ETH Zürich, D-INFK
HS 2016, 18. Januar 2017

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Lösung 9

9.1 Gruppenhomomorphismen

Sei $g \in G$ beliebig, wir zeigen direkt:

$$\psi(e_G) \overset{\text{G2}}{=} \psi(e_G) \circ e_H \overset{\text{G3}}{=} \psi(e_G) \circ \big(\psi(g) \circ \widehat{\psi(g)}\big) \overset{\text{G1}}{=} \big(\psi(e_G) \circ \psi(g)\big) \circ \widehat{\psi(g)}$$
$$\overset{\psi \text{ G.H.}}{=} \psi(e_G * g) \circ \widehat{\psi(g)} \overset{\text{G2}}{=} \psi(g) \circ \widehat{\psi(g)} \overset{\text{G3}}{=} e_H$$

9.2 Ordnung und Untergruppen

a) Durch Ausprobieren findet wir:

Element	0	1	2	3	4	5
Ordnung	1	6	3	2	3	6

b) Wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$, dann ist $H_1 \cup H_2 = H_1$ oder $H_1 \cup H_2 = H_2$ und somit eine Untergruppe von G. Zu zeigen bleibt daher die Umkehrung. Nehmen wir an, dass die Ummkehrung nicht gilt, d.h. es gibt ein $a \in H_1 \backslash H_2$ und ein $b \in H_2 \backslash H_1$. Da nach Annahme $H_1 \cup H_2$ eine Gruppe bezüglich der Gruppenoperation $\star$ bildet, gilt wegen Abgeschlossenheit: $c = a \star b \in H_1 \cup H_2$. Das Element c kann aber nicht in H_1 liegen, da sonst $b = \widehat{a} \star c \in H_1$ wäre. Analog dazu ist $c \notin H_2$, da sonst $a = c \star \widehat{b} \in H_2$ wäre. Somit ist $c \notin H_1 \cup H_2$ und daher $H_1 \cup H_2$ nicht abgeschlossen.

9.3 Die Gruppe $\mathbb{Z}_m^*$

a) Die Ordnung der Gruppe $\langle \mathbb{Z}_{36}^*; \odot \rangle$ ist $\varphi(36)$. Mit Lemma 5.12 folgt $\varphi(36) = (2-1) \cdot 2^{2-1} \cdot (3-1) \cdot 3^{2-1} = 2 \cdot 2 \cdot 3 = 12$.

Die Gruppe besteht aus allen Zahlen in $\mathbb{Z}_{36}$, die teilerfremd zu 36 sind. Somit gilt $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

b) Aus dem Satz von Lagrange folgt, dass für ein $a \in \mathbb{Z}_{11}^*$ gilt $\operatorname{ord}(a) \in \{1, 2, 5, 10\}$. Falls a ein Generator von $\mathbb{Z}_{11}^*$ ist, hat a die Ordnung $10 = \varphi(11)$. Dies ist genau dann der Fall, wenn $a^2 \neq 1$ und $a^5 \neq 1$ gilt. Durch Ausprobieren finden wir, dass 2 ein Generator ist. Die restlichen Generatoren kann man analog finden. Alternativ verwendet man folgendes Lemma.

Lemma 1. Sei g ein Generator von $\mathbb{Z}_m^*$, dann ist die Menge der Generatoren von $\mathbb{Z}_m^*$ genau

$$A = \{g^i \mid 1 \leq i < \varphi(m) \ \wedge \ \mathsf{gcd}(i, \varphi(m)) = 1\}$$

Beweis: Sei h ein Generator von $\mathbb{Z}_m^*$. Da g ein Generator ist, gibt es ein $1 \leq i < \varphi(m)$ mit $h = g^i$. Sei $d = \text{ggT}(i, \varphi(m))$, dann gilt $h^{\frac{\varphi(m)}{d}} = (g^i)^{\frac{\varphi(m)}{d}} = g^{\varphi(m)\frac{i}{d}} = 1$. Da aber h ein Generator ist, muss $d = 1$ sein. Somit ist jeder Generator in A. Sei umgekehrt $h \in A$, dann gibt es ein $1 \leq i < \varphi(m)$ mit $h = g^i$ und $\text{ggT}(i, \varphi(m)) = 1$. Es gilt $1 = h^{\text{ord}(h)} = g^{i \cdot \text{ord}(h)}$. Da g ein Generator ist, muss $i \cdot \text{ord}(h)$ ein Vielfaches von $\varphi(m)$ sein. Da $\text{ggT}(i, \varphi(m)) = 1$, muss also auch $\text{ord}(h)$ ein Vielfaches von $\varphi(m)$ sein. Somit ist h auch ein Generator.

