Lineare Algebra I
Lösungsvorschläge zum Tutoriumsblatt 5

Moritz Fleischmann

Zur Vorlesung von Prof. Dr. Fabien Morel, Dr. Andrei Lavrenov und Oliver Hendrichs im Wintersemester 2024-25

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.

Bevor wir mit der ersten Aufgabe beginnen, eine Wiederholung zu komplexen Zahlen:

Wir definieren die *komplexen Zahlen* $(\mathbb{C})$ als den Körper[a] $(\mathbb{C}, +, \cdot)$ über der Menge

$$\mathbb{R} \times \mathbb{R} \tag{1}$$

aus geordneten Paaren reeller Zahlen. Die Addition ist "komponentenweise" definiert, das heißt es gilt für $z = (a, b), w = (c, d) \in \mathbb{C}$, dass

$$z + w = (a, b) + (c, d) := (a + c, b + d) \tag{2}$$

während wir für die Multiplikation folgende Definition haben:

$$z \cdot w = (a, b) \cdot (c, d) := (ac - bd, ad + bc) \tag{3}$$

Wir können jetzt die Zahl $(a, 0)$ mit der reellen Zahl a gleichsetzen und definieren $i := (0, 1)$, sodass $i^2 = -1$ gilt. Wir schreiben für das Paar (a, b) ab jetzt $a + bi$. Weiter definieren wir für $z = a + bi$ das *komplex Konjugierte von* z als

$$\overline{z} = a - bi \tag{4}$$

und den Absolutbetrag von z als

$$|z|^2 = z \cdot \overline{z} = |a|^2 + |b|^2 \tag{5}$$

[a] Siehe hierzu die Lösung zu Aufgabe 2

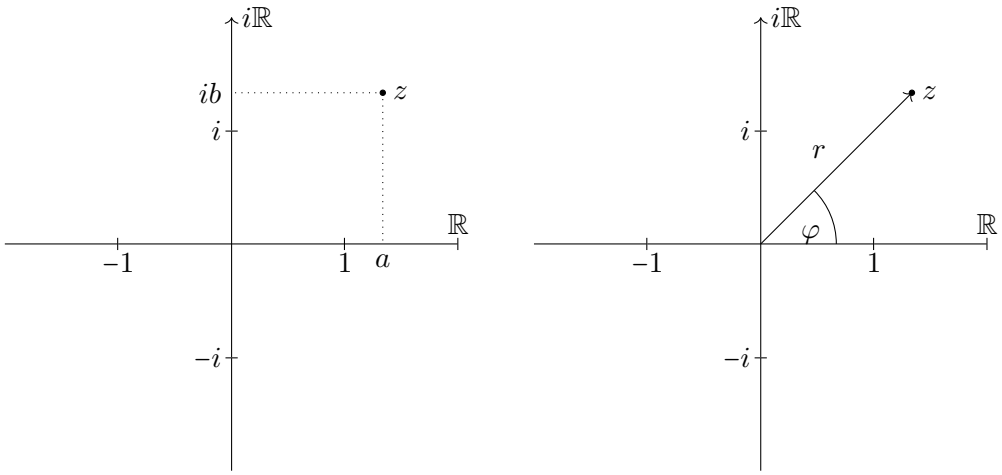
Der eigentliche Grund für die Einführung der komplexen Zahlen ist, dass man in den reellen Zahlen nicht alle polynomiellen Gleichungen lösen kann, beispielsweise hat $f(x) = x^2 + 1$ keine Nullstelle in $\mathbb{R}$. Erst durch die Einführung von i kann man also die Gleichung durch $f(i) = i^2 + 1 = -1 + 1 = 0$ lösen.[1] Man kann für die komplexen Zahlen schnell zeigen, dass $(\mathbb{C}, +, \cdot)$ mit den neutralen Elementen 0 bezüglich Addition und 1 bezüglich Multiplikation und den inversen Elementen $-z$ bezüglich Addition und

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2} \tag{6}$$

bezüglich Multiplikation einen Körper darstellt.

