MATH 620: HOMEWORK #2

1. An example of Abhyankhar

This problem is about the example of Shreeram Abhyankhar which Rachel Preis discussed in the Galois theory seminar on September 16, 2009. Let k be a field of characteristic $p > 0$. Let x be an indeterminate, and define $A = k[x]$ and $F = k(x) = \mathrm{Frac}(k[x])$. Suppose s and t are positive integers such that $2 \leq t < p$. Define the polynomial $T(Y) \in F[Y]$ by

$$T(Y) = Y^{p+t} - x^s Y^t + 1.$$

1. Show that $T(Y)$ is separable.

2. Show that to prove $T(Y)$ is irreducible in $F[Y]$, it is enough to prove it is irreducible in $k[x, Y]$. Then show is it enough to prove that $T(Y)$ is irreducible in $k(Y)[x]$.

3. Let $\overline{k}$ be an algebraic closure of k and let $L = \overline{k}(Y)$. Consider the monic polynomial

$$H(x) = -Y^{-t}T(Y) = x^s - (Y^p + Y^{-t})$$

in $L[x]$. Write $s = p^m s'$ for some integer s' prime to p and some $m \geq 0$. Let x_0 be a root of $H(x) = 0$ in algebraic closure $\overline{L}$ of L. Show that field $L(x_0)$ is an inseparable degree p^m extension of $L(x_1)$ when $x_1 = x_0^{p^m}$. Here x_1 is a root of the polynomial

$$x_1^{s'} - (Y^p + Y^{-t}).$$

Show that the roots of this polynomial have the form ζx_1 for some $\zeta \in \overline{k}$ such that $\zeta^{s'} = 1$. Prove that $L(x_1)/L$ is a Galois extension, and that there is an injective homomorphism of finite cyclic groups $\mathrm{Gal}(L(x_1)/L) \to \mu_{s'}(\overline{k})$ defined by $\sigma \to \sigma(x_1)/x_1$, where $\mu_{s'}(\overline{k})$ is the cyclic group of roots of unity of order dividing s' in $\overline{k}$. (This is an instance of Kummer theory.)

4. Deduce from problem #3 that if $d = [L(x_1) : L] = \#\mathrm{Gal}(L(x_1)/L)$ then $x_1^d \in L$ and $d|s'$. Show that then $(Y^p + Y^{-t})$ lies in $(L^*)^{s'/d}$, i.e. that $Y^p + Y^{-t}$ is a $(s'/d)^{th}$ power of an element of $L = \overline{k}(Y)$. Show this implies $Y^{p+ms'} + Y^{ms'-t}$ is then the $(s'/d)^{th}$ power of an element in $\overline{k}[Y]$ if $m \in \mathbb{Z}$ is sufficiently large. Show that this and g.c.d.$(p, s') = 1$ implies $d = s'$. Conclude that in fact, $H(x)$ is irreducible in $L[x]$.

5. Show using problems # 1 - # 4 that $T(Y) = Y^{p+t} - x^s Y^t + 1$ is irreducible in $k(x)[Y]$.

6. Let y_0 be a root of $T(Y) = 0$ in an algebraic closure $\overline{F}$ of $F = k(x) = \mathrm{Frac}(k[x])$. Let A' be the integral closure of $A = k[x]$ in the field $N = F(y_0)$. Consider the basis $\{\omega_i\}_{i=0}^{p+t-1} = \{y_0^i\}_{i=0}^{p+t-1}$ for N over F and the associated dual basis $\{\omega_j^*\}_{j=0}^{p+t-1}$ with respect to the trace $\mathrm{Tr}_{N/F}$. Show that these bases generate the same A-submodule of N. Conclude that A' is the ring $A[y_0]$ and that the trace gives a symmetric non-degenerate pairing

$$\langle\ ,\ \rangle : A' \times A' \to A \quad \text{defined by} \quad \langle \alpha, \beta \rangle = \mathrm{Tr}_{N/F}(\alpha\beta) \tag{1.1}$$

which is perfect, in the sense that if gives rise to an isomorphism of A-modules $A' \to \mathrm{Hom}_A(A', A)$ via $\alpha \to \{\beta \to \langle \alpha, \beta \rangle\}$.

7. Once we discuss discriminants, show that the discriminant ideal $d_{A'/A} \subset A$ of A' over A is A itself. This is equivalent to (1.1) being a perfect pairing.

Interpretation in algebraic geometry: The spectrum $\mathrm{Spec}(A) = \mathrm{Spec}(k[x])$ is an affine line $\mathbb{A}^1_k$. It is the complement of one point ∞ in the projective line $\mathbb{P}^1_k$, and $\mathbb{P}^1_k$ is the smooth projective curve associated to $k(x) = F$. There is a smooth projective curve C over k with function field N, and the inclusion $F \subset N$ corresponds to a morphism $\pi : C \to \mathbb{P}^1_k$. The affine curve $\mathrm{Spec}(A') \subset C$ is the inverse image of $\mathrm{Spec}(A) = \mathbb{A}^1_k$ under π. The statement that $d_{A'/A} = A$ is equivalent to saying that $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ is étale since N/F is separable. Another way to say this is that $\pi : C \to \mathbb{P}^1_k$ is unramified outside of ∞, which is what Rachel said in her talk.

2. Isometry classes of trace forms

Suppose V is a finite dimensional vector space over a field and that

$$\langle\ ,\ \rangle : V \times V \to F$$

is a non-degenerate symmetric pairing. Let $d = \dim_F(V)$.

