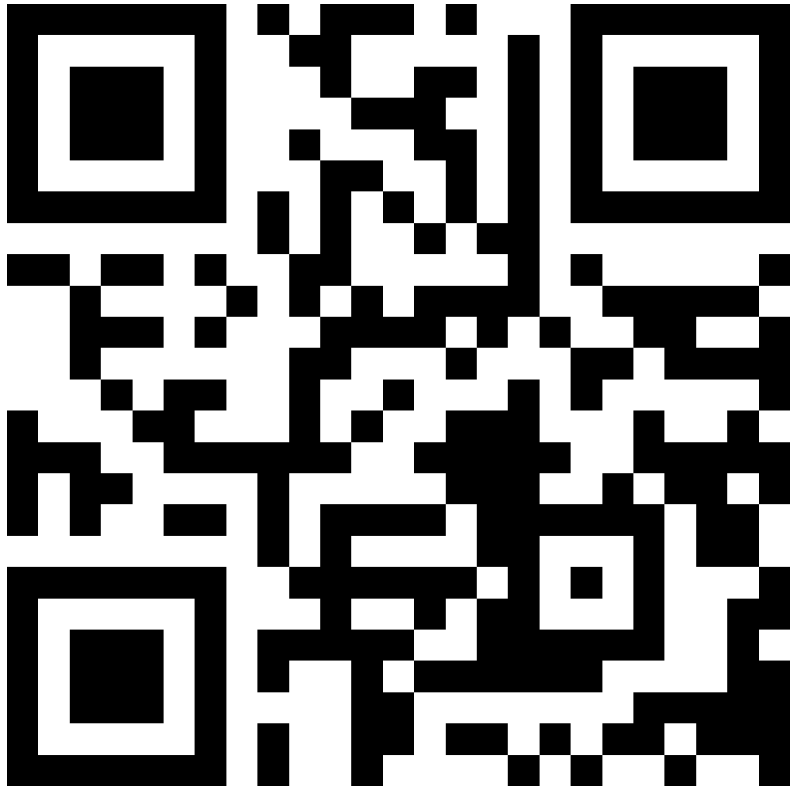
Plenarübung Lineare Algebra I

(Inhalts)-Woche 05



Link zu diesen Folien

Die Umfrageergebnisse

Zusammenfassung für G01Q02

Was soll in der Plenarübung vorrangig behandelt werden?

Antwort	Anzahl	Brutto-Prozentsatz
Wiederholung von Skriptinhalten Ansehen	21	38.89%
Erklärungen zu Skriptbeispielen Ansehen	4	7.41%
Lösungen der Hausaufgaben Ansehen	6	11.11%
Nicht beendet oder nicht gezeigt	32	59.26%
Gesamt(Brutto)	**63**	**100.00%**

Zusammenfassung für G01Q01

Welche weiteren Fragen haben Sie zum Stoff der Veranstaltung?

Antwort	Anzahl	Brutto-Prozentsatz
Antwort Ansehen	6	11.11%
Keine Antwort	16	29.63%
Nicht beendet oder nicht gezeigt	32	59.26%
Gesamt(Brutto)	**54**	**100.00%**

„Gehäuftes“ Interesse an:

(1) (Zyklischer) Erzeugung und Ordnung

(2) Nebenklassen und Äquivalenzrelationen

Ziele und Vorgehen für heute

Hauptziele

(1) Inhalte festigen

(2) Intuition verbessern

Arbeitsplan

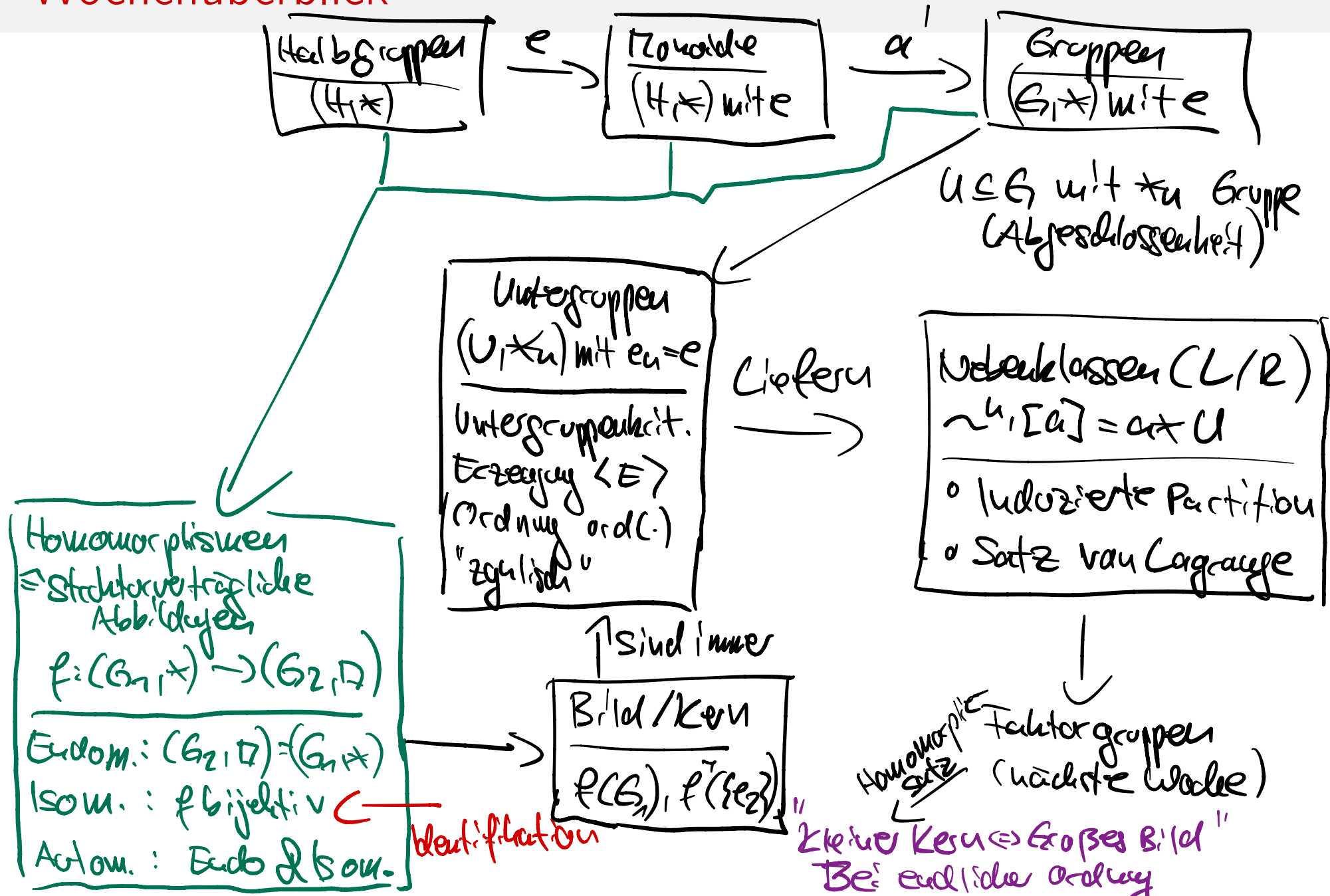
(1) Wochenüberblick

(2) Wiederholen und Ergänzen bekannter Inhalte

(3) Arbeiten mit den Begriffen
    (1) Untergruppen und (zyklische) Erzeugung
    (2) Nebenklassen und Äquivalenzrelationen
    (3) Homomorphismen (zeitabhängig)

(4) "Nutzen"der Begriffe zeigen

Wochenüberblick



Wiederholung Untergruppen und Erzeugung

Definition

Es sei $(G, \cdot)$ eine Gruppe.

(1) $U \subseteq G$ **Untergruppe**, wenn $\cdot$-abgeschlossen und selbst Gruppe

$\cdot : U \times U \to U$ $\quad 1_G,\ a^{-1}$

(2) $E \subseteq G$, dann ist die von E **erzeugte Untergruppe**

$$\langle E \rangle := \bigcap \{ U \mid (U, \cdot) \text{ ist Untergruppe von } (G, \cdot) \text{ und } E \subseteq U \}$$

$$= \{ a_1 \cdot (\cdots) \cdot a_n \mid \exists n \in \mathbb{N}_0 \ \forall i = 1, \ldots, n \ (a_i \in E \cup E') \}$$

