Math 615: Lecture of April 2, 2007

We next prove that, up to non-unique isomorphism, a coefficient ring of mixed characteristic p in which p is nilpotent is determined by its residue class field and and characteristic (the latter is a power of p). However, there is a uniqueness statement about the isomorphism once liftings of a p-base for K are chosen.

Theorem. *Let K, K' be isomorphic fields of characteristic $p > 0$ and let $g : K \to K'$ be the isomorphism. Let (V, pV, K) and (V', pV', K') be two coefficient rings of the same characteristic, $p^n > 0$. We shall also write λ' for the image of $\lambda \in K$ under g. Let Θ be a p-base for K and let $\Theta' = g(\Theta)$ be the corresponding p-base for K'. Let T be a lifting of Θ to V and let T' be a lifting of Θ' to T'. We have an obvious bijection $\widetilde{g} : T \to T'$ such that if $t \in T$ lifts $\theta \in \Theta$ then $\widetilde{g}(t) \in T'$ lifts $\theta' = g(\theta)$. Then $\widetilde{g}$ extends uniquely to an isomorphism of V with V' that lifts $g : K \to K'$.*

Proof. As in the proof of the Theorem on existence of coefficient rings stated on the first page of the Lecture Notes of March 30, we choose $N \geq n - 1$ and let $q = p^N$. For every element $\lambda \in K$ there is a unique element $\rho_\lambda \in V^q$ that maps to $\lambda^q \in K^q$. Similarly, there is a unique element $\rho'_{\lambda'} \in V'^q$ that maps to λ'^q for every $\lambda' \in K'$. If there is an isomorphism $V \cong V'$ as stated, it must map $\rho_\lambda \to \rho'_{\lambda'}$ for every $\lambda \in K$. Said otherwise, we have an obvious bijection $V^q \to V'^q$, and $\widetilde{g}$ must extend it. Just as in the proof of the Theorem on existence of coefficient rings, we can define $S_N = S$ to consist of linear combinations of distinct N-special monomials in T such that every coefficient is in V^q. Then S will map bijectively onto K. We define $S'_N = S' \subseteq V'$ analogously. Since S' maps bijectively onto K', we have an obvious bijection $\widetilde{g} : S \to S'$. We use σ' for the element of S' corresponding to $\sigma \in S$.

Every element $v \in V$ must have the form $\sigma_0 + pv_1$ where σ_0 is the unique element of S that has the same residue as v modulo pV. Continuing this way, as in the proof of the Theorem on existence of coefficient rings, we get a representation

$$v = \sigma_0 + p\sigma_1 + p^2\sigma_2 + \cdots + p^{n-1}\sigma_{n-1}$$

for the element $v \in V$, where the $\sigma_j \in S$. We claim this is unique. Suppose we have another such representation

$$v = \sigma_0^* + p\sigma_1^* + \cdots + p^{n-1}\sigma_{n-1}^*.$$

Suppose that $\sigma_i = \sigma_i^*$ for $i < j$. We want to show that $\sigma_j = \sigma_j^*$ as well. Working in $V/p^{j+1}V$ we have that $\sigma_j p^j = \sigma_{j+1} p^j$, i.e., that $(\sigma_j - \sigma_j^*)$ kills p^j working mod p^{j+1}. By part (a) of the Lemma from p. 3 of the Lecture Notes of March 30 we have that $\sigma_j - \sigma_j^* \in pV$, and so σ_j and σ_j^* represent the same element of $K = V/pV$, and therefore are equal.

Evidently, any isomorphism $V \cong V'$ satisfying the specified conditions must take

$$\sigma_0 + p\sigma_1 + \cdots + p^{n-1}\sigma_{n-1}$$

to

$$\sigma'_0 + p\sigma'_1 + \cdots + p^{n-1}\sigma'_{n-1}.$$

To show that this map really does give an isomorphism of V with V' one shows simultaneously, by induction on j, that addition is preserved in p^jV, and that multiplication is preserved when one multiplies elements in p^hV and p^iV such that $h+i \geq j$. For every element $\lambda \in K$, let σ_λ denote the unique element of S that maps to λ. Note that we may write ρ_λ as σ_λ^q, since σ_λ has residue λ mod pV.

