Mathematik für Informatiker II

Christoph Eisinger
Sommersemester 2011

Musterlösungen zum Hausübungsblatt 3

Aufgabe 1 (4+4=8 Punkte)

(a) 1. Abgeschlossenheit: für $g, h \in G$ gilt $gh \in G$ und damit $ghU \in G/U$.

2. Assoziativität: $((aU)(bU))(cU) = (abU)(cU) = ((ab)c)U = (a(bc))U = (aU)(bcU) = (aU)((bU)(cU))$.

3. Das neutrale Element ist $U = eU$, denn für alle $gU \in G/U$ gelten $(gU)(eU) = (geU) = gU$ und $(eU)(gU) = (egU) = gU$.

4. Es ist $(gU)^{-1} = g^{-1}U$, denn $(gU)(g^{-1}U) = gg^{-1}U = eU = U$ und $(g^{-1}U)(gU) = g^{-1}gU = eU = U$.

(b) Da $(12)^2 = id$, ist $U = \{id, (12)\}$. Wähle z.B. $g_1 = id, g_2 = (12), h_1 = h_2 = (13)$. Da $g_1, g_2 \in U$, gilt $g_1U = g_2U = U$, und offensichtlich ist auch $h_1U = h_2U$. Weiterhin ist $g_1h_1 = (13)$ und $g_2h_2 = (132)$ und damit $g_1h_1U = (13)U = \{(13), (123)\}$ und $g_2h_2U = (132)U = \{(132), (23)\}$, also $g_1h_1U \neq g_2h_2U$.

Aufgabe 2 (2+4+2+4+6=18 Punkte)

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

(a) Nach Aufgabe 1 (a) vom Präsenzübungsblatt 2 ist $f(e_G) = e_H$, also $e_G \in K$, d.h. $K \neq \{\}$. Seien nun $a, b \in K$. Nach Aufgabe 1 (b) vom Präsenzübungsblatt 2 gilt $f(b^{-1}) = f(b)^{-1}$ und damit $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_He_H^{-1} = e_H$. Also ist $ab^{-1} \in K$.

(b) Zu zeigen ist, dass für alle $g \in G$ gilt $gK = Kg$. Wir zeigen beide Inklusionen, sei also $h \in gK$. Z.z. ist nun, dass $h \in Kg$. Da $h \in gK$, gilt $\exists k_1 \in K$ mit $h = gk_1$. Wähle $k_2 := hg^{-1} = gk_1g^{-1}$. Dann ist $f(k_2) = f(gk_1g^{-1}) = f(g)\underbrace{f(k_1)}_{=e_H}f(g)^{-1} = f(g)f(g)^{-1} = e_H$. Also gilt $k_2 \in K$ und damit $h = k_2g \in Kg$. Das zeigt $gK \subseteq Kg$. Die Inklusion $Kg \supseteq gK$ zeigt man analog, es gilt daher $gK = Kg$, K ist also ein Normalteiler von G.

(c) Nach Aufgabe 1 (a) vom Präsenzübungsblatt 2 ist $f(e_G) = e_H$, also $e_H \in \text{Im } f$, d.h. Im $f \neq \{\}$. Seien $a, b \in \text{Im } f$, es gibt also $g, h \in G$ mit $f(g) = a$ und $f(h) = b$. Dann ist $ab^{-1} = f(g)f(h)^{-1} = f(gh^{-1}) \in \text{Im } f$.

(d) Gegeben seien $g_1, g_2 \in G$ mit $g_1K = g_2K$. Zu zeigen ist, dass dann auch $f(g_1) = f(g_2)$. Sei $h \in g_1K = g_2K$ beliebig, dann gibt es $k_1, k_2 \in K$ mit $h = g_1k_1 = g_2k_2$. Daher ist $g_1 = hk_1^{-1} = g_2k_2k_1^{-1}$ und damit $f(g_1) = f(g_2k_2k_1^{-1}) = f(g_2)f(k_2)f(k_1)^{-1} = f(g_2)e_He_H^{-1} = f(g_2)$.

(e) 1. Homomorphieeigenschaft: Für $g, h \in G$ gilt $\varphi(gKhK) = \varphi(ghK) = f(gh) = f(g)f(h) = \varphi(gK)\varphi(hK)$.

2. Surjektivität: Für $f(g) \in \text{Im } f$ ist $\varphi(gK) = f(g)$.

3. Injektivität: Seien $g, h \in G$ mit $\varphi(gK) = \varphi(hK)$. Z. z. ist, dass dann $gK = hK$. Nach der Definition von φ ist $f(g) = f(h)$ und damit $f(h^{-1}g) = f(h)^{-1}f(g) = f(g)^{-1}f(g) = e_H$, weshalb $h^{-1}g \in K$. Daher ist $g = h\underbrace{h^{-1}g}_{\in K} \in hK$. Da zwei Nebenklassen entweder disjunkt oder gleich sind, und $g \in gK \cap hK$, gK und hK also nicht disjunkt sind, muss gelten $gK = hK$.

Aufgabe 3 (3+2+3=8 Punkte)

(a) Betrachte die Gruppe $U := \langle g \rangle$. Nach Bl. 2, A3 gilt $U = \{g^k | k = 0, \ldots, n_0 - 1\}$, wobei n_0 das minimale m ist mit $g^m = e$. Die Elemente g^k mit $k \in \{0, \ldots, n_0 - 1\}$ sind alle verschieden, denn wäre $g^k = g^l$ mit $k, l \in \{0, \ldots, n_0 - 1\}$, so wäre $g^{k-l} = e$. Es ist aber $k - l < n_0$ im Widerspruch zur Minimalität von n_0, d.h. dazu, dass n_0 das minimale m ist mit $g^m = e$. Daher gilt $|U| = n_0$. Nach dem Satz von Lagrange muss aber gelten, dass $n_0 = |U||G| = n$, d.h. $n = an_0$ mit $a \in \mathbb{N}$. Es ist also $g^n = (g^{n_0})^a = e^a = e$.

(b) Da $\mathbb{Z}_p$ ein Körper ist, ist $(\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}, \cdot)$ eine Gruppe, und es ist $|\mathbb{Z}_p^*| = p - 1$. Für jedes $a \in \mathbb{Z}_p^*$ gilt daher nach Teil (a), dass $a^{p-1} = 1$ (, da die 1 das neutrale Element bezüglich der Multiplikation ist), also $a^p = aa^{p-1} = a \cdot 1 = a$. Für die 0 gilt offensichtlich ebenfalls $0^p = 0$.

(c) Das Polynom $q(x) = x^p - x \in \mathbb{Z}[x] \setminus \{0\}$ hat die geforderten Eigenschaften, denn nach Teil (b) gilt für $a \in \mathbb{Z}_p$, dass $q(a) = a^p - a = a - a = 0$.