# $p$- groupes d'automorphismes en caractéristique $p > 0$

M. Matignon[1]

[1]Laboratoire A2X Bordeaux

Journées Deschamps-Maugeais
Novembre 2006

# Plan

# Plan

# Plan

## Introduction

Monodromie et groupes d'automorphismes

## Actions de $p$-groupes sur une courbe $C$ avec $g(C) \geq 2$

Revêtements $p$ -cycliques de la droite affi ne

$p$-groupes d'automorphismes en genre $\geq 2$

Grosses actions (I)

Surfaces de Riemann

Corps de classes de rayon

Grosses actions (II)

Courbes maximales

## Références

# Monodromie et groupes d'automorphismes

- $R$ un AVD strictement hensélien d'inégale caractéristique $(0, p)$.
  $K := \mathrm{Fr} R$ ; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  $\pi$ une uniformisante.
  $k := R/\pi R$.
  $C/K$ courbe projective lisse, $g(C) \geq 2$.
- $C$ a potentiellement bonne réduction sur $K$ si il existe $L/K$ (finie) telle que $C \times_K L$ a un modèle lisse sur $O_L$. Alors
- Il existe une extension minimale $L/K$ ayant cette propriété, elle est galoisienne : c'est la **monodromie**.
- $\mathrm{Gal}(L/K)$ est le **groupe de monodromie**.
- Son $p$-sous-groupe de Sylow est le **groupe de monodromie sauvage**.

# Monodromie et groupes d'automorphismes





- $R$ un AVD strictement hensélien d'inégale caractéristique $(0, p)$.
  $K := \mathrm{Fr}R$ ; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  $\pi$ une uniformisante.
  $k := R/\pi R$.
  $C/K$ courbe projective lisse, $g(C) \geq 2$.
- $C$ a potentiellement bonne réduction sur $K$ si il existe $L/K$ (finie) telle que $C \times_K L$ a un modèle lisse sur $O_L$. Alors
- Il existe une extension minimale $L/K$ ayant cette propriété, elle est galoisienne : c'est la **monodromie**.
- $\mathrm{Gal}(L/K)$ est le **groupe de monodromie**.
- Son $p$-sous-groupe de Sylow est le **groupe de monodromie sauvage**.

# Monodromie et groupes d'automorphismes

- $R$ un AVD strictement hensélien d'inégale caractéristique $(0, p)$.
  $K := \mathrm{Fr}R$ ; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  $\pi$ une uniformisante.
  $k := R/\pi R$.
  $C/K$ courbe projective lisse, $g(C) \geq 2$.
- $C$ a potentiellement bonne réduction sur $K$ si il existe $L/K$ (finie) telle que $C \times_K L$ a un modèle lisse sur $O_L$. Alors
- Il existe une extension minimale $L/K$ ayant cette propriété, elle est galoisienne : c'est la **monodromie**.
- $\mathrm{Gal}(L/K)$ est le **groupe de monodromie**.
- Son $p$-sous-groupe de Sylow est le **groupe de monodromie sauvage**.

# Monodromie et groupes d'automorphismes

- $R$ un AVD strictement hensélien d'inégale caractéristique $(0, p)$.
  $K := \mathrm{Fr}R$ ; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  $\pi$ une uniformisante.
  $k := R/\pi R$.
  $C/K$ courbe projective lisse, $g(C) \geq 2$.
- $C$ a potentiellement bonne réduction sur $K$ si il existe $L/K$ (finie) telle que $C \times_K L$ a un modèle lisse sur $O_L$. Alors
- Il existe une extension minimale $L/K$ ayant cette propriété, elle est galoisienne : c'est la **monodromie**.
- $\mathrm{Gal}(L/K)$ est le **groupe de monodromie**.
- Son $p$-sous-groupe de Sylow est le **groupe de monodromie sauvage**.

# Monodromie et groupes d'automorphismes

- $R$ un AVD strictement hensélien d'inégale caractéristique $(0, p)$.
  $K := \mathrm{Fr}R$ ; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  $\pi$ une uniformisante.
  $k := R/\pi R$.
  $C/K$ courbe projective lisse, $g(C) \geq 2$.
- $C$ a potentiellement bonne réduction sur $K$ si il existe $L/K$ (finie) telle que $C \times_K L$ a un modèle lisse sur $O_L$. Alors
- Il existe une extension minimale $L/K$ ayant cette propriété, elle est galoisienne : c'est la **monodromie**.
- $\mathrm{Gal}(L/K)$ est le **groupe de monodromie**.
- Son $p$-sous-groupe de Sylow est le **groupe de monodromie sauvage**.

- Le changement de base $C \times_K K^{alg}$ induit alors un homomorphisme $\varphi : \mathrm{Gal}(K^{alg}/K) \to \mathrm{Aut}_k C_s$ où $C_s$ est la fi bre spéciale du modèle lisse sur $L$ et $L = (K^{alg})^{\ker \varphi}$.
- Soit $\ell$ un nombre premier, alors $n_\ell := v_\ell(|\mathrm{Gal}(L/K)|) \leq v_\ell(|\mathrm{Aut}_k C_s|)$
- Si $\ell \notin \{2, p\}$, alors $\ell^{n_\ell}$ est majoré par l'ordre maximal d'un sous-groupe $\ell$-cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ (donc unipotent), i.e. $\ell^{n_\ell} \leq 2g$.
- Si $p > 2$, on a $n_p \leq \inf_{\ell \neq 2,p} v_p(|\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = a + [a/p] + \ldots$ où $a = [\frac{2g}{p-1}]$.

  Ainsi, on obtient pour $|\mathrm{Aut}_k C_s|$ une borne exponentielle en $g$, d'où l'intérêt des bornes polynômiales en $g$ dues à Stichtenoth et Singh (73).

- Le changement de base $C \times_K K^{alg}$ induit alors un homomorphisme $\varphi : \mathrm{Gal}(K^{alg}/K) \to \mathrm{Aut}_k C_s$ où $C_s$ est la fi bre spéciale du modèle lisse sur $L$ et $L = (K^{alg})^{\ker \varphi}$.
- Soit $\ell$ un nombre premier, alors $n_\ell := v_\ell(|\mathrm{Gal}(L/K)|) \leq v_\ell(|\mathrm{Aut}_k C_s|)$
- Si $\ell \notin \{2, p\}$, alors $\ell^{n_\ell}$ est majoré par l'ordre maximal d'un sous-groupe $\ell$-cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ (donc unipotent), i.e. $\ell^{n_\ell} \leq 2g$.
- Si $p > 2$, on a $n_p \leq \inf_{\ell \neq 2,p} v_p(|\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = a + [a/p] + ...$ où $a = [\frac{2g}{p-1}]$.
  Ainsi, on obtient pour $|\mathrm{Aut}_k C_s|$ une borne exponentielle en $g$, d'où l'intérêt des bornes polynômiales en $g$ dues à Stichtenoth et Singh (73).

