Unipotent Generators for Arithmetic Groups

T.N.Venkataramana

Zariski Dense Subgroups, number theory and geometric applications, ICTS, Bengaluru

January 10, 2023

I thank G.Prasad, Q, A.Rapinchuk, B.Sury and Aleksy Tralle, for their invitation to take part in this great conference.

I thank G.Prasad, Q, A.Rapinchuk, B.Sury and Aleksy Tralle, for their invitation to take part in this great conference.

I will talk about unipotent generators for arithmetic groups. To illustrate the kind of results discussed here, let me start with a non-example.

The group $SL(2, \mathbb{Z})$

Consider a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ of finite index. The elementary subgroup Δ of Γ is the subgroup of Γ generated by the upper and lower triangular matrices $U^+ \cap \Gamma$ and $U^- \cap \Gamma$ in the group Γ.

The group $SL(2, \mathbb{Z})$

Consider a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ of finite index. The elementary subgroup Δ of Γ is the subgroup of Γ generated by the upper and lower triangular matrices $U^+ \cap \Gamma$ and $U^- \cap \Gamma$ in the group Γ.
For example, if Γ is the principal congruence subgroup of level m in $SL_2(\mathbb{Z})$, then

$$\Delta = < \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} > .$$

The group $SL(2, \mathbb{Z})$

Consider a subgroup $\Gamma \subset SL_2(\mathbb{Z})$ of finite index. The elementary subgroup Δ of Γ is the subgroup of Γ generated by the upper and lower triangular matrices $U^+ \cap \Gamma$ and $U^- \cap \Gamma$ in the group Γ.
For example, if Γ is the principal congruence subgroup of level m in $SL_2(\mathbb{Z})$, then

$$\Delta = < \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} > .$$

If $m \geq 3$, then Δ has infinite index in Γ (or in $SL_2(\mathbb{Z})$).

The Group $SL_n(\mathbb{Z})$

In contrast, a theorem of J.Tits says that if Γ is a subgroup of finite index in $SL_n(\mathbb{Z})$ for $n \geq 3$, then the subgroup Δ of Γ generated by upper and lower triangular unipotent matrices in Γ has finite index in Γ.

The Group $SL_n(\mathbb{Z})$

In contrast, a theorem of J.Tits says that if Γ is a subgroup of finite index in $SL_n(\mathbb{Z})$ for $n \geq 3$, then the subgroup Δ of Γ generated by upper and lower triangular unipotent matrices in Γ has finite index in Γ.

The proof uses the methods of the *proof* of the congruence subgroup property for $SL_n(\mathbb{Z})$ ($n \geq 3$).

The Group $SL_n(\mathbb{Z})$

In contrast, a theorem of J.Tits says that if Γ is a subgroup of finite index in $SL_n(\mathbb{Z})$ for $n \geq 3$, then the subgroup Δ of Γ generated by upper and lower triangular unipotent matrices in Γ has finite index in Γ.

The proof uses the methods of the *proof* of the congruence subgroup property for $SL_n(\mathbb{Z})$ ($n \geq 3$).

The group $SL_2(\mathbb{Z})$ is a lattice in the real rank one group $SL_2(\mathbb{R})$, whereas, for $n \geq 3$, the group $SL_n(\mathbb{Z})$ is a lattice in a "higher rank" group $SL_n(\mathbb{R})$.

Generalisation

Suppose G is a connected linear semi-simple algebraic group defined over $\mathbb{Q}$. Assume G is $\mathbb{Q}$-simple; that is, the only connected normal algebraic subgroups of G are G and the trivial group.

Generalisation

Suppose G is a connected linear semi-simple algebraic group defined over $\mathbb{Q}$. Assume G is $\mathbb{Q}$-simple; that is, the only connected normal algebraic subgroups of G are G and the trivial group.

Assume also that G has higher real rank i.e. $\mathbb{R} - rank(G) \geq 2$.

Generalisation

Suppose G is a connected linear semi-simple algebraic group defined over $\mathbb{Q}$. Assume G is $\mathbb{Q}$-simple; that is, the only connected normal algebraic subgroups of G are G and the trivial group.

