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

WS 2023/2024
Blatt 4
03.12.23

Übungen zur Vorlesung „Mathematik I"

Aufgabe 1. Gruppen und Homomorphismen *In der realen Welt treten immer wieder gewisse Strukuren auf, zum Beispiel in der Menge der ganzen Zahlen: man kann addieren und subtrahieren, und es gibt ein Element, das neutrale Element (bei den ganzen Zahlen die 0), das man addieren oder subtrahieren kann, ohne dass es etwas ändert. Es gibt auch andere Mengen, die solch eine Struktur aufweisen: man nennt sie "Gruppen". Zum Beispiel bilden die Drehungen eines Zauberwürfels eine Gruppe. Solche Strukturen haben sehr wichtige praktische Anwendungen: zum Beispiel benutzt man Gruppen, die man "elliptische Kurven" nennt, in Verschlüsselungsverfahren.*

Welche der folgenden Abbildungen sind Gruppenhomomorphismen? Falls sie es sind, sind sie auch Gruppenisomorphismen? Begründen Sie Ihre Aussagen.

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

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

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

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

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?

[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.

Aufgabe 3. Komplexe Zahlen *Komplexe Zahlen sind eine Erweiterung des reellen Zahlenraums, die eine Lösung für die Gleichung $x^2 = -1$ enthalten. Das ist mehr als nur eine theoretische Spielerei: tatsächlich braucht man komplexe Zahlenräume oft, um physikalische Phänomene in der realen Welt zu beschreiben, aber auch in 3D-Computergrafiken arbeitet man mit komplexen Zahlen. In der Mathematik braucht man komplexe Zahlen, um alle möglichen Lösungen von Gleichungen beschreiben zu können.*

(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:

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

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

(c) Bestimmen Sie alle komplexen Nullstellen des Polynoms

$$f(x) = x^3 - x^2 + x - 1$$

.

Aufgabe 4. Endliche Körper, RSA Algorithmus *Der RSA Algorithmus ist ein Beispiel von praktischen Anwendungen des Rechnens mit Restklassen und endlichen Körpern: ein Verschlüsselungsalgorithmus.*

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?