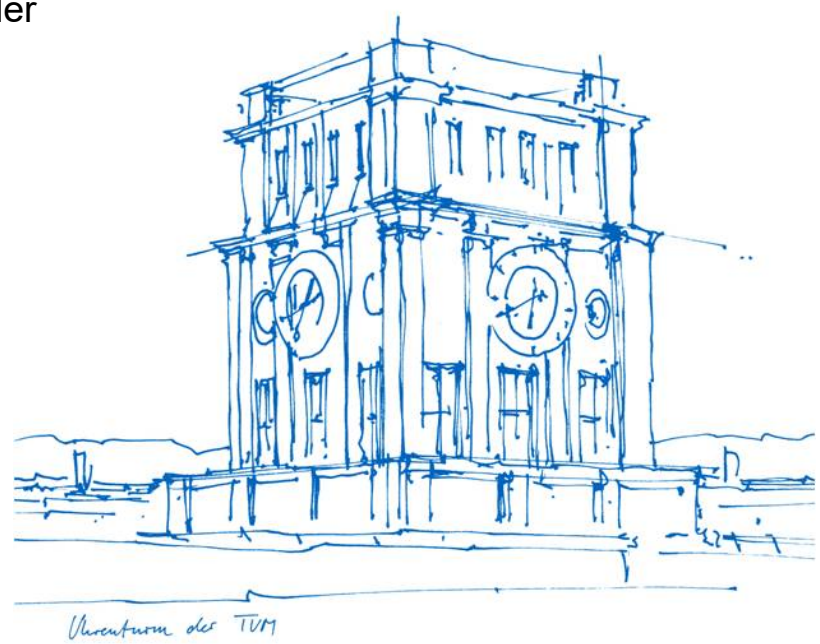
Diskrete Strukturen – Tutorium KW 07

Jeremias Bohn, Evghenii Beriozchin/Manuela Poschenrieder

Technische Universität München

Fakultät für Informatik

Garching, 11./12. Februar 2021



Gruppen

Eine Gruppe ist definiert als $\langle \mathbb{G}, \circ, n \rangle$, wobei $\mathbb{G}$ eine Menge von Elementen, $\circ$ eine binäre Funktion und $n \in \mathbb{G}$ das sogenannte **neutrale Element** ist

- Es gilt Abgeschlossenheit: $\forall a, b \in \mathbb{G}$: $a \circ b \in \mathbb{G}$
- Es gilt Assoziativität: $\forall a, b, c \in \mathbb{G}$: $a \circ (b \circ c) = (a \circ b) \circ c$
- Es gilt **nur** für das Element n: $\forall a \in \mathbb{G}$: $n \circ a = a \circ n = a$
- Es gibt Inverse: $\forall a \in \mathbb{G}\ \exists b \in \mathbb{G}$: $a \circ b = b \circ a = n$
    - Zu jedem Element $a \in \mathbb{G}$ existiert genau **ein** Inverses!

Eine Gruppe, die zusätzlich kommutativ ist, wird als **abelsche Gruppe** bezeichnet

Jede **zyklische Gruppe** ist auch eine abelsche Gruppe

Wir nennen $\mathrm{ord}(\mathbb{G}) = |\mathbb{G}|$ die **Gruppenordnung** der Gruppe

- Für jedes $a \in \mathbb{G}$ gilt $a^{\mathrm{ord}(\mathbb{G})} = n$, wenn $\mathbb{G}$ finit ist

Größter gem. Teiler & Kleinstes gem. Vielfaches

Der größte gemeinsame Teiler zweier Zahlen a, b (kurz: $\mathrm{ggT}(a, b)$) ist die größte Zahl, die sowohl a als auch b teilt

- $\mathrm{ggT}(a, b) = \max\{x \in \mathbb{N}: x|a \wedge x|b\}$
- Wir können das ggT bestimmen, indem wir a und b in ihre Primfaktoren zerlegen. Die Schnittmenge der Primfaktoren ist die Primfaktorzerlegung des ggT

Das kleinste gemeinsame Vielfache zweier Zahlen a, b (kurz: $\mathrm{kgV}(a, b)$) ist die kleinste Zahl, die sowohl von a als auch b geteilt wird

- $\mathrm{kgV}(a, b) = \min\{x \in \mathbb{N}: a|x \wedge b|x\}$
- Wir können das kgV mittels des ggT bestimmen: $\mathrm{kgV}(a, b) = \frac{a \cdot b}{\mathrm{ggT}(a,b)}$

