Wiederholung

Äquivalenzrelation

Wiederholung

Äquivalenzrelation

$\Vert$

Symmetrische

Wiederholung

Äquivalenzrelation

$$\Updownarrow$$

Symmetrische
Reflexive

Wiederholung

Äquivalenzrelation

$\Leftrightarrow$

Symmetrische
Reflexive
Transitive

Wiederholung

Äquivalenzrelation

$\Updownarrow$

Symmetrische
Reflexive
Transitive
Relation

Wiederholung

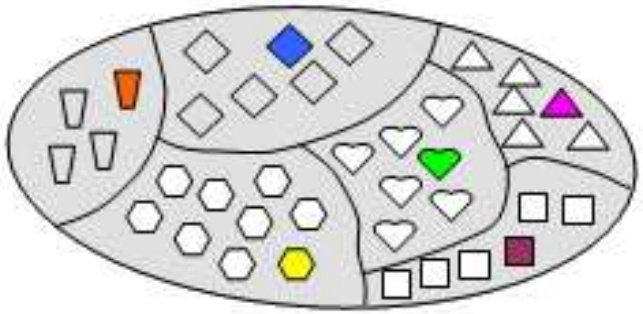
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Wiederholung

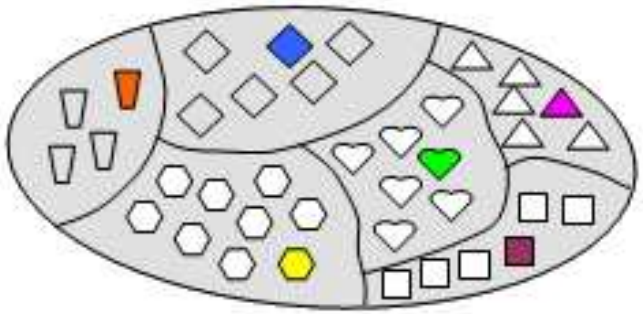
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

Wiederholung

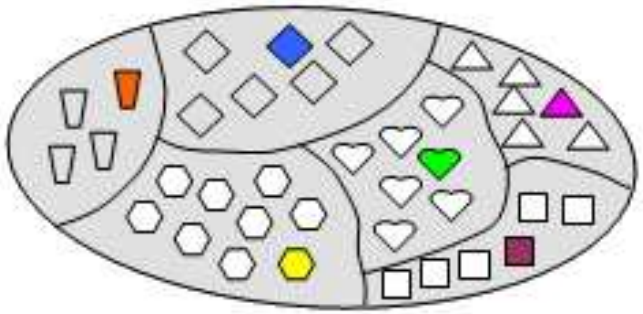
Äquivalenzrelation

$\Vert$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Wiederholung

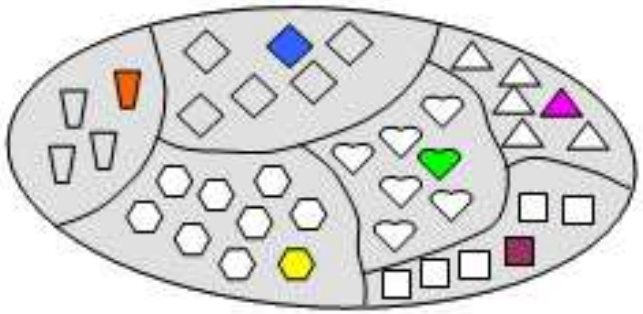
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Wiederholung

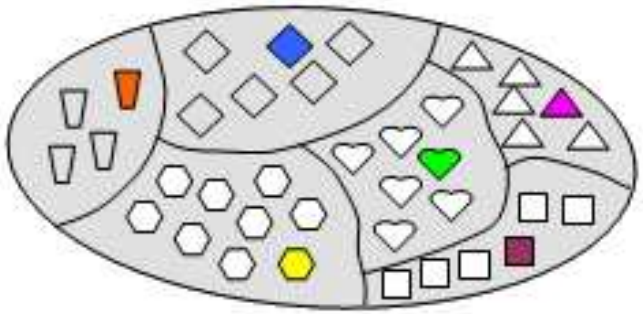
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow[\text{Fast dieselbe wie}]{\text{Satz 12}}$

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung:

Wiederholung

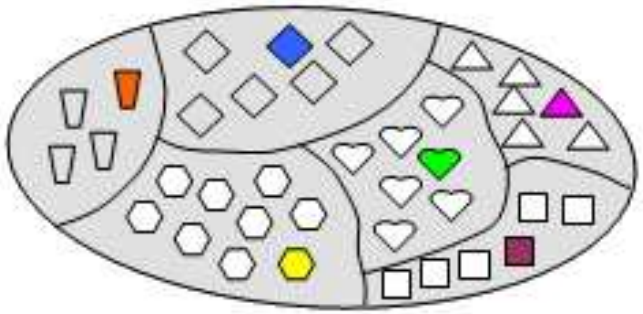
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow[\text{Fast dieselbe wie}]{\text{Satz 12}}$

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

Wiederholung

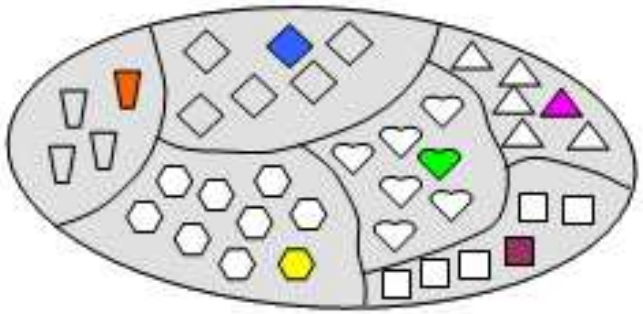
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

Wiederholung

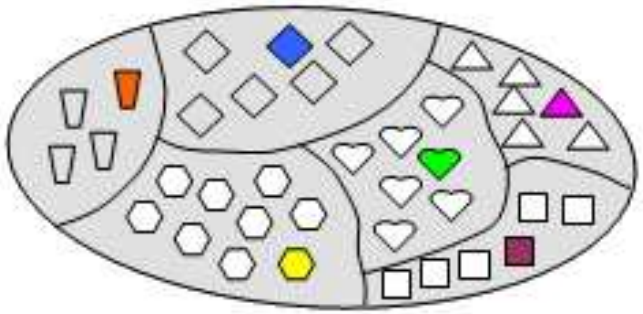
Äquivalenzrelation

$\Vert$

Symmetrische
Reflexive
Transitive
Relation

$\xleftarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

$\#G/H$ heißt Index von Untegruppe (kann $= \infty$ sein).

