PREPUBLICACIONES DEL DEPARTAMENTO DE ÁLGEBRA
DE LA UNIVERSIDAD DE SEVILLA

On Kummer extensions of the power series field

José M. Tornero

Prepublicación nº 13 (4-Octubre-2001)

Departamento de Álgebra. Universidad de Sevilla

1 Terminology and notation

Let k be an algebraically closed field, $X_1, ..., X_r$ indeterminates formally independent over k, and let K and L_m be the fields

$$K = k\left((X_1, ..., X_r)\right), \quad L_m = k\left(\left(X_1^{1/m}, ..., X_r^{1/m}\right)\right),$$

where m is a non negative integer, not divisible by the characteristic of k.

The extension $K \subset L_m$ is trivially normal, finite and separable, its Galois group being $G \simeq (C_m)^r$, where C_m stands for the cyclic group of m elements. The elements of G will be noted

$$\begin{array}{rcl}(a_1, ..., a_r) : L_m & \longrightarrow & L_m, \quad 0 \leq a_i < m \\ X_l & \longmapsto & \omega^{a_l} X_l\end{array}$$

where $\omega \in k$ is an m–th primitive root of the unity.

Let R and S_m be the rings

$$R = k\left[[X_1, ..., X_r]\right], \quad S_m = k\left[\left[X_1^{1/m}, ..., X_r^{1/m}\right]\right].$$

The elements of S_m will be called *Puiseux power series*.

Our field of study will be Kummer extensions of K. In order to do that, recall ([1]) that a *Kummer extension* of exponent n of a field F (which must containing a primitive n–th root of the unity and hence its characteristic cannot divide n), is the splitting field of a polynomial

$$\left(Z^n - \alpha_1\right) ... \left(Z^n - \alpha_q\right), \text{ with } \alpha_1, ..., \alpha_q \in F.$$

Our purpose is to prove the following result:

Theorem.– Let $K \subset K'$ be an algebraic separable extension. Then the following conditions are equivalent:

(a) K' a Kummer extension.

(b) K' can be generated by a set of monomials lying in some S_m.

(c) There exists a Puiseux power series $\zeta \in S_m$ such that $K' = K[\zeta]$.

It becomes obvious that all separable extensions of K generated by monomials lying in some S_m are Kummer extensions; that proves (b) $\Rightarrow$ (a). Using the primitive element theorem, as k must be infinite, we can find a Puiseux power series which suffices for generating these extensions (that is, (b) $\Rightarrow$ (c)). In the next sections, we will prove the remaining results.

2 Characteristic exponents of a Puiseux power series

If $\zeta \in S_m$ is written as

$$\zeta = \sum c_{i_1 ... i_r} X_1^{i_1/m} ... X_r^{i_r/m}, \; c_{i_1 ... i_r} \in k,$$

then the set

$$\Delta(\zeta) = \{(i_1, ..., i_r) \mid c_{i_1 ... i_r} \neq 0\} \subset \mathbf{N}^r$$

will be called (a bit carelessly) the *set of exponents* of ζ.

Definition.– Given $\zeta \in S_m$, a finite subset

$$\left\{\left(i_1^{(1)}, ..., i_r^{(1)}\right), ..., \left(i_1^{(s)}, ..., i_r^{(s)}\right)\right\} \subset \Delta(\zeta)$$

will be called a *set of characteristic exponents* of ζ if

$$K(\zeta) = K\left(X_1^{i_1^{(1)}/m} ... X_r^{i_r^{(1)}/m}, ..., X_1^{i_1^{(s)}/m} ... X_r^{i_r^{(s)}/m}\right).$$

In order to prove that all separable extensions of K generated by a Puiseux power series are Kummer extensions ((c) $\Rightarrow$ (a)), it suffices to check that all Puiseux power series in S_m, where m is not divisible by $\mathrm{ch}(k)$, possess a set of characteristic exponents.

We will describe here a process for obtaining such a set for a given series $\zeta \in S_m$. First of all we fix a total ordering in $\mathbf{N}^r$, say $\prec$, and assume that m is the minimal denominator for ζ (that is, $\zeta \notin S_q$ for all $q < m$).

For a given matrix A of t rows and u columns, whose elements are integers, we will write

$$(l)\,\gcd(A) = \gcd\left(\text{minors of order } l \text{ in } A\right),$$

for all $l = 1, ..., \min\{t, u\}$.

Step 1.– Consider the $r \times r$ matrix

$$M_0 = \begin{pmatrix} m & 0 & ... & 0 \\ 0 & m & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & m \end{pmatrix},$$

which obviously verifies $(r)\,\gcd(M_0) = m^r$.