- Le changement de base $C \times_K K^{alg}$ induit alors un homomorphisme $\varphi : \mathrm{Gal}(K^{alg}/K) \to \mathrm{Aut}_k C_s$ où $C_s$ est la fi bre spéciale du modèle lisse sur $L$ et $L = (K^{alg})^{\ker \varphi}$.
- Soit $\ell$ un nombre premier, alors $n_\ell := v_\ell(|\mathrm{Gal}(L/K)|) \leq v_\ell(|\mathrm{Aut}_k C_s|)$
- Si $\ell \notin \{2, p\}$, alors $\ell^{n_\ell}$ est majoré par l'ordre maximal d'un sous-groupe $\ell$-cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ (donc unipotent), i.e. $\ell^{n_\ell} \leq 2g$.
- Si $p > 2$, on a $n_p \leq \inf_{\ell \neq 2,p} v_p(|\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = a + [a/p] + \ldots$ où $a = [\frac{2g}{p-1}]$.
  Ainsi, on obtient pour $|\mathrm{Aut}_k C_s|$ une borne exponentielle en $g$, d'où l'intérêt des bornes polynômiales en $g$ dues à Stichtenoth et Singh (73).

- Le changement de base $C \times_K K^{alg}$ induit alors un homomorphisme $\varphi : \mathrm{Gal}(K^{alg}/K) \to \mathrm{Aut}_k C_s$ où $C_s$ est la fi bre spéciale du modèle lisse sur $L$ et $L = (K^{alg})^{\ker \varphi}$.
- Soit $\ell$ un nombre premier, alors $n_\ell := v_\ell(|\mathrm{Gal}(L/K)|) \leq v_\ell(|\mathrm{Aut}_k C_s|)$
- Si $\ell \notin \{2, p\}$, alors $\ell^{n_\ell}$ est majoré par l'ordre maximal d'un sous-groupe $\ell$-cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ (donc unipotent), i.e. $\ell^{n_\ell} \leq 2g$.
- Si $p > 2$, on a $n_p \leq \inf_{\ell \neq 2,p} v_p(|\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = a + [a/p] + ...$ où $a = [\frac{2g}{p-1}]$.

  Ainsi, on obtient pour $|\mathrm{Aut}_k C_s|$ une borne exponentielle en $g$, d'où l'intérêt des bornes polynômiales en $g$ dues à Stichtenoth et Singh (73).

- **Programme.** (Vague) Etudier les maxima (locaux) de monodromie sauvage en inégale caractéristique i.e. pour un genre donné et un type de réduction stable donné + autres conditions, déterminer les groupes de monodromie sauvage maximaux. Que peut-on dire sur la fi ltration de ramifi cation ?
- **Exemple.** Si $g = 2$ et inégale caractéristique $(0, 2)$, $Q_8 * D_8$ est un maximum pour la bonne réduction potentielle ; $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ pour une réduction stable avec 2 composantes elliptiques.
- **Etape initiale.** Etudier les “grosses actions” de $p$-groupes en caractéristique $p > 0$ un peu comme en caractéristique 0 on caractérise les actions qui atteignent la borne d'Hurwitz i.e. $|G| = 84(g-1)$.

- **Programme.** (Vague) Etudier les maxima (locaux) de monodromie sauvage en inégale caractéristique i.e. pour un genre donné et un type de réduction stable donné + autres conditions, déterminer les groupes de monodromie sauvage maximaux. Que peut-on dire sur la filtration de ramification ?
- **Exemple.** Si $g = 2$ et inégale caractéristique $(0, 2)$, $Q_8 * D_8$ est un maximum pour la bonne réduction potentielle ; $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ pour une réduction stable avec 2 composantes elliptiques.
- **Etape initiale.** Etudier les "grosses actions" de $p$-groupes en caractéristique $p > 0$ un peu comme en caractéristique 0 on caractérise les actions qui atteignent la borne d'Hurwitz i.e. $|G| = 84(g - 1)$.

- **Programme.** (Vague) Etudier les maxima (locaux) de monodromie sauvage en inégale caractéristique i.e. pour un genre donné et un type de réduction stable donné + autres conditions, déterminer les groupes de monodromie sauvage maximaux. Que peut-on dire sur la fi ltration de ramifi cation ?
- **Exemple.** Si $g = 2$ et inégale caractéristique $(0, 2)$, $Q_8 * D_8$ est un maximum pour la bonne réduction potentielle ; $(Q_8 \times Q_8) \rtimes \mathbb{Z}/2\mathbb{Z}$ pour une réduction stable avec 2 composantes elliptiques.
- **Etape initiale.** Etudier les “grosses actions” de $p$-groupes en caractéristique $p > 0$ un peu comme en caractéristique 0 on caractérise les actions qui atteignent la borne d'Hurwitz i.e. $|G| = 84(g - 1)$.

# Revêtements $p$-cycliques de la droite affi ne

$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,deg $f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m | 1 + p$.

# Revêtements $p$-cycliques de la droite affi ne

$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,deg $f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m | 1 + p$.

# Revêtements $p$-cycliques de la droite affi ne





$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,deg $f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m|1 + p$.

# Revêtements $p$-cycliques de la droite affi ne

$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,$\deg f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m|1+p$.

# Revêtements $p$-cycliques de la droite affi ne

$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,$\deg f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m|1+p$.

# Revêtements $p$-cycliques de la droite affi ne

$k$ **est un corps algébriquement clos de car.** $p > 0$

- $f(X) \in Xk[X]$ ,$\deg f = m > 1$, premier à $p$, unitaire
- $C_f : W^p - W = f(X)$, $\infty$ l'unique point de $C_f$ au-dessus de $X = \infty$ et $z$ un paramètre local, $g := g(C_f) = \frac{p-1}{2}(m-1)$.
- $G_\infty(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid \sigma(\infty) = \infty\}$
- $G_{\infty,1}(f) := \{\sigma \in \mathrm{Aut}_k C_f \mid v_\infty(\sigma(z) - z) \geq 2\}$ , le $p$-Sylow.
- ([St],73) Soit $g(C_f) \geq 2$, alors $G_{\infty,1}(f)$ est un $p$-Sylow de $\mathrm{Aut}_k C_f$.
- Il est normal, sauf si $f(X) = X^m$ avec $m|1 + p$.

