Lineare Algebra II
Lösungsvorschläge zum Tutoriumsblatt 5

Moritz Fleischmann

Zur Vorlesung von Prof. Dr. Fabien Morel, Dr. Andrei Lavrenov, Katharina Novikov und Oliver Hendrichs im Sommersemester 25

Disclaimer: Das sind keine offiziellen Lösungen, sondern nur eine getexte Version der Lösungen zu ausgewählten Aufgaben (Dank geht hierbei an Andrei Lavrenov für seine Lösungsskizzen), die ich in meinem Tutorium bespreche. Fehler, Fragen oder Anmerkungen gerne an m.fleischmann@mnet-online.de. Verteilung der Lösungen ist erlaubt und erwünscht.

Wie üblich, wen das Vorgeplänkel nicht interessiert, der kann die Lösungen in den grau hinterlegten Boxen finden. Es gilt grundsätzlich, dass $\mathbb{K} \subseteq \mathbb{C}$.

Aufgabe 1

Sei R ein Ring und

$$R[X_1, \dots, X_n] \coloneqq (R[X_1, \dots, X_{n-1}])[X_n]$$

der Polynomring in n Variablen. Zeige, dass

$$\begin{aligned} \Phi : \mathsf{hom}_{\mathsf{ring}}(\mathbb{Z}[X_1, \dots, X_n], R) &\to R^n \\ f &\mapsto (f(X_1), f(X_2), \dots, f(X_n)) \end{aligned}$$

eine bijektive Abbildung ist.

Lösung:

Wir zeigen Surjektivität und Injektivität. Vorher wollen wir uns noch überlegen wieso es ausreicht unsere Homomorphismen über $f(X_j)$ für alle $j \in [n]$ zu beschreiben: Sei $P \in \mathbb{Z}[X_1, \dots, X_n]$. Wir wollen es nun mithilfe von Multiindizes explizit ausdrücken. Ein Multiindex ist ein Tupel $D = (d_1, \dots, d_n) \in \mathbb{N}_0^n$. Wir definieren

$$X^D \coloneqq X_1^{d_1} \cdot \ldots \cdot X_n^{d_n}$$

Jedes mögliche Monom entspricht nun einem Term $\alpha_D X^D$ wobei $\alpha_D \in \mathbb{Z}$ die Koeffizienten sind. Wir können ein Polynom P nun schreiben als[a]

$$P = \sum_{D \in \mathbb{N}_0^n} \alpha_D X^D$$

und die Wirkung durch f ist wegen der Gleichung

$$\begin{aligned} f(P) &= f\left(\sum_{D\in\mathbb{N}_0^n} \alpha_D X^D\right) \\ &= \sum_{D\in\mathbb{N}_0^n} \alpha_D f\left(X^D\right) \\ &= \sum_{D\in\mathbb{N}_0^n} \alpha_D f\left(X_1^{d_1}\right)\cdot\ldots\cdot f\left(X_n^{d_n}\right) \\ &= \sum_{D\in\mathbb{N}_0^n} \alpha_D f(X_1)^{d_1}\cdot\ldots\cdot f(X_n)^{d_n} \end{aligned}$$

bereits vollständig bestimmt, wenn man die Terme $f(X_j)$ kennt. Man beachte dazu auch, dass die konstanten Terme unabhängig von der Wahl von f abgebildet werden. Dazu sei $\alpha_0 \in R$, dann gilt:

$$f(\alpha_0) = \alpha_0 f(\mathbb{1}_{\mathbb{Z}}) = \alpha_0 \mathbb{1}_R$$

wobei $\alpha_0\mathbb{1}_R$ hier im Sinne des α_0-fachen Aufsummierens der Eins aus R gemeint ist.

1. *Surjektivität:* Sei $(r_1,\ldots,r_n) \in R^n$ ein Tupel dessen Urbild wir suchen. Es gibt einen Homomorphismus

   $$\begin{aligned} f : \mathbb{Z}[X_1,\ldots,X_n] &\to R \\ X_j &\mapsto r_j \end{aligned}$$

   dann gilt $\Phi(f) = (f(X_1),\ldots,f(X_n)) = (r_1,\ldots,r_n)$. Mit der obigen Überlegung ist der Homomorphismus bereits eindeutig ausgewählt und die Surjektivität von Φ gezeigt.