Assume also that G has higher real rank i.e. $\mathbb{R} - rank(G) \geq 2$.

Assume further that $\mathbb{Q} - rank(G) \geq 1$ (equivalent conditions: (2) $G(\mathbb{R})/G(\mathbb{Z})$ is non-compact, (3) $G(\mathbb{Z})$ has unipotent elements and (4) G has a proper parabolic subgroup P defined over $\mathbb{Q}$) .

Generalisation

Suppose G is a connected linear semi-simple algebraic group defined over $\mathbb{Q}$. Assume G is $\mathbb{Q}$-simple; that is, the only connected normal algebraic subgroups of G are G and the trivial group.

Assume also that G has higher real rank i.e. $\mathbb{R} - rank(G) \geq 2$.

Assume further that $\mathbb{Q} - rank(G) \geq 1$ (equivalent conditions: (2) $G(\mathbb{R})/G(\mathbb{Z})$ is non-compact, (3) $G(\mathbb{Z})$ has unipotent elements and (4) G has a proper parabolic subgroup P defined over $\mathbb{Q}$) .

Fix a proper parabolic $\mathbb{Q}$-subgroup $P \subset G$, with unipotent radical $U = U^+$. Let U^- be the opposite unipotent radical.

The Main Result

Theorem 1

With the foregoing assumptions, given a subgroup $\Gamma \subset G(\mathbb{Z})$ *of finite index, the "elementary subgroup"* Δ *of* Γ *generated by* $U^+ \cap \Gamma$ *and* $U^- \cap \Gamma$ *has finite index in* Γ*.*

The Main Result

Theorem 1

With the foregoing assumptions, given a subgroup $\Gamma \subset G(\mathbb{Z})$ of finite index, the "elementary subgroup" Δ of Γ generated by $U^+ \cap \Gamma$ and $U^- \cap \Gamma$ has finite index in Γ.

This theorem is due to various people (Tits (1976) for Chevalley Groups $\mathcal{G}$ over number fields K with $K - rank(\mathcal{G}) \geq 2$; Vaserstein (1973) for classical groups of higher rank over number fields, and due to Raghunathan and myself in general (1994)).

The Main Result

Theorem 1

With the foregoing assumptions, given a subgroup $\Gamma \subset G(\mathbb{Z})$ of finite index, the "elementary subgroup" Δ of Γ generated by $U^+ \cap \Gamma$ and $U^- \cap \Gamma$ has finite index in Γ.

This theorem is due to various people (Tits (1976) for Chevalley Groups $\mathcal{G}$ over number fields K with $K - rank(\mathcal{G}) \geq 2$; Vaserstein (1973) for classical groups of higher rank over number fields, and due to Raghunathan and myself in general (1994)).

A very different, but similar looking result is due to Hee Oh (1998), Benoist-Oh (2010), Benoist and Miquel (2020), who proved that if $\Gamma \subset G(\mathbb{R})$ is a Zariski dense discrete subgroup generated by lattices in opposing unipotent radicals of *real* parabolic subgroups, then Γ is a lattice (provided $\mathbb{R} - rank(G) \geq 2$). I understand that the proof uses the foregoing theorem.

Remarks

The earlier proof by Raghunathan and myself was quite general, but especially in the $\mathbb{Q}-rank(G)=1$ case, involved some complicated case-by-case check (of an $SU(2,1)$-reduction for a complicated system of embedded $SU(2,1)$'s) . The present proof is uniform and is much shorter. It uses, however, certain embedded SL_2 (the Jacobson-Morozov Theorem).

Remarks

The earlier proof by Raghunathan and myself was quite general, but especially in the $\mathbb{Q} - rank(G) = 1$ case, involved some complicated case-by-case check (of an $SU(2,1)$-reduction for a complicated system of embedded $SU(2,1)$'s) . The present proof is uniform and is much shorter. It uses, however, certain embedded SL_2 (the Jacobson-Morozov Theorem).

