Lectures on elimination theory for semialgebraic and subanalytic sets.

A.J. Wilkie
School of Mathematics
The Alan Turing Building
University of Manchester
Manchester M13 9PL
UK

May 14, 2013

During the Fall Semester of 2010 I gave a course of lectures at the University of Illinois at Chicago, repeated at the University of Notre Dame, to the graduate students in Logic, and these are the notes of that course. I am extremely grateful to David Marker and Sergei Starchenko for the invitations, and for their kind hospitality during my visit. Many thanks also to the students for typing up the notes, which had remained in scruffy hand written form since I first gave a version of the course to the Logic Advanced Class in Oxford during the Trinity Term of 1994.

My intention in these lecture notes is to present all the mathematical background required for the proof of the quantifier elimination theorem of Denef and van den Dries for the structure $\mathbb{R}_{\mathrm{an}}$ in a language with a function symbol for division. Of course, I also give the proof of the theorem itself and here I experimented with using the model theoretic embedding criterion for quantifier elimination rather than following the original paper. However, I now feel that any improvements are minimal and cosmetic.

The prerequisites are, I hope, just a working knowledge of undergraduate algebra and analysis and an introductory graduate course in model theory. So I present the theory of Noetherian rings up to the Artin-Rees Lemma and the Krull Intersection Theorem on the algebraic side, and the basics of convergent power series and analytic functions up to the Weierstrass Preparation Theorem on the analytic side. The two sides come together in the proof of the deepest mathematical result used by Denef and van den Dries, namely the flatness of the ring of convergent power series in the ring of formal power series. (In fact, only the linear closure (and for just one linear equation) of the former ring in the latter is actually needed, so I do not need to mention the general notion of flatness, and thereby avoid a discussion of tensor products.)

Given the prerequisites, the text is intended to be understood without further references, so I have not included any. So let me mention now that for the algebra I have used

R. Y. Sharp, 'Steps in Commutative Algebra', LMS Student Texts 19, CUP, 1990, and

H. Matsumura, 'Commutative Ring Theory', Cambridge Studies in Advanced Mathematics 8, CUP, 1986.

For the theory of convergent (and formal) power series I have (slavishly) followed

J. M. Ruiz, 'The Basic Theory of Power Series', Advanced Lectures in Mathematics, Vieweg, 1993.

I acquired the material in the first section over many years and through many texts and lectures. I think my very first source was

G. E. Sacks, 'Saturated Model Theory', Mathematics Lecture Notes Series, W.A. Benjamin, 1972.

Finally, the paper itself is

J. Denef and L. van den Dries. p-Adic and Real Subanalytic Sets, Annals of Mathematics 128 (1988), 79-138.

1 Model Theoretic Generalities

Let $\mathcal{L}$ be any first-order language, and

$$\begin{aligned} \exists_0 = \forall_0 &:= \text{the class of quantifier free } \mathcal{L}\text{-formulas}, \\ \exists_{n+1} &:= \{\varphi \mid \varphi \text{ is logically equivalent to } \exists\bar{x}\ \psi \text{ for some } \psi \in \forall_n\}, \\ \forall_{n+1} &:= \{\varphi \mid \varphi \text{ is logically equivalent to } \forall\bar{x}\ \psi \text{ for some } \psi \in \exists_n\}. \end{aligned}$$

Each class $\exists_n, \forall_n$ is closed under $\wedge$ and $\vee$, and $\varphi \in \exists_n$ (or $\forall_n$) $\Leftrightarrow \neg\varphi \in \forall_n$ (or $\exists_n$, respectively).

For $\mathfrak{A}$ an $\mathcal{L}$-structure, $\mathcal{L}(\mathfrak{A})$ denotes the language obtained by adding a constant symbol c_a for each $a \in \mathfrak{A}$ (i.e. $a \in \mathrm{dom}(\mathfrak{A})$) and $\mathfrak{A}^+$ denotes the natural expansion of $\mathfrak{A}$ to an $\mathcal{L}(\mathfrak{A})$-structure.

$$D_n(\mathfrak{A}) = \left\{\varphi \;\middle|\; \varphi \text{ a } \forall_n\text{-sentence of } \mathcal{L}(\mathfrak{A}) \text{ such that } \mathfrak{A}^+ \models \varphi\right\}.$$

If $\mathfrak{B}$ is another $\mathcal{L}$-structure, $e : \mathfrak{A} \to_n \mathfrak{B}$ means that

(i) e is an embedding from $\mathfrak{A}$ to $\mathfrak{B}$, and

(ii) for all $\forall_n$ (equivalently, $\exists_n$) formulas $\varphi(\bar{x})$ of $\mathcal{L}$, and for all $\bar{a} \in \mathfrak{A}$,

$$\mathfrak{A} \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{B} \models \varphi(e(\bar{a})).$$

Further, $e : \mathfrak{A} \to_\infty \mathfrak{B}$ means $e : \mathfrak{A} \to_n \mathfrak{B}$ for all n, i.e. e is *elementary.*

Suppose $\mathfrak{A}$ is an $\mathcal{L}$-structure and $\mathfrak{B}$ an $\mathcal{L}(\mathfrak{A})$-structure such that $\mathfrak{B} \models D_n(\mathfrak{A})$. Then the map $e : \mathrm{dom}(\mathfrak{A}) \to \mathrm{dom}(\mathfrak{B})$ sending $a \mapsto c_a^{\mathfrak{B}}$ satisfies $e : \mathfrak{A} \to_n \mathfrak{B} \restriction \mathcal{L}$. Conversely, if $\mathfrak{C}$ is an $\mathcal{L}$-structure and $e : \mathfrak{A} \to_n \mathfrak{C}$, then $\langle \mathfrak{C}, e(a) \rangle_{a \in \mathfrak{A}} \models D_n(\mathfrak{A})$.

Definition 1.1. *An $\mathcal{L}$-theory T is called* model complete *if $D_0(\mathfrak{A}) \cup T$ is a complete $\mathcal{L}(\mathfrak{A})$-theory for any $\mathfrak{A} \models T$.*

Theorem 1.2. *Let T be an $\mathcal{L}$-theory. The following are equivalent:*

(i) T is model complete;

(ii) Whenever $\mathfrak{A}, \mathfrak{B} \models T$ and $e : \mathfrak{A} \to_0 \mathfrak{B}$, then $e : \mathfrak{A} \to_1 \mathfrak{B}$;

(iii) Whenever $\mathfrak{A}, \mathfrak{B} \models T$ and $e : \mathfrak{A} \to_0 \mathfrak{B}$ then $e : \mathfrak{A} \to_\infty \mathfrak{B}$;

(iv) For any formula $\varphi(\bar{x})$ there exists an $\exists_1$ formula $\psi(\bar{x})$ such that

$$T \models \forall \bar{x} \left(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}) \right).$$

Proof. (i)⇒(iii): Let $\varphi(\bar{x})$ be an $\mathcal{L}$-formula, $\bar{a} \subseteq \mathfrak{A}$, and $e : \mathfrak{A} \to_0 \mathfrak{B}$. Suppose $\mathfrak{A} \models \varphi(\bar{a})$. Now $\mathfrak{A}^+, \langle \mathfrak{B}, e(a) \rangle_{a \in \mathfrak{A}} \models D_0(\mathfrak{A}) \cup T$. Hence, by (i), $\mathfrak{A}^+ \equiv \langle \mathfrak{B}, e(a) \rangle_{a \in \mathfrak{A}}$. Therefore, $\mathfrak{B} \models \varphi(e(\bar{a}))$.

(iii)⇒(ii): Obvious.

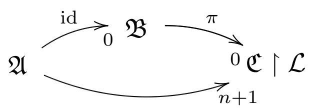
(ii)⇒(iii): We prove by induction on $n \geq 1$ that for all $\mathfrak{A}, \mathfrak{B} \models T$,

$$e : \mathfrak{A} \to_0 \mathfrak{B} \Rightarrow e : \mathfrak{A} \to_n \mathfrak{B}.$$

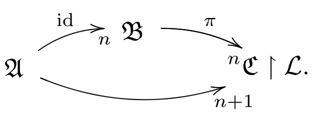
The case $n = 1$ is just (ii). Suppose true for some $n \geq 1$. Suppose $\mathfrak{A}, \mathfrak{B} \models T$ and $e : \mathfrak{A} \to_n \mathfrak{B}$. We want to show $e : \mathfrak{A} \to_{n+1} \mathfrak{B}$.

By replacing $\mathfrak{A}$ by its image we may suppose $e = \mathrm{id}_{\mathfrak{A}}$. Hence we may consider the $\mathcal{L}(\mathfrak{B})$-theory $T^* = D_{n+1}(\mathfrak{A}) \cup D_0(\mathfrak{B}) \cup T$. Suppose T^* had no model. Then $D_{n+1}(\mathfrak{A}) \cup T \models \neg\varphi$ for some $\varphi \in D_0(\mathfrak{B})$. Write φ as $\psi(c_{\bar{a}}, c_{\bar{b}})$ where $\bar{a} \subseteq \mathfrak{A}$, $\bar{b} \subseteq \mathfrak{B} \setminus \mathfrak{A}$, and $\psi(\bar{x}, \bar{y})$ is an $\exists_0$-formula of $\mathcal{L}$. Then $D_{n+1}(\mathfrak{A}) \cup T \models \neg\psi(c_{\bar{a}}, c_{\bar{b}})$, so $D_{n+1}(\mathfrak{A}) \cup T \models \forall \bar{y}\ \neg\psi(c_{\bar{a}}, \bar{y})$. Thus $\mathfrak{A} \models \neg\chi(\bar{a})$ where $\chi(\bar{x}) := \exists \bar{y}\ \psi(\bar{x}, \bar{y})$. However, $\mathfrak{B} \models \chi(\bar{a})$ (take $\bar{y} = \bar{b}$), contradicting $\mathrm{id}_{\mathfrak{A}} : \mathfrak{A} \to_1 \mathfrak{B}$.

Therefore, T^* has a model, say $\mathfrak{C}$. Then



for some π. Hence, by the induction hypothesis,



Now suppose $\bar{a} \subseteq \mathfrak{A}$, $\varphi(\bar{x})$ is $\exists_{n+1}$ and $\mathfrak{B} \models \varphi(\bar{a})$. Then $\pi : \mathfrak{B} \to_n \mathfrak{C} \restriction \mathcal{L}$ clearly implies $\mathfrak{C} \restriction \mathcal{L} \models \varphi(\pi(\bar{a}))$. So $\mathfrak{A} \models \varphi(\bar{a})$ since $\pi : \mathfrak{A} \to_{n+1} \mathfrak{C} \restriction \mathcal{L}$, as required.

(iii)⇒(iv): Let $\varphi(\bar{x})$ be any formula of $\mathcal{L}$. Let

$$S = \{ \psi(\bar{x}) \mid \psi(\bar{x}) \in \exists_1 \text{ and } T \models \forall \bar{x} \left(\psi(\bar{x}) \to \varphi(\bar{x}) \right) \}.$$

Let $\bar{c}$ be new constant symbols. It suffices to show that

$$T^* = T \cup \{\neg\psi(\bar{c}) \mid \psi(\bar{x}) \in S\} \cup \{\varphi(\bar{c})\}$$

is inconsistent, for then $T \models \forall \bar{x} \left(\bigwedge_{i=1}^{n} \neg\psi_i(\bar{x}) \to \neg\varphi(\bar{x}) \right)$ for some $\psi_1, \ldots, \psi_n \in S$ and then $\varphi(\bar{x})$ is equivalent to $\bigvee_{i=1}^{n} \psi_i(\bar{x})$ in T.

Suppose, for a contradiction, that $\mathfrak{A}' \models T^*$. Let $\mathfrak{A} = \mathfrak{A}' \restriction \mathcal{L}$ and $\bar{a} = \bar{c}^{\mathfrak{A}'}$. Then $\mathfrak{A} \models \varphi(\bar{a})$ and $\mathfrak{A} \models \neg\chi(\bar{a})$ for $\chi(\bar{x}) \in S$. Let $T' = T \cup D_0(\mathfrak{A}) \cup \{\neg\varphi(c_{\bar{a}})\}$. Then T' is consistent, for otherwise $T \models \psi(c_{\bar{a}}, c_{\bar{b}}) \to \varphi(c_{\bar{a}})$, for some $\psi(c_{\bar{a}}, c_{\bar{b}}) \in D_0(\mathfrak{A})$ where $\psi(\bar{x}, \bar{y})$ is an $\exists_0$-formula of $\mathcal{L}$, $\bar{b} \subseteq \mathfrak{A} \setminus \{\bar{a}\}$. But then $\exists \bar{y}\ \psi(\bar{x}, \bar{y}) \in S$ and $\mathfrak{A} \models \exists \bar{y}\ \psi(\bar{a}, \bar{y})$, a contradiction. Thus T' has a model, say $\mathfrak{C}$. We have $e : \mathfrak{A} \to_0 \mathfrak{C} \restriction \mathcal{L}$ and $\mathfrak{C} \restriction \mathcal{L} \models \neg\varphi(e(\bar{a}))$, contradicting (iii).

(iv)$\Rightarrow$(i): Suppose $\mathfrak{A} \models T$, $\mathfrak{B} \models T \cup D_0(\mathfrak{A})$. Let $\varphi(c_{\bar{a}})$ be any sentence of $\mathcal{L}(\mathfrak{A})$, where $\bar{a} \subseteq \mathfrak{A}$, $\varphi(\bar{x})$ an $\mathcal{L}$-formula. Let $e : \mathfrak{A} \to \mathfrak{B} \restriction \mathcal{L}$ be the natural embedding. Since $\varphi(\bar{x})$ is T-equivalent to an $\exists_1$-formula by (iv), we have

$$\mathfrak{A}^+ \models \varphi(c_{\bar{a}}) \Rightarrow \mathfrak{B}^+ \models \varphi(c_{\bar{a}}).$$

Hence $\mathrm{Th}(\mathfrak{B}) = \mathrm{Th}(\mathfrak{A}^+)$ for any $\mathfrak{B} \models T \cup D_0(\mathfrak{A})$, and $T \cup D_0(\mathfrak{A})$ is complete. □

Remark. (iv) is the interesting property; it is often proved by showing (ii), which can often be reduced to showing that whenever $\mathfrak{A}, \mathfrak{B} \models T$, $\mathfrak{A} \subseteq \mathfrak{B}$ then $\mathfrak{A}$ is "algebraically closed" in $\mathfrak{B}$ for some natural notion of algebraic closedness.