Untergruppen schnittstabil

(3) $E \subseteq G$ **Erzeugendensystem**, wenn $\langle E \rangle = G$

i.A. nicht eindeutig

(4) $a \in G$, dann ist $\langle a \rangle$ **zyklisch** erzeugte UG

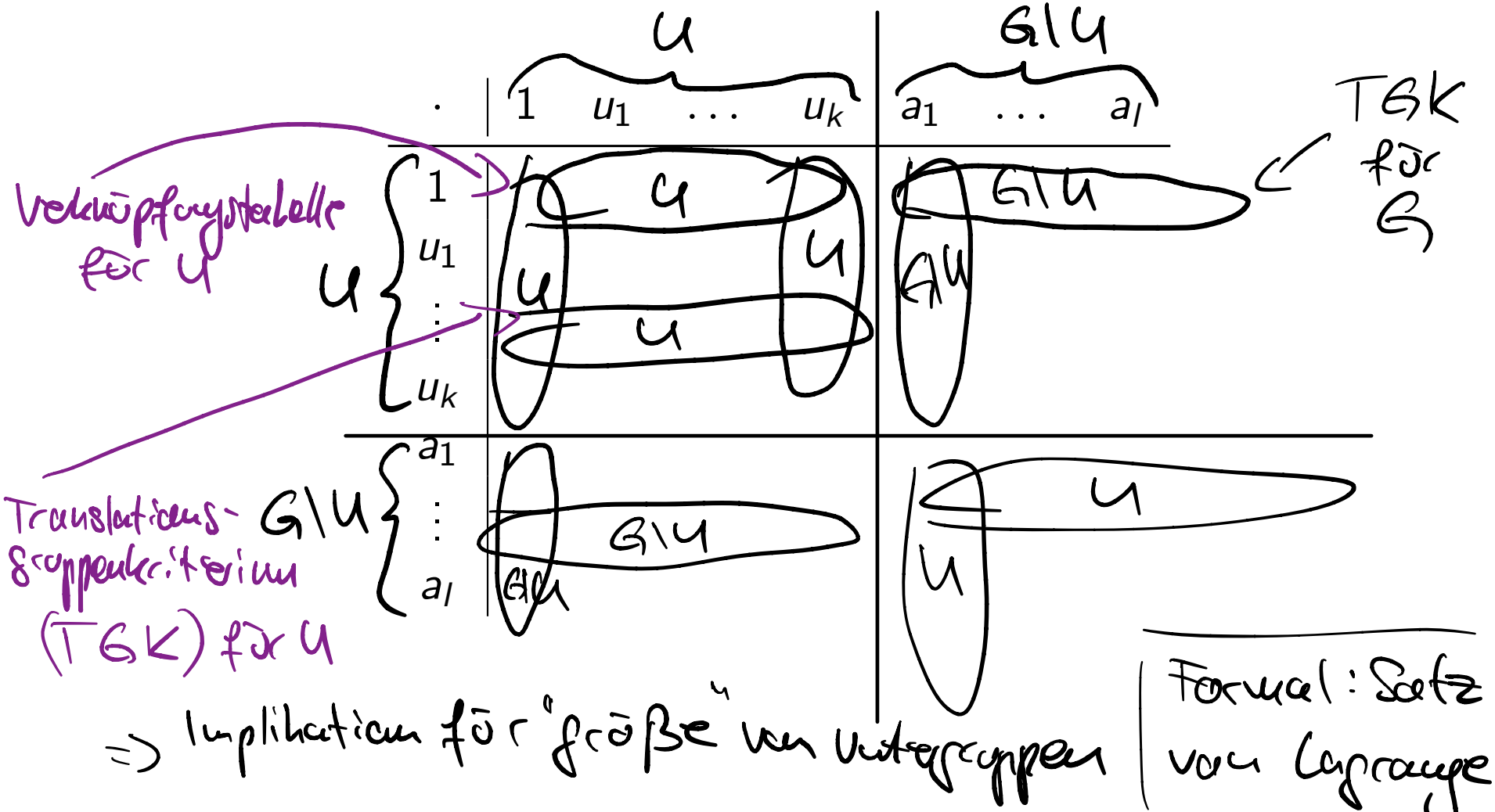
$$\langle a \rangle = \{ a^z \mid z \in \mathbb{Z} \}$$

(5) **Ordnung** $\operatorname{ord}(a)$ ist kleinstes $n \in \mathbb{N}$, so dass $a^n = 1$ (oder ∞)

$\Rightarrow \operatorname{ord}(1) = 1 \in \mathbb{N}$

Untergruppenstruktur in Verknüpfungstabellen

Es sei $(G, \cdot)$ eine (endliche) Gruppe und $(U, \cdot)$ eine Untergruppe mit $U = \{1, u_1, \ldots, u_k\}$. Wie ist die Verknüpfungstabelle strukturiert?



