Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 10

1. Sei $(G, \circ)$ eine Gruppe und U eine Untergruppe von G. Zeigen Sie, dass U genau dann ein Normalteiler ist, wenn für alle $a \in G$ die Gleichung $a \circ U = U \circ a$ gilt, also wenn Links- und Rechtsnebenklassen von U übereinstimmen.

2. Zeigen Sie, dass für alle $n \in \mathbb{N}\backslash\{0\}$ die Gruppe $(\mathbb{Z}, +)/n\mathbb{Z}$ isomorph ist zu $(\mathbb{Z}_n, +_n)$.

3. Beweisen Sie, dass für jeden Homomorphismus zwischen zwei endlichen Gruppen $\varphi : G_1 \to G_2$ gilt: $|G_1| = |\ker(\varphi)| \cdot |\mathrm{im}(\varphi)|$.

4. Gegeben sei die Gruppe $G = (\mathbb{Z}, +)$, deren Untergruppe $U = 4\mathbb{Z}$ und die Abbildung $\varphi : G/U \to (\mathbb{Z}_2, +_2)$ mit $\varphi(a + 4\mathbb{Z}) = a \mod 2$ für $a \in \mathbb{Z}$. Zeigen Sie, dass φ

   a) eine Funktion ist.

   b) ein Homomorphismus ist.

   c) kein Isomorphismus ist.

5. Geben Sie die Primfaktorzerlegung der folgenden Zahlen an:

   a) 1024

   b) 3072

   c) 15360

   d) 30030

6. Sei kgV(a, b) das kleinste gemeinsame Vielfache der Zahlen $a, b \in \mathbb{Z}$:

$$\text{kgV}(a, b) := \min\{n > 0 \mid a|n \wedge b|n\}.$$

Beweisen Sie, dass für alle $a, b \in \mathbb{Z}$ gilt

$$a \cdot b = \text{ggT}(a, b) \cdot \text{kgV}(a, b).$$

Lösung zu Übung 10

1. Sei $aU = Ua$. Daraus folgt auch $U = a^{-1}Ua$ und somit $U \supseteq a^{-1}Ua$, was der Definition von Normalteiler aus der Vorlesung entspricht, nämlich für alle $u \in U$ gilt $a^{-1}ua \in U$. Gelte nun umgekehrt, dass wenn $u \in U$, so auch $a^{-1}ua \in U$. Da die Aussage für alle $a \in G$ gilt und a das inverse Element von a^{-1} ist, muss auch $a^{-1^{-1}}ua^{-1} = aua^{-1} \in U$ gelten. Zusammen erhalten wir $U \supseteq a^{-1}Ua$ und $U \supseteq aUa^{-1}$, bzw. $aU \supseteq Ua$ und $Ua \supseteq aU$, also auch $aU = Ua$.

2. $(\mathbb{Z}, +)/n\mathbb{Z}$ ist die Menge aller Linksnebenklassen von $n\mathbb{Z}$, d.h.

$$(\mathbb{Z}, +)/n\mathbb{Z} = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\}$$

Beispiel für $n = 2$:

$$(\mathbb{Z}, +)/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}, -1 + 2\mathbb{Z}, 2 + \mathbb{Z}, -2 + \mathbb{Z}, \ldots\}$$

Wir sehen, dass z.B. $0+2\mathbb{Z} = -2+2\mathbb{Z} = 2+2\mathbb{Z}$ und $-1+2\mathbb{Z} = 1+2\mathbb{Z}$, usw. Sei nun φ definiert als:

$$\varphi : (\mathbb{Z}_n, +_n) \to (\mathbb{Z}, +)/n\mathbb{Z}$$
$$\varphi(i) = i + n\mathbb{Z}$$

Wir müssen nun zeigen, dass φ ein Isomorphismus ist:

Homomorphismus:

$$\begin{aligned}
\varphi(i +_n j) &= \varphi((i + j) \bmod n) \\
&= (i + j) \bmod n + n\mathbb{Z} \\
&= (i + j) + n\mathbb{Z} \\
&= (i + n\mathbb{Z}) + (j + n\mathbb{Z}) \\
&= \varphi(i) + \varphi(j)
\end{aligned}$$

Injektiv: Für alle $i, j \in \mathbb{Z}_n$ gilt

$$\varphi(i) = \varphi(j) \Rightarrow i + n\mathbb{Z} = j + n\mathbb{Z} \Rightarrow i = j.$$

Surjektiv: Sei $x \in (\mathbb{Z}, +)/n\mathbb{Z}$, also gibt es ein i, $0 \leq i < n$, mit $x = i + n\mathbb{Z}$. Somit gilt auch $i \in (\mathbb{Z}_n, +_n)$ und $\varphi(i) = x$.