Definition 1.3. *Let T be an $\mathcal{L}$-theory. T is called* substructure complete *if $D_0(\mathfrak{A}) \cup T$ is a complete $\mathcal{L}(\mathfrak{A})$-theory for any $\mathfrak{A}$ which is a substructure of some model of T.*

Theorem 1.4. *Let T be an $\mathcal{L}$-theory. The following are equivalent:*

(i) T is substructure complete;

(ii) T eliminates quantifiers, i.e. for any formula $\varphi(\bar{x})$ there exists an $\exists_0$-formula $\psi(\bar{x})$ such that $T \models \forall \bar{x}\, (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

Remark. *If $\bar{x}$ is the empty string here, i.e. if φ is a sentence, then we need to assume that our language contains at least one constant symbol. Where is this needed in the proof below?*

Proof. (ii)$\Rightarrow$(i): Exercise. Similar to (iv)$\Rightarrow$(i) above.

(i)$\Rightarrow$(ii): Let $\varphi(\bar{x})$ be any $\mathcal{L}$-formula. Let

$$S_0 = \{\psi(\bar{x}) \in \exists_0 \mid T \models \forall \bar{x}\, (\psi(\bar{x}) \to \varphi(\bar{x}))\}.$$

Let $\bar{c}$ be new constant symbols and $T_0 = T \cup \{\varphi(\bar{c})\} \cup \{\neg\psi(\bar{c}) \mid \psi \in S_0\}$. As in the proof of (iii)$\Rightarrow$(iv) above it is sufficient to show T_0 is inconsistent. Suppose, for contradiction, that $\mathfrak{A} \models T_0$.

Let $S_1 = \{\psi(\bar{x}) \in \exists_0 \mid \mathfrak{A} \models \psi(\bar{c})\}$. Thus $\neg\psi(\bar{x}) \in S_1$ for each $\psi(\bar{x}) \in S_0$. We claim that $T_1 = T \cup \{\neg\varphi(\bar{c})\} \cup \{\psi(\bar{c}) \mid \psi(\bar{x}) \in S_1\}$ has a model. For otherwise, $T \models \forall\bar{x}\left(\bigwedge_{i=1}^{n} \psi_i(\bar{x}) \rightarrow \varphi(\bar{x})\right)$ and hence $\bigwedge_{i=1}^{n} \psi_i(\bar{x}) \in S_0$ for some $\psi_1, \ldots, \psi_n \in S_1$. But then $\bigwedge_{i=1}^{n} \psi_i$ and $\neg \bigwedge_{i=1}^{n} \psi_i$ are in S_1, contradicting the fact that $\mathfrak{A} \models \psi(\bar{c})$ for all $\psi \in S_1$.

Now if $\mathfrak{B} \models T_1$, then $\bar{c}^{\mathfrak{B}}$ and $\bar{c}^{\mathfrak{A}}$ satisfy the same $\exists_0$-formulas in $\mathfrak{B} \restriction \mathcal{L}$ and $\mathfrak{A} \restriction \mathcal{L}$ respectively. Hence they generate canonically isomorphic substructures, and so, by (i), $\mathfrak{A} \equiv \mathfrak{B}$. But $\mathfrak{A} \models \varphi(\bar{c})$ and $\mathfrak{B} \models \neg\varphi(\bar{c})$, a contradiction. □

Theorem 1.5 (Practical test for elimination of quantifiers)**.** *Let T be an $\mathcal{L}$-theory. Suppose that whenever we have $\mathfrak{B}_1, \mathfrak{B}_2 \models T$ and an embedding $e : \mathfrak{A} \rightarrow \mathfrak{B}_2$ with $\mathfrak{A} \subseteq \mathfrak{B}_1$, and $\mathfrak{B}_2$ sufficiently saturated (relative to $|\mathfrak{A}|, |\mathcal{L}|$), then for all $a \in \mathfrak{B}_1$, e extends to some $e' : \mathfrak{A}' \rightarrow \mathfrak{B}_2$ where $\mathfrak{A} \subseteq \mathfrak{A}' \subseteq \mathfrak{B}$ and $a \in \mathfrak{A}'$. Then T eliminates quantifiers.*

Proof. Let $\mathfrak{A} \subseteq \mathfrak{B} \models T$. Let $\mathfrak{B}_1, \mathfrak{B}_2$ be two $\mathcal{L}(\mathfrak{A})$-structures such that $\mathfrak{B}_1, \mathfrak{B}_2 \models T \cup D_0(\mathfrak{A})$. We want to show, by 1.4, that $\mathfrak{B}_1 \equiv \mathfrak{B}_2$. We may suppose $\mathfrak{B}_1, \mathfrak{B}_2$ sufficiently saturated, $\mathfrak{A} \subseteq \mathfrak{B}_1 \restriction \mathcal{L}$. Define $e : \mathfrak{A} \rightarrow \mathfrak{B}_2, a \mapsto c_a^{\mathfrak{B}_2}$. One now easily shows by induction on n, using the condition above, that if $e^* : \mathfrak{A}^* \rightarrow \mathfrak{B}_2 \restriction \mathcal{L}$ extends e (where $\mathfrak{A} \subseteq \mathfrak{A}^* \subseteq \mathfrak{B}_1 \restriction \mathcal{L}$, $|\mathfrak{A}^*| \leq |\mathfrak{A}| + |\mathcal{L}| + \aleph_0$), then

$$\mathfrak{B}_1 \restriction \mathcal{L} \models \varphi(\bar{a}) \Leftrightarrow \mathfrak{B}_2 \restriction \mathcal{L} \models \varphi(e^*(\bar{a}))$$

for all formulas $\varphi(\bar{x})$ of $\mathcal{L}$ containing at most n occurrences of quantifiers and $\bar{a} \subseteq \mathfrak{A}^*$. Hence $\mathfrak{B}_1 \equiv \mathfrak{B}_2$. □

2 The Real Field

Throughout the rest of this paper we will let $\overline{\mathbb{R}} = \langle \mathbb{R}; +, \cdot, -; 0, 1; < \rangle$ denote the ordered ring of real numbers. We further let $\overline{T} = \mathrm{Th}(\overline{\mathbb{R}})$. We aim to prove that $\overline{T}$ has elimination of quantifiers. (Of course, Tarski's theorem is much stronger: let RCF be the subtheory of $\overline{T}$ axiomatized by the axioms for ordered fields together with $\{\forall y_{n-1}, \ldots, y_0 \exists x\ x^n + y_{n-1}x^{n-1} + \cdots + y_0 = 0 : n = 1, 2, \ldots\}$. Then Tarski showed that RCF has effective elimination of quantifiers and axiomatizes $\overline{T}$.)

Definition 2.1. *For k, K, fields with $k \subseteq K$, we say that k is n-closed in K if whenever $p(x) \in k[x]$ is of degree less than or equal to n and $\alpha \in K$ satisfies $p(\alpha) = 0$, then $\alpha \in k$.*

Lemma 2.2. *Suppose $K_1, K_2 \models \overline{T}$, $k \subseteq K_1$, k a field, and $e : k \rightarrow_0 K_2$. Suppose further that k is n-closed ($n \geq 1$) in K_1 and $e[k]$ is n-closed in K_2. Then if $\alpha \in K_1 \backslash k$ has degree less than or equal to $n+1$ over k, $\exists e_1 : k[\alpha] \rightarrow_0 K_2$ extending e.*

Proof. Let $q(x)$ be the minimal monic polynomial of α over k. Then $q(x) = x^{n+1} + a_n x^n + \cdots + a_0$ $(a_0, \ldots, a_n \in k)$ is irreducible over k since $\alpha \notin k$ and k is n-closed in K_1. The image of q under e is therefore irreducible over $e[k]$. Choose $a, b \in k$ such that $a < \alpha < b$ (e.g. $a = -\sum_{i=1}^{n} |a_i|$, $b = \sum_{i=1}^{n} |a_i|$). Now, all the roots in K_1 of $q'(x) = 0$ lie in k ($q'(x)$ is the formal derivative of q), so we may suppose that a and b are chosen so that $q'(x)$ has no roots in (a, b). By using sentences in $\overline{T}$ (quantify over the coefficients) it follows that $q(a)$ and $q(b)$ have opposite signs. Therefore, so do $q^e(e(a))$ and $q^e(e(b))$ (since $e : k \to K_2$) and hence (again by using sentences in $\overline{T}$) $q^e(x)$ has a root, say β in K_2 such that $e(a) < \beta < e(b)$. Since $q(x)$ is irreducible, $k(\alpha) \cong e[k](\beta)$ as fields (via $\alpha \mapsto \beta$, $s \mapsto e(s)$ $(s \in k)$).

We must show that this map preserves order. So, suppose that $p(x) \in k[x]$ is any polynomial. Choose $s(x), r(x) \in k[x]$ such that $p(x) \equiv s(x)q(x) + r(x)$ and $\deg r \leq n$ (recall that q is monic of degree n). Then $p^e(x) \equiv s^e(x)q^e(x) + r^e(x)$, $p(\alpha) = r(\alpha)$, $p^e(\beta) = r^e(\beta)$.

Suppose that $p(\alpha) > 0$. Then we want to show $p^e(\beta) > 0$. We have that $r^e(\alpha) > 0$, so it is sufficient to show that $r^e(\beta) > 0$.

Now all roots in K_1 of $r(x)$ lie in k. Similarly for K_2, $r^e(x)$, and $e[k]$. Now choose some $a' \geq a$ and $b' \leq b$ (in k) such that $\alpha \in (a', b')$ and (a', b') contains no roots of $r(x)$. Then $(e(a'), e(b'))$ contains no roots of $r^e(x)$ (consider e^{-1} to see that this is true). Now, $r(\alpha) > 0$, therefore $r(\frac{a'+b'}{2}) > 0$. Thus, $r^e(\frac{e(a')+e(b')}{2}) > 0$, and hence, $r^e(x) > 0$ for all $x \in (e(a'), e(b'))$. Now, with this information, we see that it is sufficient to show that $\beta \in (e(a'), e(b'))$.

Now, q is monotonic on (a', b'), and has a root therein. Hence, $q(a')$ and $q(b')$ have opposite signs. Thus, $q^e(e(a'))$ and $q^e(e(b'))$ have different signs, which implies that q^e has *some* root in $(e(a'), e(b'))$. Suppose it is not β. Then q^e has at least two distinct roots in $(e(a), e(b))$ and so q'^e has a root in $(e(a), e(b))$. Since $\deg q^e \leq n$, this root lies in $e[k]$, and hence (via e^{-1}) q' has a root in (a, b)-contradiction. □

Lemma 2.3. *Suppose $K_1, K_2 \models \overline{T}$, k_i is a subfield of K_i $(i = 1, 2)$, and $e : k_1 \to k_2$ is an isomorphism. Then there exist k_i^* (subfield of K_i) such that $k_i \subseteq k_i^* \subseteq K_i$ $(i = 1, 2)$ and an isomorphism $e^* : k_1^* \to k_2^*$ extending e such that k_i^* is n-closed in K_i for all n.*

Proof. Just let

$$\mathcal{S} = \{< k_1', k_2', e' >: k_i \subseteq k_i' \subseteq K_i, k_i' \text{ a subfield of } K_i \text{ and } e' \text{extends } e\}.$$

Now, order $\mathcal{S}$ by extension. Then $\mathcal{S}$ satisfies the hypotheses of Zorn's lemma. Hence, $\mathcal{S}$ has a maximal element, $\langle k_1^*, k_2^*, e^* \rangle$, say. Then k_i^* is certainly 1-closed in K_i (since k_i^* is a field). Then, 2.2 tells us that if k_i^* is n-closed in K_i, then it is $n+1$-closed. □

Lemma 2.4. *Suppose that $K_1, K_2 \models \overline{T}$, k a subring of K_1 and $e : k \to_0 K_2$. Suppose further that K_2 is sufficiently saturated (with respect to $|k|$). Then $\forall \alpha \in K_1$, we can extend e to $e' : k[\alpha] \to_0 K_2$.*

Proof. We may clearly extend e to the subfield of K_1 generated by k, so we may as well suppose that k is a subfield of K_1. Now, apply 2.3 with $k_1 = k$ and $k_2 = e[k]$ to get $e^* : k_1^* \to k_2^*$, extending e, an isomorphism with k_i^* n-closed in K_i (i.e. algebraically closed) for all n and $i = 1, 2$. If $\alpha \in k_1^*$, we're already done (let $e' = e^* \restriction k[\alpha]$). Otherwise, α is transcendental over k_1^*. Without loss of generality, we may assume that $\alpha > 0$. Now suppose $p_1(x), \ldots, p_n(x) \in k[x]$. Let $\mathcal{S} = \cup_{i=1}^n \{\text{roots of } p_i \text{ in } K_1\}$.

Then $\mathcal{S} \subseteq k_1^*$. Let $a = \sup(\{0\} \cup \{\beta \in \mathcal{S} : \beta < \alpha\})$. If $\alpha > \beta$ for all $\beta \in \mathcal{S}$, then $p_i(a+1)$ and $p_i(\alpha)$ have the same sign for $i = 1, \ldots, n$. Otherwise, let $b = \inf(\beta \in \mathcal{S} : \alpha < \beta)$. Then $p_i(\frac{a+b}{2})$ and $p_i(\alpha)$ have the same sign for $i = 1, \ldots, n$. In either case, there is some $c \in k_1^*$ such that sign$p_i(c)$ =sign$p_i(\alpha)$ for $i = 1, \ldots, n$. Therefore, sign$(p_i^e(e^*(c)))$ =sign$p_i(\alpha)$ for $i = 1, \ldots, n$.

Hence,

$$\{p^e(x) > 0 \wedge q^e(x) < 0 : p(x), q(x) \in k[x], K_1 \models p(\alpha) > 0 \wedge q(\alpha) < 0\}$$

is finitely satisfiable in K_2 and therefore satisfiable, by saturation, by $\gamma \in K_2$, say. Clearly, extending e by $\alpha \mapsto \gamma$ gives the required embedding $e' : k[\alpha] \to_0 K_2$. $\square$

Theorem 2.5. *$\overline{T}$ eliminates quantifiers.*

Proof. Apply 2.4 and 1.5. $\square$

3 Preliminary Remarks on Rings and Modules

We will take as convention, 'ring' to always mean a commutative ring with identity. Ring homomorphisms preserve 1, and scalar multiplication by 1 is the identity map on any module. Let R be a ring. An R-module is *finite* if it is finitely generated (as an R-module). Recall that R is *Noetherian* if every ideal of R is finitely generated, i.e. if any submodule of the R-module R is finite.

