MA 558 - Embedding an n Variable Power Series Ring into a Two Variable Power Series Ring

Our goal here is to prove that, if k is a field, then $k[[x_1, ..., x_n]]$, the formal power series ring in n variables over k, can be isomorphically embedded into $k[[x, y]]$, the formal power series ring in 2 variables over k, for each natural number n. The cases where $n = 1$ and $n = 2$ are obvious.

We begin with some important definitions.

Definition. Let A be a ring and B be a subring. The subset $\{a_1, ..., a_n\} \subset A$ is said to be algebraically independent over B if the homomorphism $\varphi : B[x_1, ..., x_n] \to A$ defined by $\varphi(x_i) = a_i$ is injective. Or, equivalently, if there is no nonzero polynomial in $B[x_1, ..., x_n]$ with $(a_1, ..., a_n)$ as a root.

Algebraic independence has transitivity.

Proposition 1. Let $C \subset B \subset A$ be a chain of subrings. Suppose $\{b_1, ..., b_n\} \subset B$ is algebraically independent over C. Further, suppose that $\{a_1, ..., a_m\} \subset A$ is algebraically independent over B. Then $\{b_1, ..., b_n, a_1, ..., a_m\} \subset A$ is algebraically independent over C.

Proof. This follows from induction on the fact that $R[x][y] = R[x, y]$ for a ring R. $\square$

Definition. Let A be a ring, I an A-ideal, and suppose A is complete and Hausdorff in the I-adic topology. Let B be a subring of A. The subset $\{a_1, ..., a_n\} \subset I$ is said to be analytically independent over B if the homomorphism $\varphi : B[[x_1, ..., x_n]] \to A$ defined by $\varphi(x_i) = a_i$ is injective. Or, equivalently, if there is no nonzero power series in $B[[x_1, ..., x_n]]$ with $(a_1, ..., a_n)$ as a root.

Analytic independence also has transitivity.

Proposition 2. Let $C \subset B \subset A$ be a chain of subrings. Let J be a B-ideal and I be an A-ideal so that B is complete and Hausdorff in the J-adic topology, A is complete and Hausdorff in the I-adic topology, and that $JA \subset I$. Suppose $\{b_1, ..., b_n\} \subset J$ is analytically independent over C. Further, suppose that $\{a_1, ..., a_m\} \subset I$ is analytically independent over B. Then $\{b_1, ..., b_n, a_1, ..., a_m\} \subset I$ is analytically independent over C.

Proof. This follows from induction on the fact that $R[[x]][[y]] = R[[x, y]]$ for a ring R, which we will now prove.

One can show that $R[[x, y]] \subset R[[x]][[y]]$ by considering $h(x, y) \in R[[x, y]]$. We can collect all terms with degree in y being 0, collect all terms with degree in y being 1, etc. This gives a power series in y with coefficients in $R[[x]]$.

Similarly, one can show that $R[[x]][[y]] \subset R[[x, y]]$ by considering a given power series $h(y) \in R[[x]][[y]]$ with coefficients in $R[[x]]$. We can distribute each power of y to its coefficient power series, giving us a countable collection of power series $a_{(j,0)}y^j + a_{(j,1)}xy^j + a_{(j,2)}x^2y^j + ... + a_{(j,i)}x^iy^j + ...$ for each j.

We can then arrange all terms of all these power series into an array, as follows:

$$\begin{array}{ccccc} a_{(0,0)} & a_{(0,1)}x & ... & a_{(0,i)}x^i & ... \\ a_{(1,0)}y & a_{(1,1)}xy & ... & a_{(1,i)}x^iy & ... \\ a_{(2,0)}y^2 & a_{(2,1)}xy^2 & ... & a_{(2,i)}x^iy^2 & ... \\ & & \vdots & & \\ a_{(j,0)}y^j & a_{(j,1)}xy^j & ... & a_{(j,i)}x^iy^j & ... \\ & & \vdots & & \end{array}$$