- Soit $\rho(X) = X$, $\rho(w) = W + 1$, alors $< \rho >= G_{\infty,2} \subset Z(G_{\infty,1})$.
- $0 \to < \rho > \to G_{\infty,1} \to V \to 0$ où $V = \{\tau_y | \, \tau_y(X) = X + y, \; y \in k\}$.
- $V$ est l'ensemble des solutions de l'équation fonctionnelle $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$ $P(X,y) \in Xk[X]$.
- On construit algorithmiquement un polynôme additif séparable $\mathrm{Ad}_f(Y)$ avec $Z(\mathrm{Ad}_f(Y)) = V$.

- Soit $\rho(X) = X$, $\rho(w) = W + 1$, alors $< \rho >= G_{\infty,2} \subset Z(G_{\infty,1})$.
- $0 \to < \rho > \to G_{\infty,1} \to V \to 0$ où $V = \{\tau_y | \ \tau_y(X) = X + y, \ y \in k\}$.
- $V$ est l'ensemble des solutions de l'équation fonctionnelle $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$ $P(X,y) \in Xk[X]$.
- On construit algorithmiquement un polynôme additif séparable $\mathrm{Ad}_f(Y)$ avec $Z(\mathrm{Ad}_f(Y)) = V$.

- Soit $\rho(X) = X$, $\rho(w) = W + 1$, alors $< \rho >= G_{\infty,2} \subset Z(G_{\infty,1})$.
- $0 \to < \rho > \to G_{\infty,1} \to V \to 0$ où $V = \{\tau_y |\ \tau_y(X) = X + y,\ y \in k\}$.
- $V$ est l'ensemble des solutions de l'équation fonctionnelle $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$ $P(X,y) \in Xk[X]$.
- On construit algorithmiquement un polynôme additif séparable $\mathrm{Ad}_f(Y)$ avec $Z(\mathrm{Ad}_f(Y)) = V$.

- Soit $\rho(X) = X$, $\rho(w) = W + 1$, alors $< \rho >= G_{\infty,2} \subset Z(G_{\infty,1})$.
- $0 \to < \rho > \to G_{\infty,1} \to V \to 0$ où $V = \{\tau_y |\ \tau_y(X) = X + y,\ y \in k\}$.
- $V$ est l'ensemble des solutions de l'équation fonctionnelle $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$ $P(X,y) \in Xk[X]$.
- On construit algorithmiquement un polynôme additif séparable $\mathrm{Ad}_f(Y)$ avec $Z(\mathrm{Ad}_f(Y)) = V$.

Si $m-1=\ell p^s$ avec $(\ell,p)=1$ et $s\geq 0$

- ([St] 73) $|G_{\infty,1}|=p\deg(\mathrm{Ad}_f)\leq p(m-1)^2$ i.e.

$$\frac{|G_{\infty,1}|}{g^2}\leq\frac{4p}{(p-1)^2}$$

(égalité pour $f(X)=X^{1+p^s}$)

# $p$-groupes d'automorphismes en genre $\geq 2$



- ([St 73],[Na 87]) Soit $C/k$ une courbe de genre $g \geq 2$ et $\{\mathrm{Id}\} \neq G \subset \mathrm{Aut}_k(C)$ un $p$-groupe, alors $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$

# Grosses actions (I)

- **Définition.** Soit $(C, G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C, G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

# Grosses actions (I)

- **Définition.** Soit $(C, G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C, G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

# Grosses actions (I)

- **Définition.** Soit $(C,G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C,G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

# Grosses actions (I)

- **Définition.** Soit $(C, G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C, G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

# Grosses actions (I)

- **Définition.** Soit $(C, G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C, G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

# Grosses actions (I)

- **Définition.** Soit $(C, G)$ avec $G \subset \mathrm{Aut}_k C$ un $p$-groupe.
  $(C, G)$ est une **grosse action** si :
  (N) $g_C > 0$ et $\frac{|G|}{g_C} > \frac{2p}{p-1}$.
- Alors ([Na 87], il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ étale et $G = G_{\infty,1}$.
  - $G_{\infty,2} \neq G_{\infty,1}$ et $C/G_{\infty,2} \simeq \mathbb{P}^1_k$.
  - Ainsi, $G_{\infty,1}/G_{\infty,2}$ opère comme un groupe de translations de la droite affi ne $C/G_{\infty,2} - \{\infty\}$
- Puisque $\frac{|G|}{g^2} \leq \frac{4p}{(p-1)^2}$, nous allons cribler les grosses actions par $\frac{|G|}{g^2}$.

On suppose que $(C, G)$ satisfait (N). On note $G_i := G_{\infty,i}$.

- Soit $i_0$ avec $G_2 = G_3 = .... = G_{i_0} \supsetneq G_{i_0+1}$. Alors $g_{(C/G_{i_0+1})} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$.
- Supposons que $0 < M \leq \frac{|G|}{g_C^2}$, alors
  - $|G_{i_0+1}| \leq \frac{1}{M} \frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M} \frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
  - Puisque la suite $\frac{p^n}{(p^n-1)^2}$ est décroissante et que $|G_{i_0+1}| \in p^{\mathbb{N}}$, on en déduit des bornes sur $|G_2/G_{i_0+1}|$, $|G_{i_0+1}|$ et donc sur $|G_2|$.

On suppose que $(C, G)$ satisfait (N). On note $G_i := G_{\infty,i}$.

- Soit $i_0$ avec $G_2 = G_3 = .... = G_{i_0} \supsetneq G_{i_0+1}$. Alors $g_{(C/G_{i_0+1})} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$.

- Supposons que $0 < M \leq \frac{|G|}{g_C^2}$, alors
  - $|G_{i_0+1}| \leq \frac{1}{M} \frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M} \frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
  - Puisque la suite $\frac{p^n}{(p^n-1)^2}$ est décroissante et que $|G_{i_0+1}| \in p^{\mathbb{N}}$, on en déduit des bornes sur $|G_2/G_{i_0+1}|$, $|G_{i_0+1}|$ et donc sur $|G_2|$.

On suppose que $(C, G)$ satisfait (N). On note $G_i := G_{\infty,i}$.

- Soit $i_0$ avec $G_2 = G_3 = .... = G_{i_0} \supsetneq G_{i_0+1}$. Alors $g_{(C/G_{i_0+1})} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$.
- Supposons que $0 < M \leq \frac{|G|}{g_C^2}$, alors
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
  - Puisque la suite $\frac{p^n}{(p^n-1)^2}$ est décroissante et que $|G_{i_0+1}| \in p^{\mathbb{N}}$, on en déduit des bornes sur $|G_2/G_{i_0+1}|$, $|G_{i_0+1}|$ et donc sur $|G_2|$.

On suppose que $(C, G)$ satisfait (N). On note $G_i := G_{\infty,i}$.