2. *Injektivität:* Seien $\Phi(f) = \Phi(g)$, dann gilt

   $$(f(X_1),\ldots,f(X_n)) = \Phi(f) = \Phi(g) = (g(X_1),\ldots,g(X_n))$$

   also $\forall j \in [n] : f(X_j) = g(X_j)$. Wir hatten allerdings oben gezeigt, dass ein Homomorphismus durch die Wahl seiner Wirkung auf alle X_j bereits eindeutig bestimmt wird. Also gilt $f = g$ und die Abbildung ist injektiv.

Zusammen ist die Abbildung also bijektiv.

[a] Ein Polynom ist laut Definition ein Tupel von Koeffizienten von denen nur endlich viele ungleich Null sind. Wir führen die Summe zwar über $\mathbb{N}_0^n$ durch, aber dennoch hat die Summe nur endlich viele Terme, man muss sich also keine Gedanken um Konvergenz machen.

Mit dieser Aufgabe sehen wir, dass es einfach ist, einen Homomorphismus von den ganzzahligen Polynomen in n Variablen auf einen beliebigen Ring zu konstruieren. Jeder Homomorphismus wird durch die Bilder der Variablen bereits restlos bestimmt.

Aufgabe 2

Wir betrachten den Ring $S = \mathbb{Z}[X_{j,k}, Y_{j,k}]_{j,k\in[n]}$. Wir definieren die "universellen Matrizen" durch

$$A := (X_{j,k})_{j,k\in[n]} \in S^{n\times n}, \quad B := (Y_{j,k})_{j,k\in[n]} \in S^{n\times n}$$

1. Zeige, dass $\det(AB) = \det(A)\det(B)$ gilt.

2. Sei R ein beliebiger Ring und seien $M, N \in R^{n\times n}$. Zeige, dass $\det(MN) = \det(M)\det(N)$ gilt.

Lösung:
Wir benötigen in dieser Aufgabe folgenden Satz:

> Sei R ein Ring. Dann sind die folgenden drei Aussagen äquivalent:
>
> 1. R ist ein Integritätsring.
> 2. $R[X]$ ist ein Integritätsring.
> 3. $R[X_1, \ldots, X_n]$ ist ein Integritätsring $\forall n \in \mathbb{N}$.
>
> wobei 2) $\Leftrightarrow$ 3) direkt aus 1) $\Leftrightarrow$ 2) folgt.

und folgenden Satz:

> Sei $\mathbb{K}$ ein Körper und seien $A, B \in \mathbb{K}^{n\times n}$, dann gilt
>
> $$\det(AB) = \det(A)\det(B)$$

und die Definition des Quotientenkörpers:

> Sei S ein Integritätsring. Dann definieren wir den *Quotientenkörper von* S als
>
> $$Q(S) := \{(a, b) \mid a \in R, b \in R\backslash\{0\}\}/\sim$$
>
> wobei $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ gilt. Wir schreiben $(a, b) = \frac{a}{b}$ und versehen diesen Körper mit Addition und Multiplikation analog zu $\mathbb{Q}$.

Es gibt stets einen Monomorphismus $\iota : S \to Q(S)$ der S zu einem Teilring von $Q(S)$ macht. Die Definition ist sehr ähnlich zur Definition der rationalen Zahlen. Tatsächlich gilt auch $Q(\mathbb{Z}) = \mathbb{Q}$ - diese Definition hier ist allerdings wesentlich allgemeiner, da sie eben bei alle Integritätsringen funktioniert, z.B.: auch über Polynomringen über $\mathbb{Z}$.

Wir haben es in dieser Aufgabe mit Determinanten über verschiedenen algebraischen Strukturen zu tun. Üblicherweise wird das nicht weiter gekennzeichnet, da man anhand des Arguments erkennen kann, welche Determinante gerade gemeint ist, aber wir werden hier zum besseren Verständnis für eine Determinante über einem Ring R stets $\det_R$ schreiben.