[1] Allgemeiner kann man zeigen, dass in $\mathbb{C}$ jedes Polynom von Grad n auch n Nullstellen hat (mit Vielfachheit). Diese Aussage kennt man als *Fundamentalsatz der Algebra*.

Die Darstellung komplexer Zahlen als $a + bi$ ist zwar naheliegend, für viele Anwendungen aber nicht ideal. Häufig bietet es sich an, die Zahl anders darzustellen. Dazu überlegen wir uns folgendes: Sei $z = a + bi$, dann können wir z in einem zweidimensionalen Koordinatensystem darstellen, bei dem die horizontale Koordinate für den reellen Anteil steht und die vertikale für den imaginären Anteil. Wir sehen, dass es nun zwei Möglichkeiten gibt, diesen einen Punkt zu beschreiben. Einmal per kartesischer Koordinaten als das Tupel (a, b) und per Polarkoordinaten als das Tupel (r, φ), wobei $r \in \mathbb{R}_0^+$ den Radius und $\varphi \in \mathbb{R}$ den Winkel bezeichnet. Wir berechnen Winkel, sofern nicht anders vermerkt, immer als Radiant. Ein ganzer Kreis umfasst also den Winkel 2π. Eine Möglichkeit



zur Darstellung ist $z = re^{i\varphi}$, wobei r und φ wie in der Zeichnung definiert sind. Wir wissen, dass $e^{i\varphi}$ immer auf dem Einheitskreis in der komplexen Ebene liegt, surjektiv auf ihn abbildet und 2π-periodisch ist. Wir sehen also, dass wir den ganzen komplexen Raum durch Polarkoordinaten abdecken können.[2] Hier ist es gut, wenn man sich zumindest an folgende Punkte erinnert:

$$1 = e^0 \tag{7}$$

$$i = e^{\frac{\pi}{2}} \tag{8}$$

$$-1 = e^{\pi} \tag{9}$$

$$-i = e^{\frac{3\pi}{2}} \tag{10}$$

Wir sehen aber auch noch eine weitere Möglichkeit um z per Trigonometrie darzustellen. Dazu überlegen wir uns, dass in der komplexen Ebene ein rechtwinkliges Dreieck gebildet werden kann, dessen Hypotenuse die Länge r hat. Die Ankathete am Winkel φ hat dann Länge a und die Gegenkathete hat Länge b. In einem Rechtwinkligen Dreieck wissen wir, dass $b = r\sin(\varphi)$ und $a = r\cos(\varphi)$ gilt. Drücken wir a und b auf diese Art und Weise aus, bestimmen wir $z = r\cos(\varphi) + ir\sin(\varphi)$. Die Darstellung durch Polarkoordinaten hat gewisse Vorteile, wie in folgendem Beispiel gezeigt:

Wir betrachten die komplexe Zahl $z = 1 + i \in \mathbb{C}$. Mit eben ausgeführten Überlegungen finden

[2] Eine Feinheit wäre die Frage, was die Darstellung im Ursprung ist, da man hier jeden Winkel wählen kann. Wir sagen hier aber einfach $r = 0, \varphi = 0$ und machen uns erstmal keine weiteren Gedanken darüber. Wenn man aber Abbildungen hat, die winkelabhängig sind, sollte man prüfen ob sie im Ursprung wohldefiniert sind.

wir die folgenden drei Darstellungen für die gleiche Zahl.

$$z = 1 + i \tag{11}$$
$$z = \sqrt{2}e^{i\frac{\pi}{4}} \tag{12}$$
$$z = \sqrt{2}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right) \tag{13}$$

Die verschiedenen Darstellungen haben Vorteile. $1 + i$ mag für den Anfang anschaulicher sein, als die Darstellung $\sqrt{2}e^{i\frac{\pi}{4}}$, aber nehmen wir an, wir wollen die n-te Potenz von z bestimmen. $z^n = (1 + i)^n$ ist für hohe n auch unter Verwendung der binomischen Formel nicht simpel. Allerdings können wir rechnen:

$$z^n = \left(\sqrt{2}e^{i\frac{\pi}{4}}\right)^n \tag{14}$$
$$= \sqrt{2}^n e^{i\frac{n\pi}{4}} \tag{15}$$
$$= \sqrt{2}^n \left(\cos\left(\frac{n\pi}{4}\right) + i\sin\left(\frac{n\pi}{4}\right)\right) \tag{16}$$

