Vortrag 12: Kap. §4.1, §4.2

CAYLEYGRAPHEN & DER CAYLEYGRAPH VON $PSL_2(q)$

§1 Cayleygraphen

1.1 Def.

Sei G eine (endliche oder unendliche) Gruppe, sei $\emptyset \neq S \subseteq G$ endliche Teilmenge mit

$S = S^{-1}$ (d.h. S ist symmetrisch)

Der Cayleygraph $\Gamma(G,S)$ ist definiert als der Graph mit

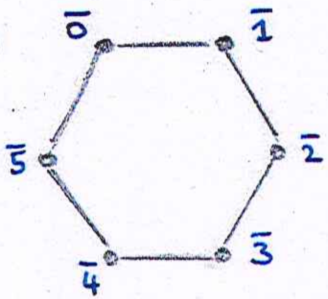
- Eckenmenge $V = G$
- Kantenmenge $E = \{\{x,y\} \mid x,y \in G, \exists s \in S: y = xs\}$

D.h. zwei Ecken sind benachbart genau dann, wenn die eine durch Verknüpfung (von rechts) mit einem Element aus S aus der anderen entsteht.
Da S symmetrisch ist, ist diese Relation symmetrisch und der Graph ist ungerichtet
(Wir wählen keine Orientierung/Pfeile für die Kanten)

$$\exists s \in S: y = xs \overset{S=S^{-1}}{\Longleftrightarrow} \exists s^{-1} \in S: ys^{-1} = x$$

1.2 Beispiele

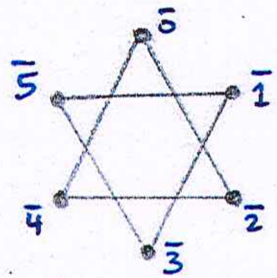
a)



$G = \mathbb{Z}/6$

$S = \{\bar{1}, \bar{5}\}$

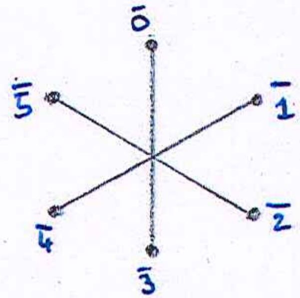
b)



$G = \mathbb{Z}/6$

$S = \{\bar{2}, \bar{4}\}$

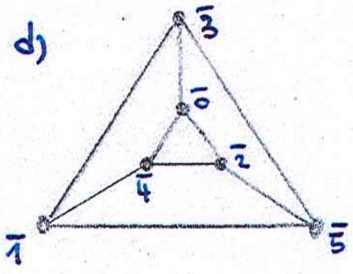
c)



$G = \mathbb{Z}/6$

$S = \{\bar{3}\}$

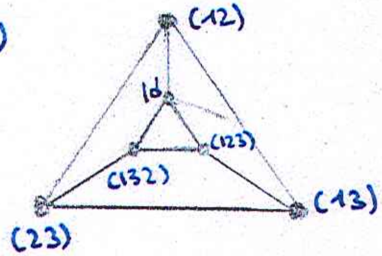
d)



$G = \mathbb{Z}/6$

$S = \{\bar{2}, \bar{4}, \bar{3}\}$

e)

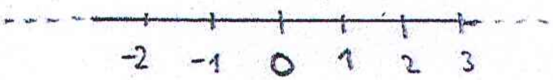


$G = \mathrm{Sym}(3)$

$S = \{(123), (132), (12)\}$

Bem: Nicht isomorphe Gruppen können isomorphe Cayleygraphen haben.

