



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 $f: G \rightarrow H$ definieren wir den *Kern* analog zum Kern von linearen Abbildungen zwischen Vektorräumen (vgl. Modul “Lineare Algebra”) als

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

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 $\text{Ker}(f)$ der Äquivalenzklasse von $\ker(f)$ entspricht, die e_G enthält.
(b) Zeigen Sie, dass für $g_1, g_2 \in G$ gilt:

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

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

(i) $(n, e) = (33, 3)$, (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 $f: R \rightarrow S$ 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 $(\mathcal{P}(M), \Delta, \cap)$ und $(\{0, 1\}^M, \oplus, \odot)$ aus den Aufgaben Ü33 und H35 betrachtet. Zeigen Sie, dass beide Ringe isomorph sind, indem Sie einen Ringisomorphismus explizit angeben.

- Ü6)
- i) P q Primzahlen, P.q = n, $f(n) = (P-1)(q-1)$
 - ii) $e \in \{2, 3, \dots, \varphi(n)\}$ mit $\text{ggT}(e, \varphi(n)) = 1$
 - iii) $d \in \{2, 3, \dots, \varphi(n)\}$ mit $d \cdot e \equiv 1 \pmod{\varphi(n)}$
 - iv) (e, n) öffentliche Schlüssel, (d, n) geheimer Schlüssel
 - v) $m \in \mathbb{Z}_n^*$, kodiert mit (e, n) : $c \equiv m^e \pmod{n}$
 - vi) $c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \pmod{n}$
↓
Satz Euler.
Format.

i) $(n, e) = (33, 3)$

$$(6^3, 4^3, 7^3, 4^3, 8^3, 12^3) \pmod{33}$$

$$6^3 = 6^2 \cdot 6 \equiv 36 \cdot 6 \equiv 3 \cdot 6 \equiv 18 \pmod{33}$$

$$4^3 = 64 \equiv 31 \pmod{33}$$

$$7^3 = 7^2 \cdot 7 = 49 \cdot 7 \equiv 16 \cdot 7 \equiv 112 \equiv 13 \pmod{33}$$

$$8^3 = 64 \cdot 8 \equiv 31 \cdot 8 \equiv 248 \equiv (-1)8 \equiv -16 \equiv 17 \pmod{33}$$

$$12^3 = 12^2 \cdot 12 = 144 \cdot 12 \equiv 12 \cdot 12 \equiv 144 \equiv 12 \pmod{33}$$

↓
 $(18, 31, 13, 31, 17, 12)$

ii) $(6^5, 4^5, 7^5, 4^5, 8^5, 12^5) \pmod{15}$

$$6^5 = 6^2 \cdot 6 \cdot 6 = 36 \cdot 36 \cdot 6 \equiv 6 \cdot 36 \cdot 6 \equiv 6 \cdot 6 \cdot 6 \equiv 6 \pmod{15}$$

$$4^5 = 4^2 \cdot 4^2 \cdot 4 = 16 \cdot 16 \cdot 4 \equiv 4 \pmod{15}$$

$$7^5 = 49 \cdot 49 \cdot 7 \equiv 4 \cdot 4 \cdot 7 \equiv 7 \pmod{15}$$

$$8^5 = 64 \cdot 64 \cdot 8 \equiv 4 \cdot 4 \cdot 8 \equiv 8 \pmod{15}$$

$$12^5 = 144 \cdot 144 \cdot 12 \equiv 9 \cdot 9 \cdot 12 = 81 \cdot 12 \equiv 6 \cdot 12 \equiv -3 \equiv 12 \pmod{15}$$

$\rightsquigarrow (6, 4, 7, 4, 8, 12)$

b) $\mathbb{Q} \cup \mathbb{T} \subset \mathbb{I} \setminus \mathbb{N}$. $(n, e) = (21, 5)$

$\varphi(21) = 2 \cdot 6 = 12$

$5d \equiv 1 \pmod{12}$

$5 \cdot 5 \equiv 1 \Rightarrow (d, n) = (5, 21)$

$\Rightarrow (16^5, 20^5, 19^5, 2^5, 8^5, 12^5) \pmod{21}$

$16^5 = 256 \cdot 256 \cdot 16 \equiv 4 \cdot 4 \cdot 16 \pmod{21} \equiv 4 \pmod{21}$

$20^5 = 400 \cdot 400 \cdot 20 \equiv 20 \pmod{21}$

$19^5 = 361 \cdot 361 \cdot 19 \equiv 4 \cdot 4 \cdot 19 \equiv 4 \cdot 13 \equiv 10 \pmod{21}$

