

Courbes algébriques lisses en caractéristique $p > 0$ munies d'un gros p -groupe d'automorphismes.

Magali Rocher

Institut de Mathématiques de Bordeaux 1.

14 novembre 2008.

Notations.

- k est un corps algébriquement clos de caractéristique $p \geq 0$.
- Si $p > 0$,
 - F est l'endomorphisme Frobenius pour une k -algèbre.
 - $\wp = F - id$.
- C/k est une courbe algébrique, projective lisse connexe de genre $g \geq 2$.
- $\text{Aut}_k(C)$ est le groupe des k -automorphismes de C .

Le cas de la caractéristique 0.

Pourquoi considérer de gros groupes d'automorphismes?

Le cas de la caractéristique 0.

Pourquoi considérer de gros groupes d'automorphismes?

- En caractéristique 0:

$$|\mathrm{Aut}_k(C)| \leq 84(g-1) \quad (\text{borne d'Hurwitz 1892})$$

Le cas de la caractéristique 0.

Pourquoi considérer de gros groupes d'automorphismes?

- En caractéristique 0:

$$|\mathrm{Aut}_k(C)| \leq 84(g-1) \quad (\text{borne d'Hurwitz 1892})$$

- Problème: classification des groupes d'automorphismes à genre donné.

Le cas de la caractéristique 0.

Pourquoi considérer de gros groupes d'automorphismes?

- En caractéristique 0:

$$|\mathrm{Aut}_k(C)| \leq 84(g-1) \quad (\text{borne d'Hurwitz 1892})$$

- Problème: classification des groupes d'automorphismes à genre donné.
- Réponse partielle pour les groupes $G \subset \mathrm{Aut}_k(C)$ dits "larges":

$$|G| \geq 4(g-1) \quad (\text{Kulkarni 1997, Breuer 2000})$$

Par la formule d'Hurwitz, $g_{C/G} = 0$ et $C \rightarrow C/G$ ramifié en 3 ou 4 points

Le cas de la caractéristique $p > 0$.

En caractéristique $p > 0$:

- $\text{Aut}_k(C)$ est encore fini (Schmid 1938).

Le cas de la caractéristique $p > 0$.

En caractéristique $p > 0$:

- $\text{Aut}_k(C)$ est encore fini (Schmid 1938).
- Si $G \subset \text{Aut}_k(C)$ d'ordre premier à p (cas modéré),

$$|G| \leq 84(g - 1) \quad (\text{Grothendieck 1963})$$

Le cas de la caractéristique $p > 0$.

En caractéristique $p > 0$:

- $\text{Aut}_k(C)$ est encore fini (Schmid 1938).
- Si $G \subset \text{Aut}_k(C)$ d'ordre premier à p (cas modéré),

$$|G| \leq 84(g-1) \quad (\text{Grothendieck 1963})$$

- Sinon, la borne est biquadratique:

$$|\text{Aut}_k(C)| \leq 16g^4 \quad (\text{Stichtenoth 1973})$$

sauf pour $C : W^q + W = X^{1+q}$, $q = p^n \geq 3$.

Explication: apparition de ramification sauvage.

Introduction des grosses actions.

Idée: comme en caractéristique 0, considérer de "gros" groupes d'automorphismes pour fixer $g_{C/G}$ et la ramification de $C \rightarrow C/G$.

Introduction des grosses actions.

Idée: comme en caractéristique 0, considérer de "gros" groupes d'automorphismes pour fixer $g_{C/G}$ et la ramification de $C \rightarrow C/G$.

Définition (Lehr-Matignon)

Soit C/k une courbe projective lisse connexe de genre g .

Soit G un sous-groupe fini de $\text{Aut}_k(C)$.

On dit que (C, G) est une **grosse action** si:

- $g \geq 1$.
- G est un p -groupe.
-

$$|G| > \frac{2p}{p-1} g.$$

Propriétés générales sur les grosses actions.

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit h l'invariant de Hasse-Witt de C .

- *Formules d'Hurwitz et Deuring-Shafarevitch à $C \rightarrow C/G$:
[Nakajima 1987]*
 - $|G| > \frac{2p}{p-1} g$ implique $h = 0$.

Propriétés générales sur les grosses actions.

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit h l'invariant de Hasse-Witt de C .

- *Formules d'Hurwitz et Deuring-Shafarevitch à $C \rightarrow C/G$: [Nakajima 1987]*
 - $|G| > \frac{2p}{p-1} g$ implique $h = 0$.
 - un seul point $\infty \in C$ est ramifié et même totalement ramifié.

Propriétés générales sur les grosses actions.

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit h l'invariant de Hasse-Witt de C .

- *Formules d'Hurwitz et Deuring-Shafarevitch à $C \rightarrow C/G$: [Nakajima 1987]*
 - $|G| > \frac{2p}{p-1} g$ implique $h = 0$.
 - un seul point $\infty \in C$ est ramifié et même totalement ramifié.
- Soit G_i le i -ième groupe de ramification inférieure de G au point ∞ . Comme G est un p -groupe, $G = G_{-1} = G_0 = G_1$.

Propriétés générales sur les grosses actions.

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit h l'invariant de Hasse-Witt de C .

- *Formules d'Hurwitz et Deuring-Shafarevitch à $C \rightarrow C/G$: [Nakajima 1987]*
 - $|G| > \frac{2p}{p-1} g$ implique $h = 0$.
 - un seul point $\infty \in C$ est ramifié et même totalement ramifié.
- Soit G_i le i -ième groupe de ramification inférieure de G au point ∞ . Comme G est un p -groupe, $G = G_{-1} = G_0 = G_1$.
- $|G| > \frac{p}{p-1} g$ implique $C/G_1 \simeq \mathbb{P}_k^1$ et $C/G_2 \simeq \mathbb{P}_k^1$. [Stichtenoth 1973]

Propriétés générales sur les grosses actions.

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit h l'invariant de Hasse-Witt de C .

- *Formules d'Hurwitz et Deuring-Shafarevitch à $C \rightarrow C/G$: [Nakajima 1987]*
 - $|G| > \frac{2p}{p-1} g$ implique $h = 0$.
 - un seul point $\infty \in C$ est ramifié et même totalement ramifié.
- Soit G_i le i -ième groupe de ramification inférieure de G au point ∞ . Comme G est un p -groupe, $G = G_{-1} = G_0 = G_1$.
- $|G| > \frac{p}{p-1} g$ implique $C/G_1 \simeq \mathbb{P}_k^1$ et $C/G_2 \simeq \mathbb{P}_k^1$. [Stichtenoth 1973]
- En particulier, $G_2 \neq \{e\}$.

Le problème de plongement.

- $|G| > \frac{2p}{p-1} g$ est nécessaire pour avoir l'inclusion **stricte**: $G_2 \subsetneq G_1 = G$.
(contre-exemple: $W^p - W = X^2, p > 2$).

Le problème de plongement.

- $|G| > \frac{2p}{p-1} g$ est nécessaire pour avoir l'inclusion **stricte**: $G_2 \subsetneq G_1 = G$.
(contre-exemple: $W^p - W = X^2, p > 2$).
- Soit X tel que $C/G_2 - \{\infty\} = \text{Spec } k[X]$.
 $G/G_2 \simeq \{X \rightarrow X + y, y \in V\}$ où V est un \mathbb{F}_p -sous-espace vectoriel de k .

Le problème de plongement.

- $|G| > \frac{2p}{p-1} g$ est nécessaire pour avoir l'inclusion **stricte**: $G_2 \subsetneq G_1 = G$.
(contre-exemple: $W^p - W = X^2, p > 2$).
- Soit X tel que $C/G_2 - \{\infty\} = \text{Spec } k[X]$.
 $G/G_2 \simeq \{X \rightarrow X + y, y \in V\}$ où V est un \mathbb{F}_p -sous-espace vectoriel de k .
- D'où la suite exacte:

$$0 \longrightarrow G_2 \longrightarrow G = G_1 \xrightarrow{\pi} V \simeq (\mathbb{Z}/p\mathbb{Z})^v \longrightarrow 0,$$

avec

$$\pi : \begin{cases} G \rightarrow V \\ g \rightarrow g(X) - X. \end{cases}$$

Plan de la thèse.

