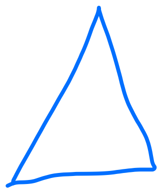
Abschnitt 19 fort.



$$D_3 = \mathrm{Sym}(\Delta)$$

$$G = \{I, A, B, 1, 2, 3\}$$

<u>Beh. 1</u> G ist abgeschlossen bez. Verknüpfung und Umkehrung.

Bewiesen

<u>Beh. 2</u> $\mathrm{Sym}(\Delta) = G$.

(Klar: $G \subseteq \mathrm{Sym}(\Delta)$)

$$\overset{?}{=}$$

Beweis von Beh. 1:

∘	I	A	B	1	2	3
I	I	A	B	1	2	3
A	A	B	I	$\boxed{3}$	1	2
B	B	I	A	2	3	1
1	1	$\boxed{2}$	3	I	A	B
2	2	3	1	B	I	A
3	3	1	2	A	B	I

(auch für Umkehrung)

Notiz:

Drehung ∘ Drehung = Drehung

Spiegelung ∘ Drehung = Spiegelung

Drehung ∘ Spiegelung = Spiegelung

Spiegelung ∘ Spiegelung = Drehung

Beweis von Beh. 2

$G \overset{?}{=} \mathrm{Sym}(\Delta)$

Offensichtlich $G \subseteq \mathrm{Sym}(\Delta)$.

Zu zeigen: $\mathrm{Sym}(\Delta) \subseteq G$.

Sei $\phi \in \mathrm{Sym}(\Delta)$. Also ϕ ist eine Isometrie von $\mathbb{R}^2$ und

$$\phi(\Delta) = \Delta$$

Dann nimmt ϕ Ecken zu Ecken, d.h. ϕ permutiert die Ecken:

$$\phi : \{A_1, A_2, A_3\} \to \{A_1, A_2, A_3\}$$

bijektiv.

$6 = 3! = 3 \cdot 2$

Aber alle 6 Permutationen von $\{A_1, A_2, A_3\}$ sind schon realisiert durch Elemente von G. D.h. für jedes $\phi \in Sym(\Delta)$ gibt es ein $\psi \in G$ mit

$$\phi(A_1) = \psi(A_1)$$
$$\phi(A_2) = \psi(A_2)$$
$$\phi(A_3) = \psi(A_3).$$

Da die Ecken nicht-kollinear sind muss

$$\phi = \psi$$

also

$$\phi \in G$$

also $Sym(\Delta) \subseteq G$

also $Sym(\Delta) = G$. QED

Einheitsquaternionen

Für die 8 Symbolen

$$\left.\begin{matrix} 1, i, j, k \\ -1, -i, -j, -k \end{matrix}\right\} Q$$

hat man die Multiplikations-regeln

1u = u1 = u   für alle u

i^2 = j^2 = k^2 = -1

$$ij = (-j)i = k$$
$$jk = (-k)j = i$$
$$ki = (-i)k = j$$

usw. (siehe Appendix im Skript.)

Übung

(1) Man konstruire die 8×8 Multiplikationstafel von Q.

(2) Man konstruire die 8×8 Multiplikationstafel von $D_4 = \mathrm{Sym}(\square)$

(3) Kann man durch schlaue Symbolensubstitution die eine Tafel in die andere umwandeln?

Abschnitt 20 Gruppen

- Definition
- Einfache Eigenschaften

Def Eine Gruppe ist ein Paar $(G, \circ)$, wobei G eine Menge ist und $\circ$ eine Funktion

$$\circ : G \times G \to G$$
$$(a, b) \mapsto a \circ b$$

S.d.

1) $\forall a, b, c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

(Assoziativität)

2) $\exists e \in G \quad \forall a \in G$

$$e \circ a = a \circ e = a$$

(Neutrales Element)

3) $\forall a \in G \quad \exists b \in G$

$$a \circ b = b \circ a = e$$

(Inversen)

Man schreibt

$$a \circ b$$

$$a \cdot b$$

$$ab$$

$$\circ(a, b)$$

Man schreibt

G für $(G, \circ)$

wenn $\circ$ offensichtlich ist.

