LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Dr. Andrei Lavrenov, Oliver Hendrichs

Wintersemester 2024/25
21. November 2024

Lineare Algebra I – Lösungsskizzen zu Übungsblatt 04

Aufgabe 1.
Erinnern wir uns daran, dass eine Abbildung $f\colon R \to S$ ein Ringhomomorphismus ist, wenn:

1. $f(1) = 1$;
2. $\forall\, a, b \in R \quad f(a+b) = f(a) + f(b)$;
3. $\forall\, a, b \in R \quad f(ab) = f(a)f(b)$.

Sei R ein Körper und S ein Ring mit $1 \neq 0$. Beweisen Sie, dass jeder Ringhomomorphismus $f\colon R \to S$ injektiv ist.

Lösung.
Da ein Ringhomomorphismus $f\colon R \to S$ insbesondere ein Gruppenhomomorphismus $(R,+) \to (S,+)$ ist, reicht es zu zeigen, dass $\mathrm{Ker}(f) = \{0\}$.

Nehmen wir an, dass $x \in \mathrm{Ker}(f) \setminus \{0\}$. Da R ein Körper ist, gibt es $x^{-1} \in R$. Da f aber ein Ringhomomorphismus ist, gilt

$$1 = f(1) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1}) = 0 \cdot f(x^{-1}) = 0.$$

Allerdings ist $1 \neq 0$ in S nach Annahme. Der Widerspruch zeigt, dass $\mathrm{Ker}(f) = \{0\}$, also f injektiv ist.

Aufgabe 2.

1. Beweisen Sie, dass i, $\sqrt{2} \in \mathbb{C}$ nicht in $\mathbb{Q}$ liegen.
   Hinweis: Beweisen Sie es durch Widerspruch.
2. Für $r = \sqrt{2}$ oder $r = i$ bezeichne

   $$\mathbb{Q}[r] = \{a + br \mid a,\, b \in \mathbb{Q}\} \subset \mathbb{C}.$$

   Beweisen Sie, dass $\mathbb{Q}[r]$ ein Teilkörper von $\mathbb{C}$ ist.

Lösung.

1. Wenn $i \in \mathbb{Q} \subset \mathbb{R}$, dann widerspricht $i^2 = -1$ dem Fakt, dass ein Quadrat einer reellen Zahl nicht-negativ ist.

   Wenn $\sqrt{2} \in \mathbb{Q}$, dann gibt es p, $q \in \mathbb{Z}$ mit dem größten gemeinsamen Teiler 1, so dass $\sqrt{2} = p/q$. Dies impliziert aber, dass $2 = p^2/q^2$, d.h., dass $q^2 = 2p^2$ gerade ist. Das ist nur möglich, wenn q gerade ist, d.h. $q = 2r$ für $r \in \mathbb{Z}$. In diesem Fall ist jedoch $2p^2 = (2r)^2 = 4r^2$, d.h. $p^2 = 2r^2$ ist gerade. Das ist nur möglich, wenn p gerade ist. Aber p und q können nicht beide gerade sein, denn der größte gemeinsame Teiler von p und q ist 1.

2. Nach der Definition des Teilkörpers müssen wir zeigen, dass $0,\ 1 \in \mathbb{Q}[r]$, und dass $\forall\, x,\ y \in \mathbb{Q}[r]$ auch $x+y,\ xy,\ x^{-1} \in \mathbb{Q}[r]$ gilt.

   Offensichtlich ist $0 = 0+0\cdot r$, $1 = 1+0\cdot r \in \mathbb{Q}[r]$. Nehmen wir weiter an, dass $x = a+br$, $y = c+dr \in \mathbb{Q}[r]$. Dann

$$x + y = (a+br) + (c+dr) = (a+b) + (c+d)r \in \mathbb{Q}[r],$$

   da $a+b,\ c+d \in \mathbb{Q}$, und ähnlich

$$x \cdot y = (a+br)(c+dr) = ac + adr + bcr + bdr^2 = (ac+bdr^2) + (bc+ad)r \in \mathbb{Q}[r],$$

   da $r^2 \in \mathbb{Q}$ und daher $ac+bdr^2,\ bc+ad \in \mathbb{Q}$.

   Zum Schluss beachten Sie, dass wenn $a-br = 0$, dann $b = 0$ durch "1.", und somit auch $a = 0$. Insbesondere, wenn $a+br \neq 0$ ist, dann ist auch $a-br \neq 0$. Dann

$$\frac{1}{a+br} = \frac{a-br}{(a+br)(a-br)} = \frac{a-br}{a^2-b^2r^2} = \frac{a}{a^2-b^2r^2} + \frac{-b}{a^2-b^2r^2}\, r \in \mathbb{Q}[r],$$

   da $\dfrac{a}{a^2-b^2r^2},\ \dfrac{-b}{a^2-b^2r^2} \in \mathbb{Q}$.

Aufgabe 3.
Erinnern wir uns daran, dass ein kommutativer Ring R mit $1 \neq 0$ ein Integritätsbereich genannt wird, falls $\forall\, a,\ b \in R$, wenn $ab = 0$ und $a \neq 0$, dann $b = 0$.

