Math 711: Lecture of November 24, 2004

Since $s_i \equiv z_i \bmod \alpha(x_n)$, it follows that $g(x,\, z) \equiv g(x,\, s) \bmod \alpha(x_n)$ and that $F_j(x,\, s) \equiv F_j(x,\, z) \bmod \alpha(x_n)$ for all j. Since $\alpha(x_n)$ and $g(x,\, s)$ are associates, we have that $\alpha(x_n)$ divides $g(x,\, z)$. Since the hypothesis of the Key Lemma tells us that $g(x,\, s)$ divides every $F_j(x,\, s)$, we have that $\alpha(x_n)$ divides every $F_j(x,\, z)$.

Recall that

$$\alpha(x_n) = x_n^q + u_{q-1}x_n^{q-1} + \cdots + u_0.$$

We can now substitute the $z_{i,\nu}$ for the $Z_{i,\nu}$ and the u_ν for the U_ν in $(*)$ and $(**)$ above. The equations that result show that the elements

$$\sum_{\nu=0}^{q-1} W_{j,\nu}(x, z, u)x_n^\nu$$

are the remainders in the Weierstrass Preparation Theorem when $g(x,\, z)$ and the $F_j(x,\, z)$ are divided by $\alpha(x_n)$: note that the variable x_n does not occur in $W_{j,\nu}$. But the results of the preceding paragraph show that these remainders are 0. It follows that

$$W_{j,\nu}(x,\, z,\, u) = 0, \quad 0 \le j \le h, \quad 0 \le \nu \le q-1.$$

Put differently, the system of $(h+1)q$ polynomial equations

$$W_{j,\nu}(x,\, Z,\, U) = 0, \quad 0 \le j \le h, \quad 0 \le \nu \le q-1$$

in the variables $Z,\, U$, which has coefficients in

$$V[x_1,\, \ldots\,, x_{n-1}] \subseteq D = V[x_1,\, \ldots\,, x_{n-1}]^{\mathrm{h}}_{(t, x_1,\, \ldots\,, x_{n-1})},$$

has the solution $Z = z$, $U = u$ in $\widehat{D} = C$.

The induction hypothesis then guarantees that for every positive integer N there is a solution of these equations $Z = \underline{z}_N$, $U = \underline{u}_N$ in D which is congruent to z, u modulo $(t,\, x_1,\, \ldots\,, x_{n-1})^N C$. We shall now use this solution to construct the elements $\underline{y}_N$ needed to prove the Key Lemma.

For all i choose any $\theta_{i,N} \in A^{\mathrm{h}}$ such that $\theta_{i,N} \equiv \theta_i \bmod m^N\widehat{A}$. Let

$$\underline{u}_N = u_{0,N},\, \ldots\,,\, u_{q-1,N}$$

and let the individual values of the $\underline{z}_N$ be denoted $z_{i,\nu,N}$. Define

$$\alpha_N(x_n) = H(\underline{u}_N,\, x_n) = x_n^q + u_{q-1,N}x_n^{q-1} + \cdots + u_{0,N},$$

while letting

$$z_{i,N} = \sum_{\nu=0}^{q-1} z_{i,\nu,N} x_n^\nu$$

and

$$y_{i,N} = \alpha_N(x_n)\theta_{i,N} + z_{i,N}.$$

Modulo $m^N \widehat{A}$ we know that $\underline{u}_N \equiv u$, and it follows that modulo $m^N \widehat{A}$ we also have that $\alpha_N(x_n) \equiv \alpha(x_n)$, that $z_{i,N} \equiv z_i$ and that $y_{i,N} \equiv s_i$. To complete the proof of the Key Lemma, it will suffice to show that $g(x, \underline{y}_N)$ divides $F_j(x, \underline{y}_N)$ for all j.

Since the $z_{i,\nu,N}$ and the $\underline{u}_N$ satisfy the equations

$$W_{j,\nu}(x,\, Z,\, U) = 0, \quad 0 \le j \le h, \quad 0 \le \nu \le q-1$$

when we substitute in $(*)$ and $(**)$ we find that $\alpha_N(x_n)$ divides $g(x,\, \underline{z}_N)$ and that it also divides every $F_j(x,\, \underline{z}_N)$. From the way we defined $y_{i,N}$ we also have that $z_{i,N} \equiv y_{i,N}$ modulo $\alpha_N(x_n)$. It follows as well that $\alpha_N(x_n)$ divides $g(x,\, \underline{y}_N)$ and every $F_j(x,\, \underline{y}_N)$. We can complete the argument by showing that $\alpha_N(x_n)$ is the unique monic associate of $g(x,\, y_N)$ for all sufficiently large N.

The point is that if N is large then the fact that

$$g(x,\, \underline{y}_N) \equiv g(x,\, s) \bmod m^N \widehat{A}$$

implies that $g(x, \underline{y}_N)$ is regular of order q in x_n, and so it has an associate $\alpha'(x_n)$ that is monic of degree q as a polynomial in x_n and has all coefficients on lower powers of x_n in the maximal ideal of C. Since $\alpha_N(x_n)$ divides $\alpha'(x_n)$ in $\widehat{A}$, since they are both monic of the same degree as polynomials in x_n, and since they both have lower degree coefficients in the maximal ideal of C, they must be equal. $\square$

This completes not only the proof of the Key Lemma, but finishes the proof of the Artin Approximation Theorem when $V = K$ is a field. When the base ring is a DVR, however, we have more work to do. In particular, we need to justify the assumption that we can reduce to the case where $\delta(x,\, s)$ is not in $t\widehat{A}$.

In order to make this reduction we need to study an idea of Néron which Artin refers to as "Néron's p-desingularization." (In Artin's paper, p is the generator of the maximal ideal of the DVR, which we are calling t here.) However, we will simply use the term *Néron desingularization*.