

Lösung 0

Aufgabe 1.

Für $n \in \{0, 1, 2\}$ ist $|\mathcal{S}_n| \in \{1, 2\}$, und mithin $\mathcal{S}_n$ abelsch.

Für $n \geq 3$ behaupten wir, daß $\mathcal{S}_n$ nicht abelsch ist. In der Tat wird darin

$$\begin{aligned}(1, 2)(2, 3) &= (1, 2, 3) \\ (2, 3)(1, 2) &= (1, 3, 2) .\end{aligned}$$

Aufgabe 2.

(1) Es wird $\langle (1, 2, 3, 4) \rangle = \{\text{id}, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$. Es ist $o(\sigma) = |\langle \sigma \rangle| = 4$ und $\text{sgn } \sigma = -1$.

(2) Es wird

$$\begin{aligned}\langle (1, 2, 5, 6)(3, 4)(8, 7, 10) \rangle &= \{\text{id}, (1, 2, 5, 6)(3, 4)(8, 7, 10), (1, 5)(2, 6)(8, 10, 7), (1, 6, 5, 2)(3, 4), (8, 7, 10), \\ &\quad (1, 2, 5, 6)(3, 4)(8, 10, 7), (1, 5)(2, 6), (1, 6, 5, 2)(3, 4)(8, 7, 10), (8, 10, 7), \\ &\quad (1, 2, 5, 6)(3, 4), (1, 5)(2, 6)(8, 7, 10), (1, 6, 5, 2)(3, 4)(8, 10, 7)\} .\end{aligned}$$

Es ist $o(\sigma) = |\langle \sigma \rangle| = 12$ und $\text{sgn } \sigma = (-1) \cdot (-1) \cdot (+1) = +1$.

(3) Zunächst schreiben wir $\sigma = (1, 2)(2, 3) = (1, 2, 3)$ als Produkt *disjunkter* Zykeln. Dann erhalten wir $\langle (1, 2, 3) \rangle = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$. Es ist $o(\sigma) = |\langle \sigma \rangle| = 3$ und $\text{sgn } \sigma = +1$. (Für das Signum hätte man keine disjunkten Zykeln benötigt.)

Aufgabe 3.

(1) Wir müssen bestimmen, wieviele reguläre Matrizen der Größe $n \times n$ mit Einträgen in K es gibt. In die erste Spalte können wir alle Vektoren bis auf den Nullvektor einstellen, haben dafür also $q^n - q^0$ Möglichkeiten. In die zweite Spalte können wir alle Vektoren bis auf die im Erzeugnis der ersten Spalte einstellen, haben dafür also $q^n - q^1$ Möglichkeiten. In die dritte Spalte können wir alle Vektoren bis auf die im Erzeugnis der ersten beiden Spalten einstellen, haben dafür also $q^n - q^2$ Möglichkeiten. Und so fort. Insgesamt erhalten wir

$$|\text{GL}_n(K)| = (q^n - q^0)(q^n - q^1) \cdots (q^n - q^{n-1}) .$$

(Formal: man zeigt die Behauptung, es gebe $\prod_{k=1}^l (q^n - q^k)$ Matrizen in $K^{n \times l}$ von Rang l mit Induktion nach l .)

(2) Sei G eine endliche Gruppe, und sei $U \leq G$. Auf G können wir die Äquivalenzrelation $x \sim y :\iff x \in yU$ einführen. Die Äquivalenzklasse von x ist dann gerade xU , und diese Teilmenge steht in Bijektion zu U , via $U \longrightarrow xU, u \longmapsto xu$. Damit ist G in Äquivalenzklassen der Kardinalität $|U|$ zerlegt, und damit ist $|U|$ ein Teiler von $|G|$.

(3) Um nun zu zeigen, daß $n!(q-1)^n$ ein Teiler von $|\text{GL}_n(K)|$ ist, genügt es mit (2), eine Untergruppe von $\text{GL}_n(K)$ von Ordnung $n!(q-1)^n$ zu finden. Wir können dazu etwa die Untergruppe der *monomialen Matrizen* verwenden.

Eine monomiale Matrix hat in jeder Zeile und in jeder Spalte genau einen Eintrag ungleich Null aus K . Eine monomiale Matrix ist regulär. Die Einheitsmatrix ist monomial. Sind A und B monomial, so auch AB^{-1} . Damit handelt es sich bei der Menge M der monomialen Matrizen um eine Untergruppe von $\text{GL}_n(K)$.

Für die Wahl der Positionen der Einträge ungleich 0 haben wir $n!$ Möglichkeiten, und für jeden der dieser n Einträge dann noch $q-1$ Möglichkeiten. Somit ergibt sich in der Tat $|M| = n! \cdot (q-1)^n$.

Gilt für $q \in \mathbf{Z}$ beliebig, daß $n! \cdot (q-1)^n$ ein Teiler von $(q^n - q^0)(q^n - q^1) \cdots (q^n - q^{n-1})$ ist?

Aufgabe 4.

- (1) Das Minimalpolynom einer Matrix von Ordnung 7 teilt $X^7 - 1$. Da wir in $\mathbf{F}_2[X]$ die Zerlegung

$$X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

in irreduzible Faktoren besitzen, und das Minimalpolynom $X + 1$ die Ordnung 1 nach sich zöge, erhalten wir als mögliche Minimalpolynome $X^3 + X + 1$ und $X^3 + X^2 + 1$. Die rationale Normalformen, die Ordnung 3 haben, sind folglich

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Dies sind dann Repräsentanten der Konjugiertenklassen.

- (2) Zunächst bemerken wir, daß jede der angegebenen Potenzen von Ordnung 7 ist, und damit in einer der beiden unter (1) angeführten Klassen liegt.

Mit z.B. $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ folgt aus $A^3 + A + E = 0$ durch Multiplikation mit A^{-3} , daß $E + A^{-2} + A^{-3} = 0$. Somit ist das Minimalpolynom von $A^6 = A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ gegeben durch $X^3 + X^2 + 1$, und folglich sind A und A^6 nicht konjugiert.

(Die Klasseneinteilung der Potenzen erfolgt in $\{A, A^2, A^4\}$ und $\{A^{-1}, A^{-2}, A^{-4}\} = \{A^6, A^5, A^3\}$, genauso für die andere in (1) angegebene Matrix.)

- (3) Das Minimalpolynom einer Matrix, welche $A^8 = 1$ erfüllt, teilt $X^8 - 1 = (X + 1)^8$. Da das Minimalpolynom von Grad ≤ 3 ist, muß es also auch $X^4 - 1$ teilen. Damit erfüllt diese Matrix auch $A^4 = 1$, und ist somit nicht von Grad 8.
- (4) Mit $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{F}_2 \right\} \leq G$ gibt es aber sehr wohl eine Untergruppe der Ordnung 8 – notwendigerweise nicht zyklisch.