An R-module M is called *Noetherian* if every submodule of M is finite. If R is Noetherian then any finite R-module is as well. For if M is a finite R-module containing a non-finite submodule then by Zorn's lemma, there exists a maximal such, N say. Since M is finite, pick $m \in M \setminus N$ and let N' be the submodule of M generated by N and m. Then N' is finite (by maximality of N), so it is generated by m and $m_1, \ldots, m_n \in N$. (Remark: if something is finitely generated then any generating set contains a finite subset which is generating.) Let $J = \{b \in R : bm \in N\}$. Then J is an ideal of R, so it is finitely generated, say by $b_1, \ldots, b_s$. I claim that the finite subset $\{m_1, \ldots, m_n, b_1 m, \ldots, b_s m\}$ of N generates all of N - contradiction. For suppose that $m' \in N$. Then certainly $m' \in N'$, so $a_1 m_1 + \cdots + a_n m_n + bm = m'$. for some $a_1, \ldots, a_n, b \in R$. It follows that $b \in J$, so $b = r_1 b_1 + \cdots + r_s b_s$ for some $r_1, \ldots, r_s \in R$. We now have

$$a_1 m_1 + \cdots + a_n m_n + r_1(b_1 m) + \cdots + r_s(b_s m) = m',$$

as required. The same proof seems to prove a totally different theorem, I.S. Cohen's lemma:

Lemma 3.1. *A ring R is Noetherian if and only if every prime ideal of R is finitely generated.*

Proof. As above, if R contains a non-finitely generated ideal it contains a maximal such, call it I. We show I is prime. Suppose not, say $\alpha\beta \in I$, for $\alpha, \beta \in R \setminus I$. Then the ideal generated by β and I is finitely generated and also $\{b \in R : b\beta \in I\}$ is an ideal of R containing I and α. This ideal is finitely generated. Now proceed as above. □

We use this to deduce the famous Hilbert Basis Theorem.

Theorem 3.2. *Let R be a Noetherian ring. Then the ring $R[x]$ of polynomials in the variable x over R is also Noetherian.*

Proof. Every $f(x) \in R[x]$ may be written in the form $f(0) + xg(x)$ for some $g(x) \in R[x]$ (with $\deg g < \deg f$).

Let P be a prime ideal of $R[x]$. If $x \in P$ then it follows that whenever $f(x) \in P$ then $f(0) \in P$, so P is generated by $\{f(0) : f(x) \in P\} \cup \{x\}$. But $\{f(0) : f(x) \in P\}$ is an ideal of R, so is finitely generated. Thus P is finitely generated as an ideal of $R[x]$.

So, suppose that $x \notin P$. If P is not finitely generated, the following process may be continued indefinitely:

$f_1(x) =$ a polynomial of minimal degree in P,

$f_{n+1}(x) =$ a polynomial of minimal degree in P not in the ideal generated by $\{f_1(x), \ldots, f_n(x)\}$.

Clearly, $f_n(x) \in P$ for all n and $i \leq j$ implies that $\deg f_i \leq \deg f_j$. Now the ideal of R generated by $\{f_n(0) : n = 1, 2, \ldots\}$ is finitely generated by $f_1(0), \ldots, f_N(0)$, say. So there exists $a_1, \ldots, a_N \in R$ such that

$$a_1 f_1(0) + \cdots + a_N f_N(0) - f_{N+1}(0) = 0.$$

Therefore,

$$a_1 f_1(x) + \cdots + a_N f_N(x) - f_{N+1}(x) = xg(x)$$

for some $g(x) \in R[x]$. Now, $\deg g < \deg f_{N+1}$, and $xg(x) \in P$. Hence $g(x) \in P$ since $x \notin P$ and P is prime. It follows that $g(x)$ is in the ideal generated by $f_1(x), \ldots, f_N(x)$ (otherwise we could have chosen $f_{N+1}(x)$ of smaller degree) and hence $f_{N+1}(x)$ is also in this ideal. This is a contradiction. □

Corollary 3.3. *Let R, S be rings with $R \subseteq S$ and let S be finitely generated (as a ring) over R. Suppose further that R is Noetherian. Then S is also Noetherian.*

Proof. Suppose that $s_1, \ldots, s_n$ generates S over R. By 3.2, and induction, the polynomial ring $R[x_1, \ldots, x_n]$ in the variables $x_1, \ldots, x_n$ is Noetherian. There exists an surjective homomorphism $R[x_1, \ldots, x_n] \to S$ sending $r \mapsto r$ for $r \in R$ and $x_i \mapsto s_i$. But clearly, a homomorphic image of a Noetherian ring is also Noetherian. □

4 Formal Power Series Rings

Definition 4.1. *Let R be a ring. The ring $R[[x]]$ of* formal power series *in the variable x consists of, by definition, all series of the form*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \qquad (a_i \in R, i = 0, 1 \dots)$$

with addition defined by

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and multiplication by

$$\Big(\sum_{n=0}^{\infty} a_n x^n\Big) \cdot \Big(\sum_{n=0}^{\infty} b_n x^n\Big) = \sum_{n=0}^{\infty} \Big(\sum_{i+j=n} a_i b_j\Big) x^n.$$

One readily checks that $R[[x]]$ is a ring and we identify R with the subring of $R[[x]]$ consisting of the f's having $0 = a_1 = a_2 = \dots$. Write $f(0)$ for a_0 ($f(r)$ has no meaning for any other $r \in R$).

Theorem 4.2. *Suppose that R is Noetherian. Then so is $R[[x]]$.*

Proof. Every $f(x) \in R[[x]]$ may be written as $f(0)+xg(x)$ for some $g(x) \in R[[x]]$, so if we let P be a prime ideal of $R[[x]]$, then as in 3.2, if $x \in P$, then P is finitely generated. Suppose $x \notin P$. Then the ideal $\{f(0) : f(x) \in P\}$ of R is finitely generated by $f_1(0), \dots, f_n(0)$, say. I claim that $f_1(x), \dots, f_n(x)$ generates P. Let $g(x) \in P$, and suppose that for some $l > 0$, we have polynomials $p_1^{(l)}(x), p_2^{(l)}(x), \dots, p_n^{(l)}(x) \in R[[x]]$ of degree $\leq l$ such that

$$(*)_l : \qquad \sum_{i=1}^{n} p_i^{(l)}(x) f_i(x) - g(x) = x^{l+1} h_l(x)$$

for some $h_l(x) \in R[[x]]$. We set $p_i^{(-1)}(x) \equiv 0$ for $i = 1, \dots, n$. Then certainly $x^{l+1} h_l(x) \in P$ so $h_l(x) \in P$ since $x \notin P$ and P is prime. Hence there exist $r_1, \dots, r_n \in R$ such that $\sum_{i=0}^{n} r_i f_i(0) = h_l(0)$. Then

$$\sum_{i=1}^{n} (p_i^{(l)}(x) - r_i x^{l+1}) f_i(x) - g(x) = x^{l+1} \underbrace{(h_l(x) - \sum_{i=1}^{n} r_i f_i(x))}_{s(x)}.$$

But $s(0) = 0$ so $s(x) = x h_{l+1}(x)$ for some $h_{l+1}(x) \in R[[x]]$ and we've "extended" the $p_i^{(l)}$'s to obtain $(*)_{l+1}$.

Let $\phi_i(x)$ be the unique element of $R[[x]]$ extending all of the $p_i^{(l)}$'s for $i = 1, \dots, n$. Then clearly the coefficients of x^l in $\sum_{i=1}^{n} \phi_i(x) f_i(x) - g(x)$ is the same as the coefficient of x^l in $\sum_{i=1}^{n} p_i^{(l)}(x) f_i(x) - g(x)$, i.e. 0, for all l. Hence $g(x) = \sum_{i=1}^{n} \phi_i(x) f_i(x)$, and we are done. $\square$

Theorem 4.3. *$f(x)$ is a unit in $R[[x]]$ if and only if $f(0)$ is a unit in R.*

Proof. First, suppose that $f(x)$ is a unit in $R[[x]]$. Then, $f(x)g(x) = 1$ implies that $f(0)g(0) = 1$, so $f(0)$ is a unit in R.

For the converse, let

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

with a_0 a unit in R. Define $b_0 = a_0^{-1}$ and

$$b_{n+1} = -a_0^{-1}(a_1 b_n + \; a_2 b_{n-1} + \cdots + a_{n+1} b_0).$$

Then we have

$$\sum_{i+j=0} a_i b_j = 1, \qquad \sum_{i+j=n} a_i b_j = 0 \text{ for } n \geq 1.$$

Hence $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1$. □

Theorem 4.4. *For an ideal I of R, let $\hat{I}$ be the ideal of $R[[x]]$ generated by I and x. Then $I \mapsto \hat{I}$ is a bijection from the maximal ideals of R to those of $R[[x]]$.*

Proof. Proof left as exercise for the reader. □

5 Adically Normed Rings

Begin by fixing a ring R.

Definition 5.1. *A function $||\cdot|| : R \to \mathbb{R}$ is called a* norm *(or rather, an* adic norm*) on R if for all a and b in R, we have:*

1. *$0 \leq ||a|| \leq 1$ with $||a|| = 0 \leftrightarrow a = 0$;*
2. *$||ab|| \leq ||a|| \; ||b||$;*
3. *$||a + b|| \leq \max\{||a||, ||b||\}$.*

Now, fix an adic norm $||\cdot||$ on R.

Lemma 5.2. *Let $u, a \in R$, with u a unit. Then $||u|| = 1$ and $||ua|| = ||a||$.*

Proof. $0 < ||1|| = ||1 \cdot 1|| \leq ||1|| \cdot ||1|| \leq 1$. Hence, $||1|| = 1$. Then, $1 = ||1|| = ||u \cdot u^{-1}|| \leq ||u|| \cdot ||u^{-1}|| \leq 1$. Thus, $||u|| = ||u^{-1}|| = 1$.

Finally, $||ua|| \leq ||u|| \; ||a|| = ||a|| = ||u^{-1}ua|| \leq ||u^{-1}|| \; ||ua|| = ||ua||$. Thus, $||ua|| = ||a||$. □

Definition 5.3. *R is* complete *with respect to $||\cdot||$ if $\langle R, d \rangle$ is a complete metric space, where $d(a, b) = ||a - b||$ for $a, b \in R$. Note that $d(a, b) = d(b, a)$ by 5.2.*

Remark. *Note the following facts.*

- *Suppose that* $a \in R$, $||a|| < 1$ *and that* R *is complete with respect to* $||\cdot||$. *Then* $1 + a$ *is a unit in* R.
- *Define* $||\cdot||_0 : R[[x]] \to \mathbb{R}$ *by*

$$||\sum_{i=0}^{\infty} a_i x^i|| = \sup\{||a_i|| : i = 0, 1, \dots\}.$$

Then, $||\cdot||_0$ *is an adic norm on* $R[[x]]$ *and* $R[[x]]$ *is complete with respect to* $||\cdot||_0$ *if* R *is complete with respect to* $||\cdot||$.

Proof. Proof left as exercise for the reader. □

Definition 5.4. *Let* $p \in \mathbb{N}$, *and* $\Phi(x) \in R[[x]]$. *Then* $\Phi(x)$ *is called* regular of order p *(with respect to* $||\cdot||$*) if* $\Phi(x) = \sum_{i=0}^{p-1} a_i x^i + u(x)x^p$ *where* $a_0, \dots, a_{p-1} \in R$ *satisfy* $||a_i|| < 1$ *for* $i = 0, \dots, p-1$ *and* $u(x)$ *is a unit of* $R[[x]]$.

Theorem 5.5 (Contraction Mapping Theorem)**.** *Let* $\langle Y, d\rangle$ *be a complete metric space,* $c \in \mathbb{R}$, $0 \le c < 1$, *and* $T : Y \to Y$ *a function such that* $d(T(a), T(b)) \le c \cdot d(a, b)\ \forall a, b \in Y$. *Then* $\exists! \alpha \in Y$ *such that* $T(\alpha) = \alpha$.

Proof. Proof left as exercise for the reader. □

Theorem 5.6 (Division Theorem for $R[[x]]$)**.** *Assume* $\langle R, ||\cdot||\rangle$ *is a complete normed ring,* $p \in \mathbb{N}$, *and* $\Phi(x) \in R[[x]]$ *is regular of order* p. *Then for any* $f(x) \in R[[x]]$, *there exist unique* $Q(x) \in R[[x]]$ *and* $S(x) \in R[x]$ *with deg* $S(x) < p$ *such that* $f(x) = Q(x) \cdot \Phi(x) + S(x)$.

Proof. Define $||\cdot||_0$ on $R[[x]]$ as in the remark above. Say $\Phi(x) = \sum_{i=0}^{p-1} a_i x^i + u(x)x^p$ as in 5.4. Let $\phi(x) = \sum_{i=0}^{p-1} a_i x^i$ so that $||\phi(x)||_0 = max\{||a_i|| : i = 0, \dots, p-1\} = c$, say where $0 \le c < 1$.

For any $Q(x) \in R[[x]]$ consider $f(x) - \phi(x)Q(x) \in R[[x]]$. Then $\exists T^*_Q(x) \in R[[x]]$ such that $f(x) - \phi(x)Q(x) = S_Q(x) + x^p T^*_Q(x)$, uniquely where $S_Q(x) \in R[x]$ and has degree $< p$. We want a $Q(x)$ such that $T^*_Q(x) = Q(x)u(x)$.

Define $T : R[[x]] \to R[[x]]$ by $T(Q(x)) = u(x)^{-1} T^*_Q(x)$. We need a $Q(x) \in R[[x]]$ such that $T_Q(x) = Q(x)$.

Now

$$\begin{aligned}
&||T(Q_1(x)) - T(Q_2(x))||_0 = ||T^*_{Q_1}(x) - T^*_{Q_2}(x)||_0 && \text{(by lemma 5.2)}\\
=\ & ||x^p(T^*_{Q_1}(x) - T^*_{Q_2}(x))||_0 && \text{(by the definition of } ||\cdot||_0)\\
\le\ & ||S_{Q_1}(x) - S_{Q_2}(x) + x^p(T^*_{Q_1}(x) - T^*_{Q_2}(x))||_0 &&\\
=\ & ||\phi(x)(Q_2(x) - Q_1(x))||_0 && \text{(from the definitions of } S_{Q_i}(x), T^*_{Q_i}(x))\\
\le\ & ||\phi(x)||_0 ||Q_1(x) - Q_2(x)||_0 &&\\
=\ & c||Q_1(x) - Q_2(x)||_0. &&
\end{aligned}$$

Hence, by the Contraction Mapping Theorem, $\exists! Q(x) \in R[[x]]$ such that $T(Q(x)) = Q(x)$. Then $T_Q^*(x) = u(x)q(x)$, so $f(x) - \phi(x)Q(x) = S_Q(x) + x^p u(x)Q(x)$.

