Automorphisms of the Affine Line over Nonreduced Rings

University of New Mexico Geometry Seminar
Taylor Dupuy

The Affine Line

	Algebra		Geometry
ring	S	scheme	$\mathrm{Spec}(S)$
	$S[T]$		$\mathbb{A}^1_S = \mathrm{Spec}(S[T])$
	$S \to S[T]$		$\mathbb{A}^1_S \to \mathrm{Spec}(S)$

affine line over S

Automorphisms of Affine Line

$$\begin{tikzcd}
\mathbb{A}^1_S \arrow[rr, "\psi"] \arrow[dr] & & \mathbb{A}^1_S \arrow[dl] \\
& \mathrm{Spec}(S) &
\end{tikzcd}$$

Schemes	Rings
$\mathrm{Aut}(\mathbb{A}^1_S)$	$\mathrm{Aut}_S(S[T])^{op}$

group of polynomials invertible under composition

Affine Linear Subgroup

$$\begin{tikzcd}
\mathbb{A}^1_S \arrow[rr, "\psi"] \arrow[dr] & & \mathbb{A}^1_S \arrow[dl] \\
& \mathrm{Spec}(S) &
\end{tikzcd}$$

$$\mathrm{AL}_1(S) \subset \mathrm{Aut}(\mathbb{A}^1_S)$$

$$\psi(T) = a + bT$$

$$a \in S$$

$$b \in S^\times$$

Group Law $\psi_1(T) = a_1 + b_1 T$, $\psi_2(T) = a_2 + b_2 T$

$$(\psi_1 \circ \psi_2)(T) = a_1 + b_1 a_2 + b_1 b_2 T$$

Automorphisms over Domains

Theorem.

$$S \text{ a domain}$$
$$\implies \mathrm{Aut}(\mathbb{A}^1_S) = \mathrm{AL}_1(S)$$

proof.

$$S[T] = S[\psi(T)] \implies \deg(\psi(T)) \leq 1$$

$\blacksquare$

Automorphisms of the affine line over domains are really really really boring.

Non-Boring Automorphisms

$S = \mathbb{Z}/p^2$ (Ring with nilpotents!)

$$\psi(T) = T + pT^{100} \mod p^2$$

$$\psi^{-1}(T) = T - pT^{100} \mod p^2$$

$$\psi(T) \in \mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/p^2})$$

Iterates have bounded degree: $\deg(\psi^n(T)) \leq 100$

Has finite order: $\psi(T)$ has order p

MAIN POINTS

- Univariate polynomials under composition have finite order (over $\mathbb{Z}/p^n$)
- Iterates of a univariate polynomial under composition have bounded degree.
- Univariate polynomials under composition are really algebraic groups! (over $\mathbb{Z}/p^n$)
- Univariate polynomials automorphism groups are solvable!

Examples

polynomial	order	coefficient ring
$1+T$	2	$\mathbb{Z}/2^3$
$1+T$	16	$\mathbb{Z}/2^4$
$T+2^2T^4$	4	$\mathbb{Z}/2^4$
$T+2^3T^4$	2	$\mathbb{Z}/2^4$
$T+2^2T^{10}+2^3T^5$	8	$\mathbb{Z}/2^4$
$T^2+2^2T^{10}$	8	$\mathbb{Z}/2^4$

More Examples

$$T + pT^2 + p^2T^4 \quad \text{mod } p^r \qquad (r = 4)$$

$p = 5$, order $= 125$

$p = 7$, order $= 343$ $\longleftarrow p^{r-1}$

$p = 11$, order $= 1331$

This is the typical case

Even More Examples

$$\mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/5^4})$$

$$\begin{array}{rl}
\text{order25} & 80T^{10}+350T^9+620T^8+300T^7+180T^6+145T^5+560T^4+525T^3 \\
 & +265T^2+571T+191, \\
\text{order125} & 555T^{10}+400T^9+605T^8+305T^7+435T^6+470T^5+250T^4+490T^3 \\
 & +515T^2+346T+356, \\
\text{order500} & 230T^{10}+405T^9+335T^8+410T^7+205T^6+325T^5+620T^4+195T^3 \\
 & +10T^2+62T+160, \\
\text{order625} & 370T^{10}+70T^9+75T^8+65T^7+385T^6+450T^5+200T^4+560T^3 \\
 & +395T^2+606T+487, \\
\text{order125} & 390T^{15}+330T^{14}+300T^{13}+290T^{12}+220T^{11}+230T^{10}+580T^9+220T^8 \\
 & +575T^7+430T^6+600T^5+365T^4+230T^3+395*T^2+T+285
\end{array}$$

Our Setup

We Study: $\mathrm{Aut}(\mathbb{A}^1_S) = \mathrm{Aut}_S(S[T])^{op}$

Where: $S = R/q^n$ (non reduced!)

