HAW LANDSHUT
FAKULTÄT FÜR INFORMATIK
Eisenreich/Hartmann/Sagraloff/Schröter

WS 2023/2024
Blatt 4

Lösungsskizzen zur Übung „Mathematik I"

Präsenzaufgabe. (a)

$$\begin{aligned}
345 &= 1 \cdot 234 \text{ Rest } 111; \quad 111 = 345 - 1 \cdot 234 \\
234 &= 2 \cdot 111 \text{ Rest } 12; \quad 12 = 234 - 2 \cdot 111 = 234 - 2 \cdot (345 - 1 \cdot 234) = 3 \cdot 234 - 2 \cdot 345 \\
111 &= 9 \cdot 12 \text{ Rest } 3; \\
3 &= 111 - 9 \cdot 12 = 345 - 1 \cdot 234 - 9 \cdot (3 \cdot 234 - 2 \cdot 345) \\
&= 345 - 234 - 27 \cdot 234 + 18 \cdot 345 \\
&= 19 \cdot 345 - 28 \cdot 234
\end{aligned}$$

Es gilt also: $ggT(345, 234) = ggT(234, 111) = ggT(111, 12) = ggT(12, 3) = 3$ und $3 = 19 \cdot 345 - 28 \cdot 234$

(b) Die $\overline{0}$ hat kein Inverses: $\overline{0} \odot \overline{a} = 0$ für alle $\overline{a}$.

(c)
- $(4 - i)(4 + i) = 4^2 + 1^2 = 17$
- $\frac{1-i}{1+i} = \frac{(1-i)(1-i)}{(1+i)(1-i)} = \frac{1-2i-1}{2} = \frac{-2i}{2} = -i$

Aufgabe 1. Gruppen und Homomorphismen Welche der folgenden Abbildungen sind Gruppenhomomorphismen? Falls sie es sind, sind sie auch Gruppenisomorphismen? Begründen Sie Ihre Aussagen.

(a) $f: \mathbb{Z} \to \mathbb{Z}, x \mapsto x^2$

(b) $f: \mathbb{Z} \to \mathbb{Z}, x \mapsto 2 \cdot x$

(c) $f: (\mathbb{Z}/5\mathbb{Z}, \oplus) \to (\mathbb{Z}/5\mathbb{Z}, \oplus), \overline{x} \mapsto \overline{2} \odot \overline{x}$.

(d) Ist die letzte Abbildung auch ein Ringhomomorphismus auf $(\mathbb{Z}/5\mathbb{Z}, \oplus, \odot)$?

Lösung 1. (a) kein Gruppenhomomorphismus, da für $a, b \in \mathbb{Z}$ gilt:

$$f(a + b) = (a + b)^2 = a^2 + 2ab + b^2,$$

aber $f(a) + f(b) = a^2 + b^2$, also gilt zum Beispiel

$$f(1 + 1) = 4 \neq f(1) + f(1) = 2.$$

(b) Ist ein Gruppenhomomorphismus, da für $a, b \in \mathbb{Z}$ gilt: $f(a+b) = 2 \cdot (a+b) = 2a + 2b = f(a) + f(b)$
Ist kein Isomorphismus, da f nicht surjektiv ist, das Bild sind nur die geraden ganzen Zahlen; z.B. gibt es kein Urbild von 3.

(c) Ist ein Gruppenhomomorphismus, da für $\overline{a}, \overline{b} \in \mathbb{Z}/5\mathbb{Z}$ gilt:

$$f(\overline{a} \oplus \overline{b}) = \overline{2} \odot (\overline{a} \oplus \overline{b}) = \overline{2} \odot \overline{a} + \overline{2} \odot \overline{b} = f(a) + f(b)$$

Ist ein Isomorphismus;