Therefore, $f(x) = (\phi(x) + u(x)x^p)Q(x) + S_Q(x) = \Phi(x)Q(x) + S_Q(x)$, as required. $\square$

Corollary 5.7. *If $\Phi(x) \in R[[x]]$, with $\langle R, ||\cdot||\rangle$ complete, is regular of order p, then $\exists b_0, \ldots, b_{p-1} \in R$ with $||b_i|| < 1$ such that $\Phi(x) = v(x)(x^p + \sum_{i=0}^{p-1} b_i x^i)$ where $v(x)$ is a unit of $R[[x]]$.*

Proof. Take $f(x) = x^p$ in theorem 5.6. Then $x^p - S(x) = Q(x)\Phi(x)$ (as in the conclusion of 5.6).

That is, for suitable $b_0, \ldots, b_{p-1} \in R$,

$$x^p + \sum_{i=0}^{p-1} b_i x^i = Q(x)\Phi(x)$$

$$= Q(x)(\sum_{i=0}^{p-1} a_i x^i + u(x)x^p) = (\sum_{i=0}^{\infty} q_i x^i)(\sum_{i=0}^{p-1} a_i x^i + u(x)x^p) \quad \text{(with the } q_i \in R\text{)}.$$

Equating the coefficients of $1, x, \ldots, x^{p-1}$ shows that $||b_i|| < 1$ for $i = 0, \ldots, p-1$. Equating the coefficients of x^p shows that $q_0 u(0) = 1 + a$ for some $a \in R$ with $||a|| < 1$.

By theorem 4.3, $u(0)$ is a unit of R and hence $Q(x)$ is a unit of $R[[x]]$, as required. $\square$

6 Formal Power Series in Many Variables

Let R be a ring. Define $\mathscr{F}_0(R) = R$ and $\mathscr{F}_{n+1}(R) = \mathscr{F}_n(R)[[x_{n+1}]]$. Here, $x_1, x_2, \ldots, x_{n+1}, \ldots$ are independent variables. $\mathscr{F}_n(R)$ is also written as $R[[x_1, \ldots x_n]]$. The multi-index notation will be useful for us. For $v \in \mathbb{N}^n$, say $v = \langle v_1, \ldots, v_n\rangle$, write X for $x_1, \ldots, x_n$ and X^v for $x_1^{v_1} \cdots x_n^{v_n}$ (similarly for an $n-$tuple of elements of R). Also, $|v| := v_1 + \cdots + v_n$.

Exercise 6.1. *We may write the elements of $\mathscr{F}_n(R)$ uniquely in the form $\sum_{v \in \mathbb{N}^n} a_v X^v$ ($a_v \in R$) so that $\sum_v a_n X^v + \sum_v b_n X^n = \sum_v (a_n + b_n)X^n$ and $\sum_v a_n X^v \cdot \sum_v b_n X^n = \sum_v (\sum_{\lambda+\mu=v} a_\lambda \cdot b_\mu)X^v$ where addition of multi-indices is co-ordinatewise.*

For $f \in \mathscr{F}_n(R)$, $f(0, \ldots, 0) := a_{0,\ldots,0}$. Let J be the ideal of $\mathscr{F}_n(R)$ generated by $X_1, \ldots, X_n$. Define a function $ord : \mathscr{F}_n(R) \to \mathbb{N} \cup \{\infty\}$ by

$$ord(f) = \begin{cases} \text{the largest } m \text{ such that } f \in J^m \text{ if such exists,} \\ \infty \text{ otherwise} \end{cases}$$

(So if $f \notin J$, $ord(f) = 0$ ($J^0 = \mathscr{F}_n(R)$).)

Exercise 6.2. *$ord_n(f) = \infty$ iff $f = 0$ and $ord_n(f) =$ the smallest m such that, writing $f(x) = \sum_v a_v X^v$, we have $a_v \neq 0$ for some v with $|v| = m$. Further, $ord_n(f + g) \geq min(ord_n(f), ord_n(g))$ and $ord_n(f \cdot g) \geq ord_n(f) + ord_n(g)$. It follows that $|| \cdot ||^n$ is a norm on $\mathscr{F}_n(R)$ where $||f||^n = 2^{-ord_n(f)}$ (we set $2^{-\infty} := 0$). Further $|| \cdot ||^n$ is discrete on R (i.e. $||a||^n = 1$ for $a \in R \backslash \{0\}$), and $||f||^n < 1 \Leftrightarrow f \in J \Leftrightarrow f(0, \ldots, 0) = 0$.*

Exercise 6.3. *$\langle \mathscr{F}_n(R), || \cdot ||^n \rangle$ is complete. ($\{f_j\}$ being a Cauchy sequence just means that the f_j become more in agreement as $j \to \infty$).*

Now consider $f \in \mathscr{F}_n(R) = \mathscr{F}_{n-1}(R)[[x_n]]$.

Then f being regular of order p with respect to $|| \cdot ||_{n-1}$ according to 5.4 means

$$f(x_1, \ldots, x_n) = \textstyle\sum_{i=0}^{p-1} a_i(x_1, \ldots, x_{n-1}) x_n^i + u(x_i, \ldots, x_n) x_n^p$$

where $a_1, \ldots, a_{p-1} \in \mathscr{F}_{n-1}(R)$ and $a_i(0, \ldots, 0) = 0$ (for $i = 0, \ldots, p-1$) and where $u(x_1, \ldots, x_n)$ is a unit of $\mathscr{F}_n(R)$. By 4.3 and induction, the latter is equivalent to $u(0, \ldots, 0)$ being a unit in R which, if R is a field, just means that $u(0, \ldots, 0) \neq 0$. This in turn is equivalent to $a_p(0, \ldots, 0) \neq 0$.

Hence, we obtain from 5.7 :

Theorem 6.4 (Weierstrass Preparation Theorem for $\mathscr{F}_n(R)$)**.** *Suppose R is a field and $n \geq 1$. Let $\Phi(x_1, \ldots, x_n) \in \mathscr{F}_n(R)$ with*

$$\Phi(x_1, \ldots, x_n) = \sum_{i=0}^{\infty} a_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Suppose Φ is regular in x_n of order p. Then there exists a unique unit $v(x_1, \ldots, x_n) \in \mathscr{F}_n(R)$ and unique $b_0(x_1, \ldots, x_{n-1}), \ldots, b_{p-1}(x_1, \ldots, x_{n-1}) \in \mathscr{F}_{n-1}(R)$, all 0 at $(0, \ldots, 0)$, such that $\Phi(x_1, \ldots, x_n) = v(x_1, \ldots, x_n)(x_n^p + b_{p-1}(x_1, \ldots, x_{n-1}) x_n^{p-1} + \cdots + b_0(x_1, \ldots, x_{n-1}))$.

Remark 6.5. *Obviously there is a corresponding version of the division theorem for $\mathscr{F}_n(R)$, R a field.*

Theorem 6.6 (The Formal Denef-van den Dries Preparation Theorem)**.** *Let R be any Noetherian ring and let $\Phi(X)$ be any element of $\mathscr{F}_n(R)$, $n \geq 1$. Then there are a positive integer d, elements a_v of R, and units $u_v(X)$ of $\mathscr{F}_n(R)$ for $v \in \mathbb{N}^n$ with $|v| < d$ such that $\Phi(X) = \displaystyle\sum_{|v|<d} a_v X^n \cdot u_v(X)$.*

Proof. Case $n = 1$.

So $X = x_1$ and $\mathscr{F}_1(R) = R[[X]]$. Say $\Phi(X) = \displaystyle\sum_{i=0}^{\infty} a_i X^i$ (the a_i being in R). Consider the ideal of R generated by $\{a_0, a_1, \ldots\}$. Since R is Noetherian, it is generated by a_i for $i < d$, for some positive integer d.

Therefore, for each $j \in \mathbb{N}$, we may choose $b_{i,j} \in R$ for $i < d$ such that

$$a_{d+j} = \sum_{i<d} b_{i,j} a_i.$$

Hence, we have

$$\begin{aligned}
\Phi(X) &= (\sum_{i<d} a_i X^i) + \sum_{j=0}^{\infty} (\sum_{i<d} b_{i,j} a_i) X^{d+j} \\
&= (\sum_{i<d} a_i X^i) + X^d \sum_{i<d} a_i (\sum_{j=0}^{\infty} b_{i,j} X^j) \\
&= \sum_{i<d} a_i X^i (1 + X^{d-i} \sum_{j=0}^{\infty} b_{i,j} X^j).
\end{aligned}$$

Hence, we are done with $u_i(x) = 1 + X^{d-i}(\sum_{j=0}^{\infty} b_{i,j} X^j)$ (= 1 at the origin, so this is a unit).

Now if $\Phi(X) = \Phi(x_1, \ldots, x_{n+1}) \in \mathscr{F}_{n+1}(R) = \mathscr{F}_n(R)[[x_{n+1}]]$, we apply the case $n = 1$ to the variable x_{n+1} and the Noetherian (by 4.2 and induction) ring $\mathscr{F}_n(R)$. So

$\Phi(X) = \sum_{i<d} a_i X_{n+1}^i u_i(X)$ with all $a_i's$ in $\mathscr{F}_n(R)$. Now apply the induction hypothesis to the a_i. □

Substitution 6.7. *Let R be an arbitrary ring. $J_n :=$ ideal of $\mathscr{F}_n(R)$ generated by $x_1, \ldots, x_n$.*

Note that for any $m \geq 0$, J_n^m consists (by definition) of all elements of the form $h(g_1, \ldots, g_r)$ for $r \in \mathbb{N}$, $h(\zeta_1, \ldots, \zeta_r) \in R[\zeta_1, \ldots, \zeta_r]$ homogeneous of degree m, and $g_1, \ldots, g_r \in J_n$.

Now fix r and consider some $f \in \mathscr{F}_r(R)$ and $g_1, \ldots, g_r \in J_n$. Write $f(x_1, \ldots, x_r) = \sum_{i=0}^{\infty} h_i(x_1, \ldots, x_r)$, where h_i is a homogeneous polynomial in $R[x_1, \ldots, x_n]$ of degree i. Then $\forall N, M$

$$(\sum_{i=0}^{N+M} h_i(g_1, \ldots, g_r) - \sum_{i=0}^{N} h_i(g_1, \ldots, g_r)) \in J_n^{N+1},$$

and hence this element of $\mathscr{F}_n(R)$ has $|| \cdot ||^n -$norm $\leq 2^{-(N+1)}$.

Thus, $\{\sum_{i=0}^{N} h_i(g_1, \ldots, g_r)\}_{N \in \mathbb{N}}$ is a Cauchy sequence in $\mathscr{F}_n(R)$ and hence converges by 6.3. We denote its limit by $f(g_1, \ldots, g_r)$.

Thus, for fixed $g_1, \ldots, g_r \in J_n$, we have a map $\mathscr{F}_r(R) \to \mathscr{F}_n(R)$ given by : $f \mapsto f(g_1, \ldots, g_r)$.

Exercise 6.8. *Check that this map is continuous (for* $||\cdot||^r$*,* $||\cdot||^n$*) and a homomorphism. Show further that if* $p_1, \ldots, p_n \in J_1$ $(\trianglelefteq \mathscr{F}_1(R))$*, then*

$$f(g_1, \ldots, g_r)(p_1, \ldots, p_n) = f(g_1(p_1, \ldots, p_n), \ldots, g_r(p_1, \ldots, p_n)).$$

Now suppose $f \in \mathscr{F}_n(R)$, $f \neq 0$, and $ord(f) = p$. Then by 6.2, we can write

$$\begin{aligned} f(x_1, \ldots, x_n) &= \sum_{|v| \geq p} a_v X^v \quad (a_v \in R) \\ &= \sum_{i=p}^{\infty} h_i(x_1, \ldots, x_n), \end{aligned}$$

where the h_i are homogeneous polynomials of degree i and $h_p \not\equiv 0$.

Consider $x_1 + c_1x_n, \ldots, x_{n-1} + c_{n-1}x_n, x_n$, where $c_1, \ldots, c_{n-1} \in R$. These are in J_n.

Substitute :

$$\begin{aligned} f(x_1 + c_1x_n, \ldots, x_{n-1} + c_{n-1}x_n, x_n) &= \sum_{i=p}^{\infty} h_i(x_1 + c_1x_n, \ldots, x_{n-1} + c_{n-1}x_n, x_n) \\ &= \sum_{i=0}^{\infty} b_i(x_1, \ldots, x_{n-1})x_n^i, \text{say.} \end{aligned}$$

Using 6.8, set $x_1, \ldots, x_{n-1}$ to zero. We have

$$\sum_{i=0}^{\infty} b_i(0, \ldots, 0)x_n^i = \sum_{i=p}^{\infty} h_i(c_1, \ldots, c_{n-1}, 1)x_n^i.$$

So $b_i(0, \ldots, 0) = \begin{cases} 0 \ \text{ for } i < p \\ h_i(c_1, \ldots, c_{n-1}) \ \text{ for } i \geq p. \end{cases}$

If R is an infinite field, we can choose $c_1, \ldots, c_{n-1}$ so that $h_p(c_1, \ldots, c_{n-1}, 1) \neq 0$. Hence we have proved the following :

Lemma 6.9. *Suppose* R *is an infinite field,* $f \in \mathscr{F}_n(R)$*,* $f \neq 0$*,* $ord(f) = p$ $(< \infty)$*. Then after an invertible linear change of co-ordinates,* f *becomes regular in* x_n *of order* p*.*

7 Convergent Power Series

In this section $R = \mathbb{R}$ or $\mathbb{C}$. Write K for R and $\mathcal{F}_n$ for $\mathcal{F}_n(K)$. Recall that for $\alpha = \langle \alpha_1, \cdots, \alpha_n \rangle \in K^n$, and $\nu = \langle \nu_1, \ldots, \nu_n \rangle \in \mathbb{N}^n$, α^ν denotes $\alpha_1^{\nu_1} \cdots \alpha_n^{\nu_n}$. Also $|\cdot|$ denotes the usual modulus on K.

Definition. For $f = f(X) \in \mathcal{F}_n$, with $n \geq 1$, $X = (X_1, \ldots, X_n)$, say $f(X) = \sum_\nu a_\nu X^\nu$ with $a_\nu \in K$ for all ν, let $\text{dom}(f)$ be the interior of the set of all points $\alpha \in K^n$ such that the set $\{|a_\nu \alpha^\nu| : \nu \in \mathbb{N}^n\}$ is bounded. We say that f is convergent iff $\text{dom}(f) \neq \emptyset$. The set $\{f \in \mathcal{F}_n : \text{f is convergent}\}$ is denoted O_n.

Example. *Let* $f(X_1, X_2) = \sum_{i=0}^{\infty} X_1^i X_2^i$. *We have* $|1 \cdot \alpha_1^i \alpha_2^i|$ *is bounded iff* $|\alpha_1\alpha_2| \leq 1$. *Thus* $\mathrm{dom}(f) = \{\langle \alpha_1, \alpha_2 \rangle \in \mathbb{R}^2 : |\alpha_1\alpha_2| < 1\}$.

