PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

MARVIN J. GREENBERG

Rational points in henselian discrete valuation rings

Publications mathématiques de l'I.H.É.S., tome 31 (1966), p. 59-64
<http://www.numdam.org/item?id=PMIHES_1966__31__59_0>

RATIONAL POINTS IN HENSELIAN DISCRETE VALUATION RINGS

by MARVIN J. GREENBERG

1.

Let R be a Henselian discrete valuation ring, with t a generator of the maximal ideal, k the residue field, and K the field of fractions. Let R^* be the completion of R, K^* its field of fractions. If $F=(F_1, \ldots, F_r)$ is a system of r polynomials in n variables with coefficients in R, and x is an n-tuple with coordinates in R, set $F(x)=(F_1(x), \ldots, F_r(x))$. If F' is another system of r' polynomials, let FF' denote the system of rr' products. By the ideal FR[X] generated by F is meant the ideal in R[X] generated by $F_1, \ldots, F_r$.

Theorem 1. — Assume, in case K *has characteristic* $p>0$, *that* K^* *is separable over* K. *Then there are integers* $N\geq 1$, $c\geq 1$, $s\geq 0$ *depending on* FR[X] *such that for any* $\nu\geq N$ *and any* x *in* R *such that*

$$F(x)\equiv 0 \pmod{t^\nu}$$

there exists y *in* R *such that*

$$y\equiv x \pmod{t^{[\nu/c]-s}}$$

$$F(y)=0$$

Corollary 1. — Let Z *be a prescheme of finite type over* R. *Then there are integers* $N\geq 1$, $c\geq 1$, $s\geq 0$ *depending on* Z *such that for* $\nu\geq N$ *and for any point* x *of* Z *in* R/t^ν, *the image of* x *in* $Z(R/t^{[\nu/c]-s})$ *lifts to a point of* Z *in* R.

Proof. — We can take a finite covering of Z by affine opens Z_i. We have $Z(S)=\bigcup_i Z_i(S)$ for any local R-algebra S, hence the maxima of the integers for the Z_i will do for Z.

Corollary 2. — Z *has a point in* R *if and only if* Z *has a point in* R/t^ν *for all* $\nu\geq 1$.

Let V be the algebraic set in affine n-space over K which is the locus of zeros of F. In the special case that R is complete and V is K-irreducible, non-singular, with a separably generated function field over K, Néron [**4**; Prop. 20, p. 38] has proved this theorem, showing that in this case one can take $c=1$. However, in the general case we may have $c>1$ (consider the polynomial Y^2-X^3 and for any even integer 2ν the point $x=(t^\nu, t^\nu)$). Theorem 1 implies that the hypothesis of non-singularity in [**4**; Prop. 22] can be dropped, so that the sets in that proposition are always constructible.

Theorem 1 is proved by induction on the dimension m of V. If $m=-1$, i.e., the ideal FR[X] contains a non-zero constant, it is clear. Suppose $m>0$.

We may assume the ideal FR[X] is equal to its own radical (i.e., the scheme over R defined by F is reduced): For let E generate its radical. Then some power E^q is in FR[X]. From $F(x)\equiv 0 \pmod{t^\nu}$

we conclude t^ν divides $E^q(x)$, so that

$$E(x) \equiv 0 \pmod{t^{[\nu/q]}}$$

If N', c', s' are integers for E, we see that $N = qN'$, $c = qc'$, $s = s'$ are integers for F.

We may further assume V is K-irreducible: For if $V = W \cup W'$, where W, W' are algebraic sets defined respectively by systems of polynomials G, G' with coefficients in R, let N', c', s' (resp. N'', c'', s'') be integers for G (resp. for G'). If x in R satisfies

$$F(x) \equiv 0 \pmod{t^\nu}$$

then either $$G(x) \equiv 0 \quad \text{or} \quad G'(x) \equiv 0 \pmod{t^{[\nu/2]}}$$

since GG' is in the ideal FR[X]. Thus

$$N = 2\max(N', N'')$$
$$c = 2\max(c', c'')$$
$$s = \max(s', s'')$$

will work for F.

Then there are two cases:

Case 1. — *V is separable over* K.

Let J be the Jacobian matrix of F, and let D be the system of minors of order $n-m$ taken from det J. The the locus of common zeros of D and F is a proper K-closed W in V. By inductive hypothesis there are integers N', c', s' for the system (D, F).

