Greenberg's Theorem

Let (R, m, k) be a Henselian DVR, t a generator of m.

$\hat{R}$ = completion of R

K = $\mathrm{Quot}(R)$ field of fractions of R

$\hat{K}$ = $\mathrm{Quot}(\hat{R})$

Let $F = (F_1, \dots, F_r) \subset R[X_1, \dots, X_n]$ be polynomials and

$$I_F := \langle F_1, \dots, F_r \rangle \subset R[X_1, \dots, X_n] =: R[X]$$

the ideal generated by F.

THEOREM (Greenberg, 1966)

Assume that $[\mathrm{char}(K) = p > 0 \implies \hat{K}/K \text{ is separable}]$.

Then there is a Greenberg triple (N, C, S) with $N \geq 1$, $C \geq 1$, $S \geq 0$ of integers, s.t. for $\nu \geq N$ and $x \in R$ with $F(x) \equiv 0 \mod t^\nu$ there is a lift $y \in R$ satisfying $F(y) = 0$ and "lying above x" in the sense that $y \equiv x \mod t^{[\frac{\nu}{C}] - S}$.

Structure of the proof:

- proof by induction on $\dim V$ of

$$V = V(F) = \{x \in \mathbb{A}^n_K \mid F(x) = 0\}$$

- reduce to the case where $K(V)$ is well-defined, i.e. where V is integral (irreducible and reduced)

- case distinction: V/K separable or not.

case separable: Construct smaller subvarieties and use induction.

Outside of these, the key lemma of Newton will help.

case inseparable "identify" V with some unreduced scheme.

Then on the reduced part we can use induction

and outside we will use the same argument as in the reduction to the reduced case.

proof Let

$$V := V(I) = \{x \in \mathbb{A}^n_K \mid F(x) = 0\} \subset \mathbb{A}^n_K$$

be the affine variety of the ideal I inside $\mathbb{A}^n_K$. Let

$$m := \dim V = \dim T_p V = \dim\left(\ker \mathcal{J}_F(p)\right)$$

the dimension of V, where p is a regular point and

$$\mathcal{J}_F = \left(\frac{\partial F_i}{\partial X_j}\right)_{i,j}$$

is the Jacobian matrix of F.

We prove the thm by induction on m

$\underline{m = -1}$ [or $-\infty$]: This means

$$K[V] := K[X_1, \dots, X_n]/_I = 0,$$

i.e. I contains a unit (= non zero constant). Then a x as in the theorem cannot exist.

Thus $m > 0$

We now assume two further properties:

① We may assume that $Y_R := \operatorname{spec}(R[X]/I)$ is reduced, i.e.

$$I = \sqrt{I} := \sqrt{\{x \in R \mid x^t \in I \text{ for some } t \in \mathbb{N}\}}$$

proof Let

$$\sqrt{I} = \langle E \rangle = \langle E_1, \dots, E_f \rangle \qquad (R[X] \text{ noetherian!})$$

By definition $E^q \subset I$ for some q where

$$E^q := \{\text{system of the } f^q \text{ product of } E_1, \dots, E_f\}$$

Let (N', c', s') be a Greenberg-triple for E, i.e.

for all $x \in R$, $\nu \geq N'$

$$F(x) \equiv 0 \quad (m^\nu) \Longrightarrow \exists y \in R: F(y) = 0 \text{ and } y \equiv x \quad (m^{[\frac{\nu}{c}]-s}).$$

Since

$$F(x) \equiv 0 \quad (m^q) \Longrightarrow E(x) \equiv 0 \quad (m^{[\frac{q}{q}]})$$

for any a, we conclude that

$$(qN', qc', s') =: (N, c, s)$$

is a triple for F.

② We may assume that V is K-irreducible.

Proof Assume $V = W \cup W'$ with irreducible components W, W'. Let G, G' be the ideals for W, W' and $(N, c, s), (N', c', s')$ the Greenberg triples.

We have

$$F(x) \equiv 0 \quad (m^v)$$

$$\Downarrow$$

$$G(x) \equiv 0 \quad \text{or} \quad G'(x) \equiv 0 \qquad (m^{[\frac{v}{2}]})$$

since $GG' \subset I$. Hence

$$\left(2\max(N, N'),\ 2\max(c, c'),\ \max(s, s')\right)$$

is a triple for F.

