MILD PRO-p-GROUPS AND p-EXTENSIONS OF $\mathbb{Q}$

JOHN LABUTE

Let p be a prime $\neq 2$ and let $S = \{q_1, \ldots, q_m\}$ be a set of m rational primes $\equiv 1 \bmod p$. Let $G = G_S(p)$ be the maximal p-extension of $\mathbb{Q}$ unramified outside S. The pro-p-group G has a minimal presentation with m generators and m relations and so by Golod-Shafarevich it is infinite if $m \geq 4$. That was all we knew about this group in this case, except for the fact that the quotients of the derived series were finite, until we showed in [5] that G has cohomological dimension 2 under certain conditions on S. We also showed that under these conditions the ranks of the lower p-central series quotients grow exponentially.

To describe these conditions we introduce the weighted directed graph $\Gamma_S(p)$ whose vertices are the primes in S. We join q_i to q_j if q_i is not a p-th power mod q_j in which case we attach a weight ℓ_{ij} to the edge q_iq_j. To define this weight we chose a primitive root g_i for each prime q_i. Then ℓ_{ij} is the unique image in $\mathbb{Z}/p\mathbb{Z}$ of any integer r satisfying

$$q_i \equiv g_j^{-r} \bmod q_j.$$

Using the Čebotarev density theorem, one can show that, for any given finite directed graph Γ, there is a set of primes S as above with $\Gamma_S(p) \cong \Gamma$ as directed graphs.

We call $\Gamma_S(p)$ a **non-singular circuit** if the the following conditions hold:

(a) There is an ordering $q_1, \ldots, q_m$ of the vertices of Γ such that $q_1q_2 \cdots q_mq_1$ is a circuit.
(b) We have $\ell_{ij} = 0$ if i, j are odd and

$$\Delta(q_1, q_2, \ldots, q_m) = \ell_{12}\ell_{23} \cdots \ell_{m-1,m}\ell_{m1} - \ell_{1m}\ell_{21}\ell_{32} \cdots \ell_{m,m-1} \neq 0.$$

In this case we also call $q_1q_2 \cdots q_m$ a circular sequence of primes. If $S = \{7, 19, 61, 163\}$ then $\Gamma_S(3)$ is a non-singular circuit. If $\Gamma_S(p)$ is not a non-singular circuit we can add m primes $\equiv 1 \bmod p$ to make it a non-singular circuit.

Note that if (a) holds then $\Delta(q_1, q_2, \ldots, q_m) \neq 0$ if there is an edge q_iq_j of the circuit $q_1q_2 \cdots q_mq_1$ such that q_jq_i is not an edge of $\Gamma_S(p)$. Also note that (a) and (b) imply that m is even and ≥ 4. Condition (b) is independent of the choice of primitive roots g_j since

$$\Delta(q_1, q_2, \ldots, q_m) \neq 0 \iff \frac{\ell_{1m}}{\ell_{m-1,m}}\frac{\ell_{21}}{\ell_{m1}}\frac{\ell_{32}}{\ell_{12}} \cdots \frac{\ell_{m,m-1}}{\ell_{m-2,m-1}} \neq 1,$$

where each ratio in the product is independent of the choice of primitive roots.

Theorem A If $\Gamma_S(p)$ is a non-singular circuit then $G_S(p)$ is of cohomological dimension 2.

Date: June 15,2006.

We want to thank the organizers for the invitation to participate in this Workshop. It was an extremely enjoyable and profitable stay in a excellent research environment.

Corollary. If $S = \{7, 19, 61, 163\}$ then then $\mathrm{cd}(G_S(3)) = 2$.

To prove this we use the fact that, due to Koch [4], the pro-p-group $G = G_S(p)$ has a presentation $G = F/R$ with F the free pro-p-group on $x_1, \ldots, x_m$ and R the closed normal subgroup generated by $r_1, \ldots, r_m$ with

$$r_i \equiv x_i^{q_i - 1} \prod_{j=1}^{n} [x_i, x_j]^{\ell_{ij}} \bmod F_3,$$

where F_n denotes the n-th term of the lower p-central series of F. The Lie algebra $L = \mathrm{gr}(F)$ associated to the lower p-central series of F is a free Lie algebra over $\mathbb{F}_p[\pi]$, where the action of the indeterminate π is induced by $x \mapsto x^p$. Let ρ_i be the image of r_i in $\mathrm{gr}_2(F)$ and let $\mathfrak{r}$ be the ideal of L generated by $\rho_1, \ldots, \rho_m$. Let $\mathfrak{g} = L/\mathfrak{r}$ and let $U_\mathfrak{g}$ be the enveloping algebra of $\mathfrak{g}$. Then $M = \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}]$ is a $U_\mathfrak{g}$-module via the adjoint representation.

Theorem B. If $\Gamma_S(p)$ is a non-singular circuit then
(a) $\mathfrak{g}$ is a free $\mathbb{F}_p[\pi]$-module,
(b) M is a free $U_\mathfrak{g}$-module on the images of $\rho_1, \ldots, \rho_m$.

We call $\rho_1, \ldots, \rho_m$ **strongly free** if the conditions (a) and (b) of Theorem B hold. In this case we call G **mild**.

Theorem C. If the sequence $r_1, \ldots, r_m$ is strongly free then $\mathrm{gr}(G) = L/\mathfrak{r}$ and $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module.

