Math 8851. Homework #5. To be completed by 5pm on Fri, Nov 3

1. This is an expanded version of Problem 3 in HW#3. The remark after the problem gives a corrected statement of Problem 7 in HW#3.

Let X be an infinite set, $F(X)$ the free abstract group on X and Λ the set of all open normal subgroups N in $F(X)$ such that N *contains all but finitely many elements* of X. The group $\widehat{F(X)}_\Lambda$ (the completion of $F(X)$ with respect to Λ) is called the free profinite group on X. It will be denoted by $\widehat{F}(X)$.

(a) Prove that $|\Lambda| = |X|$. Deduce from HW#2 that the set of open subgroups of $\widehat{F}(X)$ has the same cardinality as X. In particular, if X is countable, $\widehat{F}(X)$ is countably based. **Note:** You may use without proof that $|X \times X| = |X|$ for any infinite set X.

(b) Let H be a profinite group. A map $f : X \to H$ is called *1-convergent* if any open subgroup U of H contains $f(x)$ for all but finitely many $x \in X$. Prove that the free profinite group $\widehat{F}(X)$ satisfies the following universal property: If H is a pro-p group and $f : X \to H$ is any 1-convergent map, then there exists a unique continuous homomorphism $f_* : \widehat{F}(X) \to H$ such that $f_* \circ \iota = f$ where $\iota : X \to \widehat{F}(X)$ is the canonical inclusion.

A subset X of a profinite group H is called 1-convergent if the inclusion map $X \to H$ is 1-convergent.

(c) Deduce the following from (b). Let G be a profinite group and X a (topological) 1-convergent generating set of G. Then there exists a continuous epimorphism from $\widehat{F}(X)$ to G.

(d) Let G be a profinite group. One can show (although this is non-trivial) that G always has a 1-convergent generating set. Denote by $ON(G)$ the set of open normal subgroups of G. Prove that if G is not finitely generated, then for any 1-convergent generating set X of G we have $|X| = |ON(G)|$. **Hint:** First prove that $|X| \leq |ON(G)|$ by constructing a finite-to-one map from X to $ON(G)$. Then use (a) and (c) to prove that $|ON(G)| \leq |X|$.

Important remark: HW#3.7 claimed that $d(G) = \dim H^1(G, \mathbb{F}_p)$ for any pro-p group G. If G is not finitely generated, this statement is actually incorrect (in general) if $d(G)$ denotes the minimal size of a generating set of G. However if for an infinitely generated G we redefine $d(G)$ to be the common size of its 1-convergent generating sets (thus

$d(G) = |ON(G)|$ by (d)), then the equality becomes correct. What we actually proved in Problem Session 3 is that if $G/\Phi(G) \cong \mathbb{F}_p^X$ (and we know this is always true for some X), then $\dim H^1(G, \mathbb{F}_p) = |X|$. One can deduce the corrected version of HW#3.7 from this result and (d), but this requires some additional work.

2. This is a corrected and expanded version of Problem 2 in HW#4.

We start with some definitions. Let A be an associative ring with 1 and M an A-bimodule. A map $f : A \to M$ is called a *derivation* if

(1) $f(a + b) = f(a) + f(b)$ for all $a, b \in A$;
(2) $f(ab) = f(a).b + a.f(b)$ for all $a, b \in A$.

The set of all derivations from A to M (which is clearly an abelian group with respect to pointwise addition) will be denoted by $Der(A, M)$.

If G is a group and M is a right G-module, a derivation from G to M is a map $f : G \to M$ satisfying

(3) $f(gh) = f(g).h + f(g)$ for all $g \in G$.

Again we denote by $Der(G, M)$ the set of all derivations from G to M, which is still an abelian group. Recall that $Der(G, M)$ appeared in class in the course of the explicit description of the first cohomology, namely

$$H^1(G, M) = Der(G, M)/IDer(G, M)$$

where $IDer(G, M)$ is the subgroup of inner derivations (maps of the form $g \mapsto m - m.g$

Now the actual problem begins.

(a) Let A be an associative ring with 1 and M an A-bimodule. Prove that for every $m \in M$ the map from A to M given by $a \mapsto a.m - m.a$ is a derivation. Derivations of this form are called inner.
(b) Let G be a group and let $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ be the unique homomorphism of abelian groups such that $\varepsilon(g) = 1$ for all $g \in G$. Prove that ε is a ring homomorphism and its kernel is the augmentation ideal ω_G of $\mathbb{Z}[G]$ (by definition from class ω_G is the ideal generated by all elements of the form $g - 1$, $g \in G$).
(c) Let G be a group and M a right G-module (and hence also a right $\mathbb{Z}[G]$-module). Prove that M is actually a $\mathbb{Z}[G]$-bimodule where the left action is given by $r.m = \varepsilon(r)m$ for all $r \in \mathbb{Z}[G]$ and $m \in M$. Thus we can consider the spaces of derivations $Der(\mathbb{Z}[G], M)$ and $Der(G, M)$. Prove that the restriction map

$R : Der(\mathbb{Z}[G], M) \to Der(G, M)$ is an isomorphism of abelian groups and that a derivation $D \in Der(\mathbb{Z}[G], M)$ is inner $\iff$ $R(D)$ is inner.

