Lecture 3: A Result on $\mathbb{F}_q((t))$

GRK 2240 Workshop: C_i-FIELDS

November 12th, 2020

Speaker: Jakob Bergqvist

The Goal

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

The Goal

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Tactic:

1. Reduce the problem to considering $k[[t]]$;
2. Appeal to a result about discrete valuation rings to reduce to $k(t)$.

Definition

Let k be a field and let $(\Gamma, +, \geq)$ be a totally ordered abelian group. A **valuation** on k is a function $v\colon k^\times \to \Gamma$ such that

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

Definition

Let k be a field and let $(\Gamma, +, \geq)$ be a totally ordered abelian group. A **valuation** on k is a function $v\colon k^\times \to \Gamma$ such that

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x+y) \geq \min\{v(x), v(y)\}$.

The image $v(k^\times)$ is called the **value group**, the pair (k, v) is called a **valued field**, and the set $R = \{x \in k^\times \mid v(x) \geq 0\} \cup \{0\}$ is a ring called the **valuation ring** of v.

Definition

Let k be a field and let $(\Gamma, +, \geq)$ be a totally ordered abelian group. A **valuation** on k is a function $v\colon k^\times \to \Gamma$ such that

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

The image $v(k^\times)$ is called the **value group**, the pair (k, v) is called a **valued field**, and the set $R = \{x \in k^\times \mid v(x) \geq 0\} \cup \{0\}$ is a ring called the **valuation ring** of v.

v is sometimes extended to $0 \in k$ by adjoining an element ∞ to Γ.

General facts:

- The ring R is local (i.e. has unique maximal ideal) integral domain, with $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$. Every element not in $\mathfrak{m}$ is a unit in R (general fact of local rings). The field $R/\mathfrak{m}$ is called the **residue field** of v,R and/or (k, v).

General facts:

- The ring R is local (i.e. has unique maximal ideal) integral domain, with $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$. Every element not in $\mathfrak{m}$ is a unit in R (general fact of local rings). The field $R/\mathfrak{m}$ is called the **residue field** of v,R and/or (k, v).
- The ambient field may be recovered as $k = \text{Frac}(R)$.

General facts:

- The ring R is local (i.e. has unique maximal ideal) integral domain, with $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$. Every element not in $\mathfrak{m}$ is a unit in R (general fact of local rings). The field $R/\mathfrak{m}$ is called the **residue field** of v,R and/or (k, v).
- The ambient field may be recovered as $k = \mathrm{Frac}(R)$.
- For any $x \in k$ we have $x \in R$ or $x^{-1} \in R$ (equivalent way of defining valuation rings).

General facts:

- The ring R is local (i.e. has unique maximal ideal) integral domain, with $\mathfrak{m} = \{x \in R \mid v(x) > 0\}$. Every element not in $\mathfrak{m}$ is a unit in R (general fact of local rings). The field $R/\mathfrak{m}$ is called the **residue field** of v,R and/or (k, v).
- The ambient field may be recovered as $k = \mathrm{Frac}(R)$.
- For any $x \in k$ we have $x \in R$ or $x^{-1} \in R$ (equivalent way of defining valuation rings).
- For $x, y \in R$ we have $(x) = (y)$ if and only if $v(x) = v(y)$.

Definition

A **discrete valuation** is a valuation with value group isomorphic to $(\mathbb{Z}, +)$. A **discrete valuation ring** (DVR) is an integral domain R such that there is a discrete valuation on Frac(R) for which R is the valuation ring.

Definition

A **discrete valuation** is a valuation with value group isomorphic to $(\mathbb{Z}, +)$. A **discrete valuation ring** (DVR) is an integral domain R such that there is a discrete valuation on $\mathrm{Frac}(R)$ for which R is the valuation ring.

Keep in mind the following intrinsic definition, which does not require an ambient field:

Definition

A **discrete valuation ring** (DVR) is an integral domain R, together with a surjective function $v\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that

(i) $v(xy) = v(x) + v(y)$;

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$;

(iii) $v(x) = 0$ if and only if x is a unit in R, i.e. x has an inverse $x^{-1} \in R$.

Examples of DVRs

- $v_p \colon \mathbb{Q}^\times \to \mathbb{Z}$ the p-adic valuation $v_p(x) = a$, where $x = p^a \frac{\alpha}{\beta}$ with α, β relatively prime to p. The valuation ring is $\mathbb{Z}_{(p)}$.

