Lineare Algebra II
Lösungsvorschläge zum Tutoriumsblatt 1

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 .

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

1. Rechne in $\mathbb{C}[X]$: Teile $4x^3 + x^3$ durch $x + 1 + i$.
2. Bestimme $ggT(6787, 7194)$.

Lösung:

1. Euklidische Ringe erlauben Division mit Rest und Polynomringe über Körpern sind euklidische Ringe. Wir wenden klassische Polynomdivision an:

$$
\begin{array}{llllllll}
4x^3 & +x^2 & & & & & /x+1+i & = 4x^2 - 3x - 4ix - 1 + 7i \\
-(4x^3 & +4x^2 & +4ix^2) & & & & & \text{Rest} : 8 - 6i \\
\hline
 & -3x^2 & -4ix^2 & & & & & \\
 & -(-3x^2 & & -3x & -3ix) & & & \\
\hline
 & & -4ix^2 & +3x & +3ix & & & \\
 & & -(-4ix^2 & +4x & -4ix) & & & \\
\hline
 & & & -x & +7ix & & & \\
 & & & -(-x & & -1 & -i) & \\
\hline
 & & & & 7ix & +1 & +i & \\
 & & & & -(7ix & -7 & +7i) & \\
\hline
 & & & & & 8 & -6i & \\
\end{array}
\tag{1}
$$

An dieser Stelle bricht die Polynomdivision ab, da $\mathsf{rk}(8-6i) < \mathsf{rk}(x+1+i)$. Der Rest ist also der Term, der nach der letzten Substraktion übrig bleibt. Wir haben hier für jeden Grad die Schritte für Realteil und Imaginärteil getrennt durchgeführt. Das kann man natürlich auch jeweils auf einmal machen um Zeit zu sparen.

2. Wir wenden den euklidischen Algorithmus an. Man beachte, wie die Terme r_j von rechts

nach links wandern:

$$\begin{aligned} 7194 &= 1 \cdot (6787) + 407 \\ 6787 &= 16 \cdot (407) + 275 \\ 407 &= 1 \cdot (275) + 132 \\ 275 &= 2 \cdot (132) + 11 \\ 132 &= 12 \cdot (11) + 0 \end{aligned}$$

In der letzten Zeile erhalten wir $132 = 12 \cdot 11$ und keinen Rest. Damit ist der letzte Rest 11 und das ist auch der größte gemeinsame Teiler von 6787 und 7194

Aufgabe 2

1. Seien A_1, A_2 kommutative Ringe, deren Einselemente wir als $\mathbb{1}_1$ und $\mathbb{1}_2$ bezeichnen, sei $A := A_1 \times A_2$, seien $e_1 := (\mathbb{1}_1, 0), e_2 := (0, \mathbb{1}_2) \in A$. Sei weiter M ein A-Modul mit Skalarmultiplikation $\cdot_M$. Wir definieren für $j \in \{1, 2\}$.

   $$M_j := e_j \cdot_M M = \{e_j \cdot_M m \mid m \in M\} \subseteq M$$

   Zeige, dass M_1, M_2 Untermoduln sind und dass $M = M_1 \oplus M_2$ gilt.

2. Seien nun $A_1 = \mathbb{Z}/2\mathbb{Z}, A_2 = \mathbb{Z}/3\mathbb{Z}, M = \mathbb{Z}/6\mathbb{Z}$. Zeige, dass $(M, \star)$ mit der Operation

   $$\begin{aligned} \star : A \times M &\to M \\ ((a, b), m) &\mapsto (3a + 4b)m \end{aligned}$$

   ein A-Modul ist. Bestimmte M_1 und M_2.

Lösung:

1. Wir unterdrücken die Notation von $\cdot_M$. Wir prüfen zuerst, ob M_j für $j \in \{1, 2\}$ ein A-Untermodul ist. Wir beginnen mit den Gruppeneigenschaften (Da wir bereits wissen, dass die Moduladdition in M neutrale und inverse Elemente besitzt, müssen wir eigentlich nur zeigen, dass diese auch in M_j liegen):

   (a) *Kommutativität, Assoziativität:* Diese beiden Eigenschaften folgen sofort, da die Operation aus M geerbt wird.