For each system $F_{(i)}$ of $n-m$ polynomials out of F, (i) a system of $n-m$ indices, let $V_{(i)}$ be the locus over K of zeros of $F_{(i)}$, and let $V_{(i)}^+$ be the union of the K-irreducible components of $V_{(i)}$ which have dimension m and are different from V; let $G_{(i)}$ be a system of generators for the ideal of $V_{(i)}^+$ in R[X]. By inductive assumption there are integers $N_{(i)}$, $c_{(i)}$, $s_{(i)}$ for the system $(G_{(i)}, F)$.

If x is a point of $V_{(i)}$ in some extension of K such that for some (j)

$$D_{(i),(j)}(x) \neq 0$$

then the tangent hyperplanes of $F_{i_1}, \ldots, F_{i_{n-m}}$ at x are transversal, and x lies on exactly one component of $V_{(i)}$, that component having dimension m.

We now invoke (see Lemma 2, n° 3)

Newton's Lemma. — *If x in* R *is such that*

$$F_{(i)}(x) \equiv 0 \pmod{t^{2\mu+1}}$$
$$D_{(i),(j)}(x) \not\equiv 0 \pmod{t^\mu} \text{ for some } (j)$$

then there exists y in R *such that*

$$F_{(i)}(y) = 0$$
$$y \equiv x \pmod{t^\mu}$$

Hence $$D_{(i),(j)}(y) \neq 0$$

If we knew also $$G_{(i)}(y) \neq 0$$

we could deduce that y is a point of V.

Take ν so large that

$$\mu = [(\nu - 1)/2] \geq \max(N', \text{all } N_{(i)})$$

Let x in R be a zero mod t^ν of F. If

$$D(x) \equiv 0 \pmod{t^\mu}$$

our inductive hypothesis gives us y in R such that y is a singular point of V and

$$y \equiv x \pmod{t^{[\mu/c']-s'}}$$

If for some (i)
$$G_{(i)}(x) \equiv 0 \pmod{t^\mu}$$

then again by induction there is y in R which is a point of $V \cap V^+_{(i)}$ such that

$$y \equiv x \pmod{t^{[\mu/c_{(i)}]-s_{(i)}}}$$

Otherwise we use Newton's Lemma to find y in R which is a point of V such that

$$y \equiv x \quad \text{mod } t^\mu)$$

Thus as integers for F we can take

$$N = 2 + 2\max(N', \text{all } N_{(i)})$$
$$c = 2\max(c', \text{all } c_{(i)})$$
$$s = 1 + \max(s', \text{all } s_{(i)})$$

Case 2. — V *is inseparable over* K.

In this case we need two facts.

Fact 1. — *If* K′ *is a finite extension of* K, *then the integral closure* R′ *of* R *in* K′ *is a finite* R-*module.*

This follows from our assumption K^* separable over K (**7**; O_{IV}, 23.1.7 (ii)]. For the convenience of the reader, we sketch the proof, valid also when R is a higher dimensional local domain: $K' \otimes_K K^*$ is a finite extension field of K^*, because of our assumption. $R' \otimes_R R^*$ is a subring of this field, integral over the complete local domain R^*, hence finite over R^*. Since R^* is faithfully flat over R, R′ is a finite R-module. (The assumption that R^* is a domain, implicit in this argument, can be eliminated *(loc. cit.)*).

Fact 2. — *There is a functor* $\mathcal{F}$ *from the category of affine schemes of finite type over* R′ *to affine schemes of finite type over* R *such that* $\mathcal{F}$ *is right adjoint to the change of base functor from* R *to* R′. *Thus we have an isomorphism of bifunctors*

$$\mathrm{Mor}_R(Y, \mathcal{F}Z) \xrightarrow{\sim} \mathrm{Mor}_{R'}(Y_{R'}, Z)$$

(for Y/R, Z/R′). *Moreover,* $\mathcal{F}$ *preserves closed immersions.*

This follows from Fact 1, and can also be established in greater generality (see [**8**; p. 195-13] where the notation $\mathcal{F}Z = \pi_{R'/R}Z$ is used).

Choose a basis $b_1, \ldots, b_d$ for the R-module R′. Every element of R′ has uniquely determined coordinates in R with respect to this basis, and the addition and multiplication in R′ are given by polynomial functions in these coordinates. Hence there is a commutative ring scheme S over R, whose underlying scheme is affine d-space over R, such that for any R-algebra A,

$$\mathrm{Mor}_R(\mathrm{Spec}\ A, S) = A \otimes_R R'$$

Now the same arguments as in [**9**; pp. 638-9] can be repeated word for word. The point is that by using the basis $b_1, \ldots, b_d$, if P is a polynomial in n variables with coefficients in R′, the problem of finding a zero of P in $A \otimes_R R'$ is replaced by the problem of finding a common zero in A of d polynomials in nd variables with coefficients in R.

