

Lösung zur Vordiplomsklausur

Aufgabe 1

- (1) Wir haben $\binom{5}{3} = 10$ Möglichkeiten.
- (2) Die Konjugationsklasse von $(1, 2)(3, 4)(5, 6)$ in S_8 enthält $\frac{8!}{2^3 \cdot 2! \cdot 3!} = 420$ Elemente.
- (3) Die Anzahl der surjektiven Abbildungen von $\{1, 2, 3, 4, 5\}$ nach $\{1, 2, 3, 4\}$ ergibt sich zu

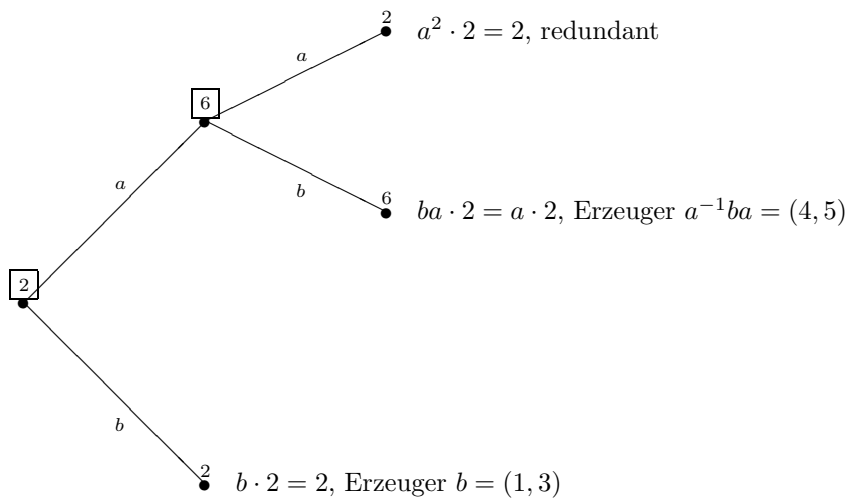
$$\sum_{i=0}^4 (-1)^i \binom{4}{i} (4-i)^5 = 1 \cdot 4^5 - 4 \cdot 3^5 + 6 \cdot 2^5 - 4 \cdot 1^5 + 1 \cdot 0^5 = 240.$$

- (4) Die Anzahl der normierten irreduziblen Polynome von Grad 8 in $\mathbf{F}_3[X]$ ergibt sich zu

$$\frac{1}{8} \sum_{d|8} 3^d \mu(8/d) = \frac{1}{8} (-3^4 + 3^8) = 810.$$

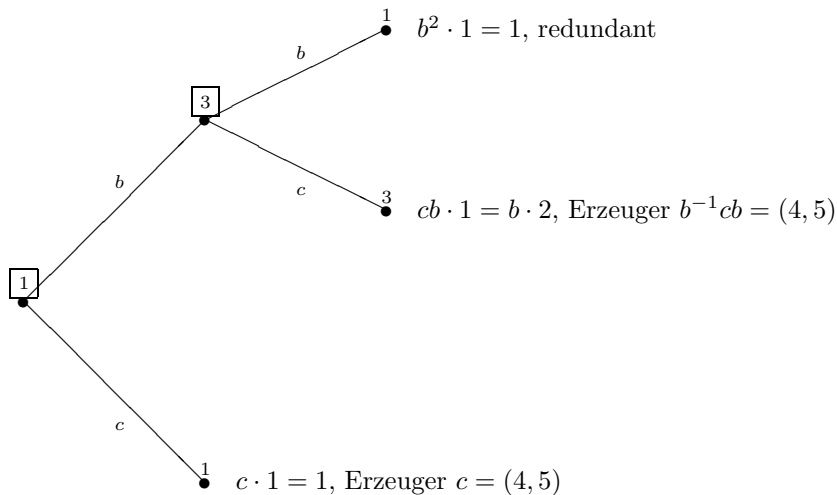
Aufgabe 2

Wir erstellen einen Baum zur Berechnung von $G \cdot 2$ und von $\text{Stab}_G(2)$.



Somit ist $G \cdot 2 = \{2, 6\}$, und $|G \cdot 2| = 2$ (Antwort zu (1)). Ferner ist $\text{Stab}_G(2) = \langle b = (1, 3), c := (4, 5) \rangle$.

Wir erstellen einen Baum zur Berechnung von $\text{Stab}_G(2) \cdot 1$ und von $\text{Stab}_G(1)$.



Somit ist $\text{Stab}_G(2) \cdot 1 = \{1, 3\}$, und $|\text{Stab}_G(2) \cdot 1| = 2$ (Antwort zu (2)). Ferner ist $\text{Stab}_G(1, 2) = \langle c = (4, 5) \rangle$.

Direkt erkennen wir, daß $\text{Stab}_G(1, 2) \cdot 4 = \{4, 5\}$ und $|\text{Stab}_G(1, 2) \cdot 4| = 2$ (Antwort zu (3)).

Insgesamt wird $|G| = \frac{|G|}{|\text{Stab}_G(1)|} \cdot \frac{|\text{Stab}_G(1)|}{|\text{Stab}_G(1,2)|} \cdot |\text{Stab}_G(1, 2)| = |G \cdot 2| \cdot |\text{Stab}_G(2) \cdot 1| \cdot |\text{Stab}_G(1, 2)| = 2 \cdot 2 \cdot 2 = 8$ (Antwort zu (4)).

