Automorphisms of Power Series Rings

Daniel Murfet

July 9, 2005

Let k be a field. We have seen earlier that if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(k)$ is an invertible 2×2 matrix over k then $\varphi : k[x, y] \longrightarrow k[x, y]$ defined by

$$\varphi(x) = ax + by, \quad \varphi(y) = cx + dy$$

is an automorphism of k-algebras, and this extends to polynomial rings over any number of variables. We wish to establish an analgous result for power series rings.

From our Analytic Independence notes (p.85 of our A&M notes) we know that if $a_1, \dots, a_n \in k[[x_1, \dots, x_n]]$ are power series with no constant term (i.e. not units) then there is a unique continuous morphism of k-algebras $\varphi : k[[x_1, \dots, x_n]] \longrightarrow k[[x_1, \dots, x_n]]$ with $\varphi(x_i) = a_i$ for $1 \le i \le n$. If $f(x_1, \dots, x_n)$ is a power series then we denote $\varphi(f)$ by $f(a_1, \dots, a_n)$.

Let $\mathfrak{m} = (x)$ be the unique maximal ideal in $k[[x]]$ and consider the power series $u(x) \in k[[x]]$ defined by

$$u = x + x^2 + x^3 + x^4 + \dots + x^n + \dots$$

Put $g(x) = x^2 + x^3 + \dots$ so $u \in \mathfrak{m}, g \in \mathfrak{m}^2$ and $u = x + g(x)$. Notice that $x = u - g$ and $g = xu$ so that $x = (1 - x)u$. We can use this fact to gradually replace the xs in $g(x)$ with us until we have $x = h(u)$ for some power series h:

$$\begin{aligned} x &= u - ux \\ &= u - u(u - ux) \\ &= u - u^2 + u^2 x = u - u^2 + u^2(u - ux) \\ &= u - u^2 + u^3 - u^3 x \end{aligned}$$

This suggests that $x = u - u^2 + u^3 - u^4 + \dots + (-1)^{n+1}u^n + \dots$ and one can check directly that this is the case. If we let $h(x)$ be the power series $x - x^2 + x^3 - x^4 + \dots$ then we have $x = h(u)$ as required.

A similar technique works in the general case:

Proposition 1. *Let $u(x) = u_1 x + u_2 x^2 + \dots$ be a power series with $u_1 \neq 0$. Then there is a power series $h(x) \in k[[x]]$ with $x = h(u)$.*

Proof. First we prove the following claim by induction: For each $n \ge 1$ there is a polynomial $h_n(x) \in k[x]$ of degree $\le n$ and a power series $b_n(x) \in \mathfrak{m}^{n+1}$ with $x = h_n(u) + b_n(x)$. Since

$$x = \frac{1}{u_1}(u - g)$$

where $g(x) = u_2 x^2 + u_3 x^3 + \dots$ this is trivial for $n = 1$. Suppose it is true for $n \ge 1$ and let $x = h_n(u) + b_n(x)$. We can then write

$$\begin{aligned} x &= h_n(u) + b_{n,1}x^{n+1} + b_{n,2}x^{n+2} + \dots \\ &= h_n(u) + b_{n,1}\left(\frac{1}{u_1}u - \frac{1}{u_1}g(x)\right)^{n+1} + b_{n,2}x^{n+2} + \dots \\ &= h_n(u) + b_{n,1}\left(\frac{1}{u_1}\right)^{n+1} u^{n+1} + b_{n+1}(x) \\ &= h_{n+1}(u) + b_{n+1}(x) \end{aligned}$$

where $b_{n+1}(x)$ belongs to $\mathfrak{m}^{n+2}$ since $g \in \mathfrak{m}^2$ and $u \in \mathfrak{m}$. Notice that the sequence $h_1(x), h_2(x), \ldots$ is a Cauchy sequence in $k[[x]]$ and hence converges to some power series $h(x) \in k[[x]]$. For each $n \geq 1$ write $h(x) = h_n(x) + h_{>n}(x)$ and note that

$$h(u) = h_n(u) + h_{>n}(u) = x - b_n(x) + h_{>n}(u)$$

But $-b_n(x) + h_{>n}(u) \in \mathfrak{m}^{n+1}$ since $u \in \mathfrak{m}$ and $b_n \in \mathfrak{m}^{n+1}$. Since n was arbitrary and the limits of Cauchy sequences in $k[[x]]$ are unique, this shows that $h(u) = x$ as required. □

Note that in the above construction $h(x) = \frac{1}{u_1}x + \ldots$.