Step 2.– Define the sets $\Delta_0 = \Delta(\zeta)$ and

$$\Delta_0' = \left\{ (i_1, ..., i_r) \in \Delta_0 \;\middle|\; (r)\,\gcd(M_0) = (r)\,\gcd\left(\left.\begin{array}{c|c} M_0 & \begin{matrix} i_1 \\ \vdots \\ i_r \end{matrix} \end{array}\right.\right) \right\}.$$

(These exponents are trivially those representing monomials of ζ which lie in R).

Step 3.– Write $\Delta_1 = \Delta_0 \setminus \Delta_0'$, define the first distinguished pair by

$$\left(i_1^{(1)}, ..., i_r^{(1)}\right) = \min_{\prec}\left(\Delta_1\right);$$

and consider the matrix

$$M_1 = \left(\begin{array}{c|c} M_0 & \begin{matrix} i_1^{(1)} \\ \vdots \\ i_r^{(1)} \end{matrix} \end{array}\right).$$

Step 4.– Once the distinguished pairs

$$\left(i_1^{(1)}, ..., i_r^{(1)}\right), ..., \left(i_1^{(l)}, ..., i_r^{(l)}\right),$$

the set Δ_l and the matrix M_l are defined, consider

$$\Delta_l' = \left\{ (i_1, ..., i_r) \in \Delta_l \;\middle|\; (r)\,\gcd(M_l) = (r)\,\gcd\left(\left.\begin{array}{c|c} M_l & \begin{matrix} i_1 \\ \vdots \\ i_r \end{matrix} \end{array}\right.\right) \right\}.$$

Step 5.– Write $\Delta_{l+1} = \Delta_l \setminus \Delta_l'$, define the $(l+1)$–th distinguished pair by

$$\left(i_1^{(l+1)}, ..., i_r^{(l+1)}\right) = \min_{\prec}\left(\Delta_{l+1}\right);$$

and consider the matrix

$$M_{l+1} = \left(\begin{array}{c|c} M_l & \begin{matrix} i_1^{(l+1)} \\ \vdots \\ i_r^{(l+1)} \end{matrix} \end{array}\right).$$

Remark.– The previous procedure must give a finite number of distinguished pairs, as for every $l > 0$ we have

$$(r)\,\gcd\left(M_{l-1}\right) > (r)\,\gcd\left(M_l\right),$$

so we must end up with a finite set

$$P = \left\{ \left(i_1^{(1)}, ..., i_r^{(1)}\right), ..., \left(i_1^{(s)}, ..., i_r^{(s)}\right) \right\}.$$

From now on we will write for short

$$K[P] = K\left[X_1^{i_i^{(l)}} ... X_r^{i_r^{(l)}} \mid l = 1, ..., s \right].$$

Now $K[P] \subset K[\zeta]$, as every element of G leaving ζ fixed, does so with the monomials having exponents in P. So, for proving that P is a set of characteristic monomials, it suffices proving the following result:

Proposition.– Let there be

$$P_1 = \left\{ X_1^{j_1^{(1)}/m} ... X_r^{j_r^{(1)}/m}, ..., X_1^{j_1^{(t)}/m} ... X_r^{j_r^{(t)}/m} \right\},$$

$$P_2 = P_1 \cup \left\{ X_1^{j_1^{(t+1)}/m} ... X_r^{j_r^{(t+1)}/m} \right\}$$

two sets of monomials in S_m (not in any S_q, with $q < m$), such that

$$(r) \gcd(M_1) = (r) \gcd(M_2),$$

where

$$M_1 = \begin{pmatrix} m & ... & 0 & j_1^{(1)} & ... & j_1^{(t)} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & ... & m & j_r^{(1)} & ... & j_r^{(t)} \end{pmatrix},$$

$$M_2 = \begin{pmatrix} m & ... & 0 & j_1^{(1)} & ... & j_1^{(t)} & j_1^{(t+1)} \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ 0 & ... & m & j_r^{(1)} & ... & j_r^{(t)} & j_r^{(t+1)} \end{pmatrix}.$$

Then $K[P_1] = K[P_2]$.

Proof.– The point is proving $K[P_1] \supset K[P_2]$ and, for this, it is necessary and sufficient showing that, if we call $G_k = \mathrm{Gal}(L_m / K[P_l])$, for $l = 1, 2$; then $G_1 = G_2$.