- Chapitre 1: Mise en perspective dans le cadre général des G -actions de courbes.
- Chapitre 2: [MR] "*Smooth curves having a large automorphism p -group in characteristic $p > 0$.*"
 - Conditions nécessaires sur G_2 . En particulier, $G_2 = D(G)$.
 - Exemples de grosses actions avec G_2 abélien d'exposant quelconque.
- Chapitre 3: [Ro1] "*Large p -group actions with a p -elementary abelian derived group.*"
 Paramétrisation des grosses actions avec $D(G) \simeq (\mathbb{Z}/p\mathbb{Z})^n$.
- Chapitre 4: [Ro2] "*Large p -group actions with $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.*"
 Résultats de finitude et poursuite de la classification des grosses actions.

Condition de transfert.

Proposition (MR)

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit H un sous-groupe distingué de G tel que $H \subsetneq G$.

Alors, $(C/H, G/H)$ est une grosse action telle que $(G/H)_2 = G_2/H$.

Condition de transfert.

Proposition (MR)

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit H un sous-groupe distingué de G tel que $H \subsetneq G$.

Alors, $(C/H, G/H)$ est une grosse action telle que $(G/H)_2 = G_2/H$.

Application: Prendre $H = \text{Fratt}(G_2) = D(G_2) G_2^p$.

On obtient ainsi une grosse action (C, G) avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$. ([Ro1]).

Condition de transfert.

Proposition (MR)

Soit (C, G) une grosse action de genre $g \geq 2$.

Soit H un sous-groupe distingué de G tel que $H \subsetneq G_2$.

Alors, $(C/H, G/H)$ est une grosse action telle que $(G/H)_2 = G_2/H$.

Application: Prendre $H = \text{Fratt}(G_2) = D(G_2) G_2^p$.

On obtient ainsi une grosse action (C, G) avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$. ([Ro1]).

Cas particulier: (C, G) grosse action avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Caractérisation des grosses actions avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème (L-M)

Soit (C, G) une grosse action de genre $g \geq 2$ telle que $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

- Alors,

$$C \sim C_f : W^p - W = f(X) := cX + XS(X) \in k[X]$$

où $S(X) = (a_0 \text{id} + a_1 F + \dots + a_s F^s)(X)$ est additif de degré p^s , $s \geq 1$.

Caractérisation des grosses actions avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème (L-M)

Soit (C, G) une grosse action de genre $g \geq 2$ telle que $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

- Alors,

$$C \sim C_f : W^p - W = f(X) := cX + XS(X) \in k[X]$$

où $S(X) = (a_0 \text{id} + a_1 F + \dots + a_s F^s)(X)$ est additif de degré p^s , $s \geq 1$.

- On définit le polynôme palindromique de S (Elkies):

$$\text{Ad}_S := \frac{1}{a_s^{p^s}} F^s \sum_{j=0}^s (a_j F^j + F^{-j} a_j) \quad \text{et} \quad V \subset Z(\text{Ad}_S) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s}.$$

Caractérisation des grosses actions avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème

- Soit $A_{\infty,1}$ le groupe d'inertie sauvage de $\text{Aut}_k(C)$ au point ∞ . Alors,

$$0 \longrightarrow Z(A_{\infty,1}) = D(A_{\infty,1}) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow A_{\infty,1} \xrightarrow{\pi} Z(\text{Ad}_S) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \longrightarrow 0$$

Pour $p > 2$, unique groupe extraspécial d'exposant p et d'ordre p^{2s+1} .

Caractérisation des grosses actions avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème

- Soit $A_{\infty,1}$ le groupe d'inertie sauvage de $\text{Aut}_k(C)$ au point ∞ . Alors,

$$0 \longrightarrow Z(A_{\infty,1}) = D(A_{\infty,1}) \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow A_{\infty,1} \xrightarrow{\pi} Z(\text{Ad}_S) \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \longrightarrow 0$$

Pour $p > 2$, unique groupe extraspécial d'exposant p et d'ordre p^{2s+1} .

- Il existe un \mathbb{F}_p -sous-espace vectoriel $V \subset Z(\text{Ad}_S)$ tel que:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & A_{\infty,1} & \xrightarrow{\pi} & Z(\text{Ad}_S) & \longrightarrow & 0 \\ & & \parallel & & \cup & & \cup & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G & \xrightarrow{\pi} & V & \longrightarrow & 0 \end{array}$$

Caractérisation des grosses actions avec $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Théorème

Réciproque:

Soit

$$C_f : W^p - W = f(X) := cX + XS(X) \in k[X]$$

où $S(X)$ est un polynôme additif de $k[X]$ de degré p^s avec $s \geq 1$.

Alors, $(C_f, A_{\infty,1})$ est une grosse action dont le G_2 est cyclique d'ordre p .

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Preuve: Si $D(G) \subsetneq G_2$,

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Preuve: Si $D(G) \subsetneq G_2$,

- Par transfert, on se ramène à une grosse action $(C/H, G/H)$ avec $(G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z}$.

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Preuve: Si $D(G) \subsetneq G_2$,

- Par transfert, on se ramène à une grosse action $(C/H, G/H)$ avec $(G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z}$.
- Alors, $C/H : W^p - W = XS(X) + cX$, où S est additif de degré p^s .

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Preuve: Si $D(G) \subsetneq G_2$,

- Par transfert, on se ramène à une grosse action $(C/H, G/H)$ avec $(G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z}$.
- Alors, $C/H : W^p - W = XS(X) + cX$, où S est additif de degré p^s .
- G/H sous-groupe abélien normal d'un groupe extraspécial: d'où $|G/H| \leq p^{s+1}$.

Détermination algébrique de G_2 .

Corollaire (MR)

Soit (C, G) une grosse action avec $g \geq 2$. Alors, $G_2 = D(G)$.

En particulier, G n'est pas abélien.

Preuve: Si $D(G) \subsetneq G_2$,

- Par transfert, on se ramène à une grosse action $(C/H, G/H)$ avec $(G/H)_2 \simeq \mathbb{Z}/p\mathbb{Z}$.
- Alors, $C/H : W^p - W = XS(X) + cX$, où S est additif de degré p^s .
- G/H sous-groupe abélien normal d'un groupe extraspécial: d'où $|G/H| \leq p^{s+1}$.
- Comme $g_{C/H} = \frac{1}{2}(p-1)p^s$, on trouve $\frac{|G/H|}{g_{C/H}} \leq \frac{2p}{p-1}$. \square

Classification des grosses actions.

Soit (C, G) une grosse action avec $g \geq 2$. Le critère de classification est $\frac{|G|}{g^2}$.

Classification des grosses actions.

Soit (C, G) une grosse action avec $g \geq 2$. Le critère de classification est $\frac{|G|}{g^2}$.

- $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$ (Stichtenoth).

Classification des grosses actions.

Soit (C, G) une grosse action avec $g \geq 2$. Le critère de classification est $\frac{|G|}{g^2}$.

- $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$ (Stichtenoth).
- D'autre part, par la formule d'Hurwitz:

$$\frac{|G|}{g^2} \geq M > 0 \quad \Rightarrow \quad |G_2| \leq \frac{4}{M} \frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}| - 1)^2}$$

où $G = G_0 = G_1 \supsetneq G_2 = \dots = G_{i_0} \supsetneq G_{i_0+1} = \dots$

Classification des grosses actions.

Soit (C, G) une grosse action avec $g \geq 2$. Le critère de classification est $\frac{|G|}{g^2}$.

- $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$ (Stichtenoth).
- D'autre part, par la formule d'Hurwitz:

$$\frac{|G|}{g^2} \geq M > 0 \quad \Rightarrow \quad |G_2| \leq \frac{4}{M} \frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}| - 1)^2}$$

où $G = G_0 = G_1 \supsetneq G_2 = \dots = G_{i_0} \supsetneq G_{i_0+1} = \dots$

- Lorsque $M = \frac{4}{(p-1)^2}$, $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ et deux cas sont possibles: [L-M]
 - $G = A_{\infty,1}$ et $V = Z(\text{Ad}_S)$. Dans ce cas, $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}$.
 - $[A_{\infty,1} : G] = p$ et V hyperplan de $Z(\text{Ad}_S)$. Dans ce cas, $\frac{|G|}{g^2} = \frac{4}{(p-1)^2}$.

