Übungsblatt 6: Matrizen und Moduln

1. MODULN

1.1. Sei R ein Ring, M ein R-Linksmodul und X eine Menge. Zeigen Sie, dass die Menge M^X der Abbildungen von X nach M zu einem R-Linksmodul wird, wenn man wie üblich die Addition von Abbildungen durch $(f+g)(x) := f(x)+g(x)$ und die Multiplikation mit Elementen $r \in R$ durch $(rf)(x) := rf(x)$ definiert.

Zeigen Sie, dass die Menge $M^{(X)}$ der Abbildungen von X nach M mit endlichem Träger ein Untermodul von M^X ist.

Lösungshinweise: — *Im ersten Teil prüft man direkt die Modul-Axiome nach und im zweiten Teil muss man noch sehen, dass die Eigenschaft des endlichen Trägers bei Addition und Multiplikation mit Ringelementen erhalten bleibt.* —

1.2. Jeder Ring R ist auf natürliche Weise ein Linksmodul über sich selbst. Zeigen Sie, dass $I \subset R$ genau dann ein Linksideal ist, wenn es ein R-Linksmodul ist.

Lösungshinweise: — *Sowohl ein Linksideal in R, als auch ein R-Modul, der in R enthalten ist, sind abelsche Untergruppen von R, die durch Multiplikation mit Elementen aus R von links in sich überführt werden. Die Ringrechenregeln und die Modulgesetze gehen dabei gerade ineinander über.* —

1.3. Kann $\mathbb{Z}/2$ zu einem $\mathbb{Z}/4$-Modul gemacht werden?
Kann umgekehrt $\mathbb{Z}/4$ zu einem $\mathbb{Z}/2$-Modul gemacht werden?

Lösungshinweise: — *Die Multiplikation $\mathbb{Z}/4 \times \mathbb{Z}/2 \to \mathbb{Z}/2 : (a,b) \mapsto ab$ ist wohldefiniert und erfüllt die Modulgesetze.*
Andersherum funktioniert es aber nicht. Wenn man eine Multiplikation $\mathbb{Z}/2 \times \mathbb{Z}/4 \to \mathbb{Z}/4$ definieren möchte, die eine Modulstruktur ergibt, so muss $1 \cdot a = a$ definiert werden. Dies führt aber auf $a = 1 \cdot a = 3 \cdot a = a+a+a = 3a$, was in $\mathbb{Z}/4$ nicht stimmt. —

S 1.4. (4 Punkte) Wir betrachten im Folgenden $\mathbb{Q}$ als $\mathbb{Z}$-Modul.

(a) Ist $\mathbb{Q}$ endlich erzeugt?
(b) Zeigen Sie, dass $\mathbb{Q}$ nicht frei ist.
(c) Zeigen Sie, dass es in $\mathbb{Q}$ eine unendliche, echt aufsteigende Kette von Untermoduln $M_1 < M_2 < \ldots < \mathbb{Q}$ gibt.
(d) Jeder endlich erzeugte $\mathbb{Z}$-Untermodul von $\mathbb{Q}$ ist frei vom Rang 1.

Bemerkung: Man nennt einen Modul M *noethersch*, wenn jede echt aufsteigende Kette $M_1 < M_2 < \ldots < M$ von Untermoduln endlich ist. $\mathbb{Q}$ ist als $\mathbb{Z}$-Modul also nicht noethersch.

