THE CONGRUENCE SUBGROUP PROPERTY AND BOUNDED GENERATION

DAVE WITTE MORRIS

Lecture II. Proof that $\mathrm{SL}(3,\mathbb{Z})$ has the Congruence Subgroup Property

Recall. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a ring homomorphism, so

$$\varphi_n \colon \mathrm{SL}(3,\mathbb{Z}) \to \mathrm{SL}(3,\mathbb{Z}/n\mathbb{Z})$$

is a group homomorphism to a finite group. So

$$\Gamma_n := \ker \varphi_n$$

is a (normal) subgroup of finite index in $\Gamma = \mathrm{SL}(3,\mathbb{Z})$.

Definition.

- Γ_n is a *principal congruence subgroup* of Γ.
- Subgroups containing Γ_n are *congruence subgroups* of Γ.

These are the obvious subgroups of finite index in Γ.

Theorem (Bass-Lazard-Serre (1964), Mennicke (1965))**.** *Every finite-index subgroup of* $\mathrm{SL}(3,\mathbb{Z})$ *is a congruence subgroup.*

For short, we say $\mathrm{SL}(3,\mathbb{Z})$ has the *Congruence Subgroup Property* ("CSP").

The remainder of this lecture is a proof of the theorem.

1. Elementary generators

Let H be a subgroup of finite index in Γ. We wish to show H contains some Γ_n.

Lemma. *We may assume $H \triangleleft \Gamma$.*

Proof. H contains a normal subgroup N of Γ, with $|\Gamma : N| < \infty$. $\square$

Notation.

- $e_{1,2}(n) = \begin{bmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ "elementary matrix"
- E_n = smallest *normal* subgroup of Γ that contains $e_{1,2}(n)$ (so $e_{i,j}(n) \in E_n$ whenever $i \neq j$).

Lemma. *It suffices to show $E_n = \Gamma_n$.*

I.e., we wish to show $\Gamma_n/E_n = \{1\}$.

2. Mennicke symbols

Key Lemma (Stable range SR_2)**.** $\begin{bmatrix} \mathrm{SL}(2,\mathbb{Z})_n & & 0 \\ & & 0 \\ 0 & 0 & 1 \end{bmatrix} \twoheadrightarrow \dfrac{\Gamma_n}{E_n}$.

I.e., $g \in \Gamma_n \implies \exists x, y \in E_n,\ xgy \in \begin{bmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix}$;

row and column operations reduce g to 2×2.

Proof. Note:

$\gcd(k,\ell,m) = 1 \Rightarrow \exists \ell' \equiv \ell \pmod{nk},\ \gcd(\ell',m) = 1.$

$$\begin{bmatrix} * & * & * \\ * & * & * \\ k & \ell & m \end{bmatrix} \rightsquigarrow \begin{bmatrix} * & * & * \\ * & * & * \\ k & \ell' & m \end{bmatrix} \rightsquigarrow \begin{bmatrix} * & * & * \\ * & * & * \\ n & \ell' & m \end{bmatrix}$$

$$\overset{e}{\rightsquigarrow} \begin{bmatrix} * & * & * \\ * & * & * \\ n & \ell' & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{bmatrix} \overset{e^{-1}}{\rightsquigarrow} \begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{bmatrix}$$

$$\rightsquigarrow \begin{bmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix}. \qquad \square$$

Let $W = W_n(\mathbb{Z}) = \left\{ (a,b) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{c} a,b \text{ rel prime} \\ a \equiv 1 \pmod{n} \\ b \equiv 0 \pmod{n} \end{array} \right\}$

$= \{\text{ 1st rows of elements of } \mathrm{SL}(2,\mathbb{Z})\ \}_n.$

Define $\begin{bmatrix} \ \end{bmatrix} : W \to \Gamma_n/E_n$ by $\begin{bmatrix} b \\ a \end{bmatrix} \equiv \begin{bmatrix} a & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

We wish to show $\begin{bmatrix} b \\ a \end{bmatrix} = 1$.

Axioms.