Thus: Assume Y_R is reduced, V is K-irreducible, $\dim V > 0$.

2 cases: ($\Leftrightarrow$ integral! $\Rightarrow$ quotient is well-defined)

1) V is separable over K This means that L/K with

$$L = \mathrm{Quot}\left(K[X_1, \dots, X_n] / \underline{I} \right)$$

is separable, i.p. all F_i are separable.

By induction, we already have triples for the following smaller varieties:

- $W \subset V$ given by (D, F) where D is the system of order-n-m minors of $\mathcal{J}$.

  Since V is separable, $W \subsetneq V$ and by induction there is a Greenberg triple (N', c', s').

- For $(i) \subset \{1, \dots, r\}$ of order $n-m$, $F_{(i)} \subset \{F_1, \dots, F_r\}$ let

$$V_{(i)} = \left\{ x \in \mathbb{A}_K^n \mid F_{(i)}(x) = 0 \right\}$$

$$V_{(i)}^+ = \bigcup_{\substack{C \text{ } K\text{-irred. comp. of } V_{(i)} \\ \text{of dim. } m}} C$$

$G_{(i)}$ = system of polynomials for $V_{(i)}^+$.

By induction there are triples $(N_{(i)}, c_{(i)}, s_{(i)})$ for all $W_{(i)} \subsetneq V$ for the system $(G_{(i)}, F)$.

Now: Construct a triple for F

Let $x \in R$ s.t. $F(x) \equiv 0 \mod m^{\nu}$

1 If x is a point in W, i.e. $D(x) \equiv 0 \mod m^{\nu}$

we get $y \in R$ with $(D, F)(y) = 0$ and $y \equiv x \mod m^{[\frac{\nu}{c}] - s'}$

for $\nu \geq N'$

2 Repeat the argument if $G_{(i)}(x) \equiv 0 \mod m^{\nu}$ for some (i) and get $y \in R$ with $(G_{(i)}, F)(y) = 0$ and $x \equiv y \mod m^{[\frac{\nu}{c_{(i)}}] - s_{(i)}}$.

3 For the remaining case we have a non-vanishing minor $D_{(i),(j)}(x) \not\equiv 0$ and $[G_{(i)}(x) \not\equiv 0$ for all $(i)]$

NEWTON'S LEMMA

Let $x \in R$, R analytically irred. Henselian local, s.t.

$$F(x) \equiv 0 \mod e^2 m$$

where

$e = D(x)$

$D = r \times r$ subdet. of $\mathfrak{J}$. $(r \leq n)$

$\Rightarrow$ There is $y \in R$ s.t.

$y \equiv x \pmod{em}$, $F(y) = 0$

$\longrightarrow$

Let $x \in R$ s.t.

$F_{(i)}(x) \equiv 0 \quad (t^{2\mu+1})$ (b)

$D_{(i),(j)}(x) \not\equiv 0 \quad (t^{\mu})$ (a)

for some (j) [(i) is fixed].

Then there is $y \in R$ s.t.

$F_{(i)}(y) = 0$

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

We apply Newton's lemma as follows:

$$D_{(i),(j)}(x) \not\equiv 0 \quad (t^\mu) \quad \Rightarrow \quad D_{(i),(j)}(x) = r \cdot t^L \quad \text{for some } r \in R^\times, \; \mu < l$$

Now let

$$F = \left(t^{\mu-l-1} \cdot F_{(i),1}, F_{(i),2}, \ldots, F_{(i),n-m} \right)$$

$$e = \det \left(\frac{\partial F_i}{\partial X_j} \right)_{(i),(j)}(x) = t^{(\mu-l-1)} D_{(i),(j)}(x) = r \cdot t^{\mu-1}$$

We have

$$F(x) = t^{\mu-l-1} F_{(i)}(x) = t^{\mu-l-1} \cdot \left[s \cdot t^{2\mu+1} \right]$$

$$= r^2 t^{2\mu} \cdot t \cdot \left[t^{\mu-l-1} \cdot s \cdot (r^{-1})^2 \right]$$

$$\equiv 0 \quad (e^2 t),$$

i.e. we find $y \in R$ s.t.

