ON THE ELEMENTARY THEORY OF RINGS OF WITT VECTORS WITH MULTIPLICATIVE SET OF REPRESENTATIVES FOR THE RESIDUE FIELD

Lou van den Dries*

Theorems of Ax, Kochen and Ersov tell us that the elementary theory of a henselian valuation ring of equal characteristic 0 is completely determined by the elementary theories of its value group and residue field, see [1], [3], [4], and the references therein. This elementary classification goes through even when a predicate is added for a field of representatives of the residue field.

Here we provide a mixed characteristic analogue of the latter when the residue field is perfect of characteristic p and the maximal ideal is generated by p. For a complete discrete valuation ring with these properties the analogue of 'field of representatives' is 'multiplicative set of representatives for the residue field' and is due to Witt. For proofs of this and related results mentioned below that we shall use we refer to Serre [5, Ch. II]. We now proceed to precise statements.

Fix a prime number p. Let A be a complete discrete valuation ring with maximal ideal $\mathfrak{m} = pA$ and perfect residue field $\boldsymbol{k} = A/\mathfrak{m}$ (of characteristic p). Let $\pi : A \to \boldsymbol{k}$ be the residue class map. There is a unique multiplicatively closed set $S \subseteq A$ that is mapped bijectively onto $\boldsymbol{k}$ by π. (Among the elements of S are 0, 1 and -1.) Each element $a \in A$ can be written uniquely as $a = \sum_{i=0}^{\infty} s_i p^i$ with coefficients $s_i \in S$. By [3, p. 413] one can axiomatize $\mathrm{Th}(A)$ in terms of $\mathrm{Th}(\boldsymbol{k})$. We extend this to an axiomatization of $\mathrm{Th}(A, S)$ in the theorem below. In its proof we shall use the functor W that assigns to $\boldsymbol{k}$ the corresponding ring $W(\boldsymbol{k})$ of "Witt vectors" over $\boldsymbol{k}$. The rings $W(\boldsymbol{k})$ and A are isomorphic.

As in [5, p. 44], let $f : \boldsymbol{k} \to A$ denote the system of multiplicative representatives, that is, $\pi(f(x)) = x$ and $f(xy) = f(x)f(y)$ for $x, y \in \boldsymbol{k}$, and thus $f(\boldsymbol{k}) = S$. The following easy result on $\mathbf{Z}$-linear relations among elements of S is decisive.

Let $k = (k_1, \ldots, k_n)$ be an n-tuple of integers, and let $X = (X_1, \ldots, X_n)$ be an n-tuple of distinct indeterminates. Given an n-tuple $b = (b_1, \ldots, b_n)$ of elements in an abelian (additive) group B, put $k \cdot b := k_1 b_1 + \cdots + k_n b_n$.

Lemma 1. *There are polynomials $R_1, \ldots, R_N \in \mathbf{F}_p[X]$, depending only on p and k and not on A, such that for all $x = (x_1, \ldots, x_n) \in \boldsymbol{k}^n$:*

$$k \cdot f(x) = 0 \Longleftrightarrow R_1(x) = \cdots = R_N(x) = 0 \qquad (\textit{where } f(x) := (f(x_1), \ldots, f(x_n)).$$

Partially supported by the National Science Foundation.

Proof. By [5, Prop. 9, p. 47] we have for $x \in \boldsymbol{k}^n$:

$$k \cdot f(x) = \sum_{i=0}^{\infty} f\big(P_i(x^{p^{-i}})\big)p^i$$

where $P_i \in \mathbf{F}_p[X]$ depends only on i, p and k. The ideal of $\mathbf{F}_p[X]$ generated by the polynomials P_i, $i \in \mathbf{N}$, is generated by finitely many among them, say $R_1, \ldots, R_N$. Then $R_1, \ldots, R_N$ have the property described in the lemma.

