

P-ADICALLY CLOSED FIELDS, HILBERT'S 17TH PROBLEM AND THE NULLSTELLENSATZ

DAVID FAVERO

1. INTRODUCTION: AN ANALOGUE BETWEEN FORMALLY REAL AND FORMALLY P-ADIC FIELDS

A p-adically closed field is meant to axiomatize \mathbb{Q}_p in the same way that a real closed field axiomatizes \mathbb{R} . As we have seen, both the theory of real closed fields and the theory of p-adically closed fields are model complete. Furthermore both admit quantifier elimination (recall that we need to modify the language of p-adically closed fields for this statement to hold in that case). My intention in this talk is to illustrate further analogies between these two theories, namely both theories admit a form of the nullstellensatz and a solution of Hilbert's 17th problem. Although many of the results provided can be proved in further generality, for simplicity I will always assume that k is a valued field with residue field $\mathbb{Z}/p\mathbb{Z}$.

To build this analogy, we first need an analogue of the squaring operator, this is provided by the Kochen operator:

$$\gamma(x) = \frac{1}{p} \frac{x^p - x}{(x^p - x)^2 - 1}.$$

Just like in the real case, we have that the image of the Kochen operator is contained in any p-valuation ring. More precisely,

Theorem 1.1. *For a field, k , the intersection of all p-valuation rings is equal to $\mathbb{Z}[\gamma(k)]$ localized over the multiplicative set $1 + pb$ where $b \in \mathbb{Z}[\gamma(k)]$.*

The intersection of all p-valuations is called the holomorphy ring and the above localized ring is called the γ -Kochen ring. So the above theorem says that the Kochen ring is equal to the holomorphy ring. This ring and it's generalizations will be of central importance to the desired analogy.

Remark 1.2. *In more general contexts we may allow the residue field to be a finite extension of $\mathbb{Z}/p\mathbb{Z}$, in which case we alter the Kochen operator to include the p-ramification index and the residue degree. If the p-ramification index is 1 then the above holds, otherwise the intersection of all p-valuations, which is called the holomorphy ring, is just the integral closure of the Kochen ring. Holomorphic functions are elements of the holomorphy ring, so in our case holomorphic functions are just elements of the Kochen ring.*

Hilbert's 17th problem which he proposed at the International Congress of Mathematicians in 1900 was to prove that any positive definite polynomial, $f \in \mathbb{R}[x_1, \dots, x_n]$, can be expressed as a sum of squares of rational functions, $g \in \mathbb{R}(x_1, \dots, x_n)$. Artin proved this theorem in 1926 for all real closed fields and in doing so, he also developed the notion of such fields. Kochen then went on to develop a similar theory, the theory of formally p-adic fields, based upon \mathbb{Q}_p . However it was Peter Roquette who later proved the following analogous theorem,

Theorem 1.3. *Let k be a p-adically closed field, then any integral definite rational function $f \in k(x_1, \dots, x_n)$ is in the Kochen ring for the rational function field.*

Here integral definite just means that f takes integral values where defined. The other analogous theorems are the real and p-adic nullstellensatz. First one needs a few definitions,

Definition 1.4. *A field k is called real if -1 is not a sum of squares in k .*

Definition 1.5. *A field k is called real closed if does not admit any real, non-trivial, algebraic extensions.*

Definition 1.6. *Let $I \subset R$ be an ideal in a ring R . Then I is called real if, $\forall a_1, \dots, a_n \in A$ such that $a_1^2 + \dots + a_n^2 \in I$ we have that $a_i \in I$ for some i or equivalently for all i .*

Theorem 1.7. *Let k be a real closed field and $I \subset k[x_1, \dots, x_n]$ be a real ideal. Then $\mathfrak{J}(V(I)) = I$.*

Similarly we have a p-adic nullstellensatz which we will actually prove in much greater generality,

Theorem 1.8. *Let k be a p -adically closed field with valuation ring σ and $I \subset R[x_1, \dots, x_n]$ be an ideal. Then $\mathfrak{J}(V_\sigma(I)) = \sqrt{I}$ as ideals in $R[x_1, \dots, x_n]$.*

Here $V_\sigma(I)$ is the locus of integral vectors that vanish for all polynomials in I .

