Aufgabe P26

a) Ja. Sei $f_g : G \to G, h \mapsto gh$ und $f_g^* : G \to G, h \mapsto g^{-1}h$. Dann gilt $(f_g \circ f_g^*)(h) = gg^{-1}h = h$ und $(f_g^* \circ f_g)(h) = g^{-1}gh = h$, also $f_g \circ f_g^* = f_g^* \circ f_g = \mathrm{id}$. Damit ist f_g bijektiv.

b) Nein. Betrachte $V_4 = \{1; (1\ 2)(3\ 4); (1\ 3)(2\ 4); (1\ 4)(2\ 3)\} \leqslant S_4$ mit $|V_4| = 4$, aber für alle $\sigma \in V_4$ ist $\sigma^2 = 1$, also existiert in V_4 kein Element der Ordnung 4.

c) Ja. Nach Definition ist $\operatorname{ord} g = |\langle g \rangle|$. Nach dem Satz von Lagrange gilt $|\langle g \rangle| \,\big|\, |G| = m$.

d) Ja. Nach Lagrange haben alle Untergruppen von G eine Ordnung, die $|G| = m$ teilt. Da aber m eine Primzahl ist, gibt es nur Untergruppen der Ordnung 1 und Ordnung m. Dies sind genau zwei Untergruppen, also ist G nach Aufgabe P25 zyklisch.

e) Ja. Nach Teil c) muß gelten: $\operatorname{ord} g | 15$. Da nach Voraussetzung $\operatorname{ord} g$ nicht 1, 3 oder 5 ist, verbleibt nur noch die Möglichkeit $\operatorname{ord} g = 15$. Damit gilt aber $\langle g \rangle = G$.

f) Nein. Sei $G = \mathbb{Z}_5^*$ und $\sim$ die durch die Partition $\{\{1; 2; 3\}; \{4\}\}$ gegebene Äquivalenzrelation. Dann ist $[1]_\sim = \{1; 2; 3\}$ keine Untergruppe in G, da $2 \cdot 2 = 4 \notin [1]_\sim$ ist.

g) Ja. Satz der Vorlesung.

h) Ja. Ist $\varphi : G \to H$ Homomorphismus, so ist nach dem Homomorphiesatz durch $a \sim a' \Leftrightarrow \varphi(a) = \varphi(a')$ eine Kongruenzrelation auf G definiert, es gilt $\operatorname{Kern} \varphi = \{g \in G \mid \varphi(g) = 1 = \varphi(1)\} = [1]_\sim$ und nach Teil g) ist $[1]_\sim \trianglelefteq G$.

Aufgabe P27

a) Nein. Mit $a = 2$, $m = 4$ ist $a^{\varphi(m)} = 2^2 = 4 \equiv 0 \mod m$.

b) Ja. Es ist $101^{6n} - 1 \equiv 1^{6n} - 1 \equiv 0 \mod 10$ und wegen $1 \in \operatorname{ggT}(7; 101)$ ist $101^{6n} = (101^6)^n = (101^{\varphi(7)})^n \equiv 1^n \equiv 1 \mod 7$, also $7 | (101^{6n} - 1)$. Da 7 und 10 teilerfremd sind, folgt damit $7 \cdot 10 = 70 | (101^{6n} - 1)$.

c) Nein. $1001^{6n} - 1 = (7 \cdot 143)^{6n} - 1 \equiv -1 \mod 7$, also $7 \nmid (1001^{6n} - 1) \Rightarrow 70 \nmid (1001^{6n} - 1)$.

d) 1 und 2. Es gilt $\varphi(p_1^{v_1} \cdots p_n^{v_n}) = (p_1 - 1)p_1^{v_1 - 1} \cdots (p_n - 1)p_n^{v_n - 1}$ für paarweise verschiedene Primzahlen p_i. Dieses Produkt ist gerade, wenn mindestens ein Faktor gerade ist. Ist ein p_i ungerade, so ist $p_i - 1$ gerade, also auch das Produkt. Damit können nur noch die $\varphi(2^v)$ ungerade sein. Es gilt $\varphi(2^v) = 2^{v-1}$, was für $v > 1$ gerade ist. Es verbleiben also nur noch $\varphi(1)$ und $\varphi(2)$ zu überprüfen. Wegen $\varphi(1) = \varphi(2) = 1$ sind 1 und 2 genau die gesuchten m.

Aufgabe P28

a) Ja. $\mathbb{Z}_m$ ist nach Vorlesung eine additive Gruppe mit m Elementen

b) Nein. Sei $g \in G$ mit $\operatorname{ord} g = 5$ und $U = \langle g \rangle$. Da U zyklisch ist, gibt nach nach Vorlesung $\varphi(5) = 4$ Elemente der Ordnung 5 in U und damit existieren in G mindestens vier Elemente der Ordnung 5. Genau zwei Elemente der Ordnung kann es daher nicht geben.

c) Ja. Vorlesung.

d) Ja. Sei g ein erzeugendes Element der zyklischen Gruppe G. Dann ist $\varphi(G) = \{\varphi(g) \mid g \in G\} = \{\varphi(g^i) \mid i \in \mathbb{Z}\} = \{\varphi(g)^i \mid i \in \mathbb{Z}\} = \langle \varphi(g) \rangle$, also ist $\varphi(G)$ zyklisch.

Aufgabe P29

a) Ja. Es gilt $H = \langle [8]_{20} \rangle$.

b) 5. Es ist $5 \cdot [8]_{20} = [40]_{20} = [0]_{20}$, also ist $|H| = \operatorname{ord}[8]_{20} = 5$.

c) 4. Vergleiche Aufgabe P28 b)

d) 4. Die Nebenklassen sind $[0]_{20} + H$, $[1]_{20} + H$, $[2]_{20} + H$ und $[3]_{20} + H$. (Es gilt $[4]_{20} + H = [4]_{20} + [20]_{20} + H = [24]_{20} + H = [0]_{20} + H$.)

e) Ja. Wegen $[-24]_{20} + H = H$ ist $[26]_{20} + H = [26]_{20} + [-24]_{20} + H = [2]_{20} + H$.