Counting Subgroups
of
Finite Index

Alex Suciu

Graduate Student Seminar

Mathematics Department

Northeastern University

May 15, 2000

The subject was initiated by Marshall Hall (*Counting subgroups of finite index in free groups*, 1949).

Definition. If G is a finitely-generated group, and n is a positive integer, let:

$$\boxed{a_n(G) = \text{number of index } n \text{ subgroups of } G.}$$

Write also: $s_n(G) = a_1(G) + \cdots + a_n(G)$.

Other numbers that come up:

- $a_n^{\triangleleft}(G)$=number of index n normal subgroups of G;
- $c_n(G)$ = number of conjugacy classes of index n subgroups of G;
- $h_n(G) = |\operatorname{Hom}(G, S_n)|$ = number of representations of G to the symmetric group;
- $t_n(G)$ = number of transitive representations of G to S_n.

If $H \leq G$ and $[G : H] = n$, we may identify $G/H \cong [n] = \{1, \ldots, n\}$, with $H \leftrightarrow 1$. There are $(n-1)!$ ways to do this identification.
G acts transitively on $[n]$, with $\mathrm{Stab}(1) = H$.
Conversely, a transitive rep. $\rho : G \to S_n$ defines an index n subgroup $H = \mathrm{Stab}_\rho(1)$. Thus:

$$a_n(G) = \frac{t_n(G)}{(n-1)!}$$

We also have:

$$h_n(G) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G) h_{n-k}(G)$$

since the orbit of 1 can have size k (with $1 \leq k \leq n$), and there are

- $\binom{n-1}{k-1}$ ways to choose the orbit of 1
- $t_k(G)$ ways to act on this orbit
- $h_{n-k}(G)$ ways to act on its complement

The two previous formulas yield:

$$a_n(G) = \frac{1}{(n-1)!}\, h_n(G) - \sum_{k=1}^{n-1} \frac{1}{(n-k)!}\, h_{n-l}(G)\, a_k(G)$$

Example (Hall)**.** Let F_r be the free group of rank r. Clearly, $h_n(F_r) = (n!)^r$. Thus:

$$a_n(F_r) = n(n!)^{r-1} - \sum_{k=1}^{n-1} ((n-k)!)^{r-1} a_k(F_r)$$

$r \backslash n$	1	2	3	4	5
2	1	3	13	71	461
3	1	7	97	2,143	68,641
4	1	15	625	54,335	8,563,601
5	1	31	3,841	1,321,471	1,035,045,121
6	1	63	23,233	31,817,471	124,374,986,561
7	1	127	139,777	764,217,343	14,928,949,808,641

Asymptotically (Newman),

$$\boxed{a_n(F_r) \sim n \cdot (n!)^{r-1}.}$$

That's because the number of *non-transitive* reps $F_r \to S_n$ is bounded by

$$P = \sum_{k=1}^{n-1} \tbinom{n-1}{k-1} h_k(F_r) h_{n-k}(F_r) = \sum_{k=1}^{n-1} \tbinom{n-1}{k-1} (k!)^r ((n-k)!)^r$$

Clearly, $\lim_{n\to\infty} \dfrac{P}{(n!)^r} = 0$, and so

$$a_n = \frac{t_n}{(n-1)!} \sim \frac{h_n}{(n-1)!} = n(n!)^{r-1}.$$

We also have (Liskovec):

$$\boxed{c_n(F_r) = \tfrac{1}{n} \sum_{k|n} a_k(F_r) \sum_{d|\frac{n}{k}} \mu\left(\tfrac{n}{kd}\right) d^{(r-1)k+1}}$$

Example (Mednykh)**.** Let $G = \pi_1(M^2)$ be the fundamental group of a compact, connected surface. Then:

$$a_n(G) = n \sum_{q=1}^{n} \frac{(-1)^{q+1}}{q} \sum_{\substack{i_1+\cdots+i_q=n \\ i_1,\ldots,i_q \geq 1}} \beta_{i_1} \cdots \beta_{i_q}$$

where $\beta_k = \displaystyle\sum_{\lambda \in \mathrm{Irreps}(S_k)} \left(\frac{k!}{\deg(\lambda)} \right)^{|\chi(M)|}$

Example (Newman)**.** For $G = \mathrm{PSL}(2, \mathbb{Z})$:

$$a_n(G) \sim \left(12\pi e^{\frac{1}{2}}\right)^{-\frac{1}{2}} \exp\left(\tfrac{n \log n}{6} - \tfrac{n}{6} + n^{1/2} + n^{1/3} + \tfrac{\log n}{2}\right)$$

$$a_{100}(G) = 159{,}299{,}552{,}010{,}504{,}751{,}878{,}902{,}805{,}384{,}624$$

Example (Lubotzky)**.** For $G = \mathrm{PSL}(3, \mathbb{Z})$:

$$n^{a \log n} \leq a_n(\mathrm{SL}(3, \mathbb{Z})) \leq n^{b \log^2 n}.$$

Example. Let $\mathbb{Z}^r$ be the free abelian group of rank r. A finite-index subgroup $L < \mathbb{Z}^r$ is also known as a *lattice*.