Wiederholung

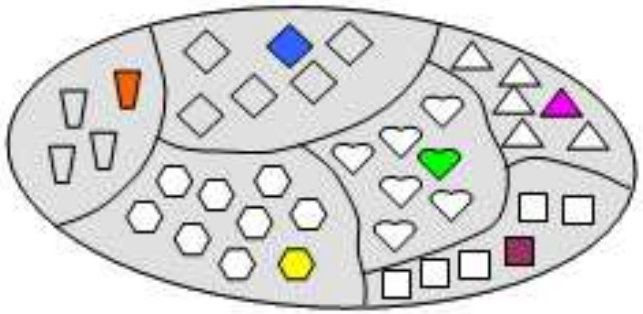
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

$\#G/H$ heißt Index von Untegruppe (kann $= \infty$ sein).

Aus Beweis des Satzes von Largange:

Wiederholung

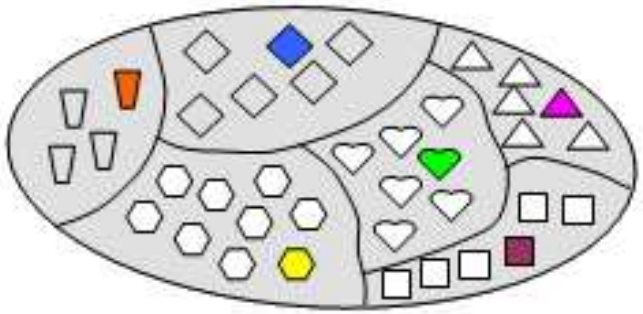
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftarrow{\text{Satz 12}}$
Fast dieselbe wie

Zerlegung



Für eine Untergruppe
$H \subseteq G$

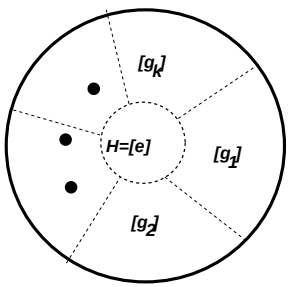
$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

$\#G/H$ heißt Index von Untegruppe (kann $= \infty$ sein).

Aus Beweis des Satzes von Largange:
$\#G = Index(G) \cdot \#H$.



Wiederholung

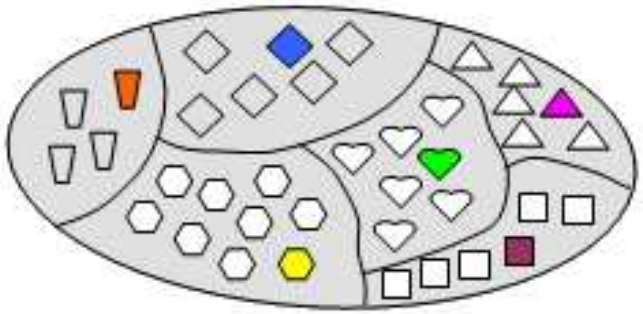
Äquivalenzrelation

$\|$

Symmetrische
Reflexive
Transitive
Relation

$\xleftrightarrow[\text{Fast dieselbe wie}]{\text{Satz 12}}$

Zerlegung



Für eine Untergruppe
$H \subseteq G$

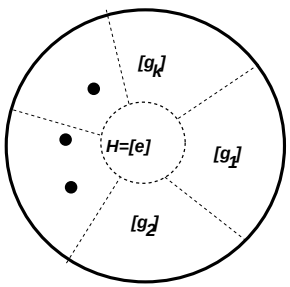
$\xrightarrow{\text{können wir}}$

Eine Äquivalenzrelation auf G definieren:
$g_1 \sim g_2 \iff hg_1 = g_2$ für ein $h \in H$

Bezeichnung: Die Menge von Äquivalenzklassen (bez. von $\sim$) wird G/H bezeichnet.

$\#G/H$ heißt Index von Untegruppe (kann $= \infty$ sein).

Aus Beweis des Satzes von Largange:
$\#G = Index(G) \cdot \#H$.



Frage: Welche Struktur erbt G/H?

Satz 15

Satz 15 *Ist H ein Normalteiler von G,*

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$.*

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung:

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet;

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$“ ist wohldefiniert

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).
(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).
(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i):

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $g_1' \sim g_1 \quad \text{d.h. } g_1' = h_1 g_1$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $g_1' \sim g_1 \quad \text{d.h. } g_1' = h_1 g_1$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$g_1' g_2' =$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$g_1' g_2' = h_1 g_1 h_2 g_2$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2$$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2$$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2$$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen,

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii)

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3]$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] =$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] =$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g]$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] =$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=}$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

(G4) Ist G abel'sch,

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

(G4) Ist G abel'sch, so ist $[g_1] \cdot [g_2] \overset{\text{Def}}{=}$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

(G4) Ist G abel'sch, so ist $[g_1] \cdot [g_2] \overset{\text{Def}}{=} [g_2 \cdot g_1] =$

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

(G4) Ist G abel'sch, so ist $[g_1] \cdot [g_2] \overset{\text{Def}}{=} [g_2 \cdot g_1] = [g_2] \cdot [g_1]$.

Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$. Ferner gilt: ist G abel'sch, so ist G/H auch abel'sch.*

Bezeichnung: Die Äquivalenzklassen von g werden oft Hg bezeichnet; $Hg := \{hg \mid h \in H\}$. Die Gruppe G/H heißt Faktorgruppe der G bzgl. H.

Beweis: Z.z.: (i) „$\cdot$" ist wohldefiniert (hängt nicht von Wahl von $g_1' \in [g_1]$ und $g_2' \in [g_2]$ ab).

(ii) hat die Eigenschaften (G1, G2, G3 und (falls G abe'sch) G4).

(i): Seien $\begin{array}{ll} g_1' \sim g_1 & \text{d.h. } g_1' = h_1 g_1 \text{ für ein } h_1 \in H \\ g_2' \sim g_2 & \text{d.h. } g_2' = h_2 g_2 \text{ für ein } h_2 \in H \end{array}$. Dann ist

$$g_1' g_2' = h_1 g_1 h_2 g_2 \overset{\text{Def. 9}}{=} h_1 g_1 h_2 \underbrace{g_1^{-1} g_1}_{e} g_2 = h_1 \underbrace{g_1 h_2 g_1^{-1}}_{h' \in H} g_1 g_2 = h g_1 g_2 \sim g_1 g_2.$$

Also, wenn wir statt g_1, g_2 andere $g_1' \in [g_1]$, $g_2' \in [g_2]$ nehmen, wird das Ergebniss $[g_1] \cdot [g_2]$ nicht geändert. (ii) :

(G1) $([g_1] \cdot [g_2]) \cdot [g_3] = [g_1 \cdot g_2] \cdot [g_3] = [(g_1 \cdot g_2) \cdot g_3] = [g_1 \cdot (g_2 \cdot g_3)] = [g_1] \cdot ([g_2] \cdot [g_3])$.

