Alg. 18: Blatt 1

A1 (a) Falsch. Gegenbeispiel:

$G = C_2 \times C_2$, $H_1 = C_2 \times \{1\}$, $H_2 = \{1\} \times C_2$.

$= \langle (a, 1) \rangle$ $= \langle (1, b) \rangle$

Dann $(a,1)$ und $(1,b) \in H_1 \cup H_2$

aber $(a,1) \cdot (1,b) = (a,b) \notin H_1 \cup H_2$.

(b) Wahr

Bew: $N \trianglelefteq G$ Normalteiler $\Rightarrow \forall g \in G, a \in N,\ gag^{-1} \in N$

$\Rightarrow \forall h \in H \subseteq G, a \in N,\ hah^{-1} \in N$.

$\Rightarrow N \trianglelefteq H$.

(c) Falsch

Gegenbeispiel: Für $n=3$ betrachte $\begin{cases} (12) \in S_3 \\ (23) \in N \end{cases}$ mit

$(12)(23)(12)^{-1} = (12)(23)(21) = (13)(2) = (13) \notin N$.

[Bem. $(23) \in N$, da $(23)[1] = 1$]

Hier ist $(12) \in S_3$ die Bijektion

$(12) = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}$. Analog $(23) = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$.

A2 (a) Beh: $P := \{a^m b^n \mid m, n \in \mathbb{Z}\} \leq G$

[Bew: Für jede $m, n \in \mathbb{Z}$,

$(a^m b^n)^{-1} = b^{-n} a^{-m} \underset{\text{abel.}}{=} a^{-m} b^{-n} \in P$.

Auch für jede $m_1, n_1, m_2, n_2 \in \mathbb{Z}$

$(a^{m_1} b^{n_1})(a^{m_2} b^{n_2}) \underset{\text{abel.}}{=} (a^{m_1} a^{m_2})(b^{n_1} b^{n_2})$

$= a^{m_1+m_2} b^{n_1+n_2} \in P$.]

Beh. $\langle a, b \rangle = P$

[Bew: ($\subseteq$) Nun $\langle a,b \rangle := \bigcap_{\substack{H \leq G \\ a,b \in H}} H \subseteq P$, da $a, b \in P$.

($\supseteq$) Klar dass $a, b \in \langle a, b \rangle$. Auch $\langle a,b \rangle \overset{(\text{Lem } 7.1.14)}{\leq} G$.

$\Rightarrow$ für jede $m, n \in \mathbb{Z}$, $a^m, b^n, a^m \cdot b^n \in \langle a,b \rangle$,

d.h. $\langle a,b \rangle \geq P$.

Folgende, dass $|\langle a,b \rangle| = |P| \leq \left| \{(n,m) \mid 0 \leq n < \operatorname{ord} a,\ 0 \leq m < \operatorname{ord} b\} \right|$

$= |\langle a \rangle| \cdot |\langle b \rangle|$.

Alg IS I

AZ (b) Beh: $D_\infty \leq \mathrm{Sym}(\mathbb{Z})$

Bew: Für jede $f, g \in D_\infty$, gibt es

$r_1, r_2 \in \{\pm 1\}$, $s_1, s_2 \in \mathbb{Z}$ mit

$f: x \longmapsto r_1 x + s_1$

$g: x \longmapsto r_2 x + s_2$.

Also, $g^{-1}: x \longmapsto (x - s_2) r_2 = r_2 x - r_2 s_2$.

($r_2 \in \{\pm 1\}$, $s_2 \in \mathbb{Z}$)

Also $g^{-1} \in D_\infty$

$f \circ g: x \xrightarrow{f} r_1 x + s_1 \xrightarrow{g} r_2 r_1 x + r_2 s_1 + s_2$ (also $f \circ g: x \longmapsto r_2 r_1 x + r_2 s_1 + s_2$)

($r_2 r_1 \in \{\pm 1\}$, $r_2 s_1 + s_2 \in \mathbb{Z}$)

$\Rightarrow f \circ g \in D_\infty$. ⌟

(c) $x \xrightarrow{a} -x \xrightarrow{a} x \Rightarrow a^2 = id$.

