Musterlösung 7

Moduln über Hauptidealringen, Jordansche Normalform

*1. Eine Folge von Elementen $(m_1, \ldots, m_n)$ eines R-Moduls M heisst eine *Basis von M*, wenn jedes Element von M auf eindeutige Weise als $a_1m_1 + \ldots + a_nm_n$ mit $a_i \in R$ darstellbar ist. Besitzt M eine Basis der Länge n, so ist M isomorph zu R^n, also frei vom Rang n.

Sei nun M ein freier Modul von endlichem Rang n über einem Hauptidealring R. Beweise oder widerlege:

(a) Jede linear unabhängige Teilmenge von M lässt sich zu einer Basis von M ergänzen.

(b) Aus jedem Erzeugendensystem von M lässt sich eine Basis von M auswählen.

(c) Jeder Untermodul von M ist frei vom Rang $\leqslant n$.

Lösung: Aussagen (a) und (b) sind falsch. Sei zum Beispiel $R = \mathbb{Z}$ und $M = \mathbb{Z}$ (freier $\mathbb{Z}$-Modul vom Rang 1). Die einzigen Basen von $\mathbb{Z}$ sind (1) und (-1), da nur 1 und -1 ganz $\mathbb{Z}$ erzeugen und zwei beliebige Elemente $m \neq n$ von $\mathbb{Z}$ wegen $n \cdot m - m \cdot n = 0$ linear abhängig sind. Die folgenden Beispiele widerlegen daher die entsprechenden Aussagen:

(a) Die Teilmenge $\{2\}$ ist linear unabhängig, da $\mathbb{Z}$ ein Integritätsbereich ist, kann aber nicht zu einer Basis von $\mathbb{Z}$ ergänzt werden.

(b) Die Teilmenge $\{2, 3\}$ ist wegen $\mathrm{ggT}(2, 3) = 1$ ein Erzeugendensystem, enthält aber keine Basis von $\mathbb{Z}$.

(c) Sei $N \subset M \cong R^n$ ein Untermodul. Wie in der Vorlesung gezeigt, ist N ebenfalls endlich erzeugt, also gilt

$$N \cong R^r \boxplus \mathop{\boxplus}_{i=1}^{k} R/e_iR$$

für Elementarteiler $e_1, \ldots, e_k \in R \smallsetminus (\{0\} \cup R^\times)$. Ist $k > 0$, so sei $n \in N$ das Element, das unter dem gegebenen Isomorphismus auf das Element $(0, \ldots, 0, 1 + e_kR)$ in der obigen Summe abgebildet wird. Wegen $e_k \cdot (1 + e_kR) = 0 + e_kR \neq 1 + e_kR$ in R/e_kR gilt dann auch $e_kn = 0 \neq n$. Andererseits sei $(a_1, \ldots, a_n)$ das Element von R^n, das unter $N \subset M \cong R^n$ dem Element n entspricht. Dann gilt ebenfalls $(e_ka_1, \ldots, e_ka_n) = e_k(a_1, \ldots, a_n) = (0, \ldots, 0) \neq (a_1, \ldots, a_n)$. Da R ein Integritätsbereich ist, ist dies unmöglich. Also ist $k = 0$ und $N \cong R^r$ ist frei. Eine Basis von N besteht also aus r linear unabhängigen Elementen. Da aber der Rang n von M die maximale Anzahl linear unabhängiger Elemente von M ist, muss $r \leqslant n$ sein.

2. Sei $A := \begin{pmatrix} 4 & 7 \\ 5 & 8 \\ 6 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 2}$ wie in Aufgabe 3 der Serie 6. Gib einen expliziten Isomorphismus von $\mathbb{Z}^3/A\mathbb{Z}^2$ auf ein direktes Produkt von zyklischen $\mathbb{Z}$-Moduln an.