Classification des grosses actions.

Soit (C, G) une grosse action avec $g \geq 2$. Le critère de classification est $\frac{|G|}{g^2}$.

- $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$ (Stichtenoth).
- D'autre part, par la formule d'Hurwitz:

$$\frac{|G|}{g^2} \geq M > 0 \quad \Rightarrow \quad |G_2| \leq \frac{4}{M} \frac{|G_2/G_{i_0+1}|^2}{(|G_2/G_{i_0+1}| - 1)^2}$$

où $G = G_0 = G_1 \supsetneq G_2 = \dots = G_{i_0} \supsetneq G_{i_0+1} = \dots$

- Lorsque $M = \frac{4}{(p-1)^2}$, $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ et deux cas sont possibles: [L-M]
 - $G = A_{\infty,1}$ et $V = Z(\text{Ad}_S)$. Dans ce cas, $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}$.
 - $[A_{\infty,1} : G] = p$ et V hyperplan de $Z(\text{Ad}_S)$. Dans ce cas, $\frac{|G|}{g^2} = \frac{4}{(p-1)^2}$.
- ([Ro2]) Poursuite de la classification pour $M = \frac{4}{(p^2-1)^2}$.

Proposition (MR)

Soit (C, G) une grosse action avec $g \geq 2$ telle que $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Alors, $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $1 \leq n \leq 3$.

Proposition (MR)

Soit (C, G) une grosse action avec $g \geq 2$ telle que $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Alors, $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $1 \leq n \leq 3$.

Preuve:

- $|G_2|$ divise p^3 .

Proposition (MR)

Soit (C, G) une grosse action avec $g \geq 2$ telle que $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Alors, $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $1 \leq n \leq 3$.

Preuve:

- $|G_2|$ divise p^3 .
- On en déduit que G_2 est abélien.

Proposition (MR)

Soit (C, G) une grosse action avec $g \geq 2$ telle que $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Alors, $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $1 \leq n \leq 3$.

Preuve:

- $|G_2|$ divise p^3 .
- On en déduit que G_2 est abélien.
- On exclut le cas $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Méthode: étude de la filtration de ramification de G_2 .

Proposition (MR)

Soit (C, G) une grosse action avec $g \geq 2$ telle que $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.

Alors, $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $1 \leq n \leq 3$.

Preuve:

- $|G_2|$ divise p^3 .
- On en déduit que G_2 est abélien.
- On exclut le cas $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Méthode: étude de la filtration de ramification de G_2 .
- Reste à exclure les cas cycliques: $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$ et $G_2 \simeq \mathbb{Z}/p^3\mathbb{Z}$.
Méthode: considérer le problème de plongement.

Grosses actions avec G_2 cyclique.

Plus généralement:

Théorème (MR)

Soit (C, G) une grosse action. Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.

Grosses actions avec G_2 cyclique.

Plus généralement:

Théorème (MR)

Soit (C, G) une grosse action. Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.

Preuve:

- Par transfert, on se ramène au cas $n = 2$, i.e. $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$.

Grosses actions avec G_2 cyclique.

Plus généralement:

Théorème (MR)

Soit (C, G) une grosse action. Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.

Preuve:

- Par transfert, on se ramène au cas $n = 2$, i.e. $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$.
- Soient $L := k(C)$ et $k(X) := L^{G_2}$.
Alors, $L/k(X)$ est une extension d'Artin-Schreier-Witt:

$$[W_0, V_0]^p - [W_0, V_0] = [f_0(X), g_0(X)] \in W_2(k[X]).$$

Grosses actions avec G_2 cyclique.

Plus généralement:

Théorème (MR)

Soit (C, G) une grosse action. Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.

Preuve:

- Par transfert, on se ramène au cas $n = 2$, i.e. $G_2 \simeq \mathbb{Z}/p^2\mathbb{Z}$.
- Soient $L := k(C)$ et $k(X) := L^{G_2}$.
Alors, $L/k(X)$ est une extension d'Artin-Schreier-Witt:

$$[W_0, V_0]^p - [W_0, V_0] = [f_0(X), g_0(X)] \in W_2(k[X]).$$

- *Problème de plongement.* Résoudre mod $\wp(W_2(k[X]))$:

$$\forall y \in V, \quad [f_0(X+y), g_0(X+y)] = n(y) [f_0(X), g_0(X)] \quad n(y) \in (\mathbb{Z}/p^2\mathbb{Z})^\times$$

Remarque

- Problème: obstruction liée au cocycle de Witt.

Il faut donc chercher G_2 sous la forme:

$$G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$$

Remarque

- Problème: obstruction liée au cocycle de Witt.

Il faut donc chercher G_2 sous la forme:

$$G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$$

- Question: trouver une borne inférieure sur t .

Remarque

- Problème: obstruction liée au cocycle de Witt.

Il faut donc chercher G_2 sous la forme:

$$G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$$

- Question: trouver une borne inférieure sur t .
- Dans la suite, on construit de telles actions avec $t = O(\log_p g)$.

Grosses actions avec G_2 abélien d'exposant p^2 .

Notations: $q := p^e$, $e \in \mathbb{N}^*$, $K := \mathbb{F}_q(X)$, K^{alg} fixé, $m \in \mathbb{N}$.

Définition

(K. Lauter 1999, R. Auer 1999) On appelle $K^m \subset K^{alg}$ l'extension abélienne maximale de K

- de conducteur $\leq m_\infty$
- totalement décomposée au-dessus de $S := \{(X - y), y \in \mathbb{F}_q\}$.

Grosses actions avec G_2 abélien d'exposant p^2 .

Notations: $q := p^e$, $e \in \mathbb{N}^*$, $K := \mathbb{F}_q(X)$, K^{alg} fixé, $m \in \mathbb{N}$.

Définition

(K. Lauter 1999, R. Auer 1999) On appelle $K^m \subset K^{alg}$ l'extension abélienne maximale de K

- de conducteur $\leq m_\infty$
- totalement décomposée au-dessus de $S := \{(X - y), y \in \mathbb{F}_q\}$.

Remarque

$$\mathcal{G}_m := \text{Gal}(K^m/K) \simeq \frac{1 + Z\mathbb{F}_q[[Z]]}{\langle 1 + Z^m\mathbb{F}_q[[Z]], 1 - yZ, y \in \mathbb{F}_q \rangle}, \quad \text{avec } Z = X^{-1}$$

(Lauter) \mathcal{G}_m est d'exposant 1 ou $p \Leftrightarrow m < m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$.

Exemples de grosses actions avec G_2 abélien d'exposant p^2 .

Proposition (MR)

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$ s'étend en un p -groupe $G_m \subset \text{Aut}_{\mathbb{F}_q}(K^m)$:

$$0 \longrightarrow \mathcal{G}_m \longrightarrow G_m \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

Exemples de grosses actions avec G_2 abélien d'exposant p^2 .

Proposition (MR)

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$ s'étend en un p -groupe $G_m \subset \text{Aut}_{\mathbb{F}_q}(K^m)$:

$$0 \longrightarrow \mathcal{G}_m \longrightarrow G_m \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

- Soit C_m/\mathbb{F}_q la courbe projective lisse de corps de fonctions K^m .
 - Pour $e \geq 6$, (C_{m_2}, G_{m_2}) est une grosse action.
 - Son deuxième groupe de ramification \mathcal{G}_{m_2} abélien d'exposant p^2 .

Exemples de grosses actions avec G_2 abélien d'exposant p^2 .

Proposition (MR)

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$ s'étend en un p -groupe $G_m \subset \text{Aut}_{\mathbb{F}_q}(K^m)$:

$$0 \longrightarrow \mathcal{G}_m \longrightarrow G_m \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

- Soit C_m/\mathbb{F}_q la courbe projective lisse de corps de fonctions K^m .
 - Pour $e \geq 6$, (C_{m_2}, G_{m_2}) est une grosse action.
 - Son deuxième groupe de ramification \mathcal{G}_{m_2} abélien d'exposant p^2 .