In the $\mathbb{Q} - rank(G) = 1$ case, the Artin reciprocity law was also used crucially, but the present proof uses "only" the Dirichlet theorem on the infinitude of primes in arithmetic progressions.

Remarks

The earlier proof by Raghunathan and myself was quite general, but especially in the $\mathbb{Q} - rank(G) = 1$ case, involved some complicated case-by-case check (of an $SU(2,1)$-reduction for a complicated system of embedded $SU(2,1)$'s) . The present proof is uniform and is much shorter. It uses, however, certain embedded SL_2 (the Jacobson-Morozov Theorem).

In the $\mathbb{Q} - rank(G) = 1$ case, the Artin reciprocity law was also used crucially, but the present proof uses "only" the Dirichlet theorem on the infinitude of primes in arithmetic progressions.

If $\mathbb{R} - rank(G) = 1$, then for most congruence subgroups $\Gamma \subset G(\mathbb{Z})$, the elementary subgroup Δ has infinite index. In this sense, the statement is always false for real rank one groups.

Remarks

The proof also gives the centrality of the congruence subgroup kernel C in the non-uniform case (due to Raghunathan). Once the centrality is proved, (assuming that G is simply connected) the finiteness and the exact computation of C follows (from the work of Raghunathan, Gopal Prasad and Rapinchuk).

Remarks

The proof also gives the centrality of the congruence subgroup kernel C in the non-uniform case (due to Raghunathan). Once the centrality is proved, (assuming that G is simply connected) the finiteness and the exact computation of C follows (from the work of Raghunathan, Gopal Prasad and Rapinchuk).

Rapinchuk (unpublished) has a proof of centrality of the congruence subgroup kernel which does not even use the Dirichlet theorem.

Given a **maximal** parabolic $\mathbb{Q}$-subgroup P, with unipotent radical U and a Levi decomposition $P = MU$, let $P^- = U^- M$ be the opposite parabolic subgroup. Let $F(m)$ denote the subgroup of $G(\mathbb{Z})$ generated by $P(m)$ and $P^-(m)$. By results of Nori and Weisfeiler, there is a smallest congruence subgroup Γ_m of $G(\mathbb{Z})$ containing $F(m)$. Note that Γ_m is an arithmetic group.

Given a **maximal** parabolic $\mathbb{Q}$-subgroup P, with unipotent radical U and a Levi decomposition $P = MU$, let $P^- = U^- M$ be the opposite parabolic subgroup. Let $F(m)$ denote the subgroup of $G(\mathbb{Z})$ generated by $P(m)$ and $P^-(m)$. By results of Nori and Weisfeiler, there is a smallest congruence subgroup Γ_m of $G(\mathbb{Z})$ containing $F(m)$. Note that Γ_m is an arithmetic group.

Theorem 2

If $\mathbb{R} - rank(G) \geq 2$, then $F(m)$ contains the commutator subgroup $[\Gamma_m, \Gamma_m]$.

Given a **maximal** parabolic $\mathbb{Q}$-subgroup P, with unipotent radical U and a Levi decomposition $P = MU$, let $P^- = U^- M$ be the opposite parabolic subgroup. Let $F(m)$ denote the subgroup of $G(\mathbb{Z})$ generated by $P(m)$ and $P^-(m)$. By results of Nori and Weisfeiler, there is a smallest congruence subgroup Γ_m of $G(\mathbb{Z})$ containing $F(m)$. Note that Γ_m is an arithmetic group.

Theorem 2

If $\mathbb{R} - rank(G) \geq 2$, then $F(m)$ contains the commutator subgroup $[\Gamma_m, \Gamma_m]$.

The Margulis normal subgroup theorem immediately implies that $F(m)$ is arithmetic.

Given a **maximal** parabolic $\mathbb{Q}$-subgroup P, with unipotent radical U and a Levi decomposition $P = MU$, let $P^- = U^- M$ be the opposite parabolic subgroup. Let $F(m)$ denote the subgroup of $G(\mathbb{Z})$ generated by $P(m)$ and $P^-(m)$. By results of Nori and Weisfeiler, there is a smallest congruence subgroup Γ_m of $G(\mathbb{Z})$ containing $F(m)$. Note that Γ_m is an arithmetic group.