Following in a similar manner to Cantor's proof that the rational numbers are countable, we can form an infinite sum containing each of these terms by choosing an appropriate order along the finite diagonals of this array. i.e., we can rewrite $h(y)$ as $a_{(0,0)} + a_{(0,1)}x + a_{(1,0)}y + a_{(0,2)}x^2 + a_{(1,1)}xy + a_{(2,0)}y^2 + ...$, a formal power series in both x and y. □

For the main result, we will restrict our attention to when k is a field. Notice that a power series ring $k[[x_1, ..., x_n]]$ is complete and Hausdorff in the $(x_1, ..., x_n)\,k[[x_1, ..., x_n]]$-adic topology.

By the First Isomorphism Theorem and the definition of analytic independence, to show that $k[[x_1, ..., x_n]]$ can be isomorphically embedded into $k[[x, y]]$, it suffices to show that there exists an analytically independent set of n elements in $(x, y)\,k[[x, y]]$.

Before we do this, however, we give a new condition, which is a weakening of algebraic independence. This condition is sufficient to prove the main result, however, and makes proving the result much easier.

Definition. Let A be a ring and B be a subring of A. A subset $\{a_1, ..., a_n\} \subset A$ is said to be homogeneously independent over B if there is no nonzero homogeneous polynomial in $B[x_1, ..., x_n]$ with $(a_1, ..., a_n)$ as a root.

Just out of curiosity, one could ask if there is an equivalent definition of homogeneous independence fitting with the ones we gave for algebraic independence and analytic independence. Indeed, there is.

Proposition 3. Let B be a subring of A. Let $\{a_1, ..., a_n\} \subset A$ and consider the homomorphism $\varphi : B[x_1, ..., x_n] \to A$ where $\varphi(x_i) = a_i$. Treat $B[x_1, ..., x_n] = R = \bigoplus_{m=0}^{\infty} R_m$ as the graded ring where R_m consists of all homogeneous polynomials of degree m. The set $\{a_1, ..., a_n\}$ is homogeneously independent over B if and only if $\varphi|_{R_m}$ is injective for each m.

Proof. φ is merely the evaluation map at the point $(a_1, ..., a_n) \in A^n$. If $(a_1, ..., a_n)$ satisfies no nonzero homogeneous polynomials, then $\varphi|_{R_m}(f) \neq 0$ whenever $f \neq 0$. Similarly, if $\varphi|_{R_m}(f) \neq 0$ for all $0 \neq f \in R_m$, then $(a_1, ..., a_n)$ satisfies no nonzero polynomial of R_m, which are all the homogeneous polynomials of degree m. □

It is fairly easy to see that homogeneous independence is a weakening of algebraic independence. Certainly, if a set is algebraically independent over B, it is also homogeneously independent over B. However, we can find sets which are homogeneously independent over B which are not algebraically independent over B.

An example of this is the set $\{1\}$. Clearly, this set is not algebraically independent (as it satisfies the polynomial $x-1$ over B). However, this set is actually homogeneously independent, which we will now prove.

Proof. Suppose $f(1)=0$ for $0\neq f(x)\in B[x]$. Then $f(x)=(x-1)g(x)$ for some $0\neq g(x)\in B[x]$. Hence $f(x)=xg(x)-g(x)$. Now, $\deg(xg(x))>\deg(g(x))$ since x is a non-zero-divisor, so $f(x)$ is not homogeneous. □

One can ask whether or not homogeneous indepence has transitivity. It does not. For example, $\{1\}\subset\mathbb{Q}$ is homogeneously independent over $\mathbb{Z}$, and $\{2\}\subset\mathbb{R}$ is homogeneously independent over $\mathbb{Q}$, but $\{1,2\}\subset\mathbb{R}$ is not homogeneously independent over $\mathbb{Z}$, since $(1,2)$ is a root of the homogeneous polynomial $2x_1-x_2$ over $\mathbb{Z}$. We can get close to transitivity, however.

