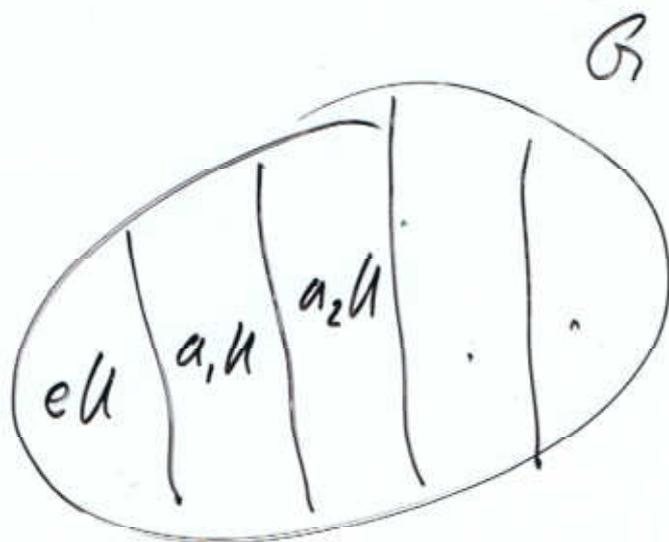


15.1.15

①



$[a:U]$ ist der Index von U in G .

$$\mathbb{Z} = (\mathbb{Z}, +).$$

$$m\mathbb{Z} = \{m \cdot n : n \in \mathbb{Z}\}$$

Nebenklassen von $m\mathbb{Z}$ sind genau die Restklassen $[0]_m, \dots, [m-1]_m$.

Satz von Fermat und Euler:

Sei $m \in \mathbb{N}$, n zu m teilerfremd.
(D.h. $[n]_m$ ist in \mathbb{Z}_m invertierbar.)

Dann gilt $n^{\varphi(m)} \equiv 1 \pmod{m}$

$\varphi(m)$: Die Zahl der zu m teilerfremden Zahlen in $\{0, \dots, m\}$.

Erinnerung: Eine Gruppe G ist zyklisch, falls ein $a \in G$ ex. mit $G = \{a^n : n \in \mathbb{Z}\}$. ②

Ist G zyklisch, so ist $G \cong \mathbb{Z}$
(D.h. ex. Bijektion $f: G \rightarrow \mathbb{Z}$
mit: $\forall a, b \in G (f(ab) = f(a) + f(b))$)
oder es gibt $m \in \mathbb{N}$ mit $G \cong \mathbb{Z}_m$.

Beweis von Satz 7.39:

Sei $U \subseteq G$, G zyklisch.

OBdA (ohne Beschränkung der Allgemeinheit) ist $G = \mathbb{Z}$ oder $G = \mathbb{Z}_m$.

1. Fall: $G = \mathbb{Z}$, $U \subseteq G$.

Sei k die kleinste Zahl > 0 mit $k \in U$ (sonst ist $U = \{0\}$ zyklisch)

Beh: $U = k\mathbb{Z}$. ($\Rightarrow U$ ist zyklisch)

Mit $k \in U$ ist $k\mathbb{Z} \subseteq U$.

Angenommen $n \in U$, n kein Vielfaches von k .

Wähle $q, r \in \mathbb{Z}$ mit

$$n = q \cdot k + r \text{ und } 0 \leq r < k.$$

$$r = n - q \cdot k \in U. \quad \textcircled{3}$$

$$0 \leq r < k. \Rightarrow r = 0$$

$$\Rightarrow n = q \cdot k.$$

(Jedes Element von U ist Vielfaches von k .)

2. Fall: $G = \mathbb{Z}_m$: Ähnlich. \square

Berechnung der Untergruppen von \mathbb{Z}_{12} :

$[0]_{12}$ erzeugt die Untergruppe $\{[0]_{12}\}$

$[1]_{12}$ " " " \mathbb{Z}_{12}

$[2]_{12}$ " " " $\{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}$

($[10]_{12}$ erzeugt dieselbe Untergruppe.)

$[3]_{12}$ " " " $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$

($[9]_{12}$ erzeugt dieselbe UA)

$[6]_{12}$ erzeugt die UA $\{[0]_{12}, [6]_{12}\}$.

$[7]_{12}$ erzeugt die ganze Gruppe \mathbb{Z}_{12} .

7 ist zu 12 teilerfremd.

D.h. $\text{ggT}(7, 12) = 1$. Also ex. λ, μ

mit $1 = \lambda 7 + \mu 12$.

Wir rechnen mod 12

④

$$1 \equiv \lambda \cdot 7 + \mu \cdot 12 \equiv \lambda \cdot 7 \pmod{12}.$$

$$\lambda [7]_{12} = [1]_{12}.$$

D.h. $[1]_{12}$ ist in der von $[7]_{12}$ erzeugten Untergruppe enthalten.

\Rightarrow Die von $[7]_{12}$ erzeugte UG ist \mathbb{Z}_{12} .

Wenn n, m teilerfremd sind, $0 < n < m$,
so erzeugt $[n]_m$ bereits die
ganze Gruppe $(\mathbb{Z}_m, +)$.

Erinnerung: für $a \in G$ ist

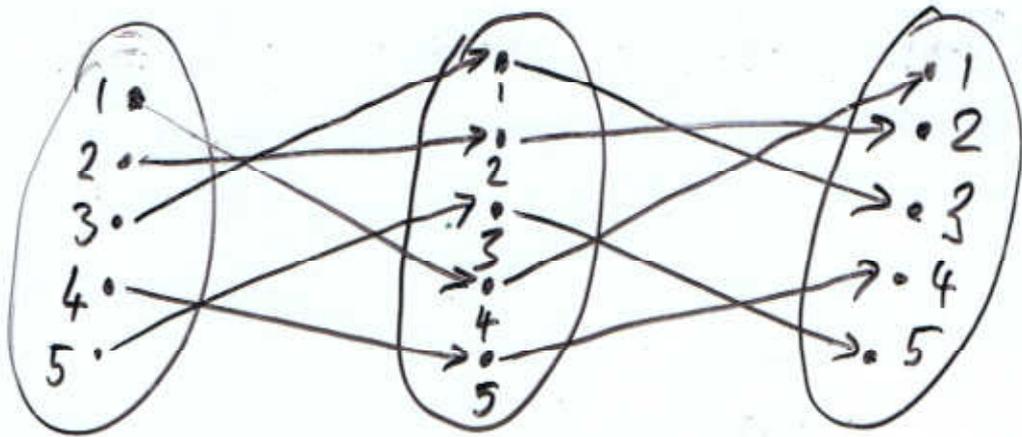
$$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$$

die von a erzeugte Untergruppe von G .

Beispiel: $G = \mathbb{Z}_{12}$, $a = [3]_{12}$

$$\Rightarrow \langle a \rangle = \{ [0]_{12}, [3]_{12}, [6]_{12}, [9]_{12} \}$$

5



A



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = \underline{\underline{(1354)}}$$

$$(12)$$

$$(a_1 a_2 a_3 \dots a_n) = (a_1 a_2)(a_2 a_3) \dots (a_{n-1} a_n)$$