Aufgabe 1

1. Zeige $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$
2. Bestimme $\sum_{k=0}^{n}\binom{n}{k} = 0$
3. Zeige $\sum_{k=0}^{n}(-1)^k\binom{2n}{2k} = 2^n\cos(\frac{n\pi}{2})$
4. Bestimme $\sum_{k=0}^{n}(-1)^{k+1}\binom{2n}{2k-1}$

Lösung:
Für diese Aufgabe brauchen wir (unter der Vereinbarung $0 \in \mathbb{N}$):

Seien $n, k \in \mathbb{N}$ mit $n \geq k$, dann definieren wir den *Binomialkoeffizienten* "n über k"[a] als

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{17}$$

[a] Im Englischen "n choose k", nicht "n over k". Mit letzterem bezeichnet man den Bruch $\frac{n}{k}$.

wobei $\binom{n}{k}$ die Möglichkeit angibt, k Elemente aus n Elementen zu wählen. Zusätzlich definiert man üblicherweise $\binom{n}{k} = 0$, falls $k > n$ gilt. Der Binomialkoeffizient ist essentiell für den binomischen Lehrsatz:

Seien $a, b \in \mathbb{C}$ und $n \in \mathbb{N}$, dann gilt:

$$(a + b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \tag{18}$$

Es gibt eine Reihe von praktischen Rechenregeln für den Binomialkoeffizienten. Angenommen $n \geq 1$, dann:

$$\binom{n}{0} = \binom{n}{n} = 1 \tag{19}$$

$$\binom{n}{1} = \binom{n}{n-1} = n \tag{20}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{21}$$

$$\tag{22}$$

und noch viele weitere. Es gilt für $k > n$, dass

$$\binom{n}{k} := 0 \tag{23}$$

Wir können nun zur Berechnung der oben genannten Summen übergehen. Die direkte Berechnung ist wenig naheliegend, da man beliebig lange Summen bekäme, da würde sich normalerweise eher Induktion anbieten, aber auch damit macht man sich zu viel Arbeit.[3] In diesem Fall ist der Trick, die Summe in etwas umzuwandeln, was man sehr viel einfacher berechnen kann. Wir wenden also den binomischen Lehrsatz mit geeigneten a, b an.

1. Wir sehen in diesem Fall, dass die Formel der binomischen Formel gleicht, lediglich $a^k b^{n-k}$ ist durch $(-1)^k$ ersetzt worden. Aber das entspricht der Wahl $a = -1, b = 1$. Es gilt also:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} (-1)^k 1^{n-k} \binom{n}{k} = (1-1)^n = 0 \tag{24}$$

2. Diese Teilaufgabe ist nahezu identisch lösbar, wir sehen mit $a = b = 1$, dass

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} 1^k 1^{n-k} \binom{n}{k} = (1+1)^n = 2^n \tag{25}$$

7. Wir werden die beiden Teilaufgaben auf einmal lösen, da sie Teil einer Summe sind. Vergleichen wir die beiden Summen in der dritten und vierten Teilaufgabe, so fällt bereits auf, dass sie sich sehr ähnlich sehen. Und das Ergebnis der dritten Teilaufgabe können wir mit unserer obigen Berechnung von $(1+i)^n$ vergleichen und erkennen den Term wieder. Wir berechnen nun:

$$(1+i)^{2n} = \sum_{k=0}^{2n} i^k \binom{2n}{k} \tag{26}$$

$$= \sum_{k=0}^{n} i^{2k} \binom{2n}{2k} + i^{2k+1} \binom{2n}{2k+1} \tag{27}$$

$$= \sum_{k=0}^{n} (-1)^k \binom{2n}{2k} + \sum_{k=1}^{n} \underbrace{i^{2k-1}}_{=i \cdot i^{2k-2}} \binom{2n}{2k-1} \tag{28}$$

$$= \sum_{k=0}^{n} (-1)^k \binom{2n}{2k} + i \sum_{k=1}^{n} (-1)^{k-1} \binom{2n}{2k-1} \tag{29}$$

[3] Ich habs nicht probiert, keine Ahnung, ob da was sinnvolles rauskommt.