2. A MODEL THEORETIC PROOF OF THE REGULAR AND REAL NULLSTELLENSATZ

First let's recall the proof of Hilbert's Nullstellensatz from S. Takeda's talk,

Theorem 2.1. *Let k be a field, $f_1, \dots, f_m \in k[x_1, \dots, x_n]$, and $I = \langle f_1, \dots, f_m \rangle \neq (1)$. Then $\exists a_1, \dots, a_n \in \bar{k}$ such that $f_i(a_1, \dots, a_n) = 0$ for all $i = 1 \dots m$.*

Proof. Let \mathfrak{m} be a maximal ideal containing I . Consider the sentence,

$$\phi := \exists X_1, \dots, X_n \left[\bigwedge_{i=1}^m f_i(X_1, \dots, X_n) = 0 \right]$$

Clearly $\phi \models \overline{k[x_1, \dots, x_n]/\mathfrak{m}}$ and \bar{k} is an elementary submodel by model completeness. Therefore $\phi \models \bar{k}$. \square

We can now adapt this proof towards the real nullstellensatz. The main difference is that we take a "real" prime ideal which contains I . We just need some quick facts.

Proposition 2.2. *A prime ideal, \mathfrak{p} is real iff. $(A/\mathfrak{p})_0$ is real.*

Proof. Notice, $(A/\mathfrak{p})_0$ is not real $\Leftrightarrow -1 = a_1^2 + \dots + a_n^2 \Leftrightarrow a_1^2 + \dots + a_n^2 + 1^2 = 0 \Leftrightarrow a_1^2 + \dots + a_n^2 + 1^2 \in \mathfrak{p} \Leftrightarrow \mathfrak{p}$ is not real. \square

Proposition 2.3. *Any real ideal is radical.*

Proof. Let I be a real ideal with $x^m \in I$ and \mathfrak{m} minimal. Since I is real m can not be even, but $x^{m+1} \in I$ implies that $x^{\frac{m+1}{2}} \in I$ which means $m = 1$. \square

Definition 2.4.

$$I_R := \{ r \in R \mid r^{2m} + b_1^2 + \dots + b_s^2 \in I \text{ with } b_i \in R \text{ and } m \in \mathbb{N}^* \}$$

is called the real radical of an ideal I in R .

Notice this is indeed an ideal by taking binomial expansions of $(a+b)^{2N}$ for N sufficiently large.

Proposition 2.5. *The real radical of an ideal is real.*

Proof. Suppose $a_1^2 + \dots + a_n^2 \in I_R$ then $\exists b_i \in R$ and $m \in \mathbb{N}^*$ such that $(a_1^2 + \dots + a_n^2)^{2m} + b_1^2 + \dots + b_s^2 \in I$ multiplying this expression out gives $a_i \in I_R$ for all i . \square

We are now ready to prove a real nullstellensatz in an analogous fashion,

Theorem 2.6. *Let k be a real field with real closure K , $f_1, \dots, f_m \in R = k[x_1, \dots, x_n]$, and $I = \langle f_1, \dots, f_m \rangle \neq (1)$ a real ideal. Then $\exists a_1, \dots, a_n \in K$ such that $f_i(a_1, \dots, a_n) = 0$ for all $i = 1, \dots, m$.*

Proof. As in the proof of theorem 2.1, we consider the sentence,

$$\phi := \exists X_1, \dots, X_n \left[\bigwedge_{i=1}^m f_i(X_1, \dots, X_n) = 0 \right]$$

and want to find a real closed field containing K where the sentence holds, because then by model completeness of the theory of real closed fields we are done. This time we find a real prime ideal, \mathfrak{p} containing I and take the real closure of the fraction field of $k[x_1, \dots, x_n]/\mathfrak{p}$. Since ϕ clearly models this field, we just need to show that there exists a real prime ideal containing I .