Lösung: Nach Aufgabe 3 der Serie 6 ist $UAV = D$, wobei

$$U = \begin{pmatrix} -1 & 1 & 0 \\ 5 & -4 & 0 \\ 1 & -2 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{und } D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix}.$$

Nach dem Beweis des Haupsatzes über endlich erzeugte Moduln über Hauptidealringen ist also $\mathbb{Z}^3/A\mathbb{Z}^2$ isomorph zu $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}$. Um einen expliziten Isomorphismus anzugeben, bemerken wir zunächst, dass der surjektive Homomorphismus

$$\pi : \begin{array}{ccc} \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z} \\ (a,b,c) & \longmapsto & (b+3\mathbb{Z},\ c) \end{array}$$

den Kern $\{(a,3b,0) \in \mathbb{Z}^3 \mid a,b \in \mathbb{Z}\} = D\mathbb{Z}^2$ hat. Wegen $U \in \mathrm{GL}_3(\mathbb{Z})$ und $V \in \mathrm{GL}_2(\mathbb{Z})$ ist daher

$$\mathrm{Ker}(\pi\circ U) = U^{-1}\,\mathrm{Ker}(\pi) = U^{-1}D\mathbb{Z}^2 = U^{-1}DV^{-1}\mathbb{Z}^2 = A\mathbb{Z}^2.$$

Wir haben also folgendes kommutatives Diagramm:

$$\begin{tikzcd} \mathrm{Ker}(\pi\circ U) = A\mathbb{Z}^2 \arrow[r, hook] & \mathbb{Z}^3 \arrow[d, "U", "\cong"'] \arrow[dr, "\pi\circ U"] & \\ & & \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z} \\ \mathrm{Ker}(\pi) = D\mathbb{Z}^2 \arrow[r, hook] & \mathbb{Z}^3 \arrow[ur, "\pi"] & \end{tikzcd}$$

Nach dem Homomorphiesatz induziert daher der surjektive Homomorphismus $\pi\circ U$ den gewünschten Isomorphismus, der nach der obigen Darstellung von U explizit durch

$$\begin{array}{ccc} \mathbb{Z}^3/A\mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z} \\ (a,b,c)+A\mathbb{Z}^2 & \longmapsto & (5a-4b+3\mathbb{Z},\ a-2b+c) \end{array}$$

gegeben ist.

3. (a) Bestimme alle Isomorphieklassen von endlichen $\mathbb{Z}$-Moduln der Kardinalität 600.
   (b) Bestimme alle Isomorphieklassen von endlichen $\mathbb{F}_2[X]$-Moduln der Kardinalität 16 (verwende Aufgabe 5 der Serie 5).

Lösung: (a) Jeder endliche $\mathbb{Z}$-Modul ist insbesondere endlich erzeugt, nach dem Struktursatz also isomorph zu

$$\mathbb{Z}^r \boxplus \bigboxplus_{i=1}^{\ell} \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$$

für Primzahlen p_i und Exponenten ν_i. Die Endlichkeit impliziert dabei $r = 0$, und die Kardinalität ist dann $\prod_{i=1}^{\ell} p_i^{\nu_i}$. Wegen $600 = 2^3 \cdot 3 \cdot 5^2$ müssen die Primzahlen $2, 3, 5$ mit den angegebenen Exponenten auftauchen. Insgesamt gibt das die Isomorphieklassen

$$\begin{aligned}
&Z_8 \times Z_3 \times Z_{25},\\
&Z_8 \times Z_3 \times Z_5 \times Z_5,\\
&Z_4 \times Z_2 \times Z_3 \times Z_{25},\\
&Z_4 \times Z_2 \times Z_3 \times Z_5 \times Z_5,\\
&Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_{25},\\
&Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_5 \times Z_5.
\end{aligned}$$

