MATH 702: HOMEWORK #2

DUE FRIDAY, OCT. 12, 2012 IN TED CHNBURG'S MAILBOX

1. Disjoint extensions with coprime disciminants

This problem generalizes Proposition 17 of Chapter 3 of Lang's "Algebraic Number Theory" book.

Suppose L and N are two finite separable extensions of a field F inside an algebraic closure $\overline{F}$ of F. We will say that L and N are disjoint over F if whenever $\{l_i\}_i$ is a basis for L over F and $\{w_j\}_j$ is a basis for N over F, the set $\{l_i w_j\}_{i,j}$ is a basis for the compositum LN over F.

Let A be a Noetherian subring of F such that $F = \mathrm{Frac}(A)$ and A is integrally closed in F. If T is a field such that $F \subset T \subset LN$, let A_T be the integral closure of A in T, and let $D(A_T/A) \subset A$ be the discriminant ideal of A_T over A. We will use without further comment the fact that if S is a multiplicatively closed subset of A, then $S^{-1}A_T$ is the integral closure of $S^{-1}A$ in T and $D(S^{-1}A_T/S^{-1}A) = S^{-1}D(A_T/A)$.

We will say that A_L and A_N have coprime discriminants over A if for each prime ideal P of A, either

$$(A - P)^{-1}D(A_L/A) = (A - P)^{-1}A = A_P$$

or

$$(A - P)^{-1}D(A_N/A) = (A - P)^{-1}A = A_P.$$

The object of this exercise is to show:

Theorem 1.1. *If L and N are disjoint finite separable extensions of F, and A_L and A_N have coprime discriminants over A, then the integral closure A_{LN} of A in LN is the subring $A_L \cdot A_N$ generated by A_L and A_N.*

1. Show the conclusion of the Theorem will follow if we show

$$(A - P)^{-1}(A_L \cdot A_N) = (A - P)^{-1}A_{LN}$$

for all primes P of A. Explain why we can then reduce to the case in which A is a local ring and either $D(A_L/A) = A$ or $D(A_N/A) = A$.

2. Suppose A is a local ring and that $D(A_N/A) = A$. Recall that $D(A_N/A)$ is the A-ideal generated by all disciminants $D(\{w_j\}_j)$ of bases $\{w_j\}_j$ for N over F such that $\{w_j\}_j \subset A_N$. Show that there is one such basis $\{w_j\}_j$ which spans the same A-module as it's dual basis $\{w_\ell^*\}_\ell$, and that A_N is the direct sum $\oplus_j A w_j$.

3. Show that if $\{w_j\}_j$ is as in problem # 2, then a basis for LN as an L-vector space is given by $\{w_j\}_j$. Use $\{w_\ell^*\}_\ell$ and the trace from LN to L to show that if $\beta = \sum_j \beta_j w_j$ lies in A_{LN} for some $\beta_j \in L$, then $\beta_j \in A_L$. Deduce Theorem 1.1 from this.

4. Show that if L/F and N/F are finite Galois extensions, then L and N are disjoint over F if and only if $L \cap N = F$. Is this still true if we drop the assumption that L/F and N/F are Galois?

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 $d = \dim_F(V)$. 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 proved by induction on dimension using the orthogonal complement of the space spanned by one non-zero element of V.) 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.

5. 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 $(V, \langle\ ,\ \rangle)$.

6. 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.

7. Suppose F is a field of characteristic 2. Is the conclusion of problem #6 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 $i \geq 2$. 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. The Carlitz module

Let p be a prime, $L = \mathbb{F}_p(t)$ and $A = \mathbb{F}_p[t]$. In class we will discuss the Carlitz module defined by the ring homomorphism $\psi : A \to L\{\tau\}$ sending t to $t + \tau$, where $L\{\tau\}$ is the twisted polynomial ring for which $\tau\beta = \beta^p\tau$ for $\beta \in L$. Then $L\{\tau\}$ acts on an algebraic closure $\overline{L}$ of L by letting $\beta \in L$ act by multiplication by β, and by letting τ send $\alpha \in \overline{L}$ to $\tau(\alpha) = \alpha^p$. If $\pi(t) \in A$ is not 0, define the $\pi(t)$-torsion subgroup of $\overline{L}$ by

$$\mu_{\pi(t)} = \{\alpha \in \overline{L} : \psi(\pi(t))(\alpha) = 0\}$$

8. Suppose $\pi(t) \in A = \mathbb{F}_p[t]$ is monic of degree $d \geq 1$ in t. Show that $\mu_{\pi(t)}$ is the set of all roots of a separable polynomial of degree p^d, and that $\mu_{\pi(t)}$ is an additive group.

9. With the notation of problem # 5, show that there is an action of the ring $A/\pi(t)A$ on $\mu_{\pi(t)}$ induced by letting the class of $h(t) \in A$ send $\alpha \in \mu_{\pi(t)}$ to $\psi(h(t))(\alpha)$. Show that this makes $\mu_{\pi(t)}$ into a free rank one module for $A/\pi(t)A$. (To prove freeness, it may be useful to factor $\pi(t)$ into a product of powers of distinct irreducibles $r(t)$ and to consider the size of $\mu_{r(t)} \subset \mu_{\pi(t)}$.)

Comment: This fact corresponds to the statement that multiplicative group of all roots of $x^n - 1$ in $\mathbb{C}$ is a free rank 1 module for the ring $\mathbb{Z}/n$.

10. Suppose $\pi(t)$ is a monic irreducible polynomial of degree d. Let $\alpha \in \mu_{\pi(t)}$ be a generator for $\mu_{\pi(t)}$ as a free rank one module for the field $A/A\pi(t)$. Try showing that the integral closure of $B = \mathbb{F}_p[t]$ in the field $L(\mu_{\pi(t)})$ obtained by adjoining to L all elements of $\mu_{\pi(t)}$ is the ring $B[\alpha]$ generated by B and α. In doing this, it may be useful to construct an analog of the proof that $\mathbb{Z}[\zeta_p]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta_p)$.