(G2) $[e] \cdot [g] \overset{\text{Def}}{=} [e \cdot g] = [g]$.

(G3) $[g^{-1}] \cdot [g] \overset{\text{Def}}{=} [g^{-1} \cdot g] = [e]$.

(G4) Ist G abel'sch, so ist $[g_1] \cdot [g_2] \overset{\text{Def}}{=} [g_2 \cdot g_1] = [g_2] \cdot [g_1]$.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$,

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,]

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv \pmod q$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1]$

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod 5$ schreiben.

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod 5$ schreiben.

(Weil $9 = -1 + 2 \cdot 5$.)

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv \pmod{q}$ oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod{5}$ schreiben.

(Weil $9 = -1 + 2 \cdot 5$.)

Rechnen is Z_q:

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod 5$ schreiben.

(Weil $9 = -1 + 2 \cdot 5$.)

Rechnen is Z_q: $q + 1 \equiv 1 \pmod q$,

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod 5$ schreiben.

(Weil $9 = -1 + 2 \cdot 5$.)

Rechnen is Z_q: $q + 1 \equiv 1 \pmod q$, $12 + 3 \equiv 0 \pmod 5$,

Wicht. Bsp.: Zyklische (Unter)Gruppen

Sei $G = (\mathbb{Z}, +)$ und $H = q\mathbb{Z} = \{k \cdot q \mid k \in \mathbb{Z}\}$, wobei $q \in \mathbb{N}$. Da $(\mathbb{Z}, +)$ abel'sch ist, ist $q\mathbb{Z}$ ein Normalteiler (s. Bsp. Vorl. 6).

Def. 10 Die Faktorgruppe $\mathbb{Z}/q\mathbb{Z}$ heißt Restklassengruppe und wird $\mathbb{Z}_q$ bezeichnet.

Frage: Was ist „$\sim$“ ?

$m \sim n \iff \exists p \in q\mathbb{Z}$ mit $p + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $kq + m = n$

$\iff \exists k \in \mathbb{Z}$ mit $n - m = kq$.

Hist. Bez: In der Gruppe $\mathbb{Z}_q$ „vergesst“ man oft [,] und ersetzt oft $=$ mit $\equiv$ (mod q) oder mit $\overset{\text{mod } q}{\equiv}$.

Z.Bsp., für $q = 5$ die (korrekte) Gleichung

$[7] + [2] = [-1] \overset{\text{Kann man}}{\longleftrightarrow} 7 + 2 \equiv -1 \pmod 5$ schreiben.

(Weil $9 = -1 + 2 \cdot 5$.)

Rechnen is Z_q: $q + 1 \equiv 1 \pmod q$, $12 + 3 \equiv 0 \pmod 5$,

$23 - 12 \equiv -1 \pmod{12}$.

Def 11

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$,

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$,

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$, ... auch in H.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$, ... auch in H.
Ähnlich: $e := a^0 \in H$,

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$, ... auch in H.
Ähnlich: $e := a^0 \in H$, $a^{-1} \in H$, $a^{-2} := a^{-1} \cdot a^{-1}$, ... Also, für $A = \{a\}$

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$, ... auch in H. Ähnlich: $e := a^0 \in H$, $a^{-1} \in H$, $a^{-2} := a^{-1} \cdot a^{-1}$, ... Also, für $A = \{a\}$ enthält $\langle a \rangle$ alle (auch negative) Potenzen von a.

Def 11 Sie G eine Gruppe, und $A \subset G$ eine Teilmenge von G. Sei $\mathbb{A}$ die Menge aller Untegruppen, die A enthalten. Z.Bsp. ist $G \in \mathbb{A}$.
Dann ist $\langle A \rangle := \bigcap_{H \in \mathbb{A}} H$ nach Satz 6 eine Untergruppe. Sie heißt von A erzeugte Untergruppe .

Bemerkung Ist $a \in H$, so sind $a \cdot a := a^2$, $a \cdot a \cdot a := a^3$, ... auch in H. Ähnlich: $e := a^0 \in H$, $a^{-1} \in H$, $a^{-2} := a^{-1} \cdot a^{-1}$, ... Also, für $A = \{a\}$ enthält $\langle a \rangle$ alle (auch negative) Potenzen von a.

Lemma 6

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung:

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis:

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0,$
- $k < 0, m < 0,$
- $k \geq 0,\ m < 0,\ |m| \geq k,$
- $k \geq 0,\ m < 0,\ |m| < k,$
- $k < 0,\ m \geq 0,\ m \geq |k|,$
- $k < 0,\ m \geq 0,\ m < |k|$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k < 0, m < 0$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle,

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k < 0, m < 0$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k < 0, m < 0$,
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0$, $m \geq 0$, $m \geq |k|$,
- $k < 0$, $m \geq 0$, $m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$a^k \cdot a^m =$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k < 0, m < 0$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} =$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$,
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} =$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0, m < 0$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}}$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$,
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots =$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0, m < 0$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii)

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$, Wir
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k =$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$,
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \right)^{-1}$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$,
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=}$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0, m < 0$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}}$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0, m < 0$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}}.$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}} = a^{-k}.$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid \ n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid \ n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0,\ m < 0,\ |m| < k$,
- $k < 0, m < 0$,
- $k < 0,\ m \geq 0,\ m \geq |k|$,
- $k \geq 0,\ m < 0,\ |m| \geq k$,
- $k < 0,\ m \geq 0,\ m < |k|$

Wir beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}} = a^{-k}.$$ Analog, ist

$$(a^{-k})^{-1} =$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$, Wir
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}} = a^{-k}.$$ Analog, ist

$$(a^{-k})^{-1} = \left(\underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=}$$

Lemma 6 Für jedes a jeder Gruppe G ist $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G.

Bemerkung: Nicht alle a^n sind verschieden (Bsple kommen) .

Beweis: Z.z.: die Menge $\{a^n \mid n \in \mathbb{Z}\}$ ist abgeschlossen bzgl. (i) Multiplikation und (ii) Invertieren.

(i): Es gibt die folgende Möglichkeiten für k, m:

- $k \geq 0, m \geq 0$,
- $k \geq 0$, $m < 0$, $|m| < k$,
- $k < 0, m < 0$,
- $k < 0$, $m \geq 0$, $m \geq |k|$, Wir
- $k \geq 0$, $m < 0$, $|m| \geq k$,
- $k < 0$, $m \geq 0$, $m < |k|$

beweisen (i) für die erste 2 Fälle, Beweis für andere Fälle ist analog.

$$a^k \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k+m \text{ Stück}}$$

$$a^k \cdot a^{-m} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m \text{ Stück}} = \underbrace{a \cdot \ldots \cdot a}_{k-1 \text{ Stück}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{m-1 \text{ Stück}} = \ldots = \underbrace{a \cdot \ldots \cdot a}_{k-m \text{ Stück}} .$$

(ii) Für $k \geq 0$ ist

$$a^k = \left(\underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}} = a^{-k}. \text{ Analog, ist}$$

$$(a^{-k})^{-1} = \left(\underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ Stück}}\right)^{-1} \overset{\text{Folg. aus Satz. 2}}{=} \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} = a^k.$$

Lemma 7 Sei G eine Gruppe.