Theorem (Bushnell-Reiner)**.**

$$a_n(\mathbb{Z}^r) = \sum_{k|n} a_k(\mathbb{Z}^{r-1})(\tfrac{n}{k})^{r-1}, \quad a_n(\mathbb{Z}) = 1$$

$r \backslash n$	1	2	3	4	5	6	7
2	1	3	4	7	6	12	8
3	1	7	13	35	31	91	57
4	1	15	40	155	156	600	400
5	1	31	121	651	781	3,751	2,801
6	1	63	364	2,667	3,906	22,932	19,608
7	1	127	1,093	10,795	19,531	138,811	137,257
8	1	255	3,280	43,435	97,656	836,400	960,800
9	1	511	9,841	174,251	488,281	5,028,751	6,725,601

We get:

- $a_n(\mathbb{Z}^2) = \sigma(n)$, the sum of the divisors of n.
- $a_p(\mathbb{Z}^r) = \frac{p^r-1}{p-1}$, for prime p.
- $a_n(\mathbb{Z}^r) \leq n^{r+1}$.

Proof (due to Lind). Every lattice in $\mathbb{Z}^r$ has a unique representation as the row space of an $r \times r$ integral matrix in Hermite normal:

$$A = \begin{pmatrix} d_1 & b_{12} & b_{13} & \cdots & b_{1r} \\ 0 & d_2 & b_{23} & \cdots & b_{2r} \\ 0 & 0 & d_3 & \cdots & b_{3r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_r \end{pmatrix},$$

where $d_i \geq 1$ for $1 \leq i \leq r$,
and $0 \leq b_{ij} \leq d_j - 1$ for $1 \leq i < j$.

Let L be a lattice of index n. Then:

$$n = d_1 d_2 \cdots d_r.$$

Let $k = d_r$. Each of $b_{r1}, \ldots, b_{r,r-1}$ can assume the values $0, 1, \ldots, k-1$, giving k^{r-1} choices for the last column. There are $a_{n/k}(\mathbb{Z}^{r-1})$ choices for the rest of the matrix. Summing over all the divisors k of n gives the formula. $\square$

Definition. The zeta function of a finitely-generated group G is the Dirichlet series with coefficients $a_n(G)$:

$$\boxed{\zeta_G(s) := \sum_{n=1}^{\infty} a_n(G) n^{-s}}$$

In other words, $\zeta_G(s) = \sum_{H \leq G} [G : H]^{-s}$.

Example (Bushnell and Reiner)**.**

$$\zeta_{\mathbb{Z}^r}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-n+1),$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is Riemann's zeta function. The formula follows from the above formula for $a_n(\mathbb{Z}^r)$, together with properties of Dirichlet series. It yields:

$$s_n(\mathbb{Z}^2) \sim \tfrac{\pi^2}{12}\, n^2$$

A far-reaching generalization to nilpotent groups was given by Grunewald, Segal, and Smith in 1988, sparking much research.

Example (Geoff Smith)**.** Let G be the Heisenberg group

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

Then:

$$\zeta_G(s) = \frac{\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)}{\zeta(3s-3)},$$

and

$$s_n(G) \sim \frac{\zeta(2)^2}{2\zeta(3)}\, n^2 \log n.$$

Theorem (GSS)**.** *Let G be a finitely-generated, nilpotent group. Then:*

1. *$a_n(G)$ grows polynomially, and so*
$$\alpha(G) := \limsup \frac{\log s_n(G)}{\log n} < \infty$$
2. *$\zeta_G(s)$ is convergent for* $\mathrm{Re}(s) > \alpha(G)$.
3. *Euler factorization:*
$$\zeta_G(s) = \prod_{p \text{ prime}} \zeta_{G,p}(s),$$
where $\zeta_{G,p}(s) = \sum_{k=1}^{\infty} a_{p^k}(G) p^{-ks}$.
4. *$\zeta_{G,p}(s)$ is a rational function of p^{-s}, $\forall p$.*

Theorem (duSautoy & Grunewald)**.**

1. *$\alpha(G)$ is* rational, *and*
$$s_n(G) \sim c \cdot n^{\alpha(G)} (\log n)^b.$$
for some $b \in \mathbb{Z}_{\geq 0}$, and $c \in \mathbb{R}$.
2. *$\zeta_G(s)$ can be meromorphically continued to* $\mathrm{Re}(s) > \alpha(G) - \delta$, *for some $\delta > 0$.*

Theorem (duSautoy, McDermott, Smith). *Let G be a finite extension of a free abelian group of finite rank. Then $\zeta_G(s)$ can be extended to a meromorphic function on the whole complex plane.*

Example. Let $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$ be the infinite dihedral group. Then:

$$\zeta_G(s) = 2^{-s}\zeta(s) + \zeta(s-1).$$

Definition. Two groups G and H are called *isospectral* if $\zeta_G(s) = \zeta_H(s)$.