Lösungshinweise: —

(a) *$\mathbb{Q}$ ist nicht endlich erzeugt, denn zu jeder endlichen Menge von Brüchen $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ kann man $b = kgV(b_1, \ldots, b_n)$ bilden. Das Erzeugnis ist dann enthalten im Untermodul $\mathbb{Z}[\frac{1}{b}] \neq \mathbb{Q}$.*
(b) *Wenn $\mathbb{Q}$ frei wäre, so müsste die Basis nach (a) unendlich viele Elemente enthalten, also insbesondere zwei verschiedene $\frac{a}{b}$ und $\frac{c}{d}$. Nun ist aber $cb\frac{a}{b} - ad\frac{c}{d} = 0$ eine nichttriviale $\mathbb{Z}$-Linarkombination der 0. Die beiden Brüche sind also nicht Elemente einer Basis.*
(c) *Man betrachte zum Beispiel $M_i = \mathbb{Z}[\frac{1}{2^i}]$. Dies sind Untermoduln von $\mathbb{Q}$ und M_{i+1} ist stets echt größer als M_i.*

(d) *Sei M ein endlich erzeugter $\mathbb{Z}$-Modul in $\mathbb{Q}$, erzeugt von den Brüchen $\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}$, so ist $M \subset \mathbb{Z}[\frac{1}{b}]$, wobei $b = kgV(b_1,\dots,b_n)$, wie in (a). Damit existiert in M ein kleinstes positives Element der Form $\frac{a}{b}$. Jedes andere ist ein $\mathbb{Z}$-Vielfaches davon, denn sei $m \in M$, dann gibt es $k \in \mathbb{Z}$ mit $k\frac{a}{b} \leq m < (k+1)\frac{a}{b}$ und damit ist $m - k\frac{a}{b} \in M$ mit $0 \leq m - k\frac{a}{b} < \frac{a}{b}$, also wegen Minimalität $m = k\frac{a}{b}$. Diese Darstellung ist auch eindeutig, weil $\mathbb{Q}$ ein Integritätsring ist.*

—

1.5. Zeigen Sie, dass alle $\mathbb{Z}$-Moduln $M \subset \mathbb{R}$ entweder dicht oder diskret sind. Dabei heißt *diskret*, dass es zu jedem Element $m \in M$ eine Umgebung $U \subset \mathbb{R}$ gibt, so dass $M \cap U = \{m\}$ gilt. *Dicht* bedeutet, dass zu jeder Zahl $r \in \mathbb{R}$ und $\varepsilon > 0$ stets ein $m \in M$ existiert, so dass $|r - m| < \varepsilon$.
Angenommen $M \subset \mathbb{R}$ ist diskret, welchen Rang kann M dann haben?

Lösungshinweise: — *Wenn M diskret ist, so gibt es ein $\delta > 0$, so dass alle positiven Modulelemente $> \delta$ sind. Damit folgt aber auch, dass der Abstand zwischen je zwei Elementen immer größer als δ sein muss, da sonst die Differenz der beiden Elemente in der δ-Umgebung der 0 liegen würde. Damit gibt es insbesondere ein minimales positives Element in M. Dieses erzeugt ganz M mit demselben Argument wie in Aufgabe 1.4 (d). Also ist der Modul frei vom Rang 1.*
Ist andererseits M nicht diskret, so gibt einen Häufungspunkt von M in $\mathbb{R}$. Damit muss aber auch 0 ein Häufungspunkt sein, da die Differenzen der Elemente am HP, selbst wieder Modulelemente sind. Zu jedem $\varepsilon > 0$ gibt es also ein $m \in M$ mit $0 < m \leq \varepsilon$. Die Vielfachen von m bilden in $\mathbb{R}$ damit ein ε-Netz. Da ε beliebig war, folgt, dass M dicht in $\mathbb{R}$ liegt.
Man kann in $\mathbb{R}$ freie $\mathbb{Z}$-Moduln von beliebig hohem (höchstens abzählbaren) Rang einbetten: Zum Beispiel ist $\mathbb{Z}[\sqrt{2},\sqrt{3}]$ frei vom Rang 2. —

1.6. Zeigen Sie, dass $\{3,5\}$ ein minimales Erzeugendensystem des $\mathbb{Z}$-Moduls $\mathbb{Z}$ ist (in dem Sinne, dass man kein Element weglassen kann), aber keine Basis. Können Sie auch eine 3-elementige Menge angeben, die ein minimales Erzeugendensystem bildet? (Eine n-elementige Menge für beliebiges n?)