Examples of DVRs

- $v_p\colon \mathbb{Q}^\times \to \mathbb{Z}$ the p-adic valuation $v_p(x) = a$, where $x = p^a \frac{\alpha}{\beta}$ with α, β relatively prime to p. The valuation ring is $\mathbb{Z}_{(p)}$.
- Fix irreducible $f \in k[t]$. Define $v_f\colon k(t)^\times \to \mathbb{Z}$ by $v_f(g) = a$ where $g = f^a \frac{\alpha}{\beta}$ with α and β not divisible by f. The valuation ring is $k[t]_{(f)}$.

Examples of DVRs

- $v_p \colon \mathbb{Q}^\times \to \mathbb{Z}$ the p-adic valuation $v_p(x) = a$, where $x = p^a \frac{\alpha}{\beta}$ with α, β relatively prime to p. The valuation ring is $\mathbb{Z}_{(p)}$.
- Fix irreducible $f \in k[t]$. Define $v_f \colon k(t)^\times \to \mathbb{Z}$ by $v_f(g) = a$ where $g = f^a \frac{\alpha}{\beta}$ with α and β not divisible by f. The valuation ring is $k[t]_{(f)}$.
- The p-adic integers $\mathbb{Z}_p$ with valuation $v_p \colon \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}$ mapping $a \in \mathbb{Z}_p$ to the index of the first non-zero coefficient in the p-adic expansion of a. The fraction field is $\mathbb{Q}_p$.

Examples of DVRs

- $v_p \colon \mathbb{Q}^\times \to \mathbb{Z}$ the p-adic valuation $v_p(x) = a$, where $x = p^a \frac{\alpha}{\beta}$ with α, β relatively prime to p. The valuation ring is $\mathbb{Z}_{(p)}$.
- Fix irreducible $f \in k[t]$. Define $v_f \colon k(t)^\times \to \mathbb{Z}$ by $v_f(g) = a$ where $g = f^a \frac{\alpha}{\beta}$ with α and β not divisible by f. The valuation ring is $k[t]_{(f)}$.
- The p-adic integers $\mathbb{Z}_p$ with valuation $v_p \colon \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}$ mapping $a \in \mathbb{Z}_p$ to the index of the first non-zero coefficient in the p-adic expansion of a. The fraction field is $\mathbb{Q}_p$.
- The field $k((t))$ of formal Laurent series, $\sum_{i=n}^{\infty} a_i t^i$, $n \in \mathbb{Z}$, equipped with valuation $v \colon k((t))^\times \to \mathbb{Z}$ given by $v(\sum_{i=n}^{\infty} a_i t^i) = m$ where m is minimal such that $a_m \neq 0$. The valuation ring is $k[[t]]$.

Equivalent definitions of DVR (there are many more):

(a) R is a local PID which is not a field.

(b) R is a local Dedekind domain which is not a field.

(c) R is regular, local integral domain of dimension 1.

(d) R is a UFD with a unique irreducible element (up to multiplication by units).

(e) R is a Noetherian, local integral domain and not a field, with principal maximal ideal.

Equivalent definitions of DVR (there are many more):

(a) R is a local PID which is not a field.

(b) R is a local Dedekind domain which is not a field.

(c) R is regular, local integral domain of dimension 1.

(d) R is a UFD with a unique irreducible element (up to multiplication by units).

(e) R is a Noetherian, local integral domain and not a field, with principal maximal ideal.

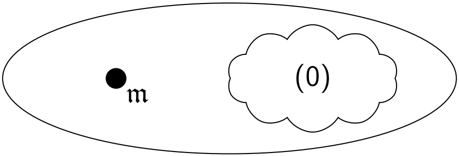

Figure: A DVR geometrically. It has a closed point $\mathfrak{m}$ and a 'fuzzy' open, dense point (0).

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal:

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal: By surjectivity of v there is an element $\pi \in R$ with $v(\pi) = 1$. Then $v(\pi^n) = n$. As $(x) = (y)$ iff $v(x) = v(y)$, the ideal (π) contains all element of valuation > 0. But these are all the non-units of R, i.e. $(\pi) = \mathfrak{m}$.