Proposition 4. Let $C\subset B\subset A$ be a chain of subrings. Let $S=\{b_1,...,b_n\}\subset B$ and $T=\{a_1,...,a_m\}\subset A$. If S is homogeneously independent over C and T is algebraically independent over B, then $\{b_1,...,b_n,a_1,...,a_m\}\subset A$ is homogeneously independent over C.

Proof. Suppose S is homogeneously independent over C and T is algebraically independent over B. By the transitivity of algebraic independence (Proposition 1), it suffices to prove the result for $m=1$; i.e., $T=\{a\}$.

By way of contradiction, suppose $0\neq f(x_1,...,x_{n+1})\in C[x_1,...,x_{n+1}]$ is a homogeneous polynomial with $(b_1,...,b_n,a)$ as a root. Define $g(x_{n+1})=f(b_1,...,b_n,x_{n+1})$. Then $g(x_{n+1})\in B[x_{n+1}]$ is a polynomial in a single variable over B.

$g(a)=f(b_1,...,b_n,a)=0$, so $g=0$, since a is algebraically independent over B.

Let $h(x_1,...,x_n)=f(x_1,...,x_n,0)$. It follows that h is a homogeneous polynomial over C, since h is obtained by removing all terms of f which have x_{n+1} as a factor. i.e., h is the sum of all the terms of f which do not have x_{n+1} as a factor.

$h(b_1,...,b_n)=f(b_1,...,b_n,0)=g(0)=0$, since $g=0$. Since S is homogeneously independent over C, it follows that $h=0$. But since h is the sum of all the terms of f which do not have x_{n+1} as a factor, it follows that x_{n+1} is a factor of f. Let d be the highest power of x_{n+1} which appears as a factor of every term of f.

Thus, $f(x_1,...,x_{n+1})=x_{n+1}^d p(x_1,...,x_{n+1})$ for some $0\neq p(x_1,...,x_{n+1})\in C[x_1,...,x_{n+1}]$. Since d is the highest power of x_{n+1} appearing as a factor in every term of f, it follows that at least one term of p does not have x_{n+1} as a factor. Since $0=g(x_{n+1})=f(b_1,...,b_n,x_{n+1})$, it follows that $x_{n+1}^d p(b_1,...,b_n,x_{n+1})=0$. Thus, it follows that $p(b_1,...,b_n,x_{n+1})=0$. In particular, the sum of all the terms of p which do not have x_{n+1} as a factor forms a homogeneous polynomial of degree $\deg(f) - d$ over C which is satisfied by the homogeneously independent set $\{b_1, ..., b_n\}$ over C. Thus, every term of $p(x_1, ..., x_{n+1})$ has x_{n+1} as a factor, which is a contradiction. Therefore $f = 0$, so $\{b_1, ..., b_n, a\}$ is homogeneously independent over C. $\square$

We turn our attention back to the main question at hand. We want to show that there exist n analytically independent power series in $(x, y)\, k[[x, y]]$ over a field k.

To do this, we will first show the following fact, due to Zariski and Samuel.

Lemma 1. If the set of power series $\{f_1(x), ..., f_n(x)\} \subset k[[x]]$ is homogeneously independent over the field k, then the set of power series $\{yf_1(x), ..., yf_n(x)\} \subset (x, y)\, k[[x, y]]$ is analytically independent over k.

Proof. First, we notice that $\{yf_1(x), ..., yf_n(x)\} \subset (x, y)\, k[[x, y]]$ since each is a multiple of y.

Suppose $g \in k[[x_1, ..., x_n]]$ such that $g(yf_1(x), ..., yf_n(x)) = 0$.