Lemma 7.1. *Suppose* $f \in \mathcal{F}_n$ *is convergent. Then (with* $f(X) = \sum_\nu a_\nu X^\nu$*)*

1. $\mathrm{dom}(f)$ *is a non-empty, open subset of* K^n*;*
2. *whenever* $\alpha \in \mathrm{dom}(f)$*, there is a* $c \in R^n$ *with* $0 < c_i < 1$ *(*$c = \langle c_1, \ldots, c_n \rangle$*) and* $M \in \mathbb{R}$ *such that* $|a_\nu \cdot \alpha^\nu| \leq M c^\nu$ *for all* $\nu \in \mathbb{N}^n$*;*
3. *whenever* $\alpha \in \mathrm{dom}(f)$*,* $\beta \in K^n$ *and* $|\beta_i| \leq |\alpha_i|$ *for* $i = 1, \ldots, n$ *then* $\beta \in \mathrm{dom}(f)$*;*
4. $\mathrm{dom}(f)$ *is a connected subset of* K^n*;*
5. *for* $\alpha \in \mathrm{dom}(f)$*,* $\Sigma_\nu a_\nu \alpha^\nu$ *is absolutely convergent.*

Proof. (1) Immediate.

(2) Suppose $\alpha \in \mathrm{dom}(f)$. Then $t \cdot \alpha = \langle t_1\alpha_1, \ldots, t_n\alpha_n \rangle \in \mathrm{dom}(f)$ for some $t = \langle t_1, \ldots, t_n \rangle \in R^n$ with $t_1, \ldots, t_n > 1$ by part (1). Then there is some M such that $|a_\nu (t \cdot \alpha)^\nu| \leq M$ for all $\nu \in \mathbb{N}^n$. . Hence the result with $c_i = t_i^{-1}$.

(3) By (1) we may suppose $|\beta_i| < |\alpha_i|$ for $i = 1, \ldots, n$. Then $|\gamma_i| \leq |\alpha_i|$ for all $\gamma = \langle \gamma_1, \ldots, \gamma_n \rangle$ close to β. Then if $|a_\nu \alpha^\nu| \leq M$ we have $|a_\nu \gamma^\nu| \leq M$ for all for all $\nu \in \mathbb{N}^n$ and γ close to β.

(4) By (3) and the fact that $\mathrm{dom}(f) \neq \emptyset$ we have that $0 \in \mathrm{dom}(f)$, and also that if $\alpha \in \mathrm{dom}(f)$ then the ray from 0 to α is included in $\mathrm{dom}(f)$.

(5) This follows from the following calculation :-

$$\begin{aligned} \sum_{|\nu| \leq N} |a_\nu \alpha^\nu| &\leq M \sum_{|\nu| \leq N} c^\nu & \text{(from (2))} \\ &\leq M \prod_{i=1}^{n} \left(\sum_{j=0}^{N} c_i^j \right) \\ &\leq \frac{M}{(1 - c_1) \cdots (1 - c_n)} \end{aligned}$$

□

For $f \in \mathcal{F}_n$ convergent and $\alpha \in \mathrm{dom}(f)$ let $\tilde{f}(\alpha)$ be the sum of the series $\sum_\nu a_\nu \alpha^\nu$, where $f = \sum a_\nu X^\nu$. So $\tilde{f} : \mathrm{dom}(f) \to K$, $\mathrm{dom}(f)$ being a connected, open subset of K^n containing 0.

Lemma 7.2. *Suppose* $f, g \in \mathcal{F}_n$ *are convergent. Then so are* $f \pm g$*,* $f \cdot g$ *. Indeed we have* $\mathrm{dom}(f * g) \supseteq \mathrm{dom}(f) \cap \mathrm{dom}(g)$ *and* $\widetilde{f * g} = \tilde{f} * \tilde{g}$*, where* $* \in \{\pm, \cdot\}$*. Thus* O_n *is a subring of* $\mathcal{F}_n$*.*

Proof. We just do the multiplication case. So suppose that $f(X) = \sum_\nu a_\nu X^\nu$, and $g(X) = \sum_\nu b_\nu X^\nu$. Then

$$f \cdot g = \sum_\nu \left(\sum_{\lambda+\mu=\nu} a_\lambda b_\mu \right) X^\nu.$$

Let $\alpha \in \mathrm{dom}(f) \cap \mathrm{dom}(g)$. By 7.1(2) we may choose $c \in \mathbb{R}^n$ where $c = \langle c_1, \ldots, c_n \rangle$ with $0 < c_i < 1$ for $i = 1, \ldots, n$, and an $M \in \mathbb{R}$ such that $|a_\nu \alpha^\nu|, |b_\nu \alpha^\nu| \leq M c^\nu$ for all ν. Then for $\nu \in \mathbb{N}^n$

$$\left| \left(\sum_{\lambda+\mu=\nu} a_\lambda b_\mu \right) \alpha^\nu \right| = \left| \sum_{\lambda+\mu=\nu} a_\lambda \alpha^\lambda b_\mu \alpha^\mu \right| \leq M^2 c^\nu (\nu_1 + 1) \cdots (\nu_n + 1)$$

which approaches 0 as $|\nu| \to \infty$, and hence is bounded. □

Lemma 7.3. *Suppose $f \in O_r$ and $g_1, \ldots, g_r \in O_n \cap J_n$. Then $f(g_1, \ldots, g_r) \in O_n$ and*

$$\widetilde{f(g_1, \ldots, g_r)} = \tilde{f}(\tilde{g}_1, \ldots, \tilde{g}_r)$$

sufficiently close to zero.

Proof. For a formal power series h let $|h|$ be the formal series obtained by "modding" the coefficients. Clearly $\mathrm{dom}(|h|) = \mathrm{dom}(h)$. Also, the coefficients of $f(g_1, \ldots, g_r)$ are bounded in absolute value by those of $|f|(|g_1|, \ldots, |g_r|)$. Now $\widetilde{|g_i|}(0) = 0$ for $i = 1, \ldots, r$ and hence, by continuity, there is an open (box) neighborhood U of zero in K^n such that $U \subseteq \cap_{i=1}^r \mathrm{dom}(g_i)$, and such that $\langle \widetilde{|g_1|}(\alpha), \ldots, \widetilde{|g_r|}(\alpha) \rangle \in \mathrm{dom}(f)$ for all $\alpha \in U$.

Now fix $\alpha \in U$. We want to show that $\alpha \in \mathrm{dom}(f(g_1, \ldots, g_r))$. It is clearly sufficient to show $\alpha \in \mathrm{dom}(|f|(|g_1|, \ldots, |g_r|))$. Fix some $\nu \in \mathbb{N}^n$ and choose a polynomial truncation $|f|_\nu$, say, of $|f|$ such that $|f|(|g_1|, \ldots, |g_r|)$ and $|f|_\nu(|g_1|, \ldots, |g_r|)$ have the same coefficient of X^ν. Now, by 7.2

$$\begin{aligned} \widetilde{|f|_\nu(|g_1|, \ldots, |g_r|)}(|\alpha|) &= \widetilde{|f|_\nu}(\beta_1, \ldots, \beta_r) \\ &\leq \widetilde{|f|}(\beta_1, \ldots, \beta_r) \end{aligned}$$

where $|\alpha| = \langle |\alpha_1|, \ldots, |\alpha_n| \rangle$ and $\beta_i = \widetilde{|g_i|}(|\alpha|)$ for $i = 1, \ldots, r$. Note that everything in sight is non-negative, and $\alpha \in U$ implies $|\alpha| \in U$. Let $|f|(|g_1|, \ldots, |g_r|) = \sum_\nu a_\nu X^\nu$. Hence, from the equation above, $|a_\nu \alpha^\nu| = |a_\nu| \cdot |\alpha|^\nu \leq \widetilde{|f|}(\beta_1, \ldots, \beta_r)$ since the middle term is one of the terms in $\widetilde{|f|_\nu}(\beta_1, \ldots, \beta_r)$.

Thus $|a_\nu \alpha^\nu|$ is bounded independently of ν, and so, since α is an arbitrary member of the open set U, $\alpha \in \mathrm{dom}(|f|(|g_1|, \ldots, |g_r|))$ as required.

The second part follows easily, again using approximation to f (and 7.2) □

Corollary 7.4. *Suppose $f \in O_n$ is a unit in $\mathcal{F}_n$ (i.e. $f(0) = \tilde{f}(0) \neq 0$). Then f is a unit in O_n. Hence the ideal generated by $X_1, \ldots, X_n$ is the unique maximal ideal of O_n.*

Proof. Suppose $f(0) \neq 0$. Then $f = a + g$ where $g \in O_n$, $g(0) = 0$ and $a \in K^*$. We may suppose $a = 1$ (consider $a^{-1}f$). Let $h(X_1) = \sum_{i=0}^{\infty} X_1^i$. Then $h \in O_1$ and $(1 - X_1)h(X_1) = 1$. Apply the map $\mathcal{F}_1 \to \mathcal{F}_n$ given by $j \mapsto j(-g)$. We get $(1 + g)h(-g) = 1$ (i.e. $f \cdot h(-g) = 1$).

By 7.3 $h(-g) \in O_n$ since $h \in O_1$ and $-g \in O_n \cap J_n$. □

Exercise 7.5. *Suppose $f \in O_n$, then $f \in \mathcal{F}_n = \mathcal{F}_{n-1}[[X_n]]$. Hence*

$$f(X_1, \dots, X_n) = \sum_{i=0}^{\infty} f_i(X_1, \dots, X_{n-1})X_n^i$$

uniquely with the f_i's in $\mathcal{F}_{n-1}$.

Then each f_i is convergent and $\pi(\mathrm{dom}(f)) \subset \mathrm{dom}(f_i)$ for each i, where $\pi : (t_1, \dots, t_n) \mapsto (t_1, \dots, t_{n-1})$ is the projection onto the first $n-1$ coordinates.

Theorem 7.6 (Division Theorem for O_n)**.** *Suppose $\Phi \in O_n$ is regular of order p with respect to X_n. Then for every $f \in O_n$ there exists an unique $Q \in O_n$ and $S \in O_{n-1}[X_n]$ of degree $< p$ such that $f = Q\Phi + S$.*

Proof. For $\alpha = \langle \alpha_1, \dots, \alpha_n \rangle \in \mathbb{R}^n$ with $\alpha_i > 0$ for $i = 1, \dots, n$, let

$$O_n^\alpha = \{f \in O_n : |f|(\bar{x}) \text{ converges at } \alpha\}.$$

Then (exercise) $\langle O_n^\alpha, || \cdot || \rangle$ is a complete normed space with $|| \sum_\nu a_\nu X^\nu || = \sum_\nu |a_\nu| \alpha^\nu$. Now we have

$$\Phi(X_1, \dots, X_n) = \sum_{i=0}^{p-1} f_i(X_1, \dots, X_{n-1})X_n^i + u(X_1, \dots, X_n)X_n^p \tag{1}$$

where $f_i \in \mathcal{F}_{n-1}$ for $i = 0 \dots, p-1$ and u is a unit of $\mathcal{F}_n$. But $\Phi \in O_n$ so $f_i \in O_{n-1}$ by 7.5 and then, clearly, $u \in O_n$ and u is a unit of O_n by 7.4. Further, by hypothesis,

$$f_i(0) = \tilde{f}_i(0) = 0$$

for $i = 0, \dots, p-1$. Let U be an open box in K^n centered at 0 and contained in the domain of all the series appearing in 1 and such that $U \subseteq \mathrm{dom}(f)$ and such that for some $M \geq 1$

$$||\widetilde{u^{-1}}|(\alpha)| < M$$

for all $\alpha \in U$. Say

$$U = \{\langle \beta_1, \dots, \beta_n \rangle \in K^n \mid |\beta_i| < \epsilon, i = 1, \dots, n\}.$$

Now set $\alpha_n = \epsilon/2$ and choose $0 < \alpha_1, \dots, \alpha_{n-1} < \epsilon$ such that

$$\sum_{i=0}^{p-1} \widetilde{|f_i|}(\alpha_1, \dots, \alpha_{n-1}) \cdot \alpha_n^i < \frac{\alpha_n^p}{2M}.$$

This is possible since $\widetilde{|f_i|}$ is continuous on U and $\widetilde{|f_i|}(0) = 0$. Let $||\cdot||$ be the norm described above on O_n^α. Let $\phi(X_1, \ldots, X_n) = \sum_{i=0}^{p-1} f_i(X_1, \ldots, X_{n-1})X_n^i$. Then $f, \Phi, f_1, \ldots, f_{p-1}, \phi, u, u^{-1} \in O_n^\alpha$ and $||\phi|| < \alpha_n^p/2M$, $||u^{-1}|| < M$.

Now for $Q \in O_n^\alpha$ define $T_Q^* \in O_n^\alpha$ by $f - \phi Q = S_Q + X_n^p T_Q^*$ (where $S_Q \in \mathcal{F}_{n-1}[X_n]$ is of degree $< p$ in X_n and $T_Q^* \in \mathcal{F}_n$). It is immediate that $S_Q, T_Q^* \in O_n^\alpha$ and $u^{-1}T_Q^* \in O_n^\alpha$.

Define $T : O_n^\alpha \to O_n^\alpha$ by

$$T(Q) = u^{-1}T_Q^*.$$

Let $Q_1, Q_2 \in O_n^\alpha$. Then

$$\begin{aligned}
||T(Q_1) - T(Q_2)|| &< M \cdot ||T_{Q_1}^* - T_{Q_2}^*|| \\
&= \frac{M}{\alpha_n^p} \cdot ||X_n^p(T_{Q_1}^* - T_{Q_2}^*)|| \\
&\leq \frac{M}{\alpha_n^p} \cdot ||(S_{Q_1} - S_{Q_2}) + X_n^p(T_{Q_1}^* - T_{Q_2}^*)|| \\
&= \frac{M}{\alpha_n^p} \cdot ||\phi(Q_2 - Q_1)|| \\
&\leq \frac{M}{\alpha_n^p} \cdot ||\phi|| \cdot ||Q_2 - Q_1|| \\
&\leq \frac{1}{2} \cdot ||Q_2 - Q_1|| \\
&= \frac{1}{2} \cdot ||Q_1 - Q_2||
\end{aligned}$$

Hence T is contractive and we finish the proof as in 5.6. □

Corollary 7.7 (Weierstrass Preparation Theorem for O_n)**.** *Suppose $\Phi \in O_n$ is regular of order p (in X_n). Then there exists a (unique) unit $u \in O_n$ and*

$$f_0, \ldots, f_{p-1} \in O_{n-1}$$

with $f_i(0) = 0$ such that

$$\Phi(X_1, \ldots, X_n) = u(X_1, \ldots, X_n) \cdot \left(X_n^p + \sum_{i=0}^{p-1} f_i(X_1, \ldots, X_{n-1})X_n^i \right).$$

(Of course we have the same equality for the corresponding functions).