3. $\ker(\varphi)$ ist eine Untergruppe von G_1. Zusätzlich ist $\ker(\varphi)$ ein Normalteiler von G_1, also ist $|G_1/\ker(\varphi)|$ die Anzahl der Linksnebenklassen von $\ker(\varphi)$. Da G_1 außerdem endlich ist, lässt sich der Satz von Lagrange anwenden:

$$\frac{|G_1|}{|\ker(\varphi)|} = |G_1/\ker(\varphi)| \Rightarrow |G_1| = |\ker(\varphi)| \cdot |G_1/\ker(\varphi)|.$$

Der Isomorphiesatz der Gruppentheorie besagt, dass $G_1/\ker(\varphi)$ isomorph zu $\mathrm{im}(\varphi)$ ist, woraus auch $|G_1/\ker(\varphi)| = |\mathrm{im}(\varphi)|$ folgt. Insgesamt haben wir also

$$|G_1| = |\ker(\varphi)| \cdot |\mathrm{im}(\varphi)|.$$

4. a) φ ist eine Funktion, denn für alle $a + 4\mathbb{Z}, b + 4\mathbb{Z} \in (\mathbb{Z}, +)/4\mathbb{Z}$ gilt: Wenn $a + 4\mathbb{Z} = b + 4\mathbb{Z}$, dann gibt es ein $c \in \mathbb{Z}$ mit $a = 4c+b$. Daraus folgt, dass $a \bmod 2 = b \bmod 2$, denn $4c+b \bmod 2 = b \bmod 2$, und somit

$$\varphi(a + 4\mathbb{Z}) = a \bmod 2 = b \bmod 2 = \varphi(b + 4\mathbb{Z}).$$

b)

$$\begin{aligned}\varphi((a + 4\mathbb{Z}) + (b + 4\mathbb{Z})) &= \varphi((a + b) + 4\mathbb{Z}) \\ &= (a + b) \bmod 2 \\ &= a \bmod 2 +_2 b \bmod 2 \\ &= \varphi(a + 4\mathbb{Z}) +_2 \varphi(b + 4\mathbb{Z})\end{aligned}$$

c) φ ist nicht injektiv, denn $0 + 4\mathbb{Z} \neq 2 + 4\mathbb{Z}$, aber $\varphi(0 + 4\mathbb{Z}) = \varphi(2 + 4\mathbb{Z}) = 0$.

5. a) $1024 = 2^{10}$

   b) $3072 = 2^{10} \cdot 3$

   c) $15360 = 2^{10} \cdot 3 \cdot 5$

   d) $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

6. Sei $d = \mathrm{ggT}(a, b)$, d.h. $d|a$ und $d|b$, also auch $d|ab$. Es gibt somit ein $\ell \in \mathbb{Z}$ mit $ab = ld$. Behauptung: $\ell = \mathrm{kgV}(a, b)$.
   Zunächst zeigen wir, dass ℓ überhaupt Vielfaches von a und von b ist: Da $d|a$, gibt es ein $a' \in \mathbb{Z}$ mit $a'd = a$, also $a'db = \ell d$, und somit $a'b = \ell$, d.h. $b|\ell$ (analog gilt auch $a|\ell$).
   Sei nun $m \in \mathbb{Z}$ ein weiteres Vielfaches von a und von b. Wir zeigen nun, dass $\ell|m$ (also auch $\ell \leq m$). Zunächst haben wir $j, k \in \mathbb{Z}$ mit $aj = bk = m$. Der Algorithmus von Euklid liefert $x, y \in \mathbb{Z}$ mit $d = ax + by$. Betrachte nun

$$\begin{aligned} md &= m(ax + by) \\ &= max + mby \\ &= bkax + ajby \\ &= ab(kx + jy) \\ &= d\ell(kx + jy) \end{aligned}$$

   Somit gilt, dass $m = \ell(kx + jy)$, also $\ell|m$.