Seminarvortrag 12: Matthis Brandwitte

Cayley-Graphen, der Cayley-Graph von $PSL_2(\mathbb{F}_q)$

§1 Cayley-Graphen

1.1 Definition/Erinnerung

Sei G eine Gruppe und S eine nichtleere, endliche, symmetrische Teilmenge von G (d.h. $S = S^{-1}$)
Wir definieren den Cayley-Graphen $\mathcal{G}(G,S)$ als Graphen mit Eckenmenge $V = G$ und Kantenmenge $E = \{(x,y) \in G \times G \mid \exists s \in S : y = x \cdot s\}$

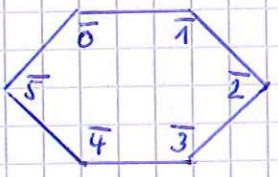
1.2 Bemerkung

Da S symmetrisch ist, ist die Kantenbildung symmetrisch, d.h. $(x,y) \in E \Leftrightarrow (y,x) \in E$, da:
$(x,y) \in E \Leftrightarrow \exists s \in S: y = xs \Leftrightarrow x = y \cdot s^{-1} \Leftrightarrow (y,x) \in E$, da $s^{-1} \in S$
Es werden also nur ungerichtete Graphen betrachtet

1.3 Beispiele

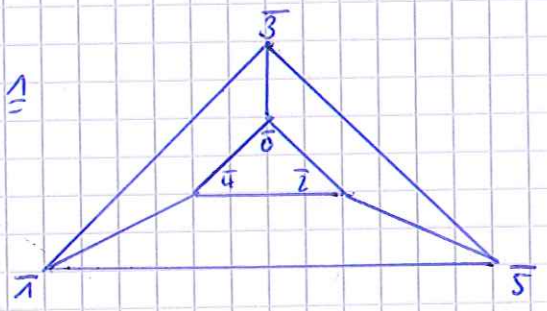
i) $G = \mathbb{Z}/6\mathbb{Z}$, $S = \{\overline{1}, \overline{5}\}$

$\Rightarrow \mathcal{G}(G,S) \cong$



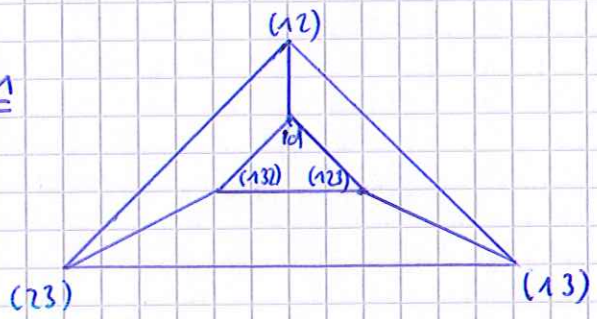
ii) $G = \mathbb{Z}/6\mathbb{Z}$, $S = \{\overline{2}, \overline{3}, \overline{4}\}$

$\Rightarrow \mathcal{G}(G,S) \cong$



iii) $G = Sym(3)$, $S = \{(123), (132), (12)\}$

$\Rightarrow$ $\mathcal{G}(G,S) \cong$



iv) $G = \mathbb{Z}$, $S = \{1, -1\}$

$\Rightarrow$ $\mathcal{G}(G,S) \cong$ 

1.4 Bemerkung

1.3ii) und 1.3iii) zeigen, dass nicht isomorphe Gruppen dennoch isomorphe Cayley-Graphen besitzen können

1.5 Satz

Sei $\mathcal{G}(G,S)$ ein Cayley-Graph mit $|S| = k$. Dann gilt:

i) $\mathcal{G}(G,S)$ ist ein einfacher, k-regulärer, Ecken-transitiver Graph

ii) $\mathcal{G}(G,S)$ besitzt Schleifen $\Leftrightarrow 1_G \in S$

iii) $\mathcal{G}(G,S)$ ist zusammenhängend $\Leftrightarrow \langle S \rangle = G$

iv) Existiert ein Homomorphismus χ von G nach $\{\pm 1\}$ mit $\chi(S) = \{-1\}$, so ist $\mathcal{G}(G,S)$ bipartit