Theorem 2

If $\mathbb{R} - rank(G) \geq 2$, then $F(m)$ contains the commutator subgroup $[\Gamma_m, \Gamma_m]$.

The Margulis normal subgroup theorem immediately implies that $F(m)$ is arithmetic. Since $\Delta_P(m) = \Delta(m) =< U(m), U^-(m) >$ is normalised by $F(m) =< U(m), M(m), U^-(m) >$, it follows that the elementary group $\Delta_P(m)$ is arithmetic, for *maximal* parabolic subgroups P.

Given a **maximal** parabolic $\mathbb{Q}$-subgroup P, with unipotent radical U and a Levi decomposition $P = MU$, let $P^- = U^- M$ be the opposite parabolic subgroup. Let $F(m)$ denote the subgroup of $G(\mathbb{Z})$ generated by $P(m)$ and $P^-(m)$. By results of Nori and Weisfeiler, there is a smallest congruence subgroup Γ_m of $G(\mathbb{Z})$ containing $F(m)$. Note that Γ_m is an arithmetic group.

Theorem 2

If $\mathbb{R} - rank(G) \geq 2$, then $F(m)$ contains the commutator subgroup $[\Gamma_m, \Gamma_m]$.

The Margulis normal subgroup theorem immediately implies that $F(m)$ is arithmetic. Since $\Delta_P(m) = \Delta(m) =< U(m), U^-(m) >$ is normalised by $F(m) =< U(m), M(m), U^-(m) >$, it follows that the elementary group $\Delta_P(m)$ is arithmetic, for *maximal* parabolic subgroups P. But, for any parabolic subgroup $Q \subset P$ with P maximal, and unipotent radicals V, U respectively, we have the inclusion of unipotent radicals $U \subset V$, and hence $\Delta_Q(m) \supset \Delta_P(m)$ is arithmetic.

A Topology on $G(\mathbb{Q})$

Assume that P is a **maximal** parabolic $\mathbb{Q}$-subgroup of G. We have the opposite parabolic subgroup P^-. The first step in the proof is to consider the system $\{F(m)\}_{m\geq 1}$ of subgroups generated by the congruence subgroups $P^{\pm}(m\mathbb{Z})$. We designate this family to be a fundamental system of neighbourhoods of identity. By left translation, we get a fundamental system of neighbourhoods of any element of $G(\mathbb{Q})$.

A Topology on $G(\mathbb{Q})$

Assume that P is a **maximal** parabolic $\mathbb{Q}$-subgroup of G. We have the opposite parabolic subgroup P^-. The first step in the proof is to consider the system $\{F(m)\}_{m\geq 1}$ of subgroups generated by the congruence subgroups $P^{\pm}(m\mathbb{Z})$. We designate this family to be a fundamental system of neighbourhoods of identity. By left translation, we get a fundamental system of neighbourhoods of any element of $G(\mathbb{Q})$.

Let us say that a sequence $(g_k)_{k\geq 1}$ in $G(\mathbb{Q})$ is a *Cauchy sequence*, if given any integer $m \geq 1$, there exists an integer $K = K(m)$ such that for $k, l \geq K$, we have $g_k^{-1} g_l \in F(m)$.

A Topology on $G(\mathbb{Q})$

Assume that P is a **maximal** parabolic $\mathbb{Q}$-subgroup of G. We have the opposite parabolic subgroup P^-. The first step in the proof is to consider the system $\{F(m)\}_{m\geq 1}$ of subgroups generated by the congruence subgroups $P^{\pm}(m\mathbb{Z})$. We designate this family to be a fundamental system of neighbourhoods of identity. By left translation, we get a fundamental system of neighbourhoods of any element of $G(\mathbb{Q})$.

