Prof. Dr. Salma Kuhlmann Dr. Itay Kaplan

VALUED FIELDS – EXERCISE 10

To be submitted on Wednesday 19.1.2011 by 14:00 in the mailbox.

Definition.

(1) Two valuation rings $\mathsf{O}_1, \mathsf{O}_2 \subseteq \mathsf{K}$ are called *dependent* iff $\mathsf{O}_1 \cdot \mathsf{O}_2 \neq \mathsf{K}$.
(2) A field K of char. $p > 0$ is called *perfect* if $\mathsf{K}^p = \mathsf{K}$.
(3) An irreducible polynomial $f \in \mathsf{K}[X]$ is called *separable* if $f'(X) \neq 0$.
(4) A polynomial is called separable if all its irreducible factors are.
(5) Let $k \subseteq \mathsf{K}$ be fields. An element $x \in \mathsf{K}$ is called separable over k if the minimal polynomial of x is separable over k.
(6) An extension K/k is called separable if every element of K is separable over k.
(7) A field $k \subseteq \mathsf{K}$ is called *separably closed* in K if for every $x \in \mathsf{K}$, if x is separable over k then $x \in k$.

Question 1.
Let R be a Dedekind Domain.

(1) Suppose $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals. Show that the corresponding $\mathfrak{p}_i$-adic valuations are independent.
Hint: Suppose $y \in \mathsf{R}$. You have to show that $1/y \in \mathsf{R}_{\mathfrak{p}_1} \cdot \mathsf{R}_{\mathfrak{p}_2}$. Reduce to the case where $y \in \mathfrak{p}_1 \cdot \mathfrak{p}_2$ (recalling that $\mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2$). Then $(1/y) = \mathfrak{p}_1' \cdot \mathfrak{p}_2' \cdot \mathfrak{p}_3' \dots \cdot \mathfrak{p}_n'$ where $\mathfrak{p}_3, \dots, \mathfrak{p}_n$ are prime ideals of R (recall the notation from Exercise 1 and 2). Show that in general, if $\mathfrak{p}, \mathfrak{q}$ are distinct prime ideals, then $\mathfrak{p}' \subseteq \mathsf{R}_\mathfrak{q}$ and $\mathfrak{q}' \subseteq \mathsf{R}_\mathfrak{p}$ and conclude. (See also the hint to Question 3, clause 3 of Exercise 2).
(2) Recall the approximation theorem from class. Deduce from it the following: Suppose R is a Dedekind Domain, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are distinct prime ideals. Then for any choice of $m_1, \dots, m_n \in \mathbb{Z}$ and $a_1, \dots, a_n \in \mathsf{K}$, there is some $x \in \mathsf{K} := \operatorname{quot}(\mathsf{R})$ such that if $(x - a_i) = \mathfrak{q}_1^{k_1} \dots \mathfrak{q}_l^{k_l}$ is the unique prime factorization (with $k_j \in \mathbb{Z}$) then for some $j \leqslant l$, $\mathfrak{p}_i = \mathfrak{q}_j$ and $k_j \geqslant m_i$.

Question 2.
Let F be a field of characteristic $p > 0$.

(1) Suppose $a \in \mathsf{F}$, but $a^{1/p} \notin \mathsf{F}$. Show that the polynomial $X^p - a$ is irreducible in $\mathsf{F}[X]$.
Hint: Suppose it is reducible. Deduce that for some $l < p$, $a^{l/p} \in \mathsf{F}$. But remember that there is some $c, d \in \mathbb{Z}$ such that $cl + dp = 1$.
(2) Show even more: the polynomial $X^{p^e} - a$ is irreducible in $\mathsf{F}[X]$ for all $e \in \mathbb{N}$.
Hint: use induction on e. For $e = 0$ it is obvious. For $e+1$, let $\mathsf{K} = \mathsf{F}\left(a^{1/p}\right)$. By induction $X^{p^e} - a^{1/p}$ is irreducible in $\mathsf{K}[X]$. So if $X^{p^{e+1}} - a$ is $f \cdot g$, then both f, g are products of $X^{p^e} - a^{1/p}$. This means that after substituting $Y = X^{p^e}$, the polynomial $Y^p - a$ is reducible in $\mathsf{F}[Y]$.
(3) Show that if F is perfect, then every polynomial f over F is separable.
Hint: let f be irreducible. By what you showed in class, if f is not separable, then $f \in \mathsf{F}[X^p]$.

(4) Show that if every polynomial f over F is separable, then F is perfect.

Question 3.

(1) Let $K \subseteq L \subseteq F$ be fields. Suppose that the extensions L/K and F/L are finite. Show that F/K is a separable extension iff L/K and F/L are both separable.
Hint: use the characterization of separable extensions showed in class (a finite extension K/k is separable iff $kK^p = K$).
(2) Let $K \subseteq L$ be fields. Show that if $x_1, \ldots, x_n \in L$ are separable over K, then $K(x_1, \ldots, x_n)$ is separable over K.
(3) Show that if $k \subseteq K$ are fields, and $k_0 = \{x \in K \mid x \text{ is separable over } k\}$ then k_0 is a field, and that it is separably closed in K.
(4) Show (1) without the assumption that the extensions are finite.

Question 4.
Let K be a field. Suppose $f \in K[X]$. Show that f is separable iff $(f, f') = 1$ (where (f, f') is the gcd) iff f has only simple roots (i.e. if $f(a) = 0$ in some field extension, then $(X - a)^2$ does not divide f).