Bsp Sym(Δ) ist eine Gruppe. (Assoziativität verifizieren)

Bsp

$\circ$	E	U
E	E	U
U	U	E

(Verknüpfungsregeln für Orientation.)

☆☆☆

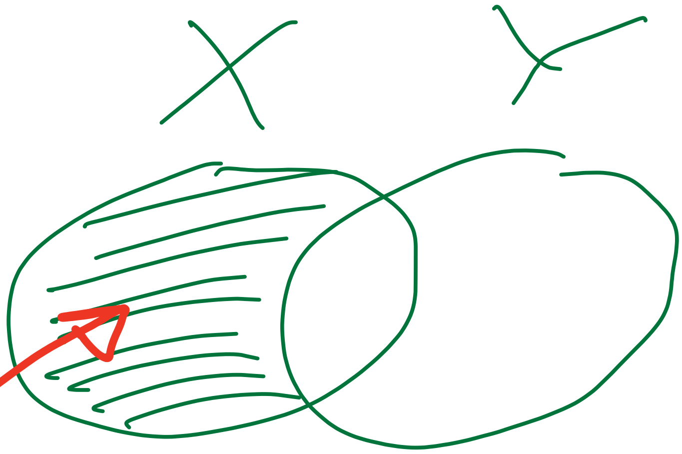
Bsp Sym(F) ist eine Gruppe, für jede Figur $F \subseteq \mathbb{R}^n$. (Abschnitt 18.)

Bsp (Algebra)

$(\mathbb{Z}, +)$ $\quad e = 0$

$(\mathbb{R}, +)$ $\quad e = 0$

$(\mathbb{R}\setminus\{0\}, \cdot)$ $\quad e = 1$



$X \setminus Y := \{x \in X \mid x \notin Y\}$

$(m \times n \text{ Matrizen}, +)$

$$e = \begin{array}{cc} \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} & m \\ n & \end{array}$$

(invertierbare $m \times m$ Matrizen, $\cdot$)

$$e = I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

$(\mathbb{R}^n, +) \qquad e = (0, \ldots, 0)$

Übung Finden Sie eine Menge und eine Operation $\circ$, die alle Gruppenaxiome erfüllt, ausser der Existenz von Inversen. (mehrere ...)

Einfache Eigenschaften

1) Wir dürfen Klammern weglassen

$$(a \cdot b)c = a(bc) = abc$$

2) **Beh** Das neutrale Element ist eindeutig.

Bew Nehme an, dass e und e' das zweite Axiom erfüllen. Dann

$$e = ee' = e'$$

QED

Wir schreiben

e_G, 1_G, oder

e oder 1

für <u>das</u> neutrale
Element von G.

3) <u>Beh.</u> Sei $a \in G$. Dann hat a ein <u>eindeutige</u> Inverse.

<u>Beweis</u> Sei $a \in G$ fest.

Seien b und b' Inversen von a. Dann

$$e = b'a \quad \longleftarrow$$

$$ab = e \quad \longleftarrow$$

Also

$$\begin{aligned} b = eb &= (b'a)b \\ &= b'(ab) \\ &= b'e = b' \end{aligned}$$

Also

$$b' = b$$

QED

Wir nennen die eindeutige Inverse von a, $\boxed{a^{-1}}$.

4) Wir definieren die $j$te Potenz von a:

$$a^j := \underbrace{a a \cdots a}_{j\text{-mal}}, \qquad j > 0$$

$$a^0 := e$$

$$a^{-k} := \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{k\text{-mal}} \qquad k > 0$$

(a^{-1} ist wohldefiniert.)

