



Prof. Dr. Fabien Morel

Dr. Andrei Lavrenov, Oliver Hendrichs

Wintersemester 2024/25

12. Dezember 2024

Lineare Algebra I – Lösungsskizzen zu Übungsblatt 07

Aufgabe 1.

Beweisen Sie, dass die Menge $\{\ln(p) \mid p \text{ eine Primzahl}\}$ $\mathbb{Q}$ -linear unabhängig ist (insbesondere ist $\dim_{\mathbb{Q}} \mathbb{R}$ unendlich).

Hinweis: Sie können benutzen, dass der natürliche Logarithmus $\ln: (\mathbb{R}^{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ ein Gruppenisomorphismus ist.

Lösung.

Um zu beweisen, dass die Menge $\{\ln(p) \mid p \text{ eine Primzahl}\}$ $\mathbb{Q}$ -linear unabhängig ist, müssen wir zeigen, dass jede Linearkombination

$$\sum_{p \text{ Primzahl}} a_p \cdot \ln(p) = 0$$

(mit fast allen $a_p \in \mathbb{Q}$ gleich Null) trivial ist.

Betrachten Sie eine solche Linearkombination. Sei $a_p = c_p/d_p$ für $c_p, d_p \in \mathbb{Z}$. Nehmen wir auch an, dass $d_p = 1$ für $a_p = 0$. Dann sind fast alle d_p gleich 1, und deshalb ist $D := \prod_{p \text{ Primzahl}} d_p$ wohldefiniert. Da $D \neq 0$ ist die Trivialität der vorherigen Linearkombination äquivalent zur Trivialität der Linearkombination

$$\sum_{p \text{ Primzahl}} D \cdot a_p \cdot \ln(p) = 0$$

für $D \cdot a_p = c_p \cdot \prod_{q \neq p \text{ Primzahl}} d_q \in \mathbb{Z}$. Jetzt können wir benutzen, dass $\ln: (\mathbb{R}^{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ ein Gruppenhomomorphismus ist:

$$0 = \sum_{p \text{ Primzahl}} (D a_p) \cdot \ln(p) = \ln \left(\prod_{p \text{ Primzahl}} p^{D a_p} \right).$$

Auf der anderen Seite, da $\ln$ ein Gruppenhomomorphismus ist, haben wir $\ln(1) = 0$. Aber $\ln$ ist auch eine Bijektion, und deshalb gilt

$$\prod_{p \text{ Primzahl}} p^{D a_p} = 1.$$

Dies ist nur möglich, wenn $a_p = 0$ für alle p . Insbesondere ist die Linearkombination trivial.

Aufgabe 2.

Sei $\mathcal{B} = \{e_i\}_{i \in I}$ ein Basis eines Vektorraums V , und sei $I = J_1 \sqcup \dots \sqcup J_m$ eine Partition der Menge I . Bezeichnen Sie mit $V_k := \langle e_j \mid j \in J_k \rangle \leq V$. Beweisen Sie, dass $V \cong \bigoplus_{k=1}^m V_k$ gilt.

Lösung.

Erinnern wir uns daran, dass $\bigoplus_{k=1}^m V_k$ bezeichnet die Menge $V_1 \times \dots \times V_m$ mit komponentenweiser Struktur eines Vektorraums. Betrachten wir die Abbildung $\varphi: \bigoplus_{k=1}^m V_k \rightarrow V$, die $(v_1, \dots, v_m)$ auf $v_1 + \dots + v_m$ schickt.

Es ist klar, dass φ linear ist: für Skalare a, a' und Elemente $(v_1, \dots, v_m), (v'_1, \dots, v'_m) \in \bigoplus_{k=1}^m V_k$ haben wir

$$\begin{aligned}\varphi(a(v_1, \dots, v_m) + a'(v'_1, \dots, v'_m)) &= \varphi((av_1 + a'v'_1, \dots, av_m + a'v'_m)) = \\ &= (av_1 + a'v'_1) + \dots + (av_m + a'v'_m) = a(v_1 + \dots + v_m) + a'(v'_1 + \dots + v'_m) = \\ &= a\varphi((v_1, \dots, v_m)) + a'\varphi((v'_1, \dots, v'_m)).\end{aligned}$$

Jetzt beweisen wir, dass φ surjektiv ist, d.h., dass jedes $v \in V$ ein Urbild bezüglich φ hat. Sei $v \in V$. Da $\mathcal{B}$ eine Basis von V ist, gibt es Skalare a_i für $i \in I$, so dass $v = \sum_{i \in I} e_i \cdot a_i$. Bezeichnen wir $v_k := \sum_{i \in J_k} e_i \cdot a_i \in V_k$. Da $I = J_1 \sqcup \dots \sqcup J_m$ eine Partition ist, haben wir $v = v_1 + \dots + v_m$. Aber dann gilt $\varphi((v_1, \dots, v_m)) = v_1 + \dots + v_m = v$, d.h., $(v_1, \dots, v_m)$ ist ein Urbild von v .

