# Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

**6. Übungsblatt – Lösungsskizze**

---

**Aufgabe P17**

Wir wissen, dass für eine Menge $X$ mit $n$ Elementen und $n \in \mathbb{N}$ stets gilt: $|\mathrm{Sym}(X)| = n!$ (Dies kann man sich per Induktion leicht überlegen). In diesem Fall müssen wir also sechs Automorphismen finden. Mittels Abzählen sehen wir

| | | | | | |
|---|---|---|---|---|---|
| A | A | C | B | C | B |
| B | C | B | A | A | C |
| C | B | A | C | B | A |

Dabei sind die Bilder von $\{A, B, C\}$ unter den Elementen von $\mathrm{Sym}(\{A, B, C\})$ spaltenweise abgetragen. Zur geometrischen Interpretation: Die erste Spalte entspricht also gerade der Identität. Die nächsten drei Spalten sind gerade die Spiegelungen an der jeweiligen Mittelsenkrechten, also die Vertauschung zweier Punkte, während der dritte Punkt fest bleibt. Die letzten beiden Spalten entsprechen einer Rotation des Dreiecks im bzw. gegen den Uhrzeigersinn (Details ggf. in der Übung).

**Aufgabe P18**

Wir zeigen zunächst, dass für jeden Ring-Automorphismus $\varphi$ von $\mathbb{Z}$ gilt, dass $\varphi = \mathrm{id}_{\mathbb{Z}}$. Sei dafür $\varphi$ ein beliebiger Ring-Automorphismus von $\mathbb{Z}$. Da $\varphi$ ein Homomorphismus ist, ist dann $\varphi(0) = 0$ und $\varphi(1) = 1$.
Wir zeigen nun durch Induktion, dass $\varphi(n) = n$ für alle $n \in \mathbb{N}$. Der Induktionsanfang wurde schon gezeigt, da $\varphi(0) = 0$. Nun nehmen wir ein $n \in \mathbb{N}$, sodass $\varphi(n) = n$ gilt. Dann gilt auch $\varphi(n+1) = \varphi(n) + \varphi(1) = \varphi(n) + 1 = n + 1$, wobei wir für die letzte Gleichheit die Induktionsvoraussetzung benutzt haben.
Nun folgt, dass $\varphi(-n) = -\varphi(n) = -n$ für alle $n \in \mathbb{N}$, da $\varphi$ ein Homomorphismus ist. Somit haben wir gezeigt, dass $\varphi(z) = z$ für alle $z \in \mathbb{Z}$.
Schließlich betrachten wir einen beliebigen Ring-Automorphismus $\psi$ von $\mathbb{Q}$. Dann gilt, dass $\psi(z) = z$ für alle $z \in \mathbb{Z}$. Da $\psi$ ein Homomorphismus von Ringen und somit von Körpern ist, gilt für beliebige $z \in \mathbb{Z} \setminus \{0\}$ nun allerdings auch, dass $\psi\left(\frac{1}{z}\right) = \frac{1}{\psi(z)} = \frac{1}{z}$. Somit gilt abschließend für alle $z \in \mathbb{Z}$ und $z' \in \mathbb{Z}\setminus\{0\}$, dass $\psi\left(\frac{z}{z'}\right) = \psi(z) \cdot \psi\left(\frac{1}{z'}\right) = z \cdot \frac{1}{z'} = \frac{z}{z'}$. Da aber $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) = \left\{\frac{z}{z'} \mid z \in \mathbb{Z}, z' \in \mathbb{Z} \setminus \{0\}\right\}$, zeigt dies bereits, dass $\psi = \mathrm{id}_{\mathbb{Q}}$.

**Aufgabe P19**

1. Wir rechnen $h \cdot g^{-1} = (x \cdot g) \cdot g^{-1} = x \cdot (g \cdot g^{-1}) = x \cdot e = x$. Die zweite Identität ist analog.