(b) Sei M ein $\mathbb{F}_2[X]$-Modul der Kardinalität 16. Nach dem Struktursatz kann M als $\mathbb{F}_2[X]^r \boxplus \bigboxplus_{i=1}^{n} \mathbb{F}_2[X]/(\pi_i^{k_i})$ mit $r \geqslant 0$, $\pi_i \in \mathbb{F}_2[X]$ prim und $k_i \geqslant 1$ geschrieben werden, wobei die in der Zerlegung auftretenden $\pi_i^{k_i}$ bis auf Reihenfolge (eigentlich auch bis auf Assoziiertheit, was aber wegen $\mathbb{F}_2^\times = \{1\}$ keinen Unterschied macht) eindeutig sind, da $\mathbb{F}_2[X]^\times = \mathbb{F}_2^\times = \{1\}$ gilt. Weil M endlich von Ordnung 16 ist, muss $r = 0$ gelten und die Dimension von M über $\mathbb{F}_2$ gleich 4 sein. Die Summanden $\mathbb{F}_2[X]/(\pi_i^{k_i})$ haben die Dimension $\deg(\pi_i^{k_i})$ über $\mathbb{F}_2$. Denn jedes Element von $\mathbb{F}_2[X]/(\pi_i^{k_i})$ kann nach Division mit Rest eindeutig in der Form $p + (\pi_i^{k_i})$ mit $\deg(p) < \deg(\pi_i^{k_i})$ geschrieben werden, weshalb $X^j + (\pi_i^{k_i})$, $0 \leqslant j < \deg(\pi_i^{k_i})$ eine Basis von $\mathbb{F}_2[X]/(\pi_i^{k_i})$ ist. Also muss $\sum_{i=1}^{n} \deg(\pi_i^{k_i}) = 4$ gelten.

Für die Grade der in der Zerlegung auftretenden $\pi_i^{k_i}$ gibt es also die Fälle i) 1,1,1,1; ii) 1,1,2; iii) 1,3; iv) 2,2; v) 4. Weil $\mathbb{F}_2[X]$ faktoriell ist, kommen dabei für die $\pi_i^{k_i}$ genau Potenzen von irreduziblen Polynomen in Frage, nach Aufgabe 5 der Serie 5 also

$$\begin{aligned}
&\text{Grad 1:} && X, X+1,\\
&\text{Grad 2:} && X^2, (X+1)^2, X^2+X+1,\\
&\text{Grad 3:} && X^3, (X+1)^3, X^3+X+1, X^3+X^2+1,\\
&\text{Grad 4:} && X^4, (X+1)^4, (X^2+X+1)^2, X^4+X^3+X^2+X+1,\\
& && X^4+X^3+1, X^4+X+1.
\end{aligned}$$

Deshalb gibt es bis auf die Reihenfolge für die $\pi_i^{k_i}$ im Fall i) 5, ii) 9, iii) 8, iv) 6 und v) 6 Möglichkeiten. Somit gibt es insgesamt 34 Isomorphieklassen von $\mathbb{F}_2[X]$-Moduln der Ordnung 16.

4. Seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Wegen der Vorlesung existieren Zahlen $r, \ell \geqslant 0$ und Primelemente $p_i \in R$ und Exponenten $\nu_i \geqslant 1$, so dass gilt
$$M \cong R^r \boxplus \boxplus_{i=1}^{\ell} R/(p_i^{\nu_i}).$$
Zeige: Für jedes Primelement $p \in R$ und jedes $\nu \geqslant 1$ gilt
$$\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) \;=\; r + \left|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i > \nu\}\right|.$$
Folgere daraus, dass die Zahlen r und ℓ, sowie die Paare (p_i, ν_i) bis auf Vertauschung und Assoziiertheit der p_i eindeutig bestimmt durch M sind.

Lösung: If $M = \boxplus_{i=1}^k M_i$, then
$$\begin{aligned} p^\nu M/p^{\nu+1}M &= p^\nu\Big(\boxplus_{i=1}^k M_i\Big) \Big/ p^{\nu+1}\Big(\boxplus_{i=1}^k M_i\Big) \\ &= \Big(\boxplus_{i=1}^k p^\nu M_i\Big) \Big/ \Big(\boxplus_{i=1}^k p^{\nu+1} M_i\Big) \\ &\cong \boxplus_{i=1}^k (p^\nu M_i/p^{\nu+1}M_i). \end{aligned}$$
Adding the dimensions obtained for each summand reduces the problem to the case $M = R$ or $M = R/(p_i^{\nu_i})$.

