Lecture 6

Bounded generation property.

Γ - group, $S \subset \Gamma$.

Def. the set S *boundedly generates* Γ if $\exists n \geq 1$:

$$\Gamma = \{ s_1^{k_1} \dots s_n^{k_n} : s_i \in S, k_i \in \mathbb{Z} \}.$$

Thm (Carter-Keller) $SL(d, \mathbb{Z})$, $d \geq 3$, is boundedly generated by elementary matrices.

Conj. Let $\Gamma = G(\mathbb{Z})$ where G is a simple algebraic group defined over $\mathbb{Q}$. Assume that $G(\mathbb{R})/G(\mathbb{Z})$ is not compact ($\Leftrightarrow$ $G(\mathbb{Z})$ contains unipotent elements), and $\mathbb{R}\text{-rank}(G) \geq 2$.
Then Γ is boundedly generated.

Rmk. This conj. is known for split groups (Tavgen) and for some orthogonal groups (Erovenko-Rapinchuk).

Thm. (Lubotzky, Platonov-Rapinchuk)
Let G be a simply connected simple alg. group defined over $\mathbb{Q}$, $\Gamma = G(\mathbb{Z})$, and $G(\mathbb{R})/G(\mathbb{Z})$ is not compact.
Then (bounded generation of Γ) $\Rightarrow$ (congruence subgroup property).

Conj (Rapinchuk)
Let G be a simply connected simple alg. group defined over $\mathbb{Q}$ and $\Gamma = G(\mathbb{Z})$. Then

Γ has congruence subgroup property $\Leftrightarrow$ Γ is boundedly generated.

Open problems.

No examples are known of $\Gamma = G(\mathbb{Z})$ where G is simple alg. group defined over $\mathbb{Q}$, $G(\mathbb{R})/G(\mathbb{Z})$ is compact and Γ is boundedly generated infinite.

Thm $\Gamma = SL_2(\mathbb{Z}[\frac{1}{p}])$, p-prime, is boundedly generated.

Rmk. $SL_2(\mathbb{Z}[\sqrt{2}])$ is boundedly generated, but not $SL_2(\mathbb{Z})$.

Artin Conj. Let $m \in \mathbb{Z}$, $m \neq 0, \pm 1$, m is not perfect square.
$a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$.

Then $\exists$ infinitely many primes q: $q = a \pmod b$
m generates $(\mathbb{Z}/q)^\times$.

Proof (assuming Artin Conj.)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} q & b \\ * & d \end{pmatrix} \sim \begin{pmatrix} q & p^k \\ * & * \end{pmatrix} \sim \begin{pmatrix} 1 & p^k \\ * & * \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$$

$$\uparrow$$

$$b = p^k \pmod q$$

Proof of Carter-Keller Thm.

A possible approach: $R = \prod_{n \geq 1}^{\infty} \mathbb{Z}$

$[SL_4(\mathbb{Z})$ is boundedly generated by elementary matrices$] \Leftrightarrow [SL_4(\mathbb{R})$ is generated by elementary matrices$]$

To prove the later, one can use the same strategy as in the proof of the congruence subgroup property for $SL_4(\mathbb{Z})$.

However, we follow a more elementary approach.

Lem. Every $A \in SL_d(\mathbb{Z})$, $d \geq 3$, can be transformed to $\left(\begin{array}{cc|c} a & b & 0 \\ c & d & 0 \\ \hline 0 & 0 & E \end{array}\right)$ using $O(d^2)$ elementary operations

$$A = \left(\begin{array}{c|c} * & \\ \hline u_1 \dots u_d & \end{array}\right)$$

If $u_1 = \dots = u_{d-1} = 0$, then $u_d = \pm 1$, and we are done by induction.

Otherwise, we pick an integer t:

$$t = \begin{cases} 1 \pmod p & \text{for primes } p \mid u_1, \dots u_{d-1} \\ 0 \pmod p & \text{for primes } p \mid u_2, \dots u_{d-1} \\ & p \nmid u_1. \end{cases}$$

Then $\gcd(u_1, \dots u_d) = 1 \Rightarrow \gcd(u_1 + t u_d, u_2, \dots u_{d-1}) = 1$.

We have

$$A \overset{1\text{-op.}}{\sim} \left(\begin{array}{c|c} * & \\ \hline u_1' u_2 \dots u_d & \end{array}\right) \overset{(d-1)\text{-op.}}{\sim} \left(\begin{array}{c|c} * & \\ \hline u_1' u_2 \dots u_{d-1} \ 1 & \end{array}\right) \overset{(d-1)\text{-op.}}{\sim} \left(\begin{array}{c|c} * & \\ \hline 0 \dots 0 \ 1 & \end{array}\right)$$

$\gcd(u_1', \dots u_{d-1}) = 1$

$t_1 u_1' + \dots + t_{d-1} u_{d-1} = u_d - 1$

The claim follows by induction on d.

Lem. Let $n \in \mathbb{N}$, $A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} a^n & b & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z})$.
Then A^n can be transformed to B using 16 elementary operations.

By Cayley-Hamilton Thm, $L^n = fE + gL$, $f, g \in \mathbb{Z}$. for $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Hence, $A^n = \begin{pmatrix} f + ga & bg & 0 \\ c'' & d'' & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$A^n = \begin{pmatrix} a^n & 0 & 0 \\ * & d^n & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod b$$

$f + ga = a^n + bu$ for some $u \in \mathbb{Z}$.