2. Es gilt $((g \cdot h)^{-1} \cdot g) \cdot h = (g \cdot h)^{-1} \cdot (g \cdot h) = e$. Somit gilt nach Aufgabenteil 1, dass $(g \cdot h)^{-1} \cdot g = e \cdot h^{-1} = h^{-1}$. Eine erneute Anwendung von Aufgabenteil 1 gibt uns dann, dass $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

   Weiterhin gilt $g^{-1} \cdot g = e$ und somit erneut nach Aufgabenteil 1, dass $g = e \cdot (g^{-1})^{-1} = (g^{-1})^{-1}$.

3. Wir zeigen $g^n \cdot g^m = g^{n+m}$ durch vollständige Induktion über $m$. Für den Induktionsanfang sehen wir zunächst, dass $g^n \cdot g^0 = g^n \cdot e = g^n = g^{n+0}$. Dann nehmen wir für ein $m \in \mathbb{N}$ an, dass $g^n \cdot g^m = g^{n+m}$. Mit dieser Induktionsvoraussetzung rechnen wir dann aus, dass $g^n \cdot g^{m+1} = g^n \cdot (g^m \cdot g) = (g^n \cdot g^m) \cdot g = g^{n+m} \cdot g = g^{n+m+1}$. Somit haben wir gezeigt, dass für alle $n, m \in \mathbb{N}$ gilt, dass $g^n \cdot g^m = g^{n+m}$. Aus der Kommutativität der Addition von natürlichen Zahlen folgt dann direkt, dass $g^{n+m} = g^{m+n} = g^m \cdot g^n$. Der Beweis, dass $(g^n)^m = g^{n \cdot m}$ läuft komplett analog.

4. Wir zeigen die Behauptung durch vollständige Induktion über $n$. Für den Induktionsanfang sehen wir, dass $(h \cdot g)^0 = e = e \cdot e = h^0 \cdot g^0$. Nun nehmen wir für ein $n \in \mathbb{N}$ an, dass $(h \cdot g)^n = h^n \cdot g^n$. Mit dieser Induktionsvoraussetzung rechnen wir dann aus, dass $(h \cdot g)^{n+1} = (h \cdot g)^n \cdot (h \cdot g) = h^n \cdot g^n \cdot h \cdot g$. Nun benutzen wir die Voraussetzung, dass $h \cdot g = g \cdot h$ um auszurechnen, dass $h^n \cdot g^n \cdot h \cdot g = h^n \cdot g^n \cdot g \cdot h = h^n \cdot g^{n+1} \cdot h$. Durch ein leichtes Induktionsargument können wir zeigen, dass ferner aus $h \cdot g = g \cdot h$ folgt, dass $g^{n+1} \cdot h = h \cdot g^{n+1}$. Damit erhalten wir schließlich, dass $(h \cdot g)^{n+1} = h^n \cdot h \cdot g^{n+1} = h^{n+1} \cdot g^{n+1}$.

---

## Hausübungen

### Aufgabe H14

Die Menge $G_m$ ist tatsächlich eine Gruppe: Es gilt $a * b \in G_m$ für $a, b \in G_m$, da der Rest bei der Division durch $m$ immer kleiner als $m$ ist. Für die Assoziativität sei

$$a + b = sm + r, \quad r + c = s'm + r', \quad b + c = tm + q, \quad a + q = t'm + q'$$

mit $r, r', q, q' \in G_m$. Dann gilt

$$\begin{aligned}(a * b) * c = r' = r + c - s'm = a + b - sm + c - s'm = a + b + c - m(s + s') = \\ a + tm + q - m(s + s') = m(t + t' - s - s') + q'.\end{aligned}$$

Da $r' \in G_m$ muss auch $m(t + t' - s - s') + q' \in G_m$ gelten, was wegen $q' \in G_m$ nur sein kann, wenn $(t + t' - s - s') = 0$ gilt. Also gilt

$$(a * b) * c = r' = q' = a * (b * c).$$

Die Kommutativität ergibt sich direkt aus $a + b = b + a$ für $a, b \in \mathbb{Z}$. Das neutrale Element ist 0, denn für jedes $a$ in $G_m$ ist

$$\begin{aligned}&\text{Rest von } a + 0 \text{ bei Division durch } m \\ =&\text{Rest von } 0 + a \text{ bei Division durch } m \\ =&\text{Rest von } a \text{ bei Division durch } m.\end{aligned}$$

