Einfürung in die Algebra Hausaufgaben Blatt Nr. 4

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: November 16, 2023)

Problem 1. Seien $n \in \mathbb{N}^*, T$ die Menge der positiven Teiler von n und G eine Gruppe der Ordnung n. Für $t \in T$ definieren wir die Mengen

$$M_t := \{g \in G | \text{ord}(g) = t\} \subseteq G.$$

(a) Zeigen Sie, dass jedes $g \in G$ in genau einer der Mengen M_t mit $t \in T$ liegt.

(b) Sei nun zudem G zyklisch. Zeigen Sie, dass dann $|M_t| = \varphi(t)$ für alle $t \in T$ gilt.

(c) Folgern Sie: Für jedes $n \in \mathbb{N}^*$ gilt $n = \sum_{t|n,t>0} \varphi(t)$.

Proof. (a) Sei $g \in G$ beliebig und $H = \langle g \rangle$. H ist eine Untergruppe von G. Es gilt auch, dass $|H| = \text{ord}(g)$. Wir wissen, dass $|H|$ teilt $|G|$. Daraus folgt, dass $\text{ord}(g)$ teilt $|G|$, und g liegt in genau einer der Mengen M_t mit $t \in T$.

(b) Weil G zyklisch ist, gibt es für jede Teiler $t|n$ eine Untergruppe der Ordnung t.

Diese Untergruppe hat genau $\varphi(t)$ Erzeuger. Für alle Erzeuger $p$gilt $\text{ord}(t) = |\langle t \rangle| = t$. Es gilt daher, für jedes $t \in T$, $|M_t| \geq \varphi(t)$.

Außerdem ist die Untergruppe der Ordnung t eindeutig. Deswegen ist genau $|M_t| = \varphi(t)$. Wir nehmen an, dass es $p \in G$ gibt, sodass $\text{ord}(p) = t$, also $|\langle p \rangle| = t$. Weil die zyklische Untergruppe der Ordnung t eindeutig ist, ist die erzeugte Gruppe genau die Gruppe, die wir vorher diskutiert haben, also p ist einer der vorherigen $\varphi(t)$ Erzeuger.

Daraus folgt, dass $|M_t| = \varphi(t)$ für alle $t \in T$.

(c) Es gibt für jedes n eine zyklische Gruppe der Ordnung n, z.B. $\mathbb{Z}/n\mathbb{Z}$.

Alle Element sind in einer der Mengen M_t. Die Zahl der Elemente ist einfach $\sum_{t \in T} |M_t| = \varphi(t) = n$

* jun-wei.tan@stud-mail.uni-wuerzburg.de

□

Problem 2. Zeigen Sie, dass für eine Gruppe G der Ordnung $n \in \mathbb{N}^*$ äquivalent sind:

(a) G ist zyklisch.

(b) G besitzt zu jedem positiven Teiler t von n genau eine Untergruppe der Ordnung t.

Proof. (a) $\Longrightarrow$ (b) ist schon in der Vorlesung bewiesen. (Satz 2.18). Es bleibt (b) $\Longrightarrow$ (a) zu zeigen. Wir betrachten dann ein Element $a \in G$ und die erzeugte zyklische Gruppe $\langle a \rangle$. Falls $\langle a \rangle = G$ sind wir fertig. Also nehmen wir an, $\langle a \rangle \neq G$. Sei $\operatorname{ord}(a) = k$, und $\langle a \rangle = k$. Diese Gruppe besitzt genau $\varphi(k)$ Erzeuger.

Dann wählen wir ein anderes b Element aus, das kein Erzeuger von $\langle a \rangle$ ist. Wir betrachten $\langle b \rangle$. Es muss gelten, dass $\operatorname{ord}(b) = |\langle b \rangle| \neq k$. Sonst wäre $\langle b \rangle = \langle a \rangle$, weil es nur *eine* Untergruppe der Ordnung k gibt.

Ähnlich fahren wir fort. Wir wählen ein Element aus, das kein Erzeuger von der voherigen betrachten zyklischen Gruppen sind. Weil es für jeder Teiler von n nur eine Untergruppe der Ordnung gibt, gilt $|M_t| = \varphi(t)$.

Sei T die Menge der positiven Teiler von n. Wir berechnen

$$\sum_{n \neq t \in T} \varphi(t) < n,$$

also wir haben Elemente, für die gilt, deren Ordnung kein positiver Teiler von n, das weniger als n ist. Weil die Ordnung ein Teiler von n sein muss, muss die Ordnung n sein, also solche Elemente sind Erzeuger der Gruppe G, und G ist zyklisch. □

Problem 3. (a) Bestimmen Sie die Ordnungen der Elemente für jede der Diedergruppen D_n mit $n \geq 3$.

