Aufgabe 1 (5 Punkte)

Sei R und S kommutative Ringe und $I \subseteq R$ ein R-Untermodul. Zeigen Sie:

a) Die Präkomposition mit dem Ringhomomorphismus

$$[-]_I : R \longrightarrow R/I, \quad r \longmapsto [r]_I$$

liefert eine Bijektion

$$\{\varphi : R/I \to S \mid \varphi \text{ ist Ringhomomorphismus}\}$$
$$\longrightarrow \{\varphi : R \to S \mid \varphi \text{ ist Ringhomomorphismus und } \forall i \in I : \varphi(i) = 0\}$$

b) Ist $\varphi : R \to S$ surjektiv, so ist die aus a) induzierte Abbildung

$$R/\ker(\varphi) \longrightarrow S$$

ein Isomorphismus.

c) Die Abbildung

$$R[T] \longrightarrow R, \quad T \longmapsto a$$

liefert einen Isomorphismus $R[T]/\langle T-a\rangle \to R$ für jedes $a \in R$.

d) Ist R ein Integritätsbereich und $a \neq 0$ so liefert

$$R[T] \longrightarrow R^{\mathrm{frc}}, \quad T \longmapsto 1/a$$

einen Isomorphismus $R[T]/\langle aT-1\rangle \to R[1/a]$, wo

$$R[1/a] = \{q \in R^{\mathrm{frc}} \mid \exists r \in R, n \in \mathbb{N} : q = r/a^n\}.$$

Bemerkung. *Insbesondere folgt aus c), dass $R[T]/\langle F\rangle$ für $F \in R[T]$ irreduzibel kein Körper sein muss, wenn R nicht euklidisch ist, und aus d) dass $R[T]/\langle F\rangle$ keine Basis als R-Modul besitzen muss, wenn $F \in R[T]$ nicht normiert ist.*

Lösungsskizze. Bezeichnen wir die Abbildung

$$[-]_I : R \longrightarrow R/I, \quad r \longmapsto [r]_I$$

einmal mit π.

a) Zunächst einmal ist die angegene Abbildung wohldefiniert, da

$$(\varphi \circ \pi)(i) = \varphi([i]) = \varphi([0]) = 0$$

und offenbar mit φ auch $\varphi \circ \pi$ ein Ringhomomorphismus ist.

Dass sie auch injektiv ist, hat nichts mit der Ringhomomorphismuseigenschaft zu tun: Sogar die Abbildung

$$-\circ\pi : \mathrm{F}(R/I, S) \longrightarrow \mathrm{F}(R, S)$$

ist nach Aufgabe 4 vom dritten Zettel des letzten Semesters injektiv, erst recht die Einschränkung, die wir hier betrachten. Die gleiche Aufgabe charakterisiert auch das Bild von $-\circ\pi$ als diejenigen Abbildungen $\psi : R \to S$ für die $\psi(r) = \psi(r')$ schon immer dann gilt, wenn $r \sim_I r'$, also $r - r' \in I$. Aber ist $\psi : R \to S$ ein Ringhomomorphismus mit $\psi(i) = 0$ für alle $i \in I$ und $r - r' \in I$, so rechnen wir

$$\psi(r) = \psi(r - r' + r') = \psi(r - r') + \psi(r') = \psi(0) + \psi(r') = \psi(r').$$

Es gilt also eine (eindeutige) Abbildung $\varphi : R/I \to S$ mit $\varphi \circ \pi = \psi$ und es bleibt zu prüfen, dass φ ein Ringhomomorphismus ist. Aber das folgt einfach durch Einsetzen der Definitionen, etwa

$$\varphi([r] + [r']) = \varphi(\pi(r) + \pi(r')) = \varphi(\pi(r + r')) = \psi(r + r') = \psi(r) + \psi(r') = \varphi(\pi(r)) + \varphi(\pi(r')) = \varphi([r]) + \varphi([r']).$$

Damit ist φ ein Urbild von ψ.

b) Offenbar ist die induzierte Abbildung, nennen wir sie $\psi: R/\ker(\varphi) \to S$, immer noch surjektiv ist: Ist etwa r ein Urbild eines beliebigen $s \in S$, so gilt schließlich $\psi([r]) = s$. Es bleibt also die Injektivität zu zeigen. Hierzu reicht es zu zeigen, dass $\ker(\psi) = \{[0]\}$ gilt (nach Korollar 3.3.1 im Skript). Aber ist $\psi([r]) = 0$, so folgt auch $\varphi(r) = \psi([r]) = 0$ und damit $r \in \ker(\varphi)$ und damit $[r] = [0]$ wie gewünscht.