8. Show that there is a basis $\{w_i\}_{i=1}^d$ for V over F such that $\langle\ ,\ \rangle$ is diagonal with respect to this basis, in the sense that $\langle w_i, w_j\rangle = 0$ if $i \neq j$. (This is a standard result, but it's good to know the proof. Induct on dimension using the orthogonal complement of the space spanned by one non-zero element of V.)

9. Two pairs $(V, \langle\ ,\ \rangle)$ and $(V', \langle\ ,\ \rangle')$ as above are isometric if there is an F-isomorphism $\psi : V \to V'$ of vector spaces which carries $\langle\ ,\ \rangle$ to $\langle\ ,\ \rangle'$, in the sense that

$$\langle \psi(m), \psi(m_0)\rangle' = \langle m, m_0\rangle$$

for all $m, m_0 \in V$. Let

$$d(V, \{w_1, \ldots, w_d\}, \langle\ ,\ \rangle) = \det(\{\langle w_i, w_j\rangle\}_{1\le i,j\le d})$$

be the discriminant of the pairing $\langle\ ,\ \rangle$ on V relative to a basis $\{w_1, \ldots, w_d\}$ of V over F. Show that the class $h_1(V, \langle\ ,\ \rangle)$ of $d(V, \{w_1, \ldots, w_d\}, \langle\ ,\ \rangle)$ in the quotient group $F^*/(F^*)^2$ does not depend on the choice of $\{w_1, \ldots, w_d\}$, and is an invariant of the isometry class of $(V, \langle\ ,\ \rangle)$.

10. Suppose F is any field of characteristic not equal to 2. Let L be a quadratic extension field of F, considered as an F-vector space. Let $\mathrm{Tr}_{L/F} : L \times L \to F$ be the trace pairing. Show that the isometry class of $(L, \mathrm{Tr}_{L/F})$ as a two-dimensional vector space with a quadratic form determines the quadratic extension L/F, in the following sense. If L' is another quadratic extension of F and $(L, \mathrm{Tr}_{L/F})$ is F-isometric to $(L', \mathrm{Tr}_{L'/F})$ then there is an isomorphism of fields $L \to L'$ which is the identity on F.

11. Suppose F is a field of characteristic 2. Is the conclusion of problem #10 true for separable quadratic extensions L of F?

Comments: The class $h_1(V, \langle\ ,\ \rangle)$ is called the first Hasse-Witt invariant of $(V, \langle\ ,\ \rangle)$. There is a higher Hasse Witt invariant $h_i(V, \langle\ ,\ \rangle)$ for each integer $i \ge 2$. The study of these when $(V, \langle , \rangle) = (L, \mathrm{Tr}_{L/\mathbb{Q}})$ for a number field L is an active research area. An excellent book about this is "Cohomological invariants, Witt invariants, and trace forms," by Jean-Pierre Serre, Notes by Skip Garibaldi, Univ. Lecture Ser., 28, Cohomological invariants in Galois cohomology, 1–100, Amer. Math. Soc., Providence, RI, 2003.

3. A counterexample to finiteness of integral closures

The following example is due to Kaplansky. Suppose k is a field of characteristic 2. Let u be an element of the formal power series $k[[x]]$ which is transcendental over $k(x)$. (One can construct u using Liouville's Theorem, as in the first homework assignment! If k is countable, a cheaper but non-explicit construction is to use the fact that $k[[x]]$ is uncountable.) Let F be the subfield $k(x,u^2)$ of $k((x)) = \mathrm{Frac}(k[[x]])$ generated over k by x and u^2. Since u^2 is transcendental over $k(x)$, this F is identified with the field of rational functions in the two indeterminates x and u^2. Define $L = k(x,u) \subset k((x))$. Let $A = F \cap k[[x]]$ and $B = L \cap k[[x]]$.

12. Show L is a quadratic extension of F, and that if $\alpha \in L$ then $\alpha^2 \in F$.

13. Show that $k[[x]]$ is integrally closed in its fraction field $k((x)) = \mathrm{Frac}(k[[x]])$. Here $k((x))$ is the field of all formal Laurent series of the form $\sum_{n=N}^{\infty} a_n x^n$ for some $N \in \mathbb{Z}$ and $a_n \in k$.

14. Show that B is the integral closure of A in L.

15. Suppose that B is finitely generated as an A-module by elements $\{q_i\}_{i=1}^{n}$. Show that each q_i can be written as $a_i + b_i u$ for a unique pair of elements $a_i, b_i \in F$. Using the fact that $k(x) \subset k((x))$, show that there is an integer $m \geq 0$ such that $x^m a_i$ and $x^m b_i$ lie in $k[[x]]$ for all $i = 1, \ldots, n$. Conclude that $x^m B \subset A + Au$.

16. Suppose

$$u = a_0 + a_1 x + a_2 x^2 + \ldots$$

is the power series expansion of $u \in k[[x]]$. With m as in Problem # 15, define

$$v = (u - (a_0 + a_1 x + \ldots + a_m x^m))x^{-(m+1)}.$$

Show that $v \in k[[x]]$ and $v \in L$, so $v \in B$.

17. Deduce from problems #15 and #16 that $x^m v \in A + Au$. Write

$$x^m v = x^{-1}(u - (a_0 + a_1 x + \ldots a_m x^m)) = x^{-1}u - x^{-1}(a_0 + \ldots + a_m x^m)$$

Show this is a contradiction.