Nachtrag zu § 3: Kleiner Satz von Fermat

Folgerung (3.13)

Für jede Primzahl p und alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \mod p$. Ist p kein Teiler von a, dann gilt darüber hinaus $a^{p-1} \equiv 1 \mod p$.

Beweis von Folgerung 3.13

geg. Primzahl p, $a \in \mathbb{Z}$, z.zg.:

- $a^p \equiv a \mod p$
- $p \nmid a \Rightarrow a^{p-1} \equiv 1 \mod p$

Die zweite Aussage ist gleichbedeutend mit

$\bar{a}^{p-1} = \bar{1}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ für alle $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^*$

$(\mathbb{Z}/p\mathbb{Z})^*$ ist die Gruppe der Ordnung $p-1$

$\Rightarrow ord(\bar{a}) \mid (p-1) \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^*$

$\Rightarrow \bar{a}^{p-1} = \bar{1} \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^*$

Aus $a^{p-1} \equiv 1 \bmod p$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$

folgt direkt $a^p \equiv a \bmod p$ (mult. beide Seiten mit a)

Unter der Vor. $p \mid a$ gilt auch $p \mid a^p$ und somit

$a^p \equiv 0 \equiv a \bmod p$ □

Überblick § 4: Homomorphismen und Faktorgruppen

- Definition der Gruppenhomomorphismen
- Struktur der Automorphismengruppe $\mathrm{Aut}(G)$ für eine zyklische Gruppe G
- Definition der Normalteiler ($N \trianglelefteq G$)
- Komplexprodukte von Untergruppen ($NU = \{nu \mid n \in N\ ,\ u \in U\}$), innere direkte Produkte
- Definition der Faktorgruppe G/N ($N \trianglelefteq G$)
- Homomorphiesatz $G/N \cong H$, falls $\phi : G \to H$ Epimorphismus und $N = \ker(\phi)$, Isomorphiesätze als Folgerung
- Korrespondenzsatz (Untergruppenstruktur von G/N vs. Untergruppenstruktur von G)

Definition (4.1)

Sind $(G, *)$ und $(H, \circ)$ Gruppen, so bezeichnet man eine Abbildung $\phi : G \to H$ als Gruppenhomomorphismus, wenn $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ gilt.

Lemma (4.2)

Sei ϕ ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \circ)$. Dann gilt

$$\phi(e_G) = e_H \qquad \text{und} \qquad \phi(g^{-1}) = \phi(g)^{-1} \quad \text{für alle} \quad g \in G.$$

Spezielle Arten von Homomorphismen

Definition (4.3)

Seien $(G, *)$ und $(H, \circ)$ Gruppen und $\phi : G \to H$ ein Homomorphismus von Gruppen. Man bezeichnet ϕ als

(i) Monomorphismus, wenn ϕ injektiv

(ii) Epimorphismus, wenn ϕ surjektiv

(iii) Isomorphismus, wenn ϕ bijektiv ist.

Zwei Gruppen G und H sind also genau dann zueinander isomorph, wenn ein Isomorphismus $\phi : G \to H$ existiert.

Ergänzungen zum Homomorphismus-Begriff

- Einen Gruppen-Homomorphismus $\phi : G \to G$ von $(G, \cdot)$ nach $(G, \cdot)$ bezeichnet man als Endomorphismus von G.
- Ist die Abbildung ϕ außerdem bijektiv, dann spricht man von einem Automorphismus der Gruppe G.
- Die Menge der Endomorphismen bezeichnen wir mit $\mathrm{End}(G)$, die der Automorphismen mit $\mathrm{Aut}(G)$.

Anwendung von Homomorphismen und Potenzierung

Lemma (4.4)

Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(g^n) = \phi(g)^n$ für alle $g \in G$ und $n \in \mathbb{Z}$.

Isomorphie von Permutationsgruppen

Satz (4.5)

Seien X, Y Mengen und $\phi : X \to Y$ eine Bijektion. Dann ist durch die Abbildung

$$\hat{\phi} : \mathrm{Per}(X) \to \mathrm{Per}(Y) \quad , \quad \sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$$

ein Isomorphismus von Gruppen definiert.

Auf Grund des Satzes gilt $\mathrm{Per}(X) \cong S_n$ für jede n-elementige Menge X.