c) Offenbar ist $\mathrm{ev}_a: R[T] \to R$ surjektiv; schließlich liefert für jedes $r \in R$ das konstante Polynome $r \in R[T]$ ein Urbild. Und es ist $\mathrm{ev}_a(F) = 0$ genau dann, wenn a eine Nullstelle von F genau dann, wenn $T - a | F$ (nach Korollar 5.2.2) und damit gilt $\ker(\mathrm{ev}_a) = \langle T - a \rangle$, sodass die gewünschte Aussage ein Spezialfall von b) ist.

d) Wieder ist $\mathrm{ev}_{1/a}: R[T] \to R[1/a]$ surjektiv: Es ist $r \cdot T^n$ schließlich ein Urbild von r/a^n. Und sicherlich gilt $\langle aT - 1 \rangle \subseteq \ker(\mathrm{ev}_{1/a})$, da offenbar $a \cdot \frac{1}{a} - 1 = 0$. Umgekehrt bedeutet $\mathrm{ev}_{1/a}(F) = 0$ für $F = \sum_{i=0}^{n} F_i \cdot T^i$ ausgeschrieben

$$\sum_{i=0}^{n} F_i \cdot \frac{1}{a^i} = 0$$

was durch Multiplikation mit a^n zu

$$\sum_{i=0}^{n} F_i \cdot a^{n-i} = 0$$

äquivalent ist, also dass a eine Nullstelle des Polynoms $\overline{F} = \sum_{i=0}^{n} F_{n-i} \cdot T^i \in R[T]$ ist. Das wiederum ist zu $T - a \mid \overline{F}$ äquivalent. Schreiben wir dann $\overline{F} = (T - a) \cdot G$ für ein $G = \sum_{i=0}^{n-1} G_i \cdot T^i \in R[T]$ aus, erhalten wir durch Koeffizientenvergleich

$$F_{n-i} = \overline{F}_i = G_{i-1} - a \cdot G_i$$

oder umnummeriert $F_j = G_{n-1-j} - a \cdot G_{n-j}$. Aber das ist auch zu $F = (aT - 1) \cdot (-\overline{G})$ mit $\overline{G} = \sum_{i=0}^{n-1} G_{n-1-i} \cdot T^i$ äquivalent, was $F \in \langle aT - 1 \rangle$ zeigt. Damit ist die Aussage wieder ein Spezialfall von b).

□

Aufgabe 2 (5 Punkte)

Konstruieren Sie, für jede Primzahl $p \in \mathbb{N}$ mit $p \equiv_4 1$ einen Ringisomorphismus

$$\mathbb{Z}/p[T]/\langle T^2 + 1 \rangle \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p.$$

Zeigen Sie auch, dass die beiden Seite für $p = 2$ nicht isomorph sind.

Lösungsskizze. Für $p \equiv_4 1$ liefert uns Korollar 5.4.10, dass $i = ((p-1)/2)!$ und damit auch $-i$ (verschiedene!) Nullstellen von $T^2 + 1$ sind. Weiterhin haben wir einen Ringhomomorphismus

$$\Delta: \mathbb{Z}/p \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p, \quad k \longmapsto (k, k)$$

mittels dem wir $\mathbb{Z}/p \times \mathbb{Z}/p$ als $\mathbb{Z}/p$-Algebra auffassen. Wir erhalten dann aus Satz 5.1.12 einen $\mathbb{Z}/p$-Algebrenhomomorphismus

$$\mathrm{ev}_{(i,-i)}: \mathbb{Z}/p[T] \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p, T \longrightarrow (i, -i).$$

Es gilt

$$\mathrm{ev}_{(i,-i)}(T^2 + 1) = (i, -i)^2 + (1, 1) = (i^2 + 1, (-i)^2 + 1) = (0, 0),$$

sodass Teil b) aus der vorigen Aufgabe einen Ringhomomorphismus

$$\varphi: \mathbb{Z}/p[T]/\langle T^2 + 1 \rangle \longrightarrow \mathbb{Z}/p \times \mathbb{Z}/p$$

liefert. Es gibt nun mehrere Möglichkeiten die Bijektivität von φ nachzuweisen.

Es bilden zum Beispiel nach Lemma 5.5.17 die Elemente $[1], [T]$ eine $\mathbb{Z}/p$-Basis von $\mathbb{Z}/p[T]/\langle T^2 + 1 \rangle$ und offenbar die Elemente $(1, 0)$ und $(0, 1)$ eine von $\mathbb{Z}/p \times \mathbb{Z}/p$ und φ ist $\mathbb{Z}/p$-linear. Die Darstellungsmatrix von φ ist bezüglich dieser Basen ist per Konstruktion

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \in \mathrm{Mat}(2, 2, \mathbb{Z}/p)$$

und diese hat Determinante $0 \neq -2i \in \mathbb{Z}/p$, ist also invertierbar.