Lösungshinweise: — *Lässt man eines der Elemente weg, so ergeben sich als Erzeugnisse $5\mathbb{Z}$ und $3\mathbb{Z}$, also offenbar nicht ganz $\mathbb{Z}$. Beide zusammen erzeugen aber $\mathbb{Z}$, da $1 = 2\cdot 3 + (-1)\cdot 5$. Es ist keine Basis, da man keine eindeutige Darstellbarkeit hat, z.B. $0 = 3\cdot 5 + (-5)\cdot 3$.*
Wenn man n Zahlen aus $\mathbb{Z}$ wählt, so dass jeweils $n-1$ davon einen echten gemeinsamen Teiler besitzen, aber der ggT aller Zahlen 1 ist, so ergibt sich ein minimales Erzeugendensystem der Größe n. Zum Beispiel ist für $n = 3$: $12 = 2^2\cdot 3, 10 = 2\cdot 5, 15 = 3\cdot 5$ eine solche Menge. —

2. Diverse Gegenbeispiele

Untermoduln eines freien Moduls sind nicht notwendig frei:

S 2.1. (3 Punkte) Sei K ein Körper und sei $R = K[X,Y]$ der Polynomring in den Variablen X,Y. Als R-Modul ist R frei mit Basis 1. Das Ideal (X,Y) ist als R-Untermodul nicht frei.

Lösungshinweise: — *Nehmen wir an, (X,Y) wäre ein freier $K[X,Y]$-Modul. Dann gäbe es Elemente $p_1,\dots,p_n \in (X,Y)$ in der Basis, so dass $X = \sum_{i=1}^n a_i p_i$ und $Y = \sum_{i=1}^n b_i p_i$ wobei $a_i, b_i \in K[X,Y]$. Wir setzen das in die Gleichung $0 = XY - YX$ jeweils für den zweiten Faktor ein und erhalten $0 = \sum_{i=1}^n (Xb_i - Ya_i)p_i$. Wenn die p_i in einer Basis enthalten sind, müssen alle Koeffizienten in der Linearkombination 0 sein, also $Xb_i = Ya_i$ für alle i. Damit sind aber alle a_i durch X teilbar und alle b_i durch Y teilbar, weil $K[X,Y]$*

faktoriell ist (Satz von Gauß). Wir bekommen also $1 = \sum_{i=1}^{n} \frac{a_i}{X} p_i \in (X,Y)$*, und somit einen Widerspruch dazu, dass* $(X,Y) \neq K[X,Y]$. —

Wenn ein Untermodul U eines freien Moduls M selbst wieder frei ist, dann muss nicht unbedingt $\operatorname{rang} U \leq \operatorname{rang} M$ gelten:

2.2. Sei $M = \{X,Y\}^*$ das freie Monoid bestehend aus allen endlichen Wörtern über dem Alphabet $\{X,Y\}$. Sei K ein Körper und sei $R = KM$ der nicht-kommutative Polynomring in den Variablen X,Y. Als R-Linksmodul ist R frei mit Basis 1. Man konstruiere einen freien Untermodul $U \subset R$ vom Rang 2.

Lösungshinweise: — *Der Untermodul RX ist frei mit Basis X; er besteht aus den R-Linearkombinationen von Monomen die mit dem Buchstaben X enden. Entsprechendes gilt für den Untermodul RY. Daraus folgt* $RX \cap RY = \{0\}$*. Der Untermodul* $RX \oplus RY$ *ist demnach frei vom Rang* 2. —

Man würde erwarten, dass in einem endlich erzeugten K-Modul jeder Untermodul $U \subset M$ über K endlich erzeugt ist. Dies gilt nicht für beliebige Ringe:

2.3. Sei $R = K[X_n \mid n \in \mathbb{N}]$ der Polynomring über einem Körper K in unendlich vielen Variablen $X_0, X_1, X_2, \ldots$. Als R-Modul ist R frei vom Rang 1, also insbesondere endlich erzeugt. Das Ideal $(X_n \mid n \in \mathbb{N})$ ist als R-Untermodul nicht endlich erzeugt.

