Vortrag 13: Der Cayley-Graph von $PSL_2(\mathbb{F}_q)$ ist regulär und zusammenhängend

1. Erinnerung

Seien p und q unterschiedliche, ungerade Primzahlen.
Im letzten Vortrag wurden Graphen $X^{p,q}$ wie untenstehend definiert. Das sind genau die Graphen, die uns nun interessieren. Wir werden zeigen, dass die $X^{p,q}$ (p+1)-regulär und zusammenhängend sind.
Um dies zu zeigen, definieren wir uns Graphen $Y^{p,q}$, die sich als isomorph zu den $X^{p,q}$ herausstellen werden.

$$X^{p,q} := \begin{cases} \mathcal{G}(PSL_2(\mathbb{F}_q),\ S_{p,q}) & \text{wenn } \left(\frac{p}{q}\right) = 1 \\ \mathcal{G}(PGL_2(\mathbb{F}_q),\ S_{p,q}) & \text{wenn } \left(\frac{p}{q}\right) = -1 \end{cases}$$

$p\ mod\ q$ ist genau dann ein Quadrat in $\mathbb{Z}$, wenn ein $x \in \mathbb{Z}$ existiert, so dass gilt: $x^2 = p\ mod\ q$.
Dafür gibt es folgende Kurzschreibweise (Legendre-Symbol):

$$\left(\frac{p}{q}\right) = 1 \Leftrightarrow p\ mod\ q \text{ ist ein Quadrat in } \mathbb{Z}$$

und

$$\left(\frac{p}{q}\right) = -1 \Leftrightarrow p\ mod\ q \text{ ist kein Quadrat in } \mathbb{Z}.$$

$S_{p,q}$ wurde wie folgt definiert:

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

Die Abbildungen φ, Ψ_q und τ_q betrachten wir später.
Für eine Quaternion $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ ist $N(\alpha)$ die Norm von α: $N(\alpha) = \alpha\overline{\alpha} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$.
$S_p \subset \mathbb{H}(\mathbb{Z})$ wurde wie folgt konstruiert: Es gibt $8(p+1)$ Quaternionen in $\mathbb{H}(\mathbb{Z})$ mit Norm p. Je acht dieser Quaternionen mit Norm p sind zueinander assoziiert (d.h. sie gehen durch Multiplikation mit Einheiten auseinander hervor). S_p enthält von jeder dieser acht zueinander assoziierten Quaternionen mit Norm p genau eine, und zwar so, dass $\alpha_0 \geq 0$ für alle $\alpha \in S_p$.

$$S_p := \{\alpha_1, \overline{\alpha_1}, ..., \alpha_s, \overline{\alpha_s}, \beta_1, ..., \beta_t\} \subset \mathbb{H}(\mathbb{Z})$$

Dabei gilt für alle α_i: $\alpha_0^{(i)} > 0$.
Und für alle β_j gilt: $\beta_0^{(j)} = 0$.
Außerdem gilt: $2s + t = \#S_p = p + 1$.
Zu guter letzt betrachten wir folgende Menge:

$$\Lambda' = \left\{\alpha \in \mathbb{H}(\mathbb{Z}) \,\middle|\, \alpha \equiv 1\ (mod\ 2) \ \vee\ \alpha \equiv i + j + k\ (mod\ 2),\ N(\alpha) = p^k, k \in \mathbb{N}, k \geq 1\right\}$$

Nach Vortrag 9 hat jedes $\alpha \in \Lambda'$ eine eindeutige Darstellung $\alpha = \pm p^k \omega_m$, wobei ω_m ein reduziertes Wort der Länge m über S_p ist.

2. Definition

Definiere folgende Äquivalenzrelation auf Λ':

$$\alpha \sim \beta :\Leftrightarrow \exists m, n \in \mathbb{N} : p^m \alpha = \pm p^n \beta$$

$[\alpha]$ sei die Äquivalenzklasse von α bzgl. $\sim$.