Nach dem Lemma sind daher genau $2, 6, 7, 8$ Generatoren von $\mathbb{Z}_{11}^*$.

c) Das Ziel ist einen Isomorphismus $\varphi : \mathbb{Z}_{15}^* \to \mathbb{Z}_{20}^*$ zu konstruieren. Wir beginnen mit folgendem Lemma.

Lemma 1. Seien n und m teilerfremde Zahlen. Die Abbildung $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ mit $f(x) = (R_n(x), R_m(x))$ ist eine Bijektion.

Beweis: Gemäss Lemma 4.17 gilt für $x \in \mathbb{Z}_{nm}$, dass $x \equiv_n R_n(x)$ und $x \equiv_m R_m(x)$. Aus Theorem 4.20 (Chinesischer Restsatz) folgt, dass es für $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$ genau ein $x \in \mathbb{Z}_{nm}$ gibt mit $x \equiv_n a$ und $x \equiv_m b$. Also ist f eine Bijektion.

Weiter gilt folgendes Lemma

Lemma 2. Seien n und m ganze Zahlen. Für $a \in \mathbb{Z}$ gilt

$$\text{ggT}(a, nm) = 1 \implies \text{ggT}(a, n) = 1 \wedge \text{ggT}(a, m) = 1$$

Beweis: Seien $\text{ggT}(a, n) = d$, $\text{ggT}(a, m) = e$, dann gilt $d \mid n$ und $e \mid m$. Damit aber auch $d \mid nm$ und $e \mid nm$. In anderen Worten sind e und d gemeinsame Teiler von a und nm. Da aber $\text{ggT}(a, nm) = 1$, gilt also $d = e = 1$.

Damit können wir zeigen, dass es für teilerfremde n, m einen Isomorphismus zwischen $\mathbb{Z}_{nm}^*$ und $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ gibt.

Lemma 3. Seien n und m teilerfremde Zahlen. Die Abbildung $f : \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ mit $f(x) = (R_n(x), R_m(x))$ ist ein Isomorphismus.

Beweis: Wir zeigen zuerst, dass f wohldefiniert ist, d.h. dass $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ für alle $x \in \mathbb{Z}_{nm}^*$ gilt. Sei $x \in \mathbb{Z}_{nm}^*$, dann ist $\text{ggT}(x, nm) = 1$. Mit **Lemma 2.** folgt $\text{ggT}(x, n) = 1$ und $\text{ggT}(x, m) = 1$. Nach Lemma 4.2 gilt somit $\text{ggT}(R_n(x), n) = 1$ und $\text{ggT}(R_m(x), m) = 1$. Daraus folgt $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$.

Nun zeigen wir, dass f bijektiv ist. Nach Lemma **Lemma 1.**, ist f injektiv und damit $|f(\mathbb{Z}_{nm}^*)| = |\mathbb{Z}_{nm}^*|$. Aus der Wohldefiniertheit folgt $f(\mathbb{Z}_{nm}^*) \subseteq \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Da nach Lemma 5.12 $|\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^* \times \mathbb{Z}_m^*|$, folgt $f(\mathbb{Z}_{nm}^*) = \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Also ist f auch surjektiv.

Es verbleibt zu zeigen, dass f ein Homomorphismus ist. Seien $a, b \in \mathbb{Z}_{nm}^*$, dann gilt mit Lemma 4.18

$$f(a \odot b) = (R_n(a \odot b), R_m(a \odot b)) \overset{Lem\ 4.18}{=} \big(R_n(R_n(a)R_n(b)), R_m(R_m(a)R_m(b))\big) = f(a) \odot f(b).$$

Aus **Lemma 3.** folgt $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_5^*$ und $\mathbb{Z}_{20}^* \simeq \mathbb{Z}_4^* \times \mathbb{Z}_5^*$. Insbesondere gibt es einen Isomorphismus $\alpha : \mathbb{Z}_{15}^* \to \mathbb{Z}_3^* \times \mathbb{Z}_5^*$ mit $\alpha(a) = (R_3(a), R_5(a))$ und einen Isomorphismus ist $\gamma : \mathbb{Z}_4^* \times \mathbb{Z}_5^* \to \mathbb{Z}_{20}^*$ mit $\gamma^{-1}(b) = (R_4(b), R_5(b))$. Wir müssen also noch einen Isomorphismus zwischen $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$ und $\mathbb{Z}_4^* \times \mathbb{Z}_5^*$ finden.

