Order and Specialisation of Torsion points

Maarten Derickx

Mathematisch Instituut
Universiteit Leiden

Topics in Arithmetic Geometry
09-05-2011

Outline

Definition

Let (R, v, m, k) be a discrete valuation ring. Then we define:

$$v : M_n(R) \longrightarrow \mathbb{Z}, \qquad (a_{ij})_{i,j=0}^n \longmapsto \min_{i,j} v(a_{ij})$$

Let $a, b \in M_n(R)$ then

1. $v(a) = \infty \Leftrightarrow a = 0$
2. $v(a+b) \geq \min(v(a), v(b))$ and equality if $v(a) \neq v(b)$
3. $v(ab) \geq v(a) + v(b)$

Proof:

1. Trivial
2. $v((a+b)_{ij}) \geq \min(v(a_{ij}), v(b_{ij})) \geq \min(v(a), v(b))$
3. $v((ab)_{ij}) = v(\sum_k a_{ik} b_{kj}) \geq \min_k(v(a_{ik} b_{kj})) \geq min_k(v(a_{ik})) + \min_k(v(b_{kj})) \geq v(a) + v(b)$

Lemma

Let (R, v, m, k) be a d.v.r. and $A \in \mathrm{GL}_n(R)$ of prime order p. If either

- $p \neq \operatorname{char} k$, *or*
- $\operatorname{char} R = 0$, $\operatorname{char} k = q$ *with q prime and* $v(q) < q - 1$

Then $\bar{A} \in \mathrm{GL}_n(k)$ also has order p.

Proof.

Assume $\bar{A} = 1$ and write $A = 1 + B$ with $v(B) \geq 1$ then

$$0 = (1 + B)^p - 1 = B^p + pB + pB^2 C$$
$$B^p = p(-B - B^2 C)$$
$$pv(B) \leq v(B^p) = v(p) + v(-B - B^2 C) = v(p) + v(B)$$

Case: $\operatorname{char} k \neq p$
Now $v(p) = 0$ so $pv(B) \leq v(B)$ is a contradion.Case: $\operatorname{char} R = 0$, $\operatorname{char} k = q$, $v(q) < q - 1$
Now $v(p) \geq p - 1 \geq 1$ hence $p = q$ and we get a contradiction.

□

Corollary

Let (R, v, m, k) be a d.v.r. and $A \in \mathrm{GL}_n(R)$ of finite order n. Then

- *if* $\mathrm{char}\, k = 0$ *then the order of A is n*
- *if* $\mathrm{char}\, R = 0$, $\mathrm{char}\, k = q$ *and* $v(q) < q - 1$ *then the order of A is n*
- *if* $\mathrm{char}\, k = q$ *then the order of A is* n/q^l *for some* $l \in \mathbb{N}$

Example

Let (R, v, m, k) be a d.v.r. with char $R = p$ and $t \in m$. Now consider the matrix

$$M = \begin{bmatrix} 0 & t & & & 0 \\ & 0 & t & & \\ & & \ddots & \ddots & \\ & & & 0 & t \\ 0 & & & & 0 \end{bmatrix}$$

in $\mathrm{GL}_p(R)$ then

$$(1 + M)^p = 1 + M^p = 1$$

but $1 + M \equiv 1 \mod m$ this shows $p \neq \text{char}\, k$ is really needed if char $R \neq 0$.

Example

Consider $R = \mathbb{Z}_{(p)}[\zeta_p]$ and $\mathrm{GL}_1(R) \cong R^*$, then ζ_p has as minimal polynomial $f(x) = \frac{x^p - 1}{x - 1}$ since $x^p - 1 = (x-1)^p \in \mathbb{F}_p[x]$ we see that p is completely ramified, i.e. $p = (p, \zeta_p - 1)^{p-1}$ so $v(p) = p - 1$. Now $f(x) = p$ and $p^2 \nmid p$ so R is nonsingular over p hence a d.v.r. Now $R/m = \mathbb{F}_p$ has only 1 as a pth root of unitiy so $\bar{\zeta}_p = 1$. This shows that the theorem cannot be generalized to $v(q) = q - 1$.

Definition

A scheme is a locally ringed space S for which locally at each $s \in S$ is isomorphic to $\operatorname{Spec} A_s$ for a A_s some ring. A morphism is just a morphism as locally ringed spaces.
Let R be a ring. A scheme over $\operatorname{Spec} R$ is a scheme together with a morphism $f_S : S \to \operatorname{Spec} R$. A morphism is a morphism of schemes $g : S \to S'$ such that $f_S = f_{S'} \circ g$.

Example

- If A is an R-algebra then $\operatorname{Spec} A$ is a scheme over R.
- $P^n(R)$
- A lot of less well behaved things like affine line over R with a double point at the origin.