Define the set

$$H_1 = \left\{ (i_1, ..., i_r) \in (\mathbf{Z}/\mathbf{Z}m)^r \,\middle|\, X_1^{i_1/m} ... X_r^{i_r/m} \in K[P_1] \right\}.$$

So, H_1 contains, up to multiples of m in all coordinates, those monomials which remain fixed by the elements of G_1. Writing up these elements in the form $(a_1, ..., a_r)$ it means that

$$(i_1, ..., i_r) \in H_1 \iff \sum_{l=1}^{r} a_l i_l = 0 \pmod m, \ \forall (a_1, ..., a_r) \in G_1,$$

and also, in particular,

$$H_1 = \left\langle \left(j_1^{(1)}, ..., j_r^{(1)} \right), ..., \left(j_1^{(t)}, ..., j_r^{(t)} \right) \right\rangle.$$

Therefore H_1 is clearly a subgroup of G (non–canonically identified with $(\mathbf{Z}/\mathbf{Z}m)^r$), but it also admits another interpretation. In fact,

$$H_1 \simeq \mathrm{Hom}(G/G_1, \mathbf{Z}/\mathbf{Z}m),$$

identifying $(i_1, ..., i_r) \in H_1$ with

$$\begin{aligned} f_{(i_1,...,i_r)} : G/G_1 &\longrightarrow \mathbf{Z}/\mathbf{Z}m \\ (x_1, ..., x_r) + G_1 &\longmapsto \sum_{l=1}^{r} x_l i_l \end{aligned}$$

As G is the direct sum of r cyclic groups of order m, we have that G/G_1 can be written up as

$$G/G_1 = C_{a_1} \oplus ... \oplus C_{a_c}, \text{ where } a_l | m, \ \forall l = 1, ..., c.$$

This leads to

$$H_1 \simeq \mathrm{Hom}(G/G_1, \mathbf{Z}/\mathbf{Z}m) \simeq \bigoplus_{l=1}^{c} \mathrm{Hom}(C_{a_l}, \mathbf{Z}/\mathbf{Z}m) \simeq \bigoplus_{l=1}^{c} C_{a_l} \simeq G/G_1,$$

as $a_l | m$, for all l.

On the other hand $|G/G_1|$ (that is, $[K[P_1] : K]$), is precisely $|H_1|$ and hence,

$$|G_1| = |G/H_1|.$$

Let us calculate $|G/H_1|$. First of all, instead of writing the group as

$$(\mathbf{Z}/\mathbf{Z}m)^r/\left\langle \left(j_1^{(1)},...,j_r^{(1)}\right),...,\left(j_1^{(t)},...,j_r^{(t)}\right)\right\rangle,$$

we will do it as $\mathbf{Z}^r/\widehat{H_1}$, where

$$\widehat{H_1}=\left\langle (m,0,...,0),...,(0,0,...,m),\left(j_1^{(1)},...,j_r^{(1)}\right),...,\left(j_1^{(t)},...,j_r^{(t)}\right)\right\rangle.$$

Let us write φ a generic element of $\mathrm{Hom}(\mathbf{Z}^r,\mathbf{Q}/\mathbf{Z})$ with $\widehat{H_1}\subset\ker(\varphi)$, and $\tilde{\varphi}$ its factorization through $\mathbf{Z}^r/\widehat{H_1}$. According to ([2], prop. 8);

$$\mathbf{Z}^r/\widehat{H_1}\simeq \mathrm{Hom}\left(\mathbf{Z}^r/\widehat{H_1},\mathbf{Q}/\mathbf{Z}\right),$$

and each of these morphisms is characterized by the images of the canonical generating set of $\mathbf{Z}^r/\widehat{H_1}$, say

$$\alpha_l=\tilde{\varphi}\left(e_l+\widehat{H_1}\right),$$

where e_l stands for the l–th element of the canonical basis of $\mathbf{Z}^r$.

But $\widehat{H_1}\subset\ker(\varphi)$ is equivalent to

$$(\alpha_1\ \ ...\ \ \alpha_r)\begin{pmatrix} m & ... & 0 & j_1^{(1)} & ... & j_1^{(t)}\\ \vdots & \ddots & \vdots & \vdots & & \vdots\\ 0 & ... & m & j_r^{(1)} & ... & j_r^{(t)}\end{pmatrix}=(0\ ...\ 0).$$