- Soit $i_0$ avec $G_2 = G_3 = .... = G_{i_0} \supsetneq G_{i_0+1}$. Alors $g_{(C/G_{i_0+1})} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$.
- Supposons que $0 < M \leq \frac{|G|}{g_C^2}$, alors
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
  - Puisque la suite $\frac{p^n}{(p^n-1)^2}$ est décroissante et que $|G_{i_0+1}| \in p^{\mathbb{N}}$, on en déduit des bornes sur $|G_2/G_{i_0+1}|$, $|G_{i_0+1}|$ et donc sur $|G_2|$.

# $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$

- **Théorème.**([Le-Ma 1]) Soit $f(X) \in Xk[X]$ avec $\deg f = m > 1$, premier à $p$, $C_f : W^p - W = f(X)$ et $G_i := G_{\infty,i}$. Si $\frac{|G_1|}{g(C_f)} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$ où $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ est un polynôme additif avec $\deg f = 1 + p^s$.
- $\mathrm{Ad}_f(Y) := F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
- On a la suite exacte : $0 \to G_2 = Z(G_1) = G_1' = Z/p\mathbb{Z} \to G_1 \to V \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$.
- Le groupe $G_1$ est le groupe extraspécial de cardinal $p^{2s+1}$, d'exposant $p$ si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.

# $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$

- **Théorème.**([Le-Ma 1]) Soit $f(X) \in Xk[X]$ avec $\deg f = m > 1$, premier à $p$, $C_f : W^p - W = f(X)$ et $G_i := G_{\infty,i}$. Si $\frac{|G_1|}{g(C_f)} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$ où $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ est un polynôme additif avec $\deg f = 1 + p^s$.
- $\mathrm{Ad}_f(Y) := F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
- On a la suite exacte : $0 \to G_2 = Z(G_1) = G_1' = Z/p\mathbb{Z} \to G_1 \to V \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$.
- Le groupe $G_1$ est le groupe extraspécial de cardinal $p^{2s+1}$, d'exposant $p$ si $p > 2$ et du type $Q_8 * D_8 * ... * D_8$ si $p = 2$.

# $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$





- **Théorème.**([Le-Ma 1]) Soit $f(X) \in Xk[X]$ avec $\deg f = m > 1$, premier à $p$, $C_f : W^p - W = f(X)$ et $G_i := G_{\infty,i}$. Si $\frac{|G_1|}{g(C_f)} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$ où $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ est un polynôme additif avec $\deg f = 1 + p^s$.
- $\mathrm{Ad}_f(Y) := F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
- On a la suite exacte : $0 \to G_2 = Z(G_1) = G_1' = Z/p\mathbb{Z} \to G_1 \to V \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$.
- Le groupe $G_1$ est le groupe extraspécial de cardinal $p^{2s+1}$, d'exposant $p$ si $p > 2$ et du type $Q_8 * D_8 * ... * D_8$ si $p = 2$.

# $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$

- **Théorème.**([Le-Ma 1]) Soit $f(X) \in Xk[X]$ avec $\deg f = m > 1$, premier à $p$, $C_f : W^p - W = f(X)$ et $G_i := G_{\infty,i}$. Si $\frac{|G_1|}{g(C_f)} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$ où $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ est un polynôme additif avec $\deg f = 1 + p^s$.
- $\mathrm{Ad}_f(Y) := F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
- On a la suite exacte : $0 \to G_2 = Z(G_1) = G_1' = Z/p\mathbb{Z} \to G_1 \to V \simeq (\mathbb{Z}/p\mathbb{Z})^{2s} \to 0$.
- Le groupe $G_1$ est le groupe extraspécial de cardinal $p^{2s+1}$, d'exposant $p$ si $p > 2$ et du type $Q_8 * D_8 * ... * D_8$ si $p = 2$.

# Passage aux groupes quotients de la condition (N)

- Soit $(C, G)$ vérifi ant (N). Si $H \lhd G$ et si $g(C/H) > 0$, alors $(C/H, G/H)$ satisfait (N).
- Soit $H \lhd G$ et $H$ d'indice $p$ dans $G_2$ ($H$ existe), alors $(C/H, G/H)$ satisfait (N),
- $(G/H)_2 = (G_2/H) \simeq \mathbb{Z}/p\mathbb{Z}$.
- Il suit du théorème précédent qu'il existe $\Sigma(F) \in k\{F\}$, $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_f$.

# Passage aux groupes quotients de la condition (N)

- Soit $(C, G)$ vérifi ant (N). Si $H \lhd G$ et si $g(C/H) > 0$, alors $(C/H, G/H)$ satisfait (N).
- Soit $H \lhd G$ et $H$ d'indice $p$ dans $G_2$ ($H$ existe), alors $(C/H, G/H)$ satisfait (N),
- $(G/H)_2 = (G_2/H) \simeq \mathbb{Z}/p\mathbb{Z}$.
- Il suit du théorème précédent qu'il existe $\Sigma(F) \in k\{F\}$, $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_f$.

# Passage aux groupes quotients de la condition (N)

- Soit $(C, G)$ vérifi ant (N). Si $H \lhd G$ et si $g(C/H) > 0$, alors $(C/H, G/H)$ satisfait (N).
- Soit $H \lhd G$ et $H$ d'indice $p$ dans $G_2$ ($H$ existe), alors $(C/H, G/H)$ satisfait (N),
- $(G/H)_2 = (G_2/H) \simeq \mathbb{Z}/p\mathbb{Z}$.
- Il suit du théorème précédent qu'il existe $\Sigma(F) \in k\{F\}$, $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_f$.

# Passage aux groupes quotients de la condition (N)

- Soit $(C, G)$ vérifi ant (N). Si $H \lhd G$ et si $g(C/H) > 0$, alors $(C/H, G/H)$ satisfait (N).
- Soit $H \lhd G$ et $H$ d'indice $p$ dans $G_2$ ($H$ existe), alors $(C/H, G/H)$ satisfait (N),
- $(G/H)_2 = (G_2/H) \simeq \mathbb{Z}/p\mathbb{Z}$.
- Il suit du théorème précédent qu'il existe $\Sigma(F) \in k\{F\}$, $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_f$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (I)

- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, W_1, \ldots, W_t)$ et $\wp(W_1, \ldots, W_t) = (f_1(X), f_2(X), \ldots, f_t(X)) \in (k[X])^t$
- $f_1(X), \ldots, f_t(X)$ sont $\mathbb{F}_p$-libres $\mod \wp(k[X])$.
- L'extension de groupes $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induit une représentation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$.
- Elle est duale de l'opération par translation de $V$ : $(v \in V) \times (f_1(X), f_2(X), \ldots, f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), \ldots, f_t(X+v))$ $\mod \wp(k[X])^t$
- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G_1)$. Dans ce cas $f_i(X) = c_i X + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (I)

- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, W_1, \ldots, W_t)$ et $\wp(W_1, \ldots, W_t) = (f_1(X), f_2(X), \ldots, f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ sont $\mathbb{F}_p$-libres $\mod \wp(k[X])$.
- L'extension de groupes $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induit une représentation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$.
- Elle est duale de l'opération par translation de $V$ : $(v \in V) \times (f_1(X), f_2(X), \ldots, f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), \ldots, f_t(X+v)) \mod \wp(k[X])^t$
- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G_1)$. Dans ce cas $f_i(X) = c_i X + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.