$qR = \langle q \rangle$ prime

Rings we are thinking about:

$R = \mathbb{Z}$	$q = p$	(wittfinitesimal)
$R = F[t]$	$q = t$	(infinitesimals)
$R =$ coord ring of affine scheme	$q = p$	(corresp. to $\mathcal{O}(U \times \mathbb{A}^1_{\mathbb{Z}})$)

Subgroups: Abelian ones!

important feature

$$\mathfrak{g}_{r,s} \subset \mathrm{Aut}(\mathbb{A}^1_{R/q^r})\,,\ s \geq r/2 \longleftarrow q^s \cdot q^s \equiv 0 \mod q^r$$

reduction map

$$\mathfrak{g}_{r,s} := \ker(\mathrm{Aut}(\mathbb{A}^1_{R/q^r}) \to \mathrm{Aut}(\mathbb{A}^1_{R/q^s})$$

$$\psi(T) = T + q^s f(T) \in \mathfrak{g}_{s,r}, \qquad f(T) \in R/q^{r-s}[T]$$

Should be viewed as q-adically close to the identity! Like a Lie algebra!

Group Law:

$$(T + p^s f(T)) \circ (T + p^s g(T)) = T + p^s (f(T) + g(T))$$

Subgroups: Bounded Degree

Defn/Proposition

$$\boxed{\begin{array}{c}\widetilde{A}_d(n,R,q) \subset \mathrm{Aut}(\mathbb{A}^1_{R/q^n}) \\ \forall m \geq 2, \ \ \deg(\psi \mod q^m) \leq d2^{m-2}\end{array}}$$

Corollaries

1) Every iterate of $\psi \in \mathrm{Aut}(\mathbb{A}^1_{R/q^n})$ has bounded degree.

2) Every $\psi \in \mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/p^n})$ has finite order.

Corollaries

1) Every iterate of $\psi \in \mathrm{Aut}(\mathbb{A}^1_{R/q^n})$ has bounded degree.

2) Every $\psi \in \mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/p^n})$ has finite order.

The Point:

If $\psi \in \mathrm{Aut}(\mathbb{A}^1_{R/q^n})$ and $\deg(\psi) = d$ then $\psi \in \widetilde{A}_d(n, R, q)$

Remark:

The explicit bound on the degree using this method is *super shitty*.

$$\widetilde{A}_d(R,q)_{\mathbf{n}} \subset \mathrm{Aut}(\mathbb{A}^1_{R/q^n})$$
$$\forall m \geq 2, \quad \deg(\psi \mod q^m) \leq d2^{m-2}$$

example: $n = 2$

$d =$ whatever

$\widetilde{A}_d(2,R,q)$ polynomials mod q^2 of degree less than d

$$\psi(T) = a_0 + a_1 T + qf(T)$$
$$\widetilde{\psi}(T) = \tilde{a}_0 + \tilde{a}_1 T + q\tilde{f}(T)$$

$$\mathrm{ord}_T(f), \mathrm{ord}_T(\tilde{f}) \geq 2$$

composing these polynomials gives

$$\begin{aligned} \psi(\widetilde{\psi}(T)) &\equiv a_0 + a_1[\tilde{a}_0 + \tilde{a}_1 T + q\tilde{f}(T)] + qf(\tilde{a} + \tilde{a}T) \\ &= a_0 + a_1\tilde{a}_0 + (a_1\tilde{a}_1)T \\ &\qquad +q(a_1\tilde{f}(T) + f(\tilde{a}_0 + \tilde{a}_1 T)) \end{aligned}$$

which shows the set is closed under composition.

next case: $\widetilde{A}_d(3, R, q)$

$\mathrm{ord}_T(f) \geq 2$

$\mathrm{ord}_T(g) \geq 3$

$$\boxed{\begin{gathered}\psi(T) = a_0 + a_1 T + q f(T) + q^2 g(T) \mod q^3 \\ \deg(\psi \mod q^2) \leq d \\ \deg(\psi \mod q^3) \leq 2d\end{gathered}}$$