Λ sei die Menge der Äquivalenzklassen und Q die Quotientenabbildung.

$$\Lambda := {}^{\Lambda'}/_{\sim} = \{[\alpha] \mid \alpha \in \Lambda'\}$$

$$Q : \Lambda' \to \Lambda, \alpha \mapsto [\alpha]$$

3. Lemma

Die Äquivalenzrelation ist mit der Multiplikation auf Λ' verträglich. Das heißt, es gilt:

$$\alpha_1 \sim \beta_1, \alpha_2 \sim \beta_2 \Rightarrow \alpha_1\alpha_2 \sim \beta_1\beta_2$$

Λ besitzt also eine assoziative Multiplikation.

Beweis: Seien $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \Lambda'$ mit $\alpha_1 \sim \beta_1$ und $\alpha_2 \sim \beta_2$.
Dann existieren natürliche Zahlen $n, m, k, l \in \mathbb{N}$, sodass $p^n\alpha_1 = \pm p^m\beta_1$ und $p^k\alpha_2 = \pm p^l\beta_2$.

$$p^{n+k}\alpha_1\alpha_2 = p^n\alpha_1 p^k\alpha_2 = \pm p^m\beta_1 p^l\beta_2 = \pm p^{m+l}\beta_1\beta_2$$

$\Rightarrow \alpha_1\alpha_2 \sim \beta_1\beta_2$
Daraus folgt direkt, dass $[\alpha] \cdot [\beta] = [\alpha\beta]$ eine wohldefinierte Verknüpfung auf Λ ist. □

4. Proposition

a) Λ ist eine Gruppe.
b) Der Cayley-Graph $\mathcal{G}(\Lambda, Q(S_p))$ ist ein (p+1)-regulärer Baum.

Beweis: a) Wir wissen bereits, dass Λ eine assoziative Multiplikation besitzt.
Für alle $\alpha \in \Lambda'$ gilt: $p\alpha \sim \alpha \Rightarrow [p][\alpha] = [p\alpha] = [\alpha] \Rightarrow [p] \in \Lambda$ ist Neutralelement.
Es bleibt also nur noch zu zeigen: Für alle $[\alpha] \in \Lambda$ existiert ein Inverses.
Für alle $\alpha \in \Lambda'$ gilt: $N(\alpha) = \alpha\overline{\alpha} = p^n$ für ein $n \in \mathbb{N}$.
$\Rightarrow p\alpha\overline{\alpha} = p^{n+1}1$
$\Rightarrow \alpha\overline{\alpha} = \overline{\alpha}\alpha \sim 1$
$\Rightarrow [\overline{\alpha}][\alpha] = [\overline{\alpha}\alpha] = [1]$
$\Rightarrow [\alpha]^{-1} = [\overline{\alpha}]$
Also ist Λ eine Gruppe.

b) Für alle $\alpha, \beta \in S_p$ gilt: $\alpha \sim \beta \Rightarrow \alpha = \beta$
Denn: $\alpha \sim \beta \Rightarrow p^k\alpha = \pm p^n\beta \Rightarrow p^{k-n}\alpha = \pm\beta \Rightarrow N(p^{k-n})N(\alpha) = N(\beta)$. Da $N(\alpha) = p = N(\beta)$, folgt $N(p^{k-n}) = 1$ und somit auch $\alpha = \pm\beta$. α kann aber nicht $-\beta$ sein, da es in S_p keine zueinander assoziierten Elemente gibt.
Das bedeutet, dass Q die Elemente von S_p injektiv abbildet. Da $\#S_p = p + 1$, folgt $\#Q(S_p) = p + 1$. Nach einem Theorem aus Vortrag 9 existiert für alle $\alpha \in \Lambda'$ eine eindeutige Darstellung $\alpha = \pm p^k\omega_m$, wobei ω_m ein reduziertes Wort der Länge m über S_p ist. $S_p \cup \{p\}$ erzeugt also Λ'. Da $p\alpha \sim \alpha$ für alle $\alpha \in \Lambda'$, erhalten wir:

$$\langle Q(S_p)\rangle = \Lambda$$

Mit Satz 1.5 (i) und (iii) aus Vortrag 12 folgt, dass $\mathcal{G}(\Lambda, Q(S_p))$ zusammenhängend und (p+1)-regulär ist, weil $Q(S_p)$ ein Erzeugendensystem mit p+1 Elementen ist.
Es bleibt noch zu zeigen, dass $\mathcal{G}(\Lambda, Q(S_p))$ keinen Kreis enthält.
Angenommen, $\mathcal{G}(\Lambda, Q(S_p))$ enthält doch einen Kreis $x_0, x_1, \ldots, x_{n-1}, x_g = x_0$ der Länge $g \geqslant 3$, $x_i \in \Lambda$ für $i = 1, \ldots, g$.