Untergruppen der S_3 in der Verknüpfungstabelle

Untergruppen der S_3

Siehe Vorlesungsmitschrift: $\{\sigma_0, \sigma_1, \sigma_2\}$, $\{\sigma_0, \sigma_3\}$, $\{\sigma_0, \sigma_4\}$, $\{\sigma_0, \sigma_5\}$

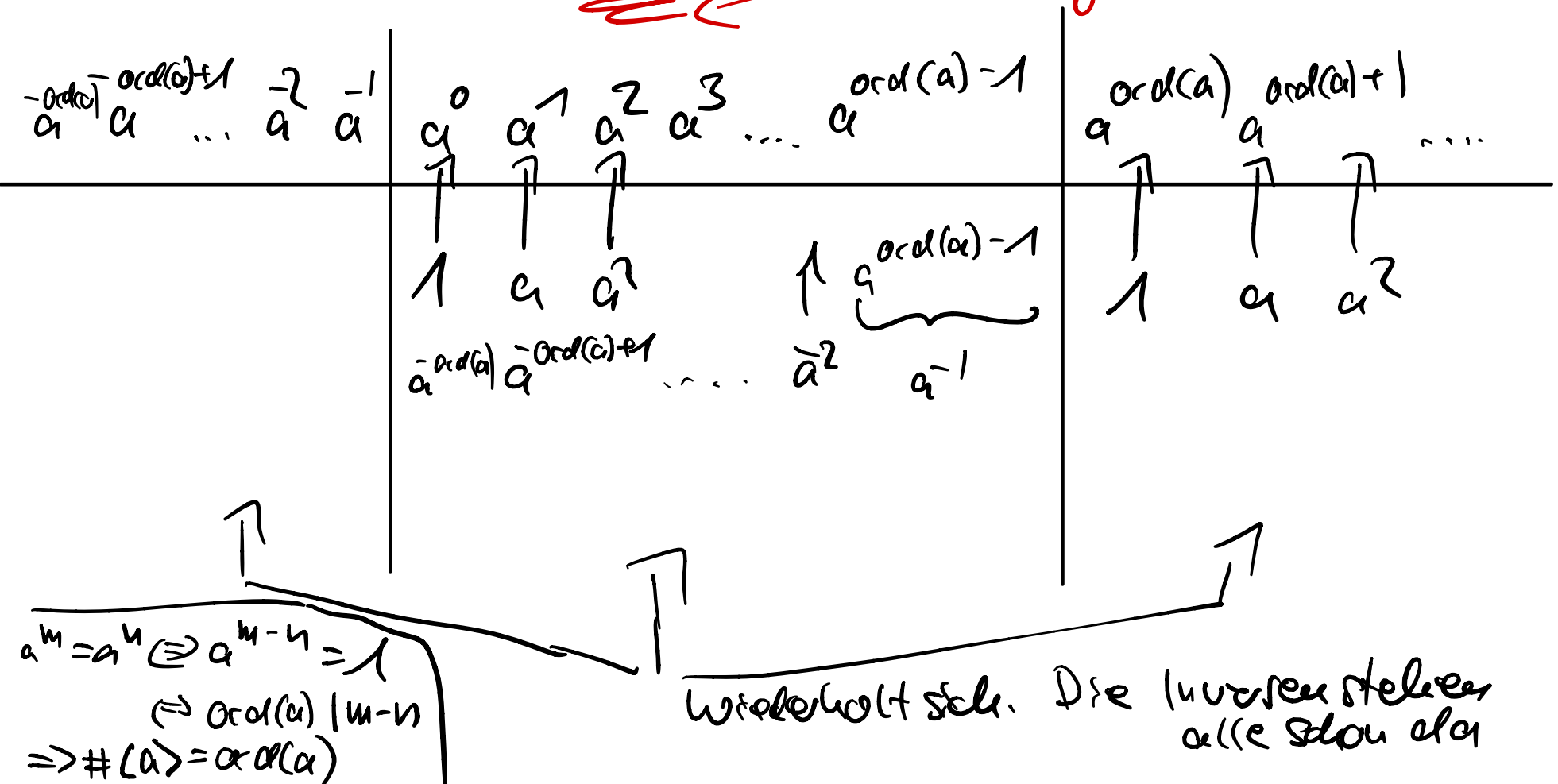
$\circ$	e	d	d^2	s_1	s_2	s_3
e	e	d	d^2	s_1	s_2	s_3
d	d	d^2	e	s_3	s_1	s_2
d^2	d^2	e	d	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	d	d^2
s_2	s_2	s_3	s_1	d^2	e	d
s_3	s_3	s_1	s_2	d	d^2	e

Visualisierung zyklisch erzeugter Gruppen

Es sei $(G, \cdot)$ eine Gruppe und $a \in G$ mit $\operatorname{ord}(a) \in \mathbb{N}$. Wie sieht $\langle a \rangle$ aus?