(b) Zeigen Sie, dass Satz 2.23 für nicht-abelsche Gruppen im Allgemeinen falsch ist.

> (Satz 2.23) Sei n die größte Elementordnung in einer abelschen Gruppe G. Dann gilt $g^n = e$ für alle $g \in G$.

Proof. (a) Wir betracten zuerst Elemente mit dem Form $r^k s^0 = r^k$. Wir haben per die letzte Übungsblatt

> Zeigen Sie, dass für $k \in \mathbb{N}$ genau dann $r^k = e$ gilt, wenn $n|k$ ist.

also wir brauchen die kleinste Zahl $\text{ord}(r^k)$, sodass $(r^k)^{\text{ord}(r^k)} = r^{k\text{ord}(r^k)} = r^{pn}, p \in \mathbb{N}$. Per Definition des kleinsten gemeinsamen Vielfaches ist

$$\text{ord}(r^k) = \frac{\text{kgV}(k,n)}{k} = \frac{n}{\text{ggT}(k,n)}.$$

Wir wissen auch, dass $s^2 = e$, also $\text{ord}(s) = 2$.

Jetzt betrachten wir alle Elemente mit dem Form $r^k s$. Es gilt

$$r^k s r^k s = r^k r^{-k} ss = ee = e,$$

also alle Elemente mit dem Form $r^k s$ haben Ordnung 2.

(b) Wir betrachten D_3. Die größte Elementordnung ist 3, weil $\text{ggT}(3,2) = 1$, und $\frac{3}{\text{ggT}(3,2)} = 3$, also r^2 hat Ordnung 3.

Keine größere Elementordnung ist möglich, weil $\frac{n}{\text{ggT}(n,k)} \leq n = 3$, und $2 \leq 3$.

Es gilt aber

$$s^3 = (s^2)s = es = s,$$

also $s^3 \neq e$, ein Widerspruch. $\square$

Problem 4. Sei $n \geq 3$.

(a) Zeigen Sie, dass die Menge $R := \{r^0, r^1, \ldots, r^{n-1}\}$ ein Normalteiler von D_n ist.

(b) Zeigen Sie, dass die Gruppe $\langle x \rangle$ für kein $x \in D_n \backslash R$ ein Normalteiler von D_n ist.

Proof. (a) Wir betrachten $x^{-1}Rx$:

(i) $x = r^p$:

Es gilt $x^{-1} = r^{-p}$. und

$$r^{-p} r^k r^p = r^k,$$

für alle $k \in \mathbb{Z}$, also $r^{-p} R r^p = R$, insbesondere $r^{-p} R r^p \subseteq R$.

(ii) $x = s$:

Es gilt $s^{-1} = s$, und

$$sr^k s = r^{-k} ss = r^{-k} \in S,$$

(Die Behauptung, dass $r^{-k} \in S$, war im letzten Übungsblatt bewiesen).

(iii) $x = r^p s$:

Wir haben schon bewiesen, dass $x^{-1} = r^p s$. Es gilt

$$r^p s r^k r^p s = r^p s r^{k+p} s = r^p r^{-(k+p)} ss = r^{-k} \in R.$$

Insgesamt gilt $x^{-1} R x \subseteq R$ für alle $x \in D_n$, also R ist ein Normalteiler.

(b) Noch einmal betrachten wir die unterschiedlichen Fälle

(i) $x = s$, also $\langle x \rangle = \{e, s\}$:

Es gilt

$$r^{-1} s r = r^{-1} r^{-1} s = r^{-2} s \neq s.$$

(Es gilt $r^{-2} \neq r^0 = e$ wenn $n \geq 3$).

(ii) $x = r^p s$, also $\langle x \rangle = \{e, r^p s\}$.

Es gilt

$$r^{-k} r^p s r^k = r^{-k} r^p r^{-k} s = r^{p-2k} s,$$

was nur ein Element von $\langle x \rangle$ ist, wenn $p - 2k \equiv p \pmod{n}$. Sei zum Beispiel $k = 1$. Weil $n \geq 3$, gilt die Gleichung nie.

Lemma 1. *Für $n \geq 3$ kann*

$$p - 2 \equiv p \pmod{n}$$

nicht gelten, für alle $p \in \mathbb{Z}$

Proof. Die Gleichung $p - 2 \equiv p \pmod{n}$ genau dann, wenn es $k \in \mathbb{Z}$ existiert, sodass

$$p - p - 2 = kn,$$

aber das impliziert

$$2 = kn,$$

was unmöglich ist, weil $n \geq 3 > 2$. □

Also $r^{-1} \langle x \rangle r \not\subseteq \langle x \rangle$

Die Gruppe $\langle x \rangle$ ist dann keine Gruppe für $x \in D_n \backslash R$. □