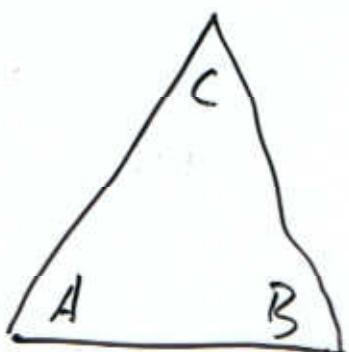


8.1.15 (1)

2. Bonusklausur: Fr., 16.1.15, 16'15 hier!

Tutorium: Mi., 14.1.15, 12'15 HS 1,  
Geomathikum



$$y \circ r = z.$$

$$ax = b$$

$$a^{-1}ax = a^{-1}b$$

$$e^x = a^{-1}b$$

$$x = a^{-1}b$$

---

$$xs = y \quad (X \text{ ist die Unbekannte})$$

$$X = ys^{-1}$$

Gruppentafel:  $s \circ r = i \Rightarrow r = s^{-1}$ ,

$$X = ys^{-1} = z.$$

(2)

$$a^n = \underbrace{a a \dots a}_{n \text{ Faktoren}}$$

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

Ordnung: kleinste  $m \geq 1$  mit  $a^m = e$ .

Beispiel: In  $S_3 = S(\{1, 2, 3\})$  berechnen wir die Ordnung von

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \pi$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$\Rightarrow \pi^1 \neq e, \pi^2 = e$$

$\Rightarrow$  Die Ordnung von  $\pi$  in  $S_3$  ist 2.

$$|\pi| = 2$$

$|a|$  ist die Ordnung von  $a$ .

### Beweis von Satz 7.16:

(3)

Sei  $G$  endliche Gruppe,  $a \in G$ .

$G$  endlich  $\Rightarrow$  ex.  $m, n \in \mathbb{N}_0$ ,  $m < n$   
mit  $a^m = a^n$ .

$$\begin{aligned} \Rightarrow a^m \cdot a^{-m} &= a^n a^{-m} \\ a^0 &= a^{n-m} \\ e &= a^{n-m} \end{aligned}$$

$$m < n \Rightarrow n - m > 0.$$

$\Rightarrow$  die Ordnung von  $a$  ist  
höchstens  $\underline{a^{n-m}}$   $n - m$   $\square$ .

Bem: In jeder Gruppe hat  $e$   
die Ordnung 1.  $e^1 = e$ .

$$[3]_{15} + [3]_{15} = [6]_{15}$$

$$3 \cdot [3]_{15} = [9]_{15}$$

$$4 \cdot [3]_{15} = [12]_{15}$$

$$5 \cdot [3]_{15} = [15]_{15} = [0]_{15},$$

(4)

$\mathbb{Z}_m^* = \{ [a]_m : a \in \mathbb{Z} \text{ ist zu } m \text{ teilerfremd} \}$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$\pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 5 \end{pmatrix}$$

$$\pi^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e \in S_5$$

$$\Rightarrow |\pi| = 4.$$

$$a^m = e$$

Sei  $\pi$  wie oben. Dann gilt

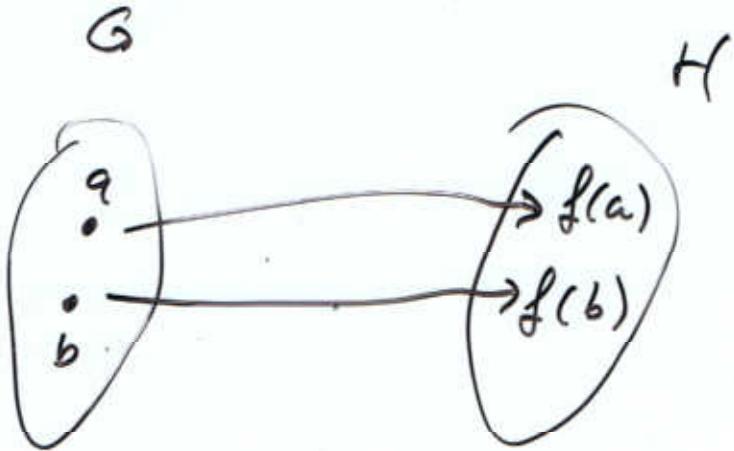
$$\pi^0 = e, \pi^4 = e, \pi^{16} = e, \pi^{-60} = e.$$

$$\pi^0 = e, \pi^1 = \pi,$$

$$\pi^4 = e, \pi^5 = \pi^1, \pi^6 = \pi^2, \pi^7 = \pi^3$$

$$\pi^8 = e$$

(5)



Beispiel: Wir hatten im wesentlichen schon gezeigt, dass  $S_4$  zu  $S_3$  isomorph ist.

$$\begin{array}{c|c|c}
 i & r & s \\
 \hline
 \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} & \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} & \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \\
 \hline
 k & \downarrow & z
 \end{array}$$

$f: S_4 \rightarrow S(\{A, B, C\})$   
ist ein Isomorphismus.