The $\mathbf{Z}$-linear relations together with the multiplicative relations $s = s_1 s_2$ among the elements of S generate all polynomial relations over $\mathbf{Z}$ among elements of S:

Lemma 2. *Let U and V be multiplicatively closed subsets of fields E and F of characteristic 0. Let $\lambda : U \to V$ be a bijection such that $\lambda(u_1 u_2) = \lambda(u_1)\lambda(u_2)$ for all $u_1, u_2 \in U$, and such that for all $k \in \mathbf{Z}^n$ and all $u \in U^n$ we have: $k \cdot u = 0 \iff k \cdot \lambda(u) = 0$. Then λ extends to an isomorphism from the subfield $\mathbf{Q}(U)$ of E onto the subfield $\mathbf{Q}(V)$ of F.*

Proof. Let $P = \sum_i c_i X^i \in \mathbf{Z}[X]$ where the sum is over finitely many $i \in \mathbf{N}^n$. Then, given $u \in U^n$, we have $P(u) = \sum_i c_i u^i = 0$ if and only if $\sum_i c_i \lambda(u^i) = \sum_i c_i \lambda(u)^i = P(\lambda(u)) = 0$, by the hypothesis of the lemma. The conclusion of the lemma follows easily.

For each $k \in \mathbf{Z}^n$ we fix a tuple $R = (R_1, \ldots, R_N) \in \mathbf{F}_p[X]^N$ with the property of Lemma 1. Let T be the theory in the language $\{0, 1, +, -, \cdot, \mathbf{S}\}$ (the language of rings with an extra unary predicate $\mathbf{S}$) whose models are the structures (B, Σ) such that

(1) B is a valuation ring with fraction field E of characteristic 0.
(2) Σ is a multiplicatively closed subset of B that is mapped bijectively onto $B/\mathfrak{m}(B)$ by the residue class map $b \mapsto \overline{b} : B \to B/\mathfrak{m}(B)$.
(3) $\mathfrak{m}(B) = pB$ and $B/\mathfrak{m}(B)$ is a perfect field.
(4) The local ring B is henselian.
(5) For each $k \in \mathbf{Z}^n$ we have: $k \cdot \sigma = 0 \iff R(\overline{\sigma}) = 0$, for all $\sigma \in \Sigma^n$, where $R \in \mathbf{F}_p[X]^N$ is the tuple associated to k, and $\overline{\sigma} := (\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$.

Theorem. *Two models (B, Σ) and (B', Σ') of T are elementarily equivalent if and only if their residue fields $B/\mathfrak{m}(B)$ and $B'/\mathfrak{m}(B')$ are elementarily equivalent, and their value groups Γ and Γ' are elementarily equivalent.*

Here $\Gamma = v(E^\times)$ is the value group of the valuation v on the fraction field E of B with valuation ring B, and Γ', v' and E' are defined in the same way with B' instead of B. These value groups are considered as ordered abelian groups.

Following Kochen [3, pp. 407-408], the idea of the proof is to pass to sufficiently saturated models where the valuation can be decomposed into a valuation of equal characteristic 0 and a complete discrete valuation.

Proof. One direction is obvious. For the other direction we assume that $B/\mathfrak{m}(B) \equiv B'/\mathfrak{m}(B')$ and $\Gamma \equiv \Gamma'$. To show that then $(B, \Sigma) \equiv (B', \Sigma')$, we may assume these two models of T are $\aleph_1$-saturated. We focus on (B, Σ), but the same analysis will apply to (B', Σ'). We coarsen v to the valuation $\widetilde{v}$ on E with value group $\widetilde{\Gamma} := \Gamma/\mathbf{Z}\cdot 1$ (where $1 := v(p)$ is the smallest positive element of Γ) by setting $\widetilde{v}(a) = v(a) + \mathbf{Z}\cdot 1$ for $a \in E^\times$. The valuation ring of $\widetilde{v}$ is

$$\widetilde{B} := B[1/p] = \{a \in E : v(a) \geq -n \cdot 1 \text{ for some } n\}$$