Let Y be the affine scheme over R defined by the polynomial system F ($Y = \operatorname{Spec} R[X]/FR[X]$). Since the scheme Y_K over K obtained from Y by change of base is inseparable over K, there is a purely inseparable finite extension K′ of K such that the scheme $Y_{K'}$ is not reduced, *a fortiori* $Y_{R'}$ is not reduced [**5**; 4.6.3].

Consider the affine scheme $\mathscr{F}Y_{R'}$ over R. There is a canonical R-morphism $\theta : Y \rightarrow \mathscr{F}Y_{R'}$ which corresponds by adjointness to the identity morphism of $Y_{R'}$. Now $\mathscr{F}((Y_{R'})_{\mathrm{red}})$ is a closed subscheme of $\mathscr{F}Y_{R'}$; let W be its pre-image under θ. Then W is a proper closed subcheme of Y, otherwise the identity morphism of $Y_{R'}$ would factor through $(Y_{R'})_{\mathrm{red}}$, i.e., $Y_{R'}$ would be reduced, contradicting the choice of R′. By inductive assumption, there are integers N′, c', s' for W.

Suppose y is a point of Y in R/t^{ν}. Let e be the ramification index of the discrete valuation ring R′ over R, u a generator of its maximal ideal. Then y induces a point of $Y_{R'}$ in $R'/u^{e\nu}$. By a previous argument, there is an integer q (independent of y) such that the image of this point mod $u^{[e\nu/q]}$ is actually a point of $(Y_{R'})_{\mathrm{red}}$. By adjointness, the image of y mod $t^{[\nu/q]}$ is actually a point of W. Hence $N = qN'$, $c = qc'$, $s = s'$ are integers for F.

Remark. — Theorem 1 is false without the separability assumption. For there exists a discrete valuation ring R whose completion R^* is a purely inseparable integral extension of R [**6**; o. 207]. R must therefore be its own Henselization. The minimal polynomial of an element of R^* not in R gives a counter-example to Corollary 2.

2. Applications to C_i questions.

Recall that a domain R is called C_i if any form with coefficients in R of degree d in n variables with $n > d^i$ has a non-trivial zero in R. C_0 means that the field of fractions of R is algebraically closed.

Theorem 2. — *If k is a C_i field, then the field $k((t))$ of formal power series in one variable t over k is C_{i+1}.*

This generalizes some results of Lang [**3**], who did the cases $i = 1$, k finite, and $i = 0$. Note that $[k : k^p] \leq p^i$ (take a basis).

It suffices to prove that $R = k[[t]]$ is C_{i+1}. By Lang [**3**], $k[t]$ is C_{i+1}. Hence the hypersurface H in projective $(n-1)$-space defined by the given form has a point in the ring R/t^{ν} for all ν. By Corollary 2, H has a point in R.

Note 1. — The same type of argument yields a short proof of Lang's theorem that if R is a Henselian discrete valuation ring with algebraically closed residue field, such that K^* is separable over K, then R is C_1. For by Corollary 2, we may assume R complete, and since C_1 is inherited by finite extensions, we may also assume R unramified. Then the argument given in [**3**; p. 384] shows H has a point in R/t^{ν} for all ν.

Note 2. — In the definition of C_i, replace the word "form" by "polynomial without constant term"; a ring with this property is called *strongly* C_i. For example, finite fields are strongly C_1. A theorem of Lang-Nagata states that an algebraic function field in one variable over a strongly C_i field is strongly C_{i+1}. It is natural to ask whether the same statement holds for the power series field in one variable. Ax-Kochen confirm this in characteristic 0 by showing that the Henselization of $k[t]$ at the origin is elementarily equivalent to $k[[t]]$.

Note 3. — In the definition of strongly C_i, suppose we take the expression "non-trivial" to mean "some coordinate is a unit in R", instead of "some coordinate is non-zero". Call this property strongly C_i^*. If R is a strongly C_i^* discrete valuation ring, then the completion of R is also strongly C_i^*, by Theorem 1. It is therefore natural to ask: If a field k is strongly C_i, is the localization of $k[t]$ at the origin strongly C_{i+1}^*?

3. Newton's Lemma.

In this section, R will be an analytically irreducible Henselian local domain with maximal ideal $\mathfrak{m}$, F will be a system of r polynomials in n variables with coefficients in R, $1 \leq r \leq n$, J the Jacobian matrix of this system.