Die Rückrichtung gilt, falls $\mathcal{G}(G,S)$ zusätzlich noch zusammenhängend ist

Beweis

i) Die Adjazenz-Matrix A von $\mathcal{G}(G,S)$ hat die Einträge

$$A_{x,y} = \begin{cases} 1, \text{falls ein } s \in S \text{ existiert mit } y = xs \\ 0 \text{ sonst} \end{cases}$$

$\Rightarrow$ $\mathcal{G}(G,S)$ ist einfach

Sei K_x die Anzahl der Kanten, die von x weggehen

$\Rightarrow K_x = \sum_{y \in G} A_{x,y} = \sum_{s \in S} 1 = |S| = k$

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

G wirkt auf $\Gamma(G,S)$ durch Linksmultiplikation.

Diese Wirkung ist transitiv auf $V = G$

$\Rightarrow \Gamma(G,S)$ ist Ecken-transitiv

ii) „$\Leftarrow$" $1_G \in S \Rightarrow (x, x) = (x, x \cdot 1_G) \in E \Rightarrow \Gamma(G,S)$ besitzt Schleifen

„$\Rightarrow$" $\Gamma(G,S)$ besitzt Schleifen

$\Rightarrow \exists\, x \in V = G: (x,x) \in E$

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

$\Rightarrow x^{-1}x = x^{-1}xs$

$\Rightarrow 1_G = s$

$\Rightarrow 1_G \in S$

iii) $\Gamma(G,S)$ ist zusammenhängend

$\Leftrightarrow \forall g \in G$ existiert ein Kantenweg zu $1_G \in G$

$\Leftrightarrow \exists\, g_1, \dots, g_n \in G: (1_G, g_1), (g_n, g), (g_i, g_{i+1}) \in E$ für $i = 1, \dots, n-1$

$\Leftrightarrow \exists\, s_1, \dots, s_{n+1} \in S: g_1 = 1_G \cdot s_1,\ g = g_n \cdot s_{n+1},\ g_i = g_{i-1} \cdot s_i$ für $i = 2, \dots, n$

$\Leftrightarrow g = g_n s_{n+1} = g_{n-1} s_n s_{n+1} = g_{n-2} s_{n-1} s_n s_{n+1}$

$= \dots = 1_G \cdot s_1 \cdots s_{n+1}$

$\Leftrightarrow \langle S \rangle = G$

iv) Sei $\chi: G \to \{\pm 1\}$ ein Homomorphismus mit $\chi(S) = \{-1\}$

$\Rightarrow V_\varepsilon = \{ g \in G \mid \chi(g) = \varepsilon \}$ definiert eine Bipartition

Sei $\Gamma(G,S)$ nun bipartit und zusammenhängend

Sei V_+ die Partitionsklasse, die 1_G enthält und V_-

die andere Partitionsklasse

$\Rightarrow S \subseteq V_-$, da für alle $s \in S$ gilt: $(1,s) \in E$

Wir definieren $\chi: G \to \{\pm 1\}$, $\chi(g) = \begin{cases} 1 & \text{falls } g \in V_+ \\ -1 & \text{falls } g \in V_- \end{cases}$

Nach iii) gilt $G(G,S)$ zusammenhängend $\Leftrightarrow \langle S \rangle = G$

$\Rightarrow \chi(g) = (-1)^{l_S(g)}$, wobei $l_S(g)$ die Länge von g bzgl S ist

Da $G = V_+ \dot\cup V_-$ und $l_S(g*h) \equiv l_S(g) + l_S(h) \pmod 2$, folgt dass χ ein Homomorphismus ist.

Da $S \subseteq V_-$, folgt $\chi(S) = \{-1\}$ □

§ 2 Konstruktion von $X^{p,q}$

2.1 Konvention

Im Folgenden seien p und q zwei verschiedene, ungerade Primzahlen

2.2 Erinnerung

Es gibt $8 \cdot (p+1)$ Quaternionen über $\mathbb{Z}$ mit Norm p

Dabei sind jeweils 8 Quaternion assoziert zueinander durch Multiplikation einer Einheit.