Wir haben für die zweite Gleichheit verwendet, dass der größte Term der zweiten Summe 0 ist, da $\binom{2n}{2n+1} = 0$. Außerdem gilt natürlich $(-1)^{k-1} = (-1)^{k+1}$, also ist die zweite Summe der letzten Zeile genau der Term aus Teilaufgabe 4. Mit obiger Berechnung können wir auf der anderen Seite zeigen, dass

$$(1+i)^{2n} = \sqrt{2}^{2n}\left(\cos\left(\frac{2n\pi}{4}\right) + i\sin\left(\frac{2n\pi}{4}\right)\right) \tag{30}$$

Durch Koeffizentenvergleich zwischen den beiden Realteilen und den Imaginärteilen der beiden Darstellungen von $(1+i)^{2n}$ sehen wir also, dass

$$\sum_{k=0}^{n}(-1)^k\binom{2n}{2k} = 2^n\cos\left(\frac{n\pi}{2}\right) \tag{31}$$

$$\sum_{k=1}^{n}(-1)^{k+1}\binom{2n}{2k-1} = 2^n\sin\left(\frac{n\pi}{2}\right) \tag{32}$$

Aufgabe 2

1. Seien $a, b \in \mathbb{Z}$ mit größtem gemeinsamen Teiler d, dass es $x, y \in \mathbb{Z}$ gibt, sodass $d = ax + by$ gilt.
2. Zeige, dass $\mathbb{Z}/n\mathbb{Z}^\times = \{\overline{a} \mid (a, n) = 1\}$
3. Zeige, dass $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist, genau wenn n eine Primzahl ist.

Lösung:
Wir haben mehrere Konzepte zu besprechen, bevor wir die Aufgabe lösen. Als erstes wiederholen wir folgende, neue algebraische Strukturen:

Ein *Monoid* ist ein Tupel $(M, *)$, bestehend aus einer Menge M und einer Verknüpfung $* : M \times M \to M$, sodass gilt

1. *Assoziativgesetz*: Für alle $a, b, c \in M$ gilt:

$$(a * b) * c = a * (b * c) \tag{33}$$

2. *Neutrales Element*: Es existiert ein Element das bezüglich der Operation neutral ist. Also

$$\exists e \in M : \forall m \in M : e * m = m * e = m \tag{34}$$

Vergleichen wir das mit der Definition einer Gruppe, so sehen wir, dass die Operationen auf Gruppen und Monoiden ähnlich sind, wir für eine Gruppe aber noch die Existenz von inversen Elementen verlangen. Weiter gibt es:

Ein *Ring* ist ein Tupel $(R, +, \cdot)$, bestehend aus einer Menge R, einer Verknüpfung $+ : R \times R \to R$, genannt *Addition* und einer Verknüpfung $\cdot : R \times R \to R$ genannt *Multiplikation* mit folgenden Eigenschaften:

1. $(R, +)$ ist eine abelsche Gruppe. Die Addition ist also assoziativ, hat ein neutrales Element, das wir 0 nennen und es gibt für jedes Element ein inverses.
2. Die Multiplikation ist assoziativ.

3. Es gelten die Distributivgesetze: $\forall a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{35}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \tag{36}$$

Ist die Multiplikation abelsch, sprechen wir von einem *kommutativen Ring*. Gibt es bezüglich der Multiplikation ein neutrales Element (das wir 1 nennen), bildet die Multiplikation also einen Monoid, dann sprechen wir von einem *unitären Ring* oder *Ring mit Eins*.