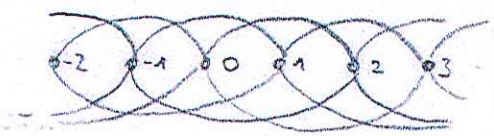
f)



$G = \mathbb{Z}$

$S = \{1, -1\}$

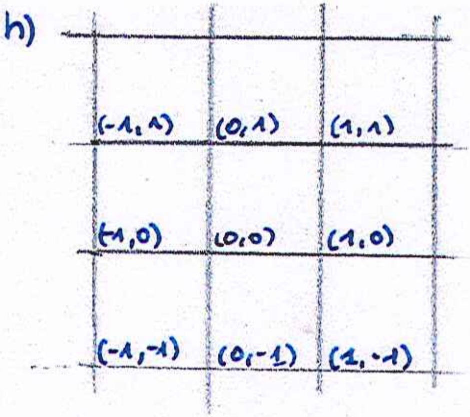
g)



$G = \mathbb{Z}$

$S = \{2, 3, -2, -3\}$

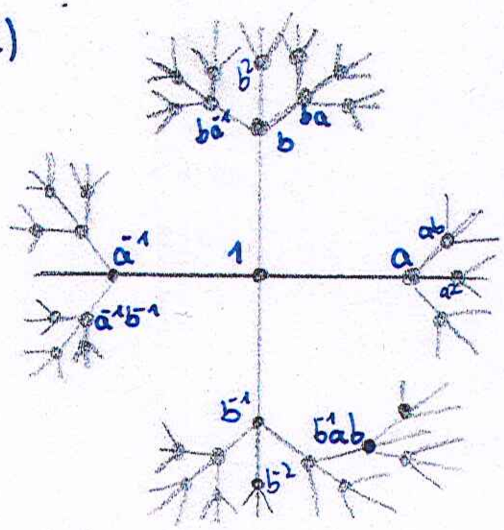
h)



$G = \mathbb{Z} \times \mathbb{Z}$

$S = \{(1,0), (-1,0), (0,1), (0,-1)\}$

i)



$G = F_2 = F(\{a, b\})$

$S = \{a, a^{-1}, b, b^{-1}\}$

Bem: Im Allgemeinen gilt für die freie Gruppe F_m über m Erzeugern $a_1, \dots, a_m$ mit
$S = \{a_1, a_1^{-1}, a_2, \dots, a_m, a_m^{-1}\}$,
dass der Cayleygraph $\Gamma(F_m, S)$ der $2m$-reguläre Baum ist

1.3. Erinnerung

Ein Graph $X=(V,E)$ mit Adjazenzmatrix $A=(a_{ij})_{i,j}$ ($a_{ij}=a_{v_i v_j}$ *Anzahl der Kanten, die v_i mit v_j verbinden*) heißt

- **einfach**, wenn gilt:

$$a_{ij}\in\{0,1\}\quad\forall i,j$$

- **k-regulär**, wenn gilt:

$$\sum_i a_{ij}=k\quad\forall v_j\in V$$

↳ *Ist ein Graph einfach und k-regulär, dann heißt das, dass jede Ecke genau k Nachbarn hat.*

- **bi-partit**, wenn gilt:

Es existiert eine Partition $V=V_+\dot\cup V_-$ der Ecken, sodass $\forall\ \{u,v\}\subseteq V$ mit $a_{u,v}\neq 0$ gilt:

$$u\in V_+\Rightarrow v\in V_-$$
$$u\in V_-\Rightarrow v\in V_+$$

(Ecken von X können in 2 Farben gefärbt werden, sodass benachbarte Ecken verschiedene Farben haben)

1.4 Proposition

Sei $\Gamma(G,S)$ ein Cayleygraph, setze $k:=\#S$. Dann gilt

i) $\Gamma(G,S)$ ist ein einfacher, k-regulärer Graph, und die Wirkung
$$G\curvearrowright\Gamma(G,S)$$
$$g\mapsto[x\mapsto gx]$$
ist transitiv.

ii) $\Gamma(G,S)$ enthält keine Schleifen $\Leftrightarrow 1\notin S$

iii) $\Gamma(G,S)$ ist zusammenhängend $\Leftrightarrow G=\langle S\rangle$

iv) Gibt es einen Gruppenhomomorphismus
$$f: G\longrightarrow(\{1,-1\},\cdot)$$
mit $f(S)=\{-1\}$

$\Rightarrow$ dann ist $\Gamma(G,S)$ bi-partit.