Eine andere Möglichkeit ist es Korollar 5.18 zu benutzen: Dieses besagt, dass die linke Seite (genau wie die rechte) p^2 Elemente hat. Es reicht also nachzuweisen, dass φ injektiv oder surjektiv ist (die jeweils andere Bedingung folgt dann). Die Injektivität folgt etwa aus Teil b) von Aufgabe 1 (angewandt auf $S = \mathrm{Im}(\varphi)$) indem man beobachtet, dass $(0,0) = \mathrm{ev}_{(i,-i)}(F) = (F(i), F(-i))$ bedeutet, dass sowohl i als auch $-i$ Nullstellen von F sind, was genau $(T-i)(T+i)|F$ bedeutet und damit

$$\ker(\mathrm{ev}_{(i,-i)}) = \langle (T-i)(T+i) \rangle = \langle T^2+1 \rangle.$$

Oder man probiert einfach ein wenig herum, bis man als Urbild von $(k,l) \in \mathbb{Z}/p \times \mathbb{Z}/p$ das Element $\left[\frac{k+l}{2} + \frac{k-l}{2i} \cdot T\right] \in \mathbb{Z}/p[T]\langle T^2+1\rangle$ errät, was die Surjektivität zeigt.

Für $p = 2$ kann man etwa beobachten, dass $[T] \neq [1]$ aber $[T]^2 = [1]$ in $\mathbb{Z}/2[T]\langle T^2+1\rangle$ gilt, aber in $\mathbb{Z}/2 \times \mathbb{Z}/2$ aus $(1,1) = (k,l)^2$ schon $(k,l) = (1,1)$ folgt. □

Bemerkung. *Wir kennen also nun vier verschiedene Ringe mit* 4 *Elementen:* $\mathbb{Z}/4$, $\mathbb{F}_4 = \mathbb{Z}/2[T]/\langle T^2+T+1\rangle$, $\mathbb{Z}/2 \times \mathbb{Z}/2$ *und* $\mathbb{Z}/2[T]/\langle T^2+1\rangle$. *Man kann sich überlegen, dass dies bis auf Isomorphie alle Möglichkeiten sind; etwa gelten*

$$\mathbb{Z}/2[T]/\langle T^2+1\rangle \cong \mathbb{Z}/2[T]/\langle T^2\rangle \quad \textit{und} \quad \mathbb{Z}/2[T]/\langle T^2+T\rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Aufgabe 3 (5 Punkte)

Entscheiden Sie, ob die Matrix

$$\begin{pmatrix} T^3+8T & -4T & -T^2+1 \\ 2T^3+18T & -9T & -2T^2+2 \\ T^4+8T^2-T & -4T^2 & -T^3+T+1 \end{pmatrix} \in \mathrm{Mat}(3,3,\mathbb{Q}(T))$$

diagonalisierbar ist, wo $\mathbb{Q}(T) = \mathbb{Q}[T]^{\mathrm{frc}}$.

Lösungsskizze. Wir bestimmen das charakteristische Polynom von obiger Matrix, nennen wir sie A. Da T schon vergeben ist, nennen wir die Polynomvariable einmal X, und berechnen dann

$$\chi_A = \det(\mathbb{I}_3 \cdot X - A) = \det\begin{pmatrix} X-T^3-8T & 4T & T^2-1 \\ -2T^3-18T & X+9T & 2T^2-2 \\ -T^4-8T^2+T & 4T^2 & X+T^3-T-1 \end{pmatrix} \in \mathbb{Q}(T)[X]$$

was mit etwas Rechenaufwand

$$\chi_A = X^3 - X^2 - T^2X + T^2$$

liefert. Offenbar sind 1, T und $-T$ Nullstellen dieses Polynoms; das Lemma von Gauß liefert, dass jede Nullstelle von χ_A ein Teiler von T^2 (in $\mathbb{Q}[T]$!) ist, was natürlich bei der Suche hilft. Es schlägt jedenfalls Korollar 6.1.7 zu und A ist diagonalisierbar, ähnlich zu

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & T & 0 \\ 0 & 0 & -T \end{pmatrix}.$$

□

Aufgabe 4 (5 Punkte)

Sei R ein kommutativer Ring, M ein R-Modul mit zwei R-Untermoduln $U, V \subseteq M$, die endliche Basen besitzen und für die $M = U \oplus V$ gilt. Zeigen Sie: Ist $\varphi : M \to M$ eine R-lineare Abbildung mit $\mathrm{Im}_\varphi(U) \subseteq U$, so gilt

$$\det(\varphi) = \det(\varphi_{|U} : U \to U) \cdot \det(\mathrm{pr}_V \circ \varphi_{|V} : V \to V)$$

wo $\mathrm{pr}_V : M \to V$ die eindeutig bestimmte R-lineare Abbildung mit $(\mathrm{pr}_V)_{|V} = \mathrm{id}_V$ und $(\mathrm{pr}_V)_{|U} = 0$ ist.