Jetzt beweisen wir, dass φ injektiv ist, d.h., dass $\text{Ker}(\varphi)$ trivial ist. Sei $(v_1, \dots, v_m) \in \text{Ker}(\varphi)$, d.h. $v_1 + \dots + v_m = 0$. Da V_k von $\{e_j \mid j \in J_k\}$ erzeugt wird, gibt es Skalare a_j für $j \in J_k$, so dass $v_k = \sum_{j \in J_k} e_j a_j$. Da $I = J_1 \sqcup \dots \sqcup J_m$ eine Partition ist, haben wir

$$0 = v_1 + \dots + v_m = \sum_{j \in J_1} e_j \cdot a_j + \dots + \sum_{j \in J_m} e_j \cdot a_j = \sum_{j \in I} e_j \cdot a_j.$$

Aber da $\mathcal{B}$ eine Basis ist, ist dies nur möglich, wenn $a_i = 0$ für alle $i \in I$ gilt. Mit anderen Worten ist $v_k = 0$ für alle $k = 1, \dots, m$. Deshalb ist $\text{Ker}(\varphi)$ in der Tat trivial.

Aufgabe 3.

Sei $f: V \rightarrow W$ eine surjektive lineare Abbildung, und $U \leq V$ ein Untervektorraum. Beweisen Sie, dass U ein Komplement zu $\text{Ker}(f)$ ist, wenn und nur wenn $f|_U: U \rightarrow W$ ein linearer Isomorphismus ist.

Lösung.

Nehmen wir zuerst an, dass U ein Komplement zu $\text{Ker}(f)$ ist, d.h. $V = U \oplus \text{Ker}(f)$.

Beweisen wir, dass $f|_U$ surjektiv ist. Sei $w \in W$, und da f surjektiv ist, gibt es ein Urbild $v \in V$ von w , d.h. $f(v) = w$. Da $V = U \oplus \text{Ker}(f)$, gibt es $u \in U$ und $u' \in \text{Ker}(f)$, so dass $v = u + u'$. Da f linear ist, gilt $f(v) = f(u + u') = f(u) + f(u')$, und da $u' \in \text{Ker}(f)$ gilt, haben wir $f(u') = 0$, mit anderen Worten: $w = f(v) = f(u)$, d.h., u ist ein Urbild von w bezüglich $f|_U$.

Beweisen wir jetzt, dass $f|_U$ injektiv ist. Sei $u \in \text{Ker}(f|_U)$, d.h. $f(u) = 0$. Mit anderen Worten gilt $u \in \text{Ker}(f)$. Aber es gilt auch $u \in U$ und, da $V = U \oplus \text{Ker}(f)$, schließen wir, dass $U \cap \text{Ker}(f) = \{0\}$ gilt. Insbesondere haben wir $u = 0$.

Nehmen wir zunächst an, dass $f|_U: U \rightarrow W$ ein Isomorphismus ist.

Beweisen wir, dass $V = U + \text{Ker}(f)$. Sei $v \in V$ und $w := f(v)$. Da $f|_U$ surjektiv ist, gibt es $u \in U$, so dass $f(u) = w$. Aber da f linear ist, schließen wir, dass $f(v - u) = f(v) - f(u) = w - w = 0$ gilt. Mit anderen Worten: $v - u \in \text{Ker}(f)$. Aber dann $v = u + (v - u) \in U + \text{Ker}(f)$.

Beweisen wir jetzt, dass $U \cap \text{Ker}(f) = \{0\}$. Sei $u \in U \cap \text{Ker}(f)$, d.h. $u \in U$ und $f(u) = f|_U(u) = 0$. Aber da $f|_U$ injektiv ist, schließen wir, dass $u = 0$ gilt.

Wir haben bewiesen, dass $V = U + \text{Ker}(f)$ und $U \cap \text{Ker}(f) = \{0\}$, mit anderen Worten gilt $V = U \oplus \text{Ker}(f)$, d.h., U ist ein Komplement zu $\text{Ker}(f)$.

Aufgabe 4.

Sei K ein endlicher Körper. Beweisen Sie, dass die Mächtigkeit $|K|$ von K gleich p^n für eine Primzahl p und eine positive ganze Zahl n ist.

Hinweis: Um die Primzahl p zu bestimmen, betrachten Sie den Ringhomomorphismus $\mathbb{Z} \rightarrow K$.

Lösung.

Betrachten wir den (einzigen) Ringhomomorphismus $f: \mathbb{Z} \rightarrow K$, der $n \in \mathbb{Z}$ auf $\underbrace{1 + \dots + 1}_{n \text{ mal}} \in K$ abbildet. Da K endlich ist, gibt es $m < m' \in \mathbb{Z}$, so dass $f(m) = f(m')$. Da f ein Ringhomomorphismus ist, haben wir $f(m' - m) = 0$. Sei $p \in \mathbb{N}$ eine kleinste Zahl, so dass $f(p) = 0$.