Remarque

De même pour obtenir G_2 abélien d'exposant quelconque.

Remarque

(Lien avec les courbes algébriques avec beaucoup de points rationnels).

$$N_m = |C_m(\mathbb{F}_q)| = 1 + q|\mathcal{G}_m| = 1 + |G_m|$$

D'où,

$$\frac{|G_m|}{g_{C_m}} \sim \frac{N_m}{g_{C_m}}$$

Problème:

- On sait donner les équations de l'extension K^{m_2}/K .

Problème:

- On sait donner les équations de l'extension K^{m_2}/K .
- On cherche à présent une sous-extension de K^{m_2} telle que:
 $G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$ avec $t \geq 1$ minimal.

Problème:

- On sait donner les équations de l'extension K^{m_2}/K .
- On cherche à présent une sous-extension de K^{m_2} telle que:
 $G_2 \simeq (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^t$ avec $t \geq 1$ minimal.
- Difficulté:
 - Pour K^{m_2} , la stabilité par \mathbb{F}_q est assurée par l'unicité et la maximalité.
 - Comment réduire le système d'équations en conservant la stabilité par $X \rightarrow X + y, y \in \mathbb{F}_q$?

Construction d'une extension "minimale".

Proposition

$q = p^e$ (cas e pair). [MR]

- Soient $p > 2$, $K = \mathbb{F}_q(X)$, avec $q = p^e$, $e = 2s$ et $r = p^s$.
- Soit $L := K(W_0, W_1 \dots W_p)$ l'extension de K paramétrée par:

$$\left\{ \begin{array}{l} W_0^p - W_0 = f_0(X) := aX^{1+r} \quad a \neq 0, a \in \{\gamma \in \mathbb{F}_q, \gamma^r + \gamma = 0\} \\ [W_0, W_p]^p - [W_0, W_p] = [f_0(X), 0] \\ W_i^q - W_i = f_i(X) := X^{ir/p} (X^q - X) \quad \forall i \in \{1, \dots, p-1\} \end{array} \right.$$

- Soit C_L/\mathbb{F}_q la courbe projective lisse de corps de fonctions L .

Proposition

- *L est une extension abélienne de K telle que toutes les places de S se décomposent totalement dans L . En particulier, $L \subset K^{m_2}$.*

Proposition

- L est une extension abélienne de K telle que toutes les places de S se décomposent totalement dans L . En particulier, $L \subset K^{m_2}$.
- $\text{Gal}(L/K)$ satisfait:

$$G_L := \text{Gal}(L/K) \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \quad \text{avec} \quad t = (p-1)e = O(\log_p(g))$$

Proposition

- L est une extension abélienne de K telle que toutes les places de S se décomposent totalement dans L . En particulier, $L \subset K^{m_2}$.
- $\text{Gal}(L/K)$ satisfait:

$$G_L := \text{Gal}(L/K) \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \quad \text{avec} \quad t = (p-1)e = O(\log_p(g))$$

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$ s'étend en un p -groupe $G \subset \text{Aut}_{\mathbb{F}_q}(L)$:

$$0 \longrightarrow G_L \longrightarrow G \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

Proposition

- L est une extension abélienne de K telle que toutes les places de S se décomposent totalement dans L . En particulier, $L \subset K^{m_2}$.
- $\text{Gal}(L/K)$ satisfait:

$$G_L := \text{Gal}(L/K) \simeq \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^t \quad \text{avec} \quad t = (p-1)e = O(\log_p(g))$$

- $\{X \rightarrow X + y, y \in \mathbb{F}_q\}$ s'étend en un p -groupe $G \subset \text{Aut}_{\mathbb{F}_q}(L)$:

$$0 \longrightarrow G_L \longrightarrow G \longrightarrow \mathbb{F}_q \longrightarrow 0.$$

- Pour $e \geq 4$, (C_L, G) est une grosse action avec $G_2 = G_L$.

Grosses actions avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ [Ro1].

Soit (C, G) une grosse action avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.

Soient $L := k(C)$, $k(X) := L^{G_2}$. Alors,

$$L/k(X) : W_i^p - W_i = g_i(X) \in k[X], \quad 1 \leq i \leq n.$$

Grosses actions avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$ [Ro1].

Soit (C, G) une grosse action avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.

Soient $L := k(C)$, $k(X) := L^{G_2}$. Alors,

$$L/k(X) : W_i^p - W_i = g_i(X) \in k[X], \quad 1 \leq i \leq n.$$

Définition

Soit

$$A := \frac{\wp(L) \cap k[X]}{\wp(k[X])} := \langle \overline{g_1(X)}, \dots, \overline{g_n(X)} \rangle$$

A est le \mathbb{F}_p -sev de $k[X]$ dual de G_2 pour le pairing d'Artin-Schreier:

$$\begin{cases} G_2 \times A \rightarrow \mathbb{Z}/p\mathbb{Z} \\ (g, \overline{\wp w}) \rightarrow g(w) - w \end{cases}$$

Action de V sur G_2 .

V agit sur G_2 par conjugaison via la représentation:

$$\phi : \begin{cases} V \rightarrow \text{Aut}(G_2) \simeq \text{GL}_n(\mathbb{F}_p) \\ y \rightarrow \phi(y) \end{cases}$$

avec

$$\phi(y) : \begin{cases} G_2 \rightarrow G_2 \\ g \rightarrow s(y) g s(y)^{-1} \end{cases}$$

où

$$0 \longrightarrow G_2 \longrightarrow G = G_1 \xrightarrow{\pi} V \simeq (\mathbb{Z}/p\mathbb{Z})^v \longrightarrow 0,$$

et s est une section (ensembliste), i.e. $\pi \circ s = id$.

Action duale de V sur A .

De manière duale, V agit sur A par translation:

$$\rho : \begin{cases} V \rightarrow \text{Aut}(A) \simeq \text{GL}_n(\mathbb{F}_p) \\ y \rightarrow \rho(y) \end{cases}$$

avec

$$\rho(y) : \begin{cases} A \rightarrow A \\ \overline{f(X)} \rightarrow \overline{f(X+y)} \end{cases}$$

Action duale de V sur A .

De manière duale, V agit sur A par translation:

$$\rho : \begin{cases} V \rightarrow \text{Aut}(A) \simeq \text{GL}_n(\mathbb{F}_p) \\ y \rightarrow \rho(y) \end{cases}$$

avec

$$\rho(y) : \begin{cases} A \rightarrow A \\ f(X) \rightarrow \overline{f(X+y)} \end{cases}$$

Problème:

- $\text{Im } \rho$ est un sous-groupe unipotent de $\text{GL}_n(\mathbb{F}_p)$.
- On cherche une base de A telle que $\text{Im } \rho$ soit un sous-groupe de matrices triangulaires supérieures avec 1 sur la diagonale.

Choix d'une base adaptée pour A .

Définition

On appelle **base adaptée** de A une base $\{\overline{f_1(X)}, \dots, \overline{f_n(X)}\}$, telle que:

- chaque $f_i \in k[X]$ est réduit modulo $\wp(k[X])$.
- $\forall i \in \{1, \dots, n-1\}, \deg(f_i) \leq \deg(f_{i+1})$
- $\forall (\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_p)^n - \{(0, \dots, 0)\},$
 $\deg(\sum_{i=1}^n \lambda_i \overline{f_i(X)}) = \max_{i=1, \dots, n} \{\deg \lambda_i \overline{f_i(X)}\}.$

Choix d'une base adaptée pour A .

Définition

On appelle **base adaptée** de A une base $\{\overline{f_1(X)}, \dots, \overline{f_n(X)}\}$, telle que:

- chaque $f_i \in k[X]$ est réduit modulo $\wp(k[X])$.
- $\forall i \in \{1, \dots, n-1\}$, $\deg(f_i) \leq \deg(f_{i+1})$
- $\forall (\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_p)^n - \{(0, \dots, 0)\}$,
 $\deg(\sum_{i=1}^n \lambda_i \overline{f_i(X)}) = \max_{i=1, \dots, n} \{\deg \lambda_i \overline{f_i(X)}\}$.