Man beachte, dass die Definition eines Ringes nicht eindeutig ist und man in jedem Text darauf achten sollte, welcher Konvention der Autor folgt. Manche Leute definieren einen Ring grundsätzlich als kommutativen Ring mit Eins. Beispiele für Ringe sind die ganzen Zahlen $\mathbb{Z}$ oder auch reellwertige Funktionen, also $\{f : \mathbb{R} \to \mathbb{R}\}$ mit punktweiser Addition und Multiplikation. Kein Beispiel sind dagegen die natürlichen Zahlen, denn in diesen gibt es bezüglich der Addition keine inversen Elemente. Zuletzt definieren wir

Ein *Körper* ist ein Tupel $(\mathbb{K}, +, \cdot)$, bestehend aus einer Menge $\mathbb{K}$, Addition und Multiplikation sodass

1. $(\mathbb{K}, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
2. $(\mathbb{K}\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1
3. Es gilt das Distributivgesetz, wie in einem Ring.

Wir könnten einen Körper auch als einen Ring definieren in dem bezüglich der Multiplikation jedes Element außer der 0 invertierbar ist und $0 \neq 1$ gilt (in einem Ring kann $0 = 1$ gelten.)[4] Beispiele für Körper sind $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ oder, wie wir zeigen werden, auch $\mathbb{Z}/p\mathbb{Z}$, wobei p eine Primzahl ist. Die ganzen Zahlen sind dagegen kein Körper, da z.B. 3 bezüglich der Multiplikation nicht invertierbar ist, denn $\frac{1}{3}$ liegt nicht in den ganzen Zahlen.

Für alle Strukturen können wir Homomorphismen definieren, diese zeichnen sich jeweils durch die Eigenschaft aus, dass es egal ist, ob wir die Operationen vor oder nach dem Homomorphismus ausführen. Wichtig ist hierbei noch, dass in Ringen und Körpern die 1 jeweils auf die 1 abgebildet werden muss.

Weiter wollen wir noch definieren:

Seien $a, b \in \mathbb{Z}$. Dann nennen wir $d \in \mathbb{Z}$ den *größten gemeinsamen Teiler von a und b*, geschrieben $d = ggT(a, b) = (a, n)$, falls gilt, dass:

1. *Teilbarkeit* $d|a$ und $d|b$, also d teilt a und b. Zur Erinnerung:

$$d|a \Leftrightarrow \exists p \in \mathbb{Z} : dp = a \tag{37}$$

2. *Maximalität* d muss auch der größte Teiler sein, das heißt: Ist $d' \in \mathbb{Z}$ ein weiterer Teiler von a und b, dann gilt $d'|d$.

Diese Definition kann auf allgemeine Ringe erweitert werden indem man einfach $\mathbb{Z}$ durch R ersetzt. Es gibt allerdings nicht in jedem Ring für jedes Elementpaar einen größten gemeinsamen Teiler. Wir wollen nun die Aufgaben lösen:

[4] Man sollte sich hier nicht verwirren lassen. Wenn wir im Kontext allgemeiner Ringe und Körper über 1 und 0 sprechen, so meinen wir damit immer die neutralen Elemente dieser Strukturen. Mit den Zahlen 0 und 1 aus $\mathbb{Z}$, bzw. $\mathbb{R}$ müssen diese nichts zu tun haben.

1. Seien $a, b \in \mathbb{Z}$ mit größtem gemeinsamen Teiler d. Wir wenden den Tipp an und schreiben

$$d' = \min\{ax + by \mid x, y \in \mathbb{Z}\} \cap (\mathbb{N}\backslash\{0\}) \tag{38}$$

dann gilt $d' = ax' + by'$ für $x', y' \in \mathbb{Z}$ und $d' > 0$. Per Division mit Rest sehen wir, dass es $q \in \mathbb{Z}$ und $0 \leq r < d'$ gibt, sodass