Lemma 4. Die Abbildung $g : \mathbb{Z}_3^* \to \mathbb{Z}_4^*$ mit $g(1) = 1$ und $g(2) = 3$ ist ein Isomorphismus.

Beweis: Beide Gruppen haben Ordnung 2. Wir bemerken, dass die Abbildung g daher bijektiv ist. Es gilt $g(1 \odot 1) = 1 = g(1) \odot g(1)$, $g(2 \odot 1) = 3 = g(2) \odot g(1)$, $g(1 \odot 2) = 3 = g(1) \odot g(2)$ und $g(2 \odot 2) = 1 = g(2) \odot g(2)$. Die Abbildung ist also auch ein Homomorphismus.

Mit **Lemma 4.** folgt, dass $\beta : \mathbb{Z}_3^* \times \mathbb{Z}_5^* \to \mathbb{Z}_4^* \times \mathbb{Z}_5^*$ mit $\beta\big((a,b)\big) = \big(g(a), b\big)$ ein Isomorphismus ist. Es gilt also $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_5^* \simeq \mathbb{Z}_4^* \times \mathbb{Z}_5^* \simeq \mathbb{Z}_{20}^*$.

Wir können den Isomorphismus $\varphi : \mathbb{Z}_{15}^* \to \mathbb{Z}_{20}^*$ als die Komposition der Isomorphismen α, β, γ schreiben, d.h. $\varphi = \gamma \circ \beta \circ \alpha$. Es gilt zum Beispiel $\varphi(11) = \gamma(\beta(\alpha(11))) = \gamma(\beta((2,1))) = \gamma((3,1)) = 11$.

Alternativ kann man auch einen Isomorphismus ψ durch Ausprobieren finden. Dann muss man aber (mühsam) zeigen, dass ϕ tatsächlich ein Isomorphismus ist.

9.4 Diffie-Hellman Revisited

a) Sei $g \in \langle \mathbb{Z}_n; \oplus \rangle$ der Erzeuger, den Alice und Bob als Basis verwenden. Für von Alice beziehungsweise Bob zufällig gewählte $x_A, x_B \in \{0, \ldots, n-1\}$ werden $R_n(g \cdot x_A)$ beziehungsweise $R_n(g \cdot x_B)$ gesendet. Der gemeinsame Schlüssel, den beide am Ende berechnen, ist $k_{AB} = R_n(g \cdot x_A \cdot x_B)$.

Nach Beispiel 5.26 gilt dann $\mathrm{ggT}(g, n) = 1$. Daher kann Eve nach Abschnitt 4.5.3 mit dem erweiterten euklidischen Algorithmus effizient ein $a \in \mathbb{Z}_n$ berechnen, so dass $R_n(a \cdot g) = 1$. Damit kann sie dann aus $R_n(g \cdot x_A)$ und $R_n(g \cdot x_B)$ unter Verwendung von Lemma 4.18 wie folgt auch k_{AB} berechnen:

$$\begin{aligned} k_{AB} &= R_n(g \cdot x_A \cdot x_B) = R_n(g \cdot x_A \cdot (ag) \cdot x_B) = R_n(R_n(g \cdot x_A) \cdot R_n(a \cdot g \cdot x_B)) \\ &= R_n(R_n(g \cdot x_A) \cdot R_n(R_n(a) \cdot R_n(g \cdot x_B))) \end{aligned}$$

b) Nein, Bobs Folgerung ist nicht richtig. Auch wenn zwei Gruppen die gleiche Struktur haben, lässt sich eine bestimmte Operation in einer Gruppe möglicherweise effizienter berechnen als in der anderen.

