TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften, Fakultät Mathematik, Institut für Algebra

Jun.-Prof. Friedrich Martin Schneider, Dr. Henri Mühle. Wintersemester 2018/19

11. Übungsblatt zur Vorlesung "Diskrete Strukturen für Informatiker"

Homomorphismen, RSA

V. Es seien $(G, \circ_G)$ und $(H, \circ_H)$ Gruppen mit neutralen Elementen e_G und e_H. Für einen Gruppenhomomorphismus $f\colon G \to H$ definieren wir den *Kern* analog zum Kern von linearen Abbildungen zwischen Vektorräumen (vgl. Modul "Lineare Algebra") als

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}.$$

Weiter sei $\ker(f) = \{(g_1, g_2) \in G \times G \mid f(g_1) = f(g_2)\}$ der Kern einer Abbildung nach Definition 4.5.

(a) Zeigen Sie, dass $\mathrm{Ker}(f)$ der Äquivalenzklasse von $\ker(f)$ entspricht, die e_G enthält.

(b) Zeigen Sie, dass für $g_1, g_2 \in G$ gilt:

$$(g_1, g_2) \in \ker(f) \quad \text{genau dann wenn} \quad g_1 \circ_G g_2^{-1} \in \mathrm{Ker}(f).$$

Ü61. (a) Zum Verschlüsseln eines Textes wird das RSA-Kryptosystem verwendet. Dabei werden die Buchstaben A, B, ..., Z mit den Zahlen $0, 1, \ldots, 25$ codiert. Verschlüsseln Sie den Klartext GEHEIM mit den öffentlichen Schlüsseln

$$\text{(i) } (n, e) = (33, 3), \quad \text{(ii) } (n, e) = (15, 5).$$

(b) Es wurde die mit dem RSA-Verfahren verschlüsselte Nachricht QUTCIM zum öffentlichen Schlüssel $(n, e) = (21, 5)$ abgefangen. Wie kann diese Nachricht entschlüsselt werden? Wie lautet die entschlüsselte Nachricht?

Ü62. Es seien $(R, +_R, \circ_R)$ und $(S, +_S, \circ_S)$ zwei Ringe. Eine Abbildung $f\colon R \to S$ heißt *Ringisomorphismus*, falls f bijektiv ist, und für alle $x, y \in R$ gilt:

$$f(x +_R y) = f(x) +_S f(y) \quad \text{und} \quad f(x \circ_R y) = f(x) \circ_S f(y).$$

Für eine endliche Menge M werden die kommutativen Ringe $\big(\mathcal{P}(M), \Delta, \cap\big)$ und $\big(\{0,1\}^M, \oplus, \odot\big)$ aus den Aufgaben Ü33 und H35 betrachtet. Zeigen Sie, dass beide Ringe isomorph sind, indem Sie einen Ringisomorphismus explizit angeben.

Ü63. Zeigen Sie, dass die Gruppen

$$\text{(i)} \quad \mathbb{Z}_8, \quad \text{(ii)} \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \text{(iii)} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

paarweise nicht isomorph sind. Bestimmen Sie dazu jeweils die zyklischen Untergruppen (d.h. die von einem Element erzeugten Untergruppen), und vergleichen Sie diese Informationen.

A64. **Hausaufgabe, bitte vor Beginn der 12. Übung (oder im Lernraum) unter Angabe von Name, Matrikelnummer, Übungsgruppe und Übungsleiter abgeben.** Es wird das RSA-Kryptosystem mit dem öffentlichen Schlüssel $(n, e) = (33, 13)$ betrachtet.

(a) Für $i \in \{1, 2, 3, 4, 5, 6, 7\}$ bezeichne a_i die i-te Ziffer Ihrer Matrikelnummer. Verschlüsseln Sie die Nachricht $m = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ mit dem oben genannten öffentlichen Schlüssel.

(b) Führen Sie eine Probe durch, indem Sie zunächst den geheimen Schlüssel (n, d) bestimmen, und anschließend die in (a) erhaltene Nachricht entschlüsseln.

H65. Sei $n \in \mathbb{N}$, und $[n] = \{1, 2, \ldots, n\}$. Die Menge aller bijektiven Abbildungen von $[n]$ nach $[n]$ bildet mit der Hintereinanderausführung $\circ$ eine Gruppe; die *symmetrische Gruppe* vom Grad n, bezeichnet mit $\mathfrak{S}_n$.

(a) Wie viele Elemente hat $\mathfrak{S}_n$ für $n \in \mathbb{N}$?

(b) Geben Sie die Verknüpfungstafeln von $\mathfrak{S}_2$ und $\mathfrak{S}_3$ an.

(c) Zeigen Sie, dass die Gruppe $\big(\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ\big)$ aus Aufgabe H18 isomorph zu $\mathfrak{S}_3$ ist.

Hinweis: Eine bijektive Abbildung $f\colon [n] \to [n]$ lässt sich einfach mit Hilfe des Tupels $\big(f(1), f(2), \ldots, f(n)\big)$ der Bildwerte darstellen.

H66. Seien $(G, \circ_G)$ und $(H, \circ_H)$ zwei Gruppen und $f\colon G \to H$ eine Abbildung. Zeigen Sie, dass folgende Aussagen äquivalent sind.

(i) Die Abbildung f ist ein Homomorphismus von $(G, \circ_G)$ nach $(H, \circ_H)$.

(ii) Die Menge $\big\{(x, y) \in G \times H \mid f(x) = y\big\}$ ist eine Untergruppe von $(G \times H, \circ_{G\times H})$.