Für ein Element $a \in G_m$ ist das Inverse durch $m - a \in G_m$ gegeben, wenn es gilt

$$\begin{aligned}a * (m - a) &= \text{Rest von } a + (m - a) \text{ bei Division durch } m \\ &= \text{Rest von } 0 \text{ bei Division durch } m = 0.\end{aligned}$$

Mit der Abbildung $\varphi : G_m \to \mathbb{Z}_m$, $\varphi(a) = \overline{a}$ hat man den geforderten Gruppenisomorphismus: Die Homomorphismuseigenschaft ergibt sich (mit den bezeichnungen wie oben) aus

$$\varphi(a * b) = \varphi(r) = \overline{r} = \overline{a + b - sm} = \overline{a} + \overline{b}.$$

Für die Surjektivität ist nichts weiter zu zeigen, da $G_m$ genau die kanonischen Repräsentanten der Äquivalenzklassen aus $\mathbb{Z}_m$ enthält. Gilt nun $\varphi(g) = 0$, so folgt, dass $g$ den Rest 0 bei Division durch $m$ hat. Da aber $g < m$ nach Definition, folgt schon $g = 0$. Der Kern der Abbildung ist also gleich $\{0\}$ und die Abbildung ist somit injektiv. Damit ist sie ein Isomorphismus.

**Aufgabe H15**

1. Wir bemerken, dass die Hintereinanderausführung von Funktionen assoziativ ist. Somit gilt insbesondere für $\varphi, \psi, \chi \in \mathrm{Aut}(R)$, dass

   $$(\varphi \circ \psi) \circ \chi = \varphi \circ (\psi \circ \chi).$$

   Weiterhin ist die Identität $\mathrm{id}_R : R \to R$ ein Automorphismus und ein neutrales Element bezüglich der Verknüpfung von Funktionen, d.h., für $\varphi \in \mathrm{Aut}(R)$ gilt:

   $$\varphi \circ \mathrm{id}_R = \varphi = \mathrm{id}_R \circ \varphi.$$

   Somit ist $(\mathrm{Aut}(R), \circ)$ ein Monoid. Weiterhin bemerken wir, dass ein Automorphismus $\varphi \in \mathrm{Aut}(R)$ insbesondere ein Isomorphismus ist und somit ein beidseitiges Inverses $\varphi^{-1}$ hat, d.h. es gilt:

   $$\varphi \circ \varphi^{-1} = \mathrm{id}_R = \varphi^{-1} \circ \varphi.$$

   Also erfüllt $(\mathrm{Aut}(R), \circ)$ alle Gruppenaxiome und ist somit eine Gruppe.

2. Sei $\varphi \in \mathrm{Aut}(k[X])$ derartig, dass die Eigenschaften (1) und (2) vom Übungsblatt gelten. Dann muss – aufgrund der Tatsache, dass $\varphi$ ein Homomorphismus ist – für ein beliebiges Polynom $\sum_{i=0}^{n} \lambda_i X^i \in k[X]$ gelten, dass

   $$\varphi\left(\sum_{i=0}^{n} \lambda_i X^i\right) = \sum_{i=0}^{n} \varphi(\lambda_i) \cdot \varphi(X)^i = \sum_{i=0}^{n} \lambda_i \cdot (aX + b)^i.$$

   Somit ist durch (1) und (2) der Automorphismus $\varphi$ auf $k[X]$ eindeutig definiert, wenn er existiert.

   Wir müssen allerdings noch nachrechnen, dass $\varphi$, wie oben definiert, für beliebige Wahlen von $a \in k \setminus \{0\}$ und $b \in k$ tatsächlich ein Automorphismus ist. Um zu sehen, dass es ein Homomorphismus ist, nehmen wir zwei Polynome $\sum_{i=0}^{n} \lambda_i X^i, \sum_{i=0}^{n} \mu_i X^i \in k[X]$ und rechnen aus,

