# MATH 703: HOMEWORK #2

DUE FRIDAY, FEB. 8, 2013

## 1. Henselizations

This problem completes the proof of the following result discussed in class. Suppose $A$ is a discrete valuation ring with fraction field $K$ and maximal ideal $m_A$. (In class we took $A$ to be any integral domain which is integrally closed in its fraction field, but the D.V.R. case is simpler.) Don't assume $A$ is complete; for instance, $A$ could be the localization of the ring of integers of a number field at a non-zero prime ideal. Let $K^s$ be a separable closure of $K$ and let $B$ be the integral closure of $K^s$ in $K$. Let $\mathcal{Q}$ be a prime over $m_A$ in $B$. Define $D$ to be the decomposition group of $\mathcal{Q}$ inside $G = \mathrm{Gal}(K^s/K)$. Then $B^D$ is the integral closure of $A$ inside the fixed field $(K^s)^D$. Define $R$ to be the localization of $B^D$ at the maximal ideal $B^D \cap \mathcal{Q}$ of $B^D$ under $\mathcal{Q}$. In class we showed that the natural inclusion $A \to R$ is a local homomorphism (in the sense that the inverse image in $A$ of the maximal ideal $m_R$ of $R$ is $m_A$), and that $R$ is a Henselian ring. The object of this exercise is to complete the proof that $R$ is in fact the Henselization of $A$.

1. Suppose $r \in R$, and let $L$ be the field $K(r)$ generated by $r$ over $K$. Let $O_L$ be the integral closure of $A$ in $L$. Show that if $\mathcal{Q}_L = \mathcal{Q} \cap L$ is the prime of $O_L$ under $\mathcal{Q}$, then $m_A$ decomposes in $O_L$ as
$$m_A \cdot O_L = \mathcal{Q}_L \cdot \mathcal{J}_1^{e_1} \cdots \mathcal{J}_s^{e_s}$$
where $s \geq 0$, $\mathcal{Q}_L, \mathcal{J}_1, \ldots, \mathcal{J}_s$ are distinct maximal ideals of $O_L$, $e_i \geq 1$ and the natural homomorphism $A/m_A \to O_L/\mathcal{Q}_L$ is an isomorphism.

   Hint: One way to do this is to show that the natural homomorphism $\nu : K_{m_A} \to L_{\mathcal{Q}_L}$ is an isomorphism when $K_{m_A}$ is the completion of $K$ with respect to the powers of $m_A$ and $L_{\mathcal{Q}_L}$ is the completion of $L$ with respect to the powers of $\mathcal{Q}_L$. To show $\nu$ is an isomorphism, you could use the normal closure $F$ of $L$ over $K$ inside $K^s$. Show that $D$ projects to the decomposition group $D_F$ of $\mathcal{Q}_F = \mathcal{Q} \cap F$ inside $H = \mathrm{Gal}(F/K)$, and $L = F^{D_F}$. You can then use the fact proved in class that the decomposition group of a prime ideal in the Galois group of a finite Galois extension can be identified with the Galois group of a suitable extension of completions.

2. With the notations of part (1), show that $r$ can be written as $\pi^a \alpha/\beta$ where $\pi \in A$ is a uniformizer and $\alpha, \beta \in O_L$ are elements for which neither $\alpha$ nor $\beta$ are in $\mathcal{Q}_L$ but $\alpha$ and $\beta$ are in $\mathcal{J}_i^{e_i}$ for $i = 1, \ldots, s$.

3. With the notations of part (2), let $\lambda$ be either $\alpha$ or $\beta$. Show that to prove $R$ is the Henselization of $A$, it will suffice to show that $\lambda$ is a root of a monic polynomial $f(x) \in A[x]$ such that the reduction $\overline{f}(x) \in (A/m_A)[x]$ of $f(x)$ mod $m_A$ factors as $(x - \overline{\lambda})x^m$ for some integer $m \geq 0$, where $\overline{\lambda} \neq 0$ is the image of $\lambda$ in $R/m_R = A/m_A$. You can use the fact proved in class that the Henselization of $A$ is the intersection of all of the Henselian local subrings of $\hat{A}$ which contain $A$.

4. Complete the proof that $R$ is the Henselization of $A$ by producing a polynomial $f(x)$ as in problem (3) using the action of $\lambda$ on $O_L$ together with problem #1.

## 2. Artin's reciprocity law and quadratic reciprocity.

The quadratic reciprocity law for odd rational primes $p \neq q$ is that

$$\begin{pmatrix} p \\ q \end{pmatrix} \cdot \begin{pmatrix} q \\ p \end{pmatrix} = (-1)^{\left(\frac{(p-1)}{2}\frac{(q-1)}{2}\right)}$$

We proved this in class when $p \equiv 1 \bmod 4$. Suppose from now on that $p \equiv 3 \bmod r$. The object of these exercises is to prove the formula for all odd $q \neq p$.