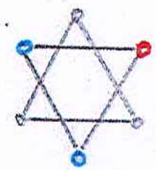
Die Umkehrung gilt, wenn $\Gamma(G,S)$ zsmhgd. ist.

Bemerkung

Die Beispiele b) und c) sind nicht zusammenhgd.
$$\langle\{\bar 3\}\rangle\neq\mathbb{Z}/6\neq\langle\{\bar 2,\bar 4\}\rangle$$

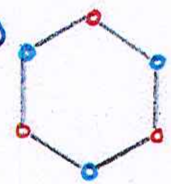
Die Beispiele b), d), e) und g) sind nicht bi-partit.

b)



nicht bi-partit

a)



bi-partit

Beweis von 1.4

i) Die Adjazenz-Matrix von $\Gamma(G,S)$ ist

$$a_{ij} = \begin{cases} 1, & \text{wenn } s \in S \text{ exist. sodass } v_j = v_i s \\ 0, & \text{sonst} \end{cases}$$

$\Rightarrow$ $\Gamma(G,S)$ ist einfach und k-regulär.

Sei nun $G \curvearrowright \Gamma(G,S)$ Wirkung von links.

$$g \mapsto [x \mapsto gx]$$

z.z.: Wirkung ist transitiv.

Seien $x, y \in V$ beliebige Ecken. Wähle

$g := yx^{-1} \in G$ (weil G Gruppe)

$\Rightarrow$ $gx = yx^{-1}x = y$ $\Rightarrow$ Wirkung ist transitiv.

ii) Angenommen, $\Gamma(G,S)$ enthält Schleife

$\Rightarrow \exists s \in S: x = xs \Rightarrow s = 1 \Rightarrow 1 \in S$

Ist $1 \in S \Rightarrow x \cdot 1 = x \Rightarrow$ Es gibt Kante von x nach x

iii) $\Gamma(G,S)$ ist zsh. $\Leftrightarrow$ jedes $x \in G$ ist mit $1 \in G$ über einen Kantenweg verbunden

$\Leftrightarrow$ jedes $x \in G$ kann als Wort über S dargestellt werden

$\Leftrightarrow$ S erzeugt G

iv) „$\Rightarrow$" Ist der Gruppenhomom. $f: G \to (\{\pm 1\}, \cdot)$ mit $f(S) = \{-1\}$ gegeben, so definiere

$$V_+ = \{x \in G : f(x) = +1\}$$
$$V_- = \{x \in G : f(x) = -1\}$$

z.z.: $V = V_+ \cup V_-$ ist Bi-partition.

Betrachte benachbarte Ecken $x, y \in V$ $\quad x \text{ — } y = xs$

$\Rightarrow \exists s \in S$ mit $y = xs$

Dann ist

$$f(y) = f(xs) \overset{\text{Gr.hom.}}{=} f(x) f(s) \overset{s \in V_-}{=} f(x) \cdot (-1)$$
$$= \begin{cases} 1, & f(x) = -1 \\ -1, & f(x) = 1 \end{cases}$$

$$\Rightarrow \begin{cases} x \in V_- \Rightarrow y \in V_+ \\ x \in V_+ \Rightarrow y \in V_- \end{cases} \Rightarrow \text{bi-partit}$$

„$\Leftarrow$" Sei $\Gamma(G,S)$ zsmh. und bi-partit mit $V = V_+ \cup V_-$, wobei $1 \in G$ in V_+ enthalten ist.