To do this consider the set, S , of proper real ideals which contain I . $I \in S$ and S is partially ordered by inclusion so by Zorn's lemma it has some maximal element, \mathfrak{p} . We need to show that \mathfrak{p} is prime. Suppose $x, y \notin \mathfrak{p}$. Then $\langle \mathfrak{p}, x \rangle_R = \langle \mathfrak{p}, y \rangle_R = (1)$ by maximality, so we have the equations:

$$1 + \text{sum of squares} = p + \alpha x \text{ where } p \in \mathfrak{p} \text{ and } \alpha \in R$$

$$1 + \text{sum of squares} = q + \beta y \text{ where } q \in \mathfrak{p} \text{ and } \beta \in R$$

Multiplying yields, $1 + \text{sum of squares} = p' + \alpha, \beta xy$ where $p' \in \mathfrak{p}$. But $1 + \text{sum of squares} \notin \mathfrak{p}$ since \mathfrak{p} is proper and real. Therefore $xy \notin \mathfrak{p}$. \square

Using the above techniques we can prove the nullstellensatz in another form, the proof that the ideal is prime is essentially the same in the following cases:

Theorem 2.7. *Let k be a field, $I \subset k[x_1, \dots, x_n]$ an ideal. Then $\mathcal{I}(V(I)) = \sqrt{I}$.*

Proof. Obviously $\mathcal{I}(V(I)) \supseteq \sqrt{I}$. Now suppose $\exists g \in \mathcal{I}(V(I)), g \notin \sqrt{I}$. Then by Zorn's lemma there exists a prime ideal, \mathfrak{p} , containing \sqrt{I} such that $g \notin \mathfrak{p}$. Since our ring is noetherian, let $\sqrt{I} = f_1, \dots, f_r$. Now, consider the sentence,

$$\phi := \exists a_1, \dots, a_n \left[\bigwedge_{i=1..r} f_i(a_1, \dots, a_n) = 0 \wedge g(a_1, \dots, a_n) \neq 0 \right]$$

Let K be the algebraic closure of $(k[x_1, \dots, x_n]/\mathfrak{p})_0$. Clearly, $\phi \models K$ and $\bar{k} \subseteq K$ therefore by the model completeness of algebraically closed fields $\phi \models \bar{k}$, this contradicts the fact that $g \in \mathcal{I}(V(I))$. \square

And for real closed fields we have:

Theorem 2.8. *Let k be a real field, with real closure R , $I \subset k[x_1, \dots, x_n]$ a real ideal. Then $\mathcal{I}(V(I)(R)) = I$.*

Proof. Obviously $\mathcal{I}(V(I)(R)) \supseteq I$. Now suppose $\exists g \in \mathcal{I}(V(I)(R)), g \notin I$. Then by Zorn's lemma there exists a real prime ideal, \mathfrak{p} , containing I such that $g \notin \mathfrak{p}$. Since our ring is noetherian, let $I = f_1, \dots, f_r$. Now, consider the sentence,

$$\psi := \exists a_1, \dots, a_n \left[\bigwedge_{i=1..r} f_i(a_1, \dots, a_n) = 0 \wedge g(a_1, \dots, a_n) \neq 0 \right]$$

Let K be the real closure of $(k[x_1, \dots, x_n]/\mathfrak{p})_0$. Clearly, $\psi \models K$ and $R \subseteq K$ therefore by the model completeness of real closed fields $\psi \models R$, this contradicts the fact that $g \in \mathcal{I}(V(I))$. \square

We now build an analogous theory in the p-adic case.

3. PRELIMINARY ALGEBRAIC FACTS AND THE RATIONAL PLACE EXISTENCE THEOREM

For the p-adic nullstellensatz, we will follow the proof in *Formally p-adic Fields* by Prestel and Roquette. We state most of the necessary lemmas and theorems here, although not all the proofs are provided, they may be found in the above reference. We begin by discussing the Riemann space, first recalling the basics facts and definitions regarding places.

Definition 3.1. *Let K be a valued field with residue field κ . A place P is a 'homomorphism' $K \rightarrow \kappa \cup \infty$, respecting $0 = \infty^{-1}, \infty + \infty = \infty, \infty * \infty = \infty, \infty * x = \infty$ for $x \neq 0$.*

Definition 3.2. *A place P of the function field K/k is called rational if $P(K)/\infty = k$ i.e. if the residue field, $\kappa = k$.*

Definition 3.3. *$S = S_k(K/k) =$ the set of rational places is called the Riemann k -space of K/k or just the Riemann space.*

For the rest of the talk if it is not otherwise specified, K is function field over k , with valuation rings Σ and σ respectively.