<u>Case 1: $M = R$</u>: Then the map $R \to p^\nu R/p^{\nu+1}R$ sending r to $p^\nu r$ is surjective with kernel (p), so we have an induced isomorphism $R/(p) \cong p^\nu R/p^{\nu+1}R$. Thus $\dim_{R/(p)}(p^\nu R/p^{\nu+1}R) = \dim_{R/(p)}(R/(p)) = 1$.

<u>Case 2: $M = R/p_i^{\nu_i}$ with $p_i \nsim p$</u>: Then $p_i^{\nu_i}$ and p^ν are relatively prime, so there exist $u, v \in R$ such that $up_i^{\nu_i} + vp^\nu = 1$. For each $m \in M$ we have $p_i^{\nu_i} m = 0$ and therefore
$$m = (up_i^{\nu_i} + vp^\nu)m = vp^\nu m = p^\nu vm.$$
This implies that $m \in p^\nu M$, from which it follows that $M = p^\nu M$. The same argument applies to $p^{\nu+1}M$, so that $M = p^\nu M = p^{\nu+1}M$. Hence $p^\nu M/p^{\nu+1}M = \{0\}$ and $\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) = 0$.

<u>Case 3: $M = R/p_i^{\nu_i}$ with $p_i \sim p$</u>: Since changing p by a unit does not affect $p^\nu M$, we may suppose without loss of generality that $p = p_i$. For $\nu < \nu_i$ we have $p^{\nu_i}R \subset p^{\nu+1}R \subset p^\nu R$ and hence
$$\begin{aligned} p^\nu M &= p^\nu(R/p^{\nu_i}R) &= p^\nu R/p^{\nu_i}R \qquad \text{and} \\ p^{\nu+1}M &= p^{\nu+1}(R/p^{\nu_i}R) &= p^{\nu+1}R/p^{\nu_i}R. \end{aligned}$$
Therefore
$$p^\nu M/p^{\nu+1}M \cong p^\nu R/p^{\nu+1}R,$$
and so $\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) = 1$ for the same reason as in the case $M = R$. For $\nu \geqslant \nu_i$, we have $p^\nu R + p^{\nu_i}R = p^{\nu_i}R$ and therefore $p^\nu(R/p^{\nu_i}R) = (p^\nu R +$

$p^{\nu_i}R)/p^{\nu_i}R = \{0\}$, and likewise $p^{\nu+1}(R/p^{\nu_i}R) = \{0\}$. Thus $\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) = 0$ in this case.

To prove the uniqueness we abbreviate

$$d_{p,\nu} \;:=\; \dim_{R/(p)}(p^\nu M/p^{\nu+1}M) \;=\; r + \bigl|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i > \nu\}\bigr|.$$

Then $d_{p,\nu} = r$ whenever $\nu \geqslant \max_i\{\nu_i\}$. Thus for all $\nu \geqslant 0$ we have

$$d_{p,\nu} - d_{p,\nu+1} \;=\; \bigl|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i = \nu\}\bigr|.$$

Thus the number of pairs (p_i, ν_i) with $p_i \sim p$ and $\nu_i = \nu$ is uniquely determined. Varying p and ν shows that the pairs (p_i, ν_i) are uniquely determined up to permutation and association. If there exists a prime element $p \in R$, the fact that $d_{p,\nu} = r$ for all $\nu \gg 0$ also shows that r is uniquely determined. Otherwise R is a field, and $r = \dim_R(M)$ is again unique.

5. Sei K ein Körper.

   (a) Konstruiere $K[X,Y]$-Moduln M und M' von endlicher Dimension über K, so dass M und M' isomorph als $K[X]$- und als $K[Y]$-Moduln sind, aber nicht als $K[X,Y]$-Moduln.