Lösungshinweise: — *Seien* $p_1, \ldots, p_k \in (X_n \mid n \in \mathbb{N})$ *endlich viele Polynome. Dann gibt es ein* $m \in \mathbb{N}$*, so dass die Variable* X_m *in keinem der Polynome* p_i *auftaucht. Wenn die obigen Polynome ein Erzeugendensystem bilden sollen, so muss die Gleichung* $X_m = \sum_{i=1}^{k} a_i p_i$ *trotzdem lösbar sein.*
Die Koeffizienten a_i *kann man dabei zerlegen in eine Summe* $a_i = X_m b_i + c_i$*, so dass* X_m *in* c_i *nicht auftritt. Damit folgt, dass* $X_m = X_m \sum_{i=1}^{k} b_i p_i + \sum_{i=1}^{k} c_i p_i$ *Die hintere Summe kann nur dann durch* X_m *teilbar sein, wenn sie verschwindet. Damit ergibt sich nach Teilen durch* X_m*:* $1 = \sum_{i=1}^{k} b_i p_i \in (X_n \mid n \in \mathbb{N})$*. Dies ist aber nicht wahr und somit haben wir einen Widerspruch.* —

3. Elementarteiler

V 3.1. Bringen Sie über $\mathbb{Z}$ die Matrix

$$A = \begin{pmatrix} 3 & 0 & 3 & -3 \\ 3 & 4 & 7 & 3 \\ -6 & -3 & -9 & -6 \\ 3 & 2 & 5 & 3 \end{pmatrix}$$

in Elementarteilerform. Zusatz: Geben Sie hierzu Matrizen $S, S^{-1}, T, T^{-1} \in GL_4(\mathbb{Z})$ an, so dass $SAT = D$ eine Diagonalmatrix mit Einträgen $d_1 \mid \cdots \mid d_4$ ist.

Lösungshinweise: — *Man führt Spalten und Zeilenumformungen durch, um auf die Elementarform der Matrix zu kommen. Dabei ergeben sich dann* S, T, S^{-1} *und* T^{-1} *aus den entsprechenden Produkten der Umformungsmatrizen, die man von links und rechts an A hinmultipliziert. Elementarteiler sind:* $1, 3, 6, 0$

$$S = \begin{pmatrix} 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & -2 & -3 \\ 0 & 1 & -2 & -5 \end{pmatrix}, \qquad S^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 4 & 1 & 1 & 1 \\ -3 & -2 & -2 & 0 \\ 2 & 1 & 1 & 0 \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

—

4. MATRIZENRINGE

4.1. Sei R ein Ring und $S = R^{n\times n}$ der Matrizenring über R. Daraus kann man nun wiederrum den Ring $T = S^{m\times m}$ bauen. Ist T isomorph zu $R^{nm\times nm}$?

Lösungshinweise: — *Dieser Isomorphismus besteht tatsächlich. Man kann sich also eine $nm\times nm$ Matrix immer aus $n\times n$ oder aus $m\times m$-Matrizen zusammengesetzt denken. Man teile dazu die Matrizen A und B in m^2 $n\times n$ Matrizen A_{ij} und B_{ij} auf ($0\le i,j<m$!!). Dann kann man den Matrixeintrag an der Stelle $(in+k, jn+l)$ $(1\le k,l\le n)$ auch folgendermaßen ausrechnen:*

$$((AB)_{ij})_{kl} = \left(\sum_{r=0}^{m-1} A_{ir}B_{rj}\right)_{kl} = \sum_{r=0}^{m-1}(A_{ir}B_{rj})_{kl} = \sum_{r=0}^{m-1}\sum_{s=1}^{n}(A_{ir})_{ks}(B_{rj})_{sl}$$
$$= \sum_{r=0}^{m-1}\sum_{s=1}^{n} a_{(in+k)(rn+s)}b_{(rn+s)(jn+l)} = \sum_{u=1}^{nm} a_{(in+k)u}b_{u(jn+l)} = (AB)_{(in+k)(jn+l)}$$

—

4.2. Sei R ein Ring und $S = R^{n\times n}$ der Matrizenring über R. Bestimmen Sie das Zentrum $Z(S) = \{A\in S : AB = BA \text{ für alle } B\in S\}$ von S.