# $G_2$ abélien de type $(p, p, ..., p)$ (I)

- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, W_1, ..., W_t)$ et $\wp(W_1, ..., W_t) = (f_1(X), f_2(X), ..., f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ sont $\mathbb{F}_p$-libres $\mod \wp(k[X])$.
- L'extension de groupes $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induit une représentation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$.
- Elle est duale de l'opération par translation de $V$ : $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v))$ $\mod \wp(k[X])^t$
- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G_1)$. Dans ce cas $f_i(X) = c_i X + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.

# $G_2$ abélien de type $(p, p, ..., p)$ (I)

- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, W_1, ..., W_t)$ et $\wp(W_1, ..., W_t) = (f_1(X), f_2(X), ..., f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ sont $\mathbb{F}_p$-libres $\mod \wp(k[X])$.
- L'extension de groupes $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induit une représentation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$.
- Elle est duale de l'opération par translation de $V$ : $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v))$ $\mod \wp(k[X])^t$
- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G_1)$. Dans ce cas $f_i(X) = c_i X + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.

# $G_2$ abélien de type $(p, p, ..., p)$ (I)

- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, W_1, ..., W_t)$ et $\wp(W_1, ..., W_t) = (f_1(X), f_2(X), ..., f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ sont $\mathbb{F}_p$-libres $\mod \wp(k[X])$.
- L'extension de groupes $0 \to G_2 \to G_1 \to V = (\mathbb{Z}/p\mathbb{Z})^v \to 0$ induit une représentation $\rho : V \to \mathrm{Gl}_t(\mathbb{F}_p)$.
- Elle est duale de l'opération par translation de $V$ : $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v))$ $\mod \wp(k[X])^t$
- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G_1)$. Dans ce cas $f_i(X) = c_i X + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p-y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p-y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a
    $f_2(X+y) = \frac{2(y^p-y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p-y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2p^2$ et $g = \frac{p-1}{2}(p+2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p - y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p-y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p - y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \dots, p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p - y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (II)





- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X+y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p - y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, ..., p)$ (II)

- Pour $p > 2$, nous donnons un exemple avec $\mathrm{Im}\rho \neq \mathrm{Id}$.
  - Soit $f_1 := X(\alpha F)(X) = \alpha X^{1+p}$ avec $\alpha^p + \alpha = 0$ ; alors $\mathrm{Ad}_{f_1} = Y^{p^2} - Y$.
  - Soit $f_2 := X^{1+2p} - X^{2+p}$, alors
  - Si $y \in Z(\mathrm{Ad}_{f_1}) = \mathbb{F}_{p^2}$ on a $f_2(X + y) = \frac{2(y^p - y)}{\alpha} f_1(X) + f_2(X) + \wp P_2$.
  - $y \to \frac{2(y^p - y)}{\alpha}$ est une forme linéaire sur $\mathbb{F}_{p^2}$ non nulle et à valeurs dans $\mathbb{F}_p$.
  - $|G| = p^2 p^2$ et $g = \frac{p-1}{2}(p + 2p^2)$.
  - $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
  - $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

# $G_2$ abélien de type $(p, p, \ldots, p)$ (III)

- **Théorème.** Pour tout $M > 0$, l'ensemble des valeurs $\frac{|G|}{g_C^2} > M$, pour $(C, G)$ une grosse action avec $G_2$ abélien d'exposant $p$, est fi ni.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut}C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut}C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# $G_2$ non abélien

- **Théorème.** Soit $(C, G)$ une grosse action. Supposons que $G_2$ n'est pas abélien, alors $G_2 = G'$.
- Idée : Si $G' \neq G_2$, il existe $H$ distingué dans $G$ avec $G' \subset H \subset G_2$ et $[G_2 : H] = p$. $(C/H, G/H)$ satisfait la condition (N).
- $C/H : W^p - W = f := X\Sigma(F)(X)$, $\deg(f) = 1 + p^S$.
- $(\mathrm{Aut} C/H)_{\infty,1} := E$ est extraspécial d'ordre $p^{2s+1}$.
- $G/H$ est abélien et normal dans $E$.
- (Huppert) $|G/H| \leq p^{s+1}$ et donc $|G/H|/g(C/H) \leq \frac{2p^{s+1}}{(p-1)p^s} = \frac{2p}{p-1}$ ;contradiction.
- On déduit le corollaire suivant de ([Su 86] 4.21 p. 75).
- **Corollaire.** Soit $(C, G)$ une grosse action. Si $|G_2| = p^3$, alors $G_2$ est abélien.

# Surfaces de Riemann

- En caractéristique 0, un analogue des grosses actions est donné par les actions d'un groupe fi ni $G$ sur une surface de Riemann compacte $C$ avec $g_C \geq 2$ telle que $|G| = 84(g_C - 1)$ (courbes d'Hurwitz).
- On connaît la quartique de Klein ($G \simeq PSL_2(\mathbb{F}_7)$)
- On peut aussi citer la courbe de Fricke-Macbeath de genre 7 ($G \simeq PSL_2(\mathbb{F}_8)$).
- ([Mc],61) Soit $C$ une courbe d'Hurwitz de genre $g_C$. Soit $n > 1$ et $C_n$ le revêtement galoisien non ramifi é maximal de groupe un groupe abélien d'exposant $n$. Le groupe de Galois de $C_n/C$ est $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. Il suit de l'unicité de $C_n$ que les $k$-automorphismes de $C$ admettent $n^{2g}$ prolongements à $C_n$. Ainsi, $g_{C_n} - 1 = n^{2g}(g_C - 1)$ et $n^{2g}|\mathrm{Aut}_k C| \leq |\mathrm{Aut}_k C_n|$, d'où $|\mathrm{Aut}_k C_n| \geq 84(g_{C_n} - 1)$ ; $C_n$ est d'Hurwitz.

