Einfürung in die Algebra Hausaufgaben Blatt Nr. 4

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: November 25, 2023)

Problem 1. (a) Begründen Sie, dass die Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 8 & 3 & 9 & 1 & 6 & 4 & 2 \end{pmatrix} \in S_9$ in der alternierenden Gruppe A_9 liegt.

(b) Finden Sie i und k, so dass die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 7 & 4 & i & 5 & 6 & k & 9 \end{pmatrix} \in S_9$ gerade ist.

Proof. (a) Wir schreiben zuerst σ als Zyklus

$$\sigma = (176)(259)(384).$$

Dann stellen wir die Zyklus als Produkte von Transpositionen dar, wie im Beweis von 2.44

$$\sigma = (17)(76)(25)(59)(38)(84).$$

Es gibt 6 Transpositionen, also σ ist gerade, und $\sigma \in A_9$.

(b) Weil jede Zahl nur einmal vorkommen darf, gibt es nur zwei Möglichkeiten

$$\begin{aligned} i &= 3 & j &= 8, \\ i &= 8 & j &= 3. \end{aligned}$$

Wir betrachten die zwei Fälle:

(i) $i = 3, j = 8$:

Wir schreiben es als Zyklus, und dann von Transpositionen

$$(3765) = (37)(76)(65),$$

also es ist gerade.

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

(ii) $i = 8, j = 3$ wir machen ähnlich

$$(37658) = (37)(76)(65)(58),$$

also es ist in diesem Fall nicht gerade. □

Problem 2. Es sei $n \in \mathbb{N}^*$. Die Permutationen $\sigma, \tau \in S_n$ seien disjunkt.

(a) Beweisen Sie Lemma 2.41: Es gilt $\sigma\tau = \tau\sigma$.

(b) Folgern Sie: Es ist $\operatorname{ord}(\sigma\tau) = \operatorname{kgV}(\operatorname{ord}(\sigma), \operatorname{ord}(\tau))$.

Proof. (a) Kurze Erinnerung am Definition von disjunkte Permutationen:

Definition 1. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *disjunkt*, falls gilt

$$\begin{aligned} \sigma(i) \neq i &\implies \tau(i) = i, \text{ und} \\ \tau(i) \neq i &\implies \sigma(i) = i \end{aligned}$$

Wir brauchen außerdem eine Ergebnis

Lemma 2. *Sei $\sigma(i) = j \neq i$. Es gilt dann $\sigma(j) \neq j$.*

Proof. Sonst wäre es ein Widerspruch zu die Definition, dass S_n die Gruppe alle bijektive funktionen $\{1, \ldots, n\} \to \{1, \ldots, n\}$ ist. Die Permutation wäre dann nicht injektiv, weil $\sigma(i) = \sigma(j)$, aber per Annahme $i \neq j$ gilt. □

Corollary 3. *Sei $\sigma, \tau \in S_n$ disjunkte Permutationen. Falls $\sigma(i) \neq i$ gilt $\tau\sigma\,(i) = \sigma(i)$.*

Remark 4. *Alle Aussagen here gelten natürlich noch, wenn man die Rollen von σ und τ vertauschen.*

Die Ergebnis folgt jetzt fast sofort. Wir betrachten drei Fälle:

(i) $\sigma(i) \neq i$, also $\tau(i) = i$.

Es gilt dann

$$\sigma\tau(i) \overset{1}{=} \sigma(i) \overset{3}{=} \tau\sigma(i).$$

(ii) $\tau(i) \neq i$, also $\sigma(i) = i$.

$$\tau\sigma(i) \overset{1}{=} \tau(i) \overset{3}{=} \sigma\tau(i).$$

(iii) $\tau(i) = i$ und $\sigma(i) = i$.

$$\tau\sigma(i) = i = \sigma\tau(i).$$

Insgesamt gilt $\tau\sigma = \sigma\tau$.

(b) Es gilt

$$(\sigma\tau)^n = \sigma^n\tau^n$$

wegen (a), weil σ und τ kommutiert, und wir können die Reihenfolge im Produkt

$$\underbrace{\sigma\tau\sigma\tau\dots\sigma\tau}_{n \text{ Mal}}$$

verändern, sodass die σ alle an einer Seite liegen, und die τ an der anderen Seite. Sei $N \ni p \leq \mathrm{kgV}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$. Sei $p = n_1\mathrm{ord}(\sigma) + a = n_2\mathrm{ord}(\tau) + b,\ a, b, n_1, n_2 \in \mathbb{N}, 0 \leq a < \mathrm{ord}(\sigma)$ und $0 \leq b < \mathrm{ord}(\tau)$.

$$\begin{aligned}(\sigma\tau)^p &= \sigma^p\tau^p \\ &= \sigma^{n_1\mathrm{ord}(\sigma)+a}\tau^{n_2\mathrm{ord}(\tau)+b} \\ &= \sigma^{n_1\mathrm{ord}(\sigma)+a}\tau^{n_2\mathrm{ord}(\tau)+b} \\ &= \sigma^{n_1\mathrm{ord}(\sigma)}\sigma^a\tau^{n_2\mathrm{ord}(\tau)}\tau^b \\ &= \sigma^a\tau^b\end{aligned}$$

Per Definition, wenn $p = \mathrm{kgV}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$, ist $a = b = 0$ und

$$(\sigma\tau)^{\mathrm{kgV}(\mathrm{ord}(\sigma),\mathrm{ord}(\tau))} = \sigma^0\tau^0 = 1.$$