$$F(y) = 0, \qquad y \equiv x \quad (et) = (rt^\mu) \subset (t^\mu).$$

FACT Since $D_{(i),(j)}(y) \not\equiv 0$, the tangent hyperplanes of $F_{i,1}, \ldots, F_{i,n-m}$ at y are transversal and y is regular in a component of $V_{(i)}$ of dim. m.

$$G_{(i)}(y) \not\equiv 0 \quad \Rightarrow \quad y \notin V_{(i)}^+. \qquad \text{But } \{\text{m-dim. comp of } V_{(i)}\} = V_{(i)}^+ \cup V,$$

$$\Rightarrow \quad y \in V$$

$$\Leftrightarrow \quad F(y) = 0.$$

Holds for

$$\mu \geq \max(N, \text{all } N_{(i)}) \qquad (a)$$

$$\nu \geq 2\mu + 1 \qquad (b)$$

since

$$\left[\frac{2 + \max(N', \text{all } N_{(i)})}{2\max(c', \text{all } c_{(i)})}\right] - \left(1 + \max(s', s_{(i)})\right)$$

$$= \frac{\max(N', \text{all } N_{(i)})}{\max(c', \text{all } c_{(i)})} - \max(s', s_{(i)})$$

this allows us the triple

keep the exponent small

we choose

$$N = 2 + 2\max(N', \text{all } N_{(i)})$$

$$c = 2\max(c', \text{all } c_{(i)})$$

$$s = 1 + \max(s', \text{all } s_{(i)})$$

2) V is inseparable over K

We need facts:

F1 If K'/K is finite, the integral closure $K' \supset R' \supset R$ of R is a finite R-module

↓

F2 There is a functor

$$\mathcal{F}: \underline{\text{Aff-Sch}}^{R'}_{<\infty} \longrightarrow \underline{\text{Aff-Sch}}^{R}_{<\infty}$$

which is right adjoint to the base-change $R \to R'$ - functor.

In particular

$$\text{Hom}_R(Y, \mathcal{F}(Z)) \cong \text{Hom}_{R'}(Y_{R'}, Z)$$

for affines Z/R', Y/R where $Y_{R'} = Y \otimes_R R'$.

F3 Let $Y = \text{spec}\left(R[X]/I\right)$. Then the following are equivalent (see EGA IV 2^{nde} 4.6.1, 4.6.3):