dass

$$\begin{aligned}\varphi\left(\sum_{i=0}^{n}\lambda_i X^i+\sum_{i=0}^{n}\mu_i X^i\right) &= \varphi\left(\sum_{i=0}^{n}(\lambda_i+\mu_i)X^i\right)\\ &= \sum_{i=0}^{n}(\lambda_i+\mu_i)(aX+b)^i\\ &= \sum_{i=0}^{n}\lambda_i(aX+b)^i+\sum_{i=0}^{n}\mu_i(aX+b)^i\\ &= \varphi\left(\sum_{i=0}^{n}\lambda_i X^i\right)+\varphi\left(\sum_{i=0}^{n}\mu_i X^i\right)\end{aligned}$$

und

$$\begin{aligned}\varphi\left(\left(\sum_{i=0}^{n}\lambda_i X^i\right)\cdot\left(\sum_{i=0}^{n}\mu_i X^i\right)\right) &= \varphi\left(\sum_{j=0}^{2n}\left(\sum_{k+\ell=j}\lambda_k\mu_\ell\right)X^j\right)\\ &= \sum_{j=0}^{2n}\left(\sum_{k+\ell=j}\lambda_k\mu_\ell\right)(aX+b)^j\\ &= \left(\sum_{i=0}^{n}\lambda_i(aX+b)^i\right)\cdot\left(\sum_{i=0}^{n}\mu_i(aX+b)^i\right)\\ &= \varphi\left(\sum_{i=0}^{n}\lambda_i X^i\right)\cdot\varphi\left(\sum_{i=0}^{n}\mu_i X^i\right)\end{aligned}$$

gilt. Wir bemerken, dass wegen (1) außerdem gilt, dass $\varphi(1)=1$. Somit ist $\varphi$ in der Tat ein Homomorphismus.

Nun bleibt zu zeigen, dass $\varphi$ bijektiv ist. Dazu zeigen wir, dass $\varphi$ ein Links- und Rechtsinverses hat. Wir definieren dazu

$$\psi : k[X]\to k[X],\ \sum_{i=0}^{n}\lambda_i X^i \mapsto \sum_{i=0}^{n}\lambda_i(a^{-1}X-b\cdot a^{-1}).$$

Dann rechnen wir nach, dass

$$\begin{aligned}\psi\circ\varphi\left(\sum_{i=0}^{n}\lambda_i X^i\right) &= \psi\left(\sum_{i=0}^{n}\lambda_i(aX+b)^i\right)=\sum_{i=0}^{n}\lambda_i(a\cdot\varphi(X)+b)^i\\ &= \sum_{i=0}^{n}\lambda_i(a\cdot(a^{-1}X-b\cdot a^{-1})+b)^i=\sum_{i=0}^{n}\lambda_i X^i\end{aligned}$$

gilt. Daraus folgt, dass $\psi\circ\varphi=\mathrm{id}_{k[X]}$. Analog zeigen wir, dass $\varphi\circ\psi=\mathrm{id}_{k[X]}$. Somit ist $\varphi$ in der Tat ein Automorphismus.

3. Sei $\varphi\in\mathrm{Aut}(k[X])$ wie in der Aufgabe vorgegeben. Dann gibt es $n\in\mathbb{N}$ und $a_i\in k$ für $i\leq n$, sodass $\varphi(X)=\sum_{i=0}^{n}a_i X^i$. Wir zeigen zunächst, dass $a_i=0$ für alle $i>1$. Dafür nehmen wir

an, es gäbe $i > 1$, sodass $a_i \neq 0$ und lassen o.B.d.A. $a_n \neq 0$. Dann nehmen wir ein beliebiges Polynom $\sum_{j=0}^{m} \mu_j X^j \in k[X]$, das nicht identisch zum Nullpolynom ist, und lassen o.b.d.A. $\mu_n \neq 0$. Dann sehen wir, dass

$$\varphi\left(\sum_{j=0}^{m} \mu_j X^j\right) = \sum_{j=0}^{m} \mu_j \varphi(X)^j = \sum_{j=0}^{m} \mu_j (\sum_{i=0}^{n} a_i X^i)^j.$$

Wir sehen, dass sich dieses Polynom schreiben lässt als $\mu_m \cdot a_n X^{n+m} + Q$, wobei $Q \in k[X]$ ein Polynom mit $\deg(Q) < n + m$ ist. Somit ist insbesondere $\varphi\left(\sum_{j=0}^{m} \mu_j X^j\right) \neq X$. Da $\sum_{j=0}^{m} \mu_j X^j$ ein beliebiges nicht-triviales Polynom war und $\varphi(0) = 0 \neq X$ gilt, folgt hieraus bereits, dass $X \notin \mathrm{im}(\varphi)$ und somit, dass $\varphi$ nicht surjektiv ist, was der Annahme widerspricht, dass $\varphi$ ein Automorphismus ist. Somit ist in der Tat $a_i = 0$ für alle $i > 1$ und wir haben $\varphi(X) = a_1 X + a_0$.