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal: By surjectivity of v there is an element $\pi \in R$ with $v(\pi) = 1$. Then $v(\pi^n) = n$. As $(x) = (y)$ iff $v(x) = v(y)$, the ideal (π) contains all element of valuation > 0. But these are all the non-units of R, i.e. $(\pi) = \mathfrak{m}$.

A generator of the maximal ideal of R is called a **uniformizing parameter**.

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal: By surjectivity of v there is an element $\pi \in R$ with $v(\pi) = 1$. Then $v(\pi^n) = n$. As $(x) = (y)$ iff $v(x) = v(y)$, the ideal (π) contains all element of valuation > 0. But these are all the non-units of R, i.e. $(\pi) = \mathfrak{m}$.

A generator of the maximal ideal of R is called a **uniformizing parameter**.
As anything not in (π) is a unit, any element of R may be expressed uniquely as $u\pi^n$ with $u \in R^\times$.

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal: By surjectivity of v there is an element $\pi \in R$ with $v(\pi) = 1$. Then $v(\pi^n) = n$. As $(x) = (y)$ iff $v(x) = v(y)$, the ideal (π) contains all element of valuation > 0. But these are all the non-units of R, i.e. $(\pi) = \mathfrak{m}$.

A generator of the maximal ideal of R is called a **uniformizing parameter**.
As anything not in (π) is a unit, any element of R may be expressed uniquely as $u\pi^n$ with $u \in R^\times$. The valuation may then be recovered as $v(u\pi^n) = n$.

The unique maximal ideal $\mathfrak{m}$ of a DVR R is principal: By surjectivity of v there is an element $\pi \in R$ with $v(\pi) = 1$. Then $v(\pi^n) = n$. As $(x) = (y)$ iff $v(x) = v(y)$, the ideal (π) contains all element of valuation > 0. But these are all the non-units of R, i.e. $(\pi) = \mathfrak{m}$.

A generator of the maximal ideal of R is called a **uniformizing parameter**.
As anything not in (π) is a unit, any element of R may be expressed uniquely as $u\pi^n$ with $u \in R^\times$. The valuation may then be recovered as $v(u\pi^n) = n$.

From now on R will always denote a DVR, and π will be its uniformizing parameter.

Definition

Let $R_n = R/(\pi^{n+1})$ and let $\varphi_n \colon R_n \to R_{n-1}$ be the quotient.

Definition

Let $R_n = R/(\pi^{n+1})$ and let $\varphi_n \colon R_n \to R_{n-1}$ be the quotient. A sequence $(\xi_0, \xi_1, \dots) \in \prod_{i=0}^{\infty} R_i$ is said to be **compatible** if $\varphi_n(\xi_n) = \xi_{n-1}$ for all n.

Definition

Let $R_n = R/(\pi^{n+1})$ and let $\varphi_n\colon R_n \to R_{n-1}$ be the quotient. A sequence $(\xi_0, \xi_1, \dots) \in \prod_{i=0}^{\infty} R_i$ is said to be **compatible** if $\varphi_n(\xi_n) = \xi_{n-1}$ for all n. The **completion** of R, denoted $\widehat{R}$, is the subring of $\prod_{i=0}^{\infty} R_i$ consisting of all compatible sequences.

Definition

Let $R_n = R/(\pi^{n+1})$ and let $\varphi_n \colon R_n \to R_{n-1}$ be the quotient. A sequence $(\xi_0, \xi_1, \dots) \in \prod_{i=0}^{\infty} R_i$ is said to be **compatible** if $\varphi_n(\xi_n) = \xi_{n-1}$ for all n. The **completion** of R, denoted $\widehat{R}$, is the subring of $\prod_{i=0}^{\infty} R_i$ consisting of all compatible sequences. Equivalently, the completion of R is the inverse limit

$$\widehat{R} := \varprojlim_{n} R_n.$$

Definition

Let $R_n = R/(\pi^{n+1})$ and let $\varphi_n \colon R_n \to R_{n-1}$ be the quotient. A sequence $(\xi_0, \xi_1, \dots) \in \prod_{i=0}^{\infty} R_i$ is said to be **compatible** if $\varphi_n(\xi_n) = \xi_{n-1}$ for all n. The **completion** of R, denoted $\widehat{R}$, is the subring of $\prod_{i=0}^{\infty} R_i$ consisting of all compatible sequences. Equivalently, the completion of R is the inverse limit

$$\widehat{R} := \varprojlim_{n} R_n.$$

Either definition gives embedding $R \hookrightarrow \widehat{R}$ mapping $x \in R$ to the element represented by the sequence $([x]_\pi, [x]_{\pi^2}, \dots)$. If $R \cong \widehat{R}$ via this embedding, R is said to be **complete**.