Ohne Einschränkung gilt $x_0 = [1]$ (Ecken-Transitivität, Vortrag 12 Satz 1.5 (i)). Per Definition eines Cayley-Graphen existieren $\gamma_1, ..., \gamma_g \in S_p$, sodass $x_i = [\gamma_1 ... \gamma_i]$. Da $x_{k-1} \neq x_{k+1}$ für alle $k = 1, ..., n-1$, ist $\gamma_1 ... \gamma_g$ ein reduziertes Wort über S_p.
Die Gleichung $[1] = [\gamma_1 ... \gamma_g]$ in Λ liefert uns die Gleichung $p^m = \pm p^n \gamma_1 ... \gamma_g$ in Λ'.
Nach einem Korollar aus Vortrag 9 besitzt jedes nicht-triviale $\alpha \in \Lambda'$ eine eindeutige Darstellung $\alpha = \pm p^r \omega_m$, wobei ω_m ein reduziertes Wort der Länge m über S_p ist. $\lightning$
Der Cayley-Graph $\mathcal{G}(\Lambda, Q(S_p))$ enthält also keinen Kreis und ist zusammenhängend, somit ist er ein Baum. □

5. Konstruktion der $Y^{p,q}$

Wir betrachten nun die Reduktion modulo q, die schon im letzten Vortrag Verwendung fand:

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$$

$\mathbb{H}(\mathbb{F}_q)$ ist isomorph zu $\mathbb{F}_q^{2x2}$. Sei Ψ_q dieser Isomorphismus. Sei $\alpha \in \Lambda'$. Dann gilt nach Vortrag 12 $det(\Psi_q(\alpha)) = N(\alpha) = p$. Die Determinante des Bildes ist ungleich null, also ist die Matrix invertierbar. $\mathbb{H}(\mathbb{F}_q)^*$ enthält genau die invertierbaren Elemente von $\mathbb{H}(\mathbb{F}_q)$. τ_q schickt Λ' also auf $\mathbb{H}(\mathbb{F}_q)^*$.
Sei $Z_q := \{\alpha \in \mathbb{H}(\mathbb{F}_q)^* \mid \alpha = \overline{\alpha}\}$ die zentrale Untergruppe von $\mathbb{H}(\mathbb{F}_q)^*$.
Für $\alpha, \beta \in S_p$ mit $\alpha \sim \beta$ gilt: $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$.
Denn: $\alpha \sim \beta \Rightarrow p^k \alpha = \pm p^n \beta \overset{o.E. n<k}{\Rightarrow} p^{k-n}\alpha = \pm\beta$.
$\tau_q(\alpha)^{-1}\tau_q(\beta) = \tau_q(\alpha)^{-1}\tau_q(\pm p^{k-n}\alpha) \overset{\tau_q Homom.}{\Rightarrow} \tau_q(\alpha)^{-1}\tau_q(p^{k-n})\tau_q(\alpha)$.
$\tau_q(p^{k-n})$ liegt in $\mathbb{F}_q$ und kommutiert deshalb mit Quaternionen aus $\mathbb{H}(\mathbb{F}_q)$, insbesondere mit $\tau_q(\alpha)$. Da $\tau_q(p^{k-n})$ keinen Imaginärteil besitzt, gilt $\tau_q(p^{k-n}) = \overline{\tau_q(p^{k-n})} \in Z_q$. $\Rightarrow \tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$.