We now endow the Riemann space with two possible topologies. Let $u = \{u_1, \dots, u_r\}$ be a finite set of elements in K . The p-adic topology for S is generated by basic opens of the form:

$$S_u := \{P | P(x) \in \sigma \text{ for } x \in u\}.$$

Now let $z = \{z_1, \dots, z_s\}$ be another finite set of elements of K . Then we take the Zariski topology on S to be generated by basic opens of the form:

$$S^z := \{P | P(x) \neq \infty, x \in z\}.$$

Definition 3.4. *Any subset of S of the form $S_u^z := S^z \cap S_u$ is called a basic subset of S .*

Remark 3.5. *If v is a valuation of κ with valuation ring σ and maximal ideal \mathfrak{m} , then $\Sigma := P^{-1}(\sigma)$ is a valuation ring with maximal ideal $\mathfrak{M} := P^{-1}(\mathfrak{m})$. In particular, notice that $P^{-1}(\kappa)$ is a valuation ring with maximal ideal $P^{-1}(0)$. This is clear because $P(X * X^{-1}) = P(X) * P(X^{-1}) = 1 \in \sigma$ therefore $P(X)$ or $P(X^{-1}) \in \sigma$, furthermore X is a unit iff. $P(X)$ is a unit. This also means that the natural map $\Sigma/\mathfrak{M} \rightarrow \sigma/\mathfrak{m}$ is an isomorphism, i.e. the residue fields agree. Furthermore if $P \in S_u$ then $x \in \Sigma$ for all $x \in u$.*

Thus we make the following definition,

Definition 3.6. *If there exists a p-valuation ring Σ on K which extends $\sigma[u] \subseteq \Sigma$ and the residue field is $\mathbb{Z}/p\mathbb{Z}$, then K is called formally p-adic over $\sigma[u]$.*

Example 3.7. *Let $k((t))$ be the field of formal Laurent series in t . For $x \in k((t))$ we define $P(x) := x(0)$ (this is infinity if the series has a pole at zero). Then P is a rational place, and $P^{-1}(\sigma)$ is all power series with no poles and first coefficient integral, the maximal ideal is all power series with a zero at $t = 0$. This place is called the canonical place.*

We will need the following theorem which was stated by J. Tsay during his lectures on the model theory of p-adically closed fields,

Theorem 3.8. *Let L/K be a p-adically closed extension of valued fields. If K is algebraically closed in L then K is p-adically closed (with the same residue field).*

We are now ready to prove,

Theorem 3.9. *Let K be a function field over a p-adically closed field k . Then $S_u^z \neq \emptyset$ iff. K is formally p-adic over $\sigma[u]$.*

Proof. \Rightarrow is clear by the above remark so we need to show \Leftarrow . For this we assume K is formally p-adic over $\sigma[u]$ and proceed by induction on the transcendence degree of the function field.

$n = 1$: By Noether's normalization we have $K = k[X, Y]/(f)$ with f monic and irreducible as a polynomial in Y so we have $K = k(x, y) = k[x, y]_0$ where $x := X \bmod (f), y := Y \bmod (f)$. Let $u = \{u_1, \dots, u_r\}$ and $z = \{z_1, \dots, z_s\}$. So we have,

$$u_j = \frac{u'_j}{u''_j} \text{ and } z_i = \frac{z'_i}{z''_i}, \text{ with } u'_j, u''_j z'_i, z''_i \in k[x, y], (u'_j, u''_j) = 1 \text{ and } (z'_i, z''_i) = 1.$$

Now since K is formally p-adic over $\sigma[u]$ by definition there is a p-valuation ring Σ on K containing $\sigma[u]$. Consider the following sentence,

$$\phi := \exists x, y \text{ such that } f(x, y) = 0 \wedge \frac{\partial f}{\partial Y}(x, y) \neq 0 \bigwedge_{i=1}^s z''_i \neq 0 \bigwedge_{j=1}^r [u''_j \neq 0 \wedge u_j \in \Sigma].$$

On (K, Σ) , ϕ just says there exists a point where u_j takes integral values for all j on some Zariski open subset. But we have constructed Σ so that $\phi \models (K, \Sigma)$. Let (L, Θ) be some p-adic closure of (K, Σ) , then since ϕ is existential and (K, Σ) is a substructure of (L, Θ) the sentence is also true in (L, Θ) . We also have that (k, σ) is a submodel of (L, Θ) , and it is elementary by the model completeness of p-adically closed fields, in particular $(k, \sigma) \models \phi$. Let $(a, b) \in k^2$ be a vector which satisfies ϕ . By multiplying out denominators we may assume that $(a, b) \in \sigma^2$.

