Exercise 6, 10/05/2005

**Definition** Let \( L/K \) be a finite separable extension field. The **discriminant** of a \( K \)-basis \( \alpha_1, \ldots, \alpha_n \) of \( L \) is defined to be

\[
d(\alpha_1, \ldots, \alpha_n) := \det (\sigma_i(\alpha_j))^2
\]

where \( \sigma_1, \ldots, \sigma_n \) are the \( K \)-embeddings of \( L \) into \( L^{\text{sep}} \). If \( \alpha \) is an element of \( L \) such that \( L = K(\alpha) \), we define an element \( d(\alpha) \in L \) by

\[
d(\alpha)d_{L/K}(\alpha) := d(1, \alpha, \ldots, \alpha^{n-1})
\]

1. Suppose that \( \mathcal{O}_K \) is a Dedekind domain with fraction field \( K \) and \( \mathcal{O}_L \) is the integral closure of \( \mathcal{O}_K \) in \( L \).

(i) Prove that if \( \alpha_1, \ldots, \alpha_n \) is an \( \mathcal{O}_K \)-basis of \( \mathcal{O}_L \), then \( \text{disc}(\mathcal{O}_L/\mathcal{O}_K) \) as defined in class is equal to the ideal of \( \mathcal{O}_K \) generated by \( d(\alpha_1, \ldots, \alpha_n) \).

(ii) Show that if \( \alpha_1, \ldots, \alpha_n \) are elements of \( \mathcal{O}_L \) and form a \( K \)-basis of \( L \), then there exists an ideal \( I \) in \( \mathcal{O}_L \) such that \( d(\alpha_1, \ldots, \alpha_n)\mathcal{O}_L = I^2 \text{disc}(\mathcal{O}_L/\mathcal{O}_K) \).

2. Notation as above. Let \( \alpha_1, \ldots, \alpha_n \) be elements of \( \mathcal{O}_L \) which form a \( K \)-basis of \( L \). Assume moreover that \( \text{disc}(\mathcal{O}_L/\mathcal{O}_K) = d(\alpha_1, \ldots, \alpha_n)\mathcal{O}_L \). Show that \( \alpha_1, \ldots, \alpha_n \) is a \( \mathcal{O}_K \)-basis of \( \mathcal{O}_L \).

3. Show that if \( L/K \) is a finite extension of number fields, \( \mathcal{D}(L/K) \) is the \( \mathcal{O}_L \)-ideal generated by all elements of the form \( f'(\alpha) \), where \( \alpha \) is an element of \( \mathcal{O}_L \) such that \( K(\alpha) = L \), and \( f(X) \) is the minimal polynomial of \( \alpha \) w.r.t. \( K \).

4. Notation as in Problem 1. Assume that \( \mathcal{O}_K \) is a complete discrete valuation ring and that the residue field extension \( \kappa_L/\kappa \) is separable. Prove that \( \text{disc}(L/K) \) is equal to the ideal of \( \mathcal{O}_L \) generated by elements of the form \( d(\alpha) := d(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \), where \( \alpha \) is an element of \( \mathcal{O}_L \) such that \( K(\alpha) = L \). Notice that \( \mathcal{D}'_{L/K} \subseteq \text{disc}(L/K) \), i.e. the discriminant \( \text{disc}(L/K) \) divides the ideal \( \mathcal{D}'_{L/K} \).

5. Let \( \alpha \) be an element of \( \mathcal{O}_L \) such that \( K(\alpha) = L \). Let \( \mathfrak{p} \) be a prime ideal of \( \mathcal{O}_K \), and let \( \mathfrak{p}_1, \ldots, \mathfrak{p}_r \) be the prime ideals of \( \mathcal{O}_L \) lying above \( \mathfrak{p} \). Let \( n_j = [L_{\mathfrak{p}_j} : K_{\mathfrak{p}}] \), \( j = 1, \ldots, r \). Let \( \alpha_{\mathfrak{p}_1}, \ldots, \alpha_{\mathfrak{p}_r} \) be the image of \( \alpha \) in \( \mathcal{O}_{L_{\mathfrak{p}_1}}, \ldots, \mathcal{O}_{L_{\mathfrak{p}_r}} \), respectively. Let \( \alpha_{\mathfrak{p}_j, 1}, \ldots, \alpha_{\mathfrak{p}_j, n_j} \) be the conjugates of \( \alpha_{\mathfrak{p}_j} \) over \( K_{\mathfrak{p}_j} \), \( j = 1, \ldots, r \). Let \( f_j(X) \) be the minimal polynomial of \( \alpha_{\mathfrak{p}_j} \) over \( K_{\mathfrak{p}_j} \), \( j = 1, \ldots, r \).