The completion $\widehat{R}$ of a DVR is in fact a complete DVR:

The completion $\widehat{R}$ of a DVR is in fact a complete DVR: The valuation on $\widehat{R}$ maps a compatible sequence $(\xi_0, \xi_1, \dots)$ to the least index n such that $\xi_n \neq 0$. To see that $\widehat{R}$ is complete, it is enough to note that by construction π becomes a unformizing parameter of $\widehat{R}$ and $\widehat{R}/(\pi^n) \cong R/(\pi^n)$.

Examples of complete DVRs

- The DVR $\mathbb{Z}_p$ is complete. It is the completion of $\mathbb{Z}_{(p)}$.

Examples of complete DVRs

- The DVR $\mathbb{Z}_p$ is complete. It is the completion of $\mathbb{Z}_{(p)}$. To prove this, note that $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} = \mathbb{Z}/p^n\mathbb{Z}$, and that mapping a powerseries in p, $a_0 + a_1 p \cdots + a_n p^n + \dots$ with $0 \leq a_i < p$ to the compatible series $(a_0, a_0 + a_1 p, \dots)$ is an isomorphism, so $\mathbb{Z}_p \cong \widehat{\mathbb{Z}_{(p)}}$.

Examples of complete DVRs

- The DVR $\mathbb{Z}_p$ is complete. It is the completion of $\mathbb{Z}_{(p)}$. To prove this, note that $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} = \mathbb{Z}/p^n\mathbb{Z}$, and that mapping a powerseries in p, $a_0 + a_1 p \cdots + a_n p^n + \dots$ with $0 \leq a_i < p$ to the compatible series $(a_0, a_0 + a_1 p, \dots)$ is an isomorphism, so $\mathbb{Z}_p \cong \widehat{\mathbb{Z}_{(p)}}$.
- The DVR $k[[t]]$ is complete. It is the completion of $k[t]_{(t)}$. The argument is symmetric to the one above

Let $k = R/\pi$, $R_n = R/(\pi^{n+1})$ and fix for each $\alpha \in k$ a representative $a \in R$. Then $b \in R_n$ may be uniquely expressed as a polynomial

$$b = a_0 + a_1\pi + \cdots + a_n\pi^n,$$

where $a_i \in R$ represents $\alpha_i \in k$.

Let $k = R/\pi$, $R_n = R/(\pi^{n+1})$ and fix for each $\alpha \in k$ a representative $a \in R$. Then $b \in R_n$ may be uniquely expressed as a polynomial

$$b = a_0 + a_1\pi + \cdots + a_n\pi^n,$$

where $a_i \in R$ represents $\alpha_i \in k$.
Algorithm: Set $\alpha_0 = [b]_\pi$. Then $b - a_0 = b_1\pi$ for some $b_1 \in R$. Then replace b by b_1, i.e. set $\alpha_1 = [b_1]_\pi$, and find $b_1 - a_1 = b_2\pi$ etc.

Let $k = R/\pi$, $R_n = R/(\pi^{n+1})$ and fix for each $\alpha \in k$ a representative $a \in R$. Then $b \in R_n$ may be uniquely expressed as a polynomial

$$b = a_0 + a_1\pi + \cdots + a_n\pi^n,$$

where $a_i \in R$ represents $\alpha_i \in k$.
Algorithm: Set $\alpha_0 = [b]_\pi$. Then $b - a_0 = b_1\pi$ for some $b_1 \in R$. Then replace b by b_1, i.e. set $\alpha_1 = [b_1]_\pi$, and find $b_1 - a_1 = b_2\pi$ etc.

With this expression, the quotient $R_n \to R_{n-1}$ is simply

$$a_0 + \cdots + a_n\pi^n \mapsto a_0 + \cdots + a_{n-1}\pi^{n-1}.$$

If the DVR R is complete, the previous may be extended to R, in the sense that each element $\xi \in R$ may be expressed **uniquely** as a power series in π, with coefficients in R/π.