Our strategy is to use (a, b) in order to embed K into $k((t))$, endowed with the canonical place, P , and restrict this place to K . Now since $f(a, b) = 0$ this means $f(a + t, Y) \in k((t))[Y]$ has a simple zero at b in the residue field $P(k((t))) = k$. Furthermore $k((t))$ is henselian, therefore by Hensel's lemma we have that there exists $h(t) \in k[[t]]$ with $h(0) = b$. Now since the canonical place is rational, the restriction is rational and we note that $P(x) = P(a + t) = a$ and $P(y) = h(0) = b$. Now $P(z_i) = z_i(a, b)$ and $P(u_j) = u_j(a, b)$, for all i, j . Now since (a, b) satisfies ϕ , z_i does not have a pole for all i , $u_j(a, b) \in \sigma$ therefore $P \in S_u^z$. So the case $n = 1$ is proven.

The induction step is actually just an application of the case $n = 1$. Again by Noether's normalization we have that $K = k(x_1, \dots, x_n, f)$. By assumption, there exists a p-valuation ring $\Sigma \supseteq \sigma[u]$ on K . Let k_1 be the relative algebraic closure of $k(x_1, \dots, x_{n-1})$ inside some p-adic closure of K with respect to Σ . By the above theorem, k_1 is p-adically closed and $k_1(x_n, f)$ is a function field of transcendence degree 1 over k_1 . Applying the case $n = 1$ to this field we get $P \in S_{k_1}(k_1(x_n, f)/k_1)_u^z$. Now restricting this place to K we get a place whose residue field has transcendence degree is $n - 1$. Composing P with a place that exists by the induction hypothesis, we get the desired place. \square

Definition 3.10. *In the situation above, let D_u^z denote the set of all places of K such that $P(x) \neq \infty$ for $x \in z \cup u$ and the residue field, $P(K) \setminus \infty$, is formally p-adic over $\sigma[P(u)]$ and of transcendence degree $n - 1$.*

Corollary 3.11. $D_u^z \neq \emptyset \Leftrightarrow S_u^z \neq \emptyset$

Proof. During the induction step of the above theorem, we constructed a place in D_u^z assuming K is formally p-adic over $\sigma[u]$. We used this place to show $S_u^z \neq \emptyset$, which by the statement of the theorem is equivalent to K being formally p-adic over $\sigma[u]$. \square

The proof of the above theorem also motivates the following terminology,

Definition 3.12. An element $x \in K$ is called *holomorphic at* $P \in S$ if $P(x) \neq \infty$, or equivalently if x is in the corresponding valuation ring, denoted $\Sigma_P := P^{-1}(P(K) \setminus \infty)$. If $T \subseteq S$ then the *holomorphy ring of* T is $\bigcap_{P \in T} \Sigma_P$, for $T = \emptyset$ the *holomorphy ring* is defined to be K .

Lemma 3.13. In the situation above, K is formally p-adic over $\sigma[u]$ iff. $\frac{1}{p} \notin \sigma[u, \gamma(K)]$

The above lemma tells us that when K is formally p-adic over $\sigma[u]$, $1 + pb \neq 0$ for all $b \in \sigma[u, \gamma(K)]$, thus the set of such elements form a multiplicative system.

Definition 3.14. If K is formally p-adic over $\sigma[u]$, the localization of $\sigma[u, \gamma(K)]$ by the above multiplicative system is called the *Kochen ring of* K over $\sigma[u]$ and denoted by R_u , if K is not formally p-adic over $\sigma[u]$ then $R_u := K$.