Beweis von Lemma 1. (7.20 im Skript, ⑥)

a)  $f^{-1}$  ist eine Bijektion.

Seien  $a, b \in H$ . Dann ex.

$x, y \in G$  mit  $f(x) = a, f(y) = b$ .

$x = f^{-1}(a), y = f^{-1}(b)$ .

$$f^{-1}(ab) = f^{-1}(f(x)f(y))$$

$$= f^{-1}(f(xy)) = xy = f^{-1}(a)f^{-1}(b)$$

$\Rightarrow f^{-1}$  ist ein Iso.  $\square$

b)  $(gof)(ab) = g(f(ab))$

$$= g(f(a)f(b)) = g(f(a))g(f(b))$$

$$= (gof)(a)(gof)(b). \quad \square$$

c) Sei  $e_G$  das neutrale Element von  $G$ ,  $a \in H$ . Dann ex.  $x \in G$  mit  $f(x) = a$ .

$$f(e_G) \cdot a = f(e_G) \cdot f(x) = f(e_G \cdot x)$$

$$= f(x) = a = e_H \cdot a$$

$$\Rightarrow e_H = f(e_G)$$

Skizze des Beweises von Satz 7.23. (7)  
(7.24 im  
Skript)

Sei  $G = \{a^n : n \in \mathbb{Z}\}$ .

1. Fall:  $a$  hat unendliche Ord.

$$f: \mathbb{Z} \rightarrow G; n \mapsto a^n$$

ist Isomorphismus.

$$\begin{aligned} f(n+m) &= a^{n+m} = a^n a^m \\ &= f(n) f(m). \end{aligned}$$

2. Fall: Sei  $m < \infty$  die Ordnung  
von  $a$ .

Dann ist  $f: \mathbb{Z}_m \rightarrow G$  mit

$$f([n]_m) = a^n$$

ein Isomorphismus  $\square$

$$G_D = \{i, r, s, x, y, z\}$$

$r, s$  Rotationen

$x, y, z$  Spiegelungen.

Beweis von Satz 2.29 a)

Sei  $U \subseteq G$  Untergruppe,  $a, b \in U$ .

Dann gilt  $ab \in U$ , da die Verknüpfung von  $G$  eingeschränkt auf  $U \times U$  verknüpft auf  $U$  ist.

$U$  Gruppe  $\Rightarrow$  ex. neutrales Element  $e_U$ .

Es gilt, in  $U$  wie in  $G$ :  $e_U e_U = e_U$

$\Rightarrow e_U = e \Rightarrow e \in U$

Sei  $a \in U$ . Dann ex.  $b \in U$  mit  
 $ab = e = ba$ . Diese Gleichung  
gilt auch in  $G$ .

$\Rightarrow b = a^{-1}$ , wobei  $a^{-1}$  das zu  
 $a$  Inverse in  $G$  ist.

$\Rightarrow a^{-1} \in U$ .

Andere Richtung: Einfach.

b) Sei  $U$  Untergruppe,  $a, b \in U$ .  
Dann ist  $a b^{-1} \in U$  (nach a))  
Damit ist  $a b^{-1} \in U$  (auch nach a))  
Andere Richtung: Sei  $U \neq \emptyset$   
Ang. f.a.  $a, b \in U$  ist  $a b^{-1} \in U$ .  
Zeigen:  $e \in U$ , f.a.  $a, b \in U$  ist  $a b \in U$ ,  
f.a.  $a \in U$  ist  $a^{-1} \in U$ .

Sei  $a \in U$ . Dann ist  $e = a a^{-1} \in U$ .  
Damit ist auch  $e a^{-1} = a^{-1} \in U$   
Seien  $a, b \in U$ . Dann ist  $b^{-1} \in U$   
Also ist  $a b = a (b^{-1})^{-1} \in U$   
 $\Rightarrow U$  ist Untergruppe nach a).

c) Sei  $a \in U$ . ( $U \neq \emptyset$ )  
Die Elemente  $a b$ ,  $b \in U$ ,  
sind pw. verschieden.  
Das sind  $|U|$ -viele verschiedene  
Elemente von  $U$ . Daher ex.  $b \in U$   
mit  $a b = a$ .  $\Rightarrow b = e$ .  
 $\Rightarrow e \in U$ .  
Analog ex.  $b \in U$  mit  $a b = e$ .  
Es gilt  $b = a^{-1}$ .  
 $\Rightarrow U$  ist Untergruppe D

(3)

$$\begin{aligned}
 6\mathbb{Z} + 4 &= \{\dots, 0+4, 6+4, 12+4, \dots\} \\
 &= \{\dots, 4, 10, 16, \dots\} \\
 &= [4]_6.
 \end{aligned}$$


---

$$2\mathbb{N} = \{2, 5\} = 5\mathbb{N}$$


---

Beweis v. Satz 2.32:

a) Sei  $a \in G$ . Es gilt  $e \in U$ .