- $\begin{bmatrix} \ \end{bmatrix}$ *is well def'd* (*easy*) *and onto* (*"stable range"*).
- (MS1) $\begin{bmatrix} b + t_1 a \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b \\ a + t_2 b \end{bmatrix}$.
  ($t_1 \in n\mathbb{Z},\ t_2 \in \mathbb{Z}$)
- (MS2a) $\begin{bmatrix} b_1 \\ a \end{bmatrix} \begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1 b_2 \\ a \end{bmatrix}$ (*we are in* SL_3*!*).

Lemma. Γ *acts on* Γ_n/E_n *by conjugation* (*since* $\Gamma_n, E_n \triangleleft \Gamma$). *This action is trivial* (*since* $\Gamma = E_1$).

Proof. We wish to show Γ_1 is trivial on Γ_n/E_n;

equivalently, Γ_n is trivial on Γ_1/E_n.

Let e be a generator of Γ_1; may assume $e = e_{1,3}(1)$.

Let $g \in \Gamma_n$; may assume $g \in \mathrm{SL}(2,\mathbb{Z})_n$.

Then

$$g^{-1} e g \in \begin{bmatrix} 1 & & n\mathbb{Z} \\ & 1 & n\mathbb{Z} \\ & & 1 \end{bmatrix} \subset E_n. \qquad \square$$

Date: Geometric Literacy Seminar, University of Chicago, May 2008.

Proof of MS2a. Since $\begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}^{\pm 1} \in E_1$ **(verify!!)**, we have

$$\begin{aligned}
\begin{bmatrix} b' \\ a \end{bmatrix} &= \begin{bmatrix} a & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
&\equiv \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix} \\
&= \begin{bmatrix} d' & 0 & -c' \\ 0 & 1 & 0 \\ -b' & 0 & a \end{bmatrix}.
\end{aligned}$$

Therefore

$$\begin{aligned}
\begin{bmatrix} b \\ a \end{bmatrix} \begin{bmatrix} b' \\ a \end{bmatrix} &\equiv \begin{bmatrix} a & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} d' & 0 & -c' \\ 0 & 1 & 0 \\ -b' & 0 & a \end{bmatrix} \\
&= \begin{bmatrix} ad' & b & -ac' \\ * & * & * \\ -b' & 0 & a \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & b & 0 \\ * & * & * \\ -b' & 0 & a \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & b & 0 \\ 0 & * & * \\ 0 & bb' & a \end{bmatrix} \\
&\rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & bb' & a \end{bmatrix} \rightsquigarrow \begin{bmatrix} a & bb' & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} bb' \\ a \end{bmatrix}.
\end{aligned}$$

□

3. Mennicke symbols are trivial

Proposition. $\begin{bmatrix} b \\ a \end{bmatrix} = 1$.

Lemma. $b \equiv \pm 1 \pmod a \implies \begin{bmatrix} b \\ a \end{bmatrix} = 1$.

Proof.

$$\begin{aligned}
\begin{bmatrix} b \\ a \end{bmatrix} &= \begin{bmatrix} b - ba \\ a \end{bmatrix} = \begin{bmatrix} b(1-a) \\ a \end{bmatrix} = \begin{bmatrix} (\pm 1 + ka)(1-a) \\ a \end{bmatrix} \\
&= \begin{bmatrix} \pm(1-a) + k(1-a)a \\ a \end{bmatrix} = \begin{bmatrix} \pm(1-a) \\ a \end{bmatrix} \\
&= \begin{bmatrix} \pm(1-a) \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1.
\end{aligned}$$

□

Remark. For Mennicke symbols over a general commutative ring R, the argument shows that if $b \equiv u \pmod a$, and u is a unit in R, then $\begin{bmatrix} b \\ a \end{bmatrix} = 1$.