It follows that $B = \begin{pmatrix} f+ag-bu & b & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$\sim \begin{pmatrix} f+ag & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Claim. [A matrix $\begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ga \\ * & * & * \end{pmatrix}$ is a product of 10 elementary matrices.]

$$\begin{pmatrix} f+ag & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ag \\ 1 & * & * \end{pmatrix} = \begin{pmatrix} f+ag & bg & 0 \\ * & * & * \\ * & * & * \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} f+ag & bg & 0 \\ * & * & 1 \\ * & * & 1 \end{pmatrix} \sim \begin{pmatrix} f+ag & bg & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\det = 1 \Rightarrow (f+ag)(c''-c''') = bg(d''-d''')$.

$\gcd(f+ag, bg) = 1 \Rightarrow$ $c''' = c'' + r \cdot bg$

$d''' = d'' + r \cdot (f+ag)$

Hence, $B \sim A^n$, as required. ∎

Proof of the claim.

$1 = \det(f \cdot E + gL) = \det(gL) \pmod f = g^2 \pmod f$.

Hence $f \mid (g-1)(g+1) \Rightarrow$ $\begin{cases} f = f^+ f^- \\ g+1 = f^+ g^+ \\ g-1 = f^- g^- \end{cases}$

$$e_{23}^{f^-} e_{32}^{g^-} e_{31}^{-1} e_{13}^{1-f^+} e_{23}^{-f^-} e_{31}^{g^+} = \begin{pmatrix} * & 0 & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & * & * \\ 0 & g & f \\ 1 & * & * \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -b \\ 0 & g & f+ga \\ 1 & * & * \end{pmatrix}$$

Lem. Every $A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SL_3(\mathbb{Z})$ can be written as product of 4 elementary matrices.

Using 1 operation, we can make b odd.
If $b \equiv 1 \pmod 4$, we consider A^{-1}, so we may assume that $b \equiv -1 \pmod 4$.
If $c = 0$ or $d = 0$, the proof is easy.
Since $\gcd(b, 4d) = 1$, $\exists$ prime $p \equiv b \pmod{4d}$ (then $p \equiv -1 \pmod 4$).

$$A \sim \begin{pmatrix} u & p & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pick integer t: $t \equiv \begin{cases} c \pmod u \\ -1 \pmod r \text{ for primes } r \mid p-1, \ r \nmid u. \end{cases}$

For primes $s \mid p-1, u$, we have

$$1 = ud - pc \equiv -c \pmod s \equiv -t \pmod s.$$

Hence, $t \equiv -1 \pmod s$ for all primes $s \mid p-1$.
In particular, $\gcd(p-1, t) = 1$, and $\gcd((p-1)u, t) = 1$.
Moreover, $\gcd\left(\frac{p-1}{2}, t-1\right) = 1$ because $\frac{p-1}{2}$ is odd.
Pick a prime $q \equiv t \pmod{(p-1)u}$.
Note that $\gcd\left(\frac{p-1}{2}, q-1\right) = 1 \Rightarrow$ $\boxed{k \cdot \frac{p-1}{2} - \ell \cdot (q-1) = 1 \text{ for integers } k \text{ and } \ell.}$

$$\left.\begin{aligned} t &= m \cdot u + c \\ q &= m'(p-1)u + t \end{aligned}\right] \Rightarrow q \equiv c \pmod u$$

$$A \sim \begin{pmatrix} u & p & 0 \\ q & v & 0 \\ 0 & 0 & 1 \end{pmatrix} = C$$

By Fermat Thm, $v^{(q-1)\ell} = 1 + \alpha q$ for some $\alpha \in \mathbb{Z}$.

Let $B = e_{12}^{-q} \cdot e_{21}^{-\alpha} = \begin{pmatrix} 1+\alpha q & -q & 0 \\ -\alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} v^{(q-1)\ell} & -q & 0 \\ -\alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

By Lemma, B can be transformed to $\begin{pmatrix} v & -q & 0 \\ -p & u & 0 \\ 0 & 0 & 1 \end{pmatrix}^{(q-1)\ell}$

using 16 elementary operations.

Note that $\begin{pmatrix} v & -q & 0 \\ -p & u & 0 \\ 0 & 0 & 1 \end{pmatrix} = {}^tC^{-1}$.

Hence, $C^{-(q-1)\ell} \sim E$.

We have $u^{k(p+1)/2} = \pm 1 \pmod p$.

1) $u^{k(p-1)/2} = 1 \pmod p$. $u^{k(p-1)/2} = 1 + \beta p$ for some $\beta \in \mathbb{Z}$.

Let $D = e_{12}^{p} e_{21}^{\beta} = \begin{pmatrix} u^{k(p-1)/2} & p & 0 \\ \beta & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

By Lemma, $D \sim C^{k(p-1)/2} \Rightarrow C^{k(p-1)/2} \sim E$.

Finally, $C = C^{k(p-1)/2} \cdot C^{-\ell(q-1)} \sim E$.

2) $u^{k(p-1)/2} = -1 \pmod p$. $u^{k(p+1)/2} = -1 + \beta p$ for some $\beta \in \mathbb{Z}$.

$$e_{12}^{-p} e_{21}^{\beta} = \begin{pmatrix} 1-p\beta & -p & 0 \\ \beta & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1-p\beta+2\beta & 2-p & 0 \\ \beta & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1-p\beta+2\beta & 2-p & 0 \\ -1+p\beta-\beta & p-1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} -1+\beta p & p & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} u^{k(p-1)/2} & p & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \underset{\text{Lemma}}{\sim} C^{k(p-1)/2} \Rightarrow C^{k(p-1)/2} \sim E.$$

Finally, $C = C^{k(p-1)/2} \cdot C^{-\ell(q-1)} \sim E$.