Erweiterter Euklidscher Algorithmus

Der erweiterte euklidsche Algorithmus (EEA) stellt eine Alternative zur Berechnung des ggT dar

- Es gilt $\mathrm{eea}(a, b) = (\alpha, \beta)$ mit $\mathrm{ggT}(a, b) = \alpha \cdot a + \beta \cdot b$

a	b	k	α	β
a	b	$\left\lfloor \frac{b}{a} \right\rfloor$	$\beta' - k \cdot \alpha'$	α'
$b \bmod a$	a		α'	β'
…	…	…	…	…
0	x		0	1

Eulersche Phi-Funktion

Die eulersche Phi-Funktion für eine Zahl $a \in \mathbb{N}$ gibt an, wie viele natürliche, teilerfremde Zahlen $< a$ existieren

- Für zwei teilerfremde Zahlen m, n gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
- Für jede Primzahl p gilt: $\forall k \in \mathbb{N}$: $\varphi(p^k) = p^{k-1} \cdot (p-1)$
  - Insbesondere gilt also $\varphi(p) = (p-1)$

Untergruppen & Gruppenexponent

Sei $\langle \mathbb{G}, \circ, n \rangle$ eine Gruppe. Wir definieren für jedes $a \in \mathbb{G}$: $\langle a \rangle = \{a^k = a \circ \cdots \circ a \mid k \in \mathbb{Z}\}$

- $\langle \langle a \rangle, \circ, n \rangle$ ist eine Gruppe und wird als **Untergruppe** von $\langle \mathbb{G}, \circ, n \rangle$ bezeichnet
- Wir bezeichnen $\mathrm{ord}(a) = |\langle a \rangle|$ als die **Ordnung** des Elementes a und es gilt $a^{\mathrm{ord}(a)} = n$
- Es gilt grundsätzlich $\mathrm{ord}(a) | \mathrm{ord}(\mathbb{G})$
- Wenn $\langle a \rangle = \mathbb{G}$ (bzw. $\mathrm{ord}(a) = \mathrm{ord}(\mathbb{G})$ wenn $\mathbb{G}$ finit) heißt a **Erzeuger** von $\langle \mathbb{G}, \circ, n \rangle$ und $\langle \mathbb{G}, \circ, n \rangle$ ist eine sogenannte **zyklische Gruppe**

Der Gruppenexponent $\lambda \in [\mathrm{ord}(\mathbb{G})]$ einer finiten Gruppe $\langle \mathbb{G}, \circ, n \rangle$ ist die kleinste Zahl, sodass

$$\forall a \in \mathbb{G}: \; a^{\lambda} = n$$

Modulogruppen

Eine (multiplikative) Modulogruppe ist definiert durch ein $n \in \mathbb{N}$. Die zugehörige Gruppe ist dann $\langle \mathbb{Z}_n^*, \cdot_n, 1 \rangle$, wobei $\mathbb{Z}_n^*$ die Menge aller zu n teilerfremden Zahlen ist und $a \cdot_n b \equiv (a \cdot b) \bmod n$

- Die Ordnung dieser Gruppe ist gegeben durch die eulersche Phi-Funktion $\varphi(n)$
- In Modulogruppen gilt grundsätzlich $a^k \equiv a^{k-\varphi(n)}$
- Eine Modulogruppe ist genau dann zyklisch, wenn $n \in \{2, 4, p^r, 2p^r \mid p \in \mathbb{P}\backslash\{2\}, r \in \mathbb{N}\}$
- (*) Wir können den Gruppenexponenten einer Modulogruppe bestimmen, indem wir die Carmichael-Funktion berechnen: Sei $n = \prod_{p_i \in \mathbb{P}} {p_i}^{r_i}$ die Primfaktorzerlegung von n. Dann ist die Carmichael-Funktion $\lambda(n) = \mathrm{kgV}(\lambda({p_1}^{r_1}), \ldots, \lambda({p_n}^{r_n}))$ und

$$\lambda(p^r) = \begin{cases} \frac{1}{2} \cdot \varphi(p^r), & p = 2 \wedge r > 2 \\ \varphi(p^r), & \text{sonst} \end{cases} \text{ für } p \in \mathbb{P}, r \in \mathbb{N}$$