Hinweis: Sie dürfen benutzen, dass sich eine nummerierte Basis b von U und b' eine von V zu einer Basis c von $U \oplus V$ zusammenfügen, und die Darstellungsmatrix dann von der Form

$$\mathrm{M}(\varphi, c) = \begin{pmatrix} \mathrm{M}(\varphi_{|U}, b, b) & \mathrm{M}(\mathrm{pr}_U \circ \varphi_{|V}, b', b) \\ 0 & \mathrm{M}(\mathrm{pr}_V \circ \varphi_{|V}, b', b') \end{pmatrix}$$

ist. Dies folgt aus Satz 1.9 des Skripts, den ich aber in der Vorlesung noch nicht bewiesen habe.

Lösungsskizze. Laut dem Hinweis reicht es zu zeigen, dass für jedes $A \in \mathrm{Mat}(n,n,R)$, $C \in \mathrm{Mat}(k,k,R)$ und $B \in \mathrm{Mat}(k,n,R)$ die Gleichung

$$\det\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A) \cdot \det(C)$$

gilt.

Hierfür gibt es mehrere Möglichkeiten. Die einfachste ist vielleicht eine Induktion über n mittels des Laplace'schen Entwicklungssatzes. Setzen wir zu Abkürzung

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}.$$

Gilt $n = 0$ so ist nichts zu zeigen. Ansonsten haben wir mittels Entwicklung nach der ersten Spalte

$$\det(M) = \sum_{i=1}^{n+1+k} (-1)^{i+1} M_{1,i} \cdot \det(M[i,1]) = \sum_{i=1}^{n+1} (-1)^{i+1} A_{1,i} \cdot \det(M[i,1])$$

Die Matrix $M[i,1]$ die aus M durch Streichen der ersten Spalte und i-ten Zeile entsteht, hat aber offenbar die Form

$$M[i,1] = \begin{pmatrix} A[i,1] & B[i] \\ 0 & C \end{pmatrix}$$

wo $B[i]$ durch Streichen der i-ten Zeile aus B entsteht. Es folgt also per Induktionshypothese

$$\det(M) = \sum_{i=1}^{n+1} (-1)^{i+1} A_{1,i} \cdot \det(A[i,1]) \cdot \det(C)$$

Aber man kann den Entwicklungssatz natürlich auch auf A anwenden und erhält

$$\det(A) = \sum_{i=1}^{n+1} (-1)^{i+1} A_{1,i} \cdot \det(A[i,1])$$

und damit insgesamt

$$\det(M) = \det(A) \cdot \det(C)$$

wie gewünscht.

Man kann aber auch direkt mit der Leibnizformel argumentieren: Es gilt

$$\det(M) = \sum_{\sigma \in \Sigma_{n+k}} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n+k} M_{i,\sigma(i)}.$$

Aber gilt für ein $\sigma(i) > n$ für ein $1 \le i \le n$, so haben wir $M_{i,\sigma(i)} = 0$, da dieser Eintrag dann in der unteren linken Ecke der Matrix M zu finden ist.

Also verschwinden alle diese Summanden, und wir müssen nur solche betrachten, bei denen σ die Menge $\{1,\dots,n\}$ in sich abbildet, und damit auch $\{n+1,\dots,n+k\}$. Solche Permutationen σ zerlegen sich als zwei Permutationen, sagen wir τ auf $\{1,\dots,n\}$ und ρ auf $\{n+1,\dots,n+k\}$, und offenbar gilt dann $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau) \cdot \mathrm{sgn}(\rho)$, da jeder Fehlstand von σ entweder von τ oder ρ herrührt. Es gilt in diesem Falle

$$M_{i,\sigma(i)} = \begin{cases} A_{i,\tau(i)} & i \neq l \\ C_{i-n,\tau(i)-n} & i > n \end{cases}$$

und wir erhalten

$$\det(M) = \sum_{\tau\in\Sigma_n,\rho\in\Sigma_k} \operatorname{sgn}(\tau)\cdot\operatorname{sgn}(\rho)\cdot\left(\prod_{i=1}^{n} A_{i,\tau(i)}\right)\cdot\left(\prod_{i=1}^{k} C_{i,\rho(i)}\right)$$

$$= \left(\sum_{\tau\in\Sigma_n} \operatorname{sgn}(\tau)\prod_{i=1}^{n} A_{i,\tau(i)}\right)\cdot\left(\sum_{\rho\in\Sigma_k} \operatorname{sgn}(\rho)\prod_{i=1}^{k} C_{i,\rho(i)}\right) = \det(A)\cdot\det(C)$$

durch umindizieren. □