Désormais, $L/k(X) : W_i^p - W_i = f_i(X) \in k[X]$, $1 \leq i \leq n$.

Le genre de $L/k(X)$ est donné par

$$g = \frac{1}{2} (p-1) \sum_{i=1}^n p^{i-1} (\deg(f_i) - 1)$$

Représentation matricielle.

Pour tout y dans V , la matrice de $\rho(y)$ dans la base adaptée s'écrit:

$$L(y) := \begin{pmatrix} 1 & \ell_{1,2}(y) & \ell_{1,3}(y) & \dots & \ell_{1,n}(y) \\ 0 & 1 & \ell_{2,3}(y) & \dots & \ell_{2,n}(y) \\ 0 & 0 & \dots & \dots & \ell_{i,n}(y) \\ 0 & 0 & 0 & 1 & \ell_{n-1,n}(y) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_p).$$

Représentation matricielle.

Pour tout y dans V , la matrice de $\rho(y)$ dans la base adaptée s'écrit:

$$L(y) := \begin{pmatrix} 1 & \ell_{1,2}(y) & \ell_{1,3}(y) & \dots & \ell_{1,n}(y) \\ 0 & 1 & \ell_{2,3}(y) & \dots & \ell_{2,n}(y) \\ 0 & 0 & \dots & \dots & \ell_{i,n}(y) \\ 0 & 0 & 0 & 1 & \ell_{n-1,n}(y) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_p).$$

En d'autres termes,

$$\forall i \in \{1, \dots, n\}, \forall y \in V, f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \quad \text{mod } \mathfrak{p}(k[X]).$$

Remarque

$f_1(X) = XS(X)$ avec $S(X) \in k[X]$ additif.

Remarque

$f_1(X) = XS(X)$ avec $S(X) \in k[X]$ additif.

Preuve:

- $A_1 := \langle \overline{f_1(X)} \rangle$ est stable sous l'action de ρ .

Remarque

$f_1(X) = XS(X)$ avec $S(X) \in k[X]$ additif.

Preuve:

- $A_1 := \langle \overline{f_1(X)} \rangle$ est stable sous l'action de ρ .
- Son orthogonal $H_1 \subset G_2$ est stable par ϕ . Donc H_1 est distingué dans G .

Remarque

$f_1(X) = XS(X)$ avec $S(X) \in k[X]$ additif.

Preuve:

- $A_1 := \langle \overline{f_1(X)} \rangle$ est stable sous l'action de ρ .
- Son orthogonal $H_1 \subset G_2$ est stable par ϕ . Donc H_1 est distingué dans G .
- Par transfert, $(C/H_1, G/H_1)$ est une grosse action de deuxième groupe de ramification cyclique d'ordre p . \square

Remarque

$f_1(X) = XS(X)$ avec $S(X) \in k[X]$ additif.

Preuve:

- $A_1 := \langle \overline{f_1(X)} \rangle$ est stable sous l'action de ρ .
- Son orthogonal $H_1 \subset G_2$ est stable par ϕ . Donc H_1 est distingué dans G .
- Par transfert, $(C/H_1, G/H_1)$ est une grosse action de deuxième groupe de ramification cyclique d'ordre p . \square

Problème: trouver la forme des autres $f_i(X)$ et généraliser cet énoncé.

Définition (Ro1)

Soit $t \geq 1$. On appelle Σ_t le k -sous-espace-vectoriel de $k[X]$ engendré par 1 et les produits d'au plus t polynômes additifs.

Définition (Ro1)

Soit $t \geq 1$. On appelle Σ_t le k -sous-espace-vectoriel de $k[X]$ engendré par 1 et les produits d'au plus t polynômes additifs.

Lemme

- Soit $a \in \mathbb{N}$ d'écriture p -adique: $a = a_0 + a_1 p + \dots + a_\ell p^\ell$, $0 \leq a_i \leq p - 1$.
On note $S_p(a) = a_0 + a_1 + \dots + a_\ell$.
Alors, $X^a \in \Sigma_t \iff S_p(a) \leq t$.

Définition (Ro1)

Soit $t \geq 1$. On appelle Σ_t le k -sous-espace-vectoriel de $k[X]$ engendré par 1 et les produits d'au plus t polynômes additifs.

Lemme

- Soit $a \in \mathbb{N}$ d'écriture p -adique: $a = a_0 + a_1 p + \dots + a_\ell p^\ell$, $0 \leq a_i \leq p - 1$.
On note $S_p(a) = a_0 + a_1 + \dots + a_\ell$.
Alors, $X^a \in \Sigma_t \Leftrightarrow S_p(a) \leq t$.
- Soit $f(X) \in k[X] - \{0\}$ tel que $f(X) = \sum_{a \in \mathbb{N}} c_a(f) X^a$.
On note $d_p(f) := \max_{c_a(f) \neq 0} \{S_p(a)\}$.
Alors, $f \in \Sigma_t \Leftrightarrow d_p(f) \leq t$.

Paramétrisation des grosses actions avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Théorème (Ro1)

Soit (C, G) une grosse action de genre $g \geq 2$ telle que $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.
Alors, $\forall i \in \{1, \dots, n\}, f_i \in \Sigma_{i+1}$.

Paramétrisation des grosses actions avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Théorème (Ro1)

Soit (C, G) une grosse action de genre $g \geq 2$ telle que $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.
Alors, $\forall i \in \{1, \dots, n\}, f_i \in \Sigma_{i+1}$.

Remarque

- Généralisation du cas $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$: $f(X) = XS(X) \in \Sigma_2$.

Paramétrisation des grosses actions avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

Théorème (Ro1)

Soit (C, G) une grosse action de genre $g \geq 2$ telle que $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 1$.
Alors, $\forall i \in \{1, \dots, n\}, f_i \in \Sigma_{i+1}$.

Remarque

- Généralisation du cas $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$: $f(X) = XS(X) \in \Sigma_2$.
- Pour $n \geq 2$, pas de réciproque.

Lemmes préliminaires pour la preuve.

Lemme

(1) Soient $y \in k$ et $f \in k[X]$. On définit l'opérateur:

$$\Delta_y(f) := f(X + y) - f(X)$$

Alors, $\forall t \in \mathbb{N}, \quad \Delta_y(\Sigma_{t+1}) \subset \Sigma_t$.

Lemmes préliminaires pour la preuve.

Lemme

(1) Soient $y \in k$ et $f \in k[X]$. On définit l'opérateur:

$$\Delta_y(f) := f(X + y) - f(X)$$

Alors, $\forall t \in \mathbb{N}, \quad \Delta_y(\Sigma_{t+1}) \subset \Sigma_t$.

Lemme

(2) Soit $g(X) := \sum_{a \in \mathbb{N}} c_a(g) X^a \in \wp(k[X])$.

Alors, pour tout $a_0 \in \mathbb{N} - p\mathbb{N}$,

$$g_{a_0}(X) := \sum_{a \in \{a_0 p^n, n \in \mathbb{N}\}} c_a(g) X^a \in \wp(k[X])$$

En particulier, si p ne divise pas $\deg(g_{a_0})$, alors $g_{a_0} \equiv 0$.

Preuve du théorème: (Récurrence sur i).

- On a vu: $f_1(X) = X\mathcal{S}(X) \in \Sigma_2$.

Preuve du théorème: (Récurrence sur i).

- On a vu: $f_1(X) = X\mathcal{S}(X) \in \Sigma_2$.
- Soit $i \geq 2$. On suppose que $\forall j \in \{1, \dots, i-1\}, f_j \in \Sigma_{j+1}$. D'où

$$\forall y \in V, \Delta_y(f_i) := f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i \quad \text{mod } \mathfrak{P}(k[X]).$$

Preuve du théorème: (Récurrence sur i).