Proof. Same way as 5.7 is deduced from 5.6. □

Corollary 7.8. *O_n is a Noetherian ring.*

Proof. By induction on n.

If $n = 0$, trivial. ($O_0 = K$ is a field.)

Suppose $n \geq 1$ and $I \trianglelefteq O_n$. Suppose I contains some element Φ which is regular in X_n of some order $p \in \mathbb{N}$. Let J be the ideal of O_n generated by Φ. Then $J \subseteq I$. Now every element of O_n, because of the division theorem, is equivalent (mod J) to an element of the form $\sum_{i=0}^{p-1} f_i X_n^i$ where $f_i \in O_{n-1}$. Hence O_n/J is generated as an O_{n-1}-module by $1, X_n, \ldots, X_n^{p-1}$ and hence is Noetherian since O_{n-1} is Noetherian by the induction hypothesis. (See the remarks at the beginning of Section 2). Hence the sub-O_{n-1}-module I/J of O_n/J is finitely generated by, say, $\Theta_1/J, \ldots, \Theta_m/J$, $(\Theta_1, \ldots, \Theta_m \in I)$. But then, every element of I is of the form $F_1\Theta_1 + \cdots + F_m\Theta_m + G\Phi$ for some $F_1, \ldots, F_m \in O_{n-1} (\subseteq O_n)$ and $G \in O_n$. So $\Theta_1, \ldots, \Theta_m, G$ generate I as an O_n-module (i.e. as an ideal of O_n).

Now, in general, if $I \neq 0$ let $\Phi \in I$ be non-zero. By 6.9 there are $c_1, \ldots, c_{n-1} \in K$ such that the map

$$\tau : f(X_1, \ldots, X_n) \mapsto f(X_1 + c_1 X_n, \ldots, X_{n-1} + c_{n-1} X_n, X_n)$$

is a homomorphism from $\mathcal{F}_n$ to $\mathcal{F}_n$ mapping Φ onto an element regular of some order p (in X_n). This map has an inverse

$$f(X_1, \ldots, X_n) \mapsto f(X_1 - c_1 X_n, \ldots, X_{n-1} - c_{n-1} X_n, X_n)$$

and is therefore a ring automorphism of $\mathcal{F}_n$. By 7.3 it restricts to an automorphism of O_n, whence the result by the first case. □

We now turn to the Denef-van den Dries Preparation Theorem for O_n. The proof requires the following deep algebraic result, the proof of which is postponed to the next section.

Proposition 7.9. *Let $f_1, \ldots, f_s, f \in O_n \subseteq \mathcal{F}_n$ and suppose that the linear equation*

$$f_1 y_1 + \cdots + f_s y_s = f$$

is solvable in $\mathcal{F}_n$. Then it is solvable in O_n.

Proof. Next Section. □

Theorem 7.10 (Denef–van den Dries Preparation Theorem for O_n)**.** *Let*

$$\Phi(X_1, \ldots, X_{m+n}) \in O_{m+n}.$$

Then there exists a positive integer d, elements $a_\nu(X_1, \ldots, X_m) \in O_m$ and units $u_\nu(X_1, \ldots, X_{m+n}) \in O_{m+n}$ for each $\nu \in \mathbb{N}^n$ with $|\nu| < d$, such that

$$(\dagger) \qquad \Phi(X_1, \ldots, X_{m+n}) = \sum_{\nu \in \mathbb{N}^n, |\nu| < d} a_\nu(X_1, \ldots, X_m) X_*^\nu u_\nu(X_1, \ldots, X_{m+n})$$

where $X_* = (X_{m+1}, \ldots, X_{m+n})$

Proof. Let $R = O_m$ in 6.6 (allowed by 7.8). Then by 6.6 we can solve ($\dagger$) with a_ν's in O_m but with u_ν's in $O_m[[X_{m+1}, \ldots, X_{m+n}]] (\subseteq \mathcal{F}_{m+n})$.

We may write

$$(*) \qquad u_\nu(X_1, \ldots, X_{m+n}) = \beta_\nu + X_1 u_\nu^{(1)} + \cdots + X_{m+n} u_\nu^{(m+n)}$$

with the $u_\nu^{(i)}$'s in $\mathcal{F}_{m+n}$ and β_ν's in $K \setminus \{0\}$ (cf. 6.2). Substituting (*) into (†) for each ν with $|\nu| < d$, we arrive at an equation of the form in 7.9 where we regard the $u_\nu^{(i)}$'s as "variables". But we can (and have already managed to) solve this equation in $\mathcal{F}_{m+n}$. Hence by 7.9 we can solve it in O_{m+n}. Now define the required units in O_{m+n} by the equation (*) (for $u_\nu^{(i)}$ the new convergent solutions). □

8 More on adically normed rings and modules

The purpose of this section is to develop further the theory of Noetherian rings up to the point that Proposition 7.9 may be easily deduced.

Let R be a ring and J any ideal of R. For $a \in R$ define

$$\operatorname{ord}_J(a) = \begin{cases} \text{the largest } m \text{ such that } a \in J^m & \text{if such exists,} \\ \infty & \text{otherwise.} \end{cases}$$

Set $\|a\|_J = 2^{-\operatorname{ord}_J(a)}$ ($= 0$ if $\operatorname{ord}_J(a) = \infty$). Then it is easy to show that for all $a, b \in R$, $0 \le \|a\|_J \le 1$, $\|a+b\|_J \le \max(\|a\|_J, \|b\|_J)$ and $\|a\, b\|_J \le \|a\|_J \|b\|_J$. Hence $\|\cdot\|_J$ is a norm on R provided $a = 0$ whenever $\|a\|_J = 0$, i.e. provided that $\bigcap_{m\in\mathbb{N}} J^m = \{0\}$. Now one can easily derive a necessary condition for this to occur. For if $\|\cdot\|_J$ *is* a norm, then whenever $\|a\|_J < 1$ (i.e. $a \in J$) it cannot be the case that $1 + a$ is a zero divisor in R. For if $b(1+a) = 0$, then $\|b\|_J = \|-b\, a\|_J \le \|-b\|_J\, \|a\|_J < \|b\|_J$. For R Noetherian this turns out to be sufficient, as we shall show in 8.4 below.

Lemma 8.1 (Artin-Rees Lemma)**.** *Let R be a Noetherian ring and M a finitely generated R-module. Suppose that N, N' are submodules of M and J is an ideal of R. Then there exists a natural number r_0 such that for all $n > r_0$*

$$J^n N \cap N' = J^{n-r_0}\left(J^{r_0} N \cap N'\right).$$

Remark. *For any ideal I and submodules N_0, N_1 of an R-module, we always have $I(N_0 \cap N_1) \subseteq I\, N_0 \cap I\, N_1$.*

Proof. The $\supseteq$ containment follows immediately from the remark. For the converse, we first treat the case $M = R$, i.e. when M, N' are ideals of R. Let $a_1, \ldots, a_m$ generate J. For each n, set

$$S_n = \{f(x_1, \ldots, x_m) \in R[x_1, \ldots, x_m] : f \text{ homogeneous of degree } n, \\ f(a_1, \ldots, a_m) \in J^n \cap N'\}.$$

Let $S = \bigcup_{n=1}^\infty S_n$ and let $\widetilde{S}$ be the ideal of $R[x_1, \ldots, x_m]$ generated by S. By the Hilbert Basis Theorem we may choose $f_1, \ldots, f_s \in S$ generating $\widetilde{S}$. Say f_i is homogeneous of degree d_i, so that $f_i \in S_{d_i}$ (for $i = 1, \ldots, s$). Let $r_0 = \max\{d_1, \ldots, d_s\}$. Suppose $n > r_0$ and $a \in J^n N \cap N'$. Then certainly $a \in J^n$ so $a = f(a_1, \ldots, a_m)$ for some $f(x_1, \ldots, x_m) \in R[x_1, \ldots, x_m]$ homogeneous of degree n (easy exercise). Since $a \in J^n N \cap N'$ we have $f \in S_n \subseteq \widetilde{S}$, so we have an identity

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{s} f_i(x_1, \ldots, x_m)\, g_i(x_1, \ldots, x_m)$$

for some $g_1, \ldots, g_s \in R[x_1, \ldots, x_m]$. Since f is homogeneous of degree n we may set the coefficient of each monomial in g_i not of degree $n - d_i$ to zero (for $i = 1, \ldots, s$) and retain the identity. Hence we may suppose that g_i is homogeneous of degree $n - d_i$, and therefore $g_i(a_1, \ldots, a_m) \in J^{n-d_i}$. Thus we have

$$\begin{aligned} g_i(a_1, \ldots, a_m) \cdot f_i(a_1, \ldots, a_m) &\in J^{n-d_i}(J^{d_i} \cap N') && \text{(since } f_i \in S_{d_i}\text{)} \\ &\subseteq J^{n-d_i-(r_0-d_i)}(J^{r_0-d_i} J^{d_i} N \cap J^{r_0-d_i} N') && \text{(by remark)} \\ &\subseteq J^{n-r_0}(J^{r_0} N \cap N'). \end{aligned}$$

Thus $a = f(a_1, \ldots, a_m) \in J^{n-r_0}(J^{r_0} N \cap N')$ as required.

Let M now be an arbitrary finitely generated R-module. Consider the additive abelian group $R \times M$ and define multiplication by

$$\langle r_1, m_1 \rangle \circ \langle r_2, m_2 \rangle = \langle r_1 r_2, r_1 m_2 + r_2 m_1 \rangle.$$

Then one easily checks that $R \oplus M := \langle R \times M, +, \circ, \langle 0, 0 \rangle, \langle 1, 0 \rangle \rangle$ is a commutative ring with 1. Further, identifying R with $\{\langle r, 0 \rangle : r \in R\}$ and M with $\{\langle 0, m \rangle : m \in M\}$ we see that $R \oplus M$ is finitely generated over R, so Noetherian (by 3.3), and any R-submodule of M is an ideal of $R \oplus M$. The general result for R, N, N' now easily follows by the above result for ideals of $R \oplus M$. □

Corollary 8.2. *Suppose R is a Noetherian ring, M a finitely generated R-module, J an ideal of R. Set $N = \bigcap_{n=0}^{\infty} J^n M$. Then $J\,N = N$.*

Proof. By 8.1 choose r_0 so that (setting $n = r_0 + 1$ in 8.1) $J^{r_0+1} M \cap N = J(J^{r_0} \cap N)$. Since $N \subseteq J^{r_0+1} M$, this gives $N = J\,N$. □

Exercise 8.3. *Let A be $s \times s$ matrix over a ring R. Then it is well known that A is an invertible matrix if and only if $\det(A)$ is a unit in R. The proof shows the following: suppose further that M is an R-module, $t_1, \ldots, t_s \in M$, and*

$$A \begin{pmatrix} t_1 \\ \vdots \\ t_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Then $\det(A)\, t_i = 0$ for $i = 1, \ldots, s$.

Theorem 8.4 (Krull Intersection Theorem)**.** *Suppose R is a Noetherian ring, M a finitely generated R-module, J an ideal of R. Then $\bigcap_{n=0}^{\infty} J^n M = \{0\}$ if and only if for all $a \in J$ and for all $m \in M \setminus \{0\}$, $(1 + a)m \neq 0$.*

Proof. (⇒) If $a \in J$, $m \in M$ and $(1+a)m = 0$ then for all odd n we have

$$(1+a^n)m = (1 - a + a^2 - \cdots + a^{n-1})(1+a)m = 0.$$

Hence $m \in J^n M$ for all n. Therefore $m = 0$.

(⇐) Let $N = \cap_{n=0}^{\infty} J^n M$ and let $t_1, \ldots, t_s$ generate N (note: M is Noetherian — see section 3). Since $J\,N = N$ by the above corollary, we have $t_1, \ldots, t_s \in J\,N$ so

$$\begin{aligned} t_1 &= a_{11}t_1 + \cdots + a_{1s}t_s \\ &\vdots \\ t_s &= a_{s1}t_1 + \cdots + a_{ss}t_s \end{aligned}$$

for some $a_{ij} \in J$. Hence

$$\begin{pmatrix} a_{11}-1 & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22}-1 & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss}-1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_s \end{pmatrix} = 0.$$

But the determinant of this matrix clearly has the form $\pm(1+a)$ for some $a \in J$. By 8.3, $(1+a)t_i = 0$ for $i, \ldots, s$. Hence $t_i = 0$ by hypothesis, and so $N = 0$. □

Corollary 8.5. *Let R be a Noetherian ring and I, J ideals of R not equal to R. Suppose that $1+a$ is a unit in R for all $a \in J$. Then $\bigcap_{n=0}^{\infty}(I + J^n) = I$.*

Proof. Let $R' = R/I$. Then R' is a Noetherian ring. Let $h : R \to R'$ be the natural homomorphism and $J' = h[J]$. Then J' is an ideal of R' and if $a' \in J'$, say $h(a) = a'$ for some $a \in J$, then $(1+a)b = 1$ for some $b \in R$ by the hypothesis. So $(1+a')\,h(b) = 1$, so $1+a'$ is a unit in R'. Hence, applying 8.4 we have $\bigcap_{n=0}^{\infty} J'^n = \{0\}$. But $h[I + J^n] \subseteq J'^n$ for all n, hence $h\left[\bigcap_{n=0}^{\infty}(I+J^n)\right] = \{0\}$. So $\bigcap_{n=0}^{\infty}(I+J^n) \subseteq \ker(h) = I$. The opposite inclusion is immediate. □

Theorem 8.6. *Let $n \geq 1$. Let I be an ideal of $\mathcal{O}_n$ and let $\hat{I}$ be the ideal of $\mathcal{F}_n$ generated by I. Then $\hat{I} \cap \mathcal{O}_n = I$.*

Proof. The $\supseteq$ inclusion is obvious. For $\subseteq$ let J be the maximal ideal of $\mathcal{O}_n$, i.e. the ideal generated by $x_1, \ldots, x_n$. Suppose $g_1, \ldots, g_s$ generates I. Let $f \in \hat{I} \cap \mathcal{O}_n$. Then $f = f_1 g_1 + \cdots + f_s g_s$ for some $f_1, \ldots, f_s \in \mathcal{F}_n$. Let $r \in \mathbb{N}$ and write f_i as $p_i + h_i$, where p_i is a polynomial in $x_1, \ldots, x_n$ of degree less than r and $h_i \in \hat{J}^r$. Then $f = \sum_{i=1}^n p_i g_i + H$ where $H \in \hat{J}^r$. But $f - \sum_{i=1}^n p_i g_i \in \mathcal{O}_n$, so $H \in O_n$. It is easy to show that the theorem holds for $\hat{J}^r$, i.e. $\mathcal{O}_n \cap \hat{J}^r = J^r$ (and $\widehat{J^r} = \hat{J}^r$), hence $H \in J^r$. Thus $f \in I + J^r$. Since this holds for all $r \in \mathbb{N}$, we have, by 8.5 (and 7.4), $f \in I$ as required. □

Proposition 7.9 is now immediate by applying the previous theorem to the ideal of $\mathcal{O}_n$ generated by $f_1, \ldots, f_s$.

