Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 9

1. a) Geben Sie alle Untergruppen der folgenden Gruppen an:
   i – S_3
   ii – $(\mathbb{Z}_8, +)$

   b) Finden Sie, falls möglich, zu den beiden Gruppen je zwei Untergruppen, deren Vereinigung keine Untergruppe ist.

2. Zeigen Sie, dass φ mit

$$\varphi : (\mathbb{Z}, +) \to (m\mathbb{Z}, +), \varphi(x) = mx$$

   für $m \in \mathbb{N} \setminus \{0\}$ ein Isomorphismus ist.

3. Zeigen Sie, dass jede Untergruppe einer unendlichen zyklischen Gruppe selbst zyklisch ist.

4. Es seien K und L zwei Untergruppen einer endlichen Gruppe $(G, \circ)$. Beweisen oder widerlegen Sie:

   a) $|K| \cdot |L| = |K \cap L| \cdot |KL|$.

   b) KL ist genau dann eine Untergruppe von G, falls $KL = LK$.

Lösung zu Übung 9

1. a) i – Seien wieder $e = \text{id}$, $d = (1, 2, 3)$, $d_2 = (1, 3, 2)$, $s_1 = (2, 3)$, $s_2 = (1, 3)$ und $s_3 = (1, 2)$. Idee: d und d_2 sind zueinander invers. Ebenso sind alle s_i $(i = 1, \ldots, 3)$ zu sich selbst invers. Die Untergruppen von S_3 sind also: $\{e\}$, S_3 selbst, $\{e, d, d_2\}$, $\{e, s_1\}$, $\{e, s_2\}$ und $\{e, s_3\}$.

ii – Die Untergruppen von $(\mathbb{Z}_8, +_8)$ sind: $(\mathbb{Z}_8, +_8)$ selbst, $(\{0,2,4,6\}, +_8)$, $(\{0,4\}, +_8)$ und $(\{0\}, +_8)$. Diese Gruppen sind isomorph zu den Teilern von 8, also $(\mathbb{Z}_8, +_8)$, $(\mathbb{Z}_4, +_4)$, $(\mathbb{Z}_2, +_2)$ und $(\mathbb{Z}_1, +_1)$.

b) Es gilt $\{0\} \subseteq \{0,4\} \subseteq \{0,2,4,6\} \subseteq \{0,\ldots,7\}$, also lassen sich keine zwei Untergruppen von $(\mathbb{Z}_8, +_8)$ finden, die vereinigt keine Gruppe sind. Hingegen ist $M = \{e, s_1\} \cup \{e, s_2\}$ keine Gruppe, da $s_2 \circ s_1 = d \notin M$ (Achtung: $(f \circ g)(x) = g(f(x))$).

2. φ ist injektiv, denn $\varphi(x) = \varphi(y) \Rightarrow mx = my \Rightarrow x = y$. Außerdem ist φ surjektiv, denn: Sei $b \in m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, dann gibt es ein $a \in \mathbb{Z}$ mit $b = ma$ und somit $\varphi(a) = ma$. φ ist ein Homomorphismus, denn $\varphi(a+b) = m(a+b) = ma + mb = \varphi(a) + \varphi(b)$.

3. Sei G eine zyklische Gruppe, d.h. es gibt ein $a \in G$ mit $G = \{a^z \mid z \in \mathbb{Z}\}$. Sei U eine Untergruppe von G. Wenn $U = \{e\}$, so ist U trivialerweise zyklisch. Sei nun $U \neq \{e\}$ und sei

$$m = \min\{k > 0 \mid a^k \in U\}.$$

Dieses m existiert, da U nun neben dem neutralen Element mindestens ein weiteres besitzen muss, und für jedes $a^k \in U$ muss auch $a^{-k} \in U$ gelten, da $(a^k)^{-1} = a^{-k}$.
Sei nun $a^n \in U$. Es gibt $q, r \in \mathbb{Z}$ mit $0 \leq r < m$ und $n = q \cdot m + r$, also auch

$$a^n = a^{m \cdot q + r} = (a^m)^q a^r.$$

Durch Umstellen erhalten wir

$$a^r = a^n((a^m)^q)^{-1} = a^n(a^m)^{-q}.$$

Da $a^m \in U$, ist auch $(a^m)^{-q} \in U$. Da zusätzlich $a^n \in U$, folgt auch ingesamt $a^r \in U$. Wegen Definition von m und weil $r < m$, muss also $r = 0$ gelten (denn sonst wäre m falsch gewählt und r die kleinste positive Zahl mit $a^r \in U$). Somit gilt, dass $a^n = (a^m)^q$. Da $a^n \in U$ beliebig gewählt war, folgt, dass U von a^m erzeugt wird.

