Math 8851. Homework #7. To be completed by 5pm on Fri, Dec 1

We will start by discussing how the Golod-Shafarevich criterion for pro-p groups follows from the corresponding result for algebras. This reduction was discussed in class at the end of Lecture 24, but things got rushed at the end, and I had to omit some details.

First we fix some notations. Let K be a field, $U = \{u_1, \ldots, u_d\}$ a finite set and $K\langle\langle U\rangle\rangle$ the algebra of power series over K in non-commuting variables $u_1, \ldots, u_d$. Given $0 \neq f \in K$, we define $\deg(f)$ to be the smallest degree of a monomial in U which appears in the expansion of f with nonzero coefficient. We also set $\deg(0) = \infty$. For each $n \in \mathbb{Z}_{\geq 0}$ let

$$K\langle\langle U\rangle\rangle_n = \{f \in K\langle\langle U\rangle\rangle : \deg(f) \geq n\}.$$

Note that $K\langle\langle U\rangle\rangle_n$ is an ideal of $K\langle\langle U\rangle\rangle$.

Now let R be a subset of $K\langle\langle U\rangle\rangle$ with $0 \notin R$. Let $I = ((R))$ be the closed ideal of $K\langle\langle U\rangle\rangle$ generated by R and $A = K\langle\langle U\rangle\rangle/I$, so we can think of elements of U as generators and elements of R as relators. Let $R_n = \{r \in R : \deg(r) = n\}$, so $R = \sqcup_{n=0}^{\infty} R_n$. As discussed in class, we can assume that $R_0 = \emptyset$ (otherwise $A = 0$) and each R_n is finite (this takes a bit of work to justify).

Let $r_n = |R_n|$ and $H_R(t) = \sum\limits_{n=0}^{\infty} r_n t^n \in \mathbb{Z}[[t]]$ the associated Hilbert series. Let $\pi : K\langle\langle U\rangle\rangle \to A$ be the natural projection, $A_n = \pi(K\langle\langle U\rangle\rangle_n)$, $a_n = \dim_K(A_n/A_{n+1})$ and $H_A(t) = \sum\limits_{n=0}^{\infty} a_n t^n$.

Theorem 1 (Golod-Shafarevich inequality for filtered algebras)**.** *In the above notations we have the following inequality of power series:*

$$\frac{H_A(t)(1 - |U|t + H_R(t))}{1-t} \geq \frac{1}{1-t} \qquad (***)$$

Recall that the inequality in (***) means that in each degree the coefficient of the power series on the left-hand side is $\geq$ the respective coefficient on the right-hand side.

Corollary 2. *Suppose there exists $\tau \in (0,1)$ such that $1 - |U|\tau + H_R(\tau) \leq 0$. Then the numerical series $H_A(\tau)$ diverges, so in particular A is infinite-dimensional.*

Suppose now that G is a pro-p group given by a pro-p presentation $\langle X|R_G\rangle$ where $X = \{x_1, \ldots, x_d\}$ is finite (the set of relators R_G may be infinite). Thus, G is isomorphic to F/N where $F = F_{\widehat{p}}(X)$ is the free pro-p group on X and $N = \langle\langle R_G\rangle\rangle$ is the closed normal subgroup generated by R_G.

As above let $U = \{u_1, \ldots, u_d\}$ and consider the subgroup Γ of $\mathbb{F}_p\langle\langle U\rangle\rangle^\times$ given by

$$\Gamma = \overline{\langle 1+u_1, \ldots, 1+u_d\rangle},$$

the closed subgroup generated by $1+u_1, \ldots, 1+u_d$. As shown in Lecture 12, Γ is isomorphic to F via the map $x_i \mapsto 1+u_i$ for $1 \le i \le d$. From now on we will identify Γ with F using this map.