   (b) Folgere aus (a), dass Matrizen A, B, A', B' geeigneter Grösse $n \times n$ über K existieren mit den Eigenschaften:

      i. $AB = BA$.
      ii. $A'B' = B'A'$.
      iii. Es existiert $U \in \mathrm{GL}_n(K)$ mit $UAU^{-1} = A'$.
      iv. Es existiert $U \in \mathrm{GL}_n(K)$ mit $UBU^{-1} = B'$.
      v. Es existiert kein $U \in \mathrm{GL}_n(K)$ mit $UAU^{-1} = A'$ und $UBU^{-1} = B'$.

Lösung: (a) Let $M := K[X,Y]/(X^2, Y^2)$ and $M' := \bigl(K[X,Y]/(X-Y, X^2)\bigr)^{\oplus 2}$. We claim that there is an isomorphism of $K[X]$-modules

$$\varphi : \bigl(K[X]/(X^2)\bigr)^{\oplus 2} \xrightarrow{\sim} M,\; \begin{pmatrix} f(X) + (X^2) \\ g(X) + (X^2) \end{pmatrix} \mapsto f(X) + g(X)Y + (X^2, Y^2).$$

Let $\binom{f(X)+(X^2)}{g(X)+(X^2)}$ be an element of $\bigl(K[X]/(X^2)\bigr)^{\oplus 2}$, and consider $f', g' \in K[X]$ representing the same element. Then $f'(X) = f(X) + p(X)X^2$ and $g'(X) = g(X) + q(X)X^2$ for some $p, q \in K[X]$. It follows that

$$\begin{aligned} f'(X) + g'(X)Y + (X^2, Y^2) &= f(X) + g(X)Y + \bigl(p(X) + q(X)\bigr)X^2 + (X^2, Y^2) \\ &= f(X) + g(X)Y + (X^2, Y^2); \end{aligned}$$

hence φ is well-defined. Next for any $f, f', g, g' \in K[X]$ we have

$$\begin{aligned}
&\varphi\begin{pmatrix} f(X)+f'(X)+(X^2) \\ g(X)+g'(X)+(X^2) \end{pmatrix} \\
&= f(X)+f'(X)+\big(g(X)+g'(X)\big)Y+(X^2,Y^2) \\
&= \varphi\begin{pmatrix} f(X)+(X^2) \\ g(X)+(X^2) \end{pmatrix} + \varphi\begin{pmatrix} f'(X)+(X^2) \\ g'(X)+(X^2) \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
&\varphi\begin{pmatrix} p(X)f(X)+(X^2) \\ p(X)g(X)+(X^2) \end{pmatrix} \\
&= p(X)f(X)+p(X)g(X)Y+(X^2,Y^2) \\
&= p(X)\cdot\big(f(X)+g(X)Y+(X^2,Y^2)\big) \\
&= p(X)\cdot\varphi\begin{pmatrix} f(X)+(X^2) \\ g(X)+(X^2) \end{pmatrix}.
\end{aligned}$$

Thus φ is a homomorphism of $K[X]$-modules. Now $f(X)+g(X)Y+(X^2,Y^2) = 0+(X^2,Y^2)$ if and only if $f, g \in (X^2)$ if only if

$$\begin{pmatrix} f(X)+(X^2) \\ g(X)+(X^2) \end{pmatrix} = \begin{pmatrix} 0+(X^2) \\ 0+(X^2) \end{pmatrix} \in \big(K[X]/(X^2)\big)^{\oplus 2}.$$

Thus φ is injective. Finally, any element of $K[X,Y]/(X^2,Y^2)$ can be written in the form $f(X)+g(X)Y+(X^2,Y^2)$, which is the image of $\left(\begin{smallmatrix} f(X)+(X^2) \\ g(X)+(X^2) \end{smallmatrix}\right)$; so φ is surjective. It is thus bijective and hence an isomorphism.

Since the definition of M is symmetric in X and Y, replacing X with Y in the above argument yields an isomorphism of $K[Y]$-modules $\big(K[Y]/(Y^2)\big)^{\oplus 2} \xrightarrow{\sim} M$.