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2).

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden.

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden. Dann gilt: $\{e, a, a^2, ..., a^{n-1}\}$ ist eine Untergruppe von G.

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden. Dann gilt: $\{e, a, a^2, ..., a^{n-1}\}$ ist eine Untergruppe von G.

Beweis:

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden. Dann gilt: $\{e, a, a^2, ..., a^{n-1}\}$ ist eine Untergruppe von G.

Beweis: $a^k \cdot a^m = \begin{cases} a^{k+m} & \text{falls } k+m < n \end{cases}$

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden. Dann gilt: $\{e, a, a^2, ..., a^{n-1}\}$ ist eine Untergruppe von G.

Beweis: $a^k \cdot a^m = \begin{cases} a^{k+m} & \text{falls } k+m < n \\ a^{k+m-n} & \text{falls } k+m \geq n \end{cases}$

Lemma 7 Sei G eine Gruppe. $a \in G$ habe Ordnung $n < \infty$ (s. Blatt 3, Hausaufgabe 2). D.h., $a^n = e$, und die Elementen $\{e, a, a^2, ..., a^{n-1}\}$ sind verschieden. Dann gilt: $\{e, a, a^2, ..., a^{n-1}\}$ ist eine Untergruppe von G.

Beweis: $a^k \cdot a^m = \begin{cases} a^{k+m} & \text{falls } k+m < n \\ a^{k+m-n} & \text{falls } k+m \geq n \end{cases}$

$(a^k)^{-1} = a^{n-k}$. □

Def 12

Def 12 Eine Gruppe G heißt zyklisch,

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten:

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$,

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.

$\overset{\text{Lemma 6}}{\Longrightarrow}$

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.

$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp.

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe,

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + ... + 1}_{n \text{ mal}} = n$

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + ... + 1}_{n \text{ mal}} = n$ und $1^{-n} = \underbrace{-1 + (-1) + ... + (-1)}_{n \text{ mal}} = -n$.)

Bsp.

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + ... + 1}_{n \text{ mal}} = n$ und $1^{-n} = \underbrace{-1 + (-1) + ... + (-1)}_{n \text{ mal}} = -n$.)
Bsp. $(q\mathbb{Z}, +)$ ist eine zyklische Gruppe,

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ mal}} = n$ und $1^{-n} = \underbrace{-1 + (-1) + \ldots + (-1)}_{n \text{ mal}} = -n$.)
Bsp. $(q\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger q.
Bsp. $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$,

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ mal}} = n$ und $1^{-n} = \underbrace{-1 + (-1) + \ldots + (-1)}_{n \text{ mal}} = -n$.)
Bsp. $(q\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger q.
Bsp. $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \cdot)$, $\mathcal{S}_n$

Def 12 Eine Gruppe G heißt zyklisch, wenn für $a \in G$ gilt $\langle a \rangle = G$.

In Worten: es gibt ein Element $a \in G$, sodass G selbst die einzige Untergruppe von G ist, die a enthält.
$\overset{\text{Lemma 6}}{\Longrightarrow}$ $\exists$ ein Element (Z.B. a) (den „Erzeuger“ der Gruppe), sodass jedes Element von G eine Potenz von a ist (negative Potenzen sind auch zugelassen).

Bsp. Endliche zyklische Gruppen, s. Vorl. 3.
Bsp. $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger 1 (weil jedes $n \in \mathbb{Z}$ ist $1^n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ mal}} = n$ und $1^{-n} = \underbrace{-1 + (-1) + \ldots + (-1)}_{n \text{ mal}} = -n$.)
Bsp. $(q\mathbb{Z}, +)$ ist eine zyklische Gruppe, mit Erzeuger q.
Bsp. $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \cdot)$, $\mathcal{S}_n$ (für $n \geq 2$) sind keine zyklische Gruppen

Klassifikationssatz für zyklische Gruppen

Satz 16

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph.

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis.

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich:

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph.
Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.**

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph.
Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen:

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph.
Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$.

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: [0], [1], [2], [3], [4]. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest),

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: [0], [1], [2], [3], [4]. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: [0], [1], [2], [3], [4]. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden:

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i-j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i-j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q:

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i-j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:*

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:* $[0]$, ... , $[q-1]$*:*

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:* $[0]$, ... , $[q-1]$*:* jedes $a \in \mathbb{Z}$ kann man in Form $k \cdot q + r$ darstellen, wobei $0 \leq r < q$

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:* $[0]$, ... , $[q-1]$*:* jedes $a \in \mathbb{Z}$ kann man in Form $k \cdot q + r$ darstellen, wobei $0 \leq r < q$(dividieren mit Rest),

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:* $[0]$, ... , $[q-1]$*:* jedes $a \in \mathbb{Z}$ kann man in Form $k \cdot q + r$ darstellen, wobei $0 \leq r < q$(dividieren mit Rest), also $[a] = [r]$,

Klassifikationssatz für zyklische Gruppen

Satz 16 Es gilt:

(a) $\mathbb{Z}_q$ ist zyklisch

(b) $\mathbb{Z}_q$ hat genau q Elementen $[0], [1], ..., [q-1]$

(c) Jede zyklische Gruppe G mit $\#G = q$ ist zur Gruppe $\mathbb{Z}_q$ isomorph. Jede unendliche zyklische Gruppe ist zu $\mathbb{Z}$ isomorph.

Beweis. (a) offensichtlich: $[1]$ erzeugt $\mathbb{Z}_q$ (weil $[n] = \underbrace{[1] + ... + [1]}_{n \text{ Stuck}}$).

(b): **Bsp.** Bzgl. $\overset{\text{mod } 5}{\equiv}$ gibt es 5 Äquivalenzklassen: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. Tatsächlich, jedes $a \in \mathbb{Z}$ kann man in der Form $k \cdot 5 + r$ darstellen,wobei $0 \leq r < 5$(dividieren mit Rest), also $[a] = [r]$, und diese 5 Teilmengen sind verschieden: Ist $[i] \overset{\text{mod } 5}{\equiv} [j]$ für $i, j \in \{0, 1, 2, 3, 4\}$, so ist $i - j = k \cdot 5$, also $\underbrace{|i - j|}_{\leq 4} = |k| \cdot 5$, also $k = 0$, und deswegen $i = j$.