   (b) *Abgeschlossenheit:* Seien hierfür $x, y \in M_j$. Dann gibt es $m_x, m_y \in M$ mit $x = e_j m_x, y = e_j m_y$. Dann gilt

   $$(x + y) = (e_j m_x + e_j m_y) = e_j(m_x + m_y)$$

   und da $m_x + m_y \in M$ liegt, folgt $(x + y) \in M_j$, die Moduladdition ist also abgeschlossen.

   (c) *Neutrales Element:* Sei 0_M das eindeutige neutrale Element von M. Wir definieren $0_j := e_j 0_M$. Dann gilt für ein belibiges $x = e_j m_x \in M_j$, dass

   $$0_j + x = e_j 0_M + e_j m_x = e_j(0_M + m_x) = e_j m_x = x$$

   also ist $0_j \in M_j$ ein neutrales Element.[a]

(d) *Inverses Element:* Sei $x = e_j m_x \in M_j$. Für $m_x \in M$ existiert ein bezüglich Moduladdition inverses Element $-m_x \in M$. Wir notieren $-x := e_j(-m_x)$ und berechnen

$$x + (-x) = e_j m_x + e_j(-m_x) = e_j(m_x - m_x) = e_j 0_M = 0_j$$

also ist $-x \in M_j$ invers zu x bezüglich der Moduladdition von M_j

Die Gruppeneigenschaften sind gezeigt, wir wollen nun noch zeigen, dass M_j mit der eingeschränkten Modulmultiplikation $\cdot_j := \cdot_M|_{A\times M_j}$ ein Modul ist. Wir zeigen

(a) *Distributivitätsgesetze, Assoziativität, Unitalität:* Diese drei Eigenschaften werden direkt aus M geerbt.

(b) *Abgeschlossenheit:* Zur Klarheit werden wir hier $\cdot_M$ nicht mehr unterdrücken. Seien $x = e_j \cdot_M m_x \in M_j$ und $\alpha = (\alpha_1, \alpha_2) \in A$, dann gilt

$$\alpha \cdot_j x = (\alpha_1, \alpha_2) \cdot_A (\mathbb{1}_1, 0) \cdot_M m_x = (\mathbb{1}_1, 0) \cdot_A (\alpha_1, 0) \cdot_M m_x = e_j \cdot_M ((\alpha_1, 0) \cdot_M m_x)$$

Da $(\alpha_1, 0) \cdot_M m_x \in M$ liegt, ist das neue Element also wieder von der Form $e_j m$ mit $m \in M$ und liegt deshalb in M_j. Die Modulmultiplikation ist also abgeschlossen.

Damit haben wir gezeigt, dass M_j ein Untermodul ist. Als nächstes zeigen wir, dass M die direkte Summe dieser beiden Untermoduln ist. Dafür zeigen wir

(a) *Summe:* Sei $m \in M$. Dann müssen wir $m_1 \in M_1, m_2 \in M_2$ finden, sodass $m = m_1 + m_2$. Wir verwenden, dass für Ringe A, B stets gilt, dass

$$\mathbb{1}_{A\times B} = (\mathbb{1}_A, \mathbb{1}_B)$$

und wählen $m_1 = e_1 m$ und $m_2 = e_2 m$, dann gilt

$$m = \mathbb{1}_A m = (\mathbb{1}_1, \mathbb{1}_2)m = (\mathbb{1}_1, 0)m + (0, \mathbb{1}_2)m = e_1 m + e_2 m = m_1 + m_2$$

Daraus folgt $M = M_1 + M_2$.

(b) *Eindeutigkeit:* Wir wollen zeigen, dass die Darstellung eindeutig ist, indem wir zeigen, dass der Schnitt der beiden Moduln nur 0_M enthält. Dafür sei $m \in M_1 \cap M_2$, dann existieren $m_1, m_2 \in M$ mit $m = e_1 m_1 = e_2 m_2$. Wir bestimmen:

$$\begin{aligned} m &= \mathbb{1}_A m \\ &= e_1 m + e_2 m \\ &= e_1 e_1 m_1 + e_2 e_2 m_2 \\ &= e_1 m_1 + e_2 m_2 = m + m \end{aligned}$$

Aus $m = m + m$ folgt direkt $m = 0_M$, also enthält der Schnitt der beiden Untermoduln nur die 0_M.