4. a) Die Aussage ist korrekt, denn: Sei f eine Funktion mit

$$f : K \times L \to KL$$
$$f(x,y) = xy$$

Beachte, dass f surjektiv ist. Idee: Wenn wir zeigen können, dass es für alle $z \in KL$ unter f genau $|K \cap L|$ Urbilder gibt, also $|f^{-1}(z)| = |K \cap L|$, dann folgt zusammen mit der Surjektivität von f, dass $|K \times L| = |K \cap L| \cdot |KL|$. Mit $|K \times L| = |K| \cdot |L|$ folgt die gewünschte Aussage.
Sei $z \in KL$, also $z = xy$ mit $x \in K$ und $y \in L$. Wir zeigen zwei Richtungen:

$|f^{-1}(xy)| \geq |K \cap L|$: Sei $a \in K \cap L$. Dann gilt $xy = xaa^{-1}y$ mit $xa \in K$ und $a^{-1}y \in L$. Außerdem gilt $(xa, a^{-1}y) \in K \times L$, weshalb $f(xa, a^{-1}y) = xy$. Aus $b \neq a \in K \cap L$ folgt außerdem $(xb, b^{-1}y) \neq (xa, a^{-1}y)$ wegen $xa \neq xb$. Insgesamt gibt es also mindestens $|K \cap L|$ Urbilder von xy.

$|f^{-1}(xy)| \leq |K \cap L|$: Sei $(u, v) \in K \times L$ ein beliebiges Urbild von xy, also $f(u, v) = xy$. Wir müssen nun zeigen, dass es ein $a \in K \cap L$ gibt mit $(u, v) = (xa, a^{-1}y)$. Wähle $a = x^{-1}u \in K$ (denn $x^{-1}, u \in K$), woraus $u = xa$ folgt. Nach Definition von f gilt, dass $uv = xy$. Durch Einsetzen von u erhalten wir $xav = xy$. Dies lässt sich umformen zu $av = y$, woraus auch $a \in L$ folgt (denn $v, y \in L$). Schließlich erhalten wir $v = a^{-1}y$.

b) Die Aussage ist korrekt, denn: Sei G eine endliche Gruppe und seien K und L Untergruppen von G. Wir zeigen wieder zwei Richtungen:

$\Rightarrow$: Sei KL Untergruppe von G. Zu zeigen ist nun, dass $KL = LK$. Wir unterteilen dies erneut in zwei Richtungen:

$KL \subseteq LK$: Sei $x \in KL$. Da KL Untergruppe von G ist, ist auch $x^{-1} \in KL$. Somit gibt es $k \in K$ und $\ell \in L$ mit $x^{-1} = k\ell$. Daraus folgt

$$x = \left(x^{-1}\right)^{-1} = (k\ell)^{-1} = \ell^{-1}k^{-1} \in LK.$$

$LK \subseteq KL$: Sei $x \in LK$, also gibt es $\ell \in L$ und $k \in K$ mit $x = \ell k$. Betrachte

$$x^{-1} = (\ell k)^{-1} = k^{-1}\ell^{-1} \in KL.$$

Da KL Untergruppe von G ist, gilt auch

$$\left(k^{-1}\ell^{-1}\right)^{-1} = \left(x^{-1}\right)^{-1} = x \in KL.$$

$\Leftarrow$: Gelte $KL = LK$. Da G endlich ist, genügt es zu zeigen, dass KL abgeschlossen ist. Seien $x, x' \in KL$. Somit gilt auch, dass

$xx' \in KLKL$. Da $KL = LK$, folgt auch, dass $xx' \in KLLK$. Da L Untergruppe von G ist, gilt $xx' \in KLK$. Da $LK = KL$, folgt $xx' \in KKL$. Da K Untergruppe von G ist, folgt schließlich auch $xx' \in KL$.