(d) Again let G be a group and ω_G the augmentation ideal. Prove that if X generates G as a group, then the set $\{x - 1 : x \in X\}$ generates ω_G as a right G-module (equivalently, $\mathbb{Z}[G]$-module).

(e) Now assume that G is a free group and X is a free generating set for G. Then one can show (this is not part of the problem) that ω_G is a free right $\mathbb{Z}[G]$-module, freely generated by $\{x-1 : x \in X\}$, that is, for any $f \in \omega_G$ there exist unique elements $\{D_x(f)\}_{x \in X}$ such that

$$f = \sum_{x \in X} (x - 1)D_x(f)$$

(if X is infinite, we implicitly require that only finitely many $D_x(f)$ are nonzero). Prove that for any $x \in X$ the map $\frac{\partial}{\partial x} : G \to \mathbb{Z}[G]$ given by $\frac{\partial}{\partial x}(g) = D_x(g - 1)$ is a derivation. It is called the (right) Fox derivative with respect to x.

3. Recall that in Lecture 16 we proved the following theorem.

Theorem 1. *Let G be a finitely presented pro-p group, and denote its minimal number of generators by $d(G)$ and its minimal number of relators by $r(G)$. Suppose that G has a pro-p presentation with n generators and m relators for some n and m. Then G also has a pro-p presentation with $d(G)$ generators and $m - (n - d(G))$ relators.*

Prove the following lemma which was used in the proof of Theorem 1.

Lemma 2. *Let $\langle X|R\rangle$ be a pro-p presentation of a pro-p group G where X and R are both finite (recall that this means that $G \cong F/N$ where $F = F_{\widehat{p}}(X)$ is the free pro-p group on X and $N = \langle\langle R\rangle\rangle$ is the closed normal subgroup of F generated by R). Suppose that $|X| > d(G)$. Then*

(a) *At least one defining relator $r \in R$ lies outside of the Frattini subgroup $\Phi(F)$;*

(b) *For any $r \in R \setminus \Phi(F)$ there exists a (topological) generating set X' of X such that $r \in X'$ and $|X'| = |X|$ (so X' is of minimal possible size).* **Hint:** *How can you construct a minimal-size generating set for F using $\Phi(F)$?*

4. Let G be a finitely presented pro-p group, $d = d(G)$ and $r = r(G)$. Thus, replacing G by an isomorphic group, we can assume that $G =$

F/N where F is a free pro-p group of rank d and N is (topologically) generated by r elements as a normal subgroup of F. In class we proved that any non-split TCE (topological central extension) of $G = F/N$ by $\mathbb{F}_p$ is equivalent to an extension of the form

$$\mathcal{E}_{K,\iota} = (1 \to \mathbb{F}_p \xrightarrow{\iota} F/K \xrightarrow{\pi} F/N \to 1)$$

where

(i) K is a closed normal subgroup of F such that $K \subseteq N$, N/K is a central subgroup of order p in F/K, $\pi : F/K \to F/N$ is the natural projection and

(ii) $\iota : \mathbb{F}_p \to N/K$ is any isomorphism.

Prove that if $\mathcal{E}_{K,\iota}$ is equivalent to $\mathcal{E}_{K',\iota'}$, then $K' = K$ and $\iota' = \iota$ (this was a key step in proving that the number of equivalence classes of TCE's of G by $\mathbb{F}_p$ is equal to $p^{r(G)}$).

Hint: Suppose that $\mathcal{E}_{K,\iota}$ and $\mathcal{E}_{K',\iota'}$ are equivalent, and let $\varphi : F/K \to F/K'$ be an isomorphism establishing the equivalence. First show that there exists a (continuous) homomorphism $\widetilde{\varphi} : F \to F$ such that

$$\widetilde{\varphi}(x) \equiv x \mod N \text{ for all } x \in F$$

and $\widetilde{\varphi}$ induced φ, that is, $\pi_{K'} \circ \widetilde{\varphi} = \varphi \circ \pi_K$ where $\pi_K : F \to F/K$ and $\pi_{K'} : F \to F/K'$ are the natural projections. Then using the fact that $N \subseteq \Phi(F) = [F, F]F^p$ (why is this true?) show that

$$\widetilde{\varphi}(x) \equiv x \mod [F, N]N^p \text{ for all } x \in N.$$

Finally deduce that $K' = K$, φ is the identity map and $\iota' = \iota$ (in this order).

5. In Lecture 20 we will prove a generalization of Hilbert's Theorem 90 due to Noether which states that $H^1(\mathrm{Gal}\,(K/F), K^\times) = 0$ for any finite Galois extension K/F (as we already proved in class, once we know this for finite Galois extensions, we get the same result for arbitrary Galois extensions).

Assume now that K/F is cyclic, that is, $\mathrm{Gal}\,(K/F)$ is cyclic. Prove that in this case the above theorem is equivalent to the classical version of Hilbert's Theorem 90 as usually stated in Algebra-II: any element $a \in K$ of norm 1 can be written as $a = \frac{b}{\sigma(b)}$ for some b where b is a fixed (in advance) generator of $\mathrm{Gal}\,(K/F)$.