Corollary 2. *Let $u(x) = u_1 x + u_2 x^2 + \ldots$ be a power series with $u_1 \neq 0$. Then the morphism of k-algebras $\varphi : k[[x]] \longrightarrow k[[x]]$ defined by $x \mapsto u$ is an automorphism.*

Proof. Let $h(x) \in k[[x]]$ be such that $h(u) = x$, that is, $\varphi(h) = x$. Let $\phi : k[[x]] \longrightarrow k[[x]]$ be defined by $x \mapsto h$. Then $\varphi\phi$ is a continuous morphism of k-algebras with $\varphi\phi(x) = x$, so by uniqueness $\varphi\phi = 1$. Since $h(x) = \frac{1}{u_1}x + \ldots$ we can apply the same argument to produce a continuous morphism of k-algebras $\psi : k[[x]] \longrightarrow k[[x]]$ with $\phi\psi = 1$. An elementary calculation shows that $\varphi = \psi$ and so φ is an automorphism. □

In particular any power series in one variable with no constant term and a nonzero linear term is analytically independent. We now extend this result to more than one variable. Consider the power series ring $k[[x_1, \ldots, x_n]]$ in n variables with maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. We have shown elsewhere that the power $\mathfrak{m}^k$ consist of those power series whose only nonzero terms involve monomials of order k or greater. For any $g(x_1, \ldots, x_n) \in k[[x_1, \ldots, x_n]]$ we write

$$g_i = \sum_{\alpha, |\alpha| = i} g(\alpha) x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

It is easily seen that g is the sum of the series $g_0 + g_1 + \ldots$. We call g_1 the *linear term* of g. Recall that is a power series is a unit iff. it has a nonzero constant term.

Proposition 3. *Let $u_1, \ldots, u_n \in k[[x_1, \ldots, x_n]]$ be nonunit power series whose linear terms are linearly independent. Then there are nonunit power series $h_1, \ldots, h_n$ whose linear terms are linearly independent with $x_i = h_i(u_1, \ldots, u_n)$ for $1 \leq i \leq n$.*

Proof. Suppose we write

$$u_i(x_1, \ldots, x_n) = u_{i,1}x_1 + \ldots u_{i,n}x_n + G_i(x_1, \ldots, x_n)$$

where $G_i \in \mathfrak{m}^2$, for $1 \leq i \leq n$. Since the linear terms are linearly independent they span k^n, so for $1 \leq i \leq n$ there are elements $\lambda_{i,1}, \ldots, \lambda_{i,n}$ with

$$\lambda_{i,1}u_1 + \ldots + \lambda_{i,n}u_n = x_i + \lambda_{i,1}G_1 + \ldots + \lambda_{i,n}G_n$$

That is,

$$x_i = \lambda_{i,1}(u_1 - G_1) + \ldots + \lambda_{i,n}(u_n - G_n) \tag{1}$$

Let us make some comments before proceeding with the proof. If $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ is any homogenous polynomial of degree $k \geq 1$ then we have

$$\begin{aligned} f(x_1, \ldots, x_n) &= f\left(\sum_j \lambda_{1,j}(u_j - G_j), \ldots, \sum_j \lambda_{n,j}(u_j - G_j)\right) \\ &= \sum_{\alpha, |\alpha| = k} f(\alpha) \prod_{i=1}^{n} (\lambda_{i,1}u_1 + \ldots + \lambda_{i,n}u_n - \lambda_{i,1}G_1 - \ldots - \lambda_{i,n}G_n)^{\alpha_i} \end{aligned}$$

Since the u_i belong to $\mathfrak{m}$ and the G_i all belong to $\mathfrak{m}^2$ we can expand this and write

$$\begin{aligned} f(x_1, \ldots, x_n) &= f\left(\sum_j \lambda_{1,j} u_j, \ldots, \sum_j \lambda_{n,j} u_j\right) + b(x_1, \ldots, x_n) \\ &= H(u_1, \ldots, u_n) + B(x_1, \ldots, x_n) \end{aligned}$$

where $H(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ is a homogenous polynomial of degree k and B is a power series belonging to $\mathfrak{m}^{k+1}$.