Für $p < \mathrm{kgV}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau)$ kann die beide nicht gleichzeitig gelten. Wir betrachten dann $\sigma^a\tau^b$. Per Definition können a und b nicht gleichzeitig 0 sein. Sei zum Beispiel $a \neq 0$. Dann haben wir nie das neutrale Element (es ist egal, was b ist). Sei i_k von σ bewegt (hier nehmen wir an, dass $\sigma \neq 1$). Dann ist i_k nicht von τ bewegt, weil σ und τ disjunkt sind.

$$\sigma^a\tau^b i_k = \sigma^a i_k.$$

Per Definition ist $\sigma^a i_k \neq i_k$ für alle mögliche i_k, sonst wäre $\mathrm{ord}(\sigma) = i_k$. Dann ist $(\sigma\tau)^p \neq 1$ für alle $p < \mathrm{kgV}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$. Ähnlich für $b \neq 0$ betrachten wir alle Elemente, die nicht von σ bewegt sind. Für entweder $\sigma = 1$ oder $\tau = 1$ ist die Behauptung klar. Sei $\sigma = 1$. Dann gilt $\mathrm{ord}(1) = 1$, und $\mathrm{ord}(\sigma\tau) = \mathrm{ord}(\tau) = \mathrm{kgV}(1, \mathrm{ord}(\tau))$. Schluss:

$$\mathrm{ord}(\sigma\tau) = \mathrm{kgV}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau)). \qquad \square$$

Problem 3. (a) Zeigen Sie: Für jeden m-Zykel σ gilt $\mathrm{ord}(\sigma) = m$.

(b) Bestimmen Sie das kleinste $n \in \mathbb{N}$, so dass S_n ein Element der Ordnung 20 enthält.

Proof. (a) Sei $\sigma = (i_1 i_2 \dots i_m)$, mit die i_j paarweise unterschiedlich. Es gilt, für $\mathbb{N} \ni x \leq m$

$$\sigma^x i_k = i_p,$$

wobei $1 \leq p \leq m$ und $p \equiv k + x \pmod n$. $\sigma^x = 1$ genau dann, wenn $\sigma^x i_k = i_k$ für alle k, also $p = k$. Für $x = m$ ist es dann klar, $p = k$, also $\sigma^x = 1$.

Für $x < m$ kann das nicht sein. Das Kongruenz gilt genau dann, wenn

$$k + x - rx = k, \; r \in \mathbb{Z}.$$

Aber per Definition, wenn $r = 1$ ist $k + x - \overset{1}{\cancel{r}}x < k$. Wenn $r = 0$ ist $k + x \neq k$, weil $x \geq 1 > 0$. Also $\sigma^x \neq 1$ für alle $1 < x < m$.

(b) Mit Hilfe von 2 können wir einfach eine solche S_n konstruieren. Sei $n = 9$. Dann haben wir 2 disjunkter Zyklus

$$(12345) \qquad \text{und} \qquad (6789).$$

mit Ordnung 4 und 5 (a). Dann hat das Produkt $(12345)(6789)$ der Ordnung 20, weil 4 und 5 Teilerfremd sind, und daher $\mathrm{kgV}(4, 5) = 4 \times 5 = 20$.

Jetzt betrachten wir die Aufgabe im Allgemein. Sei $n \in \mathbb{N}$ beliebig und σ ein Element von S_n mit der Ordnung 20. Wir können σ als Produkt von k disjunkter Zykel. Die Zykel haben länge $l_i, 2 \leq l_i \leq k \; \forall l_i$ und

$$l_1 + l_2 + \cdots + l_k \leq n.$$

Der Ordnung von σ ist

$$\operatorname{ord}(\sigma) = l_1 l_2 \dots l_n = 20 = 2^2 \times 5.$$

Weil 5 ein Primzahl ist, muss mindestens ein l_1 5 sein. Also oBdA können wir für beliebiges n so versuchen, ein solches Element so konstruieren: Wir nehmen 5 Elemente raus, und versuchen weiter, ein disjunkter Zyklus mit Länge 4 oder 2 disjunkte Zykel mit Länge 2 zu finden. Das heißt, dass wir mindestens 9 Elemente brauchen. Dann ist 9 genau dann die gewünschte Zahl. □

Problem 4. (a) Zeigen Sie, dass die Menge

$$V_4 := \{\sigma \in A_4 | \operatorname{ord}(\sigma) \leq 2\}$$

eine Untergruppe der Ordnung 4 von A_4 (und daher auch S_4) ist.

(b) Zeigen Sie, dass V_4 ein Normalteiler von S_4 (und daher auch A_4) ist.

Hinweis: V_4 heißt auch Kleinsche Vierergruppe.

Proof. (a) Jedes Element $\sigma \in S_4$ lässt sich als Produkt disjunkte Zyklen geschrieben werden. Weil wir haben genau 4 Elemente zu permutieren, muss die Zyklen Länge ≤ 4 haben. Zyklen mit Länge 4 sind ungerade, weil

$$(i_1 i_2 i_3 i_4) = (i_1 i_4)(i_1 i_3)(i_1 i_2),$$

also jedes Element $\sigma \in A_4$ lässt sich als Produkt von Zyklen mit Länge ≤ 3 schreiben.

Sei jetzt $\sigma \in A_4$. Wir nehmen an, dass es ein Produkt von ein Zyklus der Länge 3 und andere Zykeln ist. Dann ist σ genau das Zyklus der Länge 3, dessen Ordnung 3 ist, also $\sigma \notin V_4$.

Jetzt wissen wir: Alle Elemente $\sigma \in V_4$ können als Produkt von Zykeln der Länge 2 geschrieben werden. Wie viele solchen Zykeln gibt es? Wir schreiben alle Möglichkeiten

$$\begin{array}{ccc} (12) & (23) & (34) \\ (13) & (24) & (14) \end{array}$$

□