If the DVR R is complete, the previous may be extended to R, in the sense that each element $\xi \in R$ may be expressed **uniquely** as a power series in π, with coefficients in R/π.

Argument: Indeed, if ξ is represented by the compatible sequence $(\xi_0, \xi_1 \dots)$, then each ξ_n may be expressed a polynomial in π with coefficients in k.

If the DVR R is complete, the previous may be extended to R, in the sense that each element $\xi \in R$ may be expressed **uniquely** as a power series in π, with coefficients in R/π.

Argument: Indeed, if ξ is represented by the compatible sequence $(\xi_0, \xi_1 \dots)$, then each ξ_n may be expressed a polynomial in π with coefficients in k. The fact that the sequence is compatible implies that if $\xi_n = a_0 + \cdots + a_n \pi^n$ then $\xi_{n-1} = a_0 + \cdots + a_{n-1} \pi^{n-1}$.

If the DVR R is complete, the previous may be extended to R, in the sense that each element $\xi \in R$ may be expressed **uniquely** as a power series in π, with coefficients in R/π.

Argument: Indeed, if ξ is represented by the compatible sequence $(\xi_0, \xi_1 \dots)$, then each ξ_n may be expressed a polynomial in π with coefficients in k. The fact that the sequence is compatible implies that if $\xi_n = a_0 + \cdots + a_n\pi^n$ then $\xi_{n-1} = a_0 + \cdots + a_{n-1}\pi^{n-1}$.

Then we express ξ as a power series where the π^n coefficient is the π^n coefficient of $\xi_n, \xi_{n+1}, \dots$.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term. Thus $\xi_n \notin \pi R_n$, hence ξ_n is a unit.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term. Thus $\xi_n \notin \pi R_n$, hence ξ_n is a unit.

$\Leftarrow$: Fun exercise. □

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term. Thus $\xi_n \notin \pi R_n$, hence ξ_n is a unit.

$\Leftarrow$: Fun exercise. $\square$

Slogan: A complete DVR looks like a power series ring, but it need not be!

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.
$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term. Thus $\xi_n \notin \pi R_n$, hence ξ_n is a unit.
$\Leftarrow$: Fun exercise. $\square$

Slogan: A complete DVR looks like a power series ring, but it need not be!
Example: In general, if $R = k[[t]]$, then k is the residue field of R.

Suppose R is complete. Then $x \in R$ is a unit if and only if the constant term of x is non-zero.

$\Rightarrow$: Suppose $\xi = (\xi_0, \xi_1, \dots) \in R$ with $\xi_0 \neq 0$. Each ξ_n is a polynomial in π over $R/\mathfrak{m}$, and as the sequence is compatible, with $\xi_0 \neq 0$, this polynomial expression has a non-zero constant term. Thus $\xi_n \notin \pi R_n$, hence ξ_n is a unit.

$\Leftarrow$: Fun exercise. □

Slogan: A complete DVR looks like a power series ring, but it need not be!

Example: In general, if $R = k[[t]]$, then k is the residue field of R. Now, the residue field of $\mathbb{Z}_p$ is $\mathbb{F}_p$, which has characteristic p. But $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, hence $\mathbb{Z}_p$ has characteristic 0. Thus $\mathbb{Z}_p \ncong \mathbb{F}_p[[t]]$.

Suppose $x = (x_1, \ldots, x_n) \in R^n$ is a common solution to homogeneous polynomials $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$. If atleast one x_i is a unit, i.e. $x_i \notin (\pi)$, we say x is **primitive**.

Suppose $x = (x_1, \dots, x_n) \in R^n$ is a common solution to homogeneous polynomials $f_1, \dots, f_r \in R[t_1, \dots, t_n]$. If atleast one x_i is a unit, i.e. $x_i \notin (\pi)$, we say x is **primitive**.
Assume x is a not necessarily primitive solution.