$$a = qd' + r = q(ax' + by') + r \tag{39}$$

Stellen wir diese Gleichung um, so erhalten wir

$$r = a(1 - qx') + b(-qy') \tag{40}$$

haben also eine Darstellung der Form $r = ax + by$ gefunden. Da jedoch $r < d'$ gilt und d' bereits das minimale Element ungleich 0 ist, folgt damit $r = 0$ (ansonsten wäre d' nicht das kleinste Element). Es gilt also $a = qd'$, insbesondere ist d' ein Teiler von a. Analog zeigen wir, dass d' ein Teiler von b ist. Da d der größte gemeinsame Teiler von a und b ist - und d' ebenfalls beide Elemente teilt, folgt damit $d'|d$.
Auf der anderen Seite gilt aufgrund der Darstellung $d' = ax' + by'$, dass d ein Teiler von d' ist, also $d|d'$. Das kann aber nur sein, falls $d = d'$ gilt und somit haben wir eine Darstellung $d = ax' + by'$ gefunden.

2. Wir zeigen die beiden Inklusionen:

   "$\subseteq$" Angenommen $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^\times$, dann existiert $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^\times$ sodass $\overline{ax} = \overline{1}$. Per Definition heißt das, dass $y \in \mathbb{Z}$ existiert, sodass

   $$ax = 1 + ny \tag{41}$$

   Also gilt insbesondere $1 = ax - ny$. Der größte gemeinsame Teiler von a und n teilt auch $ax - ny$, also 1. Die einzige Zahl die 1 teilt ist aber 1 selbst, deswegen gilt $\overline{a} \in \{\overline{a} \mid (n, a) = 1\}$.

   "$\supseteq$" Angenommen $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ sodass $(a, n) = 1$. Dann gibt es laut Teilaufgabe 1 eine Darstellung $1 = ax + ny$, mit $x, y \in \mathbb{Z}$. Dann gilt aber in Äquivalenzklassen

   $$\overline{1} = \overline{ax} = \overline{a}\,\overline{x} \tag{42}$$

   also ist $\overline{x}$ das inverse von $\overline{a}$, insbesondere ist $\overline{a}$ invertierbar.

   Die Mengen sind also gleich.

3. "$\Rightarrow$" Wir zeigen diese Aussage per Kontraposition. Angenommen $n \geq 2$ ist keine Primzahl. Dann gibt es eine Zahl $a \in \mathbb{Z}$, sodass $1 < a < n$ und $ggT(a, n) \neq 1$. Laut Teilaufgabe 2 bedeutet das aber, dass $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ nicht invertierbar ist. Da $a \neq 0$ gilt, ist $\mathbb{Z}/n\mathbb{Z}$ dann kein Körper. Das bedeutet, wenn $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist, dann ist n eine Primzahl.

   "$\Leftarrow$" Angenommen n ist eine Primzahl. Dann hat n lediglich 1 und n als Teiler. Das heißt aber mit Teilaufgabe 2, dass alle Elemente in $\mathbb{Z}/n\mathbb{Z}$ invertierbar sind (außer $\overline{n}$ selbst, aber $\overline{n} = 0$). Damit ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper.

Aufgabe 3

1. Zeige, dass $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ ein Teilring von $\mathbb{C}$ ist.
2. Bestimme $\mathbb{Z}[i]^\times$.

Lösung:

1. Was ist notwendig um ein Teilring zu sein?

   Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $S \subseteq R$ ist genau dann ein *Teilring* oder *Unterring*, wenn $(S, +, \cdot)$ ein Ring ist.