Lösungshinweise: — *Durch Multiplikation einer Matrix A im Zentrum mit Elementarmatrizen (Vertauschung zweier Spalten/Zeilen, Addition einer Zeile/Spalte zu einer anderen) erhält man aus den Relationen $AB = BA$, dass die Nebendiagonaleinträge 0 und die Diagonaleinträge alle gleich sind. Eine solche Matrix kommutiert aber nur dann mit allen Diagonalmatrizen, wenn das Diagonalelement im Zentrum von R liegt. Diese Matrizen kommutieren nun wirklich mit allen Matrizen, wie man leicht nachprüft, also $Z(S) = Z(R)1_S$.* —

S 4.3. (3 Punkte) Zeigen Sie, dass die Spalten einer Matrix $A\in\mathbb{Z}^{n\times n}$ genau dann eine Basis von $\mathbb{Z}^n$ sind, wenn $\det(A) = \pm 1$ gilt. (Was gilt entsprechend über einem beliebigen kommutativen Ring?)

Lösungshinweise: — *Eine Matrix A in $R^{n\times n}$ ist genau dann invertierbar, wenn die Determinante in $R^\times$ liegt, wie man aus dem Determinantenmultiplikationssatz und der adjunkten Matrix sieht. Wenn eine Matrix invertierbar ist, so sind ihre Spalten eine Basis des R^n, da man jedes LGS der Form $Ax = b$ eindeutig lösen kann. Andererseits sind im Falle, dass die Spalten eine Basis bilden die Gleichungssysteme ebenfalls eindeutig lösbar und somit auch für $b = e_i$, wobei e_i die "Standardeinheitsvektoren" sind. Damit wird dann die Gleichung $AB = E$ lösbar, also ist A invertierbar.* —

5. DIMENSIONSINVARIANZ

Dass die "Dimensionsinvarianz" nicht selbstverständlich ist, zeigt bereits der Nullring $R = \{0\}$: hier ist R^n der Nullmodul für jedes $n\in\mathbb{N}$. Es gibt aber auch nicht-triviale Ringe R sodass $R^n\cong R^m$ für $n\neq m$ als R-Moduln isomorph sind:

5.1. Sei K ein Körper und $R = \mathrm{End}_K(K[X])$ der Ring der K-linearen Abbildungen $K[X]\to K[X]$. Man konstruiere einen Isomorphismus $R^2\cong R$ von R-Linksmoduln.

Hinweis: Seien $f_0, f_1\in R$ definiert durch $f_i(X^k) = X^{(k-i)/2}$ für $k-i$ gerade und $f_i(X^k) = 0$ sonst. Ist f_0, f_1 eine Basis von R über sich selbst? Kann man ebenso eine Basis von R mit beliebiger Länge $n\in\mathbb{N}_{\ge 1}$ herstellen?

Lösungshinweise: — *Wir betrachten die Abbildung: $\varphi : R^2\to R : (g,h)\mapsto gf_0+hf_1$ und wollen zeigen, dass es sich hierbei um einen R-Modulisomorphismus handelt.*
Zunächst prüft man direkt nach, dass φ additiv ist und $\varphi(r(g,h)) = r\varphi(g,h)$ erfüllt, also ein Modulhomomorphismus ist. Um zu zeigen, dass φ injektiv ist, betrachten wir die Gleichung $gf_0+hf_1 = g'f_0+h'f_1$,

