Aufgabe 1

Sei $\frac{a}{b} \in \mathbb{Q}$ gekürzt. Dann ist $b \cdot \frac{a}{b} = a \in \mathbb{Z}$ und b ist die kleinste [redacted] positive ganze Zahl mit dieser Eigenschaft. Anders ausgedrückt ist b die Ordnung von $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Insbesondere [redacted] hat jedes Element von $\mathbb{Q}/\mathbb{Z}$ endliche Ordnung.

Um nun die Elemente der Ordnungen 2 und 3 in $\mathbb{Q}/\mathbb{Z}$ zu finden, müssen wir also nur Brüche der Form $\frac{a}{2}$ und $\frac{a}{3}$ anschauen, wobei a eine positive ganze Zahl kleiner 2 bzw. 3 ist (denn jedes Element von $\mathbb{Q}/\mathbb{Z}$ hat einen Repräsentanten in $[0,1) \cap \mathbb{Q}$). Wir erhalten also ← automatisch gekürzt, da Nenner prim

$\frac{1}{2} + \mathbb{Z}$

als Element der Ordnung 2 und

[redacted] $\frac{2}{3}$

$\frac{1}{3} + \mathbb{Z}$, [redacted] $+ \mathbb{Z}$

als Elemente der Ordnung [redacted] 3.

Aufgabe 2

(i) Stimmt nicht

Die Gruppe $\mathbb{Z}/2\mathbb{Z}$ ist zyklisch mit Erzeuger $\bar{1}$. Das Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist aber nicht zyklisch, da jedes nicht-triviale Element daraus die Ordnung 2 besitzt:

$(\bar{1},\bar{0}) + (\bar{1},\bar{0}) = (\bar{0},\bar{0})$

$(\bar{0},\bar{1}) + (\bar{0},\bar{1}) = (\bar{0},\bar{0})$

$(\bar{1},\bar{1}) + (\bar{1},\bar{1}) = (\bar{0},\bar{0})$

(ii) Stimmt nicht

Wir betrachten das Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und das Element $(\bar{1},\bar{1}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Es gelten

$2(\bar{1},\bar{1}) = (\bar{0},\bar{2})$,

$3(\bar{1},\bar{1}) = (\bar{1},\bar{0})$

$4(\bar{1},\bar{1}) = (\bar{0},\bar{1})$

$5(\bar{1},\bar{1}) = (\bar{1},\bar{2})$

und

$6(\bar{1},\bar{1}) = (\bar{0},\bar{0})$,

sodass die Ordnung von $(\bar{1},\bar{1}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ genau 6 ist. Somit ist dies ein Erzeuger von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(iii) Stimmt

Ist G zyklisch mit Erzeuger $a \in G$, so lässt sich jedes Element $g \in G$ als $g = a^n$ für ein $n \in \mathbb{Z}$ schreiben. Ist nun $\bar{g} \in G/N$ ein Element eines Quotienten von G, so erhalten wir (als die Äquivalenz von g bzgl N)

$\bar{g} = \overline{a^n} = \bar{a}^n$.

Also ist G/N zyklisch mit Erzeuger $\bar{a}$.

(iv) Stimmt

Ist G eine nicht-triviale Gruppe, so besitzt G ein Element $a \neq e$. Daher ist $\langle a \rangle$ eine nicht-triviale zyklische Untergruppe von G.

(v) Stimmt nicht

Wir betrachten die Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Nach dem Satz von Lagrange haben ihre echten Untergruppen die Ordnungen 2 oder 1 und sind somit stets zyklisch (eine Gruppe von Primzahlordnung ist stets zyklisch und die triviale Gruppe wird von e erzeugt). Nun [redacted] ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ jedoch [redacted] nicht zyklisch, wie [redacted] in (i) gesehen.

Aufgabe 3

(i)

Wir erhalten

$$e_H = \varphi(e_G) = \varphi(g^m) = \varphi(g)^m,$$

sodass die Ordnung von $\varphi(g)$ ein Teiler von m ist. Wäre $\text{ord}(\varphi(g)) < m$, so erhielten wir

$$e_G = \varphi^{-1}(e_H) = \varphi^{-1}\left(\varphi(g)^{\text{ord}(\varphi(g))}\right) = \varphi^{-1}\left(\varphi(g^{\text{ord}(\varphi(g))})\right)$$

$$= g^{\text{ord}(\varphi(g))}$$

im Widerspruch dazu, dass m die Ordnung von g ist.

(ii)

Sei $\varphi: G \to H$ ein Homomorphismus von Gruppen. Dann erhalten wir vermöge des Isomorphiesatzes den Isomorphismus $\bar{\varphi}: \underbrace{G/\ker(\varphi)}_{|G/\ker(\varphi)| \text{ teilt } |G|} \to \underbrace{\text{im}(\varphi)}_{|\text{im}(\varphi)| \text{ teilt } |H|}$. Somit muss aufgrund der Teilerfremdheit der Ordnungen von G und H bereits $|\text{im}(\varphi)| = 1$ gelten. Also ist φ der triviale Homomorphismus.