9 The Denef–van den Dries paper

For $r \in \mathbb{R}$, $r > 0$, $n \in \mathbb{N}$, $n > 0$, let B_r^n (respectively $\overline{B_r^n}$) denote the set

$$\{\langle x_1, \ldots, x_n\rangle \in \mathbb{R} : |x_i| < r \text{ (respectively } \leq) \text{ for } i = 1, \ldots, n\}.$$

The language L_{an} consists of $+, \cdot, -, <$ together with a constant symbol for each real number and a function symbol for each $n \in \mathbb{N}$, $n > 0$, $r \in \mathbb{R}$, $r > 0$ and $f \in \mathcal{O}_n$ with $\overline{B_r^n} \subseteq \text{dom}(f)$. The structure $\mathbb{R}_{\text{an}}$ interprets the former symbols naturally and the function symbols of the latter kind as the functions $\mathbb{R}^n \to \mathbb{R}$,

$$\bar{x} \mapsto \begin{cases} \widetilde{f}(\bar{x}) & \text{if } \bar{x} \in B_r^n \\ 0 & \text{otherwise} \end{cases}.$$

(Recall that $\widetilde{f}$ denotes the function determined by the convergent power series f.)

L_{an}^D denotes the language L_{an} together with an additional binary function symbol D, and then $\mathbb{R}_{\text{an}}^D$ denotes the expansion of $\mathbb{R}_{\text{an}}$ obtained by interpreting D as

$$\langle x, y\rangle \mapsto \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ 0 & \text{otherwise} \end{cases}.$$

Clearly $\mathbb{R}_{\text{an}}^D$ and $\mathbb{R}_{\text{an}}$ have the same definable sets. Let T_{an}^D and T_{an} denote the complete theories of these structures.

Theorem 9.1. *T_{an} is model complete; T_{an}^D eliminates quantifiers.*

Exercise 9.2. *Deduce the first statement of the previous theorem from the second one.*

Example 9.3 (Osgood 1910)**.** T_{an} does not eliminate quantifiers.

Let

$$e(x) = \begin{cases} e^x & \text{for } |x| \leq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\varphi(a, b, c) \Leftrightarrow \exists x \exists y(a = x \wedge b = x\, y \wedge c = x\, e(y) \wedge |x|, |y| \leq 1)$. Then φ is not equivalent to any quantifier-free L_{an}-formula. For if it were then it is not too hard to see (using a little analysis) that there would have to be an $f \in \mathcal{O}_3$ such that for all x, y sufficiently close to 0 we have $\widetilde{f}(x, x\,y, x\,e(y)) = 0$, but $f \not\equiv 0$. Writing $f(x_1, x_2, x_3) = \sum_{i=0}^{\infty} h_i(x_1, x_2, x_3)$ where h_i is homogeneous of degree i we have

$$0 \equiv \sum_{i=0}^{\infty} h_i(x, x\,y, x\,e(y)) = \sum_{i=0}^{\infty} x^i\, h_i(1, y, e(y))$$

close to 0. Thus for all y, the series in x is 0. Hence $h_i(1, y, e(y)) = 0$ for all i and y, with y close to 0. But y and e^y are algebraically independent functions (over $\mathbb{R}$) — exercise. Hence $h_i(1, x_2, x_3) \equiv 0$, from which it follows that $h_i(x_1, x_2, x_3) \equiv 0$ and so $f \equiv 0$, a contradiction.

Of course, $\varphi(a, b, c)$ is equivalent to the quantifier-free L^D_{an}-formula

$$(a = b = c = 0) \vee (a \neq 0 \wedge D(c, a) = e(D(b, a)) \wedge |a| \leq 1 \wedge |D(b, a)| \leq 1).$$

Remark (Original work in the 60's by Gabrielov and Łojasiewicz)**.** *Łojasiewicz extended the notion of semi-algebraic set* [1] *to the analytic category. The right definition is as follows: A subset $X \subseteq \mathbb{R}^n$ is called semi-analytic if for all $\bar{a} \in \mathbb{R}^n$ there exists an open neighborhood $U_{\bar{a}}$ of $\bar{a}$ in $\mathbb{R}^n$ such that $X \cap U_{\bar{a}}$ can be expressed as a Boolean combination of sets of the form*

$$\{\bar{x} \in U_{\bar{a}} : \widetilde{f}(\bar{a} - \bar{x}) > 0\}$$

for $f \in \mathcal{O}_n$ with $\bar{a} - U_{\bar{a}} \subseteq \mathrm{dom}(f)$.

Exercise 9.4. *A subset $X \subseteq \mathbb{R}^n$ is semi-analytic if and only if $\overline{B^n_r} \cap X$ is quantifier-free definable in $\mathbb{R}_{an}$ for all $r \in \mathbb{R}$.*

One wanted to show that the semi-analytic sets had good properties (similar to the class of semi-algebraic sets). Unfortunately, 9.3 shows that the class of semi-analytic sets is not closed under projections. Gabrielov then defined a subset $X \subseteq \mathbb{R}^n$ to be sub-analytic if for all $\bar{a} \in \mathbb{R}^n$ there exists a neighborhood $U_{\bar{a}}$ of a, $m \in \mathbb{N}$ and a bounded semi-analytic $Y \subseteq \mathbb{R}^{n+m}$ such that $\pi[Y] = U_{\bar{a}} \cap X$. He showed that the complement of a sub-analytic set is sub-analytic.

Exercise 9.5. *Using 9.1 show (from the definition above) that a subset $X \subseteq \mathbb{R}^n$ is sub-analytic if and only if $\overline{B^n_r} \cap X$ is quantifier-free definable in $\mathbb{R}^D_{an}$ for all $r \in \mathbb{R}$. Deduce Gabrielov's theorem.*

I also mention here the following important result. One can use it to prove that all $\mathbb{R}^D_{\mathrm{an}}$-definable unary functions have Puiseax expansions at ∞.

Theorem 9.6 (Łojasiewicz)**.** *A sub-analytic subset of $\mathbb{R}^2$ is semi-analytic, i.e. (by above) any $\mathbb{R}_{an}$ (or $\mathbb{R}^D_{an}$)-definable subset of $\mathbb{R}^2$ is quantifier-free $\mathbb{R}_{an}$-definable.*

9.1 Definable subsets of $\mathbb{R}$ in $\mathbb{R}_{\mathrm{an}}$

Lemma 9.7. *For all $f \in \mathcal{O}_1 \setminus \{0\}$ there exist $r \in \mathbb{N}$, $g \in \mathcal{O}_1$, g a unit with $\mathrm{dom}(g) = \mathrm{dom}(f)$, such that for all $x \in \mathrm{dom}(g)$, $\widetilde{f}(x) = x^r \, \widetilde{g}(x)$. Hence $\widetilde{f}$ has constant non-zero sign on $(0, \varepsilon)$ for some $\varepsilon > 0$.*

Proof. Obvious. □

Lemma 9.8. *For all terms $t(x)$ of L^D_{an} there exists $\varepsilon > 0$ such that either*

(1) $t(x) = 0$ for all $x \in (0, \varepsilon)$, or

(2) $t(x) = x^n \, \widetilde{f}(x)$ for all $x \in (0, \varepsilon)$, for some unique (possibly negative) $n \in \mathbb{Z}$ and unit $f \in \mathcal{O}_1$ with $(-\varepsilon, \varepsilon) \subseteq \mathrm{dom}(f)$.

[1] i.e. quantifier-free definable set in $\overline{\mathbb{R}} = \langle \mathbb{R}; 0, 1, +, \cdot, -, < \rangle$

(We also use t to denote the function it defines in $\mathbb{R}^D_{an}$.)

Proof. This is obvious if $t(x) = x$ or a constant. Also, if it is true for some $t_1(x), t_2(x)$ then it is true for $t_1(x) \pm t_2(x)$ and $t_1(x) \cdot t_2(x)$ (using 9.7). Also, if (1) holds for t_1 or t_2 then (1) holds for $D(t_1, t_2)$. If (2) holds for t_1 and t_2 we may choose (using 9.7) some ε small enough so that $t_2(x) \neq 0$ on $(0, \varepsilon)$. It easily follows that (2) holds for $D(t_1, t_2)$ (since the ratio of units is a unit).

Now suppose that the result holds for $t_1, \ldots, t_n$ and $f \in \mathcal{O}_n$, $\alpha \in \mathbb{R}$, $\alpha > 0$ and $\overline{B^n_\alpha} \subseteq \mathrm{dom}(f)$. We must consider

$$\begin{cases} \widetilde{f}(t_1(x), \ldots, t_n(x)) & \text{if } |t_i(x)| < \alpha \text{ for all } i = 1, \ldots, n \\ 0 & \text{otherwise} \end{cases}.$$

Now if (1) holds for some t_i we can reduce n. So we can choose ε small enough, units $f_1, \ldots, f_n \in \mathcal{O}_1$ and $m_1, \ldots, m_n \in \mathbb{Z}$ such that $t_i(x) = x^{m_i}\widetilde{f_i}(x)$ for all $x \in (0, \varepsilon)$. If $m_i < 0$ for some i then (since $\widetilde{f_i}(x)$ is bounded away from 0) we may suppose $|t_i(x)| > \alpha$ for all $x \in (0, \varepsilon)$ so (1) holds for the composite term. Hence we may suppose that $m_i \geq 0$ for $i = 1, \ldots, n$. Now by 9.7 $\alpha + t_i(x)$ and $t_i(x) - \alpha$ have constant sign on $(0, \varepsilon)$. If the former is nonpositive or the latter nonnegative then (1) holds for the composite term. Otherwise $-\alpha < t_i(x) < \alpha$ for all $x \in (0, \varepsilon)$ and for $i = 1, \ldots, n$. Let $a_i = (x^{m_i}\widetilde{f_i}(x))_{x=0}$. Then $-\alpha \leq a_i \leq \alpha$. So $\langle a_1, \ldots, a_n \rangle \in \overline{B^n_\alpha} \subseteq \mathrm{dom}(f)$. So it follows that the composite term is equal to $\widetilde{g}(x)$ for all $x \in (0, \varepsilon)$ for some $g \in \mathcal{O}_1$. Hence (2) holds for the composite term with $m \geq 0$ (using 9.7). □

Corollary 9.9. *Let $t(x)$ be a term of L^D_{an}. Then there exists a partition of $\mathbb{R}$ into finitely many open intervals and points such that $t(x)$ has constant sign on each such interval.*

Proof. By 9.8 (and 9.7), if $a \in \mathbb{R}$ then there exists $\varepsilon_a > 0$ such that $t(x)$ has constant sign on $(a, a + \varepsilon_a)$ and $(a - \varepsilon_a, a)$ (consider the terms $t(a + x)$ and $t(a - x)$). Also there exists $\eta > 0$ such that $t(x)$ has constant sign on $(1/\eta, \infty)$ and $(-\infty, -1/\eta)$ (consider the terms $t(D(1, x))$ and $t(-D(1, x))$). The result follows by the compactness of the closed interval $[-1/\eta, 1/\eta]$. □

Theorem 9.10 (Assuming 9.1)**.** *Every subset of $\mathbb{R}$ definable in $\mathbb{R}^D_{an}$ is a finite union of open intervals and points. So T^D_{an} is o-minimal.*

Proof. Immediate from 9.1 and 9.9. □

9.2 The proof that T^D_{an} eliminates quantifiers

Let $M_1, M_2 \models T^D_{\mathrm{an}}$. Suppose that K is a (L^D_{an}-) substructure of M_1, that $e : K \to M_2$ is an embedding, and that M_2 is sufficiently saturated. By 1.5. we must consider $a \in M_1$ and extend e to $e' : K\langle a \rangle \to M_2$ where $K\langle a \rangle$ denotes the L^D_{an}-substructure of M_1 generated by K and a.

Note that we may suppose $\mathbb{R}^D_{\mathrm{an}} \subseteq_{L^D_{\mathrm{an}}} K$ (since we have all $r \in \mathbb{R}$ as a constant symbol of L^D_{an}), and we may suppose e is the identity on $\mathbb{R}^D_{\mathrm{an}}$.

Let

$$\mu = \{\alpha \in M_1 : |\alpha| < r \text{ for all } r \in \mathbb{R}, r > 0\}.$$

Now for $n \in \mathbb{N}$, $f \in \mathcal{O}_n$, and $r \in \mathbb{R}_{>0}$, with $\overline{B_r^n} \subseteq \mathrm{dom}(f)$ (which we abbreviate by saying that (n, r, f) is *acceptable*), let us denote by f_r the interpretation of the corresponding function symbol in M_1 and M_2. Certainly for any such suitable r, f_r defines a natural, untruncated function $\mu^n \to M_1$.

Lemma 9.11. *With the above notation, suppose that there exists a map $e'' : K\langle a\rangle \cap \mu \to M_2$ extending $e \restriction K \cap \mu$ such that for all $n \in \mathbb{N}$, for all $\alpha_1, \ldots, \alpha_n \in K\langle a\rangle \cap \mu$ and for all f, r as above,*

$$M_1 \models f_r(\alpha_1, \ldots, \alpha_n) > 0 \Rightarrow M_2 \models f_r(e''(\alpha_1), \ldots, e''(\alpha_n)) > 0$$
$$M_1 \models f_r(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow M_2 \models f_r(e''(\alpha_1), \ldots, e''(\alpha_n)) = 0.$$

Then e'' extends to an L_{an}^D-embedding $e' : K\langle a\rangle \to M_2$ (which also extends e).

Proof. If $b \in K\langle a\rangle$, then either $s + b \in \mu$ for some (unique) $s \in \mathbb{R}$, and we set $e'(b) = e''(s + b) - s$; or b is infinite and $1/b \in \mu$, in which case we set $e'(b) = 1/e''(1/b)$. It is easy to check that e' is an ordered field embedding $K\langle a\rangle \to M_2$ extending e. (Note that the $\mathcal{O}_n$'s include all polynomials.) In particular e' preserves D.