with maximal ideal $\widetilde{\mathfrak{m}} := \mathfrak{m}(\widetilde{B}) = \{a \in E : v(a) \geq n \cdot 1 \text{ for all } n\}$, and residue field $K := \widetilde{B}/\widetilde{\mathfrak{m}}$ of characteristic 0. Then $\widetilde{\mathfrak{m}}$ is also a prime ideal of B, and $A := B/\widetilde{\mathfrak{m}}$ is a valuation ring of K, with maximal ideal pA. The residue class map $\lambda : \widetilde{B} \to K$ maps B onto A, and induces by passing to quotients an isomorphism $B/pB \cong A/pA$ of the residue fields of B and A. We put $\boldsymbol{k} := B/pB = A/pA$ by identifying these residue fields via this isomorphism. Thus $p = \pi \circ (\lambda|B)$ where $p : B \to \boldsymbol{k}$ and $\pi : A \to \boldsymbol{k}$ are the residue class maps. Hence $S := \lambda(\Sigma)$ is a multiplicatively closed subset of A that is mapped bijectively onto $\boldsymbol{k}$ by the residue class map $A \to \boldsymbol{k}$. By $\aleph_1$-saturation A is a complete discrete valuation ring, and therefore (A, S) is also a model of T, by Lemma 1. We now show how to "lift" the quotient (K, A, S) of $(\widetilde{B}, B, \Sigma)$ back to $(\widetilde{B}, B, \Sigma)$. The bijection $\sigma \mapsto \lambda(\sigma) : \Sigma \to S$ is multiplicative, so by the second lemma λ maps the ring $\mathbf{Z}[\Sigma]$ isomorphically onto $\mathbf{Z}[S] \subseteq K$. Thus the fraction field $\mathbf{Q}(\Sigma) \subseteq E$ of $\mathbf{Z}[\Sigma]$ is actually contained in $\widetilde{B}$, and λ maps $\mathbf{Q}(\Sigma)$ isomorphically onto $\mathbf{Q}(S)$. Since B is henselian, so is its localization $\widetilde{B}$. The residue field K of $\widetilde{B}$ being of characteristic 0, it follows that there is a field L with $\mathbf{Q}(\Sigma) \subseteq L \subseteq \widetilde{B}$ such that λ maps L isomorphically onto all of K. Then $(L, B \cap L, \Sigma)$ is the desired lifting of (K, A, S), that is, $(L, B \cap L, \Sigma) \subseteq (\widetilde{B}, B, \Sigma)$ and λ restricts to an isomorphism $(L, B \cap L, \Sigma) \cong (K, A, S)$. We now shift our attention from (B, Σ) (an expansion of the mixed characteristic valuation ring B) to $(\widetilde{B}, L, B \cap L, \Sigma)$ which we view as the equal characteristic valuation ring $\widetilde{B}$ equipped with a lifting of its expanded residue field (K, A, S). Note that B is definable in $(\widetilde{B}, L, B \cap L, \Sigma)$ as follows: $B = \{x \in \widetilde{B} : x - y \in \widetilde{\mathfrak{m}} \text{ for some } y \in B \cap L\}$.

We now carry out the same construction with (B', Σ'), introducing $\widetilde{v}'$, $\widetilde{\Gamma}'$, $\widetilde{B}'$, K', $\boldsymbol{k}'$, A', S' and L' in the same way we obtained the corresponding unaccented objects from (B, Σ). As we indicated above it now suffices to show that $(\widetilde{B}, L, B \cap L, \Sigma) \equiv (\widetilde{B}', L', B' \cap L', \Sigma')$. Consider the rings $W(\boldsymbol{k})$ and $W(\boldsymbol{k}')$ of Witt vectors over $\boldsymbol{k}$ and $\boldsymbol{k}'$, and for perfect subfields F of $\boldsymbol{k}$ and F' of $\boldsymbol{k}'$, consider the subrings $W(F)$ and $W(F')$ of $W(\boldsymbol{k})$ and $W(\boldsymbol{k}')$, as well as the corresponding multiplicatively closed sets $S(F) \subseteq W(F)$ and $S(F') \subseteq W(F')$ that are mapped bijectively onto F and F' by the canonical maps $W(F) \to F$ and $W(F') \to F'$. In particular we have isomorphisms $(A, S) \cong (W(\boldsymbol{k}), S(\boldsymbol{k}))$ and $(A', S') \cong (W(\boldsymbol{k}'), S(\boldsymbol{k}'))$. Since $\boldsymbol{k}$ and $\boldsymbol{k}'$ are elementarily equivalent and $\aleph_1$-saturated, the isomorphisms $F \to F'$ between the countable $F \preceq \boldsymbol{k}$ and $F' \preceq \boldsymbol{k}'$ form a back-and-forth system between $\boldsymbol{k}$ and $\boldsymbol{k}'$. Each isomorphism $F \to F'$ of this system induces an isomorphism $(W(F), S(F)) \to (W(F'), S(F'))$, thus giving rise to a back-and-forth system between $(W(\boldsymbol{k}), S(F))$ and $(W(\boldsymbol{k}'), S(\boldsymbol{k}'))$. Hence $(W(\boldsymbol{k}), S(F)) \equiv (W(\boldsymbol{k}'), S(\boldsymbol{k}'))$, and so $(A, S) \equiv (A', S')$. Therefore $(K, A, S) \equiv (K', A', S')$, and thus $(L, B \cap L, \Sigma) \equiv (L', B' \cap L', \Sigma')$. This allows us to apply Lemma 3 below to reach the desired conclusion $(\widetilde{B}, L, B \cap L, \Sigma) \equiv (\widetilde{B}', L', B' \cap L', \Sigma')$. This application also depends on the fact that $\Gamma \equiv \Gamma'$ implies $\widetilde{\Gamma} \equiv \widetilde{\Gamma}'$.