Es ist auch nicht unbedingt möglich, zuerst den Isomorphismus anzuwenden, dann das Problem in der Gruppe $\langle \mathbb{Z}_n; \oplus \rangle$ zu lösen und danach das Inverse des Isomomorphismus anzuwenden, um eine Lösung für das ursprüngliche Problem zu erhalten. Es existiert zwar ein Isomorphismus zwischen diesen Gruppen und das beschriebene Vorgehen liefert eine korrekte Lösung, jedoch ist nicht klar, ob man diesen Isomorphismus und dessen Inverses effizient berechnen kann. Betrachte zum Beispiel eine Gruppe $G = \langle g \rangle$ von Ordnung n. Ein Isomorphismus von G nach $\langle \mathbb{Z}_n; \oplus \rangle$ ist $\phi : G \to \mathbb{Z}_n, g^i \mapsto i$. Die Berechnung von ϕ entspricht also gerade dem Lösen des diskreten Logarithmus-Problems.

9.5 RSA-Attacke

Sind n_1, n_2 und n_3 nicht paarweise teilerfremd, kann der Angreifer durch Berechnen der grössten gemeinsamen Teiler einen nichttrivialen Faktor eines der n_i finden. Dann kann er also dieses n_i faktorisieren und analog zur Schlüsselerzeugung den zugehörigen privaten Schlüssel berechnen und damit c_i entschlüsseln.

Nehmen wir nun an, n_1, n_2 und n_3 sind paarweise teilerfremd. Mit dem chinesischen Restsatz kann der Angreifer dann folgendes System von Kongruenzen modulo $N := n_1 \cdot n_2 \cdot n_3$

effizient lösen:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \\ x &\equiv c_3 \pmod{n_3} \end{aligned}$$

Da $c_i \equiv m^3 \pmod{n_i}$ gilt, erfüllt m^3 diese Kongruenzen. Weil $m < n_i$ für $i \in \{1, 2, 3\}$, ist $m^3 < n_1 \cdot n_2 \cdot n_3 = N$. Nach dem chinesischen Restsatz gibt es genau eine Lösung x dieser Kongruenzen mit $0 \leq x < N$. Daher führt die Berechnung gemäss des chinesischen Restsatzes zu $x = m^3$. Um m zu erhalten, muss also nur die Kubikwurzel von x in $\mathbb{Z}$ berechnet werden, was effizient möglich ist.

Hinweis: Diese Attacke ist natürlich auch für $e > 3$ möglich, jedoch ist es für sehr grosse e unwahrscheinlich, dass ein Angreifer e verschiedene Chiffrate der gleichen Nachricht erhält.

9.6 Elementare Eigenschaften von Ringen

a) Es gilt

$$(-a)b + ab \overset{\text{Distrib.}}{=} (-a + a)b \overset{\text{Def. Inverse}}{=} 0b \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

(1 Punkt)

Das heisst, $(-a)b$ ist bezüglich $+$ ein Inverses von ab. Per Definition ist $-(ab)$ bezüglich $+$ ein Inverses von ab. Nach Lemma 5.2 gilt also $(-a)b = -(ab)$. *(1 Punkt)*

b) Per Definition ist ab ein Inverses von $-ab$, d.h. $-(-ab) = ab$. *(1 Punkt)*

Wir bemerken, dass analog zu a) auch $a(-b) = -(ab)$ gilt, da

$$a(-b) + ab \overset{\text{Distrib.}}{=} a(-b + b) \overset{\text{Def. Inverse}}{=} a0 \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

(1 Punkt)

Damit folgt

$$(-a)(-b) \overset{\text{a)}}{=} -(a(-b)) \overset{\text{a) Bem.}}{=} -(-ab) \overset{\text{Def. Inverse}}{=} ab.$$

(1 Punkt)

Man kann die Aussage auch ohne die Bemerkung $a(-b) = -(ab)$ beweisen, da

$$(-a)(-b) + (-ab) \overset{\text{a)}}{=} (-a)(-b) + (-a)b \overset{\text{Distrib.}}{=} (-a)(-b + b) \overset{\text{Def. Inverse}}{=} (-a)0 \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

c) Wir zeigen die Implikation indirekt, d.h. wir zeigen: Gilt $1 = 0$, so enthält R nur ein Element. Wir nehmen also an, es gilt $1 = 0$. Sei nun $a \in R$. Dann gilt

$$a = a \cdot 1 = a \cdot 0 \overset{\text{Lemma 5.17 (i)}}{=} 0.$$

Es gilt also $a = 0$ für alle $a \in R$, d.h $R = \{0\}$. *(2 Punkte)*