$\tau_q : \Lambda' \to \mathbb{H}(\mathbb{F}_q)^*$ induziert also einen Gruppenhomomorphismus

$$\Pi_q : \Lambda \to {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q}$$

Π_q ist wohldefiniert, denn:

$$\begin{aligned} \alpha \sim \beta &\Rightarrow \tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q \\ &\Rightarrow \tau_q(\alpha)^{-1}\tau_q(\beta) = 1 \in {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} \\ &\Rightarrow \tau_q(\alpha) = \tau_q(\beta) \in {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} \end{aligned}$$

Wir definieren nun $\Lambda(q)$ als den Kern von Π_q und stellen mithilfe des Homomorphiesatzes fest, dass ${}^{\Lambda}/_{\Lambda(q)}$ isomorph ist zu dem Bild von Π_q.
Wir definieren nun $T_{p,q} := (\Pi_q \circ Q)(S_p)$. $T_{p,q}$ ist sowohl von p als auch von q abhängig!
Der Beweis, dass, für ausreichend großes q, $\#T_{p,q} = p + 1$ gilt, verläuft analog zu dem Beweis im letzten Vortrag, in dem gezeigt wurde, dass $\#S_{p,q} = p + 1$ gilt. Eine mögliche Wahl für q ist $q > 2\sqrt{p}$. Ebenfalls kann man ganz analog wie bei $S_{p,q}$ beweisen, dass $T_{p,q}$ symmetrisch ist. Nun definieren wir endlich die Graphen $Y^{p,q}$:

$$Y^{p,q} := \mathcal{G}({}^{\Lambda}/_{\Lambda(q)}, T_{p,q})$$

6. Satz

Für ausreichend großes q ist $Y^{p,q}$ (p+1)-regulär und zusammenhängend.

Beweis: $Q(S_p)$ erzeugt Λ. $\Rightarrow \langle T_{p,q} \rangle = \langle \Pi_q(Q(S_p)) \rangle = \Pi_q(\langle Q(S_p) \rangle) = \Pi_q(\Lambda) \cong {}^{\Lambda}/_{\Lambda(q)} \Rightarrow Y^{p,q}$ ist zusammenhängend.
q ausreichend groß $\Rightarrow \#T_{p,q} = p + 1 \Rightarrow Y^{p,q}$ ist (p+1)-regulär. □

7. Konstruktion von β

Betrachte nun wieder den Isomorphismus Ψ_q:

$$\Psi_q : \mathbb{H}(\mathbb{F}_q)^* \to GL_2(\mathbb{F}_q)$$

Ψ_q schickt die zentrale Gruppe Z_q auf die Menge der Skalarmatrizen, welche genau der Kern der Abbildung $\varphi : GL_2(\mathbb{F}_q) \to PGL_2(\mathbb{F}_q)$ ist.

$$\Psi_q(Z_q) = ker(\varphi)$$

Verknüpft man nun die beiden surjektiven Abbildungen Ψ_q und φ, und teilt den Kern Z_q heraus, erhält man folgenden Isomorphismus:

$$\beta : {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} \to PGL_2(\mathbb{F}_q)$$

In dem folgenden kommutativen Diagramm kann man nun sehen, wie $X^{p,q}$ und $Y^{p,q}$ miteinander in Verbindung stehen:

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^* & \xrightarrow{\Psi_q} & GL_2(\mathbb{F}_q) \\ \downarrow Q & & \downarrow & & \downarrow \varphi \\ \Lambda & \xrightarrow{\Pi_q} & {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} & \xrightarrow{\beta} & PGL_2(\mathbb{F}_q) \end{array}$$

Alle senkrecht eingezeichneten Pfeile stellen Quotientenabbildungen dar.

$$X^{p,q} := \begin{cases} \mathcal{G}(PSL_2(\mathbb{F}_q),\ S_{p,q}) & \text{wenn } \left(\frac{p}{q}\right) = 1 \\ \mathcal{G}(PGL_2(\mathbb{F}_q),\ S_{p,q}) & \text{wenn } \left(\frac{p}{q}\right) = -1 \end{cases} \qquad S_{p,q} = (\varphi \circ \Psi_q \circ \tau_q)(S_p)$$

$$Y^{p,q} := \mathcal{G}({}^{\Lambda}/_{\Lambda(q)}, T_{p,q}) \qquad T_{p,q} = (\Pi_q \circ Q)(S_p)$$

Wir wollen zeigen, dass $X^{p,q}$ zusammenhängend ist, wissen bisher aber nur, dass $Y^{p,q}$ zusammenhängend ist. Anhand des kommutativen Diagramms und der Definitionen von $S_{p,q}$ und $T_{p,q}$ sieht man, dass

$$\beta(T_{p,q}) = S_{p,q}.$$

Da $T_{p,q}$ den Graphen $Y^{p,q}$ erzeugt, ist $Y^{p,q}$ ein zusammenhängender Teilgraph von $X^{p,q}$. $Y^{p,q}$ ist sogar eine zusammenhänge Komponente von $X^{p,q}$, weil ihre Kantenmengen isomorph sind.
Es bleibt also nur noch zu zeigen, dass $X^{p,q}$ und $Y^{p,q}$ isomorph zueinander sind, dann folgt, dass die $X^{p,q}$ zusammenhängend sind.