Let us say that a sequence $(g_k)_{k\geq 1}$ in $G(\mathbb{Q})$ is a *Cauchy sequence*, if given any integer $m \geq 1$, there exists an integer $K = K(m)$ such that for $k, l \geq K$, we have $g_k^{-1} g_l \in F(m)$.

Two Cauchy sequences $\{g_k\}$ and $\{h_k\}$ are equivalent if given the "level" m, there exists an integer $K = K(m)$ such that for all $k \geq K$, we have $g_k^{-1} h_k \in F(m)$.

A Topology on $G(\mathbb{Q})$

Assume that P is a **maximal** parabolic $\mathbb{Q}$-subgroup of G. We have the opposite parabolic subgroup P^-. The first step in the proof is to consider the system $\{F(m)\}_{m\geq 1}$ of subgroups generated by the congruence subgroups $P^{\pm}(m\mathbb{Z})$. We designate this family to be a fundamental system of neighbourhoods of identity. By left translation, we get a fundamental system of neighbourhoods of any element of $G(\mathbb{Q})$.

Let us say that a sequence $(g_k)_{k\geq 1}$ in $G(\mathbb{Q})$ is a *Cauchy sequence*, if given any integer $m \geq 1$, there exists an integer $K = K(m)$ such that for $k, l \geq K$, we have $g_k^{-1} g_l \in F(m)$.

Two Cauchy sequences $\{g_k\}$ and $\{h_k\}$ are equivalent if given the "level" m, there exists an integer $K = K(m)$ such that for all $k \geq K$, we have $g_k^{-1} h_k \in F(m)$. Given two Cauchy sequences (g_k) and (h_k), we can form the product sequence $(g_k h_k)$ and the inverse sequence (g_k^{-1}).

Theorem 3

If $\mathbb{R} - rank(G) \geq 2$, then $(g_k h_k)$ and (g_k^{-1}) are Cauchy sequences. The set of equivalence classes of Cauchy sequences then becomes a topological group $\mathcal{G}$, with a continuous surjective homomorphism $\mathcal{G} \to \overline{G(\mathbb{Q})}$, with kernel K, say.

Theorem 3

If $\mathbb{R} - rank(G) \geq 2$, then $(g_k h_k)$ and (g_k^{-1}) are Cauchy sequences. The set of equivalence classes of Cauchy sequences then becomes a topological group $\mathcal{G}$, with a continuous surjective homomorphism $\mathcal{G} \to \overline{G(\mathbb{Q})}$, with kernel K, say.

If $\mathbb{R} - rank(G) \geq 2$, then the kernel K is central in $\mathcal{G}$.

Theorem 3

If $\mathbb{R} - rank(G) \geq 2$*, then* $(g_k h_k)$ *and* (g_k^{-1}) *are Cauchy sequences. The set of equivalence classes of Cauchy sequences then becomes a topological group* $\mathcal{G}$*, with a continuous surjective homomorphism* $\mathcal{G} \to \overline{G(\mathbb{Q})}$*, with kernel* K*, say.*

If $\mathbb{R} - rank(G) \geq 2$*, then the kernel* K *is central in* $\mathcal{G}$*.*

Thus, the higher rank assumption is used twice: to prove that the completion $\mathcal{G}$ of $G(\mathbb{Q})$ (with respect to the system $F(m)$ of subgroups) exists *as a topological group*, and also to prove that the relevant kernel K is central.

Theorem 3 implies Theorem 2

Suppose $\widehat{\Gamma_m}$ and $\widehat{F(m)}$ are the closures of Γ_m and $F(m)$ in the completion $\mathcal{G}$. Since Γ_m and $F(m)$ have the same closure in the congruence completion $\overline{G(\mathbb{Q})}$, it follows that $\widehat{\Gamma_m} \subset \widehat{F(m)}K$.

Theorem 3 implies Theorem 2

Suppose $\widehat{\Gamma_m}$ and $\widehat{F(m)}$ are the closures of Γ_m and $F(m)$ in the completion $\mathcal{G}$. Since Γ_m and $F(m)$ have the same closure in the congruence completion $\overline{G(\mathbb{Q})}$, it follows that $\widehat{\Gamma_m} \subset \widehat{F(m)}K$.