Nun zeigen wir, dass $a_1 \neq 0$. Dafür nehmen wir an, dass $a_1 = 0$ gelte. Dann ist aber $\varphi(X - a_0) = \varphi(X) - a_0 = a_0 - a_0 = 0$. Da $X - a_0 \neq 0$, folgt daraus, dass $\varphi$ nicht injektiv ist, was erneut ein Widerspruch ist. Somit erhalten wir die Behauptung, indem wir $a = a_1$ und $b = a_0$ setzen.

4. Wir zeigen zunächst, dass für jedes $\varphi \in \mathrm{Aut}(\mathbb{Q}[X])$ gilt, dass $\varphi|_{\mathbb{Q}} \in \mathrm{Aut}(\mathbb{Q})$. Dazu bemerken wir zunächst, dass in jedem Fall $\varphi|_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}[X]$ ein injektiver Ring-Homomorphismus ist, da $\varphi$ ein injektiver Ring-Homomorphismus ist (warum?). Es bleibt zu zeigen, dass $\mathrm{im}\left(\varphi|_{\mathbb{Q}}\right) = \mathbb{Q}$. Wir zeigen zunächst, dass $\mathrm{im}\left(\varphi|_{\mathbb{Q}}\right) \subseteq \mathbb{Q}$. Dazu bemerken wir, dass für jedes $q \in \mathbb{Q} \setminus \{0\}$ gilt, dass $\varphi(q) \cdot \varphi(q^{-1}) = \varphi(q \cdot q^{-1}) = \varphi(1) = 1$ und somit $\varphi(q) \in \mathbb{Q}[X]$ invertierbar ist. Aus Aufgabe **H4** folgt dann aber gerade, dass $\varphi(q) \in \mathbb{Q} \setminus \{0\}$. Ferner ist $\varphi(0) = 0$. Nun zeigen wir, dass $\mathbb{Q} \subseteq \mathrm{im}\left(\varphi|_{\mathbb{Q}}\right)$. Dazu nehmen wir die beidseitig inverse Abbildung $\varphi^{-1}$ zu $\varphi$. Dann ist $\varphi^{-1} \in \mathrm{Aut}(\mathbb{Q}[X])$ (siehe Aufgabenteil 1). Nun zeigen wir mit demselben Argument wie gerade benutzt, dass für jedes $q \in \mathbb{Q} \setminus \{0\}$ bereits $\varphi^{-1}(q) \in \mathbb{Q} \setminus \{0\}$. Da $\varphi$ surjektiv ist, folgt daraus, dass $\mathbb{Q} \subseteq \mathrm{im}\left(\varphi|_{\mathbb{Q}}\right)$. Somit ist in der Tat $\varphi|_{\mathbb{Q}} \in \mathrm{Aut}(\mathbb{Q}[X])$.

Nach Aufgabe **P15** ist allerdings $\mathrm{id}_{\mathbb{Q}}$ der einzige Automorphismus von $\mathbb{Q}$. Somit hat jeder Automorphismus $\varphi \in \mathrm{Aut}(\mathbb{Q}[X])$ die Eigenschaft, dass $\varphi(x) = x$ für alle $x \in \mathbb{Q}$, d.h., die Eigenschaft (1). Nach den Aufgabenteilen 2 und 3 gibt es somit für jedes $\varphi \in \mathrm{Aut}(\mathbb{Q}[X])$ eindeutige $a \in \mathbb{Q} \setminus \{0\}$ und $b \in \mathbb{Q}$, sodass – in der Notation von Aufgabenteil 2 – $\varphi = \varphi_{a,b}$, d.h., $\varphi(X) = aX + b$.