Remark 3.15. By the above lemma if K is not formally p-adic over $\sigma[u]$, then p is a unit in $\sigma[u, \gamma(K)]$. Hence the ‘multiplicative system’ is all of $\sigma[u, \gamma(K)]$, hence by Merckel’s Lemma (see below) $K = k(\gamma(K)) = (\sigma[u, \gamma(K)])_0$, so the above definition makes sense.

The following is known as Merckel’s Lemma,

Theorem 3.16. Let l/k be an extension of fields, $\gamma(t) = \frac{f(t)}{g(t)}$ be a rational function in $k(t)$ with $(f, g) = 1$. If $\#|k| \geq \max\{\deg f, \deg g\}$ then $k(\gamma(l)) = l$.

Lemma 3.17. Let K/k be a function field over a p-adically closed field. If $x \neq 0$ is a non-unit element of $R_u * k[z]$, then there exists $P \in D_u^z$ such that $P(x) = 0$.

Lemma 3.18. In the situation as above, if $x \neq 0$ is a non-unit element of $R_u * k[z]$, then there exists $P \in D_u^z$ such that $P(x) = 0$.

Definition 3.19. A ring is called a *Bezout ring* if every finitely generated ideal is principal.

Theorem 3.20. Let k be a field and $T \neq \emptyset$ be a set of valuations of k with corresponding valuation rings σ_v such that $\text{Max}_{v \in T} \#\sigma_v = N \in \mathbb{Z}$. Then the holomorphy ring $\sigma_T := \bigcap_{v \in T} \sigma_v$ is a Bezout ring with k as its fraction field, in particular any extension of σ_T is integrally closed and any overring is also a Bezout ring.

Theorem 3.21. The valuation rings above R_u centered at some maximal ideal, $\mathfrak{m} \subseteq R_u$, are precisely the p-valuation rings with residue field $\mathbb{Z}/p\mathbb{Z}$ containing $\sigma[u]$.

Theorem 3.22. Let K/k be a function field of transcendence degree n over a p-adically closed field k . Then

$$\bigcap_{P \in S_u^z} \Sigma_P = \bigcap_{P \in D_u^z} \Sigma_P = R_u * k[z].$$

Proof. If K is not formally p-adic over $\sigma[u]$, then by Theorem 3.9, $S_u^z = \emptyset$, and hence by Corollary 3.11 $D_u^z = \emptyset$, so the holomorphy ring and the Kochen ring are just defined to be K . Thus we need to prove this theorem in the case where K is formally p-adic over $\sigma[u]$ and so again by Theorem 3.9 and Corollary 3.11 we have that S_u^z and D_u^z are non-empty.

We first show $R_u * k[z] \subseteq \bigcap_{P \in S_u^z} \Sigma_P$. Given any $P \in S_u^z$, $P(K)$ is formally p-adic over $\sigma[P(u)]$. By definition this means there exists $\theta \supseteq \sigma[P(u)]$, a valuation ring on $P(K)$. Let $\Theta := P^{-1}(\theta)$, then Θ is a p-valuation ring on K with residue field $\mathbb{Z}/p\mathbb{Z}$ containing $\sigma[u]$, hence by Theorem 3.21, $R_u \subseteq \Theta := P^{-1}(\theta) \subseteq \Sigma_P := P^{-1}(P(K) \setminus \infty)$. Now $P \in S_u^z$ also means $P(x) \neq \infty$, for all $x \in z$ hence $k[z]$ is contained in Σ_P , the set of holomorphic functions at P . Therefore $R_u * k[z] \subseteq \Sigma_P$ for all $P \in S_u^z$. The proof for all $P \in D_u^z$ is exactly the same.

Now suppose $y \in K, y \notin R_u * k[z]$. Further suppose y^{-1} is a unit in $R_u * k[z, y^{-1}]$, in particular $y \in R_u * k[z, y^{-1}]$. So,

$$y = \lambda_0 + \lambda_1 y^{-1} + \dots + \lambda_m y^{-m}.$$

Multiplying through by y^m and moving everything to one side gives that y is integral over $R_u * k[z]$. But $R_u * k[z]$ is integrally closed therefore $y \in R_u * k[z]$, a contradiction. So we have that y^{-1} is not a unit in $R_u * k[z, y^{-1}]$. Now by Lemma 3.18, there exists $P \in D_u^{z, y^{-1}}$ such that $P(y^{-1}) = 0$, in particular $P \in D_u^z$ and $y \notin \Sigma_P$, hence $\bigcap_{P \in D_u^z} \Sigma_P \subseteq R_u * k[z]$. Now apply the place existence theorem to the function field