Definition

Let R be a ring, a group scheme over Spec R is a scheme S over Spec R together with a multiplication μ, identity e and inverse $^{-1}$:

- $\mu : S \times_{\text{Spec } R} S \to S$
- $e : \text{Spec } R \to S$
- $^{-1} : S \to S$

Which satisfy the group law's (for example $\mu \circ (\text{Id} \times \mu) = \mu \circ (\mu \times \text{Id})$ is associativity).

Example

- The affine line over R together with addition induced by $R[x] \to R[x_1] \otimes_R R[x_2] \cong R[x_1, x_2]$ given by $x \to x_1 + x_2$.
- $\text{GL}_n(R) := \text{Spec } R[y, (x_{ij})_{i,j=1}^n]/(y \det(x_{ij}) - 1)$
- Elliptic curves in Weierstrass form where the coefficients lie in R.

Definition

Let G, S be schemes over Spec R. An S valued point of G is just an morphism of Spec R schemes $S \to G$.

Example

An Spec R valued point of $\mathrm{GL}_n(R)$ is induced by a map $f : R[y, (x_{ij})_{i,j=1}^n]/(y \det(x_{ij}) - 1) \to R$ this just means sending all x_{ij} to a value in R such that $det(f(x_{ij}))$ is invertible and sending y to $det(f(x_{ij}))^{-1}$.

If G is a group scheme then all S we can define a group structure on $\hom(S, G) \times \hom(S, G) \to \hom(S, G)$. (i.e. the set of all S valued points form a group).

Theorem

Let (R, v, k, m) be a $d.v.r$ with field of fractions K and G a group scheme over $\operatorname{Spec} R$. Let P be a $\operatorname{Spec} R$ valued point of prime order p. If either

- $p \neq \operatorname{char} k$*, or*
- $\operatorname{char} R = 0$*,* $\operatorname{char} k = q$ *with* q *prime and* $v(q) < q - 1$

Then P_k also has order p.

sketch of proof.

Idea: Assume P_k has order 1. Reduce to the $\mathrm{GL}_n(R)$ case. And get a contradiction.
Take an affine open neighbourhood $U = \mathrm{Spec}(A)$ of the image of $e_k = P_k$. This wil also contain all multiples of P. Let F be the scheme theoretic closure in U of all multiples of P_K. Now define $f : \amalg_{i=1}^n \mathrm{Spec}(R) \to \mathrm{Spec}(A/I) = F$ to be P^i on the $i-$th component.
One can now show that the map
$\amalg_{i=1}^n \mathrm{Spec}(K) \to \amalg_{i=1}^n \mathrm{Spec}(R) \to \mathrm{Spec}(A/I)$ is equal to
$\amalg_{i=1}^n \mathrm{Spec}(K) \cong \mathrm{Spec}((A/I) \otimes K) \to \mathrm{Spec}(A/I)$. Hence
$A/I \to R^n \to K^n$ is an injection and A/I is a free R module of rank n.
Now translation by P maps F to itself by construction. Hence we get an an R-algebra morphism of A/I to itself. I.e. an element of $\mathrm{GL}_p(R)$. □

Example

Define the proj. cubic curve $E/\mathbb{Z}$ by $zy^2 + xyz = x^3 + 4x^2z + z^3$, this induces an elliptic curve $E/\mathbb{Z}_{(q)}$ for $q \neq 5, 13$. $P = (-2 : 1 : 8)$ is a point of order 2 in $E/\mathbb{Z}_{(q)}$. Now $U = \mathrm{Spec}(A)$ with $A = \mathbb{Z}_{(q)}[x, z]/(z + zx - x^3 - z^2x - z^3)$ is an affine open neigbourhood of $P = (-2, 8)$ containing $(0, 0) = P^2$. Now

$$\phi : B = A/(x, z)(x + 2, z - 8) \to \mathbb{Q}^2, \quad x \mapsto (0, -2), z \mapsto (0, 8)$$

is an injection hence $B \cong \operatorname{im}\phi$ is free as a $Z_{(q)}$ module. The automorphism of $B \cong \operatorname{im}\phi$ induced by multiplication by P gives an element in $\mathrm{GL}_2\,\mathbb{Z}_{(q)}$. To be explicit $\{(1, 1), (0, 2)\}$ is a $\mathbb{Z}_{(q)}$ basis of $\operatorname{im}\phi$ the automorphism $(x, y) \to (y, x)$ written to this basis is given by the matix

$$M = \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix}$$

This matrix has order 2 indeed and $\bar{P} = 1 \Leftrightarrow q = 2 \Leftrightarrow \bar{M} = \mathrm{Id}$