Jedes $s \in S$ ist mit 1 verbunden

$\overset{\text{bipartit}}{\Longrightarrow}$ 1 und s liegen in verschiedenen Mengen $\Rightarrow S \subseteq V_-$

Definiere

$$f: G \to \{\pm 1\}, \quad f(x) = \begin{cases} 1, & \text{falls } x \in V_+ \\ -1, & \text{falls } x \in V_- \end{cases}$$

Da $\Gamma(G,S)$ zsmh. ist, erzeugt S G (iii).

Sei $\ell_S(x)$ die Wortlänge von $x \in G$ bzgl. S.

$\Rightarrow$ $f(x) = (-1)^{\ell_S(x)}$

z.z.: f ist Gruppenhomomorphismus

Seien $x, y \in G$ beliebig.

$$f(xy) = (-1)^{\ell_S(xy)} = (-1)^{\ell_S(x) + \ell_S(y) - 2k}$$
$$= (-1)^{\ell_S(x) + \ell_S(y)} = (-1)^{\ell_S(x)} \cdot (-1)^{\ell_S(y)}$$
$$= f(x) f(y)$$

$\Rightarrow$ f ist Gruppenhomomorphismus

§2 Der Cayleygraph von $PSL_2(q)$

2.1 Prop. A

Sei q eine ungerade Primzahlpotenz

$\Rightarrow$ Dann existieren $x, y \in \mathbb{F}_q$ mit

$$x^2 + y^2 + 1 = 0$$

Beweis:

In $\mathbb{F}_q$ gibt es (0 mitgezählt)

$\frac{q+1}{2}$ Quadratzahlen.

Definiere

$$A_+ := \{ 1 + x^2 : x \in \mathbb{F}_q \}$$

$$A_- := \{ -y^2 : y \in \mathbb{F}_q \}$$

Da

$$\# A_+ = \# A_- = \frac{q+1}{2}$$

$\#\mathbb{F}_q = q$

$$\Rightarrow \quad A_+ \cap A_- \neq \emptyset$$

$\Rightarrow$ Es exist. $x, y \in \mathbb{F}_q$ mit

$$1 + x^2 = -y^2 \iff 1 + x^2 + y^2 = 0$$

Prop. B

Sei K ein Körper mit $\mathrm{char}(K) \neq 2$.

Angenommen, es gibt $x, y \in K$ mit:

$$x^2 + y^2 + 1 = 0$$

$\Rightarrow$ Dann ist $\mathbb{H}(K) \cong K^{2\times 2}$,

wobei der Isomorph. $\psi : \mathbb{H}(K) \longrightarrow K^{2\times 2}$ gegeben ist durch: $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(K)$

$$\psi(\alpha) = \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}$$

und es gilt für $\alpha \in \mathbb{H}(K)$

i) $\det(\psi(\alpha)) = N(\alpha)$ und

$\mathrm{Tr}(\psi(\alpha)) = \alpha + \bar{\alpha}$

ii) Gilt $\alpha = \bar{\alpha}$

$$\Rightarrow \psi(\alpha) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \lambda \in K \quad \text{Skalare Matrix}$$

Erinnerung: (Vortrag 9 §5.1)

$S_p = \{ \alpha_1, \bar{\alpha}_1, \ldots, \alpha_s, \bar{\alpha}_s, \beta_1, \ldots, \beta_t \} \subseteq \mathbb{H}(\mathbb{Z})$

ist Menge von Quaternionen der Norm p

Es gilt: $\# S_p = p + 1$, $\forall i$:

- α_i hat $a_0 > 0 \Rightarrow \bar{\alpha}_i \in S_p$

2.2 Konstruktion von $S_{p,q}$

Seien $p \neq q$ ungerade Primzahlen, sei

$\tau_q : \mathbb{H}(\mathbb{Z}) \longrightarrow \mathbb{H}(\mathbb{F}_q)$ die Projektion

$\overset{\text{Prop. A}}{\Longrightarrow} \exists\, x, y \in \mathbb{F}_q$ mit: $x^2 + y^2 + 1 = 0 \mod q$