   Also zeigen wir genau das:

   Wir wollen zeigen, dass $\mathbb{Z}[i]$ ein Teilring von $\mathbb{C}$ ist. Da $\mathbb{Z} \subseteq \mathbb{R}$ eine Teilmenge ist, ist auf jeden Fall $\mathbb{Z}[i] \subseteq \mathbb{C}$ eine Teilmenge. Also müssen wir nur noch zeigen, dass $\mathbb{Z}[i]$ mit den aus $\mathbb{C}$ geerbten Operationen ein Ring ist. Dabei müssen wir jedoch nicht die volle Reihe an Ringeigenschaften, die wir oben definiert hatten, erneut prüfen. Da sich an der Addition und Multiplikation nichts ändert und wir nur ihre Definitionsmengen von $\mathbb{C} \times \mathbb{C}$ auf $\mathbb{Z}[i] \times \mathbb{Z}[i]$ einschränken, bleibt die Assoziativität und Distributivität erhalten. Wir zeigen also:

   - *Addition ist eine Gruppe*: Da die Assoziativität vererbt wird, müssen wir Abgeschlossenheit, Existenz des neutralen Elements und Existenz von inversen Elementen zeigen. Das sind aber alles Eigenschaften, die direkt daraus folgen, dass $\mathbb{Z}$ ein Ring ist. Addieren wir zwei Zahlen $a + bi, c + di \in \mathbb{Z}[i]$, dann addieren wir die Real- und Imaginärteile separat und landen wieder in den ganzen Zahlen. $0 \in \mathbb{Z}[i]$ ist klar und für jedes Element $a \in \mathbb{Z}$ liegt auch das inverse in $\mathbb{Z}$.
   - *Multiplikation*: Für die Multiplikation in einem Ring verlangen wir lediglich, dass sie assoziativ ist. Das haben wir gezeigt. Es ist hier vielleicht noch hilfreich zu sehen, dass $\mathbb{Z}[i]$ ein Ring mit 1 ist.
   - *Distributivität*: Auch hier müssen wir nichts zeigen.

2. Wir wollen $\mathbb{Z}[i]^\times$ finden, also überlegen wir uns, welche Eigenschaften ein Element in $\mathbb{Z}[i]$ haben muss um invertierbar zu sein. Wir überlegen uns folgendes: Sei $z \in \mathbb{Z}[i]$ invertierbar, dann gibt es ein inverses $y \in \mathbb{Z}[i]$. Es gilt

   $$|z|^2|y|^2 = |zy|^2 = |1|^2 = 1 \tag{43}$$

   Da wir uns allerdings auf $\mathbb{Z}[i]$ eingeschränkt haben und für $z = a + bi$ gilt, dass $|z|^2 = |a|^2 + |b|^2$, gilt auch $|z|^2 \in \mathbb{Z}$. Insbesondere also $|z| = |y| = 1$. Da $|a|^2, |b|^2$ notwendigerweise nichtnegativ sind, bleibt damit nur die Wahl $a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$. Das entspräche $z \in \{1, -1, i, -i\}$. Umgekehrt können wir uns überlegen, dass jedes dieser Elemente invertierbar ist, da $i \cdot (-i) = 1$ gilt. Das heißt die Menge $\{1, -1, i, -i\}$ stimmt mit $\mathbb{Z}[i]^\times$ überein.

Aufgabe 4
Sei $\mathbb{K}$ ein Körper und sei $\mathbb{R} \subseteq \mathbb{K}$ ein Teilkörper. Sei weiter $r \in \mathbb{K} \backslash \mathbb{R}$ sodass

$$\mathbb{K} = \{a + br \mid a, b \in \mathbb{R}\} \tag{44}$$

Zeige, dass $\mathbb{K}$ isomorph zu $\mathbb{C}$ ist.

Lösung:
Wir wollen dem Hinweis folgen und Aufgabe 1 vom vierten Übungsblatt anwenden. Diese sagt aus: *Ist $\mathbb{K}$ ein Körper und S ein Ring mit $0 \neq 1$, dann ist jeder Homomorphismus $\varphi : \mathbb{K} \to S$ ein Monomorphismus.* Wir wollen also einen Ringhomomorphismus von $\mathbb{K}$ nach $\mathbb{C}$ konstruieren der surjektiv ist. Zusammen mit der vorherigen Aussage folgt dann, dass $\mathbb{K}$ und $\mathbb{C}$ isomorph sind.