1. Wir wollen das Problem der Multiplikativität der Determinante auf den Fall in Körpern zurückführen. Wir betrachten also $Q(S)$, den Körper über dem Polynomring in $2n^2$ Variablen. Da $\iota : S \to Q(S)$ garantiert, dass S ein Teilring von $Q(S)$ ist, gibt es die Elemente $X_{j,k}, Y_{j,k}, \forall j, k \in [n]$ auch als Elemente von $Q(S)$. Man kann diese Elemente direkt mit ihren Gegenstücken aus S identifizieren.
   Das heißt die Matrizen A und B, wie in der Definition angegeben, existieren auch als Matrizen in $Q(S)^{n\times n}$. Da $Q(S)$ ein Körper ist, gilt dort

   $$\det_{Q(S)}(AB) = \det_{Q(S)}(A)\det_{Q(S)}(B)$$

   Da die Determinanten Summen und Produkte von Elementen in S sind, liegen auch die Determinanten selbst in S und damit gilt $\det_S(C) = \det_{Q(S)}(C)$ für alle Matrizen $C \in S^{n\times n}$

und damit gilt

$$\det_S(AB) = \det_{Q(S)}(AB) = \det_{Q(S)}(A)\det_{Q(S)}(B) = \det_S(A)\det_S(B)$$

was wir zeigen wollten.

2. Erneut wollen wir die Multiplikativität auf einen Körper zurückführen. Da R nun allerdings ein beliebiger Ring ist, können wir nicht den gleichen Trick anwenden und die Multiplikativität in $Q(R)$ verwenden. Stattdessen nutzen wir aus, dass es eine Bijektion zwischen den Homomorphismen $S \to R$ und R^{2n^2} gibt und führen den Fall auf S und damit auf $Q(S)$ zurück. Dazu überlegen wir uns zuerst folgendes:
Sei $f : S \to R$ ein Homomorphismus, dann induziert dieser einen weiteren Homomorphismus für Matrizen:

$$F : S^{n\times n} \to R^{n\times n}$$
$$(\alpha_{j,k})_{j,k\in[n]} \mapsto (f(\alpha_{j,k}))_{j,k\in[n]}$$

wobei wir die Matrizen über ihre Einträge beschreiben.
Wir müssen zeigen, dass das ein Homomorphismus ist. Wir zeigen das beispielhaft an der Multiplikation, die Addition erfolgt analog, ist aber deutlich simpler. Seien dafür $A = (\alpha_{j,k})_{j,k\in[n]}$ und $B = (\beta_{j,k})_{j,k\in[n]}$ in $S^{n\times n}$. Dann gilt mit der Definition der Matrixmultiplikation für einen Eintrag j, k:

$$(F(AB))_{j,k} = f\left(\sum_{l=1}^{n}\alpha_{j,l}\beta_{l,k}\right) = \sum_{l=1}^{n} f(\alpha_{j,l})f(\beta_{l,k}) = (F(A)\cdot F(B))_{j,k}$$

also erhält F die Multiplikation. Zeigen wir noch die Addition sehen wir, dass F ein Homomorphismus ist.
Als nächstes zeigen wir, dass $\det_R(F(A)) = f(\det_S(A))$ für alle $A \in S^{n\times n}$ gilt. Dazu wenden wir die Leibniz-Formel für Determinanten an:

$$\begin{aligned}\det_R(F(A)) &= \sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{k=1}^{n}(F(A))_{k,\sigma(k)}\\ &= \sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{k=1}^{n} f(\alpha_{k,\sigma(k)})\\ &= f\left(\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{k=1}^{n}\alpha_{k,\sigma(k)}\right) = f(\det_S(A))\end{aligned}$$