Next let $R_A = \{r-1 : r \in R_G\}$ (viewed as a subset of $\mathbb{F}_p\langle\langle U\rangle\rangle$), $I = ((R_A))$ the closed ideal of $\mathbb{F}_p\langle\langle U\rangle\rangle$ and $A = \mathbb{F}_p\langle\langle U\rangle\rangle/I$. As explained in Lecture 23, the embedding $\Gamma = F \to \mathbb{F}_p\langle\langle U\rangle\rangle^\times$ induces a natural map $\varphi : G \to A^\times$ such that $Span(\operatorname{Im}\varphi)$ is dense in A, so in particular, G is infinite whenever A is infinite.

Now define the degree function D on the free pro-p group F (still identified with Γ) by

$$D(f) = \deg(f-1).$$

(Note that $D(f) > 0$ for all f since the power series expansion of f always has constant term 1).

Thus, if we set $H_{R_G}(t) = \sum_{i=1}^{\infty} t^{D(r)}$, then $H_{R_G}(t) = H_{R_A}(t)$ as formal power series. Hence Corollary 2 yields the following:

Corollary 3. *Suppose that a pro-p group G has a pro-p presentation $\langle X|R_G\rangle$ with X is finite and there exists $\tau \in (0,1)$ such that $1-|X|\tau + H_{R_G}(\tau) \le 0$. Then G is infinite.*

We are now ready to formulate the first 2 problems.

Problem 1. Prove the following properties of the degree function D on F:

(a) $D(fg) \ge \min(D(f), D(g))$ for all $f, g \in F$;
(b) $D([f,g]) \ge D(f) + D(g)$ for all $f, g \in F$;
(c) $D(f^p) = p \cdot D(f)$ for all $f \in F$.

Problem 2. Prove that $D(f) > 1 \iff f \in \Phi(F)$. **Hint:** The backwards direction follows from the explicit formula for $\Phi(F)$ and Problem 1. For the forward direction first show that any element of F can be uniquely written as $\prod_{i=1}^{d} x_i^{a_i} \cdot y$ where $0 \le a_i \le p-1$ for each i

and $y \in \Phi(F)$ (here $X = \{x_1, \ldots, x_d\}$ is the chosen free generating set for F, as before).

Let us now recall an important application of Problem 2 briefly discussed at the end of Lecture 24.

As a consequence of Corollary 2 we obtained the following result:

Corollary 4. *Let $A = K\langle\langle U\rangle\rangle/((R))$ for some field K and finite set U and suppose that $r_1 = 0$ (in addition to the original hypothesis that $r_0 = 0$), so all relations in R have degree ≥ 2. If $|U| > 0$ and $|R| \leq \frac{|U|^2}{4}$, then A is infinite-dimensional.*

Now recall that if $\langle X|R_G\rangle$ is a pro-p presentation of a finitely generated pro-p group G such that $|X| = d(G)$, then R_G lies inside $\Phi(F_{\widehat{p}}(X))$, the Frattini subgroup of $F_{\widehat{p}}(X)$ and so $D(r) \geq 2$ for all $r \in R_G$ by Problem 2. Hence the algebra A corresponding to G satisfies the hypotheses of Corollary 4, and we obtain the following group-theoretic counterpart of Corollary 4:

Theorem 5. *Let G be a finitely presented pro-p group and assume that $d(G) > 0$ (that is, G is non-trivial) and $r(G) \leq \frac{d(G)^2}{4}$. Then G is infinite.*

Recall that we used Theorem 5 to give a negative solution to the class field tower problem.

The next 2 problems deal with powerful pro-p groups. Recall that a pro-p group G is *powerful* if $\overline{[G,G]} \subseteq \overline{G^p}$ for $p > 2$ and if $\overline{[G,G]} \subseteq \overline{G^4}$ for $p = 2$.

More generally, a subgroup N of G is *powerfully embedded in G* (notation N p.e. G) if $\overline{[N,G]} \subseteq \overline{N^p}$ for $p > 2$ and if $\overline{[N,G]} \subseteq \overline{N^4}$ for $p = 2$. Thus, G is powerful $\iff$ G p.e. G.