- f ist injektiv: Seien $\overline{a}, \overline{b} \in \mathbb{Z}/5\mathbb{Z}$ so dass $f(\overline{a}) = f(\overline{b}) \Leftrightarrow \overline{2} \odot \overline{a} = \overline{2} \odot \overline{b}$. Da $\mathbb{Z}/5\mathbb{Z}$ ein Körper ist, gibt es ein Inverses $\overline{2}^{-1} = \overline{3}$ von $\overline{2}$ bezüglich Multiplikation, damit mulitplizieren wir die Gleichung durch, und es folgt: $\overline{a} = \overline{b}$
- f ist surjektiv: Dazu müssen wir zeigen, dass alle Elemente $\overline{y} \in \mathbb{Z}/5\mathbb{Z}$ ein Urbild unter f haben, also ein $\overline{x}$, so dass $f(\overline{x}) = \overline{2} \odot \overline{x} = \overline{y}$. Dazu multiplizieren wir die letzte Gleichung mit dem Inversen $\overline{2}^{-1} = \overline{3}$ von $\overline{2}$ bezüglich Multiplikation durch, und erhalten das Urbild: $\overline{x} = \overline{2}^{-1} \odot \overline{y} = \overline{3} \cdot \overline{y}$.

(d) Nein, da z.B. $f(\overline{1} \odot \overline{1}) = f(\overline{1}) = \overline{2}, f(\overline{1}) \odot f(\overline{1}) = \overline{2} \odot \overline{2} = \overline{4}$.

Aufgabe 2. Abbildungsgruppen, Permutationen

(a) Wir betrachten den Raum S_4 der Permutationen von $\{1, 2, 3, 4\}$, und

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Berechnen Sie $\sigma_1 \circ \sigma_2$ und $\sigma_2 \circ \sigma_1$.

(b) Die Ecken eines Quadrates seien mit den Zahlen 1 bis 4 im Gegenuhrzeigersinn nummeriert. Dreht man das Quadrat um Vielfache von 90 Grad, so werden alle 4 Ecken jeweils wieder auf die Ecken überführt.[1] Somit kann jede solche Drehung als Element in der Permutationsgruppe S_4 auffassen. Schreiben Sie jede Drehung als Permutation. Bildet die Menge aller Drehungen (mit der Komposition als Operation) eine Untergruppe von S_4?

Lösung 2. (a)

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

[1] Bei einer Drehung um genau 90 Grad im Uhrzeigersinn wird beispielsweise Ecke 1 auf 4, 4 auf 3, 3 auf 2, und 2 auf 1 überführt.

(b) Nach dem Untergruppenkriterium muss nur gezeigt werden, dass mit je zwei Drehungen auch die Kombination und mit einer Drehung auch die Inverse enthalten ist. Die Menge D der Drehungen enthält genau 4 Elemente: 0°, 90°, 180°, 270°. Die Drehung um 0°ist gerade das Eins-Element. Die Drehung um 360°ist wieder die um 0°. Es ist klar, dass je zwei Drehungen hintereinander wieder eine dieser vier Drehungen ergibt, und dass sich jede Drehung zu einer Drehung um 360°(= 0°) ergänzen lässt. Damit haben wir eine Untergruppe. Schreiben wir einmal die 4 Elemente als Permutationen auf:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = a,$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = b, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = c$$

Aufgabe 3. Komplexe Zahlen

(a) Berechnen Sie die folgenden Terme, d.h. stellen Sie das Ergebnis wieder als komplexe Zahl in der Form $a + b \cdot \mathbf{i}$ mit $a, b \in \mathbb{R}$ dar (sollte a oder $b = 0$ sein, kann man den Teil auch weglassen):

$$(1+2\cdot\mathbf{i})\cdot(2-5\cdot\mathbf{i}), \quad (\overline{3+4\cdot\mathbf{i}})\cdot(3+4\cdot\mathbf{i}), \quad |3+4\cdot\mathbf{i}|, \quad \frac{1-\mathbf{i}}{2+\mathbf{i}}, \quad \frac{1}{2+i}, \quad \left|\frac{1}{2+i}\right|.$$

(b) Geben Sie alle komplexen Lösungen der Gleichung $x^4 = 4$ an!