Again by [2] (cor. 1) we can find some linear forms $L_1,...,L_r$ with coefficients on $\mathbf{Z}$ such that the previous relations are equivalent to

$$(L_1(\alpha_1,...\alpha_r)\ \ \ldots\ \ L_r(\alpha_1,...\alpha_r))\begin{pmatrix}\eta_1 & ... & 0 & 0 & ... & 0\\ \vdots & \ddots & \vdots & \vdots & & \vdots\\ 0 & ... & \eta_r & 0 & ... & 0\end{pmatrix}=(0\ ...\ 0),$$

where $\eta_1=(1)\gcd(M_1)=1$ and $\eta_1...\eta_l=(l)\gcd(M_1)$. Therefore, as this equality must hold in $\mathbf{Q}/\mathbf{Z}$, it is plain that there are exactly $(r)\gcd(M_1)$ different morphisms in $\mathrm{Hom}\left(\mathbf{Z}^r/\widehat{H_1},\mathbf{Q}/\mathbf{Z}\right)$, hence

$$|G_1|=\frac{m^r}{|H_1|}=\frac{m^2}{m^2/(r)\gcd(M_1)}=(r)\gcd(M_1).$$

Doing exactly the same with G_2 we find

$$|G_2|=(r)\gcd(M_2)=(r)\gcd(M_1)=|G_1|.$$

This finishes the proof.

Corollary.– If $\zeta\in S_m$, having a set of charactersitic exponents

$$P=\left\{\left(i_1^{(1)},...,i_r^{(1)}\right),...,\left(i_1^{(s)},...,i_r^{(s)}\right)\right\}\subset\Delta(\zeta),$$

then

$$\Delta(\zeta)\subset\sum_{l=i}^{s}\mathbf{Z}\left(i_1^{(l)},...,i_r^{(l)}\right),\ \ \mathrm{mod}\ \mathbf{Z}m\times...\times\mathbf{Z}m$$

Remark.– This process enables to compute two well–known (sets of) arithmetic data which are most useful in Algebraic Geometry, as are the Puiseux pairs of a plane curve ([5]) and the characteristic pairs of a quasi–ordinary surface ([3]) (both of them for $k=\mathbf{C}$).

We will do the Puiseux pairs case. So, assume we have a plane algebroid curve given by $f(X,Y)\in\mathbf{C}[[X,Y]]$ and a Puiseux branch, which can always be represented (up to a change of variables) as

$$\begin{aligned}Y=\zeta\left(X^{1/m}\right) &= c_{\beta_1}X^{\beta_1/m}+\sum_{l=1}^{h_1}c_{\beta_1+le_1}X^{(\beta_1+le_1)/m}+\ ...\\ &\ ...\ +c_{\beta_g}X^{\beta_g/m}+\sum_{l=1}^{\infty}c_{\beta_g+le_g}X^{(\beta_g+le_g)/m},\end{aligned}$$

where we can assume $m < \beta_1 < ... < \beta_g$, $\beta_k \notin \mathbf{Z}m$ for all $k = 1, ..., g$ and, in addition, if we call

$$\beta_1 = p_1 e_1,\ m = q_1 e_1,\ \gcd(p_1, q_1) = 1$$

$$e_{l-1} = q_l e_l,\ \beta_l = p_l e_l,\ \gcd(p_l, q_l) = 1;\ \ \forall\, l = 2, ..., g,$$

then the pairs $(p_1, q_1), ..., (p_g, q_g)$ are called the *Puiseux pairs* of the curve. Note that these pairs are determined (and they determine as well) by the set

$$\{m, \beta_1, ..., \beta_g\},$$

called by Zariski the *characteristic of the branch* ζ. Also is direct from the formulae above that

$$e_1 = \gcd(m, \beta_1),\ \ e_l = \gcd(e_{l-1}, \beta_l),\ \ \forall\, l = 2, ..., g.$$

If we apply our process to the set of exponents on $\Delta(\zeta)$ using, for instance, the natural ordering on $\mathbf{N}$, we start up with

$$M_0 = (m)$$

and then choose the smaller element on Δ, that is, β_1, which, by the above conditions, happens to verify $\gcd(m, \beta_1) < m$, so $i^{(1)} = \beta_1$.

Assume we have already computed the first l characteristic exponents, which coincide with $\beta_1, ..., \beta_l$ (necessarily in this order because of our choosing of the ordering on $\mathbf{Z}$). Then we have the matrix

$$M_l = (m\ \ \beta_1\ \ ...\ \ \beta_l),$$

and $\gcd(m, \beta_1, ..., \beta_l) = e_l$, by the above considerations. We have discarded in previous steps those monomials which can be written as a combination of some β_t and e_t, for $t < l$. In the same way, then, we discard now those elements in Δ which do not make smaller the previous gcd, which are, precisely, those which can be written up as a combination of β_l and e_l.

By definition of β_{l+1}, it has to be the minimal element not yet discarded, and this proves that our procedure must end up computing the set $\{\beta_1, ..., \beta_g\}$.