Next we produce for each i a power series h_i with $h_i(u_1, \ldots, u_n) = x_i$. Let $1 \leq i \leq n$ be fixed. By induction we show that for each $m \geq 1$ there is a polynomial $H_m(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ with degree $\leq m$ (i.e. the highest degree monomial occurring in H_m has degree $\leq m$) and a power series $b_m \in k[[x_1, \ldots, x_n]]$ with $b_m \in \mathfrak{m}^{m+1}$ such that

$$x_i = H_m(u_1, \ldots, u_n) + b_m$$

To see the claim is true for $m = 1$ we set $H_1 = \lambda_{i,1} x_1 + \ldots + \lambda_{i,n} x_n$ and $b_m = -\lambda_{i,1} G_1 - \ldots - \lambda_{i,n} G_n$ and use Equation 1. Suppose the claim is true for m and let $x_i = H_m(u_1, \ldots, u_n) + b_m$. Denote by $b_{m,j}$ the homogenous part of b_m of degree j defined earlier. Using Equation 1 and the preceeding comment

$$\begin{aligned} b_m(x_1, \ldots, x_n) &= b_{m,m+1}(x_1, \ldots, x_n) + \sum_{j=m+2}^{\infty} b_{m,j} \\ &= H(u_1, \ldots, u_n) + B(x_1, \ldots, x_n) + \sum_{j=m+2}^{\infty} b_{m,j} \end{aligned}$$

Where $H(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ is a homogenous polynomial of degree $m + 1$ and B is a power series belonging to $\mathfrak{m}^{m+2}$. Putting $H_{m+1} = H + H_m$ and $b_{m+1} = B + \sum_{j=m+2}^{\infty} b_{m,j}$ we have $x_i = H_{m+1}(u_1, \ldots, u_n) + b_{m+1}$ as required.

Notice that in the above $H_{m+1} - H_m = H$, so at each stage we add to H_m a homogenous polynomial of degree $m + 1$. Hence the sequence $H_1, H_2, \ldots$ is Cauchy and converges to some power series $h_i(x_1, \ldots, x_n) \in k[[x_1, \ldots, x_n]]$. For each $m \geq 1$ write $h_i = H_m + H_{>m}$ and note that

$$\begin{aligned} h_i(u_1, \ldots, u_n) &= H_m(u_1, \ldots, u_n) + H_{>m}(u_1, \ldots, u_n) \\ &= x_i - b_m(x_1, \ldots, x_n) + H_{>m}(u_1, \ldots, u_n) \end{aligned}$$

But $-b_m(x_1, \ldots, x_n) + H_{>m}(u_1, \ldots, u_n) \in \mathfrak{m}^{m+1}$ since the u_i belong to $\mathfrak{m}$ and $b_m \in \mathfrak{m}^{m+1}$. Since m was arbitrary this shows that $h_i(u_1, \ldots, u_n) = x_i$, as required. By construction h_i has no constant term, and the linear term is $\lambda_{i,1} x_1 + \ldots + \lambda_{i,n} x_n$. So the power series $h_1, \ldots, h_n$ satisfy all the conditions of the Proposition, since the coefficients of the linear terms form the matrix inverse to the matrix formed from the linear coefficients of the u_i, which are linearly independent by assumption. □

Theorem 4. *Let $u_1, \ldots, u_n \in k[[x_1, \ldots, x_n]]$ be nonunit power series whose linear terms are linearly independent. Then the morphism of k-algebras*

$$\begin{aligned} \varphi : k[[x_1, \ldots, x_n]] &\longrightarrow k[[x_1, \ldots, x_n]] \\ x_i &\mapsto u_i \end{aligned}$$

is an automorphism.

Proof. Let $h_1, \ldots, h_n$ be the power series produced by the Proposition with $h_i(u_1, \ldots, u_n) = x_i$, that is, $\varphi(h_i) = x_i$. Let $\phi : k[[x_1, \ldots, x_n]] \longrightarrow k[[x_1, \ldots, x_n]]$ be defined by $x_i \mapsto h_i$. Then $\varphi\phi$ is a continuous morphism of k-algebras with $\varphi\phi(x_i) = x_i$ for all i. Hence by uniqueness $\varphi\phi = 1$. Since the h_i are also a family of nonunit power series whose linear terms are linearly independent, the same argument produces a continuous morphism of k-algebras ψ with $\phi\psi = 1$. We see immediately that $\varphi = \psi$ and hence φ is an automorphism. □