Example. Let $G = \mathbb{Z}^2$, and $H = \pi_1(K^2) = \langle x, y \mid yxy^{-1} = x^{-1} \rangle$. Then G and H are isospectral, although they have non-isomorphic lattices of subgroups of finite index.

More generally, the oriented and unoriented surface groups of same genus are isospectral, by Mednykh's result.

Question. Do there exist isospectral groups G and H, with $G \ncong H$ but $G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$?

Proposition. *Let G be a finitely-generated group, with $G^{\mathrm{ab}} = \mathbb{Z}^r$. For each prime p,*

$$a_p^{\triangleleft}(G) = \tfrac{p^r-1}{p-1},$$
$$c_p(G) = \tfrac{p^r+a_p(G)-1}{p}.$$

Proof. Every index p, normal subgroup of G is the kernel of an epimorphism $\lambda : G \to \mathbb{Z}_p$, and two epimorphisms λ and λ' have the same kernel if and only if $\lambda = q \cdot \lambda'$, for some $q \in \mathbb{Z}_p^*$. Thus, $a_p^{\triangleleft}(G) = |\,\mathbb{P}(\mathbb{Z}_p^r)|$, and the first formula follows. The second formula follows from the fact that $a_p = pc_p - (p-1)a_p^{\triangleleft}$. □

Remark. For every finitely-generated group G, the following formula of Stanley holds:

$$a_n(G \times \mathbb{Z}) = \sum_{d|n} dc_n(G).$$

Hence, if $G^{\mathrm{ab}} = \mathbb{Z}^r$, and p is prime, we have:

$$a_p(G \times \mathbb{Z}) = pc_p(G) + 1 = a_p(G) + p^r.$$

Theorem (Matei-S.). *Let G be a finitely-presented group, with $G^{\mathrm{ab}} = \mathbb{Z}^r$. Then:*

$$a_2(G) = 2^r - 1,$$

$$a_3(G) = \sum_{\rho \in \mathrm{Hom}(G,\mathbb{Z}_3^*)} \frac{3^{d_{\mathbb{Z}_3}(\rho)+1}}{2} - 3 \cdot 2^{r-1} + 1.$$

where $d_{\mathbb{Z}_3}(\rho) = \max\{d \mid \rho \in V_d(G,\mathbb{Z}_3)\}$ is the depth of ρ with respect to the stratification of the character torus $\mathrm{Hom}(G,\mathbb{Z}_3^*) \cong (\mathbb{Z}_3^*)^r$ by the characteristic varieties.

For example, $a_3(F_r) = 3(3^{r-1} - 1)2^{r-1} + 1$, which agrees with M. Hall's computation.

For orientable surface groups, we get

$$a_3(\pi_1(\Sigma_g)) = (3^{2g-1} - 3)(2^{2g-1} + 1) + 4,$$

which agrees with Mednykh's computation.

Let $G = \langle x_1, \dots, x_\ell \mid s_1, \dots, s_m \rangle$ be a f.p. group. Assume $H_1(G) \cong \mathbb{Z}^r$ (with basis $t_1, \dots, t_r$).

Let $\mathbb{K}$ be a field.

Character variety: $\operatorname{Hom}(G, \mathbb{K}^*) \cong (\mathbb{K}^*)^r$ (algebraic torus, with coordinate ring $\mathbb{K}[t_1^{\pm 1}, \dots, t_r^{\pm 1}]$).

Characteristic varieties of G (over $\mathbb{K}$):

$$V_d(G, \mathbb{K}) = \{\mathbf{t} \in \operatorname{Hom}(G, \mathbb{K}^*) \mid \dim_{\mathbb{K}} H^1(G, \mathbb{K}_{\mathbf{t}}) \geq d\}$$

where $\mathbb{K}_{\mathbf{t}}$ is the G-module $\mathbb{K}$ with action given by representation $\mathbf{t} : G \to \mathbb{K}^*$.

For $d < n$, we have:

$$V_d(G, \mathbb{K}) = \{\mathbf{t} \in (\mathbb{K}^*)^r \mid \operatorname{rank}_{\mathbb{K}} A_G(\mathbf{t}) < \ell - d\}$$

where $A_G = \left(\frac{\partial s_i}{\partial x_j}\right)^{\mathrm{ab}}$ is the Alexander matrix of G (of size $\ell \times m$).

The varieties $V_d = V_d(G, \mathbb{K})$ form a descending tower, $(\mathbb{K}^*)^r = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_{r-1} \supseteq V_r$, which depends only on the isomorphism type of G, up to a monomial change of basis in $(\mathbb{K}^*)^r$.