Note that a subgroup N of G is normal $\iff$ $[N,G] \subseteq N$, so any closed powerfully embedded subgroup is automatically normal.

Problem 3. Given $k, n \in \mathbb{N}$, let

$$GL_n^k(\mathbb{Z}_p) = \{A \in GL_n^k(\mathbb{Z}_p) : A \equiv I \mod p^k\},$$

the k^{th} congruence subgroup of $GL_n(\mathbb{Z}_p)$.

(a) Prove that $[GL_n^k(\mathbb{Z}_p), GL_n^m(\mathbb{Z}_p)] \subseteq SL_n^{k+m}(\mathbb{Z}_p)$ for all $k, m \in \mathbb{N}$; in particular, $[GL_n^k(\mathbb{Z}_p), GL_n^k(\mathbb{Z}_p)] \subseteq SL_n^{2k}(\mathbb{Z}_p)$.

(b) Assume that p is odd. Prove that every $g \in GL_n^2(\mathbb{Z}_p)$ can be written as h^p for some $h \in GL_n^1(\mathbb{Z}_p)$. **Hint:** One way to prove this is as follows. We need to show that for every $A \in Mat_n(\mathbb{Z}_p)$ the equation $(1+pX)^p = 1+p^2A$ has a solution $X \in Mat_n(\mathbb{Z}_p)$. Expand the left-hand side and prove that the equation has a solution mod p^i for all $i \in \mathbb{N}$ by induction on i; then deduce that there is a solution in $Mat_n(\mathbb{Z}_p)$.

(c) Now prove that every $g \in GL_n^4(\mathbb{Z}_2)$ can be written as h^4 for some $h \in GL_n^2(\mathbb{Z}_p)$.

(d) Deduce from (a), (b) and (c) that $GL_n^k(\mathbb{Z}_p)$ is powerful if $p > 2$ (and k is arbitrary) or $p = 2$ and $k \geq 2$.

Remark: The fact that the conclusions of (b) and (c) are seemingly stronger than what is required to be powerful is not a coincidence. We will prove in class that if G is a powerful pro-p group, then every element of G^p is a p^{th} power.

Problem 4. The following result was formulated in Lecture 25:

Lemma 6. *Let G be a pro-p group, N a subgroup of G, and suppose that N p.e. G. Then N^p p.e. G.*

Prove Lemma 6 for odd p using the outline below. Note that Lemma 6 is proved in Chapter 2 of [DDMS] using the same method, but the steps are justified slightly differently there.

(a) Prove that it is sufficient to prove Lemma 6 for finite p-groups.

(b) Assume now that Lemma 6 is false for some pair (G, N) with G finite and choose such pair with $|G|$ smallest possible. Show that we must have $(N^p)^p = \{1\}$.

(c) Let G and N be as in (b). Using the fact that inside a finite p-group, any non-trivial normal subgroup contains a central element of order p, show that $[N^p, G]$ must be central of order p, so in particular $[N^p, G]^p = [N^p, G, G] = \{1\}$ (assume the opposite and reach a contradiction with the assumption that $|G|$ is smallest possible).

(d) Recall the following formula from Lecture 26: for any group Γ and any $x, y \in \Gamma$ we have

$$(xy)^p = x^p y^p [x, y]^{\binom{p}{2}} z \qquad (***)$$

where z lies in the normal subgroup generated by the length 3 commutators $[[x, y], x]$ and $[[x, y], y]$. Use this formula and the equalities $[N^p, G]^p = [N^p, G, G] = \{1\}$ from (c) to deduce that $[N^p, G] = \{1\}$, thus reaching a contradiction. **Hint:** You need to show that $g^{-1}n^p g = n^p$ for all $n \in N$ and $g \in G$. Write $g^{-1}n^p g$ as $(n[n,g])^p$ and apply (***).