Wir wissen: $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$.

Visualisierung über $\mathbb{Z}$



Wahr/Falsch zu Untergruppen und Erzeugung

Gilt für allgemeine $(G, \cdot)$ Gruppe, $(U, \cdot)$ Untergr., $E, F \subseteq G$, $a \in G$:

(1) $\langle\emptyset\rangle = \emptyset$ Falsch, keine Gruppe, da kein neutrales Element ex.

(2) Für jedes $b \in \langle a\rangle$ ist $\langle b\rangle = \langle a\rangle$ Falsch, für $a \neq 1$ dann ist $\langle 1\rangle = \{1\} \neq \langle a\rangle$

(3) Für $E \subseteq F$ ist $\langle E\rangle \subseteq \langle F\rangle$
Ja, folgt direkt der Def. über Obermengenschnitt, oder aus der Darstellung

(4) Es gibt $(U, \cdot)$ mit $\langle u\rangle = U$ für alle $u \in U$
Klar, z.B. $U = \{e\}$, andere Bspl.

(5) Das größte Erzeugendensystem von G ist eindeutig.
Ja, das ist G selbst.

(6) Das kleinste Erzeugendensystem von G ist eindeutig.
Falsch, siehe z.B. $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$

(7) $\langle E\rangle \cup \langle G \setminus E\rangle$ ist mit $\cdot$ eine Untergruppe von G
Ja, da $E \subseteq \langle E\rangle$, $G\setminus E \subseteq \langle G\setminus E\rangle$ und $\langle E\rangle \cup \langle G\setminus E\rangle = G$

Spannend in Verbindung mit HA Woche...

(8) Ist G endlich erzeugt, so ist G endlich.
Bspl. $\mathbb{Z} = \langle 1\rangle$

Primgruppen

Satz

Es sei p eine Primzahl. Dann ist jede Gruppe $(G, \cdot)$ mit Ordnung p zyklisch und es ist $\operatorname{ord}(a) = p$ und $\langle a \rangle = G$ für alle $a \in G \setminus \{1_G\}$.

Beweis: Sei $a \in G \setminus \{1\}$. Dann ist $\langle a \rangle$ mit $\cdot$ eine nichttriviale UG von $(G, \cdot)$. Nach dem Satz von Lagrange gilt

$\operatorname{ord}(a) = \#\langle a \rangle \mid \#G = p$. $\Rightarrow \#\langle a \rangle \in \{1, p\}$ aber $\#\langle a \rangle \neq 1 \Rightarrow \langle a \rangle = G$ und $\operatorname{ord}(a) = p$. $\square$

Letzte Woche: Gruppe mit 5 Elementen ist abelsch. Das geht jetzt schneller!

5 Primzahl $\Rightarrow$ 5 Elem. Gruppen sind zyklisch $\Rightarrow$ Diese sind abelsch

Bspl. $(\underbrace{\mathbb{Z}_3}_{\{0,1,2\}}, \underbrace{+_3}_{\text{modulo plus}})$

$\langle 1 \rangle = \{1, 1+_3 1, 1+_3 1+_3 1\} = \{1, 2, 0\} = \mathbb{Z}_3$

$\langle 2 \rangle = \{2, 2+_3 2, 2+_3 2+_3 2\} = \{2, 1, 0\} = \mathbb{Z}_3$

Wiederholung Nebenklassen

Definition

Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$.

$a \sim^U b :\Leftrightarrow b \in a \star U$ $\qquad$ $a \,{}^U\!\sim b :\Leftrightarrow a \in U \star b$

$[a]_{\sim^U} = a \star U$ **Linksnebenklasse** $\qquad$ $[a]_{{}^U\!\sim} = U \star a$ **Rechtsnebenklasse**