$2^5 = 32 \equiv 11 \pmod{21}$

$8^5 \equiv 8 \pmod{21}$

$12^5 = 144 \cdot 144 \cdot 12 \equiv 9 \cdot 12 \equiv 108 \equiv 3 \pmod{21}$

$(4, 20, 10, 11, 8, 3)$

E V K L ID

62) Ringiso. $f: f \mapsto g$. $\forall x, y \in \mathbb{R}$ $f(x+y) = f(x) + f(y)$

$(P(M), \Delta, \cap, (\varnothing, \mathbb{I})^M, \oplus, \otimes)$ kommutativ (ü33, 435)

$\{\varnothing, \mathbb{I}\}^M := \{f: M \rightarrow \varnothing, \mathbb{I}\}$

$\phi: \{\varnothing, \mathbb{I}\}^M \rightarrow P(M)$, $f \mapsto f^{-1}(\{\mathbb{I}\})$ ist Bijektion.

Sei nun $f, g \in \{\varnothing, \mathbb{I}\}^M$, wir zeigen $\phi(f \oplus g) = \phi(f) \cup \phi(g)$ (\star)

Operationen auf $\{\varnothing, \mathbb{I}\}^M$ Punktes. def.

Seien dazu $m \in M$, $A = f^{-1}(\{\mathbb{I}\})$, $B = g^{-1}(\{\mathbb{I}\})$ $f \oplus g: M \rightarrow \{\varnothing, \mathbb{I}\}$
 $\rightarrow \mathbb{I} \text{ falls } f(m) = g(m)$

$f \oplus g: M \rightarrow \{\varnothing, \mathbb{I}\}$
 $\rightarrow \mathbb{I} \text{ falls } f(m) \neq g(m)$

$(f \oplus g)(m) = \mathbb{I} \Leftrightarrow f(m) \neq g(m)$

Damit ist $m \in (f \oplus g)^{-1}(\{\mathbb{I}\}) \Leftrightarrow f(m) \neq g(m)$

$\Leftrightarrow m \in f^{-1}(\mathbb{I}) \cup g^{-1}(\mathbb{I})$

$\Leftrightarrow m \in f^{-1}(\mathbb{I}) \cap g^{-1}(\mathbb{I})$

$\Leftrightarrow m \in A \Delta B$

$\Rightarrow (\star)$

$\Rightarrow (\star)$

\emptyset ist gewünscht. Ring iso.

63) i) 2_8 ii) $2_4 \times 2_2$ iii) $2_2 \times 2_2 \times 2_2$

$\langle g \rangle = \{n \cdot g \mid n \in \mathbb{Z}\}, g \in G$: von g erzeugt VG. zyklisch

i) $\langle 1 \rangle = 2_8 = \langle 3 \rangle = \langle 7 \rangle = \langle 5 \rangle$

$\langle 3 \rangle = \langle 5 \rangle$

$\langle 7 \rangle = \langle 1, 2, 4, 6 \rangle = \langle 6 \rangle$

$\langle 5 \rangle = \langle 1, 4 \rangle$

ii) $\langle (0, 0) \rangle = \{(0, 0)\}$

$\langle (0, 1) \rangle = \{(0, 1), (2, 0)\}$

$\langle (1, 0) \rangle = \{(1, 0), (1, 1), (3, 0)\}$

$\langle (1, 1) \rangle = \{(1, 0), (1, 1), (2, 1), (3, 1)\} = \langle (3, 1) \rangle$

iii) $\langle (0, 0, 0) \rangle = \{(0, 0, 0)\}$

$\langle (0, 0, 1) \rangle = \{(0, 0, 1), (2, 0, 0)\}$

$\langle (0, 1, 0) \rangle = \{(0, 0, 0), (0, 1, 0)\}$

$\langle (1, 0, 0) \rangle = \{(0, 0, 0), (1, 0, 0)\}$

$\langle (1, 0, 1) \rangle = \{(0, 0, 0), (1, 0, 1)\}$

$\langle (0, 1, 1) \rangle = \{(0, 0, 0), (0, 1, 1)\}$

$\langle (1, 1, 0) \rangle = \{(0, 0, 0), (1, 1, 0)\}$

$\langle (1, 1, 1) \rangle = \{(0, 0, 0), (1, 1, 1)\}$

nicht isomorph, da zykl. UG verschieden (z.B. \mathbb{Z}_8 UG der Ordnung 8 und die anderen nicht).

Ü63. Zeigen Sie, dass die Gruppen

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

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 $[n] = \{1, 2, \dots, n\}$. 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 $(\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ)$ aus Aufgabe H18 isomorph zu \mathfrak{S}_3 ist.

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

H66. Seien (G, \circ_G) und (H, \circ_H) zwei Gruppen und $f: G \rightarrow H$ 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 $\{(x, y) \in G \times H \mid f(x) = y\}$ ist eine Untergruppe von $(G \times H, \circ_{G \times H})$.