Damit ist  $a = a \cdot e \in aU$   
und  $a = ea \in Ua$ .

b) Klar:  $cU, Uc \subseteq U$ .

~~Se~~ Zeigen: ~~cU, Uc ⊆ U~~.

$U \subseteq cU, Uc$ .

Sei  $d \in U$ . Dann ist  $c^{-1}d \in U$ .

Also ist  $d = cc^{-1}d \in cU$ .

$\Rightarrow U \subseteq cU$ .

~~Anal~~ Analog:  $U \subseteq Uc$ .

c) Sei  $b \in aU$ . Dann ex.  $c \in U$  mit  
 $b = ac$ . Damit ist  $bU = acU$   
 $= a(cU) = aU$ .

d) Angenommen,  $\text{all} \cap \text{blk} \neq \emptyset$ . ④

Sei  $c \in \text{all} \cap \text{blk}$ . Dann ist  
 $c \in \text{all}$  und  $c \in \text{blk}$ .

Also gilt  $\text{all} = c\text{U} = \text{blk}$ .  
 $\Rightarrow \text{all} = \text{blk}$ .

e) Wir zeigen nur  $|\text{U}| = |\text{all}|$ .

Wir geben eine Bijektion

$f: \text{U} \rightarrow \text{all}$  an.

Für  $b \in \text{U}$  sei  $f(b) = ab$ .

Surjektivität: klar.

Injektivität: Ang.  $b, c \in \text{U}$ ,

$f(b) = f(c)$ . Dann gilt

$$ab = ac \Rightarrow b = c.$$

$\Rightarrow f$  ist injektiv.

Beweis von Korollar 7.34:

Sei  $G$  endlich,  $m$  die Anzahl  
der Linksnbenklassen der Untergr.  $\text{U}$   
Dann gilt  $|G| = \underline{m} \cdot |\text{U}|$ .

Welche Elemente kommen  
in die Nebenklasse? (5)

$U \subseteq G$  Untergruppe.

a ∈ G. Dann ist die Linksnaben-  
klasse

von a von U die Menge

$$aU = \{ab : b \in U\}.$$

---

Beispiel: Die Einheitengruppe von  $\mathbb{Z}_5$ .

$$\begin{aligned}\mathbb{Z}_5^* &= \{[a]_5 : a \in \mathbb{Z} \text{ ist zu 5 teilerfremd}\}, \\ &= \{[1]_5, [2]_5, [3]_5, [4]_5\}.\end{aligned}$$

Wir suchen die von  $[2]_5$  erzeugte  
Untergruppe.

$$([2]_5)^2 = [4]_5,$$

$$([2]_5)^3 = [8]_5 = [3]_5$$

$$([2]_5)^4 = [16]_5 = [1]_5.$$

$\Rightarrow \mathbb{Z}_5^*$  wird von  $[4]_5$  erzeugt.

Das Gleiche mit  $[4]_5$ .

$$([4]_5)^2 = [16]_5 = [1]_5$$

$\Rightarrow \{[1]_5, [4]_5\}$  ist eine  
Untergruppe von  $\mathbb{Z}_5^*$ .

(6)

$$U = \{[1]_5, [4]_5\},$$

$$\alpha = (\mathbb{Z}_5^*, \cdot).$$

Nebenklassen von  $U$ :

$$[1]_5 \cdot U = \{[1]_5 \cdot [1]_5, [1]_5 \cdot [4]_5\}$$

$$= \{[1]_5, [4]_5\} = U$$

$$[2]_5 \cdot U = \{[2]_5 \cdot [1]_5, [2]_5 \cdot [4]_5\}$$

$$= \{[2]_5, [3]_5\}$$

$$[3]_5 \cdot U = \{[3]_5 \cdot [1]_5, [3]_5 \cdot [4]_5\}$$

$$= \{[3]_5, [2]_5\} = [2]_5 \cdot U$$

$$[4]_5 \cdot U = \{[4]_5 \cdot [1]_5, [4]_5 \cdot [4]_5\}$$

$$= \{[4]_5, [1]_5\} = [1]_5 \cdot U.$$

Geschen: Gruppe  $G$ , Untergruppe  $H$ .  
Bestimmung der Linksnbenklassen:  
Erste (und einfachste) Nebenklaße:  
 $eH = H$ .

Nächste Nebenklaße: Wähle  
 $a \in G \setminus H$ .

Bestimme  $a_1 H$ . Es gilt  $a_1 H \cap H = \emptyset$ .

Weiter: Finde  $a_2 \in G \setminus (H \cup a_1 H)$

Bestimme  $a_2 H$ .

Setze fort bis  $G \setminus (H \cup a_1 H \cup \dots \cup a_n H)$   
 leer ist.

Dann haben wir alle Linksnben-  
klassen gefunden.