Now,

$$p^j\rho_\lambda\mu + p^j\rho_\eta\mu = p^j(\sigma_\lambda^q + \sigma_\eta^q)\mu = p^j\big((\sigma_\lambda + \sigma_\eta)^q - pG_q(\sigma_\lambda,\, \sigma_\eta)\big),$$

where $G_q(x,\, y) \in \mathbb{Z}[x,\, y]$ is such that $(x+y)^q = x^q + y^q + pG_q(x,\, y)$. Since $\sigma_\lambda + \sigma_\eta$ has residue $\lambda + \eta$ mod pV, we have that $(\sigma_\lambda + \sigma_\eta)^q = \rho_{\lambda+\eta}$, and it follows that

$$p^j\rho_\lambda\mu + p^j\rho_\eta\mu = p^j\rho_{\lambda+\eta}\mu - p^{j+1}G_q(\sigma_\lambda,\, \sigma_\eta)\mu.$$

We have similarly that

$$p^j\rho'_{\lambda'}\mu' + p^j\rho'_{\eta'}\mu' = p^j\rho'_{\lambda'+\eta'}\mu' - p^{j+1}G_q(\sigma'_{\lambda'},\, \sigma'_{\eta'})\mu',$$

and it follows easily that addition is preserved by our map $p^jV \to p^jV'$: note that $p^{j+1}G_q(\sigma_\lambda,\, \sigma_\eta)\mu$ maps to $p^{j+1}G_q(\sigma'_{\lambda'},\, \sigma'_{\eta'})\mu'$ because all terms are multiples of p^{j+1} (the argument here needs that certain multiplications are preserved as well addition).

Once we have that our map preserves addition on terms in p^jV, the fact that it preserves products of pairs of terms from $p^hV \times p^iV$ for $h+i \geq j$ follows from the distributive law, the fact that addition in p^jV is preserved, and the fact that there is a unique way of writing $\mu_1\mu_2$, where μ_1 and μ_2 are monomials in the elements of T with all exponents $\leq q-1$, in the form $\nu^q\mu_3$ where all exponents in μ_3 are $\leq q-1$, and

$$(p^h\rho_\lambda\mu_1)(p^i\rho_\eta\mu_2) = p^{h+i}(\sigma_\lambda\sigma_\eta\nu)^q\mu_3$$

in V, while

$$(p^h\rho'_{\lambda'}\mu'_1)(p^i\rho'_{\eta'}\mu'_2) = p^{h+i}(\sigma'_{\lambda'}\sigma'_{\eta'}\nu')^q\mu'_3$$

in V'. $\square$

Theorem. *Let K be a field of characteristic $p > 0$. Then there exists a complete Noetherian valuation domain $(V,\, pV,\, K)$ with residue class field K.*

Proof. It suffices to prove that there exists a Noetherian valuation domain $(V,\, pV,\, K)$: its completion will then be complete with the required properties. Choose a well-ordering of K in which 0 is the first element. We construct, by transfinite induction, a direct limit system of Noetherian valuation domains $\{V_\lambda,\, pV_\lambda,\, K_\lambda\}$ indexed by the well-ordered set K and injections $K_a \hookrightarrow K$ such that

(1) $K_0 \cong \mathbb{Z}/p\mathbb{Z}$

(2) The image of K_λ in K contains a.

(3) The diagrams

$$\begin{array}{ccccc} V_{\lambda'} & \twoheadrightarrow & K_{\lambda'} & \hookrightarrow & K \\ \uparrow & & \uparrow & & || \\ V_\lambda & \twoheadrightarrow & K_\lambda & \hookrightarrow & K \end{array}$$

commute for all $\lambda \le \lambda' \in K$.

Note the given a direct limit system of Noetherian valuation domains and injective local maps such that the same element, say, t (in our case $t = p$) generates all of their maximal ideals, the direct limit, which may be thought of as a directed union, of all of them is a Noetherian discrete valuation domain such that t generates the maximal ideal, and such that the residue class field is the directed union of the residue class fields. Every element of any of these rings not divisible by t is a unit (even in that ring): thus, if W is the directed union, pW is the unique maximal ideal. Every nonzero element of the union is a power of t times a unit, since that is true in any of the valuation domains that contain it, and it follows that every nonzero ideal is generated by the smallest power of p that it contains. The statement about residue class fields is then quite straightforward.