- On a vu: $f_1(X) = X\mathcal{S}(X) \in \Sigma_2$.
- Soit $i \geq 2$. On suppose que $\forall j \in \{1, \dots, i-1\}, f_j \in \Sigma_{j+1}$. D'où

$$\forall y \in V, \Delta_y(f_i) := f_i(X+y) - f_i(X) = \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i \quad \text{mod } \mathfrak{P}(k[X]).$$

- On suppose que $f_i \notin \Sigma_{i+1}$.
Soit X^a le monôme de plus haut degré de f_i qui n'est pas dans Σ_{i+1} .

- *On montre que p divise $a - 1$.*

Sinon, Lemme (2) à $a_0 = a - 1$ et $g(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X)$.

Pour construire $g_{a_0}(X)$, on cherche les $X^{(a-1)p^n}$, $n \geq 0$.

- On montre que p divise $a - 1$.

Sinon, Lemme (2) à $a_0 = a - 1$ et $g(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X)$.

Pour construire $g_{a_0}(X)$, on cherche les $X^{(a-1)p^n}$, $n \geq 0$.

- On cherche d'abord dans $\sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X) \in \Sigma_i$.
 - Comme $X^a \notin \Sigma_{i+1}$, alors $X^{a-1} \notin \Sigma_i$.
 - D'où, $\forall n \geq 0$, $X^{(a-1)p^n} \notin \Sigma_i$.
 - Donc, pas de $X^{(a-1)p^n}$ dans $\sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X) \in \Sigma_i$.

- On montre que p divise $a - 1$.

Sinon, Lemme (2) à $a_0 = a - 1$ et $g(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X)$.

Pour construire $g_{a_0}(X)$, on cherche les $X^{(a-1)p^n}$, $n \geq 0$.

- On cherche d'abord dans $\sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i$.
 - Comme $X^a \notin \Sigma_{i+1}$, alors $X^{a-1} \notin \Sigma_i$.
 - D'où, $\forall n \geq 0$, $X^{(a-1)p^n} \notin \Sigma_i$.
 - Donc, pas de $X^{(a-1)p^n}$ dans $\sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i$.
- Soit X^b un monôme de $f_i(X)$. On cherche les $X^{(a-1)p^n}$ dans $\Delta_y(X^b)$.
 - Si $b < a$, pas de contribution.
 - Si $b = a$, contribution en $ayc_a(f) X^{a-1}$.
 - Si $b > a$, $X^b \in \Sigma_{i+1}$ donc (Lemme 1) $\Delta_y(X^b) \in \Sigma_i$. Pas de contribution.

- On montre que p divise $a - 1$.

Sinon, Lemme (2) à $a_0 = a - 1$ et $g(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X)$.

Pour construire $g_{a_0}(X)$, on cherche les $X^{(a-1)p^n}$, $n \geq 0$.

- On cherche d'abord dans $\sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i$.
 - Comme $X^a \notin \Sigma_{i+1}$, alors $X^{a-1} \notin \Sigma_i$.
 - D'où, $\forall n \geq 0$, $X^{(a-1)p^n} \notin \Sigma_i$.
 - Donc, pas de $X^{(a-1)p^n}$ dans $\sum_{j=1}^{i-1} \ell_{j,i}(y) f_j(X) \in \Sigma_i$.
- Soit X^b un monôme de $f_i(X)$. On cherche les $X^{(a-1)p^n}$ dans $\Delta_y(X^b)$.
 - Si $b < a$, pas de contribution.
 - Si $b = a$, contribution en $ayc_a(f) X^{a-1}$.
 - Si $b > a$, $X^b \in \Sigma_{i+1}$ donc (Lemme 1) $\Delta_y(X^b) \in \Sigma_i$. Pas de contribution.

Conclusion: $g_{a_0}(X) = ayc_a(f) X^{a-1}$

- On montre que p divise $a - 1$.

Sinon, Lemme (2) à $a_0 = a - 1$ et $g(X) := \Delta_y(f_i) - \sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X)$.

Pour construire $g_{a_0}(X)$, on cherche les $X^{(a-1)p^n}$, $n \geq 0$.

- On cherche d'abord dans $\sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X) \in \Sigma_i$.
 - Comme $X^a \notin \Sigma_{i+1}$, alors $X^{a-1} \notin \Sigma_i$.
 - D'où, $\forall n \geq 0$, $X^{(a-1)p^n} \notin \Sigma_i$.
 - Donc, pas de $X^{(a-1)p^n}$ dans $\sum_{j=1}^{i-1} \ell_{j,i}(y)f_j(X) \in \Sigma_i$.
- Soit X^b un monôme de $f_i(X)$. On cherche les $X^{(a-1)p^n}$ dans $\Delta_y(X^b)$.
 - Si $b < a$, pas de contribution.
 - Si $b = a$, contribution en $ayc_a(f)X^{a-1}$.
 - Si $b > a$, $X^b \in \Sigma_{i+1}$ donc (Lemme 1) $\Delta_y(X^b) \in \Sigma_i$. Pas de contribution.

Conclusion: $g_{a_0}(X) = ayc_a(f)X^{a-1} \equiv 0$ (Lemme 2).

Alors $V = \{0\}$. *Contradiction.*

- D'où $a - 1 = \lambda p^t$, avec $t \geq 1$ et $\lambda \geq 2$ premier à p .

- D'où $a - 1 = \lambda p^t$, avec $t \geq 1$ et $\lambda \geq 2$ premier à p .
- On applique le Lemme (2) à $a_0 = a - p^t$ et au même $g(X)$.

- D'où $a - 1 = \lambda p^t$, avec $t \geq 1$ et $\lambda \geq 2$ premier à p .
- On applique le Lemme (2) à $a_0 = a - p^t$ et au même $g(X)$.
 - On trouve $g_{a_0}(X) = T(y)X^{a-p^t} \equiv 0$ avec $T(X) \in k[X]$ de degré p^t .
 - Donc $V \subset Z(T)$ et $|V| \leq p^t$.
 - Cela entraîne: $\frac{|G|}{g} = \frac{|G_2||V|}{g} \leq \frac{2p}{p-1}$. *Contradiction.* \square

Cas particulier: chaque $f_i \in \Sigma_{i+1} - \Sigma_i$.

Définition (Ro1)

Soit G un groupe. On définit une suite croissante de sous-groupes caractéristiques de G comme suit:

$$\Lambda_0(G) = \{e\}$$

$$\forall i \geq 1, \frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} = Z\left(\frac{G}{\Lambda_{i-1}(G)}\right) \cap D\left(\frac{G}{\Lambda_{i-1}(G)}\right).$$

Cas particulier: chaque $f_i \in \Sigma_{i+1} - \Sigma_i$.

Théorème (Ro1)

Soit (C, G) une grosse action de genre $g \geq 2$ avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 2$.

Alors, les assertions suivantes sont équivalentes:

- $\forall i \in \{1, \dots, n\}$, $f_i \in \Sigma_{i+1} - \Sigma_i$.
- $\forall i \in \{1, \dots, n\}$, $\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} \simeq \mathbb{Z}/p\mathbb{Z}$.
- $\forall i \in \{1, \dots, n-1\}$, $\ell_{i,i+1}$ est une \mathbb{F}_p -forme linéaire non nulle.

Cas particulier: chaque $f_i \in \Sigma_{i+1} - \Sigma_i$.

Théorème (Ro1)

Soit (C, G) une grosse action de genre $g \geq 2$ avec $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^n$, $n \geq 2$.
Alors, les assertions suivantes sont équivalentes:

- $\forall i \in \{1, \dots, n\}$, $f_i \in \Sigma_{i+1} - \Sigma_i$.
- $\forall i \in \{1, \dots, n\}$, $\frac{\Lambda_i(G)}{\Lambda_{i-1}(G)} \simeq \mathbb{Z}/p\mathbb{Z}$.
- $\forall i \in \{1, \dots, n-1\}$, $\ell_{i,i+1}$ est une \mathbb{F}_p -forme linéaire non nulle.