Wir haben also gezeigt, dass $M = M_1 \oplus M_2$ gilt.

[a] Alternativ könnte man natürlich auch zeigen, dass für $a \in A$ gilt, dass $a0_M = 0_M$ gilt. Wurde das in der Vorlesung schon gezeigt, dann kann man das natürlich verwenden um die Aufgabe trivial zu lösen.

2. Wir wollen zuerst zeigen, dass $\mathbb{Z}/6\mathbb{Z}$ ein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$-Modul ist. Da $\mathbb{Z}/6\mathbb{Z}$ bekanntermaßen ein Ring ist, ist $\mathbb{Z}/6\mathbb{Z}$ natürlich auch eine abelsche Gruppe bezüglich der Addition. Zu zeigen ist also nur die Modulstruktur bezüglich

$$\begin{aligned} \star : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} &\to \mathbb{Z}/6\mathbb{Z} \\ ((a,b),m) &\mapsto (3a+4b)m \end{aligned}$$

. Wir unterdrücken die Notation von $\cdot_A$. Seien $r = (a,b), r_1 = (a_1,b_1), r_2 = (a_2,b_2) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und $m, m_1, m_2 \in \mathbb{Z}/6\mathbb{Z}$, dann gilt

- *Assoziativität:*

$$\begin{aligned} r_1 \star (r_2 \star m) &= r_1 \star ((a_2,b_2) \star m) \\ &= (a_1,b_1) \star ((3a_2+4b_2)m) \\ &= (3a_1+4b_1)(3a_2+4b_2)m \\ &\overset{(1)}{=} (9a_1a_2 + 12(a_1b_2+b_1a_2) + 16b_1b_2)m \\ &\overset{(2)}{=} (3a_1a_2+4b_1b_2)m \\ &= (a_1a_2, b_1b_2) \star m = (r_1r_2) \star m \end{aligned}$$

  wobei wir bei (1) verwendet haben, dass in diesem Fall $a_1, a_2, b_1, b_2 \in \mathbb{Z}/6\mathbb{Z}$ liegen und wir dann natürlich Distributivität verwenden dürfen. Bei (2) haben wir verwendet, dass $6 = 0 \mod 6$ gilt. Das Assoziativitätsgesetz gilt also.

- *Distributivität bezüglich des Rings:*

$$\begin{aligned} (r_1+r_2) \star m &= (a_1+a_2, b_1+b_2) \star m \\ &= (3(a_1+a_2)+4(b_1+b_2))m \\ &= (3a_1+4b_1)m + (3a_2+4b_2)m \\ &= r_1 \star m + r_2 \star m \end{aligned}$$

- *Distributivität bezüglich des Moduls:*

$$\begin{aligned} r \star (m_1+m_2) &= (a,b) \star (m_1+m_2) \\ &= (3a+4b)(m_1+m_2) \\ &= (3a+4b)m_1 + (3a+4b)m_2 \\ &= r \star m_1 + r \star m_2 \end{aligned}$$

  also gelten auch die beiden Distributivgesetze.

Wir haben also gezeigt, dass $\mathbb{Z}/6\mathbb{Z}$ ein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-Modul ist. Wir bestimmen nun noch

$$\begin{aligned} e_1 \star \mathbb{Z}/6\mathbb{Z} &= \{3m \mid m \in \mathbb{Z}/6\mathbb{Z}\} = 3\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \\ e_2 \star \mathbb{Z}/6\mathbb{Z} &= \{4m \mid m \in \mathbb{Z}/6\mathbb{Z}\} = 4\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

und mit der ersten Teilaufgabe folgt

$$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Aufgabe 3

1. Sei $f(x) \in \mathbb{K}[x]$ und $n \in \mathbb{N}^+$. Es gelte $(x-1)|f(x^n)$ in $\mathbb{C}[x]$. Zeige, dass dann auch $(x^n-1)|f(x^n)$.
2. Sei $f(x) \in \mathbb{R}[x]$ ein Polynom ungeraden Grades. Zeige, f durch ein Polynom ersten Grades in $\mathbb{R}[x]$ teilbar ist.
3. Zeige, dass $f(x) = x^{3m} + x^{3n+1} + x^{3p+2}$ in $\mathbb{Q}[x]$ durch $x^2 + x + 1$ teilbar ist.
4. Sei $f(x) = x^{3m} - x^{3n+1} + x^{3p+2}$. Für welche $m, n, p \in \mathbb{N}_0$ ist f in $\mathbb{Q}[x]$ durch $x^2 - x + 1$ teilbar?