Lemma 1. — *Assume* $r = n$. *Given* x *in* R *such that*

$$F(x) \equiv 0 \pmod{\mathfrak{m}}$$
$$\det J(x) \not\equiv 0 \pmod{\mathfrak{m}}$$

Then there is y *in* R *such that*

(i) $$y \equiv x \pmod{\mathfrak{m}}$$
(ii) $$F(y) = 0$$

Proof. — There is y in the completion R^* satisfying (i) and (ii), by [**2**; 11.13.3]. Since $r = n$ and $\det J(y) \neq 0$, the domain $R[y]$ is separably algebraic over R. But R is separably algebraically closed in R^*, hence y is in R.

Lemma 2. — *Let* x *in* R *be such that*

$$F(x) \equiv 0 \pmod{e^2\mathfrak{m}}$$

where $e = D(x)$, D *being a subdeterminant of order* r *of* $\det J$. *Then there is* y *in* R *such that*

$$y \equiv x \pmod{e\mathfrak{m}}$$
$$F(y) = 0$$

Proof. — We may assume $e \neq 0$. We may assume $x = 0$ and that D is the subdeterminant obtained from the first r variables. If $r < n$, setting

$$F_j(X) = X_j \qquad j = r+1, \ldots, n$$

shows we can assume $r = n$, hence $D = \det J$. Let J' be the adjoint matrix to J, so that $JJ' = DI = J'J$, with I the identity matrix. By Taylor's formula,

$$F(eX) = F(0) + eJ(0)X + e^2G(X)$$

where G(X) is a vector of polynomials each beginning with terms of degree at least 2. Using

$$e = \mathrm{J}(0)\mathrm{J}'(0)$$

and the hypothesis on F(0), we can factor out $e\mathrm{J}(0)$:

$$\mathrm{F}(e\mathrm{X}) = e\mathrm{J}(0)\mathrm{H}(\mathrm{X})$$

where H is a system whose Jacobian matrix at 0 is I, and

$$\mathrm{H}(0) \equiv 0 \pmod{\mathfrak{m}}$$

By lemma 1, there is y' in $\mathfrak{m}$ such that $\mathrm{H}(y') = 0$, whence $y = ey'$ does the trick.

Note. — The following argument (due to M. Artin) should eliminate the assumption that R is analytically irreducible, used in the proof of Lemma 1: Let $\mathrm{Y} = \mathrm{Spec}\ \mathrm{R}[\mathrm{X}]/\mathrm{FR}[\mathrm{X}]$, $f : \mathrm{Y} \to \mathrm{Spec}\ \mathrm{R}$ the canonical morphism. The hypothesis of Lemma 1 gives us a point $\overline{x}$ of Y lying over the closed point of Spec R, such that $\overline{x}$ is isolated in its fibre and f is smooth at $\overline{x}$. Hence the local ring $\mathfrak{o}$ of x on Y is étale over R [5; 11, 1.4] with the same residue field. Since R is Henselian, $\mathrm{R} \to \mathfrak{o}$ is an isomorphism [1], hence we have a section $\mathrm{Spec}\ \mathrm{R} \to \mathrm{Y}$ passing through $\overline{x}$.

4. Acknowledgements.

The argument in Case 1 has been developed from ideas of P. Cohen and A. Néron. My original argument in Case 2 required the extra assumption $[k : k^p] < \infty$; the present argument is essentially due to M. Raynaud. Newton's lemma for Henselian local rings was suggested by M. Artin.

BIBLIOGRAPHY

[1] M. Artin, *Grothendieck Topologies*, pp. 86-91, Harvard Notes, 1962.
[2] A. Grothendieck, *Séminaire Géométrie algébrique*, 1960, I.H.E.S., Paris.
[3] S. Lang, On Quasi-Algebraic Closure, *Annals of Math.*, vol. 55, 1952, 373-390.
[4] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. I.H.E.S., n° 21, Paris, 1964.
[5] A. Grothendieck et J. Dieudonné, *Éléments de géométrie algébrique*, IV (2e partie), Publ. I.H.E.S., n° 24, Paris, 1965.
[6] M. Nagata, *Local Rings*, Interscience, 1962.
[7] A. Grothendieck et J. Dieudonné, *Éléments de géométrie algébrique*, IV (première partie), Publ. I.H.E.S., n° 20, Paris, 1964.
[8] A. Grothendieck, *Technique de descente*, II, Séminaire Bourbaki, 1959-60, exposé 195.
[9] M. Greenberg, Schemata Over Local Rings, *Annals of Math.*, vol. 73, 1961, 624-648.

Northeastern University, Boston, Mass.

Manuscrit reçu le 24 avril 1966.

1967. — Imprimerie des Presses Universitaires de France. — Vendôme (France)
ÉDIT. N° 29 469 IMPRIMÉ EN FRANCE IMP. N° 19 965