<u>Beh.</u> $a^j a^k = a^{j+k}$

$\forall j, k \in \mathbb{Z}$

5) <u>Beh</u> (Kürzungsregel)

Sei G eine Gruppe, $a, b, c \in G$. Dann

$$\cancel{a}b = \cancel{a}c \implies b = c \quad \leftarrow 1)$$

$$b\cancel{a} = c\cancel{a} \implies b = c \quad \leftarrow 2)$$

<u>Bew.</u> 1)

$$ab = ac \implies a^{-1}(ab) = a^{-1}(ac)$$
$$\implies (a^{-1}a)b = (a^{-1}a)c$$
$$\implies eb = ec$$
$$\implies b = c$$

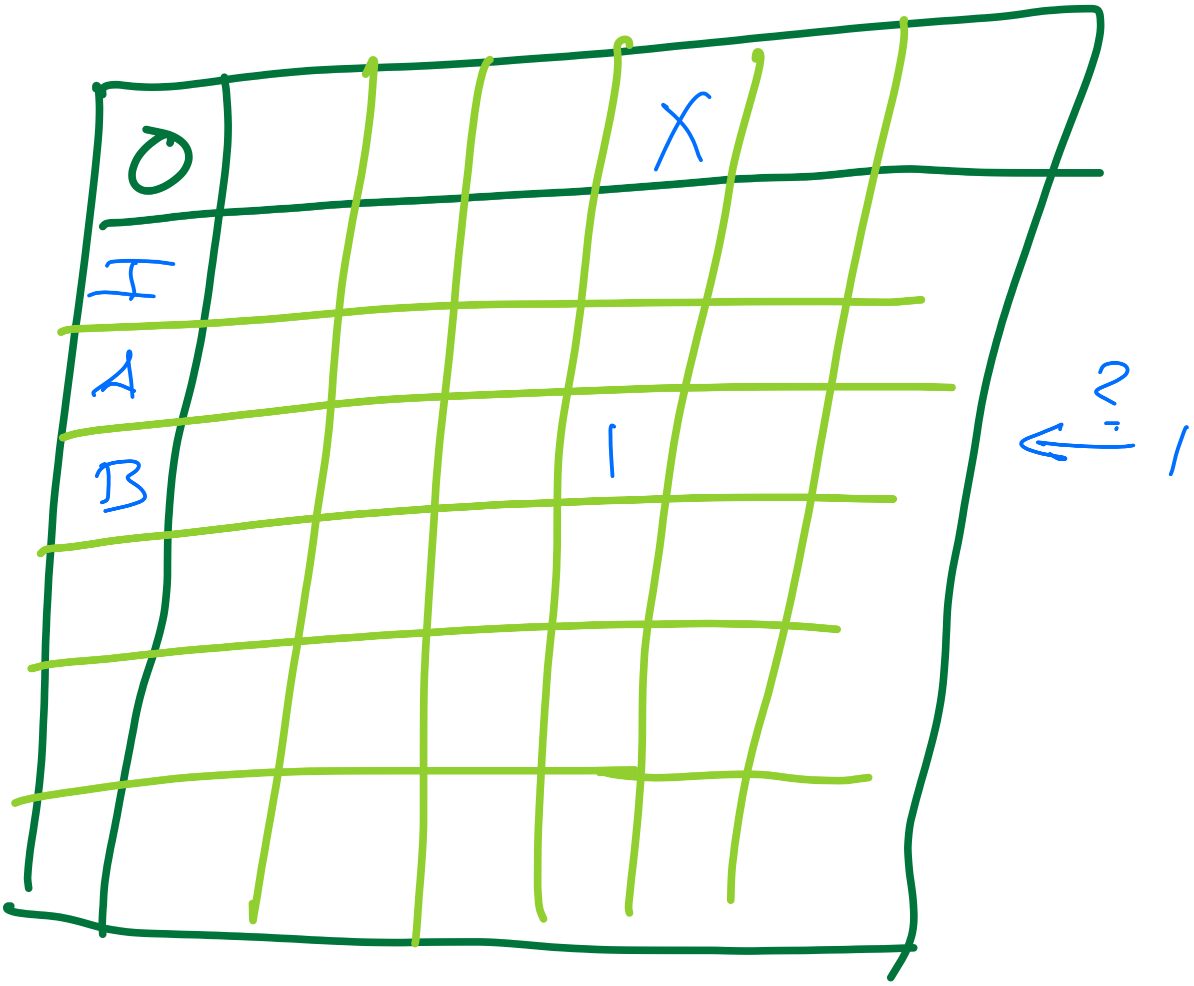
2) Ähnlich QED.