Seien nun $M, N \in R^{n\times n}$ beliebig gegeben. Jede der Matrizen hat exakt n^2 Einträge, zusammen also $2n^2$. Sei $M = (m_{j,k})_{j,k\in[n]}$ und $N = (n_{j,k})_{j,k\in[n]}$, dann existiert laut Aufgabe 1 genau ein Homomorphismus $f : S \to R$, sodass

$$\forall k, j \in [n] : f(X_{j,k}) = m_{j,k}, \quad f(Y_{j,k}) = n_{j,k}$$

Betrachten wir davon induzierten Homomorphismus $F : S^{n\times n} \to R^{n\times n}$ erhalten wir

$$F(A) = M, \quad F(B) = N$$

und mit den obigen Aussagen erhalten wir

$$\begin{aligned}\det_R(M \cdot N) &= \det_R(F(A) \cdot F(B)) \\ &\overset{(1)}{=} \det_R(F(A \cdot B)) \\ &\overset{(2)}{=} f(\det_S(A \cdot B)) \\ &\overset{(3)}{=} f(\det_S(A) \cdot \det_S(B)) \\ &\overset{(4)}{=} f(\det_S(A)) \cdot f(\det_S(B)) \\ &\overset{(2)}{=} \det_R(F(A)) \cdot \det_R(F(B)) = \det_R(M) \cdot \det_R(N)\end{aligned}$$

wobei wir in (1) verwendet haben, dass F ein Homomorphismus ist. In (2) haben wir verwendet, dass $\det_R(F(A)) = f(\det_S(A))$ gilt. In (3) haben wir die erste Teilaufgabe verwendet und in (4) haben wir verwendet, dass f ein Homomorphismus ist. Die zu zeigende Aussage ist gezeigt.

Aufgabe 3

Sei R ein beliebiger Ring und $M \in R^{n\times n}$. Sei $\hat{M}_{j,k}$ die Matrix die entsteht, wenn man in M die j-te Zeile und k-te Spalte streicht. Wir definieren den (j,k)-ten Minor als $M_{j,k} := \det(\hat{M}_{j,k})$.
Weiter definieren wir die Kofaktoren $C_{j,k} := (-1)^{j+k} M_{j,k}$ und die Kofaktormatrix als $(\tilde{M}_{j,k})_{j,k\in[n]} = C_{j,k}$.
Zeige, dass $M \cdot \tilde{M}^T = \det(M) \cdot \mathbb{1}_n$.

Lösung:
Wir werden hier nicht mehr kennzeichnen über welcher Struktur die Determinanten sind. Dennoch sollte man sich stets bewusst sein, welche Determinante man gerade behandelt.

Die Lösung verläuft ähnlich zur zweiten Teilaufgabe der zweiten Aufgabe. Wir betrachten den Polynomring $S = \mathbb{Z}[X_{i,j}]_{i,j\in[n]}$ in n^2 Variablen und die "universelle Matrix" $A = (X_{j,k})_{j,k\in[n]}$. Analog zur Aufgabe 2.1 betrachten wir den Quotientenkörper $Q(S)$ und die Matrix $A \in Q(S)$, deren Einträge jedoch noch in S liegen. Da $Q(S)$ ein Körper ist, gilt hier

$$A \cdot \tilde{A}^T = \det(A) \cdot \mathbb{1}_n$$

Sei nun eine beliebige Matrix $M = (m_{j,k})_{j,k\in[n]}$ gegeben. Wir betrachten erneut einen Homomorphismus $f : S \to R$ der durch

$$\forall j,k \in [n] : f(X_{j,k}) = m_{j,k}$$

definiert wird. Erneut betrachten wir auch den induzierten Homomorphismus

$$\begin{aligned}F : S^{n\times n} &\to R^{n\times n} \\ (\alpha_{j,k})_{j,k\in[n]} &\mapsto (f(\alpha_{j,k}))_{j,k\in[n]}\end{aligned}$$

Es gilt dann:

$$\begin{aligned} M \cdot \tilde{M}^T &= F(A) \cdot F(\tilde{A}^T) \\ &= F(A \cdot \tilde{A}^T) \\ &= F(\det(A)\mathbb{1}_n^S) \\ &= f(\det(A))F(\mathbb{1}_n^S) \\ &= \det(F(A))\mathbb{1}_n^R = \det(M)\mathbb{1}_n^R \end{aligned}$$

wobei wir verwendet haben, dass

$$\begin{aligned} F(\det(A)\mathbb{1}_n^S) &= F(\mathsf{diag}(\det(A), \det(A), \ldots, \det(A))) \\ &= \mathsf{diag}(f(\det(A)), \ldots, f(\det(A))) \\ &= f(\det(A))\mathsf{diag}(f(\mathbb{1}_S), \ldots, f(\mathbb{1}_S)) \\ &= f(\det(A))F(\mathbb{1}_n^S) \end{aligned}$$

gilt. Damit gilt die Aussage auch in beliebigen kommutativen Ringen.