Aufgabe 4

(i)

Nach dem Satz von Lagrange teilt die Ordnung eines Elementes einer Gruppe stets die Ordnung der Gruppe. Somit kommen für nicht-triviale Elemente von G nur die Ordnungen p und p^2 infrage. Da G nun aber nicht zyklisch ist, gibt es kein Element der Ordnung p^2, sodass jedes nicht-triviale Element von G die Ordnung p besitzt.

(ii)

Zunächst einmal kann aba^{-1} nicht mit $b^0 = e$ übereinstimmen, da sonst auch $b = e$ gelten würde. Ist nun $aba^{-1} = b^i$ für ein $1 \leq i \leq p-1$, so erhalten wir $ab = b^i a$ und somit

$$a^{p-1} b a^{-(p-1)} = a^{p-2} b^i a a^{-(p-1)} = a^{p-3} b^{i^2} a^2 a^{-(p-1)}$$

($a^{p-1} = a^{-1}$, $a = a$)

$$= \dots$$

$$= b^{i^{p-1}} a^{p-1} a^{-(p-1)}$$

$$= b^{i^{p-1}}$$

$|\mathbb{F}_p^\times| = p-1$ $\rightarrow$ $= b$

$\Rightarrow i^{p-1} = 1 \in \mathbb{F}_p^\times$

also $1 \bmod p$

da $\operatorname{ord}(b) = p$, also

$b^{i^{p-1}} = b^{1+p\dots} = b$

Es gilt also $ba = ab$ ↯

Daher kann aba^{-1} keine Potenz von b sein.

(iii)

Da aba^{-1} keine Potenz von b ist, ist auch kein Element von $\langle aba^{-1} \rangle$ keine Potenz von b. In der Tat, wäre $(aba^{-1})^i = ab^i a^{-1} = b^j$ eine Potenz von b, so erhielten wir, dass

$$aba^{-1} = (aba^{-1})^{p+1} = (aba^{-1})^{i+p-i+1} = b^{j+p-i+1}$$

eine Potenz von b ist. Da $|G| = p^2$ endet und $|\langle aba^{-1} \rangle| = p$, erhalten wir

$$G/\langle aba^{-1} \rangle = \{ b^i \langle aba^{-1} \rangle \mid 0 \leq i \leq p-1 \}.$$

Somit muss $a^{-1} = b^i (aba^{-1})^j = b^i a b^j a^{-1}$ sein für geeignete i und j, sodass wir $b^i a b^j = e$ und daher auch $a = b^{-i-j}$ haben ↯

Also war unsere Annahme falsch und a und b

kommutieren.

(iv)

Die Abbildung $\varphi: \langle a\rangle \times \langle b\rangle \to G, (a^n, b^m) \mapsto a^n b^m$ ist ein Homomorphismus von Gruppen, da

$$\varphi((a^n,b^m)\cdot(a^{n'},b^{m'})) = \varphi((a^{n+n'},b^{m+m'})) = a^{n+n'}\,b^{m+m'}$$

$$\overset{\text{a und b kommutieren}}{\longrightarrow} = a^n b^m a^{n'} b^{m'}$$

$$= \varphi((a^n,b^m))\,\varphi((a^{n'},b^{m'}))$$

für alle $n, n', m, m' \in \mathbb{Z}$ gilt. Um nachzuweisen, dass φ ein Isomorphismus ist, genügt es die Injektivität von φ zu zeigen, da $\operatorname{ord}(\langle a\rangle \times \langle b\rangle) = p^2 = \operatorname{ord}(G)$. Sei daher (a^n, b^m) im Kern von φ, d.h. es gelte $a^n b^m = e$. Dann erhalten wir $a^n = b^{-m}$ und somit $(a^n, b^m) = (e, e)$, da $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$ nach Wahl von a und b. Also ist φ injektiv.

(v) Wir erhalten, dass die beiden Gruppen

$\mathbb{Z}/p^2\mathbb{Z}$ (falls G zyklisch ist)

und

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (Gruppen der Ordnung p sind stets isomorph zu $\mathbb{Z}/p\mathbb{Z}$)

nach den vorherigen Aufgabenteilen bis auf Isomorphie die einzigen Gruppen der Ordnung p^2 sind. Es bleibt also nur zu begründen, dass diese nicht isomorph zueinander sind. Dies folgt jedoch aus Aufgabe 3 (i), da $\mathbb{Z}/p^2\mathbb{Z}$ ein Element der Ordnung p^2 hat und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ nicht (wie in Aufgabe 4 (i) gesehen).