \mathbb{Z}^{\geqslant 0}$.

(b) Seien M und N freie R-Moduln vom Rang r bzw. s. Dann ist $M \otimes_R N$ ein freier Modul vom Rang rs.

(c) Sei $n \in \mathbb{Z}^{\geqslant 0}$. Dann gilt:

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \begin{cases} 0, & \text{wenn } n \neq 0 \text{ ist,} \\ \mathbb{Q}, & \text{wenn } n = 0 \text{ ist.} \end{cases}$$