Aufgabe 4
Sei $\mathbb{K}$ ein Körper. Die formale Ableitung eines Polynoms

$$P(X) = \sum_{j=0}^{n} \alpha_j X^j \in \mathbb{K}[X]$$

ist definiert als

$$P'(X) = \sum_{j=1}^{n} j\alpha_j X^{j-1} \in \mathbb{K}[X]$$

1. Zeige, dass die Produktregel erfüllt wird: $\forall P, Q \in \mathbb{K}[X] : (PQ)' = P'Q + PQ'$
2. Sei $P \in \mathbb{K}[X]$ ein Polynom, sodass P und P' koprim sind. Zeige, dass P nur einfache Nullstellen haben kann.
3. Sei $\mathsf{char}(\mathbb{K}) = 0$ und sei $P \in \mathbb{K}[X]$ irreduzibel. Sei $\mathbb{E}$ eine Körpererweiterung von $\mathbb{K}$. Zeige, dass P als Polynom über $\mathbb{E}$ nur einfache Nullstellen hat.
4. Sei $P(X) := X^p - 1$ als Polynom in $\mathbb{F}_p[X]$. Sind P und P' koprim?

Lösung:

1. Diese Aufgabe lösen wir durch simples Ausrechnen: Seien dazu $P = \sum_{j=0}^{n} \alpha_j X^j$ und $Q = \sum_{j=0}^{m} \beta_j X^j$. Dann gilt

   $$PQ = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} (\alpha_k \beta_{j-k}) \right) X^j$$

   und damit

   $$(PQ)' = \sum_{j=1}^{n+m} j \left(\sum_{k=0}^{j} (\alpha_k \beta_{j-k}) \right) X^{j-1}$$

Auf der anderen Seite gilt mit der Indexverschiebung $j \to j+1$

$$P' = \sum_{j=1}^{n} j\alpha_j X^{j-1} \in \mathbb{K}[X] = \sum_{j=0}^{n-1} (j+1)\alpha_{j+1} X^j$$

, analog für Q und damit

$$P'Q = \sum_{j=0}^{n+m-1} \left(\sum_{k=0}^{j} (k+1)\alpha_{k+1}\beta_{j-k} \right) X^j, \quad PQ' = \sum_{j=0}^{n+m-1} \left(\sum_{k=0}^{j} \alpha_k (j-k+1)\beta_{j-k+1} \right) X^j$$

und die Summe ist, wobei wir die Indexverschiebung $j \to j-1$ anwenden:

$$\begin{aligned} P'Q + PQ' &= \sum_{j=0}^{n+m-1} \left(\sum_{k=0}^{j} (k+1)\alpha_{k+1}\beta_{j-k} + (j-k+1)\alpha_k\beta_{j-k+1} \right) X^j \\ &= \sum_{j=1}^{n+m} \left(\sum_{k=0}^{j-1} (k+1)\alpha_{k+1}\beta_{j-1-k} + (j-k)\alpha_k\beta_{j-k} \right) X^{j-1} \end{aligned}$$

Es gilt nun für den Koeffizienten γ_j des j-ten Terms:

$$\begin{aligned} \gamma_j &= \sum_{k=0}^{j-1} (k+1)\alpha_{k+1}\beta_{j-1-k} + (j-k)\alpha_k\beta_{j-k} \\ &= j\alpha_0\beta_j + \sum_{k=1}^{j} k\alpha_k\beta_{j-k} + (j-k)\alpha_k\beta_{j-k} \\ &= j \sum_{k=0}^{j} \alpha_k\beta_{j-k} \end{aligned}$$

wobei wir den Index so verschoben haben, dass der linke und rechte Teil unter der Summe zusammen jeweils alle Terme zwischen 1 und j abdecken.
Damit gilt nun

$$P'Q + PQ' = \sum_{j=1}^{n+m} \left(j \sum_{k=0}^{j} \alpha_k\beta_{j-k} \right) X^{j-1} = (PQ)'$$