1. Beweisen Sie, dass $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsbereich ist.
2. Beweisen Sie, dass jeder endliche Integritätsbereich ein Körper ist.

Lösung.

1. Erinnern wir uns daran, dass $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, und $\overline{2} \neq \overline{0}$ (vgl. Aufgabe 3 auf Übungsblatt 2). Aber

$$\overline{2} \cdot \overline{2} = \overline{(2\cdot 2)} = \overline{4} = \overline{0}.$$

   Mit anderen Worten: Wir schreiben a,$b \in \mathbb{Z}/4\mathbb{Z}$ so, dass $a \neq 0$, $b \neq 0$, aber $ab = 0$.

2. Sei R ein endlicher Integritätsbereich und wähle a in $R \setminus \{0\}$. Wir müssen zeigen, dass a invertierbar ist.

   Betrachten wir die Abbildung $f\colon R \to R$, die $b \in R$ zu $f(b) := ab$ schickt. Beachten Sie, dass $f\colon (R,+) \to (R,+)$ ein Gruppenhomomorphismus ist:

$$f(b+c) = a(b+c) = ab + ac = f(b) + f(c).$$

   Da R ein Integritätsbereich ist, schließen wir, dass $\mathrm{Ker}(f) = \{0\}$. Tatsächlich, wenn $b \in \mathrm{Ker}(f)$, d.h. $ab = 0$ dann $b = 0$. Daher ist f injektiv.

   Allerdings ist R endlich, daher ist jede Injektion $R \to R$ auch surjektiv. Insbesondere, da f surjektiv ist, gibt es $b \in R$ so, dass $f(b) = 1$. Dies impliziert, dass $ab = 1$, d.h., a ist invertierbar.

Aufgabe 4.
Eine Gruppe G heißt zyklisch, wenn sie von einem Element erzeugt ist, d.h. wenn $\exists\, g \in G$, sodass $\langle g \rangle = G$.

1. Sei G eine zyklische Gruppe, $H \leq G$. Beweisen Sie, dass H auch zyklisch ist.
   Hinweis: Betrachten Sie das minimale Element der Menge $\{n \in \mathbb{N} \setminus 0 \mid g^n \in H\}$.

2. Beweisen Sie, dass für $n \in \mathbb{N} \setminus \{0\}$ die Gruppe $G = \{z \in \mathbb{C} \mid z^n = 1\}$ zyklisch ist.
   Hinweis: Sie dürfen Aufgabe 4 aus Übungsblatt 4 aus Analysis einer Variablen verwenden.
3. Beweisen Sie, dass jede endliche Untergruppe von $(\mathbb{C}^\times, \cdot)$ zyklisch ist.

Lösung.

1. Sei $G = \langle g \rangle$ zyklisch, und $H \leq G$. Bezeichne d das minimale Element der Menge $\{n \in \mathbb{N} \setminus 0 \mid g^n \in H\}$. Wir beweisen, dass $H = \langle g^d \rangle$.

   Nehmen wir $h \in H$. Da insbesondere $h \in G$ und G zyklisch ist, gibt es $n \in \mathbb{N}$ so, dass $h = g^n$ oder $h = (g^{-1})^n$. In beiden Fällen ist $g^n \in H$.

   Teilen wir n durch d mit Rest:

   $$\exists\, q,\, r \in \mathbb{Z} \quad n = qd + r, \quad 0 \leq r < d.$$

   Beachten Sie, dass $g^n = g^{qd+r} = g^{qd} g^r = (g^d)^q g^r$. Weil aber g^n, $g^d \in H$, schließen wir, dass auch $g^r = (g^n)((g^d)^q)^{-1} \in H$. Aufgrund der Minimalität von d ist dies aber nur möglich, wenn $r = 0$. Mit anderen Worten: $h = (q^d)^q$ oder $h = ((q^d)^{-1})^q$. Das bedeutet, dass $H = \langle g^d \rangle$, also ist H auch zyklisch.
2. Sie wissen bereits aus Aufgabe 4 aus Übungsblatt 4 aus Analysis einer Variablen, dass $G = \{z \in \mathbb{C} \mid z^n = 1\}$ tatsächlich gleich $\{\omega_n^k \mid 0 \leq k < n\}$ für $\omega_n = \cos(2\pi/n) + i \sin(2\pi/n)$ ist. Mit anderen Worten: $G = \langle \omega_n \rangle$.
3. Sei H eine endliche Untergruppe von $(\mathbb{C}^\times, \cdot)$. Insbesondere sei für $h \in H$ die Menge $\{h^n \mid n \in \mathbb{N}\}$ endlich. Mit anderen Worten, es gibt $k \leq n$, so dass $h^k = h^n$, aber dann $h^{n-k} = 1$. Bezeichnen wir mit $\operatorname{ord}(h)$ das minimale $n > 0$, so dass $h^n = 1$.

   Da H endlich ist, gibt es N so, dass $\forall\, h \in H\ h^N = 1$ ist (z.B. nehme N als $\prod_{h \in H} \operatorname{ord}(h)$). Aber dann ist H eine Untergruppe von $G = \{z \in \mathbb{C} \mid z^N = 1\}$. Daraus folgt mit Hilfe von "1." und "2.", dass H endlich ist.