Die Automorphismen als invertierbare Elemente

Sei $(G, \cdot)$ eine Gruppe.

- Sind $\phi_1, \phi_2 \in \mathrm{End}(G)$, dann auch $\phi_1 \circ \phi_2$.
- Die Verknüpfung $\circ$ auf $\mathrm{End}(G)$ erfüllt das Assoziativgesetz.
- Außerdem gilt $\phi_1 \circ \mathrm{id}_G = \mathrm{id}_G \circ \phi_1 = \phi_1$ für alle $\phi_1 \in \mathrm{End}(G)$. Also ist $(\mathrm{End}(G), \circ)$ ein Monoid.

Proposition (4.6)

Die invertierbaren Elemente in $\mathrm{End}(G)$ sind genau die Automorphismen der Gruppe G.

Die Automorphismengruppe einer Gruppe

Aus der Tatsache, dass die invertierbaren Elemente eines Monoids eine Gruppe bilden, folgt nun

Satz (4.7)

Die Automorphismen einer Gruppe G bilden mit der Verknüpfung $\circ$ selbst eine Gruppe. Man nennt sie die Automorphismengruppe $\mathrm{Aut}(G)$ der Gruppe G.

Ergänzung:

Ist $\phi : G \to H$ ein Isomorphismus von Gruppen, dann gilt dasselbe für die Umkehrabbildung $\phi^{-1} : H \to G$.

Erhaltung von Untergruppen unter Homomorphismen

Proposition (4.8)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus, außerdem U eine Untergruppe von G und V eine Untergruppe von H. Dann gilt

(i) Die Bildmenge $\phi(U)$ ist eine Untergruppe von H.

(ii) Die Urbildmenge $\phi^{-1}(V)$ ist eine Untergruppe von G.

Beweis von Proposition 4.8:

geg: Gruppenhom. $\phi: G \to H$

$U \leq G$ (= Untergruppe), $V \leq H$

zzg: (i) $\phi(U) = \{\phi(u) \mid u \in U\} \leq H$

(ii) $\phi^{-1}(V) = \{g \in G \mid \phi(g) \in V\} \leq G$

zu (i) Überprüfe (1) $e_H \in \phi(U)$

(2) $\forall a, b \in \phi(U): ab, a^{-1} \in \phi(U)$

zu (1) $e_G \in U$ (da $U \leq G$) $\to e_H = \phi(e_G) \in \phi(U)$

zu (2) Seien $a, b \in \phi(U) \Rightarrow \exists u, v \in U$

mit $a = \phi(u)$, $b = \phi(v)$

$u, v \in U$, $U \leq G \Rightarrow uv \in U$, $u^{-1} \in U$

$\Rightarrow ab = \phi(u)\phi(v) = \phi(uv) \in \phi(U)$

$a^{-1} = \phi(u)^{-1} = \phi(u^{-1}) \in \phi(U)$

zu (iii) überprüfe: (1) $e_G \in \phi^{-1}(V)$

(2) $\forall g, h \in \phi^{-1}(V): gh, g^{-1} \in \phi^{-1}(V)$

zu (1) $V \leq H \Rightarrow e_H \in V \Rightarrow \phi(e_G) \in V$

$\Rightarrow e_G \in \phi^{-1}(V)$

zu (2) Seien $g, h \in \phi^{-1}(V) \Rightarrow \phi(g), \phi(h) \in V$

$\overset{V \leq H}{\Rightarrow} \phi(g)\phi(h) \in V$, $\phi(g)^{-1} \in V \Rightarrow$

$\phi(gh) \in V$, $\phi(g^{-1}) \in V \Rightarrow gh \in \phi^{-1}(V)$, $g^{-1} \in \phi^{-1}(V)$ □

Kern und Bild eines Homomorphismus

Eine besonders wichtige Rolle spielen in der Gruppentheorie der Kern $\ker(\phi) = \phi^{-1}(\{e_H\})$ und das Bild $\mathrm{im}(\phi) = \phi(G)$ eines Gruppenhomomorphismus.

Proposition (4.9)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Die Abbildung ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{e_G\}$ gilt.

Eindeutigkeit von Homomorphismen

Satz (4.10)

Seien G, H Gruppen und $S \subseteq G$ ein Erzeugendensystem von G. Sind $\phi, \phi' : G \to H$ Gruppenhomomorphismen mit

$$\phi(s) = \phi'(s) \quad \text{für alle } s \in S \quad ,$$

dann folgt $\phi = \phi'$.

Verhalten der Elementordnung unter Homomorphismen

Proposition (4.11)

Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Ist $g \in G$ ein Element von endlicher Ordnung n, dann ist auch $\mathrm{ord}(\phi(g))$ endlich, und ein Teiler von n.

Beweis von Prop. 4.11

geg: Gruppenhom. $\phi: G \to H$, $n \in \mathbb{N}$,
$g \in G$ mit $\operatorname{ord}(g) = n$

zzg: $\operatorname{ord}(\phi(g)) \mid n$, insb. ist $\operatorname{ord}(\phi(g))$ endlich

$\operatorname{ord}(g) = n \overset{\text{Satz 3.3}}{\Longrightarrow} g^n = e_G \Rightarrow \phi(g)^n = \phi(g^n)$

$= \phi(e_G) = e_H \overset{\text{Satz 3.3}}{\Longrightarrow} \operatorname{ord}(\phi(g))$ ist endlich, $\operatorname{ord}(\phi(g)) \mid n$. □

Bsp.: $\phi: \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $a + 6\mathbb{Z} \mapsto a + 3\mathbb{Z}$

$\operatorname{ord}(1 + 6\mathbb{Z}) = 6$, $\operatorname{ord}(\phi(1 + 6\mathbb{Z})) = \operatorname{ord}(1 + 3\mathbb{Z}) = 3$

Existenz von Homomorphismen auf zyklischen Gruppen

Proposition (4.12)

Sei G eine zyklische Gruppe, $g \in G$ ein erzeugendes Element, H eine weitere Gruppe und $h \in H$. Ist

- $\mathrm{ord}(g) = \infty$ oder
- $\mathrm{ord}(g)$ endlich und ein Vielfaches von $\mathrm{ord}(h)$,

dann existiert ein (eindeutig bestimmter) Gruppenhomomorphismus $\phi : G \to H$ mit $\phi(g) = h$.

Folgerung (4.13)

Je zwei unendliche zyklische Gruppen sind isomorph. Ebenso sind zwei endliche zyklische Gruppen derselben Ordnung isomorph.

Zusammen mit Satz 2.22 (i) folgt daraus: Für jede Primzahl p ist $(\mathbb{Z}/p\mathbb{Z}, +)$ bis auf Isomorphie die einzige Gruppe der Ordnung p.

Beweis von Prop. 4.12

geg. zyklische Gruppe G, $g \in G$ mit $G = \langle g \rangle$

H weitere Gruppe, $h \in H$

1. Fall: $\operatorname{ord}(g) = \infty$ zzg: Es gibt einen Hom. $\phi: G \to H$ mit $\phi(g) = h$.

Definiere $\phi: G \to H$ durch $\phi(g^k) = h^k \quad \forall k \in \mathbb{Z}$

(Dies ist möglich, da wg. $\operatorname{ord}(g) = \infty$ die Abb. $\mathbb{Z} \to G$, $k \mapsto g^k$ injektiv, d.h. $k \in \mathbb{Z}$ durch das Gruppenelement $g^k \in G$ eindeutig bestimmt ist.)

zu überprüfen: ϕ ist Gruppenhom. Seien $a, b \in G$.

z.zg.: $\phi(ab) = \phi(a)\,\phi(b)$. $a, b \in G$, $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$

$\rightarrow \exists\, k, l \in \mathbb{Z}$ mit $a = g^k$, $b = g^l \Rightarrow \phi(ab) = \phi(g^k g^l) =$

$\phi(g^{k+l}) = h^{k+l} = h^k\, h^l = \phi(g^k)\,\phi(g^l) = \phi(a)\,\phi(b)$

2. Fall: $n = \mathrm{ord}(g) \in \mathbb{N}$, $\mathrm{ord}(h) \mid n$

bekannt (§5) $\Rightarrow g^0, g^1, \ldots, g^{n-1}$ sind die verschiedenen Elemente von $G = \langle g \rangle$. Definiere $\phi: G \to H$ durch

$$\phi(g^k) = h^k \quad \text{für } 0 \le k \le n-1 \qquad (*)$$

Überprüfe, dass $(*)$ für alle $k \in \mathbb{Z}$ gilt. Sei also $k \in \mathbb{Z}$.

Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $k = qn + r$ und $0 \le r \le n-1$

$\Rightarrow g^k = g^{qn+r} = (g^n)^q \cdot g^r = e_G^q\, g^r = g^r$

ebenso: $h^k = h^{qn+r} = (h^n)^q \cdot h^r =$

$\overset{\text{Ord}(h) \mid n}{=} e_H^q \cdot h^r = h^r$

$\Rightarrow h^n = e_H$

$\Rightarrow \phi(g^k) = \phi(g^r) = h^r = h^k$

Nun kann die Hom.-eigenschaft wie im 1. Fall nachgerechnet werden. □

Die primen Restklassengruppen

Nach § 1 bildet die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ eine Gruppe. Man bezeichnet sie als prime Restklassengruppe.

Proposition (4.14)

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das Element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten, wenn $\mathrm{ggT}(a, n) = 1$ ist.

Beweis von Prop. 4.14:

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$.

Beh.:

$a + n\mathbb{Z}$ ist invertierbar $\iff$ $ggT(a,n) = 1$

in Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$

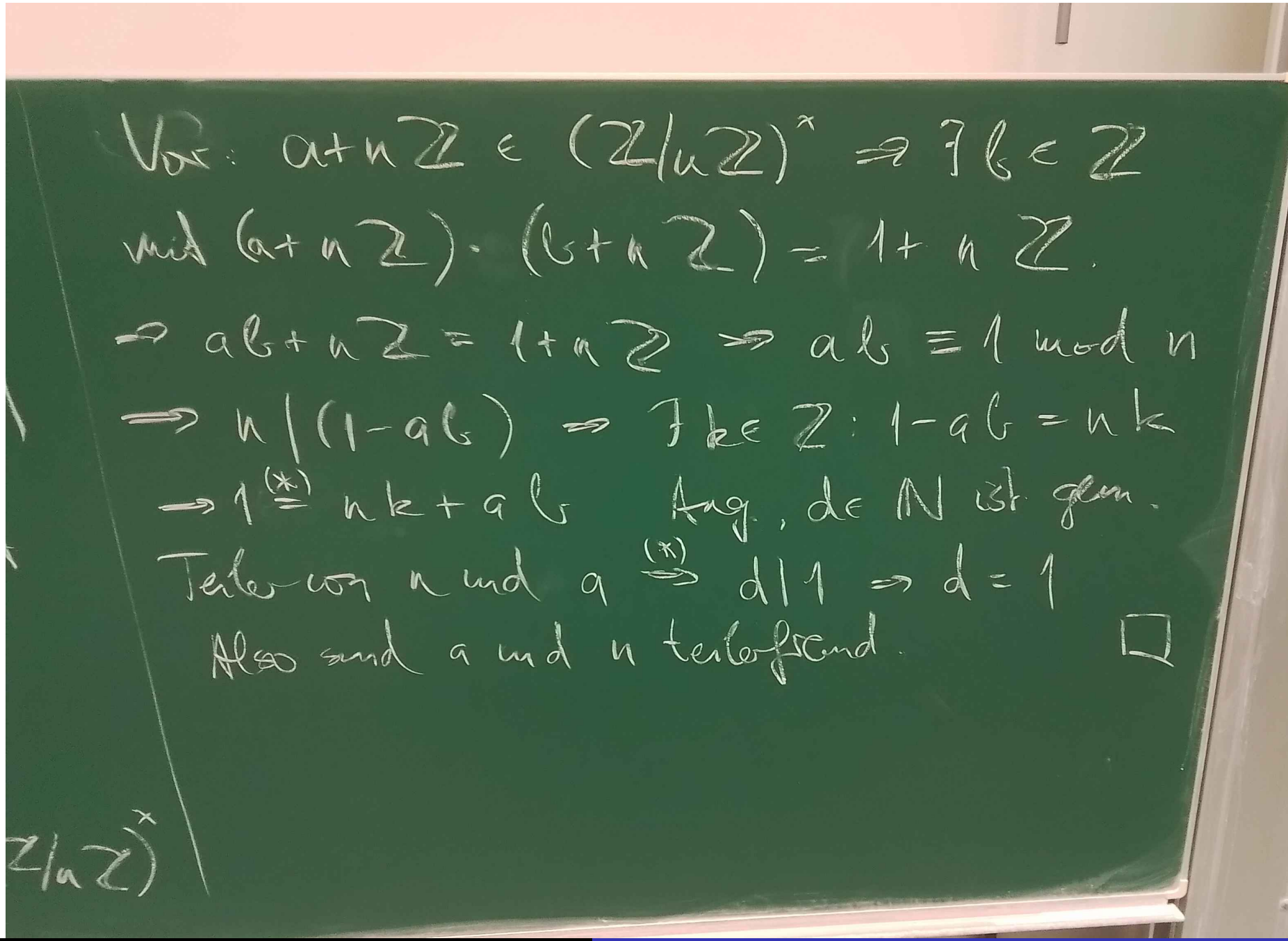
„$\Leftarrow$" $ggT(a,n) = 1 \overset{\text{Lemma von Bézout (§3)}}{\Longrightarrow}$ $\exists k, l \in \mathbb{Z}$ mit $ka + ln = 1$

$ka + ln + n\mathbb{Z} = 1 + n\mathbb{Z} \rightarrow$

$ka + n\mathbb{Z} + \underbrace{ln + n\mathbb{Z}}_{= 0 + n\mathbb{Z}} = 1 + n\mathbb{Z} \rightarrow$

$(k + n\mathbb{Z})(a + n\mathbb{Z}) = 1 + n\mathbb{Z} \rightarrow a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Beweis der Richtung „$\Rightarrow$“



Struktur der Automorphismengruppen zyklischer Gruppen

Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Für jedes $a \in \mathbb{Z}$ existiert ein eindeutig bestimmter Endomorphismus

$$\tau_a : G \to G \qquad \text{mit} \qquad \tau_a(g) = g^a.$$

Satz (4.15)

Die Abbildung $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G)$, $a + n\mathbb{Z} \mapsto \tau_a$ ist ein Isomorphismus von Gruppen.

Im Fall, dass $G = \langle g \rangle$ unendlich ist, gilt $\mathrm{Aut}(G) \cong (\mathbb{Z}/2\mathbb{Z}, +)$.

Beweis von Satz 4.15:

geg.: $n \in \mathbb{N}$, G zyklische von Ordnung n
$g \in G$ mit $G = \langle g \rangle$

z.Z.: $\Rightarrow \exists\, \mathbb{Z} \to \mathrm{End}(G)$, $a \mapsto \tau_a$
mit τ_a definiert durch $\tau_a(g) = g^a$

Beob.: Sind $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod n$,
dann folgt $\tau_a = \tau_b$.

$a \equiv b \bmod n \rightsquigarrow n \mid (a-b) \Rightarrow \exists k \in \mathbb{Z}$ mit
$kn = a - b \Rightarrow b = a - kn$
$\Rightarrow \tau_b(g) = g^b = g^{a-kn} = g^a \cdot (g^n)^{-k} \overset{\text{ord}(g) = n}{=}$

$g^q \cdot e_G^{-k} = g^q = \tau_a(g) \xrightarrow[\text{Eindeutigkeit Prop. 4.10}]{G=\langle g\rangle} \tau_a = \tau_b$

Aus der Beob. folgt, dass es ein Abb. $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ mit $\phi(a+n\mathbb{Z}) = \tau_a \; \forall a \in \mathbb{Z}$ gibt.

zu überprüfen: (1) $\phi((\mathbb{Z}/n\mathbb{Z})^\times) = \mathrm{Aut}(G)$

(2) $\phi((a+n\mathbb{Z})\cdot(b+n\mathbb{Z})) = \phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z})$

$\forall a, b \in \mathbb{Z}$.

Aus (1), (2) folgt dann, dass ϕ einen Isomorphismus zwischen $(\mathbb{Z}/n\mathbb{Z})^\times$ und $\mathrm{Aut}(G)$ definiert.