Exercise 6, 10/05/2005

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

$$\mathrm{d}(\alpha_1, \dots, \alpha_n) := \det\left(\sigma_i(\alpha_j)\right)^2$$

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

$$\mathrm{d}(\alpha)\mathrm{d}_{L/K}(\alpha) := \mathrm{d}(1, \alpha, \dots, \alpha^{n-1})$$

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 $\alpha_1, \dots, \alpha_n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, then $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$ as defined in class is equal to the ideal of $\mathcal{O}_K$ generated by $\mathrm{d}(\alpha_1, \dots, \alpha_n)$.

   (ii) Show that if $\alpha_1, \dots, \alpha_n$ 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 $\mathrm{d}(\alpha_1, \dots, \alpha_n)\mathcal{O}_L = I^2 \,\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$.

2. Notation as above. Let $\alpha_1, \dots, \alpha_n$ be elements of $\mathcal{O}_L$ which form a K-basis of L. Assume moreover that $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K) = d(\alpha_1, \dots, \alpha_n)\mathcal{O}_L$. Show that $\alpha_1, \dots, \alpha_n$ 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 α is an element of $\mathcal{O}_L$ such that $K(\alpha) = L$, and $f(X)$ is the minimal polynomial of α 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 κ_L/κ is separable. Prove that $\mathrm{disc}(L/K)$ is equal to the ideal of $\mathcal{O}_L$ generated by elements of the form $d(\alpha) := d(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$, where α is an element of $\mathcal{O}_L$ such that $K(\alpha) = L$.

In Problems 5-7, L/K is a finite extension of number fields, and we will study the phenomenon that $\mathrm{disc}(L/K)$ can be strictly bigger than the $\mathcal{O}_L$-ideal $\mathfrak{d}'_{L/K}$ generated by all elements of the form $\mathrm{d}(\alpha) := \mathrm{d}(1, \alpha, \dots, \alpha^{n-1})$, where α is an element of $\mathcal{O}_L$ such that $K(\alpha) = L$. Notice that $\mathfrak{d}'_{L/K} \subseteq \mathrm{disc}(L/K)$, i.e. the discriminant $\mathrm{disc}(L/K)$ divides the ideal $\mathfrak{d}'_{L/K}$.

5. Let α 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 $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be the prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let $n_j = [L_{\mathfrak{P}_j} : K_{\mathfrak{p}}]$, $j = 1, \dots, r$. Let $\alpha_{\mathfrak{P}_1}, \dots, \alpha_{\mathfrak{P}_r}$ be the image of α in $\mathcal{O}_{L,\mathfrak{P}_1}, \dots, \mathcal{O}_{L,\mathfrak{P}_r}$ respectively. Let $\alpha_{\mathfrak{P}_j,1}, \dots, \alpha_{\mathfrak{P}_j,n_j}$ be the conjugates of $\alpha_{\mathfrak{P}_j}$ over $K_{\mathfrak{p}}$, $j = 1, \dots, r$. Let $f_j(X)$ be the minimal polynomial of $\alpha_{\mathfrak{P}_j}$ over $K_{\mathfrak{p}}$, $j = 1, \dots, r$.

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

   $$\mathrm{R}(\mathfrak{P}_{j_1}, \mathfrak{P}_{j_2}) = \prod_{\mu=1}^{n_{j_1}} \prod_{\nu=1}^{n_{j_2}} \left(\alpha_{\mathfrak{P}_{j_1},\mu} - \alpha_{\mathfrak{P}_{j_2},\nu}\right) = \prod_{\mu=1}^{n_{j_1}} f_{j_2}(\alpha_{\mathfrak{P}_{j_1},\mu})$$

   Show that $\mathrm{R}(\mathfrak{P}_{j_1}, \mathfrak{P}_{j_2}) \in \mathcal{O}_{K_{\mathfrak{p}}}$.
   (It is the resultant of $f_{j_1}(X)$ and $f_{j_2}(X)$.)

(ii) Show that

$$\mathrm{d}_{L/K}(\alpha) = \left(\prod_{j=1}^{r} \mathrm{d}_{L_{\mathfrak{P}_j}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}_j})\right) \cdot \left(\prod_{j_1 \neq j_2} \mathrm{R}(\mathfrak{P}_{j_1}, \mathfrak{P}_{j_2})\right)$$

6. Let q be the cardinality of $\kappa_{\mathfrak{p}}$: $\kappa_{\mathfrak{p}} \cong \mathbb{F}_q$. For every positive integer f, define a natural number $\psi_q(f)$ by

$$\psi_q(f) = \mathrm{Card}\left\{x \in \overline{\mathbb{F}_q} \,|\, [\mathbb{F}_q(x) : \mathbb{F}] = f\right\}$$

(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 ℓ 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 $r_{\mathfrak{p}}(f)$ the number of prime ideals $\mathfrak{P}$ among $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ such that $[\kappa_{\mathfrak{P}} : \kappa_{\mathfrak{p}}] = f$.

(i) Show that $\sum_{j=1}^{r} [\kappa_{\mathfrak{P}_j} : \kappa_{\mathfrak{p}}] = \sum_{f=1}^{\infty} r_{\mathfrak{p}}(f) f$.

(ii) Show that $r_{\mathfrak{p}}(f) \leq \frac{[L:K]}{f}$ for all $f \geq 1$.

8. Notation as above.

(i) Prove that $\mathfrak{p}$ is prime to $\mathfrak{d}'_{L/K} \cdot \mathrm{disc}_{L/K}^{-1}$ if and only if

$$r_{\mathfrak{p}}(f) \leq \frac{\psi_q(f)}{f} \qquad \forall\, f \geq 1\,.$$

(ii) Show that the condition in (ii) above is satisfied for the prime ideal $\mathfrak{p}$ if $q = \mathrm{Card}(\kappa_{\mathfrak{p}}) \geq [L : K]$.

9. Find an example of L/K such that $\mathfrak{d}'_{L/K} \neq \mathrm{disc}_{L/K}$.

Here is an alternative approach.

10. Let κ be a finite field. Let $R_j = \kappa[X]/P_j$ be a finite set of finite local κ-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 κ-algebra.

(iii) What happens if κ is an infinite field?

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