bzw. $(g-g')f_0 = (h'-h)f_1$. *Die zwei Abbildungen sind genau dann gleich, wenn sie Polynome in der gleichen Weise abbilden. Allerdings bildet die linke Seite alle Monome mit ungeradem Exponenten auf* 0 *ab und die rechte Seite alle Monome mit geradem Exponenten. Damit müssen beide Abbildungen identisch* 0 *sein und somit* $g = g'$ *und* $h = h'$ *(da* f_0, f_1 *surjektiv und damit links kürzbar sind).*
Für die Surjektivität von φ *betrachten wir einen Endomorphismus* $t \in R$ *und suchen* g, h, *so dass* $gf_0 + hf_1 = t$. *Weil Elemente aus R durch ihre Bilder auf den Monomen* X^k *festgelegt sind, können wir* $g(X^k) = t(X^{2k})$ *und* $h(X^k) = t(X^{2k+1})$ *setzen und die Gleichung* $gf_0 + hf_1 = t$ *folgt direkt aus der Definition von* f_0 *und* f_1.

—

Wir wollen zeigen, dass solche Pathologien über kommutativen Ringen nicht möglich sind. Sei dazu im Folgenden R ein kommutativer Ring und $I \lhd R$ ein Ideal.

V 5.2. (a) Zu jedem R-Modul M ist $IM := \{\sum_{k=1}^{n} a_k m_k : a_k \in I, m_k \in M\}$ ein Untermodul von M.
(b) Wir wissen, dass M/IM ein Modul über R ist. Zeigen Sie, dass M/IM auch ein Modul über R/I wird, wenn man $(r+I)(m+IM) := (rm+IM)$ definiert.
(c) Im Fall $M = R^n$ konstruiere man einen Isomorphismus $R^n/IR^n \cong (R/I)^n$.

Lösungshinweise: —

(a) *Nachrechnen!*
(b) *Die Moduleigenschaften vererben sich von R auf* R/I. *Man muss nur prüfen, ob die Multiplikation mit Ringelementen wohldefiniert ist. Dies sieht man durch Ausmultiplizieren des Produktes, welches* $(r+I)(m+IM) = rm+Im+rIM+IIM = rm+IM$ *liefert, da I ein Ideal und IM eine abelsche Gruppe ist.*
(c) *Man zeigt zuerst, dass* $IR^n = I^n$ *gilt. Die Implikation* $\subset$ *folgt, da I ein Ideal ist und die andere Richtung daraus, dass R eine* 1 *enthält.*
Dann muss man noch zeigen, dass $\varphi : R^n \to (R/I)^n : \varphi(r_1, \ldots, r_n) \to (r_1+I, \ldots, r_n+I)$ *ein Modulhomomorphismus ist, der* I^n *als Kern besitzt. Der Rest folgt mit dem Isomorphiesatz.*

—

Wir setzen im Folgenden als bekannt voraus, dass jeder kommutative Ring mit $1 \neq 0$ ein maximales Ideal $I \subset R$ besitzt. Der Quotientenring R/I ist dann ein Körper.

V 5.3. Sei R ein kommutativer Ring mit $1 \neq 0$. Zeigen Sie, dass aus einem Isomorphismus $R^m \cong R^n$ von R-Moduln die Gleichheit $m = n$ folgt.

Lösungshinweise: — *Sei I ein maximales Ideal in R. Dann ist* R/I *ein Körper. Wenn es einen R-Modulisomorphismus* $\varphi : R^m \to R^n$ *gibt, so bildet dieser den Untermodul* IR^m *nach* IR^n *ab. Damit gibt es einen Isomorphismus zwischen* R^m/IR^m *und* R^n/IR^n. *Nach Aufgabe 5.2 sind die beiden Moduln sogar Vektorräume* $(R/I)^m$ *bzw.* $(R/I)^n$. *Aus der linearen Algebra wissen wir aber, dass isomorphe Vektorräume die gleiche Dimension haben, also* $n = m$. —