Bevor wir die Isomorphie zeigen können, müssen wir mehr über $\Lambda(q)$ herausfinden:

8. Lemma

$$\Lambda(q) = \{[\alpha] \in \Lambda \mid \alpha = a_0 + a_1 i + a_2 j + a_3 k, q \mid a_1, a_2, a_3\}$$

Beweis:

$$\begin{aligned}
[\alpha] \in \Lambda(q) = ker(\Pi_q) \text{ mit } \Pi_q : \Lambda \to {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} &\Leftrightarrow \tau_q(\alpha) \in Z_q(\text{ siehe kommutatives Diagramm}) \\
&\Leftrightarrow \tau_q(\alpha) = \overline{\tau_q(\alpha)} \\
&\Leftrightarrow \alpha \ mod\ q = \overline{\alpha} \ mod\ q \\
&\Leftrightarrow \alpha - \overline{\alpha} \equiv 0 \ mod\ q \\
&\Leftrightarrow 2a_1 i + 2a_2 j + 2a_3 k \equiv 0 \ mod\ q \\
&\Leftrightarrow q \nmid a_0 \text{ und } q \mid a_1, a_2, a_3.
\end{aligned}$$

Für alle $\alpha \in \Lambda'$ ist $N(\alpha)$ eine Potenz von p und $p \neq q$. Würde q auch a_0 teilen, würde q auch $N(\alpha) = p^n$ teilen. Dass $q \nmid a_0$ gilt, folgt also schon daraus, dass q die anderen drei Koeffizienten teilt. □

9. Proposition

Wir können nun eine untere Schranke für den Umfang der $Y^{p,q}$ angeben:

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

Gilt $\left(\frac{p}{q}\right) = -1$, erhalten wir die bessere Abschätzung:

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

Beweis: Zur Vereinfachung schreiben wir g für $g(Y^{p,q})$.
Seien $x_0, x_1, ..., x_{g-1}, x_g = x_0$ die Ecken eines Kreises der Länge g in $Y^{p,q}$. So einen Kreis gibt es, weil der Umfang eines Graphen genau der Länge des kleinsten in ihm enthaltenen Kreises entspricht.
Aufgrund der Ecken-Transitivität können wir annehmen, dass $x_0 = x_g = 1$ in ${}^{\Lambda}/_{\Lambda(q)}$.
Da $Y^{p,q}$ ein Cayley-Graph ist, finden wir $t_1, ..., t_g \in T_{p,q}$ so, dass $x_i = t_1 t_2 ... t_i$ für $1 \leq i \leq g$. Nun existieren eindeutige $\gamma_i \in S_p$ mit $\Pi_q([\gamma_i]) = t_i$ für $i = 1, ..., g$.
Sei $\alpha = \gamma_1 ... \gamma_g \in \Lambda'$ mit $\alpha = a_0 + a_1 i + a_2 j + a_3 k$. α ist also ein reduziertes Wort über S_p. Außerdem ist $[\alpha] = [\gamma_1]...[\gamma_g]$ verschieden von $[1] \in \Lambda$, denn im Beweis von Proposition 5b wurde gezeigt, dass Q die Elemente von S_p injektiv abbildet.
Dass α nicht äquivalent ist zur 1 in Λ' bedeutet, dass mindestens einer der Parameter a_1, a_2 und a_3 ungleich null sein muss. Andererseits gilt auch:

$$\Pi_q([\alpha]) = t_1 t_2 ... t_g = x_g = 1$$

Also liegt $[\alpha]$ im Kern von Π_q, den wir $\Lambda(q)$ genannt hatten. Nach Lemma 9 muss die Primzahl q a_1, a_2 und a_3 teilen. Da eines der drei a_i ungleich null ist, erhalten wir

$$p^g = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \geq q^2$$

Nimmt man von dieser Gleichung den Logarithmus zur Basis p, erhält man die erste Gleichung aus der Behauptung.
Angenommen $\left(\frac{p}{q}\right) = -1$. Zusammen mit $p^g \equiv a_0^2 (mod\ q)$ stellen wir fest, dass der Umfang der $Y^{p,q}$ in diesem Fall gerade ist.