If $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module, the canonical exact sequence

$$0 \to R/[R, R] \to \mathbb{Z}_p[[G]]^m \to \mathbb{Z}_p[[G]] \to Z_p \to 0$$

together with a result of Brumer [2] shows that the cohomological dimension of G is 2. That $R/[R, R]$ is a free $\mathbb{Z}_p[[G]]$-module is proven by showing that, under the assumption that the sequence $r_1, \ldots, r_m$ is strongly free, the above exact exact sequence lifts the exact sequence

$$0 \to \mathfrak{r}/[\mathfrak{r}, \mathfrak{r}] \to U_\mathfrak{g}^m \to U_\mathfrak{g} \to F_p[\pi] \to 0.$$

If $\overline{L} = L/\pi L$ and $\overline{\rho}_i$ is the image of ρ in $\overline{L}$ then $\rho_1, \ldots, \rho_m$ is a strongly free sequence in L if and only if $\overline{\rho}_1, \ldots, \overline{\rho}_m$ is a strongly free sequence in $\overline{L}$, which can be identified with the free Lie algebra over $\mathbb{F}_p$ on $\xi_1, \ldots, \xi_m$. The sequence $\rho_1, \ldots, \rho_m$ is strongly free if and only if the Poincaré series of the enveloping algebra of $\mathfrak{g}/\pi\mathfrak{g}$ is

$$P(t) = \frac{1}{1 - mt + mt^2}.$$

In this case one can show that the dimension of the n-th homogeneous component of $L/\mathfrak{r}$ is

$$\sum_{k=1}^{n} \frac{1}{k} \sum_{d|k} \mu(k/d)(\alpha^d + \beta^d),$$

where $1 - mt + mt^2 = (1 - \alpha t)(1 - \beta t)$. Note that $\alpha, \beta > 1$ for $m \geq 4$.

The problem of deciding strong freeness is a difficult one. However, in joint work with Michael Bush [3], we have found an algorithm for strong freeness in the case $m = 4$. In fact, we show that $\rho_1, \ldots, \rho_4$ is a strongly free sequence if and only if the dimensions of the first four homogeneous components of $\mathfrak{g}/\pi\mathfrak{g}$ are $4, 2, 4, 6$. For example, if $p = 3$ and $S = \{7, 13, 19, 31\}$, the sequence $\rho_1, \ldots, \rho_4$ is strongly free. The case $m > 4$ is the subject of ongoing research. Alexander Schmidt [6] has extended our results to give criteria on $\Gamma_S(p)$ for the cohomological dimension of $G_S(p)$ to be 2. We don't know whether in these cases $G_S(p)$ is a mild group.

More generally, a finitely presented pro-p-group G is said to be **mild** if it has a minimal presentation $G = F/R =< x_1, \ldots, x_d \mid r_1, \ldots, r_m >$ where the initial forms of the relators r_i with respect to the lower p-central series form a strongly free sequence; if h_i is largest with $r_i \in F_{h_i}$ then the initial form ρ_i of r_i is the image of r_i in $\mathrm{gr}_{h_i}(F)$.

Theorem C is true in this general context even if $p = 2$ if we assume $r_i \in F^4[F, F]$ for all i. Moreover, the sequence $r_1, \ldots, r_m$ is strongly free if and only if the Poincaré series of the enveloping algebra of $\mathfrak{g}/\pi\mathfrak{g}$ is

$$\frac{1}{1 - dt + t^{h_1} + \cdots + t^{h_m}}.$$

In this case, if $1 - dt + t^{h_1} + \cdots + t^{h_m} = (1 - \alpha_1 t) \cdots (1 - \alpha_m)$ then

$$\dim \mathrm{gr}_n(G) = \sum_{k=1}^{n} \frac{1}{k} \sum_{d|k} \mu(k/d)(\alpha_1^d + \cdots + \alpha_m^d).$$

If $h_i = h$ for all i then strong freeness implies $m < d^h/(h-1)e$. If $h = 2$ we can find strongly free sequences $r_1, \ldots, r_m$ with $1 \leq m \leq t(d)$ where $t(d) = d^2/4$ if d is even and $t(d) = (d-1)^2/4$ is d is odd; we conjecture that $t(d)$ is largest possible.

We call a pro-p-group G **tame** if it is mild and has the property **FAB**: every subgroup of G finite index has a finite abelianization. In this case, $m \geq d$. Infinite tame groups lie strictly between the class of free pro-p-groups and p-adic analytic groups but have properties in common with each of these classes. It would be interesting to have a classification of infinite tame groups in view of their relevance to the Fontaine-Mazur Conjecture, cf [1]. It is our belief that infinite tame groups appear often as Galois groups of maximal p-extensions of number fields with restricted tame ramification. See for example the recent work of Vogel [7] in the case of imaginary quadratic number fields.

References

[1] N. Boston, *Reducing the Fontaine-Mazur Conjecture to Group Theory*, (preprint).
[2] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra 4, 442-470 (1966).
[3] M. Bush, J. Labute. *Mild pro-p-groups with* 4 *generators*, (preprint).
[4] H. Koch, *Galois Theory of p-Extensions*, Springer Verlag, 2002.
[5] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, (to appear in J. Reine Angew. Math.)

[6] A. Schmidt, Circular sets of prime numbers and p-extensions of the rationals, (to appear in J. Reine Angew. Math.)
[7] D. Vogel, *Circular sets of primes of imaginary quadratic number fields*, (preprint).

Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal QC H3A 2K6, Canada
E-mail address: labute@math.mcgill.ca