$P(K)/k$ to get the existence of $P'' \in S_{P(u)}^{P(z)}$. Let $P' := P \circ P''$, then $P' \in S_u^z$ and $P'(y^{-1}) = 0$, so $y \notin \Sigma_{P'}$, hence $\bigcap_{P \in S_u^z} \subseteq R_u * k[z]$. \square

4. A p-ADIC ANALOGUE OF HILBERT'S 17TH PROBLEM AND THE NULLSTELLENSATZ

The following is a p-adic analogue of Hilbert's 17th problem,

Theorem 4.1. *Let K/k be a function field over a p-adically closed field, k , and $S_u^z \neq \emptyset$. Then $f \in K$ is integral definite on S_u^z if and only if $f \in R_u$.*

Proof. Assume $f \in R_u$. By Theorem 3.21, $R_u \in P^{-1}(\sigma)$ so $P(f) \in \sigma, \forall P$ i.e. f is integral definite.

Conversely, assume $P(f) \in \sigma, \forall P$. If $f \notin R_u$ then there exists a p-valuation $\Theta \supseteq \sigma[u]$ such that $f \notin \Theta$. Hence $(pf)^{-1} \in \Theta$ so K is formally p-adic over $\sigma[u, (pf)^{-1}]$ and so by Lemma 3.18, $S_{u, (pf)^{-1}}^z \neq \emptyset$. Let $P \in S_{u, (pf)^{-1}}^z$ then $P((pf)^{-1}) = P(p^{-1})P(f^{-1}) \in \sigma$ and thus $P(f) \notin \sigma$, a contradiction. \square

Stated more simply we have,

Corollary 4.2. *Let k be a p-adically closed field. If $h \in k(x_1, \dots, x_n)$ is an integral definite rational function then $f \in R_u$*

We are also ready to prove the p-adic nullstellensatz,

Theorem 4.3. *Let K/k be a function field over a p-adically closed field k . Let I be an ideal in the holomorphy ring of $S_u^z \neq \emptyset$. Then $\mathcal{I}(V(I)) = \sqrt{I}$ as ideals in $R_u * k[z]$ (i.e. the holomorphy ring on S_u^z).*

In analogy to algebraic varieties we have used the notation $V(I) = \{P \in S_u^z \mid P(f) = 0, \forall f \in I\}$ and $\mathcal{I}(T) = \{g \mid P(g) = 0, \forall P \in T\}$.

Proof. As usual, $\mathfrak{I}(V_\sigma(I)) \supseteq \sqrt{I}$. Now, suppose $g \in \mathfrak{I}(V_\sigma(I))$. $R_u * k[z]$ is a Bezout ring so $I = (f)$. Therefore our assumption becomes for all $P \in S_u^z$ if $P(f) = 0$ then $P(g) = 0$. Now since g doesn't vanish on $S_u^{z, g^{-1}} \subseteq S_u^z$ neither does f . Thus by Lemma 3.17 and the proof of Theorem 3.9, f is a unit in $R_u * k[z, g^{-1}] = (R_u * k[z])[g^{-1}]$. Therefore we have,

$$f^{-1} = \lambda_0 + \lambda_1 g^{-1} + \dots + \lambda_s g^{-s}, \text{ with } \lambda_i \in R_u * k[z]$$

Multiplying through by $f g^s$ yields $g \in \sqrt{I}$. \square

REFERENCES

- [1] M. Jarden-P. Roquette *The Nullstellensatz over p-adically closed fields*. J. Math. Soc. Japan 32(1980), 425-460.
- [2] A. Pasarescu *Nullstellensatz for real fields using model theory* Anul LI(2002), 153-158.
- [3] A. Prestel-P. Roquette *Formally p-adic Fields*. Berlin: Springer-Verlag, 1984.

UNIVERSITY OF PENNSYLVANIA
DEPARTMENT OF MATHEMATICS
209 SOUTH 33RD STREET
PHILADELPHIA, PA 19104
favero@math.upenn.edu