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

Sei also $g = 2h$. Nun gilt

$$p^{2h} \equiv a_0^2 \ (mod\ q^2).$$

Da q weder a_0 noch p^h teilt, folgt

$$p^h \equiv \pm a_0 (mod\ q^2)$$

Da $a_0^2 \leq p^g$, folgt $|a_0| \leq p^h$.
Wir nehmen nun an, dass $q < 4log_p q - log_p 4 = log_p \frac{q^4}{4}$ und führen die Annahme zu einem Widerspruch. Aus der Annahme folgt $p^h < \frac{q^2}{2}$. Dann gilt $|p^h \mp a_0| < q^2$ und mit der obigen Kongruenz erhalten wir $p^h = \pm a_0$. Dann ist $p^g = a_0^2$. Dann muss aber $a_1 = a_2 = a_3 = 0$ gelten, was ein Widerspruch dazu ist, dass einer dieser drei Parameter ungleich null sein muss. Aus dem Widerspruch folgt die zweite Ungleichung aus der Behauptung. □

10. Bemerkung

Im ersten Kapitel des Buches von Davidoff, Sarnak und Valette wird eine Abschätzung des Umfangs eines zusammenhängenden, k-regulären Graphen gezeigt. Wende die Abschätzung auf $Y^{p,q}$ an:

$$g(Y^{p,q}) \leq 2 + 2log_p \#Y^{p,q}$$

Zusammen mit den Abschätzungen aus Proposition 9 ergibt sich folgende Ungleichung:

$$\#Y^{p,q} \geq \frac{q}{p}$$

Angenommen, $\left(\frac{p}{q}\right) = -1$:

$$\#Y^{p,q} \geq \frac{q^2}{2p}$$

Dies zeigt, dass $\#Y^{p,q} = \#\Lambda/\Lambda(q)$ mindestens linear mit q wächst.

Beweis:

$$\begin{aligned} 2log_p q \leq g(Y^{p,q} &\leq 2 + 2log_p \#Y^{p,q} \\ \Leftrightarrow log_p q &\leq 1 + log_p \#Y^{p,q} \\ \Leftrightarrow q &\leq p\#Y^{p,q} \\ \Leftrightarrow \frac{q}{p} &\leq \#Y^{p,q} \end{aligned}$$

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

$$\begin{aligned} 4log_p q - log_p 4 \leq g(Y^{p,q}) &\leq 2 + 2log_p \#Y^{p,q} \\ \Leftrightarrow 2log_p q - \frac{1}{2}log_p 4 &\leq 1 + log_p \#Y^{p,q} \\ \Leftrightarrow log_p q^2 - log_p 2 &\leq 1 + log_p \#Y^{p,q} \\ \Leftrightarrow log_p \frac{q^2}{2} &\leq 1 + log_p \#Y^{p,q} \\ \Leftrightarrow \frac{q^2}{2} &\leq p\#Y^{p,q} \\ \Leftrightarrow \frac{q^2}{2p} &\leq \#Y^{p,q} \end{aligned}$$

□

11. Theorem

Angenommen, $p \geq 5$.
Für $q > p^8$ ist der Graph $X^{p,q}$ zusammenhängend und isomorph zu $Y^{p,q}$.

Beweis: Um zu zeigen, dass $X^{p,q}$ zusammenhängend ist, muss gezeigt werden, dass $S_{p,q}$ in beiden Fällen ein Erzeugendensystem ist. Zu zeigen ist also:

$$\langle S_{p,q} \rangle = \begin{cases} PSL_2(\mathbb{F}_q) & \text{wenn } \left(\frac{p}{q}\right) = 1 \\ PGL_2(\mathbb{F}_q) & \text{wenn } \left(\frac{p}{q}\right) = -1 \end{cases}$$