Once we have a direct limit system as described, the direct limit will be a discrete Noetherian valuation domain in which p generates the maximal ideal and the residue class field is isomorphic with K.

It will therefore suffice to construct the direct limit system.

We may take $V_0 = \mathbb{Z}_P$ where $P = p\mathbb{Z}$. We next consider an element $\lambda' \in K$ which is the immediate successor of $\lambda \in K$. We have a Noetherian discrete valuation domain $(V_\lambda,\, pV_\lambda,\, K_\lambda)$ and an embedding $K_\lambda \hookrightarrow K$. We want to enlarge V_λ suitably to form $V_{\lambda'}$. If λ' is transcendental over K_λ we simply let $V_{\lambda'}$ be the localization of the polynomial ring $V_\lambda[x]$ in one variable over V_λ at the expansion of pV_λ: the residue class field may be identified with $K_\lambda(x)$, and the embedding of $K_\lambda \hookrightarrow K$ may be extended to the simple transcendental extension $K_\lambda(x)$ so that x maps to $\lambda' \in K$.

If λ' is already in the image of K_λ we may take $V_{\lambda'} = V_\lambda$. If instead λ' is algebraic over the image of K_λ, but not in the image, then it satisfies a minimal monic polynomial

$g = g(x)$ of degree at least 2 with coefficients in the image of K_λ. Lift the coefficients to V_λ so as to obtain a monic polynomial $G = G(x)$ of the same degree over V_λ. We shall show that $V_{\lambda'} = V_\lambda[x]/\bigl(G(x)\bigr)$ has the required properties. If G were reducible over the fraction field of V_λ, by Gauss' Lemma it would be reducible over V_λ, and then g would be reducible over the image of K_λ in K. If follows that $\bigl(G(x)\bigr)$ is prime in $V_\lambda[x]$ and so $V_{\lambda'}$ is a domain that is a module-finite extension of V_λ. Consider a maximal ideal m of $V_{\lambda'}$. Then the chain $m \supset (0)$ in V_b lies over a chain of distinct primes in V_λ: since V_λ has only two distinct primes, we see that m lies over pV_λ and so $p \in m$. But

$$V_{\lambda'}/pV_{\lambda'} \cong \mathrm{Im}\,(K_\lambda)[x]/g(x) \cong \mathrm{Im}\,(K_\lambda)[\lambda'],$$

and so p must generate a unique maximal ideal in $V_{\lambda'}$, and the residue class field behaves as we require as well.

Finally, if λ' is a limit ordinal, we first take the direct limit of the system of Noetherian discrete valuation domains indexed by the predecessors of λ', and then enlarge this ring as in the preceding paragraph so that the image of its residue class field contains λ'. □

Corollary. *If p is a positive prime integer and K is field of characteristic p, there is, up to isomorphism, a unique coefficient ring of characteristic $p > 0$ with residue class field K and characteristic p^t, and it has the form V/p^tV, where (V, pV, K) is a Noetherian discrete valuation domain.*

Proof. By the preceding Theorem, we can construct V so that it has residue field K. Then V/p^tV is a coefficient ring with residue class field K of characteristic p, and we already know that such all rings are isomorphic, which establishes the uniqueness statement. □

Corollary. *Let p be a positive prime integer, K a field of characteristic p, and suppose that $(V,\, pV,\, K)$ and $(W,\, pW,\, K)$ are complete Noetherian discrete valuation domains with residue class field K. Fix a p-base Θ for K. Let T be a lifting of Θ to V and T' a lifting to W. Then there is a unique isomorphism of V with W that maps each element of T to the element with the same residue in Θ in T'.*

Proof. By our results for the case where the maximal ideal is nilpotent, we get a unique such isomorphism $V/p^nV \cong W/p^nW$ for every n, and this gives an isomorphism of the inverse limit systems

$$V/pV \twoheadleftarrow V/p^2V \twoheadleftarrow \cdots \twoheadleftarrow V/p^nV \twoheadleftarrow \cdots$$

and

$$W/pW \twoheadleftarrow W/p^2W \twoheadleftarrow \cdots \twoheadleftarrow W/p^nW \twoheadleftarrow \cdots$$

that takes the image of T in each V/p^nV to the image of T' in the corresponding W/p^nW. This induces an isomorphism of the inverse limits, which are V and W, respectively. □