# Surfaces de Riemann

- En caractéristique 0, un analogue des grosses actions est donné par les actions d'un groupe fi ni $G$ sur une surface de Riemann compacte $C$ avec $g_C \geq 2$ telle que $|G| = 84(g_C - 1)$ (courbes d'Hurwitz).
- On connaît la quartique de Klein ($G \simeq PSL_2(\mathbb{F}_7)$)
- On peut aussi citer la courbe de Fricke-Macbeath de genre 7 ($G \simeq PSL_2(\mathbb{F}_8)$).
- ([Mc],61) Soit $C$ une courbe d'Hurwitz de genre $g_C$. Soit $n > 1$ et $C_n$ le revêtement galoisien non ramifi é maximal de groupe un groupe abélien d'exposant $n$. Le groupe de Galois de $C_n/C$ est $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. Il suit de l'unicité de $C_n$ que les $k$-automorphismes de $C$ admettent $n^{2g}$ prolongements à $C_n$. Ainsi, $g_{C_n} - 1 = n^{2g}(g_C - 1)$ et $n^{2g}|\mathrm{Aut}_k C| \leq |\mathrm{Aut}_k C_n|$, d'où $|\mathrm{Aut}_k C_n| \geq 84(g_{C_n} - 1)$ ; $C_n$ est d'Hurwitz.

# Surfaces de Riemann

- En caractéristique 0, un analogue des grosses actions est donné par les actions d'un groupe fi ni $G$ sur une surface de Riemann compacte $C$ avec $g_C \geq 2$ telle que $|G| = 84(g_C - 1)$ (courbes d'Hurwitz).
- On connaît la quartique de Klein ($G \simeq PSL_2(\mathbb{F}_7)$)
- On peut aussi citer la courbe de Fricke-Macbeath de genre 7 ($G \simeq PSL_2(\mathbb{F}_8)$).
- ([Mc],61) Soit $C$ une courbe d'Hurwitz de genre $g_C$. Soit $n > 1$ et $C_n$ le revêtement galoisien non ramifi é maximal de groupe un groupe abélien d'exposant $n$. Le groupe de Galois de $C_n/C$ est $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. Il suit de l'unicité de $C_n$ que les $k$-automorphismes de $C$ admettent $n^{2g}$ prolongements à $C_n$. Ainsi, $g_{C_n} - 1 = n^{2g}(g_C - 1)$ et $n^{2g}|\mathrm{Aut}_k C| \leq |\mathrm{Aut}_k C_n|$, d'où $|\mathrm{Aut}_k C_n| \geq 84(g_{C_n} - 1)$ ; $C_n$ est d'Hurwitz.

# Surfaces de Riemann

- En caractéristique 0, un analogue des grosses actions est donné par les actions d'un groupe fi ni $G$ sur une surface de Riemann compacte $C$ avec $g_C \geq 2$ telle que $|G| = 84(g_C - 1)$ (courbes d'Hurwitz).
- On connaît la quartique de Klein ($G \simeq PSL_2(\mathbb{F}_7)$)
- On peut aussi citer la courbe de Fricke-Macbeath de genre 7 ($G \simeq PSL_2(\mathbb{F}_8)$).
- ([Mc],61) Soit $C$ une courbe d'Hurwitz de genre $g_C$. Soit $n > 1$ et $C_n$ le revêtement galoisien non ramifi é maximal de groupe un groupe abélien d'exposant $n$. Le groupe de Galois de $C_n/C$ est $(\mathbb{Z}/n\mathbb{Z})^{2g_C}$. Il suit de l'unicité de $C_n$ que les $k$-automorphismes de $C$ admettent $n^{2g}$ prolongements à $C_n$. Ainsi, $g_{C_n} - 1 = n^{2g}(g_C - 1)$ et $n^{2g}|\mathrm{Aut}_k C| \leq |\mathrm{Aut}_k C_n|$, d'où $|\mathrm{Aut}_k C_n| \geq 84(g_{C_n} - 1)$ ; $C_n$ est d'Hurwitz.

# Corps de classes de rayon

- Si $(C, G)$ satisfait (N) (une grosse action en car.$p > 0$) alors $C \to C/G$ est un revêtement étale de la droite affi ne de groupe un $p$-groupe ; il suit que l'invariant de Hasse-Witt de $C$ est nul ; ainsi, un raisonnement analogue à celui de la car. zéro nécessite d'accepter de la ramifi cation. L'analogie se fait avec les corps de classes de rayon des corps de fonctions sur un corps fi ni.
- Soit $K := \mathbb{F}_q(X)$ avec $q = p^e$, $S$ l'ensemble des places fi nies $(X - v)$, $v \in \mathbb{F}_q$, et $m \in \mathbb{N}$. On fi xe $K^{alg}$, une clôture algébrique. Soit $K_S^m \subset K^{alg}$, la plus grande extension abélienne de $K$ de conducteur $\leq m\infty$ et telle que les places de $S$ sont complètement décomposées.

# Corps de classes de rayon

- Si $(C, G)$ satisfait (N) (une grosse action en car.$p > 0$) alors $C \to C/G$ est un revêtement étale de la droite affi ne de groupe un $p$-groupe ; il suit que l'invariant de Hasse-Witt de $C$ est nul ; ainsi, un raisonnement analogue à celui de la car. zéro nécessite d'accepter de la ramifi cation. L'analogie se fait avec les corps de classes de rayon des corps de fonctions sur un corps fi ni.
- Soit $K := \mathbb{F}_q(X)$ avec $q = p^e$, $S$ l'ensemble des places fi nies $(X - v)$, $v \in \mathbb{F}_q$, et $m \in \mathbb{N}$. On fi xe $K^{alg}$, une clôture algébrique. Soit $K_S^m \subset K^{alg}$, la plus grande extension abélienne de $K$ de conducteur $\leq m\infty$ et telle que les places de $S$ sont complètement décomposées.

- ([Lauter (99), Auer (00)]) $\mathbb{F}_q$ est le corps des constantes de $K_S^m$ et $G_S^m := \mathrm{Gal}(K_S^m/K) \simeq (1 + T\mathbb{F}_q[[T]])/ < 1 + T^m\mathbb{F}_q[[T]], 1 - vT, v \in \mathbb{F}_q >$, est un $p$-groupe.
- Soit $C_m/\mathbb{F}_q$ la courbe projective lisse de corps de fonctions $K_S^m$. Les translations $X \to X + v,\ v \in \mathbb{F}_q$ laissent invariants $S$ et $\infty$ ; elles se prolongent en $\mathbb{F}_q$-automorphismes de $K_S^m$. Ainsi, on obtient une action sur $C_m$ d'un $p$-groupe $G_1(m)$ avec $0 \to G_S^m \to G_1(m) \to \mathbb{F}_q \to 0$
- ([Auer]) Si $n_m := |G_S^m|$, alors $g_{C_m} = 1 + n_m(-1 + m/2) - (1/2)\sum_{0 \leq j \leq m-1} n_j \leq n_m(-1 + m/2)$