Dazu wollen wir den Isomorphismus $\beta : {}^{\mathbb{H}(\mathbb{F}_q)^*}/_{Z_q} \to PGL_2(\mathbb{F}_q)$ verwenden, von dem wir bereits wissen, dass er $T_{p,q}$ auf $S_{p,q}$ schickt. Es ist also äquivalent zu zeigen:

$$\langle S_{p,q} \rangle = \langle \beta(T_{p,q}) \rangle = \beta({}^{\Lambda}/_{\Lambda(q)}) = \begin{cases} PSL_2(\mathbb{F}_q) & \text{wenn } \left(\frac{p}{q}\right) = 1 \\ PGL_2(\mathbb{F}_q) & \text{wenn } \left(\frac{p}{q}\right) = -1 \end{cases}$$

Im letzten Vortrag wurde bereits gezeigt:

$$\left(\frac{p}{q}\right) = 1 \Rightarrow S_{p,q} \subset PSL_2(\mathbb{F}_q)$$
$$\left(\frac{p}{q}\right) = -1 \Rightarrow S_{p,q} \subset PGL_2(\mathbb{F}_q) - PSL_2(\mathbb{F}_q)$$

Setze $H_{p,q} = PSL_2(\mathbb{F}_q) \cap \beta({}^{\Lambda}/_{\Lambda(q)})$.
Nun müssen wir nur noch zeigen, dass in beiden Fällen $H_{p,q} = PSL_2(\mathbb{F}_q)$ gilt.
Theorem §4.8 aus dem zehnten Vortrag besagte, dass eine echte Untergruppe von $PSL_2(\mathbb{F}_q)$ mit mehr als 60 Elementen metabelsch ist. Zeigen wir, dass $\#H_{p,q} > 60$ und $H_{p,q}$ nicht metabelsch ist, haben wir also bewiesen, dass $H_{p,q} = PSL_2(\mathbb{F}_q)$ ist. Um zu zeigen, dass $\#H_{p,q} > 60$ ist, benutzen wir Bemerkung 11:

$$\#Y^{p,q} \geq \frac{q}{p}$$

Nach Annahme ist $p \geq 5$ und $q > p^8$. $\Rightarrow \#Y^{p,q} = \#{}^{\Lambda}/_{\Lambda(q)} = \frac{q}{p} > 120$. $H_{p,q}$ ist eine Untergruppe von Index 2, darum gilt $\#H_{p,q} > 60$.
Um zu zeigen, dass $H_{p,q}$ nicht metabelsch ist, benutzen wir Lemma §4.3 aus dem zehnten Vortrag. Das Lemma besagt, dass eine Gruppe G genau dann metabelsch ist, wenn für alle $g_1, g_2, g_3, g_4 \in G$ gilt:
$[[g_1, g_2], [g_3, g_4]] = 1$.
Wir müssen also $g_1, g_2, g_3, g_4 \in H_{p,q}$ finden, so dass

$$[[g_1, g_2], [g_3, g_4]] \neq 1.$$

Um dies zu zeigen, unterscheiden wir die beiden Fälle $\left(\frac{p}{q}\right) = 1$ und $\left(\frac{p}{q}\right) = -1$.

a) Sei $\left(\frac{p}{q}\right) = 1$. Wir wählen die g_i's aus $S_{p,q}$. Wähle für g_1 irgendein Element in $S_{p,q}$. Wähle g_2 so, dass $g_2 \neq g_1^{\pm 1}$. Setze $g_3 = g_1$ und wähle g_4 so, dass $g_4 \notin \{g_1^{\pm 1}, g_2^{\pm 1}\}$. Mit dieser Wahl ist $[[g_1, g_2], [g_3, g_4]]$ ein

reduziertes Wort der Länge 16, denn:

$$\begin{aligned}[[g_1,g_2],[g_3,g_4]] &= [g_1,g_2][g_3,g_4][g_1,g_2]^{-1}[g_3,g_4]^{-1}\\ &= [g_1,g_2][g_3,g_4][[g_2,g_1][g_4,g_3]\\ &= g_1g_2g_1^{-1}g_2^{-1}g_3g_4g_3^{-1}g_4^{-1}g_2g_1g_2^{-1}g_1^{-1}g_4g_3g_4^{-1}g_3^{-1}\end{aligned}$$