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{p})$. The set $S$ of places of $K$ over which $L$ ramifies consists of the non-archimedean places determined by 2 and $p$. The Artin map

$$\Psi_{L/K} : I_S \to \mathrm{Gal}(L/K)$$

is defined on the group $I_S$ of fractional ideals of $K$ which are prime to all prime ideals associated to non-archimedean places in $S$. Here $\mathbb{Z}q \in I_S$. One has $\Psi_{L/K}(q\mathbb{Z}) = \Phi(\mathcal{Q}/q\mathbb{Z})$ for any prime $\mathcal{Q}$ of $O_L$ over $q\mathbb{Z}$, where $\Phi(\mathcal{Q}/p\mathbb{Z})$ is the Frobenius automorphism of $\mathcal{Q}$. As shown in class,

$$\Psi_{L/K}(q\mathbb{Z}) = \begin{pmatrix} p \\ q \end{pmatrix} = \pm 1$$

when we identify $\mathrm{Gal}(L/K)$ with $\{\pm 1\}$. This is because $q\mathbb{Z}$ splits in $L = \mathbb{Q}(\sqrt{p})$ if and only if $p$ is a square mod $q$, and $\Phi(\mathcal{Q}/q\mathbb{Z})$ is a generator of the decomposition group of $\mathcal{Q}$ in $\mathrm{Gal}(L/K)$.

Artin's reciprocity law says that there is a minimal conductor $\mathcal{M} = (\mathcal{M}_f; w_1, \ldots, w_i)$ in $K$ such that $\mathcal{M}_f$ is a product of positive powers of primes ideals associated to places in $S$ and $w_1, \ldots, w_s$ is the set of real places in $S$ such that $\Psi_{L/K}$ factors through the ray class group $\mathrm{Cl}_{\mathcal{M}}(K)$. Thus $\mathcal{M}_f = 2^a p^b$ for some integers $a, b > 0$, and $s = 0$ since the real place of $\mathbb{Q}$ does not ramify in $L$. The Artin map then defines a surjective homomorphism

$$\Psi_{L/K} : \mathrm{Cl}_{\mathcal{M}}(K) = (\mathbb{Z}/2^a p^b)^*/\{\pm 1\} \to \mathrm{Gal}(L/K) = \{\pm 1\}.$$

5. Show that the squares in $(\mathbb{Z}/2^a)^*$ are the residue classes which can be reprensted by integers which are congruent to 1 mod 8, while the squares in $(\mathbb{Z}/p^b)^*$ contain the residue classes congruent to 1 mod $p$. Use this to show that because $\mathcal{M}_f$ is minimal, one must have $1 \leq a \leq 3$ and $b = 1$. Then show that $a = 1$ is impossible because if $a = 1$ then the Artin map would factor through the natural homomorphism $\mathrm{Cl}_{\mathcal{M}}(K) \to \mathrm{Cl}_{\mathbb{Z}p^b}(K)$, so that there would be a conductor that did not involve the ramifying prime 2.

6. Show that the statement that $a = 2$ is equivalent to the law of quadratic reciprocity for the prime $p$ and all primes $q \notin \{2, p\}$. (Hint: If $a = 2$, deduce quadratic reciprocity using the fact that one can compute $\Psi_{L/K}(q\mathbb{Z}) = \left(\begin{smallmatrix} p \\ q \end{smallmatrix}\right)$ using Artin's theorem together with the fact that $\Psi_{L/K}$ which does not factor through a ray class group of smaller conductor. Conversely, show that if quadratic reciprocity holds, then one must have $a = 2$ by considering the formula for $\Psi_{L/K}$ which results.)

7. To deduce that $a = 2$ for all $p \equiv 3 \bmod 4$, first show that $a = 2$ when $p = 3$. This can be done by using a small prime $q$ and the connection with the Artin map above. Conclude that to prove quadratic reciprocity for all $p \equiv 3 \bmod 4$ and odd $q \neq p$, it will be enough to consider the case in which neither $p$ or $q$ equals 3.

8. To finish the argument, suppose now that neither $p$ nor $q$ equal 3. Then $3p \equiv 1 \bmod 4$, so the quadratic extension $L' = \mathbb{Q}(\sqrt{3p})$ does not ramify over 2. Use the Artin map for $L'/\mathbb{Q}$ to show that

$$\begin{pmatrix} 3p \\ q \end{pmatrix} = \begin{pmatrix} q \\ 3 \end{pmatrix} \cdot \begin{pmatrix} q \\ p \end{pmatrix}$$

where $\left(\begin{smallmatrix} 3p \\ q \end{smallmatrix}\right)$ is 1 if $3p$ is a square mod $q$ and $-1$ otherwise. Using that $(\mathbb{Z}/q)^*$ is cyclic show that

$$\begin{pmatrix} 3p \\ q \end{pmatrix} = \begin{pmatrix} 3 \\ q \end{pmatrix} \cdot \begin{pmatrix} p \\ q \end{pmatrix}.$$

Use these formulas together with the fact that you have checked quadratic reciprocity when one of the (odd) primes is 3 to complete the proof.