Suppose $x = (x_1, \ldots, x_n) \in R^n$ is a common solution to homogeneous polynomials $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$. If atleast one x_i is a unit, i.e. $x_i \notin (\pi)$, we say x is **primitive**.
Assume x is a not necessarily primitive solution. Then

$$f_j(\pi^{-\min\{v(x_i)\}}x) = \pi^{-\min\{v(x_i)\}}f_j(x) = 0,$$

and at least one coordinate of $\pi^{-\min\{v(x_i)\}}x$ is a unit, i.e. $\pi^{-\min\{v(x_i)\}}x$ is primitive

Suppose $x = (x_1, \ldots, x_n) \in R^n$ is a common solution to homogeneous polynomials $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$. If atleast one x_i is a unit, i.e. $x_i \notin (\pi)$, we say x is **primitive**.
Assume x is a not necessarily primitive solution. Then

$$f_j(\pi^{-\min\{v(x_i)\}}x) = \pi^{-\min\{v(x_i)\}} f_j(x) = 0,$$

and at least one coordinate of $\pi^{-\min\{v(x_i)\}}x$ is a unit, i.e. $\pi^{-\min\{v(x_i)\}}x$ is primitive
Conclusion: We need only consider primitive solutions.

Theorem (I)

Let R be a complete DVR with uniformizing parameter π and $R_m = R/\pi^{m+1}$ all finite. Let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ be homogenous.

Theorem (I)

Let R be a complete DVR with uniformizing parameter π and $R_m = R/\pi^{m+1}$ all finite. Let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ be homogenous. Then the $f_1, \ldots, f_r$ have a common primitive solution in R if and only if the system of congruences

$$f_i(x) \equiv 0 \pmod{\pi^{m+1}}, \quad i = 1, \ldots, r$$

has a primitive solution in R_m for all $m = 0, 1 \ldots.$

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.

Note that φ_m maps primitive solutions to primitive solutions.

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions. Indeed, a solution mod π^{m+1} is also a solution mod π^m.

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions. Indeed, a solution mod π^{m+1} is also a solution mod π^m. Furthermore, if $u \notin \pi R_m$, then $\varphi_m(u) \notin \pi R_{m-1}$.

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions. Indeed, a solution mod π^{m+1} is also a solution mod π^m.
Furthermore, if $u \notin \pi R_m$, then $\varphi_m(u) \notin \pi R_{m-1}$.
Now, let $S_{j,m} = \varphi_m \circ \cdots \circ \varphi_j(S_j) \subset S_m$ for $j > m$. Then

$$S_m \supseteq S_{m+1,m} \supseteq \cdots \supseteq S_{j,m} \supseteq \cdots .$$

As R_m is finite, all $S_{j,m}$ are finite (and by assumption non-empty).

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions.
Indeed, a solution mod π^{m+1} is also a solution mod π^m.
Furthermore, if $u \notin \pi R_m$, then $\varphi_m(u) \notin \pi R_{m-1}$.
Now, let $S_{j,m} = \varphi_m \circ \cdots \circ \varphi_j(S_j) \subset S_m$ for $j > m$. Then

$$S_m \supseteq S_{m+1,m} \supseteq \cdots \supseteq S_{j,m} \supseteq \cdots .$$

As R_m is finite, all $S_{j,m}$ are finite (and by assumption non-empty).
Thus the intersection T_m is non-empty.

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions. Indeed, a solution mod π^{m+1} is also a solution mod π^m. Furthermore, if $u \notin \pi R_m$, then $\varphi_m(u) \notin \pi R_{m-1}$.
Now, let $S_{j,m} = \varphi_m \circ \cdots \circ \varphi_j(S_j) \subset S_m$ for $j > m$. Then

$$S_m \supseteq S_{m+1,m} \supseteq \cdots \supseteq S_{j,m} \supseteq \cdots .$$

As R_m is finite, all $S_{j,m}$ are finite (and by assumption non-empty). Thus the intersection T_m is non-empty. In general $\varphi_m(T_m) = T_{m-1}$ and by construction, T_m consists of solutions mod π^{m+1} which lift to solutions mod π^{j+1} for all $j > m$.