Taking commutators, and noting that K is central by Theorem 3, we get the chain of inclusions

$$[\Gamma_m, \Gamma_m] \subset [\widehat{\Gamma_m}, \widehat{\Gamma_m}] = [\widehat{F(m)}, \widehat{F(m)}] \subset \widehat{F(m)}.$$

Theorem 3 implies Theorem 2

Suppose $\widehat{\Gamma_m}$ and $\widehat{F(m)}$ are the closures of Γ_m and $F(m)$ in the completion $\mathcal{G}$. Since Γ_m and $F(m)$ have the same closure in the congruence completion $\overline{G(\mathbb{Q})}$, it follows that $\widehat{\Gamma_m} \subset \widehat{F(m)}K$.

Taking commutators, and noting that K is central by Theorem 3, we get the chain of inclusions

$$[\Gamma_m, \Gamma_m] \subset [\widehat{\Gamma_m}, \widehat{\Gamma_m}] = [\widehat{F(m)}, \widehat{F(m)}] \subset \widehat{F(m)}.$$

Intersecting with $G(\mathbb{Q})$ we then get $[\Gamma_m, \Gamma_m] \subset F(m)$, proving Theorem 2.

Existence of a topological group structure on $\mathcal{G}$

It is a generality that the completion $\mathcal{G}$ with respect to the fundamental system of neighbourhoods $\{F(m)\}_{m\in\mathbb{Z}}$ is a topological group, if and only if , given m and $g \in G(\mathbb{Q})$, there exists m' such that ${}^{g}(F(m)) = gF(m)g^{-1} \supset F(m')$.

Existence of a topological group structure on $\mathcal{G}$

It is a generality that the completion $\mathcal{G}$ with respect to the fundamental system of neighbourhoods $\{F(m)\}_{m\in\mathbb{Z}}$ is a topological group, if and only if , given m and $g \in G(\mathbb{Q})$, there exists m' such that ${}^{g}(F(m)) = gF(m)g^{-1} \supset F(m')$.

To see how the higher rank assumption is used in the existence of the completion, consider the "generic conjugate" ${}^{g}(F(m))$, where $g \in U^{-}P$ is a rational element. Let $M = P \cap P^{-}$ be the Levi subgroup of P. Then for some m',

$$ {}^{g}(F(m)) \cap F(m) \supset {}^{u^{-}p}(P(m)) \cap P^{-}(m) = {}^{u^{-}}(P \cap P^{-}(m')) = {}^{u^{-}}(M(m'\mathbb{Z})). $$

Existence of a topological group structure on $\mathcal{G}$

It is a generality that the completion $\mathcal{G}$ with respect to the fundamental system of neighbourhoods $\{F(m)\}_{m\in\mathbb{Z}}$ is a topological group, if and only if , given m and $g \in G(\mathbb{Q})$, there exists m' such that ${}^{g}(F(m)) = gF(m)g^{-1} \supset F(m')$.

To see how the higher rank assumption is used in the existence of the completion, consider the "generic conjugate" ${}^{g}(F(m))$, where $g \in U^{-}P$ is a rational element. Let $M = P \cap P^{-}$ be the Levi subgroup of P. Then for some m',

$$ {}^{g}(F(m))\cap F(m) \supset {}^{u^{-}p}(P(m))\cap P^{-}(m) = {}^{u^{-}}(P\cap P^{-}(m')) = {}^{u^{-}}(M(m'\mathbb{Z})). $$

In the higher rank case, the group $M(\mathbb{Z})$ is infinite, and this allows us to prove that the above intersection has many elements, which also proves (by replacing g by $g\gamma$ for varying $\gamma \in F(m)$) that ${}^{g}(F(m))$ contains $P^{-}(m')$ for some m'. Similarly, ${}^{g}(F(m)) \supset P(m')$ for some m'.