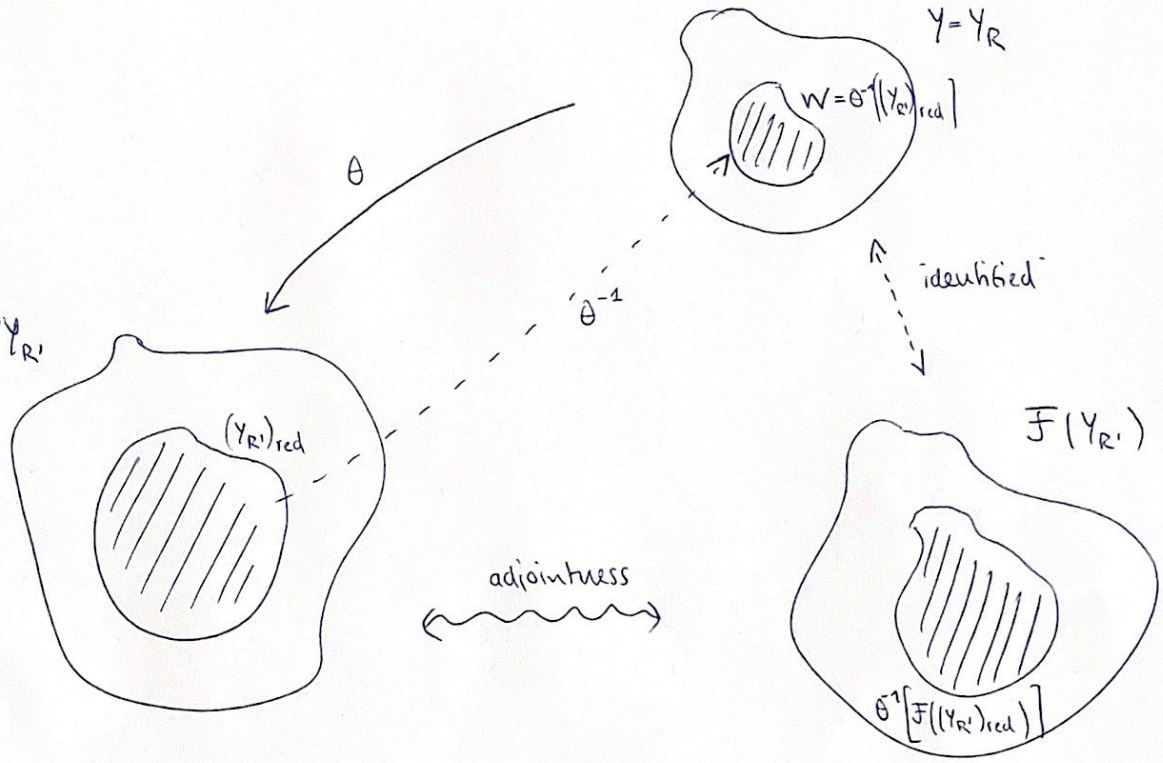
(i) Y_K is separable

(ii) For every finite purely insep. K'/K $Y_{K'}$ is reduced.

Now by **F3**, there is some finite, purely insep. K'/K s.t. $Y_{K'}$ is not reduced. Certainly $Y_{R'}$ is not reduced then, i.e.

$$(Y_{R'})_{red} \subsetneq Y_{R'}.$$

Idea:



θ is given by the obvious composition

$$Y \xrightarrow{\text{base change}} Y_{R'} \longrightarrow \mathcal{F}(Y_{R'})$$

$$Y \xrightarrow{\theta} \mathcal{F}(Y_{R'})$$

and by adjointness $\theta \longleftrightarrow \mathrm{id}_{Y_{R'}}$. Define

$$W := \theta^{-1}\left[\mathcal{F}((Y_{R'})_{red})\right] \subset Y$$

Then W is proper closed in Y (otherwise $Y_{R'}$ would be reduced, $\lightning$)

By induction there is a triple (N', c', s') for W.

Now let $x \in R$ s.t. $F(x) \equiv 0 \quad (t^v)$

R' is a DVR and let

u = generator of maximal ideal $m' \triangleleft R'$

e = "ramification index", defined as $t = \varepsilon \cdot u^e, \quad \varepsilon \in R^\times$

If $F' = F \otimes_R R'$ is the system for $Y_{R'}$,

$$F'(x) \equiv 0 \qquad (u^{ev})$$

If $\sqrt{F'}$ is the system for $(Y_{R'})_{red} \subsetneq Y_{R'}$. We have seen before that there is $q \geq 0$ s.t.

$$\sqrt{F'}(x) \equiv 0 \qquad \left(u^{\left[\frac{ev}{q}\right]}\right)$$

Let now F'' be a system for W, for which we have a triple (N', c', s') by induction. By adjointness

$$F''(x) \equiv 0 \qquad \left(t^{\left[\frac{v}{q}\right]}\right),$$

i.e. $N = qN'$ gives us for $v \geq N$ a $y \in R$ satisfying

$$y \equiv x \quad \left(t^{\left[\frac{\left[\frac{v}{q}\right]}{c'} - s'\right]}\right), \qquad F''(y) = 0 \quad (\Rightarrow F(y) = 0)$$

so choose $N = qN', \quad c = qc', \quad s = s'$ to have

$$y \equiv x \quad \left(t^{\left[\frac{v}{c}\right] - s}\right)$$

Newton's lemma

R analytically irreducible, Henselian, local domain

m = maximal ideal

$F = (F_1, \dots, F_r) \subset R[X_1, \dots, X_n]$, $r \leq n$

$\mathcal{J} = \left(\frac{\partial F_i}{\partial X_j}\right)_{i,j}$

Lemma If $r = n$: If $x \in R$ with

$$F(x) \equiv 0 \quad (m), \qquad \det \mathcal{J}(x) \not\equiv 0 \quad (m)$$

there is $y \in R$ with

$$F(y) = 0 \qquad x \equiv y \quad (m)$$

NEWTON-LEMMA Let $x \in R$ s.t.

$$F(x) \equiv 0 \qquad (e^2 m)$$

where $e = D(x)$, D = subdeterminant of order r of $\mathcal{J}$.