- ([Lauter (99), Auer (00)]) $\mathbb{F}_q$ est le corps des constantes de $K_S^m$ et $G_S^m := \mathrm{Gal}(K_S^m/K) \simeq (1 + T\mathbb{F}_q[[T]])/ < 1 + T^m\mathbb{F}_q[[T]], 1 - vT, v \in \mathbb{F}_q >$, est un $p$-groupe.
- Soit $C_m/\mathbb{F}_q$ la courbe projective lisse de corps de fonctions $K_S^m$. Les translations $X \to X + v,\ v \in \mathbb{F}_q$ laissent invariants $S$ et $\infty$ ; elles se prolongent en $\mathbb{F}_q$-automorphismes de $K_S^m$. Ainsi, on obtient une action sur $C_m$ d'un $p$-groupe $G_1(m)$ avec $0 \to G_S^m \to G_1(m) \to \mathbb{F}_q \to 0$
- ([Auer]) Si $n_m := |G_S^m|$, alors $g_{C_m} = 1 + n_m(-1 + m/2) - (1/2)\sum_{0\leq j\leq m-1} n_j \leq n_m(-1 + m/2)$

- ([Lauter (99), Auer (00)]) $\mathbb{F}_q$ est le corps des constantes de $K_S^m$ et $G_S^m := \mathrm{Gal}(K_S^m/K) \simeq (1+T\mathbb{F}_q[[T]])/ < 1+T^m\mathbb{F}_q[[T]], 1-vT, v \in \mathbb{F}_q >$, est un $p$-groupe.
- Soit $C_m/\mathbb{F}_q$ la courbe projective lisse de corps de fonctions $K_S^m$. Les translations $X \to X+v,\ v \in \mathbb{F}_q$ laissent invariants $S$ et $\infty$ ; elles se prolongent en $\mathbb{F}_q$-automorphismes de $K_S^m$. Ainsi, on obtient une action sur $C_m$ d'un $p$-groupe $G_1(m)$ avec $0 \to G_S^m \to G_1(m) \to \mathbb{F}_q \to 0$
- ([Auer]) Si $n_m := |G_S^m|$, alors $g_{C_m} = 1 + n_m(-1+m/2) - (1/2)\sum_{0\leq j\leq m-1} n_j \leq n_m(-1+m/2)$

- $\frac{|G_1(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. C'est une “grosse action” dès que $\frac{q}{-1+m/2} > \frac{2p}{p-1}$ (on a $G_2 = G_S^m$).
- Soit $N_q := |C_m(\mathbb{F}_q)|$, alors $N_q = 1 + |G_1(m)|$, ainsi le quotient $\frac{|G_1(m)|}{g_{C_m}} \sim \frac{N_q}{g_{C_m}}$.
- ([Lauter]) Si $q = p^e$,$m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ est le plus petit conducteur $m$ avec $G_S^m$ d'exposant $> p$.
- Si $e > 2$, $(C_{m_2}, G_S^{m_2})$ satisfait (N) et $G_2$ est abélien d'exposant $p^2$.

- $\frac{|G_1(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. C'est une “grosse action” dès que $\frac{q}{-1+m/2} > \frac{2p}{p-1}$ (on a $G_2 = G_S^m$).
- Soit $N_q := |C_m(\mathbb{F}_q)|$, alors $N_q = 1 + |G_1(m)|$, ainsi le quotient $\frac{|G_1(m)|}{g_{C_m}} \sim \frac{N_q}{g_{C_m}}$.
- ([Lauter]) Si $q = p^e$,$m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ est le plus petit conducteur $m$ avec $G_S^m$ d'exposant $> p$.
- Si $e > 2$, $(C_{m_2}, G_S^{m_2})$ satisfait (N) et $G_2$ est abélien d'exposant $p^2$.

- $\frac{|G_1(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. C'est une "grosse action" dès que $\frac{q}{-1+m/2} > \frac{2p}{p-1}$ (on a $G_2 = G_S^m$).
- Soit $N_q := |C_m(\mathbb{F}_q)|$, alors $N_q = 1 + |G_1(m)|$, ainsi le quotient $\frac{|G_1(m)|}{g_{C_m}} \sim \frac{N_q}{g_{C_m}}$.
- ([Lauter]) Si $q = p^e$,$m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ est le plus petit conducteur $m$ avec $G_S^m$ d'exposant $> p$.
- Si $e > 2$, $(C_{m_2}, G_S^{m_2})$ satisfait (N) et $G_2$ est abélien d'exposant $p^2$.

- $\frac{|G_1(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. C'est une "grosse action" dès que $\frac{q}{-1+m/2} > \frac{2p}{p-1}$ (on a $G_2 = G_S^m$).
- Soit $N_q := |C_m(\mathbb{F}_q)|$, alors $N_q = 1 + |G_1(m)|$, ainsi le quotient $\frac{|G_1(m)|}{g_{C_m}} \sim \frac{N_q}{g_{C_m}}$.
- ([Lauter]) Si $q = p^e, m_2 := p^{\lceil e/2 \rceil + 1} + p + 1$ est le plus petit conducteur $m$ avec $G_S^m$ d'exposant $> p$.
- Si $e > 2$, $(C_{m_2}, G_S^{m_2})$ satisfait (N) et $G_2$ est abélien d'exposant $p^2$.

# Grosses actions (II)





Soit $k$ quelconque et $(C, G)$ une action qui satisfait (N).

- Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.
- Plus généralement on espère pour $G_2$ abélien d'exposant $p^e$ avec $e \geq 2$, une minoration du $p$-rang de $G_2$ en $O(log(g_C))$. C'est le cas dans la situation précédente i.e. $(C, G) = (C_{m_2}, G_S^{m_2})$ ([M. Rocher, thèse en préparation]).

# Grosses actions (II)

Soit $k$ quelconque et $(C, G)$ une action qui satisfait (N).

- Si $G_2 \simeq \mathbb{Z}/p^n\mathbb{Z}$, alors $n = 1$.
- Plus généralement on espère pour $G_2$ abélien d'exposant $p^e$ avec $e \geq 2$, une minoration du $p$-rang de $G_2$ en $O(log(g_C))$. C'est le cas dans la situation précédente i.e. $(C, G) = (C_{m_2}, G_S^{m_2})$ ([M. Rocher, thèse en préparation]).

# Courbes maximales I

- **Théorème.** Si $\frac{|G|}{g_C^2} \geq \frac{4}{(p-1)^2}$, alors il existe $\Sigma(F) \in k\{F\}$ et $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C \simeq C_f$.
  De plus, il n'y a que deux possibilités pour $G$ :
  - $\frac{|G|}{g_C^2} = \frac{4p}{(p-1)^2}$ et $G = G_{\infty,1}(f)$ ou bien
  - $\frac{|G|}{g_C^2} = \frac{4}{(p-1)^2}$ et $G \subset G_{\infty,1}(f)$ est d'indice $p$.