Now we claim that

$$K[X]/(X^2) \xrightarrow{\sim} K[X,Y]/(X-Y,X^2),\ f(X)+(X^2) \mapsto f(X)+(X-Y,X^2).$$

is a well-defined isomorphism of $K[X]$-modules. If $f(X)+(X^2) = f'(X)+(X^2)$, it follows immediately that $f(X)+(X-Y,X^2) = f'(X)+(X-Y,X^2)$. Thus the map is well-defined. It is clear from the definition that the map is a homomorphism of $K[X]$-modules. Next $f(X)+(X-Y,X^2) = 0+(X-Y,X^2)$ if and only if $f(X) \in (X-Y,X^2)\cap K[X] \overset{!}{=} (X^2)$ if and only if $f(X)+(X^2) = 0+(X^2)$. Thus the map is injective. Lastly, for any $F(X,Y) \in K[X,Y]$ we have $F(X,Y)+(X-Y,X^2) = F(X,X)+(X-Y,X^2)$, which is the image of the element $F(X,X)+(X^2)$. It follows that the map is surjective and therefore an isomorphism, proving the claim.

Taking direct sums the claim induces an isomorphism of $K[X]$-modules

$$\big(K[X]/(X^2)\big)^{\oplus 2} \xrightarrow{\sim} M'.$$

Since $X^2 = (X+Y) \cdot (X-Y) + Y^2$, we have $(X-Y, X^2) = (X-Y, Y^2)$ and hence $M' = K[X,Y]/(X-Y,Y^2)$. Thus an analogous argument shows that $\big(K[Y]/(Y^2)\big)^{\oplus 2} \cong M'$ as $K[Y]$-modules.

Altogether it now follows that M and M' are isomorphic when considered as $K[X]$- or $K[Y]$-modules. However, they cannot be isomorphic as $K[X,Y]$-modules, since multiplication by $(X-Y)$ is zero on M' but not on M.

(b) Now recall that giving a $K[X]$-module is equivalent to giving a K-vector space M together with the endomorphism φ corresponding to multiplication by X. Suppose that $\dim_K(M) < \infty$, and let A be the matrix representing φ with respect to some ordered basis B of M. Let M' be a second $K[X]$-module, with $\varphi' \in \mathrm{End}_K(M')$ corresponding to multiplication by X, represented by the matrix A' with respect to some ordered basis B'. Then a map $\alpha\colon M \to M'$ is an isomorphism of $K[X]$-modules if and only if it is an isomorphism of K-vector spaces and satisfies $\varphi' \circ \alpha = \alpha \circ \varphi$. In that case, the representing matrices satisfy

$$A' \;=\; M_{B',B'}(\alpha \circ \varphi \circ \alpha^{-1}) \;=\; M_{B',B}(\alpha) \cdot M_{B,B}(\varphi) \cdot M_{B',B}(\alpha)^{-1} \;=\; UAU^{-1}$$

with the invertible matrix $U := M_{B',B}(\alpha)$. Conversely, if there exists an invertible matrix U with $A' = UAU^{-1}$, then the matrices have the same size, and there exists an isomorphism of K-vector spaces $\alpha\colon V \to V'$ with $M_{B',B}(\alpha) = U$. This α then satisfies $\varphi' \circ \alpha = \alpha \circ \varphi$. Thus giving M as a $K[X]$-module up to isomorphism is equivalent to giving (M, φ) up to isomorphism is equivalent to giving A up to similarity.

Similarly, every $K[X,Y]$-module M is also a $K[X]$-module and a $K[Y]$-module. Let $\varphi, \psi \in \mathrm{End}_K(M)$ be the endomorphisms corresponding to multiplication by X, respectively by Y. Since $XY = YX$ in $K[X,Y]$, for all $m \in M$ we have

$$\varphi(\psi(m)) = X \cdot (Y \cdot m) = Y \cdot (X \cdot m) = \psi(\varphi(m));$$

hence $\varphi \circ \psi = \psi \circ \varphi$. Conversely, for any endomorphisms φ, ψ of a K-vector space M we can try to turn M into a $K[X,Y]$-module by setting

$$\Big(\sum a_{ij} X^i Y^j\Big) \cdot m \;:=\; \sum a_{ij} \varphi^i(\psi^j(m)).$$