Nun definieren wir eine Abbildung $\iota : \mathrm{Aut}(k[X]) \to M$, $\varphi_{a,b} \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Diese Abbildung ist ein Homomorphismus von Gruppen, da für $a, c \in \mathbb{Q} \setminus \{0\}$ und $b, d \in \mathbb{Q}$ gilt, dass $\varphi_{a,b} \circ \varphi_{c,d}(X) = a(cX + d) + b = (ac)X + (ad + b)$. Somit gilt

$$\iota(\varphi_{a,b} \circ \varphi_{c,d}) = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \iota(\varphi_{a,b}) \cdot \iota(\varphi_{c,d}).$$

Es bleibt zu zeigen, dass $\iota$ bijektiv ist. Für Injektivität bemerken wir, dass das Urbild von $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ unter $\iota$ gerade der eindeutige Autmorphismus $\varphi_{1,0} \in \mathrm{Aut}(k[X])$ ist, sodass $\varphi_{1,0}(X) =$

$X$, d.h. genau die Identität $\mathrm{id}_{\mathrm{Aut}(k[X])}$. Für Surjektivität bemerken wir, dass für beliebige $a \in k \setminus \{0\}$ und $b \in k$ nach Aufgabenteil 2 ein $\varphi_{a,b} \in \mathrm{Aut}(k[X])$ existiert, sodass $\varphi_{a,b}(X) = aX + b$. Aber dann ist gerade $\iota(\varphi_{a,b}) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Somit ist $\mathrm{im}(\iota) = M$, d.h. $\iota$ ist surjektiv. Insgesamt zeigt dies, dass $\iota$ ein Isomorphismus ist.

**Aufgabe H16**

1. Wir rechnen zunächst nach, dass $k_s$ bezüglich Addition und Multiplikation von Matrizen ein Ring ist. Wir rechnen dafür zunächst nach, dass für $a, a', b, b' \in k$ gilt, dass

$$\begin{pmatrix} a & sb \\ b & a \end{pmatrix} - \begin{pmatrix} a' & sb' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a - a' & s(b - b') \\ b - b' & a - a' \end{pmatrix} \in k_s.$$

   Somit ist $k_s$ abgeschlossen bezüglich Addition und additiven Inversen und somit eine Untergruppe von $k^{2\times 2}$ bezüglich Addition.

   Als nächstes rechnen wir nach, dass für $a, a', b, b' \in k$ gilt, dass

$$\begin{pmatrix} a & sb \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & sb' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' + sbb' & s(ab' + a'b) \\ ab' + a'b & aa' + sbb' \end{pmatrix} \in k_s = \begin{pmatrix} a' & sb' \\ b' & a' \end{pmatrix} \cdot \begin{pmatrix} a & sb \\ b & a \end{pmatrix}$$

   Somit ist $k_s$ abgeschlossen bezüglich Multiplikation und die Multiplikation ist kommutativ. Assoziativität der Multiplikation sowie Distributivität übertragen sich von $k^{2\times 2}$ auf $k_s$. Somit müssen wir nur noch bemerken, dass $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in k_s$ das neutrale Element bezüglich Multiplikation ist. Insgesamt zeigt dies, dass $k_s$ ein kommutativer Ring ist.

   $k_s$ ist genau dann ein Körper, wenn jede Matrix in $k_s$, die nicht die Nullmatrix ist, invertierbar ist. Dies ist äquivalent zu der Aussage, dass für alle Paare $a, b \in k$ mit $a \neq 0$ oder $b \neq 0$ gilt, dass $\det \begin{pmatrix} a & sb \\ b & a \end{pmatrix} = 0$, was wiederum äquivalent dazu ist, dass für alle Paare $a, b \in k$ mit $a \neq 0$ oder $b \neq 0$ gilt, dass $a^2 - sb^2 \neq 0$, d.h., $a^2 \neq sb^2$.