Analog für alle q: *Bzgl.* $\overset{mod\ q}{\equiv}$ *gibt es* q *Äquivalenzklassen:* $[0]$, ... , $[q-1]$*:* jedes $a \in \mathbb{Z}$ kann man in Form $k \cdot q + r$ darstellen, wobei $0 \leq r < q$(dividieren mit Rest), also $[a] = [r]$, und diese q Teilmengen sind verschieden.

(c):

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.

Schema:

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3),

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11.,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert:

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist,

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$\phi(k_1) = \phi(k+m \cdot q)$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} =$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right)$$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot \ldots \cdot e}_{m \text{ Stück}} \right)$$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n])$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) \ = \phi([m + n])$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} =$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n.$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv:

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) =$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot \ldots \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv:

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot \ldots \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv: $\Longleftarrow$ Lemma 6.

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv: $\Longleftarrow$ Lemma 6.

Beweis für $\#G = \infty$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) := a^{k+m\cdot q} = \underbrace{a\cdot\ldots\cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a\cdot\ldots\cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a\cdot\ldots\cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a\cdot\ldots\cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e\cdot..\cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv: $\Longleftarrow$ Lemma 6.
Beweis für $\#G = \infty$ ist analog ($\phi : \mathbb{Z} \to G$, $\phi(n) = a^n$

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv: $\Longleftarrow$ Lemma 6.
Beweis für $\#G = \infty$ ist analog ($\phi : \mathbb{Z} \to G$, $\phi(n) = a^n$ ist ein Isomorphismus).

(c): Jede zyklische Gruppe G mit $\#G = q$ ist zu $\mathbb{Z}_q$ isomorph.
Schema: Wir definiren eine $\phi : \mathbb{Z}_q \to G$ und zeigen, dass ϕ wohldefiniert ist, dass ϕ Homorphismus ist, dass ϕ injektiv ist, und dass ϕ surjektiv ist.
Sei a der Erzeuger von G. Dann ist $G = \{e, a^1, ..., a^{q-1}\}$. Tatsächlich, die Elementen $e, a^1, ..., a^{q-1}$ sind verschieden, sonst gibt es $q' < q$ mit $a^{q'} = e$ (Hausaufgabe 2a, Blatt 3), und deswegen ist nach Lemma 7 $\{e, a^1, ..., a^{q-1}\}$ eine Untergruppe von G. Dann ist $\langle a \rangle \neq G$, s. Def. 11., und G ist nicht von a erzeugt (s. Def. 12).
Wir betrachten die Abbildung $\phi : \mathbb{Z}_q \to G$, $\phi([k]) := a^k$.
ϕ ist wohldefiniert: falls $k_1 = k + m \cdot q$ ist, so ist

$$\phi(k_1) = \phi(k+m\cdot q) \ := a^{k+m\cdot q} = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{\underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{q \text{ Stück}}}_{m \text{ Stück}} \right) = \underbrace{a \cdot \ldots \cdot a}_{k \text{ Stück}} \cdot \left(\underbrace{e \cdot .. \cdot e}_{m \text{ Stück}} \right) = a^k.$$

ϕ ist ein Homomorphismus:
$\phi([m] + [n]) = \phi([m + n]) = a^{m+n} = a^m \cdot a^n$.
ϕ ist injektiv: Tatsächlich, $\phi([0]) = e$, $\phi([1]) = a$,..., $\phi([q-1]) = a^{q-1}$ sind alle verschieden, s. oben.
ϕ ist surjektiv: $\Longleftarrow$ Lemma 6.
Beweis für $\#G = \infty$ ist analog ($\phi : \mathbb{Z} \to G$, $\phi(n) = a^n$ ist ein Isomorphismus).

Sei $H \subseteq G$ ein Normalteiler.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G,*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus.*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis:

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) =$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] =$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] =$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=}$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$=$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} =$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\}$

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$,

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz)

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus.*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$,*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) =$*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten:

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.

Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

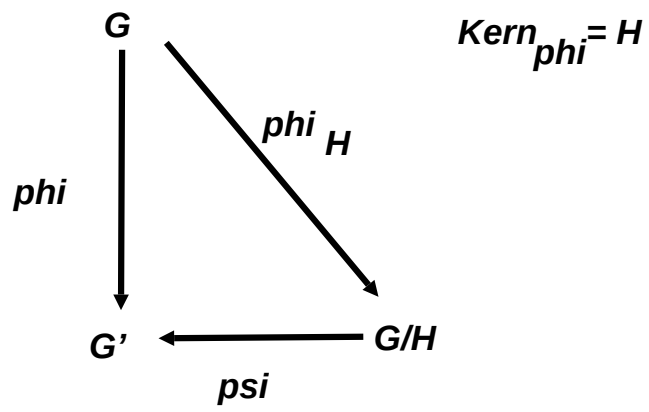
Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Sei $H \subseteq G$ ein Normalteiler.

Wiederholung: Satz 15 *Ist H ein Normalteiler von G, so ist G/H eine Gruppe (bezüglich der Multiplikations $[g_1] \cdot [g_2] := [g_1 \cdot g_2]$).*

Man betrachten die Abbildung $\phi_H : G \to G/H$, $\phi_H(g) := [g]$.

Lemma 8 *Die Abbildung ϕ_H ist ein Homomophismus. Ferner gilt: $Kern_{\phi_H} = H$ und $Bild_{\phi_H} = G/H$.*

Beweis: $\phi_H(g_1 \cdot g_2) = [g_1 \cdot g_2] = [g_1] \cdot [g_2] = \phi_H(g_1) \cdot \phi_H(g_2)$.

$Kern_\phi \overset{Def}{=} \{g \in G \mid [e] = \phi_H(g)\}$

$= \{g \in G \mid [e] = [g]\} = \{g \in G \mid he = g \text{ für ein } h \in H\} = H$.

Offensichtlich, $Bild_\phi = G/H$, da jedes $[g]$ ist $\phi_H(g)$. □

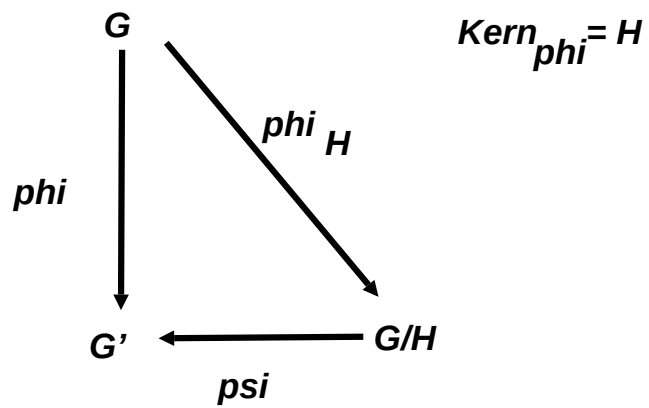
Bezeichung Die Abbildung ϕ_H heißt kanonische Projektion.

