Murty@GSS: Bounded generation, congruence subgroups and the splitting of primes

January-19-12
1:03 PM

G: Finitely generated (abstract) group.

$g_1 \cdots g_m$ generators.

We say that G has "bounded generation" (BG) if there are $g_1 \ldots g_m \in G$ s.t.

$G = \langle g_1 \rangle \cdots \langle g_m \rangle$; that is

$$G = \{ g_1^{a_1} \cdots g_m^{a_m} \}$$

Note: the g_i's need not be distinct.

<u>Examples</u> 1. If G is Abelian, FG $\Leftrightarrow$ BG.

2. A free group is FG but not BG.

If G is BG & $[G:H] < \infty$, then H is BG.

Hence

Exercise: a finite-index subgroup of a F.G. group is F.G.

3. $G = SL_2(\mathbb{Z})$ is not BG, as it has a finite-index free subgroup $\Gamma(2)$:

$$\Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = g \in SL_2(\mathbb{Z}) : g \equiv I \bmod 2 \right\}$$

freely generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{``=x"}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{=y}$

Digression on $\Gamma(2)$:

$\Gamma(2) \ni M = x^{a_1} y^{b_1} \cdots\cdots x^{a_m} y^{b_m}$

Define

$$\ell_x(M) = \sum a_i$$

$$\ker\left(\Gamma(2) \xrightarrow{\ell_x} \mathbb{Z} \longrightarrow \mathbb{Z}/r\right) =: \Gamma(2)_r$$

a "non-congruence subgroup", does not contain any "congruence" subgroup.

~~ Somehow related to the Fermat curve.

K: Alg. number field - a finite deg ext. of $\mathbb{Q}$.

S: a finite set of primes in K.

$$\mathcal{O}_S = \{x \in K : \mathrm{ord}_v(x) \geq 0,\ v \notin S\}$$

$$G = SL_n(\mathcal{O}_S)$$

joint w/ D. Loukanidis: If S is sufficiently large the G is BG.

$$|S| \geq \max(5, 2[K:\mathbb{Q}] - 3)$$

"Degree of bounded generation" $\leq d$ if there is a set of "bounded" generators with d elements.

Remarks 1. Estimates of the dBG in the above example depend on $[K:\mathbb{Q}]$ alone.

2. Cooke & Weinberger (1975): $n=2$, $|S|\geq 2$ then assuming RH, $SL_2(\mathcal{O}_S)$ is BG.

1:35

To establish BG, use "elementary matrices":

$t\in\mathcal{O}_S$ $\quad X = I + tE_{ij}$

Thm If $|S|$ is large, $n\geq 2$, $K/\mathbb{Q}$ Galois, then any matrix in $SL_n(\mathcal{O}_S)$ can be written as a product of $\leq \frac{1}{2}n(3n-1)+2$ elementary matrices.

(This implies BG because $\mathcal{O}_S$ is Abelian & f.g., at least when $\mathcal{O}_S = \mathcal{O}_K$)

1:44

G FG, $[G:H]<\infty$, is H F.G. ?

$$h = a_1 a_2 a_3 \ldots a_n \qquad a_i \in G$$

$$= a_1 g_{a_1}^{-1} g_{a_1} a_2 g_{a_1 a_2}^{-1} g_{a_1 a_2} a_3 \ldots$$

So H is generated by $g_x a_i g_y^{-1}$

where the g_y are representatives of classes in G/H.