Existence of a topological group structure on $\mathcal{G}$

It is a generality that the completion $\mathcal{G}$ with respect to the fundamental system of neighbourhoods $\{F(m)\}_{m\in\mathbb{Z}}$ is a topological group, if and only if , given m and $g \in G(\mathbb{Q})$, there exists m' such that ${}^{g}(F(m)) = gF(m)g^{-1} \supset F(m')$.

To see how the higher rank assumption is used in the existence of the completion, consider the "generic conjugate" ${}^{g}(F(m))$, where $g \in U^{-}P$ is a rational element. Let $M = P \cap P^{-}$ be the Levi subgroup of P. Then for some m',

$$ {}^{g}(F(m)) \cap F(m) \supset {}^{u^{-}p}(P(m)) \cap P^{-}(m) = {}^{u^{-}}(P \cap P^{-}(m')) = {}^{u^{-}}(M(m'\mathbb{Z})). $$

In the higher rank case, the group $M(\mathbb{Z})$ is infinite, and this allows us to prove that the above intersection has many elements, which also proves (by replacing g by $g\gamma$ for varying $\gamma \in F(m)$) that ${}^{g}(F(m))$ contains $P^{-}(m')$ for some m'. Similarly, ${}^{g}(F(m)) \supset P(m')$ for some m'. This implies ${}^{g}(F(m)) \supset F(m')$ for some m'. The existence of the completion then follows easily.

Centrality for the group $SL_2(\mathbb{Z}[\sqrt{2}])$

Consider the exact sequence $1 \to K \to \mathcal{G} \to \overline{G(\mathbb{Q})} \to 1$, where $\mathcal{G}$ is the completion of $G(\mathbb{Q})$ with respect to the "$F(m)$" completion, and $\overline{G(\mathbb{Q})}$ is the congruence completion. (By general considerations), the group K is the inverse limit of the *sets* $K_m = F(m)\backslash\Gamma_m/F(m)$ (equpped with the discrete topology) as m varies.

Centrality for the group $SL_2(\mathbb{Z}[\sqrt{2}])$

Consider the exact sequence $1 \to K \to \mathcal{G} \to \overline{G(\mathbb{Q})} \to 1$, where $\mathcal{G}$ is the completion of $G(\mathbb{Q})$ with respect to the "$F(m)$" completion, and $\overline{G(\mathbb{Q})}$ is the congruence completion. (By general considerations), the group K is the inverse limit of the *sets* $K_m = F(m)\backslash\Gamma_m/F(m)$ (equpped with the discrete topology) as m varies.

Let M be the group of diagonals; then $M(\mathbb{Z}[\sqrt{2}])$ is the group of diagonals whose diagonal entries are units in the ring $R = \mathbb{Z}[\sqrt{2}]$; it is an infinite (cyclic) group. $M(R)$ acts by conjugation on the sets $F(m)$ and Γ_m and also on the kernel K, and the inverse limit $K = \lim F(m)\backslash\Gamma_m/F(m)$ is compatible with this $M(R)$ action.

Centrality for the group $SL_2(\mathbb{Z}[\sqrt{2}])$

Consider the exact sequence $1 \to K \to \mathcal{G} \to \overline{G(\mathbb{Q})} \to 1$, where $\mathcal{G}$ is the completion of $G(\mathbb{Q})$ with respect to the "$F(m)$" completion, and $\overline{G(\mathbb{Q})}$ is the congruence completion. (By general considerations), the group K is the inverse limit of the *sets* $K_m = F(m)\backslash\Gamma_m/F(m)$ (equpped with the discrete topology) as m varies.

Let M be the group of diagonals; then $M(\mathbb{Z}[\sqrt{2}])$ is the group of diagonals whose diagonal entries are units in the ring $R = \mathbb{Z}[\sqrt{2}]$; it is an infinite (cyclic) group. $M(R)$ acts by conjugation on the sets $F(m)$ and Γ_m and also on the kernel K, and the inverse limit $K = \lim F(m)\backslash\Gamma_m/F(m)$ is compatible with this $M(R)$ action.