Alors,

- $n \leq p-1$.
- $\forall i \in \{1, \dots, n\}$, $\deg(f_i) = 1 + ip^s$.
- $\dim_{\mathbb{F}_p} V = s+1$.
- La suite $\Lambda_i(G)$ coïncide avec la suite de ramification supérieure de G_2 :
 $\forall i \in \{0, \dots, n\}$, $\Lambda_{n-i}(G) = (G_2)^{v_i}$.

Exemples.

On construit ici une famille de grosses actions vérifiant le théorème précédent.

Exemples.

On construit ici une famille de grosses actions vérifiant le théorème précédent.

Proposition (Ro2)

- Soit $p \geq 3$, $S(X) := \wp(X) = X^p - X$.
- Soit $L/k(X)$ l'extension paramétrée par:

$$\begin{cases} W_i^p - W_i = g_i(X) := \frac{S(X)^{i+1}}{(i+1)!} = \frac{(X^p - X)^{i+1}}{(i+1)!} & \forall i \in \{1, \dots, p-2\} \\ W_{p-1}^p - W_{p-1} = g_{p-1}(X) \end{cases}$$

où $g_{p-1}(X) \in k[X]$ est la réduction mod p du polynôme:

$$\frac{1}{p!} ((X^p - X)^p - X^{p^2} + X^p) \in W(k)[X].$$

- Soit C/k la courbe projective lisse de corps de fonctions L .

Proposition

Soit $S(X) := X^p - X$, $Q(X) := S(X)^p - S(X)$ et $V := Z(Q)$.

- $\{X \rightarrow X + y, y \in V\}$ s'étend en un p -groupe $G \subset \text{Aut}_k(C)$:

$$0 \longrightarrow \text{Gal}(L/k(X)) \simeq (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow G \longrightarrow V \longrightarrow 0.$$

Proposition

Soit $S(X) := X^p - X$, $Q(X) := S(X)^p - S(X)$ et $V := Z(Q)$.

- $\{X \rightarrow X + y, y \in V\}$ s'étend en un p -groupe $G \subset \text{Aut}_k(C)$:

$$0 \longrightarrow \text{Gal}(L/k(X)) \simeq (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow G \longrightarrow V \longrightarrow 0.$$

- (C, G) est une grosse action avec $G_2 = \text{Gal}(L/k(X)) \simeq (\mathbb{Z}/p\mathbb{Z})^n$.
- Cette grosse action vérifie: " $\forall i, f_i \in \Sigma_{i+1} - \Sigma_i$ " avec $s = 1$, i.e. $\dim_{\mathbb{F}_p} V = s + 1 = 2$.

Idée: Pour tout $i \geq 1$ et tout $y \in V = Z(\mathcal{S}(X)^p - \mathcal{S}(X))$,

$$\begin{aligned} g_i(X+y) - g_i(X) &= \frac{1}{(i+1)!} \{(\mathcal{S}(X) + \mathcal{S}(y))^{i+1} - \mathcal{S}(X)^{i+1}\} \\ &= \sum_{j=1}^{i-1} \frac{\mathcal{S}(y)^{i-j}}{(i-j)!} \frac{\mathcal{S}(X)^{j+1}}{(j+1)!} + \frac{\mathcal{S}(y)^i}{i!} \mathcal{S}(X) + \frac{\mathcal{S}(y)^{i+1}}{(i+1)!} \end{aligned}$$

Idée: Pour tout $i \geq 1$ et tout $y \in V = Z(S(X)^p - S(X))$,

$$\begin{aligned} g_i(X+y) - g_i(X) &= \frac{1}{(i+1)!} \{(S(X) + S(y))^{i+1} - S(X)^{i+1}\} \\ &= \sum_{j=1}^{i-1} \frac{S(y)^{i-j}}{(i-j)!} \frac{S(X)^{j+1}}{(j+1)!} + \frac{S(y)^i}{i!} S(X) + \frac{S(y)^{i+1}}{(i+1)!} \end{aligned}$$

Comme $S(y) \in \mathbb{F}_p$ et $S(X) = X^p - X$,

$$\begin{aligned} g_i(X+y) - g_i(X) &= \sum_{j=1}^{i-1} \frac{S(y)^{i-j}}{(i-j)!} g_j(X) + \wp\left(\frac{S(y)^i}{i!} X\right) + g_i(y) \\ &= \sum_{j=1}^{i-1} \ell_{j,i}(y) g_j(X) \quad \text{mod} \quad \wp(k[X]) \end{aligned}$$

avec

$$\ell_{j,i}(y) := \frac{S(y)^{i-j}}{(i-j)!} \in \mathbb{F}_p$$

D'où,

$$L(y) = \exp(S(y)J)$$

avec

$$J := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Par changement de base, on atteint $s \geq 1$ quelconque.

Par changement de base, on atteint $s \geq 1$ quelconque.

Proposition (Ro1)

Soit (C, G) la grosse action précédente. On considère le changement de base:

$$\begin{array}{ccc}
 C & \longleftarrow & \tilde{C} \\
 \downarrow & & \downarrow \\
 C/G_2 \simeq \mathbb{P}_k^1 & \xleftarrow{S_0} & \mathbb{P}_k^1
 \end{array}$$

où S_0 est un polynôme additif séparable de $k[X]$ de degré p^{s_0} .

Par changement de base, on atteint $s \geq 1$ quelconque.

Proposition (Ro1)

Soit (C, G) la grosse action précédente. On considère le changement de base:

$$\begin{array}{ccc} C & \longleftarrow & \tilde{C} \\ \downarrow & & \downarrow \\ C/G_2 \simeq \mathbb{P}_k^1 & \xleftarrow{S_0} & \mathbb{P}_k^1 \end{array}$$

où S_0 est un polynôme additif séparable de $k[X]$ de degré p^{s_0} .

- La courbe $\tilde{C} := C \times_{\mathbb{P}_k^1} \mathbb{P}_k^1$ a pour genre $g_{\tilde{C}} = p^{s_0} g_C$.
- $\tilde{C} \rightarrow C/G$ est un revêtement galoisien de groupe $\tilde{G} \simeq G \times (\mathbb{Z}/p\mathbb{Z})^{s_0}$.
- Donc $\frac{|G|}{g_C} = \frac{|\tilde{G}|}{g_{\tilde{C}}}$ et (\tilde{C}, \tilde{G}) est une grosse action avec $\tilde{G}_2 \simeq G_2 \times \{0\}$.
- Cette grosse action vérifie " $\forall i, f_i \in \Sigma_{i+1} - \Sigma_i$ " avec $s = s_0 + 1$.

Familles universelles.

- Les résultats précédents facilitent la paramétrisation des grosses actions (C, G) vérifiant " $\forall i, f_i \in \Sigma_{i+1} - \Sigma_i$ ".
- On en donne ici une illustration avec $p = 5$ et $s = 1$.

Paramétrisation de la famille universelle pour $p = 5$ et $s = 1$.

- $n = 2$ [Ro1]

$$\begin{aligned} f_1(X) &= X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2 \\ f_2(X) &= b_{11}^5X^{11} + 4b_{11}^{25}X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5}X^3 + b_1X \end{aligned}$$

avec $b_{11} \in k^\times$ et $b_1 \in k$ algébriquement indépendants.

Paramétrisation de la famille universelle pour $p = 5$ et $s = 1$.

- $n = 2$ [Ro1]

$$f_1(X) = X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2$$

$$f_2(X) = b_{11}^5X^{11} + 4b_{11}^{25}X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5}X^3 + b_1X$$

avec $b_{11} \in k^\times$ et $b_1 \in k$ algébriquement indépendants.

- L'espace des paramètres est un ouvert de l'espace affine \mathbb{A}_k^2 . Il est donc irréductible: G est unique à isomorphisme près.

Paramétrisation de la famille universelle pour $p = 5$ et $s = 1$.

- $n = 2$ [Ro1]

$$f_1(X) = X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2$$

$$f_2(X) = b_{11}^5X^{11} + 4b_{11}^{25}X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5}X^3 + b_1X$$

avec $b_{11} \in k^\times$ et $b_1 \in k$ algébriquement indépendants.