Die Menge S_p enthält jeweils den Repräsentanten, für den $a_0 > 0$ gilt. Im Falle $a_0 = 0$ gibt es zwei Repräsentanten, von denen einer ausgewählt wird:

$S_p = \{\alpha_1, \bar\alpha_1, \dots, \alpha_s, \bar\alpha_s, \beta_1, \dots, \beta_t\}$ (siehe Vortrag 9 §2.15)

$|S_p| = p+1$ und $-\beta_i^2 = \alpha_i \bar\alpha_i$

2.3 Vorüberlegung/Erinnerung

Wir definieren die Abbildung $\tau_q: \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$ durch

$a + bi + cj + dk \mapsto \bar a + \bar b \cdot i + \bar c \cdot j + \bar d \cdot k$

$\Rightarrow$ es existieren $x, y \in \mathbb{Z}$: $x^2 + y^2 + 1 \equiv 0 \pmod p$

$\Rightarrow \mathbb{H}(\mathbb{F}_q)$ ist isomorph zu $\mathbb{F}_q^{2\times 2}$

Sei Ψ_q dieser Isomorphismus

$\Rightarrow \Psi_q$ hat folgende Eigenschaften:

i) $N(\alpha) = \det(\Psi_q(\alpha)) \quad \forall \alpha \in \mathbb{H}(\mathbb{F}_q)$

ii) Wenn α real ist (d.h. $\alpha = \bar{\alpha}$), so ist $\Psi_q(\alpha)$ eine skalare Matrix (d.h. $\Psi_q(\alpha) = \lambda \cdot \mathbb{1}_2$ für ein $\lambda \in \mathbb{F}_q$)

$\Rightarrow$ Für $\alpha \in S_p$ gilt: $\Psi_q(\tau_q(\alpha)) \in GL_2(q)$, da $N(\alpha) = p \neq q$ und $\Psi_q(\tau_q(\alpha \cdot \bar{\alpha})) = \Psi_q(\tau_q(\bar{\alpha} \cdot \alpha)) = \Psi_q(\tau_q(N(\alpha))) \neq 0$ ist eine skalare Matrix

Sei $\varphi : GL_2(q) \to PGL_2(q)$ die Projektion

$\Rightarrow \ker(\varphi)$ ist genau die Untergruppe der skalaren Matrizen

2.4 Definition

Wir definieren die Menge $S_{p,q}$ als das Bild der Menge S_p unter der Abbildungen $\varphi \circ \Psi_q \circ \tau_q$:

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

2.5 Bemerkung

$S_{p,q}$ ist symmetrisch, da für $\alpha \in S_p$ gilt:

$a_0 > 0 \Rightarrow (\varphi \circ \Psi_q \circ \tau_q)(\alpha) \cdot (\varphi \circ \Psi_q \circ \tau_q)(\bar{\alpha}) = \varphi(\underbrace{\Psi_q(\tau_q(\alpha \cdot \bar{\alpha}))}_{\text{skalare Matrix}}) = \{\lambda \cdot \mathbb{1}_2 \mid \lambda \in \mathbb{F}_q^*\}$

(φ, Ψ_q, τ_q sind Homomorphismen)

$a = 0 \Rightarrow (\varphi \circ \Psi_q \circ \tau_q)(\alpha) \cdot (\varphi \circ \Psi_q \circ \tau_q)(\alpha) = PGL_2(q)$ (analog)

2.6 Lemma

Wenn q bzgl p groß genug ist (in unserem Fall nehmen wir $q > 2\sqrt{p}$ an), so gilt $|S_{p,q}| = p+1$

Beweis

Seien $\alpha, \beta \in S_p$, $\alpha \neq \beta$

$\alpha = a_0 + a_1 i + a_2 j + a_3 k$, $\beta = b_0 + b_1 i + b_2 j + b_3 k$ mit $a_0, b_0 > 0$

$\Rightarrow \exists\, i \in \{0,1,2,3\} : a_i \neq b_i$

$\alpha, \beta \in S_p \Rightarrow N(\alpha) = p = N(\beta)$

$\Rightarrow \forall j \in \{0,1,2,3\} : a_j, b_j \in (-\sqrt{p}, \sqrt{p})$

Da $q > 2\sqrt{p}$ folgt: $a_i \not\equiv b_i \pmod q$

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

Setze $A = (\psi_q \circ \tau_q)(\alpha)$, $B = (\psi_q \circ \tau_q)(\beta)$

$\Rightarrow A \neq B \in GL_2(q)$, da ψ_q Isomorphismus

Ann.: $\varphi(A) = \varphi(B)$ in $PGL_2(q)$

$\Rightarrow \exists\, \lambda \in \mathbb{F}_q^* : \lambda \neq 1$ und $A = \lambda \cdot B$