Sei $\phi : G \to G'$ ein Homomophismus.

Wiederholung:Satz 14: $Kern_\phi$ ist ein Normalteiler.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

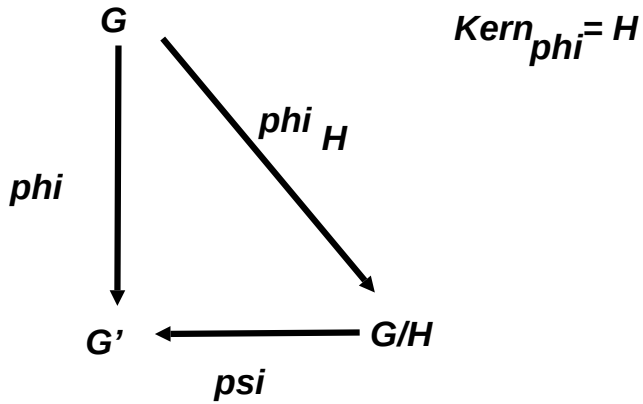
In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Also, bis zum Isomorphismus, ist jeder surjektiver Homomorphismus die kanonische Projektion.

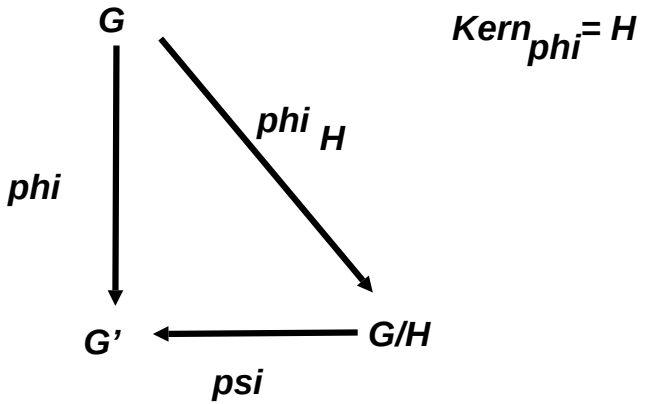
Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

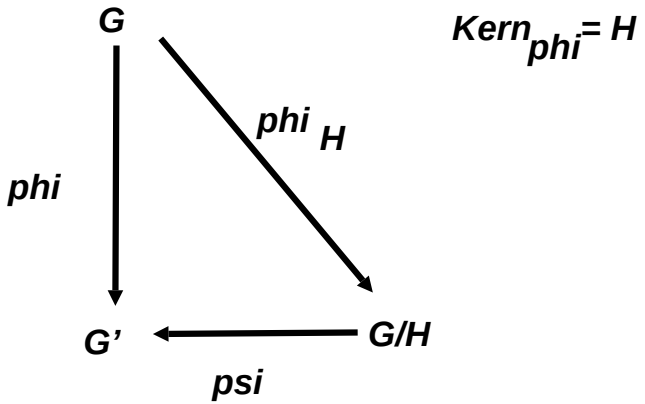
In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis:

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

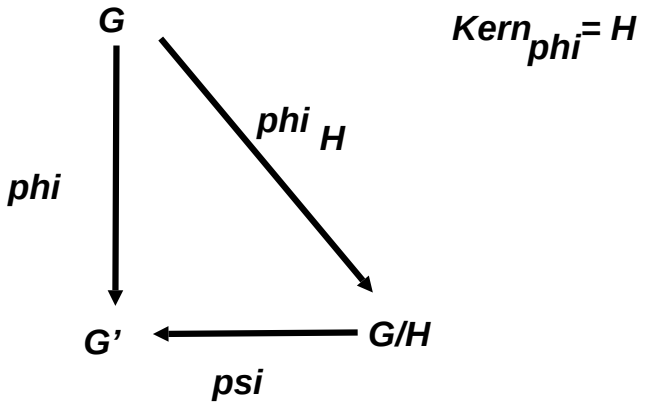
In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert:

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

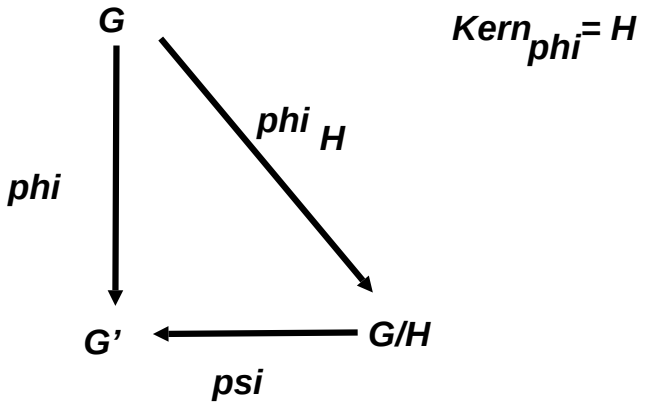
In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$,

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.

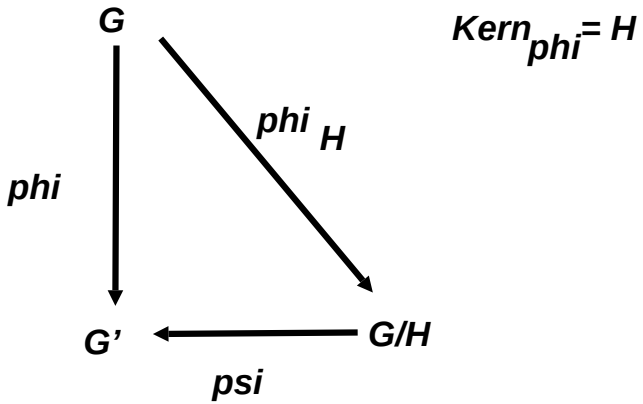


Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) =$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.

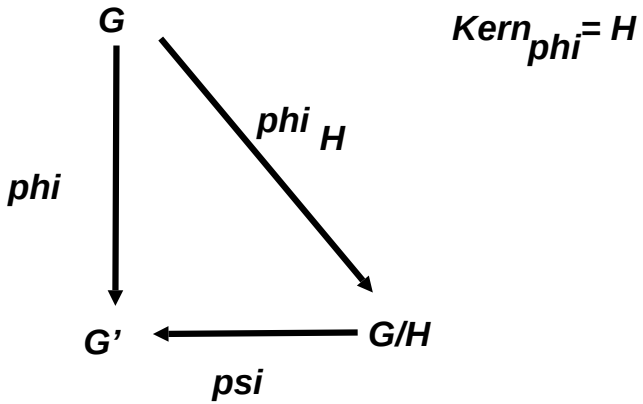


Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g)$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.