Corollary. $\begin{bmatrix} b \\ a \end{bmatrix}^{\phi(a)} = 1$*, where ϕ is the Euler totient function; i.e., $\phi(a)$ is the number of units in the ring $\mathbb{Z}/a\mathbb{Z}$.*

Proof. Since $b^{\phi(a)} \equiv 1 \pmod a$, combining (MS2a) with the lemma implies

$$\begin{bmatrix} b \\ a \end{bmatrix}^{\phi(a)} = \begin{bmatrix} b^{\phi(a)} \\ a \end{bmatrix} = 1.$$

□

Idea of proof of the proposition. We wish to show that no prime p divides the order of the element $\begin{bmatrix} b \\ a \end{bmatrix}$ of Γ_n/E_n. For simplicity, let us assume p is odd, and does not divide n.

Then, since a and b are relatively prime, it is easy to find:

- some $b' \equiv b \pmod{na}$, such that $p \nmid b'$, and
- some $a' \equiv a \pmod{b'}$, such that $p \nmid a' - 1$.

Furthermore, by Dirichlet's Theorem on primes in arithmetic progressions, we may assume a' is prime, so $p \nmid a' - 1 = \phi(a')$. Then we conclude, from the corollary, that

$$p \nmid \text{order of } \begin{bmatrix} b \\ a \end{bmatrix} \text{ in } \Gamma_n/E_n.$$

□

Remark. The above argument assumes that p is odd, but it can easily be modified to show that if n is not divisible by 2, then the order of $\begin{bmatrix} b \\ a \end{bmatrix}$ is not divisible by 2. Simply arrange that $4 \nmid a' - 1$, and conclude that $\begin{bmatrix} b \\ a \end{bmatrix}^{\phi(a')/2} = 1$, by using the fact that $\begin{bmatrix} b \\ a \end{bmatrix} = 1$ when $b \equiv \pm 1 \pmod a$, not just when $b \equiv 1 \pmod a$. The details are left as an exercise.

In the case where $p \mid n$, the proposition can be proved by a similar argument, but with a and b interchanged. This is enabled by the following additional axiom:

Axiom (MS2b). $\begin{bmatrix} b \\ a_1 \end{bmatrix} \begin{bmatrix} b \\ a_2 \end{bmatrix} = \begin{bmatrix} b \\ a_1 a_2 \end{bmatrix}$.

When $n = 1$, (MS2b) follows immediately from (MS2a) and the following interesting observation. The general case is not terribly difficult either (see [1, pp. 312–313]).

Kervaire Reciprocity. *If $n = 1$, then* $\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$.

Proof. $\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b - a \\ a \end{bmatrix} = \begin{bmatrix} b - a \\ b \end{bmatrix} = \begin{bmatrix} -a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$. □

Now, to complete the proof of the proposition (for odd p), use Dirichlet's Theorem to arrange that $b' = nq$, where q is prime, and $q \nmid n$. Then, since $a' \equiv 1 \pmod n$, we have $(a')^{\phi(q)} \equiv 1 \pmod{b'}$.

References

[1] H. Bass: *Algebraic K-Theory.* W. A. Benjamin, Inc., New York, 1968. MR 0249491 (40 #2736)

[2] H. Bass, M. Lazard, J.-P. Serre: Sous-groupes d'indice fini dans $\mathrm{SL}(n, \mathbb{Z})$, *Bull. Amer. Math. Soc.* 70 (1964) 385–392. MR 0161913 (28 #5117)

[3] H. Bass, J. Milnor, J.-P. Serre: Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, *Inst. Hautes Études Sci. Publ. Math.* 33 (1967) 59–137. MR 0244257 (39 #5574)

[4] J. L. Mennicke: Finite factor groups of the unimodular group. *Ann. of Math.* (2) 81 (1965) 31–37. MR 0171856 (30 #2083)

[5] J.-P. Serre: Le problème des groupes de congruence pour SL2, *Ann. of Math.* (2) 92 (1970) 489–527. MR 0272790 (42 #7671)

[6] B. Sury: *The Congruence Subgroup Problem. An elementary approach aimed at applications.* Hindustan Book Agency, New Delhi, 2003. ISBN 81-85931-38-0, MR 1978430 (2005g:20082)