Lösung:
Die dritte und vierte Teilaufgabe sind eine gute Möglichkeit, sein Wissen über komplexe Zahlen aufzufrischen. Eine geometrische Anschauung kann hierbei viel helfen!

1. Da $(x-1)|f(x^n)$ ist $x = 1$ eine Nullstelle von $f(x^n)$, also gilt $f(1^n) = f(1) = 0$ und damit ist 1 auch eine Nullstelle von $f(x)$, das heißt es existiert ein Polynom $q(x)$ mit $f(x) = (x-1)q(x)$. Setzen wir x^n ein erhalten wir
$$f(x^n) = (x^n - 1)q(x^n)$$
und somit ist $f(x^n)$ auch durch $x^n - 1$ teilbar.

2. Sei $f(x) = a_n x^n + \ldots + a_0$ mit $n \in \mathbb{N}^+$ ungerade. OBdA sei $a_n > 0$. Im Limes $x \to \pm\infty$ ist für ein Polynom nur der Term mit maximalem Grad relevant. Es gilt also
$$f(x) \xrightarrow{x \to \pm\infty} \pm\infty$$
Daraus folgt (zum Beispiel mit dem Zwischenwertsatz aus Analysis), dass $f(x)$ mindestens eine Nullstelle $\lambda \in \mathbb{R}$ haben muss. Das heißt es gibt ein Polynom $q(x) \in \mathbb{R}[x]$, sodass $f(x) = (x - \lambda)q(x)$ und f ist durch das Polynom ersten Grades $x - \lambda$ teilbar.

3. Wir überlegen uns zuerst, dass es ausreicht diese Aufgabe in $\mathbb{C}$ zu lösen. Seien allgemein $f, g \in \mathbb{Q}[x]$ Polynome. Weil $\mathbb{Q}[x]$ ein euklidischer Ring ist, gibt es eindeutige p_Q, r_Q mit $\mathsf{rk}(r_Q) < \mathsf{rk}(p_Q)$, sodass
$$f = p_Q g + r_Q$$
Weiter liegen f, g auch in $\mathbb{C}[x]$ und deswegen existieren analog eindeutige $p_C, r_C \in \mathbb{C}[x]$, sodass $f = p_C g + r_C$. Da p_Q, r_Q natürlich auch in $\mathbb{C}[x]$ liegen, folgt aus der Eindeutigkeit sofort $p_Q = p_C$ und $r_Q = r_C$. Wenn wir also in $\mathbb{C}[x]$ zeigen, dass $r_C = 0$ gilt, dann gilt auch $r_Q = 0$ und aus der Teilbarkeit in $\mathbb{C}[x]$ folgt die Teilbarkeit in $\mathbb{Q}[x]$.

   Nun lösen wir das Problem also in $\mathbb{C}[x]$. Sei $g(x) = x^2 + x + 1$, dann gibt es eine Zerlegung in Polynome ersten Grades. f ist genau dann durch g teilbar, wenn f alle Linearfaktoren von g enthält. Zeigen wir also, dass jede Nullstelle von g auch eine Nullstelle von f ist, folgt daraus direkt die Teilbarkeit. Es gilt
$$g(x) = (x - \xi)(x - \xi^2)$$

wobei $\xi \in \mathbb{C}$ eine beliebige kubische Einheitswurzel ungleich 1 ist (Also eine Zahl $\xi \in \mathbb{C}$, sodass $\xi^3 = 1$.) Wir bestimmen

$$f(\xi) = \xi^{3m} + \xi^{3m+1} + \xi^{3m+2} = 1 + \xi + \xi^2 = 0$$

also ist ξ eine Nullstelle von f. Analog zeigen wir, dass ξ^2 eine Nullstelle von f ist. Da damit alle Nullstellen von g auch Nullstellen von f sind, haben wir $g|f$ bewiesen.