Want to show when we compose two of these guys we get one back. Look at:

$$\begin{aligned}\deg(\psi \mod q^2) &\geq \deg(f \mod q), \\ \deg(\psi \mod q^3) &\geq \deg(g \mod q), \deg(f \mod q^2),\end{aligned}$$

composing gives

$$\begin{aligned}\psi(\widetilde{\psi}(T)) &= a_0 + a_1 \widetilde{\psi}(T) \\ &\quad + q[f(\tilde{a}_0 + \tilde{a}_1 T) + q f'(\tilde{a}_0 + \tilde{a}_1 T)\tilde{f}(T)] \\ &\quad + q^2 g(\tilde{a}_0 + \tilde{a}_1 T)\end{aligned}$$

information

d

$$\begin{aligned}\deg(\psi \mod q^2) &\geq \deg(f \mod q),\\ \deg(\psi \mod q^3) &\geq \deg(g \mod q), \deg(f \mod q^2),\end{aligned}$$

$2d$

computation

$$\begin{aligned}\psi(\widetilde{\psi}(T)) &= a_0 + a_1\widetilde{\psi}(T)\\ &+ q[f(\tilde{a}_0 + \tilde{a}_1 T) + qf'(\tilde{a}_0 + \tilde{a}_1 T)\tilde{f}(T)]\\ &+ q^2 g(\tilde{a}_0 + \tilde{a}_1 T)\end{aligned}$$

- $(\deg f(\tilde{a}_0 + \tilde{a}_1 T) \mod q^2) \leq 2d,$
- $(\deg f'(\tilde{a}_0 + \tilde{a}_1 T)\tilde{f}(T) \mod q) \leq (d-1) + d$
- $(\deg g(\tilde{a}_0 + \tilde{a}_1 T) \mod q) \leq 2d,$

↑

$deg(\psi(\widetilde{\psi}(T))) \leq 2d$

Algebraic Groups

- Algebraic varieties where group laws are given by polynomial expressions.
- Example: matrix groups like the general linear group

As Algebraic Groups!

Theorem.

There exist $G/\mathbb{F}_p$ finite dimensional such that

$$G(\mathbb{F}_p) \cong A_n(\mathbb{Z}, p).$$

There exist $G/\mathbb{F}_p$ infinite dimensional such that

$$G(\mathbb{F}_p) \cong \mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/p^n}).$$

Algebraicity Idea:

Apply (Greenberg Transform = p-Jet Functors)!

$$\mathrm{Gr}^n(X) = J_p^n(X) \mod p$$

Key Property: $\mathrm{Gr}^n(X)(\mathbb{F}_p) = X(\mathbb{Z}/p^{n+1})$

defined over $\mathbb{F}_p$

mixed characteristic

higher dimension

Solvability

Theorem.

The groups $\mathrm{Aut}(\mathbb{A}^1_{R_n})$ and $A_n(R,q)$ are solvable.

Solvable Groups

The collection of solvable groups is built inductively:

base defn: If a group is abelian then it is solvable.

inductive part: a group is solvable when one of the following is true
1) It is the the extension of an abelian group by a solvable group.
2) It is the extension of a solvable group by an abelian group.

extension of H by V

$$1 \to V \to E \to H \to 1$$

Example

Claim: $\mathrm{AL}_1(S)$ is solvable.

proof.

$$\mathrm{AL}_1(S) \cong S \rtimes S^\times$$

$$1 \to S \to S \rtimes S^\times \to S^\times \to 1$$

∎

Subgroups: Newton Polygonish condition

The collection of invertible polynomials of the form

$$\psi(T) \equiv a_0 + a_1 T + q a_2 T^2 + q^2 a_3 T^4 + \cdots + q^{d-1} a_d T^d \in R/q^d[T]$$

form a subgroup

$$\mathbb{A}_d(R,q) \subset \mathrm{Aut}(\mathbb{A}^1_{R/q^d})$$

Coefficients are increasingly divisible by q

proof is similar to the computations we did before.

Idea Behind Solvability

Use the groups

$$g_{r,s} = \ker(\mathrm{Aut}(\mathbb{A}^1_{R/q^r}) \to \mathrm{Aut}(\mathbb{A}^1_{R/q^s}))$$
$$s \geq r/2$$

or their variants to build up the groups we want.

Example. $A_2(R,q)$ is solvable.

proof is by induction.

Expected Degree Bounds

The Theorem we stated earlier is far from optimal for automorphisms of quotients of the integers.

Here is the expected better bound (for a typical element):

$$\psi \in \mathrm{Aut}(\mathbb{A}^1_{\mathbb{Z}/p^r})$$

$$\deg(\psi^n \mod p^r) \leq (\deg(\psi) - 1)(r - 1) + 1$$