Homework Assignment # 11

Plan for the week of April 26-30. Tuesday: finish the discussion of Galois correspondence for infinite Galois extensions. Thursday: transcendental extensions (section 14.8 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: Prove the following analogue of Kummer's theorem for abelian extensions: Let $n \in \mathbb{N}$ and let F be a field containing primitive n^{th} root of unity.

(a) Let K/F be a finite Galois extension such that $\mathrm{Gal}(K/F)$ is abelian of exponent dividing n. Then there exist $a_1, \ldots, a_t \in K$ s.t. $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$, or more precisely, there exist $\alpha_1, \ldots, \alpha_t \in K$ s.t. $K = F(\alpha_1, \ldots, \alpha_t)$ and $\alpha_i^n \in F$ for all i. **Hint:** Use Kummer's theorem, the Galois correspondence and the classification theorem for finite abelian groups.

(b) Conversely, suppose that $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_t})$ for some elements $a_1, \ldots, a_t \in F$. Prove that K/F is Galois, and $\mathrm{Gal}(K/F)$ is abelian of exponent dividing n.

Problem 2: DF, problem 9 on p.636. By definition a *cyclic extension* is a Galois extension with cyclic Galois group.

Problem 3: DF, problem 19 on p.654. Note: we essentially discussed in class why (a),(b) and (c) are true, so the main thing to prove is (d), but you should still write down the complete solution.

Problem 4: In all parts of this problem G is a fixed group. Given normal subgroups M and N of G with $M \subseteq N$ let $\pi_{N,M} : G/M \to G/N$ be the natural projection (given by $\pi_{M,N}(gM) = gN$).

(a) Let Ω be the poset of all normal subgroups of finite index in G ordered by reverse inclusion ($N \leq M$ if and only if $M \subseteq N$). Prove that Ω is a directed set and the quotient groups $\{G/N\}_{N\in\Omega}$ form an inverse system with respect to the transition maps $\pi_{N,M}$. The inverse limit $\varprojlim\limits_{N\in\Omega} G/N$ is called the *profinite completion* of G. **Note:** One of the homework problems from Algebra-I is relevant for this problem.

(b) Let p be a fixed prime. Prove the analogue of (a) for Ω_p defined as the poset of all normal subgroups of G which have index p^k for some $k \in \mathbb{Z}_{\geq 0}$. The inverse limit $\varprojlim_{N \in \Omega_p} G/N$ is called the *pro-p completion* of G.

Problem 5:

(a) Let $\mathcal{C}$ be the category of groups or rings. Consider natural numbers $\mathbb{N}$ as a poset with respect to the usual ordering. Let $\{X_i\}_{i \in \mathbb{N}}$ be the inverse system in $\mathcal{C}$, and let $\{\pi_{ij} : X_j \to X_i\}_{i \leq j}$ be the transition maps. Prove that the inverse limit $\varprojlim_{i \in \mathbb{N}} X_i$ coincides with the subgroup (resp. subring) of the direct product $\prod_{i \in \mathbb{N}} X_i$ consisting of all sequences $(x_1, x_2, \ldots)$ such that $x_i \in X_i$ and $\pi_{i,i+1}(x_{i+1}) = x_i$ for all i.

(b) Let $p \geq 2$ be an integer (we do NOT assume that p is prime, although the latter is the most interesting case which explains the notation). For each $i \in \mathbb{N}$ let $X_i = \mathbb{Z}/p^i\mathbb{Z}$. Then $\{X_i\}_{i \in \mathbb{N}}$ is an inverse system in the category of rings (where the transition maps π_{ij} are natural projections). The inverse limit

$$\varprojlim_{i \in \mathbb{N}} X_i = \varprojlim_{i \in \mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$$

is called the *ring of p-adic integers* and will be denoted by $\mathbb{Z}_{\widehat{p}}$ (it is common to denote p-adic integers simply by $\mathbb{Z}_p$ but we will not use the latter notation to avoid confusion with the finite field of order p).

Use (a) to prove that as a set $\mathbb{Z}_{\widehat{p}}$ can be identified with the set of formal expressions $\sum_{i=0}^{\infty} a_i p^i$ where each a_i is an integer between 0 and $p-1$ (very informally these are "power series in p") and the addition and multiplication are defined as follows: given two elements $\sum_{i=0}^{\infty} a_i p^i, \sum_{i=0}^{\infty} b_i p^i$, write the coefficient sequences $a_0, a_1, \ldots$ and $b_0, b_1, \ldots$ from right to left, one above the other, and then add and multiply using the usual carryover rules mod p (the case $p = 10$ will correspond exactly to the addition and multiplication algorithm you learn in school).

(c) Define $\iota : \mathbb{Z} \to \mathbb{Z}_{\widehat{p}}$ by $\iota(n) = (n + p\mathbb{Z}, n + p^2\mathbb{Z}, \ldots)$. Prove that ι is an injective ring homomorphism and that under the identification from (b) $\iota(\mathbb{Z}_{\geq 0})$ is equal to the set of finite sums

$\sum_{i=0}^{k} a_i p^i$. Then express $\iota(-1)$ in the form $\sum_{i=0}^{\infty} a_i p^i$ with $0 \leq a_i \leq p - 1$.