6) Jedes Element einer Gruppe erscheint genau einmal in jeder Zeile und in jeder Spalte der Multiplikationstafel der Gruppe.

(Wie angekündigt in Ab. 19)

<u>Bew.</u> Wegen der Kürzungsregel, erscheint jedes Element <u>höchstens</u> einmal. Durch Multiplikation mit einer geeigneter Inverse

Kann man zeigen, dass jedes Element der Gruppe erscheint mindestens einmal.



$$B \circ ? = 1$$

$$? = B^{-1} \circ 1 = X$$

QED

Bmk

	Dimension	
$\mathbb{R}$	1	kommutativ + assoziativ — Körper
$\mathbb{C}$	2	
$\mathbb{H}$	4	assoziativ, nicht kommutativ, Quaternionen
$\mathbb{O}$	8	nichtassoziativ, nicht kommutativ, Octonionen
$\mathbb{K}$	16	noch schlimmer ...? Cayley numbers

Blogs von John Baez

Abschnitt 21 Isomorphismen

Def Seien

$$(G, \circ_G) \qquad (H, \circ_H)$$

Gruppen. Ein Isomorphismus zwischen G und H ist eine Bijektion

$$f : G \to H,$$

die die Gruppenoperation erhält:

$$f(a \circ_G b) = f(a) \circ_H f(b)$$

$\forall a, b \in G$.

d.h.

$\boxed{\text{G und H haben genau \underline{diesselbe} Struktur}}$

Man schreibt

$$G \cong H$$

oder

$$G \underset{f}{\cong} H$$

und sagt: G und H sind <u>isomorph</u>.

"sehen gleich aus"

Beh. Seien G und H Gruppen und sei $f: G \to H$ ein Isomorphismus. Dann

1) $f(e_G) = e_H$

2) $f(a^{-1}) = f(a)^{-1}$

gerechnet in G

gerechnet in H

$$f(inv_G(a)) = inv_H(f(a))$$

$$\begin{cases} inv_G(a) = a^{-1} \text{ in } G \\ inv_H(c) = c^{-1} \text{ in } H. \end{cases}$$

Ziemlich offentsichtlich.

Es ist klar, dass ein Isomorphismus alle Eigenschaften und Beziehungen erhält, die mit o_G und o_H ausgedrückt werden können.

Bew.