$x \xrightarrow{b} 1 - x \longmapsto 1 - (1 - x) = x \Rightarrow b^2 = id$

Also $\langle a \rangle \cong C_2$, $\langle b \rangle \cong C_2$.

$\Rightarrow |\langle a \rangle| = |\langle b \rangle| = 2$.

Aber: $a \circ b: x \xrightarrow{b} 1 - x \xrightarrow{a} x - 1$ (also $a \circ b: x \longmapsto x - 1$)

analog $(a \circ b)^n: x \longmapsto x - n$, für jedes $n \in \mathbb{Z}$

$\Rightarrow \mathbb{Z} \cong H \leq \langle a, b \rangle$

$\Rightarrow |\mathbb{Z}| \leq |\langle a, b \rangle|$

$\Rightarrow |\langle a, b \rangle| \not\leq 4 = |\langle a \rangle| \cdot |\langle b \rangle|$

A3] Alg. B1

(a) Beh: $f: a \mapsto \sigma_a$ ist ein (Gruppen) Homomorphismus

d.h: $\forall a, b \in G$, $\underbrace{f(ab)}_{=\sigma_{ab}} = \underbrace{f(a)}_{=\sigma_a} \cdot \underbrace{f(b)}_{=\sigma_b}$

Bew: Sei $a, b \in G$

Für jedes $g \in G$ gilt:

$$\sigma_{ab}(g) = ab \cdot g = \sigma_a(bg) = \sigma_a(\sigma_b(g)) = \sigma_a \circ \sigma_b(g)$$

Also $\sigma_{ab} = \sigma_a \circ \sigma_b$. ⌟

(b) Beh: $\sigma_a = \sigma_b \Rightarrow a = b$ (Injektivität)

Bew: Sei $\sigma_a = \sigma_b$.

$\forall g \in G$, $\sigma_a(g) = \sigma_b(g)$

$a \cdot g = b \cdot g$

Also $agg^{-1} = bgg^{-1} \Rightarrow a = b$ ⌟

(c) [Der Satz von Cayley]

Da f ein Homomorphismus nach $\mathrm{Sym}(G)$ ist, ist $\mathrm{Im}(f) \leq \mathrm{Sym}(G)$ eine Untergruppe. (Lem. 7.2.6)

Nach (b), ist $f: G \to \mathrm{Im}(f)$ ein Isomorphismus nach $\mathrm{Im}(f)$.

Sei $|G| = n$. Es gilt $\mathrm{Sym}(G) \cong S_n$. Insbesondere ist $\mathrm{Im}(f) \cong \varphi(\mathrm{Im}(f)) \leq S_n$, φ Isomorphismus.

Also ist $G \simeq \mathrm{Im}(\dots) \leq S_n$ mit $n = |G| > 0$

A4] (a) Sei $\gamma_a: G \to G$, $\gamma_a(b) = aba^{-1}$.

(i) Beh: γ_a ist ein Homomorphismus

Für alle $b, c \in G$ gilt

$$\gamma_a(bc) = a \cdot bc \cdot a^{-1} = ab\underline{a^{-1}a}ca^{-1}$$
$$= \gamma_a(b) \cdot \gamma_a(c)$$

⌟

(ii) Beh: γ_a bijektiv.

(Injektivität) Sei $\gamma_a(b) = \gamma_a(c)$

$\Rightarrow aba^{-1} = aca^{-1}$

$\Rightarrow \underline{a^{-1}a}ba^{-1} = \underline{a^{-1}a}ca^{-1} \Rightarrow b = c$ ⌟

(Surjektivität) Für beliebiges $g \in G$, setze $x = a^{-1}ga \in G$

Dann ist $\gamma_a(x) = a \cdot a^{-1}ga \cdot a^{-1} = g$

Also $g \in \mathrm{Im}(\gamma_a) = G$ für alle $a \in G$ ⌟

Also $\gamma_a \in \mathrm{Aut}(G)$ für jedes $a \in G$

A4 (b) Sei $\sigma_a : G \to G$, $\sigma_a(b) = ab$.