$\overset{\text{Prop. B}}{\Longrightarrow} \exists$ Isomorphismus

$\psi_q : \mathbb{H}(\mathbb{F}_q) \xrightarrow{\cong} \mathbb{F}_q^{2\times 2}$ mit

a) $N(\alpha) = \det \psi_q(\alpha)$ für $\alpha \in \mathbb{H}(\mathbb{F}_q)$

b) Gilt für $\alpha \in \mathbb{H}(\mathbb{F}_q)$ $\alpha = \bar{\alpha}$

$\Rightarrow$ so ist $\psi_q(\alpha)$ eine Skalarmatrix

Für $\alpha \in S_p$ gilt:

$$\psi_q(\tau_q(\alpha)) \in GL_2(q) \subseteq \mathbb{F}_q^{2\times 2}$$

denn:

$$\det \psi_q(\tau_q(\alpha)) \overset{a)}{=} N(\alpha) \overset{\alpha \in S_p}{=} p \neq q$$

Außerdem ist

$$\psi_q(\tau_q(\alpha\bar{\alpha})) = \psi_q(\tau_q(\bar{\alpha}\alpha))$$

eine Skalarmatrix $\neq 0$ in $GL_2(q)$ $\quad (N(\alpha\bar{\alpha}) = p^2)$

Sei weiter

$$\varphi : GL_2(q) \twoheadrightarrow PGL_2(q) = GL_2(q) \Big/ \underbrace{\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{F}_q \right\}}_{\ker \varphi}$$

Homomorphismus,

dessen Kern genau die Untergr. der Skalarmatrizen ist

Also:

$$\begin{array}{ccccc} \mathbb{H}(\mathbb{Z}) & \overset{\tau_q}{\twoheadrightarrow} & \mathbb{H}(\mathbb{F}_q) & \xrightarrow[\cong]{\psi_q} & \mathbb{F}_q^{2\times 2} \\ & & & & \cup\!\!\mid \\ & & & & GL_2(q) \overset{\varphi}{\twoheadrightarrow} PGL_2(q) \end{array}$$

Setze nun

$$S_{p,q} := (\varphi \circ \psi_q \circ \tau_q)(S_p)$$

Unter den Abbildungen ist α invers zu $\bar{\alpha}$

und wegen $-\beta = \beta$

ist das Bild von β zu sich selbst invers

$\Rightarrow$ $S_{p,q}^{-1} = S_{p,q}$

und es gilt: $S_{p,q} \subseteq PGL_2(q)$

2.3 Lemma

Ist $q > 2\sqrt{p} \Rightarrow \# S_{p,q} = p+1$

Beweis:

Seien $\alpha = a_0 + a_1 i + a_2 j + a_3 k$

$\beta = b_0 + b_1 i + b_2 j + b_3 k$

$\alpha, \beta \in S_p$, $\alpha \neq \beta$. Zz: $\varphi \circ \psi_q \circ \tau_q(\alpha) \neq \varphi \circ \psi_q \circ \tau_q(\beta)$

Es gibt $i \in \{0,1,2,3\}$ mit $a_i \neq b_i$

Da $N(\alpha) = N(\beta) = p \Rightarrow a_l, b_l \in (-\sqrt{p}, \sqrt{p})\ \forall l \in \{0,1,2,3\}$

Ist $q > 2\sqrt{p} \Rightarrow a_i \not\equiv b_i \pmod{q}$

und $\tau_q(\alpha) \neq \tau_q(\beta)$

Setze $A := \psi_q \circ \tau_q(\alpha)$

$B := \psi_q \circ \tau_q(\beta)$

$\Rightarrow A \neq B$ in $GL_2(q)$ Zz: $\varphi_A \neq \varphi_B$

A: $\varphi_A = \varphi_B$ in $PGL_2(q)$

$\Rightarrow$ Dann gibt es $\lambda \in \mathbb{F}_q^\times$, $\lambda \neq 1$ mit $A = \lambda B$

Betrachte die Determinanten:

$p = \det A = \lambda^2 \det B = \lambda^2 p$

$\Rightarrow \lambda = 1$ oder $\lambda = -1$

$\lambda = 1$ wäre bereits Widerspr.