Proof: Suppose there is a primitive congruence solution for each m. Let $S_m \subset (R_m)^n$ be the set of primitive solutions, and let φ_m denote the quotient $R_m \to R_{m-1}$ as well as the induced map $(R_m)^n \to (R_{m-1})^n$.
Note that φ_m maps primitive solutions to primitive solutions.
Indeed, a solution mod π^{m+1} is also a solution mod π^m.
Furthermore, if $u \notin \pi R_m$, then $\varphi_m(u) \notin \pi R_{m-1}$.
Now, let $S_{j,m} = \varphi_m \circ \cdots \circ \varphi_j(S_j) \subset S_m$ for $j > m$. Then

$$S_m \supseteq S_{m+1,m} \supseteq \cdots \supseteq S_{j,m} \supseteq \cdots .$$

As R_m is finite, all $S_{j,m}$ are finite (and by assumption non-empty). Thus the intersection T_m is non-empty. In general $\varphi_m(T_m) = T_{m-1}$ and by construction, T_m consists of solutions mod π^{m+1} which lift to solutions mod π^{j+1} for all $j > m$. So pick $\xi_0 \in T_0$, lift to $\xi_1 \in T_1$, and so forth. This then defines a compatible sequence i.e defines $\xi \in R^n$. As ξ_0 is primitive, so is ξ. □

Why is ξ primitive?: As notation, set $\xi_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$. The j'th coordinate of ξ is then the compatible sequence $(x_{0,j}, x_{1,j}, \ldots)$. Suppose, without loss of generality, that $x_{i,1}$ is the unit coordinate of ξ_i. Then $x_{0,1}$ is a unit in R_0, so in particular $(x_{0,1}, x_{1,1}, \ldots)$ is a unit in R (since any element in a complete DVR is a unit if and only if the constant term is non-zero i.e. a unit in $R_0 = R/\pi$).

Recall:

Theorem (3, Chevalley-Warning)

Let f be a polynomial in n variables with coefficients in a finite field k and let d be its degree. If $n > d$, then the number of solutions of f in k is congruent to 0 modulo p. In particular, finite fields are C_1.

Theorem (5, Tsen/Lang-Nagata)

Let k be a C_i-field. If K is an extension of k of transcendence degree n, then K is C_{i+n}.

Recall:

Theorem (3, Chevalley-Warning)

Let f be a polynomial in n variables with coefficients in a finite field k and let d be its degree. If $n > d$, then the number of solutions of f in k is congruent to 0 modulo p. In particular, finite fields are C_1.

Theorem (5, Tsen/Lang-Nagata)

Let k be a C_i-field. If K is an extension of k of transcendence degree n, then K is C_{i+n}.

Corollary

Let k be a finite field. Then $k(t)$ is C_2.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$. Clearing denominators, we may assume the coefficients of f lie in $k[[t]]$. Our goal is then to find a primitive solution in $k[[t]]$.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$. Clearing denominators, we may assume the coefficients of f lie in $k[[t]]$. Our goal is then to find a primitive solution in $k[[t]]$. Theorem (I) implies, that it is enough to find a primitive solution modulo t^{m+1} for each $m \geq 0$.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$. Clearing denominators, we may assume the coefficients of f lie in $k[[t]]$. Our goal is then to find a primitive solution in $k[[t]]$. Theorem (I) implies, that it is enough to find a primitive solution modulo t^{m+1} for each $m \geq 0$. Reducing f modulo t^{m+1} each power series coefficient becomes a polynomial in t of degree at most m.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$. Clearing denominators, we may assume the coefficients of f lie in $k[[t]]$. Our goal is then to find a primitive solution in $k[[t]]$. Theorem (I) implies, that it is enough to find a primitive solution modulo t^{m+1} for each $m \geq 0$. Reducing f modulo t^{m+1} each power series coefficient becomes a polynomial in t of degree at most m. So we have homogeneous polynomial equations of degree d in $n > d^2$ variables, with coefficients in $k[t]$.

Theorem (Special case of Greenberg)

Let k be a finite field. Then $k((t))$ is C_2.

Proof: Let f be a homogeneous polynomial of degree d in $n > d^2$ variables with coefficients in $k((t))$. Clearing denominators, we may assume the coefficients of f lie in $k[[t]]$. Our goal is then to find a primitive solution in $k[[t]]$. Theorem (I) implies, that it is enough to find a primitive solution modulo t^{m+1} for each $m \geq 0$. Reducing f modulo t^{m+1} each power series coefficient becomes a polynomial in t of degree at most m. So we have homogeneous polynomial equations of degree d in $n > d^2$ variables, with coefficients in $k[t]$. But $k(t)$ is C_2, so there is a non-trivial solution in $k(t)$. As the equation is homogeneous, we may clear denominators of such a non-trivial solution, to obtain a non-trivial primitive solution in $k[t]$. □

Thank you for listening.