   Insgesamt haben wir also gezeigt, dass $k_s$ ein Körper ist genau dann, wenn für alle Paare $a, b \in k$ mit $a \neq 0$ oder $b \neq 0$ gilt, dass $a^2 \neq sb^2$. Wir zeigen nun, dass letztere Aussage äquivalent ist zur Aussage, dass für alle $x \in k$ gilt, dass $x^2 \neq s$. Für die $\Rightarrow$-Richtung betrachten wir einfach den Spezialfall $b = 1$. Für die $\Leftarrow$-Richtung nehmen wir an, es gäbe $a, b \in k^2$ mit $a \neq 0$ oder $b \neq 0$, sodass $a^2 = sb^2$. Wenn $b = 0$, so ist auch $a = 0$, ein Widerspruch. Somit ist $b \neq 0$ und somit $(a \cdot b^{-1})^2 = s$. Somit gibt es dann $x \in k$, sodass $x^2 = s$.

2. Ein Isomorphismus $\iota : \mathbb{C} \to \mathbb{R}_{-1}$ ist gegeben durch $\iota\,(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Wir rechnen zunächst nach, das dies ein Homomorphismus ist. Es gilt für $a, b, a', b' \in \mathbb{R}$:

$$\begin{aligned} \iota((a + bi) + (a' + b'i)) = \iota(a + a' + (b + b')i) &= \begin{pmatrix} a + a' & -b - b' \\ b + b' & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \iota(a + bi) + \iota(a' + b'i) \end{aligned}$$

und

$$\iota((a+bi)\cdot(a'+b'i)) = \iota(aa'-bb'+(ab'+a'b)i) = \begin{pmatrix} aa'-bb' & -ab'-a'b \\ ab'+a'b & aa'-bb' \end{pmatrix}$$
$$= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \iota(a+bi)\cdot\iota(a'+b'i).$$

Ferner gilt, dass $\iota(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Somit ist $\iota$ ein Homomorphismus. Um zu sehen, dass es ein Isomorphismus ist, geben wir ein beidseitiges Inverses $\sigma : \mathbb{R}_{-1} \to \mathbb{C}$, welches einfach gegeben ist durch $\sigma\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) = a+bi$. Es folgt direkt aus den Definitionen von $\iota$ und $\sigma$, dass $\sigma \circ \iota = \mathrm{id}_{\mathbb{C}}$ und $\iota \circ \sigma = \mathrm{id}_{\mathbb{R}_{-1}}$ gilt. Somit ist $\iota$ ein Isomorphismus und $\mathbb{C}$ ist isomorph zu $\mathbb{R}_{-1}$.

3. Wir zeigen zunächst, dass es ein $n < p$ gibt, sodass für alle $x \in \mathbb{Z}$ gilt, dass $x^2 \not\equiv n \pmod{p}$. Dafür bemerken wir zunächst, dass $p-1 \equiv -1 \pmod{p}$ und somit $(p-1)^2 \equiv 1 \pmod{p}$. Natürlich ist ebenfalls $1^2 \equiv 1 \pmod{p}$. Somit enthält die Menge

$$\{n < p \mid 0 \leq n \,\text{und}\, \exists x \in \mathbb{Z} :\, x^2 \equiv n \pmod{p}\}$$

strikt weniger als $p$ Elemente. Somit gibt es $n < p$, sodass für alle $x \in \mathbb{Z}$ gilt, dass $x^2 \not\equiv n \pmod{p}$. Wir fixieren dieses $n$. Wenn $\overline{n}$ die Äquivalenzklasse von $n$ in $\mathbb{Z}_p$ ist, so erhalten wir in $\mathbb{Z}_p$ dann, dass für alle $y \in \mathbb{Z}_p$ gilt, dass $y^2 \neq \overline{n}$.

Nach Aufgabenteil 1 ist somit $(\mathbb{Z}_p)_{\overline{n}}$ ein Körper. Aufgefasst als Vektorraum über $\mathbb{Z}_p$ hat er etwa $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \overline{n} \\ 1 & 0 \end{pmatrix}\right\}$ als Basis und somit gilt $\dim_{\mathbb{Z}_p}((\mathbb{Z}_p)_{\overline{n}}) = 2$. Ein Vektorraum von Dimension 2 über $\mathbb{Z}_p$ hat natürlich $p^2$ Elemente.