4. Die Aufgabe ist ähnlich zur vorherigen Teilaufgabe. Die Nullstellen von $g(x) = x^2 - x + 1$ sind genau die kubischen Teiler $\lambda, \mu \in \mathbb{C}$ von -1 ungleich -1. Das heißt wir wollen m, n, p bestimmen, sodass $f(\lambda) = f(\mu) = 0$ gilt.

   Dazu berechnen wir

   $$f(\lambda) = \lambda^{3m} - \lambda^{3n+1} + \lambda^{3p+2} = (-1)^m - (-1)^n\lambda + (-1)^p\lambda^2 = (-1)^m - (-1)^p + \lambda((-1)^p - (-1)^n)$$

   Da $\lambda \notin \mathbb{R}$ gilt, müssen sich die beiden Terme ohne Vorfaktor und mit Vorfaktor λ jeweils aufheben. Daraus folgt, dass $(-1)^m = (-1)^p = (-1)^n$ gelten muss, also entweder m, n, p gerade oder m, n, p ungerade. Für μ ist diese Rechnung genau gleich.

Aufgabe 4

1. Seien $x = 111\ldots11$ und $y = 111\ldots11$ Zahlen, die "aus m, bzw. n Einsen bestehen". Bestimmte den größten gemeinsamen Teiler von x und y.
2. Bestimmte $\mathsf{ggT}(x^n - 1, x^m - 1)$ in $\mathbb{C}[x]$ für beliebige $m, n \in \mathbb{N}^+$.

Lösung:

1. Die Grundidee ist hier, dass wir den euklidischen Algorithmus anwenden. Wir können x durch y mit Rest teilen und erhalten eine Zahl mit $m - n$ Einsen als Rest. Führen wir diese Art der Division und den euklidischen Algorithmus von m, n gleichzeitig durch, sehen wir, dass sie an der gleichen Stelle abbrechen. Daraus folgt $ggT(x, y) = 111\ldots11$, wobei letztere Zahl aus $\mathsf{ggT}(m, n)$ vielen Einsen besteht. Das ist natürlich kein formal korrekter Beweis, aber da diese Teilaufgabe direkt aus der zweiten folgt, werden wir hier auf Details verzichten.

2. Wir verwenden in dieser Aufgabe folgenden Fakt:

   $$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$$

   also gilt $(x - 1)|(x^n - 1)$ (I)

   Im Grunde ist die erste Teilaufgabe ein Spezialfall dieser Teilaufgabe. Es seien $x^n - 1, x^m - 1$ gegeben. Es sei oBdA $m > n$. Wir definieren

   $$d := \mathsf{ggT}(x^n - 1, x^m - 1)$$
   $$q := \mathsf{ggT}(m, n)$$

Da $d|x^n - 1$ gilt $x^n = 1 \mod d$ und analog $x^m = 1 \mod d$. Daraus folgt, dass

$$\forall a, b \in \mathbb{Z} : x^{an+bm} = x^{an} x^{bm} = (x^n)^a (x^m)^b = 1 \mod d$$

Es gilt mit dem Lemma von Bézout, dass es $y, z \in \mathbb{Z}$ gibt, sodass $yn + zm = q$. Setzen wir das in obige Formel ein erhalten wir

$$x^q = 1 \mod d$$

und damit sofort $d|x^q - 1$.
Umgekehrt wissen wir, dass es Zahlen $e, f \in \mathbb{Z}$ gibt, sodass $n = eq, m = fq$, also gilt auch

$$x^n - 1 = (x^q)^e - 1$$

und mit Aussage (I) folgt, dass $x^q - 1|x^n - 1$. Analog gilt

$$x^m - 1 = (x^q)^f - 1$$

und damit auch $x^q - 1|x^m - 1$. Das heißt aber, dass $x^q - 1$ ein gemeinsamer Teiler von $x^m - 1$ und $x^n - 1$ ist und damit auch ein Teiler von d. Wir haben nun gezeigt, dass $d|x^q - 1$ und $x^q - 1|d$, also muss $d = x^q - 1$ gelten. Zusammengefasst:

$$\mathsf{ggT}(x^m - 1, x^n - 1) = (x^{\mathsf{ggT}(m,n)} - 1)$$