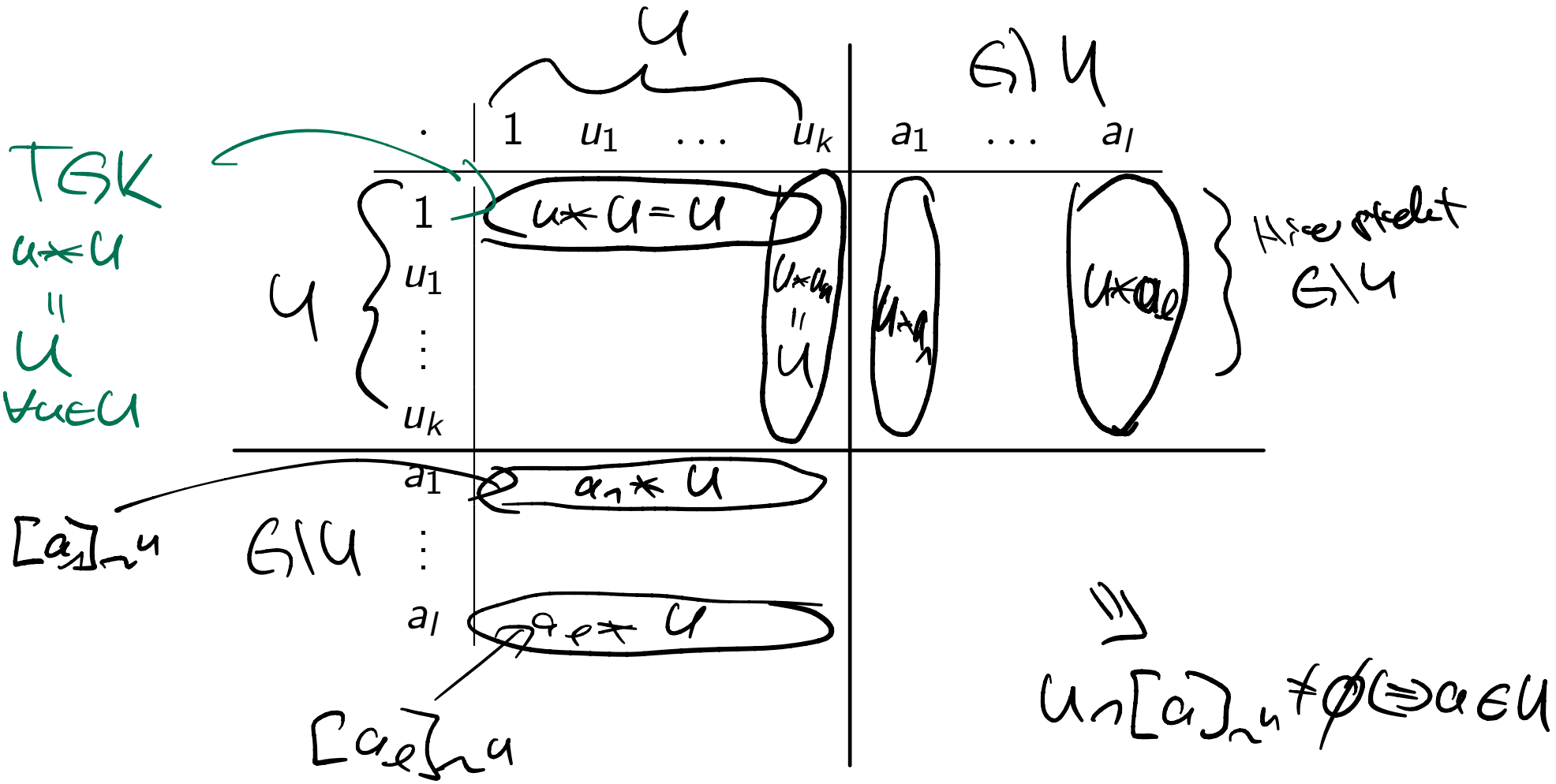
a links $\qquad$ a rechts

$a \star U = \{ a \star u \mid u \in U \}$

Was nicht aus U $\qquad$ Bild der Translation $a \star (\ )$ von U

Nebenklassen in Verknüpfungstabellen

Es sei $(G, \cdot)$ eine (endliche) Gruppe und $(U, \cdot)$ eine Untergruppe mit $U = \{1, u_1, \ldots, u_k\}$. Wo stehen die Nebenklassen?



Nebenklassen der S_3 in der Verknüpfungstabelle

Nebenklassen für $U = \{e, d, d^2\}$

$\circ$	e	d	d^2	s_1	s_2	s_3
e	e	d	d^2	s_1	s_2	s_3
d	d	d^2	e	s_3	s_1	s_2
d^2	d^2	e	d	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	d	d^2
s_2	s_2	s_3	s_1	d^2	e	d
s_3	s_3	s_1	s_2	d	d^2	e

Partitionierung in U und $G \setminus U$

Nebenklassen für $U = \{e, s_3\}$

$\circ$	e	d	d^2	s_1	s_2	s_3
e	e	d	d^2	s_1	s_2	s_3
d	d	d^2	e	s_3	s_1	s_2
d^2	d^2	e	d	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	d	d^2
s_2	s_2	s_3	s_1	d^2	e	d
s_3	s_3	s_1	s_2	d	d^2	e

