Math 8851. Homework #6. To be completed by 5pm on Fri, Nov 17

1. Let K/F be a Galois extension and p a prime. Prove that the following are equivalent:

(i) K/F is a p-extension as defined in class, that is, K/F is a compositum of finite Galois extensions K_i/F with $[K_i : F]$ a power of p.

(ii) $\mathrm{Gal}\,(K/F)$ is a pro-p group.

2.

(a) Let K/F and L/F be p-extensions. Prove that KL/F is also a p-extension.

(b) Suppose K/L and L/F are both p-extensions, and let M be the Galois closure of K over F (note: we do not know whether K/F is Galois or not). Prove that M/F is also a p-extension. **Hint:** first use (a) to show that M/L is a p-extension.

(c) As in class, given a number field K and a prime p, denote by $K^{un}(p)$ the maximal unramified p-extension of K. Prove that if L/K is an unramified p-extension of number fields, then $K^{un}(p) = L^{un}(p)$ (equality is unambiguous here as we can think of both $K^{un}(p)$ and $L^{un}(p)$ as subfields of the field of algebraic numbers).

Note: There are two general approaches to solving (a) and (b). One can first prove (a) and (b) for finite p-extensions and then extend both results to arbitrary p-extensions. Alternatively, it is possible to prove (a) and (b) directly for arbitrary p-extensions.

3. Let F be a field of characteristic p. A polynomial of the form $f(x) = x^p - x - a$ with $a \in F$ is called an *Artin-Schreier polynomial*.

(a) Let $f(x) \in F[x]$ be an Artin-Schreier polynomial. Prove the following dichotomy: either $f(x)$ splits completely over F or $f(x)$ is irreducible in $F[x]$, and if $\alpha \in \overline{F}$ is any root of $f(x)$, then $F(\alpha)/F$ is Galois with Galois group cyclic of order p.

(b) Let K be the maximal p-extension of F. Use Problem 2 and part (a) to prove that any Artin-Schreier polynomial over K has a root in K (and hence splits over K by (a)). Equivalently, the map $x \mapsto x^p - x$ from K to K is surjective. Recall that the latter fact was used to prove that the Galois group $\mathrm{Gal}(K/F)$ is free pro-p.

4. Let $q_1, \ldots, q_n$ be a sequence of odd integers (not necessarily positive) such that $q_i \equiv 1 \mod 4$ for all i and $|q_1|, \ldots, |q_n|$ are distinct primes. Let $m = \prod_{i=1}^{n} q_i$, $K = \mathbb{Q}(\sqrt{q})$ and $L = \mathbb{Q}(\sqrt{q_1}, \ldots, \sqrt{q_n})$. Prove that the extension L/K is unramified (this was Claim 22.2 from class). You can use the following properties of ramification without proof. Below by a prime of a number field M we mean a nonzero prime ideal of O_M.

(a) Let $d \in \mathbb{Z}$, and assume that d is square-free. Then the set of primes which ramify in the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is
   - exactly the set of prime of divisors of d if $d \equiv 1 \mod 4$;
   - $\{\text{prime divisors of } d\} \cup \{2\}$ if $d \equiv 2, 3 \mod 4$.

(b) Let K_1/F and K_2/F be extensions of number fields. Then a prime of F ramifies in the extension K_1K_2/F if and only if it ramifies in K_1/F or in K_2/F.

(c) Let E/F be an extension of number fields and M another number field. If a prime p of F does not ramify in E/F, then any prime $\mathcal{P}$ of M which lies over p (that is, such that $p = \mathcal{P} \cap O_F$) does not ramify in the extension ME/M.

5. Let G be a finitely presented pro-p group such that $d(G) > r(G)$. Prove that the abelianization $G^{ab} = G/[G, G]$ is infinite. **Hint:** Let $\langle X|R\rangle$ be a pro-p presentation of G with $|X| = d(G)$ and $|R| = r(G)$. Show that $G^{ab} \cong \mathbb{Z}_p^{d(G)}/I$ where $\mathbb{Z}_p^{d(G)}$ is the product of $d(G)$ copies of $\mathbb{Z}_p$ and I is the subgroup of $\mathbb{Z}_p^{d(G)}$ generated by $r(G)$ elements.

6. Let X be an infinite set, and let I be the set of all finite subsets of X. Note that if I is partially ordered by inclusion, then I is a directed set. For each $Y \in I$ let $\widehat{F}(Y)$ be the free profinite group on Y. Given $Y, Z \in I$ with $Y \subseteq Z$, define $\pi_{Z,Y} : \widehat{F}(Z) \to \widehat{F}(Y)$ be the unique continuous homomorphism such that $\pi_{Z,Y}(z) = z$ for all $z \in Y$ and $\pi_{Z,Y}(z) = 1$ for all $z \in Z \setminus \{1\}$. Clearly $(\{\widehat{F}(Y)\}, \{\pi_{Z,Y}\})$ is an inverse system. Prove that $\mathrm{proj}\lim_{Y \in I} \widehat{F}(Y)$ is isomorphic to the free profinite group on X, as defined in HW#5.1.

Remark: The result of Problem 6 is one of several ways to argue why the definition of free profinite groups given in HW#5.1 is the "right" one. (This assetion would be false if we defined free profinite groups on arbitrary sets simply as profinite completions of the corresponding abstract groups). Other nice consequences of the definition we are using (which would otherwise be false) include the following:

(2) Every countably based profinite (resp. pro-p) group is a (continuous) quoitent of a free profinite (resp. pro-p) group of countable rank.

(3) Closed subgroups of free pro-p groups are free pro-p (for profinite groups this is false already in rank 1 as $\mathbb{Z}_p$ is a closed subgroup of $\widehat{\mathbb{Z}}$).

(4) A pro-p group G is free $\iff$ $H^2(G, \mathbb{F}_p) = 0$.