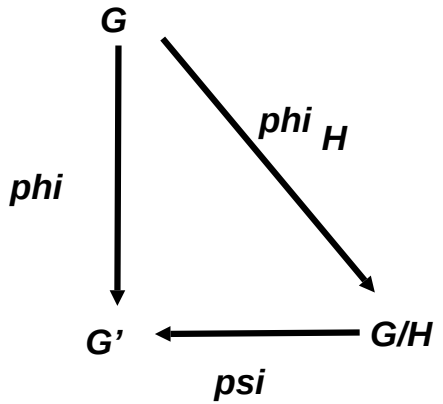


Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



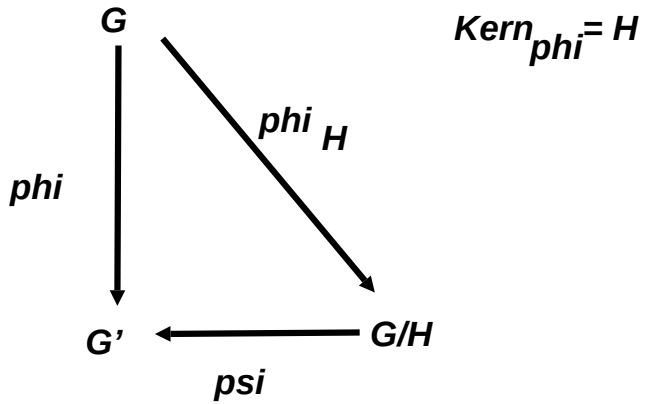
Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

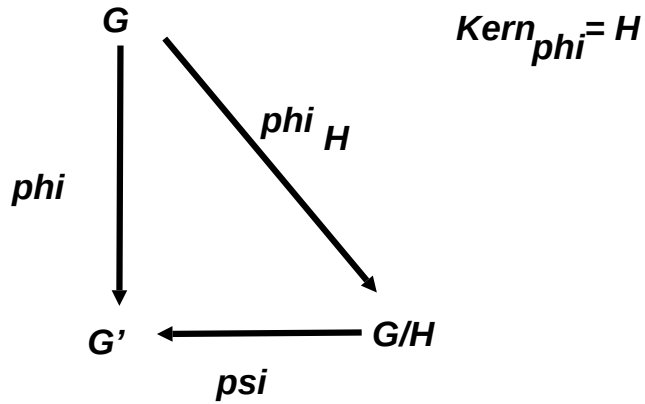
deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) =$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

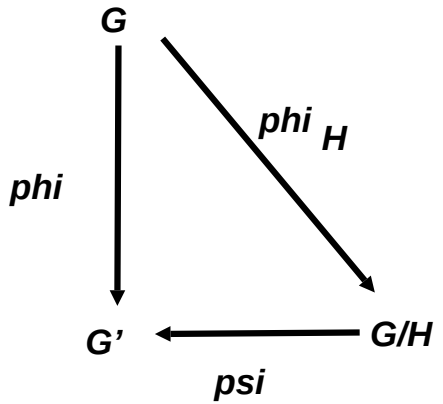
deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) =$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

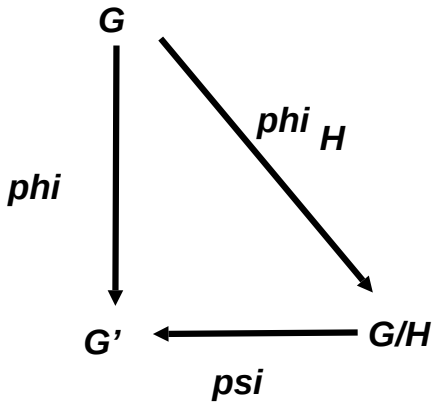
deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) =$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

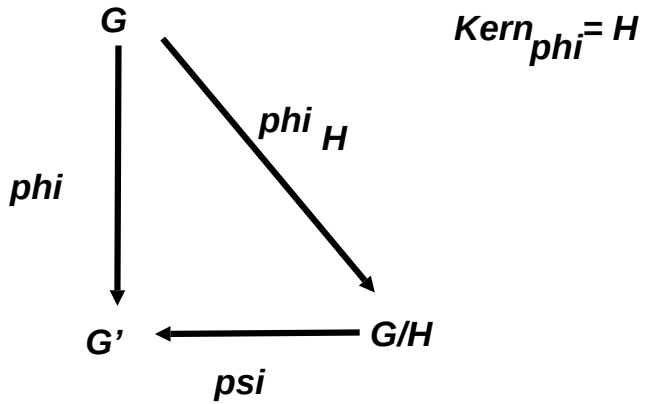
deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2)$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

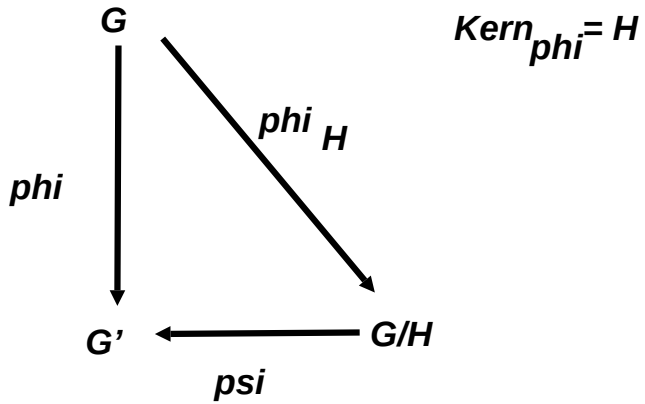
ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

ψ ist surjektiv:

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

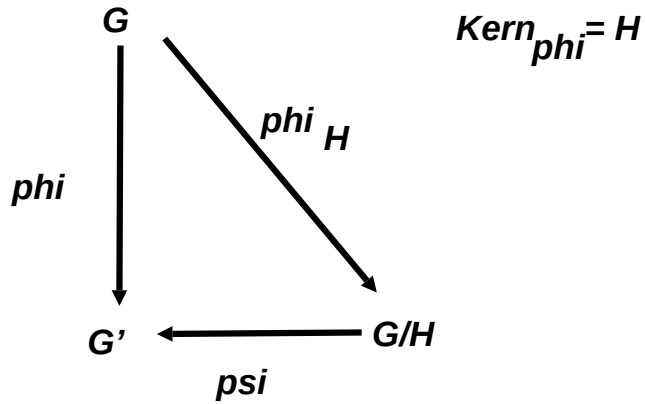
ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

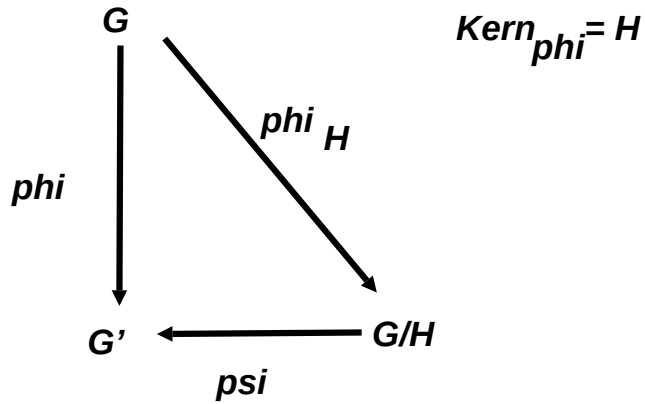
ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.