Notice that g can be written in the form $g = \sum_{j=0}^{\infty} g_j$ where g_j is a homogeneous polynomial in $k[x_1, ..., x_n]$ of degree j. Then

$$0 = g(yf_1(x), ..., yf_n(x)) = \sum_{j=0}^{\infty} g_j(yf_1(x), ..., yf_n(x))$$

Since each g_j is a homogeneous polynomial of degree j and y is a factor of each element being plugged into each variable, we get that $g_j(yf_1(x), ..., yf_n(x)) = g_j(f_1(x), ..., f_n(x))\, y^j$ for all j. Thus,

$$0 = \sum_{j=0}^{\infty} g_j(f_1(x), ..., f_n(x))\, y^j$$

Since each term contains a distinct power of y, it follows that $g_j(f_1(x), ..., f_n(x)) = 0$ for all j.

But since $f_1(x), ..., f_n(x)$ are homogeneously independent over k, it follows that $g_j = 0$ for all j, and so $g = 0$. Therefore, $yf_1(x), ..., yf_n(x)$ are analytically independent over k. $\square$

By Lemma 1, in order to show that there exist n analytically independent elements in $k[[x, y]]$, it suffices to show that there exist n homogeneously independent elements of $k[[x]]$. In fact, there are uncountably many algebraically independent elements of $k[[x]]$ over k (and hence uncountably many homogeneously independent elements), which is proven in Integral Domains Inside Noetherian Power Series Rings: Constructions and Examples by Heinzer, Rotthaus, and Wiegand. This proof involves showing that the transcendence degree of $k[[x]]$ over k is uncountable.

We will use a different approach, by showing that there exists a set of 3 homogeneously independent elements in $k[[x]]$ over k and using induction to prove that if there is a set of 3 analytically independent power series in $k[[x,y]]$, then there is a set of n analytically independent power series in $k[[x,y]]$ for all $n \geq 3$.

We begin by proving the latter result.

Lemma 2. If there exists a set of 3 analytically independent power series in $(x,y)\,k[[x,y]]$, then there exists a set of n analytically independent power series in $(x,y)\,k[[x,y]]$ for all $n \geq 3$.

Proof. Suppose that there is a set $\{f_1(x,y), f_2(x,y), f_3(x,y)\} \subset (x,y)\,k[[x,y]]$ analytically independent over k. Later, we will prove that such a set exists, and it will serve as our base case for induction here.

As an inductive hypothesis, suppose $\exists$ a set $\{f_1(x,y), ..., f_{n-1}(x,y)\} \subset (x,y)\,k[[x,y]]$ analytically independent over k.

Then we can consider $k[[f_1, ..., f_{n-1}]]$ as a power series ring. Indeed, by the definition of analytically independent, $k[[f_1, ..., f_{n-1}]]$ is a subring of $k[[x,y]]$. Moreover, $k[[f_1, f_2]]$ is a subring of $k[[f_1, ..., f_{n-1}]]$. Since the ring $k[[f_1, ..., f_{n-1}]]$ is a formal power series ring, it follows that f_3 is analytically independent over the entire subring $k[[f_1, f_2]]$ of $k[[x,y]]$.

Being a formal power series ring in two variables, $k[[f_1, f_2]] \cong k[[x,y]]$, so by the induction hypothesis, $\exists$ an analytically independent set $\{g_1, ..., g_{n-1}\} \subset (f_1, f_2)\,k[[f_1, f_2]]$ over k.

Since $k \subset k[[f_1, f_2]] \subset k[[x,y]]$, $k[[f_1, f_2]]$ is complete and Hausdorff in the $(f_1, f_2)\,k[[f_1, f_2]]$-adic topology, $k[[x,y]]$ is Hausdorff in the $(x,y)\,k[[x,y]]$-adic topology, $(f_1, f_2)\,k[[x,y]] \subset (x,y)\,k[[x,y]]$, and since f_3 is analytically independent over $k[[f_1, f_2]]$, and $\{g_1, ..., g_{n-1}\}$ is analytically independent over k, it follows from Proposition 2 that $\{g_1, ..., g_{n-1}, f_3\} \subset (x,y)\,k[[x,y]]$ is analytically independent over k, giving us an analytically independent set of n elements, completing the induction. $\square$

Now, it just remains to show that there is a homogeneously independent set of 3 elements in $k[[x]]$ over k. The lemma would then give that we have 3 analytically independent elements in $k[[x,y]]$ over k.