(c) Bestimmen Sie alle komplexen Nullstellen des Polynoms $f(x) = x^3 - x^2 + x - 1$.

Lösung 3. Komplexe Zahlen

(a) Die Rechenregeln finden Sie in der Vorlesung. Insbesondere verwenden wir, dass $|z|^2 = z \cdot \overline{z}$.

$$(1+2i)(2-5i) = 2 - 10i^2 + 4i - 5i = 12 - i$$
$$(\overline{3+4i})(3+4i) = |3+4i|^2 = 9 + 16 = 25$$
$$|3+4i| = 5$$
$$\frac{1-i}{2+i} = \frac{(1-i)(2-i)}{(2+i)(2-i)} = \frac{1-3i}{5} = \frac{1}{5} - \frac{3}{5}i$$
$$\frac{1}{2-i} = \frac{2+i}{5} = \frac{2}{5} + \frac{1}{5}i$$
$$\left|\frac{2}{5} + \frac{1}{5}i\right| = \sqrt{\frac{4}{25} + \frac{1}{25}} = \sqrt{\frac{1}{5}} = \frac{1}{\sqrt{5}}$$

(b) $\sqrt{2}, -\sqrt{2}, i\sqrt{2}, -i\sqrt{2}$.

(c) Die erste Nullstelle ist 1. Polynomdivision durch $(x-1)$:

$$(x^3 - x^2 + x - 1) \quad : (x-1) \quad = \quad x^2 + 1$$

Es gilt $f(x) = (x-1)(x^2+1)$ und $x^2 + 1 = 0 \Leftrightarrow x^2 = -1 \Leftrightarrow x \in \{i, -i\}$, also gilt:
$f(x) = (x-1)(x+i)(x-i)$ hat die Nullstellen $1, -i, i$.

Aufgabe 4. Endliche Körper, RSA Algorithmus Max möchte gerne mit seiner Freundin Mathilda auf sicherem Wege kommunizieren. Die beiden verwenden zur Verschlüsselung Ihrer Nachrichten den RSA Algorithmus. Max wählt dazu die beiden Primzahlen $p = 5$ und $q = 17$. Max schickt Mathilda den von ihm gewählten public key e. Als private key berechnet Max die Zahl $d = 49$. Mathilda möchte an Max die Nachricht $m = 15$ schicken. Wie lautet die verschlüsselte Nachricht M, die von Mathilda an Max verschickt wird?

Lösung 4. RSA Algorithmus Wie lautet der private key? Nachdem wir die Primzahlen kennen, können wir ihn aus d berechnen: Zunächst müssen wir ausrechnen: $(p-1)(q-1) = 4 \cdot 16 = 64$. Es sind d und e in $\mathbb{Z}/64\mathbb{Z}$ invers zueinander. Das Inverse berechnet man wieder mit dem erweiterten Euklid'schen Algorithmus, angewendet auf 64 und 49. Als Ergebnis erhalten Sie (rechnen Sie es nach!)

$$1 = 17 \cdot 49 - 13 \cdot 64$$

Das heißt: In $\mathbb{Z}/64\mathbb{Z}$ ist $1 = 17 \cdot 49$, also ist 17 das Inverse zu 49 und 17 ist der public Schlüssel von Max, der an Mathilda gesendet wird.
Ver- und Entschlüsselung finden modulo $n = p \cdot q = 5 \cdot 17 = 85$ statt. Zur Verschlüsselung von 15 muss $15^{17} \mod 85$ berechnet werden:

$15^{17} = 15 \cdot (15^8)^2$
$15^8 \mod 85 = 2562890625 \mod 85 = 35,35^2 \mod 85 = 35,15 \cdot 35 \mod 85 = 15$

Klartext und Schlüsseltext sind identisch, ein Ergebnis, das in der Realität sehr, sehr selten auftritt (sonst wäre der Algorithmus unbrauchbar).
Sie können auch wieder entschlüsseln: $m = 15^{49} \mod 85$ Rechnen Sie nach, ob wirklich $m = 15$ ist!