Wir wollen beweisen, dass p eine Primzahl ist. Offensichtlich $f(1) = 1 \neq 0 \in K$, deshalb ist $p > 1$. Sei $p = ab$ für natürliche $a, b \in \mathbb{N}$. Da f ein Ringhomomorphismus ist, schließen wir, dass $f(a) \cdot f(b) = f(ab) = f(p) = 0$ gilt. Aber da K ein Körper ist, ist K auch ein Integritätsbereich. Insbesondere $f(a) \cdot f(b) = 0$ ist nur möglich, wenn $f(a) = 0$ oder $f(b) = 0$. Aber p ist die kleinste Zahl, so dass $f(p) = 0$ und $a, b \leq p$. Dann ist $f(a) = 0$ nur möglich, wenn $a = p$, und ähnlich für b . Mit anderen Worten haben wir bewiesen, dass die einzigen natürlichen Teiler von p die Zahlen p und 1 sind, d.h., p ist eine Primzahl.

Jetzt wollen wir beweisen, dass K ein Vektorraum über $\mathbb{Z}/p\mathbb{Z}$ ist.

Bemerken wir zuerst, dass $f: \mathbb{Z} \rightarrow K$ einen Ringhomomorphismus $\bar{f}: \mathbb{Z}/p\mathbb{Z} \rightarrow K$ induziert. Für $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ sei $a \in \mathbb{Z}$ ein Urbild von $\bar{a}$ bezüglich der kanonischen Projektion $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. Dann setzen wir $\bar{f}(\bar{a}) := f(a)$. Wir müssen auch zeigen, dass $\bar{f}$ wohldefiniert ist. In der Tat sei $a' \in \mathbb{Z}$ ein anderes Urbild von $\bar{a}$. Dann gilt $a' - a = p \times k$ für $k \in \mathbb{Z}$, und da f ein Ringhomomorphismus ist, schließen wir, dass $f(a') = f(a) + f(p) \cdot f(k) = f(a) + 0$ gilt. Wir haben bewiesen, dass die Definition von $\bar{f}$, die wir gegeben haben, nicht von der Wahl des Urbildes abhängt, d.h., dass $\bar{f}$ wohldefiniert ist.

Da die kanonische Projektion $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ und $f: \mathbb{Z} \rightarrow K$ Ringhomomorphismen sind, ist auch $\bar{f}$ ein Ringhomomorphismus. In der Tat seien $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ und $a, b \in \mathbb{Z}$ ihre Urbilder, dann $a + b$ ist ein Urbild von $\bar{a} + \bar{b}$ und deshalb

$$\bar{f}(\bar{a} + \bar{b}) = f(a + b) = f(a) + f(b) = \bar{f}(\bar{a}) + \bar{f}(\bar{b}).$$

Ähnlich, ab ist ein Urbild von $\bar{a} \cdot \bar{b}$ und deshalb

$$\bar{f}(\bar{a} \bar{b}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b}).$$

Jetzt definieren wir die Struktur eines $\mathbb{Z}/p\mathbb{Z}$ -Vektorraums auf K wie folgt. Für $\alpha \in \mathbb{Z}/p\mathbb{Z}$ und $v \in K$ sei $\alpha \cdot v := \bar{f}(\alpha) \cdot v$. Wir müssen vier Axiome eines Vektorraums überprüfen.

Offensichtlich $\bar{1} \cdot v = \bar{f}(\bar{1}) \cdot v = f(1) \cdot v = 1 \cdot v = v$. Als nächstes

$$\alpha \cdot (u + v) = \bar{f}(\alpha)(u + v) = \bar{f}(\alpha)u + \bar{f}(\alpha)v = \alpha \cdot u + \alpha \cdot v$$

mit Hilfe der Distributivität von K . Dann

$$(\alpha + \beta) \cdot v = \bar{f}(\alpha + \beta)v = \bar{f}(\alpha)v + \bar{f}(\beta)v = \alpha \cdot v + \beta \cdot v,$$

da $\bar{f}$ ein Ringhomomorphismus ist und schließlich

$$(\alpha\beta) \cdot v = \bar{f}(\alpha\beta)v = \bar{f}(\alpha)\bar{f}(\beta)v = \bar{f}(\alpha)(\beta \cdot v) = \alpha \cdot (\beta \cdot v).$$

Wir haben bewiesen, dass K ein $\mathbb{Z}/p\mathbb{Z}$ -Vektorraum ist, aber da K endlich ist, ist K insbesondere endlich erzeugt, und deshalb ist K als $\mathbb{Z}/p\mathbb{Z}$ -Vektorraum endlichdimensional. Sei $n := \dim_{\mathbb{Z}/p\mathbb{Z}}(K)$. Dann $K \cong (\mathbb{Z}/p\mathbb{Z})^n$ als $\mathbb{Z}/p\mathbb{Z}$ -Vektorraum, insbesondere gilt

$$|K| = |(\mathbb{Z}/p\mathbb{Z})^n| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n.$$