Lemma 3. $\{1, x, f\} \subset k[[x]]$ is homogeneously independent over k where

$$f(x) = 1 + x + x^{2!} + x^{3!} + ... + x^{n!} + ...$$

Proof. We have already seen in the examples above that $1 \in k$ is homogeneously independent over k. Moreover, x is algebraically independent over k. By Proposition 4, we then get that $\{1, x\}$ is homogeneously independent over k. To show that $\{1, x, f\}$ is homogeneously independent over k, it suffices, again by Proposition 4, to show that f is algebraically independent over $k[x]$. Thus, it further suffices to show that f is transcendental over $k(x)$.

Suppose f is a root of a polynomial $F(T) = a_q(x)T^q + ... + a_1(x)T + a_0(x)$ where each $a_i(x) \in k[x]$ (we may assume this by multiplying by the product of the denominators). Let $d = \max_i \{\deg a_i(x)\}$. We may assume $F(T)$ is irreducible over $k(x)$, or else we could find a polynomial of lower degree with f as a root.

Let $p(x)$ be any polynomial. Then the power series $f(x) - p(x)$ is a root of $G(T) = F(T + p(x))$. Then $G(T) = b_q(x)T^q + ... + b_1(x)T + b_0(x)$, where $b_0(x) = a_q(x)p^q(x) + ... + a_1(x)p(x) + a_0(x)$. Since $F(T)$ is irreducible, it follows that $G(T)$ is irreducible. If not $G(T) = H_1(T)H_2(T)$, then $F(T) = G(T - p(x)) = H_1(T - p(x))H_2(T - p(x))$, a contradiction. Since $G(T)$ is irreducible, $b_0(x) \neq 0$.

We have the inequality $\deg b_0 \leq d + q \cdot \deg p$.

Let $n > \max\{d+1, q+1\}$. Now choose $p(x) = 1 + x + x^{2!} + ... + x^{(n-1)!}$. Now, $\deg p = (n-1)!$ Then

$$\deg b_0 \leq d + q \cdot \deg p < (n-1) + (n-1)(n-1)! \leq (n-1)! + (n-1)(n-1)! = n!$$

Thus, $\deg b_0 < n!$

On the other hand, $f(x) - p(x) = x^{n!} + x^{(n+1)!} + ...$ and being a root of G gives

$$b_0(x) + b_1(x)\left(x^{n!} + x^{(n+1)!} + ...\right) + ... + b_q(x)\left(x^{n!} + x^{(n+1)!} + ...\right)^q = 0$$

All of the terms above have $x^{n!}$ as a factor with the exception of $b_0(x)$. Since $\deg b_0 < n!$, it follows that in order for the above statement to be true, $b_0(x) = 0$, which is absurd as we've already stated that $b_0(x) \neq 0$. Hence, $f(x)$ is transcendental over $k(x)$. $\square$

We now prove the main result.

Theorem. Let n be any natural number, and let k be a field. The formal power series ring $k[[x_1, ..., x_n]]$ embeds isomorphically into the formal power series ring $k[[x, y]]$.

Proof. For $n = 1$ and $n = 2$, the result is trivial. Suppose $n \geq 3$.

By Lemma 3, there exists a set of 3 homogeneously independent power series in $k[[x]]$ over k. By Lemma 1, there then exists a set of 3 analytically independent power series in $k[[x, y]]$ over k. By Lemma 2, there then exists a set of n analytically independent power series in $k[[x, y]]$ over k.

By the definition of analytic independence and the First Isomorphism Theorem, we have the result. $\square$