Dann ist $\psi([g]) = y$.

ψ ist injektiv:

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

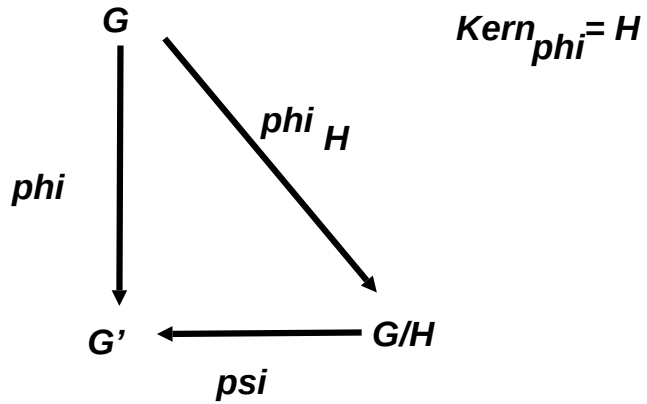
ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.

Dann ist $\psi([g]) = y$.

ψ ist injektiv: Nach Satz 9 genügend z.Z., dass $Kern_\psi = \{[e]\} = \{H\}$.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.

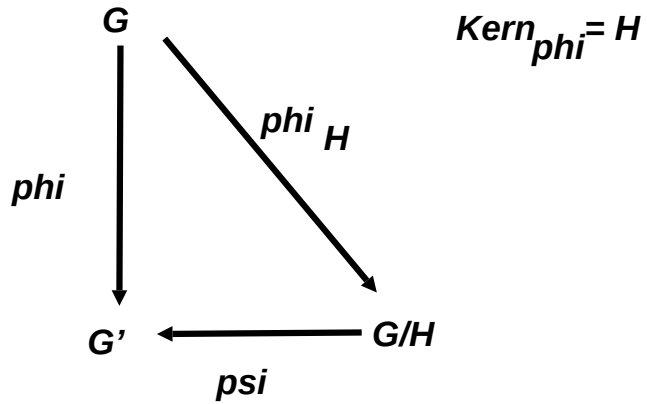
Dann ist $\psi([g]) = y$.

ψ ist injektiv: Nach Satz 9 genügend z.Z., dass $Kern_\psi = \{[e]\} = \{H\}$.

Aber das ist so: ist $[g] \in Kern_\psi$,

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:

$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.

ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.

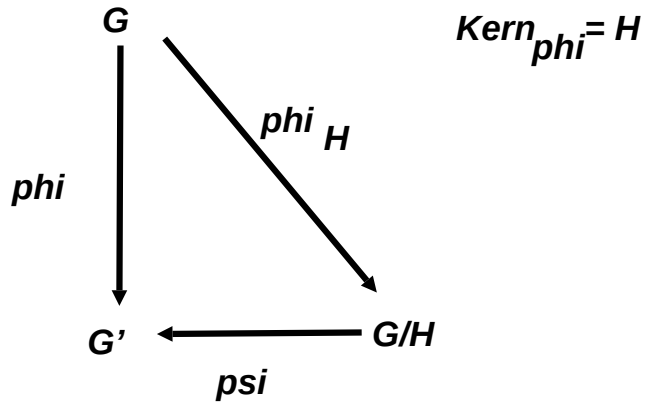
Dann ist $\psi([g]) = y$.

ψ ist injektiv: Nach Satz 9 genügend z.Z., dass $Kern_\psi = \{[e]\} = \{H\}$.

Aber das ist so: ist $[g] \in Kern_\psi$, so ist $\phi(g) = e$

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



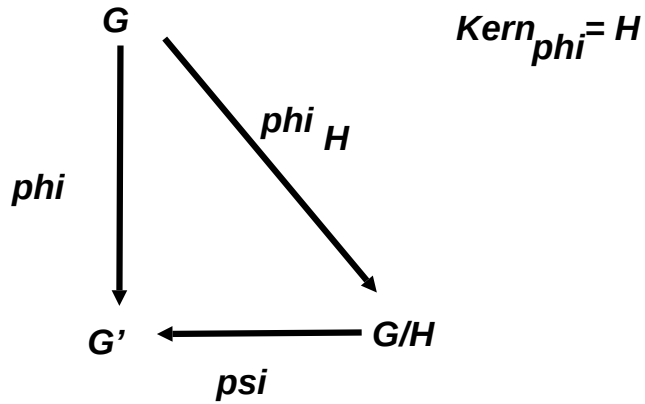
Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:
$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.
ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.
Dann ist $\psi([g]) = y$.
ψ ist injektiv: Nach Satz 9 genügend z.Z., dass $Kern_\psi = \{[e]\} = \{H\}$.
Aber das ist so: ist $[g] \in Kern_\psi$, so ist $\phi(g) = e$ und deswegen
$g \in Kern_\phi$.

Satz 17 (Homomophismussatz) *Sei $\phi : G \to G'$ ein Homomorphismus. Dann ist die Abbildung $\psi : G/Kern_\phi \to Bild_\phi$, $\psi([g]) = \phi(g)$ ein Isomorphismus*

In Worten: Bild vom Homomorphismus ist isomorph zu der Faktorgruppe bez. des Kernels.



Beweis: ϕ ist wohldefiniert: ist $g_1 \sim g$, so ist $g_1 = \underbrace{h}_{\in Kern_\phi} g$, und

deswegen $\phi(g_1) = \phi(hg) = \underbrace{\phi(h)}_{e}\phi(g) = \phi(g)$.

ψ ist ein Homomorphismus:
$\psi([g_1]\cdot[g_2]) = \psi([g_1 \cdot g_2]) = \phi(g_1 \cdot g_2) = \phi(g_1)\cdot\phi(g_2) = \psi([g_1])\cdot\psi([g_2])$.
ψ ist surjektiv: für $y \in G'$ nach Voraussetzungen $\exists g \in G$ mit $\phi(g) = y$.
Dann ist $\psi([g]) = y$.
ψ ist injektiv: Nach Satz 9 genügend z.Z., dass $Kern_\psi = \{[e]\} = \{H\}$.
Aber das ist so: ist $[g] \in Kern_\psi$, so ist $\phi(g) = e$ und deswegen
$g \in Kern_\phi$. □