# Courbes maximales I

- **Théorème.** Si $\frac{|G|}{g_C^2} \geq \frac{4}{(p-1)^2}$, alors il existe $\Sigma(F) \in k\{F\}$ et $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C \simeq C_f$.
  De plus, il n'y a que deux possibilités pour $G$ :
  - $\frac{|G|}{g_C^2} = \frac{4p}{(p-1)^2}$ et $G = G_{\infty,1}(f)$ ou bien
  - $\frac{|G|}{g_C^2} = \frac{4}{(p-1)^2}$ et $G \subset G_{\infty,1}(f)$ est d'indice $p$.

# Courbes maximales I

- **Théorème.** Si $\frac{|G|}{g_C^2} \geq \frac{4}{(p-1)^2}$, alors il existe $\Sigma(F) \in k\{F\}$ et $f = cX + X\Sigma(F)(X) \in k[X]$ avec $C \simeq C_f$.
  De plus, il n'y a que deux possibilités pour $G$ :
  - $\frac{|G|}{g_C^2} = \frac{4p}{(p-1)^2}$ et $G = G_{\infty,1}(f)$ ou bien
  - $\frac{|G|}{g_C^2} = \frac{4}{(p-1)^2}$ et $G \subset G_{\infty,1}(f)$ est d'indice $p$.

# Courbes maximales II

On suppose toujours que que $(C, G)$ satisfait (N).

- On peut pousser la “classifi cation ” des grosses actions jusqu’à la condition $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$.
- On montre d’abord que $|G_2|$ divise $p^3$.
- La condition $G_2 = G_1'$ implique que $G_2$ est abélien.
- Par des calculs de ramifi cation dans les extensions abéliennes de groupes $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ ([Marshall ] 71) on montre que $G_2$ est d’exposant $p$ (on a déjà vu que $G_2$ est cyclique ssi $G_2 = \mathbb{Z}/p\mathbb{Z}$). Le théorème précédent montre la fi nitude de l’ensemble des $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$ pour les grosses actions. La liste exhaustive de ces actions est un travail en cours de M. Rocher.

# Courbes maximales II





On suppose toujours que que $(C, G)$ satisfait (N).

- On peut pousser la "classifi cation " des grosses actions jusqu'à la condition $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$.
- On montre d'abord que $|G_2|$ divise $p^3$.
- La condition $G_2 = G_1'$ implique que $G_2$ est abélien.
- Par des calculs de ramifi cation dans les extensions abéliennes de groupes $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ ([Marshall ] 71) on montre que $G_2$ est d'exposant $p$ (on a déjà vu que $G_2$ est cyclique ssi $G_2 = \mathbb{Z}/p\mathbb{Z}$). Le théorème précédent montre la fi nitude de l'ensemble des $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$ pour les grosses actions. La liste exhaustive de ces actions est un travail en cours de M. Rocher.

# Courbes maximales II

On suppose toujours que que $(C, G)$ satisfait (N).

- On peut pousser la “classifi cation ” des grosses actions jusqu’à la condition $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$.
- On montre d’abord que $|G_2|$ divise $p^3$.
- La condition $G_2 = G_1'$ implique que $G_2$ est abélien.
- Par des calculs de ramifi cation dans les extensions abéliennes de groupes $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ ([Marshall ] 71) on montre que $G_2$ est d’exposant $p$ (on a déjà vu que $G_2$ est cyclique ssi $G_2 = \mathbb{Z}/p\mathbb{Z}$). Le théorème précédent montre la fi nitude de l’ensemble des $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$ pour les grosses actions. La liste exhaustive de ces actions est un travail en cours de M. Rocher.

# Courbes maximales II

On suppose toujours que que $(C, G)$ satisfait (N).

- On peut pousser la “classifi cation ” des grosses actions jusqu’à la condition $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$.
- On montre d’abord que $|G_2|$ divise $p^3$.
- La condition $G_2 = G_1'$ implique que $G_2$ est abélien.
- Par des calculs de ramifi cation dans les extensions abéliennes de groupes $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ ([Marshall ] 71) on montre que $G_2$ est d’exposant $p$ (on a déjà vu que $G_2$ est cyclique ssi $G_2 = \mathbb{Z}/p\mathbb{Z}$). Le théorème précédent montre la fi nitude de l’ensemble des $\frac{|G|}{g_C^2} \geq \frac{4}{(p^2-1)^2}$ pour les grosses actions. La liste exhaustive de ces actions est un travail en cours de M. Rocher.

R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. 95 (2000), no. 2, 97–122.

M. Conder, *Hurwitz groups : a brief survey*, Bull. Amer. Math. Soc. (N.S.) 23 (1990), no. 2, 359–370.

N. Elkies, *The Klein quartic in number theory*, The eightfold way, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.

K. Lauter, *A formula for constructing curves over finite fields with many rational points*, J. Number Theory 74 (1999), no. 1, 56–72.

- C. Lehr, M. Matignon, *Automorphism groups for p-cyclic covers of the affine line*, Compos. Math. 141 (2005), no. 5, 1213–1237.
- C. Lehr, M. Matignon,*Automorphisms of curves and stable reduction*, in Problems from the workshop on "Automorphisms of Curves" (Leiden, August, 2004), edited by G. Cornelissen and F.Oort, Rend. Sem. Math. Univ. Padova. Vol. 113 (2005), 151-158.
- C. Lehr, M. Matignon, *Wild monodromy and automorphisms of curves* , Duke math. J. 135, no. 3 (2006), 569-586.
- M. Matignon, *Curves with a big p-group action*, En préparation.
- A. M. Macbeath, *On a theorem of Hurwitz*, Proc. Glasgow Math. Assoc. 5 1961 90–96 (1961).
- A. M. Macbeath, *On a curve of genus 7*, Proc.

M. Marshall, *Ramification groups of abelian local field extensions*, Canad. J. Math. 23 (1971) 271–281.

S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. 303, 595-607 (1987).

M. Raynaud, *p-groupes et réduction semi-stable des courbes*, The Grothendieck Festschrift, Vol.3, Basel-Boston-Berlin : Birkhäuser (1990).

B. Singh, *On the group of automorphisms of function field of genus at least two*, J. Pure Appl. Algebra 4 (1974), 205–229.

H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I, II.* Arch. Math. 24 (1973) 527–544 , 615–631.

M. Suzuki, *Group theory II*, Grundlehren der Mathematischen Wissenschaften 248