~~$\Lambda(2q) \leq \Lambda \leq \Lambda(2)$~~ — don't need this —

Λ acts transit. on $PGL_2(\mathbb{Q}_p)/K$ $\Rightarrow$ $\Lambda \cdot K = PGL_2(\mathbb{Q}_p)$

$$\Lambda(2q) \backslash T_{p+1} = \frac{Cay(\Lambda, S)}{\Lambda(2q)} = Cay\left(\frac{\Lambda}{\Lambda(2q)}, S\right)$$

Believe that $\Lambda = \Lambda(2)$. Assume $(q,2)=1$

$\Lambda(2)/\Lambda(2q)$ ⊜

$\Gamma = SL_d(\mathbb{Z})$, $\Gamma/\Gamma(q) = SL_d(\mathbb{Z}/q) = SL_d(\mathbb{Z}/2) \times SL_d(\mathbb{Z}/q)$

Strong approximation theorem

$\cong H(\mathbb{Z}[\frac{1}{p}]/q)^*/2 = H(\mathbb{F}_q)^*/2$

Now assume $q \equiv 1 \ (4)$, $\varepsilon = \sqrt{-1} \in \mathbb{F}_q$

$H(\mathbb{F}_q) \simeq M_2(\mathbb{F}_q) \Rightarrow H(\mathbb{F}_q)^*/2 = PGL_2(\mathbb{F}_q)$

31.12 Alex

Arithmetic groups

Let k be a global field (i.e. $[k:\mathbb{Q}] < \infty$, or $[k:\mathbb{F}_p(t)] < \infty$)

Let S be a finite set of valuations of k, including all S_∞ = the arch. val.

subring of integer $\mathcal{O}_S = \{x \in k \mid v(x) \geq 0, \forall v \notin S\}$

Ex 1) $k = \mathbb{Q}$, $S = \{p, \infty\}$, $\mathcal{O}_S = \mathbb{Z}[\frac{1}{p}]$

2) $k = \mathbb{F}_q(t)$, $\mathbb{F}_q[t, \frac{1}{t+1}]$

0) $\mathbb{Z}$

0') $\mathbb{F}_q[t]$

Let G be an k-alg gp, $G \hookrightarrow GL_n$ defined by poly's with coef in k.

e.g. $G = SL_n$, $G = Sp(2n, \_)$

S - auth $\Gamma = G(k) \cap GL_n(\mathcal{O}_S) \xhookrightarrow{\text{discrete}} \prod_{v \in S} G(k_v)$

Example 0) $\Gamma = SL_n(\mathbb{Z})$, $Sp(2n, \_)$

1) $\Gamma = SL_n(\mathbb{Z}[\frac{1}{p}]) \xhookrightarrow{\text{disc}} SL_n(\mathbb{R}) \times SL_n(\mathbb{Q}_p)$
but not disc. in any of them separately

If $\{0\} \neq I \lhd \mathcal{O}_S$ an ideal, $\Gamma(I) = \ker(\Gamma \to GL_n(\mathcal{O}_S/I))$

$[\mathcal{O}_S : I] < \infty$ automatically $\to$

$\to$ therefore $[\Gamma : \Gamma(I)] < \infty$ (principal congruence subgroup)

Thm (strong approx. thm) If G is semisimple and simply connected (e.g. SL_n, but PGL_n is not simply connected)

then (??) $\Gamma \to G(\mathcal{O}_S/I)$ is onto.

(!) Not true as stated, but close enough.

e.g. $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/p\mathbb{Z})$ is onto

Exercise Prove that $SL_n(\mathbb{F}_p)$ is generated by the elementary matrices.

Theorem Let $H \leq SL_2(\mathbb{Z})$ s.t. H is not virtually abelian, then for all large primes q, $H \to SL_2(\mathbb{Q})$ is onto.

Proof (assume not.) We can assume H is non-abelian free group. Every proper subgp of $SL_2(\mathbb{Q})$ is either metabelian (second commutator vanishes) or a subgroup of A_5.

Therefore $\exists$ a word $w(x,y,z,u)$ s.t. (for example, $w(x,y,z,u) = [[x,y],[z,u]]^{60}$) s.t. if $\pi: H \simeq F(x,y,z,w) \to SL_2(\mathbb{Q})$ is not onto, then $\pi(w) = e$.

Now if $g \in SL_n(\mathbb{Z})$ satisfies $\pi_q(w) = e$ for ∞-many q's then $g = 1$.