Partitionierung in

verschiedene L/R NK

LNK $\{d, s_2\}, \{d^2, s_1\}, \{e, s_3\}$

RNK $\{d, s_1\}, \{d^2, s_2\}, \{e, s_3\}$

True/False zu Nebenklassen

Gilt für allgemeine $(G, \cdot)$ Gruppe, $(U, \cdot)$ Untergruppe, $a, b \in G$:

(1) $a \in [a]_{\sim U}$ Wahr, denn $1 \in U \Rightarrow a \cdot U \supseteq \{a \cdot 1\}$

(2) $1 \in [a]_{\sim U} \Leftrightarrow a \in U$: $1 \in [a]_{\sim_U} \Leftrightarrow a^{-1} \in U \Leftrightarrow a \in U$ also nicht i. A.

(3) $[a]_{\sim U}$ ist eine Untergruppe $\Leftrightarrow a \in U$, siehe (2) + Translationsresultat

(4) $[a]_{\sim \langle a \rangle} = \langle a \rangle$ Ja, denn $[a]_{\sim\langle a\rangle} = a \cdot \{a^z / z \in \mathbb{Z}\} = \{a^{z+1} / z \in \mathbb{Z}\} = \langle a \rangle$

(5) $[a]_{\sim \langle a \rangle} = [a]_{\langle a \rangle \sim}$ Ja, denn $[a]_{\sim\langle a\rangle} = a \cdot \langle a \rangle = \{a^{z+1} / z \in \mathbb{Z}\} = \langle a \rangle \cdot a = [a]_{\langle a\rangle\sim}$

(6) $[a]_{\sim U} = [b]_{\sim U} \Rightarrow a = b$ i. A. nicht, $[1]_{\sim \mathbb{Z}} = [5]_{\sim \mathbb{Z}}$

(7) $[a]_{\sim U} = [b]_{\sim U}\ \forall U \Rightarrow a = b$ Ja, denn $U = \{1\}$ ist UG

(8) $[a]_{\sim U_1} = [a]_{\sim U_2}\ \forall a \Rightarrow U_1 = U_2$ Ja, da $1 \in G$

Untergruppe induziert eine Äquivalenzrelation

Lemma

Es sei $(U, \star)$ eine Untergruppe der Gruppe $(G, \star)$. Dann gilt:

(1) $a \sim^U b \;:\Leftrightarrow\; b \in a \star U$ ist eine Äquivalenzrelation.

(2) Die Äquivalenzklassen sind $[a] = a \star U$.

(3) Jede Äquivalenzklasse ist gleichmächtig zu U.

Beweis. (1a) Reflexivität: $e \in U \Rightarrow a = a \star e \in a \star U \Rightarrow a \sim^U a$

(1b) Symmetrie: $a \sim^U b \Rightarrow a' \star b \in U \overset{\text{UUG}}{\Rightarrow} (a' \star b)' \in U \Rightarrow b' \star a \in U \Rightarrow a \in b \star U \Leftrightarrow b \sim^U a$

(1c) Transitiv: $a \sim^U b,\ b \sim^U c \Rightarrow a' \star b \in U$ und $b' \star c \in U \Rightarrow (a' \star b) \star (b' \star c) \in U$

$a' \star c \Rightarrow a \sim^U c$

(2) Direkt aus Def.

(3) $U \ni b \longmapsto a \star b \in a \star U$ Fasse als Abb. auf G. Surjektiv per Def.

Injektivität folgt aus Kürzungsregeln.

$a \star b_1 = a \star b_2 \overset{\text{kürzen}}{\Rightarrow} b_1 = b_2$

Ω

Homomorphismen

Definition

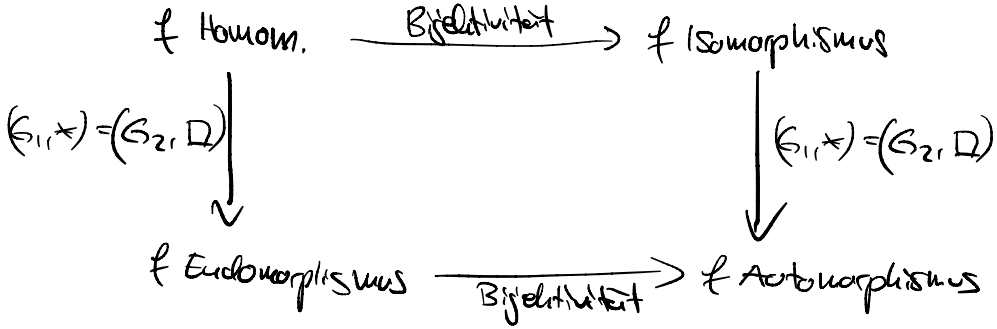
Es seien $(G_1, \star)$ und $(G_2, \square)$ zwei Gruppen und $f: G_1 \to G_2$