Then there is $y \in R$ with

$$y \equiv x \quad (em), \qquad F(y) = 0$$

proof Assume

- $e \neq 0$. Otherwise $y = x$.
- $X = 0$. If $F(x) \equiv 0 \pmod{e^2 m}$ then $F'(0) \equiv 0$ for $F'(X) = F(X + x)$, where $\partial_{F'} = \partial_F$. The lemma gives us $y' \in R$ s.t.

$$y' \equiv 0 \pmod{em}, \qquad F'(y') = 0,$$

i.e. for $y = y' + x$ we have

$$y \equiv x \pmod{em}, \qquad F(y) = F(y' + x) = F'(y') = 0$$

- we may assume that D is the subdet. of the first r variables: if D' is an arbitrary subdeterminant, $e' = D'(x)$ we simply change variables

$$(X_{i_1}, \dots, X_{i_r}) \longleftrightarrow (X_{i'_1}, \dots, X_{i'_r})$$

where

$$D = \det\left(\frac{\partial F_i}{\partial X_{i_j}}\right), \qquad D' = \det\left(\frac{\partial F_i}{\partial X_{i'_j}}\right)$$

- we may assume $r = n$. If $r < n$, we "fill up" with polynomials

$$\overline{F}_j = X_j, \qquad r+1 \leq j \leq n$$

Then no extra condition applies for $F(x) \equiv 0$

Then let $\mathcal{J}'$ be the adjoint matrix of $\mathcal{J}$, i.e.

$$\mathcal{J}\mathcal{J}' = \begin{pmatrix} D & & 0 \\ & \ddots & \\ 0 & & D \end{pmatrix} = \mathcal{J}'\mathcal{J}$$

Now use Taylor's formula (at $x_0 = 0$)

$$F(eX) = \sum_{\ell=0}^{\infty} \frac{F^{(\ell)}(0)}{\ell!} (eX)^{\ell}$$

$$= F(0) + e\,\mathcal{J}(0)X + e^2 G(X)$$

for some system of $r=n$ polynomials G, each with no terms of degree $0, 1$. Put

$$e = \mathcal{J}(0)\,\mathcal{J}'(0) = \begin{pmatrix} e & & 0 \\ & \ddots & \\ 0 & & e \end{pmatrix}$$

By assumption

$$F(0) \equiv 0 \quad (e^2 m), \quad \rightsquigarrow \quad F(0) = r e^2 t \quad (r \in R^{\text{for some}})$$

i.e.

$$F(eX) = r e^2 t + \mathcal{J}(0)\,\mathcal{J}'(0)\,\mathcal{J}(0)X + \mathcal{J}(0)\,\mathcal{J}'(0)\,\mathcal{J}(0)\,\mathcal{J}'(0)\,G(X)$$

$$= r e\,\mathcal{J}(0)\,\mathcal{J}'(0)\,t + e\mathcal{J}(0)X + e\mathcal{J}(0)\mathcal{J}'(0)G(X)$$

$$= e\,\mathcal{J}(0)\left[\underbrace{r\,\mathcal{J}'(0)\,t}_{\text{degree } 0} + X + \underbrace{\mathcal{J}'(0)\,G(X)}_{\text{degree } \geq 2}\right]$$

$$=: e\,\mathcal{J}(0)\,H(X)$$

H is a system of polynomials with Jacobian

$$\partial_H\big|_0 = I_n,$$

hence $\det \partial_H(0) \not\equiv 0 \pmod{m}$ and

$$H(0) = r\, \partial'(0)\, t \equiv 0 \pmod{m}.$$

By the preceding lemma there is $y' \in R$ s.t.

$$y' \equiv 0 \ (m), \qquad H(y') = 0,$$

$$\Leftrightarrow y' \in m$$

i.e.

$$0 = e \cdot \partial(0) \cdot H(y') \overset{\text{Taylor}}{=} F(ey') =: F(y),$$

so y satisfies $F(y) = 0$ and

$$y - ey' \in em \iff y \equiv 0 = x \ (em).$$

□