The lemma appealed to at the end is a variant of the well-known results of Ax, Kochen and Ersov, and can be proved in the same way, cf. [1, 3, 4]. In this lemma the value group Γ of a valuation ring $\mathcal{O}$ refers to the value group of the valuation v on the fraction field of $\mathcal{O}$ such that v has $\mathcal{O}$ as its valuation ring. This value group is considered as an ordered abelian group.

Lemma 3. *Let $\mathcal{O}$ and $\mathcal{O}'$ be henselian valuation rings of equal characteristic* 0 *with value groups Γ and Γ', and let $L \subseteq \mathcal{O}$ and $L' \subseteq \mathcal{O}'$ be fields that are mapped onto the residue fields of $\mathcal{O}$ and $\mathcal{O}'$ by the residue class maps $\mathcal{O} \to \mathcal{O}/\mathfrak{m}(\mathcal{O})$ and $\mathcal{O}' \to \mathcal{O}'/\mathfrak{m}(\mathcal{O}')$. Let $\mathcal{L}$ be an extension of the language of rings, and let L^* and ${L'}^*$ be expansions of the rings L and L' to $\mathcal{L}$-structures. Then*

$$(\mathcal{O}, L^*) \equiv (\mathcal{O}', {L'}^*) \Longleftrightarrow \Gamma \equiv \Gamma' \text{ and } L^* \equiv {L'}^*.$$

The following variant of the theorem can be obtained in the same way, by appealing to a corresponding variant of Lemma 3 (see [4]). We let $\boldsymbol{k}$ and $\boldsymbol{k}'$ denote the residue fields of the valuation rings B and B', and let Γ and Γ' be their value groups as in the theorem.

Proposition. *Let (B, Σ) and (B', Σ') be models of T such that $(B, \Sigma) \subseteq (B', \Sigma')$ (so there are natural inclusions $\boldsymbol{k} \subseteq \boldsymbol{k}'$ and $\Gamma \subseteq \Gamma'$). Then*

$$(B, \Sigma) \preceq (B', \Sigma') \Longleftrightarrow \boldsymbol{k} \preceq \boldsymbol{k}' \text{ and } \Gamma \preceq \Gamma'.$$

Remark. In Lemma 1 we described the $\mathbf{Z}$-linear relations among the elements of $S \subseteq A$. Another way to do this, in some respects more illuminating, is as follows.

First, any root of unity in A belongs to S and any tuple $\zeta = (\zeta_1, \dots, \zeta_n)$ $(n > 0)$ of roots of unity $\zeta_i \in A$ satisfies non-trivial $\mathbf{Z}$-linear relations. These relations produce in certain obvious ways further relations, for example, for any $s \in S \setminus \{0\}$ the tuple $s\zeta$ satisfies the same $\mathbf{Z}$-linear relations as ζ.

Secondly, an element $a \in A$ belongs to S if and only if $F(a) = a^p$, where F is the canonical lifting of the Frobenius map to an automorphism of A (see [5]).

Using this last fact one can show, following [2], that all $\mathbf{Z}$-linear relations among elements of S arise from the $\mathbf{Z}$-linear relations among the roots of unity in A. This was pointed out to me by Hrushovski.

References

[1] J. Ax, A metamathematical approach to some problems in number theory, AMS Symposium (1973), pp. 161-190.

[2] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, preprint.

[3] S. Kochen, The model theory of local fields, in "Logic Conference, Kiel 1974" (Proceedings), Lecture Notes in Mathematics 499, pp. 384-425, Springer, Berlin 1975.

[4] F.-V. Kuhlmann and A. Prestel, On places of algebraic function fields, J. reine angew. Math. 400 (1989), 185-202.

[5] J.-P. Serre, Corps Locaux, Hermann, Paris, 1962.

University of Illinois at Urbana-Champaign
E-mail address: vddries@math.uiuc.edu