Aufgabe 3

- (1) Mittels des Euklidischen Algorithmus bestimmen wir Polynome $s(X)$ und $t(X)$ so, daß

$$1 = s(X) \cdot (X^5 + X^2 + 1) + t(X) \cdot (X^2 + 1).$$

Wir erhalten z.B.

$$1 = X \cdot (X^5 + X^2 + 1) + (X^4 + X^2 + X + 1) \cdot (X^2 + 1).$$

Einsetzen von δ gibt

$$1 = \delta \cdot (\delta^5 + \delta^2 + 1) + (\delta^4 + \delta^2 + \delta + 1) \cdot (\delta^2 + 1) = (\delta^4 + \delta^2 + \delta + 1) \cdot (\delta^2 + 1),$$

und also $(\delta^2 + 1)^{-1} = \delta^4 + \delta^2 + \delta + 1$.

- (2) Es ist $\mathbf{F}_{32}^* \simeq C_{31}$. Da 31 prim ist, ist diese Gruppe von jedem Element ungleich 1 erzeugt. Da $\delta^2 + 1 \neq 1$, ist insbesondere $\delta^2 + 1$ ein Erzeuger von \mathbf{F}_{32}^* .

Aufgabe 4

Die Inzidenzmatrix unseres Graphen ist $A := \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 1 \end{pmatrix}$. Der Eintrag an Position (i, j) von A^2 gibt die Anzahl der Kantenzüge der Länge 2 von i nach j . Wir müssen also alle Einträge von A^2 aufaddieren. Da $A^2 = \begin{pmatrix} 6 & 4 & 6 \\ 4 & 8 & 4 \\ 6 & 4 & 6 \end{pmatrix}$, erhalten wir 48 Kantenzüge der Länge 2.

Aufgabe 5

- (1) Es ist $(11 - 1) \cdot (7 - 1) = 60$. Mittels Euklid ermittelt man, daß $1 = 2 \cdot 60 - 17 \cdot 7$. Das Inverse von $v = 7$ in $\mathbf{Z}/60\mathbf{Z}$ wird also repräsentiert von -17 , oder aber, im vorgeschriebenen Intervall, von $e = 43$.
- (2) Es ist $5^7 \equiv_{11 \cdot 7} 47$.
- (3) Es ist $2^{43} \equiv_{11 \cdot 7} 30$.

Aufgabe 6

- (1) Die Erzeugermatrix in Zeilenstufenform ist $\begin{pmatrix} 1 & 0 & \omega & \omega \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Dies liefert z.B. die Prüfmatrix $\begin{pmatrix} \omega & \omega \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- (2) Es gibt in der Prüfmatrix kein linear abhängiges Zeilentupel der Länge 1 (d.h. keine Nullzeile), wohl aber ein linear abhängiges Zeilentupel der Länge 2, bestehend aus der 2-ten und der 4-ten Zeile. Somit erhalten wir den Minimalabstand $d(C) = 2$.

Aufgabe 7

- (1) Als Nullstelle ergibt sich durch Probieren zunächst etwa β^3 . Daraus erhalten wir die weiteren Nullstellen $(\beta^3)^2 = \beta^6$ und $(\beta^3)^4 = \beta^{12} = \beta^5$. Da $\deg f = 3$ ist, erhalten wir $\{\beta^3, \beta^5, \beta^6\}$ als Nullstellenmenge von $f(X)$. Alternativ hat diese Menge auch die Form $\{\beta + 1, \beta^2 + \beta + 1, \beta^2 + 1\}$.
- (2) Es ist β eine primitive 7-te Einheitswurzel (da $\beta \neq 1$). Deren 2 aufeinanderfolgende Potenzen β^5 und β^6 sind Nullstellen von $f(X)$. Also beträgt der designierte Minimalabstand $2 + 1 = 3$.
- (3) Eine Prüfmatrix von C ist gegeben durch

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

In dieser ist jedes aus 2 Zeilen bestehende Tupel linear unabhängig, wie eine direkte Prüfung ergibt. Also ist $d(C) \geq 3$. Hierfür kann man alternativ auch das Ergebnis aus (2) heranziehen.

Hingegen ist das aus der 1-ten, der 2-ten und der 4-ten Zeile gebildete Tupel linear abhängig. Also ist auch $d(C) \leq 3$.

Im vorliegenden Fall stimmen also Minimalabstand und designierter Minimalabstand überein.

Alternativ kann man auch mit (2) und der Standarderzeugermatrix arbeiten.

- (4) Der Minimalabstand ist $d = d(C) = 3$, die Länge ist $N = 7$. Die Hammingsschranke ergibt sich für diese Parameter zu $7 - \log_2(V_2(7, 1)) = 7 - \log_2\left(\binom{7}{0} + \binom{7}{1}\right) = 7 - 3 = 4$. Die Dimension von C ist ebenfalls gleich 4. Die Hammingsschranke, die eine obere Schranke für diese Dimension darstellt, wird also angenommen.

Aufgabe 8

Die Aussage ist richtig. Es ist $U \cap V$ eine Untergruppe von U , und folglich $|U \cap V|$ ein Teiler von $|U|$. Genauso ist $U \cap V$ eine Untergruppe von V , und folglich $|U \cap V|$ ein Teiler von $|V|$. Da der größte gemeinsame Teiler von $|U|$ und $|V|$ gleich 1 ist, folgt $|U \cap V| = 1$, und also $U \cap V = \{1\}$.