Nach Proposition 9 (und wegen der unteren Schranken für p und q) gilt für den Umfang von $Y^{p,q}$:

$$g(Y^{p,q}) \geq 2log_p q > 16$$

Ein reduziertes Wort über $S_{p,q}$ der Länge 16 kann nicht äquivalent sein zu der 1 in $H_{p,q}$, denn das würde bedeuten, dass dieses reduzierte Wort in $Y_{p,q}$ einen Kreis der Länge 16 darstellt. Einen Kreis der Länge 16 kann es in $Y_{p,q}$ aber nicht geben, da der Umfang von $Y_{p,q}$ größer ist als 16. Der Kommutator ist also ungleich 1 und $H_{p,q}$ somit nicht metabelsch.

b) Sei $\left(\frac{p}{q}\right) = -1$. Zunächst wählen wir $h_1, h_2, h_3 \in S_{p,q}$ wie folgt: Sei h_1 beliebig, $h_2 \neq h_1^{\pm 1}$ und $h_3 \notin \{h_1^{\pm 1}, h_2^{\pm 1}\}$. Dann setzen wir $g_1 = h_1h_3, g_2 = h_2h_3, g_3 = h_1h_2, g_4 = h_3h_2$. Die $g_1, ..., g_4$ sind Elemente von $H_{p,q}$. $[[g_1,g_2],[g_3,g_4]]$ ist dann ein reduziertes Wort der Länge 24, denn:

$$\begin{aligned}[[g_1,g_2],[g_3,g_4]] &= g_1g_2g_1^{-1}g_2^{-1}g_3g_4g_3^{-1}g_4^{-1}g_2g_1g_2^{-1}g_1^{-1}g_4g_3g_4^{-1}g_3^{-1}\\ &= h_1h_3h_2h_3(h_1h_3)^{-1}(h_2h_3)^{-1}h_1h_2h_3h_2(h_1h_2)^{-1}(h_3h_2)^{-1}h_2h_3h_1h_3(h_2h_3)^{-1}(h_1h_3)^{-1}h_3h_2h_1h_2(h_3h_2)^{-1}(h_1h_2)^{-1}\\ &= h_1h_3h_2h_1^{-1}h_3^{-1}h_2^{-1}h_1h_2h_3h_1^{-1}h_2^{-1}h_3^{-1}h_2h_3h_1h_2^{-1}h_3^{-1}h_1^{-1}h_3h_2h_1h_3^{-1}h_2^{-1}h_1^{-1}\end{aligned}$$

Nach Proposition 9 (und wegen der unteren Schranken für p und q) gilt für den Umfang von $Y^{p,q}$:

$$g(Y^{p,q}) \geq 4log_p q - log_p 4 > 24$$

Dass $H_{p,q}$ nicht metabelsch ist, folgt analog zu Teil a).

□

12. Korollar

Angenommen, $p \geq 5$, $q > p^8$. Die Graphen $X^{p,q}$ sind (p+1)-regulär, zusammenhängende Graphen. Außerdem:
a) Wenn $\left(\frac{p}{q}\right) = 1$, dann ist $X^{p,q}$ nicht bipartit mit

$$g(X^{p,q}) \geq \frac{2}{3} log_p \#X^{p,q}.$$

b) Wenn $\left(\frac{p}{q}\right) = -1$, dann ist $X^{p,q}$ bipartit mit

$$g(X^{p,q}) \geq \frac{4}{3} log_p \#X^{p,q} - log_p 4.$$

Beweis: Aus Theorem 11 folgt, dass die $X^{p,q}$ zusammenhängend sind.
Die Umfangabschätzungen folgen aus Proposition 9 und der Tatsache, dass $q^3 \geq \#X^{p,q}$.
Angenommen, $\left(\frac{p}{q}\right) = 1$. Mit Satz 1.5 aus dem letzten Vortrag und dem Zusammenhang von $X^{p,q}$ sowie der Einfachheit von $PSL_2(\mathbb{F}_q)$ (die im zehnten Vortrag gezeigt wurde), folgt, dass $X^{p,q}$ nicht bipartit ist.
Angenommen,$\left(\frac{p}{q}\right) = -1$. Die Aussage, dass $X^{p,q}$ in diesem Fall bipartit ist, wurde bereits im letzten Vortrag gezeigt. □