2. Angenommen P ist ein Polynom mit zweifacher Nullstelle λ. Dann gibt es ein Polynom $Q \in \mathbb{K}[X]$ mit $P = Q(\lambda - X)^2$. In diesem Fall können wir die obige Produktregel anwenden und erhalten:

$$P' = (Q \cdot (\lambda - X)^2)' = Q'(\lambda - X)^2 + 2Q(\lambda - X) = (\lambda - X)(Q'(\lambda - X) + 2Q)$$

also ist $(\lambda - X)$ ein Teiler von P', das heißt P Und P' sind nicht teilerfremd. Sind P und P' also teilerfremd, wie angenommen, dann kann P keine zweifache Nullstelle besitzen.

3. Wir wollen die zweite Teilaufgabe nutzen, denn können wir zeigen, dass P und P' über $\mathbb{E}$ koprim sind, dann kann P keine mehrfache Nullstelle in $\mathbb{E}$ besitzen.
Es reicht aus, die Koprimheit in $\mathbb{K}$ zu zeigen: Angenommen P, P' sind in $\mathbb{K}$ koprim, dann existieren mit dem Lemma von Bézout ($\mathbb{K}[X]$ ist ein euklidischer Ring, also auch ein Haupt-

idealring) $U, V \in \mathbb{K}[X]$, sodass

$$PU + P'V = \mathbb{1}_{\mathbb{K}}$$

Da aber $\mathbb{1}_{\mathbb{K}} = \mathbb{1}_{\mathbb{E}}$ gilt und $\mathbb{K} \subseteq \mathbb{E}$, gilt damit auch

$$PU + P'V = \mathbb{1}_{\mathbb{E}}$$

mit $P, P', V, U \in \mathbb{E}[Y]$, das heißt P, P' sind auch über $\mathbb{E}$ koprim.
Nun zeigen wir die Koprimheit in $\mathbb{K}$: P ist irreduzibel, also hat P keine Teiler außer P und $\mathbb{1}_{\mathbb{K}}$ in $\mathbb{K}[X]$. Angenommen P und P' wären nicht koprim, dann hätten sie einen gemeinsamen, nichttrivialen Teiler Q. Da Q dann Teiler von P wäre, aber P nur den nichttrivialen Teiler P hat, gilt $Q = P$ und damit $P|P'$. Daraus folgt aber, dass $\deg(P) < \deg(P')$.
Da P' die formale Ableitung von P ist, können wir drei Fälle unterscheiden:

(a) Fall 1: $\deg(P) \geq 1 < \infty$. In diesem Fall ist die höchste Potenz von P gleich $X^{\deg(P)}$ also ist die höchste Potenz von P' gleich $X^{\deg(P)-1}$ und damit $\deg(P') < \deg(P)$.

(b) Fall 2: $\deg(P) = 0$. In diesem Fall ist P eine Konstante ungleich 0, also invertierbar. Das heißt aber, dass P nicht irreduzibel sein kann, da irreduzible Elemente per Definition keine Einheiten sind.

(c) Fall 3: $\deg(P) = \infty$. In diesem Fall gilt $P = 0$ und damit auch $P' = 0$. Dann gilt aber $\deg(P) = \deg(P')$.

Alle drei Fälle führen also zum Widerspruch, das heißt unsere Annahme, dass P und P' nicht koprim sind, ist falsch.

4. Da $P = X^p - 1$ gilt $P' = pX^{p-1}$. Da wir in $\mathbb{F}_p[X]$ sind, ist $p = 0$, das heißt $P' = 0$ und damit gilt $P|P'$, das heißt die beiden Polynome sind nicht koprim.