$\Rightarrow p = N(\alpha) = \det(\psi_q(\tau_q(\alpha))) = \det(A) = \det(\lambda \cdot B) = \lambda^2 \cdot \det(B)$

$= \lambda^2 \cdot \det(\psi_q(\tau_q(\beta))) = \lambda^2 \cdot N(\beta) = \lambda^2 \cdot p$

$\Rightarrow \lambda = \pm 1 \overset{\lambda \neq 1}{\Rightarrow} \lambda = -1$

$\Rightarrow A = -B$

$\Rightarrow \alpha \equiv -\beta \pmod q$

$\Rightarrow \forall j \in \{0,1,2,3\} : a_j \equiv -b_j \pmod q$

$\Rightarrow a_j = -b_j$, da $a_j, b_j \in (-\sqrt{p}, \sqrt{p})$ und $q > 2\sqrt{p}$

$\Rightarrow \alpha = -\beta$

Da gilt $a_0, b_0 > 0$ folgt $a_0 = 0 = b_0$

$\Rightarrow \alpha = \overline{\beta}$ ↯ da $\overline{\alpha} \notin S_p$, wenn $\alpha \in S$ und $a_0 = 0$

$\Rightarrow \varphi(A) \neq \varphi(B)$

$\Rightarrow \varphi \circ \psi_q \circ \tau_q$ ist injektiv

$\Rightarrow |S_{p,q}| = |(\varphi \circ \psi_q \circ \tau_q)(S_p)| \overset{\text{injektiv}}{=} |S_p| = p+1$

□

2.7 Notation

Ist p modulo q ein Quadrat, d.h. $\exists x \in \mathbb{Z} : x^2 \equiv p \pmod q$, so schreibt man $\left(\frac{p}{q}\right) = 1$. Andernfalls schreibt

man $\left(\frac{p}{q}\right) = -1$

2.8 Definition

1) Wenn gilt $\left(\frac{p}{q}\right) = 1$, so ist $S_{p,q} \leq PSL_2(q)$ und wir setzen $X^{p,q} = G(PSL_2(q), S_{p,q})$

2) Wenn gilt $\left(\frac{p}{q}\right) = -1$, so gilt $S_{p,q} \leq PGL_2(q) \setminus PSL_2(q)$ und wir setzen $X^{p,q} = G(PGL_2(q), S_{p,q})$

2.9 Satz (ohne Beweis)

Seien p, q ungerade, unterschiedliche Primzahlen mit $q > 2\sqrt{p}$. Der Graph $X^{p,q}$ ist $(p+1)$-regulär, zusammenhängend und Ramanujan.

Des weiteren gilt:

1) $\left(\frac{p}{q}\right) = 1 \Rightarrow X^{p,q}$ ist nicht bipartit mit $\frac{q \cdot (q^2-1)}{2}$ Ecken und $g(X^{p,q}) \geq 2 \cdot \log_p(q)$

2) $\left(\frac{p}{q}\right) = -1 \Rightarrow X^{p,q}$ ist bipartit mit $q \cdot (q^2-1)$ Ecken und $g(X^{p,q}) \geq 4 \cdot \log_p(q) - \log_p(4)$

2.10 Bemerkung

i) $(p+1)$-Regularität und Anzahl der Ecken sind einfach zu zeigen. Dass $X^{p,q}$ Ramanujan ist, ist deutlich schwieriger zu zeigen

ii) Dass $X^{p,q}$ zusammenhängend ist, wird in den kommenden Vorträgen noch wichtig, da dies bedeutet, dass $S_{p,q}$ $PSL_2(q)$ bzw $PGL_2(q)$ erzeugt

iii) $(X^{p,q})_{q \text{ prim}}$ bilden eine Familie von Expandergraphen