Suppose f, r as above. Let $\alpha_1, \ldots, \alpha_n \in K\langle a\rangle$. If $|\alpha_i| \geq r$ for some i, then $f_r(\alpha_1, \ldots, \alpha_n) = 0$. But $|e'(\alpha_i)| \geq e'(r) = r$ (since e' is an ordered field embedding extending e), therefore $f_r(e'(\alpha_1), \ldots, e'(\alpha_n)) = 0$. If $|\alpha_i| < r$ for $i = 1, \ldots, n$, let $\alpha_{n+1} = f_r(\alpha_1, \ldots, \alpha_n)$ and write $\alpha_i = \beta_i - s_i$ for $i = 1, \ldots, n+1$, where $\beta_i \in \mu$, $s_i \in \mathbb{R}$. Note that $|s_i| \leq r$ for $i = 1, \ldots, n$, and β_{n+1}, s_{n+1} exists because f_r is bounded and hence α_{n+1} is finite.

Define $k : \mathbb{R}^{n+1} \to \mathbb{R}$ by $k(x_1, \ldots, x_{n+1}) = \tilde{f}(x_1 - s_1, \ldots, x_n - s_n) - x_{n+1} + s_{n+1}$. Then $k = \tilde{g}$ for some $g \in \mathcal{O}_{n+1}$ since $\overline{B}_r^n \subseteq \mathrm{dom}(f)$ and so $\langle s_1, \ldots, s_n\rangle \in \mathrm{dom}(f)$. Now choose $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, such that $\overline{B}_\varepsilon^{n_1} \subseteq \mathrm{dom}(g)$ and $\overline{B}_{r+\varepsilon}^n \subseteq \mathrm{dom}(f)$. Then $0 = g_\varepsilon(\beta_1, \ldots, \beta_{n+1})$, so $0 = g_\varepsilon(e''(\beta_1), \ldots, e''(\beta_{n+1}))$ (by hypothesis). But

$$T_{\mathrm{an}}^D \models \forall x_1, \ldots, x_{n+1} (\max |x_i| < \varepsilon \to g_\epsilon(x_1, \ldots, x_{n+1}) = f_{r+\varepsilon}(x_1 - s_1, \ldots, x_n - s_n) - x_{n+1} + s_{n+1}).$$

Hence

$$\begin{aligned} 0 &= f_{r+\varepsilon}(e''(\beta_1) - s_1, \ldots, e''(\beta_n) - s_n) - e''(\beta_{n+1}) + s_{n+1} \\ &= f_{r+\varepsilon}(e'(\alpha_1), \ldots, e'(\alpha_n)) - e'(\alpha_{n+1}) \\ &= f_r(e'(\alpha_1), \ldots, e'(\alpha_n)) - e'(\alpha_{n+1}) \end{aligned}$$

(The second equality follows from the definition of e', while the third holds since $|e'(\alpha_i)| < r$ for $i = 1, \ldots, n$ as e' is an ordered field embedding.) Hence in all cases, $e'(f_r(\alpha_1, \ldots \alpha_n)) = f_r(e'(\alpha_1), \ldots, e'(\alpha_n))$. So e' is an L_{an}^D-embedding as required. □

Exercise 9.12. *Suppose $M_1, M_2 \models T_{an}^D$ with $K \subseteq M_1$, $e : K \to M_2$ as above. Then for all acceptable $(m+n, r, f)$ and $c_1, \ldots, c_m \in K \cap \mu$ we have*

$$M_1 \models \forall \bar{y} \in \mu \, f_r(\bar{c}, \bar{y}) = 0 \Rightarrow M_1 \models \forall \bar{y} \, f_r(\bar{c}, \bar{y}) = 0$$
$$\Rightarrow M_2 \models \forall \bar{y} \, f_r(e(\bar{c}), \bar{y}) = 0.$$

To prove 9.1 it is clearly sufficient, in view of 9.11 and the saturation of M_2, to establish the following:

Lemma 9.13. *Let $\varphi(\bar{x}, \bar{y}) = \varphi(x_1, \ldots, x_m, y_1, \ldots, y_n)$ be a conjunction of formulas of the form $f_r(\bar{x}, \bar{y}) > 0$ or $f_r(\bar{x}, \bar{y}) = 0$, where $(m+n, r, f)$ is acceptable. Suppose $c_1, \ldots, c_m \in \mu \cap K$, $\alpha_1, \ldots, \alpha_n \in \mu$, and $M_1 \models \varphi[\bar{c}, \bar{\alpha}]$. Then $\exists \beta_1, \ldots, \beta_n \in M_2$ such that $M_2 \models \varphi[e(\bar{c}), \bar{\beta}]$.*

Proof. By induction on n. The case $n = 0$ is trivial, but we do the case $n = 1$. We may clearly suppose that all those r's for which f_r occurs in φ are the same, say r.

Let $\mathcal{S}$ be the set of $f \in \mathcal{O}_{n+1}$ such that f_r occurs in φ. Let $c_1, \ldots, c_m \in \mu \cap K$, $\alpha_1 \in \mu$ be such that $M_1 \models \varphi[c_1, \ldots, c_n, \alpha_1]$. Let $f \in \mathcal{S}$.

By 7.10, there exist $\alpha \in \mathbb{N}$, $d > 0$, $a_i(\bar{x}) \in \mathcal{O}_m$, and units $u_i(\bar{x}, y_1) \in \mathcal{O}_{m+1}$ $(\forall i < d)$ such that in $\mathcal{O}_{m+1}$ we have the identity:

$$f(\bar{x}, y_1) = \sum_{i<d} a_i(\bar{x}) y_1^i u_i(\bar{x}, y_1).$$

Clearly we may suppose that it is the same d for all $f \in \mathcal{S}$.

Let $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ be small enough so that all $F \in \mathcal{O}_N$ considered in this proof are such that (N, ε, F) is acceptable.

Now work in M_1. We have for all $y_1 \in M_1$, $|y_1| < \varepsilon$ implies

$$f_\varepsilon(\bar{c}, y_1) = \sum_{i<d} a_{i,\varepsilon}(\bar{c}) y_1^i u_{i,\varepsilon}(\bar{c}, y_1). \tag{2}$$

If $a_i(\bar{c}) = 0$ for all $i < d$, then also $a_i(e(\bar{c})) = 0$ for all $i < d$ and we may omit all atomic formulas involving f from φ.

Otherwise, choose $i_0 < d$ such that $0 \neq |a_{i_0,\varepsilon}(\bar{c})| \geq |a_{i,\varepsilon}(\bar{c})|$ for all $i < d$. Let

$$k_i' = \frac{a_{i,\varepsilon}(\bar{c})}{|a_{i_0,\varepsilon}(\bar{c})|} \tag{3}$$

for all $i < d$. Since K is a field, $k_i' \in K$ for $i < d$. Furthermore, $|k_i'| \leq 1$ for all $i < d$ and $k_{i_0}' = \pm 1$. Define k_i's by:

$$k_i' = k_i + s_i \text{ where } k_i \in \mu \cap K \text{ and } s_i \in \mathbb{R} \text{ for all } i < d. \tag{4}$$

Note that $k_{i_0} = 0$ and $s_{i_0} = \pm 1$.

Define $g \in \mathcal{O}_{m+1+(d-1)}$, with $\bar{z} = \{z_i \mid i < d, i \neq i_0\}$ the new variables, by

$$g(\bar{x}, y_1, \bar{z}) = s_{i_0} u_{i_0}(\bar{x}, y_1) y_1^{i_0} + \sum_{i<d, i \neq i_0} u_i(\bar{x}, y_1)(z_i + s_i) y_1^i. \tag{5}$$

Then for all $y_1 \in M_1$, $|y_1| < \varepsilon$, we have (from (2)-(5))

$$f_\varepsilon(\bar{c}, y_1) = |a_{i_0,\varepsilon}(\bar{c})| g(\bar{c}, y_1, \bar{k}). \tag{6}$$

Now choose $p \in \mathbb{N}$ minimal such that $s_p \neq 0$. Obviously p exists and $p \leq i_0$. Now clearly g is regular in y_1 of order p, hence (by 7.7) (in $\mathcal{O}_{m+1+(d-1)}$):

$$g(\bar{x}, y_1, \bar{z}) = (y_1^p + h_1(\bar{x}, \bar{z}) y_1^{p-1} + \ldots + h_p(\bar{x}, \bar{z})) Q(\bar{x}, y_1, \bar{z}) \tag{7}$$

for some $h_i \in \mathcal{O}_{m+d-1}$ and a unit $Q \in \mathcal{O}_{m+1+(d-1)}$.

By (6), for all $y_1 \in M_1$, $|y_1| < \varepsilon$ implies

$$f_\varepsilon(\bar{c}, y_1) = |a_{i_0,\varepsilon}(\bar{c})| Q_\varepsilon(\bar{c}, y_1, \bar{k})(y_1^p + \ldots + h_p(\bar{c}, \bar{k})). \tag{8}$$

Now we may suppose ε has been chosen small enough so that

$$T_{\mathrm{an}}^D \vdash \forall \bar{x}, \bar{z}, y_1 \in \overline{B}_\varepsilon \, (|Q_\varepsilon(\bar{x}, y_1, \bar{z}) - Q_\varepsilon(\bar{0}, 0, \bar{0})| < \frac{1}{2} |Q_\varepsilon(\bar{0}, 0, \bar{0})|). \tag{9}$$

By the exercise, (8) also holds in M_2 upon applying e to the parameters—note they all lie in $\mu \cap K$.

By (8), (9), $\varphi(\bar{c}, y_1)$ is equivalent in M_1 to some $\psi(\overline{h_\varepsilon(\bar{c}, \bar{k})}, y_1)$ for some (quantifier-free) formula $\psi(t_1, \ldots, t_q, y_1)$ of $\overline{L}$ (where $q = \sum_{f \in \mathcal{S}} p$) and $\varphi(e(\bar{c}), y_1)$ is equivalent in M_2 to $\psi(\overline{h_\varepsilon(e(\bar{c}), e(\bar{k}))}, y_1)$, for all $y_1 \in M_2$ with $|y_1| < \varepsilon$.

Now $M_1 \models \exists y_1 \, (|y_1| < \varepsilon \wedge \varphi(\bar{c}, y_1))$ (namely $y_1 = \alpha_1$), so

$$M_1 \models \exists y_1 \left(|y_1| < \varepsilon \wedge \psi \left(\overline{h_\varepsilon \, (\bar{c}, \bar{k})}, y_1 \right) \right).$$

But $\exists y_1 \, (|y_1| < \varepsilon \wedge \psi(\bar{t}, y_1))$ is equivalent in M_1 and M_2 to a quantifier free formula of $\bar{L}$ (since $M_1 \restriction \bar{L}, M_2 \restriction \bar{L} \equiv \bar{\mathbb{R}}$), so:

$$M_2 \models \exists y_1 \left(|y_1| < \varepsilon \wedge \psi \left(e \left(\overline{h_\varepsilon(\bar{c}, \bar{k})} \right), y_1 \right) \right)$$

(since e is certainly an $\bar{L}$-embedding), and then

$$M_2 \models \exists y_1 \left(|y_1| < \varepsilon \wedge \psi \left(h_\varepsilon(e(\bar{c}), e(\bar{k})), y_1 \right) \right)$$

(since e is an L_{an}-embedding), and finally $M_2 \models \exists y_1 \, \varphi(e(\bar{c}), y_1)$ by the previous paragraph.

For the inductive step we proceed exactly as above to arrive at (5):

$$g(\bar{x}, \bar{y}, \bar{z}) = s_{\nu^0} u_{\nu^0}(\bar{x}, \bar{y}) y^{\nu^0} + \sum_{\substack{\nu \in \mathbb{N}^{n+1} \\ |\nu| < d \\ \nu \neq v^0}} u_\nu(\bar{x}, \bar{y})(z_\nu + s_\nu) \bar{y}^\nu$$

where now $\bar{y} = y_1, \ldots, y_{n+1}$.

We want to write g in the form (7), but it might not be regular in any of the $\bar{y}$-variables. To resolve this difficulty we define

$$\Lambda(\bar{y}) = \langle y_1 + y_{n+1}^{d^n}, y_2 + y_{n+1}^{d^{n-1}}, \ldots, y_n + y_{n+1}^{d}, y_{n+1}\rangle.$$

This is a bijection from $\mu^{n+1} \to \mu^{n+1}$ with inverse

$$\Omega(\bar{y}) = \langle y_1 - y_{n+1}^{d^n}, \ldots, y_n - y_{n+1}^{d}, y_{n+1}\rangle.$$

Now

$$g(\bar{0}, \Lambda(0, \ldots, 0, y_{n+1}), \bar{0}) = \sum_{\substack{v \in \mathbb{N}^{n+1} \\ |v| < d}} u_v(\bar{0}, \Lambda(\bar{0}, y_{n+1}))s_v y_{n+1}^{v_1 d^n + v_2 d^{n-1} + \ldots + v_n d + v_{n+1}}.$$

Since the exponents of y_{n+1} here are all distinct it follows that if v is lexicographically minimal such that $s_v \neq 0$ (v exists since $s_{v^0} \neq 0$) and $p = v_1 d^n + \ldots + v_{n+1}$ (where $v = \langle v_1, \ldots, v_{n+1}\rangle$). Then $g(\bar{x}, \Lambda(y_1, \ldots, y_{n+1}), \bar{z})$ is regular in y_{n+1} of order p.

Now, as above, we have (8) in the form

$$\forall y_1, \ldots, y_{n+1} \in M_1, |y_1|, \ldots, |y_{n+1}| < \varepsilon \Rightarrow$$

$$f_\varepsilon(\bar{c}, \Lambda(y_1, \ldots, y_{n+1})) = |a_{v^0,\varepsilon}(\bar{c})| Q_\varepsilon(\bar{c}, y_1, \ldots, y_{n+1}, \bar{k})(y_{n+1}^p + \ldots + h_{p,\varepsilon}(\bar{c}, \bar{k}, y_1, \ldots, y_n)). \tag{10}$$

Notice that the transformation Λ does not depend on $f \in \mathcal{S}$.

Now, writing "$\exists_\varepsilon u$..." for the quantifier "$\exists u(|u| < \varepsilon \wedge$ ...", we have that $\exists_\varepsilon y_1, \ldots, y_{n+1}\, \varphi(\bar{c}, y_1, \ldots, y_{n+1})$ is equivalent to $\exists_\varepsilon y_1, \ldots, y_{n+1}\, \varphi(\bar{c}, \Lambda(y_1, \ldots, y_{n+1}))$, and the latter is equivalent to some $\exists_\varepsilon y_1, \ldots, y_{n+1}\, \psi(\bar{c}, \bar{k}, y_1, \ldots, y_{n+1})$ where y_{n+1} only occurs polynomially. This, by Tarski, is equivalent to $\exists_\varepsilon y_1, \ldots, y_n\, \psi(\bar{c}, \bar{k}, y_1, \ldots, y_n)$ for some quantifier free formula ψ of L_{an}. Moreover, as above, these equivalences hold in M_2 with e applied to parameters (using exercise 9.12 on (10)). The result follows by induction on n. □