$\lambda = -1 \Rightarrow A = -B \Rightarrow \alpha \equiv -\beta \pmod{q}$

d.h. $a_l \equiv -b_l \pmod{q}\ \forall l \in \{0,1,2,3\}$

Da $q > 2\sqrt{p} \Rightarrow a_l = -b_l$

$\Rightarrow \alpha = -\beta$

Nach Ann. $a_0, b_0 \geq 0$

$\Rightarrow a_0 = b_0 = 0$

$\Rightarrow \beta = \bar{\alpha}$ ↯

Dies steht jedoch im Widerspruch zur Def. von S_p,

denn: für $\alpha \in S_p$ mit $a_0 = 0$ folgt $\bar{\alpha} \notin S_p$.

2.4 Der Cayleygraph von $PSL_2(q)$

a) Ist p Quadratzahl modulo q,

$\Rightarrow S_{p,q} \subseteq PSL_2(q)$

wir definieren: $X^{p,q} := \Gamma(PSL_2(q), S_{p,q})$

b) Ist p keine Quadratzahl modulo q,

$\Rightarrow S_{p,q} \subseteq PGL_2(q) - PSL_2(q)$

wir definieren: $X^{p,q} := \Gamma(PGL_2(q), S_{p,q})$

2.5 Theorem

Seien $p \neq q$ ungerade Primzahlen, $q > 2\sqrt{p}$

$\Rightarrow$ Die Graphen $X^{p,q}$

sind zusammenhängende, $(p+1)$-reguläre

Ramanujan Graphen.

Weiter gilt:

a) Ist p eine Quadratzahl modulo q

$\Rightarrow$ $X^{p,q}$ ist nicht bi-partiter Graph

mit $\frac{q(q^2-1)}{2}$ Ecken, der die

folgende Abschätzung für den Umfang erfüllt:

$$g(X^{p,q}) \geq 2 \log_p q$$

b) Ist p keine Quadratzahl modulo q,

$\Rightarrow$ $X^{p,q}$ ist bi-partiter Graph mit

$q(q^2-1)$ Ecken, der die folgende

Abschätzung für den Umfang erfüllt:

$$g(X^{p,q}) \geq 4 \log_p q - \log_p 4$$

2.6 Bemerkung

Beweisteile:

i) Lemma 2.3 und Prop. 1.4(i) $\Rightarrow$ $(p+1)$-regulär

ii) Anzahl der Ecken entspricht der Kardinalität

von $PSL_2(q)$ bzw. $PGL_2(q)$

$\rightsquigarrow$ siehe Vortrag 10 §1.7

iii) im Fall b): Betrachte den Gruppenhomom.

$$f: PGL_2(q) \longrightarrow PGL_2(q) / PSL_2(q) \cong \{\pm 1\}$$

Es gilt $f(S_{p,q}) = \{-1\} \xRightarrow{\text{Prop. 1.4 (iv)}}$ bi-partit

iv) Außerdem kann man nachrechnen:

$X^{p,q}$ hat keine Schleifen ($1 \notin S_{p,q}$ nach 1.4 ii)

Ausblick:

v) Zusammenhang von $X^{p,q}$ wichtig $\rightsquigarrow$ §4.3

Nach 1.4 (iii) genügt es dafür zu zeigen:

$S_{p,q}$ erzeugt $PSL_2(q)$ bzw. $PGL_2(q)$

(mit stärkerer Voraussetzung: $q > p^8$)

vi) Für festes p ist $(X^{p,q})_{q \text{ prim}}$

Familie von Expandergraphen.

Man kann die untere Schranke der

spektralen Lücke explizit berechnen.