If we prove that there is a fixed infinite (finite index) subgroup D of $M(R)$ which acts trivially on each K_m as m varies, then it acts trivially on K; but all of $G(\mathbb{Q})$ acts on K and the simplicity of $G(\mathbb{Q})$ then implies that $G(\mathbb{Q})$ acts trivially on K; hence K is central.

SL_2 continued

Suppose that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of Γ_m viewed as an element of the double coset $F(m)\backslash\Gamma_m/F(m)$, and let $s = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \in M(R)$.

In his proof of centrality of the congruence subgroup kernel for SL_2 (when the number field K has infinitely many units), Serre makes the following computation:

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (u^{-2}-1)\frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & (u^2-1)\frac{b}{a} \\ 0 & 1 \end{pmatrix}.$$

If $u \equiv 1 \pmod{a}$, then this says that ${}^s(g) = u^- g u^+$ where $u^{\pm}$ are lower and upper triangular matrices in $E(m)$. Hence ${}^t(g) = g$ in the double coset $F(m)\Gamma_m F(m)$, and thus the congruence subgroup $M(a)$ of level a fixes the element g in the double coset.

We may replace g by $g' = g\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ for some $x \equiv 0 \pmod m$ without altering the coset $F(m)gF(m)$. But $g' = \begin{pmatrix} a+bx & b \\ c+dx & d \end{pmatrix}$ which shows that the group $M(a+bx)$ also fixes the double coset through g. Hence the group $M_{a,b,m}$ *generated* by the collection $\{M(a+bx)\}_{x\equiv 0 \pmod m}$ fixes the double coset.

Proposition 1

(Serre) There exists a subgroup D of finite index in $M(\mathbb{Z})$ such that for any a, b, m as above, the group D is contained in the group $M_{a,b,m}$.

The proof uses the Artin reciprocity law for the field $\mathbb{Q}(\sqrt{2})$. Thus, this group Δ fixes every element (double coset) in $F(m)\backslash\Gamma_m/F(m)$ and hence acts trivially on the inverse limit K of these double coset spaces.

Centrality in the general case

The proof in the general case is similar. Recall: P is a maximal parabolic $\mathbb{Q}$-subgroup with $G \supset P = UM$ and $P^- = U^- M$. We then prove

Proposition 2

For any linear algebraic $\mathbb{Q}$-group M, and a fixed integer N, there exists a subgroup $\Delta \subset M(\mathbb{Z})$ of finite index such that for every $a, b \in \mathbb{Z}$ coprime, and every integer m coprime to a, the group generated by the collection $\{M(a + bmx)^N : x \in \mathbb{Z}\}$ contains Δ.

The proof is a consequence of Dirichlet's theorem on the infinitude of primes in arithmetic progression.

In the case of a diagonal torus, the result of Serre would follow from the

Lemma 4

Let ϕ be the Euler totient function, and let a, b be coprime integers. Then the g.c.d.

$$g.c.d.\{\phi(a+bx) : x = 0, 1, 2, \cdots\},$$

is bounded by a constant independent of a, b: this g.c.d. divides 16.

This can be proved by using the Dirichlet theorem on primes in arithmetic progression. Analogously, one can ask:

Question 1

Let n be a positive integer. Let $\mathcal{P}_n$ denote the set of polynomials of degree n, whose coefficients have content one. Does there exist a constant $C = C(n)$ such that

$$g.c.d\{\phi(P(x)) : x \in \mathbb{Z}, P \in \mathcal{P}_n\} \leq C?$$

When $n = 2$, the answer is yes, by a recent result of Sounderarajan. He also shows that the result is true in general if one assumes a well known conjecture (Schinzel's conjecture) that if $f \in \mathbb{Z}[X]$ is an irreducible polynomial with content one, then there are infinitely many integers x such that $f(x)$ is prime.

When $n = 2$, the answer is yes, by a recent result of Sounderarajan. He also shows that the result is true in general if one assumes a well known conjecture (Schinzel's conjecture) that if $f \in \mathbb{Z}[X]$ is an irreducible polynomial with content one, then there are infinitely many integers x such that $f(x)$ is prime.

THANK YOU