The quasi–ordinary surface case is similar; in fact there are no substantial differences between the two cases. Only the point that the chosen total ordering must be graded should be taken into account, as the characteristic monomials of a quasi–ordinary branch ζ (up to normalization) are determined by the following facts ([3]):

(1) They are the minimal elements of $\Delta(\zeta)$ for the natural partial order.

(2) They generate (irredundantly) the same extension field than the branch itself.

3 Monomials generating Kummer extensions

It only remains proving that all Kummer extensions can be generated by a set of monomials of S_m (that is, (a) $\Rightarrow$ (b)). In order to do that observe first that we can reduce the problem to that of the splitting field of a polynomial $F(Z) = Z^n - \zeta$, where $\zeta \in R$.

We will do the proof by induction on r, being the case $r = 1$ direct from the so–called Newton–Puiseux Theorem. So assume that, for all $\eta \in R$, there exist some $m \in \mathbf{N}$ and a set of monomials $\{M_1, ..., M_s\} \subset S_m$ such that

$$K[\sqrt[n]{\eta}] = K[M_1, ..., M_s];$$

and fix a power series

$$\zeta = \sum_{l=0}^{\infty} a_{\lambda_l}(X_1, ..., X_r) X_{r+1}^{\lambda_l},$$

with $a_{\lambda_l} \in R$ and $\lambda_0 < \lambda_1 < ...$ for all l.

Then the term with minimal degree on X_{r+1} of a $\sqrt[n]{\zeta}$, must be of the form $c_{\lambda_0/n} X_{r+1}^{\lambda_0/n}$, where it must hold

$$c_{\lambda_0/n}^n = a_{\lambda_0}.$$

So there must be a set of monomials $\{M_1, ..., M_s\} \subset S_m$ such that

$$K[\sqrt[n]{a_{\lambda_0}}] = K[c_{\lambda_0/n}] = K[M_1, ..., M_s].$$

Now, in the same way, the following term with minimal degree on X_{r+1} of a $\sqrt[n]{\zeta}$, must be of the form

$$c_{\lambda_1 - [\lambda_0(n-1)/n]} X_{r+1}^{\lambda_1 - [\lambda_0(n-1)/n]},$$

where it must hold now

$$nc_{\lambda_1-[\lambda_0(n-1)/n]}c_{\lambda_0/n}^{\lambda_0(n-1)/n} = a_{\lambda_1},$$

and hence

$$c_{\lambda_1-[\lambda_0(n-1)/n]} \in K\left[M_1, ..., M_s\right].$$

Following this, it is easy to check that an n-th root of ζ (in fact, all of them) lies in $K\left[M_1, ...M_s\right]\left[\left[X_{r+1}^{\alpha/n}\right]\right]$, where

$$\alpha = \gcd\left\{\lambda_0, n\lambda_1 - \lambda_0(n-1), ..., n\lambda_l - \lambda_0(n-1), ...\right\}.$$

In particular

$$\sqrt[n]{\zeta} \in k\left(\left(X_1, ..., X_{r+1}\right)\right)\left[M_1X_{r+1}^{\alpha/n}, ..., M_sX_{r+1}^{\alpha/n}\right].$$

Then it only remains proving that an extension which can be embedded into another one generated by monomials with rational exponents can be generated by monomials itself. This is straightforward, as we can choose a primitive element which is a Puiseux power series, hence the extension can be generated by monomials.

4 Final comments

All the arguments given here can be completely translated word–by–word to the analytic context. We hope that this work will be useful as a step to understand the geometry of algebroid (analytic) hypersurfaces which admit a Puiseux–like parametrization. In fact, characteristic exponents have proved to be a useful tool for the surface case (characteristic 0), as shown in [4]. This promising results have led us to expect that some deeper application of class field theory tools may help to the study of the geometry and the topology of these varieties.

References

[1] Artin, E. (1959). *Galois theory*. Notre Dame Mathematical Lectures, 2. University of Notre Dame Press, 1959.

[2] Bourbaki, N. (1959). *Algèbre. Ch. VII: Modules sur les anneaux principaux*. Actualités Sci. Ind., 1179. Hermann, 1959.

[3] Lipman, J. (1965). *Quasi–ordinary singularities of embedded surfaces*. Ph. D. Thesis, Harvard University.

[4] Tornero, J.M. (2001). *Aspectos locales de singularidades de superficies: Superificies de Puiseux*. Ph. D. Thesis, University of Sevilla.

[5] Zariski, O. (1965). "Studies in equisingularity I", *Amer. J. Math.* 87, 507–536.