Bevor wir den Homomorphismus selbst konstruieren, zeigen wir:

- Für ein beliebiges $x \in \mathbb{K}$ sind a, b eindeutig. Nehmen wir an, dass es Darstellungen $x = a + br = c + dr$ gibt, sodass $b \neq d$. Dann gilt:

$$a + br = c + dr \tag{45}$$
$$\Rightarrow (b - d)r = c - a \tag{46}$$
$$\Rightarrow r = \frac{c - a}{b - d} \in \mathbb{R} \tag{47}$$

  Da $a, b, c, d \in \mathbb{R}$ wäre damit auch $r \in \mathbb{R}$, wir hatten allerdings vorher die Bedingung gesetzt, dass $r \notin \mathbb{R}$, also ist das ein Widerspruch. Es gilt also $b = d$. Ziehen wir die beiden Darstellungen voneinander ab, so erhalten wir $0 = a - c$, also muss auch $a = c$ gelten und die Wahl von a, b ist eindeutig.

- Für das ausgezeichnete Element $r \in \mathbb{K}$ gilt, dass $r^2 \in \mathbb{K}$ liegt, also gilt

$$\exists a_0, b_0 \in \mathbb{R} : r^2 = a_0 + b_0 r \tag{48}$$

  Natürlich sind auch a_0, b_0 eindeutig. Wir definieren nun die Zahl

$$z = \left(-b_0 + \sqrt{b_0^2 - 4a_0} \right) \tag{49}$$

  Dann gilt auch $z^2 = a_0 + b_0 z$.

Wir definieren nun

$$\varphi : \mathbb{K} \to \mathbb{C} \tag{50}$$
$$a + br \mapsto a + bz \tag{51}$$

diese Abbildung ist wohldefiniert, da die Wahl von a, b eindeutig ist. Wir verwenden hier + sowohl für die Addition in $\mathbb{K}$, als auch in $\mathbb{C}$, obwohl es unterschiedliche Abbildungen sind. Aus dem Kontext ist allerdings jeweils klar, welche Abbildung gerade gemeint ist und die Eigenschaften sind ähnlich genug.[a] Es gilt klarerweise

$$\varphi(0) = 0 \tag{52}$$
$$\varphi(1) = 1 \tag{53}$$

und wir bestimmen weiter für $a + br, c + dr \in \mathbb{K}$

$$\varphi((a + br) + (c + dr)) = \varphi(a + br) + \varphi(c + dr) \tag{54}$$

also verträgt sich φ mit der Addition und auch

$$\begin{aligned}\varphi((a+br)(c+dr)) &= \varphi(ac+adr+bcr+bdr^2) && (55)\\ &= \varphi(ac+bda_0+(ad+bc+bdb_0)r) && (56)\\ &= ac+bda_0+(ad+bc+bdb_0)z && (57)\end{aligned}$$

sowie

$$\begin{aligned}\varphi(a+br)\varphi(c+dr) &= (a+bz)(c+dz) && (58)\\ &= ac+adz+bcz+bdz^2 && (59)\\ &= ac+bda_0+(ad+bc+bdb_0)z && (60)\end{aligned}$$

also verträgt sich φ auch mit der Multiplikation, ist insgesamt also ein Homomorphismus von Ringen. Mit Aufgabe 1 vom vierten Übungsblatt folgt bereits, dass es ein Monomorphismus ist. Da $\varphi(r) = z \notin \mathbb{R}$ gilt, ist φ auch surjektiv, insgesamt also ein Isomorphismus. Das heißt $\mathbb{K} \simeq \mathbb{C}$, was die zu zeigende Aussage ist.

[a] Das Konzept entspricht dem operator overloading im Programmieren.

Wir können uns jetzt im Nachhinein fragen, wieso wir uns den Aufwand gemacht haben und nicht einfach r auf i abgebildet haben. Da wären wir aber auf das Problem gestoßen, dass im Allgemeinen $r^2 \neq -1$ gilt und dann wäre wegen

$$\varphi(r^2) = \varphi(a_0 + b_0 r) = a_0 + b_0 i \neq -1 = \varphi(r)\varphi(r) \tag{61}$$

die Abbildung kein Homomorphismus mehr.