One checks that this succeeds if and only if φ and ψ commute. Suppose that $\dim_K(M) < \infty$, and let A and B be the matrices representing φ and ψ with respect to the same ordered basis of M. Then giving M as a $K[X,Y]$-module up to isomorphism is equivalent to giving (M, φ, ψ) up to isomorphism, and this in turn is equivalent to giving the pair (A, B) up to joint similarity, that is, up to $(A, B) \mapsto (UAU^{-1}, UBU^{-1})$ for an invertible matrix U.

Let now M and M' be $K[X,Y]$-modules of finite dimension d over K, which are isomorphic as $K[X]$-modules and as $K[Y]$-modules, but not as $K[X,Y]$-modules.

Let A and B be the matrices representing multiplication by X respectively Y in a suitable K-basis of M, and similarly A' and B' for M'. Then by the above remarks the properties i. through v. hold.

In the specific example consider the basis of M formed by the residue classes of $1, X, Y, XY$ in this order. Then we get

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Similarly, for the basis of M' formed by the residue classes of $(1,0)$, $(X,0)$, $(0,1)$, $(0,X)$ in this order, we obtain

$$A' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = B'.$$

6. Konstruiere die Jordan-Chevalley-Zerlegung der komplexen Matrix

$$A := \begin{pmatrix} 0 & 1 & 1 \\ 2 & 1 & -1 \\ -6 & -5 & -3 \end{pmatrix}$$

je einmal mit Hilfe des chinesischen Restsatzes wie im Beweis der Zerlegung, und einmal mit Hilfe der Jordan-Normalform von A. Welcher Weg ist schneller?

Lösung: Let $p_A(X)$ denote the characteristic polynomial of A. Recall that we may consider $V := \mathbb{C}^3$ as a $\mathbb{C}[X]$-module, where X acts as the endomorphism determined by A. Direct computation yields $p_A(X) = (X+2)^2(X-2)$. Then the Chinese Remainder Theorem gives an explicit isomorphism

$$\rho : \mathbb{C}[X]/(p_A(X)) \xrightarrow{\sim} \mathbb{C}[X]/((X+2)^2) \boxplus \mathbb{C}[X]/(X-2).$$

Thus there exists a polynomial $f(X) \in \mathbb{C}[X]$ congruent to -2 modulo $(X+2)^2$ and to 2 modulo $(X-2)$. Since p_A has degree 3, we may choose f of degree $\leqslant 2$. From $f(X) \equiv -2 \bmod (X+2)^2$, we deduce that $f(X) = -2 + a(X+2)^2$ for some $a \in \mathbb{C}$. Then $f(X) \equiv f(2) = -2 + 16a$ modulo $(X-2)$; so $f(X) \equiv 2 \bmod (X-2)$ implies that $a = \frac{1}{4}$. Thus

$$f(X) \;=\; -2 + \tfrac{1}{4}(X+2)^2.$$

By the proof of the Jordan-Chevalley decomposition in the course, the matrix $A_s := f(A)$ is the semisimple part of A, and $A_n := A - A_s$ is the nilpotent part of A. Direct computation yields

$$A_s = -2I_3 + \frac{1}{4}(A + 2I_3)^2 = \begin{pmatrix} -2 & 0 & 0 \\ 4 & 2 & 0 \\ -4 & -4 & -2 \end{pmatrix}$$

and

$$A_n = A - A_s = \begin{pmatrix} 2 & 1 & 1 \\ -2 & -1 & -1 \\ -2 & -1 & -1 \end{pmatrix}.$$

Variant: One computes the Jordan Normal Form of A, obtaining

$$P^{-1}AP = \begin{pmatrix} -2 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

with

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

Then

$$A_s = P \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 2 \end{pmatrix} P^{-1} = \begin{pmatrix} -2 & 0 & 0 \\ 4 & 2 & 0 \\ -4 & -4 & -2 \end{pmatrix}.$$