1) $\cancel{f(e_G)}\, f(e_G)$

$= f(e_G e_G)$

$= f(e_G)$

$= \cancel{f(e_G)}\, e_H$

$\Rightarrow f(e_G) = e_H$

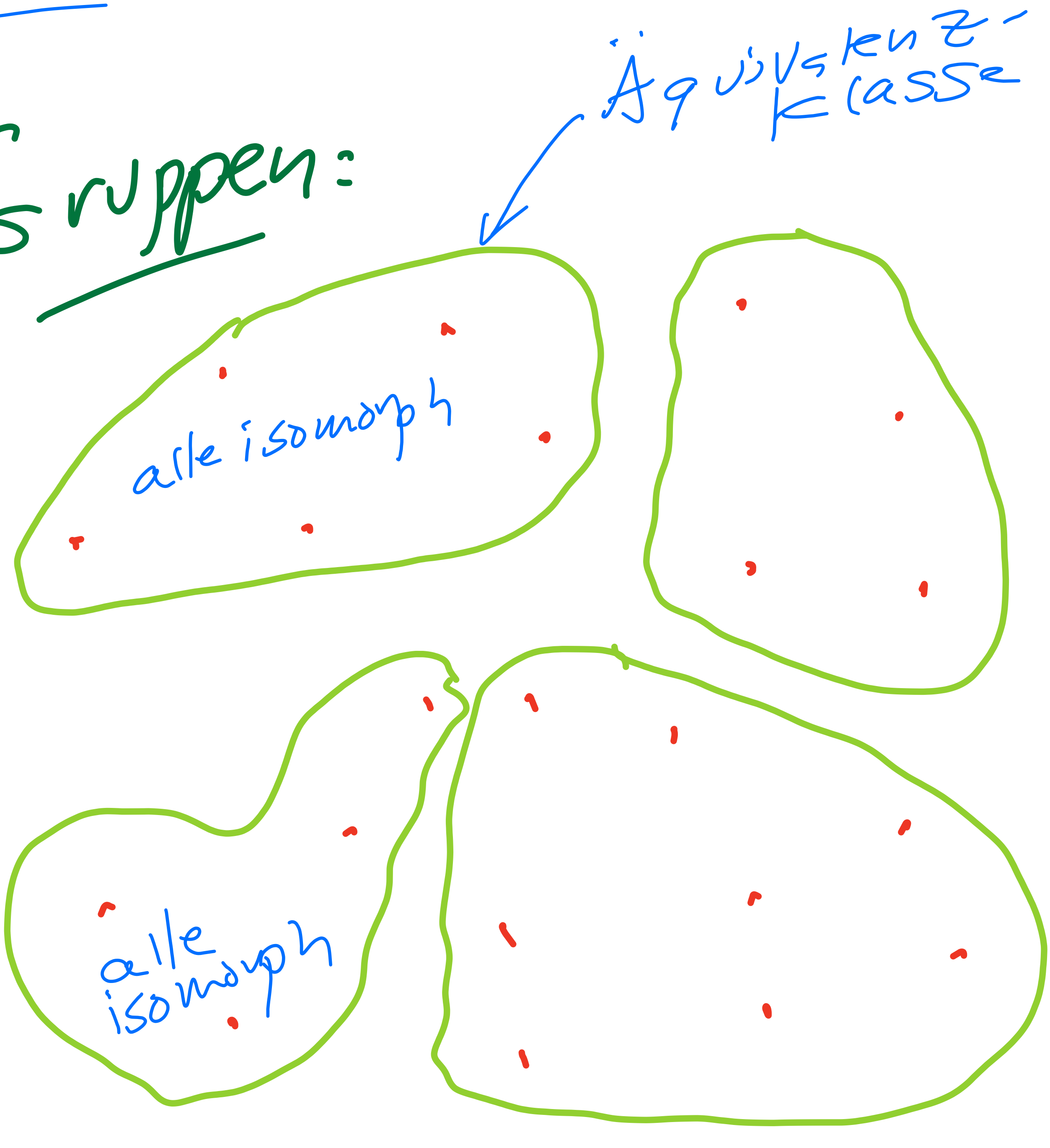
2) Lasse ich Ihnen. (Skript)

QED

$\underline{\text{Beh.}}$ $\cong$ ist ein Äquivalenzrelation

$\underline{\text{Bew.}}$ Lasse ich Ihnen.

Gruppen:



Homomorphismen

Def Seien G, H Gruppen.