- L'espace des paramètres est un ouvert de l'espace affine \mathbb{A}_k^2 . Il est donc irréductible: G est unique à isomorphisme près.
- Deux courbes $C(b_{11}, b_1)$ et $C(b'_{11}, b'_1)$ sont isomorphes si et seulement si:

$$\left(\frac{b'_{11}}{b_{11}}\right)^{24} = 1 \quad \text{et} \quad b'_1 = \pm \frac{b'_{11}}{b_{11}} b_1$$

- $n = 3$ [Ro1]

$$f_1(X) = X^6 + 2(b_{11}^{25} + b_{11})b_{11}^{-5}X^2$$

$$f_2(X) = b_{11}^5 X^{11} + 4b_{11}^{25} X^7 + 2(b_{11}^{50} - b_{11}^2)b_{11}^{-5} X^3 + 2(c_6 - c_6^5)b_{11}^{-5} X$$

$$f_3(X) = 4b_{11}^{10} X^{16} + 4b_{11}^{30} X^{12} + c_{11}^5 X^{11} + 4b_{11}^{50} X^8 + 4c_{11}^{25} X^7$$

$$+ c_6^5 X^6 + 4(b_{11}^{75} + b_{11}^3)b_{11}^{-5} X^4$$

$$+ \{(b_{11}^{25} + b_{11})c_{11}b_{11}^{-5} + 2(b_{11}^{25} + b_{11})^2 c_{11}^5 b_{11}^{-10}\} X^3$$

$$+ 2(c_6^5 b_{11}^{25} + c_6 b_{11})b_{11}^{-5} X^2 + c_1 X$$

avec $b_{11} \in k^\times$, $c_6 \in k$ et $c_1 \in k$ algébriquement indépendants
et $c_{11} \in k$ tel que:

$$c_{11}^{25} + 4(b_{11}^{25} + b_{11})b_{11}^{-5}c_{11}^5 + c_{11} = 0 \quad (\Leftrightarrow \quad c_{11}^5 \in V)$$

avec $b_{11} \in k^\times$, $c_6 \in k$ et $c_1 \in k$ algébriquement indépendants
et $c_{11} \in k$ tel que:

$$c_{11}^{25} + 4(b_{11}^{25} + b_{11})b_{11}^{-5}c_{11}^5 + c_{11} = 0 \quad (\Leftrightarrow \quad c_{11}^5 \in V)$$

Remarque

L'espace des paramètres n 'est pas connexe.

On trouve deux modèles de groupes G non isomorphes, et chacun est réalisé.

Éléments pour la classification des grosses actions [Ro2].

Remarque

Soit (C, G) une grosse action.

Soit \mathcal{S} un p -Sylow de $\text{Aut}_k(C)$ tel que $G \subset \mathcal{S}$.

Eléments pour la classification des grosses actions [Ro2].

Remarque

Soit (C, G) une grosse action.

Soit \mathcal{S} un p -Sylow de $\text{Aut}_k(C)$ tel que $G \subset \mathcal{S}$.

- Alors, (C, \mathcal{S}) est une grosse action.
- Si $\frac{|G|}{g^2} \geq M > 0$, (C, \mathcal{S}) vérifie la même condition.

Conclusion: on peut supposer que G est un p -Sylow de $\text{Aut}_k(C)$.

Proposition (Ro2)

*Soit C/k une courbe algébrique projective lisse connexe de genre $g \geq 2$.
Soit $G \subset \text{Aut}_k(C)$ tel que (C, G) soit une grosse action.*

Proposition (Ro2)

Soit C/k une courbe algébrique projective lisse connexe de genre $g \geq 2$.
Soit $G \subset \text{Aut}_k(C)$ tel que (C, G) soit une grosse action.

- Alors, il existe un point $\infty \in C$ tel que $G \subset A_{\infty,1} := (\text{Aut}_k(C))_{\infty,1}$ et

$$\begin{array}{ccccccc}
 0 & \longrightarrow & D(A_{\infty,1}) = A_{\infty,2} & \longrightarrow & A_{\infty,1} & \xrightarrow{\pi} & W \longrightarrow 0 \\
 & & \parallel & & \cup & & \cup \\
 0 & \longrightarrow & D(G) = G_{\infty,2} & \longrightarrow & G = G_{\infty,1} & \xrightarrow{\pi} & V \longrightarrow 0
 \end{array}$$

Proposition

- $A_{\infty,1}$ est un p -sous-groupe de Sylow de $\text{Aut}_k(C)$.

Proposition

- $A_{\infty,1}$ est un p -sous-groupe de Sylow de $\text{Aut}_k(C)$.
- Ce p -Sylow est **unique** (et par suite ∞) sauf lorsque C est isomorphe à

Proposition

- $A_{\infty,1}$ est un p -sous-groupe de Sylow de $\text{Aut}_k(C)$.
- Ce p -Sylow est **unique** (et par suite ∞) sauf lorsque C est isomorphe à

- La courbe hermitienne:

$$C_H: \quad W^q + W = X^{1+q} \quad \text{avec } p \geq 2, q = p^s, s \geq 1.$$

- La courbe de Deligne-Lusztig liée au groupe de Suzuki:

$$C_S: \quad W^q + W = X^{q_0} (X^q + X) \quad \text{avec } p = 2, q_0 = 2^s, s \geq 1 \text{ et } q = 2^{2s+1}.$$

- La courbe de Deligne-Lusztig liée au groupe de Ree:

$$C_R: \quad W_1^q - W_1 = X^{q_0} (X^q + X) \quad \text{et} \quad W_2^q - W_2 = X^{2q_0} (X^q + X)$$

$$\text{avec } p = 3, q_0 = 3^s, s \geq 1 \text{ and } q = 3^{2s+1}.$$

Conclusion: Dans notre classification,

- on se cible sur le(s) p -Sylow: $A_{\infty,1}$.
- on discute suivant l'ordre de son deuxième groupe de ramification.

Conclusion: Dans notre classification,

- on se cible sur le(s) p -Sylow: $A_{\infty,1}$.
- on discute suivant l'ordre de son deuxième groupe de ramification.

En effet...

Proposition (Ro2)

Soit (C, G) une grosse action telle que $\frac{|G|}{g^2} \geq M > 0$.

Alors $|G_2|$ ne prend qu'un nombre fini de valeurs.

Question: Qu'en est-il pour g , $|V|$ et par suite $\frac{|G|}{g}$?

Résultats de finitude.

Remarque

Si (C, G) est une grosse action, $\text{Fratt}(G_2) \subset [G_2, G]$.

Résultats de finitude.

Remarque

Si (C, G) est une grosse action, $\text{Fratt}(G_2) \subset [G_2, G]$.

Proposition (Ro2)

Soit (C, G) une grosse action telle que $\frac{|G|}{g^2} \geq M > 0$.

Résultats de finitude.

Remarque

Si (C, G) est une grosse action, $\text{Fratt}(G_2) \subset [G_2, G]$.

Proposition (Ro2)

Soit (C, G) une grosse action telle que $\frac{|G|}{g^2} \geq M > 0$.

- Si $\text{Fratt}(G_2) \subsetneq [G_2, G]$,
 - $g, |V|$ et $\frac{|G|}{g}$ prennent un nombre fini de valeurs.

Résultats de finitude.

Remarque

Si (C, G) est une grosse action, $\text{Fratt}(G_2) \subset [G_2, G]$.

Proposition (Ro2)

Soit (C, G) une grosse action telle que $\frac{|G|}{g^2} \geq M > 0$.

- Si $\text{Fratt}(G_2) \subsetneq [G_2, G]$,
 - $g, |V|$ et $\frac{|G|}{g}$ prennent un nombre fini de valeurs.
- Si $\text{Fratt}(G_2) = [G_2, G]$,
 - $\frac{|G|}{g}$ n'est pas toujours borné (voir $WP - W = XS(X)$ et $G = A_{\infty,1}$).
 - si $\text{Fratt}(G_2) = [G_2, G] = \{e\}$, $\frac{|G|}{g^2}$ prend un nombre fini de valeurs.
 - si $\text{Fratt}(G_2) = [G_2, G] \neq \{e\}$ et si $p > 2$, G_2 est non abélien.