(i) For any two primes \( \mathfrak{p}_{j_1} \neq \mathfrak{p}_{j_2} \) above \( \mathfrak{p} \), define an element \( R(\mathfrak{p}_{j_1}, \mathfrak{p}_{j_2}) \in K^{\text{sep}} \) by

\[
R(\mathfrak{p}_{j_1}, \mathfrak{p}_{j_2}) = \prod_{\mu=1}^{n_{j_1}} \prod_{\nu=1}^{n_{j_2}} (\alpha_{\mathfrak{p}_{j_1}, \mu} - \alpha_{\mathfrak{p}_{j_2}, \nu}) = \prod_{\mu=1}^{n_{j_1}} f_{j_2}(\alpha_{\mathfrak{p}_{j_1}, \mu})
\]

Show that \( R(\mathfrak{p}_{j_1}, \mathfrak{p}_{j_2}) \in \mathcal{O}_{K_\mathfrak{p}} \).

(It is the resultant of \( f_{j_1}(X) \) and \( f_{j_2}(X) \).)
(ii) Show that
\[ d_{L/K}(\alpha) = \left( \prod_{j=1}^{r} d_{L_{\mathfrak{q}_j}/K_{\mathfrak{q}_j}}(\alpha_{\mathfrak{q}_j}) \right) \cdot \left( \prod_{j_1 \neq j_2} R(\mathfrak{P}_{j_1}, \mathfrak{P}_{j_2}) \right) \]

6. Let \( q \) be the cardinality of \( \kappa_p \): \( \kappa_p \cong \mathbb{F}_q \). For every positive integer \( f \), define a natural number \( \psi_q(f) \) by
\[ \psi_q(f) = \text{Card} \left\{ x \in \mathbb{F}_q \mid \left[ \mathbb{F}_q(x) : \mathbb{F} \right] = f \right\} \]
(i) Show that
\[ \psi_q(f) = \sum_{d|f} \mu(d)q^{f/d} \]
where the \( \ell^a \geq \ell \) runs through powers of prime numbers \( \ell \) that exactly divide \( f \).
(ii) Show that \( \psi_q(f) \geq q \) for all \( f \geq 1 \).

7. For every natural number \( f \geq 1 \), denote by \( r_p(f) \) the number of prime ideals \( \mathfrak{P} \) among \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) such that \( [\kappa_{\mathfrak{P}} : \kappa_p] = f \).
(i) Show that \( \sum_{j=1}^{r} [\kappa_{\mathfrak{P}_j} : \kappa_p] = \sum_{f=1}^{\infty} r_p(f). \)
(ii) Show that \( r_p(f) \leq \frac{[L:K]}{f} \) for all \( f \geq 1 \).

8. Notation as above.
(i) Prove that \( p \) is prime to \( \mathfrak{d}^L_{L/K} \cdot \text{disc}^{-1}_{L/K} \) if and only if
\[ r_p(f) \leq \frac{\psi_q(f)}{f} \quad \forall f \geq 1. \]
(ii) Show that the condition in (ii) above is satisfied for the prime ideal \( p \) if \( q = \text{Card}(\kappa_p) \geq [L : K] \).

9. Find an example of \( L/K \) such that \( \mathfrak{d}^L_{L/K} \neq \text{disc}_{L/K} \).

Here is an alternative approach.

10. Let \( \kappa \) be a finite field. Let \( R_j = \kappa[X]/P_j \) be a finite set of finite local \( \kappa \)-algebras, \( j = 1, \ldots, m \), where each \( P_j \) is a power of a maximal ideal of \( \kappa[X] \), so that each \( R_j \) can be generated by one element. Let \( R := R_1 \times \cdots \times R_m. \)
(i) Find a necessary and sufficient condition for the existence of an element \( x \in R \) such that \( R = \kappa[x] \).
(ii) Give an example of an algebra \( R \) such that \( R \) cannot be generated by any element in \( R \) as a \( \kappa \)-algebra.
(iii) What happens if \( \kappa \) is an infinite field?

11. Use Problem 9 to give an alternative proof of Problem 8 (i).