Contradiction. ∎

Look now at $PGL_2(\mathbb{Z}) = GL_2(\mathbb{Z})/\pm I$

$PGL_2(\mathbb{Z}) \to PGL_2(\mathbb{F}_q)$, q - prime

$PGL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q)/\{\pm I \mid t \in \mathbb{F}_q^*\}$

$PSL_2(\mathbb{F}_q) = SL_2(\mathbb{F}_q)/\pm I$

Claim $[PGL_2(q) : PSL_2(q)] = 2$, $q \geq 3$

Ex Compute $[PGL_n(q) : PSL_2(q)]$

$$GL_2(\mathbb{Z}) \to GL_2(\mathbb{F}_q) \to PGL_2(q) \quad \text{onto ?}$$

$$SL_2(\mathbb{Z}) \xrightarrow{\text{onto}} SL_2(\mathbb{F}_q) \xrightarrow{\text{onto}} PSL_2(q)$$

$$Im(PGL_2(\mathbb{Z}) \to PGL_2(q)) \supseteq PSL_2(q)$$

$Im(PGL_2(\mathbb{Z}) \to PGL_2(q))$ is onto if

$T_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$GL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) \cup SL_2(\mathbb{Z}) \cdot T_0$

$\det = \pm 1$ $\downarrow$

$\pm SL_2(q) = SL_2(q) \cup SL_2(q) \cdot T_0$

now look modulo $Z(GL_2(q))$

Claim $\forall$ $\exists$ $A \in SL_2(q)$ s.t. $\varphi(T_0) = \varphi(A)$, where $\varphi : GL_2(q) \to PGL_2(q)$, in $PGL_2(q)$ iff $q \equiv 1 \bmod 4$

Pf. $\varphi(A) = \varphi(T_0)$ iff $\exists\, z \in Z(GL_2(q))$

$z = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ s.t. $A = T_0 \cdot z$

$1 = \det A = \det(T_0 \cdot z) = \det(T_0) \cdot \det(z) = -z^2$

this has a solution $\Leftrightarrow$ $q \equiv 1 \bmod 4$ ∎

Cor If $q \equiv 1 \bmod 4$ $Im(PGL_2(\mathbb{Z}) \hookrightarrow PGL_2(q)) = PSL_2(q)$

If $q \geq 3$ mod 4, then $PGL_2(\mathbb{Z}) \to PGL_2(q)$ is onto.

Back to "over" arith gp

R - ring, $H(R) = \{ x_0 + x_1 i + x_2 j + x_3 k \mid x_i \in R, i^2 = j^2 = k^2 = -1, ij = k = -ji \}$

$G\left(H(\quad)^* / Z(H(\quad)^*) \right)$, $G(\mathbb{C}) = H(\mathbb{C})^* / Z = GL_2(\mathbb{C}) / Z =$

$= PGL_2(\mathbb{C})$

$p \equiv 1 \ (4)$ $\Gamma = G\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) \hookrightarrow \underset{\text{comp}}{G(\mathbb{R})} \times \underset{PGL_2(\mathbb{Q}_p)}{G(\mathbb{Q}_p)} \rightsquigarrow$

$\rightsquigarrow \Gamma \subset PGL_2(\mathbb{Q}_p)$

$\Lambda = \langle S \rangle$, $S = \{ \alpha_1, \dots \alpha_s, \bar{\alpha}_1, \dots \bar{\alpha}_s \}$ $s = \frac{p+1}{2}$

$S = \{ \alpha \in H(\mathbb{Z}) \mid \|\alpha\| = p, \alpha = x_0 + x_1 i + x_2 j + x_3 k, 0 < x_0 \text{ is odd} \}$

$Cay(\Lambda, S) \iff T_{p-1} = B_2(\mathbb{Q}_p)$

Really, $\Lambda = \Gamma(2)$

If q is prime, $\Lambda(2q) = \Gamma(2q) \trianglelefteq \Lambda(2)$

Thm ~~Study~~ $\Lambda(2q) \backslash B_2(\mathbb{Q}_p)$ one $(p+1)$-regular Ramanujan graphs.

This graph is $Cay\left(\frac{\Lambda}{\Lambda(2q)}, S\right)$

$$\frac{\Gamma(2)}{\Gamma(2q)} \hookrightarrow \frac{\Gamma}{\Gamma(2q)} \longrightarrow G\left(\mathbb{Z}\left[\tfrac{1}{p}\right] / 2q\right) \longrightarrow$$

$$\longrightarrow G\left(\mathbb{Z}\left[\tfrac{1}{p}\right] / 2\right) \times G\left(\mathbb{Z}\left[\tfrac{1}{p}\right] / q\right)$$

$\Lambda = \Gamma(2)$, assume $q \equiv 1 \ (4)$ $G\left(\mathbb{Z}\left[\frac{1}{p}\right] / q\right) = G(\mathbb{F}_q) =$

$= PGL_2(\mathbb{F}_q)$

$$\frac{\Lambda}{\Lambda(2q)} \longrightarrow PGL_2(\mathbb{F}_2)$$ the image contains $PSL_2(\mathbb{F}_2)$

