Math 8851. Homework #4. To be completed by 5pm on Fri, Oct 20

Below [DDMS] refers to the book 'Analytic pro-p groups', 2nd edition by Dixon, du Sautoy, Mann and Segal.

Before stating Problem 1 we introduce several definitions.

Definition. A *supernatural number* if a formal product $\prod\limits_p p^{a_p}$ where p ranges over all primes and each a_p is either a non-negative integer or infinity.

Supernatural numbers form a monoid with respect to multiplication given by

$$\prod_p p^{a_p} \cdot \prod_p p^{b_p} = \prod_p p^{a_p+b_p}$$

where as usual we set $\infty + x = x + \infty = \infty$ for any $x \in \mathbb{Z}_{\geq 0} \sqcup \{\infty\}$.

It is not hard to show that for any non-empty set S of supernatural numbers there are unique greatest common divisor $gcd(S)$ (which is a multiple of any common divisor of the elements of S) and least common multiple $LCM(S)$ (which divides any common multiple of the elements of S), and morever both $gcd(S)$ and $LCM(S)$ are given by the standard formulas: if $S = \{s_i\}_{i\in I}$ where $s_i = \prod\limits_p p^{a_{i,p}}$, then $gcd(S) = \prod\limits_p p^{m_p}$ and $LCM(S) = \prod\limits_p p^{M_p}$ where $m_p = \inf\{a_{i,p} : i \in I\}$ and $M_p = \sup\{a_{i,p} : i \in I\}$.

If G is a profinite group, the order of G is the supernatural number $|G|$ defined by

$$|G| = LCM(\{|G/N| : N \text{ is an open normal subgroup of } G\}).$$

Note that G is pro-p for some prime $p \iff |G| = p^a$ for some $a \in \mathbb{Z}_{\geq 0} \sqcup \{\infty\}$.

If H is a closed subgroup of G, we define the index $[G : H]$ by $[G : H] = LCM(\{[G : U]\})$ where U ranges over all open subgroups of G containing H.

Definition. Let G be a profinite group and p a prime dividing $|G|$. A closed subgroup H of G is called a *Sylow pro-p subgroup* if H is a pro-p subgroup and $[G : H]$ is coprime to p.

One can show that Sylow pro-p subgroups always exist and any two Sylow pro-p subgroups of G are conjugate (see Problems 1.11 and 1.12 in [DDMS]), but this is not part of this homeowrk.

1.

(a) Prove that if G is a profinite group and H is a closed normal subgroup of G, then $|G| = |G/H| \cdot |H|$.

(b) Let $G = SL_n(\mathbb{Z}_p)$ (where as usual $\mathbb{Z}_p$ is p-adic integers). Describe explicitly a Sylow pro-p subgroup of G and prove your answer. **Hint:** Problem 5 from HW#1 is relevant here.

2. We start with some definitions. Let A be an associative ring with 1 and M a right R-module. 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) $f(ab) = f(a).b + f(b)$ 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 $G \to M$ satisfying (2) above (for all $a, b \in G$). 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

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

where $IDer(G, M)$ is the subgroup of inner derivations (maps of the form $g \mapsto m - m.g$ for some fixed $m \in M$); however, this is not directly related to this problem. The main point of this problem is to give an important example of a derivation in the case of a non-trivial action (which actually arises in some proofs that I am going to discuss in class).

Now the actual problem begins

(a) Let G be a group and M a right G-module. Prove that the restriction map $Der(\mathbb{Z}[G], M) \to Der(G, M)$ is an isomorphism of abelian groups.

(b) Again let G be a group and ω_G be the augmentation ideal of $\mathbb{Z}[G]$ (the ideal generated by all elements of the form $g - 1$, $g \in G$). 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).

(c) 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 $\frac{\partial f}{\partial x} : G \to \mathbb{Z}[G]$ given by $\frac{\partial f}{\partial x}(g) = D_x(f-1)$ is a derivation. It is called the (right) Fox derivative with respect to x.

3. Let X and Y be topological spaces and $C(X,Y)$ the space of continuous maps from X to Y. The *compact-open* topology on $C(X,Y)$ is the topology with subbase $\{U_{K,O}\}$ where $K \subseteq X$ is compact, $O \subseteq Y$ is open and $U_{K,O} = \{f \in C(X,Y) : f(K) \subseteq U\}$.

Now let W/F be a Galois extension and consider Gal(W/F) as a subset of $C(W,W)$ where W is endowed with the discrete topology. Prove that the Krull topology on Gal(W/F) coincides with the compact-open topology (that is, the topology induced from the compact-open topology on $C(W,W)$).

4. Let W/F be a Galois extension and L a subfield of W/F.

(a) Prove that the Krull topology on Gal(W/L) is induced from the Krull topology on Gal(W/F).

(b) Assume now that L/F is Galois, so that Gal(W/L) is normal in Gal(W/F) and Gal$(W/F)/$Gal(W/L) is canonically isomorphic to Gal(L/F). Prove that under this isomorphism, the Krull topology on Gal(L/F) corresponds to the quotient topology on Gal$(W/F)/$Gal(W/L).

5. Let $\{d_n\}_{n\in\mathbb{N}}$ be a sequence of pairwise coprime integers and $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots)$. Define the map $\iota : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{F}_2^\infty$ by $\iota(\varphi) = (a_1, a_2, \ldots)$ where $a_i = 0$ if $\varphi(\sqrt{d_i}) = \sqrt{d_i}$ and $a_i = 1$ if $\varphi(\sqrt{d_i}) = -\sqrt{d_i}$. Prove that ι is a group isomorphism.

6. In each part of this problem we are given a Galois extension W/F and a closed subgroup H of $G = $ Gal(W/F). Find (with proof) the fixed L of H (equivalently, find the unique field L such that Gal$(W/L) = H$). In each part we also fix a prime p.

(a) F is a finite field, $W = \overline{F}$ and $H = \prod\limits_{q \neq p} \mathbb{Z}_q$. (Recall that in this case G is canonically isomorphic to $\widehat{\mathbb{Z}} = \prod\limits_{q} \mathbb{Z}_q$.

(b) $F = \mathbb{Q}$, $W = \mathbb{Q}(\{\zeta_n : n \in \mathbb{N}\})$ where ζ_n is a primitive n^{th} root of unity and $H = \prod\limits_{q \neq p} \mathbb{Z}_q^\times$. (Recall that in this case G is canonically isomorphic to $\widehat{\mathbb{Z}}^\times = \prod\limits_{q} \mathbb{Z}_q^\times$)

(c) Let F and W be as in (b), and let H be the product of $\prod\limits_{q \neq p} \mathbb{Z}_q^\times$ (the subgroup from (b)) and the subgroup $(\mathbb{Z}_p^\times)^2$ consisting of all squares in $\mathbb{Z}_p^\times$. (As stated in class, if p is odd, then $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, so $(\mathbb{Z}_p^\times)^2$ has index 2 in $\mathbb{Z}_p^\times$ and $\mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$, so $(\mathbb{Z}_2^\times)^2$ has index 4 in $\mathbb{Z}_2^\times$).

Hint: Analyzing the proofs of the isomorhisms $\mathrm{Gal}\,(W/F) \cong \widehat{\mathbb{Z}}$ in (a) and $\mathrm{Gal}\,(W/F) \cong \widehat{\mathbb{Z}}^\times$ in (b) and (c) will probably be helpful for all parts. In (c) you may be you need to use some facts not discussed in Algebra-II to rigorously prove the answer.