Ein Homomorphismus von G nach H ist eine Abbildung

$$f: G \to H$$

wobei

$$f(ab) = f(a)f(b)$$

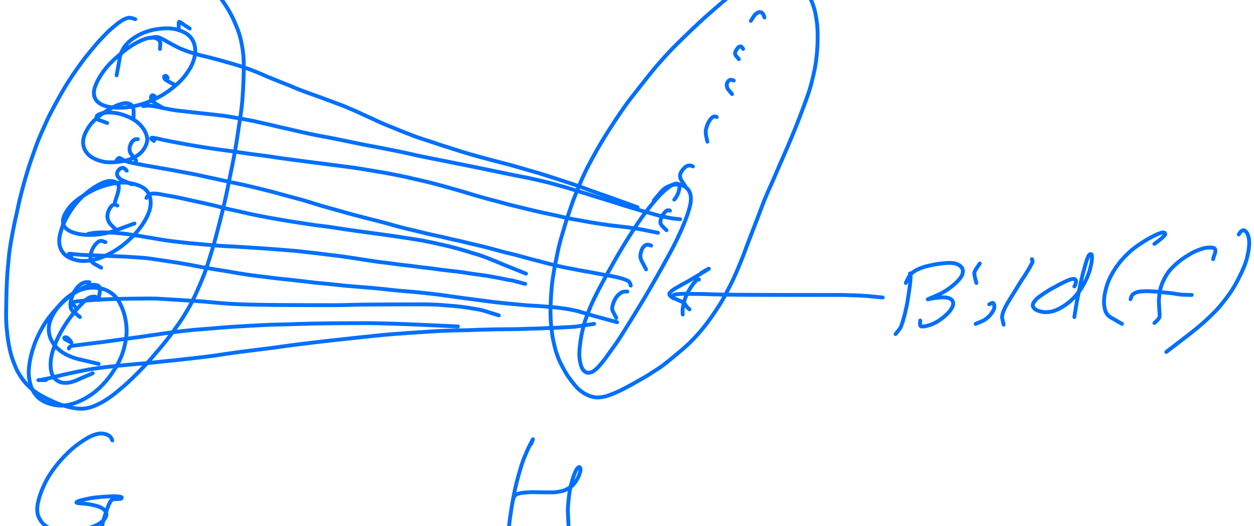
$\forall a, b \in G$.

Ein Homomorphismus erhält die Multiplikation, aber ist nicht notwendigerweise bijektiv.

d.h.

1) f kann Information / Elemente von G "vergessen".

2) H kann viel grösser als $\mathrm{Bild}(f)$ $(= f(G))$ sein.



Automorphismen

Def Ein Automorphismus einer Gruppe G ist ein Isomorphismus von G mit sich:

$$f: G \to G$$

Isomorphismus

Man schreibt

$$\mathrm{Aut}(G)$$

für die Menge aller Automorphismen von G.

Übung

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

Dann ist

$$(\mathrm{Aut}(G), \circ)$$

Verknüpfung von Abbildungen

wieder eine Gruppe!!

Diese Übung zeigt, wie die Mathematik auf sich baut.

Aufbau

Abschnitt 22

<u>Ordnung.</u> ~~Zyklische Gruppen~~

<u>Def</u> Die <u>Ordnung</u> einer Gruppe G ist die Anzahl Elemente in G:

$$\mathrm{order}(G) = |G| = \#G$$
$$\mathrm{Ordnung}(G)$$

<u>Def</u> Sei G eine Gruppe, $g \in G$ ein Element.
Die <u>Ordnung</u> von g ist die kleinste Zahl $n > 0$, sodass

$$g^n = e.$$

Man schreibt

$$\operatorname{ord}(g) := n.$$

Falls es keine solche Zahl gibt, schreibt man

$$\operatorname{ord}(g) := \infty$$

Man hat

$$\mathrm{ord}(g) \in \{1, 2, 3, \ldots, \infty\}$$

<u>Bsp</u> In $D_3 = \mathrm{Sym}(\Delta)$

$= \{I, A, B, 1, 2, 3\}$

$$I^1 = I$$

$$A^3 = B^3 = I$$

$$1^2 = 2^2 = 3^2 = I$$

$$\mathrm{ord}(I) = 1$$

$$\mathrm{ord}(A) = \mathrm{ord}(B) = 3$$

$$\mathrm{ord}(1) = \mathrm{ord}(2)$$

$$= \mathrm{ord}(3) = 2$$

$\mathrm{Ordnung}(D_3) = 6.$

Beh. Sei G eine endliche Gruppe, d.h.

$$\# G < \infty.$$

Dann hat jedes Element von G endliche Ordnung.

Beweis Man betrachtet die Folge

$$a, a^2, a^3, \ldots$$

Da G endlich ist, muss es eine Wiederholung

$$a^j = a^k, \quad 1 \le j < k,$$

geben, wobei

$$1 \le j < k$$

$$a^j = a^k$$

Dann durch die Kürzungsregel bekommt mann:

$$1 = a^{j-j} = a^{k-j}$$

$$a^{k-j} = 1 \qquad k-j > 0$$

a hat Ordnung höchstens $k-j < \infty$. QED.