$\alpha \in S$, $\pi_q : \Lambda \to PGL_2(q)$

$\alpha = x_0 + x_1 i + x_2 j + x_3 k \longrightarrow \alpha = [x_0] + [x_1] i \longrightarrow$
$x_i \in \mathbb{Z}$ mod q mod $\mathfrak{q}$

$\longrightarrow$ splitting $\begin{pmatrix} x_0 + x_1 \varepsilon & x_2 + x_3 \varepsilon \\ -x_2 + x_3 \varepsilon & x_0 - x_1 \varepsilon \end{pmatrix} \xrightarrow{\varphi_q} PGL_2(\mathbb{F}_q)$

where $\varepsilon = \sqrt{-1} \in \mathbb{F}_q$

$\det \alpha = p \bmod q$

$\varphi_q(\alpha) \in PSL_2(q)$ iff $\exists\, z = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}, z \in \mathbb{F}_q^*$, s.t.

$\det(\alpha \cdot z) = 1 \iff \underbrace{\det(\alpha)}_{p} \cdot z^2 = 1 \iff p = \left(\frac{1}{z}\right)^2 \bmod q$

$\mathrm{Im}(\Lambda \to PGL_2(q)) = PSL_2(q) \iff$ p is a quadratic residue mod q
i.e. $\left(\frac{p}{q}\right) = 1$

$\mathrm{Im}(\Lambda \to PGL_2(q)) = PGL_2(q) \iff$ p is not quad residue mod q
i.e. $\left(\frac{p}{q}\right) = -1$.

Corollary (1) If $\left(\frac{p}{q}\right) = -1$, then the Cayley graph
$\mathrm{Cay}\left(\frac{\Lambda}{N \trianglelefteq q}, S\right) \cong \mathrm{Cay}(PGL_2(q), S)$ is a bi-partite graph
one side is $PSL_2(q)$ and its coset is the other side

(2) If $\left(\frac{p}{q}\right) = -1$ then $\mathrm{Cay}\left(\frac{\Lambda}{\Lambda(q)}, S\right) = \mathrm{Cay}(PSL_2(q), S)$
is not bi-partite.

$X^{p,q} := \mathrm{Cay}\left(\frac{\Lambda}{\Lambda(q)}, S\right)$

Thm (1) The girth of $(X^{p,q})$ $\geq 2 \log_p q \sim \frac{2}{3} \log_{(k-1)}(k)$ (k-regular graph, $k = p+1$)

(2) If $\left(\frac{p}{q}\right) = -1$, girth $(X^{p,q}) \geq 4 \log_p q \sim \frac{4}{3} \log_k(n)$

$|X^{p,q}| \approx q^3$

Proposition $\forall$ k-reg graph on n vertices

$$girth(X) \leq 2\log_{k-1}(n)$$

proof

k-tree

$$1 + k + k\cdot(k-1) + \dots + k\cdot(k-1)^{\frac{g}{2}-1} \sim$$

$$\sim (k-1)^{\frac{g}{2}} \Rightarrow$$

$$\Rightarrow \quad n \geq (k-1)^{g/2}$$

$$g \leq 2\log_{k-1} n$$

□

Fix $k \geq 3$ $\exists$ graphs $X_{n,k}$, k-reg, $n \to \infty$

$girth(X_{n,k}) \geq 1 \cdot \log_{k-1}(n)$

0,67

$\frac{4}{3}$ greater than 1.

Erdös (random natural

Margulis (explicit constructi

$X^{p,q}$

Surprise!

Proof of (1) from the thm:

$S = \{\alpha_1, \dots \alpha_s, \bar{\alpha}_1, \dots \bar{\alpha}_s\}$

$Cay(\Lambda, S)$ – $(p+1)$-tree

girth in a Cayley graph $\leftrightarrow$ the shortest relation,

i.e. $w(\alpha_1, \dots \alpha_s, \bar{\alpha}_1, \dots \bar{\alpha}_s)$ is a non-reduced word which is in $\Lambda(2q)$.

$$\| w(\alpha_1, \dots \alpha_s, \dots) \| = p^{\ell}, \text{ where the length of } w \text{ is } \ell.$$

$$\| \alpha_i \alpha_j \| = \| \alpha_i \| \cdot \| \alpha_j \|.$$

$$w(\alpha_1, \dots \alpha_s \dots) \in \Lambda(2q)$$

$$w = a_0 + a_1 2q\, i + a_2 2q\, j + a_3 2q\, k$$

Claim $a_0 a_1 a_2 a_3 \neq 0$, because $w = a_0$ is in the center of Λ.

Hence $p^{\ell} = a_0^2 + a_1^2 \cdot 4q^2 + a_2^2 4q^2 + a_3^2 4q^2 \geq 4q^2 \Rightarrow$

$$\Rightarrow \quad \ell \geq 2\log_p q. \qquad \square$$