(1) f **Homomorphismus**, wenn strukturverträglich
$f(a \star b) = f(a) \square f(b)\ \forall a, b \in G_1$

(2) f **Isom.**, wenn strukturverträglich und bijektiv

(3) f **Endom.**, wenn strukturverträglich und $(G_1, \star) = (G_2, \square)$

(4) f **Autom.**, wenn Endom. und Isom.



Monoidisomorphismen bilden i.A. nicht neutrale Elemente aufeinander ab.
$(H, \cdot, e)$ ein Monoid. Füge weiteres neutrales Element $\tilde{e}$ hinzu. Betrachte Einbettung $(H, e) \xrightarrow{id} (H \cup \{\tilde{e}\}, \cdot, \tilde{e})$.

Direkte Konsequenzen aus der Strukturverträglichkeit

Es seien $(G_1, \star)$ und $(G_2, \square)$, $U_1 \subseteq G_1$, $U_2 \subseteq G_2$ Untergruppen, $E \subseteq G_1$, $a \in G_1$ und $f\colon G_1 \to G_2$ ein Homomorphismus.

(1) $f(a^n) = f(a)^n$ $f(a^n) = f(a \star a \star \ldots \star a \star a) = f(a \star a \star \ldots a) \cdot f(a)$

$= \ldots = f(a) \square f(a) \square \ldots \square f(a) = f(a)^n$

(2) $(f(a))^{-1} = f\left(a^{-1}\right)$ $f(a^{-1}) \square f(a) = f(a^{-1} \star a) = f(e_1) = e_2$ (Siehe Skript)

(3) $f(\langle E \rangle) = \langle f(E) \rangle$

Folgt direkt aus dem Darstellungssatz $f(a_1 \star a_2 \star \ldots \star a_n) = f(a_1) \square \ldots \square f(a_n)$ $n \in \mathbb{N}, a_i \in E \cup E^{-1}$

(4) $(U_1, \star)$ Untergruppe $\Rightarrow f(U_1)$ ist Untergruppe

$a, b \in U \Rightarrow f(a) \square f(b) = f(\underbrace{a \star b}_{\in U_1}) \in f(U_1)$ | $e_1 \in U_1 \Rightarrow e_2 = f(e_1) \in f(U_1)$, (2)

(5) $(U_2, \square)$ Untergruppe $\Rightarrow f^{-1}(U_2)$ ist Untergruppe

$a, b \in f^{-1}(U_2) \Rightarrow f(a \cdot b) = \underbrace{f(a)}_{\in U_2} \cdot \underbrace{f(b)}_{\in U_2} \in U_2$, $e_2 \in U_2 \Rightarrow e_1 \in f^{-1}(U_2)$ $a \in f^{-1}(U_2), f(a) \in U_2 \Rightarrow a^{-1} \in f^{-1}(U_2)$

Primgruppen 2

Satz

Es sei p eine Primzahl. Dann ist jede Gruppe $(G, \cdot)$ mit Ordnung p isomorph zu $(Z_p, +_p)$.

Gruppe! Bspl. 7.16 (V)

Beweis: $(G,\cdot)$ ist zyklisch mit $\langle a\rangle = G$ $\forall a \neq 1$. Sei $a \in G\setminus\{1\}$ und

$G = \langle a\rangle = \{a^z \mid z \in \mathbb{Z}\} = \{a^1, \dots, a^p\}$. $\mathbb{Z}_p \ni k \longmapsto a^k \in G$ ist bijektiv und

($a^{\mathrm{ord}(p)}$)

$f(k +_p l) = f((k+l) \bmod p) = a^{(k+l) \bmod p} \overset{\mathrm{ord}(a)=p}{=} a^{k+l} = a^k \cdot a^l = f(a^k)\cdot f(a^l)$

zeigt Strukturverträglichkeit.

□

Korollar: Zu jeder Primzahl p gibt es eine (bis auf Isomorphie) eindeutig bestimmte Gruppe mit $\#G = p$.