Homework Assignment # 12

Plan for the week of May 3-7. Exact sequences. Injective, projective and flat modules (section 10.5 in DF).

Here and in all future assignments "online" or "online notes" refers to Algebra-II lectures posted on my Spring 2010 Algebra-II webpage

`http://people.virginia.edu/~mve2x/7752_Spring2010/`

Problems, due by 11:59pm on Friday, April 30th.

Problem 1: This is a continuation of Problem 5 from Midterm#2. Let p be a prime, with $p \equiv 3 \mod 4$, $\omega = e^{2\pi i/p}$, $K = \mathbb{Q}(\omega)$ and L the unique subfield of K with $[L : \mathbb{Q}] = 2$. Let S be the set of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ representable as squares and T the set of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ not representable as squares.

(a) Prove that any $\alpha \in K$ can be uniquely represented as $\alpha = \sum_{s\in S} b_s\omega^s + \sum_{t\in T} c_t\omega^t$, with $b_s, c_t \in \mathbb{Q}$.

(b) Let $\alpha \in K$. Prove that $\alpha \in L$ if and only if in the above decomposition of α all b_s are the same and all c_t are the same.

(c) Let $\zeta = \sum_{s\in S} \omega^s$, $\eta = \zeta\overline{\zeta}$, and write $\eta = \sum_{s\in S} b_s\omega^s + \sum_{t\in T} c_t\omega^t$ as in (a). Prove that
   (i) there exists $d \in \mathbb{Q}$ such that $b_s = c_t = d$ for all s and t and
   (ii) $\sum_{s\in S} b_s + \sum_{t\in T} c_t = \frac{(p-1)^2}{4} - \frac{p\cdot(p-1)}{2} = -\frac{(p-1)(p+1)}{4}$

(d) Use (c) to prove that $\eta = \frac{p+1}{4}$ and deduce that $L = \mathbb{Q}(\sqrt{-p})$.

Problem 2: Let I be a poset. Let $\{j_n\}_{n\in\mathbb{N}}$ be an infinite strictly increasing sequence in I, that is, $j_n < j_{n+1}$ for all n. We will say that $\{j_n\}$ is *dominant* if for every $i \in I$ there exists $n \in \mathbb{N}$ such that $i \le j_n$ (note that the existence of such a sequence ensures that I is a directed set).

Suppose now that I is a poset which contains a dominant strictly increasing sequence $\{j_n\}_{n\in\mathbb{N}}$, let $\{X_i\}_{i\in I}$ be an inverse system of sets, groups or rings, and let $\{X_{j_n}\}_{n\in\mathbb{N}}$ be the subsystem consisting of objects index by elements of $\{j_n\}$ (with the same transition maps). Prove that

$$\varprojlim_{i\in\mathbb{N}} X_i \cong \varprojlim_{n\in\mathbb{N}} X_{j_n}. \qquad (***)$$

Note that the limit on the right-hand side can be described more explicitly using HW#11.5(a) (this is an explanation of why the statement

of Problem 2 is useful, rather than a hint on how to prove the isomorphism). **Hint:** It is probably most convenient to define a natural morphism from LHS to RHS in (***) (this can be done for any sequence $\{j_n\}$) and then prove that the map is bijective (using the fact that $\{j_n\}_{n\in\mathbb{N}}$ is strictly increasing and dominant).

Problem 3: Let $\widehat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$. It is defined as the inverse limit $\varprojlim_{i\in\mathbb{N}} \mathbb{Z}/i\mathbb{Z}$ where $\mathbb{N}$ is considered as a poset with respect to the divisibility partial order ($i \leq j \iff i \mid j$) and the maps $\pi_{ij} : \mathbb{Z}/j\mathbb{Z} \to \mathbb{Z}/i\mathbb{Z}$ (with $i \mid j$) are natural projections. Also recall that for each prime p the ring of p-adic integers $\mathbb{Z}_{\widehat{p}}$ is defined as the inverse limit $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ (this time $\mathbb{N}$ is a poset with the usual order and the transition maps are the same). Prove the following isomorphism of rings:

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_{\widehat{p}}$$

where the product is taken over all primes. This result can be thought of as the "profinite Chinese Remainder Theorem". **Hint:** This can be proved in many different ways. One possible approach is to choose a dominant strictly increasing sequence in $\mathbb{N}$ with divisibility partial order, and then use the isomorphism from Problem 2 in conjunction with the usual Chinese Remainder Theorem.

Problem 4: Let $P = \{p_1 < p_2 < \ldots\}$ be the set of all prime numbers enumerated in increasing order, let $K = \mathbb{Q}(\{\sqrt{p} : p \in P\})$.

(a) Prove that $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2^\infty$ (product of countably many copies of $\mathbb{Z}_2$) via the map $\sigma \mapsto (\varepsilon_1(\sigma), \varepsilon_2(\sigma), \ldots)$ where

$$\varepsilon_i(\sigma) = \begin{cases} 0 & \text{if } \sigma(\sqrt{p_i}) = \sqrt{p_i} \\ 1 & \text{if } \sigma(\sqrt{p_i}) = -\sqrt{p_i}. \end{cases}$$

Note: You can use the representation of $\mathrm{Gal}(K/\mathbb{Q})$ as an inverse limit of finite groups (as in HW#11.3) in conjunction with Problem 2, but you can also give a direct argument.

(b) Describe explicitly all closed subgroups of index 2 in G and their fixed subfields (you can start with subfields and then use the Galois correspondence to describe the subgroups, but you also do things in the opposite order).

(c) Now prove that G has a non-closed subgroup of index 2. **Hint:** G has exponent 2, so you can think of it as vector space over $\mathbb{F}_2$.