Wenn σ_a ein Automorphismus ist, so ist $\sigma_a(1) = 1$. (Bem. 1.2.2)

Sei $\sigma_a \in Aut(G)$.

Dann ist $1 = \sigma_a(1) = a1$ Also $a = 1$

(c) ⌈(⇐) Sei G abelsch und $\rho : G \to G$

$\rho(b) = b^2$

Für beliebige $b, c \in G$

$$\rho(bc) = (bc)^2 = b\underbrace{cb}_{\text{abel.}}c = b^2c^2 = \rho(b)\cdot\rho(c)$$

Also ρ ein Hom. $G \to G$, d.h. $\rho \in End(G)$.⌋

⌈(⇒) Sei $\rho : G \to G$, $\rho(b) = b^2$ ein Hom. ist.

Also für jede $b, c \in G$,

$$\begin{array}{ccc} \rho(bc) & = & \rho(b)\cdot\rho(c) \\ \| & & \| \\ (bc)^2 & = & b^2 \cdot c^2 \\ \Rightarrow \quad bcbc & = & b^2c^2 \\ \Rightarrow \quad cb & = & bc, \ \forall\, b, c \in G. \end{array}$$

D.h., G abelsch ist ⌋

A5 (a) $G = \langle A \rangle$, $g_1, g_2 \in Hom(G, H)$.

Beh $\left(g_1(a) = g_2(a), \forall a \in A\right) \Rightarrow \left(g_1(g) = g_2(g), \forall g \in G\right)$

⌈Strategie 1, mit folgende

⌈Lemma 1: $\langle A \rangle = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \;\middle|\; n \in \mathbb{N},\ a_i \in A,\ \varepsilon_i \in \{1, -1\} \text{ für jede } i \in \{1, \dots, n\} \right\}$

Bew. etc.⌋

Aber hier gehe mit:

⌈Lemma 2: Sei $g_1, g_2 \in Hom(G, H)$.

Es gilt $Q := \{g \in G \mid g_1(g) = g_2(g)\}$ eine Untergruppe von G ist.⌋

⌈Bew (Lem 2)

Für jede $g, h \in Q$,

$g_1(g\cdot h) \underset{g_1 \text{ Hom}}{=} g_1(g)\cdot g_1(h) \underset{Q}{=} g_2(g)\cdot g_2(h) \underset{g_2 \text{ Hom}}{=} g_2(g\cdot h)$

d.h., $g \cdot h \in Q$.

Auch, nach Bem 1.2.2, $g_1(h^{-1}) = g_1(h)^{-1} \underset{Q}{=} g_2(h)^{-1} = g_2(h^{-1})$.

Also $h^{-1} \in Q$.⌋

Alg BT1

A5] Bew. (Beh) Nach Voraussetzung, $A \subseteq Q$.

Nach Lem. 2, $Q \leq G$.

Also $\langle A \rangle \subseteq Q$. Aber $\langle A \rangle = G$.

Also $Q = G$ ⌟

(b) Nach Hinweis, wähle $1 \in \mathbb{Z}$, da $\langle 1 \rangle = \mathbb{Z}$.

Achtung: $(\mathbb{Z}, \cdot)$, $1 \neq id$!

Sei $f \in Hom(\mathbb{Z}, \mathbb{Z})$ mit $f(1) = z \in \mathbb{Z}$

Beispiel 1.7.7b

So ist $\operatorname{Im} f = f(\langle 1 \rangle) = \{ f(n1) \mid n \in \mathbb{Z} \}$

$= \{ n \cdot f(1) \mid n \in \mathbb{Z} \}$

$= \{ n \cdot z \mid n \in \mathbb{Z} \} = z\mathbb{Z}$

Also $\operatorname{Im} f = z\mathbb{Z} = \mathbb{Z} \iff z = \pm 1$

Also f surjektiv $\iff f(1) = \pm 1$

Nach (a), für jedes $z \in \mathbb{Z}$, gibt es nur eines $h \in Hom(\mathbb{Z}, \mathbb{Z})$ mit $h(1) = z$.

Also $|Aut(\mathbb{Z})| \leq 2$. (*)

Nun $id \in Hom(\mathbb{Z}, \mathbb{Z})$ mit $id(1) = 1$.

Bem. dass $id \in Aut(\mathbb{Z})$.

Betrachte $\mu : \mathbb{Z} \longrightarrow \mathbb{Z}$

$x \longmapsto -x$.

$\mu \in Hom(\mathbb{Z}, \mathbb{Z})$, da $\mu(x+y) = -(x+y) = \mu(x) + \mu(y)$ für alle $x, y \in \mathbb{Z}$.

μ ist injektiv, da $\mu(x) = \mu(y) \Rightarrow -x = -y \Rightarrow x = y$.

μ ist auch surjektiv (wie oben)

Also $\mu \in Aut(\mathbb{Z})$. So gilt $\{id, \mu\} \in Aut(\mathbb{Z})$

Nach (*) es gilt $Aut(\mathbb{Z}) = \{id, \mu\} \cong C_2$.

(c) Sei $a, b \in G$, mit $ord(a) = ord(b)$.

Sei $\varphi_b : G \longrightarrow G$ def. durch $a^k \longmapsto b^k$, $\forall k$.

Lemma 3: Wenn $\langle a \rangle = \langle b \rangle = G$,

so ist $\varphi_b \in Aut(G)$

Alg. B1

A5] Bew. (Lem. 3)

Sei $\langle a \rangle = \langle b \rangle = G$.

* φ_b ist ein Homomorphismus, da

$\forall k, s$, $\varphi_b(a^k \cdot a^s) = \varphi_b(a^{k+s}) = b^{k+s} = b^k \cdot b^s$

$= \varphi(a^k) \cdot \varphi(a^s)$.

* φ_b ist injektiv, weil

$\varphi_b(a^k) = \varphi_b(a^s) \Rightarrow b^k = b^s$

$\Rightarrow k \equiv s \pmod{\text{ord}(b)}$

(ord a = ord b) $\Rightarrow k \equiv s \pmod{\text{ord}(a)}$

$\Rightarrow a^k = a^s$.

* φ_b ist surjektiv

Da $\langle b \rangle = G$, jedes $g = b^k$ für geeignet k.

So ist $\varphi_b(a^k) = b^k = g$.

Nach Lemma 3. und (a),

es genügt zu finden alle $b \in \mathbb{Z}/10\mathbb{Z}$

mit $\langle b \rangle = \mathbb{Z}/10\mathbb{Z}$.

Dann es gilt $\text{Aut}(\mathbb{Z}/10\mathbb{Z}) = \{\varphi_b \mid \langle b \rangle = \mathbb{Z}/10\mathbb{Z}\}$

Wobei $\varphi_b : \mathbb{Z}/10\mathbb{Z} \longrightarrow \mathbb{Z}/10\mathbb{Z}$, (für solches b)

$\bar{1} \longmapsto b$

$\bar{k} \longmapsto \overline{bk}$

Nun,

$\langle \bar{1} \rangle = \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{0}\} \neq \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{3} \rangle = \{\bar{3}, \bar{6}, \bar{9}, \bar{2}, \bar{5}, \bar{8}, \bar{1}, \bar{4}, \bar{7}, \bar{0}\} = \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{4} \rangle = \{\bar{4}, \bar{8}, \bar{2}, \bar{6}, \bar{0}\} \neq \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{5} \rangle = \{\bar{5}, \bar{0}\} \neq \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{6} \rangle = \langle \bar{4} \rangle = \langle \bar{2} \rangle = \langle \bar{8} \rangle \neq \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{7} \rangle = \langle \bar{3} \rangle = \mathbb{Z}/10\mathbb{Z}$

$\langle \bar{9} \rangle = \langle \bar{1} \rangle = \mathbb{Z}/10\mathbb{Z}$

Bew. $\text{Aut}(\mathbb{Z}/10\mathbb{Z}) \cong C_4$.

Also, $\text{Aut}(